RENFORCEMENT ET SECURITE D'ADOBE® LIVECYCLE® ES3

Informations juridiques

Pour les informations juridiques, voir http://help.adobe.com/fr_FR/legalnotices/index.html.

Sommaire

Chapitre 1 : A propos de ce document

Ce document explique comment optimiser la sécurité de l'environnement de production Adobe® LiveCycle® Enterprise Suite (ES3).

Pour plus de détails sur les informations de sécurité LiveCycle, visitez le site Pôle de développement LiveCycle.

Vous pouvez également trouver des bulletins et avis de sécurité pour LiveCycle sur le site Bulletins et avis de sécurité d'Adobe.

1.1 A qui est destiné ce document ?

Ce document est destiné aux consultants, aux spécialistes de la sécurité, aux architectes de systèmes et aux professionnels de l'informatique chargés de planifier le développement et le déploiement d'application ou d'infrastructure de LiveCycle. Ces postes incluent les rôles communs suivants :

- les ingénieurs informatiques et d'exploitation, qui doivent déployer des applications et des serveurs Web sécurisés dans leur entreprise ou celle de leurs clients ;
- les architectes et les planificateurs, qui sont chargés de planifier les efforts architecturaux des clients dans leur entreprise ;
- les spécialistes de la sécurité informatique, qui sont responsables de la protection des plateformes de leur entreprise ;
- les consultants d'Adobe et de partenaires, qui ont besoin de ressources détaillées pour les clients et les partenaires.

1.2 Conventions utilisées dans ce document

Ce document utilise les conventions de désignation ci-après pour les chemins d'accès aux fichiers courants.

Nom	Valeur par défaut	Description
[racine LiveCycle]	Windows : C:\Adobe\Adobe LiveCycleES3 Linux et UNIX : opt/adobe/adobe_livecycle_es3	Répertoire d'installation utilisé pour tous les modules de LiveCycle Il contient des sous-répertoires pour Adobe® LiveCycle® Configuration Manager. Il comprend également les sous-répertoires associés aux technologies tierces.
[racine JBoss]	C:\Adobe\Adobe LiveCycle ES3\jboss	(JBoss clé en main) Répertoire d'accueil du serveur d'applications qui exécute LiveCycle.

1.3 Informations complémentaires

Les ressources indiquées dans le tableau ci-dessous peuvent vous aider à mieux comprendre LiveCycle.

Pour plus d'informations sur	**Voir**
LiveCycle, les solutions LiveCycle et les outils de développement	Présentation de LiveCycle
Préparation de l'environnement pour l'installation et la mise à niveau vers LiveCycle	Préparation à l'installation de LiveCycle sur un seul serveur Préparation à l'installation de LiveCycle sur une grappe de serveurs Préparation à la mise à niveau vers LiveCycle ES3
Installation de LiveCycle sur un seul serveur	Installation et déploiement de LiveCycle à l'aide de la procédure clé en main pour JBoss Installation et déploiement de LiveCycle pour JBoss Installation et déploiement de LiveCycle pour WebLogic Installation et déploiement de LiveCycle pour WebSphere
Configuration de LiveCycle sur une grappe de serveurs	Configuration des grappes de serveurs d'applications LiveCycle à l'aide de JBoss Configuration des grappes de serveurs d'applications LiveCycle à l'aide de WebLogic Configuration des grappes de serveurs d'applications LiveCycle à l'aide de WebSphere
Mise à niveau vers LiveCycle	Mise à niveau vers LiveCycle ES3 pour JBoss à l'aide de la procédure clé en main Mise à niveau vers LiveCycle ES3 pour JBoss Mise à niveau vers LiveCycle ES3 pour WebLogic Mise à niveau vers LiveCycle ES3 pour WebSphere
Installation de LiveCycle Workbench 10	Installation de LiveCycle Workbench
Exécution de tâches administratives générales pour LiveCycle	Aide à l'administration de LiveCycle
Les autres services et produits qui s'intègrent à LiveCycle	http://www.adobe.com/fr
Documentation de LiveCycle	Documentation de LiveCycle

Chapitre 2 : Considérations générales sur la sécurité

Cette section propose des informations introductives qui vous aideront à préparer le renforcement de votre environnement LiveCycle Elle inclut des informations prérequises sur la sécurité de LiveCycle, des systèmes d'exploitation, des serveurs d'applications et des bases de données. Consultez ces informations avant de continuer à verrouiller votre environnement.

2.1 Informations de sécurité spécifiques aux revendeurs

Cette section contient des informations sur la sécurité des systèmes d'exploitation, des serveurs d'applications et des bases de données intégrés à votre solution d'entreprise LiveCycle.

Utilisez les liens proposés dans cette section pour accéder à des informations de sécurité spécifiques au revendeur de votre système d'exploitation, de votre base de données et de votre serveur d'applications.

2.1.1 Informations sur la sécurité des systèmes d'exploitation

Lorsque vous sécurisez votre système d'exploitation, veillez à implémenter soigneusement les mesures indiquées par le revendeur de votre système d'exploitation, parmi lesquelles :

- définir et contrôler les utilisateurs, les rôles et les droits ;
- surveiller les journaux et les journaux d'audit ;
- supprimer les services et les applications inutiles ;
- sauvegarder les fichiers.

Pour plus de détails sur la sécurité des systèmes d'exploitation pris en charge par LiveCycle, reportez-vous aux ressources indiquées dans le tableau ci-dessous.

Système d'exploitation	**Ressource de sécurité**
IBM® AIX® 5.3 et 6.1	Avantages d'IBM AIX en termes de sécurité
Microsoft® Windows® XP SP 2 (pour les environnements de non-production uniquement)	Guide de sécurité de Windows XP (en anglais)
Microsoft Windows 7, 32 et 64 bits (pour les environnements de non-production uniquement)	Guide de sécurité de Windows 7 (en anglais)
Microsoft Windows Server® 2003 Editions Enterprise ou Standard	Recherchez « Guide de sécurité Windows Server 2003 » sur le site Web Microsoft.com.
Microsoft Windows Server® 2008 Editions Enterprise ou Standard	Recherchez « Guide de sécurité Windows Server 2008 » sur le site Web Microsoft.com.

Système d'exploitation	Ressource de sécurité
Microsoft Vista™ SP1, toutes versions, 32 et 64 bits (pour les environnements de non-production uniquement)	Recherchez « Guide de sécurité Windows Vista » sur le site Web Microsoft.com.
Red Hat® Linux® AP ou ES	Guide de sécurité de Red Hat Enterprise Linux (en anglais)
Sun Solaris 10	System Administration Guide: Security Services

2.1.2 Informations sur la sécurité des serveurs d'applications

Lorsque vous sécurisez votre serveur d'applications, veillez à implémenter soigneusement les mesures indiquées par le revendeur de votre serveur, parmi lesquelles :

- utiliser un nom d'utilisateur administrateur difficilement identifiable ;
- désactiver les services inutiles ;
- sécuriser le gestionnaire de console ;
- autoriser les cookies sûrs ;
- fermer les ports inutiles ;
- restreindre les clients par adresses ou domaines IP ;
- utiliser Java™ Security Manager pour limiter les droits par programme.

Pour plus de détails sur la sécurité des serveurs d'applications pris en charge par LiveCycle, reportez-vous aux ressources indiquées dans le tableau ci-dessous.

Serveur d'applications	Ressource de sécurité
Oracle WebLogic®	Recherchez « Understanding WebLogic Security » sur http://download.oracle.com/docs/.
IBM WebSphere®	Sécurisation des applications dans leur environnement
Red Hat® JBoss®	Sécurité sur JBoss (en anglais)

2.1.3 Informations sur la sécurité des bases de données

Lorsque vous sécurisez votre base de données, veillez à implémenter soigneusement les mesures indiquées par le revendeur de votre base de données, parmi lesquelles :

- restreindre les opérations avec des listes de contrôle d'accès (ACL) ;
- utiliser des ports non standard ;
- masquer la base de données derrière un pare-feu ;
- chiffrer les données sensibles avant de les écrire dans la base de données (consultez la documentation du fabricant de la base de données).

Pour plus de détails sur la sécurité des bases de données prises en charge par LiveCycle, reportez-vous aux ressources indiquées dans le tableau ci-dessous.

Base de données	Ressource de sécurité
IBM DB2® 9.1 ou 9.5	DB2 Product Family Library
Microsoft SQL Server 2005 SP2 ou 2008	Recherchez « SQL Server 2005 : sécurité » sur le Web. Recherchez « SQL Server 2008 : sécurité » sur le Web.
MySQL 5	Sécurité générale du serveur MySQL 5.0 Sécurité générale du serveur MySQL 5.1 (en anglais)
Oracle® 10g ou 11g	Voir le chapitre Security dans la Documentation d'Oracle 11g (en anglais)

Ce tableau décrit les ports par défaut devant être ouverts pendant le processus de configuration de LiveCycle Si vous vous connectez via https, reparamétrez les informations de port et les adresses IP en conséquence. Pour plus d'informations sur la configuration des ports, voir le document *Installation et déploiement de LiveCycle* pour votre serveur d'applications.

Produit ou service	Numéro de port
JBoss	8080
WebLogic	7001
Serveur géré WebLogic	Défini par l'administrateur lors de la configuration
WebSphere	9060 ; si la sécurité globale est activée, la valeur de port SSL par défaut est 9043. 9080
Serveur BAM	7001
SOAP	8880
MySQL	3306
Oracle	1521
DB2	50000
SQL Server	1433
LDAP	port sur lequel le serveur LDAP fonctionne. Il s'agit généralement du port 389. Toutefois, si vous sélectionnez l'option SSL, le port par défaut est habituellement le port 636. Vous devez vérifier auprès de votre administrateur LDAP le numéro de port à utiliser..

2.1.4 Configuration de JBoss pour utiliser un port HTTP qui n'est pas un port par défaut

Le serveur d'applications JBoss utilise 8080 en tant que port HTTP par défaut. JBoss possède également des ports 8180, 8280 et 8380 préconfigurés ; ils sont mis en commentaires dans le fichier jboss-service.xml. Si vous possédez sur votre ordinateur une application qui utilise déjà ce port, vous devez modifier celui qui est utilisé par LiveCycle comme suit :

1 Ouvrez le fichier jboss-service.xml dans un éditeur.

Installation clé en main de JBoss : *[racine JBoss]*/server/lc_turnkey/conf/

Installation manuelle de JBoss : *[racine serveur d'applications]*/server/all/conf/

2 Recherchez et annulez la mise en commentaire du mbean suivant :

```
<mbean code="org.jboss.services.binding.ServiceBindingManager"

name="jboss.system:service=ServiceBindingManager">

<attribute name="ServerName">ports-01</attribute>

<attribute name="StoreURL">${jboss.home.url}/docs/examples/binding-manager/sample-
bindings.xml</attribute>

<attribute name="StoreFactoryClassName">

org.jboss.services.binding.XMLServicesStoreFactory

</attribute>

</mbean>
```

3 Enregistrez le fichier, puis fermez-le.

4 Redémarrez JBoss.

JBoss est maintenant configuré pour utiliser le port 8180. Si vous souhaitez utiliser les ports 8280 ou 8380, modifiez la valeur de l'attribut `ServerName` pour utiliser l'un des ports suivants :

- Pour 8280 : `ports-02`
- Pour 8380 : `ports-03`

Si vous souhaitez configurer un numéro de port différent de ceux qui sont préconfigurés pour JBoss, exécutez les étapes suivantes :

1 Recherchez et ouvrez le fichier deploy/jboss-web.deployer dans *[racine JBoss]* (clé en main) ou *[racine serveur d'applications]* (installation manuelle de JBoss).

2 Recherchez et annulez la mise en commentaire du mbean comme décrit dans l'étape 2 ci-dessus.

3 Remplacez la valeur `ServerName` par le numéro de port à utiliser.

4 Enregistrez le fichier, puis fermez-le.

5 Redémarrez JBoss.

2.2 Considérations sur la sécurité de LiveCycle

Cette section décrit certains problèmes de sécurité spécifiques à LiveCycle, que vous devez connaître.

2.2.1 Informations d'identification de courrier électronique non chiffrées dans la base de données

Les informations d'identification stockées par les applications LiveCycle ne sont pas chiffrées avant d'être enregistrées dans la base de données LiveCycle Lorsque vous configurez un point de fin de service pour utiliser le courrier électronique, les informations de mot de passe utilisées pour configurer ce point de fin ne sont pas chiffrées lorsqu'elles sont enregistrées dans la base de données.

2.2.2 Contenu sensible pour Rights Management dans la base de données

LiveCycle utilise la base de données LiveCycle pour stocker des informations clés sur des documents sensibles, de même que d'autres données cryptographiques utilisées pour les documents de règles. Le fait de sécuriser la base de données contre les intrusions contribue à la protection de ces informations sensibles.

2.2.3 Mot de passe au format texte en clair dans adobe-ds.xml

Le serveur d'applications utilisé pour exécuter LiveCycle nécessite sa propre configuration pour accéder à votre base de données via une source de données configurée sur le serveur d'applications. Veillez à ce que votre serveur d'applications n'expose pas le mot de passe de votre base de données en texte lisible dans le fichier de configuration de sa source de données.

Le fichier adobe-ds.xml contient des mots de passe au format texte en clair. Consultez le revendeur de votre serveur d'applications pour savoir comment chiffrer ces mots de passe pour votre serveur d'applications. Par exemple, les instructions pour JBoss® sont dans Chiffrement des mots de passe de la source de données.

Remarque : *le programme d'installation de LiveCycle JBoss clé en main chiffre le mot de passe de la base de données.*

Il est possible que le serveur d'applications IBM WebSphere et qu'Oracle WebLogic Server chiffrent les mots de passe des sources de données par défaut. Vérifiez ce point dans la documentation de votre serveur d'applications.

Chapitre 3 : Renforcement de l'environnement

Cette section présente des conseils et des pratiques recommandées pour sécuriser des serveurs exécutant LiveCycle. Elle ne vise pas à expliquer de manière exhaustive comment renforcer des hôtes pour votre système d'exploitation et votre serveur d'applications. Au contraire, cette section décrit plusieurs paramètres de renforcement de la sécurité, que vous pouvez implémenter pour améliorer la sécurité de LiveCycle lorsqu'il est exécuté dans un intranet d'entreprise. Toutefois, pour que les serveurs d'applications LiveCycle restent sécurisés, vous devez également mettre en œuvre des procédures de surveillance, de détection et de réponse de sécurité.

Cette section décrit des techniques de renforcement à appliquer au cours des étapes suivantes, lors du cycle de vie de l'installation et de la configuration :

- **Préinstallation :** utilisez ces techniques avant d'installer LiveCycle.
- **Installation :** utilisez ces techniques pendant le processus d'installation de LiveCycle.
- **Post-installation :** utilisez ces techniques après l'installation du logiciel, puis de manière régulière.

LiveCycle est hautement personnalisable et compatible avec de nombreux environnements. Il est possible que certains des conseils présentés ici ne soient pas directement applicables à votre entreprise.

3.1 Préinstallation

Avant d'installer LiveCycle, vous pouvez appliquer des solutions de sécurité à la couche réseau et au système d'exploitation. Cette section décrit certains problèmes et propose des conseils pour réduire les vulnérabilités de la sécurité correspondantes.

Installation et configuration sous UNIX et Linux

Evitez d'installer ou de configurer LiveCycle en utilisant un shell racine. Par défaut, les fichiers sont installés sous le répertoire /opt et l'utilisateur qui effectue l'installation a besoin de disposer de toutes les autorisations de fichier sous /opt. De même, cet utilisateur peut parfaitement exécuter une installation sous un répertoire /user dans lequel il dispose de toutes les autorisations de fichier.

Installation et configuration sous Windows

Sous Windows, il est préférable d'effectuer l'installation en tant qu'administrateur si vous installez LiveCycle sur JBoss en utilisant la procédure d'installation clé en main ou si vous installez LiveCycle PDF Generator. Par ailleurs, lorsque vous installez PDF Generator sous Windows avec prise en charge des applications natives, vous devez exécuter l'installation sous la même identité que l'utilisateur Windows ayant installé Microsoft Office. Pour plus d'informations sur les droits d'installation, voir le document *Installation et déploiement de LiveCycle* pour votre serveur d'applications.

3.1.1 Sécurité de la couche réseau

Les vulnérabilités de sécurité réseau comptent parmi les premières menaces qui affectent les serveurs d'applications accessibles par Internet ou par un intranet. Cette section décrit le processus de renforcement des hôtes du réseau contre ces vulnérabilités. Elle traite de la segmentation du réseau, du renforcement de la pile TCP/IP (Transmission Control Protocol/Internet Protocol) et de l'utilisation de pare-feu pour protéger les hôtes.

Le tableau suivant décrit des processus classiques qui permettent de réduire les vulnérabilités de la sécurité réseau :

Problème	**Description**
Zones démilitarisées	Déployez des serveurs LiveCycle dans une zone démilitarisée. Une segmentation doit avoir été définie dans au moins deux niveaux avec le serveur d'applications utilisé pour exécuter LiveCycle placé derrière le pare-feu interne. Séparez le réseau externe de la zone démilitarisée qui contient les serveurs Web, lesquels doivent par ailleurs être séparés du réseau interne. Utilisez des pare-feu pour implémenter les couches de séparation. Classez et contrôlez le trafic passant par chaque couche réseau pour vous assurer que le minimum absolu de données requises est autorisé.
Adresses IP privées	Utilisez la technique NAT (Network Address Translation) avec des adresses IP privées RFC 1918 sur les serveurs d'applications LiveCycle Attribuez des adresses IP privées (10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16) pour rendre plus difficile, pour un attaquant, le routage du trafic depuis et vers un hôte interne NAT via Internet.
Pare-feu	Utilisez les critères suivants pour choisir une solution de pare-feu : • Implémentez des pare-feu qui prennent en charge les serveurs proxy et/ou la *vérification avec état* plutôt que de simples solutions de filtrage des paquets. • Utilisez un pare-feu qui prend en charge un paradigme de sécurité de type *refuser tous les services hormis ceux autorisés explicitement*. • Implémentez une solution de pare-feu à double hébergement ou à hébergement multiple. Cette architecture propose le meilleur niveau de sécurité et contribue à empêcher les utilisateurs non autorisés de contourner le pare-feu.
Ports de base de données	N'utilisez pas les ports d'écoute par défaut pour les bases de données (MySQL - 3306, Oracle - 1521, MS SQL - 1433). Pour plus de détails sur la redéfinition des ports de base de données, reportez-vous à la documentation de votre base de données. L'utilisation d'un port de base de données différent affecte la configuration globale de LiveCycle Si vous redéfinissez les ports par défaut, vous devez modifier en conséquence la configuration et, notamment, les sources de données de LiveCycle. Pour plus d'informations sur la configuration des sources de données dans LiveCycle, voir le document *Installation etdéploiement de LiveCycle* ou *Mise à niveau vers LiveCycle* pour votre serveur d'applications dans la Documentation LiveCycle.

3.1.2 Sécurité du système d'exploitation

Le tableau suivant décrit plusieurs approches utilisables pour réduire au minimum les vulnérabilités de sécurité du système d'exploitation :

Problème	Description
Correctifs de sécurité	Le risque de voir un utilisateur non autorisé accéder au serveur d'applications sera d'autant plus important que les correctifs de sécurité et les mises à niveau du revendeur n'auront pas été appliqués en temps utile. Testez les correctifs de sécurité avant de les appliquer sur les serveurs de production. De même, créez des règles et des procédures pour contrôler et installer régulièrement les correctifs.
Logiciels de protection antivirus	Les programmes antivirus identifient les fichiers infectés en recherchant des signatures ou en repérant les comportements inhabituels. Ces programmes conservent la signature des virus dans un fichier, qui est généralement stocké sur le disque dur local. De nouveaux virus étant découverts régulièrement, mettez fréquemment à jour ce fichier pour permettre au programme antivirus d'identifier tous les virus actuels.
NTP (Network Time Protocol)	Pour les analyses légales, veillez à ce que l'heure des serveurs LiveCycle soit toujours exacte. Utilisez le protocole NTP pour synchroniser l'heure sur tous les systèmes connectés directement à Internet.

Pour plus de sécurité d'informations de votre système d'exploitation, voir « 2.1.1 Informations sur la sécurité des systèmes d'exploitation » à la page 3.

3.2 Installation

Cette section décrit des techniques que vous pouvez utiliser pendant le processus d'installation de LiveCycle pour réduire les vulnérabilités de sécurité. Dans certains cas, ces techniques utilisent des options qui font partie du processus d'installation. Le tableau suivant décrit ces techniques :

Problème	Description
Droits	Utilisez le minimum de droits requis pour installer le logiciel. Connectez-vous à l'ordinateur via un compte qui n'appartient pas au groupe Administrateurs. Sous Windows, vous pouvez utiliser la commande Exécuter en tant que pour exécuter le programme d'installation de LiveCycle en tant qu'utilisateur non administrateur. Sous UNIX et Linux, utilisez une commande comme `sudo` pour installer le logiciel.
Source du logiciel	Ne téléchargez et n'exécutez pas LiveCycle depuis des sources non approuvées. Des programmes malveillants peuvent contenir des codes conçus pour violer la sécurité de multiples façons, par exemple par vol, par modification et suppression de données, ou par déni de service. Installez LiveCycle à partir du DVD Adobe ou depuis une source approuvée uniquement.
Partitions de disques	Placez LiveCycle sur une partition de disque dédiée. La segmentation de disque est un processus qui permet de conserver des données spécifiques sur des disques physiques séparés de votre serveur, pour une sécurité accrue. Le fait d'organiser les données ainsi permet de réduire le risque d'attaques par traversée d'annuaires. Prévoyez de créer une partition distincte de la partition système, dans laquelle vous pouvez installer le répertoire de contenu LiveCycle (sous Windows, la partition système contient le répertoire system32, ou partition racine).

Problème	Description
Composants	Evaluez les services existants et désactivez ou désinstallez tout service inutile. N'installez pas de composants ou de services dont vous n'avez pas besoin. L'installation par défaut d'un serveur d'applications peut inclure des services dont vous n'avez aucune utilité. Par conséquent, désactivez tous les services inutiles avant de procéder au déploiement, pour réduire ainsi au minimum les possibilités de points d'entrée d'une attaque. Par exemple, sur JBoss, vous pouvez placer en commentaire les services inutiles dans le fichier descripteur META-INF/jboss-service.xml.
Fichier de stratégie interdomaines	La présence d'un fichier `crossdomain.xml` sur le serveur peut immédiatement affaiblir ce serveur. Il est recommandé de rendre la liste des domaines aussi restrictive que possible. Ne placez pas en production le fichier `crossdomain.xml` utilisé pendant la phase de développement lors de l'utilisation des guides *(obsolète)*. Dans le cas d'un guide qui utilise les services Web, si le service figure sur le même serveur ayant servi le guide, aucun fichier `crossdomain.xml` n'est nécessaire. En revanche, si le service figure sur un autre serveur ou si des grappes sont impliquées, la présence d'un fichier `crossdomain.xml` est nécessaire. Voir http://kb2.adobe.com/fr/cps/142/tn_14213.html pour plus d'informations sur le fichier crossdomain.xml.
Paramètres de sécurité du système d'exploitation	Si vous devez utiliser un chiffrement XML 192 bits ou 256 bits sur les plateformes Solaris, assurez-vous d'installer `pkcs11_softtoken_extra.so` au lieu de `pkcs11_softtoken.so`.

3.3 Etapes de post-installation

Une fois LiveCycle installé, il est important d'assurer une maintenance régulière de l'environnement pour en optimiser la sécurité.

La section suivante décrit en détail les différentes tâches recommandées pour sécuriser le serveur LiveCycle déployé.

3.3.1 Sécurité du serveur LiveCycle

Les paramètres recommandés suivants s'appliquent au serveur LiveCycle hors de l'application Web administrative. Pour réduire les risques de sécurité du serveur, appliquez ces paramètres immédiatement après avoir installé LiveCycle.

Correctifs de sécurité

Le risque de voir un utilisateur non autorisé accéder au serveur d'applications sera d'autant plus important que les correctifs de sécurité et les mises à niveau du revendeur n'auront pas été appliqués en temps utile. Testez les correctifs de sécurité avant de les appliquer aux serveurs de production pour vous assurer de la compatibilité et de la disponibilité des applications LiveCycle De même, créez des règles et des procédures pour contrôler et installer régulièrement les correctifs. Les mises à jour LiveCycle sont sont disponibles sur le site de téléchargement des produits Enterprise.

Comptes de service (JBoss clé en main sur Windows uniquement)

LiveCycle installe un service par défaut en utilisant le compte système local. Le compte utilisateur système local intégré présente un haut niveau d'accessibilité ; il fait partie du groupe Administrateurs. Si une identité de processus de travail est exécutée en tant que compte utilisateur système local, ce processus de travail dispose d'un accès complet à l'ensemble du système.

Pour exécuter le serveur d'applications sur lequel est déployé LiveCycle, appliquez les instructions suivantes en utilisant un compte non administratif spécifique :

1 Dans Microsoft Management Console (MMC), créez un utilisateur local pour que le service LiveCycle se connecte en tant que cet utilisateur local :
   - Sélectionnez **L'utilisateur ne peut pas changer de mot de passe**.
   - Vérifiez que le groupe **Utilisateurs** figure dans l'onglet **Membre de**.

   Remarque : *vous ne pouvez pas modifier ce paramètre pour PDF Generator.*

2 Sélectionnez **Démarrer** > **Paramètres** > **Outils d'administration** > **Services**.

3 Cliquez deux fois sur le JBoss pour Adobe LiveCycle 10 et arrêtez-le.

4 Sur l'onglet **Ouvrir une session**, sélectionnez **Ce compte**, recherchez le compte utilisateur que vous avez créé, puis entrez le mot de passe pour ce compte.

5 Dans MMC, ouvrez **Paramètres de sécurité locaux** et sélectionnez **Stratégies locales** > **Attribution de droits utilisateur**.

6 Attribuez les droits suivants au compte utilisateur sous lequel le serveur LiveCycle est exécuté :
   - Interdire l'ouverture de session par les services Terminal
   - Interdire l'ouverture d'une session locale
   - Ouvrir une session en tant que service (ce droit doit être déjà défini)

7 Attribuez au nouveau compte utilisateur les autorisations de lecture et d'exécution, d'affichage du contenu des dossiers et de lecture pour les répertoires de contenu Web LiveCycle

8 Démarrez le serveur d'applications.

Désactivation de la servlet d'amorçage de Configuration Manager

Configuration Manager a utilisé une servlet déployée sur votre serveur d'applications pour amorcer la base de données LiveCycle. Configuration Manager accédant à cette servlet avant la fin de la configuration, son accès n'a pas été sécurisé pour les utilisateurs autorisés et il convient de le désactiver après avoir utilisé Configuration Manager pour configurer LiveCycle.

1 Décompressez le fichier adobe-livecycle-[serveur d'applications].ear.

2 Ouvrez le fichier META-INF/application.xml.

3 Recherchez la section adobe-bootstrapper.war :

```
<!-- bootstrapper start -->
<module id="WebApp_adobe_bootstrapper">
    <web>
        <web-uri>adobe-bootstrapper.war</web-uri>
        <context-root>/adobe-bootstrapper</context-root>
    </web>
</module>
<module id="WebApp_adobe_lcm_bootstrapper_redirector">
    <web>
        <web-uri>adobe-lcm-bootstrapper-redirector.war</web-uri>
        <context-root>/adobe-lcm-bootstrapper</context-root>
    </web>
</module>
<!-- bootstrapper end-->
```

4 Placez en commentaire les modules adobe-bootstrapper.war et adobe-lcm-bootstrapper-redirectory. war, comme suit :

```
<!-- bootstrapper start -->
<!--
<module id="WebApp_adobe_bootstrapper">
    <web>
        <web-uri>adobe-bootstrapper.war</web-uri>
        <context-root>/adobe-bootstrapper</context-root>
    </web>
</module>
<module id="WebApp_adobe_lcm_bootstrapper_redirector">
    <web>
        <web-uri>adobe-lcm-bootstrapper-redirector.war</web-uri>
        <context-root>/adobe-lcm-bootstrapper</context-root>
    </web>
</module>
-->
<!-- bootstrapper end-->
```

5 Enregistrez et fermez le fichier META-INF/application.xml.

6 Compressez le fichier EAR et redéployez-le sur le serveur d'applications.

7 Entrez l'URL dans un navigateur pour tester la modification et garantir que l'adresse ne fonctionne plus.

Verrouillage de l'accès distant à Trust Store

Configuration Manager vous permet de télécharger des informations d'identification Reader Extensions 10 dans le Trust Store LiveCycle. Ceci signifie que l'accès au service d'informations d'identification Trust Store sur les protocoles distants (SOAP et EJB) a été activé par défaut. Cet accès n'est plus nécessaire après avoir téléchargé les informations d'identification des droits en utilisant Configuration Manager, ou si vous décidez d'utiliser Configuration Manager ultérieurement pour gérer les informations d'identification.

Vous pouvez désactiver l'accès distant à tous les services Trust Store en procédant comme indiqué dans la section « 4.1 Désactivation des accès distants non indispensables à des services » à la page 37.

Désactivation de tous les accès anonymes non indispensables

Certains services LiveCycle comportent des opérations qu'un appelant anonyme peut appeler. Si l'accès anonyme à ces services n'est pas obligatoire, désactivez-le en suivant les étapes de « 4.2 Désactivation des accès anonymes non indispensables à des services » à la page 38.

3.3.1.1 Modification du mot de passe par défaut du compte administrateur

Lorsque LiveCycle est installé, un compte utilisateur par défaut unique est configuré pour l'utilisateur Super administrateur/Administrateur à ID de connexion avec un mot de passe par défaut, *password*. Modifiez immédiatement ce mot de passe à l'aide de Configuration Manager.

1 Saisissez l'URL suivante dans un navigateur Web :

`http://[host name]:[port]/adminui`

Le numéro de port par défaut est l'un des numéros suivants :

JBoss : 8080

WebLogic Server : 7001

WebSphere : 9080.

2 Dans le champ **Nom d'utilisateur**, saisissez `administrator` et dans le champ **Mot de passe**, saisissez `password`.

3 Cliquez sur **Paramètres** > **User Management** > **Utilisateurs et groupes**.

4 Saisissez `administrator` dans le champ **Rechercher**, puis cliquez sur **Rechercher**.

5 Cliquez sur **Super Administrateur** dans la liste des utilisateurs.

6 Cliquez sur **Changer de mot de passe** dans la page Modifier l'utilisateur.

7 Indiquez le nouveau mot de passe et cliquez sur **Enregistrer**.

3.3.1.2 Désactivation de la génération WSDL

La génération Web Service Definition Language (WSDL) doit être activée uniquement pour les environnements de développement dans lesquels les développeurs font appel à la génération WSDL pour créer leurs applications clientes. Vous pouvez choisir de désactiver la génération WSDL dans un environnement de production pour éviter d'exposer les détails internes d'un service.

1 Saisissez l'URL suivante dans un navigateur Web :

`http://[host name]:[port]/adminui`

2 Cliquez sur **Paramètres > Paramètres de Core System > Configurations de base**.

3 Désélectionnez la case à cocher **Activer WSDL** et cliquez sur **OK**.

3.3.1.3 Restriction des quotas d'intégration de données de l'utilisateur dans LiveCycle Content Services (obsolète)

Remarque : *Adobe procède actuellement à la migration des clients Adobe® LiveCycle® Content Services ES vers le référentiel de contenu Content Repository basé sur l'architecture modulaire CRX moderne, acquise par Adobe lors de son rachat de la société Day Software. Content Repository est fourni avec LiveCycle Foundation et il est disponible à compter de la version LiveCycle ES3.*

Par défaut, Content Services ne restreint pas le nombre de données qu'un utilisateur peut intégrer dans un serveur à tout moment. Un grand volume de données peut représenter une menace pour le système, car ce dernier ne dispose plus de ressources suffisantes pour exécuter les autres opérations. Cette situation peut causer un déni de service pour d'autres processus entrants. Utilisez les arguments JVM pour activer la gestion des quotas dans Content Services.

Important : *les arguments JVM doivent être validés avant la synchronisation des utilisateurs. Il n'est pas possible de modifier ce quota d'utilisateurs après que les utilisateurs ont été synchronisés.*

3.3.1.3.1 Activation de la gestion des quotas dans Content Services

Sur JBoss

1 Accédez au répertoire *[racine jboss]*/bin et ouvrez le fichier de script de démarrage dans un éditeur de texte :

- **(Windows)** run.bat
- **(Linux et UNIX)** run.sh

2 Ajoutez les propriétés suivantes sous l'argument `Set JAVA_OPTS` :

`-Dsystem.usages.enableQuotaSize=true -Dsystem.usages.quota=`**[taille en Ko]**

3 Enregistrez le fichier, puis fermez-le.

4 Redémarrez le serveur JBoss avant de synchroniser les utilisateurs.

Sur WebLogic

1 Accédez à WebLogic Server Administration Console, entrez http://*[host name]*:*[port]*/console dans la ligne d'adresse d'un navigateur Web, où *[port]* correspond au port d'écoute non sécurisé. Par défaut, la valeur de ce port est 7001.

2 Dans l'écran de connexion, saisissez le nom d'utilisateur et le mot de passe WebLogic, puis cliquez sur **Log In**.

3 Sous Change Center, cliquez sur **Lock & Edit**.

4 Sous Domain Structure, cliquez sur **Environment** > **Servers** et, dans le volet de droite, cliquez sur le nom du serveur géré.

5 Dans le volet Settings for Server, cliquez sur les **ongletsConfiguration** > **Server Start**.

6 Dans la zone Arguments, ajoutez les arguments suivants en les séparant par un espace :

```
-Dsystem.usages.enableQuotaSize=true
-Dsystem.usages.quota=[size in KB]
```

7 Cliquez sur **Save**, puis sur **Activate Changes**.

8 Redémarrez le serveur WebLogic avant de synchroniser les utilisateurs.

Sur WebSphere

1 Dans l'arborescence de navigation de WebSphere Administrative Console, effectuez la procédure suivante pour le serveur d'applications :

(WebSphere 6.x) Cliquez sur **Servers** > **Application servers**

(WebSphere 7.x) Cliquez sur **Servers** > **ServerTypes** > **WebSphere application servers**.

2 Cliquez sur le nom du serveur dans le volet de droite.

3 Sous Server Infrastructure, cliquez sur **Java and Process Management** > **Process Definition**.

4 Sous Additional Properties, cliquez sur **Java Virtual Machine**.

5 Dans la zone **Generic JVM arguments**, ajoutez `-Dsystem.usages.enableQuotaSize=true` et `-Dsystem.usages.quota=`<*taille en Ko*>, séparés par des virgules, aux propriétés existantes.

6 Cliquez sur **OK** ou sur **Apply**, puis sur **Save directly to master configuration**.

7 Redémarrez le serveur WebSphere avant de synchroniser les utilisateurs.

3.3.2 Sécurité du serveur d'applications

Le tableau suivant décrit certaines techniques qui permettent de sécuriser votre serveur d'applications une fois l'application LiveCycle installée.

Problème	Description
Consoles d'administration de serveur d'applications	Après avoir installé, configuré et déployé LiveCycle sur votre serveur d'applications, désactivez l'accès aux consoles d'administration de serveur d'applications. Pour plus de détails, reportez-vous à la documentation de votre serveur d'applications.
Paramétrage des cookies pour le serveur d'applications	Les cookies des applications sont contrôlés par le serveur d'applications. Lorsqu'il déploie l'application, l'administrateur du serveur d'applications peut spécifier des préférences concernant les cookies, soit à l'échelle du serveur, soit pour des applications spécifiques. Par défaut, les paramètres définis à l'échelle du serveur sont prioritaires. Tous les cookies de session générés par votre serveur d'applications devraient inclure l'attribut `HttpOnly`. Par exemple, si vous utilisez JBoss Application Server, vous pouvez redéfinir l'élément SessionCookie sur `httpOnly="true"` dans le fichier `deploy/jbossweb.sar/context.xml`. Vous pouvez limiter l'envoi de cookies au moyen de HTTPS uniquement. En conséquence, les cookies ne sont pas envoyés non codés sur HTTP. Il est conseillé aux administrateurs de serveurs d'applications d'autoriser les cookies sûrs à l'échelle du serveur. Par exemple, si vous utilisez JBoss Application Server, vous pouvez redéfinir l'élément connecteur sur `secure=true` dans le fichier `server.xml`. Reportez-vous à la documentation de votre serveur d'applications pour plus d'informations sur les paramètres des cookies.
Exploration des répertoires	Lorsqu'un utilisateur demande une page qui n'existe pas ou le nom d'un directeur (la chaîne de demande se termine par une barre oblique (/)), le serveur d'applications ne devrait pas renvoyer le contenu de ce répertoire. Pour éviter cela, vous pouvez désactiver la capacité d'exploration des répertoires sur votre serveur d'applications. Vous devriez effectuer cette action pour l'application Administration Console, mais également pour les autres applications exécutées sur votre serveur. Pour JBoss, définissez la valeur du paramètre d'initialisation des listes de la propriété `DefaultServlet` sur `false` dans le fichier web.xml, comme illustré dans l'exemple ci-dessous : <servlet> <servlet-name>default</servlet-name> <servlet-class> org.apache.catalina.servlets.DefaultServlet </servlet-class> <init-param> <param-name>listings</param-name> <param-value>false</param-value> </init-param> <load-on-startup>1</load-on-startup> </servlet> Pour WebSphere, définissez la propriété `directoryBrowsingEnabled` du fichier ibm-web-ext.xmi sur `false`. Pour WebLogic, définissez les propriétés index-directories du fichier weblogic.xml sur `false`, comme illustré dans l'exemple suivant : <container-descriptor> <index-directory-enabled>false </index-directory-enabled> </container-descriptor>

3.3.3 Utilisation de la console JMX sur JBoss

Lorsque la console JMX (Java Management Extensions) est installée avec JBoss, il est possible de construire des URL utilisées comme des exploitations de scripts intersites (XSS), capables de révéler des informations sensibles sur votre système.

Si vous avez installé LiveCycle en appliquant la méthode clé en main et que vous utilisez la version de JBoss incluse avec cette installation clé en main, la console JMX JBoss est supprimée par défaut pour garantir que les risques de sécurité sont réduits au minimum. Toutefois, si vous avez besoin d'utiliser la console JMX JBoss, réinstallez-la en procédant comme suit.

1 Téléchargez une copie de JBoss 4.2.0 (ou version ultérieure) sur JBoss.org.

2 Arrêtez le serveur d'applications JBoss.

3 Dans le fichier d'archive compressé que vous avez téléchargé, extrayez les fichiers depuis *[racine JBoss]*/deploy/jmx-console.war/.

4 Placez les fichiers jmx-console.war/... dans le répertoire déploiement du répertoire d'installation de JBoss.

5 Redémarrez JBoss.

6 Accédez à l'URL suivante pour vous assurer que la console JMX JBoss est disponible :

http://localhost:8080/jmx-console

3.3.4 Sécurité de la base de données

Lorsque vous sécurisez votre base de données, implémentez les mesures indiquées par le revendeur de votre base de données. Attribuez à l'utilisateur de la base de données le nombre minimum d'autorisations requises sur cette base de données pour permettre l'utilisation avec LiveCycle. Par exemple, n'utilisez pas de compte avec des autorisations d'administrateur de base de données.

Sur Oracle, le compte de base de données que vous utilisez nécessite uniquement les droits CONNECT, RESOURCE et CREATE VIEW. Pour connaître les exigences des autres bases de données, voir Préparation à l'installation de LiveCycle sur un seul serveur.

3.3.4.1 Configuration de la sécurité intégrée dans SQL Server sur Windows pour JBoss

1 Modifiez *[JBOSS_HOME]*\server\all\deploy\adobe-ds.xml pour ajouter `integratedSecurity=true` à l'URL de connexion, comme illustré dans l'exemple suivant :

```
jdbc:sqlserver://<serverhost>:<port>;databaseName=<dbname>;integratedSecurity=true
```

2 Ajoutez le fichier sqljdbc_auth.dll au chemin d'accès du système Windows sur l'ordinateur exécutant le serveur d'applications. Le fichier sqljdbc_auth.dll se trouve avec l'installation du pilote Microsoft SQL JDBC 1.2 (par défaut *[InstallDir]*/sqljdbc_1.2/enu/auth/x86).

3 Modifiez la propriété du service Windows JBoss (JBoss pour LiveCycle) pour Ouvrir une session en tant que dans le Système local pour un compte utilisateur disposant d'une base de données LiveCycle et d'un ensemble minimum de droits. Si vous exécutez JBoss à partir de la ligne de commande plutôt que comme un service Windows, ignorez cette étape.

4 Faites passer la sécurité de SQL Server du mode **Mixte** au mode **Authentification Windows**.

3.3.4.2 Configuration de la sécurité intégrée dans SQL Server sur Windows pour WebLogic

1 Démarrez WebLogic Server Administration Console en saisissant l'URL suivante dans la ligne d'adresse d'un navigateur Web :

```
http://[host name]:7001/console
```

2 Sous Change Center, cliquez sur **Lock & Edit**.

3 Sous Domain Structure, cliquez sur *[domaine_base]* **Services JDBC Data Sources** et, dans le volet de droite, cliquez sur **IDP_DS**.

4 Dans l'écran suivant, dans l'onglet **Configuration**, cliquez sur l'onglet **ConnectionPool** et, dans la zone **Properties**, saisissez `integratedSecurity=true`.

5 Sous Domain Structure, cliquez sur **[domaine_base]** > **Service** > **JDBC** > **Data Sources** et, dans le volet de droite, cliquez sur **RM_DS**.

6 Dans l'écran suivant, dans l'onglet **Configuration**, cliquez sur l'onglet **Connection Pool** et, dans la zone **Properties**, saisissez `integratedSecurity=true`.

7 Ajoutez le fichier sqljdbc_auth.dll au chemin d'accès du système Windows sur l'ordinateur exécutant le serveur d'applications. Le fichier sqljdbc_auth.dll se trouve avec l'installation du pilote Microsoft SQL JDBC 1.2 (par défaut *[InstallDir]*/sqljdbc_1.2/enu/auth/x86).

8 Faites passer la sécurité de SQL Server du mode **Mixte** au mode **Authentification Windows**.

3.3.4.3 Configuration de la sécurité intégrée dans SQL Server sur Windows pour WebSphere

Sur WebSphere, vous pouvez configurer la sécurité intégrée uniquement lorsque vous utilisez un pilote JDBC SQL Server externe et non le pilote JDBC SQL Server incorporé avec WebSphere.

1 Connectez-vous à WebSphere Administrative Console.

2 Dans l'arborescence de navigation, cliquez sur **Resources** > **JDBC** > **Data Sources**, puis, dans le volet de droite, cliquez sur **IDP_DS**.

3 Dans le volet de droite, sous Additional Properties, cliquez sur **Custom Properties**, puis sur **New**.

4 Dans la zone **Name**, saisissez `integratedSecurity` et, dans la zone **Value**, saisissez `true`.

5 Dans l'arborescence de navigation, cliquez sur **Resources** > **JDBC** > **Data Sources**, puis, dans le volet de droite, cliquez sur **RM_DS**.

6 Dans le volet de droite, sous Additional Properties, cliquez sur **Custom Properties**, puis sur **New**.

7 Dans la zone **Name**, saisissez `integratedSecurity` et, dans la zone **Value**, saisissez `true`.

8 Sur l'ordinateur sur lequel WebSphere est installé, ajoutez le fichier sqljdbc_auth.dll au chemin du système Windows (C:\Windows). Ce fichier est situé au même emplacement que le programme d'installation du pilote Microsoft SQL JDBC 1.2 (le chemin par défaut est *[Rep_install]*/sqljdbc_1.2/enu/auth/x86).

9 Sélectionnez **Démarrer** > **Panneau de configuration** > **Services**, cliquez avec le bouton droit de la souris sur le service Windows pour WebSphere (IBM WebSphere Application Server <version> - <nœud>), puis sélectionnez **Propriétés**.

10 Dans la boîte de dialogue Propriétés, cliquez sur l'onglet **Ouvrir une session**.

11 Sélectionnez **Ce compte** et indiquez les informations requises pour définir le compte de connexion à utiliser.

12 Faites passer la sécurité de SQL Server du mode **Mixte** au mode **Authentification Windows**.

3.3.5 Protection de l'accès aux contenus sensibles dans la base de données

Le schéma de la base de données LiveCycle contient des informations sensibles relatives à la configuration du système et aux processus de l'entreprise et doit être protégé par un pare-feu. La base de données doit être considérée comme faisant partie de la même zone de confiance que le serveur LiveCycle Pour éviter tout risque de divulgation d'informations et de vol de données d'entreprise, la base de données doit être configurée par l'administrateur de base de données (DBA) pour donner l'accès aux administrateurs autorisés uniquement.

Pour une sécurité accrue, prévoyez d'utiliser des outils spécifiques au revendeur de votre base de données pour chiffrer les colonnes des tableaux contenant les données suivantes :

- clés de document Rights Management ;
- clé de chiffrement de PIN HSM Trust Store ;
- hachages des mots de passe des utilisateurs locaux.

Pour plus d'informations des outils spécifiques à des revendeurs, voir « 2.1.3 Informations sur la sécurité des bases de données » à la page 4.

3.3.6 Sécurité LDAP

En règle générale, un répertoire LDAP (Lightweight Directory Access Protocol) est utilisé par LiveCycle comme une source d'informations relatives aux utilisateurs et aux groupes de l'entreprise et comme un moyen d'authentifier les mots de passe. Assurez-vous que votre répertoire LDAP est configuré pour utiliser le protocole SSL (Secure Socket Layer) et que LiveCycle est configuré pour accéder à votre répertoire LDAP en utilisant son port SSL.

3.3.6.1 Déni de service LDAP

Une attaque courante utilisant LDAP consiste, pour un attaquant, à omettre délibérément de s'authentifier à plusieurs reprises. Ceci oblige le serveur d'annuaires LDAP à interdire à un utilisateur l'accès à tous les services dépendant de LDAP.

Vous pouvez définir le nombre de tentatives d'authentification maximum autorisé et la durée du verrouillage appliqué par LiveCycle lorsqu'un utilisateur échoue de manière répétée à s'authentifier auprès de. Dans Administration Console, choisissez les valeurs plus faibles. Lors de la sélection du nombre d'échecs d'authentification maximum autorisé, il est important de comprendre que si toutes les tentatives échouent, LiveCycle verrouille l'utilisateur avant que le serveur d'annuaire LDAP ne le fasse.

3.3.6.2 Paramètres de verrouillage de compte automatique

1. Connectez-vous à Administration Console.
2. Cliquez sur **Paramètres** > **User Management** > **Gestion des domaines**.
3. Sous Paramètres de verrouillage de compte automatique, définissez **Echecs d'authentification consécutifs max.** sur un nombre peu élevé, 3 par exemple.
4. Cliquez sur **Enregistrer**.

3.3.7 Contrôle et consignation

L'utilisation appropriée et sécurisée des capacités de contrôle et de consignation des applications peut contribuer au suivi et à la détection rapides des événements liés à la sécurité et autres anomalies. L'utilisation efficace des capacités de contrôle et de consignation dans une application inclut des points comme le suivi des connexions réussies et échouées, de même que les événements clés de l'application comme la création ou la suppression d'enregistrements clés.

Vous pouvez utiliser les capacités de contrôle pour détecter de nombreux types d'attaques, parmi lesquels :

- les attaques de mot de passe en force ;
- les attaques par déni de service ;
- les attaques par injection de saisie hostile et les classes associées d'attaques de script.

Ce tableau décrit les techniques de contrôle et de consignation que vous pouvez utiliser pour limiter les vulnérabilités du serveur.

Problème	Description
Listes de contrôle d'accès de fichier journal	Définissez les listes de contrôle d'accès (ACL) de fichier journal LiveCycle appropriées. Définir des informations d'identification appropriées contribue à empêcher les attaquants de supprimer les fichiers. Les autorisations de sécurité sur le répertoire des fichiers journaux doivent être de type « contrôle complet » pour les Administrateurs et les groupes SYSTEM. Seules les autorisations de lecture et d'écriture doivent être attribuées au compte utilisateur LiveCycle
Fichiers journaux redondants	Si les ressources le permettent, envoyez en temps réel des journaux à un autre serveur inaccessible pour l'attaquant (en lecture seule) en utilisant Syslog, Tivoli, Microsoft Operations Manager (MOM) Server ou tout autre mécanisme équivalent. En protégeant les journaux de cette manière, vous réduisez le risque de falsification. Par ailleurs, le fait de stocker les journaux dans un référentiel central facilite les processus de corrélation et de surveillance (par exemple, si plusieurs serveurs LiveCycle sont en cours d'utilisation et qu'une attaque par recherche de mot de passe a lieu sur plusieurs ordinateurs, un mot de passe étant demandé à chaque ordinateur).

3.3.8 Dépendances des bibliothèques du système LiveCycle Unix

Les informations suivantes sont destinées à vous aider à planifier un déploiement de LiveCycle sur votre environnement UNIX.

3.3.8.1 Service Convert PDF

Le service Convert PDF fait partie de LiveCycle et requiert au minimum les bibliothèques système suivantes :

Linux

```
/lib/
    libdl.so.2 (0x00964000)
    ld-linux.so.2 (0x007f6000)
/lib/tls/
    libc.so.6 (0x00813000)
    libm.so.6 (0x0093f000)
    libpthread.so.0 (0x00a5d000)
/usr/lib/libz.so.1 (0x0096a000)
/gcc410/lib/
    libgcc_s.so.1 (0x00fc0000)
    libstdc++.so.6 (0x00111000)
```

Solaris

```
/usr/platform/SUNW,Sun-Fire-V210/lib/libc_psr.so.1
/usr/lib/
    libc.so.1
    libdl.so.1
    libintl.so.1
    libm.so.1
    libmp.so.2
    libnsl.so.1
    libpthread.so.1
    libsocket.so.1
    libstdc++.so.6
    libthread.so.1
```

AIX

```
/usr/lib/
    libpthread.a(shr_comm.o)
    libpthread.a(shr_xpg5.o)
    libc.a(shr.o)
    librtl.a(shr.o)
    libpthreads.a(shr_comm.o)
    libcrypt.a(shr.o)
/aix5.2/lib/gcc/powerpc-ibm-aix5.2.0.0/4.1.0/libstdc++.a(libstdc++.so.6)
/aix5.2/lib/gcc/powerpc-ibm-aix5.2.0.0/4.1.0/libgcc_s.a(shr.o)
```

3.3.8.2 XMLForms

XMLForms requiert au minimum les bibliothèques systèmes suivantes :

Linux

```
/lib/
    libdl.so.2
    libpthread.so.0
    libm.so.6
    libgcc_s.so.1
    libc.so.6
    librt.so.1
    ld-linux.so.2
/usr/X11R6/lib/
    libX11.so.6
```

Solaris

```
/usr/lib/
    libdl.so.1
    libpthread.so.1
    libintl.so.1
    libsocket.so.1
    libnsl.so.1
    libm.so.1
    libc.so.1
    librt.so.1
    libX11.so.4
    libmp.so.2
    libmd5.so.1
    libscf.so.1
    libaio.so.1
    libXext.so.0
    libdoor.so.1
    libuutil.so.1
    libm.so.2
usr/platform/SUNW,Sun-Fire-V210/lib/libc_psr.so.1
usr/platform/SUNW,Sun-Fire-V210/lib/libmd5_psr.so.1
```

AIX 6.1

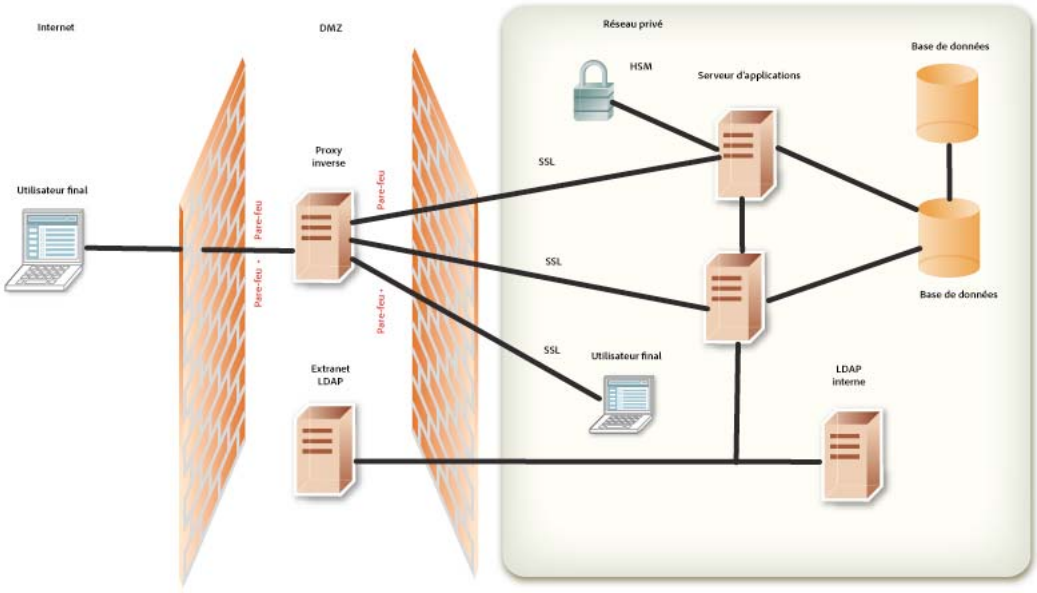
```
/usr/lib/
    libpthread.a(shr_comm.o)
    libpthread.a(shr_xpg5.o)
    libc.a(shr.o)
    librtl.a(shr.o)
    libdl.a(shr.o)
    libX11.a(shr4.o)
    libiconv.a(shr4.o)
    libpthreads.a(shr_comm.o)
/unix
    /usr/lib/libcrypt.a(shr.o)
    /usr/lib/libIM.a(shr.o)
    /usr/lib/libpthreads.a(shr_xpg5.o)
```

3.4 Configuration de LiveCycle pour un accès à l'extérieur de l'entreprise

Après avoir installé LiveCycle, il est important que vous assuriez une maintenance régulière de la sécurité de votre environnement. Cette section décrit les tâches recommandées pour assurer la maintenance de la sécurité du serveur de production LiveCycle

3.4.1 Configuration d'un proxy inverse pour l'accès Web

Un *proxy inverse* peut être utilisé pour garantir qu'un jeu d'URL d'applications Web LiveCycle est disponible à la fois pour des utilisateurs externes et internes. Cette configuration est plus sûre que si vous autorisiez des utilisateurs à se connecter directement au serveur d'applications sur lequel est exécuté LiveCycle. Le proxy inverse exécute toutes les requêtes HTTP pour le serveur d'applications qui exécute LiveCycle. Les utilisateurs disposent d'un accès réseau limité au seul proxy inverse et ne peuvent se connecter qu'aux URL prises en charge par le proxy inverse.



URL racines LiveCycle pour une utilisation avec un serveur proxy inverse

Les URL suivantes sont les URL racines de chaque application Web LiveCycle Configurez votre proxy inverse pour qu'il n'expose que les URL de fonctionnalités d'applications Web dont vous souhaitez autoriser l'accès aux utilisateurs finaux.

Certaines URL sont présentées comme des applications Web accessibles par les utilisateurs finaux. Evitez d'exposer d'autres URL Configuration Manager pour l'accès à des utilisateurs externes via le proxy inverse.

URL racine	Objectif et/ou application Web associée	Interface Web	Accès utilisateurs finaux
/ReaderExtensions/*	Application Web d'utilisateur final Reader Extensions pour appliquer des droits d'utilisation sur des documents PDF.	Oui	Oui
/edc/*	Application Web d'utilisateur final Rights Management.	Oui	Oui
/edcws/*	URL du service Web de Rights Management.	Non	Oui
/pdfgui/*	Application Web d'administration de PDF Generator.	Oui	Oui
/workspace/*	Application Web d'utilisateur final Workspace.	Oui	Oui
/workspace-server/*	Servlets et services de données Workspace requis par l'application cliente Workspace.	Oui	Oui
/contentspace/*	Application Web d'utilisateur final LiveCycle Contentspace (obsolète)	Oui	Oui

URL racine	Objectif et/ou application Web associée	Interface Web	Accès utilisateurs finaux
/adobe-bootstrapper/*	Servlet d'amorçage du référentiel LiveCycle	Non	Non
/soap/*	Page d'informations pour les services Web de LiveCycle Server	Non	Non
/soap/services/*	URL de service Web de tous les services de LiveCycle Server	Non	Non
/edc/admin/*	Application Web d'administration Rights Management.	Oui	Non
/adminui/*	Page d'accueil de Administration Console.	Oui	Non
/TruststoreComponent/secured/*	Pages d'administration de Trust Store Management	Oui	Non
/FormsIVS/*	Application Forms IVS pour tester et déboguer le rendu de formulaire.	Oui	Non
/OutputIVS/*	Application Output IVS pour tester et déboguer le service de sortie	Oui	Non
/rmws/*	URL REST pour Rights Management	Non	Oui
/OutputAdmin/*	Pages d'administration de Output	Oui	Non
/FormServer/*	Fichiers de l'application Web de Forms	Oui	Non
/FormServer/GetImage Servlet	Utilisée pour extraire du code JavaScript lors de transformations HTML	Non	Non
/FormServerAdmin/*	Pages d'administration de Forms	Oui	Non
/repository/*	URL d'accès à WebDAV (débogage)	Oui	Non
/AACComponent/*	Interface utilisateur des applications et services	Oui	Non
/WorkspaceAdmin/*	Pages d'administration de Workspace	Oui	Non
/rest/*	Pages de support de Rest	Oui	Non
/CoreSystemConfig/*	Page des paramètres de configuration de base de LiveCycle	Oui	Non
/um/	Authentification User Management	Non	Oui
/um/*	Interface d'administration de User Management	Oui	Non
/DocumentManager/*	Téléchargement des documents à traiter lors de l'accès à des points de fin Remoting et SOAP WSDL et au JDK Java à l'aide du transport SOAP ou EJB avec activation des documents HTTP.	Oui	Oui
/remoting/*	Ajouter un point de fin Remoting permet à une application Flex d'appeler le service à l'aide de LiveCycle Remoting.	Oui	Oui

3.5 Protection contre les attaques multisites par usurpation de requête

Une attaque multisites par usurpation de requête exploite la confiance d'un site Web envers l'utilisateur dans le but de transmettre des commandes non autorisées à son insu. Le principe de l'attaque consiste à inclure un lien ou un script dans une page Web, afin d'accéder à un autre site sur lequel l'utilisateur a déjà été authentifié.

Par exemple, vous pouvez être connecté à Administration Console tout en explorant un autre site Web. L'une des pages Web peut inclure une balise d'image HTML avec un attribut `src` visant un script côté serveur sur le site Web de la victime. En exploitant le mécanisme d'authentification de session basé sur les cookies, le site Web attaquant peut envoyer des requêtes malveillantes au script côté serveur ciblé en les faisant passer pour les requêtes de l'utilisateur autorisé. Pour consulter des exemples supplémentaires, voir https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)#Examples.

Les caractéristiques suivantes sont communes aux cas de CSRF :

- impliquent des sites qui reposent sur une identité de l'utilisateur ;
- exploitent la confiance du site dans cette identité ;
- trompent le navigateur de l'utilisateur pour le faire envoyer des requêtes HTTP à un site cible ;
- impliquent des requêtes HTTP ayant des effets secondaires.

LiveCycle utilise la fonctionnalité de filtrage des référents pour bloquer les attaques CSRF. Les termes suivants sont utilisés dans cette section pour décrire ce dispositif de filtrage des référents :

- **Référent autorisé :** un référent est l'adresse de la page source qui envoie une requête au serveur. Pour les pages ou les formulaires JSP, ce référent est généralement la page précédente dans l'historique de navigation. Les référents pour les images sont généralement les pages sur lesquelles les images sont affichées. Vous pouvez identifier les référents qui sont autorisés à accéder à votre serveur en les ajoutant à la liste de référents autorisés.
- **Exceptions aux référents autorisés :** si vous souhaitez restreindre l'accès pour un référent particulier dans votre liste de référents autorisés. Pour mettre en place cette restriction vous pouvez ajouter des chemins d'accès individuels de ce référent vers la liste des exceptions aux référents autorisés. Les requêtes provenant des chemins d'accès de la liste des exceptions aux référents autorisés ne peuvent appeler aucune ressource du serveur LiveCycle. Vous pouvez définir des exceptions aux référents autorisés pour une application spécifique et également utiliser une liste globale des exceptions s'appliquant à toutes les applications.
- **URI autorisés :** il s'agit d'une liste des ressources générées sans vérification de l'en-tête référent. Par exemple, les ressources telles que les pages d'aide, qui n'entraînent pas de changements d'état sur le serveur, peuvent être ajoutées à cette liste. Les ressources figurant dans la liste des URI autorisés ne sont jamais bloquées par le filtrage des référents, quel que soit le référent.
- **Référent de valeur NULL (null referer) :** une requête serveur qui n'est pas associée ou ne provient pas d'une page Web parente est considérée comme une requête de référent de valeur NULL. Par exemple, lorsque vous ouvrez une nouvelle fenêtre de navigateur, saisissez une adresse puis appuyez sur la touche Entrée, le référent envoyé au serveur est nul. Une application de bureau (.NET ou SWING), en rendant une requête HTTP à un serveur Web, envoie également un référent de valeur NULL au serveur.

3.5.1 Filtrage des référents

Le processus de filtrage des référents peut être décrit comme suit :

1 Le serveur LiveCycle vérifie la méthode HTTP utilisée pour l'appel :

   a S'il s'agit d'une méthode POST, le serveur LiveCycle vérifie l'en-tête référent.

b S'il s'agit d'une méthode GET, le serveur LiveCycle ignore la vérification du référent, à moins que la variable *CRSF_CHECK_GETS* ne soit définie sur true. Dans ce cas, il vérifie l'en-tête référent. La variable *CSRF_CHECK_GETS* est spécifiée dans le fichier *web.xml* pour votre application.

2 Le serveur LiveCycle vérifie si l'URI requis est autorisé :

a Si l'URI est autorisé, le serveur transmet la requête.

b Si l'URI requis n'est pas autorisé, le serveur récupère le référent de la requête.

3 S'il existe un référent pour la requête, le serveur vérifie s'il s'agit d'un référent autorisé. Si le référent est autorisé, le serveur vérifie qu'il ne fait pas partie des exceptions aux référents autorisés :

a S'il s'agit d'une exception, la requête est bloquée.

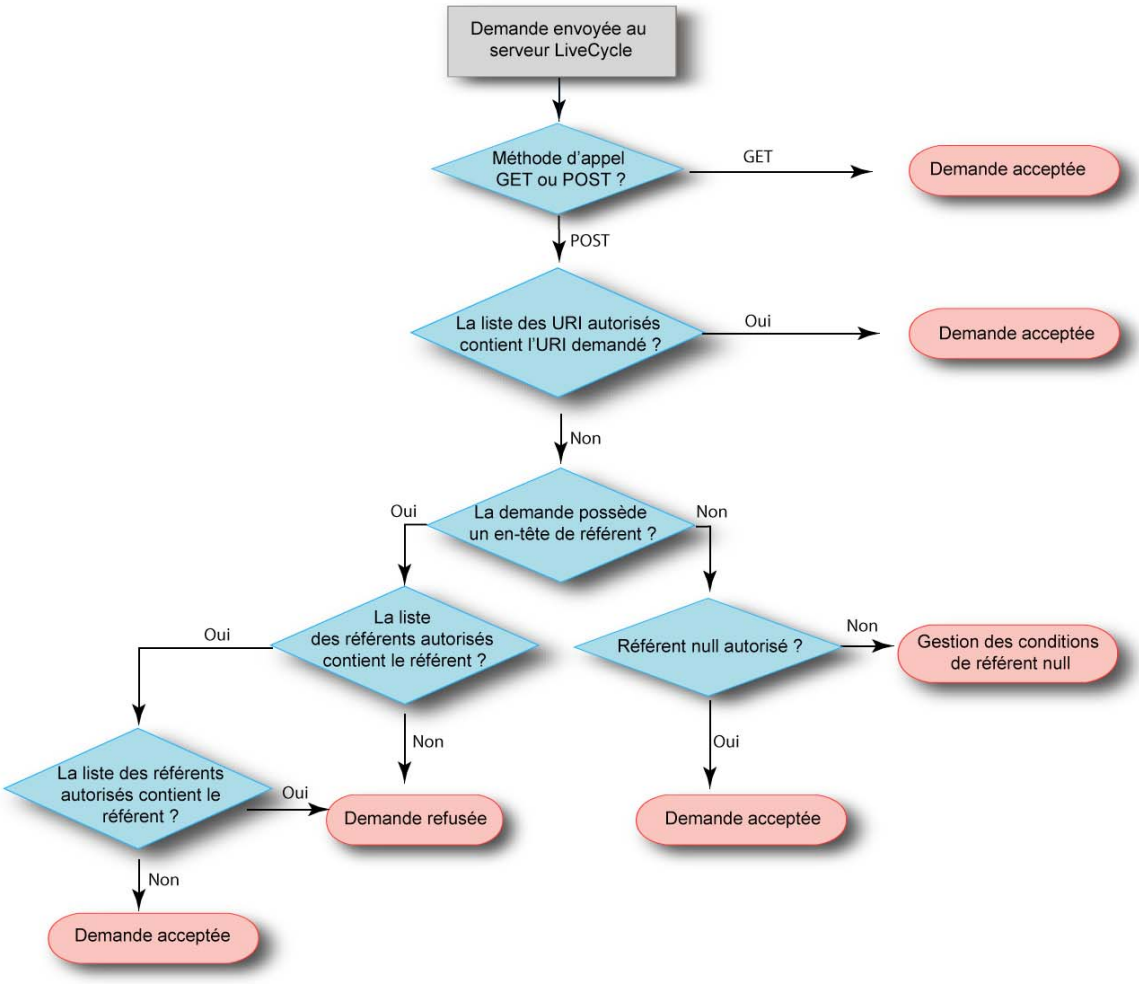
b S'il ne fait pas partie des exceptions, la requête est transmise.

4 S'il n'existe aucun référent pour la requête, le serveur vérifie que les référents de valeur NULL sont autorisés.

a Si les référents de valeur NULL sont autorisés, la requête est transmise.

b Si ce n'est pas le cas, le serveur vérifie que l'URI requis fait partie des exceptions aux référents de valeur NULL et traite la requête en fonction.

Le schéma suivant illustre la vérification CSRF que LiveCycle effectue lorsqu'une requête est envoyée au serveur.



3.5.2 Gestion du filtrage des référents

LiveCycle effectue un filtrage des référents afin de spécifier les référents qui sont autorisés à accéder aux ressources du serveur. Par défaut, le filtrage des référents ne filtre pas les requêtes qui utilisent une méthode HTTP sécurisée, par exemple GET, sauf si la variable *CSRF_CHECK_GETS* est définie sur true. Si le numéro de port pour un référent autorisé est défini sur 0, LiveCycle autorise toutes les requêtes des référents provenant de cet hôte quel que soit le numéro de port. Si aucun numéro de port n'est spécifié, seules les requêtes provenant du port par défaut 80 (HTTP) ou du port 443 (HTTPS) sont autorisées. Le filtrage des référents est désactivé si toutes les entrées de la liste de référents autorisés sont supprimées.

Lorsque vous installez Document Services pour la première fois, la liste de référents autorisés est mise à jour avec l'adresse du serveur sur lequel Document Services est installé. Les entrées pour le serveur comprennent le nom du serveur, l'adresse IPv4, l'adresse IPv6 si le protocole IPv6 est activé, l'adresse de bouclage et une entrée localhost. Les noms ajoutés à la liste des référents autorisés sont renvoyés par le système d'exploitation hôte. Par exemple, un serveur avec une adresse IP de 10.40.54.187 peut inclure les entrées suivantes : `http://nom-serveur:0, https://10.40.54.187:0, http://127.0.0.1:0, http://hôtelocal:0`. Pour chaque nom non qualifié renvoyé par le système d'exploitation hôte (les noms sans adresse IPv4 ou IPv6, ou sans nom de domaine qualifié) la liste blanche n'est pas mise à jour. Modifiez la liste de référents autorisés en fonction de votre environnement de travail. Ne déployez pas le serveur LiveCycle dans l'environnement de production avec la liste de référents autorisés par défaut. Après avoir modifié l'une des référents autorisés, l'une des exceptions aux référents ou l'un des URI, assurez-vous que vous redémarrez le serveur pour que les modifications prennent effet.

Gestion de la liste de référents autorisés

Vous pouvez gérer la liste de référents autorisés à partir de l'interface User Management d'Administration Console. L'interface User Management offre des fonctionnalités pour créer, éditer ou supprimer la liste. Reportez-vous à la section *Prévention d'attaques CSRF* du guide *Aide à l'administration* pour plus d'informations sur l'utilisation de la liste de référents autorisés.

Gestion des exceptions aux référents autorisés et des listes des URI autorisés

LiveCycle fournit des API pour gérer la liste des exceptions aux référents autorisé et la liste des URI autorisés. Vous pouvez utiliser ces API pour récupérer, créer, éditer ou supprimer la liste. Voici la liste des API disponibles :

- createAllowedURIsList
- getAllowedURIsList
- updateAllowedURIsList
- deleteAllowedURIsList
- addAllowedRefererExceptions
- getAllowedRefererExceptions
- updateAllowedRefererExceptions
- deleteAllowedRefererExceptions

Reportez-vous au *Guide de référence des API LiveCycle* pour plus d'informations sur les API.

Utilisez la liste ***LC_GLOBAL_ALLOWED_REFERER_EXCEPTION*** pour les exceptions aux référents autorisés au niveau global, c'est-à-dire pour définir les exceptions qui s'appliquent à toutes les applications. Cette liste contient uniquement des URI contenant soit un chemin absolu (par ex. `/index.html`), soit un chemin relatif (par ex. `/sample/`). Vous pouvez également ajouter une expression régulière à la fin d'un URI relatif, par ex. `/sample/(.)*`.

L'ID de liste ***LC_GLOBAL_ALLOWED_REFERER_EXCEPTION*** est définie comme une constante dans la classe `UMConstants` de l'espace de noms `com.adobe.idp.um.api`, figurant dans `adobe-usermanager-client.jar`. Vous pouvez utiliser les API LiveCycle pour créer, modifier ou éditer cette liste. Par exemple, pour créer la liste globale des exceptions aux référents autorisés, utilisez :

```
addAllowedRefererExceptions(UMConstants.LC_GLOBAL_ALLOWED_REFERER_EXCEPTION,
Arrays.asList("/index.html", "/sample/(.)*"))
```

Utilisez la liste ***CSRF_ALLOWED_REFERER_EXCEPTIONS*** pour les exceptions spécifiques à une application.

Désactivation du filtrage des référents

Dans le cas où le filtrage des référents bloque complètement l'accès au serveur LiveCycle et que vous ne pouvez pas modifier la liste des référents autorisés, vous pouvez mettre à jour le script de démarrage du serveur et désactiver le filtrage des référents.

Incluez l'argument JAVA `-Dlc.um.csrffilter.disabled=true` dans le script de démarrage et redémarrez le serveur. Assurez-vous de supprimer l'argument JAVA après avoir correctement reconfiguré la liste de référents autorisés.

Filtrage des référents pour les fichiers WAR personnalisés

Vous avez peut-être créé des fichiers WAR personnalisés afin de travailler avec LiveCycle pour répondre aux besoins de l'activité. Pour activer le filtrage des référents pour vos fichiers WAR personnalisés, vous devez inclure ***adobe-usermanager-client.jar*** dans le chemin de classe pour les fichiers WAR et inclure une entrée de filtre dans le fichier *web.xml* avec les paramètres suivants :

La variable **CSRF_CHECK_GETS** contrôle la vérification du référent sur les requêtes GET. Si ce paramètre n'est pas défini, la valeur par défaut est définie sur false. Incluez ce paramètre uniquement si vous souhaitez filtrer vos requêtes GET.

CSRF_ALLOWED_REFERER_EXCEPTIONS est l'ID de la liste des exceptions aux référents autorisés. Le filtrage des référents empêche les requêtes de référents de la liste identifiés par l'ID de la liste d'appeler toute ressource du serveur LiveCycle.

CSRF_ALLOWED_URIS_LIST_NAME est l'ID de la liste des URI autorisés. Le filtrage des référents ne bloque pas les requêtes concernant les ressources de la liste identifiées par l'ID de liste, quelle que soit la valeur de l'en-tête référent dans la requête.

CSRF_ALLOW_NULL_REFERER contrôle le comportement du filtrage des référents lorsque le référent est null ou non présent. Si ce paramètre n'est pas défini, la valeur par défaut est définie sur false. Incluez uniquement ce paramètre si vous souhaitez autoriser les référents de valeur NULL. L'autorisation des référents de valeur NULL peut permettre certains types d'attaques CSRF (Cross Site Request Forgery).

CSRF_NULL_REFERER_EXCEPTIONS est une liste des URI pour lesquels une vérification référent n'est pas exécutée lorsque le référent est nul. Ce paramètre est activé uniquement lorsque la variable *CSRF_ALLOW_NULL_REFERER* est définie sur false. Séparez les URI de la liste à l'aide de virgules.

Voici un exemple de l'entrée de filtre dans le fichier *web.xml* pour un ***exemple*** de dossier WAR :

```
<filter>
       <filter-name> filter-name </filter-name>
       <filter-class> com.adobe.idp.um.auth.filter.RemoteCSRFFilter </filter-class>
     <!-- default is false -->
     <init-param>
      <param-name> CSRF_ALLOW_NULL_REFERER </param-name>
      <param-value> false </param-value>
     </init-param>
     <!-- default is false -->
     <init-param>
      <param-name> CSRF_CHECK_GETS </param-name>
      <param-value> true </param-value>
     </init-param>
     <!-- Optional -->
     <init-param>
       <param-name> CSRF_NULL_REFERER_EXCEPTIONS </param-name>
       <param-value> /SAMPLE/login, /SAMPLE/logout  </param-value>
     </init-param>
     <!-- Optional -->
     <init-param>
      <param-name> CSRF_ALLOWED_REFERER_EXCEPTIONS </param-name>
      <param-value> SAMPLE_ALLOWED_REF_EXP_ID </param-value>
     </init-param>
     <!-- Optional -->
     <init-param>
      <param-name> CSRF_ALLOWED_URIS_LIST_NAME </param-name>
      <param-value> SAMPLE_ALLOWED_URI_LIST_ID </param-value>
     </init-param>
</filter>
    ........
    <filter-mapping>
      <filter-name> filter-name </filter-name>
      <url-pattern>/*</url-pattern>
    </filter-mapping>
```

Dépannage

Si des requêtes serveur légitimes sont bloquées par le filtre CSRF, essayez l'une des méthodes suivantes :

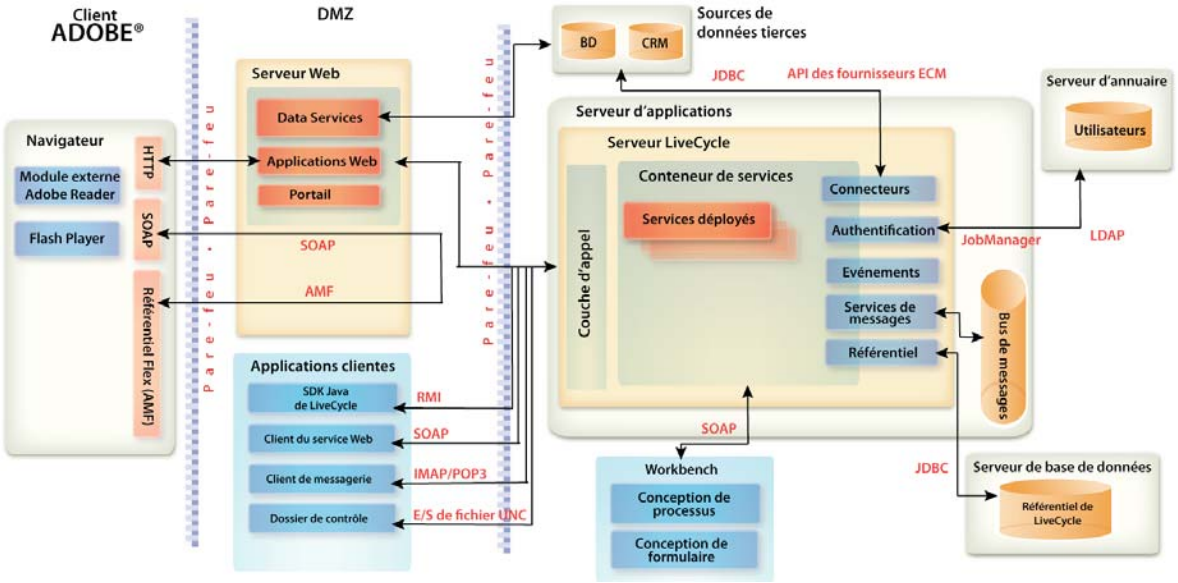
- Si la requête rejetée a un en-tête référent, il est souhaitable de l'ajouter à liste des référents autorisés. Ajoutez uniquement les références que vous approuvez.
- Si la requête rejetée ne dispose pas d'un en-tête référent, modifiez votre application client pour inclure un en-tête référent.
- Si le client peut travailler dans un navigateur, essayez ce modèle de déploiement.
- En dernier recours, vous pouvez ajouter la ressource à la liste des URI autorisés. Ceci n'est pas un paramètre recommandé.

3.6 Configuration réseau sécurisée

Cette section décrit les protocoles et les ports requis par LiveCycle et propose des recommandations pour déployer LiveCycle dans une configuration réseau sécurisée.

3.6.1 Architecture physique de LiveCycle

Cette image présente les composants et les protocoles utilisés dans un déploiement classique de LiveCycle, dont la topologie de pare-feu appropriée.



3.6.2 Protocoles réseau utilisés par LiveCycle

Lorsque vous configurez une architecture réseau sécurisée comme décrit dans la section précédente, les protocoles réseau suivants sont requis pour l'interaction entre LiveCycle et d'autres systèmes dans le réseau de votre entreprise.

Protocole	**Utilisation**
HTTP	• Le navigateur affiche Configuration Manager et des applications Web d'utilisateur final. • Toutes les connexions SOAP
SOAP	• Applications clientes de services Web telles que les applications .NET • Adobe Reader® utilise SOAP pour les services Web de LiveCycle Server • Les applications Adobe Flash® utilisent SOAP pour les services Web de serveur LiveCycle • Appels du SDK LiveCycle si utilisation en mode SOAP • Environnement de création de Workbench
RMI	Appels du SDK LiveCycle si utilisation en mode Enterprise JavaBeans (EJB)
IMAP / POP3	• Entrée par courrier électronique dans un service (point de fin de courrier électronique) • Notifications des tâches utilisateur par courrier électronique
UNC File IO	Surveillance de LiveCycle des dossiers de contrôle pour l'entrée dans un service (point de fin de dossier de contrôle)
LDAP	• Synchronisations des informations relatives aux utilisateurs et aux groupes de l'entreprise dans un annuaire • Authentification LDAP pour les utilisateurs interactifs

Protocole	Utilisation
JDBC	• Appels de requête et de procédure à une base de données externe lors de l'exécution d'un processus utilisant le service JDBC • Référentiel LiveCycle d'accès interne
WebDAV	Permet la navigation à distance dans le référentiel de conception LiveCycle (formulaires, fragments, etc.) par tout client WebDAV.
AMF	Applications Adobe Flash, dans lesquelles les services de serveur LiveCycle sont configurés avec un point de fin Remoting.
JMX	LiveCycle expose les MBeans pour le contrôle avec JMX.

3.6.3 Ports de serveur d'applications

Cette section décrit les ports par défaut (et les plages de configurations alternatives) pour chaque type de serveur d'applications pris en charge. Ces ports doivent être activés ou désactivés sur le pare-feu interne, selon la fonctionnalité réseau que vous souhaitez autoriser aux clients qui se connectent au serveur d'applications qui exécute LiveCycle.

Remarque : *Par défaut, le serveur expose plusieurs MBeans JMX sous l'espace de nom adobe.com. Seules les informations utiles à la surveillance de la santé du serveur sont exposées. Toutefois, pour éviter toute divulgation d'informations, interdisez aux appelants dans un réseau non approuvé de rechercher les MBean JMX et d'accéder aux mesures de santé.*

Ports JBoss

Fonction	Port
Accès aux applications Web	[racine JBoss]/server/all/deploy/jbossweb-tomcat50.sar/server.xml Port HTTP/1.1 Connector 8080 Port AJP 1.3 Connector 8009 Port SSL/TLS Connector 8443
Accès aux services de LiveCycle Server	[racine JBoss]/server/all/conf/jboss-service.xml Port WebService 8083 Port NamingService 1099 RMIport à partir de 1098 RMIObjectPort à partir de 4444 PooledInvoker ServerBindPort 4445

Fonction	Port
Prise en charge des grappes de serveurs J2EE	[racine JBoss]/server/all/deploy/cluster-service.xml Port ha.jndi.HANamingService à partir de 1100 RmiPort 1101 RMIObjectPort 4447 (Grappes de serveurs uniquement) ServerBindPort 4446
Prise en charge de CORBA	[racine JBoss]/server/all/conf/jacorb.properties OAPort 3528 OASSLPort 3529
Prise en charge de SNMP	[racine JBoss]/server/all/deploy/snmp-adaptor.sar/META-INF/jbossservice.xml Ports 1161, 1162 [racine JBoss]/server/all/deploy/snmp-adaptor.sar/managers.xml Port 1162

Ports WebLogic

Fonction	Port
Accès aux applications Web	• Port d'écoute d'Admin Server : 7001 par défaut • Port d'écoute SSL d'Admin Server : 7002 par défaut • Port configuré pour Managed Server, par exemple 8001
Ports d'administration de WebLogic non requis pour l'accès à LiveCycle	• Port d'écoute de Managed Server : configurable de 1 à 65534 • Port d'écoute SSL de Managed Server : configurable de 1 à 65534 • Port d'écoute de Node Manager : 5556 par défaut

Ports WebSphere 6.1

Pour plus de détails sur les ports WebSphere 6.1 requis par LiveCycle, consultez Paramètres des numéros de ports dans les versions de WebSphere Application Server.

Ports WebSphere 7.0

Pour plus d'informations sur les ports WebSphere 7.0 requis par LiveCycle, visitez le site Web http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.migration.express.doc/info/exp/ae/rmig_portnumber.html.

3.6.4 Configuration de SSL

En vous référant à l'architecture physique décrite dans la section « 3.6.1 Architecture physique de LiveCycle » à la page 30, configurez SSL pour toutes les connexions que vous prévoyez d'utiliser. Spécifiquement, toutes les connexions SOAP doivent être établies via SSL pour empêcher que les informations d'identification des utilisateurs soient exposées sur un réseau.

Pour savoir de quelle manière configurer le protocole SSL sur JBoss, WebLogic et WebSphere, voir Configuration de SSL dans Aide à l'administration de LiveCycle.

3.6.5 Configuration de la redirection SSL

Après avoir configuré votre serveur d'applications pour qu'il prenne en charge SSL, vous devez vous assurer que l'ensemble du trafic HTTP vers les applications et les services LiveCycle utilise le port SSL.

Pour configurer la redirection SSL pour WebSphere et WebLogic, reportez-vous à la documentation de votre serveur d'applications.

1 Accédez au fichier adobe-livecycle-jboss.ear et décompressez-le.

2 Extrayez le fichier adminui.war et ouvrez le fichier web.xml pour le modifier.

3 Ajoutez le code suivant au fichier web.xml :

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>app or resource name</web-resource-name>
        <url-pattern>/*</url-pattern>
        <!-- define all url patterns that need to be protected-->
        <http-method>GET</http-method>
        <http-method>POST</http-method>
    </web-resource-collection>
    <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>
```

3.7 Recommandations de sécurité spécifiques à Windows

Cette section contient des recommandations de sécurité spécifiques à Windows dans le cadre de l'exécution de LiveCycle.

3.7.1 Comptes de service JBoss

L'installation clé en main de LiveCycle installe un compte de service par défaut en utilisant le compte système local. Le compte utilisateur système local intégré présente un haut niveau d'accessibilité ; il fait partie du groupe Administrateurs. Si une identité de processus de travail est exécutée en tant que compte utilisateur système local, ce processus de travail dispose d'un accès complet à l'ensemble du système.

3.7.1.1 Exécution du serveur d'applications à l'aide d'un compte non administratif spécifique

1 Dans Microsoft Management Console (MMC), créez un utilisateur local pour que le service LiveCycle se connecte en tant que cet utilisateur local :

- Sélectionnez **L'utilisateur ne peut pas changer de mot de passe**.
- Vérifiez que le groupe Utilisateurs figure dans l'onglet **Membre de**.

2 Sélectionnez **Paramètres** > **Outils d'administration** > **Services**.

3 Cliquez deux fois sur le service de serveur d'applications et arrêtez ce service.

4 Sur l'onglet **Ouvrir une session**, sélectionnez **Ce compte**, recherchez le compte utilisateur que vous avez créé, puis entrez le mot de passe pour ce compte.

5 Dans la fenêtre Paramètres de sécurité locaux, sous Attribution des droits utilisateur, attribuez les droits suivants au compte utilisateur sous lequel est exécuté le serveur LiveCycle :

- Interdire l'ouverture de session par les services Terminal
- Interdire l'ouverture d'une session locale
- Ouvrir une session en tant que service (ce droit doit être déjà défini)

6 Attribuez au nouveau compte utilisateur les autorisations de lecture et d'exécution, d'affichage du contenu des dossiers et de lecture pour les répertoires de contenu Web LiveCycle

7 Démarrez le service de serveur d'applications.

3.7.2 Sécurité du système de fichiers

LiveCycle utilise le système de fichiers comme suit :

- stocke les fichiers temporaires utilisés lors du traitement des entrées et sorties de documents ;
- stocke dans une banque d'archives globale les fichiers utilisés pour prendre en charge les composants de la solution qui sont installés ;
- les dossiers de contrôle stockent les fichiers utilisés en entrée dans un service à partir d'un emplacement de dossier du système de fichiers.

Lorsque vous utilisez des dossiers de contrôle comme moyen d'envoyer et de recevoir des documents avec un service LiveCycle, soyez très prudent quant à la sécurité du système de fichiers. Lorsqu'un utilisateur dépose des contenus dans le dossier de contrôle, ces contenus sont exposés via le dossier de contrôle. Dès lors, le service n'authentifie pas l'utilisateur final réel. Au lieu de cela, il considère que la sécurité par liste de contrôle d'accès et par niveau de dossier a été définie au niveau des dossiers pour déterminer qui peut effectivement appeler le service.

3.8 Recommandations de sécurité spécifiques à JBoss

Cette section présente des recommandations relatives à la configuration du serveur d'applications et spécifiques à JBoss 4.2.x lorsque celui-ci est utilisé pour exécuter LiveCycle.

3.8.1 Désactivation de la console de gestion JBoss et de la console JMX

L'accès à la console de gestion JBoss et à la console JMX est déjà configuré (la surveillance JMX est désactivée) lorsque vous installez LiveCycle sur JBoss en appliquant la méthode d'installation clé en main. Si vous utilisez votre propre serveur d'applications JBoss, assurez-vous que l'accès à la console de gestion JBoss et à la console de surveillance JMX est sécurisé. L'accès à la console de surveillance JMX est défini dans le fichier de configuration de JBoss appelé jmx-invoker-service.xml.

3.8.2 Désactivation de l'exploration des répertoires

Après vous être identifié dans Administration Console, il vous est possible de parcourir la liste des répertoires de la console en modifiant l'URL. Par exemple, si vous modifiez l'URL pour l'une de ces adresses, une liste de répertoires s'affiche :

```
http://<servername>:8080/adminui/secured/
http://<servername>:8080/um/
```

Pour désactiver la liste des répertoires, définissez la valeur du paramètre d'initialisation des listes de la propriété `DefaultServlet` sur `false`, comme illustré en gras dans le fichier *[racine JBoss]* \server\default\deploy\jbossweb-tomcatxxx.sar\conf\web.xml :

```
<servlet>
    <servlet-name>default</servlet-name>
    <servlet-class>
        org.apache.catalina.servlets.DefaultServlet
    </servlet-class>
    <init-param>
        <param-name>listings</param-name><param-value>false</param-value>
    </init-param>
    <load-on-startup>1</load-on-startup>
</servlet>]
```

3.9 Recommandations de sécurité spécifiques à WebLogic

Cette section présente des recommandations relatives à la configuration du serveur d'applications et spécifiques à WebLogic 9.1 lorsque celui-ci est utilisé pour exécuter LiveCycle.

3.9.1 Désactivation de l'exploration des répertoires

Définissez les propriétés index-directories du fichier weblogic.xml sur `false`, comme illustré dans l'exemple suivant :

```
<container-descriptor>
    <index-directory-enabled>false
    </index-directory-enabled>
</container-descriptor>
```

3.9.2 Activation du port SSL de WebLogic

Par défaut, WebLogic n'active pas le port d'écoute SSL par défaut, 7002. Activez ce port dans le serveur WebLogic Server Administration Console avant de configurer SSL.

3.10 Recommandations de sécurité spécifiques à WebSphere

Cette section présente des recommandations relatives à la configuration du serveur d'applications et spécifiques à WebSphere lorsque celui-ci est utilisé pour exécuter LiveCycle.

3.10.1 Désactivation de l'exploration des répertoires

Définissez la propriété `directoryBrowsingEnabled` du fichier ibm-web-ext.xml sur `false`.

3.10.2 Activation de la sécurité administrative de WebSphere

1 Connectez-vous à WebSphere Administrative Console.

2 Dans l'arborescence de navigation, accédez à l'un des liens suivants :

(WebSphere 6.1) **Security** > **Secure administration, applications, andinfrastructure**

(WebSphere 7.0) **Security** > **Global Security**

3 Sélectionnez **Enable administrative security**.

4 Désélectionnez **Enable application security** et **Use Java 2 security**.

5 Cliquez sur **OK** ou sur **Apply**.

6 Dans la zone **Messages**, cliquez sur **Save directly to master configuration**.

Chapitre 4 : Configuration des paramètres d'administration sécurisée

En règle générale, les développeurs n'utilisent pas l'environnement de production de LiveCycle pour construire et tester leurs applications. Pour cette raison, vous devez administrer des comptes utilisateur et des services qui, bien que nécessaires dans un environnement de développement privé, ne le sont pas dans un environnement de production.

Cette section décrit les méthodes que vous pouvez appliquer pour réduire la surface d'attaque globale en utilisant des options d'administration fournies par LiveCycle

4.1 Désactivation des accès distants non indispensables à des services

Une fois LiveCycle installé et configuré, de nombreux services sont accessibles par appel distant sur SOAP, Enterprise JavaBeans™ (EJB) et LiveCycle Remoting. Ici, le terme *distant* renvoie à tout appelant disposant d'un accès réseau aux ports SOAP, EJB ou Action Message Format (AMF) du serveur d'applications.

Bien que l'utilisation des services LiveCycle implique la transmission d'informations d'identification valides pour un appelant autorisé, vous devriez limiter la possibilité d'accès distant aux seuls services dont vous souhaitez effectivement qu'ils soient accessibles à distance. Pour limiter efficacement l'accessibilité, réduisez au minimum le nombre de services accessibles à distance sans gêner le fonctionnement du système, puis activez l'appel distant pour les services supplémentaires dont vous avez besoin.

Les services LiveCycle requièrent toujours au moins un accès SOAP. Ces services sont généralement nécessaires pour Workbench, mais il peut également s'agir de services appelés par l'application Web Workspace.

Suivez cette procédure en utilisant la page Web Applications et services dans Administration Console :

1 Connectez-vous à Administration Console en saisissant l'URL suivante dans un navigateur Web :

```
http://[host name]:[port]/adminui
```

2 Cliquez sur **Services > Applications et services > Préférences**.

3 Définissez les préférences afin d'afficher jusqu'à 200 services et points de fin par page.

4 Cliquez sur **Services** > **Applications et services** > **Gestion des points de fin**.

5 Sélectionnez **EJB** depuis la liste **Fournisseur**, puis cliquez sur **Filtre**.

6 Pour désactiver tous les points de fin EJB, sélectionnez la case à cocher située en regard de chaque point de fin dans la liste et cliquez sur **Désactiver**.

7 Cliquez sur **Suivant** et répétez les étapes décrites ci-dessus pour chaque point de fin EJB. Assurez-vous qu'EJB figure dans la colonne Fournisseur avant de désactiver les points de fin.

8 Sélectionnez **SOAP** depuis la liste **Fournisseur**, puis cliquez sur **Filtre**.

9 Pour désactiver tous les points de fin SOAP, cochez la case située en regard de chaque point de fin dans la liste et cliquez sur **Supprimer**. Ne supprimez pas les points de fin suivants :

- AuthenticationManagerService
- DirectoryManagerService

- JobManager
- event_management_service
- event_configuration_service
- ProcessManager
- TemplateManager
- RepositoryService
- TaskManagerService
- TaskQueueManager
- TaskManagerQueryService
- WorkspaceSingleSignOn
- EventGenerationandReceipt

10 Cliquez sur **Suivant** et répétez les étapes précédentes pour chaque point de fin SOAP qui ne figure pas dans la liste ci-dessus. Assurez-vous que SOAP figure dans la colonne Fournisseur avant de supprimer les points de fin.

4.2 Désactivation des accès anonymes non indispensables à des services

Certains services LiveCycle permettent d'appeler sans authentification (de manière anonyme) certaines opérations. Ceci signifie qu'il est possible d'appeler une ou plusieurs opérations exposées par le service en tant qu'utilisateur authentifié ou non.

1 Connectez-vous à Administration Console en saisissant l'URL suivante dans un navigateur Web :

```
http://[host name]:[port]/adminui
```

2 Cliquez sur **Services > Applications et services > Gestion des services**.

3 Cliquez sur le nom du service à désactiver (par exemple, AuthenticationManagerService).

4 Cliquez sur l'onglet **Sécurité**, désélectionnez **Accès anonyme autorisé**et cliquez sur **Enregistrer**.

5 Effectuez les étapes 3 et 4 pour les services suivants :

- AuthenticationManagerService
- EJB
- Email
- JobManager
- WatchedFolder
- UsermanagerUtilService
- Remoting
- RemoteEvents
- RepositoryProviderService
- EMCDocumentumRepositoryProvider
- IBMFilenetRepositoryProvider

- FormAugmenter
- TaskManagerService
- TaskManagerConnector
- TaskManagerQueryService
- TaskQueueManager
- TaskEndpointManager
- LCMTMInvoker
- UserService
- WorkspaceSearchTemplateService
- WorkspaceSignleSignOn
- WorkspacePropertyService
- OutputService
- FormsService

Si vous prévoyez d'exposer l'un de ces services pour les appels distants, vous devriez également envisager de désactiver l'accès anonyme pour ces services. Si vous ne le faites pas, tout appelant disposant d'un accès réseau à ce service pourra appeler le service sans spécifier d'informations d'identification valides.

Nous vous conseillons de désactiver l'accès anonyme pour tous les services dont vous n'avez pas besoin. De nombreux services internes impliquent que l'authentification anonyme soit activée, car ils doivent pouvoir être appelés par potentiellement tout utilisateur du système sans préautorisation.

4.3 Suppression des exemples d'affectations d'utilisateurs et de rôles

Vous avez peut-être inclus des exemples d'utilisateurs et de rôles lors de l'installation de LiveCycle (par exemple, Kel Varsen et le domaine utilisateur Finance Corp). A l'aide des pages d'administration de User Management, vous devriez supprimer l'exemple de domaine utilisateur et les exemples de rôles.

4.3.1 Suppression des exemples d'utilisateurs

1 Connectez-vous à Administration Console en saisissant l'URL suivante dans un navigateur Web :

```
http://[host name]:[port]/adminui
```

2 Cliquez sur **Paramètres > User Management > Utilisateurs et groupes**.

3 Sélectionnez l'organisation d'exemples dans la liste **et domaine** et cliquez sur **Rechercher**.

4 Pour désactiver tous les exemples d'utilisateurs, cochez la case située en regard de chaque point de fin dans la liste et cliquez sur **Supprimer**.

4.3.2 Suppression des exemples de domaines

1 Connectez-vous à Administration Console en saisissant l'URL suivante dans un navigateur Web :

```
http://[host name]:[port]/adminui
```

2 Cliquez sur **Paramètres > User Management > Gestion des domaines**.

3 Pour désactiver tous les exemples de domaines, sélectionnez la case à cocher située en regard de chaque point de fin dans la liste et cliquez sur **Supprimer**.

4 Cliquez sur **Enregistrer**.

4.4 Modification du délai d'expiration global par défaut

Les utilisateurs finaux peuvent s'authentifier auprès de LiveCycle par le biais de LiveCycle Workbench, des applications Web LiveCycle ou des applications personnalisées qui appellent des services LiveCycle. Un paramètre de délai d'expiration permet de spécifier la durée pendant laquelle ces utilisateurs peuvent interagir avec LiveCycle (en utilisant une assertion SAML) avant d'être obligés de s'authentifier de nouveau. Par défaut, ce paramètre est défini sur deux heures. Dans un environnement de production, cette durée doit être réduite au nombre minimum de minutes acceptable.

4.4.1 Réduction au minimum de la durée limite avant réauthentification:

1 Connectez-vous à Administration Console en saisissant l'URL suivante dans un navigateur Web :

```
http://[host name]:[port]/adminui
```

2 Cliquez sur **Paramètres > User Management > Configuration > Importer et exporter des fichiers de configuration**.

3 Cliquez sur **Exporter** pour produire un fichier config.xml contenant les paramètres de LiveCycle

4 Ouvrez le fichier XML dans un éditeur et recherchez l'entrée suivante :

```
<entrée key="assertionValidityInMinutes" value="120"/>
```

5 Spécifiez une valeur en minutes supérieure ou égale à 5 et enregistrez le fichier.

6 Dans Administration Console, naviguez jusqu'à la page Importer et exporter des fichiers de configuration.

7 Saisissez le chemin d'accès au fichier config.xml modifié ou cliquez sur Parcourir pour le localiser.

8 Cliquez sur **Importer** pour télécharger le fichier config.xml, puis cliquez sur **OK**.