Härtung und Sicherheit für Adobe® LiveCycle® ES3

Rechtliche Hinweise

Weitere Informationen zu rechtlichen Hinweisen finden Sie unter http://help.adobe.com/de_DE/legalnotices/index.html.

Letzte Aktualisierung 7.6.2013

Inhalt

Kapitel 1: Informationen zu diesem Dokument

Dieses Dokument enthält Informationen zum Maximieren der Sicherheit der Produktionsumgebung von Adobe® LiveCycle® Enterprise Suite (ES3).

Weitere Sicherheitsinformationen für LiveCycle sind im LiveCycle Developer Center verfügbar.

Sicherheitstipps und -berichte für LiveCycle sind auf der Site Adobe Security Bulletins and Advisories verfügbar.

1.1 Zielgruppe des Dokuments

Die Zielgruppe dieses Dokuments sind IT-Berater, Sicherheitsexperten, Systemarchitekten und IT-Spezialisten, die für die Planung der Anwendungs- oder Infrastrukturentwicklung sowie die Bereitstellung von LiveCycle verantwortlich sind. Zu diesen Rollen zählen die folgenden gängigen Rollen:

- IT- und Produktionsingenieure, die sichere Webanwendungen und -server in ihren eigenen oder Kundenorganisationen bereitstellen müssen
- Architekten und Systemplaner mit der Aufgabe, die Architekturentwicklung für die Kunden in ihren Unternehmen zu planen
- IT-Sicherheitsspezialisten, die schwerpunktmäßig für die plattformübergreifende Sicherheit innerhalb ihrer Unternehmen zuständig sind
- Berater von Adobe und Partner, die detaillierte Ressourcen für Kunden und Partner benötigen

1.2 Konventionen in diesem Handbuch

In diesem Dokument werden die folgenden Benennungskonventionen für allgemeine Dateipfade verwendet.

Name	Standardwert	Beschreibung
[LiveCycle-Stammordner]	Windows: C:\Adobe\Adobe LiveCycle ES3 Linux und UNIX: opt/adobe/adobe_livecycle_es3	Der Installationsordner für alle LiveCycle-Module. Der Installationsordner enthält Unterordner für Adobe® LiveCycle® Configuration Manager. Dieser Ordner enthält außerdem Ordner im Zusammenhang mit Drittanbietertechnologien.
[JBoss-Stammordner]	C:\Adobe\Adobe LiveCycle ES3\jboss	(JBoss Turnkey) Der Basisordner des Anwendungsservers, auf dem LiveCycle ausgeführt wird.

1.3 Zusätzliche Informationen

In der folgenden Tabelle finden Sie Hinweise auf weiterführende Informationen zu LiveCycle.

Thema	Siehe
LiveCycle, die LiveCycle-Lösungen und Entwicklungswerkzeuge	LiveCycle-Übersicht
Vorbereiten Ihrer Umgebung für die Installation von oder die Aktualisierung auf LiveCycle	Vorbereiten der Installation von LiveCycle (Einzelserver) Vorbereiten der Installation von LiveCycle (Servercluster) Vorbereiten der Aktualisierung auf LiveCycle ES3
Installieren von LiveCycle (Einzelserver)	Installieren und Bereitstellen von LiveCycle mithilfe von JBoss Turnkey }Installieren und Bereitstellen von LiveCycle für JBoss Installieren und Bereitstellen von LiveCycle für WebLogic Installieren und Bereitstellen von LiveCycle für WebSphere
Konfigurieren von LiveCycle (Servercluster)	Konfigurieren von LiveCycle Application Server-Clustern mit JBoss Konfigurieren von LiveCycle-Application Server-Clustern mit WebLogic Konfigurieren von Adobe LiveCycle Application Server-Clustern mit WebSphere
Aktualisieren auf LiveCycle	Aktualisieren auf LiveCycle ES3 für JBoss Turnkey Aktualisieren auf LiveCycle ES3 für JBoss Aktualisieren auf LiveCycle ES3 für WebLogic Aktualisieren auf LiveCycle ES3 für WebSphere
Installieren von LiveCycle Workbench 10	Installing LiveCycle Workbench 10
Ausführen allgemeiner Verwaltungsaufgaben für LiveCycle	LiveCycle Administration-Hilfe
Weitere Dienste und Produkte, die mit LiveCycle integriert werden können	http://www.adobe.com/de
LiveCycle-Dokumentationssatz	LiveCycle-Dokumentationssatz

Kapitel 2: Allgemeine Überlegungen zur Sicherheit

In diesem Abschnitt finden Sie einleitende Informationen, die Ihnen die Vorbereitung auf das Härten Ihrer LiveCycle-Umgebung erleichtern sollen. Hier finden Sie Informationen zu LiveCycle, Betriebssystem, Anwendungsserver und Datenbanksicherheit, die Sie als Grundvoraussetzung benötigen. Sie sollten diese Informationen lesen, bevor Sie mit dem Sperren der Umgebung fortfahren.

2.1 Herstellerspezifische Sicherheitsinformationen

Dieser Abschnitt enthält sicherheitsbezogene Informationen zu Betriebssystemen, Anwendungsservern und Datenbanken, die in Ihre LiveCycle-Lösung integriert sind.

Verwenden Sie die angezeigten Links, um herstellerspezifische Sicherheitsinformationen zu Betriebssystem, Datenbank und Anwendungsserver zu suchen.

2.1.1 Informationen zur Betriebssystemsicherheit

Beim Schützen des Betriebssystems sollten Sie die Implementierung der vom Betriebssystemhersteller beschriebenen Sicherheitsmaßnahmen in Erwägung ziehen:

- Definieren und Steuern von Benutzern, Rollen und Berechtigungen
- Überwachen von Protokollen und Prüfspuren
- Entfernen unnötiger Dienste und Anwendungen
- Erstellen von Sicherungskopien der Dateien

Sicherheitsinformationen zu von LiveCycle unterstützten Betriebssystemen finden Sie in den nachfolgend aufgeführten Ressourcen.

Betriebssystem	**Sicherheitsressource**
IBM® AIX® 5.3 und 6.1	IBM AIX Security Benefits
Microsoft® Windows® XP SP 2 (nur für Nicht-Produktionsumgebungen)	Windows XP Security Guide
Microsoft Windows 7, 32-Bit und 64-Bit (nur für Nicht-Produktionsumgebungen)	Windows 7 Security Guide
Microsoft Windows Server® 2003 Enterprise oder Standard Edition	Suchen Sie nach „Windows Server 2003 Security Guide“ unter Microsoft.com
Microsoft Windows Server® 2008 Enterprise oder Standard Edition	Suchen Sie nach „Windows Server 2008 Security Guide“ unter Microsoft.com

Betriebssystem	Sicherheitsressource
Microsoft Vista™ SP1, alle Versionen, 32 Bit und 64 Bit (nur für Nicht-Produktionsumgebungen)	Suchen Sie nach „Windows Vista Security Guide“ unter Microsoft.com
Red Hat® Linux® AP oder ES	Red Hat Enterprise Linux Security Guide
Sun Solaris 10	System Administration Guide: Security Services

2.1.2 Informationen zur Sicherheit des Anwendungsservers

Beim Schützen des Anwendungsservers sollten Sie die Implementierung der vom Serverhersteller beschriebenen Sicherheitsmaßnahmen in Erwägung ziehen:

- Verwenden eines nicht offensichtlichen Benutzernamens für den Administrator
- Deaktivieren unnötiger Dienste
- Schützen des Konsolenmanagers
- Aktivieren sicherer Cookies
- Schließen nicht benötigter Anschlüsse
- Einschränken von Clients nach IP-Adressen oder Domänen
- Verwenden von Java™ Security Manager, um Berechtigungen programmgesteuert einzuschränken

Sicherheitsinformationen zu von LiveCycle unterstützten Anwendungsservern finden Sie in den nachfolgend aufgeführten Ressourcen.

Anwendungsserver	Sicherheitsressource
Oracle WebLogic®	Suchen Sie nach „Understanding WebLogic Security“ unter http://download.oracle.com/docs/.
IBM WebSphere®	Anwendungen und ihre Umgebung sichern
Red Hat® JBoss®	Sicherheit auf JBoss

2.1.3 Informationen zur Datenbanksicherheit

Beim Schützen der Datenbank sollten Sie die Implementierung der vom Datenbankhersteller beschriebenen Sicherheitsmaßnahmen in Erwägung ziehen:

- Einschränken der Vorgänge durch Zugriffssteuerungslisten
- Verwendung nicht standardmäßiger Anschlüsse
- Schützen der Datenbank durch eine Firewall
- Verschlüsseln sensibler Daten vor dem Schreiben in die Datenbank (siehe Dokumentation des Datenbankherstellers)

Sicherheitsinformationen zu von LiveCycle unterstützten Datenbanken finden Sie in den nachfolgend aufgeführten Ressourcen.

Datenbank	Sicherheitsressource
IBM DB2® 9.1 oder 9.5	DB2-Produktfamilienbibliothek
Microsoft SQL Server 2005 SP2 oder 2008	Suchen Sie im Web nch „SQL Server 2005: Sicherheit“ Suchen Sie im Web nach „SQL Server 2008: Sicherheit“
MySQL 5	MySQL 5.0 Allgemeine Sicherheitsprobleme MySQL 5.1 Allgemeine Sicherheitsprobleme
Oracle® 10g oder 11g	Weitere Informationen finden Sie im Kapitel „Sicherheit“ in der Oracle 11g-Dokumentation

In der folgenden Tabelle werden die Standardanschlüsse aufgeführt, die während des LiveCycle-Konfigurationsprozesses geöffnet sein müssen. Wenn Sie die Verbindung über HTTPS herstellen, passen Sie Ihre Anschlussinformationen und IP-Adressen entsprechend an. Weitere Informationen zum Konfigurieren von Anschlüssen finden Sie im Dokument *Installieren und Bereitstellen von LiveCycle* für Ihren Anwendungsserver.

Produkt oder Dienst	Anschlussnummer
JBoss	8080
WebLogic	7001
WebLogic Managed Server	Legt der Administrator während der Konfiguration fest
WebSphere	9060; wenn die globale Sicherheit aktiviert wurde, wird als standardmäßiger SSL-Anschluss der Anschluss 9043 verwendet. 9080
BAM-Server	7001
SOAP	8880
MySQL	3306
Oracle	1521
DB2	50000
SQL Server	1433
LDAP	Der Anschluss, an dem der LDAP-Server ausgeführt wird. Der Standardanschluss ist in der Regel 389. Wenn Sie jedoch die SSL-Option auswählen, ist der Standardanschluss in der Regel 636. Erkundigen Sie sich beim LDAP-Administrator, welchen Anschluss Sie angeben müssen.

2.1.4 JBoss zur Verwendung eines nicht standardmäßigen HTTP-Anschlusses konfigurieren

Der JBoss-Anwendungsserver verwendet 8080 als HTTP-Standardanschluss. JBoss verfügt außerdem über die vorkonfigurierten Anschlüsse 8180, 8280 und 8380, die in der Datei „jboss-service.xml“ auskommentiert sind. Wenn Sie auf Ihrem Computer über eine Anwendung verfügen, die bereits diesen Anschluss verwendet, ändern Sie den von LiveCycle verwendeten Anschluss, indem Sie die folgenden Schritte ausführen:

1 Öffnen Sie die Datei „jboss-service.xml“ in einem Editor.

Turnkey-Installation von JBoss: *[JBoss-Stammordner]*/server/lc_turnkey/conf/

Manuelle Installation von JBoss: *[Anwendungsserver-Stammordner]*/server/all/conf/

2 Suchen Sie den folgenden mbean-Text und heben Sie den Kommentar auf:

```
<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 Speichern und schließen Sie die Datei.

4 Starten Sie JBoss neu.

JBoss ist nun für die Verwendung des Anschlusses 8180 konfiguriert. Wenn Sie den Anschluss 8280 oder 8380 verwenden möchten, ändern Sie den Attributwert `ServerName`, um einen der folgenden alternativen Anschlüsse zu verwenden:

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

Wenn Sie eine andere Anschlussnummer als die für JBoss vorkonfigurierte konfigurieren möchten, führen Sie die folgenden Schritte aus:

1 Suchen und öffnen Sie die Datei „deploy/jboss-web.deployer“ im *[JBoss-Stammordner]* (Turnkey) oder *[Anwendungsserver-Stammordner]* (manuelle Installation von JBoss).

2 Suchen Sie den mbean-Text von Schritt 2 weiter oben und heben Sie den Kommentar auf.

3 Ändern Sie den Wert `ServerName` in die zu verwendende Anschlussnummer.

4 Speichern und schließen Sie die Datei.

5 Starten Sie JBoss neu.

2.2 Überlegungen zur Sicherheit von LiveCycle

In diesem Abschnitt werden einige LiveCycle-spezifische Sicherheitslücken beschrieben, deren Sie sich bewusst sein sollen.

2.2.1 Keine Verschlüsselung von E-Mail-Berechtigungen in der Datenbank

Die von LiveCycle-Anwendungen gespeicherten E-Mail-Berechtigungen werden nicht verschlüsselt, bevor sie in der LiveCycle-Datenbank gespeichert werden. Wenn Sie einen Dienstendpunkt für die Verwendung von E-Mail konfigurieren, werden Kennwortinformationen, die bei der Endpunktkonfiguration verwendet werden, beim Speichern in der Datenbank nicht verschlüsselt.

2.2.2 Sensibler Inhalt für Rights Management in der Datenbank

LiveCycle verwendet die LiveCycle-Datenbank, um sensible Informationen über Dokumentschlüssel und anderes Kryptografiematerial für Richtliniendokumente zu speichern. Wenn Sie die Datenbank gegen unberechtigten Zugriff schützen, erhöht dies den Schutz dieser sensiblen Informationen.

2.2.3 Kennwort in unverschlüsseltem Textformat in „adobe-ds.xml“

Der zum Ausführen von LiveCycle verwendete Anwendungsserver benötigt seine eigene Konfiguration, um über eine auf dem Anwendungsserver konfigurierte Datenquelle auf Ihre Datenbank zuzugreifen. Sie sollten sicherstellen, dass der Anwendungsserver Ihr Datenbankkennwort in seiner Datenquellenkonfigurationsdatei nicht in unverschlüsseltem Textformat offen legt.

Die Datei „adobe-ds.xml“ enthält Kennwörter in unverschlüsseltem Textformat. Fragen Sie beim Hersteller des Anwendungsservers nach, wie Sie diese Kennwörter für Ihren Anwendungsserver verschlüsseln sollen. Die JBoss®-Anleitungen finden sich beispielsweise in Encrypting DataSource Passwords.

Hinweis: *Das LiveCycle JBoss Turnkey-Installationsprogramm verschlüsselt das Datenbankkennwort.*

Bei IBM® WebSphere Application Server und Oracle WebLogic Server werden Datenquellenkennwörter eventuell standardmäßig verschlüsselt. Schlagen Sie vorsichtshalber in der Dokumentation zu Ihrem Anwendungsserver nach, um sicherzustellen, dass eine Verschlüsselung erfolgt.

Kapitel 3: Härten der Umgebung

In diesem Abschnitt werden Empfehlungen und Richtlinien für das Schützen von Servern beschrieben, auf denen LiveCycle ausgeführt wird. Dieses Dokument stellt keine umfassende Anleitung zum Härten (Absichern) des Hosts für das Betriebssystem und den Anwendungsserver dar. werden eine Reihe von Einstellungen für die Sicherheitshärtung beschrieben, die Sie implementieren sollten, um die Sicherheit von LiveCycle ES bei der Ausführung in einem firmeninternen Intranet zu verbessern. Um sicherzustellen, dass die LiveCycle-Anwendungsserver sicher bleiben, sollten Sie jedoch auch Verfahren für die Sicherheitsüberwachung, Problemerkennung und -behandlung implementieren.

In diesem Abschnitt werden Härtungsverfahren beschrieben, die in den folgenden Phasen des Installations- und Konfigurationszyklus durchgeführt werden sollten:

- **Vor der Installation:** Verwenden Sie diese Verfahren, bevor Sie LiveCycle installieren.
- **Installation:** Verwenden Sie diese Verfahren während der Installation der LiveCycle
- **Nach der Installation:** Verwenden Sie diese Verfahren nach der Installation in regelmäßigen Abständen.

LiveCycle kann in hohem Maß angepasst werden und in vielen verschiedenen Umgebungen eingesetzt werden. Einige der Empfehlungen entsprechen eventuell nicht den Anforderungen Ihrer Organisation.

3.1 Härtungsverfahren vor der Installation

Vor der Installation von LiveCycle können Sie Sicherheitslösungen auf die Netzwerkschicht und das Betriebssystem anwenden. In diesem Abschnitt finden Sie Beschreibungen zu einigen Sicherheitslücken sowie Empfehlungen dazu, wie Sie die Lücken in diesen Bereichen schließen können.

Installation und Konfiguration unter UNIX und Linux
Sie sollten LiveCycle nicht unter Verwendung einer Root Shell installieren oder konfigurieren. Standardmäßig werden alle Dateien im Ordner „/opt“ installiert. Der Benutzer, der die Installation durchführt, benötigt daher sämtliche Dateiberechtigungen für den Ordner „/opt“. Alternativ kann die Installation auch im Ordner „/user“ eines Einzelbenutzers durchgeführt werden, für das der Benutzer bereits über sämtliche Dateiberechtigungen verfügt.

Installation und Konfiguration unter Windows
Sie müssen die Installation unter Windows als Administrator durchführen, wenn Sie LiveCycle unter JBoss mit der Turnkey-Methode oder PDF Generator installieren. Wenn Sie PDF Generator unter Windows mit der Unterstützung nativer Anwendungen installieren, müssen Sie die Installation außerdem als der Windows-Benutzer durchführen, der Microsoft Office installiert hat. Weitere Informationen zu Installationsberechtigungen finden Sie im Dokument *Installieren und Bereitstellen von LiveCycle* für Ihren Anwendungsserver.

3.1.1 Sicherheit der Netzwerkschicht

Sicherheitslücken der Netzwerkschicht gehören zu den Hauptbedrohungen für Internet- oder Intranet-orientierte Anwendungsserver. In diesem Abschnitt wird der Prozess zum Absichern von Hostrechnern im Netzwerk gegen diese Schwachstellen beschrieben. Zu den behandelten Themen gehören die Netzwerksegmentierung, das Absichern des TCP/IP-Stacks (Transmission Control Protocol/Internet Protocol) und die Verwendung von Firewalls für den Hostschutz.

In der folgenden Tabelle werden gängige Prozesse beschrieben, die Schwachstellen der Netzwerksicherheit reduzieren.

Thema	Beschreibung
Demilitarisierte Zonen (DMZs)	Stellen Sie LiveCycle-Server innerhalb einer demilitarisierten Zone (DMZ) bereit. Die Segmentierung sollte in mindestens zwei Schichten bestehen, wobei sich der Anwendungsserver, auf dem LiveCycle ausgeführt wird, hinter der inneren Firewall befindet. Schirmen Sie das externe Netzwerk von der DMZ ab, die die Webserver enthält, und schirmen Sie die DMZ wiederum vom internen Netzwerk ab. Verwenden Sie Firewalls für die Implementierung der Abschirmungsebenen. Kategorisieren und Überwachen Sie den Netzwerkverkehr innerhalb der einzelnen Netzwerkschichten, um sicherzustellen, dass nur das absolute Minimum an erforderlichen Daten zulässig ist.
Private IP-Adressen	Verwenden Sie durch NAT (Network Address Translation) geschützte private IP-Adressen gemäß RFC 1918 auf LiveCycle-Anwendungsservern. Weisen Sie private IP-Adressen (10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16) zu, um es einem Angreifer zu erschweren, Netzwerkverkehr über das Internet zu und von einem internen Host mit NAT zu leiten.
Firewalls	Nutzen Sie die folgenden Kriterien für die Auswahl einer Firewall-Lösung: • Implementieren Sie Firewalls, die Proxy-Server und/oder die *statusbehaftete Inspektion* anstelle einfacher Paketfilterlösungen unterstützen. • Verwenden Sie eine Firewall, die *grundsätzlich jeden Netzwerkverkehr verbietet und nur die explizit zugelassenen Verbindungen erlaubt*. • Implementieren Sie eine Dual-Homed- oder Multi-Homed-Firewall-Lösung. Diese Architektur bietet das größte Maß an Sicherheit und trägt dazu bei, ein Umgehen des Firewall-Schutzes durch nicht berechtigte Benutzer zu verhindern.
Datenbankanschlüsse	Verwenden Sie keine standardmäßigen Listening-Anschlüsse für Datenbanken (MySQL - 3306, Oracle - 1521, MS SQL - 1433). Informationen zum Ändern von Datenbankanschlüssen finden Sie in der Datenbankdokumentation. Die Verwendung eines anderen Datenbankanschlusses wirkt sich auf die gesamte LiveCycle-Konfiguration aus. Wenn Sie die Standardanschlüsse ändern, müssen Sie auch in anderen Bereichen der Konfiguration entsprechende Änderungen durchführen, z. B. bei den Datenquellen für LiveCycle. Informationen zum Konfigurieren von Datenquellen in LiveCycle finden Sie in *Installieren undBereitstellen von LiveCycle* oder *Aktualisieren auf LiveCycle* für Ihren Anwendungsserver in der Dokumentation zu LiveCycle.

3.1.2 Betriebssystemsicherheit

In der folgenden Tabelle werden mögliche Ansätze zum Verringern von Sicherheitslücken im Betriebssystem beschrieben.

Thema	Beschreibung
Sicherheits-Patches	Wenn vom Hersteller bereitgestellte Sicherheits-Patches und -Aktualisierungen nicht zeitnah installiert werden, besteht ein erhöhtes Risiko, dass nicht autorisierte Benutzer Zugriff auf den Anwendungsserver erlangen. Testen Sie Sicherheits-Patches, bevor Sie sie auf Produktionsserver anwenden. Erstellen Sie zudem Richtlinien und Prozeduren, damit Patches regelmäßig gesucht und installiert werden.
Virenschutzsoftware	Virenscanner können infizierte Dateien erkennen, indem sie nach einer Signatur suchen oder ungewöhnliches Verhalten ermitteln. Virenscanner speichern die Virussignaturen in einer Datei, die in der Regel auf der lokalen Festplatte abgelegt wird. Da häufig neue Viren entdeckt werden, sollten Sie diese Datei häufig aktualisieren, damit der Virenscanner alle aktuellen Viren erkennt.
NTP (Network Time Protocol)	Für die forensische Analyse ist erforderlich, dass die Uhrzeit auf LiveCycle-Servern exakt ist. Verwenden Sie NTP, um die Uhrzeit auf allen Systemen zu synchronisieren, die direkt mit dem Internet verbunden sind.

Weitere Informationen zur Sicherheit für Ihr Betriebssystem finden Sie unter „2.1.1 Informationen zur Betriebssystemsicherheit“ auf Seite 3.

3.2 Installation

In diesem Abschnitt werden Verfahren beschrieben, die Sie während des LiveCycle-Installationsprozesses verwenden können, um Sicherheitslücken zu schließen. In einigen Fällen nutzen diese Verfahren Optionen, die Teil des Installationsprozesses sind. Diese Verfahren werden in der folgenden Tabelle beschrieben.

Thema	Beschreibung
Berechtigungen	Verwenden Sie Mindestanzahl an Berechtigungen, die für die Installation der Software erforderlich sind. Melden Sie sich über ein Benutzerkonto, das nicht zur Gruppe „Administratoren“ gehört, bei Ihrem Computer an. Unter Windows können Sie den Befehl „Ausführen als“ verwenden, um das LiveCycle-Installationsprogramm als Benutzer mit Administratorrechten auszuführen. Auf UNIX- und Linux-Systemen verwenden Sie einen Befehl wie `sudo` für die Installation der Software.
Ursprung der Software	Verwenden Sie zum Herunterladen oder Ausführen von LiveCycle keine nicht vertrauenswürdigen Quellen. Bösartige Programme können Code enthalten, der die Sicherheit auf verschiedene Weise verletzt, etwa durch Diebstahl, Ändern und Löschen von Daten sowie Dienstblockade (Denial of Service = DoS). Installieren Sie LiveCycle ausschließlich von der Adobe-DVD oder einer vertrauenswürdigen Quelle.
Festplattenpartitionen	Installieren Sie LiveCycle auf einer dedizierten Festplattenpartition. Die Festplattenaufteilung ist ein Prozess, bei dem bestimmte Daten auf dem Server auf separaten physischen Festplatten verwaltet werden, um die Sicherheit zu erhöhen. Durch eine solche Datenanordnung lässt sich das Risiko von Directory Traversal-Angriffen verringern. Planen Sie die Erstellung einer von der Systempartition getrennten Partition, auf der Sie das LiveCycle-Inhaltsverzeichnis installieren können. (Unter Windows enthält die Systempartition den Ordner „system32“, das auch als Boot-Partition bezeichnet wird.)

Thema	Beschreibung
Komponenten	Prüfen Sie die vorhandenen Dienste und deaktivieren oder deinstallieren Sie nicht erforderliche Dienste. Installieren Sie keine unnötigen Komponenten und Dienste. Die Standardinstallation eines Anwendungsservers kann Dienste beinhalten, die Sie nicht benötigen. Sie sollten alle unnötigen Dienste vor der Bereitstellung deaktivieren, um die Einstiegspunkte für Angriffe zu minimieren. Unter JBoss können Sie beispielsweise nicht benötigte Dienste in der Deskriptordatei „META-INF/jboss-service.xml“ durch das Einfügen von Kommentarzeichen deaktivieren.
Domänenübergreifende Richtliniendatei	Das Vorhandensein einer Datei`crossdomain.xml` auf dem Server kann diesen Server unmittelbar schwächen. Es wird empfohlen, die Liste der Domänen so weit wie möglich einzuschränken. Platzieren Sie die während der Entwicklungsphase verwendete `crossdomain.xml`-Datei nicht in der Produktionsumgebung, wenn Sie Guides verwenden *(nicht mehr unterstützt)*. Bei einem Guide, der Webdienste verwendet, wird keine `crossdomain.xml`-Datei benötigt, wenn sich der Dienst auf demselben Server befindet wie der Server, der den Guide zur Verfügung gestellt hat. Wenn es sich jedoch um einen anderen Dienst handelt oder wenn Cluster betroffen sind, muss eine `crossdomain.xml`-Datei vorhanden sein. Weitere Informationen zur Datei „crossdomain.xml“ finden Sie unter http://kb2.adobe.com/de/cps/142/tn_14213.html.
Sicherheitseinstellungen des Betriebssystems	Wenn Sie 192-Bit- oder 256-Bit-XML-Verschlüsselung auf Solaris-Plattformen verwenden müssen, sollten Sie sicherstellen, dass Sie `pkcs11_softtoken_extra.so` anstelle von `pkcs11_softtoken.so` installieren.

3.3 Schritte nach der Installation

Nachdem Sie LiveCycle erfolgreich installiert haben, sollten Sie die Sicherheitseinrichtungen der Umgebung unbedingt in regelmäßigen Abständen warten.

Im folgenden Abschnitt werden die verschiedenen Aufgaben, die zum Schützen des bereitgestellten LiveCycle-Servers empfohlen werden, detailliert beschrieben.

3.3.1 Sicherheit von LiveCycle-Server

Die folgenden, empfohlenen Einstellungen gelten für den LiveCycle-Server außerhalb der Verwaltungs-Webanwendung. Um die Sicherheitsrisiken für den Server zu verringern, wenden Sie diese Einstellungen unmittelbar nach der Installation von LiveCycle an.

Sicherheits-Patches

Wenn vom Hersteller bereitgestellte Sicherheits-Patches und -Aktualisierungen nicht zeitnah installiert werden, besteht ein erhöhtes Risiko, dass nicht autorisierte Benutzer Zugriff auf den Anwendungsserver erlangen. Testen Sie Sicherheits-Patches, bevor Sie sie auf Produktionsserver anwenden, um die Kompatibilität und Verfügbarkeit von LiveCycle-Anwendungen sicherzustellen. Erstellen Sie zudem Richtlinien und Prozeduren, damit Patches regelmäßig gesucht und installiert werden. LiveCycle-Aktualisierungen finden Sie auf der Site „Enterprise Products – Support Download“.

Dienstkonten (nur JBoss-Turnkey unter Windows)

LiveCycle installiert standardmäßig einen Dienst unter Verwendung des Kontos „Lokales System“. Das integrierte Benutzerkonto „Lokales System“ hat hohe Zugriffsrechte; es gehört zur Gruppe „Administratoren“. Wenn eine Worker Process-ID als das Benutzerkonto „Lokales System“ ausgeführt wird, hat dieser Worker Process vollen Zugriff auf das gesamte System.

Um den Anwendungsserver, auf dem LiveCycle bereitgestellt wird, mit einem bestimmten Konto ohne Administratorrechte auszuführen, führen Sie die folgenden Anweisungen aus:

1 Erstellen Sie in der Microsoft Management Console (MMC) einen lokalen Benutzer für den LiveCycle-Serverdienst, der für die Anmeldung verwendet werden soll:
   - Wählen Sie **Benutzer kann Kennwort nicht ändern aus**.
   - Stellen Sie sicher, dass auf der Registerkarte **Mitglied von** die Gruppe **Benutzer** aufgelistet wird.

   Hinweis: *Sie können diesen Wert für PDF Generator nicht ändern.*

2 Wählen Sie **Start** > **Einstellungen** > **Verwaltung** > **Dienste** aus.

3 Doppelklicken Sie auf „JBoss for Adobe LiveCycle 10“ und stoppen Sie den Dienst.

4 Wählen Sie auf der Registerkarte **Anmelden** die Option **Dieses Konto** aus, suchen Sie das Benutzerkonto, das Sie erstellt haben, und geben Sie das Kennwort für das Konto ein.

5 Öffnen Sie in MMC die **Lokale Sicherheitseinstellungen** und wählen Sie **Lokale Richtlinien** > **Zuweisen von Benutzerrechten** aus.

6 Weisen Sie dem Benutzerkonto, unter dem der LiveCycle-Server ausgeführt wird, die folgenden Rechte zu:
   - Anmeldung über Terminaldienste verweigern
   - Lokale Anmeldung verweigern
   - Als Dienst anmelden (sollte bereits festgelegt sein)

7 Weisen Sie dem neuen Benutzerkonto die Berechtigungen „Lesen und Ausführen“, „Ordnerinhalt auflisten“ und „Lesen“ für das Element mit LiveCycle-Webinhaltverzeichnissen zu.

8 Starten Sie den Anwendungsserver.

Bootstrap-Servlet von Configuration Manager deaktivieren

Configuration Manager verwendete ein auf Ihrem Anwendungsserver bereitgestelltes Servlet, um das Bootstrapping der LiveCycle-Datenbank durchzuführen. Da Configuration Manager vor Abschluss der Konfiguration auf dieses Servlet zugreift, wurde der Zugriff darauf für autorisierte Benutzer noch nicht gesichert, weshalb das Servlet deaktiviert werden sollte, nachdem Sie Configuration Manager erfolgreich für die Konfiguration von LiveCycle verwendet haben.

1 Dekomprimieren Sie die Datei „adobe-livecycle-[Anwendungsserver].ear“.

2 Öffnen Sie die Datei „META-INF/application.xml“.

3 Suchen Sie den Abschnitt „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 Deaktivieren Sie die Module „adobe-bootstrapper.war“ und „adobe-lcm-bootstrapper-redirector.war“ wie folgt durch Kommentarzeichen:

```
<!-- 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 Speichern und schließen Sie die Datei „META-INF/application.xml“.

6 Komprimieren Sie die EAR-Datei und stellen Sie sie erneut auf dem Anwendungsserver bereit.

7 Testen Sie die Änderung, indem Sie die URL in einen Browser eingeben und sicherstellen, dass sie nicht mehr funktioniert.

Remote-Zugriff auf den Trust Store sperren

Configuration Manager ermöglicht Ihnen, eine Berechtigung für Reader Extensions 10 in den LiveCycle Trust Store hochzuladen. Das bedeutet, dass der Zugriff auf den Trust Store-Berechtigungsdienst über Remote-Protokolle (SOAP und EJB) standardmäßig aktiviert wurde. Dieser Zugriff ist nicht mehr notwendig, nachdem Sie die Berechtigung für Rechte mit Configuration Manager hochgeladen haben oder beschließen, Berechtigungen später mit Administration Console zu verwalten.

Sie können den Remote-Zugriff auf sämtliche Trust Store-Dienste deaktivieren, indem Sie die im Abschnitt „4.1 Nicht erforderlichen Remote-Zugriff auf Dienste deaktivieren“ auf Seite 38 beschriebenen Schritte durchführen.

Den gesamten, nicht erforderlichen anonymen Zugriff deaktivieren

Bei einigen LiveCycle-Serverdiensten gibt es Vorgänge, die von einem anonymen Aufrufer aufgerufen werden können. Ist der anonyme Zugriff auf diese Dienste nicht erforderlich, deaktivieren Sie ihn gemäß den Schritten in „4.2 Nicht erforderlichen anonymem Zugriff auf Dienste deaktivieren“ auf Seite 39.

3.3.1.1 Standardkennwort für das Administratorkonto ändern

Beim Installieren von LiveCycle wird ein Standardbenutzerkonto für den Benutzer „Superadministrator“ mit der Anmelde-ID „Administrator“ und dem Standardkennwort *password* erstellt. Sie sollten dieses Kennwort umgehend mithilfe von Configuration Manager ändern.

1 Geben Sie in einem Webbrowser die folgende URL ein:

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

Der Standardanschluss lautet wie folgt:

JBoss: 8080

WebLogic Server: 7001

WebSphere: 9080.

2 Geben Sie in das Feld **Benutzername** den Wert `administrator` und in das Feld **Kennwort** den Wert `password` ein.

3 Klicken Sie auf **Einstellungen** > **User Management** > **Benutzer und Gruppen**.

4 Geben Sie den Begriff `administrator` in das Feld **Suchen** ein und klicken Sie auf **Suchen**.

5 Klicken Sie in der Liste der Benutzer auf **Super Administrator**.

6 Klicken Sie auf der Seite „Benutzer bearbeiten“ auf **Kennwort ändern**.

7 Geben Sie das neue Kennwort an und klicken Sie auf **Speichern**.

3.3.1.2 WSDL-Generierung deaktivieren

Die WSDL-Generierung (Web Service Definition Language) sollte nur in Entwicklungsumgebungen aktiviert sein, in denen Entwickler mithilfe der WSDL-Generierung Clientanwendungen erstellen. In einer Produktionsumgebung können Sie die WSDL-Generierung deaktivieren, um zu verhindern, dass interne Details eines Dienstes preisgegeben werden.

1 Geben Sie in einem Webbrowser die folgende URL ein:

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

2 Klicken Sie auf **Einstellungen > Core-Systemeinstellungen > Konfigurationen**.

3 Deaktivieren Sie **WSDL aktivieren** und klicken Sie auf **OK**.

3.3.1.3 Benutzerdaten-Eincheckquoten in LiveCycle Content Services (nicht mehr unterstützt) einschränken

Hinweis: *Adobe migriert Kunden, die Adobe® LiveCycle® Content Services ES verwenden, zu Inhalts-Repository, das basierend auf der modernen, modularen CRX-Architektur erstellt wurde, die durch die Übernahme von Day Software durch Adobe erhalten wurde. Das Inhalts-Repository wird mit LiveCycle Foundation bereitgestellt und ist als Teil der LiveCycle ES3-Version verfügbar.*

Standardmäßig schränkt Content Services nicht die Datenmenge ein, die ein Benutzer zu einem bestimmten Zeitpunkt beim Server einchecken. Große Datenmengen sind eine potenzielle Bedrohung für das System, da sie dem System die Ressourcen, andere Vorgänge auszuführen, nehmen. Diese Situation kann zu einer Dienstblockade für andere eingehende Prozesse führen. Verwenden Sie JVM-Argumente, um die Quotenverwaltung in Content Services zu aktivieren.

Wichtig: *Diese JVM-Argumente müssen vor der Synchronisierung der Benutzer weitergeleitet werden. Nachdem die Benutzer synchronisiert wurden, können diese Benutzerquoten nicht mehr geändert werden.*

3.3.1.3.1 Quotenverwaltung in Content Services aktivieren

Für JBoss

1 Wechseln Sie zum Ordner „*[JBoss-Stammordner]*/bin“ und öffnen Sie das Startskript in einem Texteditor:

- **(Windows)** run.bat

- **(Linux und UNIX)** run.sh

2 Fügen Sie die folgenden Eigenschaften unter dem `Set JAVA_OPTS`-Argument hinzu:

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

3 Speichern und schließen Sie die Datei.

4 Starten Sie den JBoss-Server vor der Synchronisierung der Benutzer neu.

Für WebLogic

1 Starten Sie die WebLogic Server Administration Console, indem Sie in die Adresszeile eines Browsers „http://*[Hostname]*:*[Anschluss]*/console“ eingeben. *[Anschluss]* ist der nicht sichere Überwachungsanschluss. Der Standardwert dieses Anschlusses ist 7001.

2 Geben Sie auf dem Anmeldebildschirm Ihren WebLogic-Benutzernamen und Ihr Kennwort ein und klicken Sie auf **Log In**.

3 Klicken Sie unter „Change Center“ auf **Lock & Edit**.

4 Klicken Sie unter „Domain Structure“ auf **Environment** > **Servers** und klicken Sie dann im rechten Bereich auf den Namen des verwalteten Servers.

5 Klicken Sie im Bereich „Settings for Server“ auf die **RegisterkartenConfiguration** > **Server Start**.

6 Fügen Sie im Feld „Arguments“ die folgenden Argumente, durch ein Leerzeichen getrennt, hinzu:

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

7 Klicken Sie auf **Save** und dann auf **Activate Changes**.

8 Starten Sie den WebLogic-Server vor der Synchronisierung der Benutzer neu.

Für WebSphere

1 Führen Sie in WebSphere Administration Console die folgende Aufgabe für Ihren Anwendungsserver aus:

(WebSphere 6.x) Klicken Sie auf **Servers** > **Application servers**.

(WebSphere 7.x) Klicken Sie auf **Servers** > **ServerTypes** > **WebSphere Application Servers**.

2 Klicken Sie im rechten Bereich auf den Namen des Servers.

3 Klicken Sie unter „Server Infrastructure“ auf **Java and Process Management** > **Process Definition**.

4 Klicken Sie unter „Additional Properties“ auf **Java Virtual Machine**.

5 Fügen Sie im Feld **Generic JVM arguments** die Argumente `-Dsystem.usages.enableQuotaSize=true` und `-Dsystem.usages.quota=`<*Größe in KB*>, durch Kommas getrennt, den vorhandenen Eigenschaften hinzu.

6 Klicken Sie auf **OK** oder **Apply** und klicken Sie dann auf **Save directly to Master Configuration**.

7 Starten Sie den WebSphere-Server vor der Synchronisierung der Benutzer neu.

3.3.2 Sicherheit des Anwendungsservers

In der folgenden Tabelle werden einige Verfahren zum Schützen des Anwendungsservers nach der Installation der LiveCycle-Anwendung beschrieben.

Thema	Beschreibung
Verwaltungskonsole des Anwendungsservers	Nach der Installation, Konfiguration und Bereitstellung von LiveCycle auf dem Anwendungsserver müssen Sie den Zugriff auf die Verwaltungskonsolen des Anwendungsservers deaktivieren. Detaillierte Informationen hierzu finden Sie in der Dokumentation zu Ihrem jeweiligen Anwendungsserver.
Cookie-Einstellungen des Anwendungsservers	Anwendungs-Cookies werden vom Anwendungsserver gesteuert. Beim Bereitstellen der Anwendung kann der Administrator des Anwendungsservers Cookie-Voreinstellungen serverweit oder anwendungsspezifisch festlegen. Standardmäßig haben die Servereinstellungen Vorrang. Alle vom Anwendungsserver erstellten Sitzungs-Cookies müssen das `HttpOnly`-Attribut enthalten. Bei Verwendung des JBoss-Anwendungsservers können Sie beispielsweise das Element „SessionCookie“ in der Datei `deploy/jbossweb.sar/context.xml` in `httpOnly="true"` ändern. Sie können festlegen, dass Cookies ausschließlich unter Verwendung von HTTPS gesendet werden. Dadurch wird verhindert, dass Cookies unverschlüsselt über HTTP gesendet werden. Anwendungsserveradministratoren sollten sichere Cookies für den Server global aktivieren. Bei Verwendung des JBoss-Anwendungsservers können Sie beispielsweise das Element „connector“ in der Datei `server.xml` in `secure=true` ändern. Ausführlichere Informationen zu Cookie-Einstellungen finden Sie in der Dokumentation zum Anwendungsserver.
Directory Browsing	Wenn eine Person eine nicht vorhandene Seite oder den Namen eines Ordners anfordert (die Anforderungszeichenfolge endet in diesem Fall mit einem Schrägstrich (/)), sollte der Anwendungsserver den Inhalt dieses Ordners nicht zurückgeben. Damit dies nicht geschieht, können Sie das Directory Browsing auf Ihrem Anwendungsserver deaktivieren. Sie sollten dies für die Administration Console-Anwendung und andere auf dem Server laufende Anwendungen tun. Für JBoss stellen Sie in der Datei „web.xml“ den Wert des Auflistungsinitialisierungsparameters der Eigenschaft `DefaultServlet` auf `false` ein, wie im folgenden Beispiel gezeigt wird: <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> Für WebSphere stellen Sie in der Datei „ibm-web-ext.xml“ die Eigenschaft `directoryBrowsingEnabled` auf `false` ein. Für WebLogic stellen Sie in der Datei „weblogic.xml“ die Eigenschaften zu „index-directories“ auf `false` ein, wie im folgenden Beispiel gezeigt: <container-descriptor> <index-directory-enabled>false </index-directory-enabled> </container-descriptor>

3.3.3 JMX-Console unter JBoss verwenden

Wenn die Java Management Extensions-Konsole (JMX) unter JBoss installiert ist, können URLs für die Verwendung als XSS-Exploits (Cross-Site Scripting) erzeugt werden, die vertrauliche Informationen über Ihr System offenlegen können.

Wenn Sie LiveCycle mit der Turnkey-Methode installiert haben und die Version von JBoss verwenden, die Teil der Turnkey-Installation war, wird die JBoss JMX-Konsole standardmäßig entfernt, um die Sicherheitsrisiken zu verringern. Wenn Sie die JBoss JMX-Konsole jedoch benötigen, installieren Sie sie anhand dieses Verfahrens erneut.

1. Laden Sie eine Kopie von JBoss 4.2.0 (oder höher) von JBoss.org herunter.
2. JBoss-Anwendungsserver beenden.
3. Extrahieren Sie aus der heruntergeladenen, komprimierten Archivdatei die Dateien aus dem Ordner „*[JBoss-Stammordner]*/deploy/jmx-console.war/“.
4. Legen Sie die Dateien „jmx-console.war/...“ im Bereitstellungsordner des JBoss-Installationsordners ab.
5. Starten Sie JBoss neu.
6. Wechseln Sie zur folgenden URL, um sicherzustellen, dass die JBoss JMX-Konsole zur Verfügung steht:

   http://localhost:8080/jmx-console

3.3.4 Datenbanksicherheit

Beim Schützen der Datenbank sollten Sie die vom Datenbankhersteller beschriebenen Sicherheitsmaßnahmen implementieren. Sie sollten einem Datenbankbenutzer die minimal für die Verwendung von LiveCycle erforderlichen Datenbankberechtigungen zuweisen. Verwenden Sie z. B. kein Konto mit Datenbankadministrator-Berechtigungen.

Unter Oracle benötigt das verwendete Datenbankkonto nur die Berechtigungen CONNECT, RESOURCE und CREATE VIEW. Weitere Informationen zu anderen Datenbanken finden Sie unter Installation von LiveCycle vorbereiten (Einzelserver).

3.3.4.1 Integrierte Sicherheit für SQL Server unter Windows für JBoss konfigurieren

1. Ändern Sie „*[JBOSS_HOME]*\server\all\deploy\adobe-ds.xml“, indem Sie `integratedSecurity=true` zur Verbindungs-URL hinzufügen, wie im folgenden Beispiel gezeigt:

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

2. Fügen Sie die Datei „sqljdbc_auth.dll“ zum Windows-Systempfad (C:\Windows) auf dem Computer hinzu, auf dem der Anwendungsserver ausgeführt wird. Die Datei „sqljdbc_auth.dll“ befindet sich bei der Microsoft SQL JDBC 1.2-Treiberinstallation (standardmäßig unter *[InstallDir]*/sqljdbc_1.2/enu/auth/x86).
3. Ändern Sie die Eigenschaft des JBoss Windows-Dienstes (JBoss for LiveCycle) für „Anmelden als“ von „Lokales System“ in ein Anmeldekonto mit einer LiveCycle-Datenbank und einem Mindestsatz von Berechtigungen. Wenn Sie JBoss von der Befehlszeile und nicht als Windows-Dienst ausführen, ist dieser Schritt nicht erforderlich.
4. Ändern Sie die Sicherheitseinstellung von SQL Server von **Gemischt** in **Nur Windows-Authentifizierung**.

3.3.4.2 Integrierte Sicherheit für SQL Server unter Windows für WebLogic konfigurieren

1. Starten Sie WebLogic Server Administration Console, indem Sie die folgende URL in die Adresszeile eines Webbrowsers eingeben:

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

2. Klicken Sie unter „Change Center“ auf **Lock & Edit**.

3 Klicken Sie unter „Domain Structure“ auf *[base_domain]*> **Services** > **JDBC** > **Data Sources** und klicken Sie dann im rechten Bereich auf **IDP_DS**.

4 Klicken Sie im nächsten Bildschirm auf die Registerkarte **Configuration** und dann auf die Registerkarte **ConnectionPool**. Geben Sie in das Feld **Properties** den Eintrag `integratedSecurity=true` ein.

5 Klicken Sie unter „Domain Structure“ auf **[base_domain]** > **Services** > **JDBC** > **Data Sources** und klicken Sie dann im rechten Bereich auf **RM_DS**.

6 Klicken Sie im nächsten Bildschirm auf die Registerkarte **Configuration** und dann auf die Registerkarte **Connection Pool**. Geben Sie in das Feld **Properties** den Eintrag `integratedSecurity=true` ein.

7 Fügen Sie die Datei „sqljdbc_auth.dll“ zum Windows-Systempfad (C:\Windows) auf dem Computer hinzu, auf dem der Anwendungsserver ausgeführt wird. Die Datei „sqljdbc_auth.dll“ befindet sich bei der Microsoft SQL JDBC 1.2-Treiberinstallation (standardmäßig unter *[InstallDir]*/sqljdbc_1.2/enu/auth/x86).

8 Ändern Sie die Sicherheitseinstellung von SQL Server von **Gemischt** in **Nur Windows-Authentifizierung**.

3.3.4.3 Integrierte Sicherheit für SQL Server unter Windows für WebSphere konfigurieren

Unter WebSphere können Sie die integrierte Sicherheit nur konfigurieren, wenn Sie einen externen JDBC-Treiber für SQL Server und nicht den in WebSphere eingebetteten JDBC-Treiber für SQL Server verwenden.

1 Melden Sie sich bei WebSphere Administrative Console an.

2 Klicken Sie in der Navigationsstruktur auf **Resources** > **JDBC** > **Data Sources** und klicken Sie dann im rechten Bereich auf **IDP_DS**.

3 Klicken Sie im rechten Bereich unter „Additional Properties“ auf **Custom Properties** und dann auf **New**.

4 Geben Sie in das Feld **Name** die Bezeichnung `integratedSecurity` und in das Feld **Value** den Wert `true` ein.

5 Klicken Sie in der Navigationsstruktur auf **Resources** > **JDBC** > **Data Sources** und klicken Sie dann im rechten Bereich auf **RM_DS**.

6 Klicken Sie im rechten Bereich unter „Additional Properties“ auf **Custom Properties** und dann auf **New**.

7 Geben Sie in das Feld **Name** die Bezeichnung `integratedSecurity` und in das Feld **Value** den Wert `true` ein.

8 Fügen Sie auf dem Computer, auf dem WebSphere installiert ist, die Datei „sqljdbc_auth.dll“ dem Windows-Systempfad (C:\Windows) hinzu. Die Datei „sqljdbc_auth.dll“ befindet sich am selben Speicherort wie die Microsoft SQL JDBC 1.2-Treiberinstallation (standardmäßig unter *[Installationsordner]*/sqljdbc_1.2/enu/auth/x86).

9 Wählen Sie **Start** > **Systemsteuerung** > **Dienste** aus, klicken Sie mit der rechten Maustaste auf den Windows-Dienst für WebSphere (IBM WebSphere Application Server <Version> - <Knoten>) und wählen Sie **Eigenschaften** aus.

10 Klicken Sie im Dialogfeld „Eigenschaften“ auf die Registerkarte **Anmelden**.

11 Wählen Sie **Dieses Konto** aus und geben Sie die benötigten Informationen ein, um das gewünschte Anmeldekonto festzulegen.

12 Ändern Sie die Sicherheitseinstellung von SQL Server von **Gemischt** in **Nur Windows-Authentifizierung**.

3.3.5 Sensible Inhalte in der Datenbank schützen

Das LiveCycle-Datenbankschema enthält sensible Informationen über die Systemkonfiguration und Geschäftsprozesse und sollte hinter der Firewall geschützt sein. Für die Datenbank sollte dieselbe Sicherheitsstufe wie für den LiveCycle-Server gelten. Um die Offenlegung von Informationen und den Diebstahl von Geschäftsdaten zu verhindern, muss die Datenbank vom DBA (Datenbankadministrator) so konfiguriert werden, dass nur autorisierte Administratoren Zugriff haben.

Als zusätzliche Sicherheitsmaßnahme sollten Sie überlegen, spezifische Werkzeuge des Datenbankherstellers für die Verschlüsselung von Spalten in Tabellen zu verwenden, die folgende Daten enthalten:

- Rights Management-Dokumentschlüssel
- PIN-Verschlüsselungsschlüssel für HSM-Geräte im Trust Store
- Hashes für lokale Benutzerkennwörter

Informationen zu herstellerspezifischen Werkzeugen finden Sie unter „2.1.3 Informationen zur Datenbanksicherheit“ auf Seite 4 .

3.3.6 LDAP-Sicherheit

LiveCycle nutzt meist einen LDAP-Ordner (Lightweight Directory Access Protocol) als Quelle für Informationen über Unternehmensbenutzer und Gruppen sowie zur Durchführung der Kennwortauthentifizierung. Sie sollten sicherstellen, dass Ihr LDAP-Ordner für die Verwendung von Secure Socket Layer (SSL) konfiguriert ist und LiveCycle für den Zugriff auf den LDAP-Ordner über dessen SSL-Anschluss konfiguriert ist.

3.3.6.1 LDAP-Dienstblockade

Angriffe mittels LDAP bestehen häufig darin, dass ein Angreifer die Authentifizierung bewusst mehrmals fehlschlagen lässt. Dies zwingt den LDAP-Ordnerserver dazu, einen Benutzer für alle auf LDAP basierenden Dienste zu sperren.

Sie können die Anzahl fehlgeschlagener Versuche sowie die nachfolgende Sperrdauer festlegen, die LiveCycle implementiert, wenn die LiveCycle-Authentifizierung eines Benutzers wiederholt fehlschlägt. Wählen Sie in Administration Console niedrige Werte. Bei der Auswahl der Anzahl von Fehlversuchen ist wichtig, dass Sie sich bewusst sind, dass der Benutzer nach Durchführung aller Versuche von LiveCycle ES gesperrt wird, bevor dies durch den LDAP-Ordnerserver erfolgt.

3.3.6.2 Automatische Kontosperrung festlegen

1. Melden Sie sich bei Administration Console an.
2. Klicken Sie auf **Einstellungen** > **User Management** > **Domänenverwaltung**.
3. Stellen Sie unter „Einstellungen für die automatische Kontosperrung“ für **Maximale Anzahl aufeinander folgender Authentifizierungsfehler** einen niedrigen Wert, wie etwa 3 ein.
4. Klicken Sie auf **Speichern**.

3.3.7 Prüfung und Protokollierung

Der richtige und sichere Einsatz der Anwendungsprüfung und -protokollierung kann dazu beitragen, dass sicherheitsrelevante und andere, unnormale Ereignisse schnellstmöglich verfolgt und erkannt werden. Die effektive Verwendung der Prüfung und Protokollierung innerhalb einer Anwendung beinhaltet Aspekte wie das Verfolgen erfolgreicher und fehlgeschlagener Anmeldungen sowie Schlüsselereignisse der Anwendung wie das Erstellen oder Löschen von Schlüsseldatensätzen.

Mithilfe der Prüfung lassen sich viele Arten von Angriffen feststellen wie z. B.:

- Brute-Force-Kennwortangriffe
- DoS-Angriffe (Denial of Service)
- Einschleusen schädlicher Daten und ähnliche Scripting-Angriffe

In der folgenden Tabelle werden Prüfungs- und Protokollierungsverfahren beschrieben, mit denen Sie die Anfälligkeit des Servers verringern können.

Thema	Beschreibung
Zugriffssteuerungslisten für Protokolldateien	Legen Sie geeignete Zugriffssteuerungslisten für LiveCycle-Protokolldateien fest. Das Festlegen entsprechender Berechtigungen verhindert, dass Angreifer die Dateien löschen. Als Sicherheitsberechtigung für das Protokolldateiordner sollte „Alle Berechtigungen“ für Administratoren und SYSTEM-Gruppen festgelegt werden. Das LiveCycle-Benutzerkonto sollte nur lese- und schreibberechtigt sein.
Redundanz der Protokolldateien	Falls es die Ressourcen erlauben, senden Sie Protokolle mit Syslog, Tivoli, Microsoft Operations Manager (MOM) Server oder einem anderen Mechanismus in Echtzeit an einen anderen Server, auf den Angreifer nicht zugreifen können (schreibgeschützt). Wenn Sie Protokolle auf diese Weise schützen, erschweren Sie damit mögliche Manipulationen. Das Speichern von Protokollen in einem zentralen Repository erleichtert zudem die Korrelation und Überwachung (wenn beispielsweise mehrere LiveCycle-Server verwendet werden und ein Password Guessing-Angriff auf mehrere Computer erfolgt, bei dem von jedem Computer ein Kennwort abgefragt wird).

3.3.8 LiveCycle-Abhängigkeiten von der Unix-Systembibliothek

Die folgenden Informationen sollen Ihnen bei der Planung einer LiveCycle-Bereitstellung in einer UNIX-Umgebung helfen.

3.3.8.1 Convert PDF-Dienst

Für den Convert PDF-Dienst, der Bestandteil von LiveCycle ist, stellen die folgenden Systembibliotheken die Mindestanforderung dar:

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

Für XMLForms stellen die folgenden Systembibliotheken die Mindestanforderung dar:

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

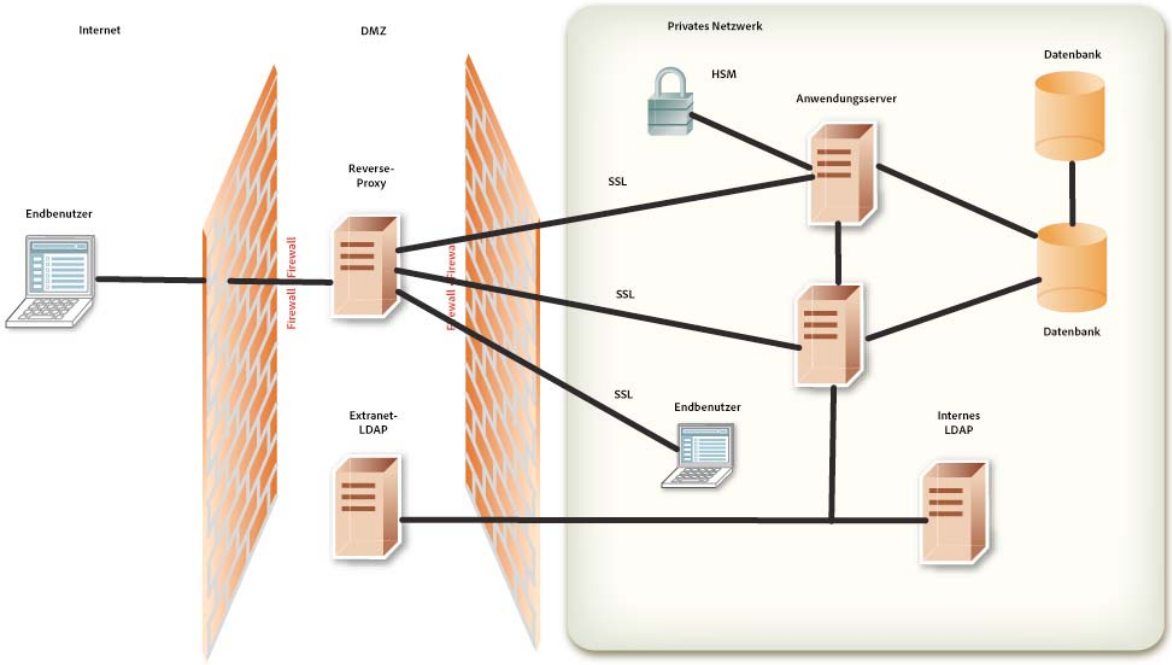
```
/usr/lib/
    libpthread.a(shr_comm.o)
    libpthread.a(shr_xpg5.o)
    libc.a(shr.o)
    librtl.a(shr.o)
    libdl.a(shr.o)
    libX11.a(shr4.o)
    libiconv.a(shr4.o)
    libpthreads.a(shr_comm.o)
/unix
    /usr/lib/libcrypt.a(shr.o)
    /usr/lib/libIM.a(shr.o)
    /usr/lib/libpthreads.a(shr_xpg5.o)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

3.4 LiveCycle für den externen Zugriff konfigurieren

Nachdem Sie LiveCycle erfolgreich installiert haben, müssen Sie die Sicherheitseinrichtungen der Umgebung unbedingt in regelmäßigen Abständen warten. In diesem Abschnitt werden die empfohlenen Aufgaben für die Sicherheitswartung des LiveCycle-Produktionsservers beschrieben.

3.4.1 Reverse-Proxys für den Webzugriff einrichten

Sie können einen *Reverse-Proxy* verwenden, um sicherzustellen, dass eine Gruppe von URLs für LiveCycle-Webanwendungen sowohl für externe als auch interne Benutzer verfügbar ist. Diese Konfiguration bietet mehr Sicherheit als die Erlaubnis für Benutzer, eine direkte Verbindung zu dem Anwendungsserver herzustellen, auf dem LiveCycle ausgeführt wird. Der Reverse-Proxy führt alle HTTP-Anfragen für den Anwendungsserver durch, auf dem LiveCycle läuft. Benutzer haben nur Netzwerkzugriff auf den Reverse-Proxy und können nur URL-Verbindungen aufbauen, die der Reverse-Proxy unterstützt.



Stammordner-URLs in LiveCycle für die Verwendung mit dem Reverse-Proxy-Server

Die folgende Tabelle enthält Anwendungsstammordner-URLs für jede LiveCycle-Webanwendung. Sie sollten den Reverse-Proxy so konfigurieren, dass er nur URLs für Webanwendungsfunktionalität offenlegt, die Endbenutzern zur Verfügung gestellt werden soll.

Einige URLs sind als Endbenutzer-orientierte Webanwendungen gekennzeichnet. Sie sollten vermeiden, andere URLs für Configuration Manager für den externen Benutzerzugriff über den Reverse-Proxy offenzulegen.

Stammordner-URL	Zweck und/oder zugeordnete Webanwendung	Webbasierte Oberfläche	Endbenutzerzugriff
/ReaderExtensions/*	Reader Extensions-Webanwendung für Endbenutzer zum Anwenden von Verwendungsrechten auf PDF-Dokumente	Ja	Ja
/edc/*	Rights Management-Webanwendung für Endbenutzer	Ja	Ja
/edcws/*	Webdienst-URL für Rights Management	Nein	Ja
/pdfgui/*	PDF Generator-Webanwendung für Administratoren	Ja	Ja
/workspace/*	Workspace-Webanwendung für Endbenutzer	Ja	Ja
/workspace-server/*	Workspace-Servlets und -Datendienste, die die Workspace-Client-Anwendung benötigt	Ja	Ja

Stammordner-URL	Zweck und/oder zugeordnete Webanwendung	Webbasierte Oberfläche	Endbenutzerzugriff
/contentspace/*	LiveCycle Contentspace-Webanwendung für Endbenutzer (nicht mehr unterstützt)	Ja	Ja
/adobe-bootstrapper/*	Servlet für das Bootstrapping des LiveCycle-Repositorys	Nein	Nein
/soap/*	Informationsseite für LiveCycle-Server-Webdienste	Nein	Nein
/soap/services/*	Webdienst-URL für alle LiveCycle-Serverdienste	Nein	Nein
/edc/admin/*	Rights Management-Webanwendung für Administratoren	Ja	Nein
/adminui/*	Administration Console-Startseite	Ja	Nein
/TruststoreComponent/secured/*	Verwaltungsseiten für die Trust Store-Verwaltung	Ja	Nein
/FormsIVS/*	Forms IVS-Anwendung zum Testen und Debuggen der Formularwiedergabe	Ja	Nein
/OutputIVS/*	Output IVS, Anwendung zum Testen und Debuggen des Output-Diensts	Ja	Nein
/rmws/*	REST-URL für Rights Management	Nein	Ja
/OutputAdmin/*	Output-Verwaltungsseite	Ja	Nein
/FormServer/*	Dateien für die Forms-Webanwendung	Ja	Nein
/FormServer/GetImage Servlet	Dient zum Abrufen von JavaScript während der HTML-Transformation	Nein	Nein
/FormServerAdmin/*	Forms-Verwaltungsseiten	Ja	Nein
/repository/*	URL für den WebDAV-Zugriff (Debugging)	Ja	Nein
/AACComponent/*	Benutzeroberfläche von „Anwendungen und Dienste“	Ja	Nein
/WorkspaceAdmin/*	Workspace-Verwaltungsseiten	Ja	Nein
/rest/*	Rest-Supportseiten	Ja	Nein
/CoreSystemConfig/*	Seite mit LiveCycle Core-Konfigurationseinstellungen	Ja	Nein
/um/	User Management-Authentifizierung	Nein	Ja
/um/*	User Management-Verwaltungsoberfläche	Ja	Nein
/DoumentManager/*	Hoch- und Herunterladen von zu verarbeitenden Dokumenten beim Zugriff auf Remoting-Endpunkte, SOAP WSDL-Endpunkte und das Java-SDK mittels SOAP-Transport oder EJB-Transport bei aktivierten HTTP-Dokumenten.	Ja	Ja
/remoting/*	Durch Hinzufügen eines Remoting-Endpunkts wird eine Flex-Anwendung zum Aufrufen des Dienstes mithilfe von LiveCycle Remoting aktiviert.	Ja	Ja

3.5 Schutz vor Cross-Site Request Forgery-Angriffen

Bei einem Cross-Site Request Forgery-Angriff (CSRF) wird die Vertrauensstellung einer Website für den Benutzer genutzt, um Befehle zu übertragen, die vom Benutzer nicht autorisiert wurden und vom Benutzer nicht beabsichtigt sind. Dazu wird ein Link oder ein Skript in eine Webseite bzw. eine URL in eine E-Mail-Nachricht eingefügt, um auf eine andere Website zuzugreifen, für die der Benutzer bereits authentifiziert wurde.

Sie können beispielsweise bei der Administration Console angemeldet sein und gleichzeitig eine andere Website durchsuchen. Eine der Webseiten kann ein HTML-Bild-Tag mit einem `src`-Attribut enthalten, dessen Ziel ein serverseitiges Skript auf einer Opfer-Website ist. Webbrowser verwenden einen auf Cookies basierenden Mechanismus zur Sitzungsauthentifizierung. Dies wird von der angreifenden Website ausgenutzt. Sie sendet bösartige Anforderungen an das serverseitige Opferskipt und gibt vor, der rechtmäßige Benutzer zu sein. Weitere Beispiele finden Sie unter https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF) #Examples.

Die folgenden Merkmale sind für CSRF-Angriffe charakteristisch:

- Betreffen Sites, die auf der Identität eines Benutzers basieren
- Nutzen das Vertrauen Site in diese Identität aus
- Bringen den Browser des Benutzers dazu, HTTP-Anforderungen an eine Ziel-Site zu senden
- Verwenden HTTP-Anforderungen mit Nebeneffekten

LiveCycle verwendet die Referrer-Filter-Funktion, um CSRF-Angriffe abzuwehren. Die folgenden Begriffe werden in diesem Abschnitt zum Beschreiben der Referrer-Filter-Funktion verwendet:

- **Zulässiger Referrer:** Ein Referrer ist die Adresse der Quellseite, die eine Anforderung an den Server sendet. Bei JSP-Seiten oder -Formularen ist der Referrer in der Regel die vorherige Seite im Browserverlauf. Referrer für Bilder sind in der Regel Seiten, auf denen die Bilder angezeigt werden. Sie können Referrer, die auf Ihre Serverressourcen zugreifen dürfen, identifizieren, indem Sie sie zur Liste der zulässigen Referrer hinzufügen.
- **Zulässige Referrer – Ausnahmen:** Möglicherweise möchten Sie den Zugriffsbereich für einen bestimmten Referrer in Ihrer Liste der zulässigen Referrer einschränken. Um diese Einschränkung vorzunehmen, können Sie einzelne Pfade dieses Referrers zur Liste „Zulässige Referrer – Ausnahmen“ hinzufügen. Anforderungen, die von Pfaden in der Liste „Zulässige Referrer – Ausnahmen“ stammen, können keine Ressourcen auf dem LiveCycle-Server aufrufen. Sie können Ausnahmen zu zulässigen Referrern für eine bestimmte Anwendung definieren und zudem eine globale Liste mit Ausnahmen verwenden, die für alle Anwendungen gilt.
- **Zulässige URIs:** Hierbei handelt es sich um eine Liste mit Ressourcen, die ohne Prüfung des Referrer-Headers bereitgestellt werden sollen. Ressourcen, z. B. Hilfeseiten, die auf dem Server keine Statusänderungen hervorrufen, können zu dieser Liste hinzugefügt werden. Die Ressourcen in der Liste der zulässigen URIs werden unabhängig vom Referrer nie durch den Referrer-Filter gesperrt.
- **Null-Referrer:** Eine Serveranforderung, die nicht mit einer übergeordneten Webseite verknüpft ist oder nicht von einer übergeordneten Webseite stammt, gilt als Anforderung von einem Null-Referrer. Wenn Sie beispielsweise ein neues Browserfenster öffnen, eine Adresse eingeben und die Eingabetaste drücken, ist der an den Server gesendete Referrer null. Eine Desktopanwendung (.NET oder SWING), die eine HTTP-Anforderung an einen Webserver sendet, sendet auch einen Null-Referrer an den Server.

3.5.1 Referrer-Filter

Der Referrer-Filter funktioniert wie folgt:

1 Der LiveCycle-Server prüft die für den Aufruf verwendete HTTP-Methode:

   a Bei POST prüft der LiveCycle-Server den Referrer-Header.

b Bei GET umgeht der LiveCycle-Server die Referrer-Prüfung, es sei denn, *CSRF_CHECK_GETS* ist auf „true“ festgelegt. In diesem Fall wird der Referrer-Header überprüft. *CSRF_CHECK_GETS* ist in der Datei *web.xml* für Ihre Anwendung festgelegt.

2 Der LiveCycle-Server prüft, ob die angeforderten URI in der Positivliste eingetragen ist:

a Wenn die URI in der Positivliste eingetragen ist, akzeptiert der Server die Anforderung.

b Wenn die angeforderte URI nicht in der Positivliste eingetragen ist, ruft der Server den Referrer der Anforderung ab.

3 Wenn in der Anforderung ein Referrer angegeben ist, prüft der Server, ob es sich um einen zulässigen Referrer handelt. Wenn der Referrer nicht zulässig ist, prüft der Server, ob es sich um eine Referrer-Ausnahme handelt:

a Wenn es sich um eine Ausnahme handelt, wird die Anforderung blockiert.

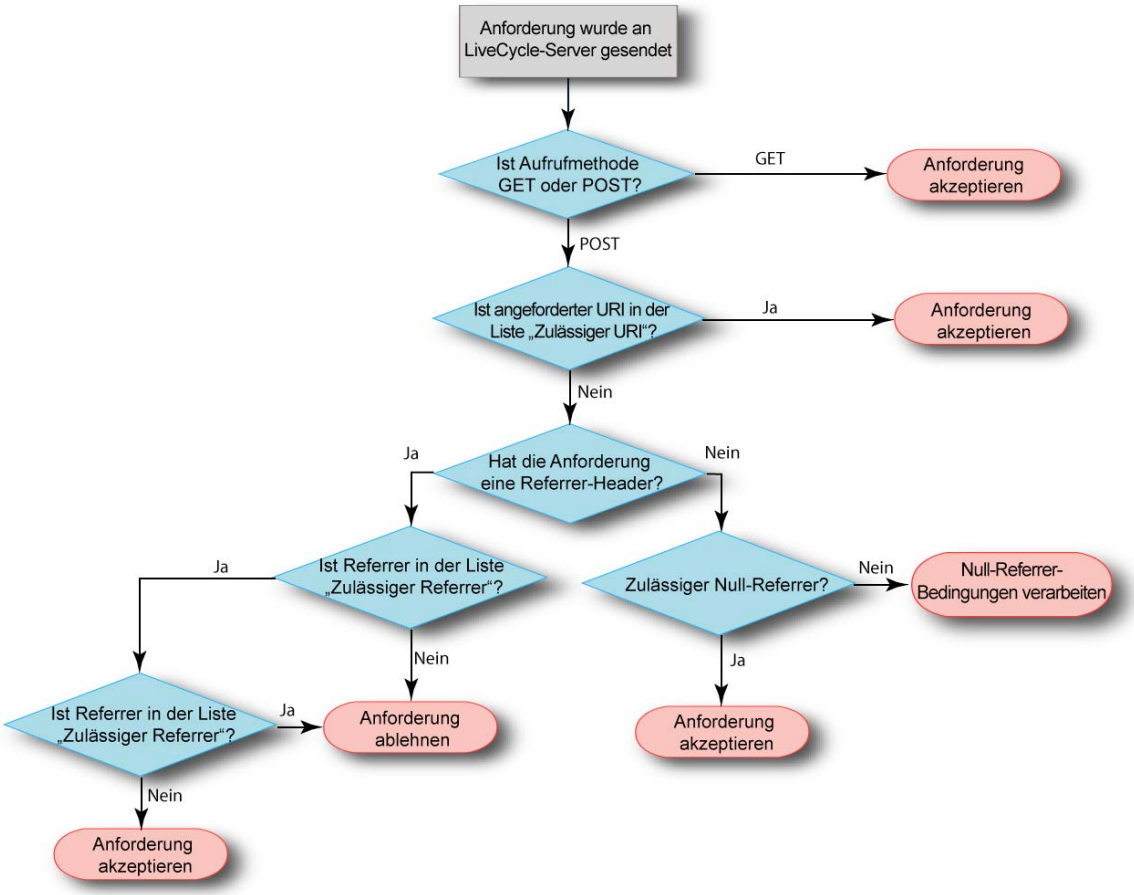
b Wenn es sich nicht um eine Ausnahme handelt, wird die Anforderung übergeben.

4 Wenn in der Anforderung kein Referrer angegeben ist, prüft der Server, ob ein Null-Referrer zulässig ist:

a Wenn ein Null-Referrer zulässig ist, wird die Anforderung übergeben.

b Wenn ein Null-Referrer nicht zulässig ist, prüft der Server, ob die angeforderte URI eine Ausnahme für den Null-Referrer ist, und behandelt die Anforderung entsprechend.

Im Folgenden wird die CSRF-Prüfung beschrieben, die LiveCycle durchführt, wenn eine Anforderung an den Server gesendet wird.



3.5.2 Referrer-Filter verwalten

LiveCycle stellt einen Referrer-Filter bereit, um Referrer anzugeben, denen der Zugriff auf Serverressourcen erlaubt wird. Der Referrer-Filter filtert standardmäßig keine Anforderungen, die eine sichere HTTP-Methode, z. B. GET, verwenden, es sei denn, *CSRF_CHECK_GETS* ist auf „true“ festgelegt. Wenn die Anschlussnummer für den Eintrag eines zulässigen Referrers auf 0 festgelegt ist, lässt LiveCycle alle Anforderungen mit Referrern von diesem Host unabhängig von der Anschlussnummer zu. Wenn keine Anschlussnummer angegeben wird, werden nur Anforderungen vom Standardanschluss 80 (HTTP) oder von Anschluss 443(HTTPS) zugelassen. Der Referrer-Filter wird deaktiviert, wenn alle Einträge in der Liste „Zulässige Referrer“ gelöscht werden.

Wenn Sie Document Services zum ersten Mal installieren, wird die Liste für zulässige Referrer mit der Adresse des Servers aktualisiert, auf dem Document Services installiert wird. Die Einträge für den Server enthalten den vollständig Servernamen, die IPv4-Adresse, die IPv6-Adresse, wenn IPv6 aktiviert ist, die Loopback-Adresse und einen „localhost“-Eintrag. Die zur Liste „Zulässige Referrer“ hinzugefügten Namen werden vom Host-Betriebssystem zurückgegeben. Ein Server mit der IP-Adresse 10.40.54.187 enthält beispielsweise folgende Einträge: `http://server-name:0, https://10.40.54.187:0, http://127.0.0.1:0, http://localhost:0`. Für alle nicht qualifizierten Namen, die vom Host-Betriebssystem zurückgegeben wurden (Namen, die keine IPv4-Adresse, IPv6-Adresse oder qualifizierte Domänennamen haben) wird die Positivliste nicht aktualisiert. Ändern Sie die Liste „Zulässige Referrer“ entsprechend Ihrer Geschäftsumgebung. Stellen Sie den LiveCycle-Server nicht mit der Standardliste „Zulässige Referrer“ in der Produktionsumgebung bereit. Nachdem Sie die zulässigen Referrer, Referrer-Ausnahmen oder URIs geändert haben, müssen Sie den Server neu starten, damit die Änderungen wirksam werden.

Liste „Zulässige Referrer“ verwalten

Sie können die Liste „Zulässige Referrer“ über die User Management-Oberfläche von Administration Console verwalten. Die User Management-Oberfläche stellt Funktionen zum Erstellen, Bearbeiten oder Löschen der Liste bereit. Weitere Informationen zur Verwendung der Liste „Zulässige Referrer“ finden Sie im Abschnitt *Verhindern von CSRF-Angriffen* der *Administration-Hilfe*.

Listen „Zulässige Referrer – Ausnahmen“ und „Zulässige URIs“ verwalten

LiveCycle stellt APIs zum Verwalten der Listen „Zulässige Referrer – Ausnahmen“ und „Zulässige URIs“ bereit. Mithilfe dieser APIs können Sie die Listen abrufen, erstellen, bearbeiten oder löschen. Im Folgenden Finden Sie eine Liste mit verfügbaren APIs:

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

Weitere Informationen zu den APIs finden Sie in der *LiveCycle API-Referenz*.

Verwenden Sie die Liste ***LC_GLOBAL_ALLOWED_REFERER_EXCEPTION*** für „Zulässige Referrer – Ausnahmen“ auf globaler Ebene, d. h. um Ausnahmen zu definieren, die für alle Anwendungen gelten. Diese Liste enthält nur URIs entweder mit einem absoluten Pfad (z. B. `/index.html`) oder einem relativen Pfad (z. B. `/sample/`). Sie können einen regulären Ausdruck am Ende eines relativen URI, z. B. `/sample/(.)*` auch anhängen.

Die Listen-ID ***LC_GLOBAL_ALLOWED_REFERER_EXCEPTIONS*** wird als Konstante in der Klasse `UMConstants` des Namespace `com.adobe.idp.um.api` definiert, der in `adobe-usermanager-client.jar` zu finden ist. Sie können die LiveCycle-APIs zum Erstellen, Ändern oder Bearbeiten dieser Liste verwenden. Um beispielsweise die Liste für globale zulässigen Referer - Ausnahmen zu verwenden, gehen Sie folgendermaßen vor:

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

Verwenden Sie die Liste ***CSRF_ALLOWED_REFERER_EXCEPTIONS*** für anwendungsspezifische Ausnahmen.

Referrer-Filter deaktivieren

Falls der Referrer-Filter den Zugriff auf den LiveCycle-Server vollkommen sperrt und Sie die Liste „Zulässige Referrer“ nicht bearbeiten können, können Sie das Startskript des Server aktualisieren und den Referrer-Filter deaktivieren.

Fügen Sie das JAVA-Argument „`-Dlc.um.csrffilter.disabled=true` in das Startskript ein und starten Sie den Server neu. Löschen Sie das JAVA-Argument, nachdem Sie die Liste „Zulässige Referrer“ entsprechend neu konfiguriert haben.

Referrer-Filter für benutzerdefinierte WAR-Dateien

Möglicherweise haben Sie benutzerdefinierte WAR-Dateien für die Verwendung mit LiveCycle speziell für Ihre Geschäftsanforderungen erstellt. Um den Referrer-Filter für Ihre benutzerdefinierten WAR-Dateien zu aktivieren, fügen Sie ***adobe-usermanager-client.jar*** in den Klassenpfad für die WAR-Datei und einen Filtereintrag in die Datei *web.xml* mit den folgenden Parametern ein:

CSRF_CHECK_GETS steuert die Referrer-Prüfung bei GET-Anforderungen. Wenn dieser Parameter nicht definiert wird, wird für den Standardwert „false“ festgelegt. Fügen Sie diesen Parameter nur ein, wenn Sie Ihre GET-Anforderungen filtern möchten.

CSRF_ALLOWED_REFERER_EXCEPTIONS ist die ID der Liste „Zulässige Referrer – Ausnahmen“. Der Referrer-Filter verhindert, dass Anforderungen, die von Referrern in der durch die Listen-ID identifizierten Liste stammen, Ressourcen auf dem LiveCycle-Server aufrufen.

CSRF_ALLOWED_URIS_LIST_NAME ist die ID der Liste „Zulässige URIs“. Der Referrer-Filter blockiert keine Anforderungen für keine der Ressourcen in der Liste, die anhand der Listen-ID angegeben wird, unabhängig vom Wert des Referer-Headers in der Anforderung.

CSRF_ALLOW_NULL_REFERER steuert das Verhalten des Referrer-Filters, wenn der Referrer null oder nicht vorhanden ist. Wenn dieser Parameter nicht definiert wird, wird für den Standardwert „false“ festgelegt. Fügen Sie diesen Parameter nur ein, wenn Sie Null-Referrer zulassen möchten. Das Zulassen eines Null-Referrers kann einige Arten von CSRF-Anriffen ermöglichen.

CSRF_NULL_REFERER_EXCEPTIONS ist eine Liste der URIs, für die keine Referrer-Prüfung durchgeführt wird, wenn der Referrer null ist. Dieser Parameter wird nur aktiviert, wenn für *CSRF_ALLOW_NULL_REFERER* „false“ festgelegt wird. Trennen Sie mehrere URIs in der Liste mit einem Komma.

Im Folgenden finden Sie ein Beispiel für den Filtereintrag in der Datei *web.xml* für die WAR-Datei ***SAMPLE***:

```
<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>
```

Fehlerbehebung

Wenn rechtmäßige Serveranforderungen vom CSRF-Filter blockiert werden, haben Sie folgende Möglichkeiten:

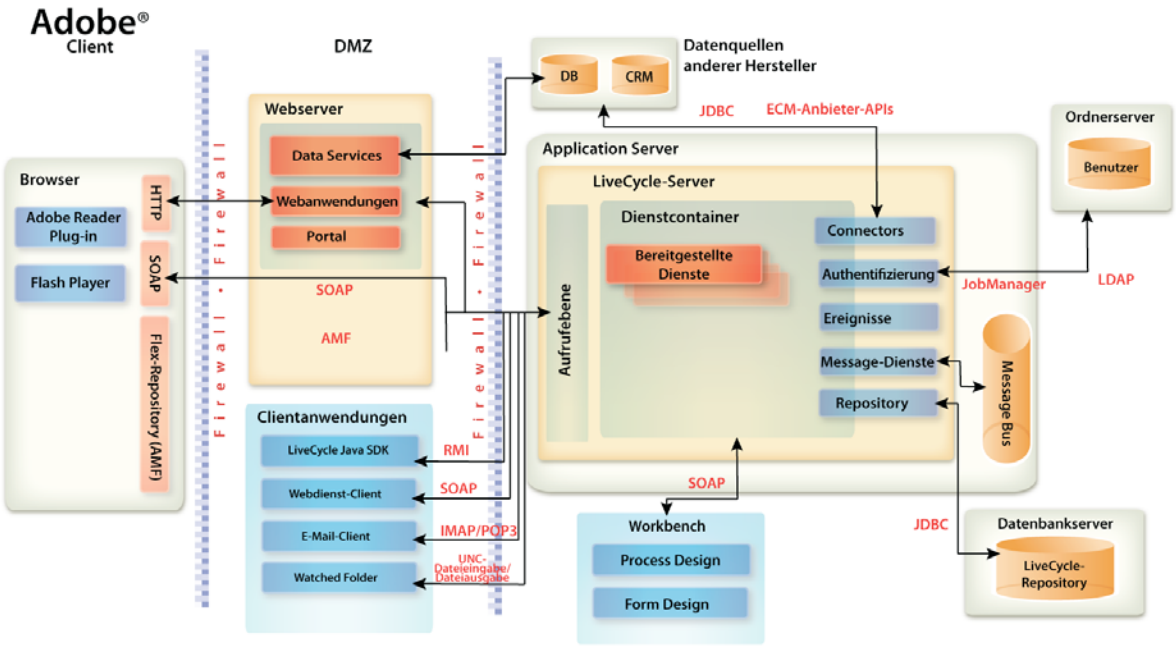
- Wenn die abgelehnte Anforderung einen Referrer-Header aufweist, sollten Sie sorgfältig abwägen, ob Sie diesen ggf. der Liste „Zulässige Referrer“ hinzufügen. Fügen Sie nur Referrer hinzu, denen Sie vertrauen.
- Wenn die abgelehnte Anforderung keinen Referrer-Header aufweist, ändern Sie Ihre Clientanwendung so, dass ein Referrer-Header eingefügt wird.
- Wenn der Client einen Browser verwenden kann, versuchen Sie es mit diesem Bereitstellungsmodell.
- Als letzten Ausweg können Sie die Ressource zur Liste „Zulässige URIs“ hinzufügen. Diese Vorgehensweise wird jedoch nicht empfohlen.

3.6 Sichere Netzwerkkonfiguration

In diesem Abschnitt finden Sie Beschreibungen der für LiveCycle erforderlichen Protokolle und Anschlüsse sowie Empfehlungen für die Bereitstellung von LiveCycle in einer sicheren Netzwerkkonfiguration.

3.6.1 Physische Architektur von LiveCycle

Diese Abbildung zeigt die Komponenten und Protokolle einer typischen LiveCycle-Bereitstellung einschließlich der entsprechenden Firewall-Topologie.



3.6.2 Von LiveCycle verwendete Netzwerkprotokolle

Wenn Sie, wie im vorherigen Abschnitt beschrieben, eine sichere Netzwerkarchitektur konfigurieren, sind die folgenden Netzwerkprotokolle für die Interaktion zwischen LiveCycle und anderen Systemen in Ihrem Unternehmensnetzwerk erforderlich.

Protokoll	**Verwendung**
HTTP	• Browser zeigt Configuration Manager und Endbenutzer-Webanwendungen an • Alle SOAP-Verbindungen
SOAP	• Webdienst-Clientanwendungen wie .NET-Anwendungen • Adobe Reader® verwendet SOAP für LiveCycle-Server-Webdienste • Adobe Flash®-Anwendungen verwenden SOAP für LiveCycle-Server-Webdienste • LiveCycle SDK-Aufrufe bei der Verwendung im SOAP-Modus • Workbench-Entwurfsumgebung
RMI	LiveCycle SDK-Aufrufe bei der Verwendung im Enterprise JavaBeans-Modus (EJB)
IMAP/POP3	• Auf E-Mail basierende Eingabe für einen Dienst (E-Mail-Endpunkt) • Aufgabenbenachrichtigungen per E-Mail
UNC-Dateieingabe/ausgabe	LiveCycle-Überwachung von überwachten Ordnern auf Eingabe in einen Dienst (Überwachter Ordner-Endpunkt)

Protokoll	Verwendung
LDAP	• Synchronisierung von Informationen über Firmenbenutzer und -gruppen in einem Ordner • LDAP-Authentifizierung für interaktive Benutzer
JDBC	• Abfrage- und Prozeduraufrufe an eine externe Datenbank, die während des Ausführung eines Prozesses mithilfe des JDBC-Diensts durchgeführt werden • LiveCycle-Repository für den internen Zugriff
WebDAV	Ermöglicht das Remote-Durchsuchen der Entwurfsversion des LiveCycle-Repositorys (Formulare, Fragmente usw.) durch einen beliebigen WebDAV-Client
AMF	Adobe Flash-Anwendungen, in denen LiveCycle-Serverdienste mit einem Remoting-Endpunkt konfiguriert sind
JMX	LiveCycle legt MBeans für die Überwachung mit JMX offen

3.6.3 Anschlüsse für Anwendungsserver

In diesem Abschnitt werden die Standardanschlüsse (und alternativen Konfigurationsbereiche) für jeden unterstützten Anwendungsservertyp beschrieben. Abhängig davon, welche Netzwerkfunktionalität Sie für Clients bereitstellen möchten, die eine Verbindung zu dem Anwendungsserver herstellen, auf dem LiveCycle ausgeführt wird, müssen diese Anschlüsse in der inneren Firewall aktiviert bzw. deaktiviert werden.

Hinweis: *Standardmäßig legt der Server mehrere JMX MBeans unter dem Namespace adobe.com offen. Dabei werden nur für die Überwachung des Serverzustands nützliche Informationen offengelegt. Um die Offenlegung von Informationen zu verhindern, sollten Sie jedoch Aufrufe von einem nicht vertrauenswürdigen Netzwerk davon abhalten, JMX MBeans zu suchen und auf Serverzustandsmetriken zuzugreifen.*

JBoss-Anschlüsse

Zweck	Anschluss
Zugriff auf Webanwendungen	[JBoss-Stammordner]/server/all/deploy/jbossweb-tomcat50.sar/server.xml HTTP/1.1 Connector-Anschluss 8080 AJP 1.3 Connector-Anschluss 8009 SSL/TLS Connector-Anschluss 8443
Zugriff auf LiveCycle-Serverdienste	[JBoss-Stammordner]/server/all/conf/jboss-service.xml WebService-Anschluss 8083 NamingService-Anschluss 1099 RMIport 1098 RMIObjectPort 4444 PooledInvoker ServerBindPort 4445

Zweck	Anschluss
Unterstützung für J2EE-Cluster	[JBoss-Stammordner]/server/all/deploy/cluster-service.xml ha.jndi.HANamingService-Anschluss 1100 RmiPort 1101 RMIObjectPort 4447 (nur Cluster) ServerBindPort 4446
CORBA-Unterstützung	[JBoss-Stammordner]/server/all/conf/jacorb.properties OAPort 3528 OASSLPort 3529
SNMP-Unterstützung	[JBoss-Stammordner]/server/all/deploy/snmp-adaptor.sar/META-INF/jbossservice. XML Anschlüsse 1161, 1162 [JBoss-Stammordner]/server/all/deploy/snmp-adaptor.sar/managers.xml Anschluss 1162

WebLogic-Anschlüsse

Zweck	Anschluss
Zugriff auf Webanwendungen	• Überwachungsanschluss des Verwaltungsservers: 7001 (Standard) • Überwachungsanschluss des Verwaltungsservers: 7002 (Standard) • Für verwalteten Server konfigurierter Anschluss, z. B. 8001
WebLogic-Verwaltungsanschlüsse sind für den Zugriff auf LiveCycle nicht erforderlich	• Überwachungsanschluss des verwalteten Servers: Konfigurierbar zwischen 1 und 65534 • SSL-Überwachungsanschluss des verwalteten Servers: Konfigurierbar zwischen 1 und 65534 • Überwachungsanschluss von Node Manager: 5556 (Standard)

WebSphere 6.1-Anschlüsse

Informationen zu WebSphere 6.1-Anschlüssen, die für LiveCycle erforderlich sind, finden Sie in „Port number settings in WebSphere Application Server versions“.

WebSphere 7.0-Anschlüsse

Informationen über WebSphere 7.0-Anschlüsse, die für LiveCycle erforderlich sind, finden Sie unter 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 Konfigurieren von SSL

Bezogen auf die in Abschnitt „3.6.1 Physische Architektur von LiveCycle“ auf Seite 31 beschriebene physische Architektur, sollten Sie SSL für alle Verbindungen konfigurieren, die Sie verwenden möchten. Besonders alle SOAP-Verbindungen müssen über SSL erfolgen, um die Offenlegung von Benutzerberechtigungen im Netzwerk zu verhindern.

Anweisungen zum Konfigurieren von SSL auf JBoss, WebLogic und WebSphere finden Sie unter „SSL konfigurieren“ in der LiveCycle Administration-Hilfe.

3.6.5 SSL-Umleitung konfigurieren

Nachdem Sie den Anwendungsserver auf die Unterstützung von SSL konfiguriert haben, müssen Sie sicherstellen, dass der gesamte HTTP-Verkehr zu LiveCycle-Anwendungen und -Diensten gezwungen wird, den SSL-Anschluss zu verwenden.

Informationen zum Konfigurieren der SSL-Umleitung für WebSphere oder WebLogic finden Sie in der Dokumentation zu Ihrem jeweiligen Anwendungsserver.

1 Wechseln Sie zur Datei „adobe-livecycle-jboss.ear“ und dekomprimieren Sie sie.

2 Extrahieren Sie die Datei „adminui.war“ und öffnen Sie die Datei „web.xml“ zur Bearbeitung.

3 Fügen Sie der Datei „web.xml“ den folgenden Code hinzu:

```
<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 Windows-spezifische Sicherheitsempfehlungen

Dieser Abschnitt enthält Sicherheitsempfehlungen, die für Windows spezifisch sind, wenn LiveCycle unter Windows ausgeführt wird.

3.7.1 JBoss-Dienstkonten

Bei der LiveCycle-Turnkey-Installation wird standardmäßig unter Verwendung des Kontos „Lokales System“ ein Dienstkonto eingerichtet. Das integrierte Benutzerkonto „Lokales System“ hat hohe Zugriffsrechte; es gehört zur Gruppe „Administratoren“. Wenn eine Worker Process-ID als Benutzerkonto „Lokales System“ ausgeführt wird, hat dieser Worker Process vollen Zugriff auf das gesamte System.

3.7.1.1 Anwendungsserver unter Verwendung eines Kontos ohne Administratorrechte ausführen

1 Erstellen Sie in der Microsoft Management Console (MMC) einen lokalen Benutzer für den LiveCycle-Serverdienst, der für die Anmeldung verwendet werden soll:

- Wählen Sie **Benutzer kann Kennwort nicht ändern aus**.
- Stellen Sie sicher, dass auf der Registerkarte **Mitglied von** die Gruppe „Benutzer“ aufgeführt ist.

2 Klicken Sie auf **Einstellungen** > **Verwaltung** > **Dienste**.

3 Doppelklicken Sie auf den Dienst „ Application Server“ und halten Sie diesen an.

4 Wählen Sie auf der Registerkarte **Anmelden** die Option **Dieses Konto** aus, suchen Sie das Benutzerkonto, das Sie erstellt haben, und geben Sie das Kennwort für das Konto ein.

5 Weisen Sie im Fenster „Lokale Sicherheitseinstellungen“ unter „Zuweisen von Benutzerrechten“ dem Benutzerkonto, unter dem der LiveCycle-Server ausgeführt wird, die folgenden Rechte zu:

- Anmeldung über Terminaldienste verweigern
- Lokale Anmeldung verweigern
- Als Dienst anmelden (sollte bereits festgelegt sein)

6 Weisen Sie dem neuen Benutzerkonto die Berechtigungen „Lesen und Ausführen“, „Ordnerinhalt auflisten“ und „Lesen“ für LiveCycle-Ordner mit Webinhalten zu.

7 Starten Sie den Application Server-Dienst.

3.7.2 Dateisystemsicherheit

LiveCycle verwendet das Dateisystem wie folgt:

- Speichern temporärer Dateien, die bei der Verarbeitung von Dokumentein- und -ausgaben verwendet werden
- Speichern von Dateien im globalen Archiv, die zur Unterstützung der installierten Lösungskomponenten verwendet werden
- Speichern von Dateien in überwachten Ordnern, die als Eingabe für einen Dienst verwendet werden und von einem Ordnerspeicherort im Dateisystem aus abgelegt werden

Wenn Sie überwachte Ordner verwenden, um Dokumente mit einem LiveCycle-Dienst zu senden und zu empfangen, müssen Sie besondere Sicherheitsmaßnahmen für das Dateisystem ergreifen. Wenn ein Benutzer Inhalte in einem überwachten Ordner ablegt, werden diese Inhalte durch den überwachten Ordner offengelegt. In diesem Fall wird der tatsächliche Endbenutzer nicht vom Dienst authentifiziert. Stattdessen ist der Dienst darauf angewiesen, dass durch Zugriffssteuerungslisten und Freigabesicherheitseinstellungen auf Ordnerebene bestimmt wird, von wem der Dienst tatsächlich aufgerufen werden darf.

3.8 JBoss-spezifische Sicherheitsempfehlungen

Dieser Abschnitt enthält spezielle Empfehlungen für die Anwendungsserverkonfiguration, die gelten, wenn JBoss 4.2.x für die Ausführung von LiveCycle verwendet wird.

3.8.1 JBoss Management Console und JMX-Konsole deaktivieren

Wenn Sie LiveCycle mit der Turnkey-Installationsmethode unter JBoss installieren, ist der Zugriff auf JBoss Management Console und die JMX-Konsole bereits konfiguriert (die JMX-Überwachung ist deaktiviert). Wenn Sie einen eigenen JBoss-Anwendungsserver verwenden, stellen Sie sicher, dass JBoss Management Console und die JMX-Überwachungskonsole geschützt sind. Der Zugriff auf die JMX-Überwachungskonsole wird in der JBoss-Konfigurationsdatei „jmx-invoker-service.xml“ festgelegt.

3.8.2 Directory Browsing deaktivieren

Nachdem Sie sich bei Administration Console angemeldet haben, können Sie durch Ändern der URL zur Ordnerliste der Konsole wechseln. Wenn Sie beispielsweise die URL in eine der folgenden URLs ändern, wird eine Liste angezeigt:

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

Legen Sie zum Deaktivieren der Ordnerauflistung den Wert des Auflistungsinitialisierungsparameters der Eigenschaft `DefaultServlet` auf `false` fest, wie im folgenden Beispiel in der Datei „*[JBoss-Stammordner]*\server\default\deploy\jbossweb-tomcatxxx.sar\conf\web.xml“ in Fettdruck gezeigt:

```
<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 WebLogic-spezifische Sicherheitsempfehlungen

Dieser Abschnitt enthält Empfehlungen für die Anwendungsserverkonfiguration zum Schützen von WebLogic 9.1 beim Ausführen von LiveCycle.

3.9.1 Directory Browsing deaktivieren

Stellen Sie in der Datei „weblogic.xml“ die Eigenschaften zu „index-directories“ auf `false` ein, wie im folgenden Beispiel gezeigt:

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

3.9.2 Aktivieren des SSL-Anschlusses in WebLogic

WebLogic aktiviert den SSL-Standardüberwachungsanschluss 7002 standardmäßig nicht. Aktivieren Sie diesen Anschluss in der WebLogic Server Administration Console, bevor Sie SSL konfigurieren.

3.10 WebSphere-spezifische Sicherheitsempfehlungen

Dieser Abschnitt enthält Empfehlungen für die Konfiguration des Anwendungsservers zum Schützen von WebSphere beim Ausführen von LiveCycle.

3.10.1 Directory Browsing deaktivieren

Stellen Sie in der Datei „ibm-web-ext.xml“ die Eigenschaft `directoryBrowsingEnabled` auf `false` ein.

3.10.2 Administrative Sicherheit in WebSphere aktivieren

1 Melden Sie sich bei WebSphere Administrative Console an.

2 Rufen Sie in der Navigationsstruktur einen der folgenden Links auf:

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

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

3 Wählen Sie **Enable administrative security** aus.

4 Deaktivieren Sie sowohl **Enable application security** als auch **Use Java 2 security**.

5 Klicken Sie auf **OK** oder **Apply**.

6 Klicken Sie im Feld **Messages** auf **Save directly to the master configuration**.

Kapitel 4: Konfigurieren sicherer Verwaltungseinstellungen

Im Allgemeinen verwenden Entwickler nicht die LiveCycle-Produktionsumgebung zum Erstellen und Testen ihrer Anwendungen. Sie müssen daher Benutzerkonten und -dienste verwalten, die, obwohl sie in einer privaten Entwicklungsumgebung benötigt werden, in einer Produktionsumgebung nicht erforderlich sind.

In diesem Abschnitt werden Methoden beschrieben, mit denen Sie die Gesamtangriffsfläche durch Verwaltungsoptionen in LiveCycle verkleinern.

4.1 Nicht erforderlichen Remote-Zugriff auf Dienste deaktivieren

Nach der Installation und Konfiguration von LiveCycle sind viele -Dienste für den Remote-Aufruf über SOAP, Enterprise JavaBeans™ (EJB) und LiveCycle Remoting verfügbar. Der Begriff *Remote* bezeichnet in diesem Fall alle Aufrufer mit Netzwerkzugriff auf die SOAP-, EJB- oder AMF-Anschlüsse (Action Message Format) für den Anwendungsserver.

LiveCycle-Serverdienste erfordern zwar, dass gültige Berechtigungen für einen autorisierten Aufrufer übergeben werden, dennoch sollten Sie den Remote-Zugriff nur für Dienste zulassen, für die der Remote-Zugriff erforderlich ist. Um die Verfügbarkeit einzuschränken, sollten Sie die Gruppe remote verfügbarer Dienste auf das Minimum für ein funktionierendes System begrenzen und dann den Remote-Aufruf für zusätzlich erforderliche Dienste aktivieren.

LiveCycle-Serverdienste erfordern in jedem Fall mindestens SOAP-Zugriff. Diese Dienste sind meist für die Verwendung durch Workbench erforderlich; es sind jedoch auch Dienste darunter, die von der Workspace-Webanwendung aufgerufen werden.

Führen Sie dieses Verfahren mithilfe der Webseite „Anwendungen und Dienste“ in Administration Console durch:

1 Melden Sie sich bei Administration Console an, indem Sie die folgende URL in einen Webbrowser eingeben:

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

2 Klicken Sie auf **Dienste > Anwendungen und Dienste > Voreinstellungen**.

3 Legen Sie unter „Voreinstellungen“ fest, dass bis zu 200 Dienste und Endpunkte auf einer Seite angezeigt werden sollen.

4 Klicken Sie auf **Dienste** > **Anwendungen und Dienste** > **Endpunktverwaltung**.

5 Wählen Sie in der Liste **Anbieter** den Eintrag **EJB** aus und klicken Sie auf **Filter**.

6 Aktivieren Sie zum Deaktivieren aller EJB-Endpunkte das Kontrollkästchen neben allen Endpunkten in der Liste und klicken Sie auf **Deaktivieren**.

7 Klicken Sie auf **Weiter** und wiederholen Sie den vorhergehenden Schritt für alle EJB-Endpunkte. Stellen Sie vor dem Deaktivieren von Endpunkten sicher, dass EJB in der Spalte „Anbieter“ aufgeführt wird.

8 Wählen Sie in der Liste **Anbieter** den Eintrag **SOAP** aus und klicken Sie auf **Filter**.

9 Aktivieren Sie zum Entfernen von SOAP-Endpunkten das Kontrollkästchen neben allen Endpunkten in der Liste und klicken Sie auf **Entfernen**. Entfernen Sie folgende Endpunkte nicht:

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

10 Klicken Sie auf **Weiter** und wiederholen Sie den vorhergehenden Schritt für SOAP-Endpunkte, die nicht in der obigen Liste aufgeführt sind. Stellen Sie vor dem Entfernen von Endpunkten sicher, dass SOAP in der Spalte „Anbieter“ aufgeführt wird.

4.2 Nicht erforderlichen anonymem Zugriff auf Dienste deaktivieren

Einige LiveCycle-Serverdienste lassen den nicht authentifizierten (anonymen) Aufruf bestimmter Vorgänge zu. Das heißt, ein oder mehrere vom Dienst offengelegte Vorgänge können von beliebigen authentifizierten Benutzern oder anonymen Benutzern aufgerufen werden.

1 Melden Sie sich bei Administration Console an, indem Sie die folgende URL in einen Webbrowser eingeben:

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

2 Klicken Sie auf **Dienste > Anwendungen und Dienste > Dienstverwaltung**.

3 Klicken Sie auf den Namen des zu deaktivierenden Dienstes (z. B. AuthenticationManagerService).

4 Klicken Sie auf die Registerkarte **Sicherheit**, deaktivieren **Sie** Anonymer Zugriff zugelassen und klicken Sie dann auf **Speichern**.

5 Wiederholen Sie die Schritte 3 und 4 für die folgenden Dienste:

- AuthenticationManagerService
- EJB
- E-Mail
- JobManager
- WatchedFolder
- UsermanagerUtilService

- Remoting
- RemoteEvents
- RepositoryProviderService
- EMCDocumentumRepositoryProvider
- IBMFilenetRepositoryProvider
- FormAugmenter
- TaskManagerService
- TaskManagerConnector
- TaskManagerQueryService
- TaskQueueManager
- TaskEndpointManager
- LCMTMInvoker
- UserService
- WorkspaceSearchTemplateService
- WorkspaceSignleSignOn
- WorkspacePropertyService
- OutputService
- FormsService

Wenn Sie vorhaben, alle oder einiger dieser Dienste für den Remote-Aufruf verfügbar zu machen, sollten Sie auch überlegen, ob Sie nicht den anonymen Zugriff für diese Dienste deaktivieren. Ansonsten kann jeder Aufrufer mit Netzwerkzugriff auf diesen Dienst den Dienst ohne Übergabe gültiger Berechtigungen aufrufen.

Der anonyme Zugriff sollte für alle nicht erforderlichen Dienste deaktiviert werden. Für viele interne Dienste muss die anonyme Authentifizierung aktiviert sein, da sie möglicherweise von jedem beliebigen Benutzer im System ohne vorherige Authentifizierung aufgerufen werden müssen.

4.3 Beispielbenutzer und Rollenzuweisungen entfernen

Eventuell haben Sie bei der Installation von LiveCycle auch Beispielbenutzer und -rollen (z. B. „Karl Müller“ und die Benutzerdomäne „Finanzunternehmen“) installiert. Sie sollten die Beispielbenutzerdomäne und die Beispielrollen mithilfe der User Management-Verwaltungsseiten entfernen.

4.3.1 Beispielbenutzer entfernen

1 Melden Sie sich bei Administration Console an, indem Sie die folgende URL in einen Webbrowser eingeben:

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

2 Klicken Sie auf **Einstellungen** > **User Management** > **Benutzer und Gruppen**.

3 Wählen Sie in der Liste **und Domäne** die Beispielorganisation aus und klicken Sie auf **Suchen**.

4 Aktivieren Sie zum Deaktivieren aller Beispielbenutzer das Kontrollkästchen neben allen Beispielbenutzern in der Liste und klicken Sie auf **Löschen**.

4.3.2 Beispieldomänen entfernen

1 Melden Sie sich bei Administration Console an, indem Sie die folgende URL in einen Webbrowser eingeben:

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

2 Klicken Sie auf **Einstellungen > User Management > Domänenverwaltung**.

3 Aktivieren Sie zum Löschen aller Beispieldomänen das Kontrollkästchen neben allen Beispieldomänen in der Liste und klicken Sie auf **Löschen**.

4 Klicken Sie auf **Speichern**.

4.4 Standardmäßiges globales Zeitlimit ändern

Endbenutzer können sich über Workbench, LiveCycle-Webanwendungen und benutzerdefinierte Anwendungen, die LiveCycle-Serverdienste aufrufen, bei LiveCycle authentifizieren. Mithilfe einer globalen Zeitlimiteinstellung wird festgelegt, wie lange solche Benutzer LiveCycle nutzen können (mittels einer auf SAML basierenden Bestätigung), bevor sie sich erneut authentifizieren müssen. Der Standardwert ist zwei Stunden. In einer Produktionsumgebung muss die Zeitdauer auf den zulässigen Mindestwert in Minuten verringert werden.

4.4.1 Zeitlimit für die erneute Authentifizierung auf das Minimum einstellen

1 Melden Sie sich bei Administration Console an, indem Sie die folgende URL in einen Webbrowser eingeben:

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

2 Klicken Sie auf **Einstellungen > User Management > Konfiguration > Konfigurationsdateien importieren und exportieren**.

3 Klicken Sie auf **Exportieren**, um eine „config.xml“-Datei mit den vorhandenen LiveCycle-Einstellungen zu erstellen.

4 Öffnen Sie die XML-Datei in einem Editor und suchen Sie folgenden Eintrag:

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

5 Ändern Sie den Wert in eine Zahl größer gleich 5 (Minuten) und speichern Sie die Datei.

6 Wechseln Sie in Administration Console zur Seite „Konfigurationsdateien importieren und exportieren“.

7 Geben Sie den Pfad der geänderten „config.xml“-Datei ein oder klicken Sie auf „Durchsuchen“, um zu dieser Datei zu wechseln.

8 Klicken Sie auf **Importieren**, um die geänderte „config.xml“-Datei hochzuladen und klicken Sie dann auf **OK**.