Härtung und Sicherheit für LiveCycle® ES2

Adobe® LiveCycle® ES2

24. September 2010

Version 9

© 2010 Adobe Systems Incorporated and its licensors. All rights reserved.

Härtung und Sicherheit für Adobe® LiveCycle® ES2
24. September 2010

This reference guide is licensed for use under the terms of the Creative Commons Attribution Non-Commercial 3.0 License. This License allows users to copy, distribute, and transmit the guide for noncommercial purposes only so long as (1) proper attribution to Adobe is given as the owner of the guide; and (2) any reuse or distribution of the guide contains a notice that use of the guide is governed by these terms. The best way to provide notice is to include the following link. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/.

Adobe, the Adobe logo, Adobe Reader, Acrobat, Flash, and LiveCycle are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. IBM and AIX trademarks of International Business Machines Corporation in the United States, other countries, or both. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Oracle, Java, Sun, and Solaris are trademarks or registered trademarks of Oracle and/or its affiliates. Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries. SUSE is a registered trademark of Novell, Inc. in the United States and other countries. UNIX is a registered trademark of The Open Group in the US and other countries. All other trademarks are the property of their respective owners.

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Inhalt

Informationen zu diesem Dokument ... 5
Zielgruppe dieses Dokuments ... 5
Konventionen in diesem Handbuch ... 5
Zusätzliche Informationen ... 6
1 Allgemeine Überlegungen zur Sicherheit ... 7
Herstellerspezifische Sicherheitsinformationen ... 7
Informationen zur Betriebssystemsicherheit ... 7
Informationen zur Anwendungsserversicherheit ... 8
Informationen zur Datenbanksicherheit ... 8
Konfigurieren von JBoss zur Verwendung eines nicht standardmäßigen HTTP-Anschlusses ... 10
Überlegungen zur Sicherheit von LiveCycle ES2 ... 11
Keine Verschlüsselung von E-Mail-Berechtigungen in der Datenbank ... 11
Sensibler Inhalt für LiveCycle Rights Management ES2 in der Datenbank ... 11
Kennwort in unverschlüsseltem Textformat in „adobe-ds.xml“ ... 11
2 Härten der Umgebung ... 12
Härtungsverfahren vor der Installation ... 12
Sicherheit der Netzwerkschicht ... 13
Betriebssystemsicherheit ... 15
Installation ... 15
Schritte nach der Installation ... 16
LiveCycle ES2-Serversicherheit ... 17
Einschränken von LiveCycle Content Services ES2-Eincheckquoten für Benutzerdaten ... 20
Sicherheit des Anwendungsservers ... 21
Verwenden der JMX-Konsole unter JBoss ... 22
Datenbanksicherheit ... 23
Konfigurieren der integrierten Sicherheit unter Windows ... 23
Schutz sensibler Inhalte in der Datenbank ... 25
LDAP-Sicherheit ... 25
Prüfung und Protokollierung ... 27
LiveCycle ES2 Abhängigkeiten von der Unix-Systembibliothek ... 27
Convert PDF-Dienst ... 27
XMLForms ... 28
Konfigurieren von LiveCycle ES2 für den externen Zugriff ... 30
Einrichten eines Reverse-Proxy für den Webzugriff ... 30
Sichere Netzwerkkonfiguration ... 32
LiveCycle ES2 Physische Architektur ... 32
Von LiveCycle ES2 verwendete Netzwerkprotokolle ... 33
Anschlüsse für Anwendungsserver ... 33
Konfigurieren von SSL ... 35
Konfigurieren der SSL-Umleitung ... 35
Windows-spezifische Sicherheitsempfehlungen ... 36
JBoss-Dienstkonten ... 36
Dateisystemsicherheit ... 37
JBoss-spezifische Sicherheitsempfehlungen ... 37

Deaktivieren von JBoss Management Console und der JMX-Konsole 37
Deaktivieren von Directory Browsing 37
WebLogic-spezifische Sicherheitsempfehlungen 38
Deaktivieren von Directory Browsing 38
Aktivieren des SSL-Anschlusses in WebLogic 38
WebSphere-spezifische Sicherheitsempfehlungen 38
Deaktivieren von Directory Browsing 38
Aktivieren der administrativen Sicherheit in WebSphere 38

3 Konfigurieren sicherer Verwaltungseinstellungen 40

Deaktivieren von nicht erforderlichem Remote-Zugriff auf Dienste 40
Deaktivieren von nicht erforderlichem anonymem Zugriff auf Dienste 41
Entfernen von Beispielbenutzern und Rollenzuweisungen 42
Ändern des standardmäßigen globalen Zeitlimits 43
Deaktivieren des API-Zugriffs für die LiveCycle 7.x-Abwärtskompatibilität 44

Informationen zu diesem Dokument

Dieses Dokument enthält Informationen über das Maximieren der Sicherheit der Adobe® LiveCycle® ES2 (Enterprise Suite) Version 9.0-Produktionsumgebung.

Zusätzliche Sicherheitsinformationen für LiveCycle ES2 finden Sie im *LiveCycle Developer Center*.

Sicherheitstipps und -berichte für LiveCycle ES2 stehen auf der Site *Security bulletins and advisories* zur Verfügung.

Zielgruppe dieses 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 ES2 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

Konventionen in diesem Handbuch

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

Name	Standardwert	Beschreibung
[LiveCycle ES2-Stammverzeichnis]	C:\Adobe\Adobe LiveCycle ES2\	Das Installationsverzeichnis für alle LiveCycle ES2-Lösungskomponenten. Dieses Verzeichnis enthält Unterverzeichnisse für LiveCycle Configuration Manager, das LiveCycle ES2 SDK und die einzelnen installierten LiveCycle ES2-Lösungskomponenten.
[JBoss_ES2-Stammverzeichnis]	C:\Adobe\Adobe LiveCycle ES2\jboss	Das Basisverzeichnis des Anwendungsservers, auf dem LiveCycle ES2 ausgeführt wird.

Zusätzliche Informationen

In der folgenden Tabelle finden Sie Hinweise auf weiterführende Informationen zu LiveCycle ES2.

Gewünschte Informationen	Siehe
LiveCycle ES2, Lösungskomponenten und Entwicklungstools	*LiveCycle ES2 Übersicht*
Vorbereiten Ihrer Umgebung für die Installation von oder die Aktualisierung auf LiveCycle ES2	*Vorbereiten der Installation von LiveCycle ES2* *Vorbereiten der Aktualisierung auf LiveCycle ES2*
Installieren von LiveCycle ES2	*Installieren und Bereitstellen von LiveCycle ES2 für JBoss* *Installieren und Bereitstellen von LiveCycle ES2 für WebSphere* *Installieren und Bereitstellen von LiveCycle ES2 für WebLogic*
Aktualisieren auf LiveCycle ES2 mithilfe der Nicht-Turnkey-Methode	*Aktualisieren auf LiveCycle ES2 für JBoss* *Aktualisieren auf LiveCycle ES2 für WebSphere* *Aktualisieren auf LiveCycle ES2 für WebLogic*
Installieren von LiveCycle Workbench ES2	*Installieren der Entwicklungsumgebung*
Ausführen allgemeiner Verwaltungsaufgaben für LiveCycle ES2	*LiveCycle ES2 Administration Help*
Weitere Dienste und Produkte, die in LiveCycle ES2 integriert werden können	*Adobe LiveCycle ES2*
Patch-Updates, technische Hinweise und zusätzliche Informationen zu dieser Produktversion	*LiveCycle Support Center*
LiveCycle ES2-Terminologie	*LiveCycle ES2 Glossar*

1 Allgemeine Überlegungen zur Sicherheit

In diesem Abschnitt finden Sie einleitende Informationen, die Ihnen die Vorbereitung auf das Härten Ihrer LiveCycle ES2-Umgebung erleichtern sollen. Hier finden Sie Informationen zu LiveCycle ES2, Betriebssystem, Anwendungsserver und Datenbanksicherheit, die Sie als Grundvoraussetzung benötigen. Sie sollten diese Informationen lesen, bevor Sie mit dem Sperren der Umgebung fortfahren.

Herstellerspezifische Sicherheitsinformationen

Dieser Abschnitt enthält sicherheitsbezogene Informationen zu Betriebssystemen, Anwendungsservern und Datenbanken, die in Ihre LiveCycle ES2-Unternehmenslösung integriert sind.

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

Informationen zur Betriebssystemsicherheit

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

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

Sicherheitsinformationen zu von LiveCycle ES2 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 *www.microsoft.com*
Microsoft Windows Server® 2008 Enterprise oder Standard Edition	Suchen Sie nach „Windows Server 2008 Security Guide“ unter *www.microsoft.com*
Microsoft Vista™ SP1, alle Derivate, 32-Bit und 64-Bit (nur für Nicht-Produktionsumgebungen)	Suchen Sie nach „Windows Vista Security Guide“ unter *www.microsoft.com*
Red Hat® Linux® AP oder ES	*Red Hat Enterprise Linux 4 Security Guide*

Betriebssystem	Sicherheitsressource
Sun Solaris10	*System Administration Guide: Security-Dienste*
SUSE™ Linux® Enterprise Server 10.0	*Linux Security*

Informationen zur Anwendungsserversicherheit

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

- Verwenden eines nicht offensichtlichen Benutzernamens für den Administrator
- Deaktivieren unnötiger Dienste
- Sichern 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 ES2 unterstützten Anwendungsservern finden Sie in den nachfolgend aufgeführten Ressourcen.

Anwendungsserver	Sicherheitsressource
Oracle WebLogic® 10g R3	Suchen Sie nach *Grundlegendes zu WebLogic Security* unter *http://download.oracle.com/docs/*
IBM WebSphere® 6.1 oder 7.0	*Sichern von Anwendungen und ihren Umgebungen (Version 6.1)* *Sichern von Anwendungen und ihren Umgebungen (Version 7.0)*
Red Hat® JBoss® 4.2.0 oder 4.2.1	*Sicherheit für JBoss*

Informationen zur Datenbanksicherheit

Beim Sichern 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 ES2 unterstützten Datenbanken finden Sie in den nachfolgend aufgeführten Ressourcen.

Datenbank	Sicherheitsressource
IBM DB2® 9.1 oder 9.5	*DB2-Produktfamilie*
Microsoft SQL Server 2005 SP2 oder 2008	*SQL Server 2005: Sicherheit* *SQL Server 2008: Sicherheit*
MySQL 5	*MySQL 5.0 Allgemeine Sicherheitsprobleme* *MySQL 5.1 Allgemeine Sicherheitsprobleme*
Oracle® 10g oder 11g	*Überlegungen zur Sicherheit und Anforderungen (Version 10g)* Informationen finden Sie im Kapitel „Sicherheit“ in der *Oracle 11g Dokumentationsbibliothek*

In der folgenden Tabelle werden die Standardanschlüsse aufgeführt, die während des LiveCycle ES2-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 ES2* für Ihren Anwendungsserver.

Produkt oder Dienst	Anschlussnummer
JBoss	8080
WebLogic	7001
Verwalteter Server fu?r WebLogic	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.

Konfigurieren von JBoss zur Verwendung eines nicht standardmäßigen HTTP-Anschlusses

JBoss Application Server verwendet 8080 als Standard-HTTP-Port. JBoss verfügt außerdem über die vorkonfigurierten Anschlüsse 8180, 8280 und 8380, die in der Datei „jboss-service.xml" kommentiert werden. Wenn Sie auf Ihrem Computer über eine Anwendung verfügen, die bereits diesen Anschluss verwendet, ändern Sie den von LiveCycle ES2 verwendeten Anschluss, indem Sie die folgenden Schritte ausführen:

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

   JBoss Turnkey-Installation: *[JBossES2 -Stammverzeichnis]*/server/lc_turnkey/conf/

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

2. Suchen Sie das folgende mbean 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-bin
dings.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 *[JBossES2 Stammverzeichnis]* (Turnkey) oder *[Anwendungsserver -Stammverzeichnis]* (Manuelle Installation von JBoss).

2. Suchen Sie das mbean von Schritt 2 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.

Überlegungen zur Sicherheit von LiveCycle ES2

In diesem Abschnitt werden einige LiveCycle ES2-spezifische Sicherheitslücken beschrieben, deren Sie sich bewusst sein sollen.

Keine Verschlüsselung von E-Mail-Berechtigungen in der Datenbank

Die von LiveCycle ES2-Anwendungen gespeicherten E-Mail-Berechtigungen werden nicht verschlüsselt, bevor sie in der LiveCycle ES2-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.

Sensibler Inhalt für LiveCycle Rights Management ES2 in der Datenbank

LiveCycle ES2 verwendet die LiveCycle ES2-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.

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

Der zum Ausführen von LiveCycle ES2 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 ES2 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.

2 Härten der Umgebung

In diesem Abschnitt werden Empfehlungen und Richtlinien für das Sichern von Servern beschrieben, auf denen LiveCycle ES2 ausgeführt wird. Dieses Dokument stellt keine umfassende Anleitung zum Härten (Absichern) des Hosts für das Betriebssystem und den Anwendungsserver dar. Es werden eine Reihe von Einstellungen für die Sicherheitshärtung beschrieben, die Sie implementieren sollten, um die Sicherheit von LiveCycle ES2 bei der Ausführung in einem firmeninternen Intranet zu verbessern. Um sicherzustellen, dass die LiveCycle ES2-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:

Härtungsverfahren vor der Installation: Verwenden Sie diese Verfahren, bevor Sie die LiveCycle ES2-Software installieren.

Härtungsverfahren bei der Installation: Verwenden Sie diese Verfahren während der Installation der LiveCycle ES2-Software.

Härtungsverfahren nach der Installation: Verwenden Sie diese Verfahren nach der Installation sowie in regelmäßigen Abständen.

LiveCycle ES2 kann in hohem Maß angepasst werden und in vielen verschiedenen Umgebungen eingesetzt werden. Einige der Empfehlungen entsprechen eventuell nicht den Anforderungen Ihrer Organisation.

Härtungsverfahren vor der Installation

Vor der Installation von LiveCycle ES2 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 ES2 nicht unter Verwendung einer Root Shell installieren oder konfigurieren. Standardmäßig werden alle Dateien unter dem Verzeichnis „/opt“ installiert. Der Benutzer, der die Installation durchführt, benötigt daher sämtliche Dateiberechtigungen für das Verzeichnis „/opt“. Alternativ kann die Installation auch unter dem Verzeichnis „/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 ES2 unter JBoss mit der Turnkey-Methode oder LiveCycle PDF Generator ES2 installieren. Wenn Sie PDF Generator ES2 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 ES2* für Ihren Anwendungsserver.

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 ES2-Server innerhalb einer demilitarisierten Zone (DMZ) bereit. Die Segmentierung sollte in mindestens zwei Schichten bestehen, wobei sich der Anwendungsserver, auf dem LiveCycle ES2 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 ES2-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.

Thema	**Beschreibung**
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. **Vorsicht:** Die Verwendung eines anderen Datenbankanschlusses wirkt sich auf die gesamte LiveCycle ES2-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 ES2. Informationen zum Konfigurieren von Datenquellen in LiveCycle ES2 finden Sie in *Installieren und Bereitstellen von LiveCycle ES2* oder *Aktualisieren auf LiveCycle ES2* für Ihren Anwendungsserver unter *Adobe LiveCycle ES2-Dokumentation*.

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 es erforderlich, dass die Uhrzeit auf LiveCycle ES2-Servern exakt ist. Verwenden Sie NTP, um die Uhrzeit auf allen Systemen zu synchronisieren, die direkt mit dem Internet verbunden sind.

Weitere Sicherheitsinformationen zu Ihrem Betriebssystem finden Sie unter „Informationen zur Betriebssystemsicherheit“ auf Seite 7.

Installation

In diesem Abschnitt werden Verfahren beschrieben, die Sie während des LiveCycle ES2-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 „Run As“ verwenden, um das LiveCycle ES2-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 ES2 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 ES2 ausschließlich von der Adobe-DVD oder einer vertrauenswürdigen Quelle.
Festplatten-partitionen	Installieren Sie LiveCycle ES2 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 ES2-Inhaltsverzeichnis installieren können. (Unter Windows enthält die Systempartition das Verzeichnis „system32“, das auch als Boot-Partition bezeichnet wird.)
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.
Abwärts-Kompatibilität	Aktivieren Sie die Abwärtskompatibilität mit LiveCycle 7.x nicht, wenn diese nicht für Ihre Bereitstellung erforderlich ist.

Schritte nach der Installation

Nachdem Sie LiveCycle ES2 erfolgreich installiert haben, sollten Sie die Sicherheitseinrichtungen der Umgebung unbedingt in regelmäßigen Abständen warten.

Im folgenden Abschnitt werden die verschiedenen Aufgaben, die zum Sichern des bereitgestellten LiveCycle ES2-Servers empfohlen werden, detailliert beschrieben.

LiveCycle ES2-Serversicherheit

Die folgenden, empfohlenen Einstellungen gelten für den LiveCycle ES2-Server außerhalb der Verwaltungs-Webanwendung. Um die Sicherheitsrisiken für den Server zu verringern, wenden Sie diese Einstellungen unmittelbar nach der Installation von LiveCycle ES2 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 ES2-Anwendungen sicherzustellen. Erstellen Sie zudem Richtlinien und Verfahren, damit Patches regelmäßig gesucht und installiert werden.
LiveCycle ES2-Aktualisierungen finden Sie auf der Site *Enterprise Products – Support Downloads*.

Dienstkonten (nur JBoss-Turnkey unter Windows)

LiveCycle ES2 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 ES2 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 ES2-Dienst, 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 ES2 nicht ändern.
2. Wählen Sie **Start** > **Einstellungen** > **Verwaltung** > **Dienste** aus.
3. Doppelklicken Sie auf den Dienst „JBoss for Adobe LiveCycle ES2“ und stoppen Sie ihn.
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 **Lokale Sicherheitseinstellungen** und wählen Sie **Lokale Richtlinien** > **Zuweisen von Benutzerrechten** aus.
6. Weisen Sie dem Benutzerkonto, unter dem der LiveCycle ES2-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 ES2-Webinhaltverzeichnissen zu.
8. Starten Sie den LiveCycle ES2 Application Server-Dienst.

Deaktivieren des Bootstrap-Servlets von LiveCycle Configuration Manager

LiveCycle Configuration Manager verwendete ein auf Ihrem Anwendungsserver bereitgestelltes Servlet, um das Bootstrapping der LiveCycle ES2-Datenbank durchzuführen. Da LiveCycle 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 LiveCycle Configuration Manager erfolgreich für die Konfiguration von LiveCycle ES2 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.

Sperren des Remote-Zugriffs auf den Trust Store

LiveCycle Configuration Manager ermöglicht Ihnen, eine Berechtigung für LiveCycle Reader Extensions ES2 in den LiveCycle ES2 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 LiveCycle Configuration Manager hochgeladen haben oder beschließen, Berechtigungen später mit LiveCycle-Verwaltungskonsole zu verwalten.

Sie können den Remote-Zugriff auf sämtliche Trust Store-Dienste deaktivieren, indem Sie die im Abschnitt „Deaktivieren von nicht erforderlichem Remote-Zugriff auf Dienste“ auf Seite 40 beschriebenen Schritte durchführen.

Deaktivieren des gesamten, nicht erforderlichen anonymen Zugriffs

In einigen LiveCycle ES2-Diensten 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 „Deaktivieren von nicht erforderlichem anonymem Zugriff auf Dienste“ auf Seite 41.

Ändern des Administratorkennworts

Beim Installieren von LiveCycle ES2 wird ein Standardbenutzerkonto für den Benutzer „Superadministrator“ mit der Anmelde-ID „Administrator“ und dem Standardkennwort *password* erstellt. Sie sollten dieses Kennwort umgehend mithilfe von LiveCycle Configuration Manager ändern.

➤ **So ändern Sie das Standardkennwort des Administrators:**

1. Geben Sie in einem Webbrowser den folgenden URL ein:

   `http://[Host name]:[Anschluss]/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 in das Feld **Suchen** den Begriff `administrator` ein und klicken Sie auf **Suchen**.
5. Klicken Sie in der Liste der Benutzer auf den **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**.

Deaktivieren der WSDL-Generierung in der Produktionsumgebung

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.

➤ **So deaktivieren Sie die WSDL-Generierung:**

1 Geben Sie in einem Webbrowser den folgenden URL ein:

```
http://[Host name]:[Anschluss]/adminui
```

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

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

Einschränken von LiveCycle Content Services ES2-Eincheckquoten für Benutzerdaten

Standardmäßig schränkt Content Services ES2 nicht die Datenmenge ein, die ein Benutzer zu einem bestimmten Zeitpunkt beim Server eincheckt. 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 ES2 zu aktivieren.

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

➤ **Aktivierung der Quotenverwaltung in Content Services ES2:**

Für JBoss

1. Wechseln Sie zum Verzeichnis *[JBoss-Stammverzeichnis]/bin* und öffnen Sie das Startskript in einem Texteditor:
   - **°(Windows)** run.bat
   - **°(Linux und UNIX)** run.sh

2. Fügen Sie die folgenden Eigenschaften unter das `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-Verwaltungskonsole, indem Sie in die Adresszeile eines Browsers „*http://[Hostname]*:*[Anschluss]* /console“ eingeben. *[Anschluss]* ist der nicht sichere Listener Port. 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 Registerkarten **Configuration**> **Server Start**.

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

   `-Dsystem.usages.enableQuotaSize=true`

   `-Dsystem.usages.quota=`***`[Größe 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 der Navigationsstruktur der Verwaltungskonsole von WebSphere die folgende Aufgabe für Ihren Anwendungsserver aus:

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

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

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

3. Wählen Sie unter „Server Infrastructure“ den Befehl **Java and Process Management > Process Definition** aus.

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.

Sicherheit des Anwendungsservers

In der folgenden Tabelle werden einige Verfahren zum Sichern des Anwendungsservers nach der Installation der LiveCycle ES2-Anwendung beschrieben.

Thema	Beschreibung
Verwaltungskonsole des Anwendungsservers	Nach der Installation, Konfiguration und Bereitstellung von LiveCycle ES2 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.

Thema	Beschreibung
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. 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 von JBoss Application Server können Sie beispielsweise das Element „connector“ in der Datei „server.xml“ in `secure=true` ändern. Weitere Informationen hierzu finden Sie in der Dokumentation zu Ihrem jeweiligen Anwendungsserver.

Directory Browsing	Wenn eine Person eine nicht vorhandene Seite oder den Namen eines Verzeichnisses anfordert (die Anforderungszeichenfolge endet in diesem Fall mit einem Schrägstrich (/)), sollte der Anwendungsserver den Inhalt dieses Verzeichnisses nicht zurückgeben. Damit dies nicht geschieht, können Sie das Directory Browsing auf Ihrem Anwendungsserver deaktivieren. Sie sollten dies für die LiveCycle-Verwaltungskonsole-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>`

Verwenden der JMX-Konsole unter JBoss

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 ES2 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.

➤ **So aktivieren Sie die JBoss JMX-Konsole:**

1. Laden Sie eine Kopie von JBoss 4.2.0 (oder höher) von *JBoss.org* herunter.
2. Beenden Sie JBoss Application Server.
3. Extrahieren Sie aus der heruntergeladenen, komprimierten Archivdatei die Dateien aus dem Verzeichnis „ *[JBoss -Stammverzeichnis]*/deploy/jmx-console.war/".
4. Legen Sie die Dateien „jmx-console.war/..." im Bereitstellungsverzeichnis des JBoss-Installationsverzeichnisses 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

Datenbanksicherheit

Beim Sichern der Datenbank sollten Sie die vom Datenbankhersteller beschriebenen Sicherheitsmaßnahmen implementieren. Sie sollten einem Datenbankbenutzer die minimal für die Verwendung von LiveCycle ES2 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. Informationen zu den entsprechenden Anforderungen für andere Datenbanken finden Sie in *Vorbereiten der LiveCycle ES2-Installation*.

Konfigurieren der integrierten Sicherheit unter Windows

Dieser Abschnitt ist relevant, wenn die SQL Server-Datenbank und LiveCycle ES2 auf einem Windows Server ausgeführt werden.

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.

➤ **So verwenden Sie die integrierte Sicherheit, um von JBoss aus eine vertrauenswürdige Verbindung mit SQL Server herzustellen:**

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>:<Anschluss>;databaseName=<Datenbankname>;integ
ratedSecurity=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 Adobe LiveCycle ES2) für „Anmelden als“ von „Lokales System“ in ein Anmeldekonto mit einer LiveCycle ES2-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**.

➤ **So verwenden Sie die integrierte Sicherheit, um von WebLogic aus eine vertrauenswürdige Verbindung mit SQL Server herzustellen:**

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

   `http://[Hostname]: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 **Connection Pool**. 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**.

➤ **So verwenden Sie die integrierte Sicherheit, um von WebSphere aus eine vertrauenswürdige Verbindung mit SQL Server herzustellen:**

1. Melden Sie sich bei WebSphere-Verwaltungskonsole 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 *[Installationsverzeichnis]*/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**.

Schutz sensibler Inhalte in der Datenbank

Das LiveCycle ES2-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 ES2-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 Tools des Datenbankherstellers für die Verschlüsselung von Spalten in Tabellen zu verwenden, die folgende Daten enthalten:

- Rights Management ES2-Dokumentschlüssel
- PIN-Verschlüsselungsschlüssel für HSM-Geräte im Trust Store
- Hashes für lokale Benutzerkennwörter

Informationen zu herstellerspezifischen Tools finden Sie unter „Informationen zur Datenbanksicherheit“ auf Seite 8.

LDAP-Sicherheit

LiveCycle ES2 nutzt meist ein LDAP-Verzeichnis (Lightweight Directory Access Protocol) als Quelle für Informationen über Unternehmensbenutzer und Gruppen sowie zur Durchführung der Kennwortauthentifizierung. Sie sollten sicherstellen, dass Ihr LDAP-Verzeichnis für die Verwendung von Secure Socket Layer (SSL) konfiguriert ist und LiveCycle ES2 für den Zugriff auf das LDAP-Verzeichnis über dessen SSL-Anschluss konfiguriert ist.

LDAP-Dienstblockade

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

Sie können die Anzahl fehlgeschlagener Versuche sowie die nachfolgende Sperrdauer festlegen, die LiveCycle ES2 implementiert, wenn die LiveCycle ES2-Authentifizierung eines Benutzers wiederholt fehlschlägt. Wählen Sie in LiveCycle-Verwaltungskonsole niedrige Werte. Bei der Auswahl der Anzahl von Fehlversuchen ist es wichtig, dass Sie sich bewusst sind, dass der Benutzer nach Durchführung aller Versuche von LiveCycle ES2 gesperrt wird, bevor dies durch den LDAP-Verzeichnisserver erfolgt.

➤ **So legen Sie Einstellungen für die automatische Kontosperrung fest:**

1. Melden Sie sich an der LiveCycle-Verwaltungskonsole 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**.

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
Zugriffssteuerung slisten für Protokolldateien	Legen Sie geeignete Zugriffssteuerungslisten für LiveCycle ES2-Protokolldateien fest. Das Festlegen entsprechender Berechtigungen verhindert, dass Angreifer die Dateien löschen. Als Sicherheitsberechtigung für das Protokolldateiverzeichnis sollte „Alle Berechtigungen“ für Administratoren und SYSTEM-Gruppen festgelegt werden. Das LiveCycle ES2-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 ES2-Server verwendet werden und ein Password Guessing-Angriff auf mehrere Computer erfolgt, bei dem von jedem Computer ein Kennwort abgefragt wird).

LiveCycle ES2 Abhängigkeiten von der Unix-Systembibliothek

Die folgenden Informationen sollen Ihnen bei der Planung einer LiveCycle ES2-Bereitstellung in einer UNIX-Umgebung helfen.

Convert PDF-Dienst

Für den Convert PDF-Dienst, der Bestandteil von LiveCycle ES2 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)
```

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

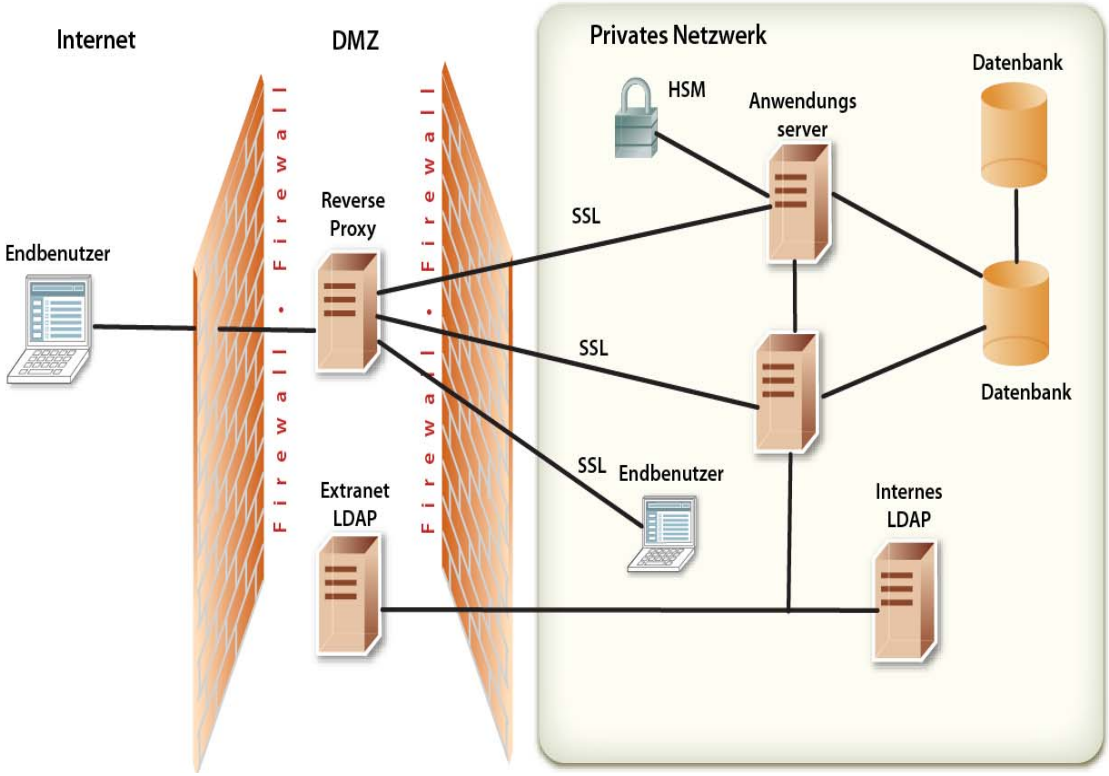
```
/usr/lib/
  libpthread.a(shr_comm.o)
  libpthread.a(shr_xpg5.o)
  libc.a(shr.o)
  librtl.a(shr.o)
  libdl.a(shr.o)
  libX11.a(shr4.o)
  libiconv.a(shr4.o)
  libpthreads.a(shr_comm.o)
/unix
  /usr/lib/libcrypt.a(shr.o)
  /usr/lib/libIM.a(shr.o)
  /usr/lib/libpthreads.a(shr_xpg5.o)
```

Konfigurieren von LiveCycle ES2 für den externen Zugriff

Nachdem Sie LiveCycle ES2 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 ES2-Produktionsservers beschrieben.

Einrichten eines Reverse-Proxy für den Webzugriff

Sie können einen *Reverse-Proxy* verwenden, um sicherzustellen, dass eine Gruppe von URLs für LiveCycle ES2-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 ES2 ausgeführt wird. Der Reverse-Proxy führt alle HTTP-Anfragen für den Anwendungsserver durch, auf dem LiveCycle ES2 läuft. Benutzer haben nur Netzwerkzugriff auf den Reverse-Proxy und können nur URL-Verbindungen aufbauen, die der Reverse-Proxy unterstützt.



Stammverzeichnis-URLs in LiveCycle ES2 für die Verwendung mit dem Reverse Proxy-Server

Die folgende Tabelle enthält Anwendungsstammverzeichnis-URLs für jede LiveCycle ES2-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 LiveCycle Configuration Manager für den externen Benutzerzugriff über den Reverse Proxy offenzulegen.

Stammverzeichnis-URL	Zweck und/oder zugeordnete Webanwendung	Webbasierte Oberfläche	Endbenutzerzugriff
/ReaderExtensions/*	LiveCycle Reader Extensions ES2-Webanwendung für Endbenutzer zum Anwenden von Verwendungsrechten auf PDF-Dokumente	Ja	Ja
/edc/*	LiveCycle Rights Management ES2-Webanwendung für Endbenutzer	Ja	Ja
/edcws/*	Webdienst-URL für Rights Management ES2	Kein	Ja
/pdfgui/*	LiveCycle PDF Generator ES2-Webanwendung für Administratoren	Ja	Ja
/workspace/*	LiveCycle Workspace ES2-Webanwendung für Endbenutzer	Ja	Ja
/workspace-server/*	LiveCycle Workspace ES2-Servlets und -Datendienste, die die Workspace ES2-Client-Anwendung benötigt	Ja	Ja
/contentspace/*	LiveCycle Contentspace ES2-Webanwendung für Endbenutzer	Ja	Ja
/adobe-bootstrapper/*	Servlet für das Bootstrapping des LiveCycle ES2-Repositorys	Kein	Kein
/adobe-lcm-boot strapper/*	Umleitung zum Bootstrap-Servlet/leitet LiveCycle 7.x-konforme Bootstrap-Anfragen zu /adobebootstrapper/ um	Kein	Kein
/soap/*	Informationsseite für LiveCycle ES2-Webdienste	Kein	Kein
/soap/services/*	Webdienst-URL für alle LiveCycle ES2-Dienste	Kein	Kein
/edc/admin/*	LiveCycle Rights Management ES2-Webanwendung für Administratoren	Ja	Kein
/adminui/*	Homepage von LiveCycle-Verwaltungskonsole	Ja	Kein
/TruststoreComponent/ secured/*	Verwaltungsseiten für die Trust Store-Verwaltung	Ja	Kein
/FormsIVS/*	Forms ES2 IVS-Anwendung zum Testen und Debuggen der Formularwiedergabe	Ja	Kein
/OutputIVS/adminui/ secured/admin/*	Verwaltungsseiten für das Output ES2-IVS zum Abrufen von Bildern in HTML	Ja	Kein
/OutputAdmin/*	LiveCycle Output ES2-Verwaltungsseiten	Ja	Kein
/FormServer/*	Dateien für die LiveCycle Forms ES2-Webanwendung	Ja	Kein
/FormServer/GetImage Servlet	Dient zum Abrufen von JavaScript während der HTML-Transformation	Kein	Kein
/FormServerAdmin/*	LiveCycle Forms ES2-Verwaltungsseiten	Ja	Kein

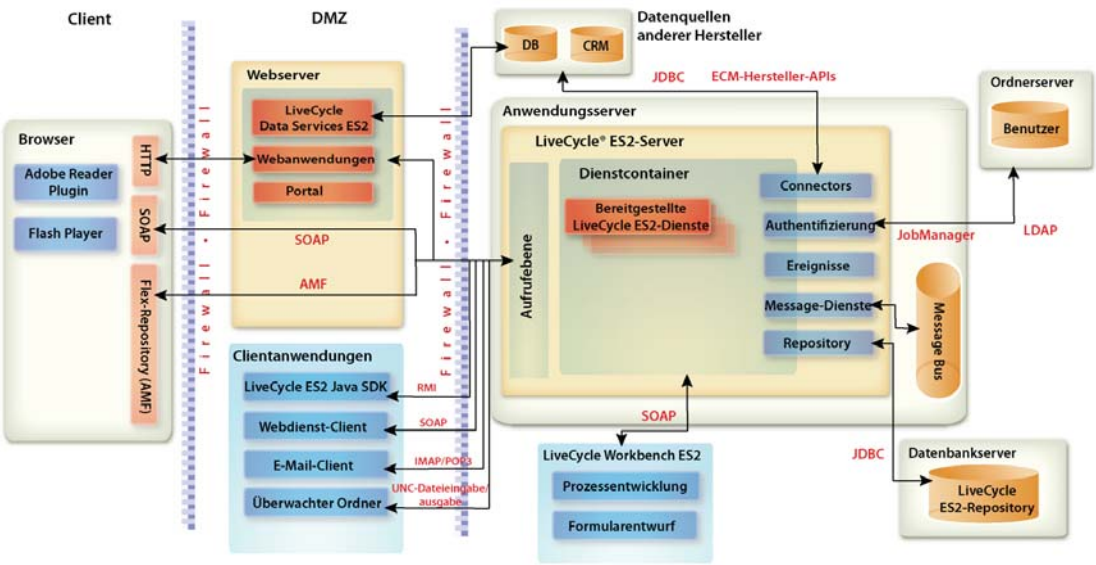
Stammverzeichnis-URL	Zweck und/oder zugeordnete Webanwendung	Webbasierte Oberfläche	Endbenut-zerzugriff
/repository/*	URL für den WebDAV-Zugriff (Debugging)	Ja	Kein
/appstore/Forms/*	Kompatibilität: Umleitung zur Repository-WebDAV-Implementierung für Clients von LiveCycle Form Manager 7.x WebDAV	Kein	Kein
/AACComponent/*	Anwendungen und Dienste-Benutzeroberfläche	Ja	Kein
/WorkspaceAdmin/*	LiveCycle Workspace ES2-Verwaltungsseiten	Ja	Kein
/rest/*	Rest-Supportseiten	Ja	Kein
/CoreSystemConfig/*	Seite mit LiveCycle ES2 Core-Konfigurationseinstellungen	Ja	Kein
/um/*	User Management-Verwaltungsoberfläche	Ja	Kein

Sichere Netzwerkkonfiguration

In diesem Abschnitt finden Sie Beschreibungen der für LiveCycle ES2 erforderlichen Protokolle und Anschlüsse sowie Empfehlungen für die Bereitstellung von LiveCycle ES2 in einer sicheren Netzwerkkonfiguration.

LiveCycle ES2 Physische Architektur

Diese Abbildung zeigt die Komponenten und Protokolle einer typischen LiveCycle ES2-Bereitstellung einschließlich der entsprechenden Firewall-Topologie.



Von LiveCycle ES2 verwendete Netzwerkprotokolle

Wenn Sie, wie im vorherigen Abschnitt beschrieben, eine sichere Netzwerkarchitektur konfigurieren, sind die folgenden Netzwerkprotokolle für die Interaktion zwischen LiveCycle ES2 und anderen Systemen in Ihrem Unternehmensnetzwerk erforderlich.

Protokoll	Verwendung
HTTP	• Browser zeigt LiveCycle Configuration Manager und Endbenutzer-Webanwendungen an • Alle SOAP-Verbindungen
SOAP	• Webdienst-Clientanwendungen wie .NET-Anwendungen • Adobe Reader® verwendet SOAP für LiveCycle ES2-Webdienste • Adobe Flash®-Anwendungen verwenden SOAP für LiveCycle ES2-Webdienste • LiveCycle ES2 SDK-Aufrufe bei der Verwendung im SOAP-Modus • LiveCycle Workbench ES2-Entwurfsumgebung
RMI	LiveCycle ES2 SDK-Aufrufe bei der Verwendung im Enterprise JavaBeans-Modus (EJB)
IIOP	LiveCycle 7.x-Anwendungen (APIs für das PDF Manipulation-Modul), die LiveCycle ES2-Dienste über die CORBA-Ebene für Abwärtskompatibilität aufrufen
IMAP/POP3	• Auf E-Mail basierende Eingabe für einen Dienst (E-Mail-Endpunkt) • Aufgabenbenachrichtigungen per E-Mail
UNC-Dateieingabe / ausgabe	LiveCycle ES2-Überwachung von überwachten Ordnern auf Eingabe in einen Dienst (Überwachter Ordner-Endpunkt)
LDAP	• Synchronisierung von Informationen über Firmenbenutzer und -gruppen in einem Verzeichnis • 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 ES2-Repository für den internen Zugriff
WebDAV	Ermöglicht das Remote-Durchsuchen der Entwurfsversion des LiveCycle ES2-Repositorys (Formulare, Fragmente usw.) durch einen beliebigen WebDAV-Client
AMF	Adobe Flash-Anwendungen, in denen LiveCycle ES2-Dienste mit einem Remoting-Endpunkt konfiguriert sind
JMX	LiveCycle ES2 legt MBeans für die Überwachung mit JMX offen

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 ES2 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-Stammverzeichnis]*/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 ES2-Dienste	*[JBoss-Stammverzeichnis]*/server/all/conf/jboss-service.xml WebService-Anschluss 8083 NamingService-Anschluss 1099 RMIport 1098 RMIObjectPort 4444 PooledInvoker ServerBindPort 4445
Unterstützung für J2EE-Cluster	*[JBoss-Stammverzeichnis]*/server/all/deploy/cluster-service.xml ha.jndi.HANamingService-Anschluss 1100 RmiPort 1101 RMIObjectPort 4447 (nur Cluster) ServerBindPort 4446
CORBA-Unterstützung	*[JBoss-Stammverzeichnis]*/server/all/conf/jacorb.properties OAPort 3528 OASSLPort 3529
SNMP-Unterstützung	*[JBoss-Stammverzeichnis]*/server/all/deploy/snmp-adaptor.sar/META-INF/ jbossservice.xml Anschlüsse 1161, 1162 *[JBoss-Stammverzeichnis]*/server/all/deploy/snmp-adaptor.sar/managers.xml Anschluss 1162

WebLogic-Anschlüsse

Zweck	Anschluss
Zugriff auf Webanwendungen	• Listen-Anschluss des Verwaltungsservers: Standard ist 7001 • SSL Listen-Anschluss des Verwaltungsservers: Standard ist 7002 • Anschluss für Managed Server konfiguriert, beispielsweise 8001
WebLogic-Verwaltungsanschlüsse sind für den Zugriff auf LiveCycle ES2 nicht erforderlich	• Listen-Anschluss des verwalteten Servers: Konfigurierbar von 1 bis 65534 • SSL Listen-Anschluss des verwalteten Servers: Konfigurierbar von 1 bis 65534 • Listen-Anschluss von Node Manager: Standard ist 5556

WebSphere 6,1-Anschlüsse

Informationen zu WebSphere 6.1-Anschlüssen, die für LiveCycle ES2 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 ES2 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.

Konfigurieren von SSL

Bezogen auf die in Abschnitt „LiveCycle ES2 Physische Architektur“ auf Seite 32 beschriebene physische Architektur, sollten Sie SSL für alle Verbindungen konfigurieren, die Sie vorhaben zu verwenden. Besonders alle SOAP-Verbindungen müssen über SSL erfolgen, um die Offenlegung von Benutzerberechtigungen im Netzwerk zu verhindern.

Anleitungen für die Konfiguration von SSL unter JBoss, WebLogic und WebSphere finden Sie unter „Konfigurieren von SSL“ in der *LiveCycle ES2Administrator-Hilfe* .

Konfigurieren der SSL-Umleitung

Nachdem Sie den Anwendungsserver auf die Unterstützung von SSL konfiguriert haben, müssen Sie sicherstellen, dass der gesamte HTTP-Verkehr zu LiveCycle ES2-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.

➤ **So konfigurieren Sie die SSL-Umleitung für JBoss:**

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>:
```

Windows-spezifische Sicherheitsempfehlungen

Dieser Abschnitt enthält Sicherheitsempfehlungen, die für Windows spezifisch sind, wenn LiveCycle ES2 unter Windows ausgeführt wird.

JBoss-Dienstkonten

Bei der LiveCycle ES2-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 das Benutzerkonto „Lokales System“ ausgeführt wird, hat dieser Worker Process vollen Zugriff auf das gesamte System.

➤ **So führen Sie den LiveCycle ES2-Anwendungsserver unter Verwendung eines bestimmten Kontos ohne Administratorrechte aus:**

1. Erstellen Sie in der Microsoft Management Console (MMC) einen lokalen Benutzer für den LiveCycle ES2-Dienst, 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.
2. Klicken Sie auf **Einstellungen** > **Verwaltung** > **Dienste**.
3. Doppelklicken Sie auf den Dienst „LiveCycle ES2 Application Server“ und stoppen Sie ihn.
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 ES2-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 ES2-Verzeichnisse mit Webinhalten zu.
7. Starten Sie den LiveCycle ES2 Application Server-Dienst.

Dateisystemsicherheit

LiveCycle ES2 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 ES2-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.

JBoss-spezifische Sicherheitsempfehlungen

Dieser Abschnitt enthält spezielle Empfehlungen für die Anwendungsserverkonfiguration, die gelten, wenn JBoss 4.2 für die Ausführung von LiveCycle ES2 verwendet wird.

Deaktivieren von JBoss Management Console und der JMX-Konsole

Wenn Sie LiveCycle ES2 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 Application Server verwenden, müssen Sie sicherstellen, 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.

Deaktivieren von Directory Browsing

Nachdem Sie sich bei LiveCycle-Verwaltungskonsole angemeldet haben, können Sie durch Ändern der URL zur Verzeichnisliste 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 Verzeichnisauflistung den Wert des Auflistungsinitialisierungsparameters der Eigenschaft `DefaultServlet` auf `false` fest, wie im folgenden Beispiel in der Datei *[JBoss_ES2-Stammverzeichnis]*\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>]
```

WebLogic-spezifische Sicherheitsempfehlungen

Dieser Abschnitt enthält Empfehlungen für die Anwendungsserverkonfiguration zum Schützen von WebLogic 9.1 beim Ausführen von LiveCycle ES2.

Deaktivieren von Directory Browsing

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>
```

Aktivieren des SSL-Anschlusses in WebLogic

WebLogic aktiviert den standardmäßigen SSL Listen-Anschluss 7002 nicht. Aktivieren Sie diesen Anschluss in WebLogic Server-Verwaltungskonsole, bevor Sie SSL konfigurieren.

WebSphere-spezifische Sicherheitsempfehlungen

Dieser Abschnitt enthält Empfehlungen für die Anwendungsserverkonfiguration zum Schützen von WebSphere beim Ausführen von LiveCycle ES2.

Deaktivieren von Directory Browsing

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

Aktivieren der administrativen Sicherheit in WebSphere

➤ **So aktivieren Sie die administrative Sicherheit in WebSphere:**

1. Melden Sie sich bei WebSphere-Verwaltungskonsole an.
2. Rufen Sie in der Navigationsstruktur einen der folgenden Links auf:

   (WebSphere 6.1) **Security** > **Secure administration, applications, and infrastructure**

   (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 auf im Feld **Messages** auf **Save directly to the master configuration**.

3 Konfigurieren sicherer Verwaltungseinstellungen

Im Allgemeinen verwenden Entwickler nicht die LiveCycle ES2-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 ES2 verkleinern.

Deaktivieren von nicht erforderlichem Remote-Zugriff auf Dienste

Nach der Installation und Konfiguration von LiveCycle ES2 sind viele LiveCycle ES2-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 ES2-Dienste 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 Diente aktivieren.

LiveCycle ES2-Dienste erfordern in jedem Fall mindestens SOAP-Zugriff. Diese Dienste sind meist für die Verwendung durch LiveCycle Workbench ES2 erforderlich; es sind jedoch auch Dienste darunter, die von der LiveCycle Workspace ES2-Webanwendung aufgerufen werden.

Führen Sie dieses Verfahren unter Verwendung der Webseite „Anwendungen und Dienste“ in LiveCycle-Verwaltungskonsole durch:

➤ **So deaktivieren Sie den Remote-Zugriff auf Dienste:**

1. Melden Sie sich bei LiveCycle-Verwaltungskonsole an, indem Sie die folgende URL in einen Webbrowser eingeben:

   ```
   http://[Host name]:[Anschluss]/adminui
   ```

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

3. Legen Sie unter „Voreinstellungen“ fest, dass bis zu 200 Dienste und Endpunkte auf derselben 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 jedem Endpunkt 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 jedem Endpunkt 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.

Deaktivieren von nicht erforderlichem anonymem Zugriff auf Dienste

Einige LiveCycle ES2-Dienste 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.

➤ **So deaktivieren Sie anonymen Zugriff auf Dienste:**

1. Melden Sie sich bei LiveCycle-Verwaltungskonsole an, indem Sie die folgende URL in einen Webbrowser eingeben:

   `http://[Host name]:[Anschluss]/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
- Email
- 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.

Entfernen von Beispielbenutzern und Rollenzuweisungen

Eventuell haben Sie bei der Installation von LiveCycle ES2 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.

➤ **So entfernen Sie Beispielbenutzer:**

1. Melden Sie sich bei LiveCycle-Verwaltungskonsole an, indem Sie die folgende URL in einen Webbrowser eingeben:

   `http://[Host name]:[Anschluss]/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 jedem Beispielbenutzer in der Liste und klicken Sie auf **Löschen**.

➤ **So entfernen Sie Beispieldomänen:**

1. Melden Sie sich bei LiveCycle-Verwaltungskonsole an, indem Sie die folgende URL in einen Webbrowser eingeben:

   `http://[Host name]:[Anschluss]/adminui`

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

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

4. Klicken Sie auf **Speichern**.

Ändern des standardmäßigen globalen Zeitlimits

Endbenutzer können sich über LiveCycle Workbench ES2, LiveCycle ES2-Webanwendungen und benutzerdefinierte Anwendungen, die LiveCycle ES2-Dienste aufrufen, bei LiveCycle ES2 authentifizieren. Mithilfe einer globalen Zeitlimiteinstellung wird festgelegt, wie lange solche Benutzer LiveCycle ES2 nutzen können (mittels einer auf SAML basierenden Bestätigung), bevor sie sich erneut authentifizieren müssen. Der Standardwert ist zweiStunden. In einer Produktionsumgebung muss die Zeitdauer auf den zulässigen Mindestwert in Minuten verringert werden.

➤ **So stellen Sie das Zeitlimit für die erneute Authentifizierung auf das Minimum ein:**

1. Melden Sie sich bei LiveCycle-Verwaltungskonsole an, indem Sie die folgende URL in einen Webbrowser eingeben:

   `http://[Host name]:[Anschluss]/adminui`

2. Klicken Sie in der LiveCycle-Verwaltungskonsole auf **Einstellungen > Benutzerverwaltung > Konfiguration > Konfigurationsdateien importieren und exportieren**.

3. Klicken Sie auf **Exportieren**, um eine „config.xml"-Datei mit den vorhandenen LiveCycle ES2-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 LiveCycle-Verwaltungskonsole 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**.

Deaktivieren des API-Zugriffs für die LiveCycle 7.x-Abwärtskompatibilität

Mit dem LiveCycle 7.x SDK entwickelte Anwendungen rufen LiveCycle ES2-Dienste nicht mit einer authentifizierten EJB- oder SOAP-Anforderung auf. Sie verwenden einen nicht gesicherten CORBA-Aufruf an einen auf dem Anwendungsserver bereitgestellten CORBA-Dienst.

Wenn Sie die in Aktualisierungsoption in LiveCycle Configuration Manager während des Installations- und Konfigurationsprozesses ausgewählt haben, wird ein CORBA-Dienst bereitgestellt, der die Ausführung bestehender LiveCycle 7.x-Anwendungen, die LiveCycle 7.x SDK verwenden, ermöglicht, wenn diese auf Ihrem Anwendungsserver bereitgestellt werden. Haben Sie die Aktualisierungsoption nicht ausgewählt, wurde dieser CORBA-Dienst nicht installiert.

➤ **So deaktivieren Sie den CORBA-Dienst für die Abwärtskompatibilität mit LiveCycle 7.x:**

1. Suchen Sie die Datei „adobe-livecycle-*[Anwendungsserver]*.ear" im Verzeichnis „*[LiveCycleES-Stammverzeichnis]*/jboss/deploy" und erstellen Sie eine Sicherungskopie dieser EAR-Datei.

2. Suchen Sie innerhalb der Datei „adobe-core-*[Anwendungsserver]*.ear" die Datei „adobe-core-compat-7to8-*[Anwendungsserver]*.ear". Diese EAR-Datei ist vorhanden, wenn Sie bereits eine LiveCycle ES2-Konfiguration und -Bereitstellung mit der Aktualisierungsoption durchgeführt haben.

3. Suchen Sie innerhalb der Datei „adobe-core-compat-7to8-*[Anwendungsserver]*.ear" die Datei „application.xml".

4. Ändern Sie die Datei „application.xml", indem Sie das folgende Modul durch Kommentarzeichen deaktivieren:

```
<!-- adobe-PDFManipulation start -->
<module id ="WebApp_PDFManipulation">
   <web>
   < web-uri>adobe-PDFManipulation.war</ web-uri>
   < context-root>/adobe-PDFManipulation</ context-root>
   </web >
</module >
```