Hewlett Packard Enterprise

Operations Orchestration

Softwareversion: 10.60
Betriebssysteme Windows und Linux

Sicherheits- und Optimierungshandbuch

Datum der Dokumentveröffentlichung: Mai 2016

Datum des Software-Release: Mai 2016

Rechtliche Hinweise

Garantie

Die Garantiebedingungen für Produkte und Services von Hewlett Packard Enterprise sind in der Garantieerklärung festgelegt, die diesen Produkten und Services beiliegt. Keine der folgenden Aussagen kann als zusätzliche Garantie interpretiert werden. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.

Eingeschränkte Rechte

Vertrauliche Computersoftware. Gültige Lizenz von Hewlett Packard Enterprise für den Besitz, Gebrauch oder die Anfertigung von Kopien erforderlich. Entspricht FAR 12.211 und 12.212. Kommerzielle Computersoftware, Computersoftwaredokumentation und technische Daten für kommerzielle Komponenten werden an die US-Regierung per Standardlizenz lizenziert.

Copyright-Hinweis

Markenhinweise

Adobe™ ist eine Marke von Adobe Systems Incorporated.

Microsoft® und Windows® sind in den USA eingetragene Marken der Microsoft Corporation.

UNIX® ist eine eingetragene Marke von The Open Group.

Dieses Produkt enthält eine Schnittstelle der freien Programmbibliothek zum Komprimieren, 'zlib', geschützt durch Copyright © 1995-2002 Jean-loup Gailly und Mark Adler.

Aktualisierte Dokumentation

Auf der Titelseite dieses Dokuments befinden sich die folgenden identifizierenden Informationen:

- Software-Versionsnummer, die Auskunft über die Version der Software gibt.
- Datum der Dokumentveröffentlichung, das bei jeder Änderung des Dokuments ebenfalls aktualisiert wird.
- Datum des Software-Release, das angibt, wann diese Version der Software veröffentlicht wurde.

Unter der unten angegebenen Internetadresse können Sie überprüfen, ob neue Updates verfügbar sind, und sicherstellen, dass Sie mit der neuesten Version eines Dokuments arbeiten: https://softwaresupport.hp.com/.

Für die Anmeldung bei dieser Website benötigen Sie einen HP Passport. Um sich für eine HP Passport-ID zu registrieren, klicken Sie auf **Register** (Registrieren) auf der HP Software Support-Site oder auf **Create an Account** (Konto erstellen) auf der HP Passport-Anmeldeseite.

Wenn Sie sich beim Support-Service eines bestimmten Produkts registrieren, erhalten Sie ebenfalls aktualisierte Softwareversionen und überarbeitete Ausgaben der zugehörigen Dokumente. Weitere Informationen erhalten Sie bei Ihrem HPE-Kundenbetreuer.

Inhalt

Einführung 6
Sicherheit – Übersicht 9
Sicherheitskonzepte 9
Sichere Implementierung und Bereitstellung 13
Standard-Sicherheitseinstellungen 13
Optimieren der Sicherheit von HPE OO 14
Physische Sicherheit 14
Richtlinien für die sichere Installation 15
Unterstützte Betriebssysteme 15
Empfehlungen zum Optimieren der Sicherheit des Betriebssystems 15
Optimieren der Sicherheit von Tomcat 15
Installationsberechtigungen 15
Sicherheit von Netzwerk und Kommunikation 16
Sicherheit von Kommunikationskanälen 16
Sicherheit der Administrationsschnittstelle 18
Zugriff auf die Administrationsschnittstelle 18
Sichern der Administrationsschnittstelle - Empfehlungen 18
Verwaltung und Authentifizierung von Benutzern 19
Authentifizierungsmodell 19
Benutzertypen 19
Verwaltung und Konfiguration der Authentifizierung 19
Datenbankauthentifizierung 20
Autorisierung 21
Autorisierungsmodell 21
Autorisierungskonfiguration 21
Sicherung 23
Verschlüsselung 24
Verschlüsselungsmodell 24
Verschlüsselungsverwaltung 24
Digitale Zertifikate 26
Sensitive Informationen in einem Content Pack 28
Audit und Protokolldateien 29

APIs und Schnittstellen 31
API- und Schnittstellenmodell 31
Funktionen und Administration der Sicherheitskonfiguration von APIs und Schnittstellen 31
Fragen und Antworten zum Thema Sicherheit 32
Optimieren der Sicherheit von Operations Orchestration 35
Empfehlungen zum Optimieren der Sicherheit 35
Standard-Sicherheitseinstellungen 37
Arbeiten mit Server- und Clientzertifikaten 38
Verschlüsseln der Kommunikation mit einem Serverzertifikat 39
Ersetzen des Central-TLS-Serverzertifikats 39
Importieren eines CA-Stammzertifikats in den Central-TrustStore 41
Importieren eines CA-Stammzertifikats in einen RAS-TrustStore 41
Importieren eines CA-Stammzertifikats in den OOSH-TrustStore 43
Importieren eines CA-Stammzertifikats in den Studio-TrustStore 44
Ändern und Verschlüsseln/Obfuskieren des KeyStore/TrustStore-Kennworts 45
Ändern der Kennwörter für KeyStore, Truststore und Serverzertifikat in der Central-Konfiguration 45
Ändern der TrustStore-Kennwörter für RAS, OOSH und Studio 47
Verschlüsseln und Obfuskieren von Kennwörtern 48
Entfernen der RC4-Verschlüsselung aus den unterstützten SSL-Verschlüsselungsverfahren 49
Ändern der HTTP/HTTPS-Ports oder Deaktivieren des HTTP-Ports 50
Ändern der Portwerte 51
Deaktivieren des HTTP-Ports 51
Fehlerbehebung 52
Clientzertifikatauthentifizierung (Gegenseitige Authentifizierung) 52
Konfigurieren der Clientzertifikatauthentifizierung in Central 52
Aktualisieren der Konfiguration eines Clientzertifikats in RAS 55
Konfigurieren eines ClientZertifikats in Studio Remote Debugger 56
Konfigurieren eines Clientzertifikats in OOSH 57
Verarbeiten der Zertifikatrichtlinien 58
Verarbeiten eines Zertifikatprinzipals 58
Konfigurieren von OO zum Lesen des Feldes "Alternativer 59

Antragstellername" in einem Zertifikat .....
Konfigurieren der FIPS 140-2-Konformität Stufe 1 in HPE OO 60
Vorbereitende Schritte für ein Upgrade 62
Konfigurieren der FIPS 140-2-Konformität von HPE OO 63
Konfigurieren der Eigenschaften in der Java-Sicherheitsdatei 63
Konfigurieren der Datei "encryption.properties" und Aktivieren des FIPS-Modus 64
Erstellen einer FIPS-kompatiblen OO-Verschlüsselung 65
Erneutes Verschlüsseln des Datenbankkennworts mit der neuen Verschlüsselung 66
Starten von HPE OO 66
Ersetzen der FIPS-Verschlüsselung 66
Ändern des FIPS-Verschlüsselungsschlüssels in Central 66
Ändern der RAS-Verschlüsselungseigenschaften 67
Konfigurieren des TLS-Protokolls 68
Verhindern des Zugriffs durch Flows auf das lokale Dateisystem von Central/RAS 68

Einführung

Willkommen beim HPE OO-Sicherheits- und Optimierungshandbuch.

Dieses Handbuch wendet sich an professionelle IT-Mitarbeiter, die Instanzen von HPE Operations Orchestration (HPE OO) mit einem hohen Grad an Sicherheit bereitstellen und verwalten. Unser Ziel besteht darin, Sie beim Treffen fundierter Entscheidungen über die verschiedenen Möglichkeiten und Funktionen, die HPE OO bereitstellt, zu unterstützen, damit die Sicherheitsanforderungen moderner Unternehmen erfüllt werden können.

Vor dem Hintergrund, dass sich die Sicherheitsanforderungen von Unternehmen ständig weiterentwickeln, sollte dieses Handbuch als Unterstützung von HPE beim Erfüllen dieser strengen Anforderungen betrachtet werden. Bei Sicherheitsanforderungen, die nicht im Rahmen dieses Handbuchs behandelt werden, öffnen Sie bitte einen Support-Fall mit dem HPE Support-Team, um sie zu dokumentieren. Wir werden sie dann in zukünftigen Editionen dieses Handbuchs berücksichtigen.

Technische Systemumgebung

HPE OO ist eine unternehmensweite Anwendung, die auf der Technologie Java 2 Enterprise Edition (J2EE) basiert. Die Technologie J2EE stellt einen komponentenbasierten Ansatz für Entwurf, Entwicklung, Assemblierung und Bereitstellung von Unternehmensanwendungen bereit.

Sicherheitsupdates

Zwischen OO 10.20 und 10.50 wurden die folgenden Sicherheitsupdates durchgeführt:

- Wenn das Kontrollkästchen **Erfassen der Anmeldeinformationen des angemeldeten Benutzers aktivieren** in Central aktiviert wurde, erfasst HPE OO vorübergehend (in sicherer Form) die Anmeldeinformationen des angemeldeten Benutzers, wenn dieser Benutzer Flows in Remote Debugger ausführt. Es wird die Warnung angezeigt, dass die Anmeldeinformationen möglicherweise erfasst werden.
- In HPE OO 10.5x gibt es standardmäßig keine Standardrolle. Damit erhält der Administrator eine bessere Kontrolle über die Benutzerautorisierung, da Benutzer nur die Rollen erhalten, die entweder ihnen oder ihrer LDAP-Gruppe explizit zugewiesen wurden.
- Wenn HPE OO mehrere LDAP-Konfigurationen enthält und der Administrator eine davon als Standard festlegt, brauchen Benutzer, die zu ihr gehören, bei der Anmeldung keine Domäne auszuwählen.
- HPE OO 10.5x sichert sensitive Daten (zum Beispiel Kennwörter) während der Ausführung. Wenn

eine Variable in Studio als sensitiv markiert wurde, wird sie in verschlüsselter Form abgerufen, wenn sie in Skriptlets verwendet wird.

Zwischen HPE OO 10.10 und 10.20 wurden die folgenden Sicherheitsupdates durchgeführt:

- Es ist jetzt möglich, Berechtigungen für Systemkonten in HPE OO zu erteilen. Dies ermöglicht es dem Administrator zu steuern, welche Benutzer welche Systemkonten anzeigen und Flows, die sie verwenden, ausführen können. Besonders nützlich ist diese Funktion für Kunden mit mehreren Organisationen, die möglicherweise einige der Systemkonten bei einigen Benutzern ausblenden möchten.

  Weitere Informationen finden Sie unter "Erweiterungen der Inhaltsverwaltung - Berechtigungen auf mehrere Rollen anwenden" in den *OO 10.20-Versionshinweisen*.

- Es ist jetzt möglich, im Dialogfeld "Berechtigungen bearbeiten" Berechtigungen auf mehrere Rollen anzuwenden. In früheren Versionen war es nur möglich, immer nur eine Rolle auszuwählen.

  Weitere Informationen finden Sie unter "Erweiterungen der Inhaltsverwaltung - Berechtigungen für Systemkonten" in den *OO 10.20-Versionshinweisen*.

- Wenn Sie ein Upgrade einer OO-Installation von einer früheren 10.x-Version durchführen, wird der SSL-Truststore so aktualisiert, dass er die von Oracle veröffentlichten aktuell vertrauenswürdigen Stammzertifikate enthält. Dazu gehört auch die Löschung der abgelaufenen Zertifikate und der Import von neuen Zertifikaten.

  Weitere Informationen finden Sie unter "Erweiterungen der Installation - Aktualisierte vertrauenswürdige Stammzertifikate" in den *OO 10.20-Versionshinweisen*.

- OO bietet jetzt die Möglichkeit, Ereignisse zu überwachen, sodass Sie Sicherheitsverletzungen verfolgen können. Das Audit ermöglicht das Verfolgen von Aktionen, die in Central stattfinden, z. B. Anmeldungen, das Auslösen von Flows, das Erstellen von Zeitplänen und das Bearbeiten von Konfigurationen.

  Derzeit können Sie das Audit-Trail nur über APIs abrufen. Weitere Informationen finden Sie im *OO API Guide*.

- OO unterstützt jetzt Verschlüsselungsschlüssel mit einer Länge von 2048 Bit (und mehr). Damit stimmen unsere Verschlüsselungsschlüssel mit dem Standard FIPS 186-4 überein.

- In der Datei **server.xml** (unter **<Installationsordner>/central/tomcat/conf/server.xml**) wurde die neue Eigenschaft sslEnabledProtocols eingefügt:

  ```
  sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
  ```

Diese Eigenschaft stellt sicher, dass nur TLS v1, TLS v1.1 und TLS v1.2 zugelassen werden, SSL 3.0 dagegen nicht. Dies beseitigt die Schwachstelle gegenüber "POODLE"-Attacken (Padding Oracle On Downgraded Legacy Encryption).

Zugehörige Dokumente

Weitere Informationen zum Optimieren der Sicherheit von OO finden Sie in den folgenden Dokumenten:

- *OO Network Architecture White Paper*

Weitere Informationen zu OO finden Sie in den folgenden Dokumenten:

- *OO-Konzepthandbuch*
- *OO Administrator Guide*
- *OO-Architekturhandbuch*
- *OO-Datenbankhandbuch*
- *OO Central-Benutzerhandbuch*
- *OO Studio-Erstellungshandbuch*
- *OO-Versionshinweise*
- *OO Installation, Upgrade, and Configuration Guide*
- *OO-Systemanforderungen*
- *OO Studio Wizards User Guide*

Diese und weitere Dokumente finden Sie auf HPE Live Network (https://hpln.hp.com/node/21/otherfiles#).

Sicherheit – Übersicht

In diesem Abschnitt finden Sie einen Überblick über die Sicherheitsmodelle und Empfehlungen für eine sichere Implementierung von HPE OO. Dies schließt Themen wie zum Beispiel Authentifizierung, Autorisierung und Verschlüsselung ein. An relevanten Stellen befinden sich Referenzen auf weitere HPE OO-Dokumente, in denen die Ausführung der sicherheitsbezogenen Aufgaben beschrieben werden.

Sicherheitskonzepte 9

Sicherheitskonzepte

HPE OO-Glossar

Weitere Informationen zu HPE OO-Konzepten finden Sie im *HPE OO-Konzepthandbuch*.

Rollenberechtigung

Eine Berechtigung ist eine vordefinierte Autorisierung zum Ausführen einer Aufgabe. HPE OO Central enthält einen Satz an Berechtigungen, die Rollen zugewiesen werden können.

So gewährt beispielsweise die Berechtigung **Zeitplan** die Möglichkeit, Ausführungspläne anzuzeigen und zu erstellen.

Rolle

Eine Rolle ist eine Sammlung von Berechtigungen.

Der Rolle **Flow-Administrator** kann beispielsweise die Berechtigung **Zeitpläne anzeigen** und die Berechtigung **Zeitpläne verwalten** zugewiesen sein.

Benutzer

Ein Benutzer ist ein Objekt, das mit einer Person (oder Anwendungsidentität) zur Darstellung der Person ein und Definition ihrer Autorisierung verknüpft ist.

Rollen werden zu Benutzern zugewiesen, um die Aktionen zu definieren, zu deren Ausführung die Benutzer in Central autorisiert sind. Dem Benutzer Joe Smith könnte beispielsweise die Rolle **Flow-Administrator** zugewiesen werden.

Es ist möglich, unterschiedliche Arten von Benutzern zu konfigurieren:

- **LDAP-Benutzer** melden sich mit ihrem LDAP-Benutzername und -Kennwort bei Central an. Zum Beispiel mit ihrem Active Directory-Benutzernamen und dem zugehörigen Kennwort.
- **Interne Benutzer** melden sich mit den lokal in Central definierten Benutzernamen- und Kennwortangaben an.
- **LWSSO** - HPE Lightweight Single Sign On (SSO) ist ein Mechanismus, bei dem mit einer einzigen Aktion der Benutzerauthentifizierung und -autorisierung einem Benutzer der Zugriff auf alle HPE-Systeme, die LWSSO unterstützen, gewährt werden kann. Wenn sich zum Beispiel Benutzer beim Webclient eines anderen HPE-Produkts, für den LWSSO aktiviert ist, angemeldet haben, können Sie direkt auf die Anwendung HPE OO Central zugreifen, also unter Umgehung des HPE OO Central-Anmeldebildschirms.

Wenn ein interner Benutzer und ein LDAP-Benutzer mit der gleichen Rolle angemeldet sind, gibt es keinen Unterschied zwischen ihren Berechtigungen.

Hinweis: Es wird empfohlen, statt internen Benutzern LDAP-Benutzer zu verwenden, da LDAP-Benutzer gemäß den Richtlinien, die durch den LDAP-Provider implementiert wurden, geschützt werden.

Inhaltsberechtigung

Die Inhaltsberechtigung ist die Berechtigung zum Anzeigen oder Ausführen von einzelnen Flows oder den Flows in einem bestimmten Ordner.

Benutzer, denen eine angegebene Rolle zugewiesen wurde, können gemäß den Inhaltsberechtigungen, die ihrer Rolle zugewiesen sind, auf die Flows zugreifen.

Zum Beispiel sind Benutzer mit der Rolle **Administrator** möglicherweise berechtigt, alle Flows im System anzuzeigen und auszuführen, während Benutzer mit der Rolle **Benutzer** möglicherweise nur bestimmte Flows ausführen und andere Flows lediglich anzeigen dürfen.

Allgemeine Sicherheitskonzepte

Systemsicherheit

Die Prozesse und Mechanismen, durch die computergestützte Geräte, Informationen und Dienste vor unbeabsichtigtem oder unbefugtem Zugriff, Änderung oder Beschädigung geschützt werden.

Mindestberechtigung

Das Beschränken des Zugriffs auf die minimale Stufe, die eine normale Funktionsweise ermöglicht. Dabei erhält ein Benutzerkonto lediglich die Berechtigungen, die für die Arbeit dieses Benutzers unverzichtbar sind.

Authentifizierung

Der Prozess zum Identifizieren einer Einzelperson, in der Regel anhand eines Benutzernamens und Kennwortes oder Zertifikats.

Autorisierung

Berechtigung zum Zugriff auf Systemobjekte auf Basis der Identität einer Einzelperson.

Verschlüsselung

Eine Methode zum Erhöhen der Sicherheit einer Nachricht oder Datei durch Verwürfeln der Inhalte, sodass sie nur durch eine Person gelesen werden kann, die den richtigen Verschlüsselungsschlüssel besitzt, um sie zu codieren. Zum Beispiel verschlüsselt das Protokoll TLS die Kommunikationsdaten.

Gegenmaßnahme

Eine Methode zum Mindern des Risikos einer Bedrohung.

Tiefengestaffelte Sicherheit

Schutz in Ebenen, damit Sie sich nicht auf eine Sicherheitsmaßnahme allein verlassen müssen.

Risiko

Ein mögliches Ereignis, das Schaden verursachen kann. Zum Beispiel, finanzieller Verlust, Schaden am Firmenimage usw.

Bedrohung

Auslösen eines Risikoereignisses, das eine Schwachstelle nutzt.

Schwachstelle

Eine Schwäche in einem Zielobjekt, die durch eine potenzielle Sicherheitsbedrohung ausgenutzt werden kann.

Sichere Implementierung und Bereitstellung

Standard-Sicherheitseinstellungen

Oftmals ist es ratsam, die voreingestellten Standard-Sicherheitseinstellungen den Anforderungen entsprechend anzupassen.

- **Authentifizierung** – In Central ist diese Option standardmäßig nicht aktiviert. Es wird empfohlen, die Option zu aktivieren, sobald Benutzer eingerichtet wurden. Weitere Informationen finden Sie unter "Aktivieren der Authentifizierung" im *HPE OO-Central-Benutzerhandbuch*.
- **Audit** – In Central ist diese Option standardmäßig nicht aktiviert. Es wird empfohlen, die Option zu aktivieren. Weitere Informationen finden Sie unter "Aktivieren des Audit" im *HPE OO-Central-Benutzerhandbuch*.
- **TLS-Verschlüsselung** – Standardmäßig unterstützt HPE OO drei TLS-Protokolle: 1.0, 1.1, 1.2. Es wird empfohlen, mit der neuesten Version zu arbeiten. Weitere Informationen finden Sie unter "Konfigurieren des TLS-Protokolls" auf Seite 68.
- **TLS-Serverzertifikat** – Standardmäßig wird der Benutzer während der Installation von OO Server aufgefordert, ein CA-Zertifikat anzugeben.
- **Clientzertifikat** – Diese Option ist standardmäßig nicht aktiviert. Für die Authentifizierung bei Central wird empfohlen, mit Clientzertifikat zu arbeiten. Weitere Informationen finden Sie unter "Konfigurieren der Clientzertifikatauthentifizierung in Central" auf Seite 52.
- **Kennwörter für KeyStore, TrustStore und das Serverzertifikat** – Standardmäßig werden die Java-Kennwörter für keyStore, trustStore und das Serverzertifikat bereitgestellt. Es wird empfohlen, diese durch verschlüsselte Kennwörter zu ersetzen. Weitere Informationen finden Sie unter "Ändern und Verschlüsseln/Obfuskieren des KeyStore/TrustStore-Kennworts" auf Seite 45.
- **RC4-Verschlüsselung** – Die RC4-Verschlüsselung ist standardmäßig aktiviert. Auf JRE-Ebene sollte die RC4-Verschlüsselung jedoch deaktiviert werden. Weitere Informationen finden Sie unter "Entfernen der RC4-Verschlüsselung aus den unterstützten SSL-Verschlüsselungsverfahren" auf Seite 49.
- **Sicherheitsbanner** – In Central ist diese Option standardmäßig nicht aktiviert. Es wird empfohlen, die Option mit Ihrer benutzerdefinierten Meldung zu aktivieren. Weitere Informationen finden Sie unter "Konfigurieren eines Sicherheitsbanners" im *HPE OO-Central-Benutzerhandbuch*.
- **Windows-Authentifizierung der Datenbank** – In Central ist diese Option standardmäßig nicht aktiviert. Falls Sie mit der Windows- und SQL-Serverumgebung arbeiten, sollten Sie HPE OO für

die Verwendung der Windows-Authentifizierung konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von HPE OO für die Verwendung der Windows-Authentifizierung" im *HPE OO-Datenbankhandbuch*.

- **Standard-Algorithmen** – Die Datei **encryption.properties** enthält die Standard-Algorithmen. Falls Sie den FIPS-Standard erfüllen möchten, finden Sie die Informationen hierzu unter "Konfigurieren der FIPS 140-2-Konformität Stufe 1 in HPE OO" auf Seite 60. Weitere Informationen zu den Standards der FIPS 140-2-Konformität Stufe 1 finden Sie unter "Verschlüsselung" auf Seite 24 im Abschnitt "Verschlüsselungsverwaltung".
- **Java-Richtlinie** – Die Datei **java.policy** ist nicht verschlüsselt. Informationen zum Anpassen der Datei **java.policy** finden Sie unter "Verhindern des Zugriffs durch Flows auf das lokale Dateisystem von Central/RAS" auf Seite 68.

Optimieren der Sicherheit von HPE OO

Das Kapitel zum Optimieren der Sicherheit enthält Empfehlungen zum Sichern Ihrer HPE OO-Bereitstellung gegen Sicherheitsrisiken oder -bedrohungen. Einige der wichtigsten Gründe für das Sichern einer Anwendung sind der Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von wichtigen Informationen einer Organisation.

Für einen umfassenden Schutz Ihres HPE OO-Systems ist es erforderlich, sowohl HPE OO als auch die IT-Umgebung (z. B. die Infrastruktur und das Betriebssystem), auf der die Anwendung ausgeführt wird, zu sichern.

Das Kapitel zum Optimieren der Sicherheit enthält Empfehlungen zum Sichern von HPE OO auf Anwendungsebene. Informationen zum Sichern der Infrastruktur innerhalb der Kundenumgebung sind nicht enthalten. Für das Verständnis seiner Infrastruktur/Umgebung und das Anwenden der entsprechenden Richtlinien zum Optimieren der Sicherheit ist der Kunde allein verantwortlich.

Physische Sicherheit

HP Software empfiehlt, dass HPE OO durch physische Sicherheitskontrollen, die durch Ihre Organisation definiert werden, geschützt wird. Die HPE OO-Serverkomponenten werden in einer physisch gesicherten Umgebung nach bewährten Verfahren installiert. Zum Beispiel muss sich der Server in einem geschlossenen Raum mit Zugangskontrolle befinden.

Richtlinien für die sichere Installation

Unterstützte Betriebssysteme

Die Typen und Versionen der unterstützten Betriebssysteme finden Sie in den *HPE OO-Systemanforderungen*.

Empfehlungen zum Optimieren der Sicherheit des Betriebssystems

Die empfohlenen Best Practices für das Optimieren der Sicherheit Ihres Betriebssystems erfahren Sie bei Ihrem Betriebssystemanbieter.

Beispiel:

- Patches sollten installiert werden
- Nicht benötigte Dienste/Software sollten entfernt oder deaktiviert werden
- Benutzern sollten nur Minimalberechtigungen zugewiesen werden
- Audit sollte aktiviert werden

Optimieren der Sicherheit von Tomcat

Bei der Installation von HPE OO Central wird Tomcat standardmäßig durch teilweise Abschottung gesichert. Wenn Sie die Sicherheit zusätzlich optimieren möchten, dann nutzen Sie die Empfehlungen im Kapitel zum Optimieren der Sicherheit.

Installationsberechtigungen

Zum Installieren und Ausführen von HPE OO sind die folgenden Berechtigungen erforderlich:

Installieren von HPE OO	Windows/Linux: Jeder Standardbenutzer, der einen Java-Prozess ausführen kann und die Berechtigung zum Erstellen von Ordnern und Diensten besitzt
Ausführen von HPE OO	• Windows: Der Windows-Dienst wird als Systembenutzer oder bestimmter Benutzer ausgeführt (der Benutzer muss Zugriff auf das HPE OO-Installationsverzeichnis besitzen) • Linux: Jeder Standardbenutzer, der einen Java-Prozess ausführen kann

Siehe auch die Empfehlungen im CIS Apache Tomcat 7.0-Dokument.

Sicherheit von Netzwerk und Kommunikation

Im *HPE OO-Architekturhandbuch* wird die Basissicherheit für OO-Topologie, Hochverfügbarkeit und Load Balancer beschrieben.

Im *HPE OO Network Architecture White Paper* wird die erforderliche Firewallkonfiguration beschrieben. Außerdem werden zwei Problemumgehungen für Fälle vorgeschlagen, bei denen wegen bestimmter Richtlinieneinschränkungen die erforderliche Firewallkonfiguration nicht implementiert werden kann:

- SSH-Rückwärtstunnelung
- Reverseproxy

Sicherheit von Kommunikationskanälen

Unterstützte Protokolle und Konfiguration

HPE OO unterstützt das Protokoll TLS.

Weitere Informationen finden Sie unter "Ersetzen des Central-TLS-Serverzertifikats" auf Seite 39.

Die Central-Ports werden während der Installation durch den Administrator definiert.

Kanalsicherheit

HPE OO unterstützt die folgenden sicheren Kanäle:

Kanal (Gerichtet)	Unterstütztes sicheres Protokoll
OOSH, Browser, Studio Remote Debugger oder RAS → Central	Für einen sicheren Kanal verwenden Sie die TLS-Kommunikation für die Verschlüsselung und das Clientzertifikat für die Authentifizierung.
Central → LDAP-Server	Zum Verschlüsseln der Kommunikation zwischen Central und LDAP verwenden Sie Secure LDAP mit dem Protokoll TLS.

RAS-Sicherheit

In einer Topologie mit einem Reverse RAS (der darauf wartet, dass Central die Verbindung initiiert) sorgt der folgende Mechanismus für den Schutz der Sicherheit des RAS:

- Wenn mehrere aufeinander folgende Verbindungsversuche fehlschlagen (weil der falsche geheime Schlüssel für gemeinsame Nutzung eingegeben wurde), kommt es zu einer Verzögerung.

Informationen zu Reverse RAS-Instanzen finden Sie unter "Einrichten der Topologie – Worker und RAS-Instanzen" im *HPE OO Central-Benutzerhandbuch*.

Sicherheit der Administrationsschnittstelle

Zugriff auf die Administrationsschnittstelle

Für die Steuerung des Zugriffs auf die Administrationsschnittstelle gibt es mehrere Möglichkeiten:

- Anmeldeinformationen
- Clientzertifikat
- SAML

Sichern der Administrationsschnittstelle - Empfehlungen

1. Es wird empfohlen, die Authentifizierung in Central zu aktivieren.

   Weitere Informationen finden Sie unter "Aktivieren der Authentifizierung" im *HPE OO Central-Benutzerhandbuch*

2. Es wird empfohlen, die Administrationsschnittstelle mit dem Protokoll TLS zu sichern. Sie sollten TLS zwischen dem Client und der Central-Schnittstelle für die Verschlüsselung einrichten.

   Weitere Informationen finden Sie unter "Arbeiten mit Server- und Clientzertifikaten" auf Seite 38.

3. Es wird empfohlen, mit LDAP-Benutzern statt mit internen Benutzern zu arbeiten, da dies sicherer ist.

4. Es wird empfohlen, die Authentifizierung für den Zugriff auf Central über Clientzertifikate einzurichten. Dies ist sicherer als Benutzerkennwörter.

   Weitere Informationen finden Sie unter "Arbeiten mit Server- und Clientzertifikaten" auf Seite 38.

Verwaltung und Authentifizierung von Benutzern

Authentifizierungsmodell

Um das einfache Bootstrapping der Authentifizierungsmechanismen in HPE OO zu ermöglichen, wird das Produkt mit deaktivierter Authentifizierung gestartet.

Es wird dringend empfohlen, sofort nach der Installation die Authentifizierung zu aktivieren.

Informationen zum Aktivieren der Authentifizierung finden Sie unter "Aktivieren der Authentifizierung" im *HPE OO Central-Benutzerhandbuch*.

Zum Authentifizieren des Zugriffs auf Central gibt es mehrere Möglichkeiten.

Wählen Sie die Methode zum Identifizieren der Benutzer:

- Benutzername und Kennwort
- Clientzertifikat
- SAML-Token
- Single Sign On (HPE LWSSO)

Wählen Sie eine der zwei Methoden zum Verwalten der Benutzer:

- LDAP-Benutzer, gespeichert auf einem LDAP-Server als Active Directory (empfohlen)
- Interne Benutzer und Kennwörter, lokal gespeichert auf dem Central-Server (nicht empfohlen)

Benutzertypen

Benutzern unterschiedlicher Typen können unterschiedliche Berechtigungen zugewiesen werden. Zum Beispiel Flow-Autor, Administrator, Systemadministrator usw.

Weitere Beispiele für die unterschiedlichen Benutzertypen finden Sie unter "Die wichtigsten Personas" im *OO-Konzepthandbuch*.

Verwaltung und Konfiguration der Authentifizierung

Interne oder LDAP-Benutzer

Sie können interne Benutzer mit Kennwörtern in der Central-Benutzeroberfläche einrichten oder die Benutzer im LDAP-Server definieren und LDAP-Gruppen zu Central-Rollen zuordnen.

Hinweis: Es wird empfohlen, interne Benutzer nicht zu verwenden, aber stattdessen eine sicherere Alternative, wie zum Beispiel LDAP-Benutzer, zu verwenden.

Informationen zum Konfigurieren von internen Benutzern finden Sie unter "Einrichten der Sicherheitseinstellungen – Interne Benutzer" im *OO Central-Benutzerhandbuch*.

Informationen zum Zuordnen von LDAP-Gruppen zu Central-Rollen finden Sie unter "Einrichten der Sicherheitseinstellungen – LDAP-Authentifizierung" im *OO Central-Benutzerhandbuch* und unter "LDAP-Konfiguration" im *OO API Guide*.

SAML / Clientzertifikate / LW SSO

Informationen zum Konfigurieren von Central für die Arbeit mit SAML finden Sie unter "Einrichten der Sicherheitseinstellungen – SAML" im *OO Central-Benutzerhandbuch*.

Informationen zum Konfigurieren von Central für die Arbeit mit Clientzertifikaten finden Sie unter "Arbeiten mit Server- und Clientzertifikaten" auf Seite 38.

Informationen zum Konfigurieren von Central für die Arbeit mit LW SSO finden Sie unter "Einrichten der Sicherheitseinstellungen – LWSSO" im *OO Central-Benutzerhandbuch*, unter "Konfigurieren der LWSSO-Einstellungen" im *OO Administration Guide* und unter "LW SSO" im *OO API Guide*

Datenbankauthentifizierung

OO unterstützt vier Datenbanken: Oracle, MS SQL, MySQL und Postgres.

Wir empfehlen die Verwendung eines sicheren Datenbankkennwortes für die Datenbankauthentifizierung und die Verwendung einer Richtlinie für sichere Kennwörter. Zum Beispiel das Blocken nach einer bestimmten Anzahl fehlgeschlagener Versuche.

Bei Verwendung von MS SQL ist es möglich, entweder mit Datenbankauthentifizierung oder mit Betriebssystemauthentifizierung zu arbeiten. Es wird empfohlen, möglichst mit Betriebssystemauthentifizierung zu arbeiten. Zum Beispiel ist es möglich, die Windows-Authentifizierung für den Zugriff auf Microsoft SQL Server-Datenbanken zu verwenden.

- Informationen zum Einrichten der Betriebssystemauthentifizierung finden Sie unter "Konfigurieren von OO für die Verwendung der Windows-Authentifizierung" im *HPE OO-Datenbankhandbuch*.
- Siehe "Ändern des Datenbankkennworts" im *HPE OO Administration Guide*.
- Siehe die durch den Datenbankanbieter empfohlenen Best Practices (sofern vorhanden).

Autorisierung

Autorisierungsmodell

Der Benutzerzugriff auf HPE OO-Ressourcen wird auf Basis der Rolle des Benutzers und der für diese Rolle konfigurierten Berechtigungen autorisiert.

Weitere Informationen finden Sie unter:

- "Einrichten der Sicherheitseinstellungen – Rollen" im *HPE OO Central-Benutzerhandbuch*
- "Zuweisen von Berechtigungen zu einem Systemkonto" im *HPE OO Central-Benutzerhandbuch*

Richtlinien für Minimalberechtigungen

Es wird empfohlen, wie folgt zu verfahren:

- Wählen Sie die geeigneten Berechtigungen für die Rolle aus.
- Verwenden Sie Minimalberechtigungen beim Erstellen von neuen Rollen.
- Erteilen Sie Minimalberechtigungen und erweitern Sie die Berechtigungen nur nach Bedarf, um eine unerwünschte Eskalation der Berechtigungen zu vermeiden. Beginnen Sie zum Beispiel mit Berechtigungen zum Anzeigen und fügen Sie zusätzliche Berechtigungen nach Bedarf individuell hinzu.

Autorisierungskonfiguration

Central wird mit einigen vordefinierten Rollen installiert, die Sie konfigurieren und Benutzern zuweisen können. Standardmäßig sind den vordefinierten Rollen die folgenden Berechtigungen zugewiesen:

Rolle	Standardberechtigungen
Administrator	Alle
End_user	Keine
Everybody	Keine
Promoter	Alle **Content**-Berechtigungen
System_admin	Alle **System**-Berechtigungen

Standardrolle

Es ist möglich, eine der Rollen mit dem Attribut **Standardrolle** zu konfigurieren. Wenn Sie dies tun, sollten Sie diese Rolle mit den Mindestberechtigungen ausstatten. Wenn Sie dieser Rolle Berechtigungen erteilen, müssen Sie immer daran denken, dass sich dies nicht nur auf die Benutzer auswirkt, denen die Rolle explizit zugewiesen wurde, sondern auf alle LDAP-Benutzer.

Weitere Informationen finden Sie im Abschnitt "Festlegen einer Rolle als Standardrolle" unter "Einrichten der Sicherheitseinstellungen – Rollen" im *HPE OO-Central-Benutzerhandbuch*.

Siehe auch:

- "Zuweisen von Berechtigungen zu einem Systemkonto" im *HPE OO Central-Benutzerhandbuch*
- "Festlegen der Berechtigungen für Inhalte" im *HPE OO Central-Benutzerhandbuch*

Zugriff auf Arbeitsbereiche in Studio

Wenn mehrere Arbeitsbereiche in Studio erstellt werden, sollte ein Arbeitsbereich immer unter Ordnern erstellt werden, für die nur der erstellende Benutzer Lese- und Schreibberechtigungen besitzt.

Da Arbeitsbereiche, die unter öffentlichen Ordnern erstellt wurden, möglicherweise für alle Benutzer zugänglich sind, könnten Sie nicht verhindern, dass sensible Informationen in ihnen manipuliert und weitergegeben werden.

Sicherung

Um Datenverlust zu verhindern, wird dringend empfohlen, dass Sie Ihre Daten auf den Servern regelmäßig auf sicheren Medien sichern. Dies ist auch für die Notfallwiederherstellung und den unterbrechungsfreien Geschäftsablauf nützlich.

Erstellen Sie nach der Installation von OO eine Sicherung des Ordners **central\var\security** und der Datei **central\conf\database.properties**.

Bestimmte Daten im Datenbankschema werden verschlüsselt und die Schlüssel für die Entschlüsselung werden lokal auf dem OO Central-Server gespeichert. Wenn diese Systemdateien beschädigt oder gelöscht werden, ist das Schema nutzlos, da es keine Möglichkeit mehr gibt, die Daten zu entschlüsseln.

Hinweis: Da die Schlüssel verschlüsselt sind, ist es wichtig, auch sie in die Sicherung einzuschließen. Die Schlüssel befinden sich im Ordner **security**.

Weitere Informationen finden Sie unter:

- "Backing Up OO" im *OO Administration Guide*
- "Setting up Disaster Recovery" im *OO Administration Guide*
- "Backing Up and Recovering the Central Security Files" im *OO Installation Guide*
- "Verwenden eines Load Balancers in der OO-Bereitstellung" im *OO-Architekturhandbuch*

Verschlüsselung

Verschlüsselungsmodell

HPE OO unterstützt Verschlüsselungs- und Hash-Algorithmen zum Schutz von sensitiven Daten. Durch Verschlüsselung soll die Offenlegung und Modifikation von sensitiven Daten, wie zum Beispiel Kennwörter, Definitionen usw., im HPE OO-System verhindert werden.

Es ist wichtig, dass bewährte Standardalgorithmen ohne bekannte Schwachstellen verwendet werden, um die Entschlüsselung durch unbefugte Personen zu verhindern.

Hinweis: Zum Beispiel wird SSL wegen bekannter Schwachstellen im SSL-Protokoll nicht verwendet.

Statische Daten

Alle gespeicherten Kennwörter werden mit bekannten Algorithmen geschützt, sodass keines davon Klartext bleibt.

Beispiel:

- Die Kennwörter der Systemkonten werden verschlüsselt.
- Die Kennwörter der internen Benutzer werden hash-verschlüsselt.
- Die Datenbankkennwörter werden verschlüsselt.

Daten beim Transport

OO verwendet das Protokoll Transport Layer Security (TLS), um die Daten zwischen Komponenten (wie zum Beispiel Central und RAS) zu verschlüsseln.

Deaktivieren des HTTP-Ports

Aus Sicherheitsgründen wird empfohlen, den HTTP-Port zu deaktivieren, sodass der einzige Kommunikationskanal TLS verwendet und verschlüsselt wird. Weitere Informationen finden Sie unter "Ändern der HTTP/HTTPS-Ports oder Deaktivieren des HTTP-Ports" auf Seite 50.

Verschlüsselungsverwaltung

Empfohlene Best Practices für die Verschlüsselung

Um höhere Niveaus der Sicherheit und Kryptographie zu erreichen, wird empfohlen, OO gemäß Federal Information Processing Standards (FIPS) 140-2 zu konfigurieren. OO kann auf Konformität mit FIPS 140-2 Stufe 1 festgelegt werden.

Standardkonfiguration

- Symmetrischer Schlüsselalgorithmus: AES mit Schlüsselgröße 128
- Hash-Algorithmus: SHA1

Erweiterte Einstellungen

Nachdem Sie die OO-Konfiguration an den FIPS 140-2-Standard angepasst haben, verwendet OO die folgenden Sicherheitsalgorithmen:

- Symmetrischer Schlüsselalgorithmus: AES256
- Hash-Algorithmus: SHA256

Weitere Informationen finden Sie unter "Konfigurieren der FIPS 140-2-Konformität von HPE OO" auf Seite 63.

Digitale Zertifikate

Ein digitales Zertifikat ist ein elektronisches "Kennwort" für eine Person, einen Server, eine Station usw.

- Um die Verschlüsselung zwischen einem Browser und dem Central-Server zu verwenden, müssen Sie ein digitales Zertifikate auf der Serverseite installieren.
- Um ein Clientzertifikat zum Authentifizieren des Central-Servers zu verwenden, müssen Sie ein Clientzertifikat auf der Clientseite (zum Beispiel Browser, RAS, OOSH, Studio usw.) installieren.

OO verwendet das Java-Dienstprogramm Keytool zur Verwaltung kryptografischer Schlüssel und vertrauenswürdiger Zertifikate. Dieses Dienstprogramm ist im Installationsordner von OO enthalten; Sie finden es unter **<Installationsverzeichnis>/java/bin/keytool**.

Speicherort für Zertifikate

Installationen von OO Central enthalten zwei Dateien für die Verwaltung von Zertifikaten mit Keytool:

- **<Installationsverzeichnis>/central/var/security/client.truststore**: Enthält die Liste der vertrauenswürdigen Zertifikate
- **<Installationsverzeichnis>/central/var/security/key.store**: Enthält das private OO-Zertifikat (mit dem privaten Schlüssel)

Steuerung des Zugriffs auf KeyStore und TrustStore

Es wird empfohlen, dass der TrustStore und KeyStore mit Leseberechtigungen nur für den Benutzer, der den Central-Dienst ausführt, gespeichert werden.

Ersetzen des selbstsignierten OO-Zertifikats

Es wird empfohlen, das selbstsignierte OO-Zertifikat im Anschluss an eine Neuinstallation von OO oder nach abgelaufener Gültigkeitsdauer Ihres aktuellen Zertifikats zu ersetzen.

Beim Ersetzen des Zertifikats muss mit Ihrer CA ein Zertifikat im PKCS12-Format generiert werden. Spezielle Details zum Zertifikatsprozess erfahren Sie bei Ihrer CA oder in Ihrer Unternehmensrichtlinie.

Weitere Informationen finden Sie unter "Ersetzen des Central-TLS-Serverzertifikats" auf Seite 39.

Hinzufügen von digitalen Signaturen zu einem Content Pack

Wenn ein Content Pack eine digitale Signatur einer vertrauenswürdigen CA enthält, bietet dies die Sicherheit, dass der Inhalt vertrauenswürdig ist.

Das Hinzufügen einer digitalen Signatur ist nicht unbedingt erforderlich.

- Die vordefinierten Content Packs von OO enthalten eine digitale Signatur von Verisign.
- Den Autoren von OO wird empfohlen, ihren benutzerdefinierten Content Packs eine digitale Signatur hinzuzufügen.
- Wenn ein signiertes Content Pack verletzt (z. B. verändert) worden ist, kann dieses Content Pack nicht bereitgestellt werden.
- Wenn die Signatur abgelaufen ist, wird vor der Bereitstellung eine Warnung angezeigt. Der Benutzer muss dann ein entsprechendes Kontrollkästchen aktivieren, um zu bestätigen, dass die abgelaufene Signatur ignoriert werden soll.

Seien Sie bei Content Packs, die nicht signiert sind, äußerst vorsichtig. Ein unsigniertes Content Pack ist nicht vertrauenswürdig und könnte Schadinhalte enthalten. Ein unsigniertes Content Pack könnte auch verletzt worden sein, indem die Signatur entfernt wurde.

Weitere Informationen zur digitalen Zertifizierung von Content Packs finden Sie unter "Bereitstellen und Verwalten von Content Packs" im *OO Central-Benutzerhandbuch*.

Sensitive Informationen in einem Content Pack

Kennwörter der Systemkonten

Kennwörter sollten beim Erstellen eines Content Pack nicht eingeschlossen werden. Die Kennwörter werden innerhalb des Content Pack verschlüsselt, was keine sichere Option ist.

Die Best Practice für die Sicherheit in OO besteht darin, die Kennwörter der Systemkonten in Central zu konfigurieren. Weitere Informationen finden Sie unter "Einrichten von Systemkonten für ein Content Pack" im *OO Central-Benutzerhandbuch*.

Audit und Protokolldateien

Audit

Das Audit ermöglicht das Verfolgen von Aktionen, die auf dem Central-Server stattfinden, z. B. Anmeldungen, das Auslösen von Flows, das Erstellen von Zeitplänen und das Bearbeiten von Konfigurationen. Anhand der Auditdaten können Sie die Benutzeraktivität auf dem Central-System verfolgen und damit nachverfolgen, wer wann welche Aktion ausgeführt hat. Zum Beispiel zeigt das Audit, dass ein Benutzer einen Flow ausgeführt, eine Konfiguration aktualisiert, einen Zeitplan gelöscht oder die Authentifizierung nicht erfolgreich durchgeführt hat.

Die Auditdaten werden in der Datenbank gespeichert. Weitere Informationen finden Sie unter "Auditing" im *HPE OO API Guide*.

Protokolle

Mit Protokollen können Sie Fehler-, Warn-, Informations- und Debugging-Meldungen aufzeichnen.

Die Protokolle werden im Dateiserver an den folgenden Positionen gespeichert:

- Central - **<OO-Installationsverzeichnis>/central/var/logs**
- Studio - **<Benutzer>/.oo/logs**
- RAS - **<OO-Installationsverzeichnis>/ras/var/logs**.

Keine sensitiven Daten in Auditdatensätzen und Protokolldateien

In den Auditdatensätzen und Protokolldateien im HPE OO-System werden keine sensitiven Daten gespeichert.

Abrufen von Auditdatensätzen

Die Auditdatensätze können Sie über API oder über eine Abfrage der Tabelle OO_AUDIT abrufen. Weitere Informationen finden Sie unter "Auditing" im *HPE OO API Guide*.

Beispiel für Auditdaten:

```
[
{
“time”:1412312016740, “type”:”AuditConfigurationChange”,
“group”:”AuditManagement”, “subject”:” mydomain\myuser2”, “outcome”:”Success”,
“data”:”{"enabled":false}”
},
```

```
{
“time”:1412312016722, “type”:”InternalUserDelete”, “group”:”Authentication-
Authorization”, “subject”:”mydomain\myuser2”, “outcome”:”Success”, “data”:
{"usersNames":["admin"]}"
}
]
```

APIs und Schnittstellen

API- und Schnittstellenmodell

Mit den öffentlichen Anwendungsprogrammierschnittstellen (Application Programming Interfaces, APIs) von HPE Operations Orchestration können Sie dieselben Aktionen wie über die HPE OO Central-Benutzeroberläche ausführen. Bestimmte Aktionen, wie zum Beispiel Bereinigung und Audit, können nur über APIs ausgeführt werden. Die öffentliche API ist HTTP-basiert. Alle APIs sind REST-konform und arbeiten mit JavaScript Object Notation.

Funktionen und Administration der Sicherheitskonfiguration von APIs und Schnittstellen

Es ist wichtig, dass mit den APIs sicher gearbeitet wird. Verwenden Sie bei der Arbeit mit den APIs die in diesem Handbuch beschriebenen Sicherheitsmechanismen (Authentifizierung, Verschlüsselung usw.).

Die API-Schnittstelle kann mit HTTP oder HTTPS arbeiten.

Hinweis: Wenn Sie unsere APIs zum Anzeigen von HTML verwenden, sind Sie für ihren Schutz vor XSS-Attacken selbst verantwortlich.

Weitere Informationen finden Sie in den folgenden Kapiteln im *HPE OO API Guide*:

- "LDAP Configuration"
- "Users"
- "LW SSO Configuration"
- "Authentication"
- "Roles"

Fragen und Antworten zum Thema Sicherheit

Wie kann ich eine Zertifikatsanforderung generieren, die durch eine externe CA signiert werden kann?

Exportieren Sie die Zertifikatsanforderung und senden Sie sie zum Signieren an die externe CA. Anweisungen hierzu finden Sie unter "Ersetzen des Central-TLS-Serverzertifikats" auf Seite 39.

Welche TCP/UDP-Ports werden durch HPE OO verwendet? Wie sieht es mit Richtung, Benutzer und Verschlüsselung aus?

Wenn Sie HPE OO installieren, müssen Sie mindestens einen verfügbaren Port für den Central Server in den HTTP/HTTPS-Feldern konfigurieren. Die standardmäßig bereitgestellten Werte sind 8080 und 8443. Sie können diese jedoch ändern. Weitere Informationen zu sicheren Kanälen zwischen Central und den anderen Komponenten finden Sie unter "Sicherheit von Netzwerk und Kommunikation" auf Seite 16

Wo und wie werden die Anmeldeinformationen (Admin-Konten, Integrationsbenutzer) gespeichert?

Weitere Informationen finden Sie unter "Verwaltung und Authentifizierung von Benutzern" auf Seite 19.

Wie konfiguriere ich selbstsignierte SSL-Zertifikate für Central/RAS/Studio?

Wenn Sie während der Installation von HPE OO kein Zertifikat angeben, wird standardmäßig ein selbstsigniertes Zertifikat erstellt. Aus Sicherheitsgründen wird jedoch nicht empfohlen, selbstsignierte Zertifikate zu verwenden. HPE empfiehlt die Verwendung eines Zertifikats von einer benutzerdefinierten Stammzertifizierungsstelle (CA) oder einer bekannten CA.

Weitere Informationen zum Konfigurieren von Zertifikaten für HPE OO finden Sie unter "Verschlüsseln der Kommunikation mit einem Serverzertifikat" auf Seite 39.

Wie aktiviere oder deaktiviere ich das Audit?

Standardmäßig ist das Audit nicht aktiviert. Informationen zum Aktivieren des Audit finden Sie unter "Aktivieren des Audit" im HPE OO Central-Benutzerhandbuch. Weitere Informationen zum Audit finden Sie unter "Audit und Protokolldateien" auf Seite 29.

Wie detailgenau sind die Protokolle und wie ändere ich den Umfang der Protokollierung?

Die Protokolle können auf unterschiedliche Granularitätsebenen eingestellt werden. Die Standardebene ist INFO. Sie können dies jedoch ändern. Weitere Informationen finden Sie unter "Anpassen der Protokollierungsebenen" im *HPE OO Administration Guide*.

Weitere Informationen zu Protokolldateien finden Sie unter "Audit und Protokolldateien" auf Seite 29.

Wie werden sensitive Informationen verschlüsselt?

Weitere Informationen finden Sie unter "Verschlüsselung" auf Seite 24.

Ist die Kommunikation zwischen Central und RAS verschlüsselt?

Wenn Sie HTTPS verwenden, wird sie verschlüsselt.

Ist die Kommunikation zwischen HPE OO und anderen Integrationskomponenten (HPNA, CSA, AD usw.) verschlüsselt?

Dies hängt von der Integration ab, die Sie verwenden. Wenn Sie HTTPS verwenden, wird sie verschlüsselt.

Wie kann ich den Zugriff auf die Flow-Bibliothek auf Basis der Benutzerrollen einschränken?

Siehe "Einrichten der Sicherheitseinstellungen – Rollen" im *HPE OO Central-Benutzerhandbuch*.

Welcher Authentifizierungsmechanismus wird durch OO unterstützt?

Die unterstützten Authentifizierungsmechanismen sind LDAP, SAML und interne Benutzer. HPE OO unterstützt auch Clientzertifikate und LWSSO. Weitere Informationen finden Sie unter "Verwaltung und Authentifizierung von Benutzern" auf Seite 19.

Ist HPE OO konform mit FIPS 140-2?

Ja. Weitere Informationen finden Sie unter "Konfigurieren der FIPS 140-2-Konformität von HPE OO" auf Seite 63.

Mit welchen Methoden erfolgt die Authentifizierung zwischen Central und RAS?

Benutzerkennwort oder Clientzertifikat.

Werden alle Kennwörter verschlüsselt oder hash-verschlüsselt gespeichert?

Ja. Alle gespeicherten Kennwörter werden mit bekannten Algorithmen geschützt, sodass keines davon Klartext bleibt.

Kann ich die Central-Benutzer-IP-Adresse beschränken?

Nein. Dies wird momentan nicht unterstützt.

Ist HPE OO nach allgemeinen Kriterien zertifiziert?

Dies ist in Bearbeitung. Wir sind gerade "in der Evaluierung". Weitere Informationen finden Sie unter https://www.cse-cst.gc.ca/en/canadian-common-criteria-scheme/publication/list/evaluation-product.

Wenn ich OOSH verwende, kann ich dann sensitive Daten an Central übergeben?

Es wird empfohlen, beim Herstellen einer Verbindung zu Central einen sicheren Kanal zu verwenden. Weitere Informationen finden Sie unter "Sicherheit von Netzwerk und Kommunikation" auf Seite 16.

Optimieren der Sicherheit von Operations Orchestration

In diesem Abschnitt wird die Konfiguration zum Optimieren der Sicherheit von Operations Orchestration beschrieben.

Empfehlungen zum Optimieren der Sicherheit 35
Arbeiten mit Server- und Clientzertifikaten 38
Verschlüsseln der Kommunikation mit einem Serverzertifikat 39
Clientzertifikatauthentifizierung (Gegenseitige Authentifizierung) 52
Konfigurieren der FIPS 140-2-Konformität Stufe 1 in HPE OO 60
Konfigurieren des TLS-Protokolls 68
Verhindern des Zugriffs durch Flows auf das lokale Dateisystem von Central/RAS 68

Hinweis: Informationen zu weiteren Verwaltungsaufgaben finden Sie im *OO Installation, Upgrade, and Configuration Guide*.

Empfehlungen zum Optimieren der Sicherheit

1. Installieren Sie die neueste Version von HPE OO. Weitere Informationen finden Sie im *OO Installation, Upgrade, and Configuration Guide*.
2. (Optional) Konfigurieren der FIPS 140-2-Konformität in OO Wenn Sie so vorgehen, muss die Konfiguration durchgeführt werden, bevor Sie den Central-Server starten. Weitere Informationen finden Sie unter "Konfigurieren der FIPS 140-2-Konformität Stufe 1 in HPE OO" auf Seite 60.
3. Konfigurieren Sie das Central-Serverzertifikat für die TLS-Verschlüsselung und das Clientzertifikat für die strikte Authentifizierung (gegenseitig).

   Hinweis: Dies kann während der Installation erfolgen.

Für RAS, Debugger und OOSH geben Sie, falls erforderlich, die Authentifizierung mit Zertifikat an (für das Serverzertifikat) und verwenden das Clientzertifikat für die Authentifizierung bei Central. Weitere Informationen finden Sie unter "Arbeiten mit Server- und Clientzertifikaten" auf Seite 38.

4. Sichern Sie den HPE OO Central-Server, indem Sie den HTTP-Port entfernen und die Kennwörter von KeyStore und TrustStore durch sichere Kennwörter ersetzen. Weitere Informationen finden Sie unter "Ändern der HTTP/HTTPS-Ports oder Deaktivieren des HTTP-Ports" auf Seite 50 und "Ändern und Verschlüsseln/Obfuskieren des KeyStore/TrustStore-Kennworts" auf Seite 45.
5. Sichern Sie HPE OO Studio, indem Sie die Kennwörter von KeyStore und TrustStore durch sichere Kennwörter ersetzen und die Kennwörter in den Konfigurationsdateien verschlüsseln oder verschleiern (obfuskieren). Weitere Informationen finden Sie unter "Ändern und Verschlüsseln/Obfuskieren des KeyStore/TrustStore-Kennworts" auf Seite 45.
6. Entfernen der RC4-Verschlüsselung aus den unterstützten SSL-Verschlüsselungsverfahren Weitere Informationen finden Sie unter "Entfernen der RC4-Verschlüsselung aus den unterstützten SSL-Verschlüsselungsverfahren" auf Seite 49.
7. (Optional) Konfigurieren der TLS-Protokollversion. Weitere Informationen finden Sie unter "Konfigurieren des TLS-Protokolls" auf Seite 68.
8. Aktivieren Sie die Authentifizierung in Central. Weitere Informationen finden Sie unter "Aktivieren der Authentifizierung" im *OO Central-Benutzerhandbuch*.

   Da interne Benutzer nicht gesichert sind, sollten Sie ein sicheres LDAP mit einer sicheren Kennwortrichtlinie verwenden. Weitere Informationen finden Sie unter "Einrichten der Sicherheitseinstellungen – LDAP-Authentifizierung" im *OO Central-Benutzerhandbuch*.
9. Sichern Sie das Betriebssystem und die Datenbank.
10. Fügen Sie ein Sicherheitsbanner mit einer aussagekräftigen Meldung hinzu. Beispiel: "Sie melden sich nun bei unserer PRODUKTIONSUMGEBUNG an! Fahren Sie nur fort, wenn Sie mit den Governance-Regeln für dieses System vertraut sind und die erforderlichen Schulungen absolviert haben." Weitere Informationen finden Sie unter "Konfigurieren eines Sicherheitsbanners" im *OO Central-Benutzerhandbuch*.
11. In der Windows- und SQL-Serverumgebung konfigurieren Sie OO für die Verwendung der Windows-Authentifizierung. Weitere Informationen finden Sie unter "Konfigurieren von OO für die Verwendung der Windows-Authentifizierung" im *OO-Datenbankhandbuch*.
12. Stellen Sie sicher, dass das Audit in Central aktiviert ist. Weitere Informationen finden Sie unter "Aktivieren des Audit" im *OO Central-Benutzerhandbuch*.

Standard-Sicherheitseinstellungen

Oftmals ist es ratsam, die voreingestellten Standard-Sicherheitseinstellungen den Anforderungen entsprechend anzupassen.

- **Authentifizierung** – In Central ist diese Option standardmäßig nicht aktiviert. Es wird empfohlen, die Option zu aktivieren, sobald Benutzer eingerichtet wurden. Weitere Informationen finden Sie unter "Aktivieren der Authentifizierung" im *HPE OO-Central-Benutzerhandbuch*.
- **Audit** – In Central ist diese Option standardmäßig nicht aktiviert. Es wird empfohlen, die Option zu aktivieren. Weitere Informationen finden Sie unter "Aktivieren des Audit" im *HPE OO-Central-Benutzerhandbuch*.
- **TLS-Verschlüsselung** – Standardmäßig unterstützt HPE OO drei TLS-Protokolle: 1.0, 1.1, 1.2. Es wird empfohlen, mit der neuesten Version zu arbeiten. Weitere Informationen finden Sie unter "Konfigurieren des TLS-Protokolls" auf Seite 68.
- **TLS-Serverzertifikat** – Standardmäßig wird der Benutzer während der Installation von OO Server aufgefordert, ein CA-Zertifikat anzugeben.
- **Clientzertifikat** – Diese Option ist standardmäßig nicht aktiviert. Für die Authentifizierung bei Central wird empfohlen, mit Clientzertifikat zu arbeiten. Weitere Informationen finden Sie unter "Konfigurieren der Clientzertifikatauthentifizierung in Central" auf Seite 52.
- **Kennwörter für KeyStore, TrustStore und das Serverzertifikat** – Standardmäßig werden die Java-Kennwörter für keyStore, trustStore und das Serverzertifikat bereitgestellt. Es wird empfohlen, diese durch verschlüsselte Kennwörter zu ersetzen. Weitere Informationen finden Sie unter "Ändern und Verschlüsseln/Obfuskieren des KeyStore/TrustStore-Kennworts" auf Seite 45.
- **RC4-Verschlüsselung** – Die RC4-Verschlüsselung ist standardmäßig aktiviert. Auf JRE-Ebene sollte die RC4-Verschlüsselung jedoch deaktiviert werden. Weitere Informationen finden Sie unter "Entfernen der RC4-Verschlüsselung aus den unterstützten SSL-Verschlüsselungsverfahren" auf Seite 49.
- **Sicherheitsbanner** – In Central ist diese Option standardmäßig nicht aktiviert. Es wird empfohlen, die Option mit Ihrer benutzerdefinierten Meldung zu aktivieren. Weitere Informationen finden Sie unter "Konfigurieren eines Sicherheitsbanners" im *HPE OO-Central-Benutzerhandbuch*.
- **Windows-Authentifizierung der Datenbank** – In Central ist diese Option standardmäßig nicht aktiviert. Falls Sie mit der Windows- und SQL-Serverumgebung arbeiten, sollten Sie HPE OO für die Verwendung der Windows-Authentifizierung konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von HPE OO für die Verwendung der Windows-Authentifizierung" im *HPE OO-Datenbankhandbuch*.

- **Standard-Algorithmen** – Die Datei **encryption.properties** enthält die Standard-Algorithmen. Falls Sie den FIPS-Standard erfüllen möchten, finden Sie die Informationen hierzu unter "Konfigurieren der FIPS 140-2-Konformität Stufe 1 in HPE OO" auf Seite 60. Weitere Informationen zu den Standards der FIPS 140-2-Konformität Stufe 1 finden Sie unter "Verschlüsselung" auf Seite 24 im Abschnitt "Verschlüsselungsverwaltung".
- **Java-Richtlinie** – Die Datei **java.policy** ist nicht verschlüsselt. Informationen zum Anpassen der Datei **java.policy** finden Sie unter "Verhindern des Zugriffs durch Flows auf das lokale Dateisystem von Central/RAS" auf Seite 68.

Arbeiten mit Server- und Clientzertifikaten

TLS-Zertifikate (Transport Layer Security) binden einen kryptografischen Schlüssel digital an die Details einer Organisation und ermöglichen so sichere und verschlüsselte Verbindungen zwischen einem Webserver und einem Browser.

HPE OO verwendet das Dienstprogramm Keytool zur Verwaltung kryptografischer Schlüssel und vertrauenswürdiger Zertifikate. Dieses Dienstprogramm ist im HPE OO-Installationsordner enthalten. Sie finden es unter **<Installationsverzeichnis>/java/bin/keytool**. Weitere Informationen zum Dienstprogramm Keytool finden Sie unter http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html.

Hinweis: Keytool ist ein Open Source-Dienstprogramm.

Installationen von HPE OO Central enthalten zwei Dateien für die Verwaltung von Zertifikaten:

- **<Installationsverzeichnis>/central/var/security/client.truststore**: Enthält die Liste der vertrauenswürdigen Zertifikate.
- **<Installationsverzeichnis>/central/var/security/key.store**: Enthält das HPE OO-Zertifikat (privater Schlüssel).

Empfehlungen:

- Es wird empfohlen, das selbstsignierte HPE OO-Zertifikat im Anschluss an eine Neuinstallation von HPE OO oder nach abgelaufener Gültigkeitsdauer Ihres aktuellen Zertifikats zu ersetzen.
- Es wird empfohlen, den TrustStore und KeyStore mit Leseberechtigungen nur für den Benutzer, der den Central-Dienst ausführt, zu speichern.
- Es wird empfohlen, den Inhalt der Konsole nach der Verwendung von Keytool zu löschen oder die Eingabeaufforderung für Kennworteingaben zu verwenden.

Verschlüsseln der Kommunikation mit einem Serverzertifikat

Ersetzen des Central-TLS-Serverzertifikats 39
Importieren eines CA-Stammzertifikats in den Central-TrustStore 41
Importieren eines CA-Stammzertifikats in einen RAS-TrustStore 41
Importieren eines CA-Stammzertifikats in den OOSH-TrustStore 43
Importieren eines CA-Stammzertifikats in den Studio-TrustStore 44
Ändern und Verschlüsseln/Obfuskieren des KeyStore/TrustStore-Kennworts 45
Entfernen der RC4-Verschlüsselung aus den unterstützten SSL-Verschlüsselungsverfahren 49
Ändern der HTTP/HTTPS-Ports oder Deaktivieren des HTTP-Ports 50
Fehlerbehebung 52

Ersetzen des Central-TLS-Serverzertifikats

Sie können ein von einer bekannten Zertifizierungsstelle signiertes Zertifikat oder ein benutzerdefiniertes Serverzertifikat von einer lokalen Zertifizierungsstelle verwenden.

Ersetzen Sie die in <Gelb> hervorgehobenen Parameter, um sie auf den Speicherort der Datei **key.store** und andere Details auf Ihrem Computer abzustimmen.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Beenden Sie Central und sichern Sie die **key.store**-Originaldatei, die sich im Ordner **<Installationsverzeichnis>/central/var/security** befindet.
2. Öffnen Sie eine Befehlszeile im Ordner **<Installationsverzeichnis>/central/var/security**.
3. Löschen Sie das vorhandene Serverzertifikat aus der Datei **key.store**, indem Sie den folgenden Befehl eingeben:

   ```
   keytool -delete -alias tomcat -keystore key.store -storepass changeit
   ```

4. Wenn Sie bereits ein Zertifikat mit der Erweiterung **.pfx** oder **.p12** besitzen, fahren Sie mit dem nächsten Schritt fort. Sollte dies nicht der Fall sein, müssen Sie das Zertifikat mit dem privaten

Schlüssel in das PKCS12-Format (.pfx, .p12) exportieren. Beispiel: Das Zertifikat liegt im Format PEM vor:

```
>openssl pkcs12 –export –in <cert.pem> -inkey <.key> -out <certificate name>.p12 –name <name>
```

Wenn das Zertifikat im Format DER vorliegt, fügen Sie den Parameter `-inform DER` hinter **pkcs12** an. Beispiel:

```
>openssl pkcs12 –inform DER –export –in <cert.pem> -inkey <.key> -out <certificate name>.p12 –name <name>
```

Hinweis:

Um das Zertifikat im PKCS12-Format zu generieren, müssen Sie Ihre CA verwenden. Da dieser Schritt je nach CA-Anbieter und -Richtlinie variieren kann, sollten Sie Ihre CA um eine detaillierte Erläuterung des Zertifikatgenerierungsprozesses bitten.

Hinweis: Notieren Sie sich das Kennwort, das Sie angeben. Sie benötigen dieses Kennwort für den privaten Schlüssel bei der späteren Eingabe der Passphrase für den Keystore.

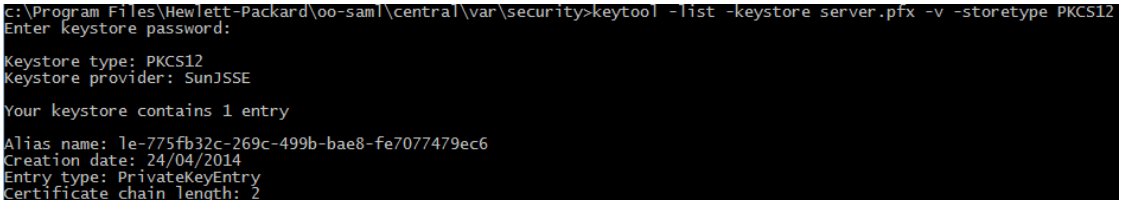
Stellen Sie sicher, dass Sie ein sicheres Kennwort wählen.

5. Listen Sie mit dem folgenden Befehl den Alias für den Alias Ihres Zertifikats auf:

   ```
   keytool -list -keystore <certificate_name> -v -storetype PKCS12
   ```

   Der Alias des Zertifikats wird angezeigt und sollte im nächsten Befehls angegeben werden.

   Im folgenden Beispiel ist dies die vierte Zeile von unten.

6. Importieren Sie mit dem folgenden Befehl das Serverzertifikat im PKCS12-Format in die Central-Datei **key.store**:

   ```
   keytool -importkeystore -srckeystore <PKCS12 format certificate path> -destkeystore key.store -srcstoretype pkcs12 -deststoretype JKS -alias <cert alias> -destalias tomcat
   ```

7. Wenn das importierte Serverzertifikat ein anderes Kennwort besitzt als das ursprüngliche

Serverzertifikat, ist es wichtig, das in keyPass angegebene Kennwort zu ändern. Folgen Sie den Anweisungen unter "Ändern und Verschlüsseln/Obfuskieren des KeyStore/TrustStore-Kennworts" auf Seite 45.

Es wird empfohlen, das Standardkennwort “changeit” im automatisch generierten Keystore des Central-Servers zu ändern. Weitere Informationen finden Sie unter "Ändern und Verschlüsseln/Obfuskieren des KeyStore/TrustStore-Kennworts" auf Seite 45.

8. Starten Sie Central.

Importieren eines CA-Stammzertifikats in den Central-TrustStore

Wenn Sie ein benutzerdefiniertes Stammzertifikat für Central verwenden, müssen Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die Datei **client.truststore** importieren. Wenn Sie eine bekannte Stamm-CA (wie Verisign) verwenden, müssen Sie das folgende Verfahren nicht durchführen, da das Zertifikat bereits in der Datei **Client.truststore** vorhanden ist.

Standardmäßig unterstützt HPE OO alle selbstsignierten Zertifikate. Allerdings ist es in einer Produktionsumgebung ratsam, diese Standardeinstellung aus Sicherheitsgründen in eine benutzerdefinierte CA oder eine bekannte CA zu ändern.

Ersetzen Sie die in <Gelb> hervorgehobenen Parameter.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Beenden Sie Central und sichern Sie die **client.truststore**-Originaldatei, die sich im Ordner **<Installationsverzeichnis>/central/var/security** befindet.
2. Importieren Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die Central-Datei **Client.truststore**, wenn sie noch nicht in der CA-Liste vorhanden ist (dort befinden sich standardmäßig alle bekannten CAs):

   ```
   keytool -importcert -alias <any_alias> -keystore <path to the client.truststore> -file <certificate_name.cer> -storepass <changeit>
   ```

3. Starten Sie Central.

Importieren eines CA-Stammzertifikats in einen RAS-TrustStore

Wenn Sie ein benutzerdefiniertes Stammzertifikat für Central verwenden und dieses Stammzertifikat bei der RAS-Installation nicht angegeben haben, müssen Sie nach der Installation eines RAS die vertrauenswürdige Stammzertifizierungsstelle (CA) in die RAS-Datei **client.truststore** importieren.

Wenn Sie eine bekannte Stamm-CA (wie Verisign) verwenden, müssen Sie das folgende Verfahren nicht durchführen, da das Zertifikat bereits in der Datei **Client.truststore** vorhanden ist.

Standardmäßig unterstützt HPE OO alle selbstsignierten Zertifikate. Allerdings ist es in einer Produktionsumgebung ratsam, diese Standardeinstellung aus Sicherheitsgründen in eine benutzerdefinierte CA oder eine bekannte CA zu ändern.

Ersetzen Sie die in <Gelb> hervorgehobenen Parameter.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Beenden Sie RAS und sichern Sie die **client.truststore**-Originaldatei, die sich im Ordner **<Installationsverzeichnis>/ras/var/security** befindet.
2. Öffnen Sie eine Befehlszeile im Ordner **<Installationsverzeichnis>/ras/var/security**.
3. Öffnen Sie die Datei **<Installationsverzeichnis>/ras/conf/ras-wrapper.conf** und stellen Sie sicher, dass `-Dssl.support-self-signed` auf den Wert **false** festgelegt ist. Dies aktiviert die vertrauenswürdige Zertifizierungsstelle (CA).

   Beispiel:

   ```
   wrapper.java.additional.<x>=-Dssl.support-self-signed=false
   ```

4. Öffnen Sie die Datei **<Installationsverzeichnis>/ras/conf/ras-wrapper.conf** und stellen Sie sicher, dass `-Dssl.verifyHostName` auf **true** festgelegt ist. Hiermit wird geprüft, ob der FQDN im Zertifikat mit dem FQDN der Anforderung übereinstimmt.

   Beispiel:

   ```
   wrapper.java.additional.<x>=-Dssl.verifyHostName=true
   ```

   Hinweis: Diese Eigenschaft ist standardmäßig auf **true** festgelegt.

5. Importieren Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die RAS-Datei **Client.truststore**, wenn sie noch nicht in der CA-Liste vorhanden ist (dort befinden sich standardmäßig alle bekannten CAs):

   ```
   keytool -importcert -alias <any_alias> -keystore <path to the
   client.truststore> -file <certificate_name.cer> -storepass <changeit>
   ```

6. Starten Sie den RAS.

Importieren eines CA-Stammzertifikats in den OOSH-TrustStore

Wenn Sie ein benutzerdefiniertes Stammzertifikat für Central verwenden, müssen Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die OOSH-Datei **client.truststore** importieren. Wenn Sie eine bekannte Stamm-CA (wie Verisign) verwenden, müssen Sie das folgende Verfahren nicht durchführen, da das Zertifikat bereits in der Datei **Client.truststore** vorhanden ist.

Standardmäßig unterstützt HPE OO alle selbstsignierten Zertifikate. Allerdings ist es in einer Produktionsumgebung ratsam, diese Standardeinstellung aus Sicherheitsgründen in eine benutzerdefinierte CA oder eine bekannte CA zu ändern.

Ersetzen Sie die in <Gelb> hervorgehobenen Parameter.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Beenden Sie Central und sichern Sie die **client.truststore**-Originaldatei, die sich im Ordner **<Installationsverzeichnis>/central/var/security** befindet.
2. Bearbeiten Sie die Datei **oosh.bat** im Ordner **<Installationsverzeichnis>/central/bin**.
3. Stellen Sie sicher, dass `-Dssl.support-self-signed` auf den Wert **false** festgelegt ist. Dies aktiviert die vertrauenswürdige Zertifizierungsstelle (CA).

   Beispiel:

   ```
   -Dssl.support-self-signed=false
   ```

4. Stellen Sie sicher, dass `-Dssl.verifyHostName` auf **true** festgelegt ist. Hiermit wird geprüft, ob der FQDN im Zertifikat mit dem FQDN der Anforderung übereinstimmt.

   Beispiel:

   ```
   -Dssl.verifyHostName=true
   ```

   Hinweis: Diese Eigenschaft ist standardmäßig auf **true** festgelegt.

5. Importieren Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die Central-Datei **Client.truststore**, wenn sie noch nicht in der CA-Liste vorhanden ist (dort befinden sich standardmäßig alle bekannten CAs):

   ```
   keytool -importcert -alias <any_alias> -keystore <path to the client.truststore> -file <certificate_name.cer> -storepass <changeit>
   ```

6. Führen Sie OOSH aus.
7. Starten Sie Central.

Importieren eines CA-Stammzertifikats in den Studio-TrustStore

Wenn Sie benutzerdefinierte Zertifikate auf den Central-, SVN- oder GIT-Servern verwenden, müssen Sie, damit Studio mit ihnen arbeiten kann, die vertrauenswürdige Stammzertifizierungsstelle (CA) in die Studio-Datei **client.truststore** importieren. Wenn Sie eine bekannte Stamm-CA (wie Verisign) verwenden, müssen Sie das folgende Verfahren nicht durchführen, da das Zertifikat bereits in der Datei **Client.truststore** vorhanden ist.

Standardmäßig unterstützt HPE OO alle selbstsignierten Zertifikate. Allerdings ist es in einer Produktionsumgebung ratsam, diese Standardeinstellung aus Sicherheitsgründen in eine benutzerdefinierte CA oder eine bekannte CA zu ändern.

Bei einem neuen **.oo**-Ordner kopiert Studio die Datei **client.truststore** aus **<Installationsverzeichnis>/studio/var/security** in den Ordner **<Benutzer>/.oo**. Dies ist eine einmalige Aktion um sicherzustellen, dass Studio Zertifikate automatisch importieren kann (zum Beispiel für Studio Remote Debugger). Studio verwendet dann diese Datei als **client.truststore**, sofern sie vorhanden ist. Andernfalls wird die aus der Studio-Installation verwendet (**<Installationsverzeichnis>/studio/var/security/client.truststore**).

Nach einem Upgrade auf 10.5x oder höher befindet sich der TrustStore im Ordner **<Benutzer>/.oo**.

Wenn Sie ein Zertifikat manuell importieren möchten, können Sie sie entweder in **.oo/client.truststore** oder in **client.truststore** im Studio-Installationsordner importieren.

Wenn Sie mehrere Arbeitsbereiche verwenden, gelten die Änderungen, die an der Datei **client.truststore** im Ordner **.oo** vorgenommen wurden, nur für den jeweiligen Arbeitsbereich. Um die Änderung auf alle neu erstellten Arbeitsbereiche anzuwenden, müssen Sie die Datei **client.truststore** im Studio-Installationsordner bearbeiten.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Schließen Sie Studio und sichern Sie die **client.truststore**-Originaldatei, die sich in **<Benutzer>/.oo** befindet.

   Beispiel: **C:/Users/<Benutzername>/.oo**
2. Bearbeiten Sie die Datei **Studio.l4j.ini** im Ordner **<Installationsverzeichnis>/studio**.

3. Stellen Sie sicher, dass `-Dssl.support-self-signed` auf den Wert **false** festgelegt ist. Dies aktiviert die vertrauenswürdige Zertifizierungsstelle (CA).

   Beispiel:

   ```
   -Dssl.support-self-signed=false
   ```

4. Stellen Sie sicher, dass `-Dssl.verifyHostName` auf **true** festgelegt ist. Hiermit wird geprüft, ob der FQDN im Zertifikat mit dem FQDN der Anforderung übereinstimmt.

   Beispiel:

   ```
   -Dssl.verifyHostName=true
   ```

5. Importieren Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die Studio-Datei **Client.truststore**, wenn sie noch nicht in der CA-Liste vorhanden ist (dort befinden sich standardmäßig alle bekannten CAs). Ersetzen Sie die in <Gelb> hervorgehobenen Parameter:

   ```
   keytool -importcert -alias <any_alias> -keystore <path to the
   client.truststore> -file <certificate_name.cer> -storepass <changeit>
   ```

6. Starten Sie Studio.

Weitere Informationen finden Sie unter "Debuggen einer Remote-Instanz von Central mit Studio" im *Studio-Erstellungshandbuch*.

Ändern und Verschlüsseln/Obfuskieren des KeyStore/TrustStore-Kennworts

Ändern der Kennwörter für KeyStore, Truststore und Serverzertifikat in der Central-Konfiguration

1. Stellen Sie sicher, dass Central ausgeführt wird.

   Hinweis: Stellen Sie vor diesem Schritt sicher, dass verschlüsselte Kennwörter vorhanden sind. Informationen zum Verschlüsseln eines Kennworts finden Sie unter "Verschlüsseln von Kennwörtern" im *HPE OO Administration Guide*.

   Führen Sie in OOSH den folgenden Befehl aus:

   ```
   set-sys-config --key <keyName> --value <ecryptedPassword>
   ```

   Dabei ist `<keyName>` einer der Werte aus der folgenden Tabelle:

Konfigurationselement	Aktion
`key.store.password`	Zum Festlegen des Kennworts für den Zugriff auf **key.store**. Der Standardwert ist `"changeit"`. Dieser Wert muss dem für `keystorePass` in den nachfolgenden Schritten festgelegten Wert entsprechen.
`key.store.private.key.alias.password`	Zum Festlegen des Kennworts, das für den Zugriff auf das Serverzertifikat (privater Schlüssel) in **key.store** verwendet wird. Der Standardwert ist `"changeit"`. Dieser Wert muss dem für `keyPass` in den nachfolgenden Schritten festgelegten Wert entsprechen.

2. Beenden Sie den Central-Dienst.
3. Ändern Sie mit Keytool die Kennwörter für KeyStore, TrustStore und Serverzertifikat.

   Verwenden Sie den folgenden keytool-Befehl zum Ändern des KeyStore-Kennworts:

   ```
   keytool -storepasswd -keystore
   <installationsordner>/central/var/security/key.store
   ```

   Verwenden Sie den folgenden keytool-Befehl zum Ändern des Kennworts des privaten Schlüsseleintrags für das Serverzertifikat:

   ```
   keytool –keypasswd -alias tomcat -keystore
   <installationsordner>/central/var/security/key.store
   ```

   Verwenden Sie den folgenden keytool-Befehl zum Ändern des TrustStore-Kennworts:

   ```
   keytool -storepasswd -keystore
   <installationsordner>/central/var/security/client.truststore
   ```

4. Ändern Sie die Kennwörter auch in der Datei **Server.xml**, die sich im Ordner **<Installationsverzeichnis>/central/tomcat/conf** befindet.

   a. Suchen Sie den HTTPS-Connector. Beispiel:

   ```
   keyPass="changeit" keystoreFile="C:/Program Files/Hewlett-Packard/HP
   Operations Orchestration/central/var/security/key.store"
   keystorePass="changeit" keystoreType="JKS" maxThreads="200" port="8443"
   protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
   secure="true" sslProtocol="TLSv1.2"
   sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" truststoreFile="C:/Program
   Files/Hewlett-Packard/HP Operations
   ```

```
Orchestration/central/var/security/client.truststore"
truststorePass="changeit" truststoreType="JKS"/>
```

Ändern Sie das erforderliche Kennwort.

- `keyPass` – Das Kennwort für den Zugriff auf den privaten Schlüssel des Serverzertifikats in der angegebenen Keystore-Datei. Der Standardwert ist "`changeit`".
- `keystorePass` – Das Kennwort für den Zugriff auf die angegebene Keystore-Datei. Der Standardwert ist der Wert des Attributs `keyPass`.

  Hinweis: Es wird empfohlen, nicht das in **keyPass** angegebene Kennwort sondern ein anderes sicheres Kennwort zu verwenden.

- `truststorePass` - Das Kennwort für den Zugriff auf den Truststore (der alle vertrauenswürdigen CAs enthält). Der Standardwert ist der Wert der Systemeigenschaft **javax.net.ssl.trustStorePassword**. Wenn diese Eigenschaft null ist, wird kein TrustStore-Kennwort konfiguriert. Wird ein ungültiges TrustStore-Kennwort angegeben, wird eine Warnung protokolliert und ein Versuch unternommen, ohne Kennwort auf den TrustStore zuzugreifen; dabei wird die Überprüfung des TrustStore-Inhalts übersprungen.

b. Speichern Sie die Datei.

5. Bearbeiten Sie die Datei **central-wrapper.conf** im Ordner **<installationsverzeichnis>\central\conf\central** und ersetzen Sie das Kennwort des TrustStore durch das neue Kennwort in verschlüsselter oder obfuskierter Form. Beispiele:

   ```
   wrapper.java.additional.<x>=-Djavax.net.ssl.trustStorePassword={ENCRYPTED}
   <verschlüsseltes_Kennwort>
   ```

   ```
   wrapper.java.additional.<x>=-Djavax.net.ssl.trustStorePassword={OBFUSCATED}
   <obfuskiertes_Kennwort>
   ```

   Weitere Informationen zum Verschlüsseln oder Obfuskieren eines Kennworts finden Sie unter "Verschlüsseln und Obfuskieren von Kennwörtern" auf der nächsten Seite.

6. Starten Sie den Central-Dienst.

Ändern der TrustStore-Kennwörter für RAS, OOSH und Studio

Hinweis: Bevor Sie die folgenden Schritte ausführen, sollten Sie mit Keytool die Kennwörter für KeyStore, TrustStore und Serverzertifikat ändern.

- **So ändern Sie das TrustStore-Kennwort für eine eigenständige RAS-Instanz**: Bearbeiten Sie die Datei **ras-wrapper.conf** und ändern Sie das Kennwort des TrustStore.
- **So ändern Sie das TrustStore-Kennwort für OOSH**: Bearbeiten Sie die Datei **oosh.bat** und ändern Sie das Kennwort des TrustStore.
- **So ändern Sie das TrustStore-Kennwort für Studio**: Fügen Sie die Eigenschaft **client.truststore.password** mit dem Kennwort in verschleiertem Format zur Datei **Studio.properties** im Ordner **<Benutzer>/.oo** hinzu.

  ```
  client.truststore.password={OBFUSCATED}6L9+NqBjKYp5heuvMEzg0g==
  ```

  Wenn diese Eigenschaft nicht definiert wurde, greift Studio auf die Systemeigenschaft **javax.net.ssl.trustStorePassword** für das TrustStore-Kennwort zurück.

Weitere Informationen zum Verschlüsseln eines Kennworts finden Sie unter "Verschlüsseln und Obfuskieren von Kennwörtern" oben.

Verschlüsseln und Obfuskieren von Kennwörtern

Mit dem Skript `encrypt-password`, das sich in **<Installationsordner>/central/bin** befindet, können Sie Kennwörter verschlüsseln oder verschleiern.

Es wird empfohlen, die Verschlüsselung zu verwenden.

Wichtig! Löschen Sie nach der Verwendung des Skripts `encrypt-password` die Befehlshistorie.

Dies ist notwendig, da bei einem Linux-Betriebssystem der Kennwortparameter in Klartext unter **/$USER/.bash_history** gespeichert wird und über den Befehl `history` zugänglich ist.

Verschlüsseln von Kennwörtern

1. Suchen Sie das Skript `encrypt-password` in **<Installationsordner>/central/bin**.
2. Führen Sie das Skript mit der Option `-e -p <Kennwort>` aus, wobei `Kennwort` das Kennwort ist, das Sie verschlüsseln möchten.

   Hinweis: Sie können entweder `-p` als Flag zum Verschlüsseln des Kennwortes oder `--password` verwenden.

   Das verschlüsselte Kennwort sollte wie folgt aussehen:

   ```
   {ENCRYPTED}<some_chars>.
   ```

Obfuskieren von Kennwörtern

1. Suchen Sie das Skript `encrypt-password` in **<Installationsordner>/central/bin**.
2. Führen Sie das Skript mit der Option `-o <Kennwort>` aus, wobei `Kennwort` das Kennwort ist, das Sie verschleiern möchten.

   Das verschleierte Kennwort sollte wie folgt aussehen:

   ```
   {OBFUSCATED}<some_chars>.
   ```

Erstellen einer Eingabeaufforderung für das Kennwort

Es wird empfohlen, das Skript `encrypt-password` ohne das Argument `-p` auszuführen. Beispiel:

```
C:\Program Files\Hewlett-Packard\HP Operations Orchestration\central\bin>encrypt-password.bat
Password (typing will be hidden):
Confirm password (typing will be hidden):
{ENCRYPTED}gAkPCLQsYDhoR1Y2q9BjCQ==

C:\Program Files\Hewlett-Packard\HP Operations Orchestration\central\bin>
```

Damit wird eine Eingabeaufforderung für die ausgeblendeten Kennworteingaben erstellt.

Entfernen der RC4-Verschlüsselung aus den unterstützten SSL-Verschlüsselungsverfahren

Der Remotehost unterstützt die Verwendung der RC4-Verschlüsselung. Diese Verschlüsselung ist bei der Generierung eines pseudozufälligen Bytestroms fehlerhaft, sodass eine Vielzahl kleiner Verzerrungen in den Strom gelangt und die Zufälligkeit der Daten reduziert.

Wenn einfacher Text wiederholt verschlüsselt wird (Beispiel: HTTP-Cookies) und ein Angreifer imstande ist, viele (im zweistelligen Millionenbereich) verschlüsselte Texte in die Hände zu bekommen, kann er den Text möglicherweise entschlüsseln.

Deaktivieren Sie die RC4-Verschlüsselung auf der JRE-Ebene (beginnend mit Java 7):

1. Öffnen Sie die Datei **$JRE_HOME/lib/security/java.security**.
2. Deaktivieren Sie die RC4-Verschlüsselung, indem Sie die Kommentare entfernen und die Parameter entsprechend dem folgenden Beispiel ändern:

   ```
   jdk.certpath.disabledAlgorithms=RC4, MD2, RSA keySize < 1024
   ```

   ```
   jdk.tls.disabledAlgorithms=RC4, MD5, DSA, RSA keySize < 1024
   ```

3. Starten Sie den OO Central-Server neu.

Weitere Informationen finden Sie unter http://stackoverflow.com/questions/18589761/restict-cipher-suites-on-jre-level.

Hinweis: Nach einem Upgrade von einer früheren Version von HPE OO 10.x müssen Sie diese Schritte wiederholen.

Ändern der HTTP/HTTPS-Ports oder Deaktivieren des HTTP-Ports

Die Datei **Server.xml** im Verzeichnis **[OO_HOME]/central/tomcat/conf** enthält zwei **<Connector>**-Elemente unter dem Element **<Service>**. Diese Connector definieren oder aktivieren die Ports, die der Server überwacht.

Jede Connector-Konfiguration wird anhand von zugehörigen Attributen definiert. Der erste Connector definiert einen Standard-HTTP- und der zweite Connector einen HTTPS-Connector.

Standardmäßig sehen diese Connectoren wie folgt aus:

HTTP-Connector:

```
<Connector URIEncoding="UTF-8" compression="on" connectionTimeout="20000"
port="8080" protocol="org.apache.coyote.http11.Http11NioProtocol"
redirectPort="8443"/>
```

HTTPS-Connector:

```
<Connector SSLEnabled="true" URIEncoding="UTF-8" clientAuth="false"
compression="on" keyAlias="tomcat" keyPass="changeit" keystoreFile="C:/Program
Files/Hewlett-Packard/HP Operations
Orchestration/central/var/security/key.store" keystorePass="changeit"
keystoreType="JKS" maxThreads="200" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
secure="true" sslProtocol="TLSv1.2" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
truststoreFile="C:/Program Files/Hewlett-Packard/HP Operations
Orchestration/central/var/security/client.truststore" truststorePass="changeit"
truststoreType="JKS"/>
```

Standardmäßig sind beide Connectoren aktiviert.

Wichtig! Wenn Sie einen der Central-Ports in der Datei **Server.xml** ändern oder deaktivieren, müssen Sie auch die Datei **Central-wrapper.conf** und jede **RAS-wrapper.conf**-Datei so ändern, dass sie auf die Central-URL mit dem aktualisierten Port verweist. Andernfalls schlagen alle Ihre Flows, die in Central ausgeführt werden, fehl. Überprüfen Sie auch die Load Balancer-Konfigurationen.

Ändern der Portwerte

So ändern Sie die Werte eines Ports:

1. Bearbeiten Sie die Datei **server.xml**, die sich im Ordner **<Installationsverzeichnis>/central/tomcat/conf** befindet.
2. Suchen Sie die Zeile mit dem HTTP- oder HTTPS-Connector und ändern Sie den Wert für **Port**.

   Hinweis: Wenn Sie sowohl HTTP und HTTPS aktiv halten und den HTTPS-Port ändern möchten, müssen Sie den Wert von **redirectPort** für den HTTP-Connector und den Wert von **port** für den HTTPS-Connector ändern.
3. Speichern Sie die Datei.
4. Starten Sie Central erneut.

Deaktivieren des HTTP-Ports

Aus Sicherheitsgründen könnten Sie den HTTP-Port deaktivieren, sodass der einzige Kommunikationskanal TLS verwendet und verschlüsselt wird.

1. Bearbeiten Sie die Datei **server.xml**, die sich im Ordner **<Installationsverzeichnis>/central/tomcat/conf** befindet.
2. Suchen Sie den HTTP-Connector und löschen Sie die Zeile oder kommentieren Sie sie aus.
3. Importieren Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die Central-Datei **Client.truststore**, wenn sie noch nicht in der CA-Liste vorhanden ist:

   ```
   keytool -importcert -alias <any_alias> -keystore <path to the client.truststore> -file <certificate_name.cer> -storepass <changeit>
   ```

   Hinweis: Wenn Sie eine bekannte Stamm-CA (wie Verisign) verwenden, müssen Sie diesen Schritt nicht durchführen, da das Zertifikat bereits in der Datei **Client.truststore** vorhanden ist.
4. Speichern Sie die Datei.
5. Starten Sie Central erneut.

Hinweis: Es ist auch möglich, den HTTP-Port während der Installation zu deaktivieren.

Fehlerbehebung

Wenn der Server nicht startet, öffnen Sie die Datei **wrapper.log** und suchen nach einem Fehler in `ProtocolHandler ["http-nio-8443"]`.

Dieser Fehler kann beim Initialisieren von Tomcat oder beim Starten des Connectors auftreten. Er tritt in vielen Variationen auf, aber die Fehlermeldung enthält weitere Informationen.

Alle HTTPS-Connector-Parameter sind in der Tomcat-Konfigurationsdatei angegeben, die sich unter **C:\HPE\oo\central\tomcat\conf\Server.xml** befindet.

Öffnen Sie die Datei und scrollen Sie nach unten, bis Sie den HTTPS-Connector sehen:

```
<Connector SSLEnabled="true" clientAuth="false" keyAlias="tomcat"
keystoreFile="C:/HPE/oo/central/var/security/keystore.p12" keystorePass="tomcat-
keystore-password" keystoreType="PKCS12" maxThreads="200" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true"
sslProtocol="TLSv1.2" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"/>
```

Prüfen Sie, ob eine Nichtübereinstimmung bei den Parametern vorliegt, indem Sie sie mit den in den vorherigen Schritten eingegebenen Parametern vergleichen.

Clientzertifikatauthentifizierung (Gegenseitige Authentifizierung)

Die X.509-Zertifikat-Authentifizierung wird am häufigsten beim Überprüfen der Identität eines Servers bei Verwendung von TLS genutzt; meist sind dies HTTPS-Verbindungen eines Browsers. Der Browser überprüft automatisch, ob das von einem Server vorgelegte Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgegeben wurde, die sich in einer von ihm verwalteten Liste befindet.

Sie können TLS aber auch für eine gegenseitige Authentifizierung verwenden. Der Server fordert als Teil des TLS-Handshake ein gültiges Zertifikat vom Client an. Der Server authentifiziert den Client, indem er prüft, ob das Zertifikat von einer vertrauenswürdigen Authentifizierungsstelle signiert wurde. Wenn ein gültiges Zertifikat bereitgestellt wurde, können Sie es über die Servlet-API in einer Anwendung abrufen.

Konfigurieren der Clientzertifikatauthentifizierung in Central

Stellen Sie vor dem Konfigurieren der Clientzertifikatauthentifizierung in Central sicher, dass Sie das TLS-Serverzertifikat wie in "Arbeiten mit Server- und Clientzertifikaten" auf Seite 38 beschrieben konfiguriert haben.

Legen Sie für das Attribut `clientAuth` den Wert `true` fest, wenn der TLS-Stack eine gültige Zertifikatskette vom Client anfordern soll, bevor eine Verbindung akzeptiert wird. Geben Sie `want` an, um festzulegen, dass der TLS-Stack ein Clientzertifikat anfordert, aber nicht fehlschlägt, wenn kein Zertifikat vorgelegt wird. Wird `false` (Standard) angegeben, ist keine Zertifikatskette erforderlich, es sei denn der Client fordert eine Ressource an, die durch eine Sicherheitseinschränkung geschützt ist, die auf einer Clientzertifikatauthentifizierung beruht. (Weitere Informationen finden Sie in der Apache Tomcat Configuration Reference.)

Geben Sie die Datei mit der **Zertifikatsperrliste (CRL)** an. Die Datei kann mehrere CRLs enthalten. Bei einigen kryptografischen Systemen, in der Regel Public-Key-Infrastrukturen (PKIs), werden in einer Zertifikatsperrliste Zertifikate (genauer gesagt Seriennummern von Zertifikaten) erfasst, die widerrufen wurden. Entitäten, die solche (widerrufene) Zertifikate vorlegen, sollten als nicht mehr vertrauenswürdig betrachtet werden.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Beenden Sie den Central-Server.
2. Importieren Sie das zugehörige Stammzertifikat (CA) in Central **client.truststore**: **<Installationsverzeichnis>/central/var/security/client.truststore**, wenn es noch nicht in der CA-Liste vorhanden ist (dort befinden sich standardmäßig alle bekannten CAs). Beispiel:

   ```
   keytool -importcert -alias <any_alias> -keystore <path>/client.truststore -file <certificate_path> -storepass <changeit>
   ```

3. Bearbeiten Sie die Datei **server.xml**, die sich im Ordner **<Installationsverzeichnis>/central/tomcat/conf** befindet.
4. Legen Sie für das Attribut `clientAuth` im Tag `Connector` den Wert `want` oder `true` fest. Die Standardeinstellung ist `false`.

   Beispiel:

   ```
   <Connector SSLEnabled="true" URIEncoding="UTF-8" clientAuth="false"
   compression="on" keyAlias="tomcat" keyPass="changeit"
   keystoreFile="C:/Program Files/Hewlett-Packard/HP Operations
   Orchestration/central/var/security/key.store" keystorePass="changeit"
   keystoreType="JKS" maxThreads="200" port="8443"
   protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
   secure="true" server="OO" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
   sslProtocol="TLSv1.2" truststoreFile="C:/Program Files/Hewlett-Packard/HP
   ```

```
Operations Orchestration/central/var/security/client.truststore"
truststorePass="changeit" truststoreType="JKS"/>
```

Hinweis: An diesem Punkt kann der Server gestartet werden. Es wird aber empfohlen, den Server erst am Ende dieser Prozedur zu starten.

5. (Optional) Fügen Sie das Attribut `crlFile` hinzu, um die Datei mit den Zertifikatsperrlisten für die TLS-Zertifikatprüfung zu definieren. Beispiel:

   ```
   crlFile="<path>/crlname.<crl/pem>"
   ```

   Die Datei kann die Erweiterung `.crl` für eine einzelne Zertifikatsperrliste oder `.pem` (PEM CRL-Format) für eine oder mehrere Zertifikatsperrlisten aufweisen. Das PEM-CRL-Format verwendet die folgenden Kopf- und Fußzeilen:

   ```
   -----BEGIN X509 CRL-----
   -----END X509 CRL-----
   ```

   Beispiel für die `.pem`-Dateistruktur mit einer CRL (mehrere CRLs werden mit weiteren CRL-Blöcken verkettet):

   ```
   -----BEGIN X509 CRL-----
   MIIBbzCB2QIBATANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJVUzEYMBYGA1UE
   ChMPVS5TLiBHb3Zlcm5tZW50MQwwCgYDVQQLEwNEb0QxEDAOBgNVBAsTB1Rlc3Rp
   bmcxFTATBgNVBAMTDFRydXN0IEFuY2hvchcNOTkwMTAxMTIwMTAwWhcNNDgwMTAx
   MTIwMTAwWjAiMCACAScXDTk5MDEwMTEyMDAwMFowDDAKBgNVHRUEAwoBAaAjMCEw
   CgYDVR0UBAMCAQEwEwYDVR0jBAwwCoAIq5rr+cLnVI8wDQYJKoZIhvcNAQEFBQAD
   gYEAC7lqZwejJRW7QvzH11/7cYcL3racgMxH3PSU/ufvyLk7ahR++RtHary/WeCv
   RdyznLiIOA8ZBiguWtVPqsNysNn7WLofQIVa+/TD3T+lece4e1NwGQvj5Q+e2wRt
   GXg+gCuTjTKUFfKRnWz7O7RyiJKKim0jtAF4RkCpLebNChY=
   -----END X509 CRL-----
   ```

6. Bearbeiten Sie die Datei **Central-wrapper.conf**, die sich im Ordner **<Installationsverzeichnis>\central\conf\central** befindet.

   Entfernen Sie das Kommentarzeichen bei den folgenden Eigenschaften und legen Sie für das Clientzertifikat den Speicherort und das Kennwort eines Clientzertifikats mit einem Administratorbenutzer fest.

   ```
   #wrapper.java.additional.23=-Djavax.net.ssl.keyStore="%CENTRAL_
   HOME%/var/security/certificate.p12"

   #wrapper.java.additional.24.stripquotes=TRUE
   ```

```
#wrapper.java.additional.25=-Djavax.net.ssl.keyStorePassword={OBFUSCATED}
ZUoMreNLw6qIOyzX7g5YKw==

#wrapper.java.additional.26=-Djavax.net.ssl.keyStoreType=PKCS12
```

Weitere Informationen zum Verschlüsseln oder Obfuskieren eines Kennworts finden Sie unter "Verschlüsseln und Obfuskieren von Kennwörtern" auf Seite 48.

7. Starten Sie den Central-Server.

Hinweis: Für jedes Clientzertifikat müssen Sie entweder einen internen Benutzer oder einen LDAP-Benutzer definieren. Der Name des Benutzers sollte in den Zertifikatattributen definiert sein. Der Standardwert ist der Wert des CN-Attributs. Weitere Informationen finden Sie im Abschnitt Verarbeiten eines Zertifikatprinzipals.

Beachten Sie Folgendes: Auch wenn Sie in HPE OO mehrere LDAP-Konfigurationen eingerichtet haben, kann ein Benutzer nur mit den Clientzertifikatattributen aus dem Standard-LDAP authentifiziert werden.

Aktualisieren der Konfiguration eines Clientzertifikats in RAS

Das Clientzertifikat wird bei der Installation des RAS konfiguriert. Wenn Sie das Clientzertifikat jedoch aktualisieren müssen, können Sie die Datei **ras-wrapper.conf** manuell bearbeiten.

Voraussetzung: Sie müssen das CA-Stammzertifikat von Central in den RAS-TrustStore importieren. Weitere Informationen finden Sie unter "Importieren eines CA-Stammzertifikats in einen RAS-TrustStore" auf Seite 41.

So aktualisieren Sie die Konfiguration des Clientzertifikats in einem externen RAS:

1. Beenden Sie den RAS-Server.
2. Öffnen Sie die Datei **Ras-wrapper.conf** im Ordner **<Installationsverzeichnis>/ras/conf**.
3. Ändern Sie die folgenden Angaben gemäß Ihrem Clientzertifikat:

```
wrapper.java.additional.<x>=-Djavax.net.ssl.keyStore=<installation
dir>/var/security/certificate.p12"

wrapper.java.additional.<x>=-Djavax.net.ssl.keyStorePassword={OBFUSCATED}
<obfuskiertes_Kennwort>

wrapper.java.additional.<x>=-Djavax.net.ssl.keyStoreType=PKCS12
```

4. Starten Sie den RAS-Server.

Wichtige Hinweise! Das X.509-Clientzertifikat muss den Prinzipalnamen des RAS, die RAS-ID, enthalten (siehe Verarbeiten eines Zertifikatprinzipals).

Sie finden die RAS-ID auf der Registerkarte **Topologie** in Central. Weitere Informationen finden Sie unter "Einrichten der Topologie – Worker" im *OO Central-Benutzerhandbuch*.

Ab HPE OO 10.20 wird der Parameter `keyStorePassword` standardmäßig verschlüsselt, wenn das Kennwort als Standard beibehalten wurde. Diesen Parameter können Sie ändern und entweder in Klartext oder verschlüsselt speichern. Weitere Informationen finden Sie unter "Verschlüsseln und Obfuskieren von Kennwörtern" auf Seite 48.

Konfigurieren eines ClientZertifikats in Studio Remote Debugger

Voraussetzung: Sie müssen das CA-Stammzertifikat von Central in den Studio Debugger-TrustStore importieren. Weitere Informationen finden Sie unter "Importieren eines CA-Stammzertifikats in den Studio-TrustStore" auf Seite 44.

So konfigurieren Sie das Clientzertifikat in Studio Remote Debugger:

1. Schließen Sie Studio.
2. Bearbeiten Sie die Datei **Studio.l4j.ini** im Ordner **<Installationsverzeichnis>/studio**.
3. Ändern Sie die folgenden Angaben gemäß Ihrem Clientzertifikat:

```
-Djavax.net.ssl.keyStore="<installation
dir>/studio/var/security/certificate.p12"

-Djavax.net.ssl.keyStorePassword={OBFUSCATED}<obfuscated_password>

-Djavax.net.ssl.keyStoreType=PKCS12
```

4. Starten Sie Studio.

Hinweise:

- Ab HPE OO 10.20 wird der Parameter `keyStorePassword` standardmäßig verschlüsselt, wenn das Kennwort als Standard beibehalten wurde. Diesen Parameter können Sie ändern und entweder in Klartext oder verschlüsselt speichern. Weitere Informationen finden Sie unter "Verschlüsseln und Obfuskieren von Kennwörtern" auf Seite 48.
- Für jedes Clientzertifikat müssen Sie entweder einen internen Benutzer oder einen LDAP-Benutzer definieren. Der Name des Benutzers sollte in den Zertifikatattributen definiert sein. Der Standardwert ist der Wert des CN-Attributs. Weitere Informationen finden Sie im Abschnitt Verarbeiten eines Zertifikatprinzipals.

- Beachten Sie Folgendes: Auch wenn Sie in HPE OO mehrere LDAP-Konfigurationen eingerichtet haben, kann ein Benutzer nur mit den Clientzertifikatattributen aus dem Standard-LDAP authentifiziert werden. Central versucht zuerst, den Benutzer mit dem Standard-LDAP zu authentifizieren, und unternimmt, wenn dies fehlschlägt, einen weiteren Authentifizierungsversuch in der internen HPE OO-Domäne.

Konfigurieren eines Clientzertifikats in OOSH

Voraussetzung: Sie müssen das CA-Stammzertifikat von Central in den OOSH-TrustStore importieren. Weitere Informationen finden Sie unter "Importieren eines CA-Stammzertifikats in den OOSH-TrustStore" auf Seite 43.

1. Beenden Sie OOSH.
2. Bearbeiten Sie die Datei **oosh.bat** im Ordner **<Installationsverzeichnis>/central/bin**.
3. Ändern Sie die folgenden Angaben gemäß Ihrem Clientzertifikat:

   ```
   -Djavax.net.ssl.keyStore="<installation dir>/var/security/certificate.p12"
   -Djavax.net.ssl.keyStorePassword={OBFUSCATED}<obfuscated_password>
   -Djavax.net.ssl.keyStoreType=PKCS12
   ```

4. Starten Sie OOSH.

Hinweis:

Ab HPE OO 10.20 wird der Parameter `keyStorePassword` standardmäßig verschlüsselt, wenn das Kennwort als Standard beibehalten wurde. Diesen Parameter können Sie ändern und entweder in Klartext oder verschlüsselt speichern. Weitere Informationen finden Sie unter "Verschlüsseln und Obfuskieren von Kennwörtern" auf Seite 48.

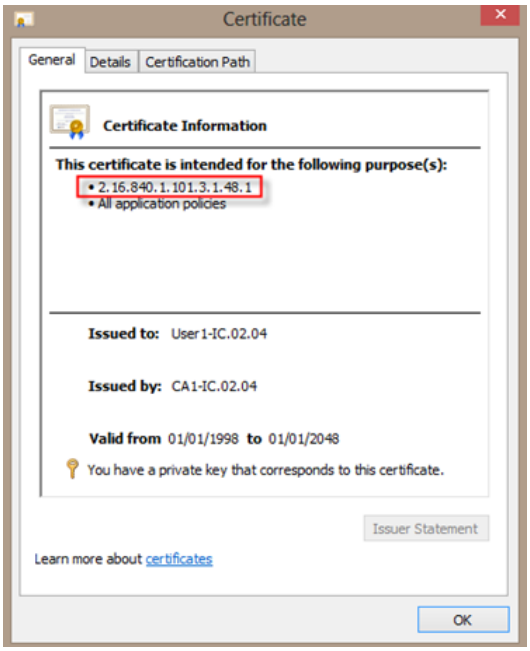
Für jedes Clientzertifikat müssen Sie entweder einen internen Benutzer oder einen LDAP-Benutzer definieren. Der Name des Benutzers sollte in den Zertifikatattributen definiert sein. Der Standardwert ist der Wert des CN-Attributs. Weitere Informationen finden Sie im Abschnitt Verarbeiten eines Zertifikatprinzipals.

Beachten Sie Folgendes: Auch wenn Sie in HPE OO mehrere LDAP-Konfigurationen eingerichtet haben, kann ein Benutzer nur mit den Clientzertifikatattributen aus dem Standard-LDAP authentifiziert werden. Central versucht zuerst, den Benutzer mit dem Standard-LDAP zu authentifizieren, und unternimmt, wenn dies fehlschlägt, einen weiteren Authentifizierungsversuch in der internen HPE OO-Domäne.

Verarbeiten der Zertifikatrichtlinien

HPE OO obliegt die Verarbeitung von Zertifikatrichtlinien für das Endpunktzertifikat.

- Sie können die Zweckzeichenfolge im Zertifikat festlegen.
- In HPE OO können Sie die Richtlinienzeichenfolge(n) als Konfigurationselement hinzufügen und die Richtlinienzeichenfolge eines jeden Endpunktzertifikats überprüfen. Wenn es nicht übereinstimmt, wird das Zertifikat abgelehnt.
- Aktivieren oder deaktivieren Sie die Überprüfung der Zertifikatrichtlinien, indem Sie das folgende Konfigurationselement hinzufügen: `x509.certificate.policy.enabled=true/false` (Standardeinstellung ist `false`).
- Definieren Sie die Richtlinienliste, indem Sie das folgende Konfigurationselement hinzufügen: `x509.certificate.policy.list=<comma_separated_list>` (Standardeinstellung ist eine leere Liste).



Weitere Informationen zum Ändern der OO-Systemeigenschaften finden Sie im *OO Shell Guide*.

Verarbeiten eines Zertifikatprinzipals

Sie können definieren, wie der Prinzipal aus einem Zertifikat abgerufen wird, indem Sie einen regulären Ausdruck als Vergleichskriterium für `Subject` angeben. Der reguläre Ausdruck sollte eine einzelne Gruppe enthalten. Der Standardausdruck `CN=(.?)` zieht für den Vergleich das Feld "Allgemeiner

Name" (Common Name, CN) heran. Beispiel: `CN=Jimi Hendrix, OU=` weist den Benutzernamen `Jimi Hendrix` zu.

- Groß- und Kleinschreibung wird ignoriert.
- Der Prinzipal des Zertifikats ist der Benutzername in HPE OO (LDAP- oder interner Benutzer).
- Um den regulären Ausdruck zu ändern, ändern Sie das Konfigurationselement `x509.subject.principal.regex`.

Konfigurieren von OO zum Lesen des Feldes "Alternativer Antragstellername" in einem Zertifikat

Sie können OO so konfigurieren, dass der Wert des Feldes `Alternativer Antragstellername` in einem Zertifikat gelesen wird. Dazu wird das Konfigurationselement `x509.principal.lookup.field` verwendet.

Dieses Konfigurationselement steuert, welches Feld eines Zertifikats zum Extrahieren des Benutzernamens verwendet wird.

Mögliche Werte sind:

- `subjectDN` - steht für das Feld `Antragsteller` des Zertifikats und bedeutet, dass OO sein Standardverhalten beibehält und versucht, den Benutzernamen aus dem Feld **Antragsteller** zu extrahieren. Dies ist der Standardwert.
- `subjectAltNames.otherName.principalName` - steht für `Benutzerprinzipalname` (OID 1.3.6.1.4.1.311.20.2.3) im Eintrag `Sonstiger Name` der Zertifikaterweiterung `Alternative Antragstellernamen`. Wenn es bei der CAC-Authentifizierung erforderlich sein sollte, den Wert von Benutzerprinzipalname zu verwenden, müssten Sie diesen Wert verwenden.

Weitere Informationen zum Ändern der HPE OO-Konfigurationselemente finden Sie im *HPE OO Shell (OOSH) User Guide*.

Konfigurieren der FIPS 140-2-Konformität Stufe 1 in HPE OO

In diesem Abschnitt wird erläutert, wie Sie HPE Operations Orchestration konfigurieren, um Übereinstimmung mit den Federal Information Processing Standards (FIPS) 140-2 Stufe 1 zu erzielen.

FIPS 140-2 ist ein Standard, der Sicherheitsanforderungen für kryptografische Module definiert und von der US-Behörde National Institute of Standards Technology (NIST) festgelegt wurde. Der Standard wurde veröffentlicht unter: csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

Nachdem Sie die HPE OO-Konfiguration an den FIPS 140-2-Standard angepasst haben, verwendet HPE OO die folgenden Sicherheitsalgorithmen:

- Symmetrischer Schlüsselalgorithmus: AES256
- Hash-Algorithmus: SHA256

HPE OO verwendet den Sicherheitsanbieter RSA BSAFE Crypto Software Version 6.1. Dies ist der einzige unterstützte Sicherheitsanbieter für FIPS 140-2.

Hinweis: Nachdem Sie die HPE OO-Konfiguration an den FIPS 140-2-Standard angepasst haben, können Sie die Standardkonfiguration nur durch eine Neuinstallation von HPE OO wiederherstellen.

Voraussetzungen

Hinweis für Upgrades:

Informationen zum Upgrade einer Installation von HPE OO 10.10 (und höher), die bereits mit FIPS konfiguriert wurde, finden Sie unter Vorbereitende Schritte für ein Upgrade.

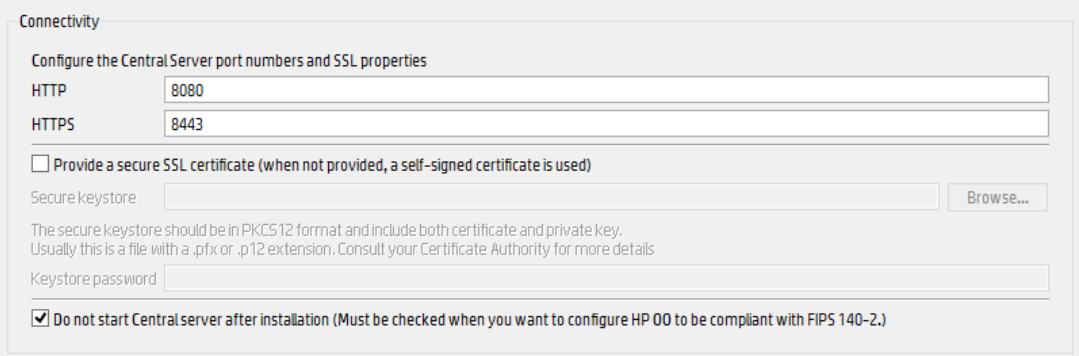
Führen Sie vor der FIPS 140-2-konformen HPE OO-Konfiguration die folgenden Schritte aus:

Hinweis: Um den FIPS140-2-Standard zu erfüllen, müssen Sie LWSSO ausschalten.

1. Vergewissern Sie sich, das Sie eine neue Installation von HPE OO – Version 10.10 oder höher konfigurieren, um den FIPS 140-2-Standard zu erfüllen, und dass diese nicht verwendet wird.

Eine Installation von HPE OO, die gerade verwendet wird (ob Version 9.x oder 10.x), kann nicht konfiguriert werden.

2. Vergewissern Sie sich, dass HPE OO bei der Installation so konfiguriert wurde, dass der Central Server nach der Installation nicht gestartet wird:
   - Bei einer Installation im Hintergrund wurde der Parameter `should.start.central` auf **no** gesetzt.
   - In einer mit dem Assistenten durchgeführten Installation wurde beim Schritt **Verbindung** das Kontrollkästchen **Do not start Central server after installation** aktiviert.



3. Sichern Sie die folgenden Verzeichnisse:
   - **<Installationsverzeichnis>\central\tomcat\webapps\oo.war**
   - **<Installationsverzeichnis>\central\tomcat\webapps\PAS.war**
   - **<Installationsverzeichnis>\central\conf**
   - **<Installationsverzeichnis>\java** (legen Sie eine Sicherheitskopie des gesamten Ordners **java** an)
4. Laden Sie **Server Oracle JRE 8** von der Oracle-Website http://www.oracle.com/technetwork/java/javase/downloads/server-jre8-downloads-2133154.html herunter, und ersetzen Sie die **OpenJDK (Zulu) JRE** durch **Server Oracle JRE**.
   a. Löschen Sei den gesamten Inhalt des Ordners **<Installationsverzeichnis>\JAVA**.
   b. Extrahieren Sie das heruntergeladene Archiv.
   c. Kopieren Sie den Inhalt des Ordners **JRE** nach **<Installationsverzeichnis>\JAVA**.
5. Laden Sie die Java Cryptographic Extension (JCE) Unlimited Strength Jurisdiction Policy Files von der folgenden Website herunter und installieren Sie sie:

   http://www.oracle.com/technetwork/java/javase/downloads/server-jre8-downloads-2133154.html

Hinweis: Informationen, wie Sie die Dateien verteilen und die von HPE OO verwendete JRE aktualisieren, finden Sie in der Datei **ReadMe.txt**, die zu den heruntergeladenen Dateien gehört.

6. Installieren Sie die RSA BSAFE Crypto-Dateien. Kopieren Sie auf dem System, auf dem HPE OO installiert ist, die folgenden Dateien in den Ordner **<oo_jre>\lib\ext** (**<oo_jre>** ist das Verzeichnis, in dem die von HPE OO verwendete JRE installiert ist. Standardmäßig ist dies der Ordner **<Installationsverzeichnis>\java**).
   - **<Installationsverzeichnis>\central\lib\cryptojce-6.2.1.jar**
   - **<Installationsverzeichnis>\central\lib\cryptojcommon-6.2.1.jar**
   - **<Installationsverzeichnis>\central\lib\jcmFIPS-6.2.1.jar**

Vorbereitende Schritte für ein Upgrade

1. Laden Sie "Server Oracle JRE 8" herunter, und ersetzen Sie die "OpenJDK (Zulu) JRE" durch "Server Oracle JRE".
   a. Löschen Sei den gesamten Inhalt des Ordners **<Upgrade-Verzeichnis>\JAVA**.
   b. Extrahieren Sie das heruntergeladene Archiv.
   c. Kopieren Sie den Inhalt des Ordners **JRE** nach **<Upgrade-Verzeichnis>\JAVA**.

   http://www.oracle.com/technetwork/java/javase/downloads/server-jre8-downloads-2133154.html
2. Laden Sie die Java Cryptographic Extension (JCE) Unlimited Strength Jurisdiction Policy Files von der folgenden Website herunter und installieren Sie sie:

   http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

   Informationen, wie Sie die Dateien verteilen und die von HPE OO verwendete JRE aktualisieren, finden Sie in der Datei **ReadMe.txt**, die zu den heruntergeladenen Dateien gehört.
3. Installieren Sie die RSA BSAFE Crypto-Dateien. Kopieren Sie auf dem System, auf dem HPE OO installiert ist, die folgenden Dateien in den Ordner **<oo_jre>\lib\ext**:

   (**<oo_jre>** ist das Verzeichnis, in dem die von HPE OO verwendete JRE installiert ist. Standardmäßig ist dies **<Upgrade-Verzeichnis\java**).
   - <Installationsverzeichnis>\central\lib\cryptojce-6.2.1.jar

- <Installationsverzeichnis>\central\lib\cryptojcommon-6.2.1.jar
- <Installationsverzeichnis>\central\lib\jcmFIPS-6.2.1.jar

Befolgen Sie dann die Schritte im Abschnitt "Konfigurieren der Eigenschaften in der Java-Sicherheitsdatei" in "Konfigurieren der FIPS 140-2-Konformität von HPE OO" oben.

Konfigurieren der FIPS 140-2-Konformität von HPE OO

Die folgende Liste enthält die Prozeduren, die Sie durchführen müssen, um HPE OO in Übereinstimmung mit FIPS 140-2 zu konfigurieren:

1. Konfigurieren der Eigenschaften in der Java-Sicherheitsdatei
2. Konfigurieren der Datei "encryption.properties" und Aktivieren des FIPS-Modus
3. Erstellen einer FIPS-kompatiblen HPE OO-Verschlüsselung
4. Erneutes Verschlüsseln des Datenbankkennworts mit der neuen Verschlüsselung
5. Starten von HPE OO

Konfigurieren der Eigenschaften in der Java-Sicherheitsdatei

Bearbeiten Sie die Java-Security-Datei für JRE, um zusätzliche Sicherheitsanbieter hinzuzufügen, und konfigurieren Sie die Eigenschaften für die FIPS 140-2-Konformität.

Hinweis: Das Upgrade auf HPE OO 10.x ersetzt alle installierten JRE-Dateien. Deshalb müssen Sie beim Upgrade auf 10.x die folgenden Schritte ausführen.

Hinweis: Beim Upgrade einer Installation von HPE OO 10.10 und höher, die bereits mit FIPS konfiguriert wurde, müssen Sie die Schritte im Abschnitt "Vorbereitende Schritte für ein Upgrade" in "Konfigurieren der FIPS 140-2-Konformität Stufe 1 in HPE OO" auf Seite 60 und danach die hier angegebenen Schritte ausführen, wobei **<oo_jre>** die JRE im Upgrade (im Verzeichnis **<Upgrade-Verzeichnis>\JAVA**) ist.

Stellen Sie sicher, dass alle Änderungen im **Java**-Ordner innerhalb des extrahierten **Upgrade**-Ordners erfolgen.

Öffnen Sie die Datei **< oo_jre>\lib\security\java.security** in einem Editor und führen Sie die folgenden Schritte aus:

1. Erhöhen Sie bei jedem im Format **security.provider.nn=<provider_name>** gelisteten Anbieter die Reihenfolgennummer `<nn>` um zwei.

   Ändern Sie beispielsweise den Anbietereintrag:

   ```
   security.provider.1=sun.security.provider.Sun
   ```

   in

   ```
   security.provider.3=sun.security.provider.Sun
   ```

2. Fügen Sie einen neuen Standardanbieter hinzu (RSA JCE). Fügen Sie den folgenden Anbieter am Anfang der Anbieterliste ein:

   ```
   security.provider.1=com.rsa.jsafe.provider.JsafeJCE
   ```

3. Fügen Sie RSA BSAFE als neuen SSL-J Java Secure Sockets Extension (JSSE) Provider hinzu.

   ```
   security.provider.2=com.rsa.jsse.JsseProvider
   ```

4. Kopieren und fügen Sie die folgende Zeile in die Datei **java.security** ein, um sicherzustellen, dass **RSA BSAFE** im FIPS 140-2-konformen Modus verwendet wird:

   ```
   com.rsa.cryptoj.fips140initialmode=FIPS140_SSL_MODE
   ```

   Sie können diese Zeile an beliebiger Stelle in der Datei **java.security** einfügen.

5. Da der Standard-DRBG-Algorithmus ECDRBG128 (gemäß NIST) nicht sicher ist, legen Sie für die security-Eigenschaft **com.rsa.crypto.default** den Wert **HMACDRBG** fest, indem Sie die folgende Zeile in die Datei **java.security** kopieren:

   ```
   com.rsa.crypto.default.random=HMACDRBG
   ```

   Sie können diese Zeile an beliebiger Stelle in der Datei **java.security** einfügen.

6. Speichern und schließen Sie die Datei **java.security**.

Konfigurieren der Datei "encryption.properties" und Aktivieren des FIPS-Modus

Die HPE OO-Datei encryption.properties muss aktualisiert werden, um FIPS 140-2-konform zu sein.

1. Sichern Sie die Datei **encryption.properties**, die sich in **<Installationsverzeichnis>\central\var\security** befindet.
2. Öffnen Sie die Datei **encryption.properties** in einem Texteditor. Bearbeiten Sie beispielsweise die folgende Datei:

C:\Programme\Hewlett-Packard\HP Operations Orchestration\central\var\security\encryption.properties.

3. Suchen Sie nach `keySize=128` und ersetzen Sie diese Angabe durch `keySize=256`.
4. Suchen Sie nach `secureHashAlgorithm=SHA1` und ersetzen Sie diese Angabe durch `secureHashAlgorithm=SHA256`.
5. Suchen Sie nach `FIPS140ModeEnabled=false` und ersetzen Sie diese Angabe durch `FIPS140ModeEnabled=true`.

   Hinweis: Wenn `FIPS140ModeEnabled=false` nicht vorhanden ist, fügen Sie `FIPS140ModeEnabled=true` als neue Zeile am Ende der Datei hinzu.

6. Speichern und schließen Sie die Datei.

Erstellen einer FIPS-kompatiblen OO-Verschlüsselung

Informationen zum Erstellen oder Ersetzen der HPE OO-Verschlüsselungsspeicherdatei, damit sie FIPS-konform ist, finden Sie unter "Ersetzen der FIPS-Verschlüsselung" auf der nächsten Seite.

Hinweis: Für AES sind drei Schlüssellängen zulässig: 128/192/256 laut NIST SP800-131A.

Die folgenden Secure-Hash-Algorithmen werden in FIPS unterstützt: SHA1, SHA256, SHA384, SHA512.

Hinweis: Es wird empfohlen, die Kennwörter für den Keystore (und den Eintrag mit dem privaten Schlüssel) und den Truststore zu ändern. Weitere Informationen finden Sie unter "Ändern und Verschlüsseln/Obfuskieren des KeyStore/TrustStore-Kennworts" auf Seite 45.

Hinweis: Es wird empfohlen, alle nicht verwendeten Standard-CA-Stammzertifikate im OO-Truststore zu löschen. (Die Datei **client.truststore** befindet sich unter **<Installation>/central/var/security**.)

Hinweis: Wenn Sie mit Clientzertifikat arbeiten, sollte das Zertifikat mit dem FIPS-konformen RSA JCE-Provider und mit den Secure-Hash-Algorithmen in der obigen Liste, die in FIPS unterstützt werden, erstellt werden.

Erneutes Verschlüsseln des Datenbankkennworts mit der neuen Verschlüsselung

Verschlüsseln Sie das Datenbankkennwort erneut. Die entsprechende Beschreibung finden Sie im *HPE OO Administration Guide* unter "Ändern des Datenbankkennworts".

Starten von HPE OO

Ersetzen der FIPS-Verschlüsselung

HPE OO Central und RAS entsprechen dem FIPS-Standard 140-2 (Federal Information Processing Standard), der die technischen Anforderungen definiert, die von US-Bundesbehörden einzuhalten sind, wenn diese Organisationen kryptografische Sicherheitssysteme zum Schutz vertraulicher oder wertvoller Daten spezifizieren.

Nach einer Neuinstallation von HPE OO haben Sie die Möglichkeit, den FIPS-Verschlüsselungsschlüssel zu ändern.

Hinweis: Dieses Verfahren ist nur bei Neuinstallationen möglich. Sie können es nicht nach Upgradeinstallationen anwenden.

Ändern des FIPS-Verschlüsselungsschlüssels in Central

Verwenden Sie die Datei **generate-keys.bat**/**sh**, um den FIPS-Verschlüsselungsschlüssel im Verschlüsselungsrepository zu ersetzen.

Hinweis: Da bei diesem Prozess eine Sicherung der Datei **encryption_repository** erstellt wird, müssen Sie die entsprechenden Schreibberechtigungen besitzen.

1. Wechseln Sie zu **<Central-Installationsordner>/var/security**.
2. Erstellen Sie eine Sicherung der Datei **encryption_repository** und löschen Sie die Datei aus dem Ordner **<Central-Installationsordner>/var/security**.
3. Wechseln Sie zu **<Central-Installationsordner>/bin**.
4. Führen Sie das Skript **generate-keys** aus.
5. Drücken Sie die Taste **J**, um fortzufahren.

Ein neuer Masterschlüssel wird in **<Central-Installationsordner>/var/security/encryption_repository** generiert.

Hinweis: Wenn Sie das Skript **generate-keys** ohne die Pausen ausführen möchten, in denen der Benutzer **J** oder **N** eingeben muss, dann verwenden Sie das Flag **–s** für den ("stillen") Automatikmodus bei der Ausführung des Skripts.

Ändern der RAS-Verschlüsselungseigenschaften

Wenn Sie die RAS-Installation an einem neuen Standort durchgeführt haben, müssen Sie alle folgenden Schritte ausführen.

Hinweis: Diese Änderungen sind nur gültig, wenn Sie eine neue RAS-Installation bearbeiten, nachdem Sie die Central-Verschlüsselungseigenschaften geändert haben.

So ändern Sie die RAS-Verschlüsselungseigenschaften:

1. Führen Sie alle Schritte im Abschnitt "Voraussetzungen" unter "Konfigurieren der FIPS 140-2-Konformität Stufe 1 in HPE OO" auf Seite 60 aus.
2. Führen Sie alle Schritte im Abschnitt "Konfigurieren der Eigenschaften in der Java Security-Datei" unter "Konfigurieren der FIPS 140-2-Konformität von HPE OO" auf Seite 63 aus.
3. Kopieren Sie die aktuelle **encryption.properties**-Datei aus dem Ordner **<Installationsverzeichnis>\ras\var\security** in den Ordner **<Installationsverzeichnis>\ras\bin**.
4. Bearbeiten und ändern Sie die Datei **encryption.properties** in einem Texteditor nach Bedarf.

   Weitere Informationen finden Sie unter "Konfigurieren der Datei encryption.properties und Aktivieren des FIPS-Modus" unter "Konfigurieren der FIPS 140-2-Konformität von HPE OO" auf Seite 63.
5. Speichern Sie die Änderungen.
6. Öffnen Sie eine Befehlszeile im Ordner **<Installationsverzeichnis>\ras\bin**.
7. Führen Sie die Datei **oosh.bat** aus.
8. Führen Sie den OOShell-Befehl aus: `replace-encryption --file encryption.properties`

   Hinweis: Wenn Sie die Datei **encryption.properties** in einen anderen Ordner kopiert haben,

müssen Sie den richtigen Speicherort im OOShell-Befehl angeben.

9. Starten Sie den RAS-Dienst wieder.

Konfigurieren des TLS-Protokolls

Sie können HPE OO konfigurieren, um die unterstützte TLS-Protokollversion festzulegen. Standardmäßig lässt HPE OO die Versionen TLS v1, TLS v1.1 und TLS v1.2 zu. Dies können aber eingrenzen.

Hinweis: SSLv3 und andere Versionen von SSL werden nicht unterstützt.

1. Öffnen Sie die Datei **<Installationsordner>/central/tomcat/conf/server.xml**.
2. Suchen Sie den SSL-Connector (am Ende der Datei).
3. Bearbeiten Sie den Standardwert von `sslEnabledProtocols`. Ändern Sie z. B.

   `sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"` in

   `sslEnabledProtocols="TLSv1.2"`
4. Starten Sie den Server neu.

Verhindern des Zugriffs durch Flows auf das lokale Dateisystem von Central/RAS

Sie sollten die Wrapper-Konfigurationsdatei und die Datei java.policy von Central oder RAS modifizieren, um zu verhindern, dass Flows auf das lokale Dateisystem von Central oder RAS zugreifen und Zugriff auf sensitive Ressourcen erlangen.

Hinweis: Für dieses Szenario müsste ein Benutzer zusätzlich zur Berechtigung für Flows oder zur Möglichkeit zum Festlegen der Berechtigungen für Flows auch die Berechtigungen zum Bereitstellen und zum Auslösen besitzen. Benutzer mit solchen Berechtigungen sind mit großer Wahrscheinlichkeit vertrauenswürdige Benutzer.

So schützen Sie sich vor diesem Szenario:

1. Fügen Sie in der Wrapper-Konfigurationsdatei von Central oder RAS (**<Installationsordner>/<ras/central>/conf/<central/ras>-wrapper.conf**) den Parameter `wrapper.java.additional.<nn>` wie folgt hinzu:

   `wrapper.java.additional.<nn>=-Djava.security.manager`

   Ersetzen Sie <nn> durch die Zahl hinter der letzten Zahl.

2. Fügen Sie in der Datei **java.policy** (unter **<Installationsordner>/java/lib/security/java.policy**) den folgenden Code hinzu. Dies ermöglicht den Zugriff auf die Ressourcen, die durch HPE OO mindestens benötigt werden, und verhindert den Zugriff auf das lokale Dateisystem von Central/RAS, das sensitive Daten enthält.

```
grant codebase "file:${oo.home}/bin/-" {
                permission java.security.AllPermission;
};

grant codebase "file:${oo.home}/lib/-" {
                permission java.security.AllPermission;
};

grant codebase "file:${oo.home}/tomcat/-" {
                permission java.security.AllPermission;
};

grant codebase "file:${oo.home}/var/cache/-" {
                permission java.io.FilePermission "${oo.home}/var/logs",
"read, write";
};
```

   Um dem Flow den Zugriff auf Ressourcen im lokalen Dateisystem von Central/RAS zu ermöglichen, sollten Sie in der Datei java.policy den folgenden Code angeben. Beispiel:

```
grant codebase "file:${oo.home}/var/cache/-" {
                permission java.io.FilePermission
"C:\\users\\cathy\\foo.bat", "read, write, execute, delete";
                permission java.io.FilePermission "C:\\users\\cathy\\-",
"read,write,execute,delete"; // Recursive Example
                permission java.io.FilePermission "C:\\users\\cathy\\*",
"read,write,execute,delete"; // Flat Example
                  .....
};
```

Hewlett Packard
Enterprise