JBoss Enterprise Application Platform 6.2

Guide de développement

À utiliser dans Red Hat JBoss Enterprise Application Platform 6

Last Updated: 2017-10-26

JBoss Enterprise Application Platform 6.2 Guide de développement

À utiliser dans Red Hat JBoss Enterprise Application Platform 6

Sande Gilda

Eamon Logue
elogue@redhat.com

Darrin Mison

Red Hat Content Services

David Ryan

Misty Stanley-Jones
misty@redhat.com

Tom Wells
twells@redhat.com

Notice légale

Copyright © 2014 Red Hat, Inc..

This document is licensed by Red Hat under the Creative Commons Attribution-ShareAlike 3.0 Unported License. If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Résumé

Cet ouvrage procure des références et des exemples pour les développeurs Java EE 6 qui utilisent Red Hat JBoss Enterprise Application Platform 6, et inclut des correctifs publiés.

Table des matières

PREFACE **12**

CHAPITRE 1. INTRODUCTION AU DÉVELOPPEMENT D'APPLICATIONS **13**
1.1. INTRODUCTION 13
1.1.1. Red Hat JBoss Enterprise Application Platform 6 (JBoss EAP 6) 13
1.2. PRÉ-REQUIS 13
1.2.1. Familiarisez vous avec Java Enterprise Edition 6 13
1.2.1.1. Les Profils EE 6 13
1.2.1.2. Web Profil de Java Enterprise Edition 6 13
1.2.1.3. Java Enterprise Edition 6 Full Profile 14
1.2.2. Les modules et le système de chargement de la nouvelle classe modulaire de JBoss EAP 6. 15
1.2.2.1. Modules 15
1.2.2.2. Chargement des classes et Modules 16
1.3. INSTALLER L'ENVIRONNEMENT DE DÉVELOPPEMENT 16
1.3.1. Télécharger et installer JBoss Developer Studio 16
1.3.1.1. Installation de JBoss Developer Studio 16
1.3.1.2. Téléchargez JBoss Developer Studio 5 17
1.3.1.3. Installer JBoss Developer Studio 5 17
1.3.1.4. Démarrer JBoss Developer Studio 17
1.3.1.5. Ajouter le serveur de JBoss EAP 6 au JBoss Developer Studio 18
1.4. EXÉCUTER VOTRE PREMIÈRE APPLICATION 24
1.4.1. Remplacer l'application web Welcome par défaut 24
1.4.2. Télécharger les exemples de codes Quickstart 25
1.4.2.1. Accès aux Quickstarts 25
1.4.3. Exécuter les Quickstarts 26
1.4.3.1. Exécuter les Quickstarts (Démarrages rapides) dans JBoss Developer Studio 26
1.4.3.2. Exécuter les Quickstarts par la Ligne de commande 28
1.4.4. Revoir les tutoriels Quickstart 28
1.4.4.1. Découvrir le Quickstart HelloWorld 29
1.4.4.2. Découvrir le Quickstart numberguess 34

CHAPITRE 2. GUIDE MAVEN **43**
2.1. POUR EN SAVOIR PLUS SUR MAVEN 43
2.1.1. Le référentiel Maven 43
2.1.2. Le fichier POM Maven 43
2.1.3. Prérequis minimum pour un fichier POM Maven 44
2.1.4. Le fichier des configurations de Maven 44
2.2. INSTALLER LE RÉFÉRENTIEL JBOSS MAVEN ET MAVEN 45
2.2.1. Télécharger et installer Maven 45
2.2.2. Installer le référentiel Maven de JBoss EAP 6 46
2.2.3. Installer le référentiel Maven de JBoss EAP 6 localement 46
2.2.4. Installer le référentiel Maven de JBoss EAP 6 à utiliser avec Appache httpd 47
2.2.5. Installer le référentiel Maven de JBoss EAP 6 en utilisant le gestionnaire de référentiels Nexus Maven 47
2.2.6. Gestionnaires de référentiels Maven 49
2.3. UTILISER LE RÉFÉRENTIEL MAVEN 49
2.3.1. Configurer le référentiel Maven de JBoss EAP 49
2.3.2. Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven 50
2.3.3. Configurer le référentiel JBoss EAP 6 Platform Maven Repository par le Projet POM 56
2.3.4. Gestion des dépendances du projet 58
Artéfacts Maven pris en charge 58

Gestion des dépendances 59
JBoss JavaEE Specs Bom de nomenclature 59
Les nomenclatures JBoss EAP BOM et les Quickstarts 60
JBoss Client BOMs 61
2.4. MISE À NIVEAU DU RÉFÉRENTIEL MAVEN 62
2.4.1. Appliquer un correctif dans le répertoire Maven local 62

CHAPITRE 3. CHARGEMENT DE CLASSES MODULAIRE ET MODULES 64
3.1. INTRODUCTION 64
3.1.1. Chargement des classes et Modules 64
3.1.2. Chargement des classes 64
3.1.3. Modules 64
3.1.4. Les dépendances de modules 65
3.1.5. Chargement des classes dans les déploiements 66
3.1.6. Précédence pour le chargement des classes 66
3.1.7. Nommage de modules dynamiques 67
3.1.8. jboss-deployment-structure.xml 68
3.2. AJOUTER UNE DÉPENDANCE DE MODULE EXPLICITE À UN DÉPLOIEMENT 68
3.3. GÉNÉRER DES ENTRÉES MANIFEST.MF EN UTILISANT MAVEN 70
3.4. EMPÊCHER QU'UN MODULE SOIT CHARGÉ IMPLICITEMENT 71
3.5. EXCLURE UN SOUS-SYSTÈME D'UN DÉPLOIEMENT 72
3.6. UTILISER LE CHARGEUR DE CLASSES PAR PROGRAMMATION DANS UN DÉVELOPPEMENT 74
3.6.1. Chargement des classes et des ressources par programmation dans le déploiement. 74
3.6.2. Itérer les ressources par programmation dans un déploiement. 76
3.7. CHARGEMENT DE CLASSE ET SOUS-DÉPLOIEMENTS 79
3.7.1. Chargement de classes et de modules dans les EAR (Archives Enterprise) 79
3.7.2. Isolement du chargeur de classes d'un sous-déploiement 80
3.7.3. Désactiver l'isolement du chargeur de classes d'un sous-déploiement dans un EAR 80
3.8. RÉFÉRENCE 81
3.8.1. Dépendances de modules implicites 81
3.8.2. Les modules inclus 85
3.8.3. Référence de descripteur de déploiement de structure de déploiement de JBoss 93

CHAPITRE 4. VALVES GLOBALES 95
4.1. VALVES 95
4.2. VALVES GLOBALES 95
4.3. LES VALVES D'AUTHENTIFICATION 95
4.4. CONFIGURER UNE APPLICATION WEB POUR UTILISER UNE VALVE. 95
4.5. CONFIGURER UNE APPLICATION WEB POUR QU'ELLE UTILISE UNE VALVE D'AUTHENTIFICATION 96
4.6. CRÉER UNE VALVE PERSONNALISÉE 97

CHAPITRE 5. LA JOURNALISATION POUR LES DÉVELOPPEURS 100
5.1. INTRODUCTION 100
5.1.1. Journalisation 100
5.1.2. Frameworks de journalisations d'applications pris en charge par JBoss LogManager 100
5.1.3. Niveaux de journalisation 100
5.1.4. Niveaux de journalisation pris en charge 101
5.1.5. Emplacements de fichiers de journalisation par défaut 102
5.2. JOURNALISATION DANS LE JBOSS LOGGING FRAMEWORK 102
5.2.1. JBoss Logging 102
5.2.2. Fonctionnalités de JBoss Logging 102
5.2.3. Ajouter une journalisation à une application par JBoss Logging 103
5.3. PROFILS DE JOURNALISATION 105
5.3.1. Profils de journalisation 105

5.3.2. Spécifier un profil de journalisation dans une application 105

CHAPITRE 6. INTERNATIONALISATION ET LOCALISATION 107
6.1. INTRODUCTION 107
6.1.1. Internationalisation 107
6.1.2. Localisation 107
6.2. OUTILS JBOSS LOGGING 107
6.2.1. Aperçu 107
6.2.1.1. JBoss Logging Tools - Internationalisation et Localisation 107
6.2.1.2. JBoss Logging Tools Quickstart 108
6.2.1.3. Message Logger 108
6.2.1.4. Lot de messages 108
6.2.1.5. Messages de journalisation internationalisés 108
6.2.1.6. Exceptions internationalisées 108
6.2.1.7. Messages internationalisés 108
6.2.1.8. Fichiers de propriétés de traduction 109
6.2.1.9. Codes de projets de JBoss Logging Tools 109
6.2.1.10. Ids de messages de JBoss Logging Tools 109
6.2.2. Création de loggers, de messages ou d'exceptions internationalisés 109
6.2.2.1. Créer des messages log internationalisés 109
6.2.2.2. Créer et utiliser des messages internationalisés 111
6.2.2.3. Créer des exceptions personnalisées 112
6.2.3. Localisation de loggers, messages ou exceptions internationalisés 113
6.2.3.1. Générer des nouveaux fichiers de propriétés de traduction avec Maven 113
6.2.3.2. Traduire un logger, une exception ou un message internationalisé 115
6.2.4. Personnalisation des messages de journalisation internationalisés 116
6.2.4.1. Ajouter les ids de messages et les codes de projets aux messages de journalisation 116
6.2.4.2. Indiquer le niveau de journalisation d'un message 117
6.2.4.3. Personnaliser les messages de journalisation par des paramètres 117
6.2.4.4. Indiquer une exception comme cause d'un message de journalisation 118
6.2.5. Personnalisation des exceptions internationalisées 119
6.2.5.1. Ajouter les ids et les codes de projets aux messages d'exceptions 119
6.2.5.2. Personnaliser les messages d'exception avec des paramètres 121
6.2.5.3. Indiquer une exception comme cause d'une autre exception 122
6.2.6. Référence 123
6.2.6.1. Configuration Maven JBoss Logging Tools 123
6.2.6.2. Format de fichier de propriétés de traduction 124
6.2.6.3. Références aux annotations de JBoss Logging Tools 125

CHAPITRE 7. ENTERPRISE JAVABEANS 127
7.1. INTRODUCTION 127
7.1.1. Entreprise JavaBeans 127
7.1.2. Groupe de fonctionnalités EJB 3.1 127
7.1.3. EJB 3.1 Lite 128
7.1.4. Fonctionnalités EJB 3.1 Lite 128
7.1.5. Beans Enterprise 128
7.1.6. Écriture des beans Enterprise 129
7.1.7. Interfaces Métier de Session Bean 129
7.1.7.1. Interfaces de métier Bean Enterprise 129
7.1.7.2. Interfaces de métier locales EJB 130
7.1.7.3. Interfaces métier à distance EJB 130
7.1.7.4. Beans EJB No-interface 130
7.2. CRÉER DES PROJETS ENTERPRISE BEAN 130

7.2.1. Créer un projet d'archives EJB avec le Studio JBoss Developer 130
7.2.2. Créer un projet EJB Archive dans Maven. 134
7.2.3. Créer un projet EAR contenant un projet EJB 136
7.2.4. Ajouter un descripteur de déploiement à un projet EJB 139
7.3. SESSION BEANS 140
7.3.1. Session Beans 140
7.3.2. Stateless Session Beans 140
7.3.3. Stateful Session Beans 141
7.3.4. Singleton Session Beans 141
7.3.5. Ajouter des Session Beans à un projet dans JBoss Developer Studio 141
7.4. MESSAGE-DRIVEN BEANS 144
7.4.1. Message-Driven Beans 144
7.4.2. Adaptateurs de ressources 144
7.4.3. Créer un Message-Driven Bean basé JMS dans JBoss Developer Studio 144
7.5. INVOQUER LES SESSION BEANS 146
7.5.1. Invoquer un session bean à distance avec JNDI 146
7.5.2. Contextes Client EJB 149
7.5.3. Considérations lors de l'utilisation d'un Contexte EJB Unique 150
7.5.4. Utiliser des Contextes Client EJB étendus 151
7.5.5. Configurer les EJB en utilisant un Contexte Client EJB Scoped 152
7.5.6. Propriétés Client EJB 154
7.6. INTERCEPTEURS DE CONTENEURS 157
7.6.1. Intercepteurs de conteneurs 157
7.6.2. Créer une classe d'intercepteur de conteneur 158
7.6.3. Configurer un intercepteur de conteneur 158
7.6.4. Modifier l'identité du contexte de sécurité 160
7.6.5. Sécurité supplémentaire pour l'authentification EJB 165
7.6.6. Utiliser un intercepteur côté client dans une application 172
7.7. JAVABEANS ENTERPRISE CLUSTERISÉS 172
7.7.1. JavaBeans clusterisées (EJB) 172
7.8. RÉFÉRENCE 173
7.8.1. Référence de nommage EJB JNDI 173
7.8.2. Résolution de référence EJB 173
7.8.3. Dépendances de projet pour les clients EJB distants 174
7.8.4. Référence de descripteur de déploiement jboss-ejb3.xml 176

CHAPITRE 8. CLUSTERING DANS LES APPLICATIONS WEB 179
8.1. RÉPLIQUE DE SESSION 179
8.1.1. La réplique de session HTTP 179
8.1.2. Cache de Session Web 179
8.1.3. Configurer le Cache de session web 179
8.1.4. Activer la copie de session pour votre application 180
8.2. PASSIVATION ET ACTIVATION HTTPSESSION 183
8.2.1. La passivation et l'activation de session HTTP 183
8.2.2. Configurer la passivation HttpSession dans votre application 184
8.3. DOMAINE DU COOKIE 186
8.3.1. Le domaine du cookie 186
8.3.2. Configurer le domaine du cookie 186
8.4. IMPLÉMENTER UN HA SINGLETON 186

CHAPITRE 9. CDI 195
9.1. CDI 195
9.1.1. CDI 195

9.1.2. CDI (Contexts and Dependency Injection) 195
9.1.3. Avantages de CDI 195
9.1.4. Injection de Dépendance de Type-safe 196
9.1.5. Relation entre Weld, Seam 2, Seam 3, et JavaServer Faces 196
9.2. UTILISER CDI 196
9.2.1. Premières étapes 196
9.2.1.1. Activer CDI 196
9.2.2. Utiliser CDI pour développer une application 197
9.2.2.1. Utiliser CDI pour développer une application 197
9.2.2.2. CDI avec le code existant 198
9.2.2.3. Exclure les beans du processus de balayage 198
9.2.2.4. Utiliser une injection pour étendre une implémentation 199
9.2.3. Dépendances ambigues ou non satisfaites 200
9.2.3.1. Dépendances ambigües et non-satisfaites 200
9.2.3.2. Qualificateurs 201
9.2.3.3. Utiliser un qualificateur pour résoudre une injection ambiguë 201
9.2.4. Beans gérés 202
9.2.4.1. Les beans gérés 202
9.2.4.2. Types de Classes qui ne sont pas des Beans 203
9.2.4.3. Utiliser CDI pour injecter un objet dans un bean 203
9.2.5. Contextes, Scopes et Dépendances 205
9.2.5.1. Contextes et scopes 205
9.2.5.2. Contexte disponibles 205
9.2.6. Cycle de vie d'un bean 206
9.2.6.1. Gestion du cycle de vie d'un bean 206
9.2.6.2. Utilisation d'une méthode Producer 207
9.2.7. Beans nommés et beans alternatifs 208
9.2.7.1. Named Beans 208
9.2.7.2. Utilisation des Named Beans 208
9.2.7.3. Beans Alternative 209
9.2.7.4. Remplacer une injection par une alternative 209
9.2.8. Stérétypes 210
9.2.8.1. Stéréotypes 210
9.2.8.2. Utilisation des stéréotypes 211
9.2.9. Méthodes Observer 212
9.2.9.1. Méthodes Observer 212
9.2.9.2. Appliquer et observer des événements 212
9.2.10. Intercepteurs 213
9.2.10.1. Les intercepteurs 213
9.2.10.2. Utiliser les intercepteurs dans CDI 214
9.2.11. Les décorateurs 215
9.2.12. Extensions portables 216
9.2.13. Proxies Beans 216
9.2.13.1. Proxys Bean 216
9.2.13.2. Utiliser un Proxy ou une Injection 216

CHAPITRE 10. JAVA TRANSACTION API (JTA) 218
10.1. APERÇU 218
10.1.1. Java Transactions API (JTA) 218
10.2. CONCEPTS DE TRANSACTIONS 218
10.2.1. Transactions 218
10.2.2. Les propriétés ACID de transactions 218
10.2.3. Coordinateur de transactions ou Gestionnaire de transactions 219

10.2.4. Participants d'une transaction. 219
10.2.5. JTA (Java Transactions API) 219
10.2.6. JTS (Java Transaction Service) 220
10.2.7. Sources de Données XA et Transactions XA 220
10.2.8. La Récupération XA 220
10.2.9. Le protocole de validation en 2-Phases 221
10.2.10. Les délais d'attente de transactions 221
10.2.11. Les transactions distribuées 222
10.2.12. API de Portabilité ORB 222
10.2.13. Transactions imbriquées 222
10.3. OPTIMISATIONS DE TRANSACTIONS 223
10.3.1. Optimisations de transactions 223
10.3.2. Optimisation LRCO pour une validation en 1 phase (1 PC) 223
10.3.3. Optimisation Presumed-Abort 223
10.3.4. Optimisation Lecture-seule 224
10.4. RÉSULTATS DE TRANSACTIONS 224
10.4.1. Résultats de transactions 224
10.4.2. Transactions de validation 224
10.4.3. Transactions Roll-Back 225
10.4.4. Résultats heuristiques 225
10.4.5. Erreurs et exceptions pour les transactions JBoss 225
10.5. APERÇU SUR LES TRANSACTIONS JTA 226
10.5.1. JTA (Java Transactions API) 226
10.5.2. Cycle de vie d'une transaction JTA 226
10.6. CONFIGURATION DE SOUS-SYSTÈME DE TRANSACTION 227
10.6.1. Configuration des transactions 227
10.6.2. Configuration de source de données transactionnelle 227
10.6.2.1. Configurez votre base de données pour utiliser les Transactions JTA 227
10.6.2.2. Configuration d'une source de données XA 228
10.6.2.3. Se conncecter à la console de gestion 229
10.6.2.4. Créer une source de données Non-XA avec les interfaces de gestion 230
10.6.2.5. Paramètres de source de données 231
10.6.3. Journalisation des transactions 239
10.6.3.1. Messages de journalisation de transactions 239
10.6.3.2. Configurer la journalisation des sous-systèmes de transactions 240
10.6.3.3. Naviguer et gérer les transactions 241
10.7. UTILISER LES TRANSACTIONS JTA 245
10.7.1. Transactions JTA 245
10.7.2. Transactions de contrôle 246
10.7.3. Démarrer une transaction 246
10.7.4. Transactions imbriquées 247
10.7.5. Valider une transaction 248
10.7.6. Annuler une transaction 249
10.7.7. Gérer un résultat heuristique dans une transaction 250
10.7.8. Temps d'expiration des transactions 251
10.7.8.1. Les délais d'attente de transactions 251
10.7.8.2. Configurer le Transaction Manager (TM) ou Gestionnaire de transactions 252
10.7.9. Gestion des erreurs de transactions JTA 256
10.7.9.1. Erreurs de transactions 256
10.8. CONFIGURATION ORB 257
10.8.1. A propos de CORBA (Common Object Request Broker Architecture) 257
10.8.2. Configurer l'ORB pour les transactions JTS 257
10.9. RÉFÉRENCES DE TRANSACTIONS 259

10.9.1. Erreurs et exceptions pour les transactions JBoss 259
10.9.2. Limitations de JTA Clustering 259
10.9.3. Exemple de transaction JTA 259
10.9.4. Documentation API pour JBoss Transactions JTA 261

CHAPITRE 11. HIBERNATE 262
11.1. HIBERNATE CORE 262
11.2. JAVA PERSISTENCE API (JPA) 262
11.2.1. JPA 262
11.2.2. Hibernate EntityManager 262
11.2.3. Guide de départ 262
11.2.3.1. Créer un projet JPA dans JBoss Developer Studio 262
11.2.3.2. Créer le fichier de paramètres de persistance dans JBoss Developer Studio 265
11.2.3.3. Exemple de fichier de configuration de persistance 267
11.2.3.4. Créer le fichier de configuration Hibernate dans JBoss Developer Studio 267
11.2.3.5. Exemple de fichier de configuration Hibernate 268
11.2.4. Configuration 269
11.2.4.1. Propriétés de configuration de Hibernate 269
11.2.4.2. Hibernate JDBC et Propriétés de Connexion 271
11.2.4.3. Propriétés d'Hibernate Cache 272
11.2.4.4. Propriétés de transaction Hibernate 273
11.2.4.5. Propriétés Hibernate diverses 274
11.2.4.6. Dialectes SQL Hibernate 275
11.2.5. Caches de second niveau 278
11.2.5.1. Les caches de second niveau 278
11.2.5.2. Configurer un cache de second niveau pour Hibernate 278
11.3. ANNOTATIONS HIBERNATE 279
11.3.1. Annotations Hibernate 279
11.4. LANGAGE DE RECHERCHE HIBERNATE 284
11.4.1. Langage de recherche d'Hibernate 284
11.4.2. Déclarations HQL 284
11.4.3. La déclaration INSERT 285
11.4.4. La clause FROM 286
11.4.5. La clause WITH 286
11.4.6. Mises à jour, Insertions et Suppressions en bloc 286
11.4.7. Références de collection 288
11.4.8. Expressions de chemins qualifiées 289
11.4.9. Fonctions scalaires 290
11.4.10. Fonctions standardisées HQL 291
11.4.11. Opération de concaténation 291
11.4.12. Instanciation dynamique 292
11.4.13. Prédicats HQL 293
11.4.14. Comparaisons relationnelles 295
11.4.15. Prédicat IN 296
11.4.16. SQL Ordering 297
11.5. SERVICES HIBERNATE 298
11.5.1. Les services Hibernate 298
11.5.2. Contrats de service 298
11.5.3. Types de dépendances de service 298
11.5.4. Le ServiceRegistry 299
11.5.4.1. Le ServiceRegistry 299
11.5.5. Services personnalisés 299
11.5.5.1. Services personnalisés 299

11.5.6. Le registre Bootstrap 301
11.5.6.1. Le registre Boot-strap 301
11.5.6.2. Utilisation de BootstrapServiceRegistryBuilder 301
11.5.6.3. Les services BootstrapRegistry 302
11.5.7. Le registre SessionFactory 303
11.5.7.1. Le registre SessionFactory 303
11.5.7.2. Services SessionFactory 303
11.5.8. Intégrateurs 303
11.5.8.1. Intégrateurs 303
11.5.8.2. Cas d'utilisation d'Integrator 304
11.6. VALIDATION D'UN BEAN 304
11.6.1. Validation Bean 305
11.6.2. Hibernate Validator 305
11.6.3. Contraintes de validation 305
11.6.3.1. Les contraintes de validation 305
11.6.3.2. Créer une annotation de contrainte dans JBoss Developer Studio 305
11.6.3.3. Créer une nouvelle classe Java dans JBoss Developer Studio 307
11.6.3.4. Contraintes d'Hibernate Validator 308
11.6.4. Configuration 310
11.6.4.1. Exemple de fichier de configuration de validation 310
11.7. ENVERS 311
11.7.1. Hibernate Envers 311
11.7.2. Audit de classes persistantes 311
11.7.3. Stratégies d'auditing 311
11.7.3.1. Stratégies d'auditing 311
11.7.3.2. Définir la stratégie d'auditing 312
11.7.4. Introduction à l'auditing d'entités 312
11.7.4.1. Ajouter une support d'auditing à une entité JPA 312
11.7.5. Configuration 314
11.7.5.1. Configurer les paramètres Envers 314
11.7.5.2. Activer ou désactiver l'auditing en cours d'exécution 315
11.7.5.3. Configurer l'auditing conditionnel. 315
11.7.5.4. Propriétés de configuration Envers 316
11.7.6. Recherches 318
11.7.6.1. Suppression de l'information d'auditing 318
11.8. RÉGLAGE DE LA PERFORMANCE 322
11.8.1. Algorithmes de chargement de lots alternatifs 322
11.8.2. Mise en cache de second niveau d'objets de référence pour les données non mutables 324

CHAPITRE 12. SERVICES WEB JAX-RS 326
12.1. JAX-RS 326
12.2. RESTEASY 326
12.3. SERVICES WEB RESTFUL 326
12.4. ANNOTATIONS DÉFINIES RESTEASY 326
12.5. CONFIGURATION RESTEASY 329
12.5.1. Paramètres de configuration RESTEasy 329
12.6. JAX-RS WEB SERVICE SECURITY 330
12.6.1. Activer la sécurité basée-rôle pour RESTEasy JAX-RS Web Service 330
12.6.2. Sécuriser un service JAX-RS Web par des annotations 332
12.7. RESTEASY LOGGING 333
12.7.1. JAX-RS Web Service Logging 333
12.7.2. Catégories de journalisation définies dans RESTEasy 333
12.8. GESTION DES EXCEPTIONS 334

12.8.1. Créer un mappeur d'exceptions 334
12.8.2. Exceptions RESTEasy lancées en interne 334
12.9. INTERCEPTEURS RESTEASY 336
12.9.1. Interception des invocations JAX-RS 336
12.9.2. Lier un intercepteur à une méthode JAX-RS 339
12.9.3. Enregistrer un intercepteur 339
12.9.4. Familles de précédence d'intercepteur 340
12.9.4.1. Familles de précédence d'intercepteur 340
12.9.4.2. Définissez une famille de précédence d'intercepteurs personnalisée 340
12.10. ANNOTATIONS BASÉES CHAÎNE 341
12.10.1. Conversion des annotations basées @*Param en objects 341
12.11. CONFIGURATION DES EXTENSIONS DE FICHIERS 345
12.11.1. Mapper les extensions de fichiers avec les types de media dans le fichier web.xml 345
12.11.2. Mapper les extensions de fichiers vers les Langues dans le fichier web.xml 346
12.11.3. Types de media supportés par RESTEasy 347
12.12. API JAVASCRIPT RESTEASY 347
12.12.1. API JavaScript RESTEasy 347
12.12.2. Activation du Servlet API JavaScript RESTEasy 348
12.12.3. Paramètres de l'API JavaScript RESTEasy 348
12.12.4. Créer des requêtes AJAX par l'API JavaScript 349
12.12.5. Membres de la classe REST.Request 350
12.13. RESTEASY ASYNCHRONOUS JOB SERVICE 351
12.13.1. Service Job Asynchrone RESTEasy 351
12.13.2. Activer le Service de jobs asynchrones 351
12.13.3. Configurer les Jobs asynchrones avec RESTEasy 352
12.13.4. Paramètres de configuration de Service Job Asynchrone 353
12.14. RESTEASY JAXB 355
12.14.1. Créer un décorateur JAXB 355
12.15. RESTEASY ATOM SUPPORT 356
12.15.1. Fournissseur et API Atom 356

CHAPITRE 13. SERVICES WEB JAX-WS 357
13.1. SERVICES WEB JAX-WS 357
13.2. CONFIGURER LE SOUS-SYSTÈME WEBSERVICES 358
13.3. PONTS DE TERMINAISON DE SERVICES WEB JAX-WS 362
13.3.1. Les points de terminaison de Services Web JAX-WS 362
13.3.2. Écrire et déployer un point de terminaison de Service Web JAX-WS 364
13.4. CLIENTS DU SERVICE JAX-WS WEB 366
13.4.1. Consommer et accéder à un Service Web JAX-WS 366
13.4.2. Développer une application client JAX-WS 370
13.5. RÉFÉRENCE DE DÉVELOPPEMENT JAX-WS 376
13.5.1. Activation de WS-Addressing (Web Services Addressing) 376
13.5.2. Référence API Commun JAX-WS 378

CHAPITRE 14. IDENTITÉ AU SEIN D'APPLICATIONS 382
14.1. CONCEPTS DE BASE 382
14.1.1. Chiffrement 382
14.1.2. Les domaines de sécurité 382
14.1.3. Cryptage SSL 382
14.1.4. Sécurité déclarative 383
14.2. SÉCURITÉ BASÉE-RÔLE POUR LES APPLICATIONS 383
14.2.1. La sécurité des applications 383
14.2.2. Authentification 384

14.2.3. L'autorisation 384
14.2.4. Security Auditing 384
14.2.5. Security Mapping 384
14.2.6. Security Extension Architecture 385
14.2.7. Java Authentication et Authorization Service (JAAS) 386
14.2.8. Java Authentication et Authorization Service (JAAS) 386
14.2.9. Utiliser un domaine de sécurité dans votre application 391
14.2.10. Utilisation de la sécurité basée-rôle dans les Servlets 393
14.2.11. Utilisation d'une authentification système de tierce partie pour votre application 395
14.3. DOMAINES DE SÉCURITÉ 402
14.3.1. Domaines de sécurité 402
14.3.2. Ajout d'un domaine de sécurité 403
14.3.3. Ajout d'un utilisateur à un domaine de sécurité 403
14.4. SÉCURITÉ DES APPLICATIONS EJB 404
14.4.1. Identité Sécurité 404
14.4.1.1. L'identité de sécurité EJB 404
14.4.1.2. Définir l'identité de sécurité d'un EJB 404
14.4.2. Permissions de méthodes EJB 405
14.4.2.1. Permissions de méthodes EJB 405
14.4.2.2. Utilisation des permissions de méthodes EJB 406
14.4.3. Annotations de sécurité EJB 409
14.4.3.1. Les annotations de sécurité EJB 409
14.4.3.2. Utilisation des annotations de sécurité EJB 409
14.4.4. Accès à distance aux EJB 410
14.4.4.1. Remote Method Access 410
14.4.4.2. Remoting Callbacks 411
14.4.4.3. Remoting Server Detection 412
14.4.4.4. Configurer le sous-système de JBoss Remoting 412
14.4.4.5. Utilisation des domaines de sécurité avec les clients EJB distants 421
14.4.4.6. Ajout d'un domaine de sécurité 422
14.4.4.7. Ajout d'un utilisateur à un domaine de sécurité 422
14.4.4.8. Accès EJB à distance utilisant le cryptage SSL 423
14.5. SÉCURITÉ APPLICATION JAX-RS 423
14.5.1. Activer la sécurité basée-rôle pour RESTEasy JAX-RS Web Service 423
14.5.2. Sécuriser un service JAX-RS Web par des annotations 425
14.6. PROTOCOLE MOTS DE PASSES DISTANTS SÉCURISÉS 425
14.6.1. Protocole pour mots de passes distants sécurisés (SRP pour Secure Remote Password) 425
14.6.2. Configuration du protocole SRP (Secure Remote Password) 426
14.7. L'ARCHIVAGE SÉCURISÉ DES MOTS DE PASSE POUR LES STRINGS DE NATURE CONFIDENTIELLE 428
14.7.1. Sécurisation des chaînes confidentielles des fichiers en texte clair 428
14.7.2. Créer un Keystore Java pour stocker des strings sensibles 429
14.7.3. Masquer le mot de passe du keystore et initialiser le mot de passe de l'archivage de sécurité 431
14.7.4. Configurer JBoss EAP pour qu'il utilise l'archivage sécurisé des mots de passe 433
14.7.5. Stocker et résoudre des strings sensibles cryptés du Keystore Java. 434
14.7.6. Stocker et résoudre des strings sensibles de vos applications 437
14.8. JAVA AUTHORIZATION CONTRACT FOR CONTAINERS (JACC) 439
14.8.1. Java Authorization Contract for Containers (JACC) 439
14.8.2. Configurer la sécurité JACC (Java Authorization Contract for Containers) 439
14.9. JAVA AUTHENTICATION SPI FOR CONTAINERS (JASPI) 441
14.9.1. Sécurité Java Authentication SPI pour Conteneurs (JASPI) 441
14.9.2. Configuration de la sécurité Java Authentication SPI pour conteneurs (JASPI) 441

CHAPITRE 15. SINGLE SIGN ON (SSO) 443

15.1. SSO (SINGLE SIGN ON) POUR LES APPLICATIONS WEB 443
15.2. SSO (SINGLE SIGN ON) CLUSTERISÉES POUR LES APPLICATIONS WEB 444
15.3. CHOISIR L'IMPLÉMENTATION SSO QUI VOUS CONVIENT 444
15.4. UTILISATION DE SSO (SINGLE SIGN ON) POUR LES APPLICATIONS WEB 445
15.5. KERBEROS 448
15.6. SPNEGO 448
15.7. MICROSOFT ACTIVE DIRECTORY 448
15.8. CONFIGURATION DE KERBEROS OU MICROSOFT ACTIVE DIRECTORY DESKTOP SSO POUR LES APPLICATIONS WEB 449

CHAPITRE 16. RÉFÉRENCES DE SÉCURITÉ POUR LE DÉVELOPPEMENT 453
16.1. RÉFÉRENCE DE CONFIGURATION JBOSS-WEB.XML 453
16.2. RÉFÉRENCE DE PARAMÈTRE DE SÉCURITÉ EJB 456

CHAPITRE 17. RÉFÉRENCES SUPPLÉMENTAIRES 458
17.1. TYPES D'ARCHIVES JAVA 458

ANNEXE A. REVISION HISTORY 460

PREFACE

CHAPITRE 1. INTRODUCTION AU DÉVELOPPEMENT D'APPLICATIONS

1.1. INTRODUCTION

1.1.1. Red Hat JBoss Enterprise Application Platform 6 (JBoss EAP 6)

Red Hat JBoss Enterprise Application Platform 6 (JBoss EAP 6) est une plate-forme middleware rapide, sécurisée et puissante construite sur des standards ouverts et compatibles avec Java Enterprise Edition 6. Elle intègre JBoss Application Server 7 avec un clustering de haute disponibilité, une puissante messagerie, une mise en cache distribuée et autres technologies pour créer une plate-forme stable et évolutive.

La nouvelle structure modulaire permet que les services soient mis en place uniquement en fonction des besoins, ce qui augmente la vitesse de démarrage de façon importante. La console de gestion et l'interface de ligne de commande de gestion suppriment le besoin de modifier les fichiers de configuration XML manuellement, et rajoute la possibilité de script et d'automatisation des tâches. En outre, elle comprend des API et des frameworks de développement, que vous pouvez utiliser pour développer des applications Java EE puissantes, sécurisées et évolutives rapidement.

Report a bug

1.2. PRÉ-REQUIS

1.2.1. Familiarisez vous avec Java Enterprise Edition 6

1.2.1.1. Les Profils EE 6

Java Enterprise Edition 6 (EE 6) inclut un support pour des profils multiples, ou sous-ensembles d'API. Les deux seuls profils que la spécification EE6 définit sont *Full Profile* et *Web Profile*.

EE 6 Full Profile inclut tous les API et toutes les spécifications incluses dans la spécification EE 6. EE 6 Web Profile inclut un sous-ensemble des APIs qui sont utiles aux développeurs web.

JBoss EAP 6 est une implémentation certifiée de Java Enterprise Edition 6 Full Profile et des spécifications Web Profile.

- Section 1.2.1.2, « Web Profil de Java Enterprise Edition 6 »
- Section 1.2.1.3, « Java Enterprise Edition 6 Full Profile »

Report a bug

1.2.1.2. Web Profil de Java Enterprise Edition 6

Le Web Profil est l'un des deux profils définis dans la spécification Java Enterprise Edition 6. Il a été conçu pour le développement d'une application web. L'autre profil défini par la spécification Java Enterprise Edition 6 est le Full Profile. Pour plus d'informations, voir Section 1.2.1.3, « Java Enterprise Edition 6 Full Profile ».

Pré-requis de Java EE 6 Web Profile

- Java Platform, Enterprise Edition 6

- **Technologies Java Web**
  - Servlet 3.0 (JSR 315)
  - JSP 2.2 et Expression Language (EL) 1.2
  - JavaServer Faces (JSF) 2.0 (JSR 314)
  - Java Standard Tag Library (JSTL) for JSP 1.2
  - Débogage du support pour les autres langages 1.0 (JSR 45)

- **Enterprise Application Technologies**
  - Contexts and Dependency Injection (CDI) (JSR 299)
  - Injection de dépendance dans Java (JSR 330)
  - Enterprise JavaBeans 3.1 Lite (JSR 318)
  - Java Persistence API 2.0 (JSR 317)
  - Annotations communes de la Plateforme Java 1.1 (JSR 250)
  - Java Transaction API (JTA) 1.1 (JSR 907)
  - Bean Validation (JSR 303)

Report a bug

1.2.1.3. Java Enterprise Edition 6 Full Profile

La spécification Java Enterprise Edition 6 (EE 6) définit un concept de profil, et définit deux d'entre eux dans le cadre de la spécification. En plus des items supportés dans le Java Enterprise Edition 6 Web Profile (Section 1.2.1.2, « Web Profil de Java Enterprise Edition 6 »), le Full Profile supporte les API suivants. JBoss Enterprise Edition 6 supporte le Full Profile.

Items inclus dans EE 6 Full Profile

- EJB 3.1 (not Lite) (JSR 318)
- Java EE Connector Architecture 1.6 (JSR 322)
- Java Message Service (JMS) API 1.1 (JSR 914)
- JavaMail 1.4 (JSR 919)

- **Technologies Service Web**
  - Jax-RS RESTful Web Services 1.1 (JSR 311)
  - Implémentation d'Enterprise Web Services 1.3 (JSR 109)
  - JAX-WS Java API for XML-Based Web Services 2.2 (JSR 224)

- Java Architecture pour XML Binding (JAXB) 2.2 (JSR 222)
- Web Services Metadata pour Java Platform (JSR 181)
- Les API Java pour XML-based RPC 1.1 (JSR 101)
- Les API Java pour XML Messaging 1.3 (JSR 67)
- Java API pour les Registres XML (JAXR) 1.0 (JSR 93)

- **Technologies de Gestion et de Sécurité**
  - Interface Fournisseur Service Java Authentification pour Conteneurs 1.0 (JSR 196)
  - Contrat Java Authentication Contract pour les Conteneurs 1.3 (JSR 115)
  - Déploiement Application Java EE 1.2 (JSR 88)
  - J2EE Management 1.1 (JSR 77)

Report a bug

1.2.2. Les modules et le système de chargement de la nouvelle classe modulaire de JBoss EAP 6.

1.2.2.1. Modules

Un module est un regroupement logique des classes utilisées pour le chargement de classes et pour la gestion de dépendances. JBoss EAP 6 identifie deux types de modules, parfois appelés modules statiques et dynamiques. Cependant, la seule différence entre les deux est la façon dont ils sont emballés. Tous les modules offrent les mêmes caractéristiques.

Modules statiques

Les modules statiques sont prédéfinis dans le répertoire ***EAP_HOME*/modules/** du serveur d'application. Chaque sous-répertoire représente un module et contient un ou plusieurs fichiers JAR et un fichier de configuration (**module.xml**). Le nom de ce module est défini dans le fichier **module.xml**. Toutes les API fournies par le serveur d'application sont fournies en tant que modules statiques, comme les API Java EE ainsi que d'autres API comme JBoss Logging.

Exemple 1.1. Exemple de fichier module.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.0" name="com.mysql">
  <resources>
    <resource-root path="mysql-connector-java-5.1.15.jar"/>
  </resources>
  <dependencies>
    <module name="javax.api"/>
    <module name="javax.transaction.api"/>
  </dependencies>
</module>
```

Le nom du module, **com.mysql**, doit correspondre à la structure du répertoire du module.

- La création de modules statiques personnalisés peut être utile si plusieurs applications sont déployées sur un même serveur utilisant les mêmes bibliothèques de tierce partie. Au lieu d'un regroupement de ces bibliothèques pour chaque application, un module contenant ces bibliothèques peut être créé et installé par l'administrateur JBoss. Les applications peuvent ensuite déclarer une dépendance explicite sur les modules statiques personnalisés.

Modules dynamiques

Les modules dynamiques sont créés et chargés par le serveur d'application pour chaque déploiement JAR ou WAR (ou sous-déploiement d'un EAR). Le nom d'un module dynamique est dérivé du nom de l'archive déployée. Comme les déploiements sont chargés sous forme de modules, ils peuvent configurer des dépendances et peuvent être utilisés comme dépendances par d'autres déploiements.

Les modules ne sont chargés qu'en fonction des besoins. Cela a généralement lieu quand une application est déployée avec des dépendances implicites ou explicites.

Report a bug

1.2.2.2. Chargement des classes et Modules

JBoss EAP 6 utilise un nouveau système de chargement de classes modulaire pour contrôler les chemins de classe d'applications déployées. Ce système offre plus de souplesse et de contrôle que le système traditionnel des chargeurs de classes hiérarchiques. Les développeurs ont un contrôle précis des classes disponibles à leurs applications et peuvent configurer un déploiement pour qu'il puisse ignorer les classes fournies par le serveur d'application en faveur de leurs propres classes.

Le nouveau chargeur de classes modulaire sépare toutes les classes Java en des groupes logiques appelés modules. Chaque module peut définir des dépendances sur d'autres modules de manière à ajouter les classes de ces modules dans leur propre chemin de classe. Le fait que chaque fichier JAR et WAR déployé soit traité comme un module permet aux développeurs de contrôler le contenu du chemin de classe de leur application en ajoutant une configuration de module à leur application.

Les informations suivantes permettent aux développeurs de comprendre comment construire et déployer des applications sous JBoss EAP 6.

Report a bug

1.3. INSTALLER L'ENVIRONNEMENT DE DÉVELOPPEMENT

1.3.1. Télécharger et installer JBoss Developer Studio

1.3.1.1. Installation de JBoss Developer Studio

1. Section 1.3.1.2, « Téléchargez JBoss Developer Studio 5 »
2. Section 1.3.1.3, « Installer JBoss Developer Studio 5 »
3. Section 1.3.1.4, « Démarrer JBoss Developer Studio »

Report a bug

1.3.1.2. Téléchargez JBoss Developer Studio 5

1. Visitez https://access.redhat.com/.
2. Sélectionner **Téléchargements** → **Red Hat JBoss Middleware** → **Téléchargements**.
3. Sélectionnez **`JBoss Developer Studio`** depuis la liste déroulante.
4. Sélectionnez la version appropriée et cliquez sur **`Télécharger`**.

Report a bug

1.3.1.3. Installer JBoss Developer Studio 5

Prérequis :

Section 1.3.1.2, « Téléchargez JBoss Developer Studio 5 »

Procédure 1.1. Installer JBoss Developer Studio 5

1. Ouvrir un terminal.
2. Aller dans le répertoire qui contient le fichier téléchargé **`.jar`**.
3. Exécuter la commande suivante pour lancer le GUI d'installation.

```
java -jar jbdevstudio-build_version.jar
```

4. Cliquer sur **`Suivant`** pour commencer le processus d'installation.
5. Sélectionner **`J'accepte les conditions de licence`** et cliquer sur **`Suivant`**.
6. Ajuster le chemin d'accès de l'installation et cliquer sur **`Suivant`**.

NOTE

Si le dossier de chemin d'installation n'existe pas, vous verrez une invite. Cliquer alors sur **`Ok`** pour créer le dossier.

7. Choisir une JVM, ou bien conserver la JVM sélectionnée par défaut, et cliquer sur **`Suivant`**.
8. Ajouter une plateforme d'applications disponible, et cliquer sur **`Suivant`**.
9. Vérifier les informations d'installation et cliquer sur **`Suivant`**.
10. Cliquer sur **`Suivant`** une fois le processus d'installation terminé.
11. Configurer les raccourcis bureau pour JBoss Developer Studio et cliquer sur **`Suivant`**.
12. Cliquer sur le bouton **`Terminé`**.

Report a bug

1.3.1.4. Démarrer JBoss Developer Studio

Prérequis :

Section 1.3.1.3, « Installer JBoss Developer Studio 5 »

Procédure 1.2. Commande pour lancer JBoss Developer Studio

1. Ouvrir un terminal.
2. Aller dans le répertoire d'installation.
3. Lancer la commande suivante pour démarrer JBoss Developer Studio :

```
[localhost]$ ./jbdevstudio
```

Report a bug

1.3.1.5. Ajouter le serveur de JBoss EAP 6 au JBoss Developer Studio

Ces instructions assument qu'il s'agit d'une introduction au JBoss Developer Studio et que vous n'avez pas encore ajouté de serveurs JBoss EAP 6.

Procédure 1.3. Ajouter le serveur

1. Ouvrir l'onglet **Serveurs**. S'il n'y a pas d'onglet **Serveurs**, l'ajouter au panneau comme suit :
   a. Cliquer sur **Window** → **Afficher Vue** → **Autres...**.
   b. Sélectionner **Serveurs** à partir du dossier **Serveur** et cliquer sur **OK**.
2. Cliquer sur le lien **nouvel assistant de serveur** ou bien cliquer à droite dans le panneau vide sur serveur, et sélectionner **Nouveau** → **Serveur**.

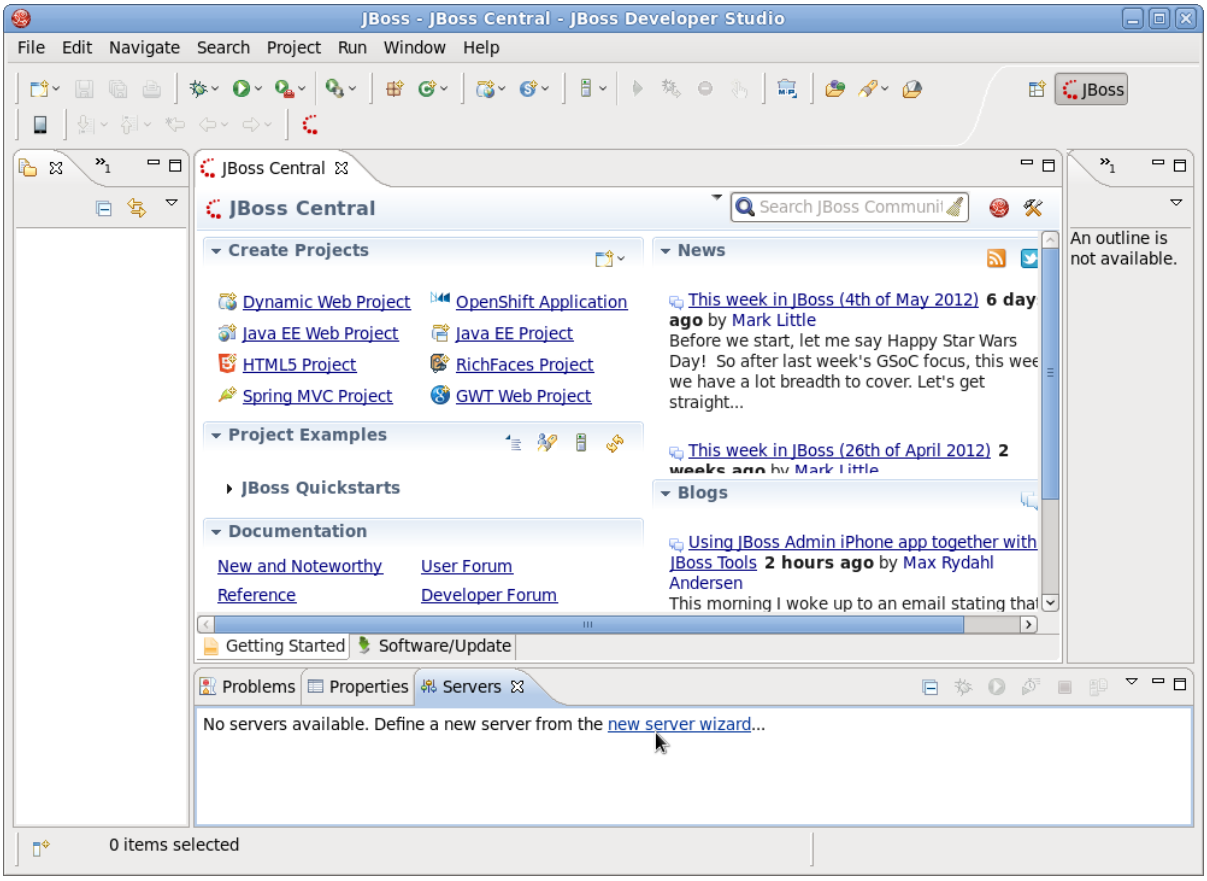


Figure 1.1. Ajouter un nouveau serveur - Aucun serveur disponible

3. Étendre **JBoss Enterprise Middleware** et choisir **JBoss Enterprise Application Platform 6.x**. Puis, cliquer sur **Suivant**.

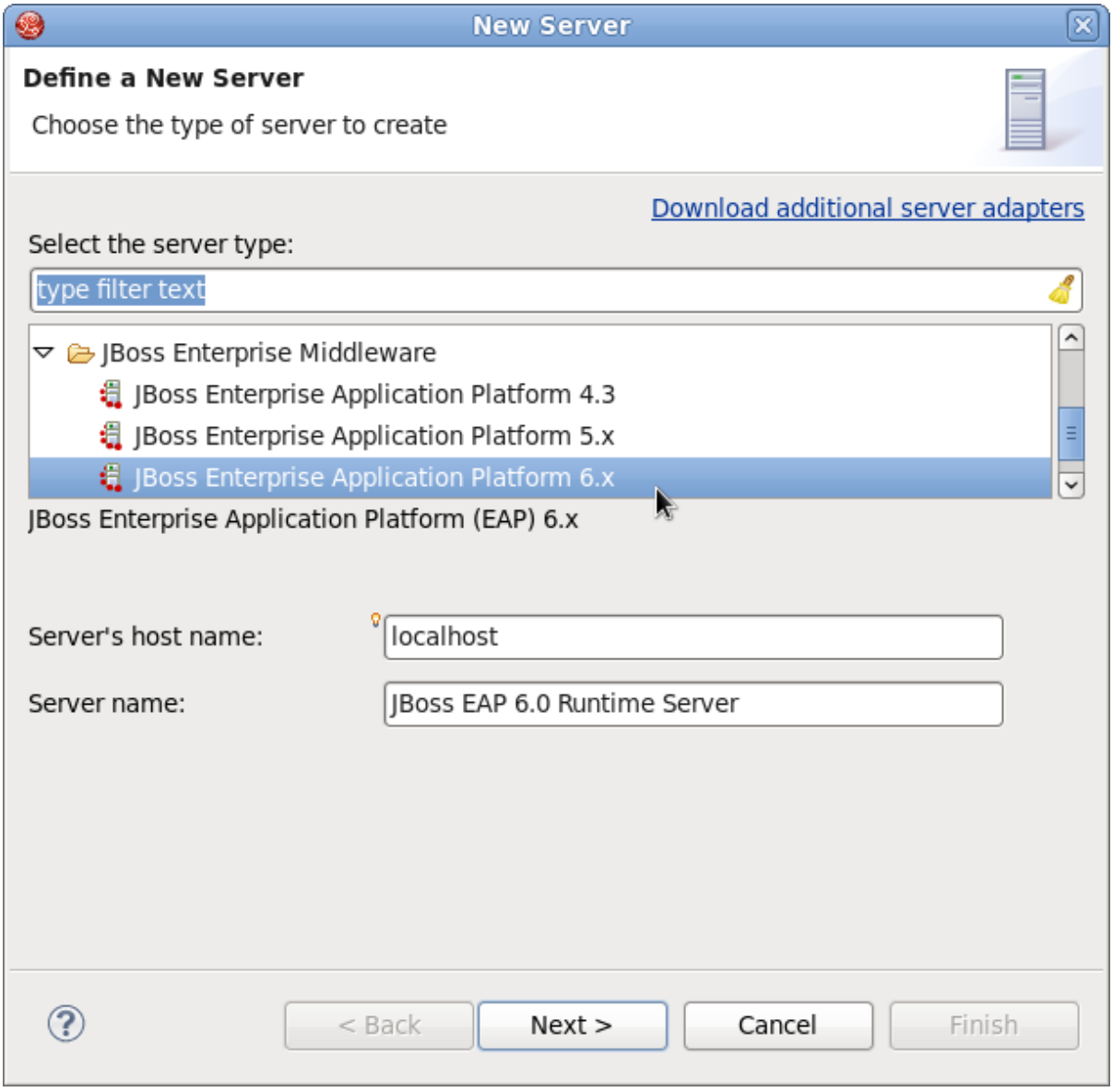


Figure 1.2. Choisir le type de serveur

4. Cliquer sur **Browse** et naviguez vers l'emplacement d'installation de JBoss EAP 6. Puis, cliquer sur **Suivant**.

Figure 1.3. Naviguer vers l'installation du serveur

5. Sur cet écran, vous définissez le comportement de serveur. Vous pouvez démarrer le serveur manuellement ou laisser JBoss Developer Studio le gérer pour vous. Vous pouvez également définir un serveur distant pour le déploiement et déterminer si vous souhaitez exposer le port de gestion pour ce serveur, par exemple, si vous avez besoin de le connecter en utilisant JMX. Dans cet exemple, supposons que le serveur est local et que vous souhaitiez que JBoss Developer Studio gère votre serveur sans que vous ayiez besoin de vérifier quoi que ce soit. Cliquer sur **`Suivant`**.

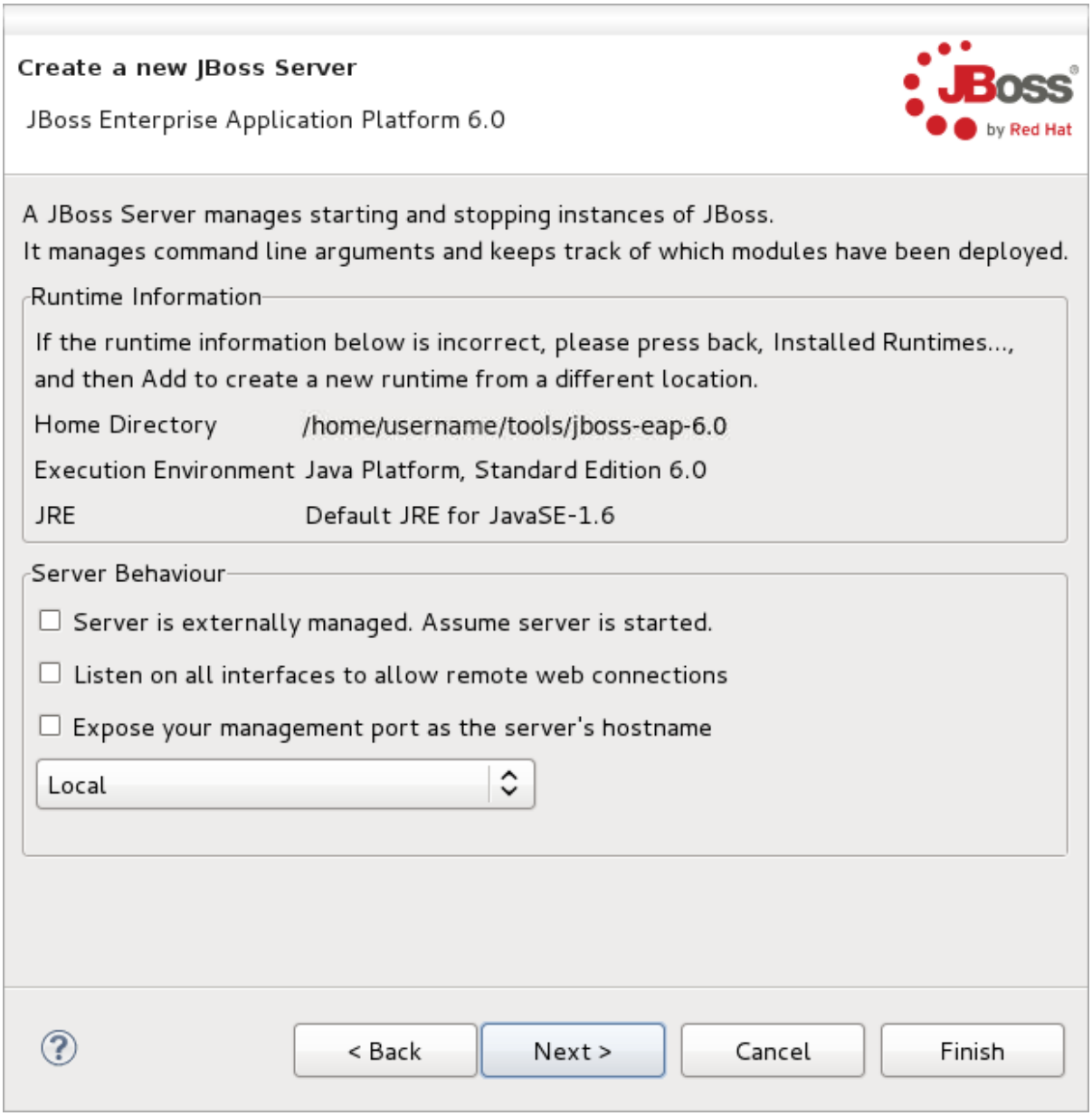


Figure 1.4. Définir le nouveau comportement du serveur de JBoss

6. Cet écran vous permet de configurer les projets existants pour le nouveau serveur. Puisque vous n'avez pas de projets à ce stade, cliquez sur **Terminé**.

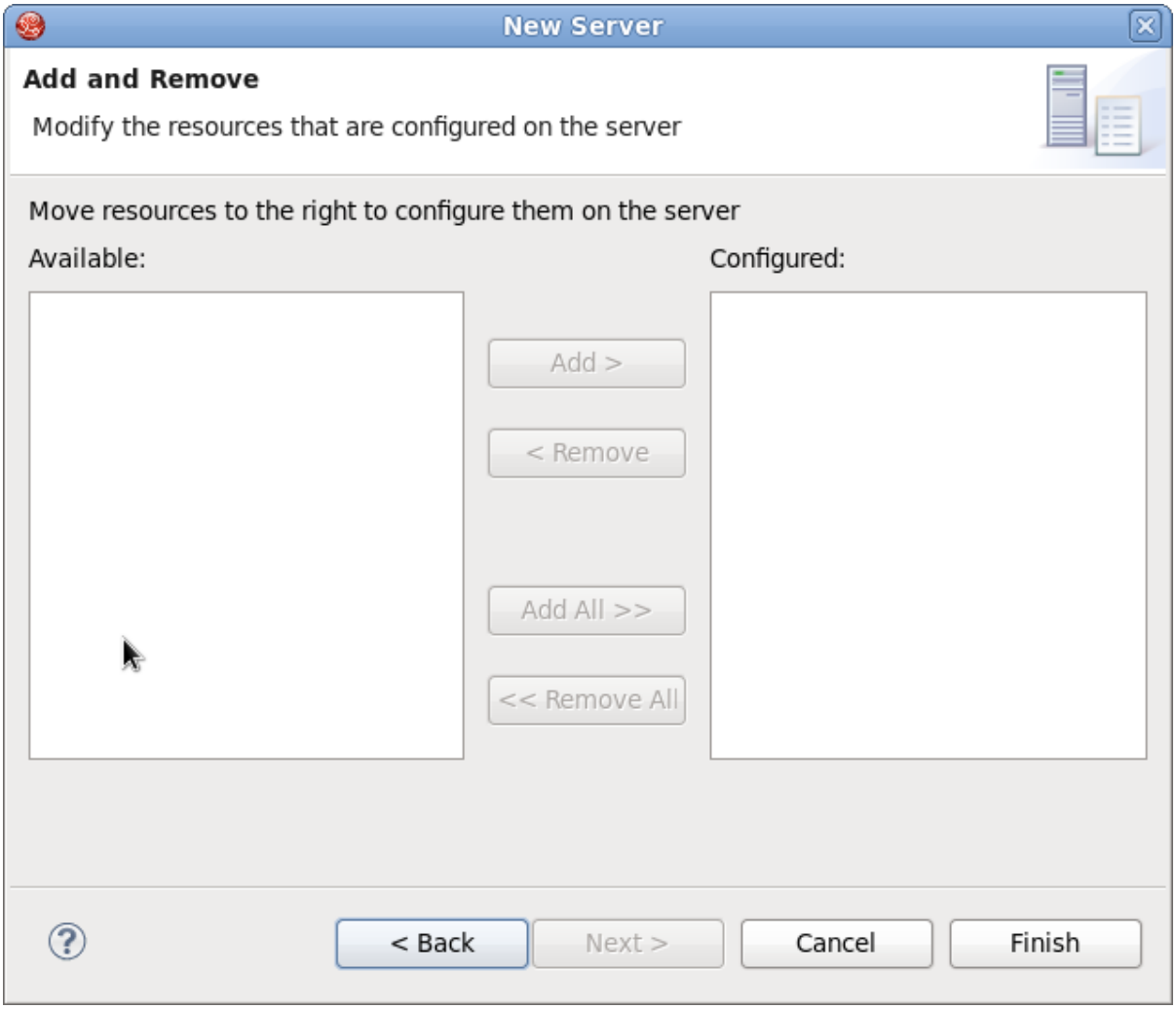


Figure 1.5. Modifier les ressources dans le nouveau serveur de JBoss

Résultat

Le serveur de JBoss Enterprise Application Server 6.0 Runtime est listé dans l'onglet **Serveurs**.

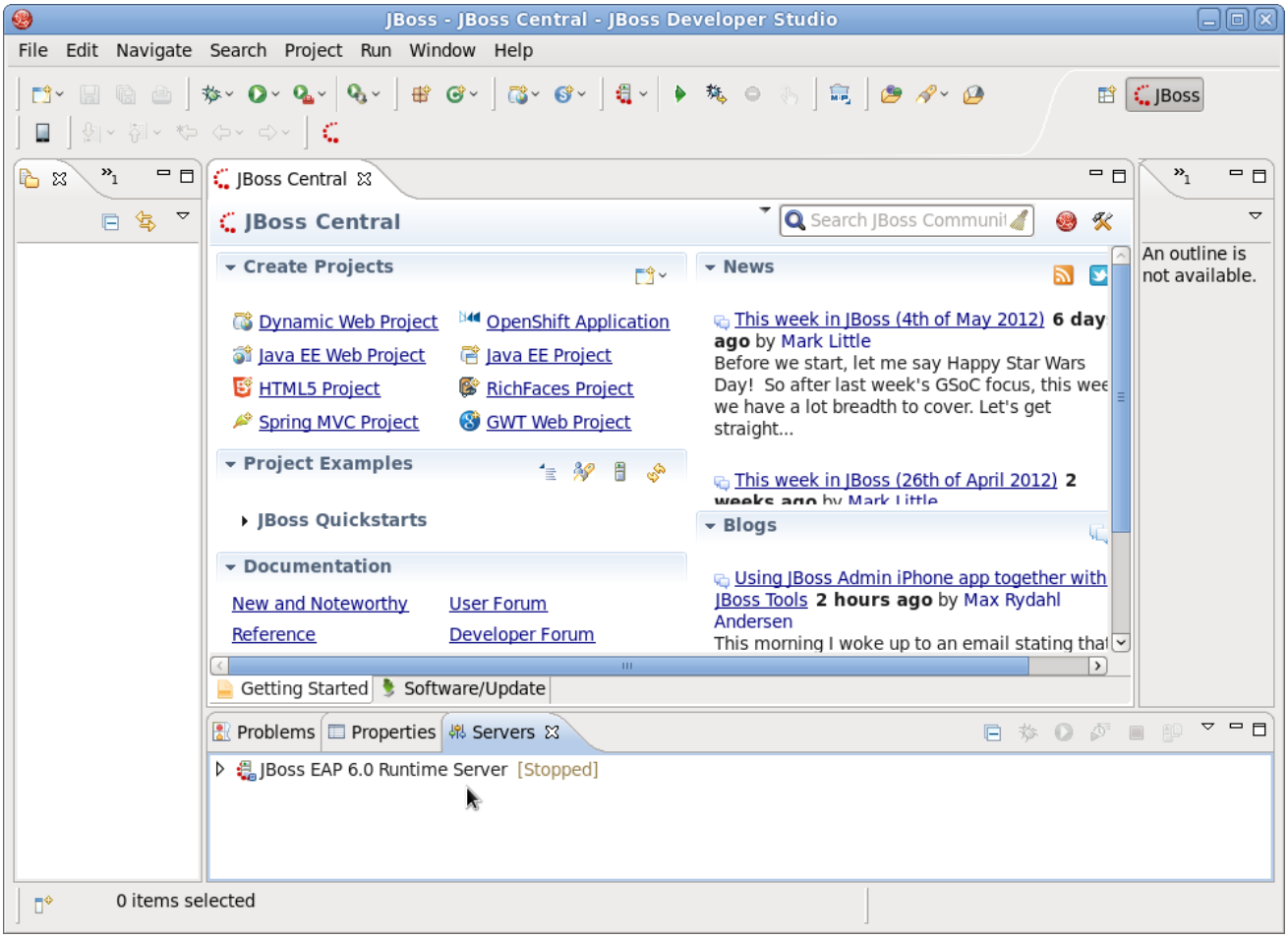


Figure 1.6. Le server apparaît sur la liste de serveurs

Report a bug

1.4. EXÉCUTER VOTRE PREMIÈRE APPLICATION

1.4.1. Remplacer l'application web Welcome par défaut

JBoss EAP 6 inclut l'application Welcome, qui s'affiche quand on ouvre l'URL du serveur sur le port 8080. Vous pouvez remplacer cette application par votre propre application web, en suivant la procédure suivante.

Procédure 1.4. Remplacer l'application web Welcome par défaut par votre propre application web

1. **Désactiver l'application Welcome**
   Utiliser le script de Management CLI ***EAP_HOME*/bin/jboss-cli.sh** pour exécuter la commande suivante. Vous aurez sans doute besoin de modifier un profil de domaine géré, ou retirer une portion de la commande **/profile=default** du serveur autonome.

   ```
   /profile=default/subsystem=web/virtual-server=default-host:write-attribute(name=enable-welcome-root,value=false)
   ```

2. **Configurer votre application web par le contexte root.**
   Afin de configurer votre application web, pour qu'elle utilise (/) comme adresse URL, modifier son fichier **jboss-web.xml**, qui se trouve dans le répertoire **META-INF/** ou **WEB-INF/**. Remplacer sa directive **<context-root>** par une autre qui ressemble à ce qui suit.

```
<jboss-web>
    <context-root>/</context-root>
</jboss-web>
```

3. **Déployer votre application.**
   Déployer votre application pour le groupe de serveurs ou le serveur que vous avez modifié lors de la première étape. L'application est maintenant disponible sur `http://SERVER_URL:PORT/`.

Report a bug

1.4.2. Télécharger les exemples de codes Quickstart

1.4.2.1. Accès aux Quickstarts

Résumé

JBoss EAP 6 contient une série d'exemples quickstart conçus pour aider les utilisateurs à commencer à rédiger des applications en utilisant les technologies Java EE 6.

Prérequis

- Maven 3.0.0 ou versions plus récentes. Pour en savoir plus sur l'installation de Maven, veuillez consulter http://maven.apache.org/download.html.
- Section 2.1.1, « Le référentiel Maven »
- Le référentiel JBoss EAP 6.2 Maven est disponible en ligne, donc il n'est pas utile de le télécharger ou de l'installer localement. Si vous envisagez de l'utiliser en ligne, passer à l'étape suivante. Si vous préférez l'installer dans un référentiel local, consulter : Section 2.2.3, « Installer le référentiel Maven de JBoss EAP 6 localement ».
- Section 2.3.2, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven »

Procédure 1.5. Télécharger les Quickstarts

1. Ouvrir un navigateur web, et accéder à cet URL: https://access.redhat.com/jbossnetwork/restricted/listSoftware.html?product=appplatform.
2. Trouver "Quickstarts" dans la liste.
3. Cliquer sur le bouton **`Télécharger`** pour télécharger un fichier ZIP contenant les exemples.
4. Décompresser l'archive dans un répertoire de votre choix.

Résultat

Les exemples de Java EE Quickstart ont été téléchargés et décompressés. Veuillez consulter le fichier **`README.md`** dans le répertoire supérieur des archives Quickstart pour des instructions concernant le déploiement de chaque quickstart.

Report a bug

1.4.3. Exécuter les Quickstarts

1.4.3.1. Exécuter les Quickstarts (Démarrages rapides) dans JBoss Developer Studio

Procédure 1.6. Importer les Quickstarts dans JBoss Developer Studio

Chaque quickstart est fourni avec un fichier POM (Project Object Model) qui contient des informations de projet et de configuration pour le Quickstart. À l'aide de ce fichier POM, vous pouvez facilement importer le quickstart dans JBoss Developer Studio.

1. Si vous ne l'avez pas encore fait, configurez le référentiel Maven de JBoss EAP en utilisant les paramètres de Maven Section 2.3.2, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven ».

2. Démarrer JBoss Developer Studio.

3. À partir du menu, sélectionner **File** → **Import**.

4. Dans la liste sélectionnée, choisir **Maven** → **Existing Maven Projects**, puis cliquer sur **Next**.

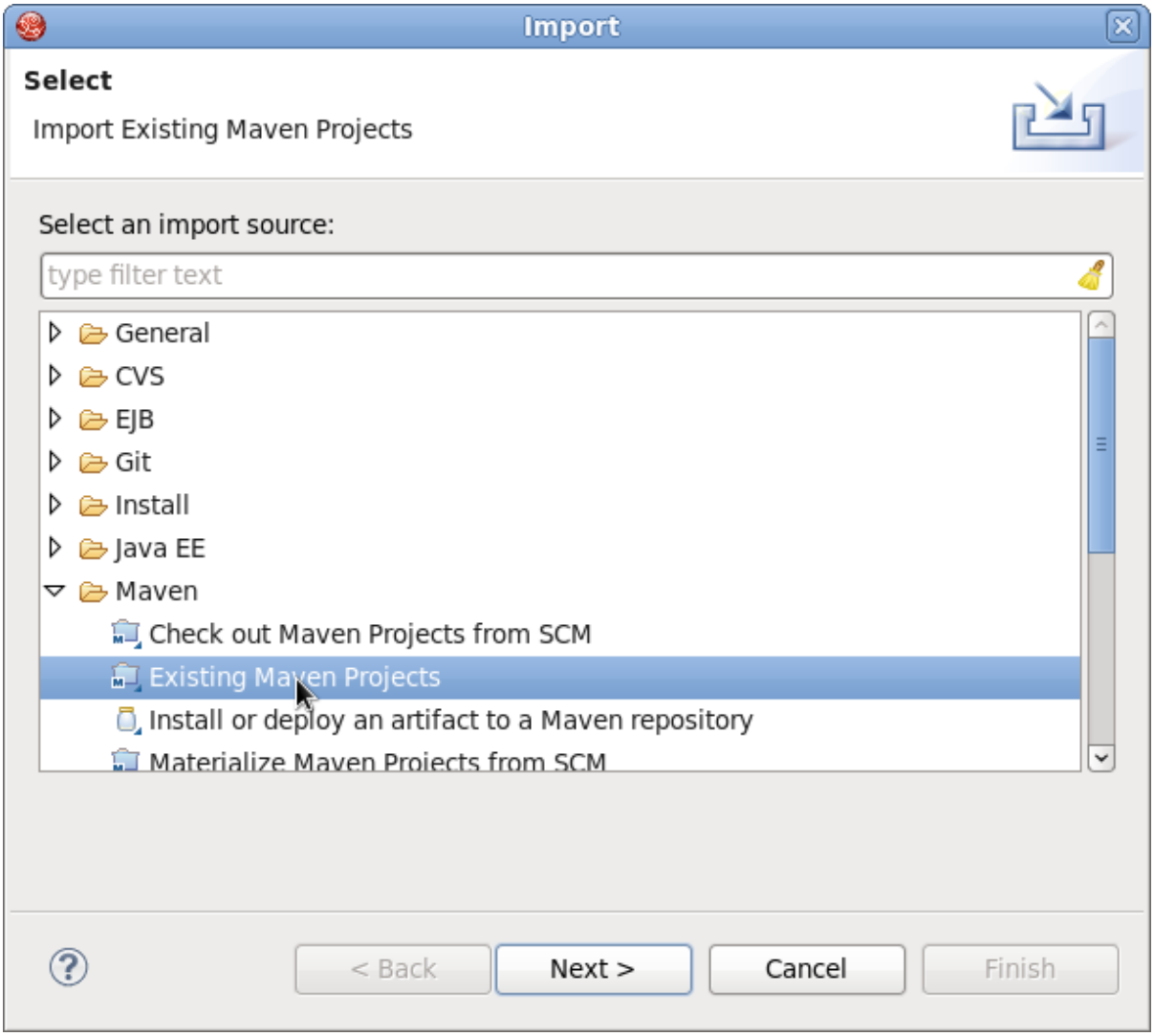


Figure 1.7. Importer les projets Maven existants

5. Naviguer vers le répertoire du quickstart que vous souhaitez importer et cliquer sur **OK**. La zone de liste **Projets** verra apparaître le fichier **pom.xml** du projet quickstart sélectionné.

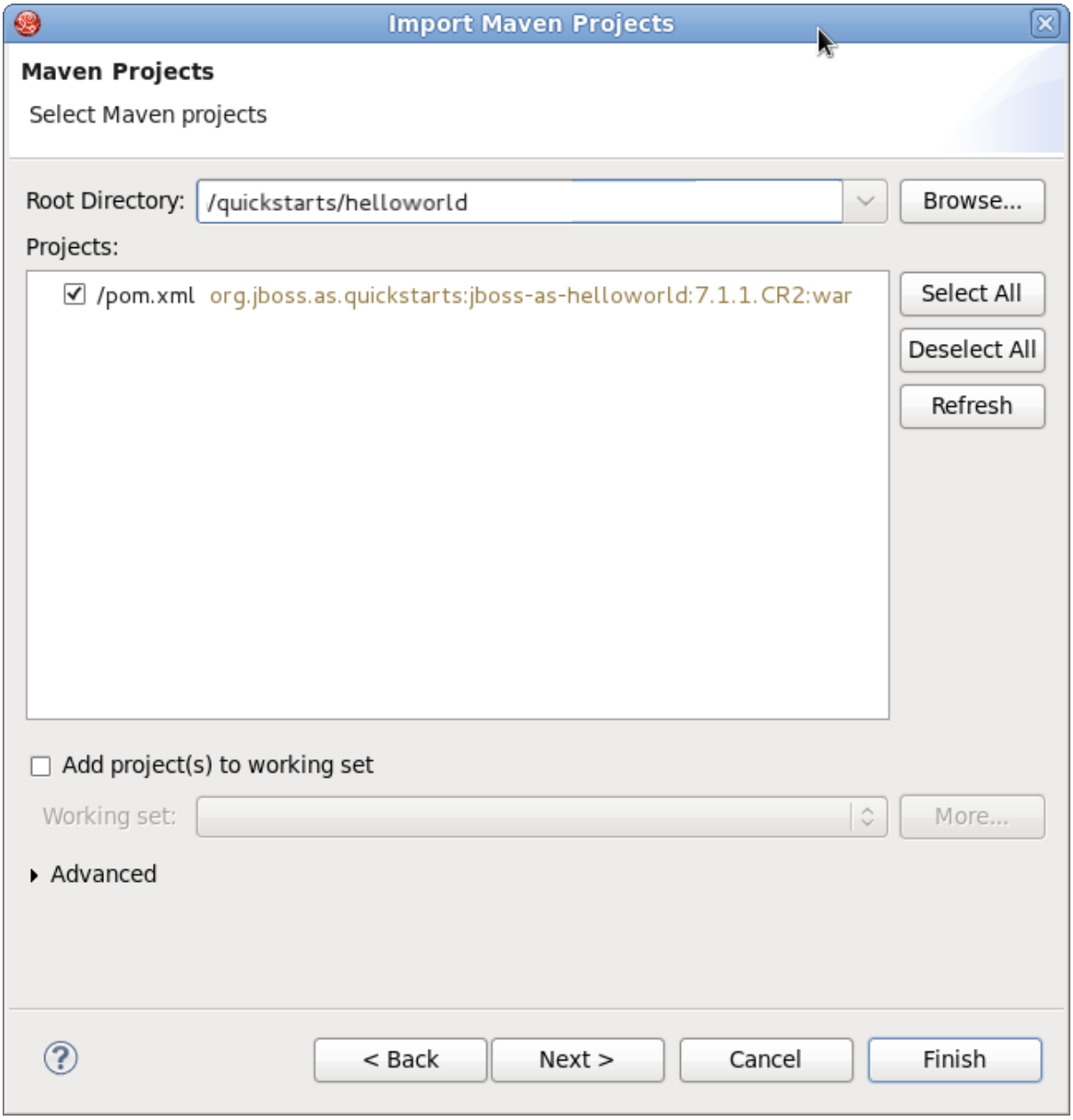


Figure 1.8. Sélectionner les projets Maven

6. Cliquer sur **Suivant**, puis **Terminer**.

Procédure 1.7. Générer et déployer le Quickstart `helloworld`

Le Quickstart **`helloworld`** est un des quickstarts les plus simples et représente une bonne façon de vérifier que le serveur JBoss est configuré et exécute correctement.

1. Ouvrir l'onglet **Serveurs**. Pour l'ajouter dans le panneau :

   a. Cliquer sur **Window** → **Afficher Vue** → **Autre...**.

   b. Sélectionner **Servers** à partir du dossier **Serveur** et cliquer sur **Ok**.

2. Cliquer avec le bouton droit de la souris sur **`helloworld`** dans l'onglet **Project Explorer**, puis sélectionner **Run As** → **Exécuter sur Serveur**.

3. Sélectionner le serveur **JBoss EAP 6.0 Runtime Server** et cliquer sur **Suivant**. Cela devrait déployer le Quickstart **`helloworld`** du serveur JBoss.

4. Afficher la console du serveur. Vous devriez apercevoir le message suivant :

```
JBAS018210: Register web context: /jboss-helloworld
JBAS018559: Deployed "jboss-helloworld.war" (runtime-name : "jboss-
helloworld.war")
```

Le contexte web enregistré se rajoute à **`http://localhost:8080`** pour fournir l'URL utilisé pour accéder à l'application qui est déployée.

5. Pour vérifier que le Quickstart **`helloworld`** a été déployé correctement dans le serveur JBoss, ouvrir le navigateur web, et accéder à l'application dans l'URL: http://localhost:8080/jboss-helloworld

Report a bug

1.4.3.2. Exécuter les Quickstarts par la Ligne de commande

Procédure 1.8. Générer et déployer les Quickstarts par la Ligne de commande

Vous pouvez facilement générer ou déployer les démarrages rapides (Quickstart) par la ligne de commande. Sachez que, lorsque vous utilisez une ligne de commande, vous devrez démarrer le serveur JBoss si nécessaire.

1. **Vérifier le fichier README qui se trouve dans le répertoire racine des quickstarts.**
   Ce fichier contient des informations générales sur les prérequis de systèmes, sur la façon de configurer Maven, comment ajouter des utilisateurs, et comment exécuter les Quickstarts. Lisez attentivement avant de commencer.

   Il contient également un tableau qui répertorie les Quickstarts disponibles. Le tableau répertorie chaque nom de Quickstart et chaque technologie dont il s'agit. Il y a une brève description pour chaque Quickstart et une indication du niveau d'expérience requis pour l'installer. Pour des informations plus détaillées, cliquez sur le nom du Quickstart.

   Certains Quickstarts sont conçus pour améliorer ou étendre d'autres Quickstarts. Ils sont indiqués dans la colonne **`Prérequis`**. Si un Quickstart est associé à une liste de prérequis, vous devrez les installer avant d'utiliser le Quickstart.

   Certains Quickstart ont besoin de l'installation et de la configuraiton des composants optionnels. Ne pas installer ces composants à moins que le Quickstart ne l'exige.

2. **Exécuter le Quickstart `helloworld`**
   Le Quickstart **`helloworld`** est l'un des Quickstarts les plus simples, et représente un bon moyen de vérifier si le serveur JBoss est configuré et exécute correctement. Ouvrir le fichier **README** dans la racine du Quickstart **`helloworld`**. Il contient des instructions détaillées sur la façon de construire et de déployer le Quickstart et d'accéder à l'application en cours.

3. **Exécuter d'autres Quickstarts.**
   Suivre les instructions dans le fichier **README** qui se trouve dans le dossier racine de chaque Quickstart pour exécuter l'exemple.

Report a bug

1.4.4. Revoir les tutoriels Quickstart

1.4.4.1. Découvrir le Quickstart HelloWorld

Résumé

Le Quickstart **`helloworld`** vous montre comment déployer un simple Servlet dans la plateforme JBoss EAP 6. La logique commerciale comprend un service fourni sous forme de bean CDI (Contexts and Dependency Injection) qui est injecté dans le Servlet. Ce Quickstart est très simple. Tout ce qu'il se contente de faire est d'imprimer "Hello World" dans une page web. C'est une bonne façon de savoir si vous avez bien configuré et démarré votre serveur.

Des instructions détaillées sur la façon de construire et de déployer ce Quickstart par la ligne de commande se trouvent dans le fichier README qui se trouve dans le répertoire de Quickstart **`helloworld`**. Nous vous montrons ici comment utiliser JBoss Developer Studio pour exécuter le Quickstart.

Procédure 1.9. Importer le quickstart `helloworld` dans JBoss Developer Studio

Si vous avez précédemment importé tous les Quickstarts dans JBoss Developer Studio en suivant les étapes ici Section 1.4.3.1, « Exécuter les Quickstarts (Démarrages rapides) dans JBoss Developer Studio », vous pouvez passer à la section suivante.

1. Si vous ne l'avez pas encore fait, configurez le référentiel Maven de JBoss EAP en utilisant les paramètres de Maven Section 2.3.2, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven ».
2. Si vous ne l'avez pas encore fait, installez JBoss Developer Studio Section 1.3.1.3, « Installer JBoss Developer Studio 5 ».
3. Section 1.3.1.4, « Démarrer JBoss Developer Studio ».
4. À partir du menu, sélectionner **Fichier** → **Importer**.
5. Dans la liste sélectionnée, choisir **Maven** → **Projets Maven existants**, puis cliquer sur **`Suivant`**.

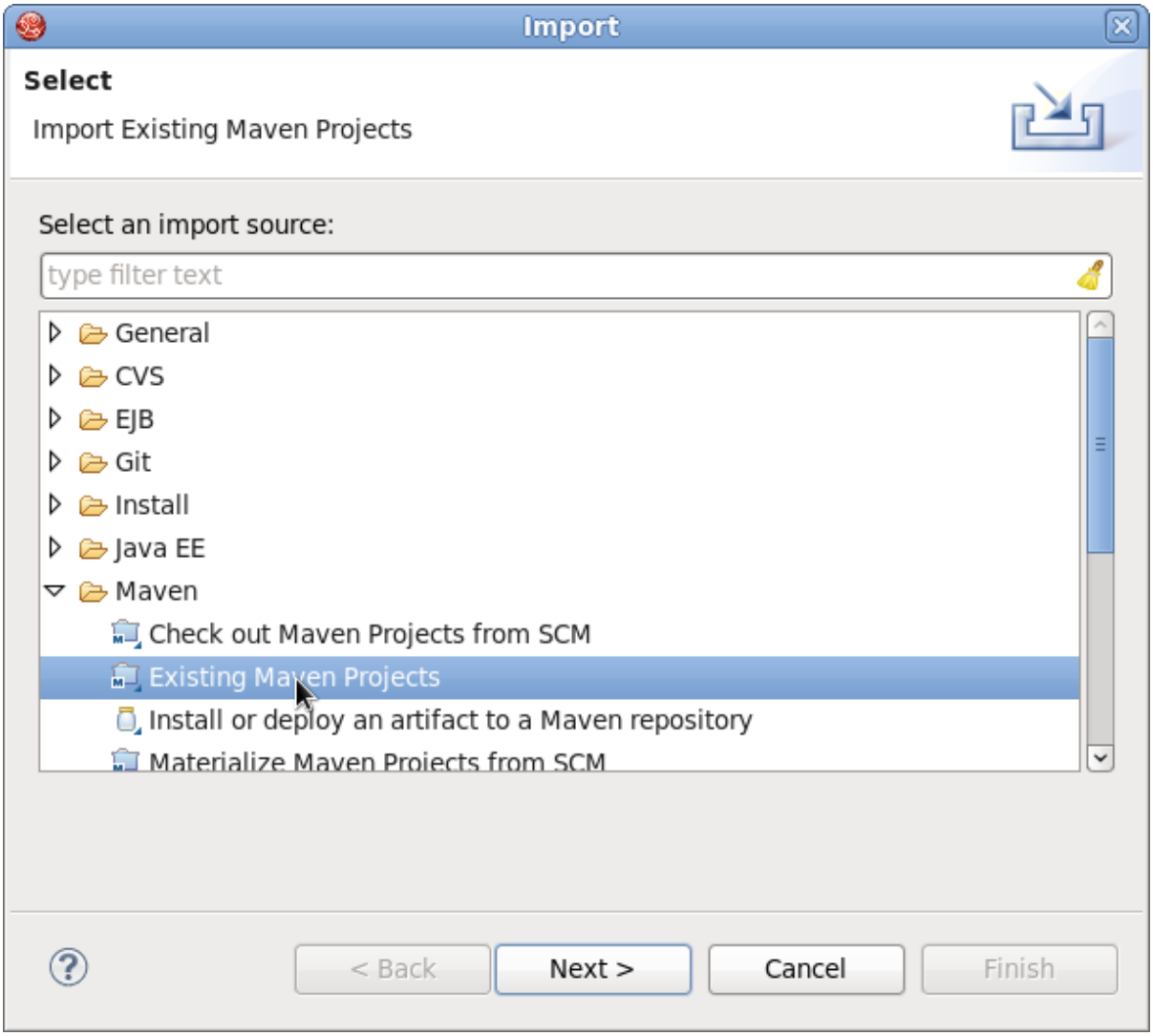


Figure 1.9. Importer les projets Maven existants

6. Naviguer dans le répertoire ***`QUICKSTART_HOME`*`/quickstart/helloworld/`** et cliquer sur le bouton **OK**. La case qui contient la liste **`Projets`** contient le fichier **`pom.xml`** qui vient du projet Quickstart **`helloworld`**.

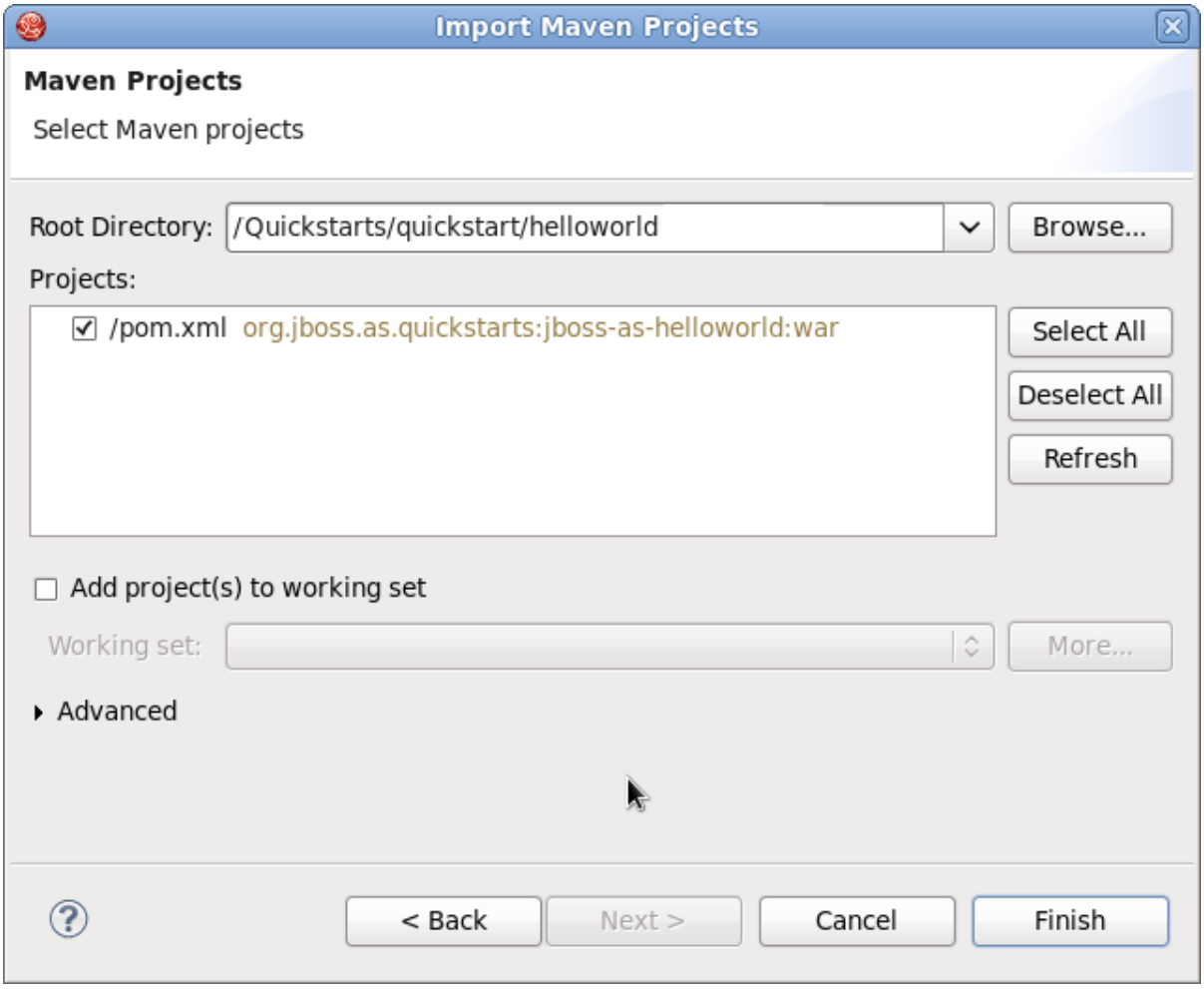


Figure 1.10. Sélectionner les projets Maven

7. Cliquer sur **Finish**.

Procédure 1.10. Générer et déployer le Quickstart `helloworld`

1. Si vous n'avez pas encore configuré JBoss Developer Studio pour JBoss EAP 6, vous devez Section 1.3.1.5, « Ajouter le serveur de JBoss EAP 6 au JBoss Developer Studio » .

2. Cliquer avec le bouton droit de la souris sur **`jboss-as-helloworld`** sur l'onglet **`Project Explorer`**, puis sélectionner **Exécuter en tant que** → **Exécuter sur le serveur**.

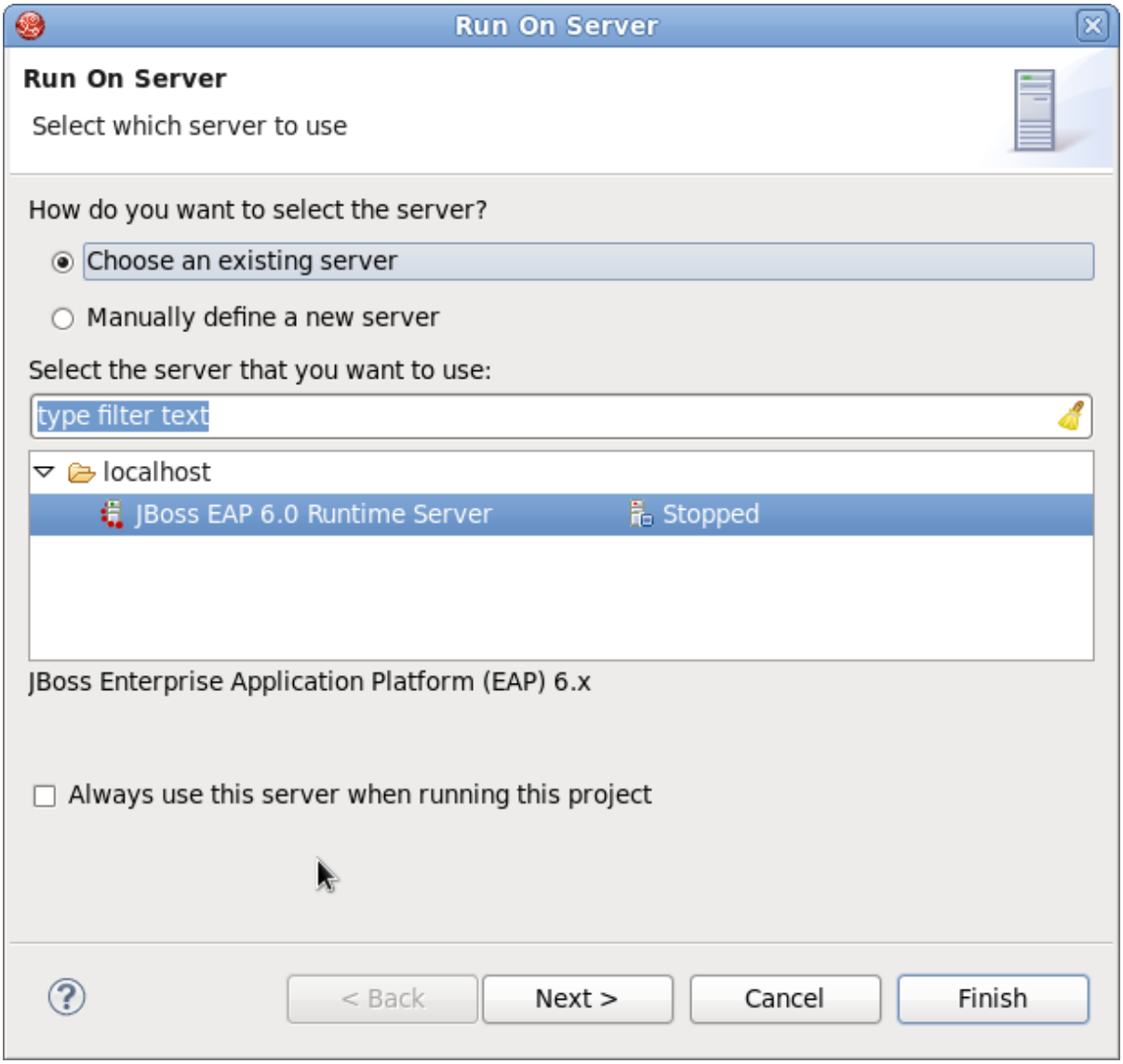


Figure 1.11. Exécuter sur le serveur

3. Sélectionner le serveur **`JBoss EAP 6.0 Runtime Server`** et cliquer sur **`Suivant`**. Cela déploiera le Quickstart **`helloworld`** du serveur JBoss.

4. Pour vérifier que le quickstart **`helloworld`** a bien été déployé dans le serveur JBoss, ouvrir le navigateur web et accéder à l'application par le lien URL suivant : http://localhost:8080/jboss-as-helloworld

Procédure 1.11. Observer la structure du répertoire

Le code du Quickstart **`helloworld`** se trouve dans le répertoire ***`QUICKSTART_HOME`***`/helloworld`. Le Quickstart **`helloworld`** comprend un Servlet et un bean CDI. Il comprend également un fichier beans.xml qui indique à JBoss EAP 6 comment trouver des beans pour cette application et comment activer le CDI.

1. Le fichier **`beans.xml`** se trouve dans le dossier **`WEB-INF/`** qui se trouve dans le répertoire **`src/main/webapp/`** du Quickstart.

2. Le répertoire **`src/main/webapp/`** inclut également un fichier **`index.html`** qui utilise une simple réactualisation meta pour rediriger le navigateur de l'utilisateur vers le Servlet, qui se trouve à http://localhost:8080/jboss-as-helloworld/HelloWorld.

3. Tous les fichiers de configuration de cet exemple se trouvent dans **`WEB-INF/`**, qui se trouve dans le répertoire **`src/main/webapp/`** de l'exemple.

4. Notez que le Quickstart n'a pas même besoin d'un fichier **`web.xml`**!

Procédure 1.12. Examiner le code

La déclaration de paquet et les importations ont été exclues de ces listes. La liste complète est disponible dans le code source du Quickstart.

1. **Vérifier le code HelloWorldServlet**
   Le fichier **`HelloWorldServlet.java`** se trouve dans le répertoire **`src/main/java/org/jboss/as/quickstarts/helloworld/`**. Le Servlet envoie les informations dans le navigateur.

```
27. @WebServlet("/HelloWorld")
28. public class HelloWorldServlet extends HttpServlet {
29.
30.    static String PAGE_HEADER = "<html><head /><body>";
31.
32.    static String PAGE_FOOTER = "</body></html>";
33.
34.    @Inject
35.    HelloService helloService;
36.
37.    @Override
38.    protected void doGet(HttpServletRequest req,
HttpServletResponse resp)
                              throws ServletException, IOException
{
39.       PrintWriter writer = resp.getWriter();
40.       writer.println(PAGE_HEADER);
41.       writer.println("<h1>" +
helloService.createHelloMessage("World") + "</h1>");
42.       writer.println(PAGE_FOOTER);
43.       writer.close();
44.     }
45.
46. }
```

Tableau 1.1. Infos HelloWorldServlet

Ligne	Note
27	Avant Java EE 6, on utilisait un fichier XML pour enregistrer les Servlets. C'est bien plus clean. Tout ce qu'il vous reste à faire est d'ajouter l'annotation **`@WebServlet`** et de fournir un mappage vers un URL qui est utilisé pour accéder au serveur.
30-32	Chaque page web a besoin d'HTML formé correctement. Ce Quickstart utilise les Strings statiques pour écrire les sorties minimum de l'en-tête et du pied de page.

Ligne	Note
34-35	Ces lignes injectent le bean CDI HelloService, qui génère le message réel. Tant que nous ne changeons les API de HelloService, cette approche nous permet de modifier l'implémentation de HelloService à une date ultérieure sans changer l'affichage.
41	Cette ligne appelle le service pour générer le message "Hello World", et l'écrire dans la requête HTTP.

2. **Vérifier le code HelloService**
   Le fichier **`HelloService.java`** se trouve dans le répertoire **`src/main/java/org/jboss/as/quickstarts/helloworld/`**. Ce service est très simple. Il renvoie un message. Nul besoin d'enregistrement d'annotation ou XML.

```
 9. public class HelloService {
10.
11.    String createHelloMessage(String name) {
12.       return "Hello " + name + "!";
32.    }
33. }
34.
```

Report a bug

1.4.4.2. Découvrir le Quickstart numberguess

Résumé

Ce Quickstart vous montre comment créer et déployer une simple application de JBoss EAP 6. Cette application ne persiste pas n'importe quelle information. Les informations sont affichées par JSF, et la logique métier est encapsulée dans deux beans CDI. Dans le Quickstart **`numberguess`**, vous obtenez 10 tentatives pour deviner un nombre entre 1 et 100. Après chaque tentative, on vous indique si votre estimation est trop élevée ou trop faible.

Le code du Quickstart **`numberguess`** se trouve dans le répertoire ***`QUICKSTART_HOME`***`/numberguess`. Le Quickstart **`hnumberguess`** comprend un certain nombre de beans, des fichiers de configuration et des affichages Facelets (JSF), tout cela dans un package de module WAR.

Des instructions détaillées sur la façon de construire et de déployer ce Quickstart par la ligne de commande se trouvent dans le fichier README qui se trouve dans le répertoire de Quickstart **`numberguess`**. Nous vous montrons ici comment utiliser JBoss Developer Studio pour exécuter le Quickstart.

Procédure 1.13. Importer le quickstart `numberguess` dans JBoss Developer Studio

Si vous avez précédemment importé tous les Quickstarts dans JBoss Developer Studio en suivant les étapes de la procédure suivante, Section 1.4.3.1, « Exécuter les Quickstarts (Démarrages rapides) dans JBoss Developer Studio », vous pouvez passer à la section suivante.

1. Si vous ne l'avez pas encore fait, effectuer les procédures suivantes : Section 1.3.1.3, « Installer JBoss Developer Studio 5 »

2. Section 1.3.1.4, « Démarrer JBoss Developer Studio »

3. À partir du menu, sélectionner **Fichier** → **Importer**.

4. Dans la liste sélectionnée, choisir **Maven** → **Projets Maven existants**, puis cliquer sur **Suivant**.

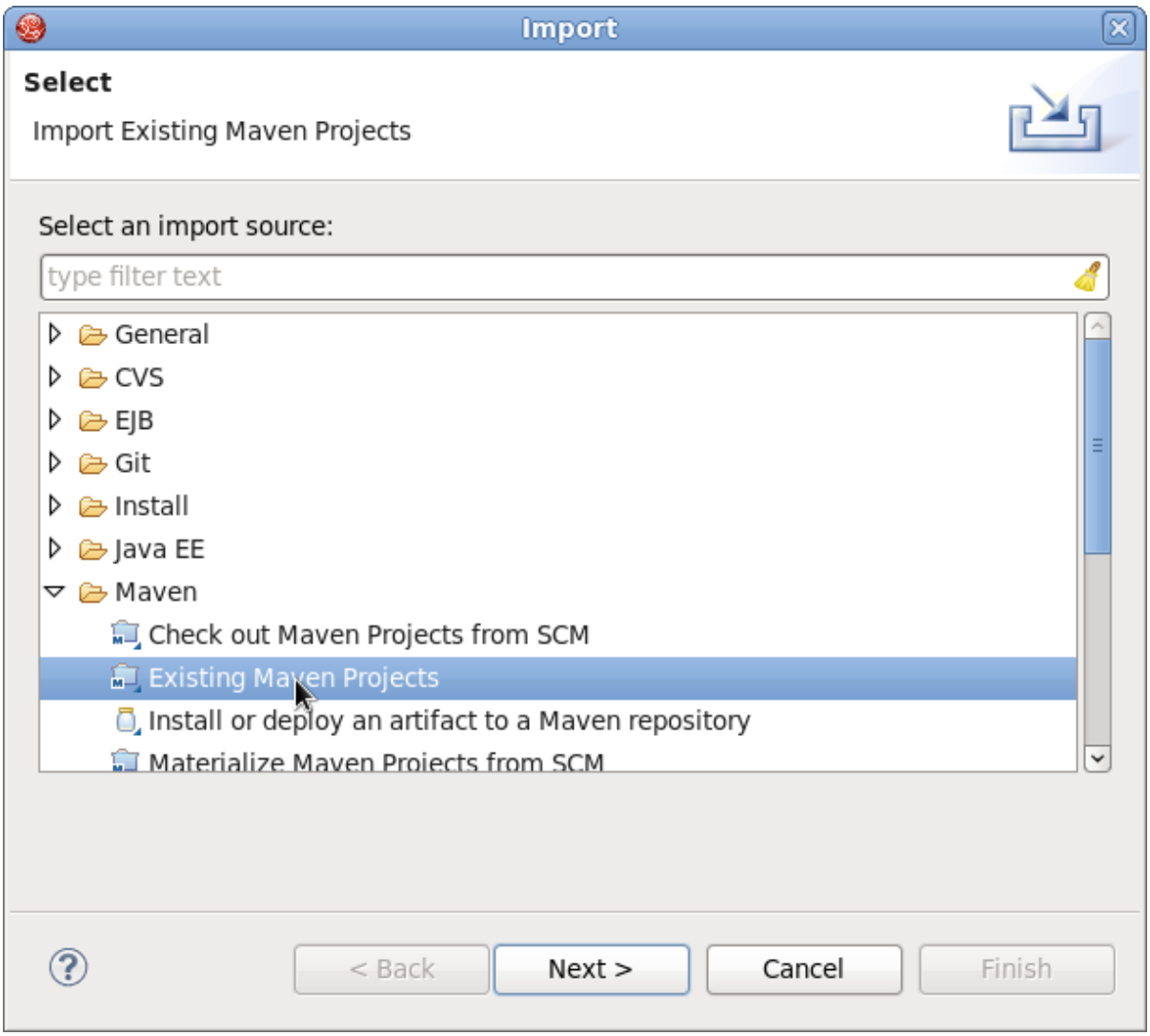


Figure 1.12. Importer les projets Maven existants

5. Naviguer dans le répertoire ***QUICKSTART_HOME*/quickstart/numberguess/** et cliquer sur le bouton **OK**. La case qui contient la liste **Projets** contient le fichier **pom.xml** qui vient du projet Quickstart **helloworld**.

6. Cliquer sur **Terminé**.

Procédure 1.14. Générer et déployer le Quickstart numberguess

1. Si vous n'avez pas encore configuré JBoss Developer Studio pour JBoss EAP 6, vous devez faire la chose suivante : Section 1.3.1.5, « Ajouter le serveur de JBoss EAP 6 au JBoss Developer Studio ».

2. Cliquer avec le bouton droit de la souris sur **jboss-as-numberguess** sur l'onglet **Project Explorer**, puis sélectionner **Exécuter en tant que** → **Exécuter sur serveur**.

3. Sélectionner le serveur **JBoss EAP 6.0 Runtime Server** et cliquer sur **Suivant**. Cela déployera le Quickstart **numberguess** du serveur JBoss.

4. Pour vérifier que le quickstart **numberguess** a bien été déployé dans le serveur JBoss, ouvrir le navigateur web et accéder à l'application en cliquant sur cet URL : http://localhost:8080/jboss-as-numberguess

Procédure 1.15. Examiner les fichiers de configuration

Tous les fichiers de configuration de cet exemple se trouvent dans le répertoire **WEB-INF/**, qui se trouvent dans le répertoire **src/main/webapp/** du Quickstart.

1. **Voir le fichier faces-config**
   Ce Quickstart utilise la version de JSF 2.0 de **faces-config.xml**. Une version normalisée de Facelets correspond au gestionnaire d'affichage par défaut de JSF 2.0, donc il n'y a par vraiment grand chose à configurer. JBoss EAP 6 va au-delà de Java EE ici. Il va automatiquement configurer JSF pour vous, si vous incluez ce fichier de configuration. En conséquence, la configuration ne consistera uniquement en l'élément racine :

```
03. <faces-config version="2.0"
04.     xmlns="http://java.sun.com/xml/ns/javaee"
05.     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
06.     xsi:schemaLocation="
07.        http://java.sun.com/xml/ns/javaee>
08.        http://java.sun.com/xml/ns/javaee/web-
facesconfig_2_0.xsd">
09.
10. </faces-config>
```

2. **Voir le fichier beans.xml**
   Il y a également un fichier **beans.xml** qui indique à JBoss EAP 6 de chercher des beans dans cette application et d'activer le CDI.

3. **Il n'y a pas de fichier web.xml**
   Notez que le Quickstart n'a pas même besoin d'un fichier **web.xml**!

Procédure 1.16. Examiner le code JSF

JSF utilise l'extension de fichier **.xhtml** pour les fichiers source, mais s'occupe des vues rendues par l'extension **.jsf**.

- **Examiner le code home.xhtml**
  Le fichier **home.xhtml** se trouve dans le répertoire **src/main/webapp/**.

```
03. <html xmlns="http://www.w3.org/1999/xhtml"
04.     xmlns:ui="http://java.sun.com/jsf/facelets"
05.     xmlns:h="http://java.sun.com/jsf/html"
06.     xmlns:f="http://java.sun.com/jsf/core">
07.
08. <head>
09. <meta http-equiv="Content-Type" content="text/html; charset=iso-
8859-1" />
10. <title>Numberguess</title>
```

```
11. </head>
12.
13. <body>
14.    <div id="content">
15.       <h1>Guess a number...</h1>
16.       <h:form id="numberGuess">
17.
18.          <!-- Feedback for the user on their guess -->
19.          <div style="color: red">
20.             <h:messages id="messages" globalOnly="false" />
21.             <h:outputText id="Higher" value="Higher!"
22.                rendered="#{game.number gt game.guess and
game.guess ne 0}" />
23.             <h:outputText id="Lower" value="Lower!"
24.                rendered="#{game.number lt game.guess and
game.guess ne 0}" />
25.          </div>
26.
27.          <!-- Instructions for the user -->
28.          <div>
29.             I'm thinking of a number between <span
30.                id="numberGuess:smallest">#
{game.smallest}</span> and <span
31.                id="numberGuess:biggest">#{game.biggest}</span>.
You have
32.             #{game.remainingGuesses} guesses remaining.
33.          </div>
34.
35.          <!-- Input box for the users guess, plus a button to
submit, and reset -->
36.          <!-- These are bound using EL to our CDI beans -->
37.          <div>
38.             Your guess:
39.             <h:inputText id="inputGuess" value="#{game.guess}"
40.                required="true" size="3"
41.                disabled="#{game.number eq game.guess}"
42.                validator="#{game.validateNumberRange}" />
43.             <h:commandButton id="guessButton" value="Guess"
44.                action="#{game.check}"
45.                disabled="#{game.number eq game.guess}" />
46.          </div>
47.          <div>
48.             <h:commandButton id="restartButton" value="Reset"
49.                action="#{game.reset}" immediate="true" />
50.          </div>
51.       </h:form>
52.
53.    </div>
54.
55.    <br style="clear: both" />
56.
57. </body>
58. </html>
```

Tableau 1.2. Infos JSF

Ligne	Note
20-24	Voici les messages qui peuvent être envoyés par l'utilisateur : "Higher!" et "Lower!"
29-32	Au fur et à mesure que l'utilisateur devine, l'étendue des nombres qu'ils devinent se rétrécit. Cette phrase change pour s'assurer qu'ils connaissent la portée d'une tentative valide.
38-42	Ce champ d'entrée est lié à une propriété de bean qui utilise une expression de valeur.
42	On utilise une liaison de validateur pour s'assurer que l'utilisateur ne mette pas le nombre qu'il devine en dehors de la limite. Si le validateur n'était pas présent, l'utilisateur peut deviner un nombre en dehors de la limite.
43-45	Il doit y avoir un moyen pour que l'utilisateur envoie le nombre qu'il devine au serveur. Ici, on associe une méthode d'action sur le bean.

Procédure 1.17. Examiner les fichiers de classe

Tous les fichiers source du Quickstart **numberguess** se trouvent dans le répertoire **src/main/java/org/jboss/as/quickstarts/numberguess/**. :a déclaration de paquet et les importations ont été exclues de ces listings. La liste complète se trouve dans le code source du Quickstart.

1. **Vérifier le code du qualificateur Random.java**
   Un qualificateur est utilisé pour supprimer l'ambiguïté entre deux beans, qui sont tous deux admissibles pour l'injection selon leur type. Pour plus d'informations sur les qualificateurs, voir Section 9.2.3.3, « Utiliser un qualificateur pour résoudre une injection ambiguë »

   Le qualificateur **@Random** est utilisé pour injecter un nombre au hasard.

```
21. @Target({ TYPE, METHOD, PARAMETER, FIELD })
22. @Retention(RUNTIME)
23. @Documented
24. @Qualifier
25. public @interface Random {
26.
27. }
```

2. **Vérifier le code du qualificateur MaxNumber.java**
   Le **qualificateur@MaxNumber** est utilisé pour injecter le nombre maximum autorisé.

```
21. @Target({ TYPE, METHOD, PARAMETER, FIELD })
22. @Retention(RUNTIME)
23. @Documented
24. @Qualifier
25. public @interface MaxNumber {
26.
27. }
```

3. **Vérifier le code du générateur**
   La classe **`Generator`** est chargé de créer le nombre aléatoire par une méthode de producteur. Elle indique également le nombre maximum possible par une méthode de producteur. Cette classe reste dans la portée de l'application, donc, vous n'obtenez pas un nombre différent au hasard à chaque fois.

```
28. @ApplicationScoped
29. public class Generator implements Serializable {
30.    private static final long serialVersionUID =
-7213673465118041882L;
31.
32.    private java.util.Random random = new
java.util.Random(System.currentTimeMillis());
33.
34.    private int maxNumber = 100;
35.
36.    java.util.Random getRandom() {
37.       return random;
38.    }
39.
40.    @Produces
41.    @Random
42.    int next() {
43.       // a number between 1 and 100
44.       return getRandom().nextInt(maxNumber - 1) + 1;
45.    }
46.
47.    @Produces
48.    @MaxNumber
49.    int getMaxNumber() {
50.       return maxNumber;
51.    }
52. }
```

4. **Vérifier le code Game**
   La classe session scoped **`Game`** est le point d'entrée principal de l'application. Elle est là pour initialiser et réinitialiser le jeu, pour capturer et valider la tentative de numéro de l'utilisateur, et afin de fournir un commentaire de retour à l'utilisateur avec un **`FacesMessage`**. Elle utilise une méthode de cycle de vie de post-construction pour initialiser le jeu, en tirant un nombre au hasard du bean **`@Random Instance<Integer>`**.

   Notez l'annotation @Named dans la classe. Cette annotation est uniquement requise quand on veut rendre le bean accessible à une vue JSF via Expression Language (EL), et dans ce cas # **`{game}`**.

```
035. @Named
036. @SessionScoped
037. public class Game implements Serializable {
038.
039.    private static final long serialVersionUID =
991300443278089016L;
040.
041.    /**
042.     * The number that the user needs to guess
```

```
043.     */
044.    private int number;
045.
046.    /**
047.     * The users latest guess
048.     */
049.    private int guess;
050.
051.    /**
052.     * The smallest number guessed so far (so we can track the
valid guess range).
053.     */
054.    private int smallest;
055.
056.    /**
057.     * The largest number guessed so far
058.     */
059.    private int biggest;
060.
061.    /**
062.     * The number of guesses remaining
063.     */
064.    private int remainingGuesses;
065.
066.    /**
067.     * The maximum number we should ask them to guess
068.     */
069.    @Inject
070.    @MaxNumber
071.    private int maxNumber;
072.
073.    /**
074.     * The random number to guess
075.     */
076.    @Inject
077.    @Random
078.    Instance<Integer> randomNumber;
079.
080.    public Game() {
081.    }
082.
083.    public int getNumber() {
084.       return number;
085.    }
086.
087.    public int getGuess() {
088.       return guess;
089.    }
090.
091.    public void setGuess(int guess) {
092.       this.guess = guess;
093.    }
094.
095.    public int getSmallest() {
096.       return smallest;
097.    }
```

```
098.
099.    public int getBiggest() {
100.       return biggest;
101.    }
102.
103.    public int getRemainingGuesses() {
104.       return remainingGuesses;
105.    }
106.
107.    /**
108.     * Check whether the current guess is correct, and update
the biggest/smallest guesses as needed.
109.     * Give feedback to the user if they are correct.
110.     */
111.    public void check() {
112.       if (guess > number) {
113.          biggest = guess - 1;
114.       } else if (guess < number) {
115.          smallest = guess + 1;
116.       } else if (guess == number) {
117.          FacesContext.getCurrentInstance().addMessage(null, new
FacesMessage("Correct!"));
118.       }
119.       remainingGuesses--;
120.    }
121.
122.    /**
123.     * Reset the game, by putting all values back to their
defaults, and getting a new random number.
124.     * We also call this method when the user starts playing for
the first time using
125.     * {@linkplain PostConstruct @PostConstruct} to set the
initial values.
126.     */
127.    @PostConstruct
128.    public void reset() {
129.       this.smallest = 0;
130.       this.guess = 0;
131.       this.remainingGuesses = 10;
132.       this.biggest = maxNumber;
133.       this.number = randomNumber.get();
134.    }
135.
136.    /**
137.     * A JSF validation method which checks whether the guess is
valid. It might not be valid because
138.     * there are no guesses left, or because the guess is not in
range.
139.     *
140.     */
141.    public void validateNumberRange(FacesContext context,
UIComponent toValidate, Object value) {
142.       if (remainingGuesses <= 0) {
143.          FacesMessage message = new FacesMessage("No guesses
left!");
144.          context.addMessage(toValidate.getClientId(context),
```

```
message);
145.          ((UIInput) toValidate).setValid(false);
146.          return;
147.       }
148.       int input = (Integer) value;
149.
150.       if (input < smallest || input > biggest) {
151.          ((UIInput) toValidate).setValid(false);
152.
153.          FacesMessage message = new FacesMessage("Invalid
guess");
154.          context.addMessage(toValidate.getClientId(context),
message);
155.       }
156.    }
157. }
```

Report a bug

CHAPITRE 2. GUIDE MAVEN

2.1. POUR EN SAVOIR PLUS SUR MAVEN

2.1.1. Le référentiel Maven

Apache Maven est un outil d'automation de construction distribué, utilisé en développement Java pour créer, gérer et générer des projets informatiques. Maven utilise des fichiers de configuration nommés Project Object Model, ou POM, pour définir des projets et gérer le processus de construction. Les POM décrivent le module et les dépendance du composant, et les sorties sont sous forme de fichier XML. Cela assure que le projet soit construit de façon correcte et uniforme.

Maven y parvient en utilisant un référentiel. Un référentiel Maven stocke les bibliothèques, plug-ins et autres artefacts de la build. Le référentiel public par défaut est le Maven 2 Central Repository , mais les référentiels peuvent être privés et internes à une entreprise dans le but de partager des artefacts communs au sein d'équipes de développeurs. Les référentiels sont également disponibles auprès de tierces parties. JBoss EAP 6 comprend un référentiel Maven contenant un grand nombre des prérequis que les développeurs de Java EE utilisent habituellement pour développer des applications sous JBoss EAP 6. Pour configurer votre projet pour utiliser ce référentiel, veuillez consulter Section 2.3.1, « Configurer le référentiel Maven de JBoss EAP ».

Un référentiel peut être local ou distant. Les référentiels distants sont accessibles par des protocoles communs tels que `http://` pour un référentiel sur un serveur HTTP ou `file://` pour un référentiel de serveur de fichiers. Un référentiel local correspond à un téléchargement cache des artefacts à partir d'un référentiel distant.

Pour davantage d'informations sur Maven, voir Welcome to Apache Maven .

Pour davantage d'informations sur les référentiels Maven, voir Apache Maven Project - Introduction to Repositories.

Pour davantage d'informations sur les fichiers POM Maven, veuillez consulter Apache Maven Project POM Reference et Section 2.1.2, « Le fichier POM Maven » .

Report a bug

2.1.2. Le fichier POM Maven

Un fichier POM (Project Object Model) est un fichier de configuration utilisé par Marven pour compiler des projets. Il s'agit d'un fichier XML contenant des informations sur un projet et sur comment le compiler, comme par exemple l'emplacement des répertoires source, test et cible, les dépendances des projets, les réferentiels de plug-ins et les objectifs qu'il peut exécuter. Il peut également comprendre des détails supplémentaires sur le projet, comme, en autre, sa version, sa description, ses développeurs, sa liste de diffusion et sa licence. Un fichier `pom.xml` requiert certaines options de configuration définissant la valeur par défaut. Voir Section 2.1.3, « Prérequis minimum pour un fichier POM Maven » pour plus de détails.

Le schéma pour le fichier `pom.xml` est disponible sur le lien http://maven.apache.org/maven-v4_0_0.xsd.

Pour plus d'informations concernant les fichiers POM, veuillez consulter Apache Maven Project POM Reference.

Report a bug

2.1.3. Prérequis minimum pour un fichier POM Maven

Prérequis minimum

Les prérequis minimum pour un fichier **pom.xml** sont les suivants :

- project root
- modelVersion
- groupId - l'id du groupe du projet
- artifactId - l'id de l'artifact (projet)
- version - la version de l'artifact dans le groupe spécifié

Échantillon de fichier pom.xml

Un fichier **pom.xml** de base devrait resssembler à ceci :

```
<project>
  <modelVersion>4.0.0</modelVersion>
  <groupId>com.jboss.app</groupId>
  <artifactId>my-app</artifactId>
  <version>1</version>
</project>
```

Report a bug

2.1.4. Le fichier des configurations de Maven

Le fichier Maven **settings.xml** contient des informations de configuration spécifiques à l'utilisateur pour Maven. Il contient des informations qui ne devraient pas être distribuées dans le fichier **pom.xml**, comme l'identité du développeur, l'information sur le proxy, l'emplacement du référentiel local, et autres paramètres propres à un utilisateur.

Il y a deux endroits où on peut trouver le fichier **settings.xml**.

Dans l'installation Maven

Le fichier de configuration se trouve dans le répertoire ***M2_HOME*/conf/**. On les appelle les paramètres **globaux**. Le fichier de configuration Maven par défaut est un modèle qui peut être copié et utilisé comme point de départ pour le fichier des paramètres utilisateur.

Dans l'installation de l'utilisateur

Le fichier de configuration se trouve dans le répertoire ***USER_HOME*/.m2/**. Si les fichiers **settings.xml** et Maven existent tous les deux, leurs contenus seront fusionnés. S'il y a une intersection, le fichier utilisateur **settings.xml** aura priorité.

Voici un exemple d'un fichier **settings.xml** Maven :

```
<?xml version="1.0" encoding="UTF-8"?>
<settings xmlns="http://maven.apache.org/SETTINGS/1.0.0"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
          xsi:schemaLocation="http://maven.apache.org/SETTINGS/1.0.0
http://maven.apache.org/xsd/settings-1.0.0.xsd">
  <profiles>
    <!-- Configure the JBoss EAP Maven repository -->
    <profile>
      <id>jboss-eap-maven-repository</id>
      <repositories>
        <repository>
          <id>jboss-eap</id>
          <url>file:///path/to/repo/jboss-eap-6.0-maven-repository</url>
          <releases>
            <enabled>true</enabled>
          </releases>
          <snapshots>
            <enabled>false</enabled>
          </snapshots>
        </repository>
      </repositories>
      <pluginRepositories>
        <pluginRepository>
          <id>jboss-eap-maven-plugin-repository</id>
          <url>file:///path/to/repo/jboss-eap-6.0-maven-repository</url>
          <releases>
            <enabled>true</enabled>
          </releases>
          <snapshots>
            <enabled>false</enabled>
          </snapshots>
        </pluginRepository>
      </pluginRepositories>
    </profile>
  </profiles>
  <activeProfiles>
    <!-- Optionally, make the repository active by default -->
    <activeProfile>jboss-eap-maven-repository</activeProfile>
  </activeProfiles>
</settings>
```

On peut trouver le schéma du fichier **`settings.xml`** à l'adresse suivante http://maven.apache.org/xsd/settings-1.0.0.xsd.

Report a bug

2.2. INSTALLER LE RÉFÉRENTIEL JBOSS MAVEN ET MAVEN

2.2.1. Télécharger et installer Maven

1. Aller dans Apache Maven Project - Download Maven et télécharger la dernière distribution de votre système d'exploitation.

2. Voir la documentation Maven pour les informations sur le façon de télécharger et installer Apache Maven sur votre système d'exploitation.

Report a bug

2.2.2. Installer le référentiel Maven de JBoss EAP 6

Il y a trois moyens d'installer le référentiel; sur votre système de fichiers local, sur le serveur web Apache, ou par un gestionnaire de référentiel Maven.

- Section 2.2.3, « Installer le référentiel Maven de JBoss EAP 6 localement »
- Section 2.2.4, « Installer le référentiel Maven de JBoss EAP 6 à utiliser avec Appache httpd »
- Section 2.2.5, « Installer le référentiel Maven de JBoss EAP 6 en utilisant le gestionnaire de référentiels Nexus Maven »

Report a bug

2.2.3. Installer le référentiel Maven de JBoss EAP 6 localement

Résumé

Le référentiel de JBoss EAP 6.2 Maven est disponible en ligne. Il n'est pas donc nécessaire de le télécharger et de l'installer localement. Toutefois, si vous préférez installer le référentiel JBoss EAP Maven localement, il y a trois façons de procéder : sur votre système de fichiers local, sur le serveur Web Apache, ou avec un gestionnaire de référentiel Maven. Cet exemple couvre les étapes pour télécharger le référentiel JBoss EAP 6 Maven sur le système de fichiers local. Cette option est facile à configurer et vous permet d'obtenir d'être opérationnel rapidement sur votre ordinateur local. Il peut vous aider à vous familiariser à l'utilisation de Maven pour le développement, mais n'est pas recommandé pour les environnements de production en équipes.

Procédure 2.1. Télécharger et installer le référentiel Maven de JBoss EAP 6 sur le système de fichier local.

1. Ouvrir un navigateur web, et accéder à cet URL: https://access.redhat.com/jbossnetwork/restricted/listSoftware.html?product=appplatform.
2. Chercher "Red Hat JBoss Enterprise Application Platform 6.2.0 Maven Repository" dans la liste.
3. Cliquer sur le bouton **`Télécharger`** pour télécharger un fichier **`.zip`** contenant le référentiel.
4. Décompresser le fichier dans le même répertoire sur votre système de fichiers local dans un répertoire de votre choix.
5. Section 2.3.2, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven ».

Résultat

Ceci crée un répertoire de référentiel Maven appelé **`jboss-eap-6.2.0.maven-repository`**.

IMPORTANT

Si vous souhaitez continuer à utiliser un référentiel local moins récent, vous devez le configurer séparemment dans le fichier de configuration **`settings.xml`** de Maven. Chaque référentiel local doit être configuré dans sa propre balise **`<repository>`**.

IMPORTANT

Quand vous téléchargez un nouveau référentiel Maven, supprimer le sous-répertoire `repository/` cache, qui se situe sous le répertoire `.m2/` avant de tenter d'utiliser le nouveau répertoire Maven.

Report a bug

2.2.4. Installer le référentiel Maven de JBoss EAP 6 à utiliser avec Appache httpd

Il y a trois moyens d'installer le référentiel; sur votre système de fichiers local, sur le serveur web Apache, ou par un gestionnaire de référentiel Maven. Cet exemple porte sur les étapes de téléchargement du référentiel Maven de JBoss EAP 6 à utiliser avec Apache httpd. Cette option se prête bien aux environnements de développement inter-équipes ou multi-utilisateurs, car n'importe quel développeur qui puisse accéder à un serveur web, peut également accéder au référentiel Maven.

Pré-requis

Il vous faut configurer Apache httpd. Voir la documentation Apache HTTP Server Project pour obtenir des instructions.

Procédure 2.2. Télécharger l'archive ZIP du Référentiel Maven de JBoss EAP 6

1. Ouvrir un navigateur web, et accéder à cet URL: https://access.redhat.com/jbossnetwork/restricted/listSoftware.html?product=appplatform.
2. Chercher "Red Hat JBoss Enterprise Application Platform 6.2.0 Maven Repository" dans la liste.
3. Cliquer sur le bouton **`Télécharger`** pour télécharger un fichier `.zip` contenant le référentiel.
4. Décompresser les fichiers dans un répertoire qui soit accessible au serveur Apache.
5. Configurer Apache pour lui donner la permission écriture et pour permettre la navigation dans le répertoire créé.
6. Section 2.3.2, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven ».

Résultat

Cela permet à un environnement multi-utilisateurs d'accéder à un référentiel Maven sur Apache httpd.

NOTE

Si vous passez à une version supérieure du référentiel, veuillez noter que les artéfacts de référentiel Maven de JBoss peuvent simplement être extraits dans un référentiel Maven de produits JBoss (comme JBoss EAP 6.1.0). Une fois que l'archive de référentiel a été extraite, les artefacts peuvent être utilisés avec les paramètres existants de Maven dans ce référentiel.

Report a bug

2.2.5. Installer le référentiel Maven de JBoss EAP 6 en utilisant le gestionnaire de référentiels Nexus Maven

Il y a trois façons d'installer un référentiel; sur votre système de fichiers local, sur le serveur web Apache, ou à l'aide d'un gestionnaire de référentiels Maven. Cette option sera plus adaptée si vous avez déjà une licence et utilisez un gestionnaire de référentiels car vous pourrez héberger le référentiel de JBoss avec vos référentiels déjà existants. Pour obtenir plus d'informations sur les gestionnaires de référentiels Maven, voir Section 2.2.6, « Gestionnaires de référentiels Maven ».

Cet exemple couvrira les étapes d'installation du référentiel Maven de JBoss EAP 6 en utilisant le référentiel Sonatype Nexus Maven. Pour obtenir davantage d'informations, voir Sonatype Nexus: Manage Artifacts.

Procédure 2.3. Télécharger l'archive ZIP du référentiel Maven de JBoss EAP 6

1. Ouvrir un navigateur web, et accéder à cet URL: https://access.redhat.com/jbossnetwork/restricted/listSoftware.html?product=appplatform.
2. Chercher "Red Hat JBoss Enterprise Application Platform 6.2.0 Maven Repository" dans la liste.
3. Cliquer sur le bouton **`Télécharger`** pour télécharger un fichier **`.zip`** contenant le référentiel.
4. Décompresser les fichiers dans un répertoire de votre choix.

Procédure 2.4. Ajouter le référentiel Maven de JBoss EAP 6 en utilisant le gestionnaire de référentiels Nexus Maven

1. Connectez-vous à Nexus en tant qu'administrateur.
2. Sélectionner la section **`Référentiels`** à partir du menu **Vues** → **Référentiels** qui se trouve à gauche du gestionnaire de référentiels.
3. Cliquer sur le menu déroulant **`Ajouter...`**, puis sélectionner **`Référentiel hébergé`**.
4. Donner un nom et une ID au nouveau référentiel.
5. Saisir le chemin du disque qui mène au référentiel décompressé dans le champ d'emplacement **`Remplacement du stockage local`**.
6. Continuer si vous souhaitez que l'artéfact soit disponible dans un groupe de référentiels. Ne pas continuer avec cette procédure si ce n'est pas ce que vous souhaitez.
7. Sélectionner le groupe de référentiels.
8. Cliquer sur l'onglet **`Configurer`**.
9. Déplacez le nouveau référentiel JBoss Maven de la liste **`Référentiels disponibles`** vers la liste **`Référentiels de groupes ordonnancés`** sur la gauche.

NOTE

Notez que l'ordre de cette liste détermine la priorité de recherche d'artefacts Maven.

10. Section 2.3.2, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven ».

Résultat

Le référentiel est configuré par le gestionnaire de référentiels Maven Nexus.

Report a bug

2.2.6. Gestionnaires de référentiels Maven

Un gestionnaire de référentiel est un outil qui vous permet de gérer facilement les référentiels Maven. Les gestionnaires de référentiels sont utiles pour différentes raisons :

- Ils donnent la possibilité de configurer des proxys entre votre organisation et des référentiels Maven à distance, ce qui offre un grand nombre d'avantages, parmi lesquels des déploiements plus rapides et plus efficaces et un meilleur niveau de contrôle sur ce qui est téléchargé par Maven.
- Ils fournissent des destinations de déploiement pour les artefacts que vous aurez vous-même générés, permettant ainsi une collaboration entre différentes équipes de développement au sein d'une organisation.

Pour de plus amples d'informations concernant les gestionnaires de référentiels Maven, veuillez consulter la liste des gestionnaires de référentiels du projet Apache Maven Apache Maven Project - The List of Repository Managers.

Gestionnaires de référentiels Maven les plus communément utilisés

Sonatype Nexus

Voir Sonatype Nexus: Manage Artifacts pour obtenir plus d'informations sur Nexus.

Artifactory

Voir Artifactory Open Source pour obtenir plus d'informations sur Artifactory.

Apache Archiva

Voir Apache Archiva: The Build Artifact Repository Manager pour obtenir plus d'informations sur Apache Archiva.

Report a bug

2.3. UTILISER LE RÉFÉRENTIEL MAVEN

2.3.1. Configurer le référentiel Maven de JBoss EAP

Aperçu

Il existe deux approches pour amener Maven à utiliser le référentiel Maven de JBoss EAP 6 dans votre projet :

- Vous pouvez configurer les référentiels dans les paramètres globaux ou d'utilisateur de Maven.
- Vous pouvez configurer les référentiels dans le fichier POM du projet.

Procédure 2.5. Configurer les paramètres Maven pour qu'ils utilisent le référentiel Maven de JBoss EAP 6

1. **Configurer le référentiel Maven par les paramètres Maven**
   Nous vous conseillons cette dernière approche. Les paramètres Maven utilisés avec un gestionnaire de référentiel ou un référentiel sur un serveur partagé offrent un meilleur contrôle et une meilleure gestion des projets. Les paramètres offrent également la capacité d'utiliser un miroir alternatif pour rediriger toutes les demandes de recherche pour un référentiel spécifique vers un gestionnaire de référentiel sans changer les fichiers du projet. Pour plus d'informations concernant les miroirs, veuillez consulter http://maven.apache.org/guides/mini/guide-mirror-settings.html.

   Cette méthode de configuration s'applique à tous les projets Maven, tant que le fichier POM du projet ne contient pas de configuration de référentiel.

   Section 2.3.2, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven ».

2. **Configurer le référentiel Maven pour qu'il utilise le fichier POM du projet.**
   Cette méthode de configuration est généralement déconseillée. Si vous décidez de configurer des référentiels dans le fichier POM de votre projet, planifiez de manière prudente et souvenez-vous que cela pourrait ralentir votre build et que vous pourriez vous retrouver avec des artefacts ne provenant pas du référentiel attendu.

   NOTE

   Dans le cas d'une entreprise, où un gestionnaire de référentiel est généralement utilisé, Maven doit interroger tous les artefacts pour tous les projets en utilisant ce gestionnaire. Maven utilise tous les référentiels déclarés pour trouver les artéfacts manquants. Par conséquent, s'il ne peut trouver ce qu'il cherche, il pourra le chercher dans la centrale de référentiels (définie dans le fichier POM parent intégré). Pour remplacer cet emplacement central, vous pouvez ajouter une définition avec `central` de manière à ce que la centrale de référentiels devienne également votre gestionnaire de référentiel. Cela fonctionne bien avec les projets établis, mais pose un problème pour les projets vierges ou récents puisque cela crée une dépendance cyclique.

   Les fichiers POM inclus de manière transitive représentent également un problème avec ce type de configuration. Maven doit interroger ces référentiels externes pour trouver les artefacts manquants. Non seulement cela ralentira votre build, mais vous fera également perdre le contrôle sur la provenance de vos artefacts et risquera d'endommager votre build.

   Cette méthode de configuration remplace les configuration utilisateur et globales pour le projet configuré.

   Section 2.3.3, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par le Projet POM ».

Report a bug

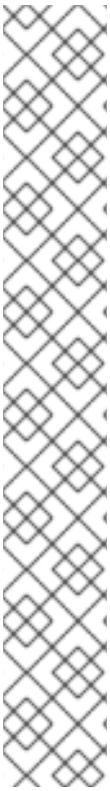
2.3.2. Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven

Il existe deux approches pour amener Maven à utiliser le référentiel Maven de JBoss EAP 6 dans votre projet :

- Vous pouvez modifier les paramètres Maven. Cela amène Maven à utiliser la configuration à travers tous les projets.
- Vous pouvez configurer le fichier POM du projet. Cela limite la configuration au projet particulier.

Cette section vous montre comment amener Maven à utiliser le référentiel JBoss EAP 6 Maven à travers tous les projets grâce aux paramètres de configuration de Maven. C'est l'approche conseillée.

Vous pouvez configurer Maven pour utiliser l'en ligne ou un référentiel de JBoss EAP 6.2 installé localement. Si vous choisissez d'utiliser le référentiel en ligne, vous pouvez utiliser un fichier de paramètres préconfigurés ou ajouter les profils de JBoss EAP 6.2 Maven pour le fichier de paramètres existants. Pour utiliser un référentiel local, vous devez télécharger le référentiel et configurer les paramètres pour pointer vers votre référentiel installé localement. Les procédures suivantes décrivent comment configurer Maven dans JBoss EAP 6.2.



NOTE

L'URL du référentiel dépendra de l'endroit où le référentiel se trouve; sur le système de fichiers ou sur le serveur web. Pour obtenir des informations sur la façon d'installer le référentiel, voir le chapitre qui s'intitule *Maven Guide* dans le *Development Guide* pour JBoss EAP 6 dans https://access.redhat.com/site/documentation/JBoss_Enterprise_Application_Platform/. Voici des exemples pour chacune des options d'installation :

Système de fichiers

file:///path/to/repo/jboss-eap-6.x-maven-repository

Apache Web Server

http://intranet.acme.com/jboss-eap-6.x-maven-repository/

Gestionnaire de référentiel Nexus

https://intranet.acme.com/nexus/content/repositories/jboss-eap-6.x-maven-repository

Vous pouvez configurer Maven soit par les paramètres d'install globaux Maven, soit par l'install utilisateur. Ces instructions configurent les paramètres d'installation utilisateur car il s'agit de l'installation la plus commune.

Procédure 2.6. Configurer Maven par les paramètres fournis dans les exemples Quickstart

Les quickstarts de Red Hat JBoss Enterprise Application Platform 6.2 contiennent un fichier `settings.xml` configuré pour utiliser le référentiel JBoss EAP 6.2 Maven en ligne. Il s'agit de l'approche la plus simple.

1. Cette procédure remplace le fichier de configuration Maven existant, donc vous devrez sauvegarder le fichier `settings.xml` Maven existant.

   a. Chercher le répertoire d'installation Maven qui corresponde à votre système d'exploitation. Il se trouve normalement dans le répertoire ***USER_HOME***`/.m2/` .

      - Dans Linux ou Mac, c'est: `~/.m2/`
      - Pour Windows, c'est : `\Documents and Settings\`***`USER_NAME`***`\.m2\` ou `\Users\`***`USER_NAME`***`\.m2\`

b. Si vous avez un fichier ***USER_HOME*/.m2/settings.xml** existant, renommer le et faire une copie de sauvegarde afin de pouvoir le restaurer plus tard.

2. Télécharger et décompresser les exemples quickstart fournis dans JBoss EAP 6.2. Pour plus d'informations, voir la section *Download the Quickstart Code Examples*du *Development Guide* dans JBoss EAP 6 à https://access.redhat.com/site/documentation/JBoss_Enterprise_Application_Platform/.

3. Copier le fichier ***QUICKSTART_HOME*/settings.xml** dans le répertoire ***USER_HOME*/.m2/** .

4. Si vous modifiez le fichier **settings.xml** tandis que JBoss Developer Studio est en cours d'exécution, suivre la procédure ci-dessous intitulée *Refresh the JBoss Developer Studio User Settings*.

Procédure 2.7. Modifier et configurer les paramètres Maven manuellement pour qu'ils utilisent le référentiel Maven de JBoss EAP 6.2 en ligne

Vous pouvez ajouter manuellement les profils JBoss EAP 6.2 à un fichier de paramètres Maven existant.

1. Chercher le répertoire d'installation Maven qui corresponde à votre système d'exploitation. Il se trouve normalement dans le répertoire ***USER_HOME*/.m2/** .
   - Dans Linux ou Mac, c'est **~/.m2/**
   - Pour Windows, c'est **\Documents and Settings*USER_NAME*\.m2** ou **\Users*USER_NAME*\.m2**

2. Si vous ne trouvez pas de fichier **settings.xml** , copier le fichier **settings.xml** du répertoire ***USER_HOME*/.m2/conf/** dans le répertoire ***USER_HOME*/.m2/**.

3. Copier l'XML suivant dans l'élément **<profiles>** du fichier.

```
<!-- Configure the JBoss GA Maven repository -->
<profile>
  <id>jboss-ga-repository</id>
  <repositories>
    <repository>
      <id>jboss-ga-repository</id>
      <url>http://maven.repository.redhat.com/techpreview/all</url>
      <releases>
        <enabled>true</enabled>
      </releases>
      <snapshots>
        <enabled>false</enabled>
      </snapshots>
    </repository>
  </repositories>
  <pluginRepositories>
    <pluginRepository>
      <id>jboss-ga-plugin-repository</id>
      <url>http://maven.repository.redhat.com/techpreview/all</url>
      <releases>
        <enabled>true</enabled>
      </releases>
      <snapshots>
```

```
        <enabled>false</enabled>
      </snapshots>
    </pluginRepository>
  </pluginRepositories>
</profile>
<!-- Configure the JBoss Early Access Maven repository -->
<profile>
  <id>jboss-earlyaccess-repository</id>
  <repositories>
    <repository>
      <id>jboss-earlyaccess-repository</id>
      <url>http://maven.repository.redhat.com/earlyaccess/all/</url>
      <releases>
        <enabled>true</enabled>
      </releases>
      <snapshots>
        <enabled>false</enabled>
      </snapshots>
    </repository>
  </repositories>
  <pluginRepositories>
    <pluginRepository>
      <id>jboss-earlyaccess-plugin-repository</id>
      <url>http://maven.repository.redhat.com/earlyaccess/all/</url>
      <releases>
        <enabled>true</enabled>
      </releases>
      <snapshots>
        <enabled>false</enabled>
      </snapshots>
    </pluginRepository>
  </pluginRepositories>
</profile>
```

Copier l'XML suivant dans l'élément **<activeProfiles>** de **settings.xml**.

```
<activeProfile>jboss-ga-repository</activeProfile>
<activeProfile>jboss-earlyaccess-repository</activeProfile>
```

4. Si vous modifiez le fichier **settings.xml** tandis que JBoss Developer Studio est en cours d'exécution, suivre la procédure ci-dessous intitulée *Refresh the JBoss Developer Studio User Settings*.

Procédure 2.8. Configurer les paramètres pour pouvoir utiliser un référentiel JBoss EAP installé localement

Vous pouvez modifier les paramètres pour utiliser le référentiel JBoss EAP 6.2 qui est installé dans le système de fichiers local.

1. Chercher le répertoire d'installation Maven qui corresponde à votre système d'exploitation. Il se trouve normalement dans le répertoire ***USER_HOME*/.m2/** .
   - Dans Linux ou Mac, c'est **~/.m2/**

- Pour Windows, c'est **\Documents and Settings*USER_NAME*\.m2** ou **\Users*USER_NAME*\.m2**

2. Si vous ne trouvez pas de fichier **settings.xml** , copier le fichier **settings.xml** du répertoire ***USER_HOME*/.m2/conf/** dans le répertoire ***USER_HOME*/.m2/**.

3. Copier l'XML suivant dans l'élément **<profiles>** du fichier **settings.xml**. Veillez bien à changer l' **<url>** au bon emplacement de référentiel.

```
<profile>
  <id>jboss-eap-repository</id>
  <repositories>
    <repository>
      <id>jboss-eap-repository</id>
      <name>JBoss EAP Maven Repository</name>
      <url>file:///path/to/repo/jboss-eap-6.x-maven-repository</url>
      <layout>default</layout>
      <releases>
        <enabled>true</enabled>
        <updatePolicy>never</updatePolicy>
      </releases>
      <snapshots>
        <enabled>false</enabled>
        <updatePolicy>never</updatePolicy>
      </snapshots>
    </repository>
  </repositories>
  <pluginRepositories>
    <pluginRepository>
      <id>jboss-eap-repository-group</id>
      <name>JBoss EAP Maven Repository</name>
      <url>
      file:///path/to/repo/jboss-eap-6.x-maven-repository
      </url>
      <layout>default</layout>
      <releases>
        <enabled>true</enabled>
        <updatePolicy>never</updatePolicy>
      </releases>
      <snapshots>
        <enabled>false</enabled>
        <updatePolicy>never</updatePolicy>
      </snapshots>
    </pluginRepository>
  </pluginRepositories>
</profile>
```

Copier l'XML suivant dans l'élément **<activeProfiles>** de **settings.xml**.

```
<activeProfile>jboss-eap-repository</activeProfile>
```

4. Si vous modifiez le fichier `settings.xml` tandis que JBoss Developer Studio est en cours d'exécution, suivre la procédure ci-dessous intitulée *Refresh the JBoss Developer Studio User Settings*.

Procédure 2.9. Réactualiser les paramètres de configuration de l'utilisateur JBoss Developer Studio

Si vous modifiez le fichier `settings.xml` tandis que JBoss Developer Studio est en cours d'exécution, vous devrez réactualiser les paramètres de configuration de l'utilisateur.

1. À partir du menu, sélectionner **Window** → **Préférences**.
2. Dans la fenêtre Window `Préférences`, étendre `Maven` et sélectionner `Paramètres de configuration utilisateur`.
3. Cliquer sur le bouton `Mise à jour Configuration` pour réactualiser les configurations utilisateur de Maven dans JBoss Developer Studio.

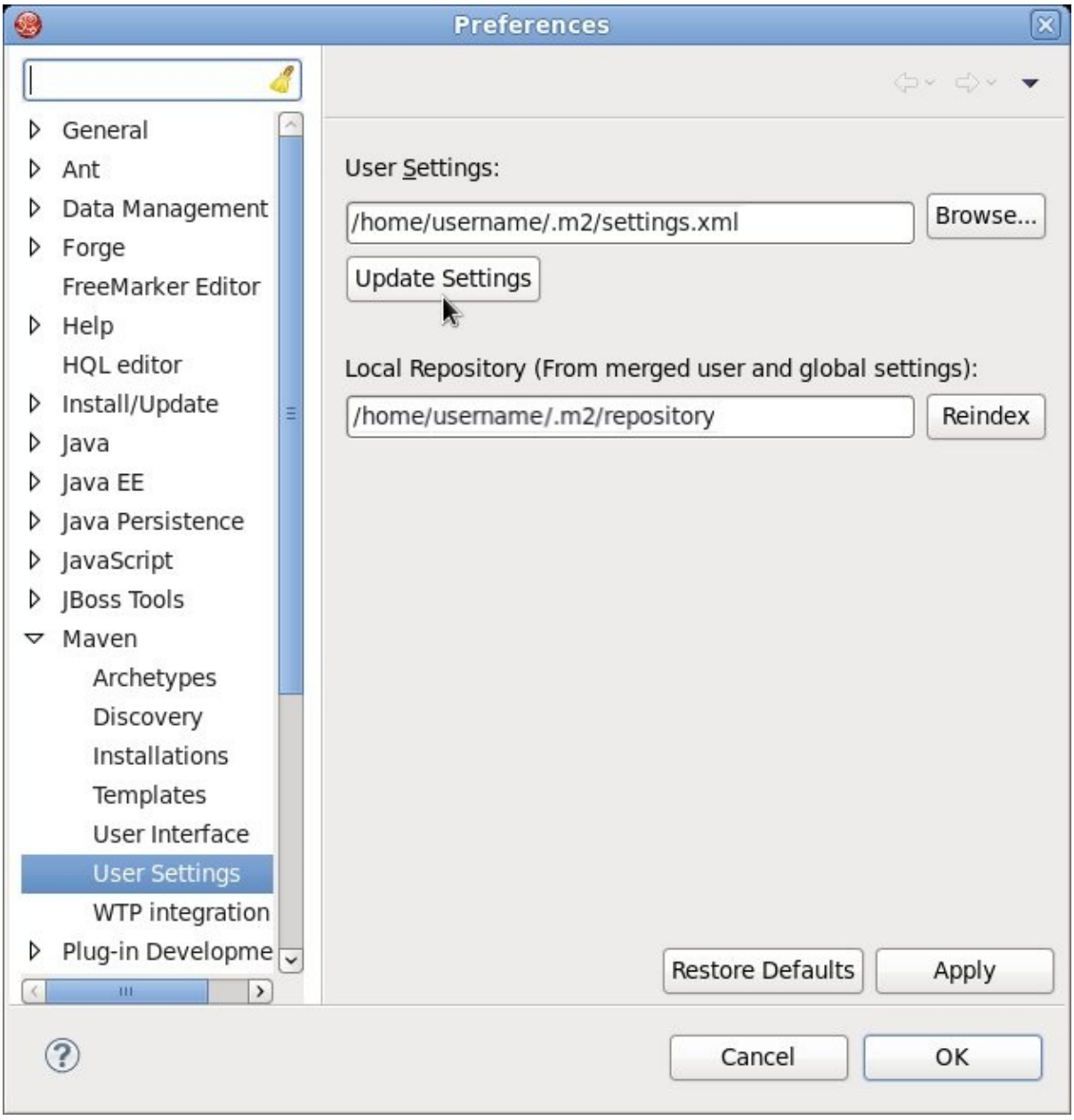


Figure 2.1. Mise à jour des paramètres de configuration de l'utilisateur Maven

IMPORTANT

Si votre référentiel Maven contient des artéfacts obsolètes, vous risquez de rencontrer un des messages d'erreur Maven suivants quand vous créez ou déployez votre projet :

- Missing artifact *ARTIFACT_NAME*
- [ERROR] Failed to execute goal on project *PROJECT_NAME*; Could not resolve dependencies for *PROJECT_NAME*

To resolve the issue, delete the cached version of your local repository to force a download of the latest Maven artifacts. The cached repository is located in your `~/.m2/repository/` subdirectory on Linux, or the `%SystemDrive%\Users\USERNAME\.m2\repository\` subdirectory on Windows.

Report a bug

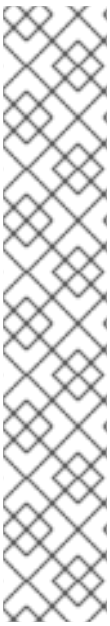
2.3.3. Configurer le référentiel JBoss EAP 6 Platform Maven Repository par le Projet POM

Il existe deux approches pour amener Maven à utiliser le référentiel Maven de JBoss EAP 6 dans votre projet :

- Vous pouvez modifier les paramètres Maven.
- Vous pouvez configurer le fichier POM du projet.

Cette tâche vous montre comment configurer un projet particulier pour utiliser le référentiel JBoss EAP 6 Maven Repository en ajoutant des informations de référentiel au projet `pom.xml`. Cette méthode de configuration remplace les configurations Utilisateur et Globales.

Cette méthode de configuration est généralement déconseillée. Si vous décidez de configurer des référentiels dans le fichier POM de votre projet, planifiez de manière prudente et souvenez-vous que cela pourrait ralentir votre build et que vous pourriez vous retrouver avec des artéfacts ne provenant pas du référentiel attendu.



NOTE

En environnement Enterprise, où un gestionnaire de référentiel est généralement utilisé, Maven doit exiger tous les artéfacts de tous les projets en utilisant ce gestionnaire. Maven utilise tous les référentiels déclarés pour trouver les artéfacts manquants, par conséquent, s'il ne peut trouver ce qu'il cherche, il pourra le chercher dans la centrale de référentiels (dans le fichier POM parent intégré). Pour remplacer cet emplacement central, vous pouvez ajouter une définition avec `central` de manière à ce que la centrale de référentiels devienne également votre gestionnaire de référentiel. Cela fonctionne bien avec les projets établis, mais pose un problème pour les projets vierges ou récents puisque cela crée une dépendance cyclique.

Les fichiers POM inclus de manière transitive représentent également un problème avec ce type de configuration. Maven doit interroger ces référentiels externes pour trouver les artéfacts manquants. Non seulement cela ralentira votre build, mais vous fera également perdre le contrôle sur la provenance de vos artéfacts et risquera d'endommager votre build.

NOTE

L'URL du référentiel dépend de si le référentiel se trouve sur le système de fichiers ou sur le serveur web. Pour plus d'informations sur l'installation du référentiel, veuillez consulter : Section 2.2.2, « Installer le référentiel Maven de JBoss EAP 6 » . Voici quelques exemples pour chacune des options d'installation :

Système de fichiers

`file:///path/to/repo/jboss-eap-6.0.0-maven-repository`

Apache Web Server

`http://intranet.acme.com/jboss-eap-6.0.0-maven-repository/`

Gestionnaire de référentiel Nexus

`https://intranet.acme.com/nexus/content/repositories/jboss-eap-6.0.0-maven-repository`

1. Ouvrir le fichier **pom.xml** de votre projet dans un éditeur de texte.
2. Ajouter la configuration du référentiel suivant. S'il y a déjà une configuration **<repositories>** qui se trouve dans le fichier, lui ajouter l'élément **<repository>**. Veillez bien à modifier l' **<url>** pour qu'il corresponde bien à l'emplacement du référentiel.

```
<repositories>
   <repository>
      <id>jboss-eap-repository-group</id>
      <name>JBoss EAP Maven Repository</name>
      <url>file:///path/to/repo/jboss-eap-6.0.0-maven-
repository/</url>
      <layout>default</layout>
      <releases>
         <enabled>true</enabled>
         <updatePolicy>never</updatePolicy>
      </releases>
      <snapshots>
         <enabled>true</enabled>
         <updatePolicy>never</updatePolicy>
      </snapshots>
   </repository>
</repositories>
```

3. Ajouter la configuration de référentiel de plug-in suivante. S'il existe déjà une configuration **<pluginRepositories>** dans le fichier, lui ajouter l'élément **<pluginRepository>**.

```
<pluginRepositories>
   <pluginRepository>
      <id>jboss-eap-repository-group</id>
      <name>JBoss EAP Maven Repository</name>
      <url>file:///path/to/repo/jboss-eap-6.0.0-maven-
repository/</url>
      <releases>
         <enabled>true</enabled>
      </releases>
      <snapshots>
```

```
            <enabled>true</enabled>
        </snapshots>
    </pluginRepository>
</pluginRepositories>
```

Report a bug

2.3.4. Gestion des dépendances du projet

Cette section décrit les fichiers POM de nomenclature (NOMENCL ou BOM de l'anglais Bills of Material) de Red Hat JBoss Enterprise Application Platform 6.

Un fichier BOM est un fichier Maven **pom.xml** (POM) qui indique les versions de toutes les dépendances d'exécution d'un module donné. Les dépendances de versions sont listées dans la section de gestion des dépendances du fichier.

Un projet utilise un NOMENCL en ajoutant son **groupId:artifactId:version** (GAV) à la section de gestion des dépendances du fichier **pom.xml** du projet et en spécifiant **<scope>import</scope>** et les valeurs de l'élément **<type>pom</type>**.

NOTE

Dans bien des cas, les dépendances des fichiers POM du projet donné utilisent la portée **fournie**. C'est parce que ces classes sont fournies par le serveur d'applications en cours d'exécution et qu'il n'est pas nécessaire de les empaqueter avec l'application utilisateur.

Artéfacts Maven pris en charge

Dans le cadre du processus de génération du produit, tous les composants d'exécution de JBoss EAP sont construits à partir de la source dans un environnement contrôlé. Cela permet d'assurer que les objets binaires ne contiennent pas de code malveillant, et qu'ils puissent être soutenus pour la durée de vie du produit. Ces objets peuvent être facilement identifiés par le qualificateur de version **-redhat**, par exemple **1.0.0-redhat-1**.

L'ajout d'un artefact pris en charge pour le fichier **pom.xml** de configuration de build garantit que le build utilise l'artefact binaire correct pour la génération de builds locaux et pour le testing. Notez qu'un artefact avec une version **-redhat** ne fait pas nécessairement partie de l'API public prise en charge et peut changer à l'avenir au cours des révisions. Pour plus d'informations sur l'API public pris en charge, voir la documentation JavaDoc incluse dans la sortie.

Ainsi, pour pouvoir utiliser la version d'Hibernate prise en charge, ajouter quelque chose de similaire à votre configuration de build.

```
<dependency>
  <groupId>org.hibernate</groupId>
  <artifactId>hibernate-core</artifact>
  <version>4.2.6.Final-redhat-1</version>
  <scope>provided</scope>
</dependency>
```

Notez que l'exemple ci-dessus contient une valeur pour le champ **<version/>**. Cependant, il est recommandé d'utiliser la gestion des dépendances Maven pour configurer les versions de dépendances.

Gestion des dépendances

Maven inclut un mécanisme de gestion des versions de dépendances directes et transitives par le build. Pour obtenir des informations générales sur la gestion des dépendances, voir le projet Apache Maven Project Introduction to the Dependency Mechanism.

En utilisant une ou plusieurs dépendances JBoss prises en charge directement dans votre build ne garantit pas que toutes les dépendances transitives du build seront des artéfacts JBoss totalement pris en charge. Il est commun pour les builds Maven d'utiliser un mélange de sources d'artéfacts en provenance du référentiel central Maven, du référentiel Maven JBoss.org, ou autres référentiels Maven.

Dans le référentiel JBoss EAP Maven, il y a une NOMENCL de dépendance de gestion, qui spécifie tous les artefacts binaires de JBoss EAP pris en charge. Cette nomenclature peut être utilisée dans un build pour s'assurer que Maven donnera la priorité à des dépendances JBoss EAP prises en charge pour toutes les dépendances directes et transitives du build. En d'autres termes, les dépendances transitives seront gérées en fonction de la version de dépendance qui convient le cas échéant. La version de BOM correspond à celle de la version de JBoss EAP.

```
<dependencyManagement>
  <dependencies>
    ...
    <dependency>
      <groupId>org.jboss.bom</groupId>
      <artifactId>eap6-supported-artifacts</artifactId>
      <version>6.2.0.GA</version>
      <type>pom</type>
      <scope>import</scope>
    </dependency>
    ...
  </dependencies>
</dependencyManagement>
```

JBoss JavaEE Specs Bom de nomenclature

Le code BOM **jboss-javaee-6.0** contient les JAR de spécification JAVA EE utilisés dans JBoss EAP.

Pour utiliser cette nomenclature BOM dans un projet, ajouter une dépendance au GAV qui contient la version du JSP et des JARS de l'API du serveur qui doivent être créés et déployer l'application.

L'exemple suivant utilise la version **3.0.2.Final-redhat-x** de la NOMENCL **jboss-javaee-6.0**.

```
<dependencyManagement>
  <dependencies>
    <dependency>
      <groupId>org.jboss.spec</groupId>
      <artifactId>jboss-javaee-6.0</artifactId>
      <version>3.0.2.Final-redhat-x</version>
      <type>pom</type>
      <scope>import</scope>
    </dependency>
    ...
```

```
  </dependencies>
</dependencyManagement>

<dependencies>
  <dependency>
    <groupId>org.jboss.spec.javax.servlet</groupId>
    <artifactId>jboss-servlet-api_3.0_spec</artifactId>
    <scope>provided</scope>
  </dependency>
  <dependency>
    <groupId>org.jboss.spec.javax.servlet.jsp</groupId>
    <artifactId>jboss-jsp-api_2.2_spec</artifactId>
    <scope>provided</scope>
  </dependency>
  ...
</dependencies>
```

Les nomenclatures JBoss EAP BOM et les Quickstarts

Les fichiers JBoss EAP BOM du projet jboss-bom se trouvent à l'adresse suivante https://github.com/jboss-developer/jboss-eap-boms.

Les quickstarts fournissent des exemples de cas d'utilisation primaires du référentiel Maven. Le tableau suivant dresse une liste des NOMENCL (BOM) utilisées par les quickstarts.

Tableau 2.1. Nomenclatures JBoss BOM utilisées par les Quickstarts

IdArtéfact Maven	Description
jboss-javaee-6.0-with-hibernate	Cette nomenclature BOM s'appuie sur le profil BOM complet de Java EE, ajoutant des projets communautaires Hibernate ORM, Hibernate Search et Hibernate Validator. Elle fournit également des projets d'outil tel que Hibernate JPA Model Gen et le processeur Hibernate Validator Annotation.
jboss-javaee-6.0-with-hibernate3	Cette nomenclature BOM s'appuie sur le profil BOM complet de Java EE, ajoutant des projets communautaires Hibernate 3 ORM, Hibernate Entity Manager (JPA 1.0) et Hibernate Validator.
jboss-javaee-6.0-with-logging	Cette nomenclature BOM s'appuie sur le profil BOM complet de Java EE, ajoutant JBoss Logging Tools et Log4 framework.
jboss-javaee-6.0-with-osgi	Cette nomenclature BOM s'appuie sur le profil BOM complet de Java EE, ajoutant OSGI.
jboss-javaee-6.0-with-resteasy	Cette nomenclature BOM s'appuie sur le profil BOM complet de Java EE, ajoutant RESTEasy
jboss-javaee-6.0-with-security	Cette nomenclature BOM s'appuie sur le profil BOM complet de Java EE, ajoutant Picketlink.

IdArtéfact Maven	Description
jboss-javaee-6.0-with-tools	Cette nomenclature BOM s'appuie sur le profil BOM complet de Java EE, ajoutant Arquillian à l'ensemble. Elle procure également une version de JUnit et de TestNG conseillés pour l'utilisation avec Arquillian.
jboss-javaee-6.0-with-transactions	Cette nomenclature BOM inclut un gestionnaire de transactions de classe mondiale. Utiliser les API JBossTS pour pouvoir profiter de toutes ses fonctionnalités.

L'exemple suivant utilise la version **`6.2.0.GA`** de la nomemclature BOM **`jboss-javaee-6.0-with-hibernate`**.

```
<dependencyManagement>
  <dependencies>
    <dependency>
      <groupId>org.jboss.bom.eap</groupId>
      <artifactId>jboss-javaee-6.0-with-hibernate</artifactId>
      <version>6.2.0.GA</version>
      <type>pom</type>
      <scope>import</scope>
    </dependency>
    ...
  </dependencies>
</dependencyManagement>

<dependencies>
  <dependency>
    <groupId>org.hibernate</groupId>
    <artifactId>hibernate-core</artifactId>
    <scope>provided</scope>
  </dependency>
  ...
</dependencies>
```

JBoss Client BOMs

Les JBoss EAP Builds comprennent deux nomenclatures BOM : **`jboss-as-ejb-client-bom`** et **`jboss-as-jms-client-bom`**.

Les NOMENCL de clients ne créent pas de section de gestion des dépendances, ni ne définissent les dépendances. Au lieu de cela, ces nomenclatures se rajoutent à d'autres BOM et sont utilisées pour empaqueter un ensemble de dépendances nécessaires pour les cas d'utilisation de clients distants.

L'exemple suivant utilise la version **`7.3.0.Final-redhat-x`** du client **`jboss-as-ejb-client-bom`** BOM.

```
<dependencies>
  <dependency>
    <groupId>org.jboss.as</groupId>
    <artifactId>jboss-as-ejb-client-bom</artifactId>
    <version>7.3.0.Final-redhat-x</version>
    <type>pom</type>
```

```
  </dependency>
  ...1
</dependencies>
```

Cet exemple utilise la version **7.3.0.Final-redhat-x** du client BOM **jboss-as-jms-client-bom**.

```
<dependencies>
  <dependency>
    <groupId>org.jboss.as</groupId>
    <artifactId>jboss-as-jms-client-bom</artifactId>
    <version>7.3.0.Final-redhat-x</version>
    <type>pom</type>
  </dependency>
  ...
</dependencies>
```

Pour plus d'informations sur les dépendances Maven et sur les fichiers BOM POM, consulter Apache Maven Project - Introduction to the Dependency Mechanism.

Report a bug

2.4. MISE À NIVEAU DU RÉFÉRENTIEL MAVEN

2.4.1. Appliquer un correctif dans le répertoire Maven local

Résumé

Un rréférentiel Maven stocke des bibliothèques Java, des plug-ins et autres objets nécessaires pour compiler et déployer des applications JBoss EAP. Le référentiel de JBoss EAP est disponible en ligne ou en fichier ZIP téléchargé. Si vous utilisez le référentiel hébergé publiquement, les mises à jour seront appliquées automatiquement. Toutefois, si vous téléchargez et installez le repository Maven localement, vous serez chargé d'appliquer les mises à jour vous-même. Chaque fois qu'un correctif sera disponible dans JBoss EAP, un correctif correspondant sera fourni pour le référentiel JBoss EAP Maven. Ce correctif est disponible sous la forme d'un fichier ZIP incrémentiel qui est décompressé dans le référentiel local existant. Le fichier ZIP contient des nouveaux fichiers JAR et POM. Il n'écrase pas les JAR existants, ni ne les supprime, donc il n'y a aucune exigence de restauration.

Pour plus d'informations sur le Management CLI, voir le chapitre intitulé *Patching and Upgrading JBoss EAP 6* de *Administration and Configuration Guide*concernant JBoss Enterprise Application Platform 6 qui se situe sur le Portail Clients à l'adresse suivante : https://access.redhat.com/site/documentation/JBoss_Enterprise_Apnplication_Platform/.

Cette tâche décrit comment appliquer les mises à jour de Maven dans votre référentiel Maven en utilisant la commande **unzip**.

Pré-requis

- Accès valide et abonnement au Portail Clients de Red Hat.
- Le fichier Red Hat JBoss Enterprise Application Platform 6.3.0 Maven Repository ZIP, téléchargé et installé localement.

Procédure 2.10. Mise à jour du Référentiel Maven

1. Ouvrir un navigateur et connectez-vous dans https://access.redhat.com.
2. Sélectionner **Téléchargements** du menu en haut de la page.
3. Chercher **`Red Hat JBoss Middleware`** et cliquer sur le bouton **`Télécharger Logiciel`**.
4. Sélectionner **`Plate-forme d'applications`** à partir du menu déroulant **`Produit`** qui se trouve sur l'écran suivant.
5. Sélectionner la version qui convient de JBoss EAP à partir du menu déroulant **`Version`** qui apparaît sur l'écran, puis cliquer sur **`Correctifs`**.
6. Chercher **`Red Hat JBoss Enterprise Application Platform 6.2 CP`***x* **`Incremental Maven Repository`** dans la liste et cliquer sur **`Téléchargement`**.
7. Vous êtes invités à sauvegarder le fichier ZIP dans un répertoire de votre choix. Sélectionner un répertoire et sauvegardez le fichier.
8. Chercher le chemin d'accès vers le répertoire JBoss EAP dont il s'agit dans les commandes ci-dessous, sous *EAP_MAVEN_REPOSITORY_PATH*, correspondant à votre système d'exploitation. Pour obtenir plus d'informations sur la façon d'installer le référentiel Maven sur le système de fichiers local, voir Section 2.2.3, « Installer le référentiel Maven de JBoss EAP 6 localement » .
9. Décompresser le fichier de correctifs Maven dans le répertoire d'installation de JBoss EAP 6.2.*x*.
   - Dans Linux, ouvrir un terminal et saisir la commande suivante :

     ```
     [standalone@localhost:9999 /] unzip -o jboss-eap-6.2.x-
     incremental-maven-repository.zip -d EAP_MAVEN_REPOSITORY_PATH
     ```

   - Dans Windows, utiliser l'utilitaire pour extraire le fichier ZIP pour le mettre dans la racine du répertoire***EAP_MAVEN_REPOSITORY_PATH*** .

Résultat

Le référentiel Maven installé localement est mis à jour au dernier correctif.

Report a bug

CHAPITRE 3. CHARGEMENT DE CLASSES MODULAIRE ET MODULES

3.1. INTRODUCTION

3.1.1. Chargement des classes et Modules

JBoss EAP 6 utilise un nouveau système de chargement de classes modulaire pour contrôler les chemins de classe d'applications déployées. Ce système offre plus de souplesse et de contrôle que le système traditionnel des chargeurs de classes hiérarchiques. Les développeurs ont un contrôle précis des classes disponibles à leurs applications et peuvent configurer un déploiement pour qu'il puisse ignorer les classes fournies par le serveur d'application en faveur de leurs propres classes.

Le nouveau chargeur de classes modulaire sépare toutes les classes Java en des groupes logiques appelés modules. Chaque module peut définir des dépendances sur d'autres modules de manière à ajouter les classes de ces modules dans leur propre chemin de classe. Le fait que chaque fichier JAR et WAR déployé soit traité comme un module permet aux développeurs de contrôler le contenu du chemin de classe de leur application en ajoutant une configuration de module à leur application.

Les informations suivantes permettent aux développeurs de comprendre comment construire et déployer des applications sous JBoss EAP 6.

Report a bug

3.1.2. Chargement des classes

Le chargement des classes est un mécanisme par lequel les classes et les ressources Java sont chargées dans l'environnement d'exécution de Java (Java Runtime Environment).

Report a bug

3.1.3. Modules

Un module est un regroupement logique des classes utilisées pour le chargement de classes et pour la gestion de dépendances. JBoss EAP 6 identifie deux types de modules, parfois appelés modules statiques et dynamiques. Cependant, la seule différence entre les deux est la façon dont ils sont emballés. Tous les modules offrent les mêmes caractéristiques.

Modules statiques

Les modules statiques sont prédéfinis dans le répertoire ***EAP_HOME*/modules/** du serveur d'application. Chaque sous-répertoire représente un module et contient un ou plusieurs fichiers JAR et un fichier de configuration (**module.xml**). Le nom de ce module est défini dans le fichier **module.xml**. Toutes les API fournies par le serveur d'application sont fournies en tant que modules statiques, comme les API Java EE ainsi que d'autres API comme JBoss Logging.

Exemple 3.1. Exemple de fichier module.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.0" name="com.mysql">
  <resources>
    <resource-root path="mysql-connector-java-5.1.15.jar"/>
  </resources>
  <dependencies>
```

```
    <module name="javax.api"/>
    <module name="javax.transaction.api"/>
  </dependencies>
</module>
```

Le nom du module, **com.mysql**, doit correspondre à la structure du répertoire du module.

La création de modules statiques personnalisés peut être utile si plusieurs applications sont déployées sur un même serveur utilisant les mêmes bibliothèques de tierce partie. Au lieu d'un regroupement de ces bibliothèques pour chaque application, un module contenant ces bibliothèques peut être créé et installé par l'administrateur JBoss. Les applications peuvent ensuite déclarer une dépendance explicite sur les modules statiques personnalisés.

Modules dynamiques

Les modules dynamiques sont créés et chargés par le serveur d'application pour chaque déploiement JAR ou WAR (ou sous-déploiement d'un EAR). Le nom d'un module dynamique est dérivé du nom de l'archive déployée. Comme les déploiements sont chargés sous forme de modules, ils peuvent configurer des dépendances et peuvent être utilisés comme dépendances par d'autres déploiements.

Les modules ne sont chargés qu'en fonction des besoins. Cela a généralement lieu quand une application est déployée avec des dépendances implicites ou explicites.

Report a bug

3.1.4. Les dépendances de modules

Une dépendance de module est une déclaration qui indique qu'un module a besoin des classes d'un autre module pour pouvoir fonctionner. Les modules peuvent déclarer leurs dépendances sur un certain nombre d'autres modules. Quand le serveur d'applications charge un module, le chargeur de classes de module traite les dépendances de ce module et ajoute les classes de chaque dépendance à son chemin de classe. Si une dépendance particulière est introuvable, le module ne pourra pas charger.

Les applications déployées (JAR et WAR) sont chargées sous forme de modules dynamiques et utilisent des dépendances pour accéder aux API fournies par JBoss EAP 6.

Il y a deux types de dépendances : explicite et implicite.

Les dépendances explicites sont déclarées dans la configuration par le développeur. Les modules statiques peuvent déclarer des dépendances dans le fichier modules.xml. Les modules dynamiques peuvent avoir des dépendances déclarées dans les descripteurs de déploiement MANIFEST.MF ou jboss-deployment-structure.xml.

Les dépendances explicites peuvent être spécifiées comme étant optionnelles. Une erreur de chargement de dépendance optionnelle n'entraînera pas l'annulation d'un chargement de module. Cependant, si la dépendance est rendue disponible par la suite, elle ne sera PAS ajoutée au chemin de classe du module. Les dépendances doivent être rendues disponibles quand le module est chargé.

Des dépendances implicites sont ajoutées automatiquement par le serveur d'applications quand certaines conditions ou meta-données se trouvent dans un déploiement. Les API Java EE 6 fournies avec JBoss EAP 6 sont des exemples de modules ajoutés par détection de dépendances implicites dans les déploiements.

Les déploiements peuvent également être configurés de façon à exclure des dépendances implicites particulières. Il vous faut pour cela le fichier de déploiement jboss-deployment-structure.xml. C'est normalement le cas quand une application empaquète une version spécifique de bibliothèque que le serveur d'applications tentera d'ajouter comme dépendance implicite.

Un chemin de classe de module ne contient que ses propres classes et celles de ses dépendances immédiates. Un module n'est pas en mesure d'accéder aux classes des dépendances. Cependant, un module peut indiquer quand une dépendance explicite est exportée. Une dépendance exportée est fournie à tout module qui dépend du module qui l'exporte.

> **Exemple 3.2. Les dépendances de module**
>
> Le Module A dépend du Module B et le Module B dépend su Module C. Le Module A peut accéder aux classes du Module B, et le Module B peut accéder aux classes du Module C. Le Module C ne peut pas accéder aux classes du Module C à moins que :
>
> - Le Module A déclare une dépendance explicite sur le Module C, ou bien
> - Le Module B exporte ses dépendances sur le Module C.

Report a bug

3.1.5. Chargement des classes dans les déploiements

Dans le cadre du chargement de classes, tous les déploiements sont traités sous forme de modules par JBoss EAP 6. On les appelle des modules dynamiques. Les comportements de chargement de classes varient selon le type de déploiement.

Déploiement WAR

Un déploiement WAR est un simple module. Les classes du répertoire **`WEB-INF/lib`** sont considérées de la même manière que celles du répertoire **`WEB-INF/classes`**. Toutes les classes empaquetées dans le war seront téléchargées par le même chargeur de classes.

Déploiement EAR

Les déploiements EAR sont faits de plus d'un module. La définition de ces modules suit ces règles :

1. Le répertoire **`lib/`** du EAR est un simple module nommé le module parent.
2. Chaque déploiement WAR du EAR est un module simple.
3. Chaque déploiement EJB JAR du EAR est un simple module.

Les modules de sous-déploiement (les déploiements WAR et JAR dans EAR) ont une dépendance automatique sur le module parent. Cependant ils n'ont pas de dépendance automatique l'un sur l'autre. Ceci est appelé l'isolement du sous-déploiement et peut être désactivé par déploiement ou pour le serveur de toute l'application dans son ensemble.

Les dépendances explicites entre les modules de sous-déploiement peuvent être ajoutées par les mêmes moyens, tout comme tout autre module.

Report a bug

3.1.6. Précédence pour le chargement des classes

Le chargeur de classes modulaires JBoss EAP 6 utilise un système de priorité pour empêcher le chargement des conflits de classes.

Pendant le déploiement, la liste complète des packages et des classes est créée pour chaque déploiement et chacune de ses dépendances. La liste est ordonnée selon les règles de priorité de chargement de classes. Lors du chargement de classes au moment de l'exécution, le chargeur de classes recherche dans cette liste et charge la première correspondance. Cela empêche plusieurs copies des mêmes classes et packages dans le chemin d'accès de classe des déploiements d'entrer en conflit avec l'un avec l'autre.

Le chargeur de classe charge les classes dans l'ordre suivant, du plus élevé au plus bas :

1. Dépendances implicites.

   Voici les dépendances qui sont ajoutées automatiquement par JBoss EAP 6, comme les API JAVA EE. Ces dépendances ont la plus haute précédence de chargeur de classe car ils contiennent des API et des fonctionnalités communes qui sont fournies par JBoss EAP 6.

   Voir Section 3.8.1, « Dépendances de modules implicites » pour obtenir des détails sur chaque dépendance implicite.

2. Dépendances explicites

   Il s'agit de dépendances qui sont ajoutées manuellement dans la configuration de l'application. Cela peut être fait à l'aide du fichier d'application **`MANIFEST.MF`** ou du nouveau fichier du descripteur de déploiement en option de JBoss **`jboss-deployment-structure.xml`**.

   Voir Section 3.2, « Ajouter une dépendance de module explicite à un déploiement » pour apprendre comment ajouter des dépendances explicites.

3. Ressources locales.

   Fichiers de classe empaquetées à l'intérieur du déploiement lui-même, par ex. les répertoires **`WEB-INF/classes`** ou **`WEB-INF/lib`** d'un fichier WAR.

4. Dépendances inter-déploiement.

   Ce sont des dépendances sur les autres déploiements d'un déploiement EAR. Cela peut inclure des classes du répertoire **`lib`** du EAR ou des classes des autres jars EJB.

Report a bug

3.1.7. Nommage de modules dynamiques

Tous les déploiements sont chargés en tant que modules par JBoss EAP 6 et sont nommés en fonction des conventions suivantes :

1. Les déploiements des fichiers WAR et JAR sont nommés selon le format suivant :

   ```
   deployment.DEPLOYMENT_NAME
   ```

   Par exemple, **`inventory.war`** et **`store.jar`** auront les mêmes noms de module que **`deployment.inventory.war`** et **`deployment.store.jar`** respectivement.

2. Les sous-déploiements des archives Enterprise sont nommés selon le format suivant :

```
deployment.EAR_NAME.SUBDEPLOYMENT_NAME
```

Ainsi, le sous-déploiement **reports.war**, qui se trouve dans l'archive enterprise **accounts.ear**, aura le nom de module du **deployment.accounts.ear.reports.war**.

Report a bug

3.1.8. jboss-deployment-structure.xml

jboss-deployment-structure.xml est un descripteur de déploiement optionnel de JBoss EAP 6. Ce descripteur de déploiement fournit un contrôle pour le chargement de classes dans le déploiement.

Le schéma XML de ce descripteur de déploiement se trouve dans ***EAP_HOME*/docs/schema/jboss-deployment-structure-1_2.xsd**

Report a bug

3.2. AJOUTER UNE DÉPENDANCE DE MODULE EXPLICITE À UN DÉPLOIEMENT

Cette tâche montre comment ajouter une dépendance explicite à une application. On peut ajouter des dépendances explicites de module aux applications pour ajouter les classes de ces modules au chemin de classe de l'application lors du déploiement.

Certaines dépendances sont automatiquement ajoutées aux déploiements par JBoss EAP 6. Voir Section 3.8.1, « Dépendances de modules implicites » pour plus d'informations.

Prérequis

1. Vous devez déjà avoir un projet de logiciel qui fonctionne, et auquel vous souhaitez ajouter une dépendance de module.
2. Vous devez connaître le nom du module qui est ajouté comme dépendance. Voir Section 3.8.2, « Les modules inclus » pour obtenir la liste des modules statiques inclus dans JBoss EAP 6. Si le module correspond à un autre déploiement, voir Section 3.1.7, « Nommage de modules dynamiques » pour déterminer le nom du module.

Les dépendances peuvent être configurées par deux méthodes différentes :

1. Par l'ajout d'entrées dans le fichier **MANIFEST.MF** du déploiement.
2. Par l'ajout d'entrées dans le descripteur de déploiement **jboss-deployment-structure.xml**.

Procédure 3.1. Par l'ajout d'une configuration de dépendance à MANIFEST.MF

Les projets Maven peuvent être configurés pour créer les entrées de dépendance requises par le fichier **MANIFEST.MF**. Voir Section 3.3, « Générer des entrées MANIFEST.MF en utilisant Maven » .

1. **Ajouter le fichier MANIFEST.MF**
   Si le projet ne possède pas de fichier **MANIFEST.MF**, créer un fichier nommé **MANIFEST.MF**. Pour une application web (WAR), ajouter ce fichier au répertoire **META-INF**. Pour une archive EJB (JAR), l'ajouter au répertoire **META-INF**.

2. **Ajouter une entrée de dépendance**
   Ajouter une entrée de dépendance au fichier **MANIFEST.MF** avec une liste de noms de modules de dépendance séparés par des virgules.

   ```
   Dépendances : org.javassist, org.apache.velocity
   ```

3. **Option: rendre une dépendance optionnelle**
   On peut rendre une dépendance optionnelle an ajoutant **optional** au nom du module de l'entrée de dépendance.

   ```
   Dépendances : org.javassist optional, org.apache.velocity
   ```

4. **Option : export d'une dépendance**
   On peut exporter une dépendance en ajoutant **export** au nom du module de l'entrée de dépendance.

   ```
   Dépendences : org.javassist, org.apache.velocity export
   ```

Procédure 3.2. Ajouter une configuration de dépendance à jboss-deployment-structure.xml

1. **Ajouter `jboss-deployment-structure.xml`**
   Si l'application n'a pas de fichier **`jboss-deployment-structure.xml`**, créer un nouveau fichier nommé **`jboss-deployment-structure.xml`** et l'ajouter au projet. Ce fichier est un fichier XML ayant l'élément racine de **`<jboss-deployment-structure>`** .

   ```
   <jboss-deployment-structure>

   </jboss-deployment-structure>
   ```

   Pour une application web (WAR), ajouter ce fichier au répertoire **WEB-INF**. Pour une archive EJB (JAR), l'ajouter au répertoire **META-INF**.

2. **Ajouter une section de dépendances**
   Créer un élément **`<deployment>`** à l'intérieur de la racine du document et un élément **`<dependencies>`** également.

3. **Ajouter les éléments du module**
   Dans le nœud de dépendances, ajouter un élément de module pour chaque dépendance du module. Définir l'attribut **name** au nom du module.

   ```
   <module name="org.javassist" />
   ```

4. **Option: rendre une dépendance optionnelle**
   On peut rendre une dépendance optionnelle en ajoutant l'attribut **`optional`** à l'entrée du module, avec la valeur **TRUE**. La valeur par défaut de cet attribut est **FALSE**.

   ```
   <module name="org.javassist" optional="TRUE" />
   ```

5. **Option : export d'une dépendance**
   On peut exporter une dépendance en ajoutant l'attribut **`optional`** à l'entrée du module, avec la valeur **TRUE**. La valeur par défaut de cet attribut est **FALSE**.

```
<module name="org.javassist" export="TRUE" />
```

Exemple 3.3. jboss-deployment-structure.xml avec deux dépendances

```
<jboss-deployment-structure>

   <deployment>

      <dependencies>
         <module name="org.javassist" />
         <module name="org.apache.velocity" export="TRUE" />
      </dependencies>

   </deployment>

</jboss-deployment-structure>
```

JBoss EAP 6 ajoutera les classes à partir des modules spécifiés dans le chemin de classes de l'application quand elle sera déployée.

Report a bug

3.3. GÉNÉRER DES ENTRÉES MANIFEST.MF EN UTILISANT MAVEN

Les projets Maven qui utilisent les plug-ins JAR, EJB ou WAR peuvent générer un fichier **MANIFEST.MF** avec une entrée **Dependencies**. Ce procédé ne génère pas automatiquement la liste de dépendances, il crée seulement le fichier **MANIFEST.MF** avec les informations spécifiées dans le fichier **pom.xml**.

Prérequis

1. Vous devez déjà posséder un projet Maven en cours
2. Le projet Maven doit utiliser l'un des plug-ins JAR, EJB, ou WAR (**maven-jar-plugin**, **maven-ejb-plugin**, **maven-war-plugin**).
3. Vous devez connaître le nom des dépendances de module du projet. Voir Section 3.8.2, « Les modules inclus » pour obtenir la liste des modules statiques inclus dans JBoss EAP 6. Si le module est dans un autre déploiement, voir Section 3.1.7, « Nommage de modules dynamiques » pour déterminer le nom du module.

Procédure 3.3. Générer un fichier MANIFEST.MF contenant des dépendances de module.

1. **Ajouter une Configuration**
   Ajouter la configuration suivante à la configuration du plug-in de l'empaquetage dans le fichier **pom.xml** du projet.

```
<configuration>
   <archive>
      <manifestEntries>
         <Dependencies></Dependencies>
```

```
        </manifestEntries>
      </archive>
    </configuration>
```

2. **Dépendances de la Liste**
   Ajouter la liste des dépendances de module dans l'élement <Dependencies> . Utiliser le même format utilisé lors de l'ajout des dépendances dans le **MANIFEST.MF**. Veuillez consulter Section 3.2, « Ajouter une dépendance de module explicite à un déploiement » pour plus d'informations concernant ce format.

```
<Dependencies>org.javassist, org.apache.velocity</Dependencies>
```

3. **Construire le projet**
   Construire le projet en utilisant l'objectif d'assemblage de Maven.

```
[Localhost ]$ mvn assembly:assembly
```

Quand un projet est construit en utilisant l'objectif d'assemblage, l'archive finale comprend un fichier **MANIFEST.MF** avec les dépendances de module spécifiées.

Exemple 3.4. Dépendances de module configurées dans pom.xml

L'exemple ci-dessous montre le plug-in WAR mais il fonctionne également avec les plug-ins JAR et EJB (maven-jar-plugin and maven-ejb-plugin).

```
<plugins>
   <plugin>
      <groupId>org.apache.maven.plugins</groupId>
      <artifactId>maven-war-plugin</artifactId>
      <configuration>
         <archive>
            <manifestEntries>
               <Dependencies>org.javassist,
org.apache.velocity</Dependencies>
            </manifestEntries>
         </archive>
      </configuration>
   </plugin>
</plugins>
```

Report a bug

3.4. EMPÊCHER QU'UN MODULE SOIT CHARGÉ IMPLICITEMENT

Cette tâche décrit comment configurer votre application pour en exclure une liste de dépendances de module.

Vous pouvez configurer une application déployable pour empêcher le chargement des dépendances implicites. Cela est commun quand il s'agit d'une version différente de bibliothèque ou d'un framework autre que celui qui sera fourni par le serveur d'applications comme dépendance implicite.

Prérequis

1. Vous devez déjà avoir un projet informatique qui fonctionne et dont vous souhaitez exclure une dépendance.

2. Vous devez connaître le nom du module à exclure. Voir Section 3.8.1, « Dépendances de modules implicites » pour obtenir une liste des dépendances implicites et de leurs conditions.

Procédure 3.4. Ajouter une configuration d'exclusion de dépendances de jboss-deployment-structure.xml

1. Si l'application n'a pas de fichier **`jboss-deployment-structure.xml`**, créer un nouveau fichier intitulé **`jboss-deployment-structure.xml`** et ajoutez-le au projet. Ce fichier est un fichier XML ayant comme élément root **`<jboss-deployment-structure>`** .

```
<jboss-deployment-structure>

</jboss-deployment-structure>
```

   Pour une application web (WAR), ajouter ce fichier au répertoire **`WEB-INF`**. Pour une archive EJB (JAR), l'ajouter au répertoire **`META-INF`**.

2. Créer un élément **`<deployment>`** dans la racine de l'élément et un **`<exclusions>`** à l'intérieur.

```
<deployment>
   <exclusions>

   </exclusions>
</deployment>
```

3. Dans l'élément d'exclusion, ajouter un élément **`<module>`** pour chaque module à exclure. Définir l'attribut **name** au nom du module.

```
<module name="org.javassist" />
```

Exemple 3.5. Exclusion de deux modules

```
<jboss-deployment-structure>
   <deployment>
      <exclusions>
         <module name="org.javassist" />
         <module name="org.dom4j" />
      </exclusions>
   </deployment>
</jboss-deployment-structure>
```

Report a bug

3.5. EXCLURE UN SOUS-SYSTÈME D'UN DÉPLOIEMENT

Résumé

Ce sujet traite des étapes nécessaires pour exclure un sous-système d'un déploiement. Pour ce faire, il

convient de modifier le fichier de configuration **`jboss-deployment-structure.xml`**. Le fait d'exclure un sous-système crée le même effet que de le retirer, sauf qu'il ne s'applique qu'à un seul déploiement.

Procédure 3.5. Exclure un sous-système

1. Ouvrir le fichier **`jboss-deployment-structure.xml`** dans un éditeur de texte.
2. Ajouter le XML suivant dans les balises de <deployment> :

```
<exclude-subsystems>
  <subsystem name="SUBSYSTEM_NAME" />
</exclude-subsystems>
```

3. Enregistrer le fichier **`jboss-deployment-structure.xml`**

Résultat

Le sous-système a bien été exclus. Les processeurs d'unité de déploiement du sous-système n'exécuteront plus sur le déploiement.

Exemple 3.6. Exemple d'un fichier `jboss-deployment-structure.xml`.

```
<jboss-deployment-structure xmlns="urn:jboss:deployment-structure:1.2">
  <ear-subdeployments-isolated>true</ear-subdeployments-isolated>
  <deployment>
    <exclude-subsystems>
      <subsystem name="resteasy" />
    </exclude-subsystems>
    <exclusions>
      <module name="org.javassist" />
    </exclusions>
    <dependencies>
      <module name="deployment.javassist.proxy" />
      <module name="deployment.myjavassist" />
      <module name="myservicemodule" services="import"/>
    </dependencies>
    <resources>
      <resource-root path="my-library.jar" />
    </resources>
  </deployment>
  <sub-deployment name="myapp.war">
    <dependencies>
      <module name="deployment.myear.ear.myejbjar.jar" />
    </dependencies>
    <local-last value="true" />
  </sub-deployment>
  <module name="deployment.myjavassist" >
    <resources>
     <resource-root path="javassist.jar" >
       <filter>
         <exclude path="javassist/util/proxy" />
       </filter>
     </resource-root>
    </resources>
```

```
  </module>
  <module name="deployment.javassist.proxy" >
    <dependencies>
      <module name="org.javassist" >
        <imports>
          <include path="javassist/util/proxy" />
          <exclude path="/**" />
        </imports>
      </module>
    </dependencies>
  </module>
</jboss-deployment-structure>
```

Report a bug

3.6. UTILISER LE CHARGEUR DE CLASSES PAR PROGRAMMATION DANS UN DÉVELOPPEMENT

3.6.1. Chargement des classes et des ressources par programmation dans le déploiement.

Vous pouvez trouver ou charger des classes ou des ressources par programmation dans votre code d'application. La méthode choisie dépendra d'un certain nombre de facteurs. Cette section décrit les méthodes disponibles et vous donne des instructions sur la façon de les utiliser.

Charger une classe en utilisant la méthode Class.forName() Method

Vous pouvez utiliser la méthode **`Class.forName()`** pour charger ou initialiser les classes par programmation. Cette méthode comprend deux signatures.

Class.forName(String className)

Cette signature ne prend en compte qu'un seul paramètre, le nom de la classe que vous devez charger. Avec cette méthode de signature, la classe est chargée par le chargeur de classes et initialise la classe nouvellement chargée par défaut.

Class.forName(String className, boolean initialize, ClassLoader loader)

Cette signature s'attend à recevoir trois paramètres : le nom de la classe, une valeur booléenne qui indique si on doit initialiser la classe, et le ClassLoader qui doit charger la classe.

La signature à trois arguments est la méthode recommandée pour charger une classe par programmation. Cette signature vous permet de contrôler si vous souhaitez que la classe cible soit initialisée pendant le chargement. Il est également plus efficace d'obtenir et de fournir le chargeur de classe parce que la JVM n'a pas besoin d'examiner la pile des appels pour déterminer quel chargeur de classe utiliser. En supposant que la classe contenant le code se nomme **`CurrentClass`**, vous pourrez obtenir le chargeur de classes de la classe par la méthode **`Current.class.getClassLoader()`**.

L'exemple suivant donne un exemple de chargeur de classes qui puisse charger et initialiser la classe **`TargetClass`** :

Exemple 3.7. Fournir un chargeur de classes pour télécharger et initialiser les TargetClass.

```
Class<?> targetClass = Class.forName("com.myorg.util.TargetClass",
true, CurrentClass.class.getClassLoader());
```

Chercher toutes les ressources avec un Prénom

Si vous connaissez le nom ou le chemin de la ressource, la meilleure façon de la charger directement serait d'utiliser la classe JDK ou l'API Classloader.

Charger une seule ressource

Pour charger une seule ressource qui se trouve dans le même répertoire que votre classe ou dans une autre classe de votre déploiement, vous pouvez utiliser la méthode **`Class.getResourceAsStream()`**.

Exemple 3.8. Charger une seule ressource dans votre déploiement.

```
InputStream inputStream =
CurrentClass.class.getResourceAsStream("targetResourceName");
```

Charger toutes les instances en une ressource unique

Pour charger toutes les instances d'une même ressource qui sont visibles par le chargeur de classe de votre déploiement, utilisez la méthode **`Class.getClassLoader retourne ().getResources(String resourceName)`**, où **`resourceName`** est le chemin d'accès qualifié complet de la ressource. Cette méthode retourne une énumération de tous les objets **URL** pour les ressources accessibles par le chargeur de classe du prénom donné. Vous pouvez ensuite parcourir le tableau des URL pour ouvrir chaque flux à l'aide de la méthode **`openStream()`**.

Exemple 3.9. Charger toutes les instances d'une ressource et itérer le résultat.

```
Enumeration<URL> urls =
CurrentClass.class.getClassLoader().getResources("full/path/to/reso
urce");
while (urls.hasMoreElements()) {
    URL url = urls.nextElement();
    InputStream inputStream = null;
    try {
        inputStream = url.openStream();
        // Process the inputStream
        ...
    } catch(IOException ioException) {
        // Handle the error
    } finally {
        if (inputStream != null) {
            try {
                inputStream.close();
            } catch (Exception e) {
                // ignore
            }
        }
    }
}
```

NOTE

Comme les instances URL sont chargées à partir du stockage local, il n'est pas utile d'utiliser **`openConnection()`** ou méthodes semblables. Les flux sont plus faciles à utiliser et minimisent la complexité du code.

Charger un fichier de classe à partir d'un chargeur de classes

Si une classe a déjà été chargée, vous pouvez charger le fichier de classe qui correspond à cette classe en utilisant la syntaxe suivante :

Exemple 3.10. Charger un fichier de classe déjà chargée.

```
InputStream inputStream =
CurrentClass.class.getResourceAsStream(TargetClass.class.getSimpleNam
e() + ".class");
```

Si la classe n'a pas encore été chargée, vous devrez utiliser le chargeur de classes et en interpréter le chemin d'accès :

Exemple 3.11. Charger un fichier de classe d'une classe qui n'a pas été chargée.

```
String className = "com.myorg.util.TargetClass"
InputStream inputStream =
CurrentClass.class.getClassLoader().getResourceAsStream(className.rep
lace('.', '/') + ".class");
```

Report a bug

3.6.2. Itérer les ressources par programmation dans un déploiement.

La bibliothèque JBoss Modules fournit plusieurs API pour itérer toutes les ressources de déploiement. La JavaDoc de l'API de JBoss Modules se trouve à cet endroit : http://docs.jboss.org/jbossmodules/1.3.0.Final/api/. Pour utiliser des API, vous devez ajouter la dépendance suivante à **`MANIFEST.MF`**:

```
Dépendences: org.jboss.modules
```

Il est important de noter que malgré que ces API fournissent une flexibilité grandissante, ils exécuteront bien plus lentement qu'une recherche de chemin d'accès directe.

Cette section décrit un nombre de façons dont vous pouvez itérer les ressources de votre code d'application par programmation.

Lister les ressources du déploiement et de toutes les importations.

Il y a des moments où il n'est pas possible de rechercher des ressources par le chemin exact. Par exemple, le chemin d'accès exact n'est peut être pas connu ou vous devrez peut-être examiner plus d'un fichier dans un chemin d'accès donné. Dans ce cas, la bibliothèque de modules de JBoss fournit

plusieurs API pour une itération de toutes les ressources de déploiement. Vous pouvez parcourir les ressources dans un déploiement en utilisant une des deux méthodes.

Itérer toutes les ressources qui se trouvent dans un seul module

La méthode **`ModuleClassLoader.iterateResources()`** itère toutes les ressources au sein de ce chargeur de classes de module. Cette méthode accepte deux arguments : le nom du répertoire de départ à rechercher et une valeur booléenne qui spécifie s'il doit agir récursivement dans les sous-répertoires.

L'exemple suivant montre comment on obtient le ModuleClassLoader ou l'itérateur pour les ressources qui se trouvent dans le répertoire **`bin/`**, récursivement dans les sous-répertoires.

Exemple 3.12. Chercher les ressources du répertoire "bin" récursivement dans les sous-répertoires.

```
ModuleClassLoader moduleClassLoader = (ModuleClassLoader)
TargetClass.class.getClassLoader();
Iterator<Resource> mclResources =
moduleClassLoader.iterateResources("bin",true);
```

L'itérateur résultant peut être utilisé pour examiner chaque ressource correspondante et pour chercher son nom et sa taille (si disponible), pour ouvrir une transmission à lire, ou pour obtenir l'URL d'une ressource.

Itérer toutes les ressources qui se trouvent dans un seul module et dans les ressources importées

La méthode **`Module.iterateResources()`** itère toutes les ressources au sein de ce chargeur de classes de module, y compris les ressources qui sont importées dans le module. Cette méthode renvoie un ensemble beaucoup plus vaste que la méthode précédente. Cette méthode requiert un argument: un filtre qui rétrécit le résultat à un modèle spécifique. Alternativement, les PathFilters.acceptAll() peuvent être fournis pour retourner l'ensemble.

Exemple 3.13. Chercher toutes les ressources de ce module, y compris les importations.

```
ModuleClassLoader moduleClassLoader = (ModuleClassLoader)
TargetClass.class.getClassLoader();
Module module = moduleClassLoader.getModule();
Iterator<Resource> moduleResources =
module.iterateResources(PathFilters.acceptAll());
```

Chercher toutes les ressources qui correspondent à un modèle particulier

Si vous avez besoin de trouver des ressources spécifiques dans votre déploiement ou dans son importation complète, vous devrez filtrer l'itération de la ressource. Les API de filtrage de JBoss Modules peuvent vous donner plusieurs outils pour y parvenir.

Examiner toutes les dépendances

Si vous devez examiner l'ensemble des dépendances, vous pouvez utiliser le paramètre **`PathFilter`** de la méthode **`Module.iterateResources()`** pour vérifier le nom de chaque ressource et trouver une correspondance.

Examiner les dépendances de déploiement

Si vous devez regarder uniquement dans le déploiement, utilisez la méthode **`ModuleClassLoader.iterateResources()`**. Toutefois, vous devez utiliser des méthodes supplémentaires pour filtrer l'itérateur qui en résulte. La méthode **`PathFilters.filtered()`** peut fournir une vue filtrée d'un itérateur de ressources dans ce cas. La classe **`PathFilters`** comprend plusieurs méthodes statiques pour créer et composer des filtres qui remplissent des fonctions diverses, y compris la recherche de chemins dépendants ou des correspondances exactes, ou encore correspondant à un motif "glob" Ant-style.

Exemples de codes supplémentaires pour filtrer les ressources

Les exemples suivants démontrent comment filtrer les ressources sur la base de critères différents.

Exemple 3.14. Trouver tous les noms qui comprennent "messages.properties" dans votre déploiement.

```
ModuleClassLoader moduleClassLoader = (ModuleClassLoader)
TargetClass.class.getClassLoader();
Iterator<Resource> mclResources =
PathFilters.filtered(PathFilters.match("**/messages.properties"),
moduleClassLoader.iterateResources("", true));
```

Exemple 3.15. Trouver tous les noms qui comprennent "messages.properties" dans votre déploiement et dans vos importations.

```
ModuleClassLoader moduleClassLoader = (ModuleClassLoader)
TargetClass.class.getClassLoader();
Module module = moduleClassLoader.getModule();
Iterator<Resource> moduleResources =
module.iterateResources(PathFilters.match("**/message.properties));
```

Exemple 3.16. Trouver tous les fichiers qui se trouvent dans tout répertoire nommé "my-resources" de votre déploiement.

```
ModuleClassLoader moduleClassLoader = (ModuleClassLoader)
TargetClass.class.getClassLoader();
Iterator<Resource> mclResources =
PathFilters.filtered(PathFilters.match("**/my-resources/**"),
moduleClassLoader.iterateResources("", true));
```

Exemple 3.17. Trouver tous les fichiers nommés "messages.properties" dans votre déploiement et dans vos importations.

```
ModuleClassLoader moduleClassLoader = (ModuleClassLoader)
TargetClass.class.getClassLoader();
Module module = moduleClassLoader.getModule();
```

```
Iterator<Resource> moduleResources =
module.iterateResources(PathFilters.any(PathFilters.match("**/messages
"), PathFilters.match("**/errors"));
```

Exemple 3.18. Trouver tous les fichiers qui se trouvent dans un package spécifique de votre déploiement.

```
ModuleClassLoader moduleClassLoader = (ModuleClassLoader)
TargetClass.class.getClassLoader();
Iterator<Resource> mclResources =
moduleClassLoader.iterateResources("path/form/of/packagename",
false);
```

Report a bug

3.7. CHARGEMENT DE CLASSE ET SOUS-DÉPLOIEMENTS

3.7.1. Chargement de classes et de modules dans les EAR (Archives Enterprise)

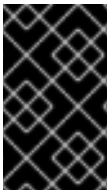
Les EAR (Archives Enterprise) ne sont pas chargées sous forme d'un simple module à la manière des déploiements JAR ou WAR. Ils sont chargés sous forme d'une multitude de modules uniques.

Les règles suivantes déterminent quels modules existent dans un EAR.

- Chaque sous-déploiement WAR ou EJB JAR est un module.
- Le contenu du répertoire **`lib/`** de la racine de l'archive EAR est un module. On l'appelle un module parent.

Ces modules possèdent le même comportement que tout autre module ayant les dépendances implicites suivantes :

- Les sous-déploiements WAR possédent des dépendances implicites sur le module parent et sur tout sous-déploiement JAR EJB.
- Les sous-déploiements EJB JAR possédent des dépendances implicites sur le module parent et sur tout sous-déploiement JAR EJB.



IMPORTANT

Aucun sous-déploiement ne gagne une dépendance implicite sur un sous-déploiement WAR. Tout sous-déploiement peut être configuré avec des dépendances explicites sur un autre sous-déploiement comme dans n'importe quel autre module.

Les dépendances implicites décrites ci-dessus ont lieu car JBoss EAP 6 a l'isolement de chargeur de classe de sous-déploiement désactivé par défaut.

Tout isolement de chargeur de classe de sous-déploiement peut être activé si une stricte compatibilité

est nécessaire. Ceci peut être activé pour un simple déploiement EAR ou pour tous les déploiements EAR. La spécification Java EE 6 recommande que les applications portables repposent pas sur des sous-déploiements pouvant accéder les uns aux autres, à moins que les dépendances soient explicitement déclarées comme entrées **Class-Path** dans le fichier **MANIFEST.MF** de chaque sous-déploiement.

Report a bug

3.7.2. Isolement du chargeur de classes d'un sous-déploiement

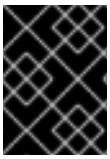
Chaque sous-déploiement d'EAR (Archive Enterprise) est un module dynamique possédant son propre chargeur de classe. Par défaut, un sous-déploiement peut accéder aux ressources d'autres sous-déploiements.

Si un sous-déploiement ne doit pas accéder aux ressources d'autres sous-déploiements (une isolation de sous-déploiement est alors requise), alors cela pourra être activé.

Report a bug

3.7.3. Désactiver l'isolement du chargeur de classes d'un sous-déploiement dans un EAR

Cette tâche vous montre comment faire pour désactiver l'isolement du chargeur de classes de sous-déploiement dans un déploiement EAR, à l'aide d'un descripteur de déploiement spécial EAR. Cela ne nécessite des modifications au serveur d'applications et n'affecte pas les autres déploiements.



IMPORTANT

Même quand l'isolement d'un chargeur de classes de sous-déploiement est désactivé, il est possible d'ajouter un déploiement WAR comme dépendance.

1. **Ajouter le fichier du descripteur de déploiement**
   Ajouter le fichier de descripteur de déploiement **jboss-deployment-structure.xml** au répertoire **META-INF** du EAR s'il n'existe pas déjà et ajouter le contenu suivant :

   ```
   <jboss-deployment-structure>

   </jboss-deployment-structure>
   ```

2. **Ajouter l'élément <ear-subdeployments-isolated>**
   Ajouter l'élément **<ear-subdeployments-isolated>** au fichier **jboss-deployment-structure.xml** s'il n'existe pas déjà dans le contenu de **false**.

   ```
   <ear-subdeployments-isolated>false</ear-subdeployments-isolated>
   ```

Résultat :

L'isolement de chargeur de classe de sous-déploiement sera maintenant désactivé pour le déploiement de cet EAR. Cela signifie que les sous-déploiements du EAR auront des dépendances automatiques sur chacun des sous-déploiements non-WAR.

Report a bug

3.8. RÉFÉRENCE

3.8.1. Dépendances de modules implicites

Le tableau suivant liste les modules qui sont ajoutés automatiquement au déploiement en tant que dépendances et les conditions qui déclenchent la dépendance.

Tableau 3.1. Dépendances de modules implicites

Sous-système	Modules toujours ajoutés	Modules ajoutés conditionnellement	Conditions
Serveur principal	• `javax.api` • `sun.jdk` • `org.jboss.logging` • `org.apache.log4j` • `org.apache.commons.logging` • `org.slf4j` • `org.jboss.logging.jul-to-slf4j-stub`	-	-
Sous-système EE	• `javaee.api`	-	-
Sous-système EJB3	-	• `javaee.api`	La présence de `ejb-jar.xml` à des emplacements valides dans le déploiement, tel que mentionné dans les spécifications Java EE 6 ou la présence d'EJB basés sur annotations (par exemple `@Stateless`, `@Stateful`, `@MessageDriven`, etc)

Sous-système	Modules toujours ajoutés	Modules ajoutés conditionnellement	Conditions
Sous-système JAX-RS (Resteasy)	• `javax.xml.bind.api`	• `org.jboss.resteasy.resteasy-atom-provider` • `org.jboss.resteasy.resteasy-cdi` • `org.jboss.resteasy.resteasy-jaxrs` • `org.jboss.resteasy.resteasy-jaxb-provider` • `org.jboss.resteasy.resteasy-jackson-provider` • `org.jboss.resteasy.resteasy-jsapi` • `org.jboss.resteasy.resteasy-multipart-provider` • `org.jboss.resteasy.async-http-servlet-30`	La présence d'annotations JAX-RS dans le déploiement

Sous-système	Modules toujours ajoutés	Modules ajoutés conditionnellement	Conditions
Sous-système JCA	• `javax.resource.api`	• `javax.jms.api` • `javax.validation.api` • `org.jboss.logging` • `org.jboss.ironjacamar.api` • `org.jboss.ironjacamar.impl` • `org.hibernate.validator`	Si le déploiement correspond à un déploiement (RAR) d'adaptateur de ressources.
Sous-système JPA (Hibernate)	• `javax.persistence.api`	• `javaee.api` • `org.jboss.as.jpa` • `org.hibernate` • `org.javassist`	La présence de l'annotation `@PersistenceUnit` ou `@PersistenceContext`, `<persistence-unit-ref>` ou encore `<persistence-context-ref>` dans un descripteur de déploiement.
Sous-système SAR	-	• `org.jboss.logging` • `org.jboss.modules`	Le déploiement correspond à une archive SAR
Sous-système de sécurité	• `org.picketbox`	-	-

Sous-système	Modules toujours ajoutés	Modules ajoutés conditionnellement	Conditions
Sous-système Web	-	• `javaee.api` • `com.sun.jsf-impl` • `org.hibernate.validator` • `org.jboss.as.web` • `org.jboss.logging`	Le déploiement correspond à une archive WAR. JavaServer Faces(JSF) est ajouté uniquement si utilisé.
Sous-système de Services Web	• `org.jboss.ws.api` • `org.jboss.ws.spi`	-	-
Sous-système Weld (CDI)	-	• `javax.persistence.api` • `javaee.api` • `org.javassist` • `org.jboss.interceptor` • `org.jboss.as.weld` • `org.jboss.logging` • `org.jboss.weld.core` • `org.jboss.weld.api` • `org.jboss.weld.spi`	Si un fichier `beans.xml` est détecté dans le déploiement

Report a bug

3.8.2. Les modules inclus

- **asm.asm**
- **ch.qos.cal10n**
- **com.google.guava**
- **com.h2database.h2**
- **com.sun.jsf-impl**
- **com.sun.jsf-impl**
- **com.sun.xml.bind**
- **com.sun.xml.messaging.saaj**
- **gnu.getopt**
- **javaee.api**
- **javax.activation.api**
- **javax.annotation.api**
- **javax.api**
- **javax.ejb.api**
- **javax.el.api**
- **javax.enterprise.api**
- **javax.enterprise.deploy.api**
- **javax.faces.api**
- **javax.faces.api**
- **javax.inject.api**
- **javax.interceptor.api**
- **javax.jms.api**
- **javax.jws.api**
- **javax.mail.api**
- **javax.management.j2ee.api**
- **javax.persistence.api**
- **javax.resource.api**

- javax.rmi.api
- javax.security.auth.message.api
- javax.security.jacc.api
- javax.servlet.api
- javax.servlet.jsp.api
- javax.servlet.jstl.api
- javax.transaction.api
- javax.validation.api
- javax.ws.rs.api
- javax.wsdl4j.api
- javax.xml.bind.api
- javax.xml.jaxp-provider
- javax.xml.registry.api
- javax.xml.rpc.api
- javax.xml.soap.api
- javax.xml.stream.api
- javax.xml.ws.api
- jline
- net.sourceforge.cssparser
- net.sourceforge.htmlunit
- net.sourceforge.nekohtml
- nu.xom
- org.antlr
- org.apache.ant
- org.apache.commons.beanutils
- org.apache.commons.cli
- org.apache.commons.codec
- org.apache.commons.collections

- **org.apache.commons.io**
- **org.apache.commons.lang**
- **org.apache.commons.logging**
- **org.apache.commons.pool**
- **org.apache.cxf**
- **org.apache.httpcomponents**
- **org.apache.james.mime4j**
- **org.apache.log4j**
- **org.apache.neethi**
- **org.apache.santuario.xmlsec**
- **org.apache.velocity**
- **org.apache.ws.scout**
- **org.apache.ws.security**
- **org.apache.ws.xmlschema**
- **org.apache.xalan**
- **org.apache.xerces**
- **org.apache.xml-resolver**
- **org.codehaus.jackson.jackson-core-asl**
- **org.codehaus.jackson.jackson-jaxrs**
- **org.codehaus.jackson.jackson-mapper-asl**
- **org.codehaus.jackson.jackson-xc**
- **org.codehaus.woodstox**
- **org.dom4j**
- **org.hibernate**
- **org.hibernate.envers**
- **org.hibernate.infinispan**
- **org.hibernate.validator**
- **org.hornetq**

- **org.hornetq.ra**
- **org.infinispan**
- **org.infinispan.cachestore.jdbc**
- **org.infinispan.cachestore.remote**
- **org.infinispan.client.hotrod**
- **org.jacorb**
- **org.javassist**
- **org.jaxen**
- **org.jboss.as.aggregate**
- **org.jboss.as.appclient**
- **org.jboss.as.cli**
- **org.jboss.as.clustering.api**
- **org.jboss.as.clustering.common**
- **org.jboss.as.clustering.ejb3.infinispan**
- **org.jboss.as.clustering.impl**
- **org.jboss.as.clustering.infinispan**
- **org.jboss.as.clustering.jgroups**
- **org.jboss.as.clustering.service**
- **org.jboss.as.clustering.singleton**
- **org.jboss.as.clustering.web.infinispan**
- **org.jboss.as.clustering.web.spi**
- **org.jboss.as.cmp**
- **org.jboss.as.connector**
- **org.jboss.as.console**
- **org.jboss.as.controller**
- **org.jboss.as.controller-client**
- **org.jboss.as.deployment-repository**
- **org.jboss.as.deployment-scanner**

- **org.jboss.as.domain-add-user**
- **org.jboss.as.domain-http-error-context**
- **org.jboss.as.domain-http-interface**
- **org.jboss.as.domain-management**
- **org.jboss.as.ee**
- **org.jboss.as.ee.deployment**
- **org.jboss.as.ejb3**
- **org.jboss.as.embedded**
- **org.jboss.as.host-controller**
- **org.jboss.as.jacorb**
- **org.jboss.as.jaxr**
- **org.jboss.as.jaxrs**
- **org.jboss.as.jdr**
- **org.jboss.as.jmx**
- **org.jboss.as.jpa**
- **org.jboss.as.jpa.hibernate**
- **org.jboss.as.jpa.hibernate**
- **org.jboss.as.jpa.hibernate.infinispan**
- **org.jboss.as.jpa.openjpa**
- **org.jboss.as.jpa.spi**
- **org.jboss.as.jpa.util**
- **org.jboss.as.jsr77**
- **org.jboss.as.logging**
- **org.jboss.as.mail**
- **org.jboss.as.management-client-content**
- **org.jboss.as.messaging**
- **org.jboss.as.modcluster**
- **org.jboss.as.naming**

- **org.jboss.as.network**
- **org.jboss.as.osgi**
- **org.jboss.as.platform-mbean**
- **org.jboss.as.pojo**
- **org.jboss.as.process-controller**
- **org.jboss.as.protocol**
- **org.jboss.as.remoting**
- **org.jboss.as.sar**
- **org.jboss.as.security**
- **org.jboss.as.server**
- **org.jboss.as.standalone**
- **org.jboss.as.threads**
- **org.jboss.as.transactions**
- **org.jboss.as.web**
- **org.jboss.as.webservices**
- **org.jboss.as.webservices.server.integration**
- **org.jboss.as.webservices.server.jaxrpc-integration**
- **org.jboss.as.weld**
- **org.jboss.as.xts**
- **org.jboss.classfilewriter**
- **org.jboss.com.sun.httpserver**
- **org.jboss.common-core**
- **org.jboss.dmr**
- **org.jboss.ejb-client**
- **org.jboss.ejb3**
- **org.jboss.iiop-client**
- **org.jboss.integration.ext-content**
- **org.jboss.interceptor**

- **org.jboss.interceptor.spi**
- **org.jboss.invocation**
- **org.jboss.ironjacamar.api**
- **org.jboss.ironjacamar.impl**
- **org.jboss.ironjacamar.jdbcadapters**
- **org.jboss.jandex**
- **org.jboss.jaxbintros**
- **org.jboss.jboss-transaction-spi**
- **org.jboss.jsfunit.core**
- **org.jboss.jts**
- **org.jboss.jts.integration**
- **org.jboss.logging**
- **org.jboss.logmanager**
- **org.jboss.logmanager.log4j**
- **org.jboss.marshalling**
- **org.jboss.marshalling.river**
- **org.jboss.metadata**
- **org.jboss.modules**
- **org.jboss.msc**
- **org.jboss.netty**
- **org.jboss.osgi.deployment**
- **org.jboss.osgi.framework**
- **org.jboss.osgi.resolver**
- **org.jboss.osgi.spi**
- **org.jboss.osgi.vfs**
- **org.jboss.remoting3**
- **org.jboss.resteasy.resteasy-atom-provider**
- **org.jboss.resteasy.resteasy-cdi**

- **org.jboss.resteasy.resteasy-jackson-provider**
- **org.jboss.resteasy.resteasy-jaxb-provider**
- **org.jboss.resteasy.resteasy-jaxrs**
- **org.jboss.resteasy.resteasy-jsapi**
- **org.jboss.resteasy.resteasy-multipart-provider**
- **org.jboss.sasl**
- **org.jboss.security.negotiation**
- **org.jboss.security.xacml**
- **org.jboss.shrinkwrap.core**
- **org.jboss.staxmapper**
- **org.jboss.stdio**
- **org.jboss.threads**
- **org.jboss.vfs**
- **org.jboss.weld.api**
- **org.jboss.weld.core**
- **org.jboss.weld.spi**
- **org.jboss.ws.api**
- **org.jboss.ws.common**
- **org.jboss.ws.cxf.jbossws-cxf-client**
- **org.jboss.ws.cxf.jbossws-cxf-factories**
- **org.jboss.ws.cxf.jbossws-cxf-server**
- **org.jboss.ws.cxf.jbossws-cxf-transports-httpserver**
- **org.jboss.ws.jaxws-client**
- **org.jboss.ws.jaxws-jboss-httpserver-httpspi**
- **org.jboss.ws.native.jbossws-native-core**
- **org.jboss.ws.native.jbossws-native-factories**
- **org.jboss.ws.native.jbossws-native-services**
- **org.jboss.ws.saaj-impl**

- **org.jboss.ws.spi**
- **org.jboss.ws.tools.common**
- **org.jboss.ws.tools.wsconsume**
- **org.jboss.ws.tools.wsprovide**
- **org.jboss.xb**
- **org.jboss.xnio**
- **org.jboss.xnio.nio**
- **org.jboss.xts**
- **org.jdom**
- **org.jgroups**
- **org.joda.time**
- **org.junit**
- **org.omg.api**
- **org.osgi.core**
- **org.picketbox**
- **org.picketlink**
- **org.python.jython.standalone**
- **org.scannotation.scannotation**
- **org.slf4j**
- **org.slf4j.ext**
- **org.slf4j.impl**
- **org.slf4j.jcl-over-slf4j**
- **org.w3c.css.sac**
- **sun.jdk**

Report a bug

3.8.3. Référence de descripteur de déploiement de structure de déploiement de JBoss

Les tâches principales qui peuvent être effectuées par ce descripteur de déploiement sont les suivantes :

- Définition des dépendances de modules explicites.
- Empêcher les dépendances implicites spécifiques de charger.
- Définir des modules supplémentaires à partir des ressources de ce déploiement.
- Modifier le comportement de l'isolation du sous-déploiement dand ce déploiement EAR.
- Ajouter des racines de ressources supplémentaires à un EAR.

Report a bug

CHAPITRE 4. VALVES GLOBALES

4.1. VALVES

Une valve est une classe Java insérée dans le pipeline de traitement de demande d'une application. Elle est insérée dans le pipeline avant les filtres servlet. Les valves peuvent apporter des modifications à la demande avant de les passer ou d'effectuer tout autre traitement comme l'authentification ou annuler la demande. Les valves sont généralement empaquetées dans une application.

Les versions 6.1.0 et supérieures prennent en charge les valves globales.

Report a bug

4.2. VALVES GLOBALES

Une valve globale est une valve insérée dans le pipeline de traitement de requête de toutes les applications déployées. Une valve est rendue globale lorsqu'elle est mise en paquetage et qu'elle est installée comme module statique dans JBoss EAP 6. Les valves globales sont configurées dans le sous-système web.

Seules les versions 6.1.0 et supérieures prennent en charge les valves globales.

Report a bug

4.3. LES VALVES D'AUTHENTIFICATION

Une valve d'authentification est une valve qui authentifie les informations d'identification d'une requête. Cette valve est une sous-classe de **`org.apache.catalina.authenticator.AuthenticatorBase`** et elle remplace la méthode **`authenticate()`**

Elle peut être utilisée pour implémenter des schémas d'authentification supplémentaires.

Report a bug

4.4. CONFIGURER UNE APPLICATION WEB POUR UTILISER UNE VALVE.

Les valves qui ne sont pas installées en tant que valves globales doivent être incluses avec votre application et configurées dans le descripteur de déploiement **`jboss-web.xml`**.

IMPORTANT

Les valves qui sont installées en tant que valves globales s'appliquent automatiquement à toutes les applications déployées.

Prérequis

- La valve doit être créée et incluse dans le chemin de classe de l'application. Pour ce faire, il convient de l'inclure dans le fichier WAR de l'application ou dans tout autre module ajouté comme dépendance. Les exemples de tels modules comprennent un module statique installé

sur le serveur ou un fichier JAR dans le répertoire **lib/** d'une archive EAR si le WAR est déployé dans un EAR.

- L'application doit inclure un descripteur de déploiement de **jboss-web.xml**.

Procédure 4.1. Configurer une application pour une valve locale.

1. **Ajouter un élément de Valve**
   Ajouter un élément de valve avec les attributs de nom et de nom de classe au fichier **jboss-web.xml** de l'application. Le nom est un identifiant unique pour la valve et la classe de nom est le nom de la classe de valve.

   ```
   <valve>
         <class-name>VALVECLASSNAME</class-name>
   </valve>
   ```

2. **Paramètres spécifiques**
   Si la valve possède des paramètres configurables, ajouter un élément enfant **param** à l'élément valve pour chaque paramètre, en spécifiant leur nom et leur valeur.

   ```
   <param name="PARAMNAME" value = "VALUE" />
   ```

Une fois l'application déployée, la valve est autorisée pour l'application avec la configuration spécifiée.

Exemple 4.1. Configuration valve jboss-web.xml

```
<valve>
    <class-name="org.jboss.samplevalves.restrictedUserAgentsValve">
    <param name="restricteduseragents"  value = "^.*MS Web Services
Client Protocol.*$" />
</valve>
```

Report a bug

4.5. CONFIGURER UNE APPLICATION WEB POUR QU'ELLE UTILISE UNE VALVE D'AUTHENTIFICATION

Afin de configurer une application pour utiliser une valve d'authentification, il convient d'installer et de configurer la valve (locale à l'application ou en tant que valve globale) et de configurer le descripteur de déploiement **web.xml** de l'application. Dans le cas le plus simple, la configuration **web.xml** revient à utiliser une authentification **BASIC** sauf que l'élément enfant **auth-method** de **login-config** est défini sous le nom de la valve qui effectue la configuration.

Prérequis

- La valve d'authentification devrait déjà être créée.
- Si la valve d'authentification est une valve globale, cette dernière devrait déjà être installée et configurée, et il vous convient de connaître le nom sous laquelle elle a été configurée.
- Informez-vous du nom de domaine de la zone de sécurité que l'application utilise.

Si vous ne savez pas quel nom de domaine de la zone de sécurité ou la valve à utiliser, informez-vous auprès de l'administrateur de votre serveur.

Procédure 4.2. Configurer une application pour utiliser une valve d'authentification

1. **Configurer la valve**
   L'utilisation d'une valve locale nécessite une configuration dans le descripteur de déploiement **`jboss-web.xml`** des applications. Voir Section 4.4, « Configurer une application web pour utiliser une valve. ».

   Cela n'est pas nécessaire pour l'utilisation d'une valve globale.

2. **Ajouter une configuration de sécurité à web.xml.**
   Ajouter la configuration de sécurité au fichier web.xml pour votre application en utilisant les éléments standards tels que la contrainte de sécurité, la configuration de l'identifiant et le rôle de la sécurité. Dans l'élément de configuration de l'identifiant, définir la valeur de la méthode d'identification en tant que nom de la valve d'identification. L'élément de nom de la zone doit également être défini en tant que nom de la zone de sécurité de JBoss utilisée par l'application.

   ```
   <login-config>
      <auth-method>VALVE_NAME</auth-method>
      <realm-name>REALM_NAME</realm-name>
   </login-config>
   ```

Quand l'application est déployée, l'authentification des requêtes est gérée par la valve d'authentification configurée.

Report a bug

4.6. CRÉER UNE VALVE PERSONNALISÉE

Une Valve est une classe Java qui est insérée dans le pipeline de traitement de requête pour une application avant les filtres de servlet de l'application.

Procédure 4.3. Créer une valve personnalisée

1. **Créer la classe Valve**
   Créer une sous-classe de **`org.apache.catalina.valves.ValveBase`**.

   ```
   package org.jboss.samplevalves;

   import org.apache.catalina.valves.ValveBase;
   import org.apache.catalina.connector.Request;
   import org.apache.catalina.connector.Response;

   public class restrictedUserAgentsValve extends ValveBase {

   }
   ```

2. **Mettre en place la méthode d'invocation**
   La méthode **`invoke()`** est utilisée lorsque la valve est exécutée dans la pipeline. Les objets de requête et de réponse sont considérés comme des paramètres. Effectuer tout procédé et modification de requête et réponse ici.

```
public void invoke(Request request, Response response)
{

}
```

3. **Invoquer la prochaine étape de pipeline**
   La dernière étape que la méthode d'invocation doit effectuer est d'invoquer l'étape suivante de la pipeline et de transmettre les objets de requête et de réponse modifiés, en utilisant la méthode **`getNext().invoke()`**.

```
getNext().invoke(request, response);
```

4. **Option : indiquer les paramètres**
   Si la valve doit être configurable, activer cette option en ajoutant un paramètre. Pour ce faire, il convient d'ajouter une variable d'instance et une méthode setter pour chaque paramètre.

```
private String restrictedUserAgents = null;

public void setRestricteduseragents(String mystring)
{
   this.restrictedUserAgents = mystring;
}
```

Exemple 4.2. Échantillon de valve personnalisée

```
package org.jboss.samplevalves;

import java.io.IOException;
import java.util.regex.Pattern;

import javax.servlet.ServletException;
import org.apache.catalina.valves.ValveBase;
import org.apache.catalina.connector.Request;
import org.apache.catalina.connector.Response;

public class restrictedUserAgentsValve extends ValveBase
{
    private String restrictedUserAgents = null;

    public void setRestricteduseragents(String mystring)
    {
        this.restrictedUserAgents = mystring;
    }

    public void invoke(Request request, Response response) throws
IOException, ServletException
    {
      String agent = request.getHeader("User-Agent");
      System.out.println("user-agent: " + agent + " : " +
restrictedUserAgents);
      if (Pattern.matches(restrictedUserAgents, agent))
      {
         System.out.println("user-agent: " + agent + " matches: " +
restrictedUserAgents);
```

```
            response.addHeader("Connection", "close");
        }
        getNext().invoke(request, response);
    }
}
```

Report a bug

CHAPITRE 5. LA JOURNALISATION POUR LES DÉVELOPPEURS

5.1. INTRODUCTION

5.1.1. Journalisation

La journalisation ou logging consiste à l'enregistrement d'une série de messages d'une application dans un fichier-journal (ou log) des activités de l'application.

Les messages de journalisation fournissent des informations importantes pour les développeurs lors du débogage d'une application et pour les administrateurs système quand au maintien des applications de production.

La plupart des frameworks de journalisation de Java incluent également des informations comme l'heure et l'origine du message.

Report a bug

5.1.2. Frameworks de journalisations d'applications pris en charge par JBoss LogManager

JBoss LogManager prend en charge les frameworks de journalisation suivants :

- JBoss Logging - inclus avec JBoss EAP 6
- Apache Commons Logging - http://commons.apache.org/logging/
- Simple Logging Facade dans Java (SLF4J) - http://www.slf4j.org/
- Apache log4j - http://logging.apache.org/log4j/1.2/
- Java SE Logging (java.util.logging) - http://download.oracle.com/javase/6/docs/api/java/util/logging/package-summary.html

Report a bug

5.1.3. Niveaux de journalisation

Les niveaux de journalisation sont des ensembles ordonnés de valeurs énumérées qui indiquent la nature et la sévérité d'un message de journalisation. Le niveau d'un message de journalisation donné est indiqué par le développeur par des méthodes qui conviennent dans un framework de journalisation particulier pour envoyer le message.

JBoss EAP 6 accepte tous les niveaux de journalisation utilisés par les frameworks de journalisation de l'application prise en charge. Les six niveaux de journalisation les plus utilisés sont (dans l'ordre croissant) : **TRACE**, **DEBOG**, **INFO**, **ATTENTION**, **ERREUR** et **FATAL**.

Les niveaux de journalisation sont utilisés par des catégories et gestionnaires de journalisation pour limiter les messages dont ils sont responsables. Chaque niveau de journalisation possède une valeur numérique qui indique son ordre par rapport à d'autres niveaux de journalisation. Les catégories et gestionnaires de journalisation correspondent à un certain niveau de journalisation, et ils traitent les

messages de journalisation du même niveau ou d'un niveau supérieur uniquement. Par exemple, un gestionnaire de journalisation du niveau **ATTENTION** enregistrera uniquement les messages des niveaux **ATTENTION**, **ERREUR** et **FATAL**.

Report a bug

5.1.4. Niveaux de journalisation pris en charge

Tableau 5.1. Niveaux de journalisation pris en charge

Niveau de journalisation	Valeur	Description
FINESSE MAX	300	-
PLUS FIN	400	-
TRACE	400	Utilisé pour des messages qui fournissent des informations détaillées sur l'état d'exécution d'une application. Les messages de journalisation **TRACE** sont habituellement capturés lors du débogage d'une application uniquement.
DEBUG	500	Utilisé pour des messages qui indiquent des demandes individuelles de progrès ou des activités d'une application. Les messages de journalisation **DEBUG** ne sont habituellement capturés que lors du débogage d'une application.
FINESSE	500	-
CONFIG	700	-
INFO	800	Utilisé pour des messages qui indiquent la progression globale de l'application. Souvent utilisé pour le démarrage de l'application, la fermeture et autres événements majeurs de cycle de vie.
AVERTISSEMENT	900	Utilisé pour indiquer une situation qui n'est pas en erreur, mais n'est pas considérée comme idéale. Peut indiquer des circonstances qui peuvent entraîner des erreurs dans le futur.
ATTENTION	900	-
ERREUR	1000	Utiliser pour indiquer une erreur qui s'est produite et qui puisse empêcher l'activité actuelle ou la demande de se remplir, mais qui n'empêchera pas l'application d'exécuter.
SÉVÈRE	1000	-
FATAL	1100	Utiliser pour indiquer les événements qui pourraient entraîner des défaillances de services critiques ou la fermeture de l'application, ou qui pourraient entraîner la fermeture de la plateforme JBoss EAP 6.

Report a bug

5.1.5. Emplacements de fichiers de journalisation par défaut

Il s'agit des fichiers de journalisation qui ont été créés pour les configurations de journalisation par défaut. La configuration par défaut écrit des fichiers de journalisation du serveur à l'aide de gestionnaires de journaux périodiques.

Tableau 5.2. Fichier de journalisation par défaut d'un serveur autonome

Fichier journal	Description
EAP_HOME/standalone/log/server.log	Le journal du serveur. Contient les messages de journalisation de serveur, dont les messages de démarrage de serveur.

Tableau 5.3. Fichiers de journalisation par défaut d'un domaine géré

Fichier journal	Description
EAP_HOME/domain/log/host-controller.log	Journal d'amorçage du contrôleur hôte. Contient les messages de journalisation liés au démarrage du contrôleur hôte.
EAP_HOME/domain/log/process-controller.log	Journal d'amorçage du contrôleur de processus. Contient les messages de journalisation liés au démarrage du contrôleur de processus.
EAP_HOME/domain/servers/*SERVERNAME*/log/server.log	Le journal du serveur pour le serveur nommé. Contient les messages de journalisation de ce serveur, dont les messages de démarrage de serveur.

Report a bug

5.2. JOURNALISATION DANS LE JBOSS LOGGING FRAMEWORK

5.2.1. JBoss Logging

JBoss Logging est le framework de journalisation d'applications inclus avec JBoss EAP 6

JBoss Logging procure un moyen facile d'ajouter une journalisation à une application. Vous ajoutez du code à votre application qui utilise le framework pour envoyer des messages de journal dans un format défini. Lorsque l'application est déployée sur un serveur d'applications, ces messages peuvent être capturés par le serveur et affichées ou écrits dans les fichiers selon la configuration du serveur.

Report a bug

5.2.2. Fonctionnalités de JBoss Logging

- Fournit un enregistreur d'événements de saisie ("typed") facile d'utilisation.
- Support total pour l'internationalisation et la localisation. Les traducteurs travaillent sur des lots de messages dans des fichiers de propriétés, tandis que les développeurs peuvent travailler sur des interfaces et annotations.

- Outils « buid-time » pour générer les enregistreurs d'événements en saisie pour la production, et la génération runtime d'enregistreurs d'événements pour le développement.

Report a bug

5.2.3. Ajouter une journalisation à une application par JBoss Logging

Pour journaliser des messages à partir de votre application, créer un objet de créateur de journal (**`org.jboss.logging.Logger`**) et utiliser la méthode appropriée de cet objet. Cette tâche décrit les étapes nécessaires pour ajouter un support pour ceci à votre application.

Prérequis

Vous devez remplir les conditions suivantes avant de continuer cette tâche :

- Si vous utilisez Maven en tant que système de build, il convient que le projet soit déjà configuré pour inclure le référentiel JBoss Maven. Voir Section 2.3.2, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven »
- Les fichiers JAR de JBoss Logging doivent se trouver dans le chemin d'accès de génération de vos applications. La façon dont vous procédez dépendra de votre décision de générer votre application avec JBoss Developer Studio ou avec Maven.
  - Quand vous générez avec JBoss Developer Studio vous pouvez procéder en sélectionnant Project -> Properties à partir du menu JBoss Developer Studio, en sélectionnant Targeted Runtimes et en veillant bien à vérifier le temps d'exécution de JBoss EAP 6.
  - Quand vous générez avec Maven, vous pouvez procéder en ajoutant la configuration de dépendance suivante au fichier **`pom.xml`** de votre projet.

    ```
    <dependency>
       <groupId>org.jboss.logging</groupId>
       <artifactId>jboss-logging</artifactId>
       <version>3.1.2.GA-redhat-1</version>
       <scope>provided</scope>
    </dependency>
    ```

    Vous n'avez pas besoin d'inclure les JAR de l'application générée car JBoss EAP 6 les fournit aux applications qui sont déployées.

Une fois que votre projet sera correctement installé, vous devrez suivre les étapes suivantes pour chaque classe à laquelle vous souhaitez ajouter une journalisation.

1. **Ajouter Imports**
   Ajouter les déclarations d'importation des espace-noms de classe JBoss Logging que vous allez utiliser. Vous devrez importer au minimum **`import org.jboss.logging.Logger`**.

   ```
   import org.jboss.logging.Logger;
   ```

2. **Créer un objet Logger**
   Créer une instance de **`org.jboss.logging.Logger`** et l'initialiser en utilisant la méthode statique **`Logger.getLogger(Class)`**. Red Hat vous recommande de la créer en tant que variable à instance unique pour chaque classe.

```
private static final Logger LOGGER =
Logger.getLogger(HelloWorld.class);
```

3. **Ajouter les messages de journalisation**
   Ajouter des appels aux méthodes de l'objet **Logger** à votre code, là où vous souhaitez qu'il envoie des messages. L'objet **Logger** comprend un certain nombre de méthodes contenant des paramètres différents suivant les types de messages. Les plus faciles à utiliser sont les suivants :

debog(message objet)
info(message objet)
erreur(message objet)
trace(message objet)
fatal(message objet)

   Ces méthodes envoient un message de journalisation avec le niveau de journalisation correspondant et le paramètre **message** comme string.

```
LOGGER.error("Configuration file not found.");
```

   Pour obtenir une liste complète des méthodes JBoss Logging, consulter le package **org.jboss.logging** dans JBoss EAP 6 API Documentation.

Exemple 5.1. Utilisation de JBoss Logging quand on ouvre un fichier de propriétés

Cet exemple vous montre un exemple de code de classe qui charge une configuration personnalisée pour une application à partir d'un fichier de propriétés. Si le fichier spécifié n'est pas trouvé, un message de journalisation sera enregistré au niveau ERROR.

```
import org.jboss.logging.Logger;
public class LocalSystemConfig
{
   private static final Logger LOGGER =
Logger.getLogger(LocalSystemConfig.class);

   public Properties openCustomProperties(String configname) throws
CustomConfigFileNotFoundException
   {
      Properties props = new Properties();
      try
      {
         LOGGER.info("Loading custom configuration from "+configname);
         props.load(new FileInputStream(configname));
      }
      catch(IOException e) //catch exception in case properties file
does not exist
      {
         LOGGER.error("Custom configuration file ("+configname+") not
```

```
found. Using defaults.");
            throw new CustomConfigFileNotFoundException(configname);
        }

        return props;
    }
```

Report a bug

5.3. PROFILS DE JOURNALISATION

5.3.1. Profils de journalisation

IMPORTANT

Les profils de journalisation ne sont disponibles qu'en version 6.1.0 ou supérieure

Les profils de journalisation sont des ensembles de configuration de journalisation indépendants qui peuvent être assignés à des applications déployées. Un profil de journalisation peut définir les handlers, les catégories et un root logger à la manière du sous-système de journalisation standard, mais ne peut pas recommander la configuration à d'autres profils ou au sous-système de journalisation principal. La conception des profils de journalisation émule le sous-système de journalisation au niveau de l'aisance de configuration.

Les profils de journalisation permettent aux administrateurs de créer une configuration de journalisation spécifique à une ou à plusieurs applications sans affecter une autre configuration de journalisation. Comme chaque profil est défini dans une configuration serveur, cela implique que la configuration de journalisation peut être modifiée sans exiger que les applications affectées ne soient redéployées.

Chaque profil de journalisation peut avoir la configuration suivante :

- Un nom unique. Ceci est requis.
- N'importe quel nombre de Log Handlers.
- N'importe quelle catégorie log.
- Un root logger maximum.

Une application peut spécifier un profil de journalisation à utiliser dans son fichier MANIFEST.MF, en utilisant l'attribut Logging-profile.

IMPORTANT

Les profils de journalisation ne peuvent pas être configurés par la console de gestion.

Report a bug

5.3.2. Spécifier un profil de journalisation dans une application

Une application spécifie le profil de journalisation à utiliser dans son fichier **MANIFEST.MF**.

Pré-requis :

1. Vous devez connaître le nom du profil de journalisation qui a été défini sur le serveur pour cette application. Demandez à votre administrateur de systèmes le nom du profil à utiliser.

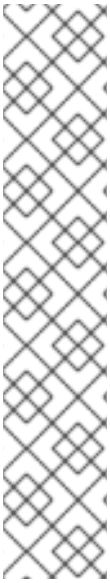
Procédure 5.1. Ajouter une configuration de profil de journalisation à une application

- **Modifier MANIFEST.MF**
  Si votre application ne possède pas de fichier **MANIFEST.MF** : le créer avec le contenu suivant, en remplaçant *NAME* par le nom de profil qui convient.

  ```
  Manifest-Version: 1.0
        Logging-Profile: NAME
  ```

  Si votre application contient déjà un fichier **MANIFEST.MF** : ajouter la ligne suivante, en remplaçant *NAME* par le nom du profil qui convient.

  ```
  Logging-Profile: NAME
  ```



NOTE

Si vous utilisez Maven et **maven-war-plugin**, vous pourrez mettre votre fichier MANIFEST.MF dans **src/main/resources/META-INF/** et ajouter la configuration suivante à votre fichier **pom.xml**.

```
<plugin>
      <artifactId>maven-war-plugin</artifactId>
      <configuration>
        <archive>
          <manifestFile>src/main/resources/META-
INF/MANIFEST.MF</manifestFile>
        </archive>
      </configuration>
   </plugin>
```

Quand l'application sera déployée, elle utilisera la configuration qui se trouve dans le profil de journalisation spécifié pour ses messages de journalisation.

Report a bug

CHAPITRE 6. INTERNATIONALISATION ET LOCALISATION

6.1. INTRODUCTION

6.1.1. Internationalisation

Le mot internationalisation fait référence au processus de design des logiciels, pour qu'ils puissent être adaptés aux différentes langues et régions sans changements d'ingénierie.

Report a bug

6.1.2. Localisation

Le mot localisation fait référence au processus d'adaptation des logiciels internationaux à une région spécifique ou à une langue spécifique, impliquant le rajout de composants particuliers à la locale et à la traduction de textes.

Report a bug

6.2. OUTILS JBOSS LOGGING

6.2.1. Aperçu

6.2.1.1. JBoss Logging Tools - Internationalisation et Localisation

JBoss Logging Tools est une API Java qui apporte un soutien pour l'internationalisation et la localisation des messages de journalisation, des messages d'exception et chaînes génériques. En plus de fournir un mécanisme de traduction, les outils JBoss Logging fournissent également un support d'identificateur unique pour chaque message de journalisation.

Les messages et les exceptions internationalisés sont créés en tant que définitions de méthode à l'intérieur des interfaces annotées à l'aide des annotations `org.jboss.logging`. Il n'est pas nécessaire d'implémenter les interfaces, JBoss Logging Tools le fait au moment de la compilation. Une fois définies, vous pouvez utiliser ces méthodes pour enregistrer des messages ou d'obtenir des objets d'exception dans votre code.

Les interfaces d'exception et de journalisation internationalisées créées parJBoss Logging Tools peuvent être localisées en créant un fichier de propriétés pour chaque lot contenant les traductions pour un langage et une région spécifiques. JBoss Logging Tools peut générer des fichiers de propriétés de modèle pour chaque lot qui peut ensuite être édité par un traducteur.

JBoss Logging Tools crée une implémentation de chaque lot pour chaque fichier de propriétés de traductions correspondantes dans votre projet. Tous que vous devez faire est d'utiliser les méthodes définies dans les lots et JBoss Logging Tools veillera à ce que l'implémentation qui convient soit invoquée pour vos paramètres régionaux en cours.

Les ids de messages et des codes de projets sont des identificateurs uniques qui sont ajoutés à chaque message du journal. Ces identificateurs uniques peuvent servir de documentation pour faciliter la recherche d'informations sur les messages de journalisation. Avec une documentation suffisante, la signification d'un message de journalisation peut être déterminée par les identificateurs, quelle que soit la langue dans laquelle le message a été rédigé.

Report a bug

6.2.1.2. JBoss Logging Tools Quickstart

JBoss Logging Tools Quickstart, **`logging-tools`**, contient un simple projet Maven qui démontre les fonctionnalités de JBoss Logging Tools. A été utilisé extensivement dans cette documentation pour les exemples de code.

Voir ce Quickstart pour obtenir une démonstration complète de toutes les fonctionnalités décrites dans cette documentation.

Report a bug

6.2.1.3. Message Logger

Un Message Logger est une interface utilisée pour définir les messages de journalisation internationalisés. Une interface de Message Logger est annotée par **`@org.jboss.logging.MessageLogger`**.

Report a bug

6.2.1.4. Lot de messages

Un lot de messages est une interface qui peut être utilisée pour définir des messages génériques à traduire et des objets d'Exception avec des messages internationalisés. Un lot de messages n'est pas utilisé pour créer des messages de journalisation.

Une interface de lot de messages est annoté par **`@org.jboss.logging.MessageBundle`**.

Report a bug

6.2.1.5. Messages de journalisation internationalisés

Les messages de journalisation internationalisés sont des messages de journalisation créés en définissant une méthode dans un Message Logger. La méthode doit contenir les annotations **`@LogMessage`** et **`@Message`** et spécifier le message de journalisation en utilisant l'attribut de la valeur de **`@Message`**. Les messages de journalisation internationalisés sont localisés en fournissant des traductions dans un fichier de propriétés.

JBoss Logging Tools génère les classes de journalisation requises pour chaque traduction au moment de la compilation et invoque les méthodes qui conviennent à la locale en cours d'exécution.

Report a bug

6.2.1.6. Exceptions internationalisées

Une exception internationalisée est un objet d'exception retourné par une méthode définie dans un lot de messages. Les méthodes de lots de messages qui retournent des objets d'Exception Java peuvent être annotés pour définir un message d'exception par défaut. Le message par défaut est remplacé par une traduction, si un elle se trouve dans un fichier de propriétés correspondant pour le paramètres régionaux en cours. Les exceptions internationalisées peuvent aussi avoir des codes de projet et des ID de messages assignés.

Report a bug

6.2.1.7. Messages internationalisés

Un message internationalisé est un string retourné par une méthode définie dans un lot de messages. Les méthodes de lots de messages qui retournent des objets String Java peuvent être annotées afin de définir le contenu par défaut de ce string, connu comme message. Le message par défaut est remplacé par une traduction, si une traduction se trouve dans un fichier de propriétés correspondant pour les paramètres régionaux en cours.

Report a bug

6.2.1.8. Fichiers de propriétés de traduction

Les fichiers de propriétés de traductions sont des fichiers de propriétés Java qui contiennent les traductions des messages à partir d'une interface pour une variante, locale et pays. Les fichiers de propriétés de traductions sont utilisés par JBoss Logging Tools pour créer des classes qui renvoient les messages.

Report a bug

6.2.1.9. Codes de projets de JBoss Logging Tools

Les codes de projets sont des chaînes de caractères qui identifient des groupes de messages. Ils se trouvent au début de chaque message de journalisation, et contiennent l'ID du message. Les codes de projets sont définis dans l'attribut **`projectCode`** de l'annotation **`@MessageLogger`**.

Report a bug

6.2.1.10. Ids de messages de JBoss Logging Tools

Les Ids de messages sont des nombres, qui lorsque combinés avec un code de projet, identifient de façon unique un message de journalisation. Les Ids de messages sont affichées au début de chaque message du journal, ajoutés au code de projet du message. Les Ids de messages sont définis par l'attribut **`id`** de l'annotation **`@Message`**.

Report a bug

6.2.2. Création de loggers, de messages ou d'exceptions internationalisés

6.2.2.1. Créer des messages log internationalisés

Cette tâche vous montre comment utiliser JBoss Logging Tools pour créer des messages de journalisation internationalisés en créant des interfaces MessageLogger. Elle ne traite pas de toutes les caractéristiques optionnelles ou de la localisation des messages de journalisation.

Voir le guide de démarrage **`logging-tools`** pour trouver un exemple complet.

Prérequis :

1. Vous devez déjà posséder un projet Maven en cours. Voir Section 6.2.6.1, « Configuration Maven JBoss Logging Tools ».
2. Le projet doit avoir la configuration Maven qui convient pour JBoss Logging Tools.

Procédure 6.1. Créer un lot de messages log internationalisés

1. **Créer une interface de Message Logger**

Ajouter une interface Java à votre projet pour contenir les définitions de messages log. Définir l'interface de façon descriptive pour les messages log qui seront définis à l'intérieur.

L'interface de messages log ont les prérequis suivants :

- Doit être annotée par **`@org.jboss.logging.MessageLogger`**.
- Doit étendre **`org.jboss.logging.BasicLogger`**.
- L'interface doit définir un champ qui est un Logger typed quiimpléemnte cette interface. Procédez par la méthode **`getMessageLogger()`** de **`org.jboss.logging.Logger`**.

```
package com.company.accounts.loggers;

import org.jboss.logging.BasicLogger;
import org.jboss.logging.Logger;
import org.jboss.logging.MessageLogger;

@MessageLogger(projectCode="")
interface AccountsLogger extends BasicLogger
{
   AccountsLogger LOGGER = Logger.getMessageLogger(
         AccountsLogger.class,
         AccountsLogger.class.getPackage().getName() );
}
```

2. **Ajouter les définitions de méthode**
   Ajouter une définition de méthode à l'interface de chaque message log. Nommez chaque méthode descriptivement par rapport au message log qu'elle représente.

   Chaque méthode a les prérequis suivants :

   - La méthode doit renvoyer **`void`**.
   - La méthode doit être annotée par **`@org.jboss.logging.LogMessage`**.
   - La méthode doit être annotée par **`@org.jboss.logging.Message`**.
   - L'attribut de **`@org.jboss.logging.Message`** contient le message log par défaut. Il s'agit du message qui est utilisé s'il n'y a pas de traduction.

   ```
   @LogMessage
   @Message(value = "Customer query failed, Database not available.")
   void customerQueryFailDBClosed();
   ```

   Le niveau de journalisation par défaut est **`INFO`**.

3. **Invoquer les méthodes**
   Ajouter les appels aux méthodes d'interface dans votre code là où les messages doivent être journalisés. Il n'est pas utile de créer des implémentations des interfaces, le processeur d'annotations le fait pour vous quand le projet est compilé.

   ```
   AccountsLogger.LOGGER.customerQueryFailDBClosed();
   ```

Les loggers personnalisés sont des sous-classes de BasicLogger, donc les méthodes de journalisation de **`BasicLogger`** (**`debug()`**, **`error()`** etc) peuvent également être utilisées. Il n'est pas utile de créer d'autres loggers pour enregistrer les messages non internationalisés.

```
AccountsLogger.LOGGER.error("Invalid query syntax.");
```

RÉSULTAT: le projet supporte maintenant un ou plusieurs loggers internationalisés qui peuvent maintenant être localisés.

Report a bug

6.2.2.2. Créer et utiliser des messages internationalisés

Cette tâche vous montre comment créer des messages internationalisés et comment les utiliser. Cette tâche ne couvre pas toutes les fonctionnalités en option ou la localisation de ces messages de journalisation.

Voir le guide de démarrage **`logging-tools`** pour trouver un exemple complet.

Prérequis

1. Vous avez un projet Maven utilisant le référentiel JBoss EAP 6. Voir Section 2.3.2, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven ».
2. La configuration Maven requise pour JBoss Logging Tools a été ajoutée. Voir Section 6.2.6.1, « Configuration Maven JBoss Logging Tools ».

Procédure 6.2. Créer et utiliser des messages internationalisés

1. **Créer une interface pour les exceptions.**
   JBoss Logging Tools définit les messages internationalisés dans les interfaces. Nommer chaque interface de manière descriptive pour les messages qui seront définis à l'intérieur.

   L'interface possède les prérequis suivants :

   - Elle doit être déclarée publique
   - Elle doit être annotée par **`@org.jboss.logging.MessageBundle`**.
   - L'interface doit définir un champ qui corresponde à un lot de messages du même type que l'interface.

   ```
   @MessageBundle(projectCode="")
   public interface GreetingMessageBundle
   {
      GreetingMessageBundle MESSAGES =
   Messages.getBundle(GreetingMessageBundle.class);
   }
   ```

2. **Ajouter les définitions de méthode**
   Ajouter une définition de méthode dans l'interface de chaque message.

   Chaque méthode a les prérequis suivants :

- Elle doit renvoyer un objet de type **`String`**.
- La méthode doit être annotée par **`@org.jboss.logging.Message`**.
- L'attribut**`@org.jboss.logging.Message`** doit être défini à la valeur par défaut du message. Il s'agit du message qui est utilisé si aucune traduction n'est disponible.

```
@Message(value = "Hello world.")
   String helloworldString();
```

3. **Méthodes d'invocation**
   Invoquer les méthodes d'interface dans votre application quand vous aurez besoin d'obtenir le message.

```
System.console.out.println(helloworldString());
```

RÉSULTAT : le projet prend maintenant en charge des chaînes de messages internationalisés qui peuvent être localisés.

Report a bug

6.2.2.3. Créer des exceptions personnalisées

Cette tâche vous montre comment créer des exceptions personnalisées et comment les utiliser. Cette tâche ne couvre pas toutes les fonctionnalités en option ou le processus de localisation de ces exceptions.

Voir le guide de démarrage **`logging-tools`** pour trouver un exemple complet.

Pour cette tâche, on assume que vous possédez déjà un projet informatique dans le JBoss Developer Studio ou Maven sur lequel vous souhaitez ajouter des exceptions internationalisées.

Procédure 6.3. Créer et utiliser des exceptions internationalisées

1. **Ajouter une configuration JBoss Logging Tools**
   Ajouter la configuration de projet qui convient pour prendre en charge JBoss Logging Tools. Voir Section 6.2.6.1, « Configuration Maven JBoss Logging Tools »
2. **Créer une interface pour les exceptions.**
   JBoss Logging Tools définit les exceptions internationalisées dans les interfaces. Nommer chaque interface de façon descriptive pour les exceptions qui seront décrites à l'intérieur.

   L'interface possède les prérequis suivants :

   - Elle doit être déclarée **`public`**.
   - Elle doit être annotée par **`@org.jboss.logging.MessageBundle`**.
   - L'interface doit définir un champ qui correspond à un lot de messages du même type que l'interface.

```
@MessageBundle(projectCode="")
public interface ExceptionBundle
{
```

```
   ExceptionBundle EXCEPTIONS =
Messages.getBundle(ExceptionBundle.class);
}
```

3. **Ajouter les définitions de méthode**
   Ajouter un définition de méthode à l'interface pour chaque exception. Nommez chaque méthode de façon descriptive pour chaque exception qu'elle représente.

   Chaque méthode a les prérequis suivants :

   - Elle doit renvoyer un objet du type **`Exception`** ou bien un sous-type de **`Exception`**.
   - La méthode doit être annotée par **`@org.jboss.logging.Message`**.
   - L'attribut de **`@org.jboss.logging.Message`** doit être défini à la valeur du message d'exception par défaut. Il s'agit du message qui est utilisé s'il n'y a pas de traduction.
   - Si l'exception est retournée à un constructeur qui nécessite des paramètres en plus d'une chaîne de message, alors ces paramètres doivent être fournis dans la définition de méthode à l'aide de l'annotation **`@param`**. Les paramètres doivent être du même type et même ordre que le constructeur.

```
@Message(value = "The config file could not be opened.")
IOException configFileAccessError();

@Message(id = 13230, value = "Date string '%s' was invalid.")
ParseException dateWasInvalid(String dateString, @Param int
errorOffset);
```

4. **Méthodes d'invocation**
   Invoquer les méthodes d'interface de votre code quand vous devrez obtenir une des exceptions. Les méthodes ne lancent pas d'exceptions, elles envoient l'objet d'exception que vous pourrez alors envoyer vous-même.

```
try
{
   propsInFile=new File(configname);
   props.load(new FileInputStream(propsInFile));
}
catch(IOException ioex) //in case props file does not exist
{
   throw ExceptionBundle.EXCEPTIONS.configFileAccessError();
}
```

RÉSULTAT : le projet prend maintenant en charge les exceptions internationalisées qui peuvent être localisées.

Report a bug

6.2.3. Localisation de loggers, messages ou exceptions internationalisés

6.2.3.1. Générer des nouveaux fichiers de propriétés de traduction avec Maven

Des projets qui sont construits avec Maven peuvent générer des fichiers de propriétés de traduction vides pour chaque Message Logger et Lots de messages qu'ils contiennent. Ensuite, ces fichiers peuvent être utilisés comme nouveaux fichiers de propriétés de traduction.

La procédure suivante montre comment configurer un projet Maven pour créer des nouveaux fichiers de propriétés de traduction.

Voir le guide de démarrage **`logging-tools`** pour trouver un exemple complet.

Prérequis :

1. Vous devez déjà posséder un projet Maven en cours.
2. Le projet devra avoir été configuré pour JBoss Logging Tools.
3. Le projet doit contenir une ou plusieurs interfaces qui définissent des exceptions ou des messages de journalisation internationalisés

Procédure 6.4. Générer des nouveaux fichiers de propriétés de traduction avec Maven

1. **Ajouter la configuration Maven**
   Ajouter l'argument de compilateur **`-AgenereatedTranslationFilePath`** à la configuration du plug-in du compilateur Maven et lui assigner le chemin d'accès où les nouveaux fichiers devront être créés.

```
<plugin>
   <groupId>org.apache.maven.plugins</groupId>
   <artifactId>maven-compiler-plugin</artifactId>
   <version>2.3.2</version>
   <configuration>
      <source>1.6</source>
      <target>1.6</target>
      <compilerArgument>
      -
AgeneratedTranslationFilesPath=${project.basedir}/target/generated-
translation-files
      </compilerArgument>
      <showDeprecation>true</showDeprecation>
   </configuration>
</plugin>
```

   La configuration ci-dessus va créer des nouveaux fichiers dans le répertoire **`target/generated-translation-files`** de votre projet Maven.

2. **Créer votre projet**
   Créer votre projet en utilisant Maven.

```
[Localhost]$ mvn compile
```

Un fichier de propriétés est créé par interface annotée par **`@MessageBundle`** ou **`@MessageLogger`**. Les nouveaux fichiers sont créés dans un sous-répertoire qui correspond au package Java dans lequel chaque interface est déclarée.

Chaque nouveau fichier est nommé par la syntaxe suivante, avec **`InterfaceName`** comme nom d'interface pour laquelle ce fichier a été créé : ***`InterfaceName`*`.i18n_locale_COUNTRY_VARIANT.properties`**.

Ces fichiers peuvent alors être copiés dans votre projet pour servir de base à des nouvelles traductions.

Report a bug

6.2.3.2. Traduire un logger, une exception ou un message internationalisé

Les messages d'exception ou de journalisation définis dans les interfaces qui utilisent JBoss Logging Tools peuvent avoir des traductions dans les fichiers de propriétés.

La procédure suivante vous montre comment créer et utiliser un fichier de propriétés de traduction. On assume que vous possédez déjà un projet avec une ou plusieurs interfaces définies pour les exceptions internationalisées ou pour les messages de journalisation.

Voir le guide de démarrage **`logging-tools`** pour trouver un exemple complet.

Prérequis

1. Vous devez déjà posséder un projet Maven en cours
2. Le projet devra avoir été configuré pour JBoss Logging Tools.
3. Le projet devra contenir une ou plusieurs interfaces qui définissent les exceptions ou message log d'internationalisation.
4. Le projet devra être configuré pour générer des fichiers de propriétés modèles.

Procédure 6.5. Traduire un message, une exception ou un message internationalisé

1. **Créer des fichiers de propriétés modèles**
   Exécuter la commande **`mvn compile`** pour créer les modèles de fichiers de propriétés de traduction.
2. **Ajouter le fichier modèle à votre projet.**
   Copier le modèle des interfaces que vous souhaitez traduire depuis le répertoire où elles ont été créées dans le répertoire **`src/main/resources`** de votre projet. Les fichiers de propriétés doivent figurer dans le même package des interfaces qu'ils traduisent.
3. **Renommer le fichier modèle copié**
   Renommer la copie du fichier modèle selon la traduction qu'il contient. Par exemple, **`GreeterLogger.i18n_fr_FR.properties`**.
4. **Traduire le contenu du modèle**
   Modifier le nouveau fichier de propriétés de traduction de manière à contenir la traduction appropriée.

   ```
   # Level: Logger.Level.INFO
   # Message: Hello message sent.
   logHelloMessageSent=Bonjour message envoyé.
   ```

   Répéter les étapes deux, trois et quatre pour chaque traduction de chaque lot exécuté.

RÉSULTAT : le projet contient désormais des traductions pour un ou plusieurs lots de messages ou de loggers. La construction du projet génèrera les classes appropriées aux messages de journalisation avec les traductions fournies. Il n'est pas nécessaire d'invoquer des méthodes explicitement ou de fournir des paramètres pour des langues spécifiques, JBoss Logging Tools choisit automatiquement la bonne classe pour la locale actuelle du serveur d'application.

Le code source des classes générées peuvent être consultées dans **`target/generated-sources/annotations/`**.

Report a bug

6.2.4. Personnalisation des messages de journalisation internationalisés

6.2.4.1. Ajouter les ids de messages et les codes de projets aux messages de journalisation

Cette tâche montre comment ajouter les ids de messages et les codes de projets aux messages de journalisation internationalisés créés en utilisant JBoss Logging Tools. Un message de journalisation doit contenir à la fois un code de projet et un id de message afin qu'ils puissent s'afficher dans le journal. Si un message ne contient pas à la fois un code de projet et un id de message, alors aucun ne s'affichera.

Voir le guide de démarrage **`logging-tools`** pour trouver un exemple complet.

Prérequis

1. Vous devez déjà posséder un projet avec des messages de journalisation internationalisés. Voir Section 6.2.2.1, « Créer des messages log internationalisés ».

2. Vous devrez connaître le code de projet que vous utilisez. Vous pouvez utiliser un code de projet simple, ou en définir un différent pour chaque interface.

Procédure 6.6. Ajouter les ids et les codes de projets aux messages de journalisation

1. **Indiquer le code de projet de l'interface.**
   Indiquer le code du projet par l'attribut projectCode de l'annotation **`@MessageLogger`** qui est attachée à une interface de logger personnalisée. Tous les messages définis dans l'interface utiliseront ce code de projet.

   ```
   @MessageLogger(projectCode="ACCNTS")
   interface AccountsLogger extends BasicLogger
   {

   }
   ```

2. **Indiquer les ids de messages**
   Indiquer un id de message pour chaque message qui utilise un attribut id de l'annotation @Message liée à la méthode qui définit le message.

   ```
   @LogMessage
   @Message(id=43, value = "Customer query failed, Database not
   available.")  void customerQueryFailDBClosed();
   ```

Les messages de journalisation qui ont à la fois un id de message et un code de projet associés ajouteront ces informations au message enregistré.

```
10:55:50,638 INFO  [com.company.accounts.ejb] (MSC service thread 1-4)
ACCNTS000043: Customer query failed, Database not available.
```

Report a bug

6.2.4.2. Indiquer le niveau de journalisation d'un message

Le niveau de journalisation par défaut d'un message défini par une interface par JBoss Logging Tools est **INFO**. Un niveau de journalisation différent peut être indiqué avec l'attribut `level` de l'annotation **@LogMessage** jointe à la méthode de journalisation.

Procédure 6.7. Indiquer le niveau de journalisation d'un message

1. **Indiquer l'attribut du niveau**
   Ajouter l'attribut `level` à l'annotation de **@LogMessage** de la définition de la méthode de message de journalisation.

2. **Allouer un niveau de journalisation**
   Allouer l'attribut `level` à la valeur du niveau de journalisation de ce message. Les valeurs valides de `level` sont les six constantes énumérées définies dans `org.jboss.logging.Logger.Level` : **DEBUG**, **ERROR**, **FATAL**, **INFO**, **TRACE**, et **WARN**.

   ```
   Import org.jboss.logging.Logger.Level;

   @LogMessage(level=Level.ERROR)
   @Message(value = "Customer query failed, Database not available.")
   void customerQueryFailDBClosed();
   ```

Invoquer une méthode de journalisation dans l'échantillon ci-dessus produira un message de journalisation du niveau **ERROR**.

```
10:55:50,638 ERROR  [com.company.app.Main] (MSC service thread 1-4)
 Customer query failed, Database not available.
```

Report a bug

6.2.4.3. Personnaliser les messages de journalisation par des paramètres

Les méthodes d'enregistrement personnalisé peuvent définir les paramètres. Ces paramètres sont utilisés pour passer des informations supplémentaires à afficher dans le message journalisé. L'endroit où les paramètres apparaissent dans le message de journal est spécifié dans le message lui-même à l'aide d'une indexation explicite ou ordinaire.

Procédure 6.8. Personnaliser les messages de journalisation avec les paramètres

1. **Ajouter des paramètres à la définition de la méthode**
   Les paramètres d'un type donné peuvent être ajoutés à la définition de la méthode. Quel que soit le type, la représentation String du paramètre est ce qui est affiché dans le message.

2. **Ajouter les références de paramètre dans le message de journalisation**
   Les références peuvent utiliser des indexations explicites ou ordinaires.

- Pour utiliser des indexes ordinaires, insérer les caractères %s dans la chaîne de message où vous souhaitez voir apparaître chaque paramètre. Le premier %s insèrera le premier paramètre, le deuxième insèrera le deuxième paramètre, et ainsi de suite.
- Pour les indexations explicites, insérer les caractères %{#} dans le message où # correspond au numéro du paramètre que vous souhaitez apercevoir.

IMPORTANT

L'utilisation des indexations explicites permet aux références de paramètres du message d'être dans un ordre différent que celui défini dans la méthode. C'est important pour les messages traduits qui peuvent nécessiter un ordonnancement des paramètres différent.

Le nombre de paramètres doit correspondre au nombre de références aux paramètres dans le message spécifié ou le code ne compilera pas. Un paramètre marqué avec l'annotation @Cause n'est pas inclus dans le nombre de paramètres.

Exemple 6.1. Paramètres de messages qui utilisent des indexations ordinaires.

```
@LogMessage(level=Logger.Level.DEBUG)
@Message(id=2, value="Customer query failed, customerid:%s, user:%s")
void customerLookupFailed(Long customerid, String username);
```

Exemple 6.2. Paramètres de messages qui utilisent des indexations explicites

```
@LogMessage(level=Logger.Level.DEBUG)
@Message(id=2, value="Customer query failed, customerid:%{1}, user:%
{2}")
void customerLookupFailed(Long customerid, String username);
```

Report a bug

6.2.4.4. Indiquer une exception comme cause d'un message de journalisation

JBoss Logging Tools permet à un paramètre d'une méthode de journalisation personnalisée d'être défini comme cause du message. Ce paramètre doit être du type **Throwable** ou d'une de ses sous-classes et doit être marqué par l'annotation **@Cause** . Ce paramètre ne peut pas être référencé dans le message de journal comme les autres paramètres et il s'affiche à la suite du message de journalisation.

La procédure suivante montre comment mettre à jour une méthode de journalisation en utilisant le paramètre @Cause pour indiquer l'exception « causer ». Il est supposé que vous avez déjà créé des messages de journalisation internationalisés auxquels vous souhaitez ajouter cette fonctionnalité.

Procédure 6.9. Indiquer une exception comme cause d'un message de journalisation

1. **Ajouter le paramètre**
   Ajouter un paramètre **Throwable** ou une sous-classe à la méthode.

```
@Message(id=404, value="Loading configuration failed. Config
file:%s")
void loadConfigFailed(Exception ex, File file);
```

2. **Ajouter l'annotation**
   Ajouter l'annotation **@Cause** au paramètre.

```
import org.jboss.logging.Cause

@Message(value = "Loading configuration failed. Config file: %s")
void loadConfigFailed(@Cause Exception ex, File file);
```

3. **Invoquer la méthode**
   Quand la méthode est invoquée dans votre code, un objet du type qui convient devra être passé et sera affiché à la suite du message de journalisation.

```
try
{
   confFile=new File(filename);
   props.load(new FileInputStream(confFile));
}
catch(Exception ex) //in case properties file cannot be read
{
     ConfigLogger.LOGGER.loadConfigFailed(ex, filename);
}
```

   Vous trouverez ci-dessous la sortie des extraits de code ci-dessus, si le code à lancé une exception de type **`FileNotFoundException`**.

```
10:50:14,675 INFO [com.company.app.Main] (MSC service thread 1-3)
Loading configuration failed. Config file: customised.properties
java.io.FileNotFoundException: customised.properties (No such file
or directory)
   at java.io.FileInputStream.open(Native Method)
   at java.io.FileInputStream.<init>(FileInputStream.java:120)
   at com.company.app.demo.Main.openCustomProperties(Main.java:70)
   at com.company.app.Main.go(Main.java:53)
   at com.company.app.Main.main(Main.java:43)
```

Report a bug

6.2.5. Personnalisation des exceptions internationalisées

6.2.5.1. Ajouter les ids et les codes de projets aux messages d'exceptions

La procédure suivante montre les étapes requises pour ajouter des ID de message et des codes de projets aux messages d'exception internationalisés créés en utilisant les JBoss Logging Tools.

Les ID de message et les codes de projet sont des identificateurs uniques qui sont ajoutés à chaque message affiché par les exceptions internationalisées. Ces codes d'identification permettent de créer une référence pour tous les messages d'exception d'une application pour qu'une personne puisse

rechercher le sens d'un message d'exception écrit dans une langue qu'elle ne comprent pas.

Prérequis

1. Vous devrez déjà avoir un projet avec des exceptions internationalisées. Voir Section 6.2.2.3, « Créer des exceptions personnalisées ».

2. Vous devrez connaître le code de projet que vous utilisez. Vous pouvez utiliser un code de projet simple, ou en définir un différent pour chaque interface.

Procédure 6.10. Ajouter les ids et les codes de projets aux messages d'exceptions

1. **Indiquer un code de projet**
   Indiquer le code de projet en utilisant l'attribut **`projectCode`** de l'annotation **`@MessageBundle`** attachée à une interface de lot d'exceptions. Tous les messages qui sont définis dans l'interface utiliseront ce code de projet.

   ```
   @MessageBundle(projectCode="ACCTS")
   interface ExceptionBundle
   {
      ExceptionBundle EXCEPTIONS =
   Messages.getBundle(ExceptionBundle.class);
   }
   ```

2. **Indiquer les ID de messages**
   Indiquer l'id de message pour chaque exception en utilisant l'attribut **`id`** de l'annotation **`@Message`** associée à la méthode qui définit l'exception.

   ```
   @Message(id=143, value = "The config file could not be opened.")
   IOException configFileAccessError();
   ```

IMPORTANT

Un message qui comprend à la fois un code de projet et un ID de message les affiche à la suite du message. Si un message ne les possède pas, ils ne seront pas affichés.

Exemple 6.3. Créer des exceptions internationalisées

Cette interface de lot d'exceptions possède le code de projet d'ACCTS, avec une simple méthode d'exception ayant comme Id 143.

```
@MessageBundle(projectCode="ACCTS")
interface ExceptionBundle
{
    ExceptionBundle EXCEPTIONS =
Messages.getBundle(ExceptionBundle.class);

    @Message(id=143, value = "The config file could not be opened.")
    IOException configFileAccessError();
}
```

L'objet d'exception peut être obtenu et lancé grâce au code suivant.

```
throw ExceptionBundle.EXCEPTIONS.configFileAccessError();
```

Cela aurait pour effet d'afficher un message d'exception qui ressemble à ce qui suit :

```
Exception in thread "main" java.io.IOException: ACCTS000143: The config
file could not be opened.
at com.company.accounts.Main.openCustomProperties(Main.java:78)
at com.company.accounts.Main.go(Main.java:53)
at com.company.accounts.Main.main(Main.java:43)
```

Report a bug

6.2.5.2. Personnaliser les messages d'exception avec des paramètres

Les méthodes de lots d'exceptions qui définissent des exceptions peuvent définir les paramètres. Ces paramètres sont utilisés pour passer des informations supplémentaires à afficher dans le message d'exception. L'endroit où les paramètres apparaissent dans le message d'exception est spécifié dans le message lui-même à l'aide d'une indexation explicite ou ordinaire.

La procédure suivante vous montre les étapes requises pour utiliser les paramètres de méthodes pour personnaliser des exceptions de méthodes.

Procédure 6.11. Personnaliser les messages d'exception avec les paramètres

1. **Ajouter des paramètres à la définition de la méthode**
   Les paramètres d'un type donné peuvent être ajoutés à la définition de la méthode. Quel que soit le type, la représentation `String` du paramètre est ce qui est affiché dans le message.

2. **Ajouter les références de paramètre au message d'exception**
   Les références peuvent utiliser des indexations explicites ou ordinaires.

   - Pour utiliser des indexations ordinaires, insérer les caractères **%s** dans la chaîne de message où vous souhaitez voir apparaître chaque paramètre. Le premier **%s** insèrera le premier paramètre, le deuxième insèrera le deuxième paramètre, et ainsi de suite.

   - Pour les indexations explicites, insérer les caractères **%{#}** dans le message où *#* correspond au numéro du paramètres que vous souhaitez apercevoir.

   L'utilisation des indexations explicites permet aux références de paramètre du message d'être dans un ordre différent que celui défini dans la méthode. C'est important pour les messages traduits qui peuvent nécessiter un ordonnancement des paramètres différent.

IMPORTANT

Le nombre de paramètres doit correspondre au nombre de références aux paramètres dans le message spécifié ou le code ne compilera pas. Un paramètre marqué avec l'annotation **@Cause** n'est pas inclus dans le nombre de paramètres.

Exemple 6.4. Utilisation des indexations ordinaires

```
@Message(id=143, value = "The config file %s could not be opened.")
IOException configFileAccessError(File config);
```

Exemple 6.5. Utilisation des indexations explicites

```
@Message(id=143, value = "The config file %{1} could not be opened.")
IOException configFileAccessError(File config);
```

Report a bug

6.2.5.3. Indiquer une exception comme cause d'une autre exception

Les exceptions renvoyées par les méthodes de lots d'exceptions peuvent avoir une autre exception spécifiée comme cause sous-jacente. Cela se fait par l'ajout d'un paramètre à la méthode et en annotant le paramètre @Cause. Ce paramètre est utilisé pour passer l'exception de « cause ». Ce paramètre ne peut pas être référencé dans le message d'exception.

La procédure suivante montre comment mettre à jour une méthode de lot d'exception en utilisant le paramètre @Cause pour indiquer l'exception de « cause ». Il est supposé que vous avez déjà créé des messages de journalisation internationalisés auxquels vous souhaitez ajouter cette fonctionnalité.

Procédure 6.12. Indiquer une exception comme « cause » d'une autre exception

1. **Ajouter le paramètre**
   Ajouter un paramètre **`Throwable`** ou une sous-classe à la méthode.

   ```
   @Message(id=328, value = "Error calculating: %s.")
   ArithmeticException calculationError(Throwable cause, String msg);
   ```

2. **Ajouter l'annotation**
   Ajouter l'annotation **`@Cause`** au paramètre.

   ```
   import org.jboss.logging.Cause

   @Message(id=328, value = "Error calculating: %s.")
   ArithmeticException calculationError(@Cause Throwable cause, String
   msg);
   ```

3. **Invoquer la méthode**
   Invoquer la méthode d'interface pour obtenir un objet d'exception. Le cas d'utilisation le plus commun est de lancer une exception à partir d'un bloc catch en utilisant l'exception récupérée comme « cause ».

   ```
   try
   {
      ...
   }
   catch(Exception ex)
   {
      throw ExceptionBundle.EXCEPTIONS.calculationError(
                                        ex, "calculating payment due
   per day");
   }
   ```

-

Exemple 6.6. Indiquer une exception comme « cause » d'une autre exception

Ce lot d'exceptions définit une méthode simple qui renvoie une exception du type ArithmeticException.

```
@MessageBundle(projectCode = "TPS")
interface CalcExceptionBundle
{
 CalcExceptionBundle EXCEPTIONS =
Messages.getBundle(CalcExceptionBundle.class);

    @Message(id=328, value = "Error calculating: %s.")
    ArithmeticException calcError(@Cause Throwable cause, String value);

}
```

Cet extrait de code exécute une opération qui lève une exception parce qu'il tente de diviser un entier par zéro. L'exception est interceptée et une nouvelle exception est créée en utilisant la première comme « cause ».

```
int totalDue = 5;
int daysToPay = 0;
int amountPerDay;

try
{
   amountPerDay = totalDue/daysToPay;
}
catch (Exception ex)
{
   throw CalcExceptionBundle.EXCEPTIONS.calcError(ex, "payments per
day");
}
```

Voici à quoi ressemble le message :

```
Exception in thread "main" java.lang.ArithmeticException: TPS000328:
Error calculating: payments per day.
 at com.company.accounts.Main.go(Main.java:58)
 at com.company.accounts.Main.main(Main.java:43)
Caused by: java.lang.ArithmeticException: / by zero
 at com.company.accounts.Main.go(Main.java:54)
 ... 1 more
```

Report a bug

6.2.6. Référence

6.2.6.1. Configuration Maven JBoss Logging Tools

Pour construire un projet Maven qui utilise JBoss Logging Tools pour l'internationalisation, vous devrez appliquer les changements suivants à la configuration du projet dans le fichier **pom.xml** :

Veuillez vous référer au quick start **logging-tools** pour obtenir un exemple de fichier **pom.xml** complet.

1. Le référentiel JBoss Maven Repository doit être activé pour le projet. Voir Section 2.3.2, « Configurer le référentiel JBoss EAP 6 Platform Maven Repository par les paramètres de configuration de Maven ».

2. Les dépendances Maven de **jboss-logging** et **jboss-logging-processor** doivent être ajoutées. Les deux dépendances sont disponibles sur JBoss EAP 6, ainsi l'étendue de chaque dépendance peut être définie comme **provided** tel qu'il a été montré.

```
<dependency>
   <groupId>org.jboss.logging</groupId>
   <artifactId>jboss-logging-processor</artifactId>
   <version>1.0.0.Final</version>
   <scope>provided</scope>
</dependency>

<dependency>
   <groupId>org.jboss.logging</groupId>
   <artifactId>jboss-logging</artifactId>
   <version>3.1.0.GA</version>
   <scope>provided</scope>
</dependency>
```

3. Le **maven-compiler-plugin** doit utiliser au minimum la version **2.2** et être configuré pour la cible et les sources générées de **1.6**.

```
<plugin>
   <groupId>org.apache.maven.plugins</groupId>
   <artifactId>maven-compiler-plugin</artifactId>
   <version>2.3.2</version>
   <configuration>
      <source>1.6</source>
      <target>1.6</target>
   </configuration>
</plugin>
```

Report a bug

6.2.6.2. Format de fichier de propriétés de traduction

Les fichiers de propriété utilisés pour les traductions de messages dans JBoss Logging Tools sont des fichiers de propriétés Java standards. Le format du fichier est le format **key=value** simple, orienté-ligne, décrit dans la documentation **java.util.Properties** class, http://docs.oracle.com/javase/6/docs/api/java/util/Properties.html.

Le format du nom du fichier a le format suivant :

```
InterfaceName.i18n_locale_COUNTRY_VARIANT.properties
```

- **InterfaceName** est le nom de l'interface où les traductions s'appliquent.

- **locale**, **COUNTRY**, et **VARIANT** identifient les paramètres régionaux correspondant à la traduction.
- **locale** et **COUNTRY** indiquent la langue et le pays en utilisant respectivement les codes Langues et Pays ISO-639 et ISO-3166. **COUNTRY** est optionnel.
- **VARIANT** est un identifiant optionnel pouvant être utilisé pour identifier les traductions qui ne s'appliquent qu'à un système d'exploitation ou navigateur en particulier.

Les propriétés contenues dans le fichier de traduction sont les noms des méthodes de l'interface en cours de traduction. La valeur assignée de la propriété est la traduction. Si une méthode est surchargée c'est indiqué en ajoutant un point, puis le nombre de paramètres pour le nom. Les méthodes de traduction peuvent seulement être surchargées en fournissant un nombre différent de paramètres.

Exemple 6.7. Échantillon de fichier de propriétés de traductions

Nom du fichier : **GreeterService.i18n_fr_FR_POSIX.properties**.

```
# Level: Logger.Level.INFO
# Message: Hello message sent.
logHelloMessageSent=Bonjour message envoyé.
```

Report a bug

6.2.6.3. Références aux annotations de JBoss Logging Tools

Les annotations suivantes sont définies dans JBoss Logging pour pouvoir être utilisées pour l'internationalisation et la localisation des messages de journalisation, strings et exceptions.

Tableau 6.1. Annotations de JBoss Logging Tools

Annotation	Cible	Description	Attributs
@MessageBundle	Interface	Définit l'interface en tant que Lot de Messages	**projectCode**
@MessageLogger	Interface	Définit l'interface en tant que Message Logger	**projectCode**
@Message	Méthode	Peut être utilisé dans les Lots de Messages et Message Loggers. Dans un Message Logger, définit une méthode comme étant un logger localisé. Dans un Lot de Messages, définit la méthode comme étant une méthode qui renvoie une Chaîne localisées ou un objet d'Exception.	**value**, **id**
@LogMessage	Méthode	Définit une méthode dans un Message Logger comme étant une méthode de logging.	**level** (default **INFO**)

Annotation	Cible	Description	Attributs
`@Cause`	Paramètre	Définit un paramètre comme étant un paramètre faisant passer une exception en tant que cause d'un Message Log ou autre exception.	-
`@Param`	Paramètre	Définit un paramètre comme étant un paramètre passé au constructeur d'une Exception.	-

Report a bug

CHAPITRE 7. ENTERPRISE JAVABEANS

7.1. INTRODUCTION

7.1.1. Entreprise JavaBeans

Enterprise JavaBeans (EJB) 3.1 est une API pour développer des applications de Java EE distribuées, transactionnelles, sécurisées et portables grâce à l'utilisation des composants côté serveur appelés Enterprise Beans. Enterprise Beans implémente la logique métier d'une application, de manière découplée, qui encourage la réutilisation. Enterprise JavaBeans 3.1 est documenté dans la spécification Java EE JSR-318.

JBoss EAP 6 prend en charge la génération d'applications qui utilisent la spécification Enterprise JavaBeans 3.1. Le conteneur EJB est implémenté par le projet communautaire JBoss EJB3, http://www.jboss.org/ejb3.

Report a bug

7.1.2. Groupe de fonctionnalités EJB 3.1

Les fonctionnalités suivantes sont prises en charge dans EJB 3.1

- Session Beans
- Message Driven Beans
- Vues non-interfaces
- interfaces locales
- interfaces distantes
- services web JAX-WS
- services web JAX-RS
- Service de minuterie
- Appels asynchrones
- Intercepteurs
- Interopérabilité RMI/IIOP
- Support de transaction
- Sécurité
- API intégrable

Les fonctionnalités suivantes sont prises en charge dans EJB 3.1 mais sont susceptibles d'être supprimées. Cela signifie qu'elles seront certainement optionnelles dans Java EE 7.

- Entity Beans (persistance gérée-bean et conteneur))
- Vues client Entity Beans EJB 2.1

- EJB Query Language (EJB QL)
- Services Web basés JAX-RPC (points de terminaison et vues client)

Report a bug

7.1.3. EJB 3.1 Lite

EJB Lite est un sous-ensemble de la spécification EJB 3.1. Il fournit une version simplifiée de la spécification EJB 3.1 complète dans le cadre du profil web Java EE 6.

EJB Lite simplifie l'implémentation de la logique métier dans les applications web avec les beans entreprise en :

1. ne supportant que les fonctionnalités qui sont utiles pour les applications-web, et
2. en permettant aux EJB d'être déployés dans le même fichier WAR sous forme d'application web.

Report a bug

7.1.4. Fonctionnalités EJB 3.1 Lite

EJB Lite inclut les fonctionnalités suivantes :

- Session Beans sans état, avec état, et singleton
- Interfaces commerciales locales et beans "sans interface"
- Intercepteurs
- Transactions gérées-conteneur et gérées-bean
- Sécurité déclarative et programmatique
- API intégrable

Les fonctionnalités suivantes d'EJB 3.1 ne sont par incluses spécifiquement :

- Interfaces éloignées
- Intéropérabilité RMI-IIOP
- Points de terminaison de Services Web JAX-WS
- Service de minuterie EJB
- Invocations de session beans asynchrones
- Message-driven beans

Report a bug

7.1.5. Beans Enterprise

Les beans Enterprise sont des composants d'applications côté serveur, ainsi définis dans la spécification Enterprise JavaBeans (EJB) 3.1, JSR-318. Les beans Enterprise sont conçus pour

l'implémentation d'une logique commerciale d'application d'une manière découplée, pour encourager sa réutilisation.

Les beans Enterprise sont écrits comme des classes Java et sont annotés avec les annotations EJB appropriées. Ils peuvent être déployés sur le serveur d'applications dans leurs propres archives (un fichier JAR) ou être déployés dans le cadre d'une application Java EE. Le serveur d'applications gère le cycle de vie de chaque bean Entreprise et leur fournit des services comme la sécurité, les transactions et la gestion de concurrence.

Un bean Enterprise peut également définir un nombre d'interfaces de métier. Les interfaces de métier vous proposent un plus grand contrôle sur les méthodes bean disponibles aux clients et peut également vous donner accès aux clients qui exécutent dans les JVM à distance.

Il existe trois types de beans Enterprise : les Session beans, les Message-driven beans et les Entity beans.

IMPORTANT

Les Entity beans sont maintenant obsolètes dans EJB 3.1 et Red Hat recommande d'utiliser des entités JPA à la place. Red Hat ne recommande d'utiliser des Entity beans que pour les compatibilités rétroactives avec les systèmes hérités.

Report a bug

7.1.6. Écriture des beans Enterprise

Les beans Enterprise sont des composants côté serveur conçus pour encapsuler la logique métier d'une manière découplée d'une application client spécifique. En implémentant votre logique de métier dans des beans Enterprise, vous serez en mesure de réutiliser ces beans dans plusieurs applications.

Les beans Enterprise sont écrits sous forme de classes Java annotées et n'ont pas besoin d'implémenter des interfaces EJB particulières, ni de représenter des sous-classes de classes EJB Super pour pouvoir être considérés bean Enterprise.

Les beans Enterprise EJB 3.1 sont empaquetés et déployés dans des fichiers JAR (Archives Java). Un fichier JAR Bean Enterprise peut être déployé dans votre serveur d'applications, ou être inclus dans un fichier EAR et déployé dans cette application. Il est également possible de déployer des beans Enterprise dans un fichier WAR en parallèle à une application web si les beans respectent la spécification EJB 3.1 Lite.

Report a bug

7.1.7. Interfaces Métier de Session Bean

7.1.7.1. Interfaces de métier Bean Enterprise

Une interface de métier EJB est une interface Java écrite par le développeur Bean qui fournit les déclarations de méthodes publiques d'un bean de session disponible aux clients. Les beans de session peuvent implémenter un certain nombre d'interface ou pas du tout (bean "no-interface").

Les interfaces de métier peuvent être déclarées comme interfaces locales ou à distance, mais pas les deux à la fois.

Report a bug

7.1.7.2. Interfaces de métier locales EJB

Une interface de métier locale EJB déclare les méthodes qui sont disponibles quand le bean et le client sont dans la même JVM. Quand un bean de session implémente une interface de métier locale, seules les méthodes déclarées dans cette interface seront disponibles pour les clients.

Report a bug

7.1.7.3. Interfaces métier à distance EJB

Une interface de métier à distance EJB déclare les méthodes qui sont disponibles pour les clients à distance. L'accès à distance à un bean de session qui implémente une interface à distance est fourni automatiquement par un conteneur EJB.

Un client à distance est un client qui exécute sur une JVM différente et peut inclure des applications de bureau ainsi que des applications web, des services et bean Enterprise déployés dans un serveur d'applications différent.

Les clients locaux peuvent accéder aux méthodes exposées par une interface de métier à distance. Cela est effectué par les mêmes méthodes que pour les clients à distance et comprend les mêmes protocoles de départ que pour une demande à distance.

Report a bug

7.1.7.4. Beans EJB No-interface

Un bean de session qui n'implémente pas d'interface de métier s'appelle un bean « no-interface ». Toutes les méthodes publiques de beans no-interface sont accessibles aux clients locaux.

Un bean de session qui implémente une interface de métier peut également être écrit pour exposer un affichage « no-interface ».

Report a bug

7.2. CRÉER DES PROJETS ENTERPRISE BEAN

7.2.1. Créer un projet d'archives EJB avec le Studio JBoss Developer

Cette tâche décrit comment créer un EJB (Enterprise JavaBeans) avec le Studio JBoss Developer

Prérequis

- Un serveur et un temps d'exécution du serveur ont été établis pour JBoss EAP 6.

Procédure 7.1. Créer un projet EJB avec le Studio JBoss Developer

1. **Créer un nouveau projet**
   Pour ouvrir l'Assistant New EJB Project, naviguer jusqu'au menu **Fichier**, sélectionner **Nouveau** puis **Projet EJB**.

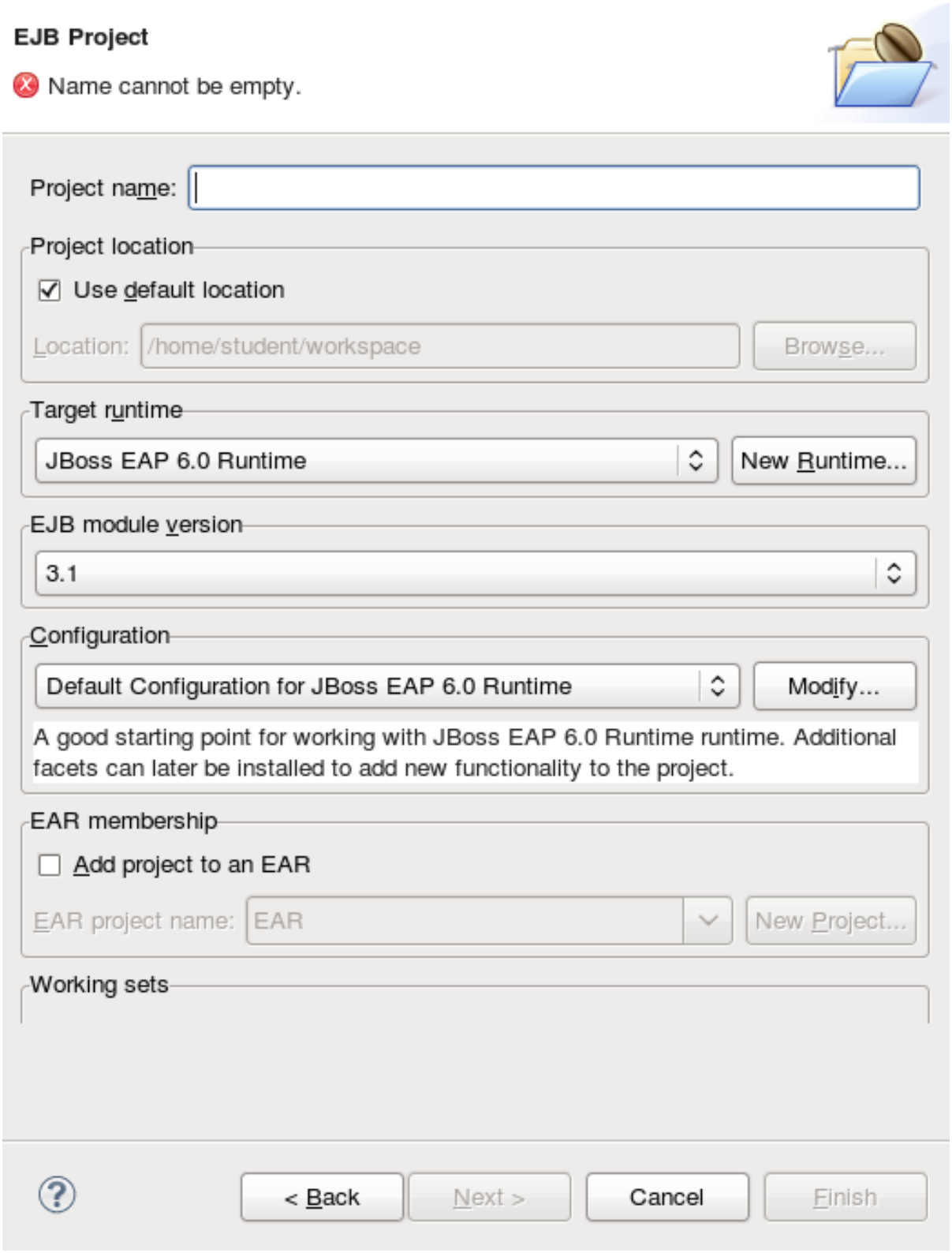


Figure 7.1. Assistant New EJB Project

2. **Détails**
   Fournir les informations suivantes :

   - Nom du projet.

     Il s'agira du nom du projet qui apparaît dans JBoss Developer Studio, et également le nom du fichier par défaut du fichier JAR déployé.

   - Emplacement du projet

Le répertoire où les fichiers du projet seront sauvegardés. La valeur par défaut est un répertoire qui se trouve dans l'espace de travail en cours.

- Runtime cible.

  Il s'agit du runtime de serveur utilisé pour le projet. Il devra être défini au même runtime JBoss EAP 6, qui est utilisé par le serveur dans lequel vous souhaitez déployer.

- Version de module EJB. Il s'agit de la version de la spécification EJB avec laquelle vos beans enterprise devront se conformer. Red Hat recommande que vous utilisiez **3.1**.

- Configuration. Cela vous permet d'ajuster les fonctionnalités prises en charge par votre projet. Utiliser la configuration par défaut pour le runtime que vous avez sélectionné.

Cliquer sur **Suivant** pour continuer.

3. **Java Build Configuration**
   Cet écran vous permet de personnaliser les répertoires qui contiennent les fichiers source de Java et le répertoire où les résultats de la génération se trouvent.

   Conservez cette configuration sans y apporter aucun changement et cliquer sur le bouton **Suivant**.

4. **Paramétrage du Module EJB**
   Cocher la case **Générer descripteur de déploiement ejb-jar.xml** si un descripteur de déploiement est requis. Le descripteur de déploiement est une option dans EJB 3.1, et peut être rajouté plus tard si nécessaire.

   Cliquer sur le bouton **Terminé** et le projet sera créé. Il s'affichera dans Project Explorer.

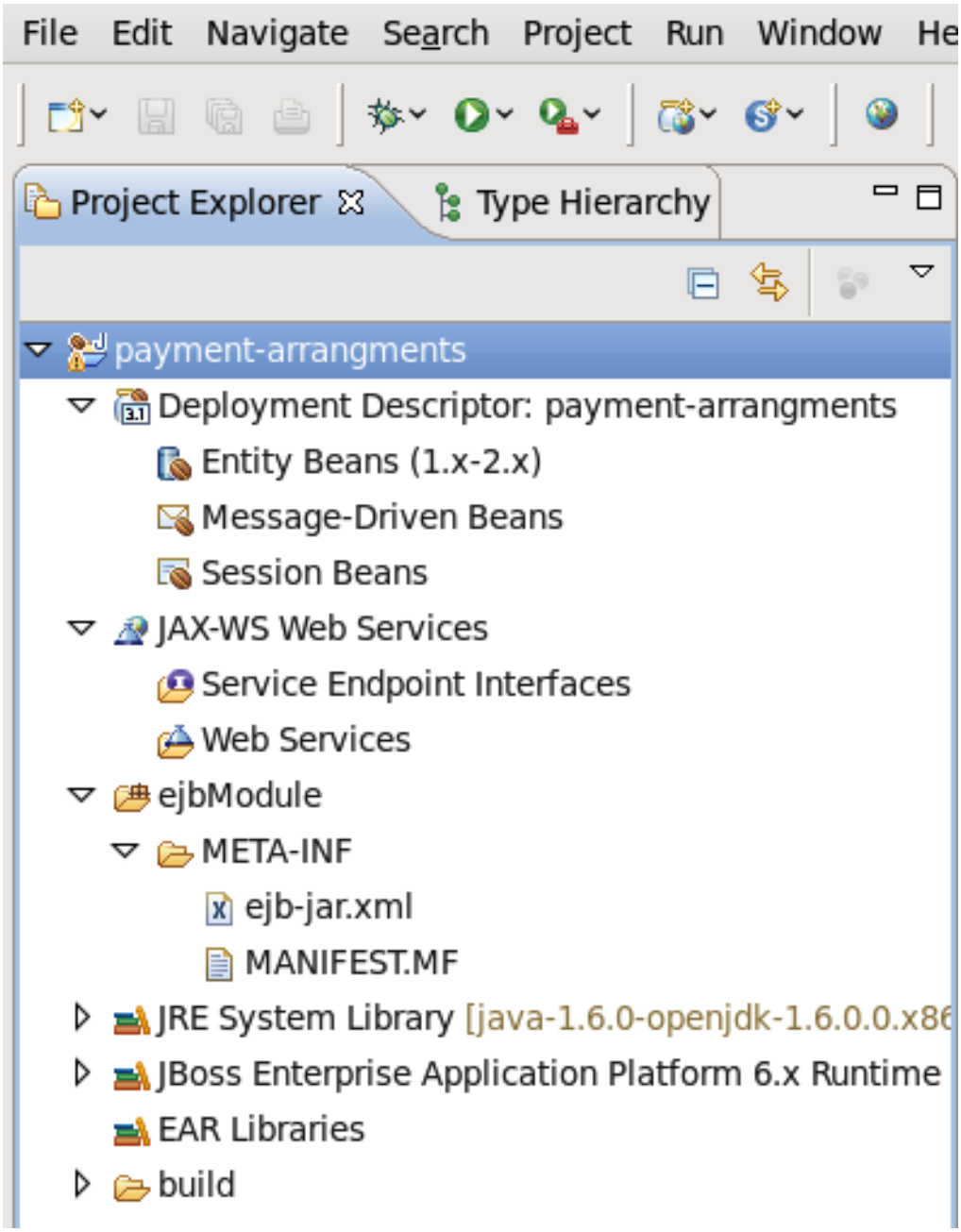


Figure 7.2. Nouveau projet EJB créé dans Project Explorer

5. **Ajouter l'artifact généré dans le serveur en vue du déploiement**
   Ouvrir le dialogue **`Ajouter et Supprimer`** en cliquant à droite sur le serveur dans lequel vous souhaitez générer l'artefact dans l'onglet serveur, et sélectionner 'Ajouter et Supprimer'.

   Sélectionner la ressource à déployer à partir de la colonne **`Disponible`** et cliquer sur le bouton **`Ajouter`**. La ressource sera déplacée dans la colonne **`Configurer`**, Cliquer sur **`Terminé`** pour fermer le dialogue.

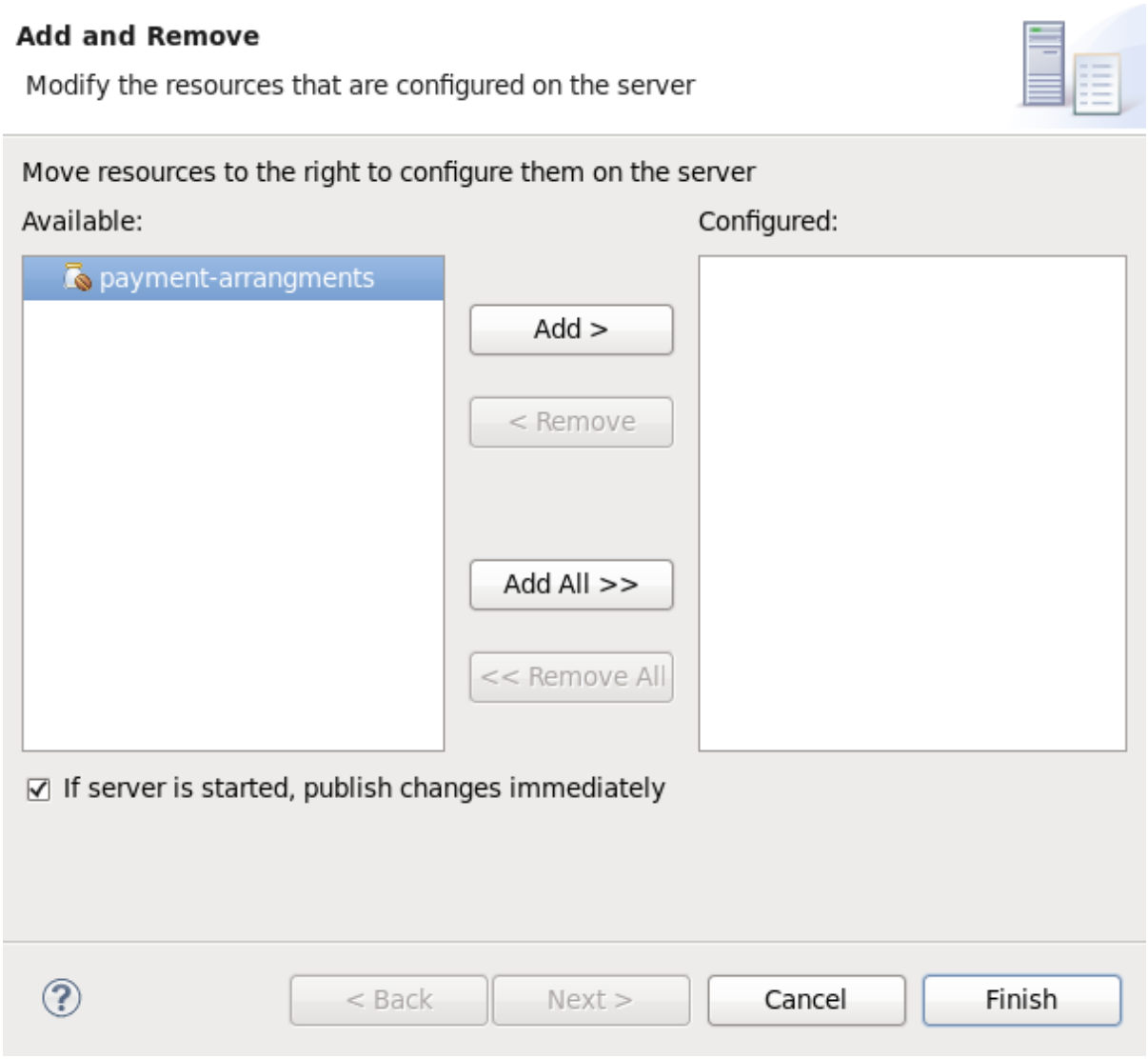


Figure 7.3. Ajouter et Supprimer le dialogue

Résultat

Vous avez maintenant un Projet EJB dans JBoss Developer Studio pouvant être construit et déployé pour un serveur spécifique.

Si aucun bean enterprise n'est ajouté au projet, alors JBoss Developer Studio affichera l'avertissement « un module EJB doit contenir un ou plusieurs beans enterprise. » Cet avertissement disparaîtra une fois qu'un ou plusieurs beans enterprise beans auront été ajoutés au projet.

Report a bug

7.2.2. Créer un projet EJB Archive dans Maven.

Cette tâche montre comment créer, dans Maven, un projet contenant un ou plusieurs Beans Enterprise empaquetés dans un fichier JAR.

Prérequis :

- Maven est déjà installé.
- Vous comprenez les bases d'utilisation de Maven.

Procédure 7.2. Créer un projet EJB Archive dans Maven

1. **Créer le projet Maven**
   Un projet EJB peut être créé en utilisant le système archétype de Maven et l'archétype **ejb-javaee6**. Pour ce faire, exécuter la commande **mvn** avec les paramètres suivants :

```
 mvn archetype:generate -
DarchetypeGroupId=org.codehaus.mojo.archetypes -
DarchetypeArtifactId=ejb-javaee6
```

   Maven vous demandera le **groupId**, le **artifactId**, la **version** et le **package** de votre projet.

```
[localhost]$ mvn archetype:generate -
DarchetypeGroupId=org.codehaus.mojo.archetypes -
DarchetypeArtifactId=ejb-javaee6
[INFO] Scanning for projects...
[INFO]
[INFO] ------------------------------------------------------------
--------------
[INFO] Building Maven Stub Project (No POM) 1
[INFO] ------------------------------------------------------------
--------------
[INFO]
[INFO] >>> maven-archetype-plugin:2.0:generate (default-cli) @
standalone-pom >>>
[INFO]
[INFO] <<< maven-archetype-plugin:2.0:generate (default-cli) @
standalone-pom <<<
[INFO]
[INFO] --- maven-archetype-plugin:2.0:generate (default-cli) @
standalone-pom ---
[INFO] Generating project in Interactive mode
[INFO] Archetype [org.codehaus.mojo.archetypes:ejb-javaee6:1.5]
found in catalog remote
Define value for property 'groupId': : com.shinysparkly
Define value for property 'artifactId': : payment-arrangments
Define value for property 'version':  1.0-SNAPSHOT: :
Define value for property 'package':  com.shinysparkly: :
Confirm properties configuration:
groupId: com.company
artifactId: payment-arrangments
version: 1.0-SNAPSHOT
package: com.company.collections
Y: :
[INFO] ------------------------------------------------------------
--------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------
--------------
[INFO] Total time: 32.440s
[INFO] Finished at: Mon Oct 31 10:11:12 EST 2011
[INFO] Final Memory: 7M/81M
[INFO] ------------------------------------------------------------
--------------
[localhost]$
```

2. **Ajouter vos beans enterprise**
   Ecrire vos beans enterprise et les ajouter au projet sous le répertoire **`src/main/java`** dans le sous-répertoire approprié pour le paquetage du bean.

3. **Créer votre projet**
   Pour construire ce projet, exécuter la commande **`mvn package`** dans le même répertoire que le fichier **`pom.xml`**. Cela compilera les classes Java et empaquettera le fichier JAR. Le fichier JAR construit se nomme ***`artifactId-version`*`.jar`** et se trouve dans le répertoire **`target/`**.

RÉSULTAT : Vous avez maintenant un projet Maven qui construit et empaquette un fichier JAR. Ce projet peut contenir des beans enterprise et le fichier JAR peut être déployé vers un serveur d'application.

Report a bug

7.2.3. Créer un projet EAR contenant un projet EJB

Cette tâche décrit comment créer dans JBoss Developer Studio un nouveau projet Enterprise Archive (EAR) contenant un Projet EJB.

Prérequis

- Un serveur et runtime de serveur pour JBoss EAP 6 a été installé. Veuillez vous référer à Section 1.3.1.5, « Ajouter le serveur de JBoss EAP 6 au JBoss Developer Studio » .

Procédure 7.3. Créer un projet EAR contenant un projet EJB

1. **Ouvrir le nouvel Assistant de Projet de l'Application EAR.**
   Naviguer vers le menu **Fichier**, sélectionner **Nouveau**, puis **Projet** et l'assistant **`Nouveau Projet`** apparaîtra. Sélectionner **Java EE/Enterprise Application Project** et cliquer sur le bouton **`Suivant`**.

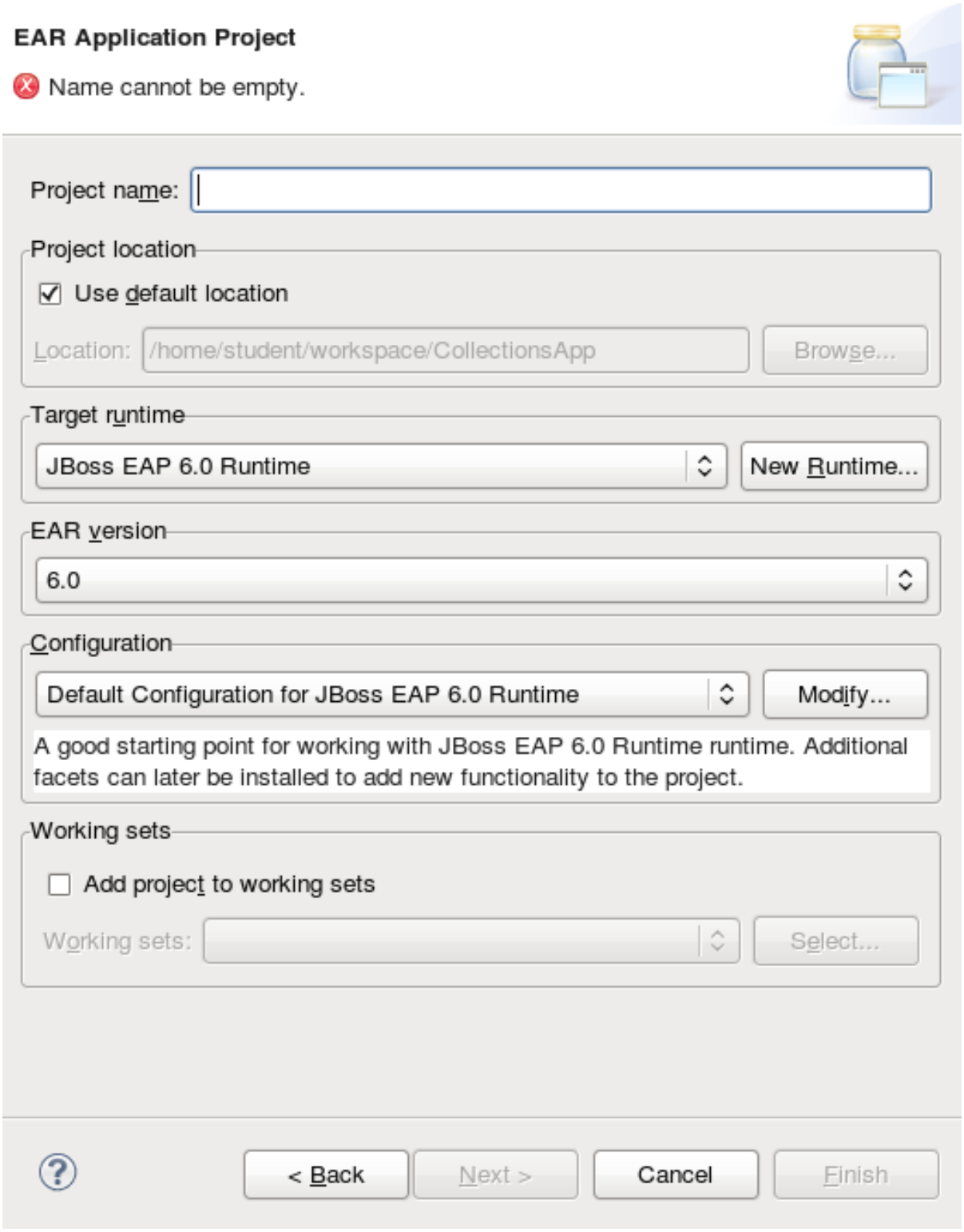


Figure 7.4. Nouvel Assistant de Projet de l'Application EAR.

2. **Fournir des Informations**
   Fournir les informations suivantes :

   - Nom du projet.

     En plus d'être le nom du projet qui apparaît dans le JBoss Developer Studio, c'est également le nom de fichier par défaut pour le fichier EAR déployé.

   - Emplacement du Projet

Le répertoire où les fichiers du projet seront sauvegardés. La valeur par défaut est un répertoire qui se trouve dans l'espace de travail en cours.

- Runtime cible.

  Il s'agit du runtime de serveur utilisé pour le projet. Il devra être défini au même runtime JBoss EAP 6, qui est utilisé par le serveur dans lequel vous souhaitez déployer.

- Version EAR.

  C'est la version des spécifications de Java Enterprise Edition auquel votre projet devra se conformer. Red Hat recommande d'en utiliser **6**.

- Configuration. Cela vous permet d'ajuster les fonctionnalités prises en charge par votre projet. Utiliser la configuration par défaut pour le runtime que vous avez sélectionné.

Cliquer sur **Suivant** pour continuer.

3. **Ajouter un nouveau module EJB.**
   Les nouveaux Modules peuvent être ajoutés à partir de la page **Enterprise Application** de l'assistant. Pour ajouter un nouveau Projet EJB en tant que module, veuillez suivre les étapes suivantes :

   a. **Ajouter un nouveau Module EJB.**
   Cliquer sur **Nouveau Module**, décocher la case **Créer Modules par Défaut**, sélectionner **Enterprise Java Bean** et cliquer sur **Suivant**. L'assistant **Nouveau Projet EJB** apparaîtra.

   b. **Créer un Projet EJB.**
   L'assistant **Nouveau Projet EJB** est le même que l'assistant utilisé pour créer de nouveaux projets EJB autonomes et est décrit dans Section 7.2.1, « Créer un projet d'archives EJB avec le Studio JBoss Developer ».

   Les détails minimales requis pour créer le project sont les suivants :

   - Nom du Projet
   - Runtime de la cible
   - Version Module EJB
   - Configuration

   Toutes les autres étapes de l'assistant sont optionnelles. Cliquer sur **Terminé** pour finir de créer le Projet EJB.

   Le Projet EJB tout juste créé est listé dans les dépendances du module Java EE et la case est cochée.

4. **Optionnel : ajouter un descripteur de déploiement application.xml**
   Cocher la case **Générer descripteur de déploiement d'application.xml** le cas échéant.

5. **Cliquer sur Finish**
   Deux nouveaux projets vont apparaître, le projet EJB et le projet EAR.

6. **Ajouter l'artifact généré dans le serveur en vue du déploiement**

Ouvrir la boîte de dialogue **Ajouter et Supprimer** en cliquant avec le bouton droit de la souris, dans l'onglet **Serveurs**, sur le serveur dans lequel vous souhaitez déployer l'artéfact de la build dans l'onglet serveur, et sélectionner **Ajouter et Supprimer**.

Sélectionner la ressource EAR à déployer depuis la colonne **Disponible** et cliquer sur le bouton **Ajouter**. La ressource sera déplacée vers la colonne **Configuré**. Cliquer sur **Terminé** pour fermer la boîte de dialogue.

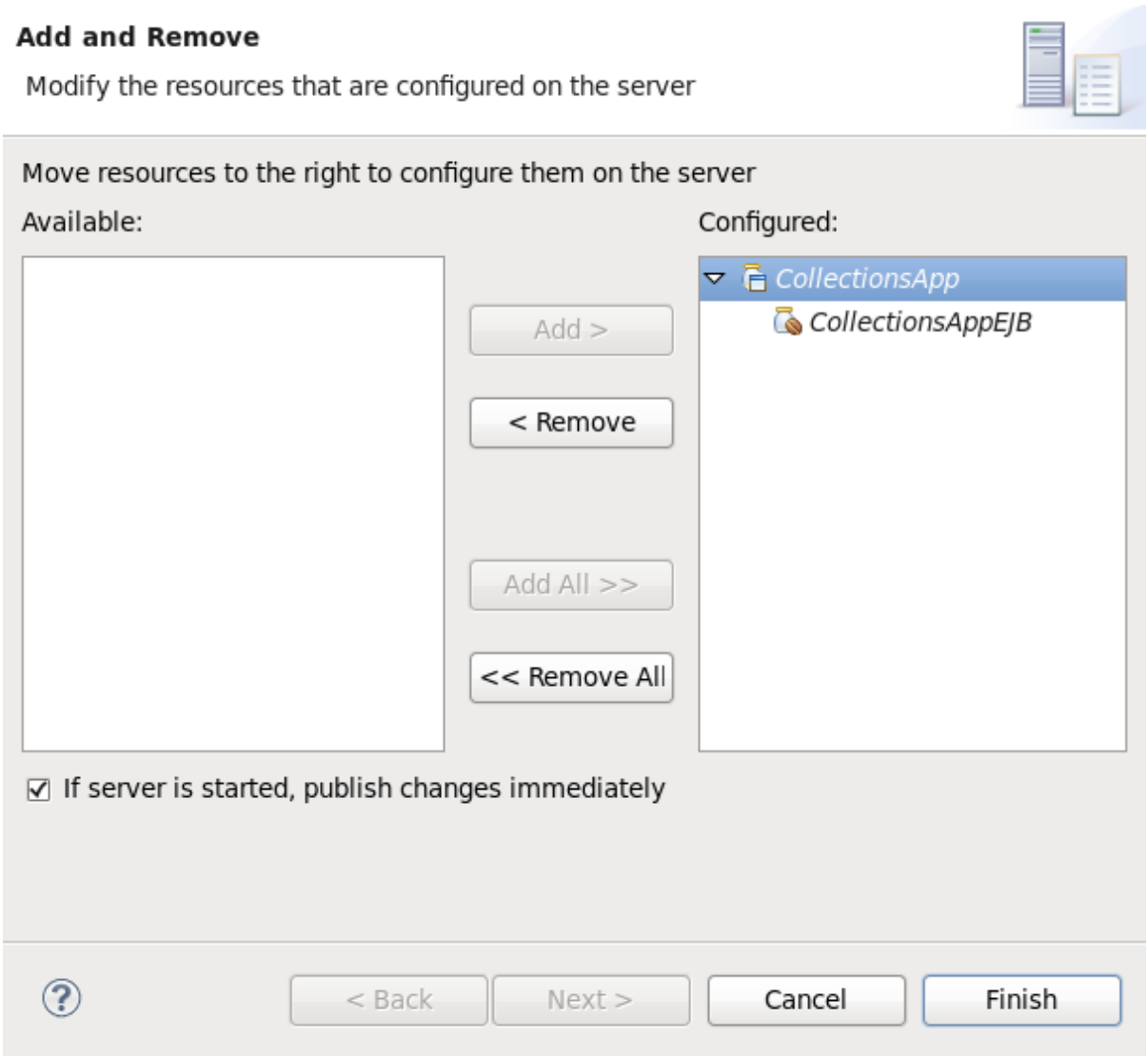


Figure 7.5. Ajouter et Supprimer le dialogue

Résultat

Vous avez maintenant un Projet d'Application Enterprise avec un Projet EJB membre. Celui-ci se créera et se déploiera vers le serveur indiqué en tant que déploiement EAR unique contenant un sous-déploiement EJB.

Report a bug

7.2.4. Ajouter un descripteur de déploiement à un projet EJB

On peut ajouter un descripteur de déploiement à un projet EJB qui a été créé sans descripteur. Pour cela, suivre la procédure ci-dessous.

Prérequis :

- Vous avez un projet EJB dans JBoss Developer Studio auquel vous souhaitez ajouter un descripteur de déploiement EJB.

Procédure 7.4. Ajouter un descripteur de déploiement à un projet EJB.

1. **Ouvrir le projet**
   Ouvrir le projet dans JBoss Developer Studio.

2. **Ajouter un descipteur de déploiement**
   Cliquer à droite sur le dossier Descripteur de déploiement dans la vue du projet et sélectionner **Générer Descripteur de déploiement**.

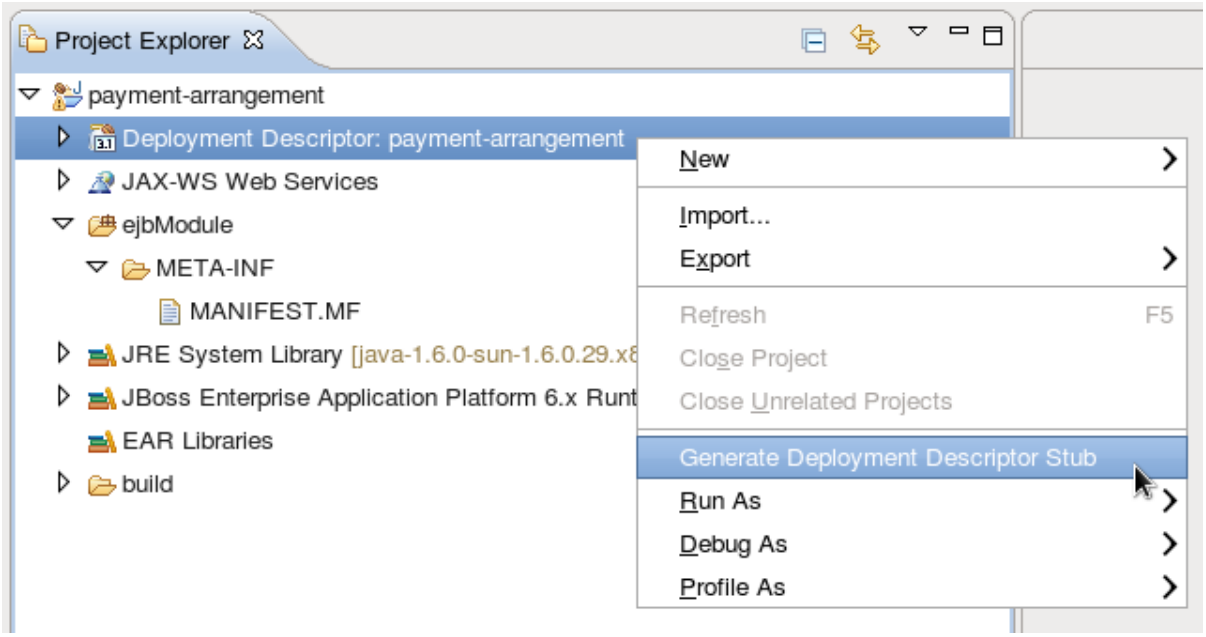


Figure 7.6. Ajouter un descripteur de déploiement

Le nouveau fichier, `ejb-jar.xml`, sera créé dans `ejbModule/META-INF/`. Cliquer deux fois dans le dossier Descripteur de déploiement dans la vue du projet, ce qui permettra d'ouvrir ce fichier également.

Report a bug

7.3. SESSION BEANS

7.3.1. Session Beans

Les Session Beans sont des Beans Enterprise qui encapsulent un ensemble de processus métier connexes ou des tâches, et qui sont injectés dans les classes qui en ont fait la demande. Il existe trois types de Session Beans : sans état, avec état et singleton.

Report a bug

7.3.2. Stateless Session Beans

Les Stateless Session Beans sont à la fois les types de bean de session les plus simples et les plus largement utilisés. Ils fournissent des méthodes commerciales à des applications client, mais ne maintiennent pas d'état entre les appels de méthode. Chaque méthode est une tâche complète, qui ne

s'appuie pas sur un état partagé au sein de ce bean de session. Parce qu'il n'y a aucun état, le serveur d'application n'est pas tenu de s'assurer que chaque appel de méthode soit effectué sur la même instance. Cela rend les beans de session stateless très efficaces et évolutifs.

Report a bug

7.3.3. Stateful Session Beans

Les Stateful Session Beans sont des beans Enterprise qui fournissent des modèles commerciaux aux applications client et qui maintiennent un état conversationnel avec le client. Ils doivent être utilisés pour des tâches en plusieurs étapes - appels de méthode - chacun répondant à l'état de l'étape précédente ayant été maintenue. Le serveur d'applications veille à ce que chaque client reçoive la même instance d'un stateful session bean pour chaque appel de méthode.

Report a bug

7.3.4. Singleton Session Beans

Les Singleton Session Beans sont des beans de session qui sont instanciés une fois par application, et chaque requête de client de Singleton Bean va dans la même instance. Les Singleton Beans représentent une implémentation du Singleton Design Pattern décrit dans le l'ouvrage *Design Patterns: Elements of Reusable Object-Oriented Software* d'Erich Gamma, Richard Helm, Ralph Johnson et John Vlissides; publié par Addison-Wesley en 1994.

Les beans Singleton fournissent la plus petite empreinte parmi tous les types de beans de session, mais ils doivent être thread-safe. EJB 3.1 fournit la CMC (de l'anglais Container Managed Concurrency) pour permettre aux développeurs d'implémenter des beans Singleton facilement. Cependant, les beans Singleton peuvent également être écrits grâce à un code multi-thread BMC (de l'anglais Bean Managed Concurrency) si CMC n'offre pas suffisamment de flexibilité.

Report a bug

7.3.5. Ajouter des Session Beans à un projet dans JBoss Developer Studio

JBoss Developer Studio possède plusieurs assistants qui peuvent être utilisés pour créer rapidement des classes bean enterprise. La procédure suivante vous montre comment utiliser les assistants du JBoss Developer Studio pour ajouter un session bean à un projet.

Prérequis :

- Vous avec un EJB ou Dynamic Web Project dans JBoss Developer Studio auquel vous souhaitez ajouter un ou plusieurs session beans.

Procédure 7.5. Ajouter des Session Beans à un projet dans JBoss Developer Studio

1. **Ouvrir le projet**
   Ouvrir le projet dans JBoss Developer Studio.

2. **Ouvrir l'assistant "Create EJB 3.x Session Bean" (Créer EJB 3.x Session Bean)**
   Pour ouvrir l'assistant **`Créer EJB 3.x Session Bean`**, naviguer dans le menu **Fichier**, et sélectionner **Nouveau**, puis **Session Bean (EJB 3.x)** .

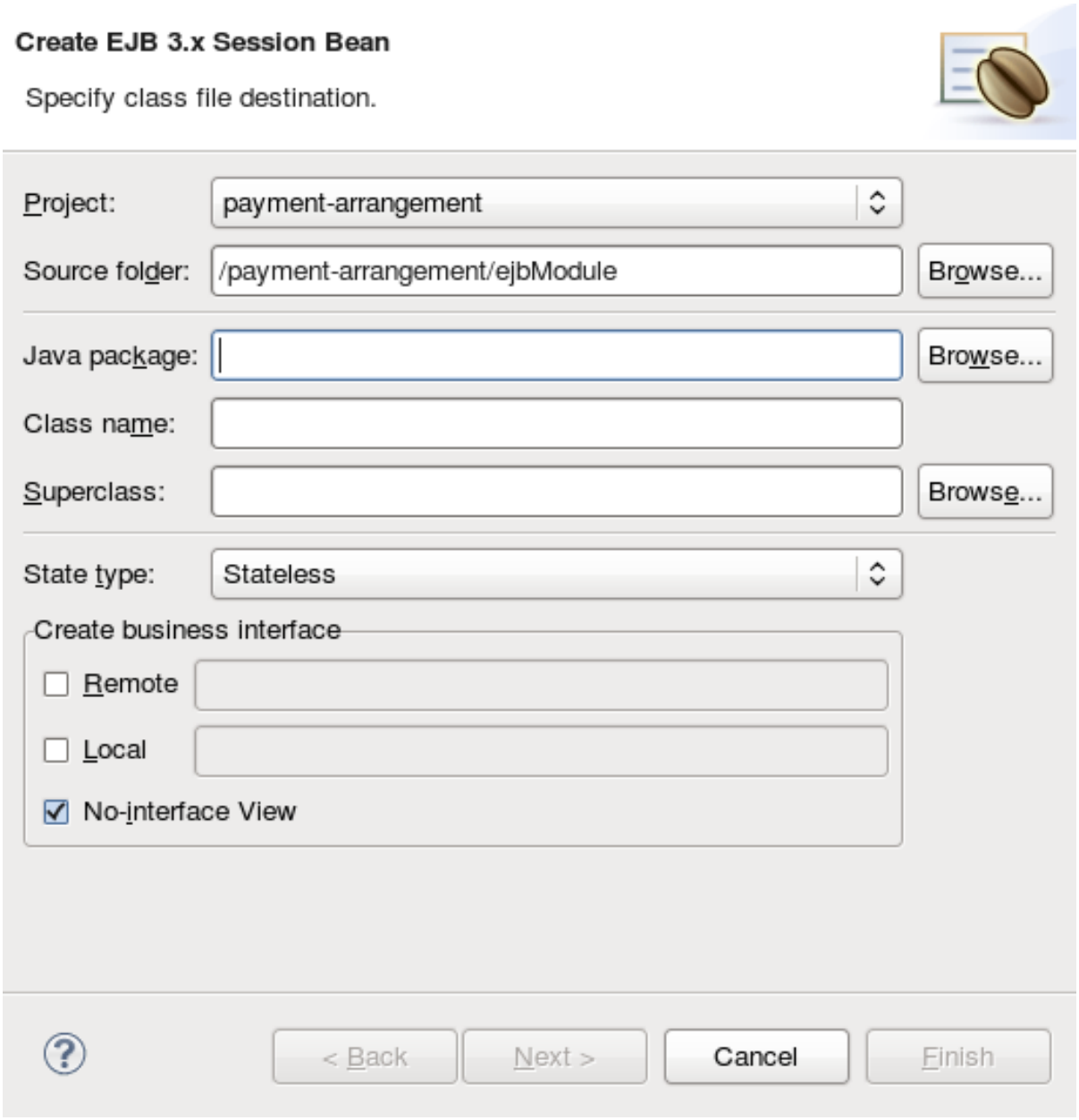


Figure 7.7. Créer un assistant EJB 3.x Session Bean

3. **Indiquer les informations de classe**
   Donner les informations suivantes :

   - Projet

     Verifier que le projet qui convient a bien été sélectionné.

   - Dossier source

     Il s'agit du dossier dans lequel les fichiers source de Java seront créés. Cela n'a pas normalement besoin d'être changé.

   - Package

     Indiquer le package auquel cette classe appartient.

   - Nom de la classe

     Indiquer le nom de la classe qui représentera le session bean.

- Superclass

  La classe de session bean peut hériter d'une Superclass. Indiquer ici si votre session a une Superclass.

- Type d'état

  Indiquer le type d'état du session bean: stateless, stateful, ou singleton.

- Interfaces commerciales

  Par défaut, la case No-interface est cochée, donc aucune interface ne sera créée. Cocher les cases des interfaces que vous souhaitez définir et ajuster les noms si nécessaire.

  Nous vous rappelons que les beans Enterprise d'un WAR (Web Archive) ne supportent qu'EJB 3.1 Lite, et que cela n'inclut pas les interfaces commerciales distantes.

Cliquez sur **`Suivant`**.

4. **Informations spécifiques aux Session Bean**
   Vous pouvez saisir des informations supplémentaires ici pour personnaliser encore plus le session bean. Vous n'avez pas besoin de changer quoi que ce soit ici.

   Les items que vous pouvez changer sont :

   - Nom de bean.
   - Nom mappé.
   - Type de transaction (géré conteneur ou géré bean).
   - On peut fournir des interfaces supplémentaires que le bean doit implémenter.
   - Vous pouvez également spécifier des interfaces EJB 2.x Home et Component si nécessaire.

5. **Terminer**
   Cliquer sur le bouton **`Terminé`** et le nouveau session bean sera créé, et ajouté au projet. Les fichiers de toute nouvelle interface commerciale seront également créés, s'ils ont été spécifiés.

RÉSULTAT: un nouveau session bean sera ajouté au projet.

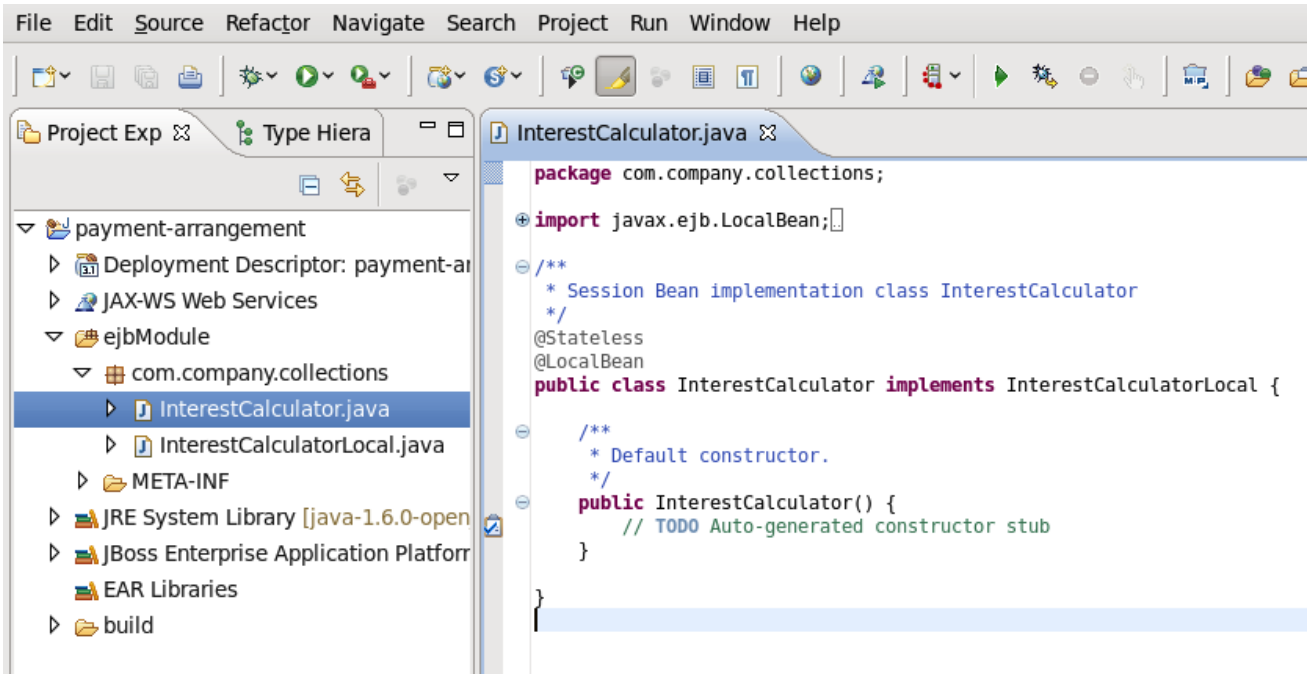


Figure 7.8. Nouveau Session Bean dans JBoss Developer Studio

Report a bug

7.4. MESSAGE-DRIVEN BEANS

7.4.1. Message-Driven Beans

Les Message-driven Beans (MDB) fournissent un modèle basé-événement pour le développement de l'application. Les méthodes des MDB ne sont pas injectées ou invoquées du code client mais sont déclenchées par la réception de messages d'un service de messagerie tel que le serveur Java Messaging Service (JMS). La spécification Java EE 6 exige que JMS soit pris en charge, mais les autres systèmes de messagerie peuvent être supportés également.

Report a bug

7.4.2. Adaptateurs de ressources

Un adaptateur de ressources est un composant Java EE déployable qui permet la communication entre une application Java EE et une entreprise d'informations système (EIE) à l'aide de la spécification Java Connector Architecture (JCA). Un adaptateur de ressources est souvent fourni par les fournisseurs de l'EIE pour permettre une intégration facile de leurs produits aux applications Java EE.

Un système d'information Enterprise peut être n'importe quel autre système de logiciel au sein d'une organisation. Les exemples incluent les systèmes ERP (Enterprise Resource Planning), les systèmes de base de données, les serveurs d'e-mails et les systèmes de messagerie propriétaires.

Un adaptateur de ressources est empaqueté dans un fichier de Ressources Adaptateur Archive (RAR) qui peut être déployé dans JBoss EAP 6. Un fichier RAR peut également être inclus dans un déploiement Enterprise Archive (EAR).

Report a bug

7.4.3. Créer un Message-Driven Bean basé JMS dans JBoss Developer Studio

Cette procédure montre comment ajouter un Message-Driven Bean basé JMS dans JBoss Developer Studio. Cette procédure crée un Message-Driven Bean EJB 3.x qui utilise des annotations.

Prérequis :

1. Vous devrez avoir un projet existant ouvert dans JBoss Developer Studio.
2. Vous devrez connaître le nom et le type de la destination JMS que le bean écoutera.
3. Le support pour JMS (Java Messaging Service) doit être autorisé dans la configuration JBoss EAP 6 dans laquelle ce bean sera déployé.

Procédure 7.6. Ajouter un Message-Driven Bean basé JMS dans JBoss Developer Studio.

1. **Ouvrir l'assistant `Créer EJB 3.x Message-Driven Bean`**
   Aller à **Fichier** → **Nouveau** → **Autre**. Sélectionner **`EJB/Message-Driven Bean (EJB 3.x)`** et cliquer sur le bouton **`Suivant`**.

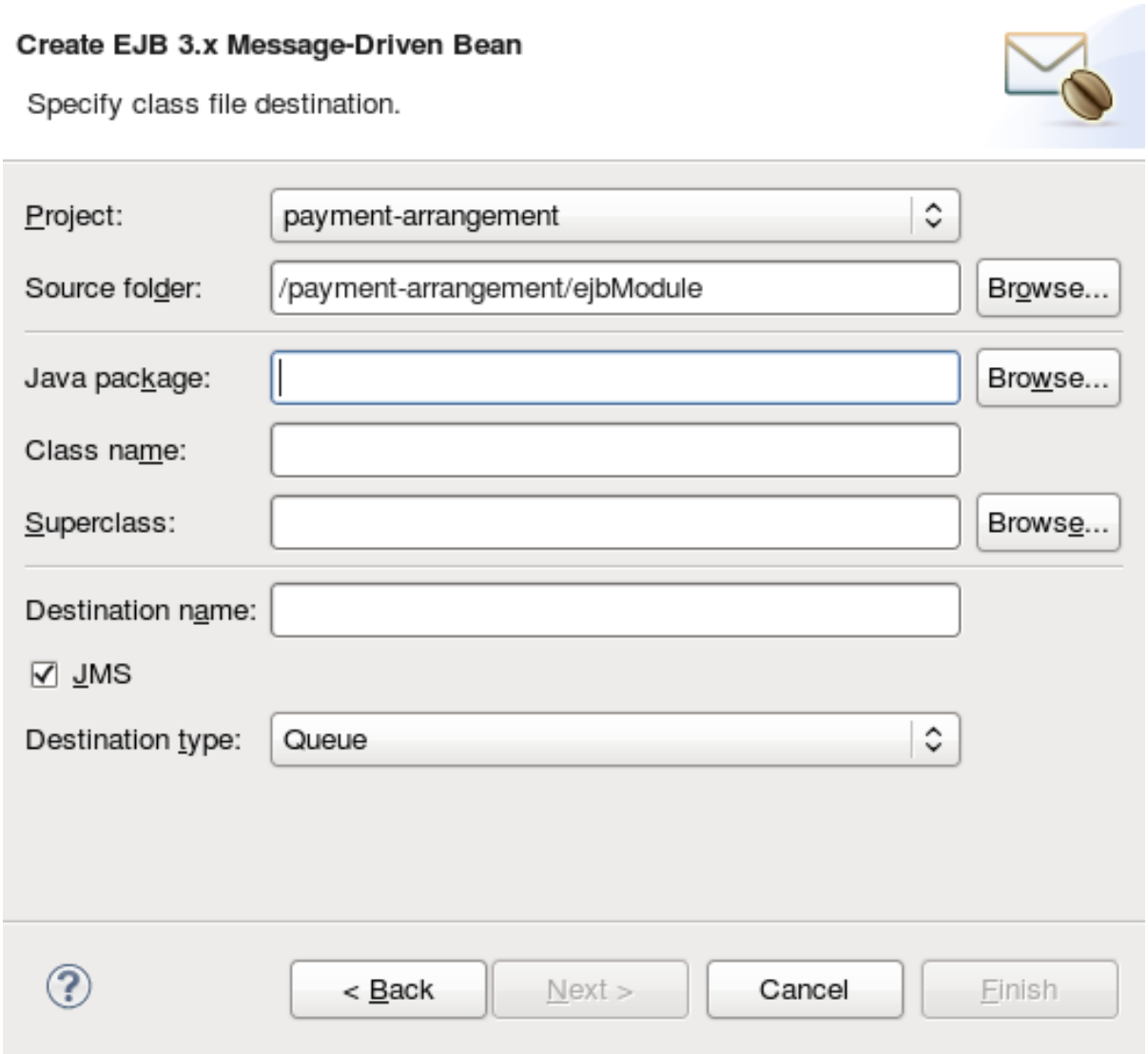


Figure 7.9. Créer l'assistant Message-Driven Bean EJB 3.x

2. **Indiquer les détails de la destination de fichier de classe**
   Il existe trois ensembles de détails à indiquer pour la classe de bean : le Projet, la classe Java et le message de destination.

Projet

- Si plusieurs projets existent dans **`Espace de travail`**, assurez-vous que le bon projet est sélectionné dans le menu **Projet**.
- Le dossier où le fichier source du nouveau bean sera créé est **`ejbModule`** sous le répertoire du projet sélectionné. Ne peut être changé que pour répondre à des cas particuliers.

Classe Java

- Les champs obligatoires sont les suivants : **`Package Java`** et **`nom de classe`**.
- Il n'est pas nécessaire de fournir une **`Superclasse`** à moins que la logique commerciale de votre application ne l'exige.

Destination du message

Voici les informations à fournir pour un Message-Driven Bean basé JMS :

- **`Nom de Destination`**. C'est la file d'attente ou le nom du sujet qui contient les messages auxquels le Bean répondra.
- La case **`JMS`** est sélectionnée par défaut. Veuillez ne pas la changer.
- Définir **`Type de destination`** comme **`File d'attente`** ou **`Sujet`** tel qu'il vous est demandé.

Cliquer sur le bouton **`Suivant`**.

3. **Saisir les informations spécifiques aux Message-Driven Bean**
   Les valeurs par défaut sont appropriées pour un Message-Driven Bean basé JMS utilisant des transactions gérées conteneur.
   - Changer le type de transaction à Bean si le Bean doit utiliser des transactions gérées bean.
   - Changer le nom du Bean s'il est demandé un nom de bean différent du nom de classe.
   - L'interface JMS Message Listener sera déjà listée. Vous n'aurez pas besoin d'ajouter ou de supprimer des interfaces, à moins qu'elles soient spécifiques à votre logique commerciale d'applications.
   - Laisser les cases décochées pour créer les méthodes stub sélectionnées.

   Cliquer sur le bouton **`Terminé`**.

Résultat : le Message-Driven Bean sera créé avec des méthodes stub pour le constructeur par défaut et la méthode **`onMessage()`**. Une fenêtre d'édition de JBoss Developer Studio est apparue avec le fichier correspondant.

Report a bug

7.5. INVOQUER LES SESSION BEANS

7.5.1. Invoquer un session bean à distance avec JNDI

Cette tâche décrit comment ajouter un support à un client distant pour l'invocation de session beans par JNDI. La tâche assume que le projet est construit avec Maven.

Le Quickstart **`ejb-remote`** contient des projets Maven qui démontrent cette fonctionnalité. Le Quickstart contient des projets à la fois pour le déploiement des session beans et pour le client distant. Les exemples de code ci-dessous sont extraits du projet du client distant.

Cette tâche assume que les session beans n'ont pas besoin d'authentification.

Pré-requis

Les prérequis suivants doivent être respectés avant de commencer :

- Vous devez déjà avoir un projet Maven créé, prêt à l'utilisation.
- La configuration du référentiel JBoss EAP 6 Maven a déjà été ajoutée.
- Les session beans que vous souhaitez invoquer sont déjà déployés.
- Les session beans déployés implémentent les interfaces commerciales éloignées.
- Les interfaces commerciales éloignées des session beans sont disponibles sous forme de dépendance de Maven. Si les interfaces commerciales éloignées ne sont disponibles que sous forme de fichier JAR, alors il est recommandé d'ajouter le JAR à votre référentiel Maven comme un artefact. Reportez-vous à la documentation de Maven pour obtenir des directives **`install:install-file`**, http://maven.apache.org/plugins/maven-install-plugin/usage.html
- Vous aurez besoin de connaître le nom d'hôte et le port JNDI du serveur qui hébergent les session beans.

Pour invoquer un session bean d'un client distant, vous devez tout d'abord configurer le projet correctement.

Procédure 7.7. Ajouter une configuration de projet Maven pour l'invocation à distance des session beans

1. **Ajouter les dépendances de projet utiles**
   Le **`pom.xml`** du projet doit être mis à jour pour pouvoir inclure les dépendances nécessaires.
2. **Ajouter le fichier `jboss-ejb-client.properties`**
   L'API du client JBoss EJB s'attend à trouver un fichier dans le root du projet nommé **`jboss-ejb-client.properties`** qui contient les informations de connexion aux services JNDI. Ajouter ce fichier au répertoire **`src/main/resources/`** de votre projet avec le contenu suivant.

   ```
   # In the following line, set SSL_ENABLED to true for SSL
   remote.connectionprovider.create.options.org.xnio.Options.SSL_ENABLE
   D=false
   remote.connections=default
   # Uncomment the following line to set SSL_STARTTLS to true for SSL
   #
   remote.connection.default.connect.options.org.xnio.Options.SSL_START
   TLS=true
   remote.connection.default.host=localhost
   remote.connection.default.port = 4447
   ```

```
remote.connection.default.connect.options.org.xnio.Options.SASL_POLI
CY_NOANONYMOUS=false
# Add any of the following SASL options if required
#
remote.connection.default.connect.options.org.xnio.Options.SASL_POLI
CY_NOANONYMOUS=false
#
remote.connection.default.connect.options.org.xnio.Options.SASL_POLI
CY_NOPLAINTEXT=false
#
remote.connection.default.connect.options.org.xnio.Options.SASL_DISA
LLOWED_MECHANISMS=JBOSS-LOCAL-USER
```

Changer le nom d'hôte et le port pour qu'ils correspondent au serveur. **4447** est le numéro de port par défaut. Pour une connexion sécurisée, définir la ligne **SSL_ENABLED** à **`true`** et décommenter la ligne **SSL_STARTTLS**. L'interface éloignée du conteneur supporte les connexions sécurisées et non sécurisées en utilisant le même port.

3. **Ajouter des dépendances aux interfaces commerciales à distance.**
   Ajouter les dépendances Maven au **`pom.xml`** aux interfaces commerciales éloignées des session beans.

```
<dependency>
   <groupId>org.jboss.as.quickstarts</groupId>
   <artifactId>jboss-as-ejb-remote-server-side</artifactId>
   <type>ejb-client</type>
   <version>${project.version}</version>
</dependency>
```

Maintenant que le projet a été configuré correctement, vous pouvez ajouter le code pour accéder et invoquer les session beans.

Procédure 7.8. Obtenez un Bean Proxy par JNDI et invoquer les méthodes du Bean

1. **Exceptions vérifiées par Handle**
   Deux des méthodes utilisées dans le code suivant (**`InitialContext()`** et **`lookup()`**) ont une exception vérifiée du type **`javax.naming.NamingException`**. Ces appels de méthode doivent soit être contenus dans un bloc try/catch qui intercepte **`NamingException`** ou dans une méthode déclarée pour lancer **`NamingException`**. Le Quickstart **`ejb-remote`** utilise la seconde technique.

2. **Créer un contexte JNDI**
   Un objet de contexte JNDI fournit le mécanisme pour demander les ressources dans le serveur. Créer un contexte JNDI avec le code suivant :

```
final Hashtable jndiProperties = new Hashtable();
jndiProperties.put(Context.URL_PKG_PREFIXES,
"org.jboss.ejb.client.naming");
final Context context = new InitialContext(jndiProperties);
```

   Les propriétés de connexion du service JNDI sont lues à partir du fichier **`jboss-ejb-client.properties`**.

3. **Utiliser la méthode JNDI Context's lookup() pour obtenir un Bean Proxy**
   Invoquer le méthode **`lookup()`** du bean proxy et lui faire passer le nom JNDI du session bean dont vous avez besoin. Un objet sera renvoyé et il devra correspondre au type de méthode d'interface commerciale qui contient les méthodes que vous souhaitez invoquer.

   ```
   final RemoteCalculator statelessRemoteCalculator =
   (RemoteCalculator) context.lookup(
       "ejb:/jboss-as-ejb-remote-server-side/CalculatorBean!" +
       RemoteCalculator.class.getName());
   ```

   Les noms de session bean JNDI sont définis par une syntaxe particulière. Pour plus d'informations, consulter Section 7.8.1, « Référence de nommage EJB JNDI » .

4. **Méthodes d'invocation**
   Maintenant que vous avez un objet bean proxy, vous pouvez invoquer n'importe quelle méthode qui contient l'interface commerciale distante.

   ```
   int a = 204;
   int b = 340;
   System.out.println("Adding " + a + " and " + b + " via the remote
   stateless calculator deployed on the server");
   int sum = statelessRemoteCalculator.add(a, b);
   System.out.println("Remote calculator returned sum = " + sum);
   ```

   Le proxy bean transmet la demande d'invocation de méthode au bean de session sur le serveur, où elle est exécutée. Le résultat est retourné au proxy bean qui, ensuite, le retourne à l'appelant. La communication entre le proxy bean et le bean de session distant est transparente à l'appelant.

Vous devriez maintenant être en mesure de configurer un projet Maven pour soutenir les sessions beans invoquant de session sur un serveur distant et écrire le code d'invocation des méthodes de sessions beans à l'aide d'un proxy bean récupéré du serveur par JNDI.

Report a bug

7.5.2. Contextes Client EJB

JBoss EAP 6 a introduit l'API client EJB pour gérer les invocations EJB à distance. L'API client EJB JBoss utilise le Contexte Client EJB, qui peut être associé à, et être utilisé par un ou plusieurs threads simultanément. Cela signifie qu'un Contexte Client EJB pourrait contenir n'importe quel nombre de récepteur EJB. Un récepteur EJB est un composant qui sait communiquer avec un serveur capable de gérer l'invocation EJB.

- Un client à distance, exécuté comme application Java autonome.
- Un client à distance, exécuté dans une autre instance de JBoss EAP 6.

Selon le type de client à distance, d'un point de vue API Client EJB, il pourrait y avoir plus d'un Context Client EJB au sein de la JVM.

Bien que les applications autonomes possèdent généralement un Contexte Client EJB unique pouvant être sauvegardé par n'importe quel nombre de récepteurs EJB, cela n'est pas obligatoire. Si une application autonome possède plus d'un Contexte Client EJB, un sélecteur de Contexte Client EJB

sera chargé de retourner le contexte approprié.

Dans le cas où des clients à distance s'exécutent dans une autre instance de JBoss EAP 6, chaque application déployée aura un contexte client EJB correspondant. A chaque fois que cette application invoque un autre EJB, le contexte client EJB correspondant est utilisé pour trouver le récepteur EJB correct, qui gère ensuite l'invocation.

Report a bug

7.5.3. Considérations lors de l'utilisation d'un Contexte EJB Unique

Résumé

Vous devez considérer les prérequis de votre application lors de l'utilisation d'un contexte client EJB unique avec des clients à distance autonomes. Pour plus d'informations sur les différents types de clients à distance, veuillez consulter : Section 7.5.2, « Contextes Client EJB » .

Procédure typique pour un Client Autonome à distance avec un Contexte Client EJB unique.

Un client autonome à distance possède généralement un seul contexte client EJB sauvegardé par n'importe quel nombre de récepteurs EJB. Voici un exemple d'application client à distance autonome :

```
public class MyApplication {
    public static void main(String args[]) {
        final javax.naming.Context ctxOne = new
javax.naming.InitialContext();
        final MyBeanInterface beanOne =
ctxOne.lookup("ejb:app/module/distinct/bean!interface");
        beanOne.doSomething();
        ...
    }
}
```

Les recherches JNDI de client à distance sont généralement sauvegardées par un fichier **`jboss-ejb-client.properties`**, utilisé pour installer le contexte client EJB et les récepteurs EJB. Cette configuration comprend également les informations de sécurité, qui sont ensuite utilisées pour créer le récepteur EJB qui relie le serveur JBoss EAP 6. Quand le code ci-dessus est invoqué,l'API client EJB recherche le contexte client EJB, qui est ensuite utilisé pour sélectionner le récepteur EJB qui recevra et traitera la requête d'invocation EJB. Dans ce cas, il n'y a que le contexte client EJB unique, donc ce contexte est utilisé par le code ci-dessus pour invoquer le bean. La procédure pour invoquer un bean de session à distance en utilisant JNDI est décrite plus en détails ici : Section 7.5.1, « Invoquer un session bean à distance avec JNDI » .

Client autonome à distance nécessitant différentes informations

Une application d'utilisateur pourrait vouloir invoquer un bean plus d'une fois, mais se connecter au serveur JBoss EAp 6 en utilisant différentes informations de sécurité. Voici un exemple d'une application client à distance autonome qui invoque deux fois le même bean :

```
public class MyApplication {
    public static void main(String args[]) {
        // Use the "foo" security credential connect to the server and
invoke this bean instance
        final javax.naming.Context ctxOne = new
javax.naming.InitialContext();
        final MyBeanInterface beanOne =
ctxOne.lookup("ejb:app/module/distinct/bean!interface");
```

```
        beanOne.doSomething();
        ...

        // Use the "bar" security credential to connect to the server and
invoke this bean instance
        final javax.naming.Context ctxTwo = new
javax.naming.InitialContext();
        final MyBeanInterface beanTwo =
ctxTwo.lookup("ejb:app/module/distinct/bean!interface");
        beanTwo.doSomething();
        ...
    }
}
```

Dans ce cas, l'application veut se connecter à la même instance de serveur pour invoquer l'EJB hébergé sur ce serveur, mais veut utiliser deux informations différentes pour se connecter au serveur. Puisque l'application du client possède un contexte de client EJB unique, qui peut avoir seulement un récepteur EJB pour chaque instance de serveur, cela signifie que le code ci-dessus n'utilise qu'une seule information pour se connecter au serveur et que le code ne s'exécute pas comme il le devrait.

Solution

Les Contextes Client EJB étendus offrent une solution à ce problème. Ils offrent un plus grand contrôle sur les contextes client EJB et leurs contextes JNDI associés, qui sont généralement utilisés pour les invocations EJB. Pour plus d'informations sur les Contextes Client EJB de l'étendue, veuillez consulter Section 7.5.4, « Utiliser des Contextes Client EJB étendus » et Section 7.5.5, « Configurer les EJB en utilisant un Contexte Client EJB Scoped » .

Report a bug

7.5.4. Utiliser des Contextes Client EJB étendus

Résumé

Pour invoquer un EJB dans les versions antérieures de JBoss EAP 6, il faut généralement créer un contexte JNDI et lui passer le PROVIDER_URL, qui indique le serveur de cible. Toute invocation faite sur les proxys EJB recherchées en utilisant ce contexte JNDI finiraient sur ce serveur. Avec les contextes client EJB étendus, les applications utilisateur contrôlent quel récepteur EJB est utilisé pour une invocation spécifique.

Utiliser le Contexte Client EJB étendu dans un client autonome à distance

Avant l'introduction des contextes client EJB étendus, le contexte était généralement étendu à l'application client. Les contextes client étendus autorisent maintenant les contextes client EJB à être étendus avec les contextes JNDI. Voici un exemple d'une application client autonome à distance qui invoque le même bean deux fois en utilisant un contexte client EJB étendu.

```
public class MyApplication {
    public static void main(String args[]) {

        // Use the "foo" security credential connect to the server and
invoke this bean instance
        final Properties ejbClientContextPropsOne =
getPropsForEJBClientContextOne():
        final javax.naming.Context ctxOne = new
javax.naming.InitialContext(ejbClientContextPropsOne);
        final MyBeanInterface beanOne =
```

```
ctxOne.lookup("ejb:app/module/distinct/bean!interface");
        beanOne.doSomething();
        ...
        ctxOne.close();

        // Use the "bar" security credential to connect to the server and
invoke this bean instance
        final Properties ejbClientContextPropsTwo =
getPropsForEJBClientContextTwo():
        final javax.naming.Context ctxTwo = new
javax.naming.InitialContext(ejbClientContextPropsTwo);
        final MyBeanInterface beanTwo =
ctxTwo.lookup("ejb:app/module/distinct/bean!interface");
        beanTwo.doSomething();
        ...
        ctxTwo.close();
    }
}
```

Pour utiliser le contexte client EJB, configurer les propriétés client EJB par programmation et passer les propriétés sur la création de contexte. Les propriétés correspondent au même ensemble de propriétés que celles qui sont utilisées dans le fichier standard **`jboss-ejb-client.properties`**. Pour étendre le contexte client EJB au contexte JNDI, il faut également indiquer la propriété **`org.jboss.ejb.client.scoped.context`** et définir sa valeur sur **`true`**. Cette propriété notifie à l'API client EJB qu'il doit créer un contexte client EJB, sauvegardé par des récepteurs EJB, et que le contexte créé doit ensuite être étendu ou visible uniquement au contexte JNDI qui l'a créé. Tout proxy EJB recherché ou invoqué en utilisant ce contexte JNDI ne connaîtra que le contexte client EJB associé à ce contexte JNDI. Les autres contextes JNDI utilisés par l'application pour rechercher ou invoquer des EJB ne reconnaîtra pas les autres contextes client EJB étendus.

Les contextes JNDI qui ne passent pas les propriétés **`org.jboss.ejb.client.scoped.context`** et ne sont pas étendus vers un contexte client EJB, utiliseront le comportement par défaut, qui utilise le contexte client EJB existant normalement attaché à l'application entière.

Les contextes client EJB étendus donnent aux applications d'utilisateur la même souplesse qui caractérisait les invocations JNDI basées JNP dans les versions précédentes de JBoss EAP 6. Ils donnent aux applications utilisateurs un plus grand contrôle sur quel contexte JNDI communique avec quel serveur et sur comment il se connecte à ce serveur.

NOTE

Dans le contexte étendu, les ressources sous-jacentes ne sont plus gérées par le conteneur ou l'API, donc vous devez fermer l' **`InitialContext`** lorsqu'il n'est plus utile. Lorsque l'**`InitialContext`** est fermé, les ressources sont libérées immédiatement. Les proxys qui y sont liés ne sont plus valides et tout invocation soulèvera une exception. Une mauvaise fermeture du **`InitialContext`** peut entraîner les problèmes de ressource ou de performance.

Report a bug

7.5.5. Configurer les EJB en utilisant un Contexte Client EJB Scoped

Résumé

Les EJB peuvent être configurés en utilisant un contexte scoped basé mappe. Cela est possible en

complétant par programmation une mappe **`Properties`** en utilisant les propriétés standards trouvées dans **`jboss-ejb-client.properties`**, en indiquant **`true`** pour la propriété **`org.jboss.ejb.client.scoped.context`**, et en passant les propriétés sur la création **`InitialContext`**.

L'avantage d'utiliser un contexte scoped est qu'il vous permet de configurer l'accès sans référencer directement l'EJB ou importer les classes JBoss. Il permet également de configurer et de répartir la charge d'un hôte lors du runtime dans un environnement multithreadé.

Procédure 7.9. Configurer un EJB en utilisant un contexte scoped basé mappage

1. **Configurer les propriétés**
   Configurer les propriétés client EJB par programmation, en indiquant le même ensemble de propriétés utilisées dans le fichier **`jboss-ejb-client.properties`** standard. Pour activer le contexte étendu, vous devez indiquer la propriété **`org.jboss.ejb.client.scoped.context`** et configurer sa valeur comme **`true`**. Voici un exemple de configuration des propriétés par programmation :

   ```
   // Configure  EJB Client properties for the InitialContext
   Properties ejbClientContextProps = new Properties();
   ejbClientContextProps.put(“remote.connections”,”name1”);
   ejbClientContextProps.put(“remote.connection.name1.host”,”localhost”
   );
   ejbClientContextProps.put(“remote.connection.name1.port”,”4447”);
   // Property to enable scoped EJB client context which will be tied
   to the JNDI context
   ejbClientContextProps.put("org.jboss.ejb.client.scoped.context",
   “true”);
   ```

2. **Passer les propriétés en création de contexte**

   ```
   // Create the context using the configured properties
   InitialContext ic = new InitialContext(ejbClientContextProps);
   MySLSB bean = ic.lookup("ejb:myapp/ejb//MySLSBBean!" +
   MySLSB.class.getName());
   ```

Informations supplémentaires

- Les contextes générés par les proxys EJB de recherche sont liés par ce contexte étendu et n'utilisent que les paramètres de connexion appropriés. Cela permet de créer différents contextes pour accéder aux données au sein d'une application client ou pour accéder aux serveurs de manière indépendante en utilisant différents logins.
- Dans le client, le **`InitialContext`** étendu et le proxy étendu sont tous les deux transférés vers les threads, permettant à chaque thread de fonctionner avec le contexte donné. Il est également possible de transférer le proxy vers de multiples threads qui peuvent l'utiliser simultanément.
- Le contexte étendu proxy EJB est sérialisé sur l'appel distant, puis désérialisé sur le serveur. Lorsqu'il est désérialisé, les informations de contexte étendu sont supprimées et il retourne à son état par défaut. Si le proxy désérialisé est utilisé sur le serveur distant, c-a-d s'il n'a plus le contexte étendu utilisé lors de sa création, cela peut provoquer une erreur **`EJBCLIENT000025`** ou éventuellement appeler une cible indésirable en utilisant le nom de l'EJB.

Report a bug

7.5.6. Propriétés Client EJB

Résumé

Les tableaux suivants énumèrent les propriétés pouvant être configurées par programmation ou dans le fichier `jboss-ejb-client.properties`.

Propriétés Globales de Client EJB

Le tableau suivant énumère les propriétés valides pour la bibliothèque entière au sein de la même étendue.

Tableau 7.1. Propriétés globales

Nom de propriété	Description
`endpoint.name`	Nom du point de terminaison du client. Si pas configuré, sa valeur par défaut sera `client-endpoint`. Cela peut s'avérer utile pour distinguer différentes configurations de point de terminaison puisque le nom de thread comprend cette propriété.
`remote.connectionprovider.create.options.org.xnio.Options.SSL_ENABLED`	Valeur booléenne qui indique si le protocole SSL est activé pour toutes les connexions.
`deployment.node.selector`	Nom complet de l'implémentation de `org.jboss.ejb.client.DeploymentNodeSelector`. Ceci est utilisé pour équilibrer les charges de l'invocation des EJB.
`invocation.timeout`	Délai pour la liaison EJB ou le cycle requête/réponse de l'invocation de la méthode. Valeur exprimée en millisecondes. L'invocation de toute méthode lève une `java.util.concurrent.TimeoutException` si l'exécution prend plus de temps que la période de délai. L'exécution se termine et le serveur n'est pas interrompu.
`reconnect.tasks.timeout`	Délai des tâches de reconnexion de l'arrière-plan. Valeur exprimée en millisecondes. Si des connexions sont éteintes, la prochaine invocation EJB de client utilisera un algorithme pour décider si une reconnexion est nécessaire pour trouver le bon nœud.
`org.jboss.ejb.client.scoped.context`	Valeur booléenne indiquant s'il faut activer le contexte client EJB d'étendue. La valeur par défaut est `false`. Si défini comme `true`, le client EJB utilisera le contexte étendu lié au contexte JNDI. Sinon, le contexte de client EJB utilisera la sélecteur global dans le JVM pour déterminer les propriétés utilisées pour appeler l'hôte et l'EJB à distance.

Propriétés de connexion de client EJB

Les propriétés de connexion commencent par le préfixe **`remote.connection.`*`CONNECTION_NAME`*** où le *CONNECTION_NAME* est un identifiant local utilisé uniquement pour identifier la connexion de manière exclusive.

Tableau 7.2. Propriétés de connexion

Nom de propriété	Description
`remote.connections`	Liste de **`connection-names`** actifs séparés par des virgules. Chaque connexion est configurée sous ce nom.
`remote.connection.`*`CONNECTION_NAME`*`.host`	Nom d'hôte ou IP de cette connexion
`remote.connection.`*`CONNECTION_NAME`*`.port`	Port de la connexion. La valeur par défaut est 4447.
`remote.connection.`*`CONNECTION_NAME`*`.username`	Nom d'utilisateur utilisé pour authentifier la sécurité de connexion.
`remote.connection.`*`CONNECTION_NAME`*`.password`	Mot de passe utilisé pour authentifier l'utilisateur.
`remote.connection.`*`CONNECTION_NAME`*`.connect.timeout`	Période de délai de la connexion initiale. Après cela, la tâche de reconnexion vérifiera périodiquement si la connexion peut être établie. Valeur exprimée en millisecondes.
`remote.connection.`*`CONNECTION_NAME`*`.callback.handler.class`	Nom complet de la classe **`CallbackHandler`**. Sera utilisé pour établir la connexion et ne peut être changé tant que la connexion sera ouverte.
`remote.connection.`*`CONNECTION_NAME`*`.` `channel.options.org.jboss.remoting3.RemotingOptions.MAX_OUTBOUND_MESSAGES`	Valeur entière indiquant le nombre maximale de requêtes sortantes. La valeur par défaut est 80. Il n'y a qu'une connexion entre le client (JVM) et le serveur pour gérer les invocations.

Nom de propriété	Description
remote.connection.*CONNECTION_NAME*.connect.options.org.xnio.Options.SASL_POLICY_NOANONYMOUS	Valeur booléenne déterminant si les identifiants doivent être fournis par le client pour réussir la connexion. La valeur par défaut est **true**. Si défini comme **true**, le client doit fournir les identifiants. Si défini comme **false**, l'invocation est autorisée tant que le connecteur à distance ne demande pas un domaine de sécurité.
remote.connection.*CONNECTION_NAME*.connect.options.org.xnio.Options.SASL_DISALLOWED_MECHANISMS	Désactive certains mécanismes SASL utilisés pour l'authentification pendant la création de la connexion. **JBOSS_LOCAL_USER** signifie que le mécanisme d'authentification silencieuse, utilisé lorsque le client et le serveur sont sur la même machine, est désactivé.
remote.connection.*CONNECTION_NAME*.connect.options.org.xnio.Options.SASL_POLICY_NOPLAINTEXT	Valeur booléenne qui active ou désactive l'utilisation de messages de texte brut pendant l'authentification. Si JAAS est utilisé, il doit être défini comme « false » pour autoriser un mot de passe de texte brut.
remote.connection.*CONNECTION_NAME*.connect.options.org.xnio.Options.SSL_ENABLED	Valeur booléenne indiquant si le protocole SSL est activé pour cette connexion.
remote.connection.*CONNECTION_NAME*.connect.options.org.jboss.remoting3.RemotingOptions.HEARTBEAT_INTERVAL	Intervalle pour envoyer une pulsation entre le client et le serveur afin de prévenir les fermetures automatiques, dans le cas d'un pare-feu par exemple. Valeur exprimée en millisecondes.

Propriétés de cluster de client EJB

Si la connexion initiale se connecte à un environnement clusterisé, la topologie du cluster est reçue de manière automatique et asynchrone. Ces propriétés sont utilisées pour se connecter à chaque membre reçu. Chaque propriété commence avec le préfixe **remote.cluster.*CLUSTER_NAME*** où le *CLUSTER_NAME* se réfère à la configuration du sous-système Infinispan du serveur associé.

Tableau 7.3. Propriétés de Cluster

Nom de propriété	Description

`remote.cluster.CLUSTER_NAME.`
 	
`clusternode.selector`
	Le nom complet de l'implémentation de `org.jboss.ejb.client.ClusterNodeSelector`.
	
	Cette classe, plutôt que `org.jboss.ejb.clientDeploymentNodeSelector`, est utilisée pour équilibrer la charge des invocations EJB dans un environnement clusterisé. Si le cluster est complètement arrêté, l'invocation échouera avec comme message `No ejb receiver available`.

`remote.cluster.CLUSTER_NAME.`
 	
`channel.options.org.jboss.remoting3.RemotingOptions.MAX_OUTBOUND_MESSAGES`
	Valeur entière indiquant le nombre maximale de requêtes sortantes pouvant être faites au cluster entier.

`remote.cluster.CLUSTER_NAME.`
 	
`node.NODE_NAME.channel.options.org.jboss.remoting3.RemotingOptions.MAX_OUTBOUND_MESSAGES`
	Valeur entière indiquant le nombre maximale de requêtes sortantes pouvant être faites à ce nœud de cluster spécifique.

Report a bug

7.6. INTERCEPTEURS DE CONTENEURS

7.6.1. Intercepteurs de conteneurs

Les intercepteurs standard Java EE, définis dans la spécification JSR 318, Enterprise JavaBeans 3.1 sont sensés exécuter une fois que le conteneur a complété la propagation de contexte de sécurité, la gestion des transactions, et que d'autres conteneurs ont fourni le traitement de l'invocation. C'est un problème si l'application de l'utilisateur doit intercepter un appel avant qu'un intercepteur spécifique de conteneur soit exécuté.

Les versions antérieures de JBoss EAP 6.0 fournissent un moyen de connecter des intercepteurs côté serveur dans le flux de l'invocation, donc vous pourriez exécuter la logique spécifique de l'application utilisateur avant que le conteneur ne termine le traitement de l'invocation. JBoss EAP 6.1 implémente désormais cette fonctionnalité. Cela permet aux intercepteurs standards de Java EE d'être utilisés comme des intercepteurs de conteneur, ce qui signifie qu'ils utilisent les mêmes éléments XSD que ceux autorisés dans le fichier `ejb-jar.xml` pour la version 3.1 du descripteur de déploiement ejb-jar.

Positionnement de l'intercepteur du conteneur dans la chaîne d'intercepteur

Les intercepteurs de conteneur configurés pour un EJB sont garantis d'être exécutés avant que le JBoss EAP 6.1 ne fournisse des intercepteurs de sécurité, des intercepteurs de gestion de transaction ou autres intercepteurs fournis par le serveur. Cela permet aux intercepteurs de conteneurs

spécifiques à l'application de traiter ou de configurer des données de contexte pertinentes avant l'invocation.

Différences entre l'intercepteur de conteneur et l'API Java EE Interceptor

Bien que les intercepteurs de conteneur soient modélisés pour pouvoir ressembler aux intercepteurs de Java EE, il y a quelques différences dans la sémantique de l'API. Par exemple, il est illégal pour les intercepteurs de conteneur d'invoquer la méthode **`javax.interceptor.InvocationContext.getTarget()`** parce que ces intercepteurs sont invoqués bien avant que les composants EJB ne soient configurés ou instanciés.

Report a bug

7.6.2. Créer une classe d'intercepteur de conteneur

Résumé

Les classes d'intercepteur de conteneur sont de simples POJO (Plain Old Java Objects). Ils utilisent **`@javax.annotation.AroundInvoke`** pour marquer la méthode qui devra être invoquée lors de l'invocation du bean.

Voici un exemple de classe d'intercepteur de conteneur qui marque la méthode **`iAmAround`** de l'invocation :

Exemple 7.1. Exemple de Classe d'intercepteur de Conteneur

```
public class ClassLevelContainerInterceptor {
    @AroundInvoke
    private Object iAmAround(final InvocationContext invocationContext)
throws Exception {
        return this.getClass().getName() + " " +
invocationContext.proceed();
    }
}
```

Pour voir un exemple de fichier de descripteur d'intercepteur de conteneur configuré pour utiliser cette classe, voir l'exemple **`jboss-ejb3.xml`** ici: Section 7.6.3, « Configurer un intercepteur de conteneur ».

Report a bug

7.6.3. Configurer un intercepteur de conteneur

Résumé

Les intercepteurs de conteneurs utilisent les bibliothèques d'intercepteur J2EE standard, ce qui signifie qu'ils utilisent les mêmes éléments XSD que ceux qui sont autorisés dans le fichier **`ejb-jar.xml`** pour la version 3.1 du descripteur de déploiement ejb-jar. Comme ils se reposent sur les bibliothèques standard d'interceptor Jave EE, les intercepteurs de conteneur peuvent uniquement être configurés à l'aide de descripteurs de déploiement. Cela a été conçu pour que les applications n'exigent pas une annotation spécifique de JBoss ou autre dépendance de bibliothèque. Pour plus d'informations sur les intercepteurs de conteneur, voir : Section 7.6.1, « Intercepteurs de conteneurs » .

Procédure 7.10. Créer le fichier de descripteur pour configurer l'intercepteur de conteneur

1. Créer un fichier **`jboss-ejb3.xml`** dans le répertoire **`META-INF`** du déploiement EJB.
2. Configurer les éléments de l'intercepteur du conteneur dans le fichier du descripteur.
   a. Utiliser l'espace-nom **`urn:container-interceptors:1.0`** pour indiquer la configuration des éléments de l'intercepteur du conteneur.
   b. Utiliser l'élément **`<container-interceptors>`** pour indiquer les intercepteurs du conteneur.
   c. Utiliser les éléments **`<interceptor-binding>`** pour relier l'intercepteur du conteneur aux EJB. Les intercepteurs peuvent être reliés d'une des manières suivantes :
      - Relier l'intercepteur à tous les EJB du déploiement par le caractère générique **`*`**.
      - Relier l'intercepteur au niveau bean individuel par le nom spécifique de l'EJB.
      - Relier l'intercepteur au niveau de méthode spécifique des EJB.

NOTE

Ces éléments sont configurés par EJB 3.1 XSD de la même façon que pour les intercepteurs Java EE.

3. Vérifier les exemples d'éléments ci-dessus dans le fichier de descripteur suivant.

Exemple 7.2. jboss-ejb3.xml

```
<jboss xmlns="http://www.jboss.com/xml/ns/javaee"
       xmlns:jee="http://java.sun.com/xml/ns/javaee"
       xmlns:ci ="urn:container-interceptors:1.0">

    <jee:assembly-descriptor>
        <ci:container-interceptors>
            <!-- Default interceptor -->
            <jee:interceptor-binding>
                <ejb-name>*</ejb-name>
                <interceptor-
class>org.jboss.as.test.integration.ejb.container.interceptor.Cont
ainerInterceptorOne</interceptor-class>
            </jee:interceptor-binding>
            <!-- Class level container-interceptor -->
            <jee:interceptor-binding>
                <ejb-name>AnotherFlowTrackingBean</ejb-name>
                <interceptor-
class>org.jboss.as.test.integration.ejb.container.interceptor.Clas
sLevelContainerInterceptor</interceptor-class>
            </jee:interceptor-binding>
            <!-- Method specific container-interceptor -->
            <jee:interceptor-binding>
                <ejb-name>AnotherFlowTrackingBean</ejb-name>
                <interceptor-
class>org.jboss.as.test.integration.ejb.container.interceptor.Meth
```

```
odSpecificContainerInterceptor</interceptor-class>
                <method>
                    <method-
name>echoWithMethodSpecificContainerInterceptor</method-name>
                </method>
            </jee:interceptor-binding>
            <!-- container interceptors in a specific order -->
            <jee:interceptor-binding>
                <ejb-name>AnotherFlowTrackingBean</ejb-name>
                <interceptor-order>
                    <interceptor-
class>org.jboss.as.test.integration.ejb.container.interceptor.Clas
sLevelContainerInterceptor</interceptor-class>
                    <interceptor-
class>org.jboss.as.test.integration.ejb.container.interceptor.Meth
odSpecificContainerInterceptor</interceptor-class>
                    <interceptor-
class>org.jboss.as.test.integration.ejb.container.interceptor.Cont
ainerInterceptorOne</interceptor-class>
                </interceptor-order>
                <method>
                    <method-
name>echoInSpecificOrderOfContainerInterceptors</method-name>
                </method>
            </jee:interceptor-binding>
        </ci:container-interceptors>
    </jee:assembly-descriptor>
</jboss>
```

L'XSD de l'espace-nom **`urn:container-interceptors:1.0`** se trouve dans ***`EAP_HOME`*`/docs/schema/jboss-ejb-container-interceptors_1_0.xsd`**.

Report a bug

7.6.4. Modifier l'identité du contexte de sécurité

Résumé

Par défaut, lorsque vous effectuez un appel distant à un EJB déployé sur le serveur d'applications, la connexion au serveur est authentifiée et toute demande reçue via cette connexion sera exécutée tant qu'identité qui a authentifié la connexion. Cela est vrai pour les appels client-serveur et serveur-serveur. Si vous avez besoin d'utiliser différentes identités de la part d'un même client, vous devrez normalement ouvrir des connexions multiples au serveur afin que chacune d'entre elles soient authentifiée en tant qu'identité différente. Plutôt que d'ouvrir plusieurs connexions de client, vous pouvez donner l'autorisation à l'utilisateur authentifié d'exécuter une requête sous un nom différent.

Cette section décrit comment changer d'identité sur une connexion client existante. Voir le Quickstart **`ejb-security-interceptors`** pour obtenir un exemple complet. Les exemples de code suivants sont des versions abrégées du code du Quickstart.

Procédure 7.11. Modifier l'identité du contexte de sécurité

Pour modifier l'identité d'une connexion sécurisée, vous devez créer les 3 composants suivants.

1. **Créer l'intercepteur côté client**
   Cet intercepteur doit implémenter **`org.jboss.ejb.client.EJBClientInterceptor`**. L'intercepteur doit passer l'identité requise par le mappage de données contextuelles, par l'intermédiaire d'un appel **`EJBClientInvocationContext.getContextData()`**. Voici un exemple de code d'intercepteur côté client :

```
public class ClientSecurityInterceptor implements
EJBClientInterceptor {

    public void handleInvocation(EJBClientInvocationContext context)
throws Exception {
        Principal currentPrincipal =
SecurityActions.securityContextGetPrincipal();

        if (currentPrincipal != null) {
            Map<String, Object> contextData =
context.getContextData();

contextData.put(ServerSecurityInterceptor.DELEGATED_USER_KEY,
currentPrincipal.getName());
        }
        context.sendRequest();
    }

    public Object handleInvocationResult(EJBClientInvocationContext
context) throws Exception {
        return context.getResult();
    }
}
```

   Les applications utilisateur peuvent alors se connecter à l'intercepteur dans le **`EJBClientContext`** par l'un des moyens suivants :

   - **Par programmation**
     Par cette approche, vous appelez l'API **`org.jboss.ejb.client.EJBClientContext.registerInterceptor(int order, EJBClientInterceptor interceptor)`** et passez **`order`** et l'instance **`interceptor`**. Le **`order`** est utilisé pour déterminer où exactement cet **`interceptor`** est placé dans la chaîne d'intercepteur du client.

   - **Mécanisme ServiceLoader**
     Cette approche nécessite la création d'un fichier **`META-INF/services/org.jboss.ejb.client.EJBClientInterceptor`** et le placer ou le conditionneur dans le chemin de classe de l'application client. Les règles du fichier sont dictées par le Java ServiceLoader Mechanism. Ce fichier devrait contenir, dans chaque ligne distincte, le nom de classe qualifié complet de l'implémentation d'intercepteur de client EJB. Les classes d'intercepteur de client EJB doivent être disponibles dans le chemin de classe. Les intercepteurs de client EJB ajoutés en utilisant le mécanisme de **`ServiceLoader`** sont ajoutés à la fin de la chaîne d'intercepteur de client, dans l'ordre dans lequel ils se trouvent dans le chemin de classe (classpath). Le démarrage rapide ou quickstart **`ejb-security-interceptors`** utilise cette approche.

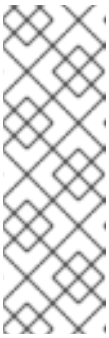
2. **Créer et configurer l'intercepteur du conteneur côté serveur**
   Les classes d'intercepteur de conteneur sont de simples Plain Old Java Objects (POJOs). Elles

utilisent **`@javax.annotation.AroundInvoke`** pour marquer la méthode qui sera invoquée lors de l'invocation sur le bean. Pour plus d'informations sur les intercepteurs de conteneur, consulter : Section 7.6.1, « Intercepteurs de conteneurs ».

a. **Créer l'intercepteur de conteneur**
Cet intercepteur reçoit le **`InvocationContext`** en même temps que l'identité et demande le changement. Ce qui suit est une version modifiée de l'exemple de code :

```
    public class ServerSecurityInterceptor {

        private static final Logger logger =
Logger.getLogger(ServerSecurityInterceptor.class);
        static final String DELEGATED_USER_KEY =
ServerSecurityInterceptor.class.getName() + ".DelegationUser";

        @AroundInvoke
        public Object aroundInvoke(final InvocationContext
invocationContext) throws Exception {
            Principal desiredUser = null;
            RealmUser connectionUser = null;

            Map<String, Object> contextData =
invocationContext.getContextData();
            if (contextData.containsKey(DELEGATED_USER_KEY)) {
                desiredUser = new SimplePrincipal((String)
contextData.get(DELEGATED_USER_KEY));
                Connection con =
SecurityActions.remotingContextGetConnection();
                if (con != null) {
                    UserInfo userInfo = con.getUserInfo();
                    if (userInfo instanceof SubjectUserInfo) {
                        SubjectUserInfo sinfo =
(SubjectUserInfo) userInfo;
                        for (Principal current :
sinfo.getPrincipals()) {
                            if (current instanceof RealmUser) {
                                connectionUser = (RealmUser)
current;
                                break;
                            }
                        }
                    }
                } else {
                    throw new IllegalStateException("Delegation
user requested but no user on connection found.");
                }
            }

            SecurityContext cachedSecurityContext = null;
            boolean contextSet = false;
            try {
                if (desiredUser != null && connectionUser !=
null
                        &&
(desiredUser.getName().equals(connectionUser.getName()) ==
false)) {
```

```
                    // The final part of this check is to verify
that the change does actually indicate a change in user.
                    try {
                        // We have been requested to switch user
and have successfully identified the user from the connection
                        // so now we attempt the switch.
                        cachedSecurityContext =
SecurityActions.securityContextSetPrincipalInfo(desiredUser,
                                new
OuterUserCredential(connectionUser));
                        // keep track that we switched the
security context
                        contextSet = true;
                        SecurityActions.remotingContextClear();
                    } catch (Exception e) {
                        logger.error("Failed to switch security
context for user", e);
                        // Don't propagate the exception
stacktrace back to the client for security reasons
                        throw new EJBAccessException("Unable to
attempt switching of user.");
                    }
                }
                return invocationContext.proceed();
            } finally {
                // switch back to original security context
                if (contextSet) {

SecurityActions.securityContextSet(cachedSecurityContext);
                }
            }
        }
    }
```



NOTE

L'exemple de code ci-dessus utilise deux classes, org.jboss.as.controller.security.SubjectUserInfo et org.jboss.as.domain.management.security.RealmUser, qui font partie de l'API privée de JBoss EAP. Une API publique deviendra disponible dans la version EAP 6.3 et les classes privées seront obsolètes, mais ces classes seront entretenues et rendues disponible pendant toute la durée du cycle de version EAP 6.x.

b. **Configurer l'intercepteur de conteneur**
Pour plus d'informations sur la façon de configurer les intercepteurs de conteneurs côté serveur, consulter : Section 7.6.3, « Configurer un intercepteur de conteneur ».

3. **JAAS LoginModule**
Ce composant doit vérifier que l'utilisateur est en mesure d'exécuter les requêtes suivant l'identité de la requête. Les exemples de code suivants indiquent les méthodes de login et de validation :

```
@SuppressWarnings("unchecked")
@Override
```

```
public boolean login() throws LoginException {
    if (super.login() == true) {
        log.debug("super.login()==true");
        return true;
    }

    // Time to see if this is a delegation request.
    NameCallback ncb = new NameCallback("Username:");
    ObjectCallback ocb = new ObjectCallback("Password:");

    try {
        callbackHandler.handle(new Callback[] { ncb, ocb });
    } catch (Exception e) {
        if (e instanceof RuntimeException) {
            throw (RuntimeException) e;
        }
        return false; // If the CallbackHandler can not handle the
required callbacks then no chance.
    }
    String name = ncb.getName();
    Object credential = ocb.getCredential();
    if (credential instanceof OuterUserCredential) {
        // This credential type will only be seen for a delegation
request, if not seen then the request is not for us.
        if (delegationAcceptable(name, (OuterUserCredential)
credential)) {
            identity = new SimplePrincipal(name);
            if (getUseFirstPass()) {
                String userName = identity.getName();
                if (log.isDebugEnabled())
                    log.debug("Storing username '" + userName + "'
and empty password");
                // Add the username and an empty password to the
shared state map
                sharedState.put("javax.security.auth.login.name",
identity);

sharedState.put("javax.security.auth.login.password", "");
            }
            loginOk = true;
            return true;
        }
    }
    return false; // Attempted login but not successful.
}
```

```
protected boolean delegationAcceptable(String requestedUser,
OuterUserCredential connectionUser) {
    if (delegationMappings == null) {
        return false;
    }

    String[] allowedMappings =
loadPropertyValue(connectionUser.getName(),
connectionUser.getRealm());
```

```
    if (allowedMappings.length == 1 &&
"*".equals(allowedMappings[1])) {
        // A wild card mapping was found.
        return true;
    }
    for (String current : allowedMappings) {
        if (requestedUser.equals(current)) {
            return true;
        }
    }
    return false;
}
```

Voir le fichier Quickstart **README** pour obtenir des instructions complètes et des informations détaillées sur le code.

Report a bug

7.6.5. Sécurité supplémentaire pour l'authentification EJB

Résumé

Par défaut, lorsque vous effectuez un appel distant à un EJB déployé sur le serveur d'applications, la connexion au serveur est authentifiée et toute demande reçue via cette connexion est exécutée en utilisant les informations d'identification qui ont authentifié la connexion. L'authentification au niveau de la connexion dépend des capacités des mécanismes sous-jacents SASL (Simple Authentication and Security Layer). Plutôt que d'écrire des mécanismes SASL personnalisés, vous pouvez ouvrir et authentifier une connexion au serveur, puis plus tard ajouter les jetons de sécurité supplémentaires avant d'appeler un EJB. Cette rubrique décrit comment passer des informations supplémentaires sur la connexion existante du client pour l'authentification de l'EJB.

Les exemples de code ci-dessous sont uniquement à des fins de démonstration. Ils ne présentent qu'une approche possible et doivent être personnalisés pour répondre aux besoins précis de l'application. Le mot de passe est échangé par le mécanisme SASL. Si l'authentification DIGEST-MD5 SASL est utilisée, le mot de passe est toujours haché avec difficulté et non clair. Toutefois, les jetons restants, eux, sont clairs. Si ces jetons contiennent des informations sensibles, vous pouvez activer le cryptage pour la connexion.

Procédure 7.12. Information de sécurité pour l'authentification EJB

Pour un token de sécurité supplémentaire de connexion authentifiée, vous devrez créer les 3 composants suivants.

1. **Créer l'intercepteur côté client**
   Cet intercepteur doit implémenter **`org.jboss.ejb.client.EJBClientInterceptor`**. L'intercepteur doit passer le token de sécurité supplémentaire par le mappage de données contextuelles, par l'intermédiaire d'un appel **`EJBClientInvocationContext.getContextData()`**. Voici un exemple de code d'intercepteur côté client qui crée un token de sécurité supplémentaire :

```
public class ClientSecurityInterceptor implements
EJBClientInterceptor {

    public void handleInvocation(EJBClientInvocationContext context)
throws Exception {
```

```
        Object credential =
SecurityActions.securityContextGetCredential();

        if (credential != null && credential instanceof
PasswordPlusCredential) {
            PasswordPlusCredential ppCredential =
(PasswordPlusCredential) credential;
            Map<String, Object> contextData =
context.getContextData();

contextData.put(ServerSecurityInterceptor.SECURITY_TOKEN_KEY,
                                ppCredential.getAuthToken());
        }
        context.sendRequest();
    }

    public Object handleInvocationResult(EJBClientInvocationContext
context)
            throws Exception {
        return context.getResult();
    }
}
```

Pour obtenir des informations sur la façon de connecter l'intercepteur client dans une application, voir Section 7.6.6, « Utiliser un intercepteur côté client dans une application ».

2. **Créer et configurer l'intercepteur du conteneur côté serveur**
   Les classes d'intercepteur de conteneur sont de simples Plain Old Java Objects (POJOs). Elles utilisent **`@javax.annotation.AroundInvoke`** pour marquer la méthode qui est invoquée lors de l'invocation sur le bean. Pour plus d'informations sur les intercepteurs de conteneur, consulter : Section 7.6.1, « Intercepteurs de conteneurs ».

   a. **Créer l'intercepteur de conteneur**
      Cet intercepteur récupère le jeton d'authentification de sécurité du contexte et le passe au domaine JAAS (Java Authentication and Autorisation Service) pour vérification. Voici un exemple de code d'intercepteur de conteneur :

```
public class ServerSecurityInterceptor {

    private static final Logger logger =
Logger.getLogger(ServerSecurityInterceptor.class);
    static final String SECURITY_TOKEN_KEY =
ServerSecurityInterceptor.class.getName() + ".SecurityToken";

    @AroundInvoke
    public Object aroundInvoke(final InvocationContext
invocationContext) throws Exception {
        Principal userPrincipal = null;
        RealmUser connectionUser = null;
        String authToken = null;

        Map<String, Object> contextData =
invocationContext.getContextData();
        if (contextData.containsKey(SECURITY_TOKEN_KEY)) {
            authToken = (String)
```

```
contextData.get(SECURITY_TOKEN_KEY);

            Connection con =
SecurityActions.remotingContextGetConnection();

            if (con != null) {
                UserInfo userInfo = con.getUserInfo();
                if (userInfo instanceof SubjectUserInfo) {
                    SubjectUserInfo sinfo = (SubjectUserInfo)
userInfo;
                    for (Principal current :
sinfo.getPrincipals()) {
                        if (current instanceof RealmUser) {
                            connectionUser = (RealmUser)
current;
                            break;
                        }
                    }
                }
                userPrincipal = new
SimplePrincipal(connectionUser.getName());

            } else {
                throw new IllegalStateException("Token
authentication requested but no user on connection found.");
            }
        }

        SecurityContext cachedSecurityContext = null;
        boolean contextSet = false;
        try {
            if (userPrincipal != null && connectionUser != null
&& authToken != null) {
                try {
                    // We have been requested to use an
authentication token
                    // so now we attempt the switch.
                    cachedSecurityContext =
SecurityActions.securityContextSetPrincipalCredential(userPrincip
al,
                            new
OuterUserPlusCredential(connectionUser, authToken));
                    // keep track that we switched the security
context
                    contextSet = true;
                    SecurityActions.remotingContextClear();
                } catch (Exception e) {
                    logger.error("Failed to switch security
context for user", e);
                    // Don't propagate the exception stacktrace
back to the client for security reasons
                    throw new EJBAccessException("Unable to
attempt switching of user.");
                }
            }
```

```
            return invocationContext.proceed();
        } finally {
            // switch back to original security context
            if (contextSet) {

SecurityActions.securityContextSet(cachedSecurityContext);
            }
        }
    }
}
```

NOTE

L'exemple de code ci-dessus utilise deux classes, org.jboss.as.controller.security.SubjectUserInfo et org.jboss.as.domain.management.security.RealmUser, qui font partie de l'API privée de JBoss EAP. Une API publique sera rendue disponible dans la version EAP 6.3 et les classes privées seront obsolètes, mais ces classes seront entretenues et rendues disponible pendant toute la durée du cycle de version EAP 6.x.

b. **Configurer l'intercepteur du conteneur**
Pour plus d'informations sur la façon de configurer les intercepteurs de conteneurs côté serveur, consulter: Section 7.6.3, « Configurer un intercepteur de conteneur ».

3. **Créer le JAAS LoginModule**
Ce module personnalisé exécute l'authentification à l'aide de l'information de la connexion authentifiée existante ainsi qu'à l'aide qu'un jeton de sécurité supplémentaire. Voici un exemple de code qui utilise le jeton de sécurité supplémentaire et qui exécute l'authentification :

```
public class SaslPlusLoginModule extends AbstractServerLoginModule {

    private static final String ADDITIONAL_SECRET_PROPERTIES =
"additionalSecretProperties";
    private static final String DEFAULT_AS_PROPERTIES = "additional-
secret.properties";
    private Properties additionalSecrets;
    private Principal identity;

    @Override
    public void initialize(Subject subject, CallbackHandler
callbackHandler, Map<String, ?> sharedState, Map<String, ?> options)
{
        addValidOptions(new String[] { ADDITIONAL_SECRET_PROPERTIES
});
        super.initialize(subject, callbackHandler, sharedState,
options);

        // Load the properties that contain the additional security
tokens
        String propertiesName;
        if (options.containsKey(ADDITIONAL_SECRET_PROPERTIES)) {
            propertiesName = (String)
```

```
options.get(ADDITIONAL_SECRET_PROPERTIES);
        } else {
            propertiesName = DEFAULT_AS_PROPERTIES;
        }
        try {
            additionalSecrets =
SecurityActions.loadProperties(propertiesName);
        } catch (IOException e) {
            throw new
IllegalArgumentException(String.format("Unable to load properties
'%s'", propertiesName), e);
        }
    }

    @Override
    public boolean login() throws LoginException {
        if (super.login() == true) {
            log.debug("super.login()==true");
            return true;
        }

        // Time to see if this is a delegation request.
        NameCallback ncb = new NameCallback("Username:");
        ObjectCallback ocb = new ObjectCallback("Password:");

        try {
            callbackHandler.handle(new Callback[] { ncb, ocb });
        } catch (Exception e) {
            if (e instanceof RuntimeException) {
                throw (RuntimeException) e;
            }
            return false; // If the CallbackHandler can not handle
the required callbacks then no chance.
        }

        String name = ncb.getName();
        Object credential = ocb.getCredential();

        if (credential instanceof OuterUserPlusCredential) {
            OuterUserPlusCredential oupc = (OuterUserPlusCredential)
credential;
            if (verify(name, oupc.getName(), oupc.getAuthToken())) {
                identity = new SimplePrincipal(name);
                if (getUseFirstPass()) {
                    String userName = identity.getName();
                    if (log.isDebugEnabled())
                        log.debug("Storing username '" + userName +
"' and empty password");
                    // Add the username and an empty password to
the shared state map

sharedState.put("javax.security.auth.login.name", identity);

sharedState.put("javax.security.auth.login.password", oupc);
                }
                loginOk = true;
```

```
                return true;
            }
        }

        return false; // Attempted login but not successful.
    }

    private boolean verify(final String authName, final String
connectionUser, final String authToken) {
        // For the purpose of this quick start we are not supporting
switching users, this login module is validation an
        // additional security token for a user that has already
passed the sasl process.
        return authName.equals(connectionUser) &&
authToken.equals(additionalSecrets.getProperty(authName));
    }

    @Override
    protected Principal getIdentity() {
        return identity;
    }

    @Override
    protected Group[] getRoleSets() throws LoginException {
        Group roles = new SimpleGroup("Roles");
        Group callerPrincipal = new SimpleGroup("CallerPrincipal");
        Group[] groups = { roles, callerPrincipal };
        callerPrincipal.addMember(getIdentity());
        return groups;
    }
}
```

4. **Ajouter le LoginModule personnalisé à la chaîne**
   Vous devez ajouter le nouveau LoginModule personnalisé à l'endroit qui convient dans la chaîne pour qu'il soit invoqué dans le bon ordre. Dans cet exemple, le **`SaslPlusLoginModule`** doit être mis dans la chaîne avant le LoginModule qui charge les rôles par l'option **`password-stacking`** .

   - **Configurer l'ordonnancement du LoginModule par le Management CLI**
     Ce qui suit est un exemple de commandes de Management CLI qui enchaînent le **`SaslPlusLoginModule`** personnalisé avant le LoginModule **`RealmDirect`** qui définit l'option **`password-stacking`**.

     ```
     [standalone@localhost:9999 /] ./subsystem=security/security-
     domain=quickstart-domain:add(cache-
     type=default)[standalone@localhost:9999 /]
     ./subsystem=security/security-domain=quickstart-
     domain/authentication=classic:add[standalone@localhost:9999 /]
     ./subsystem=security/security-domain=quickstart-
     domain/authentication=classic/login-
     module=DelegationLoginModule:add(code=org.jboss.as.quickstarts.ej
     b_security_plus.SaslPlusLoginModule,flag=optional,module-options=
     {password-stacking=useFirstPass})[standalone@localhost:9999 /]
     ./subsystem=security/security-domain=quickstart-
     domain/authentication=classic/login-
     ```

```
module=RealmDirect:add(code=RealmDirect,flag=required,module-
options={password-stacking=useFirstPass})
```

Pour plus d'informations sur le Management CLI, voir le chapitre intitulé *Management Interfaces* du guide *Administration and Configuration Guide*de JBoss EAP 6 qui se trouve sur le Portail Clients https://access.redhat.com/site/documentation/JBoss_Enterprise_Application_Platform/

- **Configurer l'ordonnancement du LoginModule manuellement**
  Ce qui suit est un exemple de XML qui configure l'ordonnancement du LoginModule dans le sous-système de **`security`** du fichier de configuration du serveur. Le **`SaslPlusLoginModule`** doit précéder le LoginModule **`RealmDirect`** pour qu'il puisse vérifier l'utilisateur distant avant que les rôles utilisateurs ne soient chargés et l'option **`password-stacking`** définie.

```
<security-domain name="quickstart-domain" cache-type="default">
    <authentication>
        <login-module
code="org.jboss.as.quickstarts.ejb_security_plus.SaslPlusLoginMod
ule" flag="required">
            <module-option name="password-stacking"
value="useFirstPass"/>
        </login-module>
        <login-module code="RealmDirect" flag="required">
            <module-option name="password-stacking"
value="useFirstPass"/>
        </login-module>
    </authentication>
</security-domain>
```

5. **Créer le client distant**
   Dans l'exemple de code suivant, on assume que le fichier **`additional-secret.properties`** auquel accède le JAAS LoginModule ci-dessus contient la propriété suivante :

```
quickstartUser=7f5cc521-5061-4a5b-b814-bdc37f021acc
```

Le code suivant montre comment créer un token de sécurité et comment le définir avant l'appel EJB. Le token secret est codé en dur dans des buts de démonstration uniquement. Ce client se contente d'afficher les résultats sur la console.

```
import static
org.jboss.as.quickstarts.ejb_security_plus.EJBUtil.lookupSecuredEJB;

public class RemoteClient {

    /**
     * @param args
     */
    public static void main(String[] args) throws Exception {
        SimplePrincipal principal = new
```

```
SimplePrincipal("quickstartUser");
        Object credential = new
PasswordPlusCredential("quickstartPwd1!".toCharArray(), "7f5cc521-
5061-4a5b-b814-bdc37f021acc");


SecurityActions.securityContextSetPrincipalCredential(principal,
credential);
        SecuredEJBRemote secured = lookupSecuredEJB();

        System.out.println(secured.getPrincipalInformation());
    }
}
```

Report a bug

7.6.6. Utiliser un intercepteur côté client dans une application

Résumé

Vous pouvez connecter un intercepteur côté client dans une application par programmation ou en utilisant un mécanisme ServiceLoader. La procédure suivante décrit les deux méthodes.

Procédure 7.13. Connecter l'intercepteur

- **Par programmation**
  Par cette approche, vous appelez l'API **`org.jboss.ejb.client.EJBClientContext.registerInterceptor(int order, EJBClientInterceptor interceptor)`** et passez l'instance **`order`** et l'instance **`interceptor`**. L'instance **`order`** est utilisé pour déterminer où exactement cet **`interceptor`** est placé dans la chaîne d'intercepteur du client.

- **Mécanisme ServiceLoader**
  Cette approche nécessite la création d'un fichier **`META-INF/services/org.jboss.ejb.client.EJBClientInterceptor`** et le placer ou le conditionner dans le chemin de classe de l'application client. Les règles du fichier sont dictées par le Java ServiceLoader Mechanism. Ce fichier devrait contenir, dans chaque ligne distincte, le nom de classe qualifié complet de l'implémentation d'intercepteur de client EJB. Les classes d'intercepteur de client EJB doivent être disponibles dans le chemin de classe. Les intercepteurs de client EJB ajoutés en utilisant le mécanisme de **`ServiceLoader`** sont ajoutés à la fin de la chaîne d'intercepteur de client, dans l'ordre dans lequel ils se trouvent dans le chemin de classe.

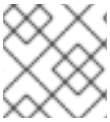
Report a bug

7.7. JAVABEANS ENTERPRISE CLUSTERISÉS

7.7.1. JavaBeans clusterisées (EJB)

Les composants EJB peuvent être clusterisés dans les scénarios de haute disponibilité. Ils utilisent différents protocoles HTTP, donc ils doivent être clusterisés différemment. Les beans avec ou sans état EJB 2 et 3 peuvent être clusterisés.

Pour plus d'informations sur les singletons, veuillez consulter : Section 8.4, « Implémenter un HA Singleton ».



NOTE

Les bean d'entité EJB 2 ne peuvent pas être clusterisés.

Report a bug

7.8. RÉFÉRENCE

7.8.1. Référence de nommage EJB JNDI

Le nom de recherche JNDI d'une session bean a la syntaxe suivante :

```
 ejb:<appName>/<moduleName>/<distinctName>/<beanName>!<viewClassName>?
stateful
```

<appName>

Si le fichier JAR du session bean a été déployé dans une EAR, alors voici le nom de cette EAR. Par défaut, le nom d'un EAR correspond à son nom de fichier sans le suffixe **.ear**. Le nom de l'application peut également être remplacé dans son fichier **application.xml**. Si le bean de session n'est pas déployé dans un EAR, laisser le vide.

<moduleName>

Le nom du module correspond au nom du fichier dans lequel le session bean est déployé. Par défaut, le nom du fichier JAR correspond à son nom de fichier sans le suffixe **.jar**. Le nom du module peut également être remplacé par le **ejb-jar.xml** du JAR.

<distinctName>

JBoss EAP 6 permet à chaque déploiement de spécifier un nom distinct en option. Si le déploiement n'a pas de nom distinct, laisser le vide.

<beanName>

Le nom du bean est le nom de classe de la session bean à invoquer.

<viewClassName>

Le nom de classe de vue est le nom de classe complet de l'interface distante de l'interface distante. Inclut le nom du package de l'interface.

?stateful

Le suffixe **?stateful** est requis quand le nom JNDI se réfère à un bean de session stateful. Non inclus dans d'autres types de bean.

Report a bug

7.8.2. Résolution de référence EJB

Cette section explique comment JBoss implémente **@EJB** et **@Resource**. Veuillez noter qu'XML remplace toujours les annotations, mais que les mêmes règles s'appliquent.

Règles pour les annotations @EJB

- L'annotation **@EJB** possède également un attribut **mappedName()**. La spécification le considère comme une métadonnée spécifique au fournisseur tandis que JBoss reconnait **mappedName()** en tant que nom JNDI global du EJB que vous référencez. Si vous avez indiqué un **mappedName()**, alors tous les autres attributs seront ignorés et ce nom JNDI global sera utilisé comme liaison.
- Si vous indiquez **@EJB** sans attributs définis :

  ```
  @EJB
  ProcessPayment myEjbref;
  ```

  Alors les règles suivantes vont s'appliquer :

  - Le jar EJB du bean de référencement est analysé pour trouver un EJB avec l'interface, utilisée dans l'injection **@EJB**. S'il existe plus d'un EJB qui publie la même interface commerciale, alors une exception apparaîtra. S'il n'y a qu'un seul bean dans cette interface, alors celui-là sera utilisé.
  - Chercher l'EAR des EJB qui publient cette interface. S'il y a des doubles, alors il y aura une exception. Sinon le bean correspondant sera renvoyé.
  - Chercher globalement dans le runtime de JBoss un EJB de cette interface. Une fois de plus, s'il y a des doubles, il y aura une exception.
- **@EJB.beanName()** correspond à **<ejb-link>**. Si le **beanName()** est défini, il vous faudra utiliser le même algorithme que **@EJB** sans attribut défini mis à part **beanName()** comme une clé de la recherche. Il existe une exception à cette règle si vous utilisez la syntaxe ejb-link '#'. La syntaxe '#' vous permettra de mettre un chemin d'accès relatif dans un jar de l'EJB qui contient l'EJB de référencement. Reportez-vous à la spécification EJB 3.1 pour plus de détails.

Report a bug

7.8.3. Dépendances de projet pour les clients EJB distants

Les projets Maven qui incluent l'invocation de session beans de clients éloignés ont besoin des dépendances suivantes du référentiel JBoss EAP 6 Maven.

Tableau 7.4. Dépendances Maven pour les clients EJB

GroupID	ArtifactID
org.jboss.spec	jboss-javaee-6.0
org.jboss.as	jboss-as-ejb-client-bom
org.jboss.spec.javax.transaction	jboss-transaction-api_1.1_spec
org.jboss.spec.javax.ejb	jboss-ejb-api_3.1_spec

GroupID	ArtifactID
org.jboss	jboss-ejb-client
org.jboss.xnio	xnio-api
org.jboss.xnio	xnio-nio
org.jboss.remoting3	jboss-remoting
org.jboss.sasl	jboss-sasl
org.jboss.marshalling	jboss-marshalling-river

A l'exception de **`jboss-javaee-6.0`** et **`jboss-as-ejb-client-bom`**, ces dépendances doivent être ajoutées à la section **`<dependencies>`** du fichier **`pom.xml`**.

Les dépendances **`jboss-javaee-6.0`** et **`jboss-as-ejb-client-bom`** doivent être ajoutées à la section **`<dependencyManagement>`** du fichier **`pom.xml`** avec l'étendue de **`import`**.

NOTE

Les versions de **`artifactID`** peuvent être modifiées. Veuillez consulter le référentiel Maven pour connaître la version la plus récente.

```
<dependencyManagement>
   <dependencies>
      <dependency>
         <groupId>org.jboss.spec</groupId>
         <artifactId>jboss-javaee-6.0</artifactId>
         <version>3.0.0.Final-redhat-1</version>
         <type>pom</type>
         <scope>import</scope>
      </dependency>

      <dependency>
         <groupId>org.jboss.as</groupId>
         <artifactId>jboss-as-ejb-client-bom</artifactId>
         <version>7.1.1.Final-redhat-1</version>
         <type>pom</type>
         <scope>import</scope>
      </dependency>
   </dependencies>
</dependencyManagement>
```

Voir **`remote-ejb/client/pom.xml`** pour obtenir un exemple complet de configuration de dépendance pour une invocation de session bean éloignée.

Report a bug

7.8.4. Référence de descripteur de déploiement jboss-ejb3.xml

jboss-ejb3.xml est un descripteur de déploiement personnalisé pouvant être utilisé dans un JAR EJB ou des archives WAR. Dans une archive JAR EJB il doit être situé dans le répertoire **META-INF/**. Dans une archive WAR, il doit être situé dans le répertoire **WEB-INF/**.

Le format ressemble à **ejb-jar.xml**, qui utilise les mêmes espace-noms et qui fournit des espace-noms supplémentaires. Les contenus de **jboss-ejb3.xml** sont mergés avec les contenus de **ejb-jar.xml**, et les items **jboss-ejb3.xml** ont la priorité.

Ce document ne couvre que les espace-noms supplémentaires non-standard utilisés par **jboss-ejb3.xml**. Voir http://java.sun.com/xml/ns/javaee/ pour la documentation sur les espace-noms standard.

L'espace-nom root est **http://www.jboss.com/xml/ns/javaee**.

Espace-nom de descripteur d'assemblage

Les espace-noms suivants peuvent être utilisés dans l'élément **<assembly-descriptor>** . Ils peuvent être utilisés pour appliquer leur configuration à un simple bean, ou à tous les beans du déploiement en utilisant ***** comme **ejb-name**.

Espace-nom de clustering : urn:clustering:1.0

```
xmlns:c="urn:clustering:1.0"
```

Cela vous permet de marquer les EJB comme étant clusterisés. Il s'agit du descripteur de déploiement équivalent au **@org.jboss.ejb3.annotation.Clustered**.

```
<c:clustering>
   <ejb-name>DDBasedClusteredSFSB</ejb-name>
   <c:clustered>true</c:clustered>
</c:clustering>
```

L'espace-nom de sécurité (urn:security)

```
xmlns:s="urn:security"
```

Cela vous permet de définir le domaine de sécurité et le principal prétendant pour l'EJB.

```
<s:security>
  <ejb-name>*</ejb-name>
  <s:security-domain>myDomain</s:security-domain>
  <s:run-as-principal>myPrincipal</s:run-as-principal>
</s:security>
```

L'espace-nom d'adaptateur de ressource : urn:resource-adapter-binding

```
xmlns:r="urn:resource-adapter-binding"
```

Cela vous permet de définir l'adaptateur de ressource d'un Message-Driven Bean.

```
<r:resource-adapter-binding>
```

```
  <ejb-name>*</ejb-name>
  <r:resource-adapter-name>myResourceAdaptor</r:resource-adapter-name>
</r:resource-adapter-binding>
```

L'espace-nom IIOP : `urn:iiop`

```
xmlns:u="urn:iiop"
```

L'espace-nom IIOP est l'endroit où les paramètres IIOP sont configurés.

L'espace-nom du pool : `urn:ejb-pool:1.0`

```
xmlns:p="urn:ejb-pool:1.0"
```

Cela vous permet de sélectionner le pool qui est utilisé par les stateless session beans ou par les Message-Driven Beans. Les pools sont définis dans la configuration du serveur.

```
<p:pool>
   <ejb-name>*</ejb-name>
   <p:bean-instance-pool-ref>my-pool</p:bean-instance-pool-ref>
</p:pool>
```

L'espace-nom du cache : `urn:ejb-cache:1.0`

```
xmlns:c="urn:ejb-cache:1.0"
```

Cela vous permet de sélectionner le cache qui est utilisé par les stateful session beans inclus. Les caches sont définis dans la configuration du serveur.

```
<c:cache>
   <ejb-name>*</ejb-name>
   <c:cache-ref>my-cache</c:cache-ref>
</c:cache>
```

Exemple 7.3. Fichier exemple de jboss-ejb3.xml

```
<?xml version="1.1" encoding="UTF-8"?>
   <jboss:ejb-jar xmlns:jboss="http://www.jboss.com/xml/ns/javaee"
                  xmlns="http://java.sun.com/xml/ns/javaee"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  xmlns:c="urn:clustering:1.0"

xsi:schemaLocation="http://www.jboss.com/xml/ns/javaee
http://www.jboss.org/j2ee/schema/jboss-ejb3-2_0.xsd
http://java.sun.com/xml/ns/javaee http://java.sun.com/xml/ns/javaee/ejb-
jar_3_1.xsd"
                  version="3.1"
                  impl-version="2.0">
      <enterprise-beans>
         <message-driven>
            <ejb-name>ReplyingMDB</ejb-name>
            <ejb-
```

```
class>org.jboss.as.test.integration.ejb.mdb.messagedestination.ReplyingM
DB</ejb-class>
            <activation-config>
               <activation-config-property>
                  <activation-config-property-
name>destination</activation-config-property-name>
                  <activation-config-property-
value>java:jboss/mdbtest/messageDestinationQueue
                  </activation-config-property-value>
               </activation-config-property>
            </activation-config>
         </message-driven>
      </enterprise-beans>
      <assembly-descriptor>
         <c:clustering>
            <ejb-name>DDBasedClusteredSFSB</ejb-name>
            <c:clustered>true</c:clustered>
         </c:clustering>
      </assembly-descriptor>
   </jboss:ejb-jar>
```

Report a bug

CHAPITRE 8. CLUSTERING DANS LES APPLICATIONS WEB

8.1. RÉPLIQUE DE SESSION

8.1.1. La réplique de session HTTP

La réplique de session veille à ce que les sessions client d'applications distribuables ne soient pas interrompues par des défaillances de noeuds dans le système. Chaque noeud du cluster partage des informations sur les sessions en cours, et peut les récupérer si le noeud d'origine disparaît.

La réplique de session est un mécanisme par lequel les clusters mod_cluster, mod_jk, mod_proxy, ISAPI, et NSAPI procurent une haute disponibilité.

Report a bug

8.1.2. Cache de Session Web

Le cache de session web peut être configuré quand vous utilisez l'un des profils HA, dont le profil `standalone-ha.xml`, ou les profils de domaine gérés `ha` ou `full-ha`. Les éléments les plus couramment configurés sont le mode cache et le nombre de propriétaires de cache pour un cache distribué.

Mode Cache

Le mode cache peut être **REPL** (par défaut) ou **DIST**.

REPL

Le mode **REPL** reproduit tout le cache un nœud sur deux dans le cluster. Cela constitue l'option la plus sûre, mais elle introduit aussi plus de surcharge de temps.

DIST

Le mode **DIST** est semblable au *buddy mode* fourni dans les exécutions précédentes. Il réduit la surcharge de temps en répartissant le cache entre le nombre de nœuds indiqués dans le paramètre `owners`. Ce nombre de propriétaires est défini par défaut sur `2`.

Propriétaires

Le paramètre `owners` contrôle combien de nœuds de clusters détiennent des duplicatas de la session. La valeur par défaut est **2**.

Report a bug

8.1.3. Configurer le Cache de session web

Par défaut, le cache de session web est **REPL**. Si vous souhaitez utiliser le mode **DIST**, exécutez les deux commandes suivantes dans le Management CLI. Si vous utilisez un profil différent, changez le nom de profil dans les commandes. Si vous utilisez un serveur autonome, retirez la partie `/profile=ha` des commandes.

Procédure 8.1. Configurer le Cache de session web

1. **Modifier le mode cache par défaut en `DIST`.**
   –

```
/profile=ha/subsystem=infinispan/cache-container=web/:write-
attribute(name=default-cache,value=dist)
```

2. **Définir le nombre de propriétaires de cache distribué.**
   La commande suivante définit **5** propriétaires. La valeur par défaut est **2**.

```
/profile=ha/subsystem=infinispan/cache-container=web/distributed-
cache=dist/:write-attribute(name=owners,value=5)
```

3. **Modifier le mode cache par défaut en REPL.**

```
/profile=ha/subsystem=infinispan/cache-container=web/:write-
attribute(name=default-cache,value=repl)
```

4. **Relancer le serveur**
   Après avoir modifié le mode cache du web, vous devez relancer le serveur.

Résultat

Votre serveur est configuré pour une copie de session. Pour utiliser une copie de session dans vos propres applications, veuillez vous référer au sujet suivant : Section 8.1.4, « Activer la copie de session pour votre application ».

Report a bug

8.1.4. Activer la copie de session pour votre application

Résumé

Pour profiter des fonctionnalités HA (High Availability) de JBoss EAP 6, configurer votre application de manière à ce qu'elle soit distribuable. Cette procédure vous montrera comment y parvenir puis vous expliquera certaines options de configuration avancées que vous pourrez utiliser.

Procédure 8.2. Rendez votre Application Distribuable

1. **Prérequis : indiquer que votre application est distribuable**
   Si votre application n'apparaît pas comme distribuable, ses sessions ne seront jamais distribuées. Ajouter l'élément **<distributable />** dans la balise **<web-app>** du fichier descriptif **web.xml** de votre application. Voici un exemple :

Exemple 8.1. Configuration minimum pour une application distribuable

```
<?xml version="1.0"?>
<web-app  xmlns="http://java.sun.com/xml/ns/j2ee"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee

http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
          version="2.4">

      <distributable/>
```

```
</web-app>
```

2. **Modifier le comportement de réplication par défaut si vous le souhaitez.**
Si vous souhaitez changer une des valeurs qui affectent la réplique de session, vous pouvez les changer dans l'élément **<replication-config>** qui est un dépendant de l'élément **<jboss-web>**. Pour un exemple donné, ne l'inclure que si vous souhaitez remplacer les valeurs par défaut. L'exemple suivant énumère tous les paramètres par défaut, et est suivi d'un tableau qui explique les options les plus fréquemment modifiées.

Exemple 8.2. Valeurs <replication-config> par défaut

```
<!DOCTYPE jboss-web PUBLIC
    "-//JBoss//DTD Web Application 5.0//EN"
    "http://www.jboss.org/j2ee/dtd/jboss-web_5_0.dtd">

<jboss-web>

   <replication-config>
      <cache-name>custom-session-cache</cache-name>
      <replication-trigger>SET</replication-trigger>
      <replication-granularity>ATTRIBUTE</replication-
granularity>
      <use-jk>false</use-jk>
      <max-unreplicated-interval>30</max-unreplicated-interval>
      <snapshot-mode>INSTANT</snapshot-mode>
      <snapshot-interval>1000</snapshot-interval>
      <session-notification-
policy>com.example.CustomSessionNotificationPolicy</session-
notification-policy>
  </replication-config>

</jboss-web>
```

Tableau 8.1. Options communes pour la réplique de session

Option	Description

Option	Description
<replication-trigger>	Contrôle quelles conditions doivent déclencher la réplication de données de session dans l'ensemble du cluster. Cette option est utile, quand un objet mutable stocké comme attribut de session est accessible à partir de la session, le conteneur n'a aucun moyen évident de savoir si l'objet a été modifié et s'il doit être reproduit, sauf si la méthode **setAttribute()** est appelée directement. **Valeurs valides pour <replication-trigger>** **SET_AND_GET** Il s'agit de l'option la plus sécurisée, mais la moins performante. Les données de session sont toujours répliquées, même si on a accédé à son contenu sans l'avoir modifié. Cette configuration est préservée à but d'héritage uniquement. Éviter cette configuration et définir **<max_unreplicated_interval>** à 0, pour avoir le même comportement et une meilleure performance. **SET_AND_NON_PRIMITIVE_GET** La valeur par défaut. Les données de session ne sont répliquées que si on a accédé à un objet de type non primitif. Cela signifie que l'objet n'est pas d'un type Java connu comme **Integer**, **Long**, ou **String**. **SET** Cette option présume que l'application va explicitement appeler **setAttribute** sur la session quand les données auront besoin d'être répliquées. Cela empêche la réplication inutile et peut bénéficier à la performance dans son ensemble, mais il y a un problème de sécurité. Quelle que soit la configuration, vous pourrez toujours déclencher la réplication de session en appelant **setAttribute()**.
<replication-granularity>	Détermine la granularité des données répliquées. La valeur par défaut est **SESSION**, mais peut être définie à **ATTRIBUTE** à la place, pour augmenter la performance dans les sessions où la plupart des attributs restent inchangés.

Les options suivantes ont rarement besoin d'être modifiées.

Tableau 8.2. Options les moins communément modifiées pour les réplications de session

Option	Description
<useJK>	Présumons qu'un équilibreur de charge tel que **mod_cluster**, **mod_jk**, ou **mod_proxy** soit utilisé. La valeur par défaut est **false**. Si définie comme **true**, le conteneur examine l'ID de session associé à chaque requête et remplace la partie **jvmRoute** de l'ID de session s'il y a un basculement.

Option	Description
<max-unreplicated-interval>	Le plus grand intervalle (en secondes) à attendre après une session avant de déclencher une réplication d'un horodateur de session, même s'il est considéré comme inchangé. Cela permet aux nœuds de cluster d'être informés de l'horodateur de chaque session et aux sessions non répliquées de ne pas expirer de manière incorrecte pendant un basculement. Cela vous permet également de vous fier à une valeur correcte pour les appels à méthode **HttpSession.getLastAccessedTime()** pendant un baculement. Par défaut, aucune valeur n'est indiquée. Cela signifie que la configuration **jvmRoute** du conteneur détermine si le basculement JK est utilisé. Une valeur **0** entraîne une réplication de l'horodateur à chaque accès à la session. Une valeur **-1** n'entraîne une réplication de l'horodateur seulement si une autre activité pendant la requête entraîne une réplication. Une valeur positive supérieure à **HttpSession.getMaxInactiveInterval()** est traitée comme une erreur de configuration et convertie à **0**.
<snapshot-mode>	Indique quand les sessions sont répliquées vers d'autres nœuds. La valeur par défaut est **INSTANT** et l'autre valeur possible est **INTERVAL**. En mode **INSTANT**, les modifications sont répliquées à la fin d'une requête, au moyen du thread de traitement des requêtes. L'option **<snapshot-interval>** est ignorée. En mode **INTERVAL**, une tâche d'arrière-plan s'exécute à l'intervalle indiqué par **<snapshot-interval>**, et réplique les sessions modifiées.
<snapshot-interval>	L'intervalle, en millisecondes, pendant lequel les sessions modifiées doivent être répliquées si elles utilisent **INTERVAL** pour la valeur de **<snapshot-mode>**.
<session-notification-policy>	Nom complet de la classe de l'implémentation de l'interface **ClusteredSessionNotificationPolicy** qui contrôle si les notifications de spécification servlet sont émises vers un **HttpSessionListener**, **HttpSessionAttributeListener**, ou **HttpSessionBindingListener** enregistré.

Report a bug

8.2. PASSIVATION ET ACTIVATION HTTPSESSION

8.2.1. La passivation et l'activation de session HTTP

La *Passivation* est le processus de contrôle de l'utilisation de la mémoire, qui consiste au retrait de sessions relativement inutiles de la mémoire quand on les stocke en stockage persistant.

L'*Activation* signifie que les données sont extraites d'un stockage persistant et sont renvoyées dans la mémoire.

La passivation a lieu à trois reprises au cours du cycle de vie d'une session HTTP :

- Quand le conteneur réclame la création d'une nouvelle session, si le nombre de sessions actives en cours dépasse une limite configurable, le serveur tentera de passiver certaines sessions pour faire de la place à une nouvelle.
- De façon périodique, à un intervalle précis configuré, une tâche d'arrière-plan vérifiera si les sessions doivent être passivées.
- Quand une application web est déployée et qu'une copie de sauvegarde de sessions actives sur d'autres serveurs est acquise par le gestionnaire de session de l'application web récemment déployée, les sessions peuvent être passivées.

Une session est passivée si elle remplit les conditions suivantes :

- La session n'a pas été utilisée pendant une durée plus longue qu'une période d'inactivité configurable maximale.
- Le nombre de sessions actives dépasse un maximum configurable et la session n'a pas été utilisée pendant une durée plus longue qu'une période d'inactivité configurable maximale.

Les sessions sont toujours passivées en utilisant un algorithme LRU (Least Recently Used).

Report a bug

8.2.2. Configurer la passivation HttpSession dans votre application

Aperçu

La Passivation HttpSession est configurée dans le fichier **`WEB_INF/jboss-web.xml`** ou **`META_INF/jboss-web.xml`** de votre application.

Exemple 8.3. Exemple de fichier `jboss-web.xml`

```
<!DOCTYPE jboss-web PUBLIC
    "-//JBoss//DTD Web Application 5.0//EN"
    "http://www.jboss.org/j2ee/dtd/jboss-web_5_0.dtd">

<jboss-web version="6.0"
           xmlns="http://www.jboss.com/xml/ns/javaee"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           xsi:schemaLocation="http://www.jboss.com/xml/ns/javaee
http://www.jboss.org/j2ee/schema/jboss-web_6_0.xsd">

   <max-active-sessions>20</max-active-sessions>
   <passivation-config>
      <use-session-passivation>true</use-session-passivation>
      <passivation-min-idle-time>60</passivation-min-idle-time>
      <passivation-max-idle-time>600</passivation-max-idle-time>
   </passivation-config>


</jboss-web>
```

Éléments de configuration de passivation

<max-active-sessions>

Nombre maximal de sessions actives autorisé. Si le nombre de sessions gérées par le gestionnaire de sessions dépasse cette valeur et que la passivation est activée, ce dépassement sera passivé sur la base du **<passivation-min-idle-time>** configuré. Ensuite, si le nombre de sessions actives dépasse toujours cette limite, les tentatives de création de nouvelles sessions échoueront. La valeur par défaut de **-1** ne définit aucune limite quant au nombre maximal de sessions actives.

<passivation-config>

Cet élément contient le reste des paramètres de configuration de passivation, en tant qu'éléments enfants.

<passivation-config> Eléments enfants

<use-session-passivation>

Si oui ou non la passivation de session doit être utilisée. La valeur par défaut est **false**.

<passivation-min-idle-time>

La durée minimum, en secondes, pendant laquelle une session doit être inactive avant que le conteneur n'envisage de la passiver de manière à réduire le nombre de sessions actives pour être conforme à la valeur définie par les max-active-sessions. La valeur par défaut **-1** empêche les sessions d'être passivée avant que le temps **<passivation-max-idle-time>** ne se soit écoulé. Les valeurs -1 ou supérieures sont déconseillées si **<max-active-sessions>** est configuré.

<passivation-max-idle-time>

La durée maximum, en secondes, pendant laquelle une session peut être inactive avant que le conteneur ne tente de la passiver pour économiser de la mémoire. La passivation de ces sessions aura lieu, que le nombre de sessions actives excède **<max-active-sessions>** ou pas. Cette valeur doit être inférieure à la configuration **<session-timeout>** dans le fichier **web.xml**. La valeur par défaut **-1** désactive la passivation selon l'inactivité maximum.

NOTE

Le nombre total de sessions en mémoire comprend les sessions répliquées à partir d'autres nœuds de cluster dont l'accès ne se trouve pas sur ce nœud. Tenez-en compte lors de la configuration de **<max-active-sessions>**. Le nombre de sessions répliquées à partir d'autres nœuds dépend également de si le mode cache **REPL** ou **DIST** est désactivé. Dans le mode cache **REPL**, chaque session est répliquée vers chaque nœud. Dans le mode cache **DIST**, chaque session n'est répliquée que vers le nombre de nœuds indiqué par le paramètre **owner**. Veuillez vous référer à Section 8.1.2, « Cache de Session Web » et Section 8.1.3, « Configurer le Cache de session web » pour plus de renseignements sur la configuration des modes cache de session.

Prenons comme exemple un cluster à huit nœuds, dont chaque nœud gère les requêtes de 100 utilisateurs. Avec le mode cache **REPL**, chaque nœud peut stocker 800 sessions en mémoire. Avec le mode cache **DIST** désactivé, et la configuration **owners** définie par défaut sur **2**, chaque nœud stocke 200 sessions en mémoire.

Report a bug

8.3. DOMAINE DU COOKIE

8.3.1. Le domaine du cookie

Le *cookie domain* fait référence à l'ensemble des hôtes capables de lire un cookie à partir du navigateur client qui accède votre application. C'est un mécanisme de configuration pour réduire le risque de voir des tierce-parties accéder à des informations que votre application stocke dans les cookies de navigateur.

La valeur par défaut pour le domaine de cookie est `/`. Cela signifie que seul l'hôte d'origine peut lire le contenu d'un cookie. Le fait de configurer un domaine de cookie particulier rend le contenu du cookie disponible à un plus grand nombre d'hôtes. Pour configurer le domaine de cookie, veuillez vous référer à Section 8.3.2, « Configurer le domaine du cookie » .

Report a bug

8.3.2. Configurer le domaine du cookie

Pour autoriser votre valve SSO à partager un contexte SSO, configurer le domaine de cookie dans la configuration de valve. La configuration suivante autoriserait les applications sur **`http://app1.xyz.com`** et **`http://app2.xyz.com`** à partager un contexte SSO, même si ces applications fonctionnent sur des serveurs différents dans un cluster ou si l'hôte virtuel avec lequel ils sont associés possède plusieurs alias.

Exemple 8.4. Exemple de configuration de domaine de cookie

```
<Valve
className="org.jboss.web.tomcat.service.sso.ClusteredSingleSignOn"
                cookieDomain="xyz.com" />
```

Report a bug

8.4. IMPLÉMENTER UN HA SINGLETON

Résumé

Dans JBoss EAP 5, les archives HA Singleton ont été déployées dans le répertoire **`deploy-hasingleton/`** distinct d'autres déploiements. Cela a été fait pour empêcher le déploiement automatique et pour veiller à ce que le service HASingletonDeployer contrôle le déploiement et déploie les archives uniquement sur le nœud maître du cluster. Il y n'avait aucune fonctionnalité de déploiement à chaud, ce redéploiement exigeait un redémarrage du serveur. Aussi, si le nœud maître échouait nécessitant un autre nœud pour prendre le relais de nœud maître, le service singleton devait passer par le processus de déploiement complet afin de fournir le service.

Dans JBoss EAP 6, cela a changé. Grâce à un SingletonService, le service cible est installé sur chaque nœud du cluster, mais ne peut démarrer que sur un nœud à la fois. Cette approche simplifie les exigences de déploiement et minimise le temps requis pour relocaliser le Service Singleton Master entre les nœuds.

Procédure 8.3. Implémenter un Service HA Singleton

1. **Rédiger une application de Service HA Singleton**
   Vous trouverez ci-dessous un exemple simple de Service intégré dans le Decorater du SingletonService qui puisse être déployé en tant que service singleton.

   a. **Créer un service singleton**
   Vous trouverez ci-dessous un exemple simple de service singleton.

```
package com.mycompany.hasingleton.service.ejb;

import java.util.concurrent.atomic.AtomicBoolean;
import java.util.logging.Logger;

import org.jboss.as.server.ServerEnvironment;
import org.jboss.msc.inject.Injector;
import org.jboss.msc.service.Service;
import org.jboss.msc.service.ServiceName;
import org.jboss.msc.service.StartContext;
import org.jboss.msc.service.StartException;
import org.jboss.msc.service.StopContext;
import org.jboss.msc.value.InjectedValue;

/**
 * @author <a href="mailto:wfink@redhat.com">Wolf-Dieter Fink</a>
 */
public class EnvironmentService implements Service<String> {
    private static final Logger LOGGER =
Logger.getLogger(EnvironmentService.class.getCanonicalName());
    public static final ServiceName SINGLETON_SERVICE_NAME =
ServiceName.JBOSS.append("quickstart", "ha", "singleton");
    /**
     * A flag whether the service is started.
     */
    private final AtomicBoolean started = new
AtomicBoolean(false);

    private String nodeName;

    private final InjectedValue<ServerEnvironment> env = new
InjectedValue<ServerEnvironment>();

    public Injector<ServerEnvironment> getEnvInjector() {
        return this.env;
    }

    /**
     * @return the name of the server node
     */
    public String getValue() throws IllegalStateException,
IllegalArgumentException {
        if (!started.get()) {
            throw new IllegalStateException("The service '" +
this.getClass().getName() + "' is not ready!");
        }
        return this.nodeName;
```

```
    }

    public void start(StartContext arg0) throws StartException {
        if (!started.compareAndSet(false, true)) {
            throw new StartException("The service is still
started!");
        }
        LOGGER.info("Start service '" + this.getClass().getName()
+ "'");
        this.nodeName = this.env.getValue().getNodeName();
    }

    public void stop(StopContext arg0) {
        if (!started.compareAndSet(true, false)) {
            LOGGER.warning("The service '" +
this.getClass().getName() + "' is not active!");
        } else {
            LOGGER.info("Stop service '" +
this.getClass().getName() + "'");
        }
    }
}
```

b. **Créer un EJB singleton pour démarrer le service en tant que SingletonService au démarrage du serveur.**
La liste suivante est un exemple d'EJB singleton qui démarre un SingletonService au démarrage d'un serveur :

```
package com.mycompany.hasingleton.service.ejb;

import java.util.Collection;
import java.util.EnumSet;

import javax.annotation.PostConstruct;
import javax.annotation.PreDestroy;
import javax.ejb.Singleton;
import javax.ejb.Startup;

import org.jboss.as.clustering.singleton.SingletonService;
import org.jboss.as.server.CurrentServiceContainer;
import org.jboss.as.server.ServerEnvironment;
import org.jboss.as.server.ServerEnvironmentService;
import org.jboss.msc.service.AbstractServiceListener;
import org.jboss.msc.service.ServiceController;
import org.jboss.msc.service.ServiceController.Transition;
import org.jboss.msc.service.ServiceListener;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;


/**
 * A Singleton EJB to create the SingletonService during startup.
 *
 * @author <a href="mailto:wfink@redhat.com">Wolf-Dieter Fink</a>
 */
```

```
@Singleton
@Startup
public class StartupSingleton {
  private static final Logger LOGGER =
LoggerFactory.getLogger(StartupSingleton.class);

  /**
   * Create the Service and wait until it is started.<br/>
   * Will log a message if the service will not start in 10sec.
   */
  @PostConstruct
  protected void startup() {
    LOGGER.info("StartupSingleton will be initialized!");

    EnvironmentService service = new EnvironmentService();
    SingletonService<String> singleton = new
SingletonService<String>(service,
EnvironmentService.SINGLETON_SERVICE_NAME);
    // if there is a node where the Singleton should deployed the
election policy might set,
    // otherwise the JGroups coordinator will start it
    //singleton.setElectionPolicy(new
PreferredSingletonElectionPolicy(new
NamePreference("node2/cluster"), new
SimpleSingletonElectionPolicy()));
    ServiceController<String> controller =
singleton.build(CurrentServiceContainer.getServiceContainer())
        .addDependency(ServerEnvironmentService.SERVICE_NAME,
ServerEnvironment.class, service.getEnvInjector())
        .install();

    controller.setMode(ServiceController.Mode.ACTIVE);
    try {
      wait(controller, EnumSet.of(ServiceController.State.DOWN,
ServiceController.State.STARTING), ServiceController.State.UP);
      LOGGER.info("StartupSingleton has started the Service");
    } catch (IllegalStateException e) {
      LOGGER.warn("Singleton Service {} not started, are you sure
to start in a cluster (HA)
environment?",EnvironmentService.SINGLETON_SERVICE_NAME);
    }
  }

  /**
   * Remove the service during undeploy or shutdown
   */
  @PreDestroy
  protected void destroy() {
    LOGGER.info("StartupSingleton will be removed!");
    ServiceController<?> controller =
CurrentServiceContainer.getServiceContainer().getRequiredService(
EnvironmentService.SINGLETON_SERVICE_NAME);
    controller.setMode(ServiceController.Mode.REMOVE);
    try {
      wait(controller, EnumSet.of(ServiceController.State.UP,
ServiceController.State.STOPPING, ServiceController.State.DOWN),
```

```
ServiceController.State.REMOVED);
    } catch (IllegalStateException e) {
      LOGGER.warn("Singleton Service {} has not be stopped
correctly!",EnvironmentService.SINGLETON_SERVICE_NAME);
    }
  }

  private static <T> void wait(ServiceController<T> controller,
Collection<ServiceController.State> expectedStates,
ServiceController.State targetState) {
    if (controller.getState() != targetState) {
      ServiceListener<T> listener = new
NotifyingServiceListener<T>();
      controller.addListener(listener);
      try {
        synchronized (controller) {
          int maxRetry = 2;
          while (expectedStates.contains(controller.getState())
&& maxRetry > 0) {
            LOGGER.info("Service controller state is {}, waiting
for transition to {}", new Object[] {controller.getState(),
targetState});
            controller.wait(5000);
            maxRetry--;
          }
        }
      } catch (InterruptedException e) {
        LOGGER.warn("Wait on startup is interrupted!");
        Thread.currentThread().interrupt();
      }
      controller.removeListener(listener);
      ServiceController.State state = controller.getState();
      LOGGER.info("Service controller state is now {}",state);
      if (state != targetState) {
        throw new IllegalStateException(String.format("Failed to
wait for state to transition to %s.  Current state is %s",
targetState, state), controller.getStartException());
      }
    }
  }

  private static class NotifyingServiceListener<T> extends
AbstractServiceListener<T> {
    @Override
    public void transition(ServiceController<? extends T>
controller, Transition transition) {
      synchronized (controller) {
        controller.notify();
      }
    }
  }
}
```

c. **Créer un Stateless Session Bean pour accéder au service à partir d'un client.**
Voici un exemple de Stateless Session Bean qui accède au service à partir d'un client :

```
package com.mycompany.hasingleton.service.ejb;

import javax.ejb.Stateless;

import org.jboss.as.server.CurrentServiceContainer;
import org.jboss.msc.service.ServiceController;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

/**
 * A simple SLSB to access the internal SingletonService.
 *
 * @author <a href="mailto:wfink@redhat.com">Wolf-Dieter Fink</a>
 */
@Stateless
public class ServiceAccessBean implements ServiceAccess {
    private static final Logger LOGGER =
LoggerFactory.getLogger(ServiceAccessBean.class);

    public String getNodeNameOfService() {
        LOGGER.info("getNodeNameOfService() is called()");
        ServiceController<?> service =
CurrentServiceContainer.getServiceContainer().getService(
                EnvironmentService.SINGLETON_SERVICE_NAME);
        LOGGER.debug("SERVICE {}", service);
        if (service != null) {
            return (String) service.getValue();
        } else {
            throw new IllegalStateException("Service '" +
EnvironmentService.SINGLETON_SERVICE_NAME + "' not found!");
        }
    }
}
```

d. **Créer une interface de logique commerciale pour le SingletonService.**
Voici un exemple d'interface de logique commerciale pour le SingletonService.

```
package com.mycompany.hasingleton.service.ejb;

import javax.ejb.Remote;

/**
 * Business interface to access the SingletonService via this EJB
 *
 * @author <a href="mailto:wfink@redhat.com">Wolf-Dieter Fink</a>
 */
@Remote
public interface ServiceAccess {
    public abstract String getNodeNameOfService();
}
```

2. **Démarrez chaque instance de JBoss EAP 6 avec le clustering activé.**

La méthode d'activation du clustering dépend si les serveurs exécutent en autonome ou en domaine géré.

a. **Activer le clustering pour les serveurs qui exécutent dans un domaine géré.**
Vous pourrez utiliserle Management CLI, ou bien, vous pourrez éditer le fichier de configuration manuellement pour activer le clustering.

- **Activer le clustering par le Management CLI.**

i. **Démarrer votre contrôleur de domaine.**

ii. **Ouvrir une invite de commande de votre système d'exploitation.**

iii. **Connectez vous au Management CLI en faisant passer l'adresse IP du contrôleur de domaine ou le nom DNS.**
Dans cet exemple, considérons que l'adresse IP du contrôleur du domaine est **`192.168.0.14`**.

- Dans Linux, saisir ce qui suit au niveau de la ligne de commande :

```
$ EAP_HOME/bin/jboss-cli.sh --connect --
controller=192.168.0.14
```

- Dans Windows, saisir ce qui suit au niveau de la ligne de commande :

```
C:\>EAP_HOME\bin\jboss-cli.bat --connect --
controller=192.168.0.14
```

Vous devriez voir apparaître le résultat suivant :

```
Connected to domain controller at 192.168.0.14
```

iv. **Ajouter le groupe de serveurs `main-server`.**

```
[domain@192.168.0.14:9999 /] /server-group=main-server-
group:add(profile="ha",socket-binding-group="ha-sockets")
{
    "outcome" => "success",
    "result" => undefined,
    "server-groups" => undefined
}
```

v. **Créer un serveur nommé `server-one` et ajoutez-le au groupe de serveurs `main-server`.**

```
[domain@192.168.0.14:9999 /]  /host=station14Host2/server-
config=server-one:add(group=main-server-group,auto-
start=false)
{
    "outcome" => "success",
    "result" => undefined
}
```

vi. **Configurer la JVM pour le groupe de serveurs `main-server`.**

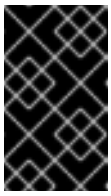
```
[domain@192.168.0.14:9999 /] /server-group=main-server-
group/jvm=default:add(heap-size=64m,max-heap-size=512m)
{
    "outcome" => "success",
    "result" => undefined,
    "server-groups" => undefined
}
```

vii. **Créer un serveur nommé `server-one` , mettez-le dans un groupe de serveurs séparés et définir son Port Offset à 100.**

```
[domain@192.168.0.14:9999 /]  /host=station14Host2/server-
config=server-two:add(group=distinct2,socket-binding-port-
offset=100)
{
    "outcome" => "success",
    "result" => undefined
}
```

- **Activer le clustering en modifiant manuellement les fichiers de configuration du serveur.**

  i. **Stopper le serveur JBoss EAP 6.**

  IMPORTANT

  Vous devez interrompre le serveur avant de modifier le fichier de configuration du serveur pour que votre changement puisse être persisté au redémarrage du serveur.

  ii. **Ouvrir le fichier de configuration `domain.xml` pour modifier**
  Désignez un groupe de serveurs qui puisse utiliser le profil **ha** et le groupe de liaisons de sockets **`ha-sockets`** comme suit :

```
<server-groups>
  <server-group name="main-server-group" profile="ha">
    <jvm name="default">
      <heap size="64m" max-size="512m"/>
    </jvm>
    <socket-binding-group ref="ha-sockets"/>
  </server-group>
</server-groups>
```

  iii. **Ouvrir le fichier de configuration `host.xml` pour modifier**
  Éditez le fichier comme suit :

```
<servers>
  <server name="server-one" group="main-server-group" auto-
start="false"/>
  <server name="server-two" group="distinct2">
    <socket-bindings port-offset="100"/>
```

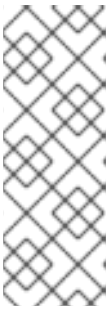
```
  </server>
<servers>
```

iv. **Démarrer le serveur :**

- Dans Linux, tapez : ***EAP_HOME*/bin/domain.sh**
- Dans Microsoft Windows, tapez : ***EAP_HOME*\bin\domain.bat**

b. **Activer le clustering pour les serveurs autonomes**
Pour activer le clustering dans les serveurs autonomes, démarrer le serveur par le nom du nœud et le fichier de configuration **standalone-ha.xml** comme ce qui suit :

- Dans Linux, saisir : ***EAP_HOME*/bin/standalone.sh --server-config=standalone-ha.xml -Djboss.node.name=*UNIQUE_NODE_NAME***
- Dans Microsoft Windows, saisir : ***EAP_HOME*\bin\standalone.bat --server-config=standalone-ha.xml -Djboss.node.name=*UNIQUE_NODE_NAME***



NOTE

Pour éviter les conflits de ports quand on exécute plusieurs serveurs sur une machine, configurez le fichier **standalone-ha.xml** pour que chaque instance de serveur puisse se lier à une interface séparée. Sinon, vous pourrez démarrer les instances de serveurs suivants par une référence de port, par l'argument suivant, ou similaire, dans votre ligne de commande : **-Djboss.socket.binding.port-offset=100**.

3. **Déployer l'application dans les serveurs**
Si vous utilisez Maven pour déployer votre application, utiliser la commande Maven pour vous déployer dans le serveur qui exécute sur les ports par défaut :

```
mvn clean install jboss-as:deploy
```

Pour déployer des serveurs supplémentaires, indiquer le nom du serveur et le numéro de port dans la ligne de commande :

```
mvn clean package jboss-as:deploy -Ddeploy.hostname=localhost -
Ddeploy.port=10099
```

Report a bug

CHAPITRE 9. CDI

9.1. CDI

9.1.1. CDI

- Section 9.1.2, « CDI (Contexts and Dependency Injection) »
- Section 9.1.5, « Relation entre Weld, Seam 2, Seam 3, et JavaServer Faces »
- Section 9.1.3, « Avantages de CDI »

Report a bug

9.1.2. CDI (Contexts and Dependency Injection)

Context and Dependency Injection (CDI) est une spécification conçue pour permettre aux composants EJB 3.0 "d'être utilisés comme beans JSF (java Server Faces), réunissant les deux modèles de composants et permettant la simplification du modèle de programmation des applications basées-web dans Java". La citation suivante est extraite de la spécification JSR-299, que l'on peut trouver à http://www.jcp.org/en/jsr/detail?id=299.

JBoss EAP 6 inclut Weld, qui est l'implementation de référence de JSR-299. Pour obtenir plus d'informations sur l'injection de dépendance type-safe, voir Section 9.1.4, « Injection de Dépendance de Type-safe ».

Report a bug

9.1.3. Avantages de CDI

- CDI simplifie et rétrécit votre base code en remplaçant des gros morceaux de code par des annotations.
- CDI est flexible, ce qui vous permet de désactiver ou d'activer des injections et des événements, d'utiliser des autres beans, ou d'injecter des objets non-CDI facilement.
- Il est facile d'utiliser votre ancien code avec CDI. Vous n'avez qu'à y inclure un **`beans.xml`** dans votre répertoire **`META-INF/`** ou **`WEB-INF/`**. Le fichier peut être vide.
- CDI simplifie le packaging et les déploiements, et réduit le montant d'XML que vous aurez besoin d'ajouter à vos déploiements.
- CDI propose une gestion du cycle de vie par contexte. Vous pouvez lier des injections aux requêtes, sessions, conversations, ou contextes personnalisés.
- CDI propose un injection de dépendance type-safe, qui est plus sécurisée et facile à débogger qu'une injection basée string.
- CDI découple les intercepteurs des beans.
- CDI fournit une notification d'événements complexe.

Report a bug

9.1.4. Injection de Dépendance de Type-safe

Avant JSR-299 et DCI, la seule façon d'injecter des dépendances dans Java était par chaînes. Cela portait à erreur. DCI a introduit la possibilité d'injecter des dépendances d'une manière plus sûre.

Pour plus d'information sur CDI, voir Section 9.1.2, « CDI (Contexts and Dependency Injection) ».

Report a bug

9.1.5. Relation entre Weld, Seam 2, Seam 3, et JavaServer Faces

Le but de *Seam 2* était d'unifier les beans gérés Enterprise Java Beans (EJBs) et JavaServer Faces (JSF).

JavaServer Faces (JSF) implémente JSR-314. Il s'agit d'un API qui construit les interfaces utilisateur côté serveur. *JBoss Web Framework Kit* inclut *RichFaces*, qui est une implémentation de JavaServer Faces et AJAX.

Weld est l'implémentation de référence de *Contexts and Dependency Injection (CDI)*, définie dans JSR-299. Weld est inspiré de Seam 2 et d'autres frameworks d'injection de dépendances. Weld est inclus dans JBoss EAP 6.

Report a bug

9.2. UTILISER CDI

9.2.1. Premières étapes

9.2.1.1. Activer CDI

Résumé

Le CDI (Contexts and Dependency Injection) est l'une des technologies de base de la JBoss EAP 6, et est activé par défaut. Si, pour une raison ou une autre, il était désactivé et que vous souhaitiez l'activer, veuillez suivre le procédé suivant :

Procédure 9.1. Activer CDI dans JBoss EAP 6

1. **Vérifier si les informations du sous-système sont dé-commentées dans le fichier de configuration.**
   On peut désactiver un sous-système en dé-commentant la section qui convient dans les fichiers de configuration **`domain.xml`** ou **`standalone.xml`**, ou en supprimant la section qui convient.

   Pour trouver le sous-système dans ***`EAP_HOME`*`/domain/configuration/domain.xml`** ou ***`EAP_HOME`*`/standalone/configuration/standalone.xml`**, le chercher dans les strings suivants. S'il existe, il se trouve dans la section <extensions>.

   ```
   <extension module="org.jboss.as.weld"/>
   ```

   La ligne suivante doit se trouver dans le profil que vous utilisez. Les profils se trouvent dans des éléments de <profile> dans la section <profiles>.

   ```
   <subsystem xmlns="urn:jboss:domain:weld:1.0"/>
   ```

2. **Avant de modifier un fichier, arrêter JBoss EAP 6.**
   JBoss EAP 6 modifie les fichiers de configuration pendant le temps d'exécution, vous devez donc arrêter le serveur avant de modifier directement les fichiers de configuration.

3. **Modifer le fichier de configuration pour restaurer le sous-système CDI.**
   Si le sous-système CDI est dé-commenté, supprimer les commentaires.

   S'il était supprimé totalement, le restaurer en ajoutant cette ligne au fichier dans une nouvelle ligne directement au dessus de la balise </extensions> :

   ```
   <extension module="org.jboss.as.weld"/>
   ```

4. Vous devez également ajouter la ligne suivante dans le profil concerné qui se trouve dans la section <profiles>.

   ```
   <subsystem xmlns="urn:jboss:domain:weld:1.0"/>
   ```

5. **Démarrer à nouveau JBoss EAP 6.**
   Démarrer JBoss EAP 6 avec votre configuration mise à jour.

Résultat

JBoss EAP 6 démarre avec le sous-système CDI activé.

Report a bug

9.2.2. Utiliser CDI pour développer une application

9.2.2.1. Utiliser CDI pour développer une application

Introduction

Le CDI (Contexts and Dependency Injection) vous offre une très grande flexibilité pour développer des applications, réutiliser des codes, adapter votre code au déploiement ou à l'exécution et tester des unités. JBoss EAP 6 comprend Weld, l'implémentation de référence de CDI. Ces tâches vous montrent comment utiliser CDI dans vos applications enterprise.

- Section 9.2.1.1, « Activer CDI »
- Section 9.2.2.2, « CDI avec le code existant »
- Section 9.2.2.3, « Exclure les beans du processus de balayage »
- Section 9.2.2.4, « Utiliser une injection pour étendre une implémentation »
- Section 9.2.3.3, « Utiliser un qualificateur pour résoudre une injection ambiguë »
- Section 9.2.7.4, « Remplacer une injection par une alternative »
- Section 9.2.7.2, « Utilisation des Named Beans »
- Section 9.2.6.1, « Gestion du cycle de vie d'un bean »
- Section 9.2.6.2, « Utilisation d'une méthode Producer »
- Section 9.2.10.2, « Utiliser les intercepteurs dans CDI »

- Section 9.2.8.2, « Utilisation des stéréotypes »
- Section 9.2.9.2, « Appliquer et observer des événements »

Report a bug

9.2.2.2. CDI avec le code existant

Presque chaque classe concrète de Java qui a un constructeur sans paramètre, ou un constructeur désigné avec l'annotation @Inject, est un bean. La seule chose que vous devez faire avant de commencer à injecter des beans est de créer un fichier appelé **beans.xml** dans le répertoire **META-INF/** ou **WEB-INF/** de votre archive. Ce fichier peut rester vide.

Procédure 9.2. Utiliser les anciens beans dans les applications CDI

1. **Groupez vos beans dans une archive.**
   Groupez vos beans dans une archive JAR ou WAR.

2. **Inclure un fichier beans.xml dans votre archive.**
   Mettez un fichier **beans.xml** dans votre répertoire d'archive JAR **META-INF/** ou d'archive WAR **WEB-INF/**. Ce fichier peut rester vide.

Résultat :

Vous pouvez utiliser ces beans avec CDI. Le conteneur peut créer et détruire des instances de vos beans et les associer à un contexte désigné, les injecter dans les autres beans, les utiliser dans des expressions EL, les spécialiser par des annotations de qualifier et y ajouter des intercepteurs et des décorateurs, sans aucune modification de votre code existant. Dans certains cas, vous devrez peut-être ajouter des annotations.

Report a bug

9.2.2.3. Exclure les beans du processus de balayage

Résumé

Une des caractéristiques de Weld, l'implémentation de CDI de JBoss EAP 6, est la possibilité d'exclure des classes de balayage de votre archive, d'avoir des événements de cycle de vie conteneur émis, et déployés comme beans. Cela ne fait pas partie de la spécification JSR-299.

> **Exemple 9.1. Exclure des packages de votre bean.**
>
> L'exemple suivant possède plusieurs balises <weld:exclude>.
>
> 1. Le premier exclut toutes les classes Swing.
> 2. Le second exclut les classes Google Web Toolkit id le Google Web Toolkit n'est pas installé.
> 3. Le troisième exclut les classes qui finissent dans la chaîne **Blether** (en utilisant une expression régulière), si la propriété de système verbosity est définie comme **low**.
> 4. Le quatrième exclut les classes JSF (Java Server Faces) si les classes Wicket sont présentes et la propriété de système viewlayer n'est pas définie.

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://java.sun.com/xml/ns/javaee"
```

```
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xmlns:weld="http://jboss.org/schema/weld/beans"
       xsi:schemaLocation="
          http://java.sun.com/xml/ns/javaee
http://docs.jboss.org/cdi/beans_1_0.xsd
          http://jboss.org/schema/weld/beans
http://jboss.org/schema/weld/beans_1_1.xsd">

    <weld:scan>

        <!-- Don't deploy the classes for the swing app! -->
        <weld:exclude name="com.acme.swing.**" />

        <!-- Don't include GWT support if GWT is not installed -->
        <weld:exclude name="com.acme.gwt.**">
            <weld:if-class-available name="!com.google.GWT"/>
        </weld:exclude>

        <!--
            Exclude classes which end in Blether if the system property
verbosity is set to low
            i.e.
              java ... -Dverbosity=low
        -->
        <weld:exclude pattern="^(.*)Blether$">
            <weld:if-system-property name="verbosity" value="low"/>
        </weld:exclude>

       <!--
             Don't include JSF support if Wicket classes are present,
and the viewlayer system
             property is not set
        -->
        <weld:exclude name="com.acme.jsf.**">
            <weld:if-class-available name="org.apache.wicket.Wicket"/>
            <weld:if-system-property name="!viewlayer"/>
        </weld:exclude>
    </weld:scan>
</beans>
```

La spécification formelle des options de configuration spéciale Weld se trouve dans http://jboss.org/schema/weld/beans_1_1.xsd.

Report a bug

9.2.2.4. Utiliser une injection pour étendre une implémentation

Résumé

Vous pouvez utiliser une injection pour ajouter ou modifier une caractéristique de votre code existant. Cet exemple vous montre comment ajouter une capacité de traduction à une classe existante. La traduction est une caractéristique hypothétique et la façon dont elle est implémentée dans cet exemple est pseudo-code, et elle est fournie à titre illustratif uniquement.

L'exemple part du principe que vous avez déjà une classe Welcome, qui possède une méthode **buildPhrase**. La méthode **buildPhrase** utilise le nom d'une ville comme paramètre et crée une formule telle que "Welcome to Boston". Votre objectif est de créer une version de cette classe **Welcome** pouvant traduire cette formule d'accueil dans une autre langue.

Exemple 9.2. Injecter un Bean Translator dans la classe Welcome.

Le pseudo-code suivant injecte un objet **Translator** hypothétique dans la classe **Welcome**. L'objet **Translator** peut être un bean sans état EJB ou un autre type de bean, pouvant traduire des phrases d'une langue à une autre. Ainsi, le **Translator** est utilisé pour traduire la formule d'accueil complète, sans avoir à modifier la classe **Welcome** d'origine. Le **Translator** est injecté avant que la méthode **buildPhrase** ne soit implémentée.

L'échantillon de code ci-dessous est un exemple de classe Welcome de Traduction.

```
public class TranslatingWelcome extends Welcome {

    @Inject Translator translator;

    public String buildPhrase(String city) {
        return translator.translate("Welcome to " + city + "!");
    }
    ...
}
```

Report a bug

9.2.3. Dépendances ambigues ou non satisfaites

9.2.3.1. Dépendances ambigües et non-satisfaites

On parle de dépendances ambigües quand le conteneur ne peut pas résoudre une injection dans un bean précisément.

On parle de dépendances non-satisfaites quand le conteneur ne peut pas résoudre une injection dans aucun bean.

Le conteneur suit les étapes suivantes pour essayer de résoudre les dépendances :

1. Il résout les annotations de qualificateur sur tous les beans qui implémentent le bean d'un point d'injection.

2. Il filre les beans désactivés. Les beans désactivés sont des beans @Alternative qui ne sont pas explicitement activés.

Dans le cas d'une dépendance ambigüe ou non satisfaite, le conteneur stoppe le déploiement et envoie une exception.

Pour fixer une dépendance ambigüe, voir Section 9.2.3.3, « Utiliser un qualificateur pour résoudre une injection ambiguë ».

Report a bug

9.2.3.2. Qualificateurs

Un qualificateur est une annotation qui relie un bean à un autre. Cela vous permet d'indiquer avec précision quel bean vous souhaitez injecter. Les qualificateurs possèdent une rétention et une cible, définies comme dans l'exemple ci-dessous.

Exemple 9.3. Définit les qualificateurs @Synchronous et @Asynchronous

```
@Qualifier
@Retention(RUNTIME)
@Target({TYPE, METHOD, FIELD, PARAMETER})
public @interface Synchronous {}
```

```
@Qualifier
@Retention(RUNTIME)
@Target({TYPE, METHOD, FIELD, PARAMETER})
public @interface Asynchronous {}
```

Exemple 9.4. Utiliser les qualificateurs @Synchronous et @Asynchronous

```
@Synchronous
public class SynchronousPaymentProcessor implements PaymentProcessor {

   public void process(Payment payment) { ... }

}
```

```
@Asynchronous
public class AsynchronousPaymentProcessor implements PaymentProcessor {

   public void process(Payment payment) { ... }
}
```

Report a bug

9.2.3.3. Utiliser un qualificateur pour résoudre une injection ambiguë

Résumé

Cette tâche indique une injection ambiguë et la retire par un qualificateur. Pour en savoir plus sur les injections ambiguës, voir Section 9.2.3.1, « Dépendances ambigües et non-satisfaites ».

Exemple 9.5. Injections ambiguës

Il y a deux implémentations de la classe **`Welcome`**, une qui traduit, et l'autre non. Dans cette situation, l'injection ci-dessous est ambiguë et a besoin d'être spécifiée pour qu'on puisse utiliser la classe de traduction **`Welcome`**.

```
public class Greeter {
  private Welcome welcome;
```

```
  @Inject
  void init(Welcome welcome) {
    this.welcome = welcome;
  }
  ...
}
```

Procédure 9.3. Résoudre une injection ambiguë avec un qualificateur

1. **Créer une annotation de qualificateur nommée `@Translating`.**

```
@Qualifier
@Retention(RUNTIME)
@Target({TYPE,METHOD,FIELD,PARAMETERS})
public @interface Translating{}
```

2. **Annoter votre classe `Welcome` par l'annotation `@Translating`.**

```
@Translating
public class TranslatingWelcome extends Welcome {
    @Inject Translator translator;
    public String buildPhrase(String city) {
        return translator.translate("Welcome to " + city + "!");
    }
    ...
}
```

3. **Demander la classe de traduction `Welcome` dans votre injection.**
   Vous devez demander une implémentation explicitement qualifiée, qui ressemble au modèle de la méthode de fabrique. L'ambiguité se résout au point d'injection.

```
public class Greeter {
  private Welcome welcome;
  @Inject
  void init(@Translating Welcome welcome) {
    this.welcome = welcome;
  }
  public void welcomeVisitors() {
    System.out.println(welcome.buildPhrase("San Francisco"));
  }
}
```

Résultat

`TranslatingWelcome` est utilisé, et il n'y a pas d'ambiguité.

Report a bug

9.2.4. Beans gérés

9.2.4.1. Les beans gérés

Les beans gérés, nommés également MBeans, sont des JavaBeans qui sont créés par injection de dépendance. Chaque MBean représente une ressource exécutée dans la JVM (Java Virtual Machine).

Java EE 6 est une extension de cette définition. Un bean est implémenté par une classe Java, à laquelle on fait référence en tant que classe bean. Un bean géré est une classe Java de niveau supérieur.

Pour plus d'informations sur les beans gérés, voir la spécification JSR-255 qui se trouve à http://jcp.org/en/jsr/detail?id=255. Pour plus d'informations sur CDI, voir Section 9.1.2, « CDI (Contexts and Dependency Injection) ».

Report a bug

9.2.4.2. Types de Classes qui ne sont pas des Beans

Un bean géré est une classe Java. Le cycle de base et la sémantique d'un bean géré est définie par la spécification de Beans gérés. Vous pouvez explicitement déclarer un bean géré en annotant la classe bean **@ManagedBean**, mais en CDI cela n'est pas nécessaire. Conformément à la spécification, le conteneur CDI traite n'importe quelle classe qui remplit les conditions suivantes en tant que bean géré :

- Il s'agit d'une classe interne non-statique
- Il ne s'agit pas d'une classe concrète, ou bien elle est annotée par **`@Decorator`**
- Elle n'est pas annotée par une annotation définie par un composant EJB, ni déclarée comme classe bean EJB dans **`ejb-jar.xml`**.
- Elle n'implémente pas l'interface **`javax.enterprise.inject.spi.Extension`**.
- Possède un constructeur sans paramètre ou un constructeur annoté avec **`@Inject`**.

L'ensemble de types de beans non-restraints d'un bean géré contient la classe de bean, toutes les superclasses et interfaces qu'il implémente directement ou indirectement.

Si un bean géré contient un champ public, il devra avoir comme scope par défaut @Dependent.

Report a bug

9.2.4.3. Utiliser CDI pour injecter un objet dans un bean

Quand votre archive de déploiement inclut un fichier **`META-INF/beans.xml`** ou **`WEB-INF/beans.xml`**, chaque objet de votre déploiement peut être injecté par CDI.

Cette procédure vous explique les moyens les plus courants d'injecter des objets dans d'autres objets.

1. **Injecter un objet dans n'importe quelle partie de bean par l'annotation `@Inject`.**
   Pour obtenir une instance de classe, dans votre bean, annotez ce champ avec **`@Inject`**.

   Exemple 9.6. Injecter une instance `TextTranslator` dans un `TranslateController`

   ```
   public class TranslateController {

      @Inject TextTranslator textTranslator;
      ...
   ```

2. **Utiliser les méthodes de l'objet injecté**
   Vous pouvez directement utiliser les méthodes de vos objets injectés. Partez du principe que **`TextTranslator`** possède une méthode **`translate`**.

   Exemple 9.7. Utiliser les méthodes de l'objet injecté

   ```
   // in TranslateController class

   public void translate() {

      translation = textTranslator.translate(inputText);

   }
   ```

3. **Utiliser l'injection dans le contructeur d'un bean**
   Vous pouvez injecter des objets dans le constructeur d'un bean, ou bien, vous pouvez utiliser une fabrique ou un localisateur de service pour les créer.

   Exemple 9.8. Utiliser l'injection pour la construction d'un bean

   ```
   public class TextTranslator {

      private SentenceParser sentenceParser;

      private Translator sentenceTranslator;



      @Inject

      TextTranslator(SentenceParser sentenceParser, Translator
   sentenceTranslator) {

         this.sentenceParser = sentenceParser;

         this.sentenceTranslator = sentenceTranslator;

      }

      // Methods of the TextTranslator class
      ...
   }
   ```

4. **Utiliser l'interface `Instance(<T>)` pour obtenir les instances de façon programmatique.**
   L'interface **`Instance`** peut renvoyer une instance de TextTranslator si paramétrée par le type de bean.

   Exemple 9.9. Obtenir une instance par programmation

   ```
   @Inject Instance<TextTranslator> textTranslatorInstance;
   ```

```
...
public void translate() {
   textTranslatorInstance.get().translate(inputText);
}
```

Résultat :

Lorsque vous injectez un objet dans un bean, toutes les méthodes et les propriétés de l'objet sont disponibles pour votre bean. Si vous injectez dans le constructeur de votre bean, les instances des objets injectés sont créés quand le constructeur de votre bean est appelé, à moins que l'injection ne fasse référence à une instance qui existe déjà. Par exemple, une nouvelle instance ne serait pas créée si vous injectiez un bean basé-session pendant la durée de la session.

Report a bug

9.2.5. Contextes, Scopes et Dépendances

9.2.5.1. Contextes et scopes

Un contexte, en terme de CDI, est une zone de stockage, qui contient des instances de beans associées à une portée particulière.

Un scope est un lien entre un bean et un contexte. Un scope/context peut avoir un cycle de vie particulier. Il existe plusieurs scopes pré-définis, et vous pouvez créer vos propres scopes. Voici des exemples de scopes pré-définis **@RequestScoped**, **@SessionScoped**, et **@ConversationScope**.

Report a bug

9.2.5.2. Contexte disponibles

Tableau 9.1. Contextes disponibles

Contexte	Description
@Dependent	Le bean est lié au cycle de vie du bean qui contient la référence.
@ApplicationScoped	Lié au cycle de vie de l'application.
@RequestScoped	Lié au cycle de vie de la requête.
@SessionScoped	Lié au cycle de vie de la session.
@ConversationScoped	Lié au cycle de vie de la conversation. Le scope de la conversation correspond aux longueurs de la requête et de la session, et est contrôlé par l'application.

Contexte	Description
Scopes personnalisés	Si les contextes ne correspondent pas à vos besoins, vous pourrez définir des scopes personnalisés.

Report a bug

9.2.6. Cycle de vie d'un bean

9.2.6.1. Gestion du cycle de vie d'un bean

Résumé

Cette tâche vous montre comment sauvegarder un bean pendant la durée de vie d'une requête. Il existe plusieurs autres scopes, et vous pouvez définir vos propres scopes.

Le scope par défaut d'un bean injecté est**@Dependent**. Cela veut dire que le cycle de vie du bean dépend du cycle de vie du bean qui contient la référence. Pour plus d'informations, voir Section 9.2.5.1, « Contextes et scopes ».

Procédure 9.4. Gestion du cycle de vie d'un bean

1. **Annoter le bean par le scope qui correspond au scope désiré.**

```
@RequestScoped
@Named("greeter")
public class GreeterBean {
  private Welcome welcome;
  private String city; // getter & setter not shown
  @Inject   void init(Welcome welcome) {
    this.welcome = welcome;
  }
  public void welcomeVisitors() {
    System.out.println(welcome.buildPhrase(city));
  }
}
```

2. **Quand votre bean est utilisé dans la vue JSF, il contient un état.**

```
<h:form>
  <h:inputText value="#{greeter.city}"/>
  <h:commandButton value="Welcome visitors" action="#
{greeter.welcomeVisitors}"/>
</h:form>
```

Résultat :

Votre bean est sauvegardé dans le contexte lié au scope que vous spécifiez, et dure aussi longtemps que le scope est applicable.

- Section 9.2.13.1, « Proxys Bean »
- Section 9.2.13.2, « Utiliser un Proxy ou une Injection »

Report a bug

9.2.6.2. Utilisation d'une méthode Producer

Résumé

Cette tâche vous montre comment utiliser les méthodes Producer pour créer un certain nombre d'objets qui ne sont pas des beans, pour l'injection.

Exemple 9.10. Utiliser une méthode Producer au lieu d'une méthode Alternative, pour permettre le polymorphisme suite au déploiement.

L'annotation **@Preferred** dans l'exemple donné est une annotation qualifiante. Pour plus d'informations sur les qualificateurs, veuillez vous référer à : Section 9.2.3.2, « Qualificateurs ».

```
@SessionScoped
public class Preferences implements Serializable {
   private PaymentStrategyType paymentStrategy;
   ...
   @Produces @Preferred
   public PaymentStrategy getPaymentStrategy() {
       switch (paymentStrategy) {
           case CREDIT_CARD: return new CreditCardPaymentStrategy();
           case CHECK: return new CheckPaymentStrategy();
           default: return null;
       }
   }
}
```

Le point d'injection suivant a les mêmes type et qualificateur d'annotations que la méthode de Producer, donc il se résout à la méthode Producer en utilisant les règles usuelles d'injection CDI. La méthode Producer est appelée par le conteneur pour obtenir une instance au service de ce point de l'injection.

```
@Inject @Preferred PaymentStrategy paymentStrategy;
```

Exemple 9.11. Assigner un scope à une méthode Producer

L'étendue par défaut d'une méthode Producer est **@Dependent**. Si vous attribuez une étendue à un bean, celle-ci est destinée au contexte approprié. La méthode Producer dans cet exemple n'est appelée qu'une fois par session.

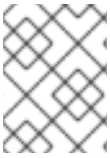
```
@Produces @Preferred @SessionScoped
public PaymentStrategy getPaymentStrategy() {
   ...
}
```

Exemple 9.12. Utiliser une injection à l'intérieur d'une méthode Producer

Les objets instanciés directement par une application ne peuvent pas profiter de l'injection de dépendance, et n'ont pas d'intercepteurs. Cependant, vous pouvez utiliser l'injection de dépendance dans la méthode Producer pour obtenir des instances de bean.

```
@Produces @Preferred @SessionScoped
public PaymentStrategy getPaymentStrategy(CreditCardPaymentStrategy
ccps,
                                          CheckPaymentStrategy cps )
{
   switch (paymentStrategy) {
      case CREDIT_CARD: return ccps;
      case CHEQUE: return cps;
      default: return null;
   }
}
```

Si vous injectez un bean de demande (request-scoped) dans un Producer de session (session-scoped), la méthode Producer favorise l'instance actuelle de demande (request-scoped) dans le scope de la session. Ce n'est certainement pas le comportement souhaité, alors soyez prudent lorsque vous utilisez une méthode de Producer de cette façon.



NOTE

L'étendue de la méthode Producer ne provient pas du bean qui déclare la méthode producer.

Résultat

Les méthodes Producer vous permettent d'injecter des objets non-bean et de changer votre code de façon dynamique.

Report a bug

9.2.7. Beans nommés et beans alternatifs

9.2.7.1. Named Beans

Un Named Bean est un bean nommé qui utilise l'annotation **@Named**. Nommer un bean vous permet de l'utiliser directement dans JSF (Java Server Faces).

L'annotation **@Named** prend un paramètre optionnel, qui correspond au nom du bean. Si le paramètre est omis, le nom du bean en minuscules sera utilisé.

Report a bug

9.2.7.2. Utilisation des Named Beans

1. **Utiliser l'annotation @Named pour assigner un nom à un bean.**

```
@Named("greeter")
public class GreeterBean {
  private Welcome welcome;

  @Inject
  void init (Welcome welcome) {
    this.welcome = welcome;
```

```
  }

  public void welcomeVisitors() {
    System.out.println(welcome.buildPhrase("San Francisco"));
  }
}
```

Le nom du bean en soi est une option. Si vous l'oubliez, le bean sera nommé par rapport à son nom de classe, avec la première lettre en non capitale. Dans l'exemple ci-dessus, le nom par défaut serait donc **greeterBean**.

2. **Utiliser le bean nommé dans une vue JSF**

```
<h:form>
  <h:commandButton value="Welcome visitors" action="#
{greeter.welcomeVisitors}"/>
</h:form>
```

Résultat :

Votre bean nommé correspond à une action dans le contrôle de votre vue JSF, et à un minimum de code.

Report a bug

9.2.7.3. Beans Alternative

Les beans alternatifs sont des beans qui possèdent une implémentation spécifique à un modèle de client particulier ou à un scénario de déploiement particulier.

Exemple 9.13. Définition d'alternatif

Cet alternative se rapporte à une implémentation factice d'à la fois un @Synchronous PaymentProcessor et d'un @Asynchronous PaymentProcessor, en un :

```
@Alternative @Synchronous @Asynchronous

public class MockPaymentProcessor implements PaymentProcessor {

   public void process(Payment payment) { ... }

}
```

Par défaut, les beans @Alternative sont désactivés. Ils sont activés pour une archive bean particulière grâce à la modification du fichier **beans.xml**.

Report a bug

9.2.7.4. Remplacer une injection par une alternative

Résumé

Les beans Alternative vous permettent de remplacer des beans existants. On peut les concevoir comme un moyen d'ajouter une classe qui remplit le même rôle, mais qui fonctionne différemment. Ils sont désactivés par défaut. Cette tâche vous montre comment indiquer et activer une alternative.

Procédure 9.5. Remplacer une injection

Cette tâche part du principe que vous possédez déjà une classe **`TranslatingWelcome`** dans votre projet, mais que vous souhaitez la remplacer par une "fausse" classe TranslatingWelcome. Cela serait le cas pour un déploiement test, où le vrai bean Translator ne peut être utilisé.

1. **Définir l'alternative.**

```
@Alternative
@Translating
public class MockTranslatingWelcome extends Welcome {
  public String buildPhrase(string city) {
    return "Bienvenue Ã  " + city + "!");
  }
}
```

2. **Substituer l'alternative.**
   Pour activer l'implémentation de substitution, ajouter le nom complet de la classe à votre fichier **`META-INF/beans.xml`** ou **`WEB-INF/beans.xml`**.

```
<beans>
  <alternatives>
    <class>com.acme.MockTranslatingWelcome</class>
  </alternatives>
</beans>
```

Résultat

L'implémentation alternative est maintenant utilisée à la place de l'implémentation d'origine.

Report a bug

9.2.8. Stérétypes

9.2.8.1. Stéréotypes

Dans de nombreux systèmes, l'utilisation de modèles architectes produit un ensemble de rôles de beans récurrents. Un stéréotype vous permet d'identifier un tel rôle et de déclarer certaines métadonnées communes pour les beans avec ce rôle dans un emplacement centralisé.

Un stéréotype englobe toute combinaison de :

- scope par défaut
- un groupe de liaisons d'intercepteur

Un stéréotype peut également indiquer un des deux scénarios :

- tous les beans avec un stéréotype ont des noms EL de bean par défaut
- tous les beans avec un stéréotype sont des alternatifs

Un bean peut déclarer zéro, un ou plusieurs stéréotypes. Les annotations de stéréotype peuvent être appliquées à une classe de bean, à une méthode Producer ou à un champ.

Un stéréotype est une annotation, annotée @Stereotype, qui regroupe plusieurs autres annotations.

Une classe qui hérite d'un scope d'un stéréotype peut remplacer ce stéréotype et spécifier un scope directement sur le bean.

De plus, si un stéréotype possède une annotation **@Named**, tout bean sur lequel elle se trouve, a un nom de bean par défaut. Le bean peut remplacer ce nom id l'annotation @Named est directement spécifiée sur le bean. Pour plus d'informations sur les beans nommés, voir Section 9.2.7.1, « Named Beans ».

Report a bug

9.2.8.2. Utilisation des stéréotypes

Résumé

Sans les stéréotypes, les annotations peuvent devenir encombrées. Cette tâche vous montre comment utiliser les stéréotypes pour réduire l'encombrement et simplifier votre code. Pour plus d'informations sur ce que sont les stéréotypes, voir Section 9.2.8.1, « Stéréotypes ».

Exemple 9.14. Encombrement d'annotation

```
@Secure
@Transactional
@RequestScoped
@Named
public class AccountManager {
  public boolean transfer(Account a, Account b) {
    ...
  }
}
```

Procédure 9.6. Définition et utilisation des stéréotypes

1. **Définir le stéréotype**

```
@Secure
@Transactional
@RequestScoped
@Named
@Stereotype
@Retention(RUNTIME)
@Target(TYPE)
public @interface BusinessComponent {
 ...
}
```

2. **Utilisation d'un stéréotype.**

```
@BusinessComponent
public class AccountManager {
  public boolean transfer(Account a, Account b) {
```

```
    ...
  }
}
```

Résultat :

Les stéréotypes rationalisent et simplifient votre code.

Report a bug

9.2.9. Méthodes Observer

9.2.9.1. Méthodes Observer

Les *méthodes Observer* reçoivent des notifications quand un événement a lieu.

CDI fournit des *méthodes Observer de transactions*, qui reçoivent des notifications d'événements *avant* ou *après* la phase de complétion de la transaction dans laquelle l'événement a été dirigé.

Report a bug

9.2.9.2. Appliquer et observer des événements

Exemple 9.15. Appliquer un événement

Ce code vous montre un événement injecté et utilisé dans une méthode.

```
public class AccountManager {
  @Inject Event<Withdrawal> event;

  public boolean transfer(Account a, Account b) {
    ...
    event.fire(new Withdrawal(a));
  }
}
```

Exemple 9.16. Appliquer un événement par un qualificateur

Vous pouvez annoter votre injection d'événement par un qualificateur, pour le rendre plus précis. Pour plus d'informations sur les qualificateurs, voir Section 9.2.3.2, « Qualificateurs ».

```
public class AccountManager {
  @Inject @Suspicious Event <Withdrawal> event;

  public boolean transfer(Account a, Account b) {
    ...
    event.fire(new Withdrawal(a));
  }
}
```

Exemple 9.17. Observer un événement

Pour observer un événement, utiliser l'annotation **@Observes**.

```
public class AccountObserver {
  void checkTran(@Observes Withdrawal w) {
    ...
  }
}
```

Exemple 9.18. Oberver un événement qualifié

Vous pouvez utiliser des qualificateurs pour observer uniquement certains types d'événements. Pour plus d'informations, voir Section 9.2.3.2, « Qualificateurs »

```
public class AccountObserver {
  void checkTran(@Observes @Suspicious Withdrawal w) {
    ...
  }
}
```

Report a bug

9.2.10. Intercepteurs

9.2.10.1. Les intercepteurs

Les intercepteurs font partie de la spécification Enterprise JavaBeans Specification, qui se trouve http://jcp.org/aboutJava/communityprocess/final/jsr318/. Les intercepteurs vous permettent d'ajouter des fonctionnalités aux méthodes commerciales d'un bean sans modifier la méthode de bean directement. L'intercepteur est exécuté avant toute autre méthode commerciale du bean.

CDI améliore cette fonctionnalité en vous permettant d'utiliser des annotations pour lier les intercepteurs aux beans.

Points d'interception

Interception de méthodes commerciales

Un intercepteur de méthode commeciale s'applique aux invocations de méthodes du bean par les clients du bean.

Interception de lifecycle callback

Un intercepteur de lifecycle callback s'applique aux invocations de lifecycle callback par le conteneur.

Interception de méthode de timeout

Un intercepteur de méthode de timeout s'applique aux invocations de métodes d'EJB timeout par le conteneur.

Report a bug

9.2.10.2. Utiliser les intercepteurs dans CDI

Exemple 9.19. Intercepteurs sans CDI

Sans CDI, les intercepteurs ont deux problèmes.

- Le bean doit indiquer l'implémentation de l'intercepteur directement.
- Chaque bean de l'application doit indiquer l'ensemble des intercepteurs dans l'ordre qui convient. Cela fait que l'ajout ou le retrait d'intercepteurs sur la base d'une application prend beaucoup de temps et comporte un risque d'erreur non négligeable.

```
@Interceptors({
  SecurityInterceptor.class,
  TransactionInterceptor.class,
  LoggingInterceptor.class
})
@Stateful public class BusinessComponent {
  ...
}
```

Procédure 9.7. Utiliser les intercepteurs dans CDI

1. **Définir le type de liaison d'intercepteur**

```
@InterceptorBinding
@Retention(RUNTIME)
@Target({TYPE, METHOD})
public @interface Secure {}
```

2. **Marquer l'implémentation de l'intercepteur**

```
@Secure
@Interceptor
public class SecurityInterceptor {
  @AroundInvoke
  public Object aroundInvoke(InvocationContext ctx) throws Exception
{
    // enforce security ...
    return ctx.proceed();
    }
}
```

3. **Utiliser l'intercepteur dans votre code commercial.**

```
@Secure
public class AccountManager {
  public boolean transfer(Account a, Account b) {
    ...
  }
}
```

4. **Activer l'intercepteur dans votre déploiement, en l'ajoutant à votre fichier `META-INF/beans.xml` ou `WEB-INF/beans.xml`.**

```
<beans>
  <interceptors>
    <class>com.acme.SecurityInterceptor</class>
    <class>com.acme.TransactionInterceptor</class>
  </interceptors>
</beans>
```

   Les intercepteurs sont appliqués dans l'ordre indiqué.

Résultat :

CDI simplifie votre code d'intercepteur et simplifie l'application de votre code commercial.

Report a bug

9.2.11. Les décorateurs

Un décorateur intercepte les invocations d'une interface Java particulière. Il est conscient de tous les sémantiques de cette interface. Les décorateurs sont utiles pour des modèles commerciaux particuliers, mais ne possèdent pas la généralité des intercepteurs. C'est un bean, voire même une classe abstraite, qui implémente le type qu'il décore, et est annoté avec `@Decorator`.

Exemple 9.20. Exemple de décorateur

```
@Decorator

public abstract class LargeTransactionDecorator

      implements Account {

   @Inject @Delegate @Any Account account;

   @PersistenceContext EntityManager em;

   public void withdraw(BigDecimal amount) {

      ...

   }

   public void deposit(BigDecimal amount);

      ...

   }

}
```

Report a bug

9.2.12. Extensions portables

CDI doit être une fondation de frameworks, d'extensions et d'intégration à d'autres technologies. De ce fait, CDI expose un ensemble de SPI à utiliser par les développeurs d'extensions portables aux CDI. Les extensions fournissent ces types de fonctionnalités :

- intégration par les moteurs de Business Process Management
- intégration aux frameworks de tierce partie comme Spring, Seam, GWT ou Wicket
- nouvelle technologie basée sur le modèle de programmation CDI

D'après la spécification JSR-299, une extension portable peut s'intégrer avec le conteneur d'une des manières suivantes :

- En fournissant ainsi ses propres beans, intercepteurs et décorateurs au conteneur
- En injectant des dépendances dans ses propres objets en utilisant le service d'injections de dépendances
- En fournissant une implémentation de contexte pour un scope personnalisé
- En augmentant ou en remplaçant les métadonnées basées annotation par les métadonnées d'autres sources

Report a bug

9.2.13. Proxies Beans

9.2.13.1. Proxys Bean

Un proxy est une sous-classe de bean, qui est générée lors de l'exécution. Il est injecté au moment de la création du bean et les beans scoped dépendants peuvent être injectés, parce que les cycles de vie des beans dépendants sont liés au proxy. Les proxys sont utilisées en tant que substitut pour l'injection de dépendance et de résolvent deux problèmes différents.

Problèmes d'injection de dépendance, qui sont résolus en utilisant les proxys.

- Performance - les proxys sont bien plus rapides que l'injection de dépendance, donc vous pouvez les utiliser dans des beans qui requièrent une haute performance.
- Thread safety - les proxys envoient des requêtes vers l'instance de bean qui convient, même quand plusieurs threads accèdent à un bean en même temps.

Classes qui ne peuvent pas être mises en proxy

- Types Primitives ou Tableaux
- Classes `final` ou qui possèdent une méthode `final`
- Classes qui ont un constructeur non-privé par défaut

Report a bug

9.2.13.2. Utiliser un Proxy ou une Injection

Aperçu

Un proxy est utilisé pour l'injection quand les cycles de vie des beans sont différents les uns des autres. Le proxy est une sous-classe du bean qui est créée au moment de l'exécution et qui remplace toutes les méthodes non privées de la classe de bean. Le serveur proxy transmet l'invocation sur l'instance réelle du bean.

Dans cet exemple, l'instance **`PaymentProcessor`** n'est pas injectée directement dans **Shop**. À la place, un proxy est injecté, et quand la méthode **`processPayment()`** est appelée, le proxy cherche l'instance de bean courante **`PaymentProcessor`** et appelle la méthode **`processPayment()`** dessus.

Exemple 9.21. Injection de proxy

```
@ConversationScoped
class PaymentProcessor
{
  public void processPayment(int amount)
  {
    System.out.println("I'm taking $" + amount);
  }
}

@ApplicationScoped
public class Shop
{

  @Inject
  PaymentProcessor paymentProcessor;

  public void buyStuff()
  {
    paymentProcessor.processPayment(100);
  }
}
```

Pour plus d'informations sur les proxys, y compris les types de classes qui peuvent être mises en proxy, voir Section 9.2.13.1, « Proxys Bean ».

Report a bug

CHAPITRE 10. JAVA TRANSACTION API (JTA)

10.1. APERÇU

10.1.1. Java Transactions API (JTA)

Introduction

Ces topics vous donnent des explications de base sur l'API Java Transactions (JTA).

- Section 10.2.5, « JTA (Java Transactions API) »
- Section 10.5.2, « Cycle de vie d'une transaction JTA »
- Section 10.9.3, « Exemple de transaction JTA »

Report a bug

10.2. CONCEPTS DE TRANSACTIONS

10.2.1. Transactions

Une transaction se compose de deux ou plusieurs actions qui doivent toutes réussir ou échouer. Le succès est une validation et un échec est un roll-back. Dans un roll-back, l'état de chaque membre retourne à son état d'origine, avant que la transaction ait été commise.

Le standard d'une transaction bien conçue est qu'elle doit être *Atomique, Consistante, Isolée, et Durable (ACID).*

Report a bug

10.2.2. Les propriétés ACID de transactions

ACID est un acronyme pour **`Atomicity`**, **`Consistency`**, **`Isolation`**, et **`Durability`**. Cette terminologie est normalement utilisée dans le contexte de bases de données ou d'opérations transactionnelles.

Définitions ACID

Atomicité

Pour qu'une transaction soit atomique, tous les membres de la transaction doivent prendre la même décision. Ils doivent soit tous valider, soit tous se retirer. Si l'atomicité est cassée, ce qui en résultera s'appelle un *heuristic outcome*..

Homogénéité

Homogénéité signifie que les données écrites dans la base de données doivent être valides, en terme de schéma de base de données. La base de donnée et les autres sources de données doivent toujours être dans un état consistant. Par exemple, un état inconsistant pourrait correspondre à un champ dans lequel la moitié des données sont écrites avant qu'une opération n'échoue. Dans le cas d'un état consistant, toutes les données sont écrites, et l'écriture est retirée si incomplète.

Isolation

Isolation signifie que les données ajoutées à l'opération doivent être verrouillées avant toute modification, pour ne pas que les processus modifient les données au delà de la portée de la transaction en question.

Durabilité

Durabilité signifie qu'en cas d'échec externe, après que les membres d'une transaction aient été instruits de valider, tous les membres seront disponibles pour continuer la validation de la transaction quand l'échec sera résolu. Cette défaillance est sans doute liée au matériel, logiciels, réseau, ou tout autre système impliqué.

Report a bug

10.2.3. Coordinateur de transactions ou Gestionnaire de transactions

Les termes *Transaction Coordinator* et *Transaction Manager* sont généralement interchangeables en terme de transaction avec JBoss EAP 6. Le terme Transaction Coordinator est généralement utilisé dans un contexte de transactions distribuées.

Dans les transactions JTA, le *Transaction Manager* s'exécute dans JBoss EAP 6 et communique avec les participants de la transaction pendant le protocole *two-phase commit*.

Le gestionnaire de transactions ordonne aux participants de commettre ou de retirer leurs données, selon le résultat des autres participants. De cette façon, il s'assure que les transactions respectent la norme ACID.

Pour les transactions JTS, le Coordinateur de transactions gère les interactions entre les gestionnaires de transactions sur des serveurs différents.

- Section 10.2.4, « Participants d'une transaction. »
- Section 10.2.2, « Les propriétés ACID de transactions »
- Section 10.2.9, « Le protocole de validation en 2-Phases »

Report a bug

10.2.4. Participants d'une transaction.

Un participant est un processus qui se trouve dans une transaction, avec une possibilité de valider ou de retirer l'état. Il peut s'agir d'une base de données ou d'une toute autre application. Chaque participant à une transaction se mettent d'accord pour valider son état si tous les autres participants peuvent le faire également. Sinon, chacun d'entre eux sera retiré et la transaction n'aura pas lieu. Le gestionnaire de transactions coordonne les opérations de validation ou de renvoi et il détermine le résultat de la transaction.

- Section 10.2.1, « Transactions »
- Section 10.2.3, « Coordinateur de transactions ou Gestionnaire de transactions »

Report a bug

10.2.5. JTA (Java Transactions API)

Java Transactions API (JTA) est une spécification pour les transactions à utiliser dans les applications JBoss Enterprise Edition. Définie dans JSR-907.

Les transactions JTA ne sont pas distribuées à travers les serveurs d'applications multiples, et ne peuvent pas être imbriquées.

Les transactions JTA sont contrôlées par le conteneur EJB. Les annotations sont une méthode pour créer et contrôler des transactions dans votre code.

Report a bug

10.2.6. JTS (Java Transaction Service)

*Java Transaction Service (JTS)*est un mécanisme servant à soutenir les transactions Java Transaction API (JTA) quand les participants des transactions se trouvent dans de multiples conteneurs Java Enterprise Edition (serveurs d'application). Tout comme dans les transactions JTA locales, chaque conteneur exécute un procédé appelé *Transaction Manager (TM)*. Les TM communiquent entre eux grâce à un procédé appelé *Object Request Broker (ORB)*, et une communication standard appelée *Common Object Request Broker Architecture (CORBA)*.

D'un point de vue d'une application, une transaction JTS fonctionne de la même façon qu'une transaction JTA. La différence est que les participants de la transaction et les sources de données se trouvent dans des conteneurs différents.

NOTE

L'implémentation de JTS compris dans JBoss EAP 6 prend en charge les *distributed JTA transactions*. La différence entre les transactions JTA distribuées et les transactions JTS entièrement compatibles est l'interopérabilité avec les ORB de tierce-parties externes. Cette fonctionnalité n'est pas prise en charge dans JBoss EAP 6. Les configurations prises en charge distribuent des transactions à travers des conteneurs JBoss EAP 6 multiples uniquement.

- Section 10.2.11, « Les transactions distribuées »
- Section 10.2.3, « Coordinateur de transactions ou Gestionnaire de transactions »

Report a bug

10.2.7. Sources de Données XA et Transactions XA

Une source de données XA correspond à une source de données qui peut participer à une transaction globale XA.

Une transaction XA est une transaction qui peut s'étendre sur plusieurs ressources. Comprend un gestionnaire de coordination des transactions, avec une ou plusieurs bases de données ou d'autres ressources transactionnelles, toutes impliquées dans une transaction globale unique.

Report a bug

10.2.8. La Récupération XA

L'API JTA (Java Transaction API) autorise les transactions distribuées sur de multiples *X/Open XA resources*. XA signifie *Extended Architecture*, qui a été développée par le groupe X/Ouvert pour définir une transaction qui utilise plus d'une banque de données principale. La norme XA décrit l'interface

entre un *Transaction Manager (TM)* global et un manager de ressources local. XA autorise de multiples ressources, telles que les serveurs d'application, les bases de données, les caches et les queues de message, à participer à la même transaction, tout en préservant l'atomicité de la transaction. Atomicité signifie que si l'un des participants ne parvient pas à appliquer ses changements, les autres participants metteront fin à la transaction, et restaureront leur état au même statut qu'ils possédaient avant que la transaction n'ait été effectuée.

XA Recovery est le procédé visant à garantir que toutes les ressources affectées par une transaction soient mises à jour ou annulées, même si certaines de ces ressources sont un crash de participants à la transaction ou deviennent indisponibles. Dans le scope de JBoss EAP 6, le sous-système de transaction fournit les mécanismes pour une récupération XA à toute ressource XA ou à tout sous-systèmes qui les utilise, comme les sources de données XA, les queues de messages JMS et les adaptateurs de ressources JCA.

La récupération XA se produit sans l'intervention de l'utilisateur. Dans le cas d'un échec de récupération XA, les erreurs sont enregistrées dans la sortie du journal. Veuillez contacter le Service d'assistance globale de Red Hat pour toute demande d'assistance.

Report a bug

10.2.9. Le protocole de validation en 2-Phases

Le protocole de validation en 2 phases (2PC) correspond à un algorithme qui détermine le résultat d'une transaction.

Phase 1

Au cours de la première phase, les participants à la transaction indiquent au coordinateur de transaction s'ils sont en mesure de valider la transaction ou bien, ils devront la retirer.

Phase 2

Dans la deuxième phase, le coordinateur de transactions prend la décision à savoir si l'opération globale doit être validée ou bien, retirée. Si l'un des participants ne peut pas valider, la transaction sera retirée. Sinon, l'opération peut être validée. Le coordinateur dirige les opérations et en notifie le coordinateur quand les décisions sont prises. À ce moment-là, la transaction est terminée.

Report a bug

10.2.10. Les délais d'attente de transactions

Afin de préserver l'atomicité et de respecter la norme ACID des transactions, certaines parties d'une transaction peuvent être longues. Les participants à la transaction doivent verrouiller des pièces de sources de données lorsqu'ils commettent, et le gestionnaire de transactions doit attendre d'avoir des nouvelles de chaque participant à une transaction avant de pouvoir tous les diriger à commettre ou à annuler. Les ressources d'être verrouillés indéfiniment pour cause de panne de matériel ou de réseau.

Les délais d'attente de transactions peuvent être associés à des transactions afin de contrôler leur cycle de vie. Si un seuil de délai d'attente passe avant que la transaction s'engage ou annule, le délai d'attente provoque l'annulation de l'opération automatiquement.

Vous pouvez configurer les valeurs de délai d'attente par défaut pour tout le sous-système de la transaction, ou bien, vous pouvez désactiver les valeurs de délai d'attente par défaut et spécifier les délais d'attente sur une base d'une transaction.

Report a bug

10.2.11. Les transactions distribuées

Une *distributed transaction*, ou *distributed Java Transaction API (JTA) transaction*est une transaction avec des participants sur de multiples serveurs JBoss EAP 6. Les transactions distribuées diffèrent des *Java Transaction Service (JTS) transactions*du fait que les spécifications JTS requièrent que les transactions puissent être distribuées à travers les serveurs d'application de différents fournisseurs. Le JBoss EAP prend en charge les transactions JTA distribuées.

Report a bug

10.2.12. API de Portabilité ORB

L'Object Request Broker (ORB) est un processus qui envoie et reçoit des messages pour des participants de la transaction, des coordonnateurs, des ressources et autres services distribués sur plusieurs serveurs d'applications. Un ORB utilise un IDL (Interface Description Language) pour communiquer et interpréter des messages. *Common Object Request Broker Architecture (CORBA)*est l'IDL utilisé par l'ORB dans JBoss EAP 6.

Le principal type de service qui utilise un ORB est un système de Transactions Java distribuées, qui utilise le protocole Java Transaction Service (JTS). Les autres systèmes, notamment les systèmes hérités, peuvent choisir d'utiliser un ORB pour la communication, plutôt que d'autres mécanismes tels que Enterprise JavaBeans à distance ou les services JAX-WS ou JAX-RS Web.

L'API de portabilité ORB fournit des mécanismes pour interagir avec un ORB. Cet API fournit des méthodes pour obtenir une référence à l'ORB, ainsi que pour placer une application dans un mode d'écoute des connexions entrantes de l'ORB. Certaines des méthodes de l'API ne sont pas supportées par tous les ORB. Dans ces cas, une exception sera levée.

Un API comprend plusieurs classes :

Classes API de la Portabilité ORB

- `com.arjuna.orbportability.orb`
- `com.arjuna.orbportability.oa`

Voir les documents JBoss EAP 6 Javadocs du portail Red Hat Customer pour obtenir des détails sur les méthodes et les propriétés incluses dans l'API de Portabilité ORB.

Report a bug

10.2.13. Transactions imbriquées

Les transactions imbriquées sont des transactions dans lesquelles les participants sont également des transactions.

Les avantages des transactions imbriquées

Isolation des erreurs

Si une sous-transaction s'annule, par exemple parce qu'un objet utilisé échoue, la transaction englobante ne nécessite pas d'être annulée.

Modularité

Si une transaction est déjà associée à un appel quand une nouvelle transaction commence, la nouvelle transaction sera imbriquée à l'intérieur. Dès lors, si vous savez qu'un objet requiert des

transactions, vous pouvez les imbriquer dans l'objet. Si les méthodes de l'objet sont invoquées sans une transaction client, alors les transactions de l'objet sont de niveau supérieur. Sinon, elles sont imbriquées dans l'étendue des transactions du client. De la même manière, un client n'a pas besoin de savoir si un objet est transactionnel. Il peut commencer sa propre transaction.

Les transactions imbriquées sont seulement prises en charge dans le cadre de l'API JTS (Java Transaction Service) et non pas dans le cadre du JTA (Java Transaction API). Le fait de tenter d'imbriquer des transactions JTA (non distribuées) entraîne une exception.

Report a bug

10.3. OPTIMISATIONS DE TRANSACTIONS

10.3.1. Optimisations de transactions

Introduction

Le sous-système de transactions de JBoss EAP 6 inclut plusieurs optimisations dont vous pouvez tirer avantage pour vos applications.

- Section 10.3.3, « Optimisation Presumed-Abort »
- Section 10.3.4, « Optimisation Lecture-seule »
- Section 10.3.2, « Optimisation LRCO pour une validation en 1 phase (1 PC) »

Report a bug

10.3.2. Optimisation LRCO pour une validation en 1 phase (1 PC)

Bien que le protocole de validation en deux phases (2PC) soit plus commun, certaines situations ne peuvent pas accommoder les deux phases. Dans ces cas, vous pouvez utiliser le protocole *single phase commit (1PC)*. Un cas d'application est quand une source de données non-XA-aware doit participer à la transaction.

Dans ces situations, une optimisation appelée *Last Resource Commit Optimization (LRCO)*est employée. La ressource monophasée est traitée en dernier dans la phase de préparation de la transaction, et il y a une tentative de validation. Si la validation réussit, le journal des transactions est écrit et les ressources restantes passent par le protocole 2PC. Si la dernière ressource ne parvient pas à être validée, la transaction est annulée.

Malgré que ce protocole permet le traitement de la plupart des opérations, certains types d'erreurs peuvent aboutir à des résultats de transactions inconsistants. Il est donc recommandé d'utiliser cette approche en dernier ressort.

Quand on utilise une source de données locale TX dans une transaction, l'optimisation LRCO est automatiquement appliquée.

- Section 10.2.9, « Le protocole de validation en 2-Phases »

Report a bug

10.3.3. Optimisation Presumed-Abort

Quand une transaction est sur le point d'être supprimée, elle peut enregistrer ces informations

localement et informer tous les participants inscrits. Cette notification est une courtoisie seulement et n'a aucun effet sur le résultat de la transaction. Après que tous les participants aient été contactés, les informations sur la transaction peuvent être supprimés.

Si une demande subséquente au sujet de l'état de la transaction se produit, il y n'aura aucun information disponible. Dans ce cas, le demandeur suppose que la transaction a avorté et a été restaurée. Cette Optimisation *presumed-abort* indique qu'aucune information sur les participants ne doit être rendue persistante tant que la transaction n'a pas été engagée, car tout échec avant ce point sera considéré comme un abandon de la transaction.

Report a bug

10.3.4. Optimisation Lecture-seule

Lorsqu'un participant est invité à se préparer, il peut indiquer au coordonnateur qu'il n'a pas modifié de données durant la transaction. Une tel participant n'a pas besoin d'être informé de l'issue de l'opération, puisque le sort du participant n'a aucun effet sur la transaction. Ce participant *read-only* peut être omis de la deuxième phase du protocole de validation.

Report a bug

10.4. RÉSULTATS DE TRANSACTIONS

10.4.1. Résultats de transactions

Il y a trois résultats possibles suite à une transaction.

Roll-back

Si un participant à une transaction ne peut pas effectuer une validation, ou si le coordinateur de transaction ne peut pas indiquer aux participants de valider, la transaction sera annulée. Voir Section 10.4.3, « Transactions Roll-Back » pour plus d'informations.

Valider

Si chaque participant à une transaction peut valider, le coordinateur de transactions leur indique comment procéder, Voir Section 10.4.2, « Transactions de validation » pour plus d'informations.

Résultat heuristique

Si certains participants à une transaction valident, et que d'autres annulent, on parle de résultat heuristique. Les résultats heuristiques dérivent d'interventions humaines. Voir Section 10.4.4, « Résultats heuristiques » pour plus d'informations.

Report a bug

10.4.2. Transactions de validation

Lorsqu'un participant à une transaction fait une validation, il rend son nouvel état durable. Le nouvel état est créé par le participant qui effectue le travail dans la transaction. L'exemple le plus courant est lorsqu'un membre de la transaction écrit des enregistrements à une base de données.

Suite à la validation, les informations sur la transaction sont retirées du coordinateur de transactions, et l'état nouvellement inscrit est maintenant l'état durable.

Report a bug

10.4.3. Transactions Roll-Back

Un participant à une transaction est considéré «roll-back» quand son état est restauré pour refléter son état qui précède le début de la transaction. Après un «roll-back», l'état n'est le même que si la transaction n'avait jamais eu lieu.

Report a bug

10.4.4. Résultats heuristiques

Un résultat heuristique, ou résultat non atomique, est une anomalie de la transaction. Il se réfère à une situation où certains participants de transaction ont validé leur état, et d'autres l'ont annulé. Un résultat heuristique entraîne une incompatibilité entre les états.

Les résultats heuristiques se produisent généralement au cours de la deuxième phase du protocole de validation à 2 phases (2PC). Ils sont souvent causées par des échecs au niveau du matériel sous-jacent ou des sous-systèmes de communication des serveurs sous-jacents.

Il y a quatre types de résultats heuristiques différents.

Rollback heuristique

L'opération de validation a échoué car certains ou tous les participants ont abandonné la transaction.

Validation heuristique

Une opération de tentative de restauration a échoué, car tous les participants ont validé unilatéralement. Cela peut se produire si, par exemple, le coordinateur est en mesure de préparer correctement la transaction, mais décide alors de l'annuler en raison d'une défaillance de son côté, comme un oubli de mettre à jour son journal. Dans l'intervalle, les participants peuvent décider de valider.

Mixed heuristiques

Certains participants ont validé et d'autres ont abandonné

Danger heuristique

Le résultat de certaines mises à jour est inconnu. Pour les connus, ils ont soit tous été validés ou annulés.

Les résultats heuristiques peuvent entraîner pertes d'intégrité dans le système, et nécessitent généralement une intervention humaine pour être résolus. Ne créez pas de code qui en dépende.

- Section 10.2.9, « Le protocole de validation en 2-Phases »

Report a bug

10.4.5. Erreurs et exceptions pour les transactions JBoss

Pour obtenir des informations lancées par les méthodes de la classe **`UserTransaction`**, voir la spécification *UserTransaction API* dans http://download.oracle.com/javaee/1.3/api/javax/transaction/UserTransaction.html.

Report a bug

10.5. APERÇU SUR LES TRANSACTIONS JTA

10.5.1. JTA (Java Transactions API)

Java Transactions API (JTA) est une spécification pour les transactions à utiliser dans les applications JBoss Enterprise Edition. Définie dans JSR-907.

Les transactions JTA ne sont pas distribuées à travers les serveurs d'applications multiples, et ne peuvent pas être imbriquées.

Les transactions JTA sont contrôlées par le conteneur EJB. Les annotations sont une méthode pour créer et contrôler des transactions dans votre code.

Report a bug

10.5.2. Cycle de vie d'une transaction JTA

Quand une ressource demande à participer dans une transaction, une chaîne d'événements est démarrée. Le *Transaction Manager* ou Gestionnaire de transactions est un processus qui réside dans le serveur de l'application et qui gère les transactions. Les *participants à la transaction*sont des objets qui participent à une transaction. Les *Resources* sont des sources de données, des usines de connexion JMS, ou autres connexions JCA.

1. **Votre application démarre une nouvelle transaction**
   Pour démarrer une transaction, votre application doit obtenir une instance de la classe **`UserTransaction`** du JNDI ou bien, s'il s'agit d'un EJB, en provenance d'une annotation. L'interface **`UserTransaction`** comprend des méthodes pour commencer, valider, ou annuler des transactions au plus haut niveau. Les transactions nouvellement créées sont associées automatiquement à leur thread invoquant. Les transactions imbriquées ne sont pas supportées dans JTA, donc toutes les transactions sont des transactions au plus haut niveau.

   En appelant **`UserTransaction.begin()`**, on commence une nouvelle transaction. Toute ressource qui est utilisée après cela sera associée à la transaction. S'il y a plus plus d'une seule ressource listée, votre transaction devient une transaction XA, et participera au protocole de validation en deux temps.

2. **Votre application modifie son état.**
   Dans l'étape suivante, votre transaction effectue son travail et précède aux changements d'état.

3. **Votre application décide de valider ou de s'annuler**
   Quand votre application a fini de changer d'état, elle décide si elle doit valider ou s'annuler. Elle appelle la méthode qui convient. Elle appelle **`UserTransaction.commit()`** ou **`UserTransaction.rollback()`**. C'est quand le protocole en deux phases (2PC) a lieu si vous avez listé plus d'une ressource. Section 10.2.9, « Le protocole de validation en 2-Phases »

4. **Le gestionnaire de transactions supprime la transaction des archives.**
   Après la validation ou l'annulation, le gestionnaire de transactions nettoie ses archives et supprime les informations sur votre transaction.

Recouvrement d'échec

Le recouvrement d'échec a lieu automatiquement. Si une ressource, un participant à une transaction, ou un serveur d'applications est disponible, le gestionnaire de transactions s'occupe du recouvrement quand l'échec sous-jacent est résolu.

- Section 10.2.1, « Transactions »
- Section 10.2.3, « Coordinateur de transactions ou Gestionnaire de transactions »
- Section 10.2.4, « Participants d'une transaction. »
- Section 10.2.9, « Le protocole de validation en 2-Phases »
- Section 10.2.7, « Sources de Données XA et Transactions XA »

Report a bug

10.6. CONFIGURATION DE SOUS-SYSTÈME DE TRANSACTION

10.6.1. Configuration des transactions

Introduction

Les procédures suivantes vous montrent comment configurer le sous-système de transactions de JBoss EAP 6.

- Section 10.6.2.1, « Configurez votre base de données pour utiliser les Transactions JTA »
- Section 10.6.2.2, « Configuration d'une source de données XA »
- Section 10.7.8.2, « Configurer le Transaction Manager (TM) ou Gestionnaire de transactions »
- Section 10.6.3.2, « Configurer la journalisation des sous-systèmes de transactions »

Report a bug

10.6.2. Configuration de source de données transactionnelle

10.6.2.1. Configurez votre base de données pour utiliser les Transactions JTA

Résumé

Cette tâche vous montre comment activer JTA (Java Transactions API) sur votre source de données.

Prérequis

Vous devez remplir les conditions suivantes avant de continuer cette tâche :

- Votre base de données ou autre ressource devra supporter JTA. Dans le doute, veuillez consulter la documentation.
- Créer une source de données. Veuillez vous référer à Section 10.6.2.4, « Créer une source de données Non-XA avec les interfaces de gestion ».
- Stopper le serveur JBoss EAP 6
- Obtenir un accès pour pouvoir éditer les fichiers de configuration directement, dans un éditeur de texte.

Procédure 10.1. Configurer la Source de données pour utiliser les Transactions JTA.

1. **Ouvrir le fichier de configuration dans l'éditeur de texte.**
   Selon si vous exécutez JBoss EAP 6 sur un domaine géré ou un serveur autonome, votre fichier de configuration ne se trouvera pas au même endroit.

   - **Domaine géré**
     Le fichier de configuration par défaut d'un domaine géré se trouve dans `EAP_HOME/domain/configuration/domain.xml` pour Red Hat Enterprise Linux, et `EAP_HOME\domain\configuration\domain.xml` pour Microsoft Windows Server.

   - **Serveur autonome**
     Le fichier de configuration par défaut d'un serveur autonome se trouve dans `EAP_HOME/standalone/configuration/domain.xml` pour Red Hat Enterprise Linux, et `EAP_HOME\standalone\configuration\domain.xml` pour Microsoft Windows Server.

2. **Chercher la balise `<datasource>` qui correspond à votre source de données.**
   La source de données aura un attribut `jndi-name` correspondant à celui que vous aviez indiqué quand vous l'avez créée. Par exemple, la source de données ExampleDS ressemble à ceci :

   ```
   <datasource jndi-name="java:jboss/datasources/ExampleDS" pool-
   name="H2DS" enabled="true" jta="true" use-java-context="true" use-
   ccm="true">
   ```

3. **Définir l'attribut `jta` à `true`.**
   Ajouter l'élément suivant au contenu de votre balise **`<datasource>`**, tel qu'il apparaît à l'étape précédente : **`jta="true"`**

4. **Sauvegarder le fichier de configuration.**
   Sauvegarder le fichier de configuration et sortir de l'éditeur de texte.

5. **Démarrer JBoss EAP 6.**
   Relancer le serveur JBoss EAP 6.

Résultat :

JBoss EAP 6 démarre, et votre source de données est configurée pour utiliser les transactions JTA.

Report a bug

10.6.2.2. Configuration d'une source de données XA

Prérequis

Pour pouvoir ajouter une source de données XA, vous devrez vous connecter à la console de gestion. Voir Section 10.6.2.3, « Se conncecter à la console de gestion » pour plus d'informations.

1. **Ajouter une nouvelle source de données.**
   Ajouter une nouvelle source de données à la plateforme JBoss EAP 6. Suivre les instructions qui se trouvent dans Section 10.6.2.4, « Créer une source de données Non-XA avec les interfaces de gestion », puis, cliquer sur l'onglet **`XA Datasource`** en haut.

2. **Configurer les propriétés supplémentaires suivant les besoins.**

Tous les paramètres de la source de données se trouvent dans Section 10.6.2.5, « Paramètres de source de données ».

Résultat

Votre source de données XA est configurée et prête à l'utilisation.

Report a bug

10.6.2.3. Se conncecter à la console de gestion

Prérequis

- JBoss EAP doit être en cours d'exécution.

Procédure 10.2. Se conncecter à la console de gestion

1. **Naviguer vers la page de démarrage de la console de gestion**
   Naviguer vers la console de gestion. L'emplacement par défaut est http://localhost:9990/console/, où le port 9990 est prédéfini comme liaison de socket de console de gestion.

2. **Se conncecter à la console de gestion**
   Saisir le nom d'utilisateur et le mot de passe du compte que vous avez déjà créé pour vous connecter à l'écran de connexion de la console de gestion.

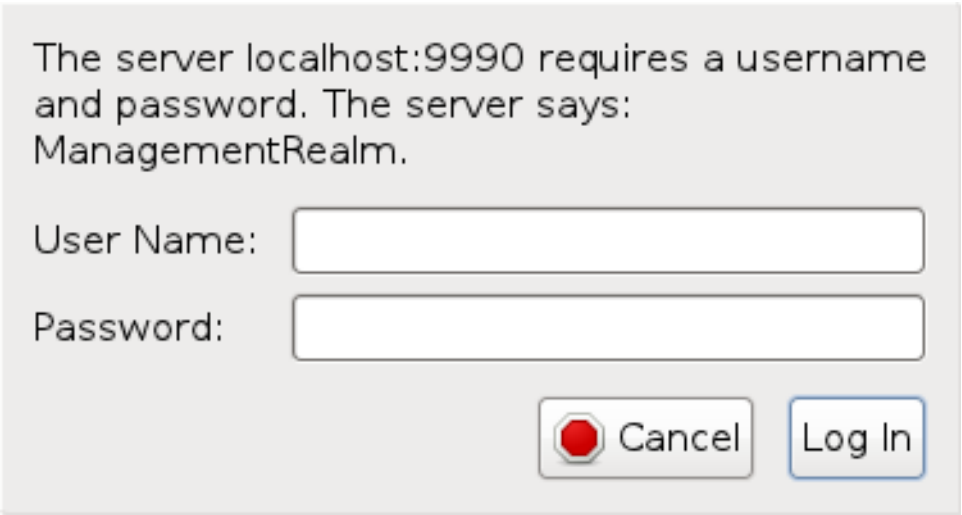


Figure 10.1. Écran de connexion de la console de gestion

Résultat

Une fois connecté, une des pages de la console de gestion apparaîtra :

Domaine géré

http://localhost:9990/console/App.html#server-instances

Serveur autonome

http://localhost:9990/console/App.html#server-overview

Report a bug

10.6.2.4. Créer une source de données Non-XA avec les interfaces de gestion

Résumé

Cette section explique les étapes à suivre pour créer une source de données non-XA, en utilisant la console de gestion ou le Management CLI.

Prérequis

- Le serveur JBoss EAP 6 doit être en cours d'exécution.

NOTE

Avant la version 10.2 de la source de données Oracle, le paramètre <no-tx-separate-pools/> était requis, car le mélange de connexions transactionnelles et non-transactionnelles auraient créé une erreur. Ce paramètre n'est plus requis pour certaines applications.

Procédure 10.3. Créer une source de données en utilisant le Management CLI ou la console de gestion

- **Management CLI**
  a. Lancer l'outil CLI et connectez-vous à votre serveur.
  b. Exécuter la commande suivante pour créer une source de données non-XA, et configurer les variables comme il se doit :

```
data-source add --name=DATASOURCE_NAME --jndi-name=JNDI_NAME --driver-name=DRIVER_NAME  --connection-url=CONNECTION_URL
```

  c. Activer la source de données :

```
data-source enable --name=DATASOURCE_NAME
```

- **Console de gestion**
  a. Connectez-vous à la Console de gestion.
  b. **Naviguez dans le panneau `Datasources` qui se trouve dans la console de gestion**
    i. - **Mode autonome**
       Sélectionnez l'onglet **`Profil`** qui se trouve en haut et à droite de la console.
       - **Mode Domaine**
         A. Sélectionnez l'onglet **`Profiles`** qui se trouve en haut et à droite de la console.
         B. Sélectionner le profil qui convient à partir du menu déroulant en haut à gauche.
         C. Étendre le menu **Subsystems** qui se trouve à gauche de la console.
    ii. Sélectionner **Connector** → **Datasources** à partir du menu à gauche de la console.

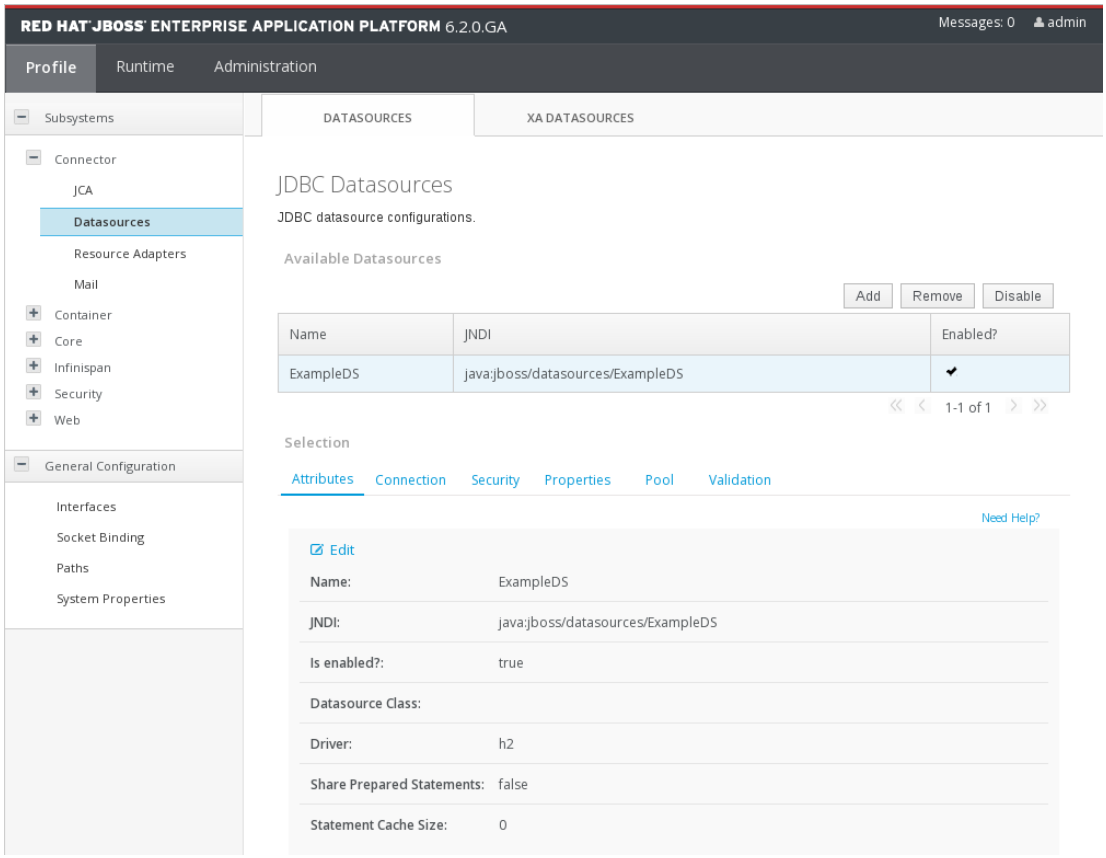


Figure 10.2. Panneau de sources de données

c. **Créer une nouvelle source de données**

   i. Sélectionner le bouton **Add** qui se trouve en haut du panneau **`Datasources`**.

   ii. Saisir les attributs de la nouvelle source de données de l'assistant **`Create Datasource`** et appuyez sur **`Next`**.

   iii. Saisir les informations sur le pilote JDBC dans l'assistant **`Create Datasource`** et appuyez sur **`Next`**.

   iv. Saisir les paramètres de connexion dans l'assistant **`Create Datasource`** et appuyez sur **Done**.

Résultat

La source de données non-Xa a été ajoutée au serveur. Elle est maintenant visible dans le fichier **`standalone.xml`** ou le fichier **`domain.xml`**, ainsi que dans les interfaces de gestion.

Report a bug

10.6.2.5. Paramètres de source de données

Tableau 10.1. Les paramètres de source de données communs aux sources XA ou non-XA

Paramètre	Description
jndi-name	Le nom JNDI unique pour la source de données.

Paramètre	Description
pool-name	Le nom du pool de gestion de la source de données.
activé	Indique si la source de données est activée.
use-java-context	Indique si on doit relier la source de données au JNDI global.
spy	Activer la fonctionnalité **spy** sur la couche JDBC. Cela journalisera tout le trafic JDBC dans la source de données. Le paramètre **logging-category** doit également être défini à **org.jboss.jdbc**.
use-ccm	Activer le gestionnaire de connexion cache.
new-connection-sql	Un énoncé SQL qui exécute quand la connexion est ajoutée au pool de connexion.
transaction-isolation	Un parmi : • TRANSACTION_READ_UNCOMMITTED • TRANSACTION_READ_COMMITTED • TRANSACTION_REPEATABLE_READ • TRANSACTION_SERIALIZABLE • TRANSACTION_NONE
url-delimiter	Le délimiteur d'URLs d'une connexion url pour les bases de données clusterisées HA (Haute disponibilité).
url-selector-strategy-class-name	Une classe qui implémente l'interface **org.jboss.jca.adapters.jdbc.URLSelectorStrategy**.
sécurité	Contient des éléments dépendants en tant que paramètres de sécurité. Voir Tableau 10.6, « Paramètres de sécurité ».
validation	Contient des éléments dépendants en tant que paramètres de validation. Voir Tableau 10.7, « Paramètres de validation ».
timeout	Contient des éléments dépendants en tant que paramètres de timeout. Voir Tableau 10.8, « Paramètres de timeout ».

Paramètre	Description
énoncé	Contient des éléments dépendants en tant que paramètres d'énoncés. Voir Tableau 10.9, « Paramètres d'instruction ».

Tableau 10.2. Paramètres de source de données non-xa

Paramètre	Description
jta	Active l'intégration JTA pour les sources de données non-XA. Ne s'applique pas aux sources de données XA.
connection-url	L'URL de connexion du pilote JDBC.
driver-class	Le nom complet de la classe de pilote JDBC.
connection-property	Propriétés de connexions arbitraires passées à la méthode **`Driver.connect(url,props)`**. Chaque connection-property indique une paire name/value. Le nom de la propriété provient du nom, et la valeur provient du contenu de l'élément.
pool	Contient des éléments dépendants en tant que paramètres de pooling. Voir Tableau 10.4, « Les paramètres de pool communs aux sources XA ou non-XA ».

Tableau 10.3. Paramètres de source de données XA

Paramètre	Description
xa-datasource-property	Une propriété pour assigner la classe d'implémentation **`XADataSource`**. Spécifiée par *name=value*. Si une méthode setter existe, dans le format **`set`*`Name`***, la propriété sera définie en appelant une méthode setter sous le format **`set`*`Name`*`(`*`value`*`)`**.
xa-datasource-class	Le nom complet de la classe d'implémentation de **`javax.sql.XADataSource`**.
pilote	Unique référence au module de chargeur de classe qui contient le pilote JDBC. Le format accepté est *driverName#majorVersion.minorVersion*.
xa-pool	Contient des éléments dépendants en tant que paramètres de pooling. Voir Tableau 10.4, « Les paramètres de pool communs aux sources XA ou non-XA » et Tableau 10.5, « Paramètres du pool XA »

Paramètre	Description
recouvrement	Contient des éléments dépendants en tant que paramètres de recouvrement. Voir Tableau 10.10, « Paramètres de recouvrement ».

Tableau 10.4. Les paramètres de pool communs aux sources XA ou non-XA

Paramètre	Description
min-pool-size	Le nombre minimum de connexions contenues par un pool.
max-pool-size	Le nombre maximum de connexions qu'un pool peut contenir
Pré-remplissage	Indique si l'on doit essayer de pré-remplir un pool de connexion. Un élément vide indique une valeur `true`. La valeur par défaut est`false`.
use-strict-min	Indique si la taille du pool est stricte. `false` par défaut.
flush-strategy	Indique si le pool est vidé en cas d'erreur. Les valeurs acceptées sont : • FailingConnectionOnly • IdleConnections • EntirePool La valeur par défaut est `FailingConnectionOnly`.
allow-multiple-users	Indique si plusieurs utilisateurs pourront avoir accès à la source de données par la méthode getConnection(user, password), et si les types de pools internes ont une influence sur ce comportement.

Tableau 10.5. Paramètres du pool XA

Paramètre	Description
is-same-rm-override	Indique si la classe `javax.transaction.xa.XAResource.isSameRM(XAResource)` retourne `true` ou `false`.

Paramètre	Description
entrelacement	Indique si on doit activer l'entrelacement pour les fabriques de connexion XA.
no-tx-separate-pools	Indique si on doit créer des sous-répertoires distincts pour chaque contexte. Cela est nécessaire pour les sources de données Oracle, qui ne permettent pas aux connexions XA d'être utilisées à la fois à l'intérieur et à l'extérieur d'une transaction de JTA
pad-xid	Indique si on doit remplir le Xid.
wrap-xa-resource	Indique si on doit inclure XAResource dans une instance `org.jboss.tm.XAResourceWrapper`.

Tableau 10.6. Paramètres de sécurité

Paramètre	Description
user-name	Le nom d'utilisation pour créer une nouvelle connexion.
mot de passe	Le mot de passe à utiliser pour créer une nouvelle connexion
security-domain	Contient le nom d'un gestionnaire de sécurité JAAS, qui gère l'authentification. Ce nom correspond à l'attribut application-policy/name de la configuration de connexion JAAS.
reauth-plugin	Définit un plugin d'authentification à nouveau pour la ré authentification de connexions physiques.

Tableau 10.7. Paramètres de validation

Paramètre	Description
valid-connection-checker	Une mise en œuvre d'interface `org.jboss.jca.adaptors.jdbc.ValidConnectionChecker` qui fournit une méthode `SQLException.isValidConnection(Connection e)` pour valider une connexion. Une exception signifie que la connexion est détruite. Cela remplace le paramètre `check-valid-connection-sql` s'il est présent.

Paramètre	Description
check-valid-connection-sql	Un énoncé SQL pour vérifier la validité d'un pool de connexion. Peut être appelé quand une connexion gérée est tirée d'un pool.
validate-on-match	Indique si la validation de niveau de connexion est exécutée lorsqu'une fabrique de connexions essaie de correspondre à une connexion gérée pour un ensemble donné. Spécifier « true » pour **`Validate-on-match`** n'est généralement pas effectué conjointement avec la spécification « true » de **`background-validation`**. **`Validate-on-match`** est nécessaire lorsqu'un client doit avoir une connexion validée avant l'utilisation. Ce paramètre est true par défaut.
background-validation	Indique que les connexions sont validées sur un thread d'arrière-plan. La validation de l'arrière-plan (Background validation) est une optimisation de performance lorsque non utilisé avec **`validate-on-match`**. Si **`Validate-on-match`** est sur true, l'utilisation de **`background-validation`** pourrait entraîner des contrôles redondants. La validation de l'arrière-plan pourrait provoquer une mauvaise connexion (une connexion qui irait mal entre le moment de l'analyse de validation et avant d'être donnée au client), l'application cliente doit par conséquent tenir compte de cette possibilité.
background-validation-millis	La durée, en millisecondes, pendant laquelle la validation d'arrière-plan exécute.
use-fast-fail	Si défini sur true, échoue une allocation de connexion lors de la première tentative, si la connexion est non valide. La valeur par défaut est **`false`**.
stale-connection-checker	Une instance de **`org.jboss.jca.adapters.jdbc.StaleConnectionChecker`** qui produit une méthode booléenne **`isStaleConnection(SQLException e)`**. Si cette méthode renvoie un **`true`**, l'exception sera contenue dans **`org.jboss.jca.adapters.jdbc.StaleConnectionException`**, qui correspond à une sous-classe de **`SQLException`**.

Paramètre	Description
exception-sorter	Une instance de **`org.jboss.jca.adapters.jdbc.ExceptionSorter`** qui fournit une méthode booléenne **`isExceptionFatal(SQLException e)`**. Cette méthode validera si une exception est envoyée à toutes les instances d'un **`javax.resource.spi.ConnectionEventListener`** en tant que message **`connectionErrorOccurred`**.

Tableau 10.8. Paramètres de timeout

Paramètre	Description
use-try-lock	Utiliser **`tryLock()`** au lieu de **`lock()`**. Vous essayerez ainsi d'obtenir un verrou pour le nombre de secondes configurées, avant le timeout, au lieu d'échouer immédiatement quand le verrou n'est pas disponible. La valeur par défaut est de **`60`** secondes. Par exemple, pour définir un timeout de 5 minutes, définir **`<use-try-lock>`**300**`</use-try-lock>`**.
blocking-timeout-millis	La durée maximale, en millisecondes, de blocage lorsque vous attendez une connexion. Après que ce délai soit dépassé, une exception sera levée. Cela bloque uniquement pendant que vous attendez un permis de connexion et ne lève pas d'exception si la création d'une nouvelle connexion prend beaucoup de temps. Par défaut, 30000, qui correspond à 30 secondes.
idle-timeout-minutes	La durée maximale, en minutes, avant qu'une connexion inactive soit fermée. La durée maximale réelle dépend de la durée d'analyse de l'idleRemover, qui correspond à la moitié du plus petit **`idle-timeout-minutes`** de n'importe quel pool.
set-tx-query-timeout	Indique si on doit définir le timeout d'interrogation par rapport au temps qui reste avant le timeout de transaction. Si aucune transaction n'existe, on utilisera le timeout de recherche qui a été configuré. La valeur par défaut est **`false`**.
query-timeout	Timeout pour les recherches, en secondes. La valeur par défaut est « no timeout ».
allocation-retry	Le nombre de tentatives de connexion avant d'envoyer une connexion. La valeur par défaut est **`0`**, pour qu'une exception puisse être envoyée à la première défaillance.

Paramètre	Description
allocation-retry-wait-millis	Le temps, en millisecondes, qu'il faut attendre avant de retenter d'allouer une connexion. La valeur par défaut est 5 000, soit 5 secondes.
xa-resource-timeout	Si la valeur est non nulle, elle passe à la méthode `XAResource.setTransactionTimeout`.

Tableau 10.9. Paramètres d'instruction

Paramètre	Description
track-statements	Indique si l'on doit vérifier les instructions non fermées lorsqu'une connexion est renvoyée à un pool ou qu'une instruction est retournée dans le cache d'instruction préparée. Si false, les instructions ne seront pas suivies. **Valeurs valides** • `true` : les instructions et les ensembles de résultats sont suivis, et un avertissement sera émis s'ils ne sont pas fermés. • `false` : ni les instructions, ni les ensembles de résultats ne seront suivis. • `nowarn` : les instructions sont suivies, mais il n'y a aucun avertissement. Valeur par défaut.
prepared-statement-cache-size	Le nombre d'instructions préparées par connexion, dans le cache LRU (le moins souvent utilisé récemment).
share-prepared-statements	Indique si le fait de demander la même instruction deux fois sans la fermer utilise la même instruction préparée sous-jacente. La valeur par défaut est `false`.

Tableau 10.10. Paramètres de recouvrement

Paramètre	Description
recover-credential	Une paire nom d'utilisateur/mot de passe ou domaine de sécurité pour le recouvrement.

Paramètre	Description
recover-plugin	Une mise en œuvre de la classe **`org.jboss.jca.core.spi.recovery.RecoveryPlugin`** à utiliser pour le recouvrement.

Report a bug

10.6.3. Journalisation des transactions

10.6.3.1. Messages de journalisation de transactions

Pour suivre le statut de la transaction tout en gardant les fichiers de journalisation lisibles, utiliser le niveau de journalisation **DEBUG** pour le logger de transaction. Pour un débogage détaillé, utiliser le niveau de journalisation **TRACE**. Veuillez consulter Section 10.6.3.2, « Configurer la journalisation des sous-systèmes de transactions » pour plus d'informations sur la configuration du logger de transaction.

Le gestionnaire de transaction peut générer beaucoup d'informations de journalisation si configuré pour se connecter au niveau de journalisation **TRACE**. Vous trouverez ci-dessous quelques-uns des messages les plus courants. Cette liste n'est pas exhaustive, il se peut que vous rencontriez d'autres messages.

Tableau 10.11. Changement d'état de transaction

Début de transaction	Quand une transaction commence, le code suivant s'exécute :
	`com.arjuna.ats.arjuna.coordinator.BasicAction::Begin:1342`
	`tsLogger.logger.trace("BasicAction::Begin() for action-id "+ get_uid());`

Validation de transaction	Quand une transaction est validée, le code suivant s'exécute :
	`com.arjuna.ats.arjuna.coordinator.BasicAction::End:1342`
	`tsLogger.logger.trace("BasicAction::End() for action-id "+ get_uid());`

Restauration de transaction	Quand une transaction est restaurée, le code suivant s'exécute :
	`com.arjuna.ats.arjuna.coordinator.BasicAction::Abort:1575`
	`tsLogger.logger.trace("BasicAction::Abort() for action-id "+ get_uid());`

Délai d'expiration de transaction	Quand une transaction expire, le code suivant s'exécute :
	`com.arjuna.ats.arjuna.coordinator.TransactionReaper::doCancellations:349`
	`tsLogger.logger.trace("Reaper Worker " + Thread.currentThread() + " attempting to cancel " + e._control.get_uid());`
	Vous verrez ensuite le même thread restaurer la transaction comme montré ci-dessus.

Report a bug

10.6.3.2. Configurer la journalisation des sous-systèmes de transactions

Résumé

Utiliser cette procédure pour contrôler la quantité d'informations enregistrées sur les transactions, indépendamment des autres paramètres de journalisation dans JBoss EAP 6. La procédure montre comment procéder dans la console de gestion sur le web. La commande de gestion CLI est donnée par la suite.

Procédure 10.4. Configurer le Transaction Logger par la console de gestion

1. **Naviguer vers la zone de configuration de la journalisation**
   Dans la console de gestion, cliquer sur l'onglet **`Profiles`** en haut et à gauche de l'écran. Si vous utilisez un domaine géré, fermer le profil du serveur que vous souhaitez configurer, à partir de la case de sélection **`Profile`** qui se trouve en haut et à droite.

   Dérouler le menu **`Core`**, et cliquer sur l'étiquette **`Logging`**.

2. **Modifier les attributs de `com.arjuna`.**
   Cliquer sur le bouton **`Edit`** dans la section **`Details`** qui se situe en bas de la page. Vous pourrez ajouter ici les informations de journalisation spécifiques à la classe. La classe **`com.arjuna`** est déjà présente. Vous pourrez modifier le niveau de journalisation et décider si vous souhaitez utiliser les gestionnaires parents.

   Niveau de journalisation

Le niveau de journalisation est **WARN** par défaut. Comme les transactions peuvent produire une grande quantité de messages de journalisation, la signification des niveaux de journalisation standard est légèrement différente pour le Transaction Logger. En général, les messages avec des niveaux de gravité moins élevés que le niveau choisi sont ignorés.

Niveaux de journalisation des transactions, du plus au moins détaillé.

- TRACE
- DEBUG
- INFO
- WARN
- ERROR
- FAILURE

Utiliser les gestionnaires parents

Indique si l'enregistreur d'événements doit envoyer ses sorties vers l'enregistreur d'événements parent. Le comportement par défaut est **`true`**.

3. Les changements prennent effet immédiatement.

Report a bug

10.6.3.3. Naviguer et gérer les transactions

Le CLI de gestion basé de ligne de commande prend en charge la capacité de naviguer et de manipuler les enregistrements des transactions. Cette fonctionnalité est fournie par l'interaction entre le gestionnaire de transactions et l'API de Gestion (Management) de JBoss EAP 6.

Le gestionnaire de transactions stocke des informations sur chaque transaction en attente et les participants impliqués dans la transaction, dans un stockage persistant appelé *object store*. L'API de gestion expose le store objet sous forme de ressource appelée **`log-store`**. Une opération API nommée **`probe`** lit les journaux de transactions et crée un noeud pour chaque journal. Vous pouvez invoquer la commande **`probe`** manuellement, quand vous souhaitez réactualiser le **`log-store`**. Il est normal pour les journaux de transactions d'apparaître ou de disparaître rapidement.

Exemple 10.1. Réactualiser le Log Store

Cette commande réactualise le Log Store des groupes de serveurs qui utilisent le profil par défaut **`default`** dans un domaine géré. Dans le cas d'un serveur autonome, supprimer **`profile=default`** de la commande.

```
/profile=default/subsystem=transactions/log-store=log-store/:probe
```

Exemple 10.2. Voir toutes les transactions préparées

Pour voir toutes les transactions préparées, commencer par réactualiser le log store (voir Exemple 10.1, « Réactualiser le Log Store »), puis exécuter la commande suivante, qui fonctionne de la même manière qu'une commande **ls** de système de fichier.

```
ls /profile=default/subsystem=transactions/log-store=log-
store/transactions
```

Chaque transaction est visible, ainsi que son identifiant unique. Les opérations individuelles peuvent être exécutées contre une transaction individuelle (voir Gérer une transaction).

Gérer une transaction

Voir des attributs de transaction.

Pour voir des informations sur une transaction, comme son nom JNDI, son nom de produit EIS ou sa version, ou statut, utiliser la commande CLI **:read-resource**.

```
/profile=default/subsystem=transactions/log-store=log-
store/transactions=0\:ffff7f000001\:-b66efc2\:4f9e6f8f\:9:read-resource
```

Voir tous les participants d'une transaction.

Chaque journal de transaction contient un élément enfant nommé **participants**. Utiliser la commande CLI **read-resource** CLI sur cet élément pour voir les participants des transactions. Les participants sont identifiés par leurs noms JNDI.

```
/profile=default/subsystem=transactions/log-store=log-
store/transactions=0\:ffff7f000001\:-
b66efc2\:4f9e6f8f\:9/participants=java\:\/JmsXA:read-resource
```

Le résultat devrait ressembler à ceci :

```
{
   "outcome" => "success",
   "result" => {
       "eis-product-name" => "HornetQ",
       "eis-product-version" => "2.0",
       "jndi-name" => "java:/JmsXA",
       "status" => "HEURISTIC",
       "type" => "/StateManager/AbstractRecord/XAResourceRecord"
   }
}
```

Le statut du résultat affiché ici est dans un état **HEURISTIC** et est susceptible d'être recouvert. Voir Recouvrement d'une transaction. pour plus d'informations.

Supprimer une transaction.

Chaque journal de transaction supporte une opération **:delete** pour effacer l'enregistrement qui représente la transaction.

```
/profile=default/subsystem=transactions/log-store=log-
store/transactions=0\:ffff7f000001\:-b66efc2\:4f9e6f8f\:9:delete
```

Recouvrement d'une transaction.

Chaque journal de transaction supporte le recouvrement par la commande CLI `:recover`.

Recouvrement des transactions heuristiques et des participants

- Si le statut de la transaction est **HEURISTIC**, l'opération de recouvrement change l'état en **PREPARE** et déclenche un recouvrement.
- Si l'un des participants de la transaction est heuristique, l'opération de recouvrement tente de reprendre l'opération **commit** (validation) à nouveau. En cas de succès, le participant est retiré du journal des transactions. Vous pouvez vérifier cela en exécutant à nouveau l'opération **:probe** sur le **log-store** et en vérifiant que le participant n'est plus inscrit. Si c'est le dernier participant, la transaction sera également supprimée.

Réactualiser le statut de la transaction qui a besoin d'être recouvrée.

Si une transaction a besoin d'être recouvrée, vous pourrez utiliser la commande CLI **:refresh** pour vous assurer qu'elle a toujours besoin d'être recouvrée, avant de tenter le recouvrement.

```
/profile=default/subsystem=transactions/log-store=log-
store/transactions=0\:ffff7f000001\:-b66efc2\:4f9e6f8f\:9:refresh
```

Voir les statistiques de transaction

Si les statistiques de TM (Transaction Manager) sont activées, vous pouvez consulter les statistiques à propos du Gestionnaire de Transactions et du sous-système de transactions. Veuillez consulter Section 10.7.8.2, « Configurer le Transaction Manager (TM) ou Gestionnaire de transactions » pour plus d'informations sur l'activation des statistiques de TM.

Vous pouvez consulter les statistiques soit par la console de gestion basée-web, soit par la gestion de ligne de commande CLI. Dans la console de gestion basée-web, les statistiques de transaction seront disponibles via **Runtime** → **Subsystem Metrics** → **Transactions**. Les statistiques de transaction sont disponibles pour chaque serveur dans un domaine géré, également. Vous pourrez spécifier le serveur dans la case de sélection **Server** située en haut à gauche.

La table suivante affiche chaque statistique disponible, sa description et la commande CLI pour afficher le statistique.

Tableau 10.12. Les statistiques de sous-système de transaction

Statistique	Description	Commande CLI
Total	Le nombre total de transactions exécutées par le gestionnaire de transactions sur ce serveur.	`/host=master/server=server-one/subsystem=transactions/:read-attribute(name=number-of-transactions,include-defaults=true)`

Statistique	Description	Commande CLI
Validé	Le nombre de transactions validées exécutées par le gestionnaire de transactions sur ce serveur.	`/host=master/server=server-one/subsystem=transactions/:read-attribute(name=number-of-committed-transactions,include-defaults=true)`
Abandonné	Le nombre de transactions interrompues exécutées par le gestionnaire de transactions sur ce serveur.	`/host=master/server=server-one/subsystem=transactions/:read-attribute(name=number-of-aborted-transactions,include-defaults=true)`
Délai expiré	Le nombre de transactions expirées exécutées par le gestionnaire de transactions sur ce serveur.	`/host=master/server=server-one/subsystem=transactions/:read-attribute(name=number-of-timed-out-transactions,include-defaults=true)`
Heuristiques	Pas disponible dans la Console de Gestion. Nombre de transactions dans un état heuristique.	`/host=master/server=server-one/subsystem=transactions/:read-attribute(name=number-of-heuristics,include-defaults=true)`

Statistique	Description	Commande CLI
Transactions In-Flight	Pas disponible dans la console de gestion. Nombre de transactions commencées mais pas encore achevées.	`/host=master/server=server-one/subsystem=transactions/:read-attribute(name=number-of-inflight-transactions,include-defaults=true)`
Origine de l'échec - Applications	Le nombre de transactions échouées dont l'origine de l'échec était une application.	`/host=master/server=server-one/subsystem=transactions/:read-attribute(name=number-of-application-rollbacks,include-defaults=true)`
Origine de l'échec - Ressources	Le nombre de transactions échouées dont l'origine de l'échec était une ressource.	`/host=master/server=server-one/subsystem=transactions/:read-attribute(name=number-of-resource-rollbacks,include-defaults=true)`

Report a bug

10.7. UTILISER LES TRANSACTIONS JTA

10.7.1. Transactions JTA

Introduction

Les procédures suivantes sont utiles quand vous aurez besoin d'utiliser des transactions dans votre application.

- Section 10.7.2, « Transactions de contrôle »
- Section 10.7.3, « Démarrer une transaction »
- Section 10.7.5, « Valider une transaction »
- Section 10.7.6, « Annuler une transaction »

- Section 10.7.7, « Gérer un résultat heuristique dans une transaction »
- Section 10.7.8.2, « Configurer le Transaction Manager (TM) ou Gestionnaire de transactions »
- Section 10.7.9.1, « Erreurs de transactions »

Report a bug

10.7.2. Transactions de contrôle

Introduction

Cette liste de procédures expose les différentes façons de contrôler les transactions dans vos applications utilisant les API JTA ou JTS.

- Section 10.7.3, « Démarrer une transaction »
- Section 10.7.5, « Valider une transaction »
- Section 10.7.6, « Annuler une transaction »
- Section 10.7.7, « Gérer un résultat heuristique dans une transaction »

Report a bug

10.7.3. Démarrer une transaction

Cette procédure montre comment démarrer une nouvelle transaction JTA, ou comment participer à une transaction distribuée en utilisant le protocole JTS (Java Transaction Service).

Transactions distribuées

Dans une transaction distribuée, les participants à la transaction se trouvent dans des applications séparées sur de multiples serveurs. Si un participant rejoint une transaction déjà existante, plutôt que de créer un nouveau contexte de transaction, les deux (ou plus) participants qui partagent le contexte participent à une transaction distribuée. Pour utiliser une transaction distribuée, vous devez configurer l'ORB. Veuillez consulter la section *ORB Configuration* du *Administration and Configuration Guide*pour plus d'informations sur la configuration ORB.

1. **Obtenez une instance de `UserTransaction`.**
   Vous pouvez obtenir une instance par JNDI, injection, ou un EjbContext d'EJB, si l'EJB utilise des transactions gérées-bean, par l'annotation **`@TransactionManagement(TransactionManagementType.BEAN)`**.

   - **JNDI**

     ```
     new InitialContext().lookup("java:comp/UserTransaction")
     ```

   - **Injection**

     ```
     @Resource UserTransaction userTransaction;
     ```

   - **EjbContext**

     ```
     EjbContext.getUserTransaction()
     ```

2. **Appeler `UserTransaction.begin()` une fois connecté à votre source de données.**

```
...
try {
    System.out.println("\nCreating connection to database: "+url);
    stmt = conn.createStatement();  // non-tx statement
    try {
        System.out.println("Starting top-level transaction.");
        userTransaction.begin();
        stmtx = conn.createStatement(); // will be a tx-statement
        ...
    }
}
```

Participer à une transaction en utilisant l'API JTS.

L'un des avantages des EJB est que le conteneur gère toutes les transactions. Si vous avez configuré l'ORB, le conteneur gérera les transactions distribuées pour vous.

Résultat :

La transaction est lancée. Toute utilisation de votre source de données sera transactionnelle jusqu'à ce que vous validiez ou annuliez la transaction.

NOTE

Pour une exemple complet, voir Section 10.9.3, « Exemple de transaction JTA ».

Report a bug

10.7.4. Transactions imbriquées

Les transactions imbriquées ne sont prises en charge que lorsque vous utilisez les transactions distribuées avec les API JTS. De plus, beaucoup de fournisseurs de base de données ne prennent pas en charge les transactions imbriquées, renseignez-vous donc auprès de votre fournisseur de base de données avant d'ajouter des transactions imbriquées à votre application.

Les spécifications OTS permettent un type limité de transaction imbriquée, où le protocole de validation de sous-transaction est le même que pour les transactions de niveau supérieur. Il existe deux phases : une phase **`prepare`** et une phase **`commit`** ou **`abort`**. Ce type de transaction imbriquée peut mener à des résultats incohérents, comme un coordinateur de sous-transaction en cours de validation qui découvre qu'une ressource ne peut être validée. Il se peut que le coordinateur ne puisse être capable de dire aux ressources validées de s'interrompre, causant ainsi un résultat heuristique. Cette transaction stricte imbriquée OTS est disponible via l'interface **`CosTransactions::SubtransactionAwareResource`**.

La mise en œuvre de JTS de JBoss EAP 6 prend en charge ce type de transaction imbriquée. Elle prend également en charge un type de transaction imbriquée avec un protocole de validation multiphase, évitant ainsi les problèmes que l'on peut rencontrer avec le modèle OTS strict. Ce type de transaction imbriquée est disponible via le **`ArjunaOTS::ArjunaSubtranAwareResource`**. Il est poussé par un protocole de validation à deux phases à chaque fois qu'une transaction imbriquée est validée.

Pour créer une transaction imbriquée, créer une nouvelle transaction à l'intérieur d'une transaction parente. Veuillez consulter Section 10.7.3, « Démarrer une transaction » pour plus d'informations sur la création d'une transaction.

L'effet d'une transaction imbriquée dépend de la validation/annulation de ses transactions intégrées. Les effets sont récupérés si la transaction intégrée s'interrompt, même si la transaction imbriquée a été validée.

Report a bug

10.7.5. Valider une transaction

Cette procédure montre comment valider une transaction en utilisant JTA (Java Transaction Api). Cet API est utilisé à la fois pour les transactions locales et les transactions distribuées. Les transactions distribuées sont gérées par le JTS (Java Transaction Server) et nécessitent la configuration d'un ORB (Object Request Broker). Pour plus d'informations sur la configuration d'un ORB, veuillez consulter la section *ORB Configuration* du *Administration and Configuration Guide*

Prérequis

Vous devez démarrer une transaction avant de pouvoir la valider. Pour plus d'informations sur le démarrage d'une transaction, veuillez consulter Section 10.7.3, « Démarrer une transaction ».

1. **Appeler la méthode `commit()` sur `UserTransaction`.**
   Lorsque vous appelez la méthode **`commit()`** sur **`UserTransaction`**, le gestionnaire de transactions tente de valider la transaction.

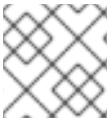
```
@Inject
private UserTransaction userTransaction;

public void updateTable(String key, String value)
    EntityManager entityManager =
entityManagerFactory.createEntityManager();
    try {
        userTransaction.begin():
        <!-- Perform some data manipulation using entityManager -->
        ...
        // Commit the transaction
        userTransaction.commit();
    } catch (Exception ex) {
        <!-- Log message or notify Web page -->
        ...
        try {
            userTransaction.rollback();
        } catch (SystemException se) {
            throw new RuntimeException(se);
        }
        throw new RuntimeException(e);
    } finally {
        entityManager.close();
    }
}
```

2. **Si vous utilisez des CMT (Container Managed Transactions), vous n'avez pas besoin de valider manuellement.**

Si vous configurez votre bean pour qu'il puisse utiliser des transactions gérées conteneur, le conteneur devra gérer le cyle de vie des transactions pour vous sur la base d'annotations que vous aurez configurées dans le code.

Résultat

Votre source de données valide et votre transaction se termine, ou une exception est lancée.



NOTE

Pour une exemple complet, voir Section 10.9.3, « Exemple de transaction JTA ».

Report a bug

10.7.6. Annuler une transaction

Cette procédure montre comment annuler une transaction en utilisant JTA (Java Transaction Api). Cet API est utilisé à la fois pour les transactions locales et les transactions distribuées. Les transactions distribuées sont gérées par le JTS (Java Transaction Server) et nécessitent la configuration d'un ORB (Object Request Broker). Pour plus d'informations sur la configuration d'un ORB, veuillez consulter la section *ORB Configuration* du *Administration and Configuration Guide*

Prérequis

Vous devez démarrer une transaction avant de pouvoir la supprimer. Pour plus d'informations sur le démarrage d'une transaction, veuillez consulter Section 10.7.3, « Démarrer une transaction ».

1. **Appeler la méthode `rollback()` sur `UserTransaction`.**
   Lorsque vous appelez la méthode **`rollback()`** sur **`UserTransaction`**, le gestionnaire de transactions tentera de valider la transaction.

```
@Inject
private UserTransaction userTransaction;

public void updateTable(String key, String value)
    EntityManager entityManager =
entityManagerFactory.createEntityManager();
    try {
        userTransaction.begin():
        <!-- Perform some data manipulation using entityManager -->
          ...
          // Commit the transaction
        userTransaction.commit();
    } catch (Exception ex) {
        <!-- Log message or notify Web page -->
        ...
        try {
            userTransaction.rollback();
        } catch (SystemException se) {
            throw new RuntimeException(se);
        }
        throw new RuntimeException(e);
    } finally {
        entityManager.close();
```

```
        }
    }
```

2. **Si vous utilisez des CMT (Container Managed Transactions), vous n'avez pas besoin de supprimer la transaction manuellement.**
   Si vous configurez votre bean pour qu'il puisse utiliser des transactions gérées conteneur, le conteneur devra gérer le cyle de vie des transactions pour vous sur la base d'annotations que vous aurez configurées dans le code.

Résultat

Votre transaction est annulée par le gestionnaire de transactions.

NOTE

Pour voir un exemple complet Section 10.9.3, « Exemple de transaction JTA ».

Report a bug

10.7.7. Gérer un résultat heuristique dans une transaction

Cette procédure montre comment gérer un résultat heuristique dans une transaction JTA, qu'elle soit locale ou distribuée, en utilisant JTS (Java Transaction Service). Pour utiliser des transactions distribuées, il vous faut configurer l'ORB. Veuillez consulter la section *ORB Configuration* du *Administration and Configuration Guide*pour plus d'informations sur la configuration ORB.

Les résultats de transaction heuristique sont rares et ont généralement des causes exceptionnelles. Le mot *heuristique* signifie «manuellement», et c'est ainsi que ces résultats doivent généralement être traités. Voir Section 10.4.4, « Résultats heuristiques » pour plus d'informations sur les résultats de l'opération heuristique.

Procédure 10.5. Gérer un résultat heuristique dans une transaction

1. **Déterminer la cause**
   En général, la cause d'un résultat heuristique pour une transaction est qu'un gestionnaire de ressources a promis qu'il pourrait commettre ou annuler, et il n'a pas pu remplir sa promesse. Cela pouvait être dû à un problème avec un composant de tierce partie, la couche d'intégration entre le composant tiers et la plate-forme EAP 6 ou bien la plate-forme JBoss EAP 6 elle-même.

   De loin, les deux causes les plus communes d'erreurs heuristiques sont des erreurs temporaires situées dans l'environnement ou des erreurs de code liées aux gestionnaires de ressources.

2. **Solution aux échecs temporaires de l'environnement**
   Normalement, s'il y a un échec temporaire dans votre environnement, vous le saurez avant d'être au courant de l'erreur heuristique. Il peut s'agir d'une défaillance de réseau ou de matériel, d'une erreur de base de données, d'une panne de courant, d'un hôte ou de tout autre cause.

   En cas de résultat heuristique ayant lieu dans un environnement de test, au cours de test de stress, cela vous fournit des informations sur les points faibles de votre environnement.

AVERTISSEMENT

La plate-forme JBoss EAP 6 restaurera automatiquement les transactions qui ne sont pas dans un état heuristique au moment de la défaillance, mais elle ne tentera pas de restaurer les transactions heuristiques.

3. **Contacter les fournisseurs de gestionnaires de ressources**
   Si vous n'expérimentez aucun échec évident dans votre environnement, ou si le résultat heuristique est facilement reproductible, c'est probablement une erreur de codage. Contacter les fournisseurs de tierce partie pour savoir si une solution est disponible. Si vous pensez que le problème est dans le gestionnaire de transactions de la plate-forme JBoss EAP 6 elle-même, veuillez prendre contact avec Red Hat Global Support Services.

4. **Dans un environnement de test, supprimer les logs et démarrez à nouveau la plate-forme JBoss EAP 6.**
   Dans un environnement de test, ou bien dans les cas où vous ne vous souciez pas de l'intégrité des données, le fait de supprimer les journaux des transactions et de redémarrer la plate-forme JBoss EAP 6 se débarrasse du résultat heuristique. Les journaux des transactions sont situés dans ***EAP_HOME***`/standalone/data/tx-object-store/` pour les serveurs autonomes, ou dans ***EAP_HOME***`/domain/servers/`***SERVER_NAME***`/data/tx-object-store` pour les domaines gérés, par défaut. Dans le cas d'un domaine géré, *SERVER_NAME* se rapporte au nom du serveur individuel qui participe à un groupe de serveurs.

5. **Résoudre le résultat à la main**
   Le processus de résolution de résultat à la main dépend des circonstances particulières de l'incident. Normalement, vous aurez besoin de procéder aux étapes suivantes, en les appliquant à votre situation.

   a. Identifier les gestionnaires de ressources impliqués.

   b. Examiner l'état dans le gestionnaire de transactions et dans les gestionnaires de ressources.

   c. Forcer manuellement le nettoyage des journaux et la reconciliation des données dans un ou plusieurs des composants impliqués.

   La façon dont procéder à ces étapes sont au delà de la portée de ce document.

Report a bug

10.7.8. Temps d'expiration des transactions

10.7.8.1. Les délais d'attente de transactions

Afin de préserver l'atomicité et de respecter la norme ACID des transactions, certaines parties d'une transaction peuvent être longues. Les participants à la transaction doivent verrouiller des pièces de sources de données lorsqu'ils commettent, et le gestionnaire de transactions doit attendre d'avoir des nouvelles de chaque participant à une transaction avant de pouvoir tous les diriger à commettre ou à annuler. Les ressources d'être verrouillés indéfiniment pour cause de panne de matériel ou de réseau.

Les délais d'attente de transactions peuvent être associés à des transactions afin de contrôler leur cycle de vie. Si un seuil de délai d'attente passe avant que la transaction s'engage ou annule, le délai d'attente provoque l'annulation de l'opération automatiquement.

Vous pouvez configurer les valeurs de délai d'attente par défaut pour tout le sous-système de la transaction, ou bien, vous pouvez désactiver les valeurs de délai d'attente par défaut et spécifier les délais d'attente sur une base d'une transaction.

Report a bug

10.7.8.2. Configurer le Transaction Manager (TM) ou Gestionnaire de transactions

Vous pouvez configurer le Transaction Manager (TM) à l'aide de la Console de gestion sur le web ou la ligne de commande Management CLI. Pour chaque commande ou option donnée, on assume que vous exécutez JBoss EAP 6 comme un domaine géré. Si vous utilisez un serveur autonome ou que vous souhaitez modifier un profil différent de la valeur par défaut **`default`**, il se peut que vous ayez à modifier les étapes et les commandes de la manière suivante.

Notes sur les commandes d'exemple

- Pour la console de gestion, le profil par défaut **`default`** est celui qui sera sélectionné quand vous vous connectez. Si vous souhaitez modifier la configuration du Transaction Manager dans un autre profile, sélectionnez votre profile à la place, et non pas **`default`**, pour chaque instruction.

  De même, substituez votre profil à la place du profil par défaut **`default`** pour les commandes CLI de l'exemple.

- Si vous utilisez un Serveur Autonome, un seul profil existe. Ignorer toute instruction pour choisir un profil spécifique. Dans les commandes CLI, retirer la partie **`/profile=default`** des commandes d'échantillon.

NOTE

Pour que les options du TM soient visibles dans la Console de gestion ou dans le Management CLI, le sous-système **`transactions`** doit être activé. Il est activé par défaut, et il faut pour cela qu'un certain nombre d'autres sous-systèmes fonctionnent correctement, donc il est improbable qu'il soit désactivé.

Configurer le TM par la Console de gestion

Pour configurer le TM à l'aide de la Console de gestion sur le web, sélectionnez l'onglet **`Runtime`** de la liste dans la partie supérieure gauche de l'écran de la console de gestion. Si vous utilisez un domaine géré, vous avez le choix de plusieurs profils. Choisir le bon **`profil`** de la boîte de sélection dans la partie supérieure droite de l'écran Profils. Étendez le menu **`Container`**, et sélectionnez **`Transactions`**.

Vous verrez la plupart des options dans la page de configuration du Transaction Manager. Les options **`Recovery`** sont cachées par défaut. Cliquer sur l'en-tête **`Recovery`** pour les étendre. Cliquer sur le bouton **`Edit`** pour éditer une des options. Les changements prendront place immédiatement.

Cliquer sur l'étiquette **`Need Help?`** pour afficher le texte d'aide en ligne.

Configurer le TM par le Management CLI

Dans le Management CLI, vous pouvez configurer le TM en utilisant une série de commandes. Les commandes commencent toutes par **`/profile=default/subsystem=transactions/`** pour un domaine géré avec **`default`** de profil, ou par **`/subsystem=transactions`** pour un serveur autonome.

Tableau 10.13. Options de configuration de la TM

Option	Description	Commande CLI
Activer les statistiques	Indique s'il faut activer les statistiques de transaction. Ces statistiques se trouvent dans la console de gestion dans la section **`Subsystem Metrics`** de l'onglet **`Runtime`**.	**`/profile=default/subsystem=transactions/:write-attribute(name=enable-statistics,value=true)`**
Activer le statut TSM	Indique si l'on doit activer le service de gestion du statut de transaction (TSM), qui est utilisé pour le recouvrement hors-processus.	**`/profile=default/subsystem=transactions/:write-attribute(name=enable-tsm-status,value=false)`**
Délai d'attente par défaut	Délai d'attente de transaction par défaut. La valeur par défaut est de **`300`** secondes. Vous pouvez la remplacer par programmation, sur la base d'une transaction.	**`/profile=default/subsystem=transactions/:write-attribute(name=default-timeout,value=300)`**
Chemin	Le chemin d'accès relatif ou absolu du système de fichiers dans lequel le cœur du gestionnaire de transactions stocke les données. Par défaut, la valeur est un chemin d'accès relatif à la valeur de l'attribut **`relative-to`**.	**`/profile=default/subsystem=transactions/:write-attribute(name=path,value=var)`**
Relatif à	Référence une configuration de chemin global dans le modèle du domaine. La valeur par défaut correspond au répertoire de données de JBoss EAP 6, qui correspond à la valeur de la propriété **`jboss.server.data.dir`**, et qui a pour valeur par défaut ***`EAP_HOME`*`/domain/data/`** pour un Domaine Géré, ou ***`EAP_HOME`*`/standalone/data/`** pour une instance de Serveur Autonome. La valeur de l'attribut TM du chemin **`path`** est relative à ce chemin. Utiliser une chaîne vide pour désactiver le comportement par défaut et forcer la valeur de l'attribut du chemin **`path`** qui doit être traité comme un chemin absolu.	**`/profile=default/subsystem=transactions/:write-attribute(name=relative-to,value=jboss.server.data.dir)`**

Option	Description	Commande CLI
Chemin de Store Objet	Un chemin de système de fichiers relatif ou absolu où le store objet TM stocke des données. Relatif, par défaut, à la valeur du paramètre **`object-store-relative-to`**.	**`/profile=default/subsystem=transactions/:write-attribute(name=object-store-path,value=tx-object-store)`**
Chemin de Store Objet Relatif à	Référence une configuration de chemin global dans le modèle du domaine. La valeur par défaut correspond au répertoire de données de JBoss EAP 6, qui correspond à la valeur de la propriété **`jboss.server.data.dir`**, et qui a pour valeur par défaut ***`EAP_HOME`*`/domain/data/`** pour un Domaine Géré, ou ***`EAP_HOME`*`/standalone/data/`** pour une instance de Serveur Autonome. La valeur de l'attribut TM du chemin **`path`** est relative à ce chemin. Utiliser une chaîne vide pour désactiver le comportement par défaut et forcer la valeur de l'attribut du chemin **`path`** qui doit être traité comme un chemin absolu.	**`/profile=default/subsystem=transactions/:write-attribute(name=object-store-relative-to,value=jboss.server.data.dir)`**
Liaisons de sockets	Indique le nom de la liaison du socket utilisé par le gestionnaire de transactions pour la récupération et la création des identificateurs de transactions, lorsque le mécanisme du socket est utilisé. Se référer à **`processus-id-socket-max-ports`** pour plus d'informations sur la génération de l'identificateur unique. Les liaisons de socket sont spécifiées par le groupe de serveurs dans l'onglet **`Serveur`** de la console de gestion.	**`/profile=default/subsystem=transactions/:write-attribute(name=socket-binding,value=txn-recovery-environment)`**
Liaison de socket de statut	Indique la liaison de socket à utiliser pour le gestionnaire de statuts de transactions.	**`/profile=default/subsystem=transactions/:write-attribute(name=status-socket-binding,value=txn-status-manager)`**

Option	Description	Commande CLI
Listener de recouvrement	Indique si oui ou non le processus de recouvrement de transaction doit écouter au socket de réseau. La valeur par défaut est **false**.	**/profile=default/subsystem=transactions/:write-attribute(name=recovery-listener,value=false)**

Les options suivantes sont pour une utilisation avancée et ne peuvent être modifiées qu'à l'aide du Management CLI. Soyez prudent lors de leur modification à partir de la configuration par défaut. Communiquer avec Red Hat Global Support Services pour plus d'informations.

Tableau 10.14. Options de configuration TM avancées

Option	Description	Commande CLI
jts	Indique si l'on doit utiliser les transactions Java Transaction Service (JTS). La valeur par défaut est **false**, qui utilise des transactions JTA uniquement.	**/profile=default/subsystem=transactions/:write-attribute(name=jts,value=false)**
Identifiant de nœud	L'identifiant de nœud pour le service JTS. Ce dernier doit être unique pour le service JTS, parce que le gestionnaire de transactions l'utilise pour la récupération.	**/profile=default/subsystem=transactions/:write-attribute(name=node-identifier,value=1)**
process-id-socket-max-ports	Le gestionnaire de transactions crée un identifiant unique pour chaque journal des transactions. Deux mécanismes différents sont fournis pour générer des identificateurs uniques : un mécanisme basé sur le socket et un mécanisme fondé sur l'identificateur de processus du processus. Dans le cas de l'identifiant basé-socket, le socket est ouvert et son numéro de port est utilisé pour l'identifiant. Si le port est déjà utilisé, on cherchera le port suivant, jusqu'à ce qu'un port libre soit trouvé. Les **processus-id-socket-max-ports** représentent le nombre maximal de sockets que le TM va essayer avant d'abandonner. La valeur par défaut est **10**.	**/profile=default/subsystem=transactions/:write-attribute(name=process-id-socket-max-ports,value=10)**

Option	Description	Commande CLI
process-id-uuid	Définir à **true** avec un identifiant de processus pour créer un identifiant unique pour chaque transaction. Sinon, le mécanisme basé socket sera utilisé. La valeur par défaut est **true**. Se référer à **process-id-socket-max-ports** pour obtenir davantage d'informations.	**/profile=default/subsystem=transactions/:write-attribute(name=process-id-uuid,value=true)**
use-hornetq-store	Utiliser les mécanismes de stockage journalisés de HornetQ au lieu du stockage basé sur des fichiers, pour les journaux de transactions. Ceci est désactivé par défaut, mais peut améliorer les performances I/O. Il n'est pas recommandé pour les transactions JTS sur les gestionnaires de transactions séparés .	**/profile=default/subsystem=transactions/:write-attribute(name=use-hornetq-store,value=false)**

Report a bug

10.7.9. Gestion des erreurs de transactions JTA

10.7.9.1. Erreurs de transactions

Les erreurs de transactions sont difficiles à résoudre car souvent dépendantes du timing. Voici quelques erreurs courantes et quelques idées pour les résoudre.

NOTE

Ces recommandations ne s'appliquent pas aux erreurs heuristiques. Si vous rencontrez des erreurs heuristiques, voir Section 10.7.7, « Gérer un résultat heuristique dans une transaction » et contacter Red Hat Global Support Services pour obtenir une assistance.

La transaction a expiré mais le thread de logique commerciale ne s'en est pas aperçu.

Ce type d'erreur se manifeste souvent quand Hibernate n'est pas en mesure d'obtenir une connexion de base de données pour le chargement différé. Si cela survient fréquemment, vous pourrez augmenter la valeur du temps d'expiration. Voir Section 10.7.8.2, « Configurer le Transaction Manager (TM) ou Gestionnaire de transactions ».

Si cela n'est pas possible, vous pourrez sans doute régler votre environnement extérieur pour aller plus vite, ou restructurer votre code pour être plus efficace. Contacter Red Hat Global Services si vous avez des problèmes avec le temps d'expiration.

La transaction exécute déjà sur un thread, ou reçoit une exception `NotSupportedException`

L'exception **`NotSupportedException`** indique habituellement que vous avez tenté d'insérer une transaction JTA, et que ce n'est pas pris en charge. Si vous n'étiez pas en train d'essayer d'insérer une transaction, il est probable qu'une autre transaction a commencé dans une tâche de pool de threads,

mais a terminé la tâche sans suspendre, ni mettre fin à la transaction.

Les application utilisent normalement `UserTransaction`, qui s'en occupe automatiquement. Si tel est le cas, il y a peut-être un problème dans le framework.

Si votre code utilise les méthodes `TransactionManager` ou `Transactions` directement, considérez le comportement suivant lors de la validation ou de l'annulation d'une transaction. Si votre code utilise les méthodes du `TransactionManager` pour contrôler vos transactions, la validation ou l'annulation d'une transaction dissociera la transaction du thread actuel. Toutefois, si votre code utilise les méthodes `Transaction`, l'opération peut être pas associée au thread en cours d'exécution, et il faudra la dissocier de son thread manuellement, avant de la retourner au pool de threads.

Vous n'êtes pas en mesure d'enlister une seconde ressource locale

Cette erreur a lieu si vous essayez d'enlister une seconde ressource non-XA dans une transaction. Si vous avez besoin de ressources multiples pour une transaction, elles doivent être XA.

Report a bug

10.8. CONFIGURATION ORB

10.8.1. A propos de CORBA (Common Object Request Broker Architecture)

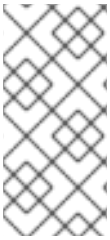
*Common Object Request Broker Architecture (CORBA)*est une norme qui autorise les applications et services à travailler ensemble même lorsqu'ils sont écrits dans de multiples langages normalement incompatibles ou lorsqu'ils sont hébergés sur des plateformes différentes. Les requêtes CORBA sont émises par un composant côte serveur appelé *Object Request Broker (ORB)*. JBoss EAP 6 fournit une instance ORB au moyen du composant JacORB.

L'ORB est utilisé en interne pour les transactions *Java Transaction Service (JTS)*, et peut également être utilisé par votre propre application.

Report a bug

10.8.2. Configurer l'ORB pour les transactions JTS

Dans une installation JBoss EnAP 6 par défaut, l'ORB est désactivé. Vous pouvez activer l'ORB en utilisant le Management CLI de ligne de commande.



NOTE

Dans un domaine géré, le sous-système JacORB est disponible dans les profils `full` et `full-ha` uniquement. Dans un serveur autonome, il est disponible uniquement quand vous utilisez les configurations `standalone-full.xml` ou `standalone-full-ha.xml`.

Procédure 10.6. Configurer l'ORB par la console de gestion

1. **Voir les paramètres de configuration du profil.**
   Sélectionnez `Profiles` (domaine géré) ou `Profile` (serveur autonome) dans la partie supérieure droite de la console de gestion. Si vous utilisez un domaine géré, sélectionnez soit le profil `full` ou `full-ha` à partir de la boîte de dialogue de sélection en haut à gauche.

2. **Modifier les paramètres `Initialisateurs`**
   Étendre le menu **`Sous-système`** sur la gauche, si nécessaire. Étendre le sous-menu **`Conteneur`** et cliquer sur **`JacORB`**.

   Sur le formulaire qui apparaît sur l'écran principal, sélectionner l'onglet **`Initialisateur`**, et cliquer sur le bouton **`Modofier`**.

   Activer les intercepteurs de sécurité en configurant la valeur de **`Security`** à **`active`**.

   Pour activer ORB sur JTS, définir la valeur des **`Intercepteurs de transations`** à **`active`**, au lieu de la valeur par défaut **`spec`**.

   Voir le lien **`Besoin d'aide ?`** sur le formulaire pour accéder à des explications sur ces valeurs. Cliquer sur **`Sauvegarde`** quand vous aurez fini de modifier les valeurs.

3. **Configuration ORB avancée**
   Voir les autres sections du formulaire pour les options de configuration avancées. Chaque section inclut un lien **`Besoin d'aide ?`** avec des informations détaillées sur les paramètres.

Configurer l'ORB par le Management CLI

Vous pouvez configurer chaque aspect de l'ORB à l'aide du Management CLI. Les commandes suivantes configurent les initialisateurs aux mêmes valeurs que celles de la procédure ci-dessus, pour la console de gestion. Il s'agit de la configuration minimale pour l'ORB, si utilisé avec JTS.

Ces commandes sont configurées pour un domaine de sécurité utilisant le profil **`full`**. Si nécessaire, modifier le profil pour qu'il convienne mieux à celui que vous aurez besoin de configurer. Si vous utilisez un serveur autonome, n'utilisez pas la portion **`/profile=full`** des commandes.

Exemple 10.3. Activer les intercepteurs de sécurité

```
/profile=full/subsystem=jacorb/:write-attribute(name=security,value=on)
```

Exemple 10.4. Activer l'ORB pour JTS

```
/profile=full/subsystem=jacorb/:write-
attribute(name=transactions,value=on)
```

Exemple 10.5. Activer les transactions dans le sous-système JacORB

```
/profile=full/subsystem=jacorb/:write-
attribute(name=transactions,value=on)
```

Exemple 10.6. Activer JTS dans le sous-système de transactions

```
/subsystem=transactions:write-attribute(name=jts,value=true)
```

Report a bug

10.9. RÉFÉRENCES DE TRANSACTIONS

10.9.1. Erreurs et exceptions pour les transactions JBoss

Pour obtenir des informations lancées par les méthodes de la classe **`UserTransaction`**, voir la spécification *UserTransaction API* dans http://download.oracle.com/javaee/1.3/api/javax/transaction/UserTransaction.html.

Report a bug

10.9.2. Limitations de JTA Clustering

Les transactions JTA ne peuvent pas être clusterisées à travers les instances multiples de JBoss EAP 6. Pour ce comportement, utiliser les transactions JTS.

Pour pouvoir utiliser les transactions JTS, vous devrez configurer l'ORB, qui inclut l'activation des transactions dans le sous-système JacORB, puis la configuration du sous-système JTS.

- Section 10.8.2, « Configurer l'ORB pour les transactions JTS »

Report a bug

10.9.3. Exemple de transaction JTA

Cet exemple illustre comment démarrer, valider et annuler une transaction JTA. Vous devrez ajuster les paramètres de connexion et de source de données pour accommoder votre environnement, et mettre deux tableaux de tests dans votre base de données.

Exemple 10.7. Exemple de transaction JTA

```
public class JDBCExample {
    public static void main (String[] args) {
        Context ctx = new InitialContext();
        // Change these two lines to suit your environment.
        DataSource ds = (DataSource)ctx.lookup("jdbc/ExampleDS");
        Connection conn = ds.getConnection("testuser", "testpwd");
        Statement stmt = null; // Non-transactional statement
        Statement stmtx = null; // Transactional statement
        Properties dbProperties = new Properties();

        // Get a UserTransaction
        UserTransaction txn = new
InitialContext().lookup("java:comp/UserTransaction");

        try {
            stmt = conn.createStatement();  // non-tx statement

            // Check the database connection.
            try {
                stmt.executeUpdate("DROP TABLE test_table");
                stmt.executeUpdate("DROP TABLE test_table2");
            }
            catch (Exception e) {
                // assume not in database.
            }
```

```
            try {
                stmt.executeUpdate("CREATE TABLE test_table (a
INTEGER,b INTEGER)");
                stmt.executeUpdate("CREATE TABLE test_table2 (a
INTEGER,b INTEGER)");
            }
            catch (Exception e) {
            }

            try {
                System.out.println("Starting top-level transaction.");

                txn.begin();

                stmtx = conn.createStatement(); // will be a tx-
statement

                // First, we try to roll back changes

                System.out.println("\nAdding entries to table 1.");

                stmtx.executeUpdate("INSERT INTO test_table (a, b)
VALUES (1,2)");

                ResultSet res1 = null;

                System.out.println("\nInspecting table 1.");

                res1 = stmtx.executeQuery("SELECT * FROM test_table");

                while (res1.next()) {
                    System.out.println("Column 1: "+res1.getInt(1));
                    System.out.println("Column 2: "+res1.getInt(2));
                }
                System.out.println("\nAdding entries to table 2.");

                stmtx.executeUpdate("INSERT INTO test_table2 (a, b)
VALUES (3,4)");
                res1 = stmtx.executeQuery("SELECT * FROM test_table2");

                System.out.println("\nInspecting table 2.");

                while (res1.next()) {
                    System.out.println("Column 1: "+res1.getInt(1));
                    System.out.println("Column 2: "+res1.getInt(2));
                }

                System.out.print("\nNow attempting to rollback
changes.");

                txn.rollback();

                // Next, we try to commit changes
                txn.begin();
                stmtx = conn.createStatement();
```

```
                ResultSet res2 = null;

                System.out.println("\nNow checking state of table 1.");

                res2 = stmtx.executeQuery("SELECT * FROM test_table");

                while (res2.next()) {
                    System.out.println("Column 1: "+res2.getInt(1));
                    System.out.println("Column 2: "+res2.getInt(2));
                }

                System.out.println("\nNow checking state of table 2.");

                stmtx = conn.createStatement();

                res2 = stmtx.executeQuery("SELECT * FROM test_table2");

                while (res2.next()) {
                    System.out.println("Column 1: "+res2.getInt(1));
                    System.out.println("Column 2: "+res2.getInt(2));
                }

                txn.commit();
            }
            catch (Exception ex) {
                ex.printStackTrace();
                System.exit(0);
            }
        }
        catch (Exception sysEx) {
            sysEx.printStackTrace();
            System.exit(0);
        }
    }
}
```

Report a bug

10.9.4. Documentation API pour JBoss Transactions JTA

La documentation API pour le sous-système de Transaction de JBoss EAP 6 est disponible à l'endroit suivant :

- UserTransaction - http://download.oracle.com/javaee/1.3/api/javax/transaction/UserTransaction.html

Si vous utilisez JBoss Development Studio pour développer vos applications, la documentation API est incluse dans le menu **Help**.

Report a bug

CHAPITRE 11. HIBERNATE

11.1. HIBERNATE CORE

Hibernate Core est une bibliothèque de mappages objet/relationnel. Elle fournit le framework de mappage des tables de la base de données, permettant aux applications d'éviter une interaction directe avec la base de données.

Pour plus d'information, consulter Section 11.2.2, « Hibernate EntityManager » et Section 11.2.1, « JPA ».

Report a bug

11.2. JAVA PERSISTENCE API (JPA)

11.2.1. JPA

L'API Java Persistence (JPA) est standard pour l'utilisation de la persistance dans les projets Java. Les applications Java EE 6 utilisent la spécification Java Persistence 2.0, documentée ici : http://www.jcp.org/en/jsr/detail?id=317.

Hibernate EntityManager implémente les interfaces de programmation et les règles de cycle de vie définies par la spécification. Il fournit une solution Java Persistence complète pour la plate-forme JBoss EAP 6.

JBoss EAP 6 est conforme à 100% avec la spécification Java Persistence 2.0. Hibernate fournit également quelques fonctionnalités supplémentaires à la spécification.

Pour commencer avec JPA et JBoss EAP 6, voir les quickstarts **`bean-validation`**, **`greeter`**, et **`kitchensink`** : Section 1.4.2.1, « Accès aux Quickstarts » .

Report a bug

11.2.2. Hibernate EntityManager

Hibernate EntityManager implémente les interfaces de programmation et les règles de cycles de vie définies dans JPA 2.0 specification. Il procure une solution Java Persistence complète pour la plateforme JBoss EAP 6.

Pour plus d'informations, voir Section 11.2.1, « JPA » and Section 11.1, « Hibernate Core ».

Report a bug

11.2.3. Guide de départ

11.2.3.1. Créer un projet JPA dans JBoss Developer Studio

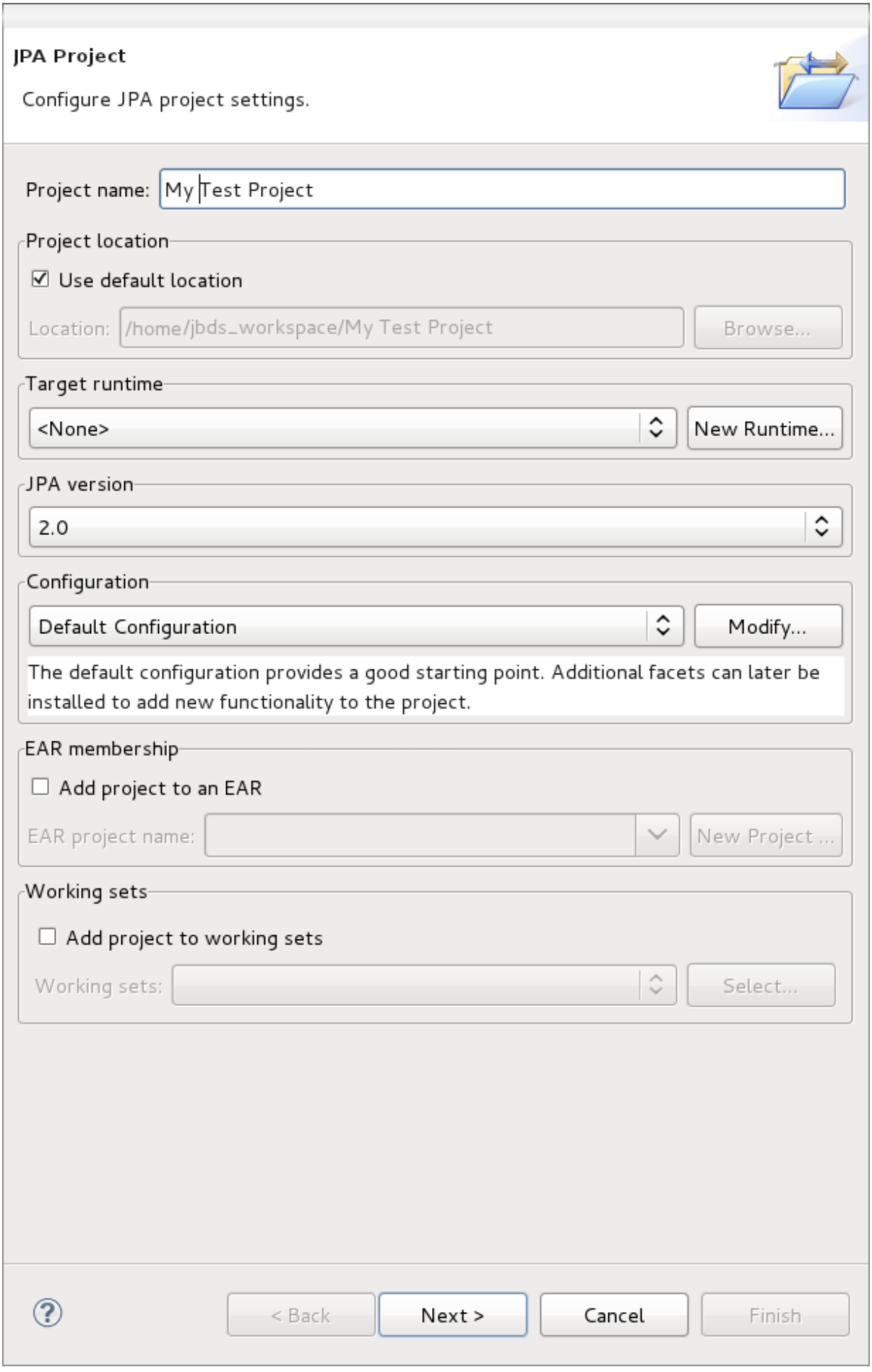
Résumé

Cet exemple indique les étapes à effectuer pour créer un projet JPA dans JBoss Developer Studio.

Procédure 11.1. Créer un projet JPA dans JBoss Developer Studio

1. Dans la fenêtre JBoss Developer Studio, cliquer sur **Fichier** → **Nouveau** → **Projet JPA**.

2. Dans la boîte de dialogue du projet, taper le nom du projet.

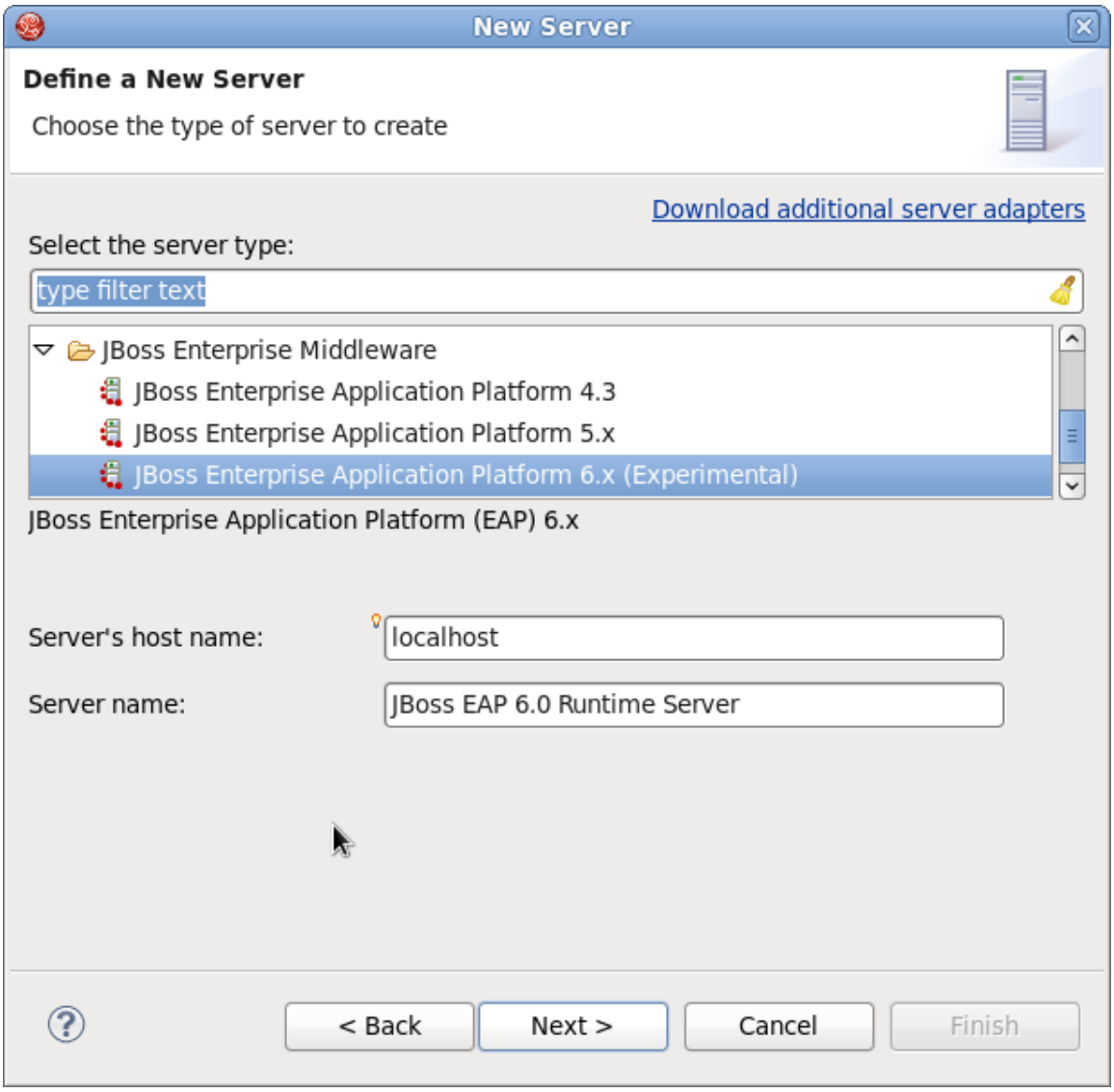


3. Sélectionner un runtime cible depuis le menu déroulant.

4. a. Si aucun runtime cible n'est disponible, cliquer sur **`Runtime Cible`**.

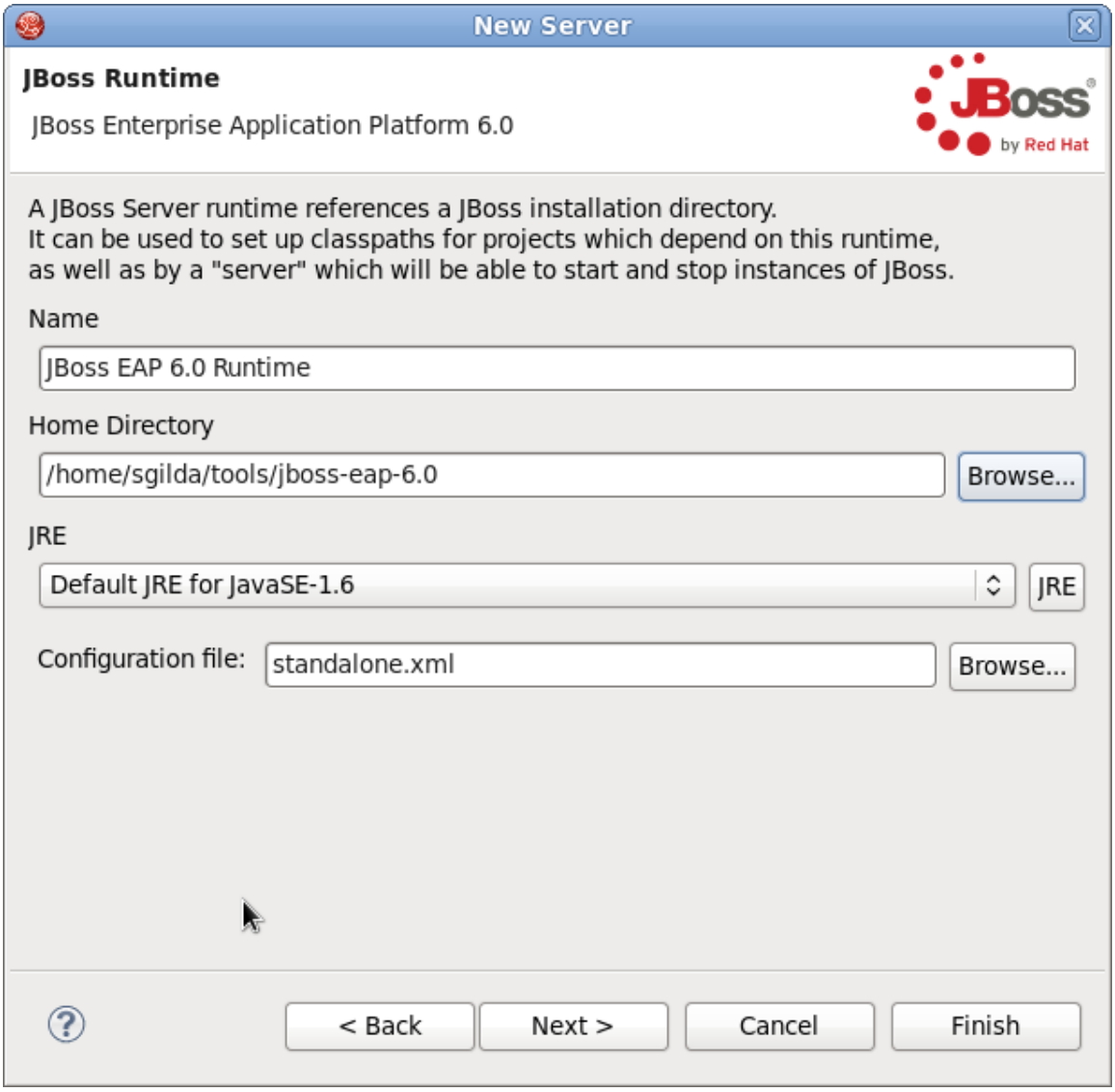
   b. Trouver le Dossier JBoss Community dans la liste.

   c. Sélectionner JBoss Enterprise Application Platform 6.x Runtime



   d. Cliquer sur **`Suivant`**.

   e. Dans le champ Répertoire Personnel, cliquer sur **`Naviguer`** pour définir le dossier source JBoss EAP comme Répertoire Personnel.



f. Cliquer sur **Terminé**.

5. Cliquer sur **Suivant**.
6. Laisser les dossiers source sur la fenêtre de chemin de build en mode défaut, et cliquer sur **Suivant**.
7. Dans le menu déroulant de la Plateforme, vous assurer que Hibernate (JPA 2.x) est sélectionné.
8. Cliquer sur **Terminé**.
9. Si cela vous est demandé, choisissez si vous souhaitez ouvrir la fenêtre de perspective JPA.

Report a bug

11.2.3.2. Créer le fichier de paramètres de persistance dans JBoss Developer Studio

Résumé

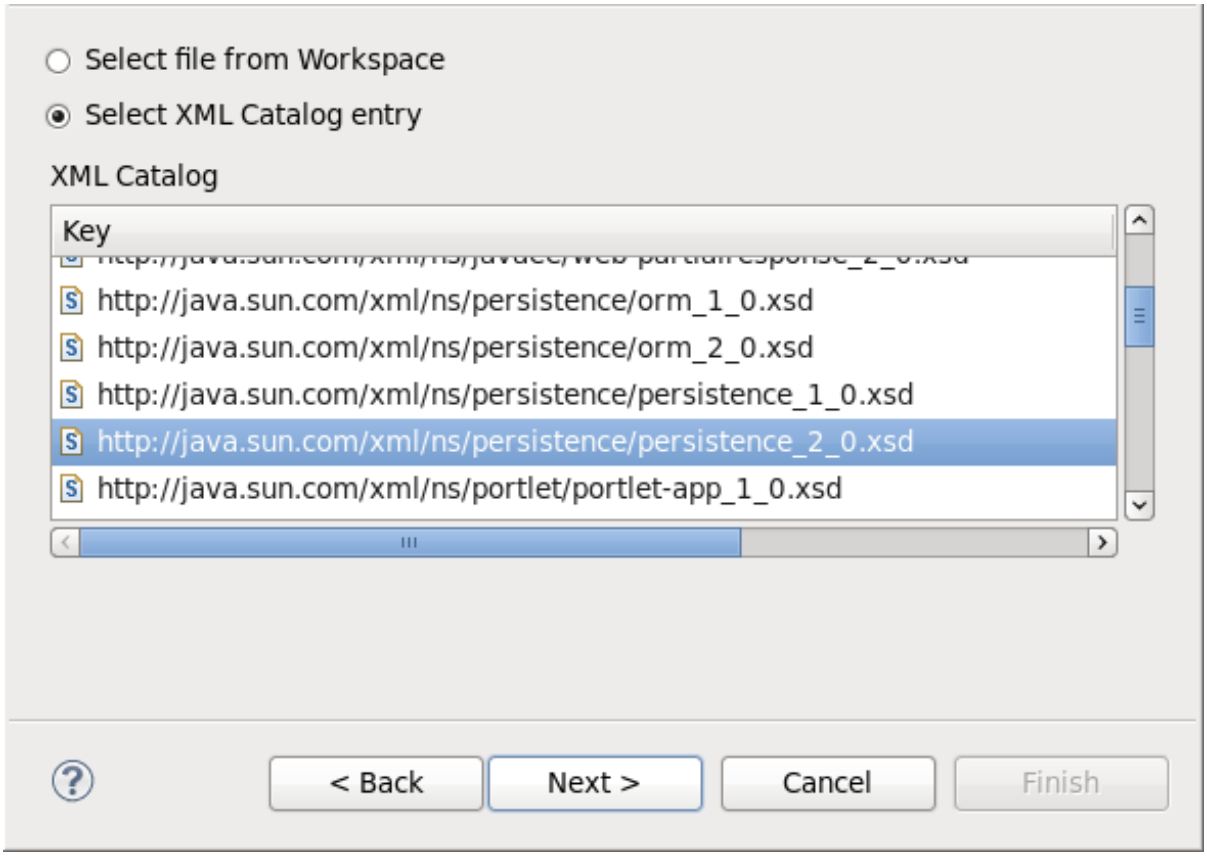
Ce sujet couvre le processus de création du fichier `persistence.xml` dans un projet Java qui utilise JBoss Developer Studio.

Prérequis

- Section 1.3.1.4, « Démarrer JBoss Developer Studio »

Procédure 11.2. Créer et configurer un nouveau fichier de configuration de persistance

1. Ouvrir un projet EJB 3.x dans JBoss Developer Studio.
2. Cliquer à droite sur le répertoire racine du projet dans le panneau **`Project Explorer`**
3. Sélectionner **Nouveau** → **Autres...**.
4. Sélectionner **`Fichier XML`** à partir du dossier **`XML`** et cliquer sur **`Suivant`**.
5. Sélectionner le dossier **`ejbModule/META-INF`** comme répertoire parent.
6. Nommer le fichier **`persistence.xml`** et cliquer sur **`Suivant`**.
7. Sélectionner **`Créer fichier XML à partir d'un fichier de schéma XML`** et cliquer sur **`Suivant`**.
8. Sélectionner **`http://java.sun.com/xml/ns/persistence/persistence_2.0.xsd`** dans la liste **`Sélectionner une entrée de Catalogue XML`** et cliquer sur **`Suivant`**.



9. Cliquer sur **`Terminé`** pour créer le fichier.

Résultat :

Le fichier **`persistence.xml`** a été créé dans le dossier **`META-INF/`** et est prêt pour la configuration. Un exemple de fichier se trouve ici : Section 11.2.3.3, « Exemple de fichier de configuration de persistance »

Report a bug

11.2.3.3. Exemple de fichier de configuration de persistance

Exemple 11.1. persistence.xml

```
<persistence xmlns="http://java.sun.com/xml/ns/persistence"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://java.sun.com/xml/ns/persistence
http://java.sun.com/xml/ns/persistence/persistence_2_0.xsd"
   version="2.0">
   <persistence-unit name="example" transaction-type="JTA">
      <provider>org.hibernate.ejb.HibernatePersistence</provider>
      <jta-data-source>java:jboss/datasources/ExampleDS</jta-data-
source>
      <mapping-file>ormap.xml</mapping-file>
      <jar-file>TestApp.jar</jar-file>
      <class>org.test.Test</class>
      <shared-cache-mode>NONE</shared-cache-mode>
      <validation-mode>CALLBACK</validation-mode>
      <properties>
         <property name="hibernate.dialect"
value="org.hibernate.dialect.H2Dialect"/>
         <property name="hibernate.hbm2ddl.auto" value="create-drop"/>
      </properties>
   </persistence-unit>
</persistence>
```

Report a bug

11.2.3.4. Créer le fichier de configuration Hibernate dans JBoss Developer Studio

Prérequis

- Section 1.3.1.4, « Démarrer JBoss Developer Studio »

Résumé

Ce sujet traite du procédé à suivre pour créer le fichier **`hibernate.cfg.xml`** dans un Projet Java en utilisant JBoss Developer Studio.

Procédure 11.3. Créer un nouveau fichier de Configuration Hibernate

1. Ouvrir un projet Java dans JBoss Developer Studio
2. Cliquer à droite sur le répertoire racine du projet dans le panneau **`Project Explorer`**
3. Sélectionner **Nouveau** → **Autre...**.
4. Sélectionner **`Fichier de configuration Hibernate`** depuis le dossier **`Hibernate`** et cliquer sur **`Suivant`**.
5. Sélectionner le répertoire **`src/`** et cliquer sur **`Suivant`**.
6. Configurer :

- Nom de la fabrique à Session
- Dialecte de base de données
- Classe pilote
- URL de connexion
- Nom d'utilisateur
- Mot de passe

7. Cliquer sur **Terminer** pour créer le fichier.

Résultat :

Le fichier **hibernate.cfg.xml** a été créé dans le dossier **src/**. Un exemple de fichier est disponible ici : Section 11.2.3.5, « Exemple de fichier de configuration Hibernate » .

Report a bug

11.2.3.5. Exemple de fichier de configuration Hibernate

Exemple 11.2. hibernate.cfg.xml

```
<?xml version='1.0' encoding='utf-8'?>
<!DOCTYPE hibernate-configuration PUBLIC
        "-//Hibernate/Hibernate Configuration DTD 3.0//EN"
        "http://www.hibernate.org/dtd/hibernate-configuration-3.0.dtd">

<hibernate-configuration>

    <session-factory>

        <!-- Datasource Name -->
        <property name="connection.datasource">ExampleDS</property>

        <!-- SQL dialect -->
        <property
name="dialect">org.hibernate.dialect.H2Dialect</property>

        <!-- Enable Hibernate's automatic session context management --
>
        <property
name="current_session_context_class">thread</property>

        <!-- Disable the second-level cache  -->
        <property
name="cache.provider_class">org.hibernate.cache.NoCacheProvider</propert
y>

        <!-- Echo all executed SQL to stdout -->
        <property name="show_sql">true</property>

        <!-- Drop and re-create the database schema on startup -->
        <property name="hbm2ddl.auto">update</property>
```

```
        <mapping
resource="org/hibernate/tutorial/domain/Event.hbm.xml"/>

    </session-factory>

</hibernate-configuration>
```

Report a bug

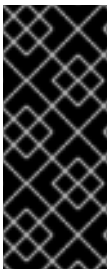
11.2.4. Configuration

11.2.4.1. Propriétés de configuration de Hibernate

Tableau 11.1. Propriétés

Nom de propriété	Description
hibernate.dialect	Le nom de classe d'un **`org.hibernate.dialect.Dialect`** Hibernate. Permet à Hibernate de générer SQL optimisé pour une base de données relative particulière. Dans la plupart des cas, Hibernate pourra choisir la mise en œuvre **`org.hibernate.dialect.Dialect`** correcte, selon les **`JDBC metadata`** renvoyées par le pilote JDBC.
hibernate.show_sql	Booléen. Écrit toutes les déclarations SQL à la console. C'est une alternative pour définir la catégorie du journal **`org.hibernate.SQL`** sur **`debug`**.
hibernate.format_sql	Booléen. Mettre en forme le SQL dans le journal et la console.
hibernate.default_schema	Qualifie les noms de tableaux non qualifiés avec le schéma/espace tableau donné dans le SQL généré.
hibernate.default_catalog	Qualifie les noms de tableaux non qualifiés avec le catalogue donné dans le SQL généré.
hibernate.session_factory_name	Le **`org.hibernate.SessionFactory`** sera automatiquement lié à ce nom dans JNDI après avoir été créé. Par exemple, **`jndi/composite/name`**.

Nom de propriété	Description
hibernate.max_fetch_depth	Définit une "profondeur" maximum pour l'arborescence de récupération de la jointure externe pour les associations à fin unique (un-à-un, plusieurs-à-un). Un **0** désactive la récupération de jointure externe par défaut. La valeur recommandée se situe entre **0** et **3**.
hibernate.default_batch_fetch_size	Définit une taille par défaut pour la récupération en lot d'associations de Hibernate. Les valeurs recommandées sont **4**, **8**, et **16**.
hibernate.default_entity_mode	Définit un mode par défaut pour la réprésentation d'entité pour toutes les sessions ouvertes à partir de **SessionFactory**. Les valeurs comprennent : **dynamic-map**, **dom4j**, **pojo**.
hibernate.order_updates	Booléen. Oblige Hibernate à ordonner les mises à jour SQL par la valeur clé principale des éléments mis à jour. Cela se traduira en un nombre inférieur de blocages de transactions dans des systèmes hautement simultanés.
hibernate.generate_statistics	Booléen. Si autorisé, Hibernate va collecter les statistiques utiles pour le réglage de performance.
hibernate.use_identifier_rollback	Booléen. Si autorisé, les propriétés d'identifiant générées seront restaurées à leur valeur par défaut lorsque les objets sont supprimés.
hibernate.use_sql_comments	Booléen. Si activé, Hibernate génèrera des commentaires à l'intérieur de SQL, pour faciliter de débogage. La valeur par défaut est **false**.
hibernate.id.new_generator_mappings	Booléen. Cette propriété est appropriée lorsque **@GeneratedValue** est utilisée. Elle indique si les nouvelles implémentations **IdentifierGenerator** sont utilisées pour **javax.persistence.GenerationType.AUTO**, **javax.persistence.GenerationType.TABLE** et **javax.persistence.GenerationType.SEQUENCE**. La valeur par défaut est**true**.



IMPORTANT

Dans **hibernate.id.new_generator_mappings**, les nouvelles applications devront garder la valeur par défaut **true**. Les applications existantes qui utilisent Hibernate 3.3.x devront sans doute modifier cette valeur à **false** pour continuer à utiliser un objet de séquence ou un générateur basé-table et pour maintenir la compatibilité rétro-active.

Report a bug

11.2.4.2. Hibernate JDBC et Propriétés de Connexion

Tableau 11.2. Propriétés

Nom de propriété	Description
hibernate.jdbc.fetch_size	Valeur non nulle qui détermine la taille de récupération JDBC (appelle `Statement.setFetchSize()`).
hibernate.jdbc.batch_size	Une valeur non nulle active l'utilisation des mises à jour de lots de JDBC2 par Hibernate. Les valeurs recommandées se situent entre `5` et `30`.
hibernate.jdbc.batch_versioned_data	Booléen. Définir cette propriété sur `true` si le pilote JDBC renvoie des nombres de lignes corrects avec `executeBatch()`. Hibernate utilisera ensuite un DML en lot pour les données versionnées automatiquement. La valeur par défaut est `false`.
hibernate.jdbc.factory_class	Sélectionner un `org.hibernate.jdbc.Batcher` personnalisé. La plupart des applications n'auront pas besoin de cette propriété de configuration.
hibernate.jdbc.use_scrollable_resultset	Booléen. Active l'utilisation des ensembles de résultats déroulants de JDBC2 par Hibernate. Cette propriété n'est nécessaire que lorsque l'on utilise des connexions JDBC fournies par l'utilisateur. Sans quoi, Hibernate utilise des métadonnées de connexion.
hibernate.jdbc.use_streams_for_binary	Booléen. Ceci est une propriété de niveau système. Utiliser les flux lors de l'écriture/la lecture de types `binary` ou `serializable` depuis/vers JDBC.
hibernate.jdbc.use_get_generated_keys	Booléen. Active l'utilisation de JDBC3 `PreparedStatement.getGeneratedKeys()` pour récupérer les cléfs générées en mode natif après insertion. Requiert le pilote JDBC3+ et JRE1.4+. Défini sur false si le pilote JDBC rencontre des problèmes avec les générateurs d'identifiants Hibernate. Par défaut, il tente de déterminer les capacités du pilote en utilisant les métadonnées de connexion.
hibernate.connection.provider_class	Le nom de classe d'un `org.hibernate.connection.ConnectionProvider` personnalisé qui fournit des connexions JDBC à Hibernate.
hibernate.connection.isolation	Définit le niveau d'isolation des transactions JDBC. Vérifier `java.sql.Connection` pour des valeurs compréhensibles, mais veuillez noter que la plupart des bases de données ne prennent pas en charge tous les niveaux d'isolation et que quelques unes définissent des isolations additionnelles, non-standard. Les valeurs standard sont `1, 2, 4, 8`.

Nom de propriété	Description
hibernate.connection.autocommit	Booléen. Cette propriété n'est pas recommandée à l'utilisation. Active l'autovalidation pour les connexions « en commun » de JDBC.
hibernate.connection.release_mode	Indique à quel moment Hibernate devra diffuser les connexions JDBC. Par défaut, une connexion JDBC est maintenue jusqu'à ce que la session soit explicitement fermée ou déconnectée. La valeur par défaut **`auto`** choisira **`after_statement`** pour les stratégies de transaction JTA et CMT, et **`after_transaction`** pour la stratégie de transaction JDBC. Les valeurs disponibles sont **`auto`** (par défaut) | **`on_close`** | **`after_transaction`** | **`after_statement`**. Ce paramètre n'affecte que les **`Session`**s renvoyées depuis **`SessionFactory.openSession`**. Pour les **`Session`**s obtenues par **`SessionFactory.getCurrentSession`**, l'implémentation **`CurrentSessionContext`** configurée pour l'utilisation contrôle le mode de publication de connexion pour ces **`Session`**s.
hibernate.connection.<*propertyName*>	Passer la propriété JDBC <*propertyName*> à **`DriverManager.getConnection()`**.
hibernate.jndi.<*propertyName*>	Passer la proriété <*propertyName*> à **`InitialContextFactory`** de JNDI.

Report a bug

11.2.4.3. Propriétés d'Hibernate Cache

Tableau 11.3. Propriétés

Nom de propriété	Description
`hibernate.cache.provider_class`	Le nom de classe d'un **`CacheProvider`** personnalisé.

Nom de propriété	Description
hibernate.cache.use_minimal_puts	Booléen. Optimise l'opération cache de second niveau pour minimiser les écritures, au détriment de lectures plus fréquentes. Cette configuration est surtout utile pour les caches clusterisés et, dans Hibernate 3, est activée par défaut pour les implémentations cache clusterisées.
hibernate.cache.use_query_cache	Booléen. Active le cache de recherche. Les recherches individuelles doivent toujours être définies comme cachables.
hibernate.cache.use_second_level_cache	Booléen. Utilisé pour désactiver totalement le cache de second niveau, qui est activé par défaut pour les classes qui spécifient un mappage **<cache>**.
hibernate.cache.query_cache_factory	Le nom de classe d'une interface **QueryCache** personnalisée. La valeur par défaut est le **StandardQueryCache** intégré.
hibernate.cache.region_prefix	Un préfixe à utiliser pour les noms régionaux de cache de second niveau.
hibernate.cache.use_structured_entries	Booléen. Force Hibernate à stocker des données dans un cache de second niveau dans un format plus amical pour l'utilisateur.
hibernate.cache.default_cache_concurrency_strategy	Configuration utilisée pour donner le nom de la statégie qu'il faut **org.hibernate.annotations.CacheConcurrencyStrategy** quand **@Cacheable** ou **@Cache** sont utilisés. **@Cache(strategy="..")** est utilisé pour remplacer cette valeur par défaut.

Report a bug

11.2.4.4. Propriétés de transaction Hibernate

Tableau 11.4. Propriétés

Nom de propriété	Description
hibernate.transaction.factory_class	Le nom de classe d'une **TransactionFactory** à utiliser avec l'API de **Transaction** de Hibernate. Valeur par défaut : **JDBCTransactionFactory**.
jta.UserTransaction	Un nom JNDI utilisé par **JTATransactionFactory** pour obtenir la **UserTransaction** JTA depuis le serveur d'applications.

Nom de propriété	Description
`hibernate.transaction.manager_lookup_class`	Le nom de classe d'une **`TransactionManagerLookup`**. Requis lorsque la mise en cache de niveau JVM est activée ou lorsque le générateur hilo est utilisé dans un environnement JTA.
`hibernate.transaction.flush_before_completion`	Booléen. Si activé, la session sera automatiquement vidée avant la phase d'achèvement de la transaction. Une gestion de contexte de session automatique et intégrée est préférée.
`hibernate.transaction.auto_close_session`	Booléen. Si activé, la session sera automatiquement fermée après la phase d'achèvement de la transaction. Une gestion de contexte de session automatique et intégrée est préférable.

Report a bug

11.2.4.5. Propriétés Hibernate diverses

Tableau 11.5. Propriétés

Nom de propriété	Description
`hibernate.current_session_context_class`	Fournit une stratégie personnalisée pour l'étendue de la **`Session`** « actuelle ». Les valeurs comprennent **`jta`** | **`thread`** | **`managed`** | **`custom.Class`**.
`hibernate.query.factory_class`	Choisir l'implémentation de l'analyseur de HQL : **`org.hibernate.hql.internal.ast.ASTQueryTranslatorFactory`** ou **`org.hibernate.hql.internal.classic.ClassicQueryTranslatorFactory`**.
`hibernate.query.substitutions`	Utilisé pour mapper à partir de jetons dans les requêtes Hibernate aux jetons SQL (les jetons peuvent avoir un nom fonctionnel ou littéral). Par exemple, **`hqlLiteral=SQL_LITERAL, hqlFunction=SQLFUNC`**.
`hibernate.hbm2ddl.auto`	Valide ou exporte automatiquement le schéma DDL vers la base de données quand la **`SessionFactory`** est créée. Avec **`create-drop`**, le schéma de base de données sera déposé lorsque la **`SessionFactory`** est fermée explicitement. Les options de valeur de propriété sont **`validate`** | **`update`** | **`create`** | **`create-drop`**

Nom de propriété	Description
hibernate.hbm2ddl.import_files	Les noms séparés par des virgules des fichiers optionnels contenant des déclarations SQL DML exécutées pendant la création de **SessionFactory**. Cela est utile pour tester ou démontrer. Par exemple, en ajoutant des déclarations INSERT, la base de données peut être remplie avec un lot minimum de données quand elle est déployée. Exemple de valeur : **/humans.sql,/dogs.sql**. L'ordre de fichier compte, puisque les déclarations d'un fichier donné sont exécutées avant la déclaration du fichier suivant. Ces déclarations ne sont exécutées que si le schéma est créé (c'est-à-dire si **hibernate.hbm2ddl.auto** est défini comme **create** ou **create-drop**).
hibernate.hbm2ddl.import_files_sql_extractor	Le nom de classe d'un **ImportSqlCommandExtractor** personnalisé. Valeur par défaut de **SingleLineSqlCommandExtractor** intégré. Cela est utile pour implémenter un analyseur dédié qui extrait une déclaration unique de SQL depuis chaque fichier d'importation. Hibernate fournit également **MultipleLinesSqlCommandExtractor**, qui prend en charge des instructions/commentaires et des chaînes citées réparties sur de multiples lignes (point-virgule obligatoire à la fin de chaque déclaration).
hibernate.bytecode.use_reflection_optimizer	Booléen. Ceci est une propriété de niveau système, qui ne peut pas être définie dans le fichier **hibernate.cfg.xml**. Elle permet l'utilisation de la manipulation bytecode au lieu de la réflexion d'exécution. La réflexion peut parfois être utile lors de la résolution de problèmes. Hibernate requiert toujours soit CGLIB ou javassist même si l'optimizer est éteint.
hibernate.bytecode.provider	Javassist et cglib peuvent tous les deux être utilisés comme moteurs de manipulation de byte. La valeur par défaut est **javassist**. La valeur de propriété est soit **javassist** soit **cglib**.

Report a bug

11.2.4.6. Dialectes SQL Hibernate

IMPORTANT

La propriété **`hibernate.dialect`** devrait être définie sur la sous-classe **`org.hibernate.dialect.Dialect`** correcte pour la base de données de l'application. Si un dialecte est indiqué, Hibernate utilisera des valeurs par défaut raisonnables pour quelques unes des autres propriétés. Cela signifie qu'elles n'ont pas besoin d'être spécifiées manuellement.

Tableau 11.6. Dialectes SQL (`hibernate.dialect`)

RDBMS	Dialecte
DB2	**`org.hibernate.dialect.DB2Dialect`**
DB2 AS/400	**`org.hibernate.dialect.DB2400Dialect`**
DB2 OS390	**`org.hibernate.dialect.DB2390Dialect`**
Firebird	**`org.hibernate.dialect.FirebirdDialect`**
FrontBase	**`org.hibernate.dialect.FrontbaseDialect`**
H2 Database	**`org.hibernate.dialect.H2Dialect`**
HypersonicSQL	**`org.hibernate.dialect.HSQLDialect`**
Informix	**`org.hibernate.dialect.InformixDialect`**
Ingres	**`org.hibernate.dialect.IngresDialect`**
Interbase	**`org.hibernate.dialect.InterbaseDialect`**
Mckoi SQL	**`org.hibernate.dialect.MckoiDialect`**
Microsoft SQL Server 2000	**`org.hibernate.dialect.SQLServerDialect`**
Microsoft SQL Server 2005	**`org.hibernate.dialect.SQLServer2005Dialect`**
Microsoft SQL Server 2008	**`org.hibernate.dialect.SQLServer2008Dialect`**
Microsoft SQL Server 2012	**`org.hibernate.dialect.SQLServer2008Dialect`**

RDBMS	Dialecte
MySQL5	`org.hibernate.dialect.MySQL5Dialect`
MySQL5 avec InnoDB	`org.hibernate.dialect.MySQL5InnoDBDialect`
MySQL avec MyISAM	`org.hibernate.dialect.MySQLMyISAMDialect`
Oracle (toute version)	`org.hibernate.dialect.OracleDialect`
Oracle 9i	`org.hibernate.dialect.Oracle9iDialect`
Oracle 10g	`org.hibernate.dialect.Oracle10gDialect`
Oracle 11g	`org.hibernate.dialect.Oracle10gDialect`
Pointbase	`org.hibernate.dialect.PointbaseDialect`
PostgreSQL	`org.hibernate.dialect.PostgreSQLDialect`
PostgreSQL 9.2	`org.hibernate.dialect.PostgreSQL82Dialect`
Postgres Plus Advanced Server	`org.hibernate.dialect.PostgresPlusDialect`
Progress	`org.hibernate.dialect.ProgressDialect`
SAP DB	`org.hibernate.dialect.SAPDBDialect`
Sybase	`org.hibernate.dialect.SybaseASE15Dialect`
Sybase 15.7	`org.hibernate.dialect.SybaseASE157Dialect`
Sybase Anywhere	`org.hibernate.dialect.SybaseAnywhereDialect`

Report a bug

11.2.5. Caches de second niveau

11.2.5.1. Les caches de second niveau

Un cache de second niveau est un store de données locales qui contient des informations persistées en dehors de la session d'application. Le cache est géré par le fournisseur de persistances, qui améliore le temps d'exécution en gardant les données séparées de l'application.

JBoss EAP 6 prend en charge la mise en cache dans les cas suivants :

- Web Session Clustering
- Stateful Session Bean Clustering
- SSO Clustering
- Cache de second niveau d'Hibernate

Chaque conteneur cache définit un "repl" et un "dist". Ces caches ne doivent pas être utilisés directement par les applications utilisateur.

Report a bug

11.2.5.2. Configurer un cache de second niveau pour Hibernate

Ce sujet couvre les besoins de configuration pour permettre à Infinispan d'agir en tant que second niveau de cache pour Hibernate.

Procédure 11.4. Créer et modifier le fichier `hibernate.cfg.xml`

1. **Créer le fichier hibernate.cfg.xml**
   Créer le fichier **`hibernate.cfg.xml`** dans le chemin de classe du déploiement. Pour plus de détails, voir Section 11.2.3.4, « Créer le fichier de configuration Hibernate dans JBoss Developer Studio » .

2. Ajouter ces lignes d'XML au fichier **`hibernate.cfg.xml`** de votre application. Le XML doit être à l'intérieur des balises <session-factory>:

   ```
   <property
   name="hibernate.cache.use_second_level_cache">true</property>
   <property name="hibernate.cache.use_query_cache">true</property>
   ```

3. Ajouter un élément ci-dessous à la section <session-factory> de votre fichier **`hibernate.cfg.xml`** :

   - **Si le CacheManager Infinispan est lié au JNDI :**

     ```
     <property name="hibernate.cache.region.factory_class">
         org.hibernate.cache.infinispan.JndiInfinispanRegionFactory
     </property>
     <property name="hibernate.cache.infinispan.cachemanager">
         java:CacheManager
     </property>
     ```

   - **Si le CacheManager Infinispan est autonome :**

```
<property name="hibernate.cache.region.factory_class">
    org.hibernate.cache.infinispan.InfinispanRegionFactory
</property>
```

Résultat

Infinispan est configuré au second niveau de cache dans Hibernate.

Report a bug

11.3. ANNOTATIONS HIBERNATE

11.3.1. Annotations Hibernate

Tableau 11.7. Annotations définies d'Hibernate

Annotation	Description
AccessType	Type d'accès de propriété
Tous	Définit une association ToOne pointant vers plusieurs types d'entités. L'association du type d'entité correspondant se fait à travers une colonne discriminatoire de métadonnées. Ce type de mappage devrait seulement être marginal.
AnyMetaDef	Définit les métadonnées @Any et @manyToAny.
AnyMedaDefs	Définit les ensembles de métadonnées @Any et @ManyToAny. Peut être défini au niveau d'entité ou de paquetage.
BatchSize	Taille de lot pour chargement SQL.
Cache	Ajouter une stratégie de mise en cache à une entité root ou une collection.
Cascade	Appliquer une stratégie de cascade sur une association
Check	Contraintes de vérification SQL arbitraires qui peuvent être définies aux niveaux de classe, de propriété ou de collection.
Columns	Prend en charge une gamme de colonnes. Utile pour les mappages de type utilisateur de composant.

Annotation	Description
ColumnTransformer	Expression SQL personnalisée utilisée pour lire la valeur depuis et écrire une valeur vers une colonne. Utiliser pour le chargement/enregistrement d'objet direct ainsi que les requêtes. L'expression de lecture doit contenir exactement un "?" pour la valeur.
ColumnTransformers	Annotation plurielle pour @ColumnTransformer. Utile lorsque plus d'une colonne utilise ce comportement.
DiscriminatorFormula	Formule discriminatoire à placer à l'entité de root.
DiscriminatorOptions	Annotation optionnelle pour exprimer les propriétés discriminatoires spécifiques à Hibernate.
Entity	Prolonge l'entité avec les caractéristiques Hibernate.
Fetch	Définit la stratégie de récupération utilisée pour l'association donnée.
FetchProfile	Définit le profil de stratégie de récupération
FetchProfiles	Annotation plurielle pour @FetchProfile.
Filter	Ajoute des filtres à une entité ou une entité de cible d'une collection.
FilterDef	Définition de Filtre.
FilterDefs	Gamme de définitions de filtre.
FilterJoinTable	Ajoute des filtres pour une collection rejoindre une table
FilterJoinTables	Ajoute de multiples @FilterJoinTable à une collection
Filters	Ajoute de multiples @Filters.
Formula	A utiliser comme remplacement pour @Column dans la plupart des emplacements. La formule doit être un fragment SQL valide.
Generated	Cette propriété annotée est générée par la base de données.

Annotation	Description
GenericGenerator	Annotation de générateur décrivant toute sorte de générateur Hibernate d'une manière non-typée.
GenericGenerators	Gamme de définitions de générateur génériques.
Immutable	Marque une Entité ou une Collection comme immuable. Si aucune annotation, l'élément est mutable. Une entité immuable peut ne pas être mise à jour par l'application. Les mises à jour vers une entité immuable seront ignorées, mais aucune exception ne sera levée. Placer @Immutable sur une collection rend la collection immuable, ce qui signifie que les additions et suppressions vers et depuis la collection ne sont pas autorisées. Une HibernateException est levée dans ce cas.
Index	Définit un indice de base de données.
JoinFormula	A utiliser comme remplacement pour @JoinColumn dans la plupart des emplacements. La formule doit être un fragment SQL valable.
LazyCollection	Définit le statut lazy d'une collection
LazyToOne	Définit le statut lazy d'une association ToOne (c'est-à-dire OneToOne or ManyToOne).
Loader	Ecrase la méthode FIND par défaut de Hibernate.
ManyToAny	Définit une association ToMany en indiquant différent types d'entité. L'association du type d'entité correspondant se fait à travers une colonne discriminatoire de métadonnées. Ce type de mappage devrait seulement être marginal.
MapKeyType	Définit le type de clé d'une mappe persistante.
MetaValue	Représente une valeur discriminatoire associée à un type d'entité donné.
NamedNativeQueries	Prolonge les NamedNativeQueries pour maintenir les objets NamedNativeQuery de Hibernate.
NamedNativeQuery	Prolonge la NamedNativeQuery avec les caractéristiques Hibernate.

Annotation	Description
NamedQueries	Etend les NamedQueries pour maintenir les objets NamedQuery de Hibernate.
NamedQuery	Prolonge NamedQuery avec les caractéristiques Hibernate.
IdNaturel	Indique que la propriété fait partie de l'identifiant naturel de l'entité.
NotFound	Action à accomplir lorsqu'un élément est introuvable dans une association.
OnDelete	Stratégie à utiliser pour la suppression de collections, de tableaux ou de sous-classes jointes. OnDelete des tableaux secondaires n'est pas actuellement pris en charge.
OptimisticLock	Indique si une modification de la propriété annotée déclenchera une incrémentation de version d'entité. Si l'annotation n'est pas présente, la propriété est impliquée dans la stratégie de verrouillage optimiste (par défaut).
OptimisticLocking	Utilisé pour définir le style de verrouillage optimiste à appliquer à une entité. Dans une hiérarchie, seulement valide sur l'entité de root.
OrderBy	Ordonner une collection en utilisant l'ordre SQL (pas l'ordre HSL).
ParamDef	Une définition de paramètre.
Paramètre	Modèle clé/valeur
Parent	Renvoie la référence de la propriété en tant que pointeur vers le propriétaire (en général l'entité propriétaire).
Persister	Indique un persister personnalisé
Polymorphisme	Utilisé pour définir le type de polymorphisme qu'Hibernate appliquera aux hiérarchies d'entité.
Proxy	Configuration proxy et lazy d'une classe particulière.
RowId	Prend en charge les caractéristiques de mappage ROWID de Hibernate

Annotation	Description
Tri	Tri de collection (tri de niveau Java).
Source	Annotation optionnelle conjointement avec les propriétés de Version et de version Timestamp. La valeur d'annotation décide de l'endroit où timestamp est généré.
SQLDelete	Ecrase la méthode DELETE par défaut de Hibernate.
SQLDeleteAll	Ecrase la méthode DELETE ALL par défaut de Hibernate.
SQLInsert	Remplace la méthode INSERT INTO par défaut de Hibernate.
SQLUpdate	Remplace la méthode UPDATE par défaut de Hibernate.
Subselect	Mappe une entité immuable et en lecture seule vers une expression sous-sélection SQL donnée.
Synchronize	S'assure qu'auto-flush fonctionne correctement et que les requêtes concernant l'entité dérivée ne renvoient pas des données obsolètes. Principalement utilisé avec Subselect.
Table	Information complémentaire d'une table primaire ou secondaire
Tables	Annotation plurielle de Table
Cible	Définit une source explicite et évite la résolution de réflexion et de génériques.
Tuplizer	Définit un tuplizer pour une entité ou un composant.
Tuplizers	Définit un ensemble de tuplizers pour une entité ou un composant.
Type	Type Hibernate.
TypeDef	Définition d'un type Hibernate
TypeDefs	Gamme de définition de Type Hibernate
Where	Clause Where à ajouter à l'élément Entité ou entité de cible d'une collection. La clause est écrite en SQL.

Annotation	Description
WhereJoinTable	Clause Where à ajouter à la collection joindre une table. La clause est écrite en SQL.

Report a bug

11.4. LANGAGE DE RECHERCHE HIBERNATE

11.4.1. Langage de recherche d'Hibernate

Les langages HQL (Hibernate Query Language) et JPQL (Java Persistence Query Language) sont tous les deux des langages de recherche qui se concentrent sur un modèle objet et sont similaires à SQL de par leur nature. HQL est un sur-ensemble de JPQL. Une requête HQL n'est pas toujours une requête JPQL valide, mais une requête JPQL est toujours une requête HQL valide.

HQL et JPQL sont des manières non sécurisées d'effectuer des opérations de recherche. Les requêtes de critère offrent une approche sécurisée pour les requêtes.

Report a bug

11.4.2. Déclarations HQL

HQL autorise les déclarations **SELECT**, **UPDATE**, **DELETE**, et **INSERT**. La déclaration **INSERT** de HQL n'a pas d'équivalent dans JPQL.

IMPORTANT

Veuillez être attentif au moment où une déclaration **UPDATE** ou **DELETE** est exécutée.

Tableau 11.8. Déclarations HQL

Déclaration	Description

SELECT	Le BNF pour les déclarations **SELECT** dans HQL est :
	`select_statement :: = [select_clause] from_clause [where_clause] [groupby_clause] [having_clause] [orderby_clause]`
	La déclaration **SELECT** de HQL la plus simple qui soit est sous la forme :
	`from com.acme.Cat`

Déclaration	Description
UDPATE	Le BNF pour la déclaration UPDATE dans HQL est le même que dans JPQL.
DELETE	Le BNF pour les déclarations DELETE dans HQL est le même que dans JPQL.

Report a bug

11.4.3. La déclaration INSERT

HQL ajoute la possibilité de définir les déclarations **INSERT**. Il n'existe pas d'équivalent JPQL. Le BNF d'une déclaration **INSERT** HQL est :

```
insert_statement ::= insert_clause select_statement

insert_clause ::= INSERT INTO entity_name (attribute_list)

attribute_list ::= state_field[, state_field ]*
```

La **attribute_list** est analogue à la **column specification** dans la déclaration **INSERT** de SQL. Pour les entités impliquées dans un héritage mappé, seuls les attributs définis directement sur l'entité nommée peuvent être utilisés dans la **attribute_list**. Les propriétés de sur-classe ne sont pas autorisées et les propriétés de sous-classe sont inutiles. En d'autres termes, les déclarations **INSERT** sont, par nature, non-polymorphes.

AVERTISSEMENT

select_statement peut être n'importe quelle requête sélectionnée HQL valide, avec l'avertissement que les types de renvoi doivent correspondre aux types attendus par l'insertion. Actuellement, cela est vérifié lors de la compilation de requêtes plutôt que de permettre une vérification reléguée à la base de données. Cela pourrait causer des problèmes entre les types Hibernate qui sont *equivalent* et non pas *equal*. Par exemple, cela pourrait entraîner des problèmes avec des incompatibilités entre un attribut mappé en tant que **org.hibernate.type.DateType** et un attribut défini en tant que **org.hibernate.type.TimestampType**, bien que la base de données puisse ne pas faire la distinction ou puisse être capable de traiter la conversion.

Pour l'attribut de l'identifiant, la déclaration d'insertion vous propose deux options. Vous pouvez soit indiquer de manière spécifique la propriété de l'identifiant dans la **attribute_list**, dans quel cas sa valeur sera prise à partir de l'expression sélectionnée correspondante, ou l'omettre à partir de la **attribute_list**, dans quel cas une valeur générée est utilisée. Cette dernière option n'est disponible que lors de l'utilisation de générateurs d'identifiants qui opèrent « dans la base de données ». Tenter d'utiliser cette option avec n'importe quel générateur de type « en mémoire » causera une exception en cours de traitement.

Pour les attributs de verrouillages optimistes, la déclaration d'insertion vous propose à nouveau deux options : vous pouvez soit indiquer l'attribut dans la **`attribute_list`**, dans quel cas sa valeur sera prise à partir des expressions sélectionnées correspondantes, ou l'omettre à partir de la **`attribute_list`** dans quel cas la **`seed value`** définie par le **`org.hibernate.type.VersionType`** correspondant est utilisé.

Exemple 11.3. Exemple d'énoncé de requêtes INSERT

```
String hqlInsert = "insert into DelinquentAccount (id, name) select
c.id, c.name from Customer c where ...";
int createdEntities = s.createQuery( hqlInsert ).executeUpdate();
```

Report a bug

11.4.4. La clause FROM

La clause **`FROM`** est chargée de définir l'étendue des types de modèles objets disponibles au reste de la requête. Elle est également chargée de définir toutes les « variables d'identification » disponibles au reste de la requête.

Report a bug

11.4.5. La clause WITH

HQL définit une clause **`WITH`** pour qualifier les conditions de jointure. Cela est spécifique à HQL. JPQL ne définit pas cette fonctionnalité.

Exemple 11.4. Exemple de jointure with-clause

```
select distinct c
from Customer c
    left join c.orders o
        with o.value > 5000.00
```

La grande différence est que, dans le SQL généré, les conditions de **`with clause`** font partie de **`on clause`** dans le SQL généré contrairement aux autres requêtes dans cette section où les conditions HQL/JPQL font partie de la **`where clause`** dans le SQL généré. La différence dans cet exemple en particulier n'est sûrement pas très importante. Le **`with clause`** est quelques fois nécessaire pour des requêtes plus compliquées.

Les jointures explicites peuvent faire référence à des attributs d'association ou de composant/intégrés. Dans le cas d'attributs de composant/intégrés, la jointure est tout simplement logique et n'est pas en corrélation avec une jointure (SQL) physique.

Report a bug

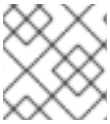
11.4.6. Mises à jour, Insertions et Suppressions en bloc

Hibernate autorise l'utilisation de DML (Data Manipulation Language) pour les données d'insertions, de mises à jour et de suppressions en bloc directement dans la base de données mappée à travers le Langage de Requête Hibernate.

AVERTISSEMENT

L'utilisation de DML pourrait enfreindre le mappage objet/relationnel et affecter l'état objet. L'état objet reste en mémoire et, en utilisant DML, l'état d'un objet en mémoire ne sera pas affecté selon l'opération effectuée sur la base de données sous-jacente. Les données en mémoire doivent être utilisées avec soin si DML est utilisé.

La pseudo-syntaxe pour les déclarations UPDATE et DELETE est : **`( UPDATE | DELETE ) FROM? EntityName (WHERE where_conditions)?`**.



NOTE

Le mot clé **`FROM`** et le **`WHERE Clause`** sont optionnels.

Le résultat d'exécution d'une déclaration UPDATE ou DELETE est le nombre de lignes réellement affectées (mises à jour ou supprimées).

Exemple 11.5. Exemple de déclaration de mise à jour en bloc

```
Session session = sessionFactory.openSession();
Transaction tx = session.beginTransaction();

String hqlUpdate = "update Company set name = :newName where name =
:oldName";
int updatedEntities = s.createQuery( hqlUpdate )
        .setString( "newName", newName )
        .setString( "oldName", oldName )
        .executeUpdate();
tx.commit();
session.close();
```

Exemple 11.6. Exemple de déclaration de suppression en bloc

```
Session session = sessionFactory.openSession();
Transaction tx = session.beginTransaction();

String hqlDelete = "delete Company where name = :oldName";
int deletedEntities = s.createQuery( hqlDelete )
        .setString( "oldName", oldName )
        .executeUpdate();
tx.commit();
session.close();
```

La valeur **`int`** renvoyées par la méthode **`Query.executeUpdate()`** indique le nombre d'entités qui se trouvent dans la base de données et qui sont affectées par l'opération.

En interne, la base de données peut utiliser plusieurs déclarations SQL pour exécuter l'opération en réponse à une mise à jour DML ou à une demande de suppression. Cela est sans doute en raison des relations existantes entre les tableaux et les tableaux de liaisons qui ont besoin d'être mis à jour ou effacés.

Ainsi et par exemple, si on émet une déclaration de suppression (exemple ci-dessus), on risque d'avoir une délétion non seulement des **`Company`** (entreprises) qui contiennent **`oldName`** dans le tableau, mais aussi dans les tableaux de liaisons. Donc, un tableau d'entreprises (Companies) qui se trouve dans une relation BiDirectionelle ManyToMany avec un tableau d'employés (Employee) perdrait des lignes dans le tableau de liaison correspondant **`Company_Employee`** suite à l'exécution de l'exemple précédent.

La valeur **`int deletedEntries`** ci-dessus contiendra le nombre de lignes affectées par cette opération, y compris les lignes qui se trouvent dans les tableaux de liaisons.

La pseudo-syntaxe pour les déclarations INSERT est: **`INSERT INTO EntityName properties_list select_statement`**.

NOTE

Seule la forme INSERT INTO ... SELECT ... est prise en charge; et non pas la forme INSERT INTO ... VALUES ...

Exemple 11.7. Exemple de déclaration d'insertion en bloc

```
Session session = sessionFactory.openSession();
Transaction tx = session.beginTransaction();

String hqlInsert = "insert into Account (id, name) select c.id, c.name
from Customer c where ...";
int createdEntities = s.createQuery( hqlInsert )
        .executeUpdate();
tx.commit();
session.close();
```

Si vous ne fournissez pas la valeur de l'attribut **`id`** via SELECT, un ID sera généré, tant que la base de données sous-jacente prend en charge les clés générées automatiquement. La valeur de retour de cette opération d'insertion en bloc est le nombre d'entrées créées dans la base de données.

Report a bug

11.4.7. Références de collection

Les références aux associations collection-valued font en fait référence aux *valeurs* de cette collection.

Exemple 11.8. Exemple de références de collection

```
select c
from Customer c
    join c.orders o
    join o.lineItems l
    join l.product p
```

```
where o.status = 'pending'
  and p.status = 'backorder'

// alternate syntax
select c
from Customer c,
    in(c.orders) o,
    in(o.lineItems) l
    join l.product p
where o.status = 'pending'
  and p.status = 'backorder'
```

Dans cet exemple, la variable d'identification **o** fait référence au type de modèle de variable **`Order`** qui correspond au type d'éléments de l'association **`Customer#orders`**.

L'exemple montre une autre syntaxe d'association de collection avec **`IN`**. Les deux formes sont équivalentes. La forme choisie par une application est tout simplement une question de goût.

Report a bug

11.4.8. Expressions de chemins qualifiées

Dans le passé, il était indiqué que les associations collection-valued faisaient référence aux *valeurs* de la dite collection. Pour ce type de collection, il existe également un ensemble d'expressions de qualification explicites.

Tableau 11.9. Expressions de chemins

Expression	Description
VALUE	Correspond à la valeur de la collection. C'est équivalent à ne pas spécifier de qualificateur. Utile pour démontrer une intention. Valide pour n'importe quel type de référence collection-valued.
INDEX	Selon les règles HQL, ceci est valable pour les mappages et pour les listes qui spécifient une annotation **`javax.persistence.OrderColumn`** pour désigner la clé de Mappage ou la position de la Liste (aka la valeur OrderColumn). JPQL toutefois réserve ceci pour une utilisation dans la case Liste et ajoute la **`clé`** dans la case Mappage. Les applications intéressées par la transférabilité des fournisseurs JPA doivent tenir compte de cette distinction.
KEY	Uniquement valide pour le mappage. Se réfère à la clé de mappage. Si la clé elle-même est une entité, elle peut naviguer davantage.

Expression	Description
ENTRY	Uniquement valide pour les mappages. Voir le tuple (combinaison d'une clé et de sa valeur) logique du Mappagev`java.util.Map.Entry`. **ENTRY** n'est valide qu'en tant que chemin final et uniquement pour la clause sélectionnée.

Exemple 11.9. Exemple de références de collection qualifiée

```
// Product.images is a Map<String,String> : key = a name, value = file
path

// select all the image file paths (the map value) for Product#123
select i
from Product p
    join p.images i
where p.id = 123

// same as above
select value(i)
from Product p
    join p.images i
where p.id = 123

// select all the image names (the map key) for Product#123
select key(i)
from Product p
    join p.images i
where p.id = 123

// select all the image names and file paths (the 'Map.Entry') for
Product#123
select entry(i)
from Product p
    join p.images i
where p.id = 123

// total the value of the initial line items for all orders for a
customer
select sum( li.amount )
from Customer c
        join c.orders o
        join o.lineItems li
where c.id = 123
  and index(li) = 1
```

Report a bug

11.4.9. Fonctions scalaires

HQL définit des fonctions standard disponibles quelle que soit la base de données sous-jacente utilisée. HQL peut également comprendre des fonctions supplémentaires définies par le Dialect ou l'application.

Report a bug

11.4.10. Fonctions standardisées HQL

Les fonctions suivantes sont disponibles en HQL quelle que soit la base de données utilisée sous-jacente.

Tableau 11.10. Fonctions standardisées HQL

Fonction	Description
BIT_LENGTH	Renvoie la longueur des données binaires.
CAST	Effectue une transcription SQL. La cible de transcription doit désigner le type de mappage Hibernate à utiliser. Voir le chapitre sur les types de données pour obtenir plus d'informations.
EXTRACT	Effectue une extraction SQL sur les valeurs Heure/Date. L'extraction soutire une partie de la valeur (l'année, par exemple). Voir les formes d'abréviation ci-dessous.
SECOND	Abréviation pour extraire une Seconde.
MINUTE	Forme d'abréviation pour extraire une Minute.
HOUR	Abréviation pour extraire une Heure.
DAY	Abréviation pour extraire un Jour.
MONTH	Abréviation pour extraire un Mois.
YEAR	Abréviation pour extraire une Année.
STR	Abréviation pour la conversion d'une valeur en caractère.

Les développeurs d'applications peuvent également fournir leur propre ensemble de fonctions. Habituellement, cela représente des fonctions SQL personnalisées ou des alias pour les extraits de code SQL. Ces déclarations de fonction sont effectuées au moyen de la méthode **`addSqlFunction`** de **`org.hibernate.cfg.Configuration`**

Report a bug

11.4.11. Opération de concaténation

HQL définit un opérateur de concaténation en plus de sa prise en charge de la fonction (**CONCAT**). N'est pas défini par JPQL, donc les applications portables doivent éviter de l'utiliser. L'opérateur de concaténation vient d'un opérateur de concaténation SQL - **||**.

Exemple 11.10. Exemple d'opération de concaténation

```
select 'Mr. ' || c.name.first || ' ' || c.name.last
from Customer c
where c.gender = Gender.MALE
```

Report a bug

11.4.12. Instanciation dynamique

Il y a un type d'expression particulier qui n'est valide que dans la clause Select. Hibernate nomme cela une "dynamic instanciation". JPQL supporte cette fonctionnalité et nomme cela une "constructor expression".

Exemple 11.11. Exemple d'instanciation dynamique - Constructor

```
select new Family( mother, mate, offspr )
from DomesticCat as mother
    join mother.mate as mate
    left join mother.kittens as offspr
```

Au lieu de s'affairer avec l'Object[], nous englobons ici les valeurs dans un objet java de type-safe qui sera retourné en tant que résultat de la demande. La référence de la classe doit être totalement qualifiée et doit avoir un constructeur correspondant.

La classe doit ici être mappée. Si elle représente une entité, les instances résultantes devront être renvoyées dans un état NEW (non géré!).

C'est la partie que JPQL prend en charge également. HQL prend en charge des fonctionnalités en "dynamic instantiation" supplémentaires. Tout d'abord, la recherche peut spécifier de renvoyer une Liste à la place d'un Object[] pour les résultats scalaires :

Exemple 11.12. Exemple d'instanciation dynamique - List

```
select new list(mother, offspr, mate.name)
from DomesticCat as mother
    inner join mother.mate as mate
    left outer join mother.kittens as offspr
```

Les résultats de cette recherche correspondront à List<List> et non pas à List<Object[]>

HQL supporte également l'absorption de résultats scalaires dans une Mappe.

Exemple 11.13. Exemple d'instanciation dynamique - Mappe

```
select new map( mother as mother, offspr as offspr, mate as mate )
```

```
from DomesticCat as mother
    inner join mother.mate as mate
    left outer join mother.kittens as offspr

select new map( max(c.bodyWeight) as max, min(c.bodyWeight) as min,
count(*) as n )
from Cat cxt"/>
```

Les résultats de cette recherche correspondront à List<Map<String,Object>> et non pas à List<Object[]> . Les clés de la mappe sont définies par les alias donnés aux expressions Select.

Report a bug

11.4.13. Prédicats HQL

Les prédicats sont à la base des expressions de recherche, la clause «where», la clause «having». Ce sont des expressions qui résolvent une valeur de vérité, comme **TRUE** ou **FALSE**, bien que les comparaison booléènnes comportant des NULL résolvent les **UNKNOWN**.

Prédicats HQL

Prédicat Nullness

Cherchez une valeur nulle et sans effet. Peut s'appliquer à des références d'attributs de base, à des références d'entité et à des paramètres. De plus, HQL permet une application à des types de composants/intégrables.

Exemple 11.14. Exemples de vérification de Nullness

```
// select everyone with an associated address
select p
from Person p
where p.address is not null

// select everyone without an associated address
select p
from Person p
where p.address is null
```

Prédicat Like

Procède à une comparaison d'équivalence entre des valeurs de chaîne. La syntaxe est la suivante :

```
like_expression ::=
   string_expression
   [NOT] LIKE pattern_value
   [ESCAPE escape_character]
```

Les sémantiques suivent l'expression Like SQL. La **`pattern_value`** est un modèle qui tente de correspondre à l'expression de chaîne **`string_expression`**. Tout comme pour l'expresion «like» SQL, le modèle ou **`pattern_value`** peut utiliser "_" et "%" comme caractères génériques. Les

significations sont les mêmes. "_" correspond à n'importe quel caractère unique. "%" correspond à un certain nombre de caractères.

Le caractère **escape** optionnel est utilisé pour spécifier un caractère d'échappement en combinaison à ce qui est impliqué par "_" ou "%" dans le modèle ou **pattern_value**. Ceci est utile quand on doit chercher des modèles contenant des "_" ou des "%".

Exemple 11.15. Exemples de prédicats «Like»

```
select p
from Person p
where p.name like '%Schmidt'

select p
from Person p
where p.name not like 'Jingleheimmer%'

// find any with name starting with "sp_"
select sp
from StoredProcedureMetadata sp
where sp.name like 'sp|_%' escape '|'
```

Prédicat Between

Ressemble à l'expression SQL **BETWEEN**. Détermine qu'une valeur est entre 2 autres valeurs. Tous les opérandes doivent avoir des types comparables.

Exemple 11.16. Exemples de prédicats «Between»

```
select p
from Customer c
    join c.paymentHistory p
where c.id = 123
  and index(p) between 0 and 9

select c
from Customer c
where c.president.dateOfBirth
        between {d '1945-01-01'}
            and {d '1965-01-01'}

select o
from Order o
where o.total between 500 and 5000

select p
from Person p
where p.name between 'A' and 'E'
```

Report a bug

11.4.14. Comparaisons relationnelles

Les comparaison impliquent un des opérateurs de comparaison - =, >, >=, <, <=, <>]>. HQL also defines <![CDATA[!= comme opérateur de comparaison synonyme de <> . Les opérandes doivent être du même type.

Exemple 11.17. Exemples de comparaisons relationnelles

```
// numeric comparison
select c
from Customer c
where c.chiefExecutive.age < 30

// string comparison
select c
from Customer c
where c.name = 'Acme'

// datetime comparison
select c
from Customer c
where c.inceptionDate < {d '2000-01-01'}

// enum comparison
select c
from Customer c
where c.chiefExecutive.gender = com.acme.Gender.MALE

// boolean comparison
select c
from Customer c
where c.sendEmail = true

// entity type comparison
select p
from Payment p
where type(p) = WireTransferPayment

// entity value comparison
select c
from Customer c
where c.chiefExecutive = c.chiefTechnologist
```

Les comparaison peuvent également impliquer des qualificateurs de sous-requêtes - **ALL**, **ANY**, **SOME**. **SOME** et **ANY** sont synonymes.

Le qualificateur **ALL** passe à true si la comparaison est true pour toutes les valeurs qui se trouvent dans le résultat de la sous-requête. Passe à false si le résultat de la sous-requête est vide.

Exemple 11.18. Exemple de qualificateur de comparaison de sous-requête ALL

```
// select all players that scored at least 3 points
// in every game.
```

```
select p
from Player p
where 3 > all (
   select spg.points
   from StatsPerGame spg
   where spg.player = p
)
```

Le qualificateur **ANY/SOME** passe à true si la comparaison est true pour toutes les valeurs qui se trouvent dans le résultat de la sous-requête. Passe à false si le résultat de la sous-requête est vide.

Report a bug

11.4.15. Prédicat IN

Le prédicat **IN** effectue une vérification pour savoir si une valeur donnée fait partie de la liste des valeurs. Sa syntaxe est la suivante :

```
in_expression ::= single_valued_expression
            [NOT] IN single_valued_list

single_valued_list ::= constructor_expression |
            (subquery) |
            collection_valued_input_parameter

constructor_expression ::= (expression[, expression]*)
```

Les types d'expression **single_valued_expression** et des valeurs individuelles qui se trouvent dans la liste **single_valued_list** doivent être consistantes. JPQL limite les types valides ici à des chaînes, des valeurs numériques, date, heure, heure/date, et enum. Dans JPQL, **single_valued_expression** ne peut se référer qu'à des :

- "state fields", son terme pour attributs simples. Cela exclut en particulier les attributs composants/intégrés et associations.
- expression de type d'entité.

Dans HQL, **single_valued_expression** peut désigner un bien plus large éventail de types d'expression. Les association de valeurs simples sont autorisées, ainsi que les attributs composant/intégré, bien que cette fonctionnalité dépend du niveau de soutien pour le tuple ou pour la «syntaxe de constructeur de valeur de ligne» dans la base de données sous-jacente. En outre, les HQL ne limitent pas le type de valeur en aucune façon, bien que les développeurs d'applications doivent être conscients que les différents types peuvent encourir un soutien limité basé sur le fournisseur de base de données sous-jacent. C'est en grande partie la raison des limitations JPQL

La liste des valeurs peut venir d'un certain nombre de sources. Dans **constructor_expression** et **collection_valued_input_parameter**, la liste des valeurs ne doit pas rester vide; elle doit contenir une valeur au moins.

Exemple 11.19. Exemples de prédicat

```
select p
from Payment p
```

```
where type(p) in (CreditCardPayment, WireTransferPayment)

select c
from Customer c
where c.hqAddress.state in ('TX', 'OK', 'LA', 'NM')

select c
from Customer c
where c.hqAddress.state in ?

select c
from Customer c
where c.hqAddress.state in (
    select dm.state
    from DeliveryMetadata dm
    where dm.salesTax is not null
)

// Not JPQL compliant!
select c
from Customer c
where c.name in (
    ('John','Doe'),
    ('Jane','Doe')
)

// Not JPQL compliant!
select c
from Customer c
where c.chiefExecutive in (
    select p
    from Person p
    where ...
)
```

Report a bug

11.4.16. SQL Ordering

Les résultats de la demande peuvent également être ordonnancés. La clause **ORDER BY** est utilisée pour spécifier les valeurs sélectionnées à utiliser pour ordonnancer le résultat. Les types d'expressions considérées comme valides pour la clause order-by sont les suivantes :

- state fields
- attributs composant/intégré
- expressions scalaires comme les opérations arithmétiques, les fonctions, etc.
- variable d'identification déclarée dans la clause Select pour n'importe quel type d'expression antérieure.

HQL ne prescrit pas que toutes les valeurs référencées dans la clause orde-by doivent être nommées dans la clause Select, mais ceci est requis dans JPQL. Les applications désireuses de portabilité de base de données doivent noter que toutes les bases de données ne prennent pas en charge les valeurs

de références dans la clause order-by qui ne sont pas référencées dans la clause select

Les expressions individuelles d'order-by peuvent être soit qualifiées par **ASC** (ascendant) ou **DESC** (descendant) pour indiquer la direction d'ordonnancement désirée.

Exemple 11.20. Exemple Order-by

```
// legal because p.name is implicitly part of p
select p
from Person p
order by p.name

select c.id, sum( o.total ) as t
from Order o
    inner join o.customer c
group by c.id
order by t
```

Report a bug

11.5. SERVICES HIBERNATE

11.5.1. Les services Hibernate

Les services sont des classes qui procurent à Hibernate des implémentations connectables de divers types de fonctionnalité. Plus précisément, ce sont des implémentations de certaines interfaces de contrats de service. L'interface est connue comme rôle de service; la classe d'implémentation est connue comme implémentation du service. De manière générale, les utilisateurs peuvent se raccorder sur d'autres implémentations des rôles de service standard (par substitution); ils peuvent également définir des services supplémentaires au-delà de l'ensemble de base des rôles de service (extension).

Report a bug

11.5.2. Contrats de service

La nécessité de base d'un service est d'implémenter l'interface du marqueur **`org.hibernate.service.Service`**. Hibernate l'utilise en interne pour des raisons de sécurité de base.

En option, le service peut également implémenter les interfaces **`org.hibernate.service.spi.Startable`** et **`org.hibernate.service.spi.Stoppable`** pour recevoir des notifications de démarrage ou d'arrêt. Il existe un autre service en option **`org.hibernate.service.spi.Manageable`** que marque le service comme étant gérable dans le JMX dans la mesure où l'intégration JMX est activée.

Report a bug

11.5.3. Types de dépendances de service

Les services peuvent déclarer des dépendances sur d'autres services par l'une des approches suivantes :

`@org.hibernate.service.spi.InjectService`

Toute méthode de classe d'implémentation de service qui accepte un seul paramètre et qui est annotée par **`@InjectService`** est considérée comme réclamant une injection de la part d'un autre service.

Par défaut, le type du paramètre de méthode doit correspondre au rôle de service à injecter. Si le type de paramètre est différent du rôle de service, l'attribut **`serviceRole`** du **`InjectService`** devra être utilisé pour nommer explicitement le rôle.

Les services injectés sont requis par défaut, c'est à dire que le démarrage échouera si un service dépendant nommé est manquant. Si le service injecté est optionnel, l'attribut **`requis`** d' **`InjectService`** devra être déclaré **`false`** (la valeur par défaut est **`true`**).

`org.hibernate.service.spi.ServiceRegistryAwareService`

La seconde approche est une approche pull pour laquelle le service implémente l'interface de service optionnelle **`org.hibernate.service.spi.ServiceRegistryAwareService`** qui déclare une méthode **`injectServices`** unique.

En cours de démarrage, Hibernate injectera le **`org.hibernate.service.ServiceRegistry`** lui-même dans les services qui implémentent cette interface. Le service peut alors utiliser la référence **`ServiceRegistry`** pour trouver les services additionnels dont il pourrait avoir besoin.

Report a bug

11.5.4. Le ServiceRegistry

11.5.4.1. Le ServiceRegistry

L'API du service central, mis à part les services eux-même, correspond à l'interface **`org.hibernate.service.ServiceRegistry`**. Le but principal d'un registre de service est de contenir, de gérer et de donner accès aux services.

Les registres de services sont hiérarchiques. Les services d'un registre peuvent dépendre ou utiliser des services de ce même registre, ou bien de registres parents.

Utiliser **`org.hibernate.service.ServiceRegistryBuilder`** pour créer une instance **`org.hibernate.service.ServiceRegistry`**.

Exemple 11.21. Utiliser ServiceRegistryBuilder pour créer un ServiceRegistry

```
ServiceRegistryBuilder registryBuilder = new ServiceRegistryBuilder(
bootstrapServiceRegistry );
    ServiceRegistry serviceRegistry =
registryBuilder.buildServiceRegistry();
```

Report a bug

11.5.5. Services personnalisés

11.5.5.1. Services personnalisés

Une fois qu'un **`org.hibernate.service.ServiceRegistry`** est créé, il est considéré comme immuable. Les services eux-mêmes pourraient accepter une reconfiguration, mais ici, l'immuabilité signifie un ajout/remplacement des services. Et donc, un autre rôle assuré par **`org.hibernate.service.ServiceRegistryBuilder`** est de permettre de peaufiner des services qui figureront dans le **`org.hibernate.service.ServiceRegistry`** qu'il génère.

Il y a 2 façons d'informer le **`org.hibernate.service.ServiceRegistryBuilder`** à propos de services personnalisés.

- Implémenter une classe **`org.hibernate.service.spi.BasicServiceInitiator`** pour contrôler la construction sur demande de la classe du service et y ajouter le **`org.hibernate.service.ServiceRegistryBuilder`** via sa méthode **`addInitiator`**.
- Il vous suffit d'instancier la classe de service et de l'ajouter au **`org.hibernate.service.ServiceRegistryBuilder`** via sa méthode **`addService`**.

L'ajout d'une approche de service ou l'ajout d'une approche d'initiateur sont valables pour l'extension d'un registre (ajout de nouveaux rôles de service) et pour la substitution de services (remplacer les implémentations de service).

Exemple 11.22. Utiliser ServiceRegistryBuilder pour remplacer un service existant par un service personnalisé

```
   ServiceRegistryBuilder registryBuilder = new ServiceRegistryBuilder(
bootstrapServiceRegistry );
   serviceRegistryBuilder.addService( JdbcServices.class, new
FakeJdbcService() );
   ServiceRegistry serviceRegistry =
registryBuilder.buildServiceRegistry();


   public class FakeJdbcService implements JdbcServices{

       @Override
       public ConnectionProvider getConnectionProvider() {
           return null;
       }

       @Override
       public Dialect getDialect() {
           return null;
       }

       @Override
       public SqlStatementLogger getSqlStatementLogger() {
           return null;
       }

       @Override
       public SqlExceptionHelper getSqlExceptionHelper() {
           return null;
       }

       @Override
       public ExtractedDatabaseMetaData getExtractedMetaDataSupport() {
           return null;
```

```
        }

        @Override
        public LobCreator getLobCreator(LobCreationContext
lobCreationContext) {
            return null;
        }

        @Override
        public ResultSetWrapper getResultSetWrapper() {
            return null;
        }

        @Override
        public JdbcEnvironment getJdbcEnvironment() {
            return null;
        }
    }
```

Report a bug

11.5.6. Le registre Bootstrap

11.5.6.1. Le registre Boot-strap

Le registre de bootstrap contient les services qui doivent absolument être disponibles pour que tout fonctionne. Le service principal ici est le **`ClassLoaderService`** qui en est un parfait exemple. Même la résolution des fichiers de configuration doit avoir accès aux services de chargement de classes (resource look ups). C'est le registre racine (sans parent) en conditions normales d'utilisation.

Les instances de boot-strap sont créées par la classe **`org.hibernate.service.BootstrapServiceRegistryBuilder`**.

Report a bug

11.5.6.2. Utilisation de BootstrapServiceRegistryBuilder

Exemple 11.23. Utilisation de BootstrapServiceRegistryBuilder

```
BootstrapServiceRegistry bootstrapServiceRegistry = new
BootstrapServiceRegistryBuilder()
        // pass in org.hibernate.integrator.spi.Integrator instances
which are not
        // auto-discovered (for whatever reason) but which should be
included
        .with( anExplicitIntegrator )
        // pass in a class-loader Hibernate should use to load
application classes
        .withApplicationClassLoader(
anExplicitClassLoaderForApplicationClasses )
        // pass in a class-loader Hibernate should use to load
resources
        .withResourceClassLoader( anExplicitClassLoaderForResources )
```

```
        // see BootstrapServiceRegistryBuilder for rest of available
methods
        ...
        // finally, build the bootstrap registry with all the above
options
        .build();
```

Report a bug

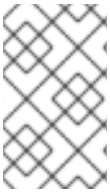
11.5.6.3. Les services BootstrapRegistry

`org.hibernate.service.classloading.spi.ClassLoaderService`

Hibernate a besoin d'interagir avec les chargeurs de classes. Cependant, la manière dont Hibernate (ou n'importe quelle bibliothèque) doit interagir avec les chargeurs de classe parents varie selon l'environnement d'exécution qui héberge l'application. Les serveurs d'applications, les conteneurs OSGi et autres systèmes de chargement de classes modulaires ont des exigences très spécifiques de chargement de classes. Ce service fournit à Hibernate une abstraction de cette complexité environnementale. Et tout aussi important, il le fait par l'intermédiaire d'un composant simple et interchangeable.

En terme d'interaction avec ClassLoader, Hibernate doit avoir les fonctionnalités suivantes :

- la capacité de localiser des classes d'application
- la capacité de localiser des classes d'intégration
- la capacité de localiser des ressources (fichiers de propriétés, fichiers xml, etc.)
- la capacité à charger **`java.util.ServiceLoader`**



NOTE

Actuellement, la capacité à charger des classes d'application et la capacité à charger des classes d'intégration sont combinées en une même capacité de "chargement de classe" pour le service. Cela risque de changer dans les versions à venir.

`org.hibernate.integrator.spi.IntegratorService`

Les applications, modules et autres avaient tous besoin de s'intégrer dans Hibernate moyennant quelque chose, généralement de la part de l'application, pour coordonner l'inscription les pièces de chaque intégration nécessaire au nom de chaque intégrateur. Ce service vise à permettre à ces intégrateurs d'être découverts et à les faire s'intégrer dans Hibernate.

Ce service se focalise sur l'aspect discovery. Il utiliser la capacité Java standard **`java.util.ServiceLoader`** fournie par **`org.hibernate.service.classloading.spi.ClassLoaderService`** pour découvrir les implémentations du contrat **`org.hibernate.integrator.spi.Integrator`**.

Les intégrateurs se contentaient de définir un fichier nommé **`/META-INF/services/org.hibernate.integrator.spi.Integrator`** et de le rendre disponible sur le chemin de classe. **`java.util.ServiceLoader`** couvre le format de ce fichier en détails, et surtout dresse une liste des classes par FQN qui implémentent le **`org.hibernate.integrator.spi.Integrator`** un par ligne.

Report a bug

11.5.7. Le registre SessionFactory

11.5.7.1. Le registre SessionFactory

Malgré qu'il soit recommandé de traiter les instances de tous les types de registres comme ciblant une **`org.hibernate.SessionFactory`** donnée, les instances de service de ce groupe appartiennent explicitement à une **`org.hibernate.SessionFactory`** unique.

La différence est une question de savoir quand elles doivent être initiées. En général, elles doivent avoir accès à la **`org.hibernate.SessionFactory`** pour pouvoir être initiées. Ce registre spécial est **`org.hibernate.service.spi.SessionFactoryServiceRegistry`**

Report a bug

11.5.7.2. Services SessionFactory

`org.hibernate.event.service.spi.EventListenerRegistry`

Description

Service pour gérer les listeners d'événements

Initiateur

`org.hibernate.event.service.internal.EventListenerServiceInitiator`

Implémentations

`org.hibernate.event.service.internal.EventListenerRegistryImpl`

Report a bug

11.5.8. Intégrateurs

11.5.8.1. Intégrateurs

Le **`org.hibernate.integrator.spi.Integrator`** a pour but de procurer un simple moyen de permettre aux développeurs de raccrocher un processus de création de SessionFactory en état de fonctionnement. L'interface **`org.hibernate.integrator.spi.Integrator`** définit 2 méthodes intéressantes: **`integrate`** permet de se joindre à un processus de création; **`disintegrate`** nous permet de raccrocher la fermeture de la SessionFactory.

NOTE

Il y a une 3ème méthode définie dans **`org.hibernate.integrator.spi.Integrator`**, une forme surchargée de **`integrate`** qui accepte un **`org.hibernate.metamodel.source.MetadataImplementor`** à la place d'une **`org.hibernate.cfg.Configuration`**. Cette forme a pour dessein d'être utilisée avec le nouveau code de méta modèle qui devra est opérationnel dans 5.0.

En plus de l'approche discovery fournie dans IntegratorService, les applications peuvent enregistrer des implémentations manuellement quand elles créent le BootstrapServiceRegistry.

Report a bug

11.5.8.2. Cas d'utilisation d'Integrator

Les cas principaux d'intégration d'un **`org.hibernate.integrator.spi.Integrator`** actuellement consistent à enregistrer des listeners d'événements et de fournir des services (voir **`org.hibernate.integrator.spi.ServiceContributingIntegrator`**). Dans 5.0, nous espérons étendre ceci afin de permettre de modifier les méta modèles qui décrivent le mappage entre les modèles relationnels et les objets.

Exemple 11.24. Enregistrement des listeners d'événements

```
public class MyIntegrator implements
org.hibernate.integrator.spi.Integrator {

    public void integrate(
            Configuration configuration,
            SessionFactoryImplementor sessionFactory,
            SessionFactoryServiceRegistry serviceRegistry) {
        // As you might expect, an EventListenerRegistry is the thing
with which event listeners are registered  It is a
        // service so we look it up using the service registry
        final EventListenerRegistry eventListenerRegistry =
serviceRegistry.getService( EventListenerRegistry.class );

        // If you wish to have custom determination and handling of
"duplicate" listeners, you would have to add an
        // implementation of the
org.hibernate.event.service.spi.DuplicationStrategy contract like this
        eventListenerRegistry.addDuplicationStrategy(
myDuplicationStrategy );

        // EventListenerRegistry defines 3 ways to register listeners:
        //     1) This form overrides any existing registrations with
        eventListenerRegistry.setListeners( EventType.AUTO_FLUSH,
myCompleteSetOfListeners );
        //     2) This form adds the specified listener(s) to the
beginning of the listener chain
        eventListenerRegistry.prependListeners( EventType.AUTO_FLUSH,
myListenersToBeCalledFirst );
  //     3) This form adds the specified listener(s) to the end of the
listener chain
        eventListenerRegistry.appendListeners( EventType.AUTO_FLUSH,
myListenersToBeCalledLast );
    }
}
```

Report a bug

11.6. VALIDATION D'UN BEAN

11.6.1. Validation Bean

Bean Validation, ou JavaBeans Validation, est un modèle de validation des données dans des objets Java. Le modèle utilise les contraintes d'annotations prédéfinies et personnalisées afin d'assurer l'intégrité des données d'application. La spécification est documentée ici http://jcp.org/en/jsr/detail?id=303.

Hibernate Validator est l'implémentation JBoss EAP 6 de Bean Validation. C'est également l'implémentation de référence du JSR.

JBoss EAP 6 est conforme à 100% avec JSR 303 - Bean Validaiton. Hibernate Validator fournit également quelques fonctionnalités supplémentaires à la spécification.

Pour débuter avec Bean Validation, consulter **`bean-validation`** quickstart example: Section 1.4.2.1, « Accès aux Quickstarts ».

Report a bug

11.6.2. Hibernate Validator

Hibernate Validator est l'implémentation de référence de JSR 303 - Bean Validation.

Bean Validation donne aux utilisateurs un modèle de validation des données d'objets Java. Pour plus d'informations, voir Section 11.6.1, « Validation Bean » et Section 11.6.3.1, « Les contraintes de validation ».

Report a bug

11.6.3. Contraintes de validation

11.6.3.1. Les contraintes de validation

Les contraintes de validation sont des règles qui s'appliquent à un élément Java, comme un champ, une propriété ou un bean. Une contrainte aura sans doute un groupe d'attributs utilisés pour définir ses limites. Il existe des contraintes prédéterminées, et des contraintes personnalisées peuvent être créées. Chaque contrainte est exprimée sous forme d'annotation.

Les contraintes de validation intégrées d'Hibernate Validator sont listées ici : Section 11.6.3.4, « Contraintes d'Hibernate Validator »

Pour plus d'informations, voir Section 11.6.2, « Hibernate Validator » et Section 11.6.1, « Validation Bean ».

Report a bug

11.6.3.2. Créer une annotation de contrainte dans JBoss Developer Studio

Résumé

Cette tâche couvre le processus de création d'une annotation de contrainte dans JBoss Developer Studio, à utiliser dans une application Java.

Prérequis

- Section 1.3.1.4, « Démarrer JBoss Developer Studio »

Procédure 11.5. Créer une annotation de contrainte

1. Ouvrir un projet Java dans JBoss Developer Studio
2. **Créer un ensemble de données**
   Une annotation de contrainte requiert un ensemble de données qui définissent les valeurs qui conviennent.
   a. Cliquer à droite sur le dossier racine du projet dans le panneau **`Project Explorer`**.
   b. Sélectionner **Nouveau** → **Enum**.
   c. Configurer les éléments suivants :
      - **`Package :`**
      - **`Nom :`**
   d. Cliquer sur le bouton **`Ajouter...`** pour ajouter des interfaces selon les besoins.
   e. Cliquer sur **`Terminé`** pour créer le fichier.
   f. Ajouter un ensemble de valeurs à l'ensemble de données et cliquer sur **Sauvegarde**.

   Exemple 11.25. Exemple d'ensemble de données

   ```
   package com.example;

   public enum CaseMode {
       UPPER,
       LOWER;
   }
   ```

3. **Créer le fichier Annotation**
   Créer une nouvelle classe Java. Pour les détails, consulter Section 11.6.3.3, « Créer une nouvelle classe Java dans JBoss Developer Studio ».
4. Configurez l'annotation de la contrainte et cliquer sur **Sauvegarde**.

   Exemple 11.26. Exemple de fichier d'annotation de contrainte

   ```
   package com.mycompany;

   import static java.lang.annotation.ElementType.*;
   import static java.lang.annotation.RetentionPolicy.*;

   import java.lang.annotation.Documented;
   import java.lang.annotation.Retention;
   import java.lang.annotation.Target;

   import javax.validation.Constraint;
   import javax.validation.Payload;

   @Target( { METHOD, FIELD, ANNOTATION_TYPE })
   ```

```
@Retention(RUNTIME)
@Constraint(validatedBy = CheckCaseValidator.class)
@Documented
public @interface CheckCase {

    String message() default "
{com.mycompany.constraints.checkcase}";

    Class<?>[] groups() default {};

    Class<? extends Payload>[] payload() default {};

    CaseMode value();

}
```

Résultat

Une annotation de contrainte personnalisée possédant un ensemble de valeurs possibles a été créé, prêt à l'utilisation dans le projet Java.

Report a bug

11.6.3.3. Créer une nouvelle classe Java dans JBoss Developer Studio

Prérequis

- Section 1.3.1.4, « Démarrer JBoss Developer Studio »

Résumé

Ce sujet couvre le processus de création d'une classe Java dans un projet Java qui utilise JBoss Developer Studio.

Procédure 11.6. Créer une nouvelle classe Java

1. Cliquer à droite sur le dossier racine du projet dans le panneau **`Project Explorer`**.
2. Sélectionner **Nouveau** → **Classe**.
3. Configurer les éléments suivants :
   - **`Package`** :
   - **`Nom`** :
4. **Option: ajouter une interface**
   a. Cliquer sur **`Ajouter...`**
   b. Rechercher le nom de l'interface
   c. Sélectionner l'interface qui convient.
   d. Répéter les étapes 2 et 3 pour chaque interface requise.

e. Cliquer sur **Ajouter**.

5. Cliquer sur **Terminer** pour créer le fichier.

Résultat

Une nouvelle Classe Java a maintenant été créée dans le projet, prête à la configuration.

Report a bug

11.6.3.4. Contraintes d'Hibernate Validator

Tableau 11.11. Contraintes intégrées

Annotation	+	Vérification du runtime	Impact des métadonnées Hibernate
@Length(min=, max=)	propriété (String)	Vérifier si la longueur de la chaîne de caractères correspond à la plage.	La colonne sera définie à la longueur maximum.
@Max(value=)	propriété (numérique ou représentation par chaîne d'un numérique)	Vérifiez si la valeur est inférieure ou égale à la valeur maximum.	Ajouter un contrôle sur la colonne.
@Min(value=)	propriété (numérique ou représentation par chaîne d'un numérique)	Vérifier si la valeur est supérieure ou égale à la valeur minimale.	Ajouter un contrôle sur la colonne.
@NotNull	propriété	Vérifier si la valeur est non nulle.	Colonne(s) non nulles.
@NotEmpty	propriété	Vérifier si la chaîne est non nulle ou vide. Vérifier si la connexion est non nulle ou vide.	Colonne(s) non nulles (pour Chaîne).
@Past	propriété (date ou calendrier)	Vérifier si la date est dans le passé.	Ajouter un contrôle sur la colonne.
@Future	propriété (date ou calendrier)	Vérifier si la date est dans le futur.	Aucun(e).
@Pattern(regex="regexp", flag=) or @Patterns({@Pattern(...)})	propriété (String)	Vérifier si la propriété correspond à une expression standard avec un indicateur de correspondance (voir **java.util.regex.Pattern**).	Aucun(e).

Annotation	+	Vérification du runtime	Impact des métadonnées Hibernate
@Range(min=, max=)	propriété (numérique ou représentation par chaîne d'un numérique)	Vérifier si la valeur est comprise entre la valeur minimum et la valeur maximum (comprise).	Ajouter un contrôle sur la colonne.
@Size(min=, max=)	propriété (tableau, collection, mappe)	Vérifier si la taille de l'élément est comprise entre la valeur minimum et la valeur maximum (comprise).	Aucun(e).
@AssertFalse	propriété	Vérifier si la méthode évalue à false (utile pour les contraintes en code et non pas sous forme d'annotations).	Aucun(e).
@AssertTrue	propriété	Vérifier si la méthode évalue à true (utile pour les contraintes en code et non pas sous forme d'annotations).	Aucun(e).
@Valid	propriété (objet)	Procède à une validation récursive de l'objet associé. Si l'objet correspond à une collection ou à un tableau, les éléments seront validés de façon récursive. Si l'objet est une mappe, les éléments correspondant à la valeur seront validés de façon récursive.	Aucun(e).
@Email	propriété (String)	Vérifier si la chaîne de caractères est bien conforme à la spécification de l'adresse email.	Aucun(e).
@CreditCardNumber	propriété (String)	Vérifier si la chaîne de caractères correspond à un numéro de carte de crédit formaté (dérivatif de l'algorithme Luhn).	Aucun(e).

Annotation	+	Vérification du runtime	Impact des métadonnées Hibernate
@Digits(integerDigits=1)	propriété (numérique ou représentation par chaîne d'un numérique)	Vérifier si la propriété est un numéro qui comprend un maximum de **`integerDigits`** chiffres et **`fractionalDigits`** chiffres sous forme de fraction.	Définit la précision et l'échelle de la colonne.
@EAN	propriété (String)	Vérifie si la chaîne correspond à un code UPC-A ou EAN formaté comme il faut.	Aucun(e).

Report a bug

11.6.4. Configuration

11.6.4.1. Exemple de fichier de configuration de validation

Exemple 11.27. validation.xml

```
<validation-config
xmlns="http://jboss.org/xml/ns/javax/validation/configuration"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://jboss.org/xml/ns/javax/validation/configurati
on">

    <default-provider>
        org.hibernate.validator.HibernateValidator
    </default-provider>
    <message-interpolator>

org.hibernate.validator.messageinterpolation.ResourceBundleMessageInterp
olator
    </message-interpolator>
    <constraint-validator-factory>
        org.hibernate.validator.engine.ConstraintValidatorFactoryImpl
    </constraint-validator-factory>

    <constraint-mapping>
        /constraints-example.xml
    </constraint-mapping>

    <property name="prop1">value1</property>
    <property name="prop2">value2</property>
</validation-config>
```

Report a bug

11.7. ENVERS

11.7.1. Hibernate Envers

Hibernate Envers est un système d'audit et de gestion des versions, offrant un moyen de suivre les changements historiques à des classes persistantes de JBoss EAP 6. Des tableaux de vérification sont créées pour les entités annotées avec **`@Audited`**, et ils stockent l'historique des modifications apportées à l'entité. Les données peuvent ensuite être récupérées et interrogées.

Envers permet aux développeurs de :

- vérifier tous les mappages définis par la spécification JPA,
- vérifier tous les mappages qui étendent la spécification JPA,
- vérifier toules les entités mappées ou qui utilisent l'API Hibernate natif
- journaliser des données pour chaque révision par l'intermédiaire d'une entité de révision, et
- interroger les données historiques.

Report a bug

11.7.2. Audit de classes persistantes

L'auditing de classes persistantes est fait par l'intermédiaire d'Hibernate Envers dans JBoss EAP 6 et de l'annotation **`@Audited`** . Quand l'annotation s'applique à une classe, un tableau est créé, et ce tableau stocke l'historique de révision de l'entité.

À chaque fois qu'il y a un changement de classe, une entrée est ajoutée au tableau d'audit. L'entrée contient les changements apportés à la classe, et reçoit un numéro de révision. Cela signifie que les changements peuvent être annulés, ou que les révisions précédentes peuvent être consultées.

Report a bug

11.7.3. Stratégies d'auditing

11.7.3.1. Stratégies d'auditing

Les stratégies d'auditing définissent comment l'information d'audit est persistée, interrogée et stockée. Il existe actuellement deux stratégies d'audit disponibles dans Hibernate Envers :

Stratégie d'audit par défaut

Cette stratégie persiste les données d'audit avec la révision de départ. Pour chaque ligne insérée, mise à jour ou effacée dans un tableau audité, une ou plusieurs lignes seront insérées dans les tableaux d'audit, avec la révision de départ de sa validité.

Les lignes des tableaux d'audit ne sont jamais mises à jour suite à une insertion. Les demandes d'informations d'audit utilisent des sous-requêtes pour sélectionner les lignes qui s'appliquent aux tableaux d'audit, et qui sont lentes et difficiles à indexer.

Stratégie d'audit de validité

Cette stratégie stocke la révision de départ, ainsi que la révision de fin de l'information d'audit. Pour chaque rangée insérée, mise à jour ou effacée dans un tableau audité, un ou plusieurs rangées seront insérées dans les tableaux d'audit, avec la révision de départ de sa validité.

En même temps, le champ de révision de fin des lignes d'audit précédentes (si disponible) est défini pour cette révision. Les demandes d'informations d'audit peuvent ensuite utiliser *entre révision de départ ou de fin*, à la place des sous-requêtes. Cela signifie que persister les informations d'audit est un peu plus lent à cause des mises à jour supplémentaires, mais la récupération d'informations d'audit est beaucoup plus rapide.

Cela peut également être amélioré en ajoutant des indices supplémentaires.

Pour obtenir plus d'informations sur l'auditing, consulter Section 11.7.2, « Audit de classes persistantes ». Pour définir la stratégie d'auditing de l'application, voir : Section 11.7.3.2, « Définir la stratégie d'auditing ».

Report a bug

11.7.3.2. Définir la stratégie d'auditing

Résumé

Il y a deux stratégies d'auditing prises en charge par JBoss EAP 6 : la stratégie d'audit de validité ou la stratégie d'audit par défaut. Cette tâche couvre les étapes nécessaires requises pour définir la stratégie d'auditing d'une application.

Procédure 11.7. Définir une stratégie d'auditing

- Configurer la propriété **`org.hibernate.envers.audit_strategy`** qui se trouve dans le ficher **`persistence.xml`** de l'application. Si la propriété est définie dans le fichier **`persistence.xml`**, alors la stratégie d'audit par défaut sera utilisée.

  Exemple 11.28. Définir la stratégie d'auditing par défaut

  ```
  <property name="org.hibernate.envers.audit_strategy"
  value="org.hibernate.envers.strategy.DefaultAuditStrategy"/>
  ```

  Exemple 11.29. Définir la stratégie d'auditing de validité

  ```
  <property name="org.hibernate.envers.audit_strategy"
  value="org.hibernate.envers.strategy.ValidityAuditStrategy"/>
  ```

Report a bug

11.7.4. Introduction à l'auditing d'entités

11.7.4.1. Ajouter une support d'auditing à une entité JPA

JBoss EAP 6 utilise l'auditing d'entités, par l'intermédiaire de Section 11.7.1, « Hibernate Envers », pour suivre les changements historiques d'une classe persistante. Cette rubrique couvre l'ajout d'un support d'auditing pour une entité JPA.

Procédure 11.8. Ajouter une support d'auditing à une entité JPA

1. Configurer les paramètres d'auditing disponible qui conviennent au déploiement : Section 11.7.5.1, « Configurer les paramètres Envers ».
2. Ouvrir l'entité JPA à auditer.
3. Importer l'interface **`org.hibernate.envers.Audited`**.
4. Appliquer l'annotation **`@Audited`** à chaque champ ou propriété à auditer, ou l'appliquer une seule fois à toute la classe.

Exemple 11.30. Audit de deux champs

```
import org.hibernate.envers.Audited;

import javax.persistence.Entity;
import javax.persistence.Id;
import javax.persistence.GeneratedValue;
import javax.persistence.Column;

@Entity
public class Person {
    @Id
    @GeneratedValue
    private int id;

    @Audited
    private String name;

    private String surname;

    @ManyToOne
    @Audited
    private Address address;

    // add getters, setters, constructors, equals and hashCode
here
}
```

Exemple 11.31. Audit d'une classe complète

```
import org.hibernate.envers.Audited;

import javax.persistence.Entity;
import javax.persistence.Id;
import javax.persistence.GeneratedValue;
import javax.persistence.Column;

@Entity
```

```
@Audited
public class Person {
    @Id
    @GeneratedValue
    private int id;

    private String name;

    private String surname;

    @ManyToOne
    private Address address;

    // add getters, setters, constructors, equals and hashCode
here
}
```

Résultat

L'entité JPA a été configurée pour l'auditing. Un tableau intitulé ***Entity*_AUD** sera créé pour stocker les changements historiques.

Report a bug

11.7.5. Configuration

11.7.5.1. Configurer les paramètres Envers

JBoss EAP 6 utilise l'auditing d'entités, par l'intermédiaire d'Hibernate Envers, pour suivre les changements historiques d'une classe persistante. Cette rubrique couvre la configuration des paramètres Envers disponibles.

Procédure 11.9. Configurer les paramètres Envers

1. Ouvrir le fichier **`persistence.xml`** de l'application.
2. Ajouter, supprimer ou configurer les propriétés Envers selon les besoins. Pour obtenir une liste complète des propriétés disponibles, consulter Section 11.7.5.4, « Propriétés de configuration Envers ».

Exemple 11.32. Exemples de paramètres Envers

```
<persistence-unit name="mypc">
  <description>Persistence Unit.</description>
  <jta-data-source>java:jboss/datasources/ExampleDS</jta-data-source>
  <shared-cache-mode>ENABLE_SELECTIVE</shared-cache-mode>
  <properties>
    <property name="hibernate.hbm2ddl.auto" value="create-drop" />
    <property name="hibernate.show_sql" value="true" />
    <property name="hibernate.cache.use_second_level_cache" value="true"
/>
    <property name="hibernate.cache.use_query_cache" value="true" />
    <property name="hibernate.generate_statistics" value="true" />
    <property name="org.hibernate.envers.versionsTableSuffix" value="_V"
```

```
/>
    <property name="org.hibernate.envers.revisionFieldName"
value="ver_rev" />
  </properties>
</persistence-unit>
```

Résultat

L'auditing a été configuré pour toutes les entités JPA de l'application.

Report a bug

11.7.5.2. Activer ou désactiver l'auditing en cours d'exécution

Résumé

Cette tâche couvre les étapes de configuration requises pour activer/désactiver l'auditing de version d'entité en cours d'exécution.

Procédure 11.10. Activer/désactiver l'auditing

1. Sous-classe la classe **`AuditEventListener`**.
2. Remplace les méthodes suivantes appelées sur les événements Hibernate :
   - onPostInsert
   - onPostUpdate
   - onPostDelete
   - onPreUpdateCollection
   - onPreRemoveCollection
   - onPostRecreateCollection
3. Spécifie la sous-classe comme listener des événements.
4. Détermine si le changement doit être vérifié.
5. Passe l'appel à la sur-classe si le changement doit être vérifié.

Report a bug

11.7.5.3. Configurer l'auditing conditionnel.

Résumé

Hibernate Envers persiste les données d'auditing en réaction à certains événements, en utilisant une série de listeners d'événements. Ces listeners sont enregistrés automatiquement si le jar Envers est sur le chemin de classe. Cette tâche couvre les étapes requises pour mettre en place l'auditing conditionnel, en remplaçant certains listeners d'événements Envers.

Procédure 11.11. Implémentation de l'Auditing conditionnel

1. Définir la propriété Hibernate **`hibernate.listeners.envers.autoRegister`** à false dans le fichier **`persistence.xml`**.

2. Sous-classer chaque listener d'événement à remplacer. Mettez la logique d'auditing conditionnel dans la sous-classe, et appeler la super méthode si on doit procéder à l'auditing.

3. Créer une implémentation personnalisée de **`org.hibernate.integrator.spi.Integrator`**, semblable à **`org.hibernate.envers.event.EnversIntegrator`**. Utiliser les sous-classes de listeners d'événements créées à la deuxième étape, à la place des classes par défaut.

4. Ajouter un fichier **`META-INF/services/org.hibernate.integrator.spi.Integrator`** au jar. Ce fichier doit contenir le nom complet de la classe qui implémente d'interface.

Résultat

L'auditing conditionnel alors est configuré, remplaçant ainsi les listeners d'événements Envers par défaut.

Report a bug

11.7.5.4. Propriétés de configuration Envers

Tableau 11.12. Paramètres de configuration du Versioning de données d'entité

Nom de propriété	Valeur par défaut	Description
org.hibernate.envers.audit_table_prefix		String attaché au nom d'une entité auditée, pour créer le nom de l'entité qui contiendra l'audit en formation.
org.hibernate.envers.audit_table_suffix	_AUD	String attaché au nom d'une entité auditée, pour créer le nom de l'entité qui contiendra l'audit en formation. Par exemple, si une entité ayant comme nom de tableau **`Person`** est auditée, Envers créera un tableau nommé **`Person_AUD`** pour stocker les données historiques.
org.hibernate.envers.revision_field_name	REV	Le nom du champ qui contient le numéro de révision dans l'entité d'audit.
org.hibernate.envers.revision_type_field_name	REVTYPE	Le nom du champ de l'entité d'audit qui contient le type de révision. Les types actuels de révision possibles sont : **`add`**, **`mod`** et **`del`**.

Nom de propriété	Valeur par défaut	Description
org.hibernate.envers.revision_on_collection_change	true	Cette propriété indique si une révision doit être créée si un champ relationnel qui n'appartient à personne change. Il peut s'agir d'une collection d'une relation one-to-many, ou bien du champ qui utilise l'attribut `mappedBy` dans une relation one-to-one.
org.hibernate.envers.do_not_audit_optimistic_locking_field	true	Si true, les propriétés utilisées pour le verrouillage optimiste (annoté par `@Version`) sera exclus automatiquement de l'audit.
org.hibernate.envers.store_data_at_delete	false	Cette propriété définit si oui ou non les données d'entité doivent être stockées dans la révision lorsque l'entité est supprimée, au lieu de l'ID uniquement, avec toutes les autres propriétés marquées comme null. Ce n'est pas généralement nécessaire, car les données sont présentes dans l'avant dernière révision. Parfois, il est plus facile et plus efficace d'y accéder dans la dernière révision. Cependant, cela signifie que les données de l'entité contenues avant suppression apparaissent deux fois.
org.hibernate.envers.default_schema	null (comme dans les tableaux normaux)	Le nom de schéma par défaut utilisé pour les tableaux d'audit. Peut être substitué à l'aide de l'annotation `@AuditTable(schema="...")`. Si absent, le schéma sera le même que le schéma des tableaux normaux.
org.hibernate.envers.default_catalog	null (comme dans les tableaux normaux)	Le nom de catalogue par défaut qui doit être utilisé dans les tableaux d'audit. Peut être substitué par l'annotation `@AuditTable(catalog="...")`. Si non présent, le catalogue sera le même que le catalogue des tableaux normaux.

Nom de propriété	Valeur par défaut	Description
org.hibernate.envers.audit_strategy	org.hibernate.envers.strategy.DefaultAuditStrategy	Cette propriété définit la stratégie d'auditing qui doit être utilisée lors de la persistance des données d'audit. Par défaut, seule la révision où une entité a été modifiée est stockée. Alternativement, **`org.hibernate.envers.strategy.ValidityAuditStrategy`** stocke la révision du départ et révision de la fin. Ceux-ci définissent ensemble quand une ligne d'auditing est valide.
org.hibernate.envers.audit_strategy_validity_end_rev_field_name	REVEND	Le nom de la colonne qui contiendra le dernier numéro de révision dans les entités d'auditing. Cette propriété n'est valide que si la stratégie d'auditing de validité est utilisée.
org.hibernate.envers.audit_strategy_validity_store_revend_timestamp	false	Cette propriété définit si l'horodatage du dernier numéro de révision des dernières données valides doit être conservé en plus de la dernière révision elle-même. Ceci est utile pour pouvoir purger les archives d'audit sur une base de données relationnelle en utilisant le partitionnement de la table. Le partitionnement exige une colonne qui existe dans la table. Cette propriété n'est évaluée que si la **`ValidityAuditStrategy`** est utilisée
org.hibernate.envers.audit_strategy_validity_revend_timestamp_field_name	REVEND_TSTMP	Nom de la colonne d'horodatage de la dernière révision au moment où les données étaient encore valides. Utilisé uniquement si **`ValidityAuditStrategy`** est utilisé, et si **`org.hibernate.envers.audit_strategy_validity_store_revend_timestamp`** évalue sur true.

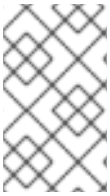
Report a bug

11.7.6. Recherches

11.7.6.1. Suppression de l'information d'auditing

Résumé

Hibernate Envers fournit une fonctionnalité qui permet d'extraire des informations d'audit par des requêtes. Cette section vous donne des exemples de telles requêtes.



NOTE

Les requêtes sur données auditées seront, dans la plupart des cas, bien plus lentes que les requêtes correspondantes sur données **live**, car elles impliquent des sous-sélections en corrélation.

Exemple 11.33. Chercher des entités d'une classe pour une révision donnée

Le point d'entrée de ce type de recherche est :

```
AuditQuery query = getAuditReader()
    .createQuery()
    .forEntitiesAtRevision(MyEntity.class, revisionNumber);
```

Des contraintes peuvent alors être spécifiées, par la classe de fabrique **AuditEntity**. La recherche ci-dessous ne sélectionne que des entités dont la propriété **nom** est égale à **John**:

```
query.add(AuditEntity.property("name").eq("John"));
```

Les demandes ci-dessous ne sélectionnent que des entités liées à une entité donnée :

```
query.add(AuditEntity.property("address").eq(relatedEntityInstance));
// or
query.add(AuditEntity.relatedId("address").eq(relatedEntityId));
```

Les résultats peuvent alors être classés, limités, et avoir des agrégations ou des projections (sauf en groupings) définis. L'exemple ci-dessous correspond à une recherche complète.

```
List personsAtAddress = getAuditReader().createQuery()
    .forEntitiesAtRevision(Person.class, 12)
    .addOrder(AuditEntity.property("surname").desc())
    .add(AuditEntity.relatedId("address").eq(addressId))
    .setFirstResult(4)
    .setMaxResults(2)
    .getResultList();
```

Exemple 11.34. Chercher les révisions de demandes pour lesquelles les entités d'une classe donnée ont changé

Le point d'entrée de ce type de recherche est :

```
AuditQuery query = getAuditReader().createQuery()
    .forRevisionsOfEntity(MyEntity.class, false, true);
```

Des contraintes peuvent être ajoutées à cette recherche de la même façon que dans l'exemple précédent. Il y a d'autres possibilités pour cette recherche :

`AuditEntity.revisionNumber()`

Spécifie les contraintes, les projections et l'ordre en considération desquels l'entité auditée a été modifiée dans le numéro de révision.

`AuditEntity.revisionProperty(propertyName)`

Spécifier les contraintes, les projections et l'ordre de l'entité de révision sur une propriété , correspondants à la révision dans laquelle l'entité auditée a été modifiée.

`AuditEntity.revisionType()`

Fournit des accès au type de révision (ADD, MOD, DEL).

Les résultats de la recherche peuvent alors être ajustées selon les besoins. La recherche ci-dessous sélectionne le plus petit nombre de révision au cours desquelles l'entité de la classe de **`MyEntity`**, ayant pour ID **`entityId`** a changé, après le numéro de révision `42` :

```
Number revision = (Number) getAuditReader().createQuery()
    .forRevisionsOfEntity(MyEntity.class, false, true)
    .setProjection(AuditEntity.revisionNumber().min())
    .add(AuditEntity.id().eq(entityId))
    .add(AuditEntity.revisionNumber().gt(42))
    .getSingleResult();
```

Les demandes de révision peuvent aussi minimiser/maximiser une propriété. La recherche ci-dessous sélectionne la révision au cours de laquelle la valeur de **`actualDate`** d'une entité donnée est supérieure à une valeur donnée, mais aussi petite que possible :

```
Number revision = (Number) getAuditReader().createQuery()
    .forRevisionsOfEntity(MyEntity.class, false, true)
    // We are only interested in the first revision
    .setProjection(AuditEntity.revisionNumber().min())
    .add(AuditEntity.property("actualDate").minimize()
        .add(AuditEntity.property("actualDate").ge(givenDate))
        .add(AuditEntity.id().eq(givenEntityId)))
    .getSingleResult();
```

Les méthodes **`minimize()`** et **`maximize()`** renvoient un critère, auquel des contraintes peuvent être ajoutées, et qui doit être respecté par les entités avec des propriétés maximisées/minimisées.

Il y a deux paramètres booléens qui ont été passés quand on crée une recherche

`selectEntitiesOnly`

Ce paramètre n'est valide que lorsqu'une projection explicite n'est pas définie.

Si true, le résultat de la recherche correspondra à une liste d'entités qui ont changé lors de révisions satisfaisant les contraintes spécifiées.

Si false, le résultat correspondra à une liste de trois tableaux d'éléments. Le premier élément correspondra à l'instance d'entité modifiée. Le second correspondra à une entité qui contient les données de révision. Si aucune entité personnalisée n'est utilisée, alors on aura une instance de **`DefaultRevisionEntity`**. Le troisième tableau d'éléments correspondra au type de révision (ADD, MOD, DEL).

`selectDeletedEntities`

Ce paramètre indique si les révisions dans lesquelles les entités ont été supprimées doivent être incluses dans les résultats. Si true, les entités auront le type de révision **`DEL`**, et tous les champs, à part l'id, auront pour valeur **`null`**.

Exemple 11.35. Chercher les révisions d'une entité qui ont pu modifier une propriété donnée

La recherche ci-dessous renverra toutes les révisions de **`MyEntity`** pour une id donnée, quand la propriété **`actualDate`** a été modifiée.

```
AuditQuery query = getAuditReader().createQuery()
  .forRevisionsOfEntity(MyEntity.class, false, true)
  .add(AuditEntity.id().eq(id));
  .add(AuditEntity.property("actualDate").hasChanged())
```

La condition **`hasChanged`** peut être combinée à des critères supplémentaires. La recherche ci-dessous renvoie une coupe horizontale de **`MyEntity`** au moment où le *revisionNumber* est créé. Ce sera limité aux révisions qui ont modifié **`prop1`**, et non pas **`prop2`**.

```
AuditQuery query = getAuditReader().createQuery()
  .forEntitiesAtRevision(MyEntity.class, revisionNumber)
  .add(AuditEntity.property("prop1").hasChanged())
  .add(AuditEntity.property("prop2").hasNotChanged());
```

Le jeu de résultats contiendra également des révisions avec des nombres inférieurs au *revisionNumber*. Cela signifie que cette recherche ne peut être interprétée comme « Renvoyer toutes les **`MyEntities`** modifiées dans le *revisionNumber* avec **`prop1`** modifié et **`prop2`** intact. »

Le recherche ci-dessous montre comment ce résultat peut être retourné, par l'intermédiaire de la recherche **`forEntitiesModifiedAtRevision`** :

```
AuditQuery query = getAuditReader().createQuery()
  .forEntitiesModifiedAtRevision(MyEntity.class, revisionNumber)
  .add(AuditEntity.property("prop1").hasChanged())
  .add(AuditEntity.property("prop2").hasNotChanged());
```

Exemple 11.36. Recherche d'entités modifiées dans une révision donnée

L'exemple ci-dessous montre la recherche de base d'entités modifiées pour une révision donnée. Cela permet aux noms d'entités et à leurs classes Java correspondantes d'être modifiées dans une révision spéciale que l'on souhaite extraire :

```
Set<Pair<String, Class>> modifiedEntityTypes = getAuditReader()

.getCrossTypeRevisionChangesReader().findEntityTypes(revisionNumber);
```

Il y a un certain nombre de recherches accessibles de **`org.hibernate.envers.CrossTypeRevisionChangesReader`**:

`List<Object> findEntities(Number)`

Retourne des instantanés de toutes les entités d'auditing changées (ajoutées, mises à jour et supprimées) dans une révision donnée. Exécute des requêtes SQL **n + 1**, où **n** est un nombre de classes d'entités différentes modifiées dans la révision spécifiée.

`List<Object> findEntities(Number, RevisionType)`

Retourne des instantanés de toutes les entités d'auditing changées (ajoutées, mises à jour et supprimées) dans une révision donnée filtrée par type de modification. Exécute des requêtes SQL **n + 1**, où **n** est un nombre de classes d'entités différentes modifiées dans la révision spécifiée.

`Map<RevisionType, List<Object>> findEntitiesGroupByRevisionType(Number)`

Retourne une carte contenant les listes des instantanés d'entité regroupés par opération de modification (ajout, mise à jour et suppression). Exécute des requêtes SQL **3n + 1**, où **n** est un nombre de classes d'entités différentes modifiées au cours de la révision spécifiée.

Report a bug

11.8. RÉGLAGE DE LA PERFORMANCE

11.8.1. Algorithmes de chargement de lots alternatifs

Hibernate permet de charger les données d'associations à l'aide de l'une des quatre stratégies de récupération : joindre (join), sélectionnez (select), sous-sélectionner (subselect) et par lots (batch). En dehors de ces quatre stratégies, le chargement par lots permet des plus grands gains de performance car c'est une stratégie d'optimisation pour l'extraction sélective. Dans cette stratégie, Hibernate récupère un lot d'instances d'entités ou de collections dans une instruction SELECT unique en spécifiant une liste de clés primaires ou étrangères. L'extraction de lot est une optimisation de la stratégie de récupération sélective différée.

Il existe deux manières de configurer l'extraction par batch: Niveau Par classe ou Niveau Par collection.

- Niveau Par classe

  Lors du chargement de données sur un niveau par classe, Hibernate, requiert la taille de lot de l'association à pré-charger lorsqu'il est interrogé. Par exemple, imaginons que lors de l'exécution, vous ayez 30 instances d'un objet **`voiture`** chargées dans la session. Chaque objet **`voiture`** appartient à un objet **`propriétaire`**. Si vous deviez parcourir tous les objets **`voiture`** et appeler leurs propriétaires, par un chargement **`différé`** (lazy loading), Hibernate émettra 30 instructions select - une pour chaque propriétaire. Il s'agit d'un goulot d'étranglement de performance.

  À la place, vous pouvez dire à Hibernate de charger à l'avance le prochain lot de propriétaires avant qu'ils aient été interrogés par une requête. Quand un objet **`owner`** (propriétaire) est interrogé, Hibernate interrogera ces objets à plusieurs reprises dans le même énoncé SELECT.

  Le nombre d'objets **`owner`** (propriétaire) à interroger à l'avance dépend du paramètre ***`batch-size`*** spécifié en cours de configuration :

  ```
  <class name="owner" batch-size="10"></class>
  ```

Cela indique à Hibernate d'interroger au moins 10 objets **`owner`** au cas où ils seraient nécessaires dans un avenir proche. Lorsqu'un utilisateur interroge le propriétaire **`owner`** de **`car A`**, le propriétaire **`owner`** de **`car B`** peut déjà avoir été chargé dans un lot de chargement. Lorsque l'utilisateur a besoin du propriétaire **`owner`** de **`car B`**, au lieu d'aller à la base de données (et émettre une instruction SELECT), la valeur peut être récupérée de la session en cours.

En plus du paramètre **`batch-size`**, Hibernate 4.2.0 a introduit un nouvel élément de configuration pour améliorer la performance de chargement de lots. La configuration s'appelle **`Batch Fetch Style`** et est spécifiée par le paramètre ***`hibernate.batch_fetch_style`***.

Il existe trois styles d'extraction de lots pris en charge : LEGACY, PADDED et DYNAMIC. Pour spécifier le style, utiliser **`org.hibernate.cfg.AvailableSettings#BATCH_FETCH_STYLE`**.

- LEGACY : dans le style hérité de chargement, une série de tailles de lots pré-construits basé **`ArrayHelper.getBatchSizes(int)`** sont utilisées. Les lots sont chargés à l'aide de la taille de lot de pré-construction suivante à partir du nombre d'identificateurs existants pouvant être mis en lot.

  En continuant avec l'exemple suivant, ayant une taille **`batch-size`** de 30, les tailles de lot pré-construits sont [30, 15, 10, 9, 8, 7, .., 1]. Si l'on tente de mettre en lots 29 identifiants, on obtiendra des lots de 15, 10 et 4. Il y aura 3 requêtes SQL correspondantes, chacune chargeant 15, 10 et 4 propriétaires de la base de données.

- PADDED - similaire au style de chargement de classes LEGACY. Utilise toujours des tailles de lots pré-construits, mais utilise la taille de lot supérieure et remplit les espaces réservés de l'identifiant supplémentaire.

  Tout comme dans l'exemple ci-dessus, si 30 objets propriétaires doivent être initialisés, il ne pourra y avoir qu'une demande exécutée dans la base de données.

  Cependant, si 29 objets propriétaires doivent être initialisés, Hibernate n'exécutera qu'un seul énoncé select SQL de taille de lot 30, avec l'espace supplémentaire rempli par un identifiant répété.

- Dynamic - bien que toujours conforme à la limitation de la taille des lots, ce style de chargement dynamiquement de lots construit son énoncé SQL SELECT à l'aide du nombre réel d'objets à charger.

  Par exemple, pour 30 objets propriétaires, et une taille de lot maximale de 30, un appel pour récupérer 30 objets propriétaires entraînera une instruction SQL SELECT. Un appel pour récupérer 35 se traduira en deux énoncés SQL, ayant pour taille de lot 30 et 5, respectivement. Hibernate modifiera dynamiquement le second énoncé SQL pour maintenir à 5, le nombre requis, tout en restant sous la restriction de 30 pour la taille des lots. C'est différent de la version PADDED, car le deuxième SQL ne sera pas PADDED et à la différence du style LEGACY, il n'y a pas de taille fixe pour le second énoncé SQL - le second SQL est créé dynamiquement.

  Pour une requête inférieure à 30 identifiants, ce style ne chargera de façon dynamique que le nombre d'identifiants requis.

- Niveau Par collection

Hibernate peut aussi mettre en lots des collections de chargement, en respectant la taille ou les styles des lots d'extraction suivant la liste de la section par-classe ci-dessus.

Pour inverser l'exemple utilisé dans la section précédente, considérons que vous deviez charger tous les objets **car** (voiture) appartenant à chaque objet **owner** (propriétaire). Si 10 objets propriétaire **owner** sont chargés dans la session en cours, itérer tous les propriétaires va générer 10 énoncés SELECT, un pour chaque appel de méthode à **getCars()**. Si vous activez l'extraction de lot pour la collection de voitures dans le mappage du propriétaire, Hibernate pourra chercher ces collections à l'avance, comme illustré ci-dessous.

```
<class name="Owner"><set name="cars" batch-size="5"></set></class>
```

Donc, avec une taille de lot **batch-size** égale à 5 et en utilisant le style de lot hérité, Hibernate chargera 5 collections dans deux énoncés SELECT.

Report a bug

11.8.2. Mise en cache de second niveau d'objets de référence pour les données non mutables

Hibernate met en cache automatiquement les données dans la mémoire pour des performances améliorées. Ceci est accompli par un cache en mémoire, ce qui réduit le nombre de fois où les recherches de base de données sont nécessaires, surtout pour les données qui changent rarement.

Hibernate administre deux types de caches. Le cache principal (également appelé le cache de premier niveau) est obligatoire. Ce cache est associé à la session en cours et toutes les demandes doivent passer à travers. Le cache secondaire (également appelé le cache de second niveau) est facultatif et est consulté seulement après consultation préalable du cache primaire.

Les données sont stockées dans le cache de second niveau en commençant par un désassemblement dans un tableau d'états. Ce tableau est copié complètement, et cette copie complète est mise en cache. L'inverse est fait pour la lecture du cache. Cela fonctionne bien pour les données qui ne changent pas (données mutables), mais est inefficace pour des données immuables.

La copie complète des données est une opération coûteuse en termes de vitesse de traitement et d'utilisation de la mémoire. Pour les grands ensembles de données, la vitesse de traitement et la mémoire deviennent un facteur de limitation de la performance. Hibernate vous permet de spécifier le référencement des données immuables au lieu de les copier. Au lieu de copier des ensembles de données complets, Hibernate peut maintenant stocker la référence aux données dans le cache.

Cela peut être effectué en modifiant la valeur du paramètre de configuration de **hibernate.cache.use_reference_entries** à **true**. Par défaut, **hibernate.cache.use_reference_entries** est défini à **false**.

Lorsque **hibernate.cache.use_reference_entries** a pour valeur **true**, un objet de données immuables qui n'a pas d'associations n'est pas copié dans le cache de second niveau, et seulement sa référence y sera stockée.

AVERTISSEMENT

Lorsque **hibernate.cache.use_reference_entries** a pour valeur **true**, un objet de données immuables qui possède des associations sera copié dans le cache de second niveau.

Report a bug

CHAPITRE 12. SERVICES WEB JAX-RS

12.1. JAX-RS

JAX-RS est l'API Java API des services web RESTful. Il fournit un support pour construire des services web avec REST, à l'aide d'annotations. Ces annotations simplifient le processus de mappage d'objets Java dans des ressources web. La spécification est définie dans http://www.jcp.org/en/jsr/detail?id=311.

RESTEasy est l'implémentation JBoss EAP 6 de JAX-RS. Il procure également des fonctionnalités supplémentaires de spécification.

JBoss EAP 6 est compatible avec JSR 311 - JAX-RS.

Pour démarrer avec JAX-RS et JBoss EAP 6, voir **`helloworld-rs`**, **`jax-rs-client`**, et **`kitchensink`** quickstart: Section 1.4.2.1, « Accès aux Quickstarts ».

Report a bug

12.2. RESTEASY

RESTEasy est une implémentation portable de l'API Java JAX-RS. Fournit également des fonctionnalités supplémentaires, comme un framework côté client (RESTEasy JAX-RS Client Framework) pour mapper les demandes sortantes vers les serveurs distants, ce qui permet à JAX-RS d'opérer en tant que client ou spécification côté serveur.

Report a bug

12.3. SERVICES WEB RESTFUL

Les services web RESTful sont conçus pour exposer les API sur le web. Ils sont destinés à améliorer la performance, l'adaptabilité, et la flexibilité par rapport aux services web traditionnels, tout en permettant aux clients d'accéder à des données et à des ressources par des URL prédictibles.

La spécification Java Enterprise Edition 6 des services RESTful est JAX-RS. Pour obtenir davantage d'informations sur JAX-RS, voir Section 12.1, « JAX-RS » et Section 12.2, « RESTEasy ».

Report a bug

12.4. ANNOTATIONS DÉFINIES RESTEASY

Tableau 12.1. Annotations JAX-RS/RESTEasy

Annotation	Utilisation
`ClientResponseType`	Il s'agit d'une annotation que vous pouvez ajouter à une interface de client RESTEasy qui a un type de renvoi Réponse.
`ContentEncoding`	Méta annotation qui indique un Contenet-Encoding à appliquer par l'annotation annotée.

Annotation	Utilisation
`DecorateTypes`	Doit être mis sur une classe DecoratorProcessor pour spécifier les types pris en charge.
`Decorator`	Méta annotation à mettre dans une autre annotation qui déclenche décoration.
`Form`	Peut être utilisé comme objet de valeur pour les requêtes/réponses entrantes/sortantes.
`StringParameterUnmarshallerBinder`	Méta annotation à mettre dans une autre annotation qui déclenche un StringParameterUnmarshaller à appliquer à un injecteur d'annotation basé chaîne.
`Cache`	Définit l'en-tête Cache-Control de réponse automatiquement.
`NoCache`	Définit la réponse Cache-Control à "nocache".
`ServerCached`	Indique que la réponse à cette méthode jax-rs devrait être mise en cache sur le serveur.
`ClientInterceptor`	Identifie un intercepteur en tant qu'intercepteur côté client.
`DecoderPrecedence`	Cet intercepteur est un décodeur Content_Encoding.
`EncoderPrecedence`	Cet intercepteur est un encodeur Content_Encoding.
`HeaderDecoratorPrecedence`	Les intercepteurs HeaderDecoratorPrecedence doivent toujours venir en premier car ils décorent une réponse (sur le serveur), ou une réquête sortante (sur le client) avec des en-têtes spéciaux définis utilisateur.
`RedirectPrecedence`	Doivent être mis dans un PreProcessInterceptor.
`SecurityPrecedence`	Doivent être mis dans un PreProcessInterceptor.
`ServerInterceptor`	Identifie un intercepteur en tant qu'intercepteur côté client.
`NoJackson`	Mis sur une classe, un paramètre, un champ ou une métode quand vous ne souhaitez pas déclencher un fournisseur Jackson.

Annotation	Utilisation
`ImageWriterParams`	Annotation qu'une classe de ressource peut utiliser pour passer des paramètres au IIOImageProvider.
`DoNotUseJAXBProvider`	Mettre ceci sur une classe ou sur un paramètre quand vous ne souhaitez pas utiliser le MessageBodyReader/Writer JAXB, mais que vous avez à la place un fournisseur plus spécifique que vous souhaitez utliser pour marshaler le type.
`Formatted`	Formate la sortie XNL par des indentations et des nouvelles lignes. Il s'agit d'un Decorateur JAXB.
`IgnoreMediaTypes`	Mis sur un type, une méthode, un paramètre ou un champ pour indiquer au JAXRS de ne pas utiliser de fournisseur JAXB pour une certain type de media.
`Stylesheet`	Indique un en-tête de feuille de style XML.
`Wrapped`	Mettre ceci sur une méthode ou un paramètre quand vous souhaitez marshaller ou démarshaller une collection ou un tableau d'objets JAXB.
`WrappedMap`	Mettre ceci sur une méthode ou un paramètre quand vous souhaitez marshaller ou démarshaller une mappe d'objets JAXB.
`XmlHeader`	Définit un en-tête XML de document renvoyé.
`BadgerFish`	Un JSONConfig.
`Mapped`	Un JSONConfig.
`XmlNsMap`	Un JSONToXml.
`MultipartForm`	Peut être utilisé comme objet de valeur pour les requêtes/réponses entrantes/sortantes d'un type de mime multipart/form-data.
`PartType`	Doit être utilisé en conjonction avec des fournisseurs Multipart quand on écrit une liste ou un mappage de type multipart/*.
`XopWithMultipartRelated`	Cette annotation peut être utilisée pour traiter/produire des messages XOP entrants/sortants (packagés comme multipart/related) vers/en provenance d'objets annotés JAXB.

Annotation	Utilisation
`After`	Utilisée pour ajouter un attribut d'expiration quand on signe ou comme contrôle.
`Signed`	Annotation pratique qui déclenche la signature d'une requête ou d'une réponse utilisant la spécification DOSETA.
`Verify`	Vérification d'une signature entrante spécifiée dans un en-tête de signature.

Report a bug

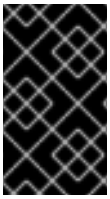
12.5. CONFIGURATION RESTEASY

12.5.1. Paramètres de configuration RESTEasy

Tableau 12.2. Éléments

Nom d'option	Valeur par défaut	Description
resteasy.servlet.mapping.prefix	Pas de valeur par défaut	Si le modèle d'url du mappage de servlet Resteasy n'est pas /*.
resteasy.scan	false	Scanner automatiquement les jars WEB-INF/lib et le répertoire WEB-INF/classes pour @Provider et les classes de ressource JAX-RS (@Path, @GET, @POST etc..) à la fois et les enregistrer.
resteasy.scan.providers	false	Scanner les classes @Provider et les enregistrer.
resteasy.scan.resources	false	Scanner les classes de ressources JAX-RS.
resteasy.providers	pas de valeur par défaut	Une liste de noms de classes @Provider complètes que vous souhaitez enregistrer délimitée par des virgules.
resteasy.use.builtin.providers	true	Indique si on doit ou non enregistrer les classes @Provider intégrées, par défaut.

Nom d'option	Valeur par défaut	Description
resteasy.resources	Pas de valeur par défaut	Une liste de noms de classes de ressources JAX-RS complètes que vous souhaitez enregistrer délimitée par des virgules.
resteasy.jndi.resources	Pas de valeur par défaut	Une liste délimitée par des virgules de noms JNDI qui référencent des objets que vous souhaitez enregistrer comme ressources JAX-RS.
javax.ws.rs.Application	Pas de valeur par défaut	Nom qualifié de classe d'application à amorcer en spec portable.
resteasy.media.type.mappings	Pas de valeur par défaut	Remplace le besoin d'un en-tête Accept par mappage des extensions de noms de fichier (comme .xml ou .txt) avec un type de media. Utilisé quand le client n'est pas en mesure d'utiliser un en-tête Accept pour choisir une représentation (par ex. un navigateur).
resteasy.language.mappings	Pas de valeur par défaut	Remplace le besoin d'un en-tête Accept-Language par mappage des extensions de noms de fichier (comme .en ou .fr) avec une langue. Utilisé quand le client n'est pas en mesure d'utiliser un en-tête Accept-Language pour choisir une représentation (par ex. un navigateur).



IMPORTANT

Dans un conteneur Servlet 3.0, les configurations `resteasy.scan.*` du fichier `web.xml` seront ignorées, et tous les composants annotés JAX-RS seront scannés automatiquement.

Report a bug

12.6. JAX-RS WEB SERVICE SECURITY

12.6.1. Activer la sécurité basée-rôle pour RESTEasy JAX-RS Web Service

Résumé

RESTEasy supporte les annotations @RolesAllowed, @PermitAll, et @DenyAll sur les méthodes JAX-RS. Cependant, il ne reconnaît pas ces annotations par défaut. Suivre les étapes suivantes pour configurer le fichier `web.xml` et pour activer la sécurité basée-rôle.

AVERTISSEMENT

Ne pas activer la sécurité basée-rôle si l'application utilise les EJB. Le conteneur EJB procurera la fonctionnalité à la place de RESTEasy.

Procédure 12.1. Activer la sécurité basée-rôle pour RESTEasy JAX-RS Web Service

1. Ouvrir le fichier `web.xml` de l'application dans l'éditeur de textes.
2. Ajouter le <context-param> suivant au fichier, dans les balises `web-app`:

```
<context-param>
    <param-name>resteasy.role.based.security</param-name>
    <param-value>true</param-value>
</context-param>
```

3. Déclarer tous les rôles utilisés dans le fichier RESTEasy JAX-RS WAR file, en utilisant les balises de <security-role>:

```
<security-role><role-name>ROLE_NAME</role-name></security-role>
<security-role><role-name>ROLE_NAME</role-name></security-role>
```

4. Autorise l'accès à tous les URL gérés par le runtime JAX-RS pour tous les rôles :

```
<security-constraint><web-resource-collection><web-resource-
name>Resteasy</web-resource-name><url-pattern>/PATH</url-pattern>
</web-resource-collection><auth-constraint><role-
name>ROLE_NAME</role-name><role-name>ROLE_NAME</role-name></auth-
constraint></security-constraint>
```

Résultat

La sécurité basée rôle à été activée dans l'application, avec un certain nombre de rôles définis.

Exemple 12.1. Exemple de configuration de sécurité basée rôles

```
<web-app>

    <context-param>
 <param-name>resteasy.role.based.security</param-name>
 <param-value>true</param-value>
    </context-param>

    <servlet-mapping>
 <servlet-name>Resteasy</servlet-name>
 <url-pattern>/*</url-pattern>
    </servlet-mapping>

    <security-constraint>
 <web-resource-collection>
     <web-resource-name>Resteasy</web-resource-name>
     <url-pattern>/security</url-pattern>
 </web-resource-collection>
 <auth-constraint>
     <role-name>admin</role-name>
     <role-name>user</role-name>
 </auth-constraint>
    </security-constraint>

    <security-role>
 <role-name>admin</role-name>
    </security-role>
    <security-role>
 <role-name>user</role-name>
    </security-role>

</web-app>
```

Report a bug

12.6.2. Sécuriser un service JAX-RS Web par des annotations

Résumé

Cette rubrique couvre les étapes à parcourir pour sécuriser un service JAX-RS Web par les annotations de sécurité supportées.

Procédure 12.2. Sécuriser un service JAX-RS Web par des annotations de sécurité supportées.

1. Activer la sécurité basée-rôle. Pour plus d'informations, voir Section 12.6.1, « Activer la sécurité basée-rôle pour RESTEasy JAX-RS Web Service ».

2. Ajouter des annotations de sécurité au service JAX-RS Web. RESTEasy supporte les annotations suivantes :

   @RolesAllowed

Définit les rôles qui peuvent accéder à la méthode. Tous les rôles doivent être définis dans le fichier `web.xml`.

@PermitAll

Autorise tous les rôles définis dans le fichier `web.xml` à accéder à la méthode.

@DenyAll

Refuse tout accès à la méthode.

Report a bug

12.7. RESTEASY LOGGING

12.7.1. JAX-RS Web Service Logging

RESTEasy supporte la journalisation via java.util.logging, log4j, et slf4j. Le framework est choisi avec l'algorithme suivant :

1. Si log4j est dans le chemin de classe de l'application, log4j sera utilisé.
2. Si slf4j est dans le chemin de classe de l'application, slf4j sera utilisé.
3. java.util.logging est la valeur par défaut si ni log4j ni slf4j sont dans le chemin de classe.
4. Si le param de contexte de servlet resteasy.logger.type est défini à java.util.logging, log4j, ou slf4j remplaceront le comportement par défaut.

Report a bug

12.7.2. Catégories de journalisation définies dans RESTEasy

Tableau 12.3. Catégories

Catégorie	Fonction
`org.jboss.resteasy.core`	Journalise toutes les activités par l'implémentation RESEasy principale.
`org.jboss.resteasy.plugins.providers`	Journalise toutes les activités par les fournisseurs d'entité RESTEasy.
`org.jboss.resteasy.plugins.server`	Journalise tous les activités par l'implémentation RESEasy.
`org.jboss.resteasy.specimpl`	Journalise toutes les activités par les classes d'implémentation JAX-RS.
`org.jboss.resteasy.mock`	Journalise les activités par le framework factice RESTEasy.

Report a bug

12.8. GESTION DES EXCEPTIONS

12.8.1. Créer un mappeur d'exceptions

Résumé

Les mappeurs d'exceptions sont des composants fournis par des applications, personnalisés qui interceptent les exceptions lancées et qui écrivent des réponses HTTP spécifiques.

Exemple 12.2. Mappeur d'exceptions

Un mappeur d'exceptions est une classe annotée par @Provider qui implémente l'interface **`ExceptionMapper`** .

Voici un exemple de mappeur d'exceptions ci-dessous.

```
@Provider
public class EJBExceptionMapper implements
ExceptionMapper<javax.ejb.EJBException>
    {
    Response toResponse(EJBException exception) {
    return Response.status(500).build();
    }
}
```

Pour enregistrer un mappeur d'exceptions, listez-le dans le fichier **`web.xml`** sous le paramètre de contexte **`resteasy.providers`**, ou bien renvoyez-le par programmation via la classe **`ResteasyProviderFactory`**.

Report a bug

12.8.2. Exceptions RESTEasy lancées en interne

Tableau 12.4. Liste des exceptions

Exception	Code HTTP	Description
BadRequestException	400	Échec de la requête. La requête n'a pas été formatée correctement, ou il y a eu un problème lors de son traitement.
UnauthorizedException	401	Non autorisé. Exception de sécurité envoyée si vous utilisez la sécurité basée rôle annotée RESTEasy.
InternalServerErrorException	500	Erreur interne de serveur.

Exception	Code HTTP	Description
MethodNotAllowedException	405	Il n'y a pas de méthode JAX-RS pour la ressource qui peut gérer l'opération HTTP invoquée.
NotAcceptableException	406	Il n'y a pas de méthode JAX-RS qui puisse produire les types de media listés dans l'en-tête Accept
NotFoundException	404	Il n'y a pas de méthode JAX-RS qui serve le chemin/la ressource de la requête.
ReaderException	400	Toutes les exceptions envoyées, à partir des **`MessageBodyWriters`** sont incluses dans cette exception. S'il n'y a pas de **`ExceptionMapper`** dans l'exception, ou si l'exception n'est pas une **`WebApplicationException`**, alors RESTEasy renverra un code 400 par défaut.
WriterException	500	Toutes les exceptions envoyées, à partir des **`MessageBodyWriters`** sont incluses dans cette exception. S'il n'y a pas de **`ExceptionMapper`** dans l'exception, ou si l'exception n'est pas une **`WebApplicationException`**, alors RESTEasy renverra un code 400 par défaut.
JAXBUnmarshalException	400	Les fournisseurs JAXB (XML et Jettison) envoient cette exception sur les lectures. Peuvent correspondre à des wrapping JAXBExceptions. Cette classe s'étend à **`ReaderException`**.

Exception	Code HTTP	Description
JAXBMarshalException	500	Les fournisseurs JAXB (XML et Jettison) envoient cette exception sur les lectures. Peuvent correspondre à des wrapping JAXBExceptions. Cette classe s'étend à **`WriterException`**.
ApplicationException	N/A	Encapsule toutes les exceptions levées à partir du code d'application. Fonctionne de la même façon que **`InvocationTargetException`**. S'il y a un ExceptionMapper pour l'exception encapsulée, elle sera utilisée pour traiter la demande
Échec	N/A	Erreur RESTEasy interne. Non journalisée.
LoggableFailure	N/A	Erreur RESTEasy interne. Journalisée.
DefaultOptionsMethodException	N/A	Si l'utilisateur invoque **HTTP `OPTIONS`** et qu'il n'y a pas de méthode JAX-RS, RESTEasy fournira un comportement par défaut en lançant cette exception.

Report a bug

12.9. INTERCEPTEURS RESTEASY

12.9.1. Interception des invocations JAX-RS

Résumé

RESTEasy peut intercepter les invocations JAX-RS et les re-router vers des objets style listener que l'on appelle des intercepteurs. Cette section couvre les descriptions de quatre types d'intercepteurs.

> **Exemple 12.3. MessageBodyReader/Writer Interceptors**
>
> Les MessageBodyReaderInterceptors et les MessageBodyWriterInterceptors peuvent être utilisés soit côté cleint, soit côté serveur. Ils sont annotés par **`@Provider`**, ainsi que par **`@ServerInterceptor`** ou **`@ClientInterceptor`**, de façon à ce que RESTEasy sache s'il doit les ajouter ou non à la liste d'intercepteurs.

Ces intercepteurs encapsulent l'invocation de **`MessageBodyReader.readFrom()`** ou de **`MessageBodyWriter.writeTo()`**. Ils peuvent être utilisés pour encapsuler les flux d'entrée ou de sortie.

Le Support RESTEasy GZIP possède des intercepteurs qui créent ou remplacent les flux d'entrée ou de sortie par défaut par un GzipOutputStream ou un GzipInputStream afin que l'encodage gzip puisse opérer. Ils peuvent également être utilisés pour ajouter les en-têtes à la réponse, ou la requête sortante côté client.

```
public interface MessageBodyReaderInterceptor
  {
     Object read(MessageBodyReaderContext context) throws IOException,
WebApplicationException;

  }

public interface MessageBodyWriterInterceptor
  {
     void write(MessageBodyWriterContext context) throws IOException,
WebApplicationException;

  }
```

Les intercepteurs et le MessageBodyReader ou Writer sont invoqués dans une seule pile d'appels de Java. **`MessageBodyReaderContext.proceed()`** ou **`MessageBodyWriterContext.proceed()`** est appelé pour aller vers le prochain intercepteur, ou, s'il n'y a plus d'intercepteur à invoquer, la méthode **`readFrom()`** ou **`writeTo()`** du MessageBodyReader ou du MessageBodyWriter. Cette encapsulation permet aux objets d'être modifiés avant d'aller vers le Reader ou Writer, puis d'être nettoyés, après **`proceed()`**.

L'exemple ci-dessous montre un serveur côté intercepteur, qui ajoute une valeur d'en-tête à la réponse.

```
@Provider
@ServerInterceptor
public class MyHeaderDecorator implements MessageBodyWriterInterceptor {

    public void write(MessageBodyWriterContext context) throws
IOException, WebApplicationException
    {
       context.getHeaders().add("My-Header", "custom");
       context.proceed();
    }
}
```

Exemple 12.4. PreProcessInterceptor

Les PreProcessInterceptors sont exécutés après qu'une méthode de ressource JAX-RS ait été trouvée pour l'invocation, mais avant l'invocation réelle. Ils sont annotés avec @ServerInterceptor et exécutent en séquence.

Ces interfaces ne sont pas utilisables sur le serveur. Elles peuvent être utilisées pour implémenter

des fonctionnalités de sécurité, ou afin de préempter la demande Java. La mise en œuvre de la sécurité RESTEasy utilise ce type d'intercepteur pour abandonner les demandes avant qu'elles aient lieu si l'utilisateur ne passe pas d'autorisation. Le framework de mise en cache de RESTEasy cela utilise ceci également pour renvoyer des réponses mises en cache afin d'éviter une fois de plus l'invocation de méthodes.

```
public interface PreProcessInterceptor
    {
       ServerResponse preProcess(HttpRequest request, ResourceMethod
method) throws Failure, WebApplicationException;
    }
```

Si la méthode **`preProcess()`** renvoie une ServerResponse, alors la méthode JAX-RS sous-jacente ne sera pas invoquée, et le runtime traitera la réponse et retournera au client. Si la méthode **`preProcess()`** ne renvoie pas une ServerResponse, la méthode JAX-RS sous-jacente sera alors invoquée.

Exemple 12.5. PostProcessInterceptors

Les PreProcessInterceptors sont exécutés après qu'une méthode de ressource JAX-RS soit invoquée. Ils sont utilisés si un en-tête de réponse a besoin d'être défini quand un MessageBodyWriter n'a pas été invoqué.

Ils ne peuvent être utilisés que du côté du serveur. Ils ne peuvent pas encapsuler quoi que ce soit, et sont invoqués séquentiellement.

```
public interface PostProcessInterceptor
  {
    void postProcess(ServerResponse response);
  }
```

Exemple 12.6. ClientExecutionInterceptors

Les ClientExecutionInterceptors ne sont utilisables que du côté client. Ils sont encapsulés dans l'invocation HTTP qui va vers le serveur. Ils doivent être annotés par **`@ClientInterceptor`** et **`@Provider`**. Ces intercepteurs sont exécutés après que le MessageBodyWriter, et que le ClientRequest aient été créés côté client.

Le support RESTEasy GZIP utilise des ClientExecutionInterceptors pour que l'en-tête Accept puisse contenir «gzip, deflate» avant que la demande soit envoyée. Le cache du client RESTEasy l'utilise pour vérifier si son cache contient la ressource avant qu'elle soit envoyée.

```
public interface ClientExecutionInterceptor
{
  ClientResponse execute(ClientExecutionContext ctx) throws Exception;
}

public interface ClientExecutionContext
{
  ClientRequest getRequest();
```

```
  ClientResponse proceed() throws Exception;
}
```

Report a bug

12.9.2. Lier un intercepteur à une méthode JAX-RS

Résumé

Par défaut, tous les intercepteurs sont invoqués pour chaque requête. L'interface **`AcceptedByMethod`** peut être implémentée pour préciser ce comportement.

Exemple 12.7. Exemple de liaison d'intercepteurs

RESTEasy appelera la méthode **`accept()`** pour les intercepteurs qui implémentent l'interface **`AcceptedByMethod`**. Si la méthode renvoie true, l'intercepteur sera ajouté à la chaîne d'appel de la méthode JAX-RS; sinon, il sera ignoré avec cette méthode.

Dans l'exemple ci-dessous, **`accept()`** détermine si l'annotation @GET est présente dans la méthode JAX-RS. Si tel est le cas, l'intercepteur sera appliqué à la chaîne d'appel de la méthode.

```
@Provider
@ServerInterceptor
public class MyHeaderDecorator implements MessageBodyWriterInterceptor,
AcceptedByMethod {

    public boolean accept(Class declaring, Method method) {
       return method.isAnnotationPresent(GET.class);
    }

   public void write(MessageBodyWriterContext context) throws
IOException, WebApplicationException
   {
      context.getHeaders().add("My-Header", "custom");
      context.proceed();
   }
}
```

Report a bug

12.9.3. Enregistrer un intercepteur

Résumé

Cette section couvre la façon dont on doit enregistrer un intercepteur RESTEasy JAX-RS dans une application.

Procédure 12.3. Enregistrer un intercepteur

- Pour enregistrer un intercepteur, listez-le dans le fichier `web.xml` sous le paramètre de contexte `resteasy.providers`, ou bien renvoyez-le sous forme de classe ou d'objet dans `Application.getClasses()` ou `Application.getSingletons()`

Report a bug

12.9.4. Familles de précédence d'intercepteur

12.9.4.1. Familles de précédence d'intercepteur

Résumé

Les intercepteurs peuvent être sensibles à l'ordre dans lequel ils sont invoqués. Mettre les intercepteurs de groupes RESTEasy en familles pour faciliter l'ordonnancement. Cette section couvre les familles de précédence d'intercepteurs intégrés et les intercepteurs associés à chaque famille.

Il existe cinq familles prédéfinies. Elles sont invoquées dans l'ordre suivant :

SECURITY

Les intercepteurs SECURITY sont normalement des PreProcessInterceptors. Ils sont invoqués en premier car on ne doit pas faire grand chose avant que l'invocation soit autorisée.

HEADER_DECORATOR

Les intercepteurs HEADER_DECORATOR ajoutent des en-têtes à une réponse ou à une requête sortante. Ils suivent les intercepteurs de sécurité car les en-têtes ajoutés peuvent affecter le comportement des autres familles d'intercepteurs.

ENCODER

Les intercepteurs ENCODER changent l'OutputStream. Par exemple, l'intercepteur GZIP crée un GZIPOutputStream pour envelopper l'outputStream réel pour la compression.

REDIRECT

Les intercepteurs REDIRECT sont normalement utilisés dans PreProcessInterceptors, car ils peuvent router à nouveau la demande et éviter ainsi totalement la méthode JAX-RS.

DECODER

Les intercepteurs DECODER englobent l'lutputStream. Par exemple, le décodeur d'intercepteur GZIP englobe le GZIPInputStream.

Les intercepteurs qui ne sont pas associés à une famille de précédence sont invoqués après les autres. Pour assigner un intercepteur à une famille de précédence, utiliser l'annotation @Precedence, et voir Section 12.4, « Annotations définies RESTEasy ».

Report a bug

12.9.4.2. Définissez une famille de précédence d'intercepteurs personnalisée

Résumé

Les familles de précédence personnalisées peuvent être créées ou enregistrées dans le fichier `web.xml`. Ce sujet couvre des exemples des paramètres de contexte disponibles pour définir les familles de précédence d'intercepteurs.

Il existe trois paramètres de contexte qui puissent être utilisés pour définir une nouvelle famille de précédence.

Exemple 12.8. resteasy.append.interceptor.precedence

Le paramètre de contexte **`resteasy.append.interceptor.precedence`** rajoute la nouvelle famille de précédence à la liste de famille de précédent par défaut.

```
<context-param>
    <param-name>resteasy.append.interceptor.precedence</param-name>
    <param-value>CUSTOM_PRECEDENCE_FAMILY</param-value>
</context-param>
```

Exemple 12.9. resteasy.interceptor.before.precedence

Le paramètre de contexte **`resteasy.interceptor.before.precedence`** définit la famille de précédence par défaut exécutée avant la famille personnalisée. La valeur du paramètre est sous la forme *DEFAULT_PRECEDENCE_FAMILY/CUSTOM_PRECEDENCE_FAMILY*, délimitée par un ':'.

```
<context-param>
    <param-name>resteasy.interceptor.before.precedence</param-name>
    <param-value>DEFAULT_PRECEDENCE_FAMILY :
CUSTOM_PRECEDENCE_FAMILY</param-value>
</context-param>
```

Exemple 12.10. resteasy.interceptor.after.precedence

Le paramètre de contexte **`resteasy.interceptor.after.precedence`** définit la famille de précédence par défaut exécutée après la famille personnalisée. La valeur du paramètre est sous la forme *DEFAULT_PRECEDENCE_FAMILY/CUSTOM_PRECEDENCE_FAMILY*, délimitée par un `:`.

```
<context-param>
    <param-name>resteasy.interceptor.after.precedence</param-name>
    <param-value>DEFAULT_PRECEDENCE_FAMILY :
CUSTOM_PRECEDENCE_FAMILY</param-value>
</context-param>
```

Les familles de précédence sont appliquées aux intercepteurs à l'aide de l'annotation @Precedence. Pour la liste de famille de précédence par défaut, reportez-vous à: Section 12.9.4.1, « Familles de précédence d'intercepteur ».

Report a bug

12.10. ANNOTATIONS BASÉES CHAÎNE

12.10.1. Conversion des annotations basées @*Param en objects

Les annotations **@*Param** JAX-RS,@PathParam et @FormParam incluses, sont représentées par des chaînes dans une requête HTTP brut. Ces types de paramètres injectés peuvent être convertis en objets si ces objets ont une méthode valueOf(String) statique ou un constructeur qui prend un paramètre String.

RESTEasy fournit deux interfaces **@Provider** commerciales pour effectuer cette conversion pour les classes qui n'ont ni de méthode **valueOf(String)** statique, ni de constructeur de string.

Exemple 12.11. StringConverter

L'interface StringConverter est mise en place afin de fournir un marshalling de chaîne personnalisée. Elle est inscrite dans resteasy.providers context-param du fichier web.xml. Elle peut également être enregistrée manuellement en appelant la méthode ResteasyProviderFactory.addStringConverter().

L'exemple suivant est un simple exemple qui utilise le StringConverter.

```
import org.jboss.resteasy.client.ProxyFactory;
import org.jboss.resteasy.spi.StringConverter;
import org.jboss.resteasy.test.BaseResourceTest;
import org.junit.Assert;
import org.junit.Before;
import org.junit.Test;

import javax.ws.rs.HeaderParam;
import javax.ws.rs.MatrixParam;
import javax.ws.rs.PUT;
import javax.ws.rs.Path;
import javax.ws.rs.PathParam;
import javax.ws.rs.QueryParam;
import javax.ws.rs.ext.Provider;

public class StringConverterTest extends BaseResourceTest
{
  public static class POJO
  {
     private String name;

     public String getName()
     {
 return name;
     }

     public void setName(String name)
     {
 this.name = name;
     }
  }

  @Provider
  public static class POJOConverter implements StringConverter<POJO>
  {
     public POJO fromString(String str)
     {
 System.out.println("FROM STRNG: " + str);
 POJO pojo = new POJO();
```

```
 pojo.setName(str);
 return pojo;
     }

     public String toString(POJO value)
     {
 return value.getName();
     }
  }

  @Path("/")
  public static class MyResource
  {
     @Path("{pojo}")
     @PUT
     public void put(@QueryParam("pojo")POJO q, @PathParam("pojo")POJO
pp,
       @MatrixParam("pojo")POJO mp, @HeaderParam("pojo")POJO hp)
     {
 Assert.assertEquals(q.getName(), "pojo");
 Assert.assertEquals(pp.getName(), "pojo");
 Assert.assertEquals(mp.getName(), "pojo");
 Assert.assertEquals(hp.getName(), "pojo");
     }
  }

  @Before
  public void setUp() throws Exception
  {

dispatcher.getProviderFactory().addStringConverter(POJOConverter.class);
     dispatcher.getRegistry().addPerRequestResource(MyResource.class);
  }

  @Path("/")
  public static interface MyClient
  {
     @Path("{pojo}")
     @PUT
     void put(@QueryParam("pojo")POJO q, @PathParam("pojo")POJO pp,
       @MatrixParam("pojo")POJO mp, @HeaderParam("pojo")POJO hp);
  }

  @Test
  public void testIt() throws Exception
  {
     MyClient client = ProxyFactory.create(MyClient.class,
"http://localhost:8081");
     POJO pojo = new POJO();
     pojo.setName("pojo");
     client.put(pojo, pojo, pojo, pojo);
  }
}
```

Exemple 12.12. StringParameterUnmarshaller

L'interface **`StringParameterUnmarshaller`** est sensible aux annotations placées sur le paramètre ou le champ sur lesquels vous injectez. Il est créé par injecteur. La méthode setAnnotations() est appelée par resteasy pour initialiser l'unmarshaller.

Cette interface peut être ajoutée en créant et en enregistrant un fournisseur qui implémente l'interface. Il peut être également lié à une meta-annotations appelée **`org.jboss.resteasy.annotations.StringsParameterUnmarshallerBinder`**.

L'exemple ci-dessous formate un **`java.util.Date`** basé @PathParam.

```
public class StringParamUnmarshallerTest extends BaseResourceTest
{
   @Retention(RetentionPolicy.RUNTIME)
   @StringParameterUnmarshallerBinder(DateFormatter.class)
   public @interface DateFormat
   {
      String value();
   }

   public static class DateFormatter implements
StringParameterUnmarshaller<Date>
   {
      private SimpleDateFormat formatter;

      public void setAnnotations(Annotation[] annotations)
      {
         DateFormat format = FindAnnotation.findAnnotation(annotations,
DateFormat.class);
         formatter = new SimpleDateFormat(format.value());
      }

      public Date fromString(String str)
      {
         try
         {
            return formatter.parse(str);
         }
         catch (ParseException e)
         {
            throw new RuntimeException(e);
         }
      }
   }

   @Path("/datetest")
   public static class Service
   {
      @GET
      @Produces("text/plain")
      @Path("/{date}")
      public String get(@PathParam("date") @DateFormat("MM-dd-yyyy")
Date date)
      {
         System.out.println(date);
```

```
            Calendar c = Calendar.getInstance();
            c.setTime(date);
            Assert.assertEquals(3, c.get(Calendar.MONTH));
            Assert.assertEquals(23, c.get(Calendar.DAY_OF_MONTH));
            Assert.assertEquals(1977, c.get(Calendar.YEAR));
            return date.toString();
         }
      }

      @BeforeClass
      public static void setup() throws Exception
      {
         addPerRequestResource(Service.class);
      }

      @Test
      public void testMe() throws Exception
      {
         ClientRequest request = new
   ClientRequest(generateURL("/datetest/04-23-1977"));
         System.out.println(request.getTarget(String.class));
      }
   }
```

Définit une nouvelle annotation appelée @DateFormat. L'annotation est annotée avec la meta-annotation StringParameterUnmarshallerBinder avec une référence aux classes DateFormater.

La méthode Service.get() possède un paramètre @PathParam qui est aussi annoté avec @DateFormat. L'application @DateFormat déclenche la liaison du DateFormatter. Le DateFormatter sera désormais exécuté pour supprimer le marshalling du paramètre de chemin d'accès dans le paramètre date de la méthode get().

Report a bug

12.11. CONFIGURATION DES EXTENSIONS DE FICHIERS

12.11.1. Mapper les extensions de fichiers avec les types de media dans le fichier web.xml

Résumé

Certains clients, comme les navigateurs, ne peuvent pas utiliser les en-têtes Accept et Accept-Language pour négocier le type de média de la représentation ou la langue. RESTEasy peut mapper des suffixes de noms de fichier aux langues et types de médias pour régler ce problème. Procédez comme suit pour mapper les types de media avec les extensions de fichier, dans le fichier `web.xml`

Procédure 12.4. Mapper des types de media avec les extensions de fichiers

1. Ouvrir le fichier `web.xml` de l'application dans l'éditeur de textes.
2. Ajouter le paramètre de contexte `resteasy.media.type.mappings` au fichier, dans les balises `web-app` :

```
<context-param>
```

```
    <param-name>resteasy.media.type.mappings</param-name>
</context-param>
```

3. Configurer les valeurs des paramètres. Les mappages forment une liste délimitée par des virgules. Chaque mappage est délimité par un `:`:

Exemple 12.13. Exemple de mappage

```
<context-param>
    <param-name>resteasy.media.type.mappings</param-name>
    <param-value>html : text/html, json : application/json, xml :
application/xml</param-value>
</context-param>
```

Report a bug

12.11.2. Mapper les extensions de fichiers vers les Langues dans le fichier web.xml

Résumé

Certains clients, comme les navigateurs, ne peuvent pas utiliser les en-têtes Accept et Accept-Language pour négocier le type de média de la représentation ou la langue. RESTEasy peut mapper des suffixes de noms de fichier aux langues et types de médias pour régler ce problème. Procédez comme suit pour mapper les langues avec les extensions de fichier, dans le fichier `web.xml`

Procédure 12.5. Mapper les extensions de fichiers vers les Langues dans le fichier web.xml

1. Ouvrir le fichier `web.xml` de l'application dans un éditeur de texte.

2. Ajouter le paramètre de contexte `resteasy.language.mappings` au fichier, dans les balises `web-app` :

```
<context-param>
    <param-name>resteasy.language.mappings</param-name>
</context-param>
```

3. Configurer les valeurs de paramètres. Les mappages forment une liste délimitée par des virgules. Chaque mappage est délimité par un `:`:

Exemple 12.14. Exemple de mappage

```
<context-param>
    <param-name>resteasy.language.mappings</param-name>
    <param-value> en : en-US, es : es, fr : fr</param-name>
</context-param>
```

Report a bug

12.11.3. Types de media supportés par RESTEasy

Tableau 12.5. Types de media

Type de media	Type Java
application/*+xml, text/*+xml, application/*+json, application/*+fastinfoset, application/atom+*	Classes annotées JaxB
application/*+xml, text/*+xml	org.w3c.dom.Document
/	java.lang.String
/	java.io.InputStream
text/brut	primtives, java.lang.String, ou tout type qui possède un contructeur de String, ou une méthode valueOf(String) pour les entrées et toString() pour les sorties
/	javax.activation.DataSource
/	byte[]
/	java.io.File
application/x-www-form-urlencoded	javax.ws.rs.core.MultivaluedMap

Report a bug

12.12. API JAVASCRIPT RESTEASY

12.12.1. API JavaScript RESTEasy

RESTEasy peut générer un API JavaScript qui utilise les appels AJAX pour invoquer les opérations JAX-RS. Chaque classe de ressource JAX-RS va générer un objet JavaScript du même nom que la classe ou l'interface qui déclare. L'objet JavaScript contient chaque méthode JAX-RS sous forme de propriété.

Exemple 12.15. Simple exemple d'API JavaScript JAX-RS

```
@Path("/")
public interface X{
 @GET
 public String Y();
 @PUT
 public void Z(String entity);
}
```

L'interface ci-dessus définit les méthodes Y et Z, qui deviennent des propriétés dans l'API JavaScript, comme ci-dessous :

```
var X = {
 Y : function(params){...},
 Z : function(params){...}
};
```

Chaque méthode d'API JavaScript prend un objet optionnel comme simple paramètre avec chaque propriété comme cookie, en-tête, chemin d'accès, requête ou paramètre de formulaire identifiés par un nom, ou les propriétés de paramètre de l'API. Les propriétés disponibles sont les suivantes : Section 12.12.3, « Paramètres de l'API JavaScript RESTEasy » .

Report a bug

12.12.2. Activation du Servlet API JavaScript RESTEasy

Résumé

L'API JavaScript RESTEasy n'est pas activé par défaut. Suivre les étapes suivantes en utilisant le fichier **web.xml**.

Procédure 12.6. Modifier web.xml pour activer l'API RESTEasy JavaScript

1. Ouvrir le fichier **web.xml** de l'application dans l'éditeur de textes.
2. Ajouter la configuration suivante dans le fichier, dans les balises **web-app** :

```
<servlet><servlet-name>RESTEasy JSAPI</servlet-name><servlet-
class>org.jboss.resteasy.jsapi.JSAPIServlet</servlet-class>
</servlet><servlet-mapping><servlet-name>RESTEasy JSAPI</servlet-
name><url-pattern>/URL</url-pattern></servlet-mapping>
```

Report a bug

12.12.3. Paramètres de l'API JavaScript RESTEasy

Tableau 12.6. Propriétés des paramètres

Propriété	Valeur par défaut	Description
$entity		L'entité pour envoyer une requête PUT ou POST.

Propriété	Valeur par défaut	Description
$contentType		Type MIME de l'entité de contenu envoyée comme en-tête de type de contenu ou Content-Type. Déterminé par l'annotation @Consumes.
$accepts	*/*	Types MIME de l'entité envoyés comme en-tête de Accept. Déterminé par l'annotation @Provides.
$callback		Définir à une fonction (httpCode, xmlHttpRequest, value) pour un appel asynchrone. Si non présent, l'appel sera synchronisé et renverra une valeur.
$apiURL		Définit la base de l'URI du point de terminaison JAX-RS, sans la dernière barre oblique.
$username		Si le nom d'utilisateur ou le mot de passe sont définis, ils seront utilisés comme informations d'authentification pour la demande.
$password		Si le nom d'utilisateur ou le mot de passe sont définis, ils seront utilisés comme informations d'authentification pour la demande.

Report a bug

12.12.4. Créer des requêtes AJAX par l'API JavaScript

Résumé

L'API JavaScript RESTEasy peut être utilisé pour créer des requêtes manuellement. Cette section couvre des exemples de ce comportement.

> **Exemple 12.16. L'Objet REST**
>
> L'objet REST peut être utilisé pour remplacer le comportement du client API JavaScript RESTEasy :
>
> ```
> // Change the base URL used by the API:
> REST.apiURL = "http://api.service.com";
>
> // log everything in a div element
> ```

```
REST.log = function(text){
 jQuery("#log-div").append(text);
};
```

L'objet RESTEasy contient les propriétés lecture-écriture suivantes :

apiURL

Défini par défaut à l'URL root JAX-RS. Utilisé par chaque fonction d'API Client JavaScript lors de la création de requêtes.

log

Définir à une fonction(string) pour pouvoir recevoir les logs d'API Client RESTEasy. Cela est utile si vous souhaitez déboguer votre API Client ou mettre les logs là où vous pouvez les voir.

Exemple 12.17. La classe REST.Request

La classe REST.Request peut être utilisée pour créer des requêtes personnalisées :

```
var r = new REST.Request();
r.setURI("http://api.service.com/orders/23/json");
r.setMethod("PUT");
r.setContentType("application/json");
r.setEntity({id: "23"});
r.addMatrixParameter("JSESSIONID", "12309812378123");
r.execute(function(status, request, entity){
 log("Response is "+status);
});
```

Report a bug

12.12.5. Membres de la classe REST.Request

Tableau 12.7. Classe REST.Request

Membre	Description
execute(callback)	Exécute la requête avec toutes les informations définies pour l'objet en cours. La valeur est passée à la fonction de rappel de l'argument optionnel, et n'est pas renvoyée.
setAccepts(acceptHeader)	Définit l'en-tête de la requête Accept. Par défaut */*.
setCredentials(username, password)	Définit les informations d'identification de la requête.

Membre	Description
setEntity(entity)	Définit les informations d'identification de l'entité.
setContentType(contentTypeHeader)	Définit l'en-tête de la requête Type de contenu
setURI(uri)	Définit l'URI de la requête. Doit correspondre à un URI absolu.
setMethod(method)	Définit la méthode de requête. GET par défaut.
setAsync(async)	Contrôle si la requête doit être asynchrone. True par défaut.
addCookie(name, value)	Définit le cookie donnée dans le document en cours quand on exécute la requête. Sera persistant dans le navigateur.
addQueryParameter(name, value)	Ajoute un paramètre d'interrogation à la partie de requête URI.
addMatrixParameter(name, value)	Ajoute un paramètre de matrix (paramètre de chemin d'accès) au dernier segment de l'URI de la requête.
addHeader(nom, valeur)	Ajoute un en-tête de requête.

Report a bug

12.13. RESTEASY ASYNCHRONOUS JOB SERVICE

12.13.1. Service Job Asynchrone RESTEasy

Le Service Job Asynchrone RESTEasy est conçu pour ajouter un comportement asynchrone au protocole HTTP. Alors que HTTP est un protocole synchrone, il possède une faible idée des appels asynchrones. Le HTTP 1.1 réponse code 202, « Accepted » signifie que le serveur a reçu et accepté la réponse pour le traitement, mais le traitement n'est pas encore terminé. Le Service Job Asynchrone est construit autour.

Pour activer le service, consulter : Section 12.13.2, « Activer le Service de jobs asynchrones » . Pour obtenir des informations sur la façon dont le service fonctionne, voir Section 12.13.3, « Configurer les Jobs asynchrones avec RESTEasy ».

Report a bug

12.13.2. Activer le Service de jobs asynchrones

Procédure 12.7. Modifier le fichier web.xml

- Activer le Service de jobs asynchrones dans le fichier `web.xml` :

```
<context-param>
    <param-name>resteasy.async.job.service.enabled</param-name>
    <param-value>true</param-value>
</context-param>
```

Résultat

Le service de jobs asynchrones a été activé. Pour les options de configuration, consulter : Section 12.13.4, « Paramètres de configuration de Service Job Asynchrone » .

Report a bug

12.13.3. Configurer les Jobs asynchrones avec RESTEasy

Résumé

Cette section couvre des exemples de paramètres de recherche de jobs asynchrones avec RESTEasy.

AVERTISSEMENT

La sécurité basée rôle ne fonctionne pas dans le Service de jobs asynchrones car il ne fonctionne pas de manière portable. Si le Service de jobs asynchrones est utilisé, la sécurité d'application doit être effectuée via déclarations XML par le fichier `web.xml` à la place.

IMPORTANT

Bien que les méthodes GET, DELETE, et PUT soient invoquées de manière asynchrones, cela rompt le contrat HTTP 1.1 de ces méthodes. Bien que ces invocations ne changent sans doute pas l'état de la ressource en cas d'invocations multiples, elles changent d'état du serveur en nouvelles entrées de Job pour chaque invocation.

Exemple 12.18. Le paramètre Asynch

Le paramètre de requête **asynch** est utilisé pour exécuter des invocations en arrière-plan. Une réponse 202 Accepted est retourné, ainsi que d'un en-tête d'emplacement avec un URL pointant vers la réponse de la méthode de base.

```
POST http://example.com/myservice?asynch=true
```

L'exemple ci-dessus retournera une réponse Accepted 202. Il retournera également un en-tête d'emplacement avec un URL pointant vers la réponse de la méthode de base. Voici un exemple de l'en-tête d'emplacement :

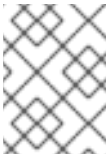
```
HTTP/1.1 202 Accepted
Location: http://example.com/asynch/jobs/3332334
```

L'URI prendra la forme suivante :

```
/asynch/jobs/{job-id}?wait={millisconds}|nowait=true
```

Les opérations GET, POST et DELETE peuvent être effectuées sur cet URL.

- GET renvoie la méthode de ressources JAX-RS invoquée comme réponse si le job est complété. Si le job n'a pas été complété, ce GET renverra un code de réponse 202 Accepted. L'invocation de GET ne supprime pas le job; peut être appelé à plusieurs reprises.
- POST procède à une lecture de la réponse du job et supprime le job s'il est terminé.
- DELETE est appelé pour nettoyer manuellement la file d'attente du job.



NOTE

Quand la file d'attente du job est pleine, il expulsera job le plus ancien de la mémoire automatiquement, sans avoir besoin d'appeler DELETE.

Exemple 12.19. Wait / Nowait

Les opérations GET et POST permettent de définir une durée d'attente maximum, par les paramètres de demande **`wait`** et **`nowait`**. Si le paramètre **`wait`** n'est pas spécifié, l'opération aura par défaut **`nowait=true`**, et n'attendra pas si le job n'est pas terminé. Le paramètre **`wait`** est défini en millisecondes.

```
POST http://example.com/asynch/jobs/122?wait=3000
```

Exemple 12.20. Le Paramètre Oneway

RESTEasy supporte «fire and forget jobs» (abandonner les jobs) avec le paramètre de requête **oneway**.

```
POST http://example.com/myservice?oneway=true
```

L'exemple ci-dessus retournera la réponse 202 Accepted, mais aucun job ne sera créé.

Report a bug

12.13.4. Paramètres de configuration de Service Job Asynchrone

Résumé

Le tableau suivant donne des informations sur la paramètres contextuels configurables du Service Job Asynchrone. Ces paramètres sont configurés dans le fichier **`web.xml`**.

Tableau 12.8. Paramètres de configuration

Paramètre	Description

Paramètre	Description
resteasy.async.job.service.max.job.results	Nombre de résultats de jobs qui peuvent être conservés en toute harmonie à un moment donné. La valeur par défaut est 100.
resteasy.async.job.service.max.wait	Temps d'attente maximum quand un client interroge un job. La valeur par défaut est 300000.
resteasy.async.job.service.thread.pool.size	Taille de thread pool des threads d'arrière-plan qui exécutent le job. La valeur par défaut est 100.
resteasy.async.job.service.base.path	Définit le chemin de base des URI de job. La valeur par défaut est /asynch/jobs

Exemple 12.21. Exemple de configuration de jobs asynchrones

```
<web-app>
    <context-param>
        <param-name>resteasy.async.job.service.enabled</param-name>
        <param-value>true</param-value>
    </context-param>

    <context-param>
        <param-name>resteasy.async.job.service.max.job.results</param-
name>
        <param-value>100</param-value>
    </context-param>
    <context-param>
        <param-name>resteasy.async.job.service.max.wait</param-name>
        <param-value>300000</param-value>
    </context-param>
    <context-param>
        <param-name>resteasy.async.job.service.thread.pool.size</param-
name>
        <param-value>100</param-value>
    </context-param>
    <context-param>
        <param-name>resteasy.async.job.service.base.path</param-name>
        <param-value>/asynch/jobs</param-value>
    </context-param>

    <listener>
        <listener-class>
            org.jboss.resteasy.plugins.server.servlet.ResteasyBootstrap
        </listener-class>
    </listener>

    <servlet>
        <servlet-name>Resteasy</servlet-name>
        <servlet-class>

org.jboss.resteasy.plugins.server.servlet.HttpServletDispatcher
```

```
        </servlet-class>
    </servlet>

    <servlet-mapping>
        <servlet-name>Resteasy</servlet-name>
        <url-pattern>/*</url-pattern>
    </servlet-mapping>

</web-app>
```

Report a bug

12.14. RESTEASY JAXB

12.14.1. Créer un décorateur JAXB

Résumé

Les fournisseurs JAXB de RESTEasy ont une manière enfichable de décorer des Instances Marshaller ou Unmarshaller. Il y a une annotation qui est créée soit par un Marshaller, soit par un Unmarshaller. Cette section couvre toutes les étapes pour créer un décorateur JAXB dans RESTEasy.

Procédure 12.8. Créer un décorateur JAXB dans RESTEasy

1. **Créer la classe de processeur**

   a. Créer une classe qui implémente DecoratorProcessor<Target, Annotation>. La cible sera soit une classe de Marshaller ou Unmarshaller JAXB. L'annotation est créée dans la seconde étape.

   b. Annoter la classe par @DecorateTypes, et déclarer les Types MIME que le décorateur doit décorer.

   c. Définir les propriétés ou les valeurs au sein de la fonction `decorate`.

Exemple 12.22. Exemple de classe de processeur

```
import org.jboss.resteasy.core.interception.DecoratorProcessor;
import org.jboss.resteasy.annotations.DecorateTypes;

import javax.xml.bind.Marshaller;
import javax.xml.bind.PropertyException;
import javax.ws.rs.core.MediaType;
import javax.ws.rs.Produces;
import java.lang.annotation.Annotation;

@DecorateTypes({"text/*+xml", "application/*+xml"})
public class PrettyProcessor implements
DecoratorProcessor<Marshaller, Pretty>
{
    public Marshaller decorate(Marshaller target, Pretty
annotation,
   Class type, Annotation[] annotations, MediaType mediaType)
```

```
    {
 target.setProperty(Marshaller.JAXB_FORMATTED_OUTPUT,
Boolean.TRUE);
    }
}
```

2. **Créer une annotation**

   a. Créer une interface personnalisée annotée par @Decorator.

   b. Déclarer le processeur ou la cible de l'annotation @Decorator. Le processeur est créé dans la première étape. La cible sera soit la classe Marshaller JAXB ou la classe Unmarshaller JAXB.

Exemple 12.23. Exemple d'annotation

```
import org.jboss.resteasy.annotations.Decorator;

@Target({ElementType.TYPE, ElementType.METHOD,
ElementType.PARAMETER, ElementType.FIELD})
@Retention(RetentionPolicy.RUNTIME)
@Decorator(processor = PrettyProcessor.class, target =
Marshaller.class)
public @interface Pretty {}
```

3. Ajouter l'annotation créée dans une fonction dans la seconde étape de façon à ce que l'entrée ou la sortie soit décorée quand elle sera mise en ordre.

Résultat

Le décorateur JAXB a été créé et sera appliqué au sein du service web JAX-RS.

Report a bug

12.15. RESTEASY ATOM SUPPORT

12.15.1. Fournissseur et API Atom

Le Fournisseur et l'API Atom RESTEasy est un modèle d'objet simple que RESTEasy définit pour représenter Atom. Les classes principales de l'API se trouvent dans le package **`org.jboss.resteasy.plugins.providers.atom`**. RESTEasy utilise JAXB pour marshaller et démarshaller l'API. Le fournisseur est basé JAXB, et ne se limite pas à envoyer des objets Atom par XML. Tous les fournisseurs JAXB que RESTEasy contient peuvent être réutilisés par le fournisseur et l'API Atom, y compris JSON. Voir Javadocs pour obtenir plus d'informations sur l'API.

Report a bug

CHAPITRE 13. SERVICES WEB JAX-WS

13.1. SERVICES WEB JAX-WS

API Java pour les Services Web XML (JAX-WS) est une API incluse dans la plate-forme Enterprise Edition (J2EE) et est utilisé pour créer des Services Web. Les Services Web sont des applications conçues pour communiquer entre elles via un réseau, typiquement échangeant des informations en XML ou autres formats de texte structuré. Les Services Web sont indépendants de la plate-forme. Une application typique de JAX-WS utilise un modèle client/serveur. Le composant de serveur s'appelle un *Point de terminaison de Service Web*

JAX-WS a un équivalent pour les plus petits et plus simples Services Web qui utilisent un protocole appelé JAX-RS. JAX-RS est un protocole de *Representational State Transfer*, ou REST. Les applications JAX-RS sont généralement légères et ne comptent que sur le protocole HTTP proprement dit pour la communication. JAX-WS rend plus facile de soutenir divers protocoles de services web, tels que **`WS-Notification`**, **`WS-Addressing`**, **`WS-Policy`**, **`WS-Security`** et **`WS-Trust`**. Ils communiquent à l'aide d'un XML spécialisé appelé *Simple Object Access Protocol (SOAP)*, qui définit une architecture de message et le message de formats.

Les Services Web JAX-WS incluent également une description lisible par machine des opérations fournies, écrite en *Web Services Description Language (WSDL)*, qui est un type spécialisé de document XML.

Un Point de terminaison de service web consiste en une classe qui implémente les interfaces **`WebService`** et **`WebMethod`**.

Un Client de Service Web est un client qui dépend de plusieurs classes appelées des *stubs* générées à partir de la définition WSDL. JBoss EAP 6 comprend les outils pour générer les classes à partir de WSDL.

Dans un Service Web JAX-WS, un contrat formel est créé pour décrire l'interface qui offre le Service Web. Le contrat est généralement écrit en WSDL, mais peut-être être écrit dans les messages SOAP. L'architecture du Service Web aborde généralement les besoins opérationnels, comme les transactions, la sécurité, la messagerie et la coordination. JBoss EAP 6 fournit des mécanismes pour traiter ces besoins commerciaux.

*Web Services Description Language (WSDL)*est un langage basé XML utilisé pour décrire des Services Web et comment y avoir accès. Le Service Web lui-même est écrit en Java ou autre langage de programmation. La définition WSDL est composée des références à l'interface, des définitions de port et des instructions sur la façon dont les autres Services Web doit interagir avec lui sur un réseau. Les Services Web communiquent entre eux à l'aide de *Simple Object Access Protocol (SOAP)*. Ce type de Service Web contraste avec les *Services Web RESTful* conçus à l'aide du principe *Representative State Transfer (REST)*. Ces Services Web RESTful n'exigent pas l'utilisation de WSDL ou de SOAP, mais reposent sur la structure du protocole HTTP lui-même pour définir comment les autres services interagissent avec eux.

JBoss EAP 6 inclut un support pour le déploiement des points de terminaison du service JAX-WS Web Service. Ce support est donné par JBossWS. La configuration du sous-système de services web, comme la configuration des points de terminaison, les chaînes de gestionnaires, les gestionnaires, est fournie via le sous-système **`webservices`**.

Exemples

Les JBoss EAP Quickstarts incluent plusieurs applications JAX-WS Web Services qui fonctionnent correctement. Exemples :

- wsat-simple
- wsba-coordinator-completion-simple
- wsba-participant-completion-simple

Report a bug

13.2. CONFIGURER LE SOUS-SYSTÈME WEBSERVICES

Il existe de nombreuses options de configuration pour le sous-système de **webservices**, qui contrôle le comportement des Services Web déployés dans JBoss EAP 6. La commande pour modifier chaque élément dans le script de gestion CLI (***EAP_HOME*** **/bin/jboss-cli.sh** ou ***EAP_HOME*** **/bin/jboss-cli.bat**) est fournie. Supprimer la partie de la commande **/ Profil = default** pour un serveur autonome, ou la modifier pour effectuer un changement au sous-système pour un profil différent sur un domaine géré.

Adresse de point de terminaison publiée

Vous pouvez écrire à nouveau l'élément **<soap:address>** dans les contrats WSDL endpoint-published. Cette solution peut être utilisée pour contrôler l'adresse du serveur qui est publiée aux clients pour chaque point de terminaison. Chacun des éléments suivants en option peuvent être modifiés pour satisfaire vos besoins. La modification de ces éléments exige un redémarrage du serveur.

Tableau 13.1. Éléments de configuration pour les adresses de points de terminaison publiés.

Élément	Description	Commande CLI
modify-wsdl-address	Indique s'il faut toujours modifier l'adresse WSDL. Si true, le contenu de **< adresse:soap >** sera toujours remplacé. Si false, le contenu de **< adresse:soap >** sera remplacé seulement si ce n'est pas une URL valide. Les valeurs utilisées seront **wsdl-host**, **wsdl-port**, et **wsdl-secure-port** décrit ci-dessous.	**/profile=default/subsystem=webservices/:write-attribute(name=modify-wsdl-address,value=true)**
wsdl-host	Le nom d'hôte / adresse IP à utiliser pour écrire à nouveau **<soap:address>**. Si **wsdl-host** est défini au string **jbossws.undefined.host**, l'hôte du demandeur sera utilisé quand on écrit à nouveau une **<soap:address>**.	**/profile=default/subsystem=webservices/:write-attribute(name=wsdl-host,value=10.1.1.1)**

Élément	Description	Commande CLI
wsdl-port	Entier relatif qui définit explicitement le port HTTP qui sera utilisé pour écrire à nouveau l'adresse SOAP. Si non défini, le port HTTP peut être identifié en cherchant la liste de connecteurs HTTP installés.	**`/profile=default/subsystem=webservices/:write-attribute(name=wsdl-port,value=8080)`**
wsdl-secure-port	Entier relatif qui définit explicitement le port HTTPS qui sera utilisé pour écrire à nouveau l'adresse SOAP. Si non défini, le port HTTPS peut être identifié en cherchant la liste de connecteurs HTTPS installés.	**`/profile=default/subsystem=webservices/:write-attribute(name=wsdl-secure-port,value=8443)`**

Configurations de point de terminaison prédéfinis

Vous pouvez définir des configurations de points de terminaison qui peuvent être référencées par les implémentations de points de terminaison. Une des façons dont cela puisse être utilisé consiste à ajouter un gestionnaire donné à n'importe quel point de terminaison WS, pour lequel il est indiqué une configuration de point de terminaison donnée avec l'annotation **`@org.jboss.ws.api.annotation.EndpointConfig`**.

JBoss EAP 6 inclut une **`Standard-Endpoint-Config`** par défaut. Il existe également une configuration **`Recording-Endpoint-Config`** personnalisée, également incluse. Cela vous donne un exemple de gestionnaire d'enregistrement. La **`Standard-Endpoint-Config`** est utilisée automatiquement pour tout point de terminaison non associé à une autre configuration.

Pour lire la **`Standard-Endpoint-Config`** par le Management CLI, il suffit d'utiliser la commande suivante :

```
/profile=default/subsystem=webservices/endpoint-config=Standard-Endpoint-Config/:read-resource(recursive=true,proxies=false,include-runtime=false,include-defaults=true)
```

Configurations des points de terminaison

La configuration d'un point de terminaison, à laquelle on fait référence ainsi **`endpoint-config`** dans l'API de gestion, inclut **`post-handler-chain`**, **`post-handler-chain`** et quelques propriétés qui sont appliquées à un point de terminaison particulier. Les commandes suivantes lisent et ajoutent un point de config.

Exemple 13.1. Lecture d'une config de point de terminaison

```
/profile=default/subsystem=webservices/endpoint-config=Recording-Endpoint-Config:read-resource
```

Exemple 13.2. Ajout d'une config de point de terminaison

```
/profile=default/subsystem=webservices/endpoint-config=My-Endpoint-
Config:add
```

Chaînes de gestionnaires

Chaque config de point de terminaison peut être associée à des chaînes de gestionnaires **PRE** ou **POST**. Chaque chaîne de gestionnaire peut inclure des gestionnaires conformes à JAXWS. Pour les messages sortants, les gestionnaires de chaînes de gestionnaires PRE sont exécutés avant tout gestionnaire attaché aux points de terminaison, à l'aide de moyens JAXWS standards, comme avec l'annotation **@HandlerChain**. Les gestionnaires de chaînes de POST handler sont exécutés après les gestionnaires de points de terminaison habituels. Pour les messages entrants, c'est l'opposé. JAX-WS est une API standard pour les services basés XML, et est documenté à l'adresse suivante http://jcp.org/en/jsr/detail?id=224.

Une chaîne de gestionnaire peut aussi inclure un attribut **protocol-binding**, qui définit les protocoles qui déclenchent le démarrage de la chaîne.

Exemple 13.3. Lecture d'une chaîne de gestionnaire

```
/profile=default/subsystem=webservices/endpoint-config=Recording-
Endpoint-Config/pre-handler-chain=recording-handlers:read-resource
```

Exemple 13.4. Ajouter un chaîne de gestionnaire

```
/profile=default/subsystem=webservices/endpoint-config=My-Endpoint-
Config/post-handler-chain=my-handlers:add(protocol-
bindings="##SOAP11_HTTP")
```

Gestionnaires

Un gestionnaire JAXWS est un **<gestionnaire>** d'élément dépendant, qui se trouve à l'intérieur d'une chaîne de gestionnaire. Le gestionnaire prend un attribut de **classe** , qui est le nom de classe complet de la classe du gestionnaire. Quand le point de terminaison est déployé, une instance de cette classe sera créée pour chaque déploiement référençant. Le chargeur de classes de déploiement ou le chargeur de classes du module **org.jboss.as.webservices.server.integration** doivent pouvoir charger la classe de gestionnaire.

Exemple 13.5. Lecture d'un gestionnaire

```
/profile=default/subsystem=webservices/endpoint-config=Recording-
Endpoint-Config/pre-handler-chain=recording-
handlers/handler=RecordingHandler:read-resource
```

Exemple 13.6. Ajout d'un gestionnaire

```
/profile=default/subsystem=webservices/endpoint-config=My-Endpoint-
Config/post-handler-chain=my-handlers/handler=foo-
handler:add(class="org.jboss.ws.common.invocation.RecordingServerHandler
")
```

Information de Runtime à propos des Services Web

Vous pouvez afficher des informations d'exécution sur les Services Web, tels que le contexte web et l'URL WSDL, en interrogeant les points de terminaison eux-mêmes. Vous pouvez utiliser le caractère de * pour interroger tous les points de terminaison à la fois. Les deux annotations suivantes montrent la commande pour un serveur dans un domaine géré, puis pour un serveur autonome.

Exemple 13.7. Voir les informations de Runtime sur tous les points de terminaison d'un serveur dans un domaine géré.

Cette commande montre les informations sur tous les points de terminaison sur le serveur nommé **server-one** qui se trouve sur l'hôte physique **master** d'un domaine géré.

```
/host=master/server=server-
one/deployment="*"/subsystem=webservices/endpoint="*":read-resource
```

Exemple 13.8. Voir les informations de Runtime sur tous les points de terminaison d'un serveur dans un domaine autonome

Cette commande montre les informations sur tous les points de terminaison sur le serveur autonome nommé **server-one** qui se trouve sur l'hôte physique nommé **master**.

```
/host=master/server=server-
one/deployment="*"/subsystem=webservices/endpoint="*":read-resource
```

Exemple 13.9. Exemple d'information de point de terminaison

L'exemple suivant est une sortie hypothétique.

```
{
   "outcome" => "success",
   "result" => [{
       "address" => [
           ("deployment" => "jaxws-samples-handlerchain.war"),
           ("subsystem" => "webservices"),
           ("endpoint" => "jaxws-samples-handlerchain:TestService")
       ],
       "outcome" => "success",
       "result" => {
           "class" =>
"org.jboss.test.ws.jaxws.samples.handlerchain.EndpointImpl",
           "context" => "jaxws-samples-handlerchain",
           "name" => "TestService",
           "type" => "JAXWS_JSE",
           "wsdl-url" => "http://localhost:8080/jaxws-samples-
handlerchain?wsdl"
       }
   }]
}
```

Report a bug

13.3. PONTS DE TERMINAISON DE SERVICES WEB JAX-WS

13.3.1. Les points de terminaison de Services Web JAX-WS

Cette section est une vue d'ensemble des points de terminaison de service JAX-WS web et des concepts qui l'accompagnent. Un point de terminaison de Service Web JAX-WS est le composant de serveur d'un Service Web. Les clients et les autres Services Web le communiquent via le protocole HTTP à l'aide d'un langage XML appelé *Simple Object Access Protocol (SOAP)*. Le point de terminaison lui-même est déployé dans le conteneur JBoss EAP 6.

Vous pouvez écrire un descripteur WSDL à la main, ou bien, vous pouvez utiliser des annotations JAX-WS pour le créer automatiquement. C'est la pratique habituelle.

Un bean d'implémentation de point de terminaison est annoté d'annotations JAX-WS et est déployé sur le serveur. Le serveur génère et publie automatiquement le contrat abstrait en format WSDL pour la consommation client. Tous les marshalling et unmarshalling sont délégués au service *Architecture Java pour XML Binding (JAXB)*.

Le point de terminaison peut être un POJO (Plain Old Java Object) ou une Application Web Java EE. Vous pouvez également exposer des points de terminaison à l'aide d'un bean de session stateless EJB3. Il est empaqueté dans un fichier d'Archive Web (WAR). La spécification d'emballage de point de terminaison, appelée *Java Service Endpoint (JSE)* est définie dans JSR-181, qui se trouve dans http://jcp.org/aboutJava/communityprocess/mrel/jsr181/index2.html.

Pré-requis de développement

Un service web doit se conformer aux pré-requis de l'API JAXWS et à la spécification des métadonnées des services web qui se trouvent dans http://www.jcp.org/en/jsr/summary?id=181. Une implémentation valide devra remplir les critères suivants:

- Contenir une annotation **`javax.jws.WebService`**.
- Tous les paramètres de méthode et les types de renvoi doivent être compatibles avec la spécification JAXB 2.0, JSR-222. Voir http://www.jcp.org/en/jsr/summary?id=222 pour plus d'informations.

Exemple 13.10. Exemple de point de terminaison POJO

```
@WebService
@SOAPBinding(style = SOAPBinding.Style.RPC)
public class JSEBean01
{
   @WebMethod
   public String echo(String input)
   {
      ...
   }
}
```

Exemple 13.11. Exemple de point de terminaison de Services Web

```
<web-app ...>
  <servlet>
    <servlet-name>TestService</servlet-name>
    <servlet-
class>org.jboss.test.ws.jaxws.samples.jsr181pojo.JSEBean01</servlet-
class>
  </servlet>
  <servlet-mapping>
    <servlet-name>TestService</servlet-name>
    <url-pattern>/*</url-pattern>
  </servlet-mapping>
</web-app>
```

Exemple 13.12. Exposer un point de terminaison dans un EJB

Le bean de session stateless EJB3 expose la même méthode sur l'interface éloignée et en tant qu'opération de point de terminaison.

```
@Stateless
@Remote(EJB3RemoteInterface.class)
@RemoteBinding(jndiBinding = "/ejb3/EJB3EndpointInterface")

@WebService
@SOAPBinding(style = SOAPBinding.Style.RPC)
public class EJB3Bean01 implements EJB3RemoteInterface
{
   @WebMethod
   public String echo(String input)
   {
      ...
   }
}
```

Fournisseurs de points de terminaison

Les services JAX-WS implémentent généralement une interface de point de terminaison de service Java (SEI), qui peut être mappée à partir d'un type de port WSDL, soit directement ou à l'aide d'annotations. Ce SEI fournit une abstraction de haut niveau qui masque les détails entre les objets Java et leurs représentations XML. Toutefois, dans certains cas, les services doivent pouvoir opérer au niveau du message XML. L'interface de point de terminaison **`Provider`** (fournisseur) fournit cette fonctionnalité aux Services Web qui l'implémentent.

Consommer et accéder au point de terminaison.

Une fois que vous aurez déployé votre Service Web, vous pourrez consommer le WSDL pour créer les stubs de composants qui seront à la base de votre application. Votre application pourra alors accéder au point de terminaison et faire son travail.

Exemples

Les JBoss EAP Quickstarts incluent plusieurs applications JAX-WS Web Services qui fonctionnent correctement. Exemples :

- wsat-simple
- wsba-coordinator-completion-simple
- wsba-participant-completion-simple

Report a bug

13.3.2. Écrire et déployer un point de terminaison de Service Web JAX-WS

Introduction

Cette rubrique décrit le développement d'un simple point de terminaison du service JAX-WS, qui est le composant côté serveur qui répond aux demandes des clients JAX-WS et publie la définition WSDL pour lui-même. Pour plus d'informations sur les points de terminaison de service JAX-WS, consulter Section 13.5.2, « Référence API Commun JAX-WS » et la documentation de l'API en format Javadoc distribuée dans JBoss EAP 6.

Pré-requis de développement

Un service web doit se conformer aux pré-requis de l'API JAXWS et à la spécification des métadonnées des services web qui se trouvent dans http://www.jcp.org/en/jsr/summary?id=181. Une implémentation valide devra remplir les critères suivants :

- Doit contenir l'annotation **`javax.jws.WebService`**.
- Tous les paramètres de méthode et les types de renvoi doivent être compatibles avec la spécification JAXB 2.0, JSR-222. Voir http://www.jcp.org/en/jsr/summary?id=222 pour plus d'informations.

Exemple 13.13. Exemple d'implémentation de service

```
package org.jboss.test.ws.jaxws.samples.retail.profile;

import javax.ejb.Stateless;
import javax.jws.WebService;
import javax.jws.WebMethod;
import javax.jws.soap.SOAPBinding;

@Stateless
@WebService(
   name="ProfileMgmt",
   targetNamespace = "http://org.jboss.ws/samples/retail/profile",
   serviceName = "ProfileMgmtService")
@SOAPBinding(parameterStyle = SOAPBinding.ParameterStyle.BARE)
public class ProfileMgmtBean {

   @WebMethod
   public DiscountResponse getCustomerDiscount(DiscountRequest request)
{
      return new DiscountResponse(request.getCustomer(), 10.00);
   }
}
```

Exemple 13.14. Exemple de charge XML

Ce qui suit est un exemple de classe **DiscountRequest** utilisée par le bean **ProfileMgmtBean** dans l'exemple précédent. Les annotations sont incluses par souci de verbosité. Normalement, les valeurs par défaut JAXB sont raisonnables et n'ont pas besoin d'être spécifiées.

```
package org.jboss.test.ws.jaxws.samples.retail.profile;

import javax.xml.bind.annotation.XmlAccessType;
import javax.xml.bind.annotation.XmlAccessorType;
import javax.xml.bind.annotation.XmlType;

import org.jboss.test.ws.jaxws.samples.retail.Customer;

@XmlAccessorType(XmlAccessType.FIELD)
@XmlType(                                                    (1)
  name = "discountRequest",
  namespace="http://org.jboss.ws/samples/retail/profile",
  propOrder = { "customer" }
)
public class DiscountRequest {

   protected Customer customer;

   public DiscountRequest() {
   }

   public DiscountRequest(Customer customer) {
      this.customer = customer;
   }

   public Customer getCustomer() {
      return customer;
   }

   public void setCustomer(Customer value) {
      this.customer = value;
   }

}
```

Pour les mappages plus complexe possibles, voir la spécification JAXB API à l'adresse suivante https://jaxb.java.net/ pour plus d'information.

Packager votre déploiement

La classe d'implémentation est encapsulée dans un déploiement de **JAR**. Toutes les métadonnées requises pour le déploiement proviennent des annotations qui se trouvent sur la classe d'implémentation et l'interface de point de terminaison de service. Déployer le JAR à l'aide du Management CLI ou de l'Interface de gestion, et le point de terminaison HTTP sera créé automatiquement.

Le listing suivant vous montre un exemple de structure qui convient pour un développement JAR de Service Web EJB.

Exemple 13.15. Exemple de structure JAR pour un déploiement de service web

```
[user@host ~]$ jar -tf jaxws-samples-retail.jar
org/jboss/test/ws/jaxws/samples/retail/profile/DiscountRequest.class
org/jboss/test/ws/jaxws/samples/retail/profile/DiscountResponse.class
org/jboss/test/ws/jaxws/samples/retail/profile/ObjectFactory.class
org/jboss/test/ws/jaxws/samples/retail/profile/ProfileMgmt.class
org/jboss/test/ws/jaxws/samples/retail/profile/ProfileMgmtBean.class
org/jboss/test/ws/jaxws/samples/retail/profile/ProfileMgmtService.class
org/jboss/test/ws/jaxws/samples/retail/profile/package-info.class
```

Report a bug

13.4. CLIENTS DU SERVICE JAX-WS WEB

13.4.1. Consommer et accéder à un Service Web JAX-WS

Après avoir créé un point de terminaison de Service Web, soit manuellement ou à l'aide d'annotations de JAX-WS, vous pouvez accéder à son WSDL, qui peut être utilisé pour créer l'application client de base qui communiquera avec le Service Web. Le processus de génération de code Java de la publication WSDL est appelé consommer le service Web. Cela se produit en deux phases :

1. Créer les artefacts client.
2. Construire un service stub.
3. Accéder au point de terminaison.

Créer les artefacts client

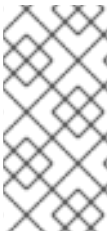
Avant de pouvoir créer des artefacts client, vous devrez créer votre contrat WSDL. Le contrat WSDL suivant est utilisé dans les exemples présentés dans le reste de cette section.

Exemple 13.16. Exemple de contrat WSDL

```
<definitions
    name='ProfileMgmtService'
    targetNamespace='http://org.jboss.ws/samples/retail/profile'
    xmlns='http://schemas.xmlsoap.org/wsdl/'
    xmlns:ns1='http://org.jboss.ws/samples/retail'
    xmlns:soap='http://schemas.xmlsoap.org/wsdl/soap/'
    xmlns:tns='http://org.jboss.ws/samples/retail/profile'
    xmlns:xsd='http://www.w3.org/2001/XMLSchema'>

   <types>

      <xs:schema targetNamespace='http://org.jboss.ws/samples/retail'
                 version='1.0'
xmlns:xs='http://www.w3.org/2001/XMLSchema'>
         <xs:complexType name='customer'>
```

```
            <xs:sequence>
               <xs:element minOccurs='0' name='creditCardDetails'
type='xs:string'/>
               <xs:element minOccurs='0' name='firstName'
type='xs:string'/>
               <xs:element minOccurs='0' name='lastName'
type='xs:string'/>
            </xs:sequence>
         </xs:complexType>
      </xs:schema>

      <xs:schema
          targetNamespace='http://org.jboss.ws/samples/retail/profile'
          version='1.0'
          xmlns:ns1='http://org.jboss.ws/samples/retail'
          xmlns:tns='http://org.jboss.ws/samples/retail/profile'
          xmlns:xs='http://www.w3.org/2001/XMLSchema'>

         <xs:import namespace='http://org.jboss.ws/samples/retail'/>
         <xs:element name='getCustomerDiscount'
                     nillable='true' type='tns:discountRequest'/>
         <xs:element name='getCustomerDiscountResponse'
                     nillable='true' type='tns:discountResponse'/>
         <xs:complexType name='discountRequest'>
            <xs:sequence>
               <xs:element minOccurs='0' name='customer'
type='ns1:customer'/>

            </xs:sequence>
         </xs:complexType>
         <xs:complexType name='discountResponse'>
            <xs:sequence>
               <xs:element minOccurs='0' name='customer'
type='ns1:customer'/>
               <xs:element name='discount' type='xs:double'/>
            </xs:sequence>
         </xs:complexType>
      </xs:schema>

   </types>

   <message name='ProfileMgmt_getCustomerDiscount'>
      <part element='tns:getCustomerDiscount'
name='getCustomerDiscount'/>
   </message>
   <message name='ProfileMgmt_getCustomerDiscountResponse'>
      <part element='tns:getCustomerDiscountResponse'
            name='getCustomerDiscountResponse'/>
   </message>
   <portType name='ProfileMgmt'>
      <operation name='getCustomerDiscount'
                 parameterOrder='getCustomerDiscount'>

         <input message='tns:ProfileMgmt_getCustomerDiscount'/>
         <output
message='tns:ProfileMgmt_getCustomerDiscountResponse'/>
```

```
      </operation>
   </portType>
   <binding name='ProfileMgmtBinding' type='tns:ProfileMgmt'>
      <soap:binding style='document'
                    transport='http://schemas.xmlsoap.org/soap/http'/>
      <operation name='getCustomerDiscount'>
         <soap:operation soapAction=''/>
         <input>

            <soap:body use='literal'/>
         </input>
         <output>
            <soap:body use='literal'/>
         </output>
      </operation>
   </binding>
   <service name='ProfileMgmtService'>
      <port binding='tns:ProfileMgmtBinding' name='ProfileMgmtPort'>

         <soap:address
             location='SERVER:PORT/jaxws-samples-
retail/ProfileMgmtBean'/>
      </port>
   </service>
</definitions>
```



NOTE

Si vous utilisez les annotations de JAX-WS pour créer votre point de terminaison de Service Web, le contrat WSDL sera généré automatiquement, et vous n'aurez seulement besoin que de son URL. Vous pouvez obtenir cet URL dans la section **Webservices** de **Runtime** de la console de gestion sur le web, une fois le point de terminaison déployé.

L'outil **wsconsume.sh** ou **wsconsume.bat** est utilisé pour consommer le contrat abstrait (WSDL) et produire les classes Java annotées et les sources optionnelles qui le définissent. La commande se trouve dans le répertoire ***EAP_HOME*/bin/** de l'installation JBoss EAP 6.

Exemple 13.17. Syntaxe de la commande wsconsume.sh

```
[user@host bin]$ ./wsconsume.sh --help
WSConsumeTask is a cmd line tool that generates portable JAX-WS
artifacts from a WSDL file.

usage: org.jboss.ws.tools.cmd.WSConsume [options] <wsdl-url>

options:
    -h, --help                  Show this help message
    -b, --binding=<file>        One or more JAX-WS or JAXB binding
files
    -k, --keep                  Keep/Generate Java source
    -c  --catalog=<file>        Oasis XML Catalog file for entity
```

```
resolution
    -p  --package=<name>         The target package for generated source
    -w  --wsdlLocation=<loc>     Value to use for
@WebService.wsdlLocation
    -o, --output=<directory>     The directory to put generated artifacts
    -s, --source=<directory>     The directory to put Java source
    -t, --target=<2.0|2.1|2.2>  The JAX-WS specification target
    -q, --quiet                  Be somewhat more quiet
    -v, --verbose                Show full exception stack traces
    -l, --load-consumer          Load the consumer and exit (debug
utility)
    -e, --extension              Enable SOAP 1.2 binding extension
    -a, --additionalHeaders      Enable processing of implicit SOAP
headers
    -n, --nocompile              Do not compile generated sources
```

La commande suivante génère les fichiers source **.java** listés dans la sortie, à partir du fichier **ProfileMgmtService.wsdl**. Les sources utilisent la structure de répertoire du package, qui est spécifié par le commutateur **-p**.

```
[user@host bin]$  wsconsume.sh -k -p
org.jboss.test.ws.jaxws.samples.retail.profile ProfileMgmtService.wsdl
output/org/jboss/test/ws/jaxws/samples/retail/profile/Customer.java
output/org/jboss/test/ws/jaxws/samples/retail/profile/DiscountRequest.java
output/org/jboss/test/ws/jaxws/samples/retail/profile/DiscountResponse.jav
a
output/org/jboss/test/ws/jaxws/samples/retail/profile/ObjectFactory.java
output/org/jboss/test/ws/jaxws/samples/retail/profile/ProfileMgmt.java
output/org/jboss/test/ws/jaxws/samples/retail/profile/ProfileMgmtService.j
ava
output/org/jboss/test/ws/jaxws/samples/retail/profile/package-info.java
output/org/jboss/test/ws/jaxws/samples/retail/profile/Customer.class
output/org/jboss/test/ws/jaxws/samples/retail/profile/DiscountRequest.clas
s
output/org/jboss/test/ws/jaxws/samples/retail/profile/DiscountResponse.cla
ss
output/org/jboss/test/ws/jaxws/samples/retail/profile/ObjectFactory.class
output/org/jboss/test/ws/jaxws/samples/retail/profile/ProfileMgmt.class
output/org/jboss/test/ws/jaxws/samples/retail/profile/ProfileMgmtService.c
lass
output/org/jboss/test/ws/jaxws/samples/retail/profile/package-info.class
```

Les fichiers source **.java** et les fichiers **.class** compilés sont générés dans le répertoire **output/** qui se trouve dans le répertoire où vous exécutez la commande.

Tableau 13.2. Descriptions d'artefacts créés par wsconsume.sh

Fichier	Description
ProfileMgmt.java	Interface de point de terminaison de service.

Fichier	Description
Customer.java	Personnaliser le type de données.
Discount*.java	Personnaliser les types de données.
ObjectFactory.java	Référentiel JAXB XML.
package-info.java	Annotations de package JAXB.
ProfileMgmtService.java	Usine de connexions.

La commande **wsconsume.sh** génère tous les types de données personnalisés (classes JAXB annotées), l'interface de point de terminaison de service et une classe de fabrique de services. Ces artefacts sont utilisés pour créer les implémentations web service clients.

Créer un Service Stub

Les clients de service Web permet d'abstraire les détails d'un appel de service web distant stubs de service. Pour une application cliente, une invocation WS ressemble à une invocation de tout autre composant de l'entreprise. Dans ce cas, l'interface de point de terminaison de service agit comme l'interface de l'entreprise, et une classe de fabrique de service n'est pas utilisée pour sa construction comme une ébauche de service.

Exemple 13.18. Créer un Service Stub et accéder à un point de terminaison

L'exemple suivant crée d'abord une fabrique de services à l'aide de l'emplacement WSDL et le nom du service. Il utilise ensuite l'interface de point de terminaison de service créée par la commande **wsconsume.sh** pour construire le stub de service. Enfin, le stub peut être utilisé comme le serait toute autre interface commerciale.

Vous pouvez trouver l'URL du WSDL de votre point de terminaison dans la Console de gestion sur le web. Choisissez l'élément de menu **Runtime** en haut à gauche, puis l'élément de menu **Déploiements** en bas à gauche. Cliquez sur les **Services Web** et sélectionnez votre déploiement pour afficher ses détails.

```
import javax.xml.ws.Service;
[...]
Service service = Service.create(
new URL("http://example.org/service?wsdl"),
new QName("MyService")
);
ProfileMgmt profileMgmt = service.getPort(ProfileMgmt.class);

// Use the service stub in your application
```

Report a bug

13.4.2. Développer une application client JAX-WS

Cette section traite des clients de Services Web JAX-WS en général. Le client communique avec et réclame une tâche du point de terminaison de JAX-WS, qui est déployé dans le conteneur Java Enterprise Edition 6. Pour obtenir des informations détaillées sur les classes, méthodes et autres détails d'implémentation mentionnés ci-dessous, reportez-vous à Section 13.5.2, « Référence API Commun JAX-WS » et aux sections pertinentes du package Javadocs inclus dans JBoss EAP 6.

Service

Aperçu

Un **`Service`** est une abstraction qui représente un service WSDL. Un service WSDL est une collection de ports liés les uns aux autres, dont chacun comprend un type de port lié à un protocole particulier et une adresse de point de terminaison particulière.

Généralement, le service est créé quand le reste des stubs du composant sont générés à partir d'un contrat WSDL existant. Le contrat WSDL est disponible via l'URL WSDL du point de terminaison déployé, ou peut être créé à partir de la source de point de terminaison à l'aide de la commande **`wsprovide.sh`** dans le répertoire de **`/bin/`** ***`EAP_HOME`***.

On appelle cela une utilisation *statique*. Dans un tel cas, vous créez des instances de la classe **`Service`** , créée elle-même comme un des composants stubs.

Vous pouvez également créer le service manuellement, par la méthode **`Service.create`**. On appelle cela une utilisation *dynamic*.

Utilisation

Cas d'utilisation static

Le cas d'utilisation *statique* pour un client JAX-WS suppose que vous ayez déjà un contrat WSDL. Ceci peut être généré par un outil externe ou généré à l'aide des annotations JAX-WS qui conviennent lorsque vous créez votre point de terminaison de JAX-WS.

Pour générer vos stubs de composants, vous pouvez utiliser le script **`wsconsume.sh`** ou **`wsconsume.bat`** inclus dans ***`EAP_HOME`***`/bin/`. Ce script prend le WSDL URL ou fichier en tant que paramètre, et génère de nombreux fichiers structurés dans un arborescence de répertoires. La source et les fichiers de classe représentant votre **`Service`** s'appellent ***`CLASSNAME`***`_Service.java` et ***`CLASSNAME`***`_Service.class`, respectivement.

La classe d'implémentation générée possède deux constructeurs publics, un sans argument et un avec deux arguments. Les deux arguments représentent respectivement l'emplacement WSDL (un **`java.net.URL`**) et le nom du service (un **`javax.xml.namespace.QName`**).

Le constructeur sans argument est celui qui est le plus souvent utilisé. Dans ce cas, l'emplacement WSDL et le nom du service sont ceux que l'on trouve dans le fichier WSDL. Ceux-ci sont définis implicitement à partir de l'annotation **`@WebServiceClient`** qui décore la classe générée.

Exemple 13.19. Exemple de classe de service générée

```
@WebServiceClient(name="StockQuoteService",
targetNamespace="http://example.com/stocks",
wsdlLocation="http://example.com/stocks.wsdl")
public class StockQuoteService extends javax.xml.ws.Service
{
   public StockQuoteService()
   {
```

```
        super(new URL("http://example.com/stocks.wsdl"), new
QName("http://example.com/stocks", "StockQuoteService"));
    }

    public StockQuoteService(String wsdlLocation, QName serviceName)
    {
        super(wsdlLocation, serviceName);
    }

    ...
}
```

Cas d'utilisation dynamic

Dans un cas d'utilisation dynamic, aucun stub n'est généré automatiquement. Au lieu de cela, le client de service web utilise la méthode **`Service.create`** pour créer des instances de **`Service`**. Le fragment de code suivant illustre ce processus.

Exemple 13.20. Création de service manuellement

```
URL wsdlLocation = new URL("http://example.org/my.wsdl");
QName serviceName = new QName("http://example.org/sample",
"MyService");
Service service = Service.create(wsdlLocation, serviceName);
```

Handler Resolver

JAX-WS fournit un framework plug-in flexible pour des modules de traitement des messages, appelés *gestionnaires*. Ces gestionnaires étendent les fonctionnalités d'un système de runtime JAX-WS. Une instance de **`Service`** donnera accès à un **`HandlerResolver`** grâce à une paire de méthodes **`getHandlerResolver`** et **`setHandlerResolver`** qui peuvent configurer un ensemble de gestionnaires sur la base de service, de port ou de protocole.

Lorsqu'une instance de **`Service`** crée un proxy ou une instance **`Dispatch`**, le Handler Resolver enregistré dans le service crée la chaîne de gestionnaires requise. Les changements ultérieurs apportés au Handler Resolver qui sont configurés pour une instance de **`Service`** n'affectent pas les gestionnaires sur proxies préalablement créés ou les instances de **`Dispatch`**.

Exécuteur

Les instances de **`Service`** peuvent être configurées par un **`java.util.concurrent.Executor`**. **`Executor`** invoque les callbacks asynchrones demandés par l'application. Les méthodes **`setExecutor`** et **`getExecutor`** de **`Service`** peuvent modifier et extraire l' **`Executor`** configuré pour un service.

Proxy dynamique

Un *dynamic proxy* est une instance de proxy de client utilisant une des méthodes **`getPort`** fournie par le **`Service`**. Le **`portName`** indique le nom du port WSDL que le service utilise. La **`serviceEndpointInterface`** indique l'interface du point de terminaison du service prise en charge par l'instance du proxy dynamique créé.

Exemple 13.21. Méthodes getPort

```
public <T> T getPort(QName portName, Class<T> serviceEndpointInterface)
public <T> T getPort(Class<T> serviceEndpointInterface)
```

Le *interface du point de terminaison du service*ou Service Endpoint Interface (SEI) est normalement créé par la commande **wsconsume.sh** qui interprète le WSDL et qui, à partir de cela, crée des classes Java.

Il y a aussi une méthode typée retournant un port qui est fournie. Ces méthodes renvoient également des proxys dynamiques qui implémentent la SEI. Voir les exemples suivants.

Exemple 13.22. Revoie le Port d'un Service

```
@WebServiceClient(name = "TestEndpointService", targetNamespace =
"http://org.jboss.ws/wsref",
   wsdlLocation = "http://localhost.localdomain:8080/jaxws-samples-
webserviceref?wsdl")

public class TestEndpointService extends Service
{
    ...

    public TestEndpointService(URL wsdlLocation, QName serviceName) {
        super(wsdlLocation, serviceName);
    }

    @WebEndpoint(name = "TestEndpointPort")
    public TestEndpoint getTestEndpointPort()
    {
        return (TestEndpoint)super.getPort(TESTENDPOINTPORT,
TestEndpoint.class);
    }
}
```

@WebServiceRef

L'annotation **@WebServiceRef** déclare une référence à un Service Web. Elle suit un modèle de ressource indiqué par l'annotation **javax.annotation.Resource** définie dans http://www.jcp.org/en/jsr/summary?id=250.

Cas d'utilisateur @WebServiceRef

- Vous pouvez l'utiliser pour définir une référence dont le type est une classe de **Service** générée. Dans ce cas, l'élément de valeur et le type font tous deux référence au type de classe de **Service** généré. En outre, si le type de référence peut être déduit grâce au champ ou à la déclaration de méthode à laquelle l'annotation est s'applique, les éléments de type et de valeur peuvent (mais n'y sont pas tenus) avoir la valeur par défaut de **Object.class**. Si le type ne peut pas être déduit, alors l'élément au moins doit être présent, avec une valeur par défaut.

- Vous pouvez l'utiliser pour définir une référence de type SEI. Dans ce cas, l'élément de type peut (mais pas forcément) se présenter avec sa valeur par défaut si le type de référence peut

être déduit de la déclaration de champ ou de méthode annotée. Toutefois, l'élément de valeur doit toujours être présent et faire référence à un type de classe de service généré, qui est un sous-type de **`javax.xml.ws.Service`**. L'élément **`wsdlLocation`**, s'il est présent, substitue les informations d'emplacement WSDL spécifiées dans l'annotation **`@WebService`** de la classe de service générée référencée.

Exemple 13.23. Exemples de `@WebServiceRef`

```
public class EJB3Client implements EJB3Remote
{
   @WebServiceRef
   public TestEndpointService service4;

   @WebServiceRef
   public TestEndpoint port3;
```

Dispatch

Les Services Web XML utilisent des messages XML pour la communication entre le point de terminaison, qui est déployé dans le conteneur Java EE, et tous les clients. Les messages XML utilisent un langage XML appelé *Simple Object Access Protocol (SOAP)*. L'API JAX-WS fournit les mécanismes pour que le point de terminaison et les clients àpuissent chacun être en mesure d'envoyer et de recevoir des messages SOAP et de convertir les messages SOAP en Java et vice versa. Cela s'appelle **`marshalling`** et **`unmarshalling`**.

Dans certains cas, vous devez accéder aux messages SOAP bruts eux-mêmes, plutôt qu'au résultat de la conversion. La classe de **`Dispatch`** fournit cette fonctionnalité. **`Dispatch`** opère dans un des deux modes d'utilisation, qui sont identifiés par l'une des constantes suivantes.

- **`javax.xml.ws.Service.Mode.MESSAGE`** - Ce mode ordonne aux applications clientes de travailler directement avec les structures de message qui sont spécifiques au protocole. Si utilisé avec une liaison de protocole SOAP, une application cliente fonctionne directement avec un message SOAP.
- **`javax.xml.ws.Service.Mode.PAYLOAD`** - ce mode amène le client à travailler avec la charge elle-même. Par exemple, s'il est utilisé avec une liaison de protocole SOAP, une application cliente travaillera alors avec le contenu SOAP plutôt qu'avec l'intégralité du message SOAP.

`Dispatch` est une API de bas niveau qui exige des clients de structurer les messages ou les charges en XML, avec une adhérence stricte aux normes du protocole individuel et une connaissance approfondie de la structure de message ou de la charge. **`Dispatch`** est une classe générique qui prend en charge l'entrée et la sortie des messages ou des charges de message de n'importe quel type.

Exemple 13.24. `Dispatch` Usage

```
Service service = Service.create(wsdlURL, serviceName);
Dispatch dispatch = service.createDispatch(portName, StreamSource.class,
Mode.PAYLOAD);

String payload = "<ns1:ping
xmlns:ns1='http://oneway.samples.jaxws.ws.test.jboss.org/'/>";
dispatch.invokeOneWay(new StreamSource(new StringReader(payload)));
```

```
payload = "<ns1:feedback
xmlns:ns1='http://oneway.samples.jaxws.ws.test.jboss.org/'/>";
Source retObj = (Source)dispatch.invoke(new StreamSource(new
StringReader(payload)));
```

Invocations asynchrones

L'interface **`BindingProvider`** représente un composant qui fournit une liaison de protocole que les clients peuvent utiliser. Elle est implémentée et étendue par l'interface **`Dispatch`**.

Les instances de **`BindingProvider`** peuvent fournir des possibilités d'opérations asynchrones. Comme les opérations asynchrones, les invocations sont découplées de l'instance **`BindingProvider`** au moment de l'invocation. Le contexte de réponse n'est pas mis à jour lorsque l'opération est terminée. Au lieu de cela, un contexte de réponse distinct est mis à disposition à l'aide de l'interface de **réponse**.

Exemple 13.25. Invocation asynchrone

```
public void testInvokeAsync() throws Exception
{
   URL wsdlURL = new URL("http://" + getServerHost() + ":8080/jaxws-
samples-asynchronous?wsdl");
   QName serviceName = new QName(targetNS, "TestEndpointService");
   Service service = Service.create(wsdlURL, serviceName);
   TestEndpoint port = service.getPort(TestEndpoint.class);
   Response response = port.echoAsync("Async");
   // access future
   String retStr = (String) response.get();
   assertEquals("Async", retStr);
}
```

Invocations @Oneway

L'annotation **@Oneway** indique que la méthode web donnée ne prend un message d'entrée mais ne renvoie aucun message de sortie. Habituellement, une méthode **@Oneway** renvoie le thread de contrôle à l'application appelante avant l'exécution de la méthode commerciale.

Exemple 13.26. Exemple d'invocation @Oneway

```
@WebService (name="PingEndpoint")
@SOAPBinding(style = SOAPBinding.Style.RPC)
public class PingEndpointImpl
{
   private static String feedback;

   @WebMethod
   @Oneway
   public void ping()
   {
      log.info("ping");
      feedback = "ok";
   }
```

```
    @WebMethod
    public String feedback()
    {
       log.info("feedback");
       return feedback;
    }
}
```

Configuration du timeout

Il y a deux propriétés qui contrôlent le comportement du délai d'expiration de la connexion HTTP et le délai d'attente d'un client qui attend de recevoir un message. Le premier est **`javax.xml.ws.client.connectionTimeout`** et le second est **`javax.xml.ws.client.receiveTimeout`**. Chacun est exprimé en millisecondes, et la syntaxe correcte est indiquée ci-dessous.

Exemple 13.27. Configuration de timeout JAX-WS

```
public void testConfigureTimeout() throws Exception
{
   //Set timeout until a connection is established

((BindingProvider)port).getRequestContext().put("javax.xml.ws.client.con
nectionTimeout", "6000");

   //Set timeout until the response is received
   ((BindingProvider)
port).getRequestContext().put("javax.xml.ws.client.receiveTimeout",
"1000");

   port.echo("testTimeout");
}
```

Report a bug

13.5. RÉFÉRENCE DE DÉVELOPPEMENT JAX-WS

13.5.1. Activation de WS-Addressing (Web Services Addressing)

Prérequis

- Votre application doit posséder un service JAX-WS et une configuration client.

Procédure 13.1. Annoter et mettre à jour le code client

1. **Annoter le point de terminaison du service**
   Ajouter l'annotation **`@Addressing`** au code du point de terminaison de l'application.

   Exemple 13.28. annotation `@Addressing`

Cet exemple montre un point de terminaison normal avec l'ajout de l'annotation **@Addressing**.

```
package org.jboss.test.ws.jaxws.samples.wsa;

import javax.jws.WebService;
import javax.xml.ws.soap.Addressing;

@WebService
(
   portName = "AddressingServicePort",
   serviceName = "AddressingService",
   wsdlLocation = "WEB-INF/wsdl/AddressingService.wsdl",
   targetNamespace = "http://www.jboss.org/jbossws/ws-
extensions/wsaddressing",
   endpointInterface =
"org.jboss.test.ws.jaxws.samples.wsa.ServiceIface"
)
@Addressing(enabled=true, required=true)
public class ServiceImpl implements ServiceIface
{
   public String sayHello()
   {
      return "Hello World!";
   }
}
```

2. **Mise à jour du code client**
   Mettez à jour le code client dans l'application pour configurer WS-Addressing.

Exemple 13.29. La configuration client pour WS-Addressing

Cet exemple montre un client JAX-WS mis à jour pour configurer WS-Addressing.

```
package org.jboss.test.ws.jaxws.samples.wsa;

import java.net.URL;
import javax.xml.namespace.QName;
import javax.xml.ws.Service;
import javax.xml.ws.soap.AddressingFeature;

public final class AddressingTestCase
{
   private final String serviceURL =
       "http://localhost:8080/jaxws-samples-
wsa/AddressingService";

   public static void main(String[] args) throws Exception
   {
      // construct proxy
      QName serviceName =
          new QName("http://www.jboss.org/jbossws/ws-
extensions/wsaddressing",
                    "AddressingService");
```

```
        URL wsdlURL = new URL(serviceURL + "?wsdl");
        Service service = Service.create(wsdlURL, serviceName);
        ServiceIface proxy =
            (ServiceIface)service.getPort(ServiceIface.class,
                                          new
AddressingFeature());
        // invoke method
        proxy.sayHello();
    }
}
```

Résultat

Le client et le point de terminaison communiquent maintenant avec WS-Addressing.

Report a bug

13.5.2. Référence API Commun JAX-WS

Plusieurs concepts de développement de JAX-WS sont partagés entre les clients et les points de terminaison de Service Web. Incluent le framework de gestionnaires, le contexte du message et la gestion des erreurs.

Framework de gestionnaires

Le framework de gestionnaires est implémenté par une liaison de protocole de JAX-WS dans le runtime du client et le point de terminaison, qui est le composant de serveur. Les proxies et les instances **`Dispatch`**, connus collectivement en tant que *fournisseurs de liaison*, chacun utilisant des liaisons de protocole pour lier leur fonctionnalité abstraite à des protocoles spécifiques.

Les gestionnaires côté client et côté serveur sont organisés en une liste ordonnée, connue sous le nom de *chaîne de gestionnaire*. Les gestionnaires au sein d'une chaîne de gestionnaires sont appelés à chaque fois qu'un message est envoyé ou reçu. Les messages entrants sont traités par des gestionnaires avant que le fournisseur de liaison les traite. Les messages sortants sont traités par les gestionnaires après que le fournisseur de liaison les aient traités.

Les gestionnaires sont invoqués avec un contexte de message qui fournit des méthodes pour accéder et modifier les messages entrants et sortants et gérer un ensemble de propriétés. Les propriétés de contexte de message facilitent la communication entre des gestionnaires individuels, ainsi qu'entre les gestionnaires, les clients et les implémentations de services. Différents types de gestionnaires sont invoqués avec différents types de contextes de messages.

Types de gestionnaires de messages

Gestionnaire logique

Les *gestionnaires logiques* n'opèrent que sur des propriétés de contexte de messages et sur des charges utiles de messages. Les gestionnaires logiques sont libérés des protocoles et ne peuvent pas affecter les parties d'un message qui soient spécifiques à un protocole. Les gestionnaires logiques implémentent l'interface **`javax.xml.ws.handler.LogicalHandler`**.

Gestionnaire de protocoles

Les *gestionnaires de protocoles* fonctionnent sur les propriétés de contexte de message et les messages de protocole spécifique. Les gestionnaires de protocoles sont spécifiques à un protocole particulier et peuvent accéder et modifier les aspects spécifiques d'un protocole de message. Les

gestionnaires de protocoles implémentent une interface dérivée de **`javax.xml.ws.handler.Handler except javax.xml.ws.handler.LogicalHandler`**.

Gestionnaire de points de terminaison

Sur un point de terminaison de service, les gestionnaires sont définis à l'aide de l'annotation **`@HandlerChain`**. L'emplacement du fichier de chaîne de gestionnaires peut être soit un **`java.net.URL`** absolu dans **`externalForm`** ou un chemin d'accès relatif du fichier source ou du fichier de classe.

Exemple 13.30. Exemple de gestionnaire de points de terminaison

```
@WebService
@HandlerChain(file = "jaxws-server-source-handlers.xml")
public class SOAPEndpointSourceImpl
{
   ...
}
```

Service Client Handler

Sur un client JAX-WS, les gestionnaires sont définis soit en utilisant l'annotation **`@HandlerChain`**, comme dans les points de terminaison de service, soit de façon dynamique, à l'aide de l'API JAX-WS.

Exemple 13.31. Définir un Service Client Handler par une API

```
Service service = Service.create(wsdlURL, serviceName);
Endpoint port = (Endpoint)service.getPort(Endpoint.class);

BindingProvider bindingProvider = (BindingProvider)port;
List<Handler> handlerChain = new ArrayList<Handler>();
handlerChain.add(new LogHandler());
handlerChain.add(new AuthorizationHandler());
handlerChain.add(new RoutingHandler());
bindingProvider.getBinding().setHandlerChain(handlerChain);
```

L'appel à la méthode **`setHandlerChain`** est requis.

Contexte du message

L'interface **`MessageContext`** est une super interface pour tous les contextes de message JAX-WS. Elle étend **`Map <String,Object>`** de méthodes et des constantes supplémentaires pour gérer un ensemble de propriétés qui permettent aux gestionnaires d'une chaîne de gestionnaires de partager l'état connexe de traitement. Par exemple, un gestionnaire peut utiliser la méthode **`put`** pour insérer une propriété dans le contexte du message. Un ou plusieurs autres gestionnaires de la chaîne de gestionnaires peuvent obtenir par la suite le message via la méthode **`get`**.

Les propriétés sont catégorisées soient comme **`APPLICATION`** ou **`GESTIONNAIRE`**. Toutes les propriétés sont disponibles pour tous les gestionnaires d'une instance d'un *modèle d'échange de*

messages ou MEP (de l'anglais Message Exchange Pattern) d'un point de terminaison particulier. Par exemple, si un gestionnaire logique met une propriété dans le contexte du message, cette propriété sera également disponible à tous les gestionnaires de protocole dans la chaîne au cours de l'exécution d'une instance MEP.

NOTE

Un modèle d'échanges de messages asynchrone (MEP) permet d'envoyer et de recevoir des messages de façon asynchrone au niveau de la connexion HTTP. Vous pouvez l'activer en définissant des propriétés supplémentaires dans le contexte de la demande.

Les propriétés catégorisées en tant qu' **`APPLICATION`** sont également rendues disponibles en tant qu'applications clients et implémentations de point de terminaison de services. Le **`defaultscope`** d'un propriété est **`HANDLER`** par défaut.

Les messages logiques et SOAP utilisent des contextes différents.

Contexte de message logique

Lorsque les gestionnaires logiques sont invoqués, ils reçoivent un contexte de message de type **`LogicalMessageContext`**. Le **`LogicalMessageContext`** étend **`MessageContext`** par des méthodes qui récupèrent et modifient la charge du message. Il ne donne pas accès aux aspects spécifiques au protocole d'un message. Une liaison de protocole définit quels composants d'un message sont disponibles via un contexte logique message. Un gestionnaire logique déployé dans une liaison SOAP peut accéder au contenu du corps SOAP, mais pas aux en-têtes SOAP. En revanche, la liaison XML/HTTP définit qu'un gestionnaire de logique accède à l'entière charge XML d'un message.

Contexte de message SOAP

Quand les gestionnaires SOAP sont invoqués, ils reçoivent un **`SOAPMessageContext`**. Le **`SOAPMessageContext`** étend **`MessageContext`** par des méthodes qui obtiennent et modifient la charge du message SOAP.

Gestion des fautes

Une application peut lever une **`SOAPFaultException`** ou une exception spécifique à l'application utilisateur. Dans ce dernier cas, les wrapper beans de faute requis seront générés en cours d'exécution s'ils ne font pas déjà partie du déploiement.

Exemple 13.32. Exemple de gestion des fautes

```
public void throwSoapFaultException()
{
   SOAPFactory factory = SOAPFactory.newInstance();
   SOAPFault fault = factory.createFault("this is a fault string!", new
QName("http://foo", "FooCode"));
   fault.setFaultActor("mr.actor");
   fault.addDetail().addChildElement("test");
   throw new SOAPFaultException(fault);
}
```

```
public void throwApplicationException() throws UserException
{
   throw new UserException("validation", 123, "Some validation error");
```

```
}
```

Annotations JAX-WS

Les annotations disponibles via JAX-WS API sont définies dans JSR-224, que l'on peut trouver à l'adresse suivante http://www.jcp.org/en/jsr/detail?id=224. Ces annotations sont dans le package `javax.xml.ws`.

Les annotations disponibles via JWS API sont définies dans JSR-181, que l'on peut trouver à l'adresse suivante http://www.jcp.org/en/jsr/detail?id=181. Ces annotations sont dans le package `javax.jws`.

Report a bug

CHAPITRE 14. IDENTITÉ AU SEIN D'APPLICATIONS

14.1. CONCEPTS DE BASE

14.1.1. Chiffrement

Le *chiffrement* désigne le brouillage des informations sensibles en appliquant des algorithmes mathématiques. Le chiffrement est une des fondations de la sécurisation de votre infrastructure pour les violations de données, les pannes de système et autres risques.

Le chiffrement peut être appliqué aux données de chaînes simples, comme les mots de passe. Il peut également être appliqué aux flux de communication de données. Le protocole HTTPS, par exemple, crypte toutes les données en en transférant une partie à une autre. Si vous vous connectez d'un serveur à un autre en utilisant le protocole Secure Shell (SSH), l'ensemble de votre communication sera envoyée vers un *tunnel* crypté.

Report a bug

14.1.2. Les domaines de sécurité

Les domaines de sécurité font partie du sous-système de sécurité JBoss EAP. La configuration de la sécurité est désormais gérée de façon centralisée, ou par le contrôleur de domaines d'un domaine géré ou par le serveur autonome.

Un domaine de sécurité se compose de configurations d'authentification, d'autorisation, de mappage de sécurité et d'audit. Il met en place la sécurité déclarative *Java Authentication and Authorization Service (JAAS).*

L'authentification est impliquée dans la vérification de l'identité d'un utilisateur. Dans la terminologie de la sécurité, cet utilisateur est appelé un *principal*. Bien que l'authentification et l'autorisation soient différentes, de nombreux modules d'authentification intégrés gèrent également l'autorisation.

Une *authorization* est une police de sécurité par laquelle le serveur détermine si un utilisateur authentifié a la permission d'accéder à des privilèges ou ressources particulières dans le système ou opération. Dans la terminologie de sécurité, on parle de « role ».

Security mapping se rapporte à la possibilité d'ajouter, de modifier ou de supprimer des informations d'un principal, rôle ou attribut avant de passer les informations à votre application.

L'Auditing Manager vous permet de configurer les *provider modules* pour contrôler la façon dont les événements de sécurité sont rapportés.

Si vous utilisez des domaines de sécurité, vous pouvez supprimer toutes les configurations de sécurité spécifiques à votre application proprement dite. Cela permet de modifier les paramètres de sécurité de façon centralisée. Un scénario courant qui bénéficie de ce type de structure de configuration est le processus de déplacement des applications entre les environnements de test et de production.

Report a bug

14.1.3. Cryptage SSL

SSL (Secure Sockets Layer) crypte le trafic réseau entre deux systèmes. Le trafic entre les deux systèmes est crypté à l'aide d'une clé bidirectionnelle, générée au cours de la phase de connexion de protocole de *transfert,* qui n'est connu que par ces deux systèmes.

Pour établir un échange sécurisé de la clé de cryptage bidirectionnelle, SSL utilise PKI (Public Key Infrastructure), une méthode de cryptage qui utilise une *paire de clés*. Une paire de clés est composée de deux clés cryptographiques distinctes, mais correspondantes - une clé publique et une clé privée. La clé publique est partagée avec les autres et est utilisée pour crypter les données et la clé privée est tenue secrète et est utilisée pour déchiffrer des données qui ont été chiffrées à l'aide de la clé publique.

Lorsqu'un client demande une connexion sécurisée, une phase de protocole de transfert a lieu avant que la communication sécurisée puisse commencer. Pendant la négociation SSL, le serveur transmet sa clé publique au client sous la forme d'un certificat. Le certificat contient l'identité du serveur (son URL), la clé publique du serveur et une signature numérique valide le certificat. Ensuite, le client valide le certificat et prend une décision quant à savoir si le certificat doit être approuvé ou non. Si le certificat est approuvé, le client génère la clé de cryptage bidirectionnel pour la connexion SSL, la chiffre à l'aide de la clé publique du serveur et la renvoie sur le serveur. Le serveur décrypte la clé de cryptage bidirectionnel à l'aide de sa clé privée, et ensuite, la communication entre les deux machines est cryptée via cette connexion par la clé de cryptage bidirectionnel.

Report a bug

14.1.4. Sécurité déclarative

La *sécurité déclarative* est une méthode de séparation des problèmes de sécurité du code d'application, en utilisant le conteneur pour gérer la sécurité. Le conteneur procure un système d'autorisation basé soit sur les permissions de fichiers ou basé utilisateur, groupe ou rôle. Cette approche est normalement supérieure à la sécurité *programmatique*, qui donne à l'application toutes les responsabilités pour la sécurité.

La plate-forme JBoss EAP 6 fournit une sécurité déclarative par les domaines de sécurité.

Report a bug

14.2. SÉCURITÉ BASÉE-RÔLE POUR LES APPLICATIONS

14.2.1. La sécurité des applications

Pour chaque développeur d'applications, sécuriser vos applications est une tâche importante et couvrant des aspects multiples. JBoss EAP 6 vous donne tous les outils dont vous aurez besoin pour rédiger des applications sécurisées, y compris les possibilités suivantes :

- Section 14.2.2, « Authentification »
- Section 14.2.3, « L'autorisation »
- Section 14.2.4, « Security Auditing »
- Section 14.2.5, « Security Mapping »
- Section 14.1.4, « Sécurité déclarative »
- Section 14.4.2.1, « Permissions de méthodes EJB »
- Section 14.4.3.1, « Les annotations de sécurité EJB »

Voir également Section 14.2.9, « Utiliser un domaine de sécurité dans votre application » .

Report a bug

14.2.2. Authentification

L'authentification consiste à identifier un sujet et à vérifier l'authenticité de l'identification. Le mécanisme d'authentification le plus commun est une combinaison de nom d'utilisateur et de mot de passe. D'autres mécanismes d'authentification communs utilisent des clés partagées, des smart cards (cartes à puce) ou des empreintes digitales. Le résultat d'une authentification réussie s'appelle un Principal, en termes de sécurité déclarative Java Enterprise Edition.

JBoss EAP utilise un système pouvant se connecter à des modules d'authentification en vue de flexibilité et d'intégration avec les systèmes d'authentification que vous utilisez dans votre organisation. Chaque domaine de sécurité contient un ou plusieurs modules d'authentification configurés. Chaque module comprend des paramètres de configuration supplémentaires pour personnaliser son comportement. Le plus simple consiste à configurer le sous-système d'authentification dans la console de gestion web.

L'authentification n'est pas la même chose que l'autorisation, même si elles sont souvent liées. Bon nombre des modules d'authentification intégrés peuvent également gérer des autorisations.

Report a bug

14.2.3. L'autorisation

L'autorisation est un mécanisme d'octroi ou de refus de permission d'accéder à une ressource, basé sur l'identité. Ce mécanisme est implémenté sous forme de rôles de sécurité déclarative, qui peuvent être donnés à des principaux.

JBoss EAP utilise un système modulaire pour configurer l'autorisation. Chaque domaine de sécurité peut contenir une ou plusieurs stratégies d'autorisation. Chaque stratégie possède un module de base qui définit son comportement. Il est configuré via les attributs et indicateurs spécifiques. La façon la plus simple consiste à configurer le sous-système de l'autorisation à l'aide de la console de gestion basée web.

L'authentification est différente de l'autorisation, et a lieu, en général, après l'authentification. La plupart des modules d'authentification gèrent également l'autorisation.

Report a bug

14.2.4. Security Auditing

Security Auditing se réfère au déclenchement d'événements, comme écrire un blog en réponse à un événement qui a lieu dans le sous-système de sécurité. Les mécanismes de sécurité sont configurés dans le cadre du domaine de sécurité, avec les informations d'authentification, d'autorisation ou de mappage de sécurité.

Auditing utilise *des modules de fournisseur.* Vous pouvez en utiliser un existant ou bien créer le vôtre.

Report a bug

14.2.5. Security Mapping

Le mappage de sécurité vous permet de combiner l'authentification et l'autorisation d'informations après que l'authentification ou l'autorisation aient eu lieu, mais avant que l'information ait été passée à votre application. Un exemple qui l'illustre est l'utilisation d'un certificat X509 pour l'authentification, puis la conversion du principal du certificat en nom logique que votre application puisse afficher.

Vous pouvez mapper vos principaux (authentification), rôles (autorisation), ou identifiants (attributs qui ne sont ni principaux, ni rôles).

Le mappage de rôles est utilisé pour ajouter, remplacer ou supprimer des rôles du sujet après l'authentification.

Le mappage du principal est utilisé pour modifier un principal après l'authentification.

Le mappage d'attributs est utilisé pour convertir des attributs d'un système externe à utiliser par votre application, et vice versa.

Report a bug

14.2.6. Security Extension Architecture

L'architecture des extensions de sécurité de la plateforme JBoss EAP se compose de trois parties. Ces trois parties connectent votre application à votre infrastructure de sécurité sous-jacente, que ce soit LDAP, Kerberos ou un autre système externe.

JAAS

La première partie de l'infrastructure est l'API JAAS. JAAS est un framework additionnel qui procure une couche d'abstraction entre l'infrastructure de sécurité et votre application.

L'implémentation JAAS est **`org.jboss.security.plugins.JaasSecurityManager`**, qui implémente les interfaces **`AuthenticationManager`** et **`RealmMapping`**. **`JaasSecurityManager`** s'intègre dans les couches de conteneur EJB et web, basées sur l'élément **`<security-domain>`** du descripteur de déploiement du composant correspondant.

Pour plus d'information sur JAAS, voir Section 14.2.7, « Java Authentication et Authorization Service (JAAS) ».

Le MBean `JaasSecurityManagerService`

Le service MBean **`JaasSecurityManagerService`** s'occupe des gestionnaires de la sécurité. Bien que son nom commence par Jaas, les gestionnaires de sécurité qu'il gère n'ont pas besoin pas d'utiliser JAAS dans leur implémentation. Le nom reflète le fait que l'implémentation de gestionnaire de sécurité par défaut est le **`JaasSecurityManager`**

Le rôle principal du **`JaasSecurityManagerService`** est d'externaliser la mise en œuvre du gestionnaire de sécurité. Vous pouvez modifier la mise en œuvre du gestionnaire de sécurité en fournissant une implémentation alternative des interfaces **`AuthenticationManager`** et **`RealmMapping`**.

Le deuxième rôle fondamental de **`JaasSecurityManagerService`** est de fournir une implémentation **`javax.naming.spi.ObjectFactory`** JNDI pour permettre une gestion simple de la liaison dépourvue de code entre le nom JNDI et l'implémentation du gestionnaire de sécurité, sans code. Pour activer la sécurité, spécifiez le nom JNDI de l'implémentation du gestionnaire de sécurité par l'intermédiaire de l'élément de descripteur de déploiement **`<security-domain>`**.

Quand vous spécifiez un nom JNDI, un object-binding doit déjà être présent. Pour simplifier l'installation de la liaison entre le nom JNDI et le gestionnaire de sécurité, le service **`JaasSecurityManagerService`** relie un *next naming system reference*, qui se nomme lui-même comme **`ObjectFactory`** JNDI sous le nom **`java:/jaas`**. Cela permet à une convention de nommage de la forme **`java:/jaas/`*`XYZ`*** à correspondre à la valeur de l'élément **`<security-domain>`**, et l'instance du gestionnaire de sécurité du domaine de sécurité ***`XYZ`*** sera créée selon les besoins, en créant une instance de la classe spécifiée par l'attribut **`SecurityManagerClassName`** par

l'intermédiaire d'un constructeur qui prendra le nom du domaine de sécurité.

NOTE

Vous n'avez pas besoin d'ajouter le préfixe **`java:/jaas`** à votre descripteur de déploiement. Vous pouvez le faire, pour les raisons de compatibilité rétroactive, mais ce sera ignoré.

JaasSecurityDomain MBean

`org.jboss.security.plugins.JaasSecurityDomain` est une extension de **`JaasSecurityManager`**, qui ajoute la notion de **`KeyStore`**, de **`KeyManagerFactory`** et de **`TrustManagerFactory`** pour SSL et autres cas d'utilisation cryptographique.

Pour plus d'informations

Pour plus d'informations, et pour obtenir des exemples pratiques de l'architecture de sécurité en action, voir Section 14.2.8, « Java Authentication et Authorization Service (JAAS) » .

Report a bug

14.2.7. Java Authentication et Authorization Service (JAAS)

*Java Authentication and Authorization Service (JAAS)*est une API de sécurité qui consiste en un ensemble de packages Java conçus pour l'autorisation et l'authentification des utilisateurs. L'API est une implémentation Java du framework standard PAM (de l'anglais Pluggable Authentication Modules). Il étend l'architecture de contrôle d'accès de Java Enterprise Edition pour approuver l'autorisation basée utilisateur.

Dans JBoss EAP 6, JAAS ne fournit qu'une sécurité déclarative basée rôle. Pour plus d'informations sur le sécurité déclarative, voir Section 14.1.4, « Sécurité déclarative ».

JAAS est indépendant de toute technologie d'authentification sous-jacente, comme Kerberos ou LDAP. Vous pouvez modifier votre structure de sécurité sous-jacente sans modifier votre application. Vous devez uniquement modifier la configuration JAAS.

Report a bug

14.2.8. Java Authentication et Authorization Service (JAAS)

L'architecture de sécurité de JBoss EAP 6 comprend le sous-système de configuration de sécurité, des configurations de sécurité propres aux applications qui sont incluses dans plusieurs fichiers de configuration de l'application et le gestionnaire de sécurité JAAS, qui est implémenté comme un MBean.

Domaine, Groupe serveur et Configuration spécifique au serveur

Les groupes de serveurs (dans un domaine géré) et les serveurs (dans un serveur autonome) comprennent la configuration des domaines de la sécurité. Un domaine de sécurité comprend des informations sur une combinaison d'authentification, autorisation, mapping et modules, avec détails de configuration. Une application spécifie quel domaine de sécurité est exigé, par son nom, dans son fichier **`jboss-web.xml`**.

Configuration spécifique à une application

Une configuration spécifique à une application a lieu dans un ou plusieurs fichiers.

Tableau 14.1. Fichiers de configuration spécifique à une application

Fichier	Description
ejb-jar.xml	Le descripteur de déploiement pour une application Enterprise JavaBeans (EJB), situé dans le répertoire **`META-INF`** de l'EJB. Utiliser le fichier **`ejb-jar.xml`** pour préciser les rôles et les mapper aux principaux, au niveau de l'application. Vous pouvez également limiter certaines méthodes et classes spécifiques à certains rôles. Également utilisé pour les autres configurations EJB spécifiques non liées à la sécurité.
web.xml	Le descripteur de déploiement pour une application web en Java Enterprise Edition (EE). Utilisez le fichier **`web.xml`** pour déclarer le domaine de sécurité que l'application utilise pour l'authentification et l'autorisation, ainsi que les contraintes de transport et ressources, comme limiter les types de demandes HTTP autorisées. Vous pouvez également configurer l'authentification basée-web dans ce fichier. Utilisé également pour d'autre configurations spécifiques à l'application non liées à la sécurité.
jboss-ejb3.xml	Contient des extensions au descripteur **`ejb-jar.xml`** spécifiques à JBoss.
jboss-web.xml	Contient des extensions au descripteur **`web.xml`** spécifiques à JBoss.

NOTE

Les fichiers **`ejb-jar.xml`** et **`web.xml`** sont définis dans la spécification Java Enterprise Edition (Java EE). Le fichier **`jboss-ejb3.xml`** fournit des extensions spécifiques à JBoss pour le fichier **`ejb-jar.xml`**, et le fichier **`jboss-web.xml`** fournit des extensions spécifiques à JBoss pour le fichier **`web.xml`**.

JAAS Security Manager MBean

*Java Authentication and Authorization Service (JAAS)*est un cadre de sécurité au niveau utilisateur pour les applications Java, utilisant des modules d'authentification enfichables (PAM). Il est intégré dans le Java Runtime Environment (JRE). Dans JBoss EAP 6, le composant côté conteneur est le MBean **`org.jboss.security.plugins.JaasSecurityManager`**. Il fournit les implémentations par défaut des interfaces **`AuthenticationManager`** et **`RealmMapping`**.

JaasSecurityManager MBean s'intègre dans EJB et dans les couches de conteneur web basées sur le domaine de sécurité spécifié dans EJB ou dans les fichiers de descripteur de déploiement de l'application. Lorsqu'une application se déploie, le conteneur associe le domaine de sécurité spécifié dans le descripteur de déploiement avec l'instance de gestionnaire de sécurité du conteneur. Le gestionnaire de sécurité applique la configuration du domaine de sécurité telle qu'elle est configurée sur le serveur de groupe ou autonome.

Flux des interactions entre le Client et le Conteneur dans JAAS

JaasSecurityManager utilise les packages JAAS pour implémenter le comportement d'interface

AuthenticationManager et RealmMapping. En particulier, son comportement découle de l'exécution des instances de modules de connexion qui sont configurées dans le domaine de sécurité assigné au JaasSecurityManager. Les modules de connexion implémentent l'authentification principale du domaine de sécurité et le comportement de mappage de rôle. Vous pouvez utiliser le JaasSecurityManager à travers tous les domaines de la sécurité en assignant des configurations de modules de connexion différentes pour les domaines.

Pour montrer comment le JaasSecurityManager utilise le processus d'authentification JAAS, les étapes suivantes vont indiquer une méthode d'invocation du client qui implémente la méthode **`EJBHome`**. L'EJB a déjà été déployé dans le serveur et ses méthodes d'interface **`EJBHome`** ont déjà été sécurisées par les éléments <method-permission> qui se trouvent dans le descripteur **`ejb-jar.xml`**. Utilise le domaine de sécurité **`jwdomain`**, qui est indiqué dans l'élément <security-domain> du fichier **`jboss-ejb3.xml`**. L'image ci-dessous indique les étapes qui seront expliquées par la suite.

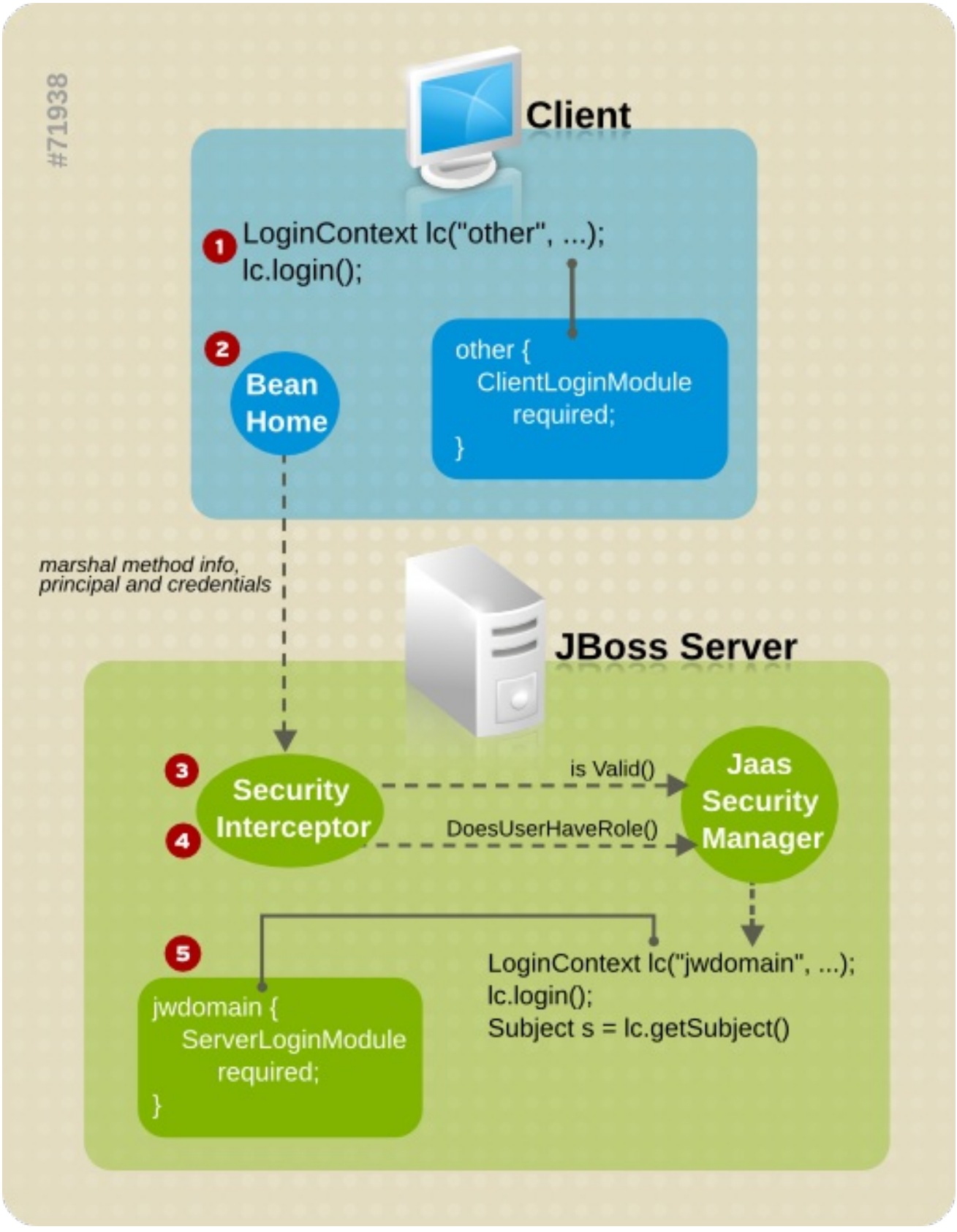


Figure 14.1. Étapes d'une invocation de méthode EJB sécurisée

1. Le client effectue une connexion JAAS pour établir le principal et les informations d'identification pour l'authentification. Correspond à **`Client Side Login`** dans le schéma. Peut être exécuté via JNDI.

   Pour effectuer une connexion JAAS, vous devez créer une instance de LoginContext et y indiquer le nom de la configuration à utiliser. Ici, le nom de configuration est **`other`**. Cette connexion unique associe la connexion principale et les informations d'identification à toutes

les invocations de méthode EJB. Le processus n'authentifie pas forcément l'utilisateur. La nature de la connexion côté client dépend de la configuration du module de connexion que le client utilise. Dans cet exemple, l'entrée de configuration **other** côté client utilise le module de connexion **ClientLoginModule**. Ce module lie le nom d'utilisateur et le mot de passe à la couche d'invocation EJB pour une authentification ultérieure sur le serveur. L'identité du client n'est pas authentifiée sur le client.

2. Le client obtient la méthode **EJBHome** et l'invoque sur le serveur. L'invocation inclut les arguments de la méthode adoptée par le client, ainsi que l'identité de l'utilisateur et les informations d'identification de la connexion JAAS de côté client.

3. Sur le serveur, l'intercepteur de sécurité authentifie l'utilisateur qui a invoqué la méthode. Cela nécessite une autre connexion JAAS.

4. Le domaine de sécurité ci-dessous détermine le choix des modules de connexion. Le nom du domaine de sécurité est passé au constructeur **LoginContext** en tant que nom de configuration de la connexion. Le domaine de sécurité des EJB est **jwdomain**. Si l'authentification JAAS est réussie, un sujet JAAS sera créé. Un sujet JAAS comprend un PrincipalSet avec les détails suivants :

    - Une instance **java.security.Principal** qui correspond à l'identité du client en provenance de l'environnement de sécurité du déploiement.

    - Un groupe **java.security.acl.Group** appelé **Roles**, qui contient les noms de rôles du domaine d'application de l'utilisateur. Les objets de type **org.jboss.security.SimplePrincipal** représentent les noms de rôles. Ces rôles valident l'accès aux méthodes EJB suivant les contraintes de **ejb-jar.xml** et de l'implémentation de la méthode **EJBContext.isCallerInRole(String)**.

    - Un **java.security.acl.Group** optionnel nommé **CallerPrincipal**, contenant un seul **org.jboss.security.SimplePrincipal** qui correspond à l'identité de l'appelant du domaine de l'application. Le membre du groupe CallerPrincipal correspond à la valeur renvoyée par la méthode **EJBContext.getCallerPrincipal()**. Ce mappage permet au Principal de l'environnement de sécurité professionnel de se mapper à un Principal connu de l'application. En l'absence d'un mappage CallerPrincipal, le principal opérationnel est le même que le principal du domaine d'application.

5. Le serveur vérifie que l'utilisateur qui appelle la méthode EJB a la permission de le faire. Cette autorisation requiert les étapes suivantes :

    - Obtenir les noms des rôles autorisés à accéder à la méthode EJB à partir du conteneur EJB. Les noms de rôles sont déterminés par les éléments <role-name> de tous les éléments <method-permission> du descripteur **ejb-jar.xml** qui contiennent la méthode invoquée.

    - Si aucun des rôles n'a été attribué, ou si la méthode est spécifiée dans un élément de la liste d'exclusion, l'accès à la méthode sera refusé. Sinon, la méthode **doesUserHaveRole** sera appelée dans le gestionnaire de sécurité par l'intercepteur de sécurité pour vérifier si l'appelant possède l'un des noms de rôles assignés. Cette méthode effectue une itération dans les noms de rôles et vérifie si le groupe **Subject Roles** de l'utilisateur authentifié contient un SimplePrincipal avec le nom de rôle assigné. L'accès est autorisé si un nom de rôle est membre du groupe Rôles. L'accès est refusé si aucun des noms de rôles n'est membre.

    - Si l'EJB utilise un proxy de sécurité personnalisé, l'invocation de méthode sera déléguée au proxy. Si le proxy de sécurité refuse l'accès à l'appelant, elle lève une exception

java.lang.SecurityException. Sinon, l'accès à la méthode EJB sera autorisé et l'invocation de méthode passera au prochain intercepteur de conteneur. Le SecurityProxyInterceptor s'occupe de ce contrôle et cet intercepteur n'est pas affiché.

- Pour les demandes de connexion web, le serveur web vérifie les contraintes de sécurité définies dans **web.xml** qui correspondent à la ressource demandée et à la méthode HTTP à laquelle on a accédé.

  S'il existe une contrainte pour la demande, le serveur web appelle le JaasSecurityManager pour effectuer l'authentification du principal, qui assure à son tour veille à ce que les rôles d'utilisateur soient associés à cet objet principal.

Report a bug

14.2.9. Utiliser un domaine de sécurité dans votre application

Aperçu

Pour utiliser un domaine de sécurité dans votre application, vous devez tout d'abord configurer le domaine dans le fichier de configuration du serveur ou dans le fichier de descripteur de l'application. Ensuite, vous devez ajouter les annotations requises à l'EJB qui l'utilisent. Cette rubrique décrit les étapes requises pour utiliser un domaine de sécurité dans votre application.

Procédure 14.1. Configurer votre application pour qu'elle puisse utiliser un Domaine de sécurité

1. **Définir le domaine de sécurité**
   Vous pouvez définir le domaine de sécurité soit dans le fichier de configuration du serveur, soit dans le fichier du descripteur de l'application.

   - **Configurer le domaine de sécurité dans le fichier de configuration du serveur**
     Le domaine de sécurité est configuré dans le sous-système de **sécurité** du fichier de configuration du serveur. Si l'instance de JBoss EAP 6 s'exécute dans un domaine géré, il s'agira du fichier **domain/configuration/domain.xml**. Si l'instance de JBoss EAP 6 s'exécute comme un serveur autonome, ce sera le fichier **standalone/configuration/standalone.xml**.

     Les domaines de sécurité **other**, **jboss-web-policy**, et **jboss-ejb-policy** sont fournis par défaut dans JBoss EAP 6. L'exemple XML suivant a été copié à partir du sous-système de **sécurité** dans le fichier de configuration du serveur.

```
<subsystem xmlns="urn:jboss:domain:security:1.2">
    <security-domains>
        <security-domain name="other" cache-type="default">
            <authentication>
                <login-module code="Remoting" flag="optional">
                    <module-option name="password-stacking"
value="useFirstPass"/>
                </login-module>
                <login-module code="RealmDirect"
flag="required">
                    <module-option name="password-stacking"
value="useFirstPass"/>
                </login-module>
            </authentication>
        </security-domain>
        <security-domain name="jboss-web-policy" cache-
```

```
type="default">
            <authorization>
                <policy-module code="Delegating"
flag="required"/>
            </authorization>
        </security-domain>
        <security-domain name="jboss-ejb-policy" cache-
type="default">
            <authorization>
                <policy-module code="Delegating"
flag="required"/>
            </authorization>
        </security-domain>
    </security-domains>
</subsystem>
```

Vous pouvez configurer des domaines de sécurité supplémentaires selon les besoins par la console de gestion ou par le Management CLI.

- **Configurer le domaine de sécurité dans le fichier de descripteur de l'application.**
  Le domaine de sécurité est spécifié dans l'élément enfant **`<security-domain>`** de l'élément **`<jboss-web>`** du fichier **`WEB-INF/jboss-web.xml`** de l'application. L'exemple suivant configure un domaine de sécurité nommé **`my-domain`**.

```
<jboss-web>
    <security-domain>my-domain</security-domain>
</jboss-web>
```

Il s'agit d'une des configurations que vous pouvez indiquer dans le descripteur **`WEB-INF/jboss-web.xml`**.

2. **Ajouter l'annotation requise à l'EJB.**
   Vous pouvez configurer la sécurité dans EJB par les annotations **`@SecurityDomain`** et **`@RolesAllowed`**. L'exemple de code EJB suivant limite l'accès au domaine de sécurité **`other`** aux utilisateurs ayant pour rôle **`guest`** (invité).

```
package example.ejb3;

import java.security.Principal;

import javax.annotation.Resource;
import javax.annotation.security.RolesAllowed;
import javax.ejb.SessionContext;
import javax.ejb.Stateless;

import org.jboss.ejb3.annotation.SecurityDomain;

/**
 * Simple secured EJB using EJB security annotations
 * Allow access to "other" security domain by users in a "guest"
role.
 */
```

```
@Stateless
@RolesAllowed({ "guest" })
@SecurityDomain("other")
public class SecuredEJB {

   // Inject the Session Context
   @Resource
   private SessionContext ctx;

   /**
    * Secured EJB method using security annotations
    */
   public String getSecurityInfo() {
      // Session context injected using the resource annotation
      Principal principal = ctx.getCallerPrincipal();
      return principal.toString();
   }
}
```

Pour obtenir des exemples de code supplémentaires, voir **`ejb-security`** Quickstart dans le package JBoss EAP 6 Quickstarts disponible à partir du Portail Clients Red Hat.

Report a bug

14.2.10. Utilisation de la sécurité basée-rôle dans les Servlets

Pour ajouter la sécurité à un servlet, vous mappez chaque servlet à un type d'URL et créez des contraintes de sécurité sur les types d'URL qui doivent être sécurisés. Les contraintes de sécurité limitent l'accès des URL aux rôles. L'authentification et l'autorisation sont gérées par le domaine de sécurité spécifié dans **`jboss-web.xml`** du WAR.

Prérequis

Avant d'utiliser la sécurité basée-rôles dans une servlet, le domaine de sécurité utilisé pour authentifier et autoriser l'accès doit être configuré sur la plateforme JBoss EAP 6.

Procédure 14.2. Ajout de la sécurité basée-rôle dans les servlets

1. **Ajout de mappages entre les types d'URL et les servlets.**
   Utiliser les éléments **`<servlet-mapping>`** du fichier **`web.xml`** pour mapper les servlets individuels à des types d'URL. L'exemple suivant mappe le serveur nommé **`DisplayOpResult`** au type d'URL **`/DisplayOpResult`**.

   ```
   <servlet-mapping>
       <servlet-name>DisplayOpResult</servlet-name>
       <url-pattern>/DisplayOpResult</url-pattern>
   </servlet-mapping>
   ```

2. **Ajout des contraintes de sécurité aux types d'URL.**
   Pour mapper le type d'URL avec une contrainte de sécurité, utilisez un **`<security-constraint>`**. L'exemple suivant limite l'accès d'un type d'URL **`/DisplayOpResult`** afin qu'il soit accessible aux principaux ayant pour rôle **`eap_admin`**. Le rôle doit être présent dans le domaine de sécurité.

```
<security-constraint>
 <display-name>Restrict access to role eap_admin</display-name>
 <web-resource-collection>
  <web-resource-name>Restrict access to role eap_admin</web-
resource-name>
  <url-pattern>/DisplayOpResult/*</url-pattern>
 </web-resource-collection>
 <auth-constraint>
  <role-name>eap_admin</role-name>
 </auth-constraint>
</security-constraint>

<security-role>
  <role-name>eap_admin</role-name>
</security-role>


<login-config>
    <auth-method>BASIC</auth-method>
</login-config>
```

Vous aurez besoin d'indiquer la méthode d'authentification, qui peut être une des suivantes : **BASIC, FORM, DIGEST, CLIENT-CERT, SPNEGO.**. Cet exemple utilise l'authentification **BASIC**.

3. **Indiquer le domaine de sécurité et le fichier `jboss-web.xml` du WAR.**
   Ajouter le domaine de sécurité au fichier **`jboss-Web.xml`** du WAR afin de connecter les servlets au domaine de la sécurité configuré sachant comment authentifier et autoriser les principaux selon les contraintes de sécurité. L'exemple suivant utilise le domaine de sécurité appelé **`acme_domain`**.

```
<jboss-web>
 ...
 <security-domain>acme_domain</security-domain>
 ...
</jboss-web>
```

Exemple 14.1. Exemple `web.xml` avec la sécurité basée rôle configurée.

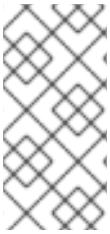
```
<web-app xmlns="http://java.sun.com/xml/ns/javaee"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd"
         version="3.0">

<display-name>Use Role-Based Security In Servlets</display-name>

<welcome-file-list>
  <welcome-file>/index.jsp</welcome-file>
</welcome-file-list>
```

```
<servlet-mapping>
    <servlet-name>DisplayOpResult</servlet-name>
    <url-pattern>/DisplayOpResult</url-pattern>
</servlet-mapping>

<security-constraint>
  <display-name>Restrict access to role eap_admin</display-name>
    <web-resource-collection>
      <web-resource-name>Restrict access to role eap_admin</web-
resource-name>
      <url-pattern>/DisplayOpResult/*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
        <role-name>eap_admin</role-name>
      </auth-constraint>
    </security-constraint>

    <security-role>
      <role-name>eap_admin</role-name>
    </security-role>

    <login-config>
        <auth-method>BASIC</auth-method>
    </login-config>

</web-app>
```

Report a bug

14.2.11. Utilisation d'une authentification système de tierce partie pour votre application

Vous pouvez intégrer des systèmes de sécurité de tierce partie avec JBoss EAP 6. Ces types de systèmes sont habituellement basés sur des tokens. Le système externe effectue l'authentification et passe un token à l'application web via les en-têtes de demande. Ceci est souvent dénommé *authentification de périmètre* Pour configurer l'authentification de périmètre dans votre application, ajoutez une valve d'authentification personnalisée. Si vous avez une valve de fournisseur tiers, veillez à ce qu'elle soit sur votre chemin de classe et suivez les exemples ci-dessous, ainsi que la documentation pour votre module d'authentification tiers.



NOTE

L'emplacement pour la configuration des valves a changé dans JBoss EAP 6. Il n'y a plus de descripteur de déploiement **`context.xml`**. Les valves sont configurées directement dans le descripteur **`jboss-web.xml`** à la place. Le fichier **`context.xml`** peut maintenant être ignoré.

Exemple 14.2. Valve d'authentification de base

```
<jboss-web>
  <valve>
```

```
    <class-
name>org.jboss.security.negotiation.NegotiationAuthenticator</class-
name>
  </valve>
</jboss-web>
```

Cette valve est utilisée pour les SSO basés-Kerberos. Montre également les modèles les plus simples d'indication d'authentificateurs de tierce partie pour votre application web.

Exemple 14.3. Personnaliser une valve avec des attributs d'en-tête

```
<jboss-web>
  <valve>
    <class-
name>org.jboss.web.tomcat.security.GenericHeaderAuthenticator</class-
name>
    <param>
      <param-name>httpHeaderForSSOAuth</param-name>
      <param-value>sm_ssoid,ct-remote-user,HTTP_OBLIX_UID</param-value>
    </param>
    <param>
      <param-name>sessionCookieForSSOAuth</param-name>
      <param-value>SMSESSION,CTSESSION,ObSSOCookie</param-value>
    </param>
  </valve>
</jboss-web>
```

Cet exemple montre comment définir des attributs personnalisés sur votre valve. L'authentificateur vérifie la présence de l'en-tête ID et de la clé de session, puis les passe au framework JAAS qui actionne la couche de sécurité, comme le nom d'utilisateur et le mot de passe. Vous avez besoin d'un module de connexion JAAS personnalisé qui puisse traiter le nom d'utilisateur et le mot de passe tout en remplissant le sujet par les rôles qui conviennent. Si aucune valeur d'en-tête ne correspond aux valeurs configurées, les sémantiques de d'authentification basée sur les formulaires réguliers s'appliqueront.

Rédaction d'un authentificateur personnalisé

Rédiger vous-même votre authentificateur est en dehors de la portée de ce document. Cependant, le code Java suivant est fourni comme exemple.

Exemple 14.4. GenericHeaderAuthenticator.java

```
/*
 * JBoss, Home of Professional Open Source.
 * Copyright 2006, Red Hat Middleware LLC, and individual contributors
 * as indicated by the @author tags. See the copyright.txt file in the
 * distribution for a full listing of individual contributors.
 *
 * This is free software; you can redistribute it and/or modify it
 * under the terms of the GNU Lesser General Public License as
 * published by the Free Software Foundation; either version 2.1 of
```

```
 * the License, or (at your option) any later version.
 *
 * This software is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
 * Lesser General Public License for more details.
 *
 * You should have received a copy of the GNU Lesser General Public
 * License along with this software; if not, write to the Free
 * Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA
 * 02110-1301 USA, or see the FSF site: http://www.fsf.org.
 */

package org.jboss.web.tomcat.security;

import java.io.IOException;
import java.security.Principal;
import java.util.StringTokenizer;

import javax.management.JMException;
import javax.management.ObjectName;
import javax.servlet.http.Cookie;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import org.apache.catalina.Realm;
import org.apache.catalina.Session;
import org.apache.catalina.authenticator.Constants;
import org.apache.catalina.connector.Request;
import org.apache.catalina.connector.Response;
import org.apache.catalina.deploy.LoginConfig;
import org.jboss.logging.Logger;

import org.jboss.as.web.security.ExtendedFormAuthenticator;

/**
 * JBAS-2283: Provide custom header based authentication support
 *
 * Header Authenticator that deals with userid from the request header
Requires
 * two attributes configured on the Tomcat Service - one for the http
header
 * denoting the authenticated identity and the other is the SESSION
cookie
 *
 * @author <a href="mailto:Anil.Saldhana@jboss.org">Anil Saldhana</a>
 * @author <a href="mailto:sguilhen@redhat.com">Stefan Guilhen</a>
 * @version $Revision$
 * @since Sep 11, 2006
 */
public class GenericHeaderAuthenticator extends
ExtendedFormAuthenticator {
  protected static Logger log = Logger
      .getLogger(GenericHeaderAuthenticator.class);

  protected boolean trace = log.isTraceEnabled();
```

```
  // JBAS-4804: GenericHeaderAuthenticator injection of ssoid and
  // sessioncookie name.
  private String httpHeaderForSSOAuth = null;

  private String sessionCookieForSSOAuth = null;

  /**
   * <p>
   * Obtain the value of the <code>httpHeaderForSSOAuth</code>
attribute. This
   * attribute is used to indicate the request header ids that have to
be
   * checked in order to retrieve the SSO identity set by a third party
   * security system.
   * </p>
   *
   * @return a <code>String</code> containing the value of the
   *         <code>httpHeaderForSSOAuth</code> attribute.
   */
  public String getHttpHeaderForSSOAuth() {
    return httpHeaderForSSOAuth;
  }

  /**
   * <p>
   * Set the value of the <code>httpHeaderForSSOAuth</code> attribute.
This
   * attribute is used to indicate the request header ids that have to
be
   * checked in order to retrieve the SSO identity set by a third party
   * security system.
   * </p>
   *
   * @param httpHeaderForSSOAuth
   *            a <code>String</code> containing the value of the
   *            <code>httpHeaderForSSOAuth</code> attribute.
   */
  public void setHttpHeaderForSSOAuth(String httpHeaderForSSOAuth) {
    this.httpHeaderForSSOAuth = httpHeaderForSSOAuth;
  }

  /**
   * <p>
   * Obtain the value of the <code>sessionCookieForSSOAuth</code>
attribute.
   * This attribute is used to indicate the names of the SSO cookies
that may
   * be present in the request object.
   * </p>
   *
   * @return a <code>String</code> containing the names (separated by a
   *         <code>','</code>) of the SSO cookies that may have been
set by a
   *         third party security system in the request.
   */
```

```
  public String getSessionCookieForSSOAuth() {
    return sessionCookieForSSOAuth;
  }

  /**
   * <p>
   * Set the value of the <code>sessionCookieForSSOAuth</code>
attribute. This
   * attribute is used to indicate the names of the SSO cookies that may
be
   * present in the request object.
   * </p>
   *
   * @param sessionCookieForSSOAuth
   *            a <code>String</code> containing the names (separated
by a
   *            <code>','</code>) of the SSO cookies that may have been
set by
   *            a third party security system in the request.
   */
  public void setSessionCookieForSSOAuth(String sessionCookieForSSOAuth)
{
    this.sessionCookieForSSOAuth = sessionCookieForSSOAuth;
  }

  /**
   * <p>
   * Creates an instance of <code>GenericHeaderAuthenticator</code>.
   * </p>
   */
  public GenericHeaderAuthenticator() {
    super();
  }

  public boolean authenticate(Request request, HttpServletResponse
response,
      LoginConfig config) throws IOException {
    log.trace("Authenticating user");

    Principal principal = request.getUserPrincipal();
    if (principal != null) {
      if (trace)
        log.trace("Already authenticated '" + principal.getName() +
"'");
      return true;
    }

    Realm realm = context.getRealm();
    Session session = request.getSessionInternal(true);

    String username = getUserId(request);
    String password = getSessionCookie(request);

    // Check if there is sso id as well as sessionkey
    if (username == null || password == null) {
      log.trace("Username is null or password(sessionkey) is
```

```
null:fallback to form auth");
      return super.authenticate(request, response, config);
    }
    principal = realm.authenticate(username, password);

    if (principal == null) {
      forwardToErrorPage(request, response, config);
      return false;
    }

    session.setNote(Constants.SESS_USERNAME_NOTE, username);
    session.setNote(Constants.SESS_PASSWORD_NOTE, password);
    request.setUserPrincipal(principal);

    register(request, response, principal, HttpServletRequest.FORM_AUTH,
        username, password);
    return true;
  }

  /**
   * Get the username from the request header
   *
   * @param request
   * @return
   */
  protected String getUserId(Request request) {
    String ssoid = null;
    // We can have a comma-separated ids
    String ids = "";
    try {
      ids = this.getIdentityHeaderId();
    } catch (JMException e) {
      if (trace)
        log.trace("getUserId exception", e);
    }
    if (ids == null || ids.length() == 0)
      throw new IllegalStateException(
          "Http headers configuration in tomcat service missing");

    StringTokenizer st = new StringTokenizer(ids, ",");
    while (st.hasMoreTokens()) {
      ssoid = request.getHeader(st.nextToken());
      if (ssoid != null)
        break;
    }
    if (trace)
      log.trace("SSOID-" + ssoid);
    return ssoid;
  }

  /**
   * Obtain the session cookie from the request
   *
   * @param request
   * @return
   */
```

```
protected String getSessionCookie(Request request) {
  Cookie[] cookies = request.getCookies();
  log.trace("Cookies:" + cookies);
  int numCookies = cookies != null ? cookies.length : 0;

  // We can have comma-separated ids
  String ids = "";
  try {
    ids = this.getSessionCookieId();
    log.trace("Session Cookie Ids=" + ids);
  } catch (JMException e) {
    if (trace)
      log.trace("checkSessionCookie exception", e);
  }
  if (ids == null || ids.length() == 0)
    throw new IllegalStateException(
        "Session cookies configuration in tomcat service missing");

  StringTokenizer st = new StringTokenizer(ids, ",");
  while (st.hasMoreTokens()) {
    String cookieToken = st.nextToken();
    String val = getCookieValue(cookies, numCookies, cookieToken);
    if (val != null)
      return val;
  }
  if (trace)
    log.trace("Session Cookie not found");
  return null;
}

/**
 * Get the configured header identity id in the tomcat service
 *
 * @return
 * @throws JMException
 */
protected String getIdentityHeaderId() throws JMException {
  if (this.httpHeaderForSSOAuth != null)
    return this.httpHeaderForSSOAuth;
  return (String) mserver.getAttribute(new ObjectName(
      "jboss.web:service=WebServer"), "HttpHeaderForSSOAuth");
}

/**
 * Get the configured session cookie id in the tomcat service
 *
 * @return
 * @throws JMException
 */
protected String getSessionCookieId() throws JMException {
  if (this.sessionCookieForSSOAuth != null)
    return this.sessionCookieForSSOAuth;
  return (String) mserver.getAttribute(new ObjectName(
      "jboss.web:service=WebServer"), "SessionCookieForSSOAuth");
}
```

```
    /**
     * Get the value of a cookie if the name matches the token
     *
     * @param cookies
     *            array of cookies
     * @param numCookies
     *            number of cookies in the array
     * @param token
     *            Key
     * @return value of cookie
     */
    protected String getCookieValue(Cookie[] cookies, int numCookies,
        String token) {
      for (int i = 0; i < numCookies; i++) {
        Cookie cookie = cookies[i];
        log.trace("Matching cookieToken:" + token + " with cookie name="
            + cookie.getName());
        if (token.equals(cookie.getName())) {
          if (trace)
            log.trace("Cookie-" + token + " value=" + cookie.getValue());
          return cookie.getValue();
        }
      }
      return null;
    }
  }
```

Report a bug

14.3. DOMAINES DE SÉCURITÉ

14.3.1. Domaines de sécurité

Un *domaine de sécurité*est une série de mappages entre les utilisateurs et les mots de passe, les utilisateurs et les rôles. Les domaines de sécurité représentent un mécanisme permettant d'ajouter l'authentification et l'autorisation à vos applications Web et EJB. JBoss EAP 6 fournit deux domaines de sécurité par défaut :

- **`ManagementRealm`** stocke les informations d'authentification pour l'API de gestion, qui fournit les fonctionnalités pour le Management CLI et la Console de gestion sur le web. Il fournit un système d'authentification pour gérer JBoss EAP 6 . Vous pouvez également utiliser le **`ManagementRealm`** si votre application a besoin des mêmes règles commerciales que vous utilisez pour l'API de gestion, lors de son authentification.
- **`ApplicationRealm`** stocke l'utilisateur, le mot de passe et les informations de rôle pour les applications Web et les EJB.

Chaque domaine est stocké dans deux fichiers du système de fichiers :

- ***`REALM`*`-users.properties`** stocke les mots de passe et les mots de passe hachés.
- ***`REALM`*`-users.properties`** stocke les mappages user-to-role.

Les fichiers de propriété sont stockés dans les répertoires **domain/configuration/** et **standalone/configuration/**. Les fichiers sont inscrits simultanément par la commande **add-user.sh** ou **add-user.bat**. Quand vous exécutez la commande, la première décision est de décider dans quel domaine ajouter votre premier utilisateur.

Report a bug

14.3.2. Ajout d'un domaine de sécurité

1. **Exécuter le Management CLI**
   Démarrer par la commande **jboss-cli.sh** ou **jboss-cli.bat** et connectez-vous au serveur.

2. **Créer le nouveau domaine de sécurité lui-même.**
   Exécutez la commande suivante pour créer un nouveau domaine de sécurité nommé **MyDomainRealm** sur un contrôleur de domaine ou sur un serveur autonome.

   ```
   /host=master/core-service=management/security-
   realm=MyDomainRealm:add()
   ```

3. **Créer les références du fichier de propriétés qui stocke les informations sur le nouveau rôle.**
   Exécuter la commande suivante pour créer un pointeur au fichier nommé **myfile.properties**, qui contiendra les propriétés attachées au nouveau rôle.

   NOTE

   Le fichier de propriétés nouvellement créées n'est pas géré par les scripts **add-user.sh** et **add-user.bat** inclus. Il devra être administré en externe.

   ```
   /host=master/core-service=management/security-
   realm=MyDomainRealm/authentication=properties:add(path=myfile.proper
   ties)
   ```

Résultat

Votre nouveau domaine de sécurité est créé. Lorsque vous ajoutez des utilisateurs et des rôles à ce nouveau domaine, l'information va être stockée dans un fichier séparé des domaines de sécurité par défaut. Vous pouvez gérer ce nouveau fichier à l'aide de vos propres applications ou procédures.

Report a bug

14.3.3. Ajout d'un utilisateur à un domaine de sécurité

1. **Éxécuter la commande add-user.sh ou add-user.bat.**
   Ouvrez un terminal (shell) et changez de répertoire ***EAP_HOME*/bin/**. Si vous exécutez Red Hat Enterprise Linux ou un autre système d'exploitation style UNIX, exécutez **add-user.sh**. Si vous exécutez sur un serveur Microsoft Windows, exécutez **add-user.bat**.

2. **Choisissez d'ajouter un utilisateur de gestion ou un utilisateur d'application.**
   Pour cette procédure, saisir **b** pour ajouter un utilisateur d'application.

3. **Choisir le domaine dans lequel l'utilisateur sera ajouté.**

Par défaut, le seul domaine disponible est **ApplicationRealm**. Si vous avez ajouté un domaine personnalisé, vous pouvez saisir son nom à la place.

4. **Saisir le nom d'utilisateur, le mot de passe et les rôles lorsque vous y serez invité.** Saisir le nom d'utilisateur, le mot de passe et les rôles lorsque vous y serez invité. Vérifiez votre choix en tapant **yes**, ou **no** pour annuler les changements. Les changements sont inscrits dans les fichiers de propriétés du domaine de sécurité.

Report a bug

14.4. SÉCURITÉ DES APPLICATIONS EJB

14.4.1. Identité Sécurité

14.4.1.1. L'identité de sécurité EJB

L'*identité de sécurité*, connue également sous le nom *identité d'invocation*, se réfère à la balise **<security-identity>** qui se trouve dans la configuration de la sécurité. Il s'agit d'une référence à l'identité qu'un autre EJB doit utiliser quand il invoque des méthodes ou des composants.

L'identité d'invocation peut soit correspondre à l'appelant actuel, ou correspondre à un rôle spécifique. Dans le premier cas, la balise **<use-caller-identity>** sera présente, et dans le second cas, la balise **<run-as>** sera utilisée.

Pour plus d'information sur la configuration de l'identité de sécurité sur un EJB, voir Section 14.4.1.2, « Définir l'identité de sécurité d'un EJB ».

Report a bug

14.4.1.2. Définir l'identité de sécurité d'un EJB

Exemple 14.5. Définir l'identité de sécurité d'un EJB pour que ce soit la même que celle de l'appelant

Cet exemple définit l'identité de sécurité pour les invocations de méthode faîtes par un EJB de façon à ce qu'elle soit la même identité que celle de l'appelant actuel. Ce comportement correspond au comportement par défaut si vous ne spécifiez pas une déclaration d'élément **<security-identity>**.

```
<ejb-jar>
  <enterprise-beans>
  <session>
  <ejb-name>ASessionBean</ejb-name>
  <!-- ... -->
  <security-identity>
    <use-caller-identity/>
  </security-identity>
  </session>
  <!-- ... -->
  </enterprise-beans>
</ejb-jar>
```

Exemple 14.6. Définir l'idendité de sécurité d'un EJB à un rôle spécifique

Pour définir l'id de sécurité à un rôle spécifique, utiliser **<run-as>** et les balises **<role-name>** dans la balise **<security-identity>**.

```
<ejb-jar>
  <enterprise-beans>
  <session>
  <ejb-name>RunAsBean</ejb-name>
  <!-- ... -->
  <security-identity>
    <run-as>
    <description>A private internal role</description>
    <role-name>InternalRole</role-name>
    </run-as>
  </security-identity>
  </session>
  </enterprise-beans>
  <!-- ... -->
</ejb-jar>
```

Par défaut, quand vous utilisez **<run-as>**, un principal nommé **anonymous** est assigné aux appels sortants. Pour assigner un autre principal, utiliser **<run-as-principal>**.

```
<session>
    <ejb-name>RunAsBean</ejb-name>
    <security-identity>
        <run-as-principal>internal</run-as-principal>
    </security-identity>
</session>
```

NOTE

Vous pouvez utiliser les éléments **<run-as>** et **<run-as-principal>** à l'intérieur d'un élément de servlet.

Voir également :

- Section 14.4.1.1, « L'identité de sécurité EJB »
- Section 16.2, « Référence de paramètre de sécurité EJB »

Report a bug

14.4.2. Permissions de méthodes EJB

14.4.2.1. Permissions de méthodes EJB

EJB fournit une déclaration d'élément **<method-permisison>**. Cette déclaration définit les rôles qui sont autorisés à appeler des méthodes de l'interface EJB. Vous pouvez définir des permissions pour les combinaisons suivantes :

- Toutes les méthodes d'interface de composant ou d'accueil de l'EJB nommé
- Une méthode spécifiée d'interface de composant ou d'accueil de l'EJB nommé
- Une méthode spécifiée à l'intérieur d'un ensemble de méthodes avec un nom surchargé

Pour obtenir des exemples, voir Section 14.4.2.2, « Utilisation des permissions de méthodes EJB ».

Report a bug

14.4.2.2. Utilisation des permissions de méthodes EJB

Aperçu

L'élément **<method-permission>** définit les roles logiques qui peuvent accéder aux méthodes EJB définies par les éléments **<method>**. Un certain nombre d'exemples expliquent la syntaxe XML. Plusieurs énoncés de method-permission peuvent être présents, et avoir un effet cumulatif. L'élément **<method-permission>** est un dépendant de l'élément **<assembly-descriptor>** du descripteur **<ejb-jar>**.

La syntaxe XML est une alternative aux annotations pour les permissions de méthode EJB.

Exemple 14.7. Permet aux rôles d'accéder à toutes les méthodes d'un EJB

```
<method-permission>
  <description>The employee and temp-employee roles may access any
method
  of the EmployeeService bean </description>
  <role-name>employee</role-name>
  <role-name>temp-employee</role-name>
  <method>
    <ejb-name>EmployeeService</ejb-name>
    <method-name>*</method-name>
  </method>
</method-permission>
```

Exemple 14.8. Permet aux rôles d'accéder uniquement à des méthodes spécifiques d'un EJB, et de déterminer quels paramètres de méthode peuvent être passés.

```
<method-permission>
  <description>The employee role may access the findByPrimaryKey,
  getEmployeeInfo, and the updateEmployeeInfo(String) method of
  the AcmePayroll bean </description>
  <role-name>employee</role-name>
  <method>
 <ejb-name>AcmePayroll</ejb-name>
 <method-name>findByPrimaryKey</method-name>
  </method>
```

```
  <method>
 <ejb-name>AcmePayroll</ejb-name>
 <method-name>getEmployeeInfo</method-name>
  </method>
  <method>
 <ejb-name>AcmePayroll</ejb-name>
 <method-name>updateEmployeeInfo</method-name>
 <method-params>
   <method-param>java.lang.String</method-param>
 </method-params>
  </method>
</method-permission>
```

Exemple 14.9. Permet à n'importe quel utilisateur authentifié d'accéder aux méthodes des EJB

Utiliser l'élément **<unchecked/>** permet à un utilisateur authentifié d'utiliser les méthodes spécifiées.

```
<method-permission>
  <description>Any authenticated user may access any method of the
  EmployeeServiceHelp bean</description>
  <unchecked/>
  <method>
 <ejb-name>EmployeeServiceHelp</ejb-name>
 <method-name>*</method-name>
  </method>
</method-permission>
```

Exemple 14.10. Exclut totalement certaines méthodes EJB à l'utilisation

```
<exclude-list>
  <description>No fireTheCTO methods of the EmployeeFiring bean may be
  used in this deployment</description>
  <method>
 <ejb-name>EmployeeFiring</ejb-name>
 <method-name>fireTheCTO</method-name>
  </method>
</exclude-list>
```

Exemple 14.11. Un <assembly-descriptor> complet contenant plusieurs blocs de <method-permission>

```
<ejb-jar>
    <assembly-descriptor>
        <method-permission>
            <description>The employee and temp-employee roles may
access any
```

```
                method of the EmployeeService bean </description>
            <role-name>employee</role-name>
            <role-name>temp-employee</role-name>
            <method>
                <ejb-name>EmployeeService</ejb-name>
                <method-name>*</method-name>
            </method>
        </method-permission>
        <method-permission>
            <description>The employee role may access the
findByPrimaryKey,
                getEmployeeInfo, and the updateEmployeeInfo(String)
method of
                the AcmePayroll bean </description>
            <role-name>employee</role-name>
            <method>
                <ejb-name>AcmePayroll</ejb-name>
                <method-name>findByPrimaryKey</method-name>
            </method>
            <method>
                <ejb-name>AcmePayroll</ejb-name>
                <method-name>getEmployeeInfo</method-name>
            </method>
            <method>
                <ejb-name>AcmePayroll</ejb-name>
                <method-name>updateEmployeeInfo</method-name>
                <method-params>
                    <method-param>java.lang.String</method-param>
                </method-params>
            </method>
        </method-permission>
        <method-permission>
            <description>The admin role may access any method of the
                EmployeeServiceAdmin bean </description>
            <role-name>admin</role-name>
            <method>
                <ejb-name>EmployeeServiceAdmin</ejb-name>
                <method-name>*</method-name>
            </method>
        </method-permission>
        <method-permission>
            <description>Any authenticated user may access any method
of the
                EmployeeServiceHelp bean</description>
            <unchecked/>
            <method>
                <ejb-name>EmployeeServiceHelp</ejb-name>
                <method-name>*</method-name>
            </method>
        </method-permission>
        <exclude-list>
            <description>No fireTheCTO methods of the EmployeeFiring
bean may be
                used in this deployment</description>
            <method>
                <ejb-name>EmployeeFiring</ejb-name>
```

```
                <method-name>fireTheCTO</method-name>
            </method>
        </exclude-list>
    </assembly-descriptor>
</ejb-jar>
```

Report a bug

14.4.3. Annotations de sécurité EJB

14.4.3.1. Les annotations de sécurité EJB

Les EJB utilisent des annotations de sécurité pour faire passer des informations de sécurité au déployeur. Celles-ci comprennent :

@DeclareRoles

Déclare quels rôles sont disponibles.

@RolesAllowed, @PermitAll, @DenyAll

Indique quelles permissions de méthodes sont autorisées. Pour obtenir des informations sur les permissions de méthode, voir Section 14.4.2.1, « Permissions de méthodes EJB ».

@RunAs

Configure l'identification de sécurité propagée d'un composant.

Pour plus d'information, voir Section 14.4.3.2, « Utilisation des annotations de sécurité EJB ».

Report a bug

14.4.3.2. Utilisation des annotations de sécurité EJB

Aperçu

Vous pouvez utiliser deux descripteurs XML ou des annotations pour contrôler quels rôles de sécurité sont en mesure d'appeler des méthodes dans votre Enterprise JavaBeans (EJB). Pour plus d'informations sur l'utilisation des descripteurs XML, reportez-vous à Section 14.4.2.2, « Utilisation des permissions de méthodes EJB ».

Annotations pour contrôler les permissions de sécurité des EJB

@DeclareRoles

Utiliser @DeclareRoles pour déterminer sur quels rôles de sécurité vérifier les permissions. Si aucun @DeclareRoles n'est présent, la liste sera édifié automatiquement à partir de l'annotation @RolesAllowed.

@SecurityDomain

Indique le domaine de sécurité à utiliser pour l'EJB. Si l'EJB est annoté pour autorisation avec **@RolesAllowed**, l'autorisation ne s'appliquera que si l'EJB est annoté par un domaine de sécurité.

@RolesAllowed, @PermitAll, @DenyAll

Utiliser @RolesAllowed pour lister les rôles autorisés pour accéder à une méthode ou à des méthodes. Utiliser @PermitAll ou @DenyAll pour permettre ou refuser à tous les roles d'utiliser une méthode ou des méthodes.

@RunAs

Utiliser @RunAs pour spécifier un rôle permanent pour une méthode.

Exemple 14.12. Exemple d'annotations de sécurité

```
@Stateless
@RolesAllowed({"admin"})
@SecurityDomain("other")
public class WelcomeEJB implements Welcome {
 @PermitAll
 public String WelcomeEveryone(String msg) {
  return "Welcome to " + msg;
 }
 @RunAs("tempemployee")
 public String GoodBye(String msg) {
     return "Goodbye, " + msg;
 }
 public String GoodbyeAdmin(String msg) {
  return "See you later, " + msg;
 }
}
```

Avec ce code, tous les rôles peuvent accéder à la méthode **`WelcomeEveryone`**. La méthode **`GoodBye`** exécute sous la forme du rôle **`tempemployee`** pour les appels. Seul le rôle **`admin`** peut accéder à la méthode **`GoodbyeAdmin`**, ou à toute autre méthode sans annotation de sécurité.

Report a bug

14.4.4. Accès à distance aux EJB

14.4.4.1. Remote Method Access

JBoss Remoting est le framework qui fournit un accès à distance aux EJBs, JMX MBeans, et autres services similaires. Fonctionne avec les types de transport suivants, avec ou sans SSL :

Types de services pris en charge

- Socket / Secure Socket
- RMI / RMI sur SSL
- HTTP / HTTPS
- Servlet / Secure Servlet
- Bisocket / Secure Bisocket

JBoss Remoting fournit aussi automatic discovery via Multicast ou JNDI.

Il est utilisé par bon nombre des sous-systèmes au sein de la plateforme JBoss EAP 6 et permet également de concevoir, d'implémenter et de déployer des services pouvant être appelés à distance par les clients sur plusieurs mécanismes de transport différents. Il vous permet également d'accéder aux services existants dans JBoss EAP 6.

Data Marshalling

Le système Remoting d'accès distant fournit également des services de marshalling et unmarshalling de données. Le marshaling de données désigne la capacité de déplacer en toute sécurité des données au-delà des limites de réseau et de la plate-forme, afin qu'un système séparé puisse effectuer des tâches dessus. Le travail est ensuite renvoyé vers le système d'origine et se comporte comme s'il avait eu lieu localement.

Aperçu de l'architecture

Lorsque vous créez une application cliente qui utilise Remoting, vous indiquez à votre application de communiquer avec le serveur en la configurant pour qu'elle utilise un type spécial de localisateur de ressources appelé un **`InvokerLocator`**, qui est une chaîne simple avec un format de type URL. Le serveur écoute les requêtes des ressources distantes sur un **`connecteur`**, qui est configuré comme faisant partie du sous-système **`remoting`**. Le **`connecteur`** transmet la demande à un **`ServerInvocationHandler`** configuré. Chaque **`ServerInvocationHandler`** implémente une méthode **`invoke(InvocationRequest)`** qui sait comment gérer la demande.

Le framework JBoss Remoting contient trois couches qui se miroitent les unes par rapport aux autres côté client et côté serveur.

Couches de framework JBoss Remoting

- L'utilisateur interagit avec la couche externe. Côté client, la couche externe est la classe **`Client`**, qui envoie des requêtes d'invocation. Côté serveur, c'est InvocationHandler, mis en œuvre par l'utilisateur, qui reçoit des demandes d'invocation.
- Le transport est contrôlé par la couche d'invocateur.
- La couche inférieure contient le marshaller et le unmarshaller, qui convertit les formats de données en formats de transmission.

Report a bug

14.4.4.2. Remoting Callbacks

Lorsqu'un client Remoting (à distance) demande des informations du serveur, il peut y avoir un blocage et il faut alors attendre que le serveur réponde, mais ce n'est pas un comportement idéal. Pour permettre au client d'être à l'écoute des événements asynchrones sur le serveur et pour pouvoir continuer à faire d'autre tâches en attendant que le serveur complète la requête, votre application peut demander au serveur d'envoyer une notification quand il aura fini. C'est ce que l'on appelle un callback. Un client peut s'ajouter comme un écouteur d'événements asynchrones générés au nom d'un autre client, aussi bien. Il y a deux choix différents pour recevoir des callbacks : «pull callbacks» ou «push callbacks». Les clients vérifient les «pull callbacks» de façon synchrone, mais écoutent passivement les «push callbacks».

En substance, un callback fonctionne de cette façon: le serveur envoie une **`InvocationRequest`** au client. Votre code côté serveur fonctionne de la même façon que le rappel soit synchrone ou asynchrone. Seul le client a besoin de connaître la différence. InvocationRequest du serveur envoie un

responseObject au client. Il s'agit de la charge que le client a demandé. C'est peut-être une réponse directe à une demande ou à une notification d'événement.

Votre serveur suit aussi les listeners à l'aide d'un objet **m_listeners**. Il contient une liste de tous les listeners qui ont été ajoutés à votre server handler. L'interface du **ServerInvocationHandler** inclut des méthodes qui vous permettent de gérer cette liste.

Le client gère les «pull callbacks» et les «push callbacks» de différentes manières. Dans les deux cas, il doit implémenter un callback handler. Un callback handler est une implémentation de l'interface **org.jboss.remoting.InvokerCallbackHandler**, qui traite les données de callback. Après l'implémentation du callback handler, soit vous vous ajoutez vous-même, en tant que listener de «pull callback», ou bien, vous installez un serveur de callbacks pour un «push callback».

Pull Callbacks

Pour un «pull callback», votre client s'ajoute à la liste du serveur des listeners à l'aide de la méthode **Client.addListener()**. Ensuite, il interroge le serveur périodiquement au sujet de l'exécution synchrone des données de callback. Ce sondage est effectué à l'aide de **Client.getCallbacks()**.

Push Callback

Un «push callback» requiert que votre application cliente exécute elle-même son propre InvocationHandler. Pour ce faire, vous devez exécuter un service Remoting sur le client lui-même. Ceci s'appelle un *callback server*. Le callback server accepte les requêtes entrantes de façon asynchrone et les traite pour l'auteur de la demande (dans ce cas, le serveur). Pour inscrire le callback server de votre client avec le serveur principal, passez l'argument **InvokerLocator** du callback server comme deuxième argument à la méthode **addListener**.

Report a bug

14.4.4.3. Remoting Server Detection

Les clients et les serveurs d'accès distant peuvent se détecter les uns les autres automatiquement à l'aide de JNDI ou Multicast. Un détecteur Remoting Detector est ajouté aux client et serveur, et un NetworkRegistry est ajoutée au client.

Le détecteur côté serveur scanne périodiquement InvokerRegistry et extrait tous les invocateurs de serveur qu'il a créés. Il utilise ces informations pour publier un message de détection, qui contient le localisateur et les sous-systèmes pris en charge par chaque invocateur de serveur. Il publie ce message via une multidiffusion ou une liaison vers un serveur JNDI.

Côté client, le détecteur reçoit le message de multidiffusion ou interroge périodiquement le serveur JNDI pour récupérer les messages de détection. Si le détecteur remarque qu'un message de détection est pour un serveur d'accès distant nouvellement détecté, il l'inscrit dans NetworkRegistry. Le détecteur met également à jour NetworkRegistry s'il détecte qu'un serveur n'est plus disponible

Report a bug

14.4.4.4. Configurer le sous-système de JBoss Remoting

Aperçu

JBoss Remoting a trois éléments configurables de niveau supérieur : le pool de worker threads, un ou plusieurs connecteurs et une série de lien URI locaux et distants. Cette rubrique propose une explication pour chaque élément configurable, des exemples de commandes CLI pour savoir comment configurer chaque élément et un exemple XML d'un sous-système entièrement configuré. Cette configuration s'applique uniquement au serveur. La plupart des gens n'auront pas à configurer le sous-

système de communication à distance, sauf s'ils utilisent des connecteurs personnalisés pour leurs propres applications. Les applications qui agissent comme des clients Remoting, comme les EJB, nécessitent une configuration distincte pour se connecter à un connecteur spécifique.

NOTE

La configuration du sous-système Remoting n'est pas exposée à la Console de gestion sur web, mais est entièrement configurable du Management CLI en ligne de commande. Il n'est pas recommandé de modifier le code XML à la main.

Adaptation des commandes CLI

Les commandes CLI sont formulées pour un domaine géré, lorsque vous configurez le profil **`par défaut`**. Pour configurer un profil différent, changez-en le nom. Pour un serveur autonome, omettre la section **`/profile=default`** de la commande.

Configuration en dehors du sous-système Remoting

Il y a un certain nombre d'aspects de configuration qui sont en dehors du sous-système **`remoting`** :

Network Interface

L'interface de réseau qui est utilisée par le sous-système **`remoting`** est l'interface **`unsecure`** définie dans **`domain/configuration/domain.xml`** ou dans **`standalone/configuration/standalone.xml`**.

```
<interfaces>
   <interface name="management"/>
   <interface name="public"/>
   <interface name="unsecure"/>
</interfaces>
```

La définition par-hôte de l'interface **`unsecure`** est définie dans **`host.xml`** dans le même répertoire que **`domain.xml`** ou **`standalone.xml`**. Cette interface est également utilisée par plusieurs autres sous-systèmes. Soyez vigilants quand vous la modifierez.

```
<interfaces>
   <interface name="management">
      <inet-address
value="${jboss.bind.address.management:127.0.0.1}"/>
   </interface>
   <interface name="public">
      <inet-address value="${jboss.bind.address:127.0.0.1}"/>
   </interface>
   <interface name="unsecure">
      <!-- Used for IIOP sockets in the standard configuration.
         To secure JacORB you need to setup SSL -->
      <inet-address value="${jboss.bind.address.unsecure:127.0.0.1}"/>
   </interface>
</interfaces>
```

socket-binding

La liaison-socket par défaut utilisée par le sous-système **remoting** se lie au port TCP 4777. Reportez-vous à la documentation sur les liaisons de socket et de groupes de liaisons de socket pour plus d'informations si vous avez besoin de procéder à une modification.

Remoting Connector Reference pour EJB

Le sous-système EJB contient une référence vers le connecteur à distance pour les invocations de méthodes à distance. Voici la configuration par défaut :

```
<remote connector-ref="remoting-connector" thread-pool-name="default"/>
```

Configuration du transport sécurisé

Les transports à distance (Remoting) utilisent StartTLS pour avoir une connexion sécurisée (HTTPS, Secure Servlet, etc.) si le client le demande. La même liaison de socket (port réseau) est utilisée pour les connexions sécurisées et non sécurisées, donc aucune configuration côté serveur supplémentaire n'est nécessaire. Le client demande le transport sécurisé ou non sécurisé, tel que le dictent ses besoins. Les composants JBoss EAP 6 qui utilisent Remoting, tels que les fournisseur JMS, EJB et ORB exigent des interfaces sécurisées par défaut.

AVERTISSEMENT

StartTLS fonctionne en activant une connexion sécurisée si le client le demande au lieu de, par défaut, d'une connexion non sécurisée. StartTLS est, par nature, sensible à un exploit de style *Man in the Middle*, dans lequel un attaquant intercepte la demande du client et la modifie pour demander une connexion non sécurisée. Les clients doivent avoir reçu des écritures pour échouer correctement s'ils ne reçoivent pas une connexion sécurisée, sauf si une connexion non sécurisée constitue un fall-back approprié.

Worker Thread Pool

Un Worker Thread Pool est un ensemble de threads qui peuvent traiter les tâches qui arrivent par les connecteurs Remoting. Il s'agit d'un seul élément **<worker-thread-pool>**, et nécessite un certain nombre d'attributs. Régler ces attributs si vous avez des timeouts de réseau, ou si vous devez limiter l'utilisation de la mémoire. Les conseils varient suivant la situation dans laquelle vous vous trouvez. Contacter Red Hat Global Support Services pour obtenir davantage d'informations.

Tableau 14.2. Attributs de Worker Thread Pool

Attribut	Description	Commande CLI
read-threads	Le nombre de read-threads à créer pour le worker à distance. La valeur par défaut est **1**.	**/profile=default/subsystem=remoting/:write-attribute(name=worker-read-threads,value=1)**

Attribut	Description	Commande CLI
write-threads	Le nombre de write-threads à créer pour le worker à distance. La valeur par défaut est **1**.	**/profile=default/subsystem=remoting/:write-attribute(name=worker-write-threads,value=1)**
task-keepalive	Le nombre de millisecondes pour conserver les threads de tâche de workers à distance non-core vivants. La valeur par défaut est **60**.	**/profile=default/subsystem=remoting/:write-attribute(name=worker-task-keepalive,value=60)**
task-max-threads	Le nombre de maximum de threads pour le Worker Task Thread Pool distant. La valeur par défaut est **60**.	**/profile=default/subsystem=remoting/:write-attribute(name=worker-task-max-threads,value=16)**
task-core-threads	Le nombre de threads principaux pour le Worker Task Thread Pool distant. La valeur par défaut est **4**.	**/profile=default/subsystem=remoting/:write-attribute(name=worker-task-core-threads,value=4)**
task-limit	Le nombre de maximum de tâches de worker distantes. La valeur par défaut est **16384**.	**/profile=default/subsystem=remoting/:write-attribute(name=worker-task-limit,value=16384)**

Connecteur

Le connecteur est le principal élément de configuration de Remoting (d'accès à distance). Les connecteurs multiples sont autorisés. Chacun se compose d'un élément **<connector>** avec plusieurs sous-éléments, ainsi que quelques attributs possibles. Le connecteur par défaut est utilisé par plusieurs sous-systèmes de JBoss EAP 6. Des paramètres spécifiques pour les éléments et les attributs de vos connecteurs personnalisés dépendent de vos applications, donc contactez Red Hat Global Support Services pour plus d'informations.

Tableau 14.3. Attributs de connecteur

Attribut	Description	Commande CLI
socket-binding	Le nom de la liaison de socket à utiliser pour ce connecteur.	**/profile=default/subsystem=remoting/connector=remoting-connector/:write-attribute(name=socket-binding,value=remoting)**

Attribut	Description	Commande CLI
authentication-provider	Le module JASPIC (de l'anglais Java Authentication Service Provider Interface for Containers) à utiliser avec ce connecteur. Le module doit être dans le chemin de classes.	`/profile=default/subsystem=remoting/connector=remoting-connector/:write-attribute(name=authentication-provider,value=myProvider)`
security-realm	En option. Le domaine de la sécurité qui contient les utilisateurs, mots de passe et les rôles de votre application. Un EJB ou une Application Web peut authentifier sur un domaine de sécurité. `ApplicationRealm` est disponible dans une installation de JBoss EAP 6 par défaut.	`/profile=default/subsystem=remoting/connector=remoting-connector/:write-attribute(name=security-realm,value=ApplicationRealm)`

Tableau 14.4. Éléments de connecteur

Attribut	Description	Commande CLI
sasl	Élément englobant des mécanismes d'authentification SASL (Simple Authentication and Security Layer)	`N/A`
propriétés	Contient un ou plusieurs éléments `<property>`, contenant chacun un attribut `name` et un attribut`value` optionnel.	`/profile=default/subsystem=remoting/connector=remoting-connector/property=myProp/:add(value=myPropValue)`

Les connexions de sortie

Vous pouvez spécifier trois types différents d'attribut de connexion sortante :

- Connexion sortante vers un URI.
- Connexion sortante locale – se connectant à une ressource locale, comme un socket.
- Connexion sortante à distance – se connectant à une ressource à distance et s'authentifiant par l'intermédiaire d'un domaine de sécurité.

Toutes les connexions sortantes sont enfermées dans un élément `<outbound-connections>`. Chacun de ces types de connexion prend un attribut `outbound-socket-binding-ref`. La connexion sortante-prend un attribut `uri`. La connexion sortante à prend les attributs facultatifs `username` (nom d'utilisateur) et `security-realm` (domaine de sécurité) à utiliser pour l'autorisation.

Tableau 14.5. Éléments de connexion sortante

Attribut	Description	Commande CLI
outbound-connection	Connexion sortante standard	**/profile=default/subsystem=remoting/outbound-connection=my-connection/:add(uri=http://my-connection)**
local-outbound-connection	Connexion sortante en schéma implicite local:// URI.	**/profile=default/subsystem=remoting/local-outbound-connection=my-connection/:add(outbound-socket-binding-ref=remoting2)**
remote-outbound-connection	Connexions sortantes en schéma remote:// URI, utilisant l'authentification de base/digest avec domaine de sécurité.	**/profile=default/subsystem=remoting/remote-outbound-connection=my-connection/:add(outbound-socket-binding-ref=remoting,username=myUser,security-realm=ApplicationRealm)**

Éléments SASL

Avant de définir des éléments enfants SASL, vous devez créer l'élément SASL initial. Utiliser la commande suivante :

```
/profile=default/subsystem=remoting/connector=remoting-
connector/security=sasl:add
```

Les éléments enfants de l'élément SASL sont décrits dans le tableau ci-dessous.

Attribut	Description	Commande CLI
include-mechanisms	Contient un attribut **value**, qui correspond à une liste de mécanismes SASL séparés par des espaces.	`/profile=default/subsystem=remoting/connector=remoting-connector/security=sasl:write-attribute(name=include-mechanisms,value=["DIGEST","PLAIN","GSSAPI"])`

Attribut	Description	Commande CLI
qop	Contient un attribut **`value`**, qui correspond à une liste de valeurs de protection SASL séparées par des espaces, en ordre décroissant de préférence.	`/profile=default/subsystem=remoting/connector=remoting-connector/security=sasl:write-attribute(name=qop,value=["auth"])`
puissance	Contient un attribut **`value`**, qui correspond à une liste de valeurs de puissance cipher SASL séparées par des espaces, en ordre décroissant de préférence.	`/profile=default/subsystem=remoting/connector=remoting-connector/security=sasl:write-attribute(name=strength,value=["medium"])`
reuse-session	Contient un attribut **`value`**, qui correspond à une valeur booléenne. Si sur true, tente de réutiliser les sessions.	`/profile=default/subsystem=remoting/connector=remoting-connector/security=sasl:write-attribute(name=reuse-session,value=false)`
server-auth	Contient un attribut **`value`**, qui correspond à une valeur booléenne. Si sur true, le serveur s'authentifie auprès du client.	`/profile=default/subsystem=remoting/connector=remoting-connector/security=sasl:write-attribute(name=server-auth,value=false)`
politique	Un élément clôturé qui contient zéro ou plusieurs des éléments suivants, prenant chacun une seule **`valeur`**. • forward-secrecy – indique on a besoin de mécanismes pour implémenter la forward-secrecy (l'infiltration dans une session ne va pas forcément donner	`/profile=default/subsystem=remoting/connector=remoting-connector/security=sasl/sasl-policy=policy:add` `/profile=default/subsystem=remoting/conn`

Attribut	Description	Commande CLI
	des informations sur la façon de s'infiltrer dans des sessions futures) • no-active – indique si les mécanismes susceptibles d'attaques hors dictionnaire sont permis. Une valeur **`false`** le permet, et **`true`** non. • no-anonymous – indique si les mécanismes qui acceptent la connexion anonyme sont permis. Une valeur de **`false`** le permet, et **`true`** non. • no-active – indique si les mécanismes susceptibles d'attaques dictionnaire passives sont permis. Une valeur **`false`** le permet, et **`true`** non. • no-plain-text – indique si les mécanismes susceptibles de simples attaques dictionnaire passives sont permis. Une valeur **`false`** le permet, et **`true`** non. • pass-credentials – indique si les mécanismes qui font passer les authentifications clients sont permis.	ector=remoting-connector/security=sasl/sasl-policy=policy:write-attribute(name=forward-secrecy,value=true) /profile=default/subsystem=remoting/connector=remoting-connector/security=sasl/sasl-policy=policy:write-attribute(name=no-active,value=false) /profile=default/subsystem=remoting/connector=remoting-connector/security=sasl/sasl-policy=policy:write-attribute(name=no-anonymous,value=false) /profile=default/subsystem=remoting/connector=remoting-connector/security=sasl/sasl-policy=policy:write-attribute(name=no-dictionary,value=true) /profile=default/subsystem=remoting/connector=remoting-connector/security=sasl/sasl-policy=policy:write-attribute(name=no-plain-text,value=false) /profile=default/subsystem=remoting/connector=remoting-connector/security=sasl/sasl-policy=policy:write-

Attribut	Description	Commande CLI
		attribute(name=pass-credentials,value=true)
propriétés	Contient un ou plusieurs éléments **<property>**, contenant chacun un attribut **name** et un attribut**value** optionnel.	/profile=default/subsystem=remoting/connector=remoting-connector/security=sasl/property=myprop:add(value=1) /profile=default/subsystem=remoting/connector=remoting-connector/security=sasl/property=myprop2:add(value=2)

Exemple 14.13. Exemples de configurations

Cet exemple montre le sous-système à distance par défaut qui est fourni dans JBoss EAP 6.

```
<subsystem xmlns="urn:jboss:domain:remoting:1.1">
    <connector name="remoting-connector" socket-binding="remoting"
security-realm="ApplicationRealm"/>
</subsystem>
```

Cet exemple contient de nombreuses valeurs hypothétiques, est est présenté de façon à ce que l'on puisse mettre les éléments et les attributs dont on a discutés plus haut en contexte.

```
<subsystem xmlns="urn:jboss:domain:remoting:1.1">
    <worker-thread-pool read-threads="1" task-keepalive="60' task-max-
threads="16" task-core-thread="4" task-limit="16384" write-threads="1"
/>
    <connector name="remoting-connector" socket-binding="remoting"
security-realm="ApplicationRealm">
        <sasl>
            <include-mechanisms value="GSSAPI PLAIN DIGEST-MD5" />
            <qop value="auth" />
            <strength value="medium" />
            <reuse-session value="false" />
            <server-auth value="false" />
            <policy>
                <forward-secrecy value="true" />
                <no-active value="false" />
                <no-anonymous value="false" />
                <no-dictionary value="true" />
                <no-plain-text value="false" />
                <pass-credentials value="true" />
```

```
            </policy>
            <properties>
                <property name="myprop1" value="1" />
                <property name="myprop2" value="2" />
            </properties>
        </sasl>
        <authentication-provider name="myprovider" />
        <properties>
            <property name="myprop3" value="propValue" />
        </properties>
    </connector>
    <outbound-connections>
        <outbound-connection name="my-outbound-connection"
uri="http://myhost:7777/"/>
        <remote-outbound-connection name="my-remote-connection"
outbound-socket-binding-ref="my-remote-socket" username="myUser"
security-realm="ApplicationRealm"/>
        <local-outbound-connection name="myLocalConnection" outbound-
socket-binding-ref="my-outbound-socket"/>
    </outbound-connections>
</subsystem>
```

Aspects de la configuration non encore documentés

- JNDI et Détection automatique multi diffusion

Report a bug

14.4.4.5. Utilisation des domaines de sécurité avec les clients EJB distants

Une façon d'ajouter la sécurité aux clients qui font appel aux EJB à distance consiste à utiliser des domaines de sécurité. Un domaine de sécurité est une simple base de données de paires nom d'utilisateur/mot de passe et nom d'utilisateur/rôle. La terminologie est également utilisée dans le cadre de conteneurs web, avec un sens légèrement différent.

Pour authentifier un EJB par un nom d'utilisateur ou un mot de passe particulier existant déjà dans un domaine de sécurité, suivre les étapes suivantes :

- Ajouter un nouveau domaine de sécurité au contrôleur de domaine ou au serveur autonome.
- Ajoutez les paramètres suivants au fichier **`jboss-ejb-client.properties`**, qui est dans le chemin de classes de l'application. Cet exemple suppose que la connexion est appelée **`par défaut`** par les autres paramètres qui se trouvent dans le fichier.

  ```
  remote.connection.default.username=appuser
  remote.connection.default.password=apppassword
  ```

- Créer un connecteur Remoting personnalisé sur le domaine ou sur le serveur autonome qui utilise le nouveau domaine de sécurité.

- Déployer votre EJB dans le groupe de serveur configuré pour utiliser le profil avec le connecteur Remoting personnalisé, ou dans le serveur autonome si vous n'utilisez pas de domaine géré.

Report a bug

14.4.4.6. Ajout d'un domaine de sécurité

1. **Exécuter le Management CLI**
   Démarrer par la commande **`jboss-cli.sh`** ou **`jboss-cli.bat`** et connectez-vous au serveur.

2. **Créer le nouveau domaine de sécurité lui-même.**
   Exécutez la commande suivante pour créer un nouveau domaine de sécurité nommé **`MyDomainRealm`** sur un contrôleur de domaine ou sur un serveur autonome.

   ```
   /host=master/core-service=management/security-
   realm=MyDomainRealm:add()
   ```

3. **Créer les références du fichier de propriétés qui stocke les informations sur le nouveau rôle.**
   Exécuter la commande suivante pour créer un pointeur au fichier nommé **`myfile.properties`**, qui contiendra les propriétés attachées au nouveau rôle.

   NOTE

   Le fichier de propriétés nouvellement créées n'est pas géré par les scripts **`add-user.sh`** et **`add-user.bat`** inclus. Il devra être administré en externe.

   ```
   /host=master/core-service=management/security-
   realm=MyDomainRealm/authentication=properties:add(path=myfile.proper
   ties)
   ```

Résultat

Votre nouveau domaine de sécurité est créé. Lorsque vous ajoutez des utilisateurs et des rôles à ce nouveau domaine, l'information va être stockée dans un fichier séparé des domaines de sécurité par défaut. Vous pouvez gérer ce nouveau fichier à l'aide de vos propres applications ou procédures.

Report a bug

14.4.4.7. Ajout d'un utilisateur à un domaine de sécurité

1. **Éxécuter la commande `add-user.sh` ou `add-user.bat`.**
   Ouvrez un terminal (shell) et changez de répertoire ***`EAP_HOME`*`/bin/`**. Si vous exécutez Red Hat Enterprise Linux ou un autre système d'exploitation style UNIX, exécutez **`add-user.sh`**. Si vous exécutez sur un serveur Microsoft Windows, exécutez **`add-user.bat`**.

2. **Choisissez d'ajouter un utilisateur de gestion ou un utilisateur d'application.**
   Pour cette procédure, saisir **b** pour ajouter un utilisateur d'application.

3. **Choisir le domaine dans lequel l'utilisateur sera ajouté.**
   Par défaut, le seul domaine disponible est **`ApplicationRealm`**. Si vous avez ajouté un domaine personnalisé, vous pouvez saisir son nom à la place.

4. **Saisir le nom d'utilisateur, le mot de passe et les rôles lorsque vous y serez invité.** Saisir le nom d'utilisateur, le mot de passe et les rôles lorsque vous y serez invité. Vérifiez votre choix en tapant **yes**, ou **no** pour annuler les changements. Les changements sont inscrits dans les fichiers de propriétés du domaine de sécurité.

Report a bug

14.4.4.8. Accès EJB à distance utilisant le cryptage SSL

Par défaut, le trafic réseau pour les RMI (Remote Method Invocation) des Beans EJB2 et EJB3 n'est pas crypté. Dans le cas où le cryptage est requis, SSL (Secure Sockets Layer) peut être utilisé afin que la connexion entre le client et le serveur soit cryptée. L'utilisation SSL a l'avantage supplémentaire de permettre au trafic réseau de traverser les pare-feu qui bloquent le port RMI.

Report a bug

14.5. SÉCURITÉ APPLICATION JAX-RS

14.5.1. Activer la sécurité basée-rôle pour RESTEasy JAX-RS Web Service

Résumé

RESTEasy supporte les annotations @RolesAllowed, @PermitAll, et @DenyAll sur les méthodes JAX-RS. Cependant, il ne reconnaît pas ces annotations par défaut. Suivre les étapes suivantes pour configurer le fichier `web.xml` et pour activer la sécurité basée-rôle.

AVERTISSEMENT

Ne pas activer la sécurité basée-rôle si l'application utilise les EJB. Le conteneur EJB procurera la fonctionnalité à la place de RESTEasy.

Procédure 14.3. Activer la sécurité basée-rôle pour RESTEasy JAX-RS Web Service

1. Ouvrir le fichier `web.xml` de l'application dans l'éditeur de textes.
2. Ajouter le <context-param> suivant au fichier, dans les balises **web-app**:

```
<context-param>
    <param-name>resteasy.role.based.security</param-name>
    <param-value>true</param-value>
</context-param>
```

3. Déclarer tous les rôles utilisés dans le fichier RESTEasy JAX-RS WAR file, en utilisant les balises de <security-role>:

```
<security-role><role-name>ROLE_NAME</role-name></security-role>
<security-role><role-name>ROLE_NAME</role-name></security-role>
```

4. Autorise l'accès à tous les URL gérés par le runtime JAX-RS pour tous les rôles :

```
<security-constraint><web-resource-collection><web-resource-
name>Resteasy</web-resource-name><url-pattern>/PATH</url-pattern>
</web-resource-collection><auth-constraint><role-
name>ROLE_NAME</role-name><role-name>ROLE_NAME</role-name></auth-
constraint></security-constraint>
```

Résultat

La sécurité basée rôle à été activée dans l'application, avec un certain nombre de rôles définis.

Exemple 14.14. Exemple de configuration de sécurité basée rôles

```
<web-app>

   <context-param>
 <param-name>resteasy.role.based.security</param-name>
 <param-value>true</param-value>
   </context-param>

   <servlet-mapping>
 <servlet-name>Resteasy</servlet-name>
 <url-pattern>/*</url-pattern>
   </servlet-mapping>

   <security-constraint>
 <web-resource-collection>
    <web-resource-name>Resteasy</web-resource-name>
    <url-pattern>/security</url-pattern>
 </web-resource-collection>
 <auth-constraint>
    <role-name>admin</role-name>
    <role-name>user</role-name>
 </auth-constraint>
   </security-constraint>

   <security-role>
 <role-name>admin</role-name>
   </security-role>
   <security-role>
 <role-name>user</role-name>
   </security-role>
```

```
</web-app>
```

Report a bug

14.5.2. Sécuriser un service JAX-RS Web par des annotations

Résumé

Cette rubrique couvre les étapes à parcourir pour sécuriser un service JAX-RS Web par les annotations de sécurité supportées.

Procédure 14.4. Sécuriser un service JAX-RS Web par des annotations de sécurité supportées.

1. Activer la sécurité basée-rôle. Pour plus d'informations, voir Section 14.5.1, « Activer la sécurité basée-rôle pour RESTEasy JAX-RS Web Service ».

2. Ajouter des annotations de sécurité au service JAX-RS Web. RESTEasy supporte les annotations suivantes :

   @RolesAllowed

   Définit les rôles qui peuvent accéder à la méthode. Tous les rôles doivent être définis dans le fichier `web.xml`.

   @PermitAll

   Autorise tous les rôles définis dans le fichier `web.xml` à accéder à la méthode.

   @DenyAll

   Refuse tout accès à la méthode.

Report a bug

14.6. PROTOCOLE MOTS DE PASSES DISTANTS SÉCURISÉS

14.6.1. Protocole pour mots de passes distants sécurisés (SRP pour Secure Remote Password)

Le protocole SRP est l'implémentation d'une poignée de main d'échange de clés publiques décrite dans Internet Standards Working Group Request For Comments 2945 (RFC2945). L'extrait de RFC2945 énonce ce qui suit :

> Ce document décrit un mécanisme d'authentification de réseau à cryptage puissant connu comme le nom de protocole SRP (Secure Remote Password). Ce mécanisme est approprié pour négocier des connexions sécurisées avec un mot de passe fourni par l'utilisateur, tout en éliminant les problèmes de sécurité traditionnellement associés à des mots de passe réutilisables. Ce système effectue également un échange de clés sécurisée dans le processus d'authentification, ce qui permet à ce que des couches de sécurité (protection de la vie privée et/ou de l'intégrité) soient activées lors de la session. Il n'est nul besoin de serveurs de clés de confiance ou d'infrastructures de certificats, et les clients ne sont pas tenus de stocker ou de gérer des clés à long

terme. SRP offre des avantages tant au niveau de la sécurité qu'au niveau déploiement sur les techniques existantes de stimulation / réponse, ce qui en fait un remplacement idéal pour les besoins d'authentification de mots de passe sécurisés.

On trouvera la description complète de la spécification RFC2945 à http://www.rfc-editor.org/rfc.html. Vous trouverez plus d'informations sur l'algorithme SRP et son historique à http://srp.stanford.edu/.

Les algorithmes Diffie-Hellman et RSA sont connus comme algorithmes d'échange de clés publiques. Le concept d'algorithmes à clé publique est d'avoir deux clés, une publique accessible à tous et une privée et uniquement connue par vous-même. Quand des personnes veulent vous envoyer des informations cryptées, ils cryptent les informations à l'aide de votre clé publique. Vous seul êtes capable de déchiffrer les informations à l'aide de votre clé privée. Cela contraste avec les systèmes de déchiffrage de mots de passe partagés plus traditionnels qui exigent que l'émetteur et le récepteur partagent le mot de passe. Les algorithmes à clé publiques éliminent le besoin de partager des mots de passe.

Report a bug

14.6.2. Configuration du protocole SRP (Secure Remote Password)

Afin d'utiliser le protocole SRP (Secure Remote Password) dans votre application, vous devrez tout d'abord créer un MBean qui implémente l'interface **`SRPVerifierStore`**. Vous trouverez des informations sur l'implémentation à Implémentation SRPVerifierStore.

Procédure 14.5. Intégrer le store de mots de passe existant

1. **Créer un store d'informations de mots de passe hachés.**
   Si vos mots de passe sont déjà stockés sous une forme hachée irréversible, vous aurez besoin de faire cela sur la base utilisateur.

   Vous pouvez implémenter un **`setUserVerifier(String, VerifierInfo)`** en tant que méthode noOp, ou d'une méthode qui envoie une exception signifiant que le store est en lecture-seule.

2. **Créer l'interface SRPVerifierStore.**
   Créer une implémentation d'interface **`SRPVerifierStore`** personnalisée qui puisse obtenir **`VerifierInfo`** du store que vous avez créé.

   Le **`verifyUserChallenge(String, Object)`** peut servir à intégrer des schémas basés token de matériel existant comme SafeWord ou Radius dans l'algorithme SRP. Cette méthode d'interface est appelée uniquement lorsque la configuration SRPLoginModule du client spécifie l'option hasAuxChallenge.

3. **Créer le MBean JNDI.**
   Créer un MBean qui expose l'interface **`SRPVerifierStore`** disponible à JNDI, et expose tous les paramètres configurables requis.

   Le service **`org.jboss.security.srp.SRPVerifierStoreService`** par défaut vous permet d'implémenter ceci. Vous pouvez également implémenter le MBean par une implémentation de fichier de propriétés Java du **`SRPVerifierStore`**.

Implémentation SRPVerifierStore

L'implémentation par défaut de l'interface **`SRPVerifierStore`** n'est pas recommandée pour les systèmes de production, car elle exige que toutes les informations de hachage de mot de passe soient disponibles sous forme de fichier d'objets sérialisés.

L'implémentation du **SRPVerifierStore** fournit un accès à l'objet **SRPVerifierStore.VerifierInfo** pour un nom d'utilisateur donné. La méthode **getUserVerifier(String)** est appelée par le SRPService au départ d'une session SRP utilisateur pour obtenir les paramètres requis par l'algorithme SRP.

Éléments d'un Objet VerifierInfo

nom d'utilisateur

Le nom d'utilisateur ou l'ID utilisateur pour s'authentifier

verifier

Un hachage unidirectionnel du mot de passe que l'utilisateur saisit comme preuve d'identité. La classe **org.jboss.security.Util** inclut une méthode **calculateVerifier** qui exécute l'algorithme de hachage de mot de passe. Le mot de passe de sortie prend la forme **H(salt | H(username | password))**, où **H** est la fonction de hachage sécurisée SHA, telle que définie par RFC2945. Le nom d'utilisateur est converti d'une chaîne en un byte [] en utilisant le codage UTF-8.

salt

Un nombre aléatoire utilisé pour augmenter la difficulté d'une attaque de force brute de dictionnaire sur la base de données de mot de passe de vérification dans le cas où la base de données soit compromise. La valeur doit être générée à partir d'un algorithme de cryptage fort composé de nombres aléatoires lorsque le mot de passe en texte clair existant de l'utilisateur est haché.

g

Le générateur primitif d'algorithme SRP. Cela peut être un paramètre fixe bien connu plutôt qu'un paramètre par utilisateur. La classe d'utilitaire de **org.jboss.security.srp.SRPConf** fournit plusieurs paramètres pour **g**, avec une valeur par défaut appropriée obtenue par l'intermédiaire de **SRPConf.getDefaultParams().g()**.

N

SRP algorithm safe-prime modulus. Cela peut être un paramètre fixe bien connu, plutôt qu'un paramètre par utilisateur. La classe d'utilitaire de **org.jboss.security.srp.SRPConf** fournit plusieurs paramètres pour «N», y compris un bon nombre de valeurs par défaut obtenues via **SRPConf.getDefaultParams().N()**.

Exemple 14.15. L'interface SRPVerifierStore

```
package org.jboss.security.srp;

import java.io.IOException;
import java.io.Serializable;
import java.security.KeyException;

public interface SRPVerifierStore
{
    public static class VerifierInfo implements Serializable
    {

        public String username;
```

```
        public byte[] salt;
        public byte[] g;
        public byte[] N;
    }


    public VerifierInfo getUserVerifier(String username)
        throws KeyException, IOException;

    public void setUserVerifier(String username, VerifierInfo info)
        throws IOException;


     public void verifyUserChallenge(String username, Object
auxChallenge)
         throws SecurityException;
}
```

Report a bug

14.7. L'ARCHIVAGE SÉCURISÉ DES MOTS DE PASSE POUR LES STRINGS DE NATURE CONFIDENTIELLE

14.7.1. Sécurisation des chaînes confidentielles des fichiers en texte clair

Les applications web et autres déploiements incluent souvent des fichiers en texte clair, comme des descripteurs de déploiement XML, qui comprennent des informations sensibles telles que les mots de passe et autres strings sensibles. JBoss EAP 6 inclut un mécanisme d'archivage sécurisé de mots de passe qui vous permet de crypter les strings sensibles et de les stocker dans un keystore chiffré. Le mécanisme d'archivage sécurisé parvient à décrypter les strings à utiliser dans les domaines de sécurité, ou autres systèmes de vérification. Ceci fournit une couche supplémentaire de sécurité. Le mécanisme s'appuie sur les outils qui sont inclus dans toutes les implémentations de Java Development Kit (JDK) prises en charge.

AVERTISSEMENT

Des problèmes ont été décelés lors de l'utilisation de la fonctionnalité de sécurité d'archivage sécurisé avec JBoss EAP 6. Il a été constaté que le vault.keystore générant le Sun/Oracle keytool n'est pas un fichier de clés valide lorsqu'il est utilisé avec un JDK IBM. Cela est dû au fait que les implémentations de keystore JCEKS diffèrent selon les vendeurs de Java.

Le problème se présente lorsqu'un fichier de clés généré par Oracle Java est utilisé dans une instance de JBoss EAP sur une installation Java d'IBM. Dans ces cas, le serveur ne démarre pas et lève l'exception suivante :

```
java.io.IOException:
com.sun.crypto.provider.SealedObjectForKeyProtector
```

À l'heure actuelle, la seule solution qui existe consiste à éviter toute tentative d'utilisation d'un fichier de clés généré avec un keytool Oracle dans un environnement utilisant une implémentation de Java d'IBM.

Report a bug

14.7.2. Créer un Keystore Java pour stocker des strings sensibles

Prérequis

- La commande **keytool** doit être disponible. Elle est fournie par le Java Runtime Environment (JRE). Chercher le chemin du fichier. Se trouve à l'emplacement suivant **/usr/bin/keytool** dans Red Hat Enterprise Linux.

Procédure 14.6. Installation du Java Keystore

1. **Créer un répertoire pour stocker votre keystore et autres informations cryptées.**
   Créer un répertoire qui contiendra votre keystore et autres informations pertinentes. Le reste de cette procédure assume que le répertoire est **/home/*USER*/vault/**.

2. **Déterminer les paramètres à utiliser avec keytool.**
   Déterminer les paramètres suivants :

   alias

   L'alias est un identificateur unique pour l'archivage sécurisé ou autres données stockées dans le keystore. L'alias dans l'exemple de commande à la fin de cette procédure est **vault** (archivage sécurisé). Les alias sont insensibles à la casse.

   keyalg

   L'algorithme à utiliser pour le cryptage. Dans cette procédure, l'exemple utilise **RSA**. Consultez la documentation de votre JRE et de votre système d'exploitation pour étudier vos possibilités.

keysize

La taille d'une clé de cryptage impacte sur la difficulté de décrypter au seul moyen de la force brutale. Dans cette procédure, l'exemple utilise **`1024`**. Pour plus d'informations sur les valeurs appropriées, voir la documentation distribuée avec **`keytool`**.

keystore

Le keystore est une base de données qui contient des informations chiffrées et des informations sur la façon de déchiffrer. Si vous ne spécifiez pas de keystore, le keystore par défaut à utiliser est un fichier appelé **`.keystore`** dans votre répertoire personnel. La première fois que vous ajoutez des données dans un keystore, il sera créé. L'exemple de cette procédure utilise le keystore **`vault.keystore`**.

La commande du **`keytool`** a plusieurs options. Consulter la documentation de votre JRE ou de votre système d'exploitation pour obtenir plus d'informations.

3. **Détermine les réponses aux questions que la commande `keystore` vous demandera.**
   Le **`keystore`** a besoin des informations suivantes pour remplir l'entrée du keytore :

   Mot de passe du keystore

   Lorsque vous créez un keystore, vous devez définir un mot de passe. Pour pouvoir travailler dans keystore dans le futur, vous devez fournir le mot de passe. Créer un mot de passe dont vous vous souviendrez. Le keystore est sécurisé par son mot de passe et par la sécurité du système d'exploitation et du système de fichiers où il se trouve.

   Mot de passe clé (en option)

   En plus du mot de passe du keystore, vous pouvez indiquer un mot de passe pour chaque clé contenue. Pour utiliser une clé, le mot de passe doit être donné à chaque utilisation. Normalement, cette fonction n'est pas utilisée.

   Prénom et nom de famille

   Cela, ainsi que le reste de l'information dans la liste, aide à identifier la clé de façon unique et à la placer dans une hiérarchie par rapport aux autres clés. Il ne doit pas nécessairement correspondre à un nom, mais doit être composé de deux mots et doit être unique à une clé. L'exemple dans cette procédure utilise **`Admninistrateur Comptabilité`**. En terme de répertoires, cela devient le *nom commun* du certificat.

   Unité organisationnelle

   Il s'agit d'un mot unique d'identification qui utilise le certificat. Il se peut que ce soit l'application ou l'unité commerciale. L'exemple de cette procédure utilise **`enterprise_application_platform`**. Normalement, tous les keystores utilisés par un groupe ou une application utilisent la même unité organisationnelle.

   Organisation

   Il s'agit normalement d'une représentation de votre nom d'organisation en un seul mot. Demeure constant à travers tous les certificats qui sont utilisés par une organisation. Cet exemple utilise **`MyOrganization`**.

   Ville ou municipalité

   Votre ville.

État ou province

Votre état ou province, ou l'équivalent pour votre localité.

Pays

Le code pays en deux lettres.

Ces informations vont créer ensemble une hiérarchie de vos keystores et certificats, qui garantira qu'ils utilisent une structure de nommage consistante, et unique.

4. **Exécuter la commande `keytool`, en fournissant les informations que vous avez collectées.**

Exemple 14.16. Exemple d'entrée et de sortie de la commande `keystore`

```
$ keytool -genseckey -alias vault -storetype jceks -keyalg AES -
keysize 128 -storepass vault22 -keypass vault22 -keystore
/home/USER/vault/vault.keystore
Enter keystore password: vault22
Re-enter new password:vault22
What is your first and last name?
  [Unknown]:  Accounting Administrator
What is the name of your organizational unit?
  [Unknown]:  AccountingServices
What is the name of your organization?
  [Unknown]:  MyOrganization
What is the name of your City or Locality?
  [Unknown]:  Raleigh
What is the name of your State or Province?
  [Unknown]:  NC
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=Accounting Administrator, OU=AccountingServices,
O=MyOrganization, L=Raleigh, ST=NC, C=US correct?
  [no]:  yes

Enter key password for <vault>
        (RETURN if same as keystore password):
```

Résultat

Un fichier nommé **`vault.keystore`** est créé dans le répertoire **`/home/`*`USER`*`/vault/`**. Il stocke une clé simple, nommée **`vault`**, qui sera utilisée pour stocker des strings cryptés, comme des mots de passe, pour la plateforme JBoss EAP 6.

Report a bug

14.7.3. Masquer le mot de passe du keystore et initialiser le mot de passe de l'archivage de sécurité

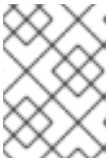
Prérequis

- Section 14.7.2, « Créer un Keystore Java pour stocker des strings sensibles »

- L'application ***EAP_HOME*/bin/vault.sh** doit pouvoir être accessible via l'interface de ligne de commande.

1. **Exécuter la commande `vault.sh`.**
   Exécuter ***EAP_HOME*/bin/vault.sh**. Démarrer une nouvelle session interactive en tapant **`0`**.

2. **Saisir le nom du répertoire où les fichiers cryptés seront stockés.**
   Ce répertoire doit être raisonnablement sécurisé, mais JBoss EAP 6 doit pouvoir y accéder. Si vous suivez Section 14.7.2, « Créer un Keystore Java pour stocker des strings sensibles » , votre keystore sera dans un répertoire nommé **`vault/`** dans votre répertoire de base (home). Cet exemple utilise le répertoire **`/home/`*`USER`*`/vault/`**.

   NOTE

   N'oubliez pas d'inclure la barre oblique finale dans le nom du répertoire. Soit / ou \, selon votre système d'exploitation.

3. **Saisir le nom de votre keystore.**
   Saisir le nom complet vers le fichier de keystore. Cet exemple utilise **`/home/`*`USER`*`/vault/vault.keystore`**.

4. **Crypter le mot de passe du keystore.**
   Les étapes suivantes vous servent à crypter le mot de passe du keystore, afin que vous puissiez l'utiliser dans les applications et les fichiers de configuration en toute sécurité

   a. **Saisir le mot de passe du keystore.**
      Quand vous y serez invité, saisir le mot de passe du keystore.

   b. **Saisir une valeur salt.**
      Entrez une valeur salt de 8 caractères. La valeur salt, ainsi que le nombre d'itérations (ci-dessous), sont utilisés pour créer la valeur de hachage

   c. **Saisir le nombre d'itérations.**
      Saisir un nombre pour le nombre d'itérations.

   d. **Notez les informations de mot de passe masqué.**
      Le mot de passe masqué, salt et le nombre d'itérations sont imprimés en sortie standard. Prenez-en note dans un endroit sûr. Un attaquant pourrait les utiliser pour déchiffrer le mot de passe.

   e. **Saisir un alias pour l'archivage de sécurité.**
      Quand on vous y invite, saisir un alias pour l'archivage de sécurité. Si vous suivez Section 14.7.2, « Créer un Keystore Java pour stocker des strings sensibles » pour créer votre archivage de sécurité, l'alias sera **`vault`**.

5. **Sortir de la console interactive.**
   Saisir **2** pour sortir de la console interactive.

Résultat

Votre mot de passe de keystore est masqué afin de pouvoir être utilisé dans les fichiers de configuration et de déploiement. De plus, votre archivage de sécurité est complètement configuré et prêt à l'utilisation.

Report a bug

14.7.4. Configurer JBoss EAP pour qu'il utilise l'archivage sécurisé des mots de passe

Aperçu

Avant de masquer les mots de passe et d'autres attributs sensibles dans les fichiers de configuration, vous devez sensibiliser JBoss EAP 6 à l'archivage sécurisé des mots de passe qui les stocke et les déchiffre. Actuellement, cela vous oblige à arrêter Enterprise Application Platform et à modifier la configuration directement.

Prérequis

- Section 14.7.2, « Créer un Keystore Java pour stocker des strings sensibles »
- Section 14.7.3, « Masquer le mot de passe du keystore et initialiser le mot de passe de l'archivage de sécurité »

Procédure 14.7. Assigner un mot de passe d'archivage sécurisé.

1. **Déterminer les valeurs qui conviennent pour la commande.**
   Déterminer les valeurs pour les paramètres suivants, déterminés par les commandes utilisées pour créer le keystore lui-même. Pour obtenir des informations sur la façon de créer un keystore, voir les sujets suivants : Section 14.7.2, « Créer un Keystore Java pour stocker des strings sensibles » et Section 14.7.3, « Masquer le mot de passe du keystore et initialiser le mot de passe de l'archivage de sécurité ».

Paramètre	Description
KEYSTORE_URL	Le chemin d'accès ou URI du fichier keystore, qui s'appelle normalement `vault.keystore`
KEYSTORE_PASSWORD	Le mot de passe utilisé pour accéder au keystore. Cette valeur devrait être masquée.
KEYSTORE_ALIAS	Le nom du keystore.
SALT	Le salt utilisé pour crypter et décrypter les valeurs de keystore.
ITERATION_COUNT	Le nombre de fois que l'algorithme de chiffrement est exécuté.
ENC_FILE_DIR	Le chemin d'accès au répertoire à partir duquel les commandes de keystore sont exécutées. Normalement, le répertoire contient les mots de passe sécurisés.
hôte (domaine géré uniquement)	Le nom de l'hôte que vous configurez

2. **Utiliser le Management CLI pour activer les mots de passe sécurisés.**
   Exécutez une des commandes suivantes, selon que vous utilisez un domaine géré ou une configuration de serveur autonome. Substituez les valeurs de la commande par celles de la première étape de cette procédure.

NOTE

Si vous utilisez Microsoft Windows Server, remplacer chaque caractère de / dans un chemin d'accès de nom de fichier ou de répertoire par quatre caractères \. C'est parce qu'il faut deux caractères \, chacun échappé. Cela n'a pas besoin d'être fait pour les autres caractères /.

- **Domaine géré**

```
/host=YOUR_HOST/core-service=vault:add(vault-options=
[("KEYSTORE_URL" => "PATH_TO_KEYSTORE"), ("KEYSTORE_PASSWORD" =>
"MASKED_PASSWORD"), ("KEYSTORE_ALIAS" => "ALIAS"), ("SALT" =>
"SALT"),("ITERATION_COUNT" => "ITERATION_COUNT"), ("ENC_FILE_DIR"
=> "ENC_FILE_DIR")])
```

- **Serveur autonome**

```
/core-service=vault:add(vault-options=[("KEYSTORE_URL" =>
"PATH_TO_KEYSTORE"), ("KEYSTORE_PASSWORD" => "MASKED_PASSWORD"),
("KEYSTORE_ALIAS" => "ALIAS"), ("SALT" => "SALT"),
("ITERATION_COUNT" => "ITERATION_COUNT"), ("ENC_FILE_DIR" =>
"ENC_FILE_DIR")])
```

Ce qui suit est un exemple de la commande avec des valeurs hypothétiques :

```
/core-service=vault:add(vault-options=[("KEYSTORE_URL" =>
"/home/user/vault/vault.keystore"), ("KEYSTORE_PASSWORD" => "MASK-
3y28rCZlcKR"), ("KEYSTORE_ALIAS" => "vault"), ("SALT" =>
"12438567"),("ITERATION_COUNT" => "50"), ("ENC_FILE_DIR" =>
"/home/user/vault/")])
```

Résultat

JBoss EAP 6 est configuré pour décrypter les strings masqués par l'intermédiaire de l'archivage sécurisé de mots de passe. Pour ajouter des strings à l'archivage sécurisé, et les utiliser dans votre configuration, voir la section suivante : Section 14.7.5, « Stocker et résoudre des strings sensibles cryptés du Keystore Java. ».

Report a bug

14.7.5. Stocker et résoudre des strings sensibles cryptés du Keystore Java.

Résumé

En comptant les mots de passe et les autres strings sensibles, les fichiers de configuration en texte brut ne sont pas sécurisés. JBoss EAP 6 inclut la capacité de stocker et d'utiliser les valeurs masquées dans les fichiers de configuration, et d'utiliser ces valeurs masquées dans les fichiers de configuration.

Prérequis

- Section 14.7.2, « Créer un Keystore Java pour stocker des strings sensibles »
- Section 14.7.3, « Masquer le mot de passe du keystore et initialiser le mot de passe de l'archivage de sécurité »

- Section 14.7.4, « Configurer JBoss EAP pour qu'il utilise l'archivage sécurisé des mots de passe »
- L'application ***EAP_HOME*/bin/vault.sh** doit pouvoir être accessible via l'interface de ligne de commande.

Procédure 14.8. Installation du Java Keystore

1. **Exécuter la commande `vault.sh`.**
   Exécuter ***EAP_HOME*/bin/vault.sh**. Démarrer une nouvelle session interactive en tapant **`0`**.

2. **Saisir le nom du répertoire où les fichiers cryptés seront stockés.**
   Si vous suivez Section 14.7.2, « Créer un Keystore Java pour stocker des strings sensibles » , votre keystore sera dans un répertoire nommé **`vault/`** de votre répertoire de base. Dans la plupart des cas, il est logique de stocker toutes vos informations cryptées au même endroit dans le keystore. Cet exemple utilise le répertoire **`/home/`*`USER`*`/vault/`**.

   NOTE

   N'oubliez pas d'inclure la barre oblique finale dans le nom du répertoire. Soit `/` ou `\`, selon votre système d'exploitation.

3. **Saisir le nom de votre keystore.**
   Saisir le nom complet vers le fichier de keystore. Cet exemple utilise **`/home/`*`USER`*`/vault/vault.keystore`**.

4. **Saisir le mot de passe du keystore, le nom de l'archivage sécurisé, salt, et le nombre d'itérations.**
   Quand vous y êtes invité, saisir le mot de passe du keystore, le nom de l'archivage sécurisé, salt, et le nombre d'itérations.

5. **Sélectionner l'option de stockage d'un mot de passe.**
   Sélectionner l'option **`0`** de stockage d'un mot de passe ou autre string sensible.

6. **Saisir la valeur.**
   Une fois que vous y êtes invité, saisir la valeur deux fois. Si les valeurs ne correspondent pas, vous serez invité à essayer à nouveau.

7. **Saisir le bloc d'archivage sécurisé.**
   Saisir le bloc d'archivage sécurisé, qui est un conteneur pour les attributs qui ont trait à la même ressource. Un exemple de nom d'attribut serait **`ds_ExampleDS`**. Cela fera partie de la référence à la chaîne cryptée, dans votre source de données ou autre définition de service.

8. **Saisir le nom de l'attribut.**
   Saisir le nom de l'attribut que vous stockez. Exemple de nom d'attribut **`password`**.

   Résultat

   Un message comme celui qui suit montre que l'attribut a été sauvegardé.

   ```
   Valeur de l'attribut pour (ds_ExampleDS, password) sauvegardé
   ```

9. **Notez les informations pour ce string crypté.**

Un message s'affiche sur la sortie standard, montrant le bloc d'archivage sécurisé, le nom de l'attribut, la clé partagée et des conseils sur l'utilisation du string dans votre configuration. Prendre note de ces informations dans un emplacement sécurisé. Voici un exemple de sortie.

```
*****************************************
Vault Block:ds_ExampleDS
Attribute Name:password
Configuration should be done as follows:
VAULT::ds_ExampleDS::password::1
*****************************************
```

10. **Utiliser le string crypté dans votre configuration.**
Utiliser le string de l'étape de configuration précédente, à la place du string en texte brut. Une source de données utilisant le mot de passe crypté ci-dessus, est montrée ci-dessous.

```
...
  <subsystem xmlns="urn:jboss:domain:datasources:1.0">
    <datasources>
      <datasource jndi-name="java:jboss/datasources/ExampleDS"
enabled="true" use-java-context="true" pool-name="H2DS">
        <connection-url>jdbc:h2:mem:test;DB_CLOSE_DELAY=-
1</connection-url>
        <driver>h2</driver>
        <pool></pool>
        <security>
          <user-name>sa</user-name>
          <password>${VAULT::ds_ExampleDS::password::1}</password>
        </security>
      </datasource>
      <drivers>
         <driver name="h2" module="com.h2database.h2">
            <xa-datasource-class>org.h2.jdbcx.JdbcDataSource</xa-
datasource-class>
         </driver>
      </drivers>
    </datasources>
  </subsystem>
...
```

Vous pouvez utiliser un string crypté n'importe où dans votre fichier de configuration autonome ou de domaine pour lequel les expressions sont autorisées.

NOTE

Pour vérifier si les expressions sont utilisées dans un sous-système particulier, exécuter la commande CLI suivante sur ce sous-système :

```
/host=master/core-service=management/security-
realm=TestRealm:read-resource-description(recursive=true)
```

À partir du résultat de cette commande, chercher la valeur du paramètre **`expressions-allowed`**. Si 'true', vous pourrez utiliser des expressions dans la configuration de ce sous-système particulier.

Une fois que vous aurez mis votre string dans le keystore, utiliser la syntaxe suivante pour remplacer tout string en texte claire par un texte crypté.

```
${VAULT::<replaceable>VAULT_BLOCK</replaceable>::
<replaceable>ATTRIBUTE_NAME</replaceable>::
<replaceable>ENCRYPTED_VALUE</replaceable>}
```

Voici un exemple de valeur réelle, où le bloc d'archivage sécurisé est **ds_ExampleDS** et l'attribut est **password**.

```
<password>${VAULT::ds_ExampleDS::password::1}</password>
```

Report a bug

14.7.6. Stocker et résoudre des strings sensibles de vos applications

Aperçu

Les éléments de configuration de la plate-forme JBoss EAP 6 prennent en charge la capacité de régler les chaînes cryptées en fonction des valeurs stockées dans Java Keystore, via le mécanisme Security Vault. Vous pouvez ajouter le support pour cette fonctionnalité à vos propres applications.

Tout d'abord, ajoutez le mot de passe dans votre Security Vault. En second lieu, remplacer le mot de passe de texte clair par celui qui est stocké dans le Security Vault. Vous pouvez utiliser cette méthode pour obscurcir les strings sensibles de votre application.

Prérequis

Avant d'effectuer cette procédure, assurez-vous que le répertoire pour stocker vos fichiers dans le Security Vault existe bien. Qu'importe où vous les placez, tant que l'utilisateur qui exécute JBoss EAP 6 dispose de l'autorisation de lire et écrire des fichiers. Cet exemple situe le répertoire **vault/** dans le répertoire **/home/*USER*/vault/**. Le Security Vault lui-même correspond à un fichier nommé **vault.keystore** qui se trouve dans le répertoire **vault/**.

Exemple 14.17. Ajout du string de mot de passe au Security Vault

Ajouter le string au Security Vault par la commande ***EAP_HOME*/bin/vault.sh**. La série de commandes et réponses est incluse dans la session suivante. Les valeurs saisies par l'utilisateur apparaîtront clairement. Certaines sorties seront supprimées pour le formatage. Dans Microsoft Windows, le nom de la commande est **vault.bat**. Notez que dans Microsoft Windows, les chemins d'accès au fichier utilisent le caractère \ comme séparateur de répertoire, et non pas le caractère /.

```
[user@host bin]$ ./vault.sh
*********************************
****  JBoss Vault ********
*********************************
Please enter a Digit::   0: Start Interactive Session  1: Remove
Interactive Session  2: Exit
0
Starting an interactive session
Enter directory to store encrypted files:/home/user/vault/
Enter Keystore URL:/home/user/vault/vault.keystore
Enter Keystore password: ...
Enter Keystore password again: ...
```

```
Values match
Enter 8 character salt:12345678
Enter iteration count as a number (Eg: 44):25

Enter Keystore Alias:vault
Vault is initialized and ready for use
Handshake with Vault complete
Please enter a Digit::   0: Store a password  1: Check whether password
exists  2: Exit
0
Task:  Store a password
Please enter attribute value: sa
Please enter attribute value again: sa
Values match
Enter Vault Block:DS
Enter Attribute Name:thePass
Attribute Value for (DS, thePass) saved

Please make note of the following:
********************************************
Vault Block:DS
Attribute Name:thePass
Configuration should be done as follows:
VAULT::DS::thePass::1
********************************************

Please enter a Digit::   0: Store a password  1: Check whether password
exists  2: Exit
2
```

La chaîne qui sera ajoutée au code Java est la dernière valeur de sortie, la ligne commençant par **VAULT**.

Le servlet suivant utilise la chaîne voûtée au lieu d'un mot de passe de texte clair. La version en texte clair est commentée afin que vous puissiez voir la différence.

Exemple 14.18. Servlet qui utilise un mot de passe Vaulted

```
package vaulterror.web;

import java.io.IOException;
import java.io.Writer;

import javax.annotation.Resource;
import javax.annotation.sql.DataSourceDefinition;
import javax.servlet.ServletException;
import javax.servlet.annotation.WebServlet;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import javax.sql.DataSource;


/*@DataSourceDefinition(
        name = "java:jboss/datasources/LoginDS",
```

```
        user = "sa",
        password = "sa",
        className = "org.h2.jdbcx.JdbcDataSource",
        url = "jdbc:h2:tcp://localhost/mem:test"
)*/
@DataSourceDefinition(
        name = "java:jboss/datasources/LoginDS",
        user = "sa",
        password = "VAULT::DS::thePass::1",
        className = "org.h2.jdbcx.JdbcDataSource",
        url = "jdbc:h2:tcp://localhost/mem:test"
)
@WebServlet(name = "MyTestServlet", urlPatterns = { "/my/" },
loadOnStartup = 1)
public class MyTestServlet  extends HttpServlet {

    private static final long serialVersionUID = 1L;


    @Resource(lookup = "java:jboss/datasources/LoginDS")
    private DataSource ds;

    @Override
    protected void doGet(HttpServletRequest req, HttpServletResponse
resp) throws ServletException, IOException {
        Writer writer = resp.getWriter();
        writer.write((ds != null) + "");
    }
}
```

Votre servlet est maintenant capable de résoudre le string Vaulted.

Report a bug

14.8. JAVA AUTHORIZATION CONTRACT FOR CONTAINERS (JACC)

14.8.1. Java Authorization Contract for Containers (JACC)

Java Authorization Contract for Containers (JACC) est une norme qui définit un contrat entre les conteneurs et les fournisseurs de services d'autorisation, et qui se traduit par l'implémentation de fournisseurs qui seront utilisés par des conteneurs. Elle a été définie dans JSR-115, qui se trouve sur le site Web de Java Community Process http://jcp.org/en/jsr/detail?id=115. Elle a fait partie de la spécification Java Enterprise Edition (Java EE) depuis la version 1.3 de Java EE.

JBoss EAP 6 implémente un support pour JACC dans la fonctionnalité de sécurité du sous-système de sécurité.

Report a bug

14.8.2. Configurer la sécurité JACC (Java Authorization Contract for Containers)

Pour configurer JACC (Java Authorization Contract for Containers), il convient de configurer votre domaine de sécurité avec le module qui convient, puis de modifier votre fichier **`jboss-web.xml`** pour y inclure les paramètres qu'il faut.

Ajouter JACC Support au domaine de sécurité

Pour ajouter JACC au domaine de sécurité, ajouter la police d'autorisation **JACC** à la pile d'autorisations du domaine de sécurité, avec l'indicateur **`requis`**. Voici un exemple de domaine de sécurité avec support JACC. Cependant, le domaine de sécurité est configuré dans la console de gestion ou Management CLI, plutôt que directement dans le code XML.

```
<security-domain name="jacc" cache-type="default">
    <authentication>
        <login-module code="UsersRoles" flag="required">
        </login-module>
    </authentication>
    <authorization>
        <policy-module code="JACC" flag="required"/>
    </authorization>
</security-domain>
```

Configurer une application web qui utilise JACC

Le fichier **`jboss-web.xml`** se trouve dans **`META-INF/`** ou dans le répertoire **`WEB-INF/`** de votre déploiement, et contient des ajouts ou remplacements de configuration spécifique JBoss pour le conteneur web. Pour utiliser votre domaine de sécurité activé-JACC, vous devrez inclure l'élément **`<security-domain>`**, et aussi définir l'élément **`<use-jboss-authorization>`** sur **`true`**. L'application suivante est configurée correctement pour pouvoir utiliser le domaine de sécurité JACC ci-dessus.

```
<jboss-web>
    <security-domain>jacc</security-domain>
    <use-jboss-authorization>true</use-jboss-authorization>
</jboss-web>
```

Configurer une application EJB pour utiliser JACC

La façon de configurer les EJB pour qu'ils utilisent un domaine de sécurité et pour qu'ils utilisent JACC diffère des applications Web. Pour un EJB, vous pouvez déclarer des *method permissions* (permissions de méthode) sur une méthode ou sur un groupe de méthodes, dans le descripteur **`ejb-jar.xml`**. Dans l'élément **`<ejb-jar>`**, chaque élément **`<method-permission>`** dépendant contient des informations sur les rôles JACC. Voir l'exemple de configuration pour plus d'informations. La classe **`EJBMethodPermission`** fait partie de l'API Java Enterprise Edition 6, et est documentée dans http://docs.oracle.com/javaee/6/api/javax/security/jacc/EJBMethodPermission.html.

Exemple 14.19. Exemple de permissions de méthode JACC dans un EJB

```
<ejb-jar>
  <method-permission>
    <description>The employee and temp-employee roles may access any
method of the EmployeeService bean </description>
    <role-name>employee</role-name>
    <role-name>temp-employee</role-name>
    <method>
```

```
      <ejb-name>EmployeeService</ejb-name>
      <method-name>*</method-name>
    </method>
  </method-permission>
</ejb-jar>
```

Vous pouvez également contraindre les mécanismes d'authentification et d'autorisation d'un EJB à l'aide d'un domaine de sécurité, comme vous pouvez le faire pour une application web. Les domaines de sécurité sont déclarés dans le descripteur **jboss-ejb3.xml** qui se trouve dans l'élément enfant **<security>**. En plus du domaine de sécurité, vous pouvez également spécifier le *run-as principal*, qui change le principal que l'EJB exécute.

Exemple 14.20. Exemple de déclaration de domaine de sécurité dans un EJB

```
<security>
  <ejb-name>*</ejb-name>
  <security-domain>myDomain</security-domain>
  <run-as-principal>myPrincipal</run-as-principal>
</security>
```

Report a bug

14.9. JAVA AUTHENTICATION SPI FOR CONTAINERS (JASPI)

14.9.1. Sécurité Java Authentication SPI pour Conteneurs (JASPI)

Java Application SPI pour Conteneurs (JASPI ou JASPIC) est une interface enfichable pour applications JSR-196 du Java Community Process. Consulter http://www.jcp.org/en/jsr/detail?id=196 pour obtenir des informations sur la spécification.

Report a bug

14.9.2. Configuration de la sécurité Java Authentication SPI pour conteneurs (JASPI)

Pour s'authentifier auprès d'un fournisseur JASPI, ajouter un élément **<authentication-jaspi>** à votre domaine de sécurité. La configuration est similaire à celle d'un module d'authentification standard, mais les éléments de module de login sont inclus dans l'élément **<login-module-stack>**. La structure de configuration est la suivante :

Exemple 14.21. Structure de l'élément authentication-jaspi

```
<authentication-jaspi>
 <login-module-stack name="...">
   <login-module code="..." flag="...">
```

```
      <module-option name="..." value="..."/>
    </login-module>
  </login-module-stack>
  <auth-module code="..." login-module-stack-ref="...">
    <module-option name="..." value="..."/>
  </auth-module>
</authentication-jaspi>
```

Le module de connexion est lui-même configuré de la même façon que le module d'authentification standard.

Comme la console de gestion basée web n'expose pas la configuration des modules d'authentification JASPI, vous devez stopper la plateforme JBoss EAP 6 complètement avant d'ajouter la configuration directement dans le fichier ***EAP_HOME*/domain/configuration/domain.xml** ou dans le fichier ***EAP_HOME*/standalone/configuration/standalone.xml**.

Report a bug

CHAPITRE 15. SINGLE SIGN ON (SSO)

15.1. SSO (SINGLE SIGN ON) POUR LES APPLICATIONS WEB

Aperçu

*Single Sign On (SSO)*autorise l'authentification à une ressource, en vue d'autoriser implicitement l'accès à d'autres ressources.

SSO clusterisés ou non-clusterisés

SSO Non-clusterisé limite le partage des informations d'autorisation pour les applications d'un même hôte virtuel. En outre, il n'y a aucun mécanisme de résilience en cas de défaillance de l'hôte. Les données d'authentification SSO clusterisées peuvent être partagées entre les applications de plusieurs hôtes virtuels et sont résistantes au basculement. De plus, SSO clusterisé est capable de recevoir des demandes d'un équilibreur de charges.

La façon dont SSO fonctionne

Si une ressource n'est pas protégée, un utilisateur n'a pas besoin de s'authentifier. Si un utilisateur accède à une ressource protégée, l'utilisateur devra s'authentifier.

Si l'authentification réussit, les rôles associés à l'utilisateur seront stockés et utilisés pour l'autorisation de toutes les ressources associées.

Si l'utilisateur se déconnecte d'une application, ou bien si l'application produit la session par programmation, toutes les données d'autorisation persistées seront retirées, et le processus recommencera.

Un timeout de session ne rend pas la session SSO valide si d'autres sessions sont encore valides.

Les limitations de SSO

Aucune propagation au-delà des limites de tierce-parties.

SSO ne peut être utilisé qu'entre des applications déployées au sein de conteneurs JBoss EAP 6.

Authentification gérée-conteneur uniquement.

Vous devez utiliser des éléments d'authentification géré-conteneurs, comme **`<login-config>`** dans le **`web.xml`** de votre application.

Nécessite des cookies.

SSO se maintient par des cookies de navigateur et la ré-écriture d'URL n'est pas prise en charge.

Limitations de domaine et de domaine de sécurité

À moins que le paramètre **`requireReauthentication`** soit défini à **`true`**, toutes les applications web configurées pour la même valve SSO devront partager la même configuration Realm dans **`web.xml`** et le même domaine de sécurité.

Vous pouvez imbriquer l'élément Realm à l'intérieur de l'élément Hôte ou de l'élément Engine environnant, mais pas à l'intérieur d'un élément context.xml pour une des applications web concernées

Le **`<security-domain>`** configuré dans **`jboss-web.xml`** doit être consistant à travers toutes les applications web.

Toutes les intégrations de sécurité doivent pouvoir accepter les mêmes informations d'autorisation (comme les noms d'utilisateur et mots de passe).

Report a bug

15.2. SSO (SINGLE SIGN ON) CLUSTERISÉES POUR LES APPLICATIONS WEB

SSO (Single Sign On) est la possibilité pour les utilisateurs de s'authentifier à une application web unique au moyen d'une authentification réussie, afin d'obtenir l'autorisation de plusieurs autres applications. SSO clusterisée stocke les informations d'authentification et d'autorisation dans un cache clusterisé. Cela permet aux applications de serveurs différents de partager l'information et rend également l'information résistante à une défaillance de l'un des hôtes.

Une configuration SSO s'appelle une vanne. Une vanne est connectée à un domaine de sécurité, qui est configuré au niveau du serveur ou du groupe de serveurs. Chaque application qui doit partager les mêmes informations d'authentification mises en cache est configurée pour utiliser la même valve. Cette configuration s'effectue dans le fichier **`jboss-Web.xml`** de l'application.

Voici quelques valves SSO standards prises en charge par le sous-système de JBoss EAP 6 :

- Apache Tomcat ClusteredSingleSignOn
- Apache Tomcat IDPWebBrowserSSOValve
- SSO basée-SPNEGO de PicketLink

Suivant le type particulier de valve, vous aurez sans doute besoin d'ajouter des configurations supplémentaires au domaine de sécurité, pour que votre valve puisse fonctionner normalement.

Report a bug

15.3. CHOISIR L'IMPLÉMENTATION SSO QUI VOUS CONVIENT

JBoss EAP 6 exécute des applications de JBoss Enterprise Edition (EE), qui peuvent être des applications web, des applications EJB, des services web ou autres. SSO (Single Sign On) permet de propager les informations de contexte et d'identité de sécurité entre ces applications. Selon les besoins de votre organisation, il existe des solutions SSO différentes. La solution que vous utiliserez dépendra du fait que vous utilisez des applications web, les applications EJB ou des services web; si vos applications s'exécutent sur le même serveur, plusieurs serveurs non-clusterisés ou plusieurs serveurs clusterisés; ou si vous souhaitez l'intégrer dans un système d'authentification basé-bureau où vous avez seulement besoin d'authentification entre vos applications.

SSO Desktop basé-Kerberos

Si votre organisation utilise déjà une authentification basée Kerberos et un système d'autorisation comme Microsoft Active Directory, vos pourrez utiliser les mêmes systèmes pour vous authentifier de façon transparente à vos applications enterprise en cours d'exécution sur JBoss EAP 6.

SSO Application Web et Non clusterisée

Si vous avez besoin de propager des informations de sécurité entre des applications qui s'exécutent dans le même groupe de serveurs ou instance, vous pourrez utiliser le SSO non-clusterisé. Cela implique uniquement la configuration de la valve dans le descripteur de **`jboss-web.xml`** de votre application.

SSO Application Web et clusterisée

Si vous avez besoin de propager des informations de sécurité entre des applications qui s'exécutent dans un environnement clusterisé sur plusieurs instances de JBoss EAP 6, vous pourrez utiliser la valve SSO clusterisée. Ce paramètre est configuré dans le fichier **`jboss-Web.xml`** de votre application.

Report a bug

15.4. UTILISATION DE SSO (SINGLE SIGN ON) POUR LES APPLICATIONS WEB

Aperçu

Les fonctionnalités SSO (Single Sign On) sont fournies par les sous-systèmes web et Infinispan. Utiliser cette procédure pour configurer SSO dans les applications web.

Prérequis

- Vous devez avoir un domaine de sécurité configuré qui gère les authentifications et autorisations.
- Le sous-système **`infinispan`** doit être présent. Il se trouve dans le profil **`complet-ha`** pour un domaine géré, ou en utilisant la configuration **`standalone-full-ha.xml`** dans un serveur autonome.
- Le **web** **`cache-conteneur`** et le cache-conteneur SSO doivent chacun être présents. Les exemples de fichiers de configurations contiennent déjà le cache-conteneur **web**, et certaines des configurations contiennent déjà le cache-conteneur SSO également. Utilisez les commandes suivantes pour vérifier et activer le cache conteneur SSO. Notez que ces commandes modifient le profil **ha** d'un domaine géré. Vous pouvez modifier les commandes pour utiliser un profil différent, ou supprimer la portion **`/profile=ha`** de la commande, pour un serveur autonome.

> **Exemple 15.1. Vérifier le cache-conteneur `web`**
>
> Les profils et les configurations mentionnées ci-dessus incluent le cache-conteneur **web** par défaut. Utilisez la commande suivante pour vérifier sa présence. Si vous utilisez un profil différent, remplacez par son nom à la place de **ha**.
>
> ```
> /profile=ha/subsystem=infinispan/cache-container=web/:read-
> resource(recursive=false,proxies=false,include-
> runtime=false,include-defaults=true)
> ```
>
> Si le résultat affiche un **success**, le sous-système sera présent. Sinon, vous devrez l'ajouter.

> **Exemple 15.2. Ajouter le cache-conteneur `web`**
>
> Utiliser les trois commandes suivantes pour activer le cache-conteneur **web** à votre configuration. Modifier le nom du profil selon le cas, ainsi que les autres paramètres. Ici, les paramètres sont ceux utilisés dans une configuration par défaut.

```
/profile=ha/subsystem=infinispan/cache-container=web:add(aliases=
["standard-session-cache"],default-
cache="repl",module="org.jboss.as.clustering.web.infinispan")
```

```
/profile=ha/subsystem=infinispan/cache-
container=web/transport=TRANSPORT:add(lock-timeout=60000)
```

```
/profile=ha/subsystem=infinispan/cache-container=web/replicated-
cache=repl:add(mode="ASYNC",batching=true)
```

Exemple 15.3. Vérifier le cache-conteneur SSO

Éxécuter la commande de Management CLI suivante :

```
/profile=ha/subsystem=infinispan/cache-container=web/:read-
resource(recursive=true,proxies=false,include-
runtime=false,include-defaults=true)
```

Chercher une sortie qui ressemble à ceci : **`"sso" => {`**

Si vous ne la trouvez pas, le cache-conteneur ne sera pas présent dans votre configuration.

Exemple 15.4. Ajouter le cache-conteneur SSO

```
/profile=ha/subsystem=infinispan/cache-container=web/replicated-
cache=sso:add(mode="SYNC", batching=true)
```

- Le sous-système **web** doit être configuré pour utiliser SSO. La commande suivante active SSO sur le serveur virtuel appelé **`default-host`** et le domaine de cookies **`domaine.com`**. Le nom de cache est **sso**, et une nouvelle authentification est désactivée.

```
/profile=ha/subsystem=web/virtual-server=default-
host/sso=configuration:add(cache-container="web",cache-
name="sso",reauthenticate="false",domain="domain.com")
```

- Chaque application qui partage les informations SSO doit être configurée pour utiliser le même <security-domain> dans son descripteur de déploiement de **`jboss-web.xml`** et le même Realm dans son fichier de configuration **`web.xml`**.

Différences entre les valves clusteriées et les valves non-clusterisées

SSO clusterisée permet le partage d'authentification entre des hôtes distincts, tandis que ce n'est pas le cas pour SSO non-clusterisée. Les valves SSO en cluster et non clusterisées sont configurées de la même manière, mais SSO clusterisée comprend les paramètres **`cacheConfig`**, **`processExpiresInterval`** et **`maxEmptyLife`**, qui contrôlent la réplication en groupement des données persistantes.

Exemple 15.5. Exemple de configuration SSO clusterisée

Comme les configurations SSO clusterisées ou non sont si semblables, on ne montre que la configuration clusterisée. Cet exemple utilise un domaine de sécurité nommé **tomcat**.

```
<jboss-web>
 <security-domain>tomcat</security-domain>
 <valve>
  <class-
name>org.jboss.web.tomcat.service.sso.ClusteredSingleSignOn</class-name>
  <param>
   <param-name>maxEmptyLife</param-name>
   <param-value>900</param-value>
  </param>
 </valve>
</jboss-web>
```

Tableau 15.1. Options de configuration SSO

Option	Description
cookieDomain	Domaine hôte utilisé pour les cookies SSO. La valeur par défaut est **/**. Pour permettre à **app1.xyz.com** et à **app2.xyz.com** de partager les cookies SSO, vous devrez définir le cookieDomain à **xyz.com**.
maxEmptyLife	SSO clusterisée uniquement. Le nombre maximum de secondes qu'une valve SSO sans sessions actives sera utilisable par une demande, avant d'expirer. Une valeur positive permet une manipulation appropriée d'arrêt d'un nœud si c'est le seul avec des sessions actives attachées à la valve. Si maxEmptyLife est défini sur **0**, la vanne se terminera en même temps que les copies de la session locale, mais des copies de sauvegarde des sessions, des applications en cluster, seront disponibles à d'autres nœuds du cluster. Si on permet à la vanne à vivre au-delà de la durée de ses sessions gérées, cela donne du temps à l'utilisateur d'effectuer une autre demande qui puisse basculer sur un nœud différent, où il active la copie de sauvegarde de la session. La valeur par défaut, est de **1800** secondes (30 minutes).
processExpiresInterval	SSO clusterisé uniquement. Le nombre minimum de secondes entre les efforts de la valve pour trouver et invalider des instances SSO qui ont expiré le délai d'attente de **MaxEmptyLife**. La valeur par défaut est de **60** (1 minute).
requiresReauthentication	Si true, chaque requête utilise des informations d'authentification en cache pour authentifier à nouveau le domaine de sécurité. Si false (la valeur par défaut), une cookie SSO valide sera suffisante pour que la valve puisse authentifier chaque nouvelle requête.

Rendre une session non valide

Une application peut rendre invalide une session en invoquant la méthode `javax.servlet.http.HttpSession.invalidate()`.

Report a bug

15.5. KERBEROS

Kerberos est un protocole d'authentification réseau pour les applications client/serveur. Il permet l'authentification sur un réseau non sécurisé en toute sécurité, à l'aide de la clé secrète de cryptographie symétrique.

Kerberos utilise les tokens de sécurité appelés «tickets». Pour utiliser un service sécurisé, vous devez obtenir un ticket auprès du Ticket Granting Service (TGS), qui est un service de délivrance de tickets exécuté sur un serveur sur votre réseau. Après avoir obtenu le ticket, vous pourrez demander un Ticket de Service (ST ou Service Ticket) d'un Service d'authentification (AS), qui est un autre service s'exécutant sur votre réseau. Utilisez ensuite ST pour vous authentifier auprès du service que vous souhaitez utiliser. Les TGS et AS tous exécutent tous deux à l'intérieur d'un service intégré appelé KDC (Key Distribution Center).

Kerberos est conçu pour être utilisé dans un environnement client-serveur et est rarement utilisé dans les applications Web ou des environnements clients légers. Cependant, de nombreuses organisations utilisent déjà un système Kerberos pour l'authentification desktop et préfèrent réutiliser leur système existant plutôt que d'en créer un second pour leurs applications web. Kerberos est partie intégrante de Microsoft Active Directory et est également utilisé dans de nombreux environnements Red Hat Enterprise Linux.

Report a bug

15.6. SPNEGO

Simple and Protected GSS_API Negotiation Mechanism (SPNEGO) propose un mécanisme d'expension d'environnement SSO (Single Sign On) pour les applications web.

Lorsqu'une application d'ordinateur client, comme un navigateur web, tente d'accéder à une page de protection sur le serveur web, le serveur répond qu'une autorisation est requise. Ensuite, l'application demande un ticket de service du Centre de distribution des clés Kerberos (KDC). Après l'obtention du ticket, l'application le renvoie dans une requête formatée SPNEGO et l'envoie à l'application web, par l'intermédiaire du navigateur. Le conteneur web exécutant l'application web déployée ouvre la requête et authentifie le billet. Après une authentification réussie, l'accès est accordé.

SPNECO fonctionne avec tous les types de fournisseurs Kerberos, y compris le service Kerberos inclus dans Red Hat Enterprise Linux et le serveur Kerberos, qui fait partie intégrale du Microsoft Active Directory.

Report a bug

15.7. MICROSOFT ACTIVE DIRECTORY

Microsoft Active Directory est un service de répertoires développé par Microsoft pour authentifier les utilisateurs et les ordinateurs d'un domaine Microsoft Windows. Il est inclus dans Microsoft Windows Server. L'ordinateur dans Microsoft Windows Server est nommé le Contrôleur de domaine. Les serveurs de Red Hat Enterprise Linux exécutant le service Samba peuvent aussi agir comme Contrôleur de domaine dans ce type de réseau.

Active Directory repose sur trois technologies principales dépendantes les unes des autres :

- LDAP (Lightweight Directory Access Protocol) stocke les informations utilisateurs, ordinateurs, mots de passe et autres ressources.
- Kerberos procure une authentification sécurisée sur le réseau.
- DNS (Domain Service Name) fournit des mappages entre les adresses IP, les noms d'hôtes et les ordinateurs ou autres périphériques du réseau.

Report a bug

15.8. CONFIGURATION DE KERBEROS OU MICROSOFT ACTIVE DIRECTORY DESKTOP SSO POUR LES APPLICATIONS WEB

Introduction

Pour authentifier vos applications web ou EJB à l'aide de l'authentification basée Kerberos existante de votre organisation et de votre infrastructure d'autorisation, comme Microsoft Active Directory, vous pouvez utiliser les fonctionnalités de JBoss Negotation intégrées dans JBoss EAP 6. Si vous configurez votre application web correctement, une connexion réussie en desktop ou réseau sera suffisante pour vous authentifier en toute transparence dans votre application web, donc aucune invite de connexion supplémentaire ne sera nécessaire.

Différence par rapport aux versions précédentes de la plateforme

Il existe des différences notables entre la plateforme JBoss EAP 6 et les versions précédentes :

- Les domaines de sécurité sont configurés centralement, pour chaque profil d'un domaine géré, ou pour chaque serveur autonome. Ils ne font pas partie du déploiement lui-même. Le domaine de sécurité qu'un déploiement doit utiliser est nommé dans le fichier de déploiement `jboss-web.xml` ou `jboss-ejb3.xml`.
- Les propriétés de sécurité sont configurées dans le cadre du domaine de sécurité, faisant partie de sa configuration centrale. Elles ne font pas partie du déploiement.
- Vous pouvez ne plus remplacer les authentificateurs dans votre déploiement. Toutefois, vous pouvez ajouter une valve NegotiationAuthenticator à votre descripteur `jboss-web.xml` afin d'obtenir le même effet. La valve nécessite toujours les éléments `<security-constraint>` et `<login-config>` à définir dans le fichier `web.xml`. Ils servent à décider quelles ressources sont sécurisées. Cependant, l'auth-method choisie sera substituée par la valve NegotiationAuthenticator du fichier `jboss-web.xml`.
- Les attributs **CODE** des domaines de sécurité utilisent maintenant un nom simple au lieu d'un nom de classe complet. Le tableau suivant montre les mappages entre les classes utilisées pour JBoss Negotiation, et leurs classes.

Tableau 15.2. Codes de modules de connexion et Noms de classes

Nom simple	Nom de classe	But
Kerberos	com.sun.security.auth.module.Krb5LoginModule	Module de connexion Kerberos

Nom simple	Nom de classe	But
SPNEGO	org.jboss.security.negotiation.spnego.SPNEGOLoginModule	Le mécanisme qui permet aux applications web de s'authentifier à votre serveur d'authentification Kerberos.
AdvancedLdap	org.jboss.security.negotiation.AdvancedLdapLoginModule	Utilisé avec les serveurs LDAP autres que Microsoft Active Directory.
AdvancedAdLdap	org.jboss.security.negotiation.AdvancedADLoginModule	Utilisé avec les serveurs Microsoft Active Directory LDAP.

Jboss Negotiation Toolkit

`JBoss Negotiation Toolkit` est un outil de débogage que vous pouvez télécharger à partir de https://community.jboss.org/servlet/JiveServlet/download/16876-2-34629/jboss-negotiation-toolkit.war. Il est fourni comme un outil supplémentaire pour vous aider à déboguer et tester les mécanismes d'authentification avant d'introduire votre application en production. C'est un outil non pris en charge, mais considéré comme très utile. Comme SPNEGO, cet outil peut être difficile à configurer pour les applications web.

Procédure 15.1. Installation de l'authentification SSO (Single Sign On) pour les Applications Web ou EJB

1. **Configurer un domaine de sécurité qui représente l'identité de votre serveur. Définir les propriétés système si nécessaire.**
   Le premier domaine de sécurité authentifie le conteneur lui-même au service de répertoires. Il a besoin d'utiliser un module de connexion qui accepte un type de mécanisme de connexion statique, car un utilisateur réel n'est pas impliqué. Cet exemple utilise une entité de sécurité statique et fait référence à un fichier keytab qui contient les informations d'identification.

   Le code XML est donné ici dans un but de clarification, mais vous devez utiliser la console de gestion ou le Management CLI pour configurer vos domaines de sécurité.

```
<security-domain name="host" cache-type="default">
   <authentication>
      <login-module code="Kerberos" flag="required">
         <module-option name="storeKey" value="true"/>
         <module-option name="useKeyTab" value="true"/>
         <module-option name="principal"
value="host/testserver@MY_REALM"/>
         <module-option name="keyTab"
value="/home/username/service.keytab"/>
         <module-option name="doNotPrompt" value="true"/>
         <module-option name="debug" value="false"/>
      </login-module>
   </authentication>
</security-domain>
```

2. **Configurer un second domaine de sécurité pour sécuriser l'application web ou les applications. Définir les propriétés système si nécessaire.**
   Le deuxième domaine de sécurité est utilisé pour authentifier l'utilisateur particulier au serveur d'authentification Kerberos ou SPNEGO. Vous avez besoin d'au moins un module de connexion pour authentifier l'utilisateur et un autre à la recherche de rôles à appliquer à l'utilisateur. Le code XML suivant montre un exemple de domaine de sécurité SPNEGO. Il inclut un module d'autorisation pour mapper les rôles aux utilisateurs individuels. Vous pouvez également utiliser un module de recherche pour les rôles sur le serveur d'authentification lui-même.

```
<security-domain name="SPNEGO" cache-type="default">
   <authentication>
      <!-- Check the username and password -->
      <login-module code="SPNEGO"  flag="requisite">
         <module-option name="password-stacking"
value="useFirstPass"/>
         <module-option name="serverSecurityDomain" value="host"/>
      </login-module>
      <!-- Search for roles -->
      <login-module code="UsersRoles" flag="required">
         <module-option name="password-stacking"
value="useFirstPass" />
         <module-option name="usersProperties" value="spnego-
users.properties" />
         <module-option name="rolesProperties" value="spnego-
roles.properties" />
      </login-module>
   </authentication>
</security-domain>
```

3. **Spécifier la security-constraint et la login-config dans le fichier `web.xml`**
   Le descripteur `web.xml` contient des informations sur les contraintes de sécurité et sur la configuration de la connexion. En voici des exemples :

```
<security-constraint>
   <display-name>Security Constraint on Conversation</display-name>
   <web-resource-collection>
      <web-resource-name>examplesWebApp</web-resource-name>
      <url-pattern>/*</url-pattern>
   </web-resource-collection>
   <auth-constraint>
   <role-name>RequiredRole</role-name>
   </auth-constraint>
</security-constraint>

<login-config>
   <auth-method>SPNEGO</auth-method>
   <realm-name>SPNEGO</realm-name>
</login-config>

<security-role>
   <description> role required to log in to the
Application</description>
```

```
    <role-name>RequiredRole</role-name>
</security-role>
```

4. **Indiquer le domaine de sécurité et les autres paramètres dans le descripteur `jboss-web.xml`.**
   Spécifiez le nom du domaine de la sécurité côté client (l'autre dans cet exemple) dans le descripteur **`jboss-Web.xml`** de votre déploiement, pour obliger votre application à utiliser ce domaine de sécurité.

   Vous ne pouvez plus remplacer les authentificateurs directement. À la place, vous devez ajouter NegotiationAuthenticator comme valve au descripteur **`jboss-web.xml`** si nécessaire. **`<jacc-star-role-allow>`** vous permet d'utiliser un astérisque (*) pour faire correspondre plusieurs noms de rôles, et est optionnel.

```
<jboss-web>
   <security-domain>java:/jaas/SPNEGO</security-domain>
   <valve>
      <class-
name>org.jboss.security.negotiation.NegotiationAuthenticator</class-
name>
   </valve>
   <jacc-star-role-allow>true</jacc-star-role-allow>
</jboss-web>
```

5. **Ajouter une dépendance au `MANIFEST.MF` de votre application, pour trouver l'emplacement des classes Negotiation.**
   L'application web a besoin d'une dépendance sur la classe **`org.jboss.security.negotiation`** à ajouter au manifeste **`META-INF/MANIFEST.MF`** du déploiement pour pouvoir localiser les classes JBoss Negotiation. Ce qui suit vous montre une entrée formatée correctement.

```
Manifest-Version: 1.0
Build-Jdk: 1.6.0_24
Dependencies: org.jboss.security.negotiation
```

Résultat

Votre application web accepte et authentifie les informations d'identification avec Kerberos, Active Directory de Microsoft ou autre service de répertoire compatible SPNEGO. Si l'utilisateur exécute l'application d'un système qui est déjà enregistré dans le service de répertoires, et où les rôles sont déjà appliqués à l'utilisateur, l'application web n'aura pas besoin d'authentification, et les fonctionnalités SSO seront opérationnelles.

Report a bug

CHAPITRE 16. RÉFÉRENCES DE SÉCURITÉ POUR LE DÉVELOPPEMENT

16.1. RÉFÉRENCE DE CONFIGURATION JBOSS-WEB.XML

Introduction

Le fichier `jboss-web.xml` se trouve dans `WEB-INF` ou dans le répertoire `META-INF` de votre déploiement. Il contient des informations de configuration sur des fonctionnalités que le conteneur JBoss Web ajoute au Servlet 3.0. Les paramètres de configuration spécifiques à la spécification de Servlet 3.0 se trouvent dans `web.xml`, dans le même répertoire.

L'élément qui se trouve tout en haut dans le fichier `jboss-web.xml` est l'élément `<jboss-web>`.

Mappage des ressources globales aux prérequis WAR

La plupart des paramètres de configuration font correspondre les prérequis définis dans le fichier `web.xml` de l'application à des ressources locales. Pour plus d'explications sur les paramètres de configuration de `web.xml` consulter http://docs.oracle.com/cd/E13222_01/wls/docs81/webapp/web_xml.html.

Ainsi, si `web.xml` requiert `jdbc/MyDataSource`, alors `jboss-web.xml` fera sans doute correspondre la source de données globale `java:/DefaultDS` pour remplir ce besoin. Le WAR utilise la source de données globale pour faire correspondre `jdbc/MyDataSource`.

Tableau 16.1. Attributs de haut niveau communs

Attribut	Description
env-entry	Un mappage à `env-entry` requis par `web.xml`.
ejb-ref	Un mappage à `ejb-ref` requis par `web.xml`.
ejb-local-ref	Un mappage à `ejb-local-ref` requis par `web.xml`.
service-ref	Un mappage à `service-ref` requis par `web.xml`.
resource-ref	Un mappage à `resource-ref` requis par `web.xml`.
resource-env-ref	Un mappage à `resource-env-ref` requis par `web.xml`.
message-destination-ref	Un mappage à `message-destination-ref` requis par `web.xml`.
persistence-context-ref	Un mappage à `persistence-context-ref` requis par `web.xml`.
persistence-unit-ref	Un mappage à `persistence-unit-ref` requis par `web.xml`.

Attribut	Description
post-construct	Un mappage à `post-context` requis par `web.xml`.
pre-destroy	Un mappage à `pre-destroy` requis par `web.xml`.
data-source	Un mappage à `data-source` requis par `web.xml`.
context-root	Le contexte root de l'application. La valeur par défaut est le nom du déploiement sans le suffixe `.war`.
virtual-host	Le nom de l'hôte virtuel HTTP à partir duquel l'application accepte les requêtes. Se réfère au contenu de l'en-tête de l'`Host` HTTP.
annotation	Décrit une annotation utilisée par l'application. Voir <annotation> pour plus d'informations.
listener	Décrit un listener utilisé par l'application. Voir <listener> pour plus d'informations.
session-config	Cet élément remplit la même fonction que l'élément `<session-config>` du fichier `web.xml` et est inclus dans un but de compatibilité seulement.
valve	Décrit une valve utilisée par l'application. Voir <valve> pour plus d'informations.
overlay	Le nom d'une couche supplémentaire à ajouter à l'application.
security-domain	Le nom du domaine de sécurité utilisé par l'application. Le domaine de sécurité lui-même est configuré à partir de la console de gestion basée web ou le Management CLI.
security-role	Cet élément remplit la même fonction que l'élément `<session-role>` du fichier `web.xml` et est inclus dans un but de compatibilité seulement.
use-jboss-authorization	Si cet élément est présent et contient la valeur non sensible à la casse "true", la pile d'autorisation web JBoss sera utilisée. S'il n'est pas présent ou contient une valeur non "true", alors seuls les mécanismes d'autorisation indiqués dans les spécifications Java Enterprise Edition seront utilisés. Cet élément est nouveau dans JBoss EAP 6.

Attribut	Description
disable-audit	Si cet élément vide est présent, l'auditing de sécurité web sera désactivé. Sinon, il sera activé. L'auditing de sécurité web ne fait pas partie de la spécification Java EE. Cet élément est nouveau dans JBoss EAP 6.
disable-cross-context	Si sur `false`, l'application sera en mesure d'appeler un autre contexte d'application. La valeur par défaut est `true`.

Les éléments suivants ont chacun des éléments enfants.

<annotation>

Décrit une annotation utilisée par l'application. Le tableau suivant liste les éléments enfants d'une `<annotation>`.

Tableau 16.2. Éléments de configuration d'une annotation

Attribut	Description
class-name	Nom de la classe de l'annotation
servlet-security	L'élément, comme `@ServletSecurity`, qui représente la sécurité du servlet.
run-as	L'élément, comme `@RunAs`, qui représente l'information run-as
multi-part	L'élément, comme `@MultiPart`, qui représente l'information multi-part.

<listener>

Décrit un listener. Le tableau suivant liste les éléments enfants d'un `<listener>`.

Tableau 16.3. Éléments de configuration d'un listener

Attribut	Description
class-name	Nom de la classe du listener

Attribut	Description
listener-type	Liste les éléments de **condition** qui indiquent quel sorte de listener ajouter au contexte de l'application. Les choix valides sont les suivants : **CONTAINER** Ajoute un ContainerListener au contexte. **LIFECYCLE** Ajoute un LifecycleListener au contexte. **SERVLET_INSTANCE** Ajoute un InstanceListener au contexte **SERVLET_CONTAINER** Ajoute un WrapperListener au contexte. **SERVLET_LIFECYCLE** Ajoute un WrapperLifecycle au contexte.
module	Le nom du module qui contient la classe du listener.
param	Un paramètre. Contient deux éléments enfants, **<param-name>** et **<param-value>**.

<valve>

Décrit une valve de l'application. Contient les mêmes éléments de configuration que <listener>.

Report a bug

16.2. RÉFÉRENCE DE PARAMÈTRE DE SÉCURITÉ EJB

Tableau 16.4. Éléments de paramètres de sécurité EJB

Élément	Description
<security-identity>	Contient des éléments enfants relatifs à l'identité de sécurité d'un EJB.
<use-caller-identity />	Indique que l'EJB utilise la même identité de sécurité que l'appelant.
<run-as>	Contient un élément **<role-name>**.
<run-as-principal>	Si présent, indique le principal assigné aux appels sortants. Si non présent, les appels sortants sont assignés à un principal nommé **anonymous**.

Élément	Description
<role-name>	Spécifie le role d'exécution de l'EJB.
<description>	Décrit le role nommé dans **<role-name>** .

Exemple 16.1. Exemples d'identité de sécurité

Cet exemple décrit chaque balise décrite dans Tableau 16.4, « Éléments de paramètres de sécurité EJB ». Peuvent également être mis dans un **<session>**.

```
<ejb-jar>
    <enterprise-beans>
        <session>
            <ejb-name>ASessionBean</ejb-name>
            <security-identity>
                <use-caller-identity/>
            </security-identity>
        </session>
        <session>
            <ejb-name>RunAsBean</ejb-name>
            <security-identity>
                <run-as>
                    <description>A private internal role</description>
                    <role-name>InternalRole</role-name>
                </run-as>
            </security-identity>
        </session>
    <session>
    <ejb-name>RunAsBean</ejb-name>
    <security-identity>
    <run-as-principal>internal</run-as-principal>
    </security-identity>
    </session>
    </enterprise-beans>
</ejb-jar>
```

Report a bug

CHAPITRE 17. RÉFÉRENCES SUPPLÉMENTAIRES

17.1. TYPES D'ARCHIVES JAVA

JBoss EAP 6 reconnaît différents types de fichiers d'archives. Les fichiers d'archives sont utilisés pour empaqueter des services et des applications déployables.

En général, les fichiers d'archives sont des archives Zip, avec des extensions de fichiers spécifiques et des structures de répertoires spécifiques. Si l'archive Zip est extraite avant d'être déployée sur le serveur d'application, on s'y réfère comme d'une archive explosée. Dans ce cas, le nom du répertoire contient toujours l'extension de fichier, et les conditions de structure de répertoire continuent de s'appliquer.

Tableau 17.1.

Type d'archive	Extension	But	Exigences pour la structure de répertoire
Archive Java	.jar	Contient les bibliothèques de classes Java.	Le fichier **`META-INF/MANIFEST.MF`** (optionnel), spécifiant des informations comme quelle classe est la classe **`principale`**.
Archive Web	.war	Contient des fichiers Java Server Pages (JSP), des servlets, et des fichiers XML, en plus des classes et des bibliothèques. Le contenu Archive Web s'appelle aussi Web Application.	Le fichier **`WEB-INF/web.xml`**, qui contient des informations sur la structure de l'application web. Il y a également d'autres fichiers présents dans **`WEB-INF/`**.
Resource Adapter Archive	.rar	La structure du répertoire est dans la spécification JCA.	Contient un adaptateur de ressources Java Connector Architecture (JCA). S'appelle également un connecteur.
Enterprise Archive	.ear	Utilisé par Java Enterprise Edition (EE) pour empaqueter un ou plusieurs modules dans une simple archive, pour que les modules puissent être déployés dans le serveur d'applications simultanément. Maven et Ant sont les outils les plus communément utilisés pour générer les archives EAR.	Le répertoire **`META-INF/`** qui contient un ou plusieurs fichiers de descripteurs de déploiement XML.

Type d'archive	Extension	But	Exigences pour la structure de répertoire
			N'importe quel type de module. • WAR (Web Archive) • Une ou plusieurs JAR (Java Archives) contenant des POJO (Plain Old Java Objects) • Un ou plusieurs modules Enterprise JavaBean (EJB), contenant son propre répertoire **`META-INF/`**. Ce répertoire inclut des descipteurs pour les classes de persistence qui sont déployées. • Une ou plusieurs Archives de ressources (RAR).
Service Archive	.sar	Ressemble à une Archive Enterprise, spécifique à Enterprise Application Platform.	Répertoire **`META-INF/`** contenant un fichier **`jboss-service.xml`** ou **`jboss-beans.xml`**.

Report a bug

ANNEXE A. REVISION HISTORY

Version 1.0.0-1 **Wed Jun 18 2014** **CS Builder Robot**

Built from Content Specification: 14875, Revision: 608382