

Schnelleinstieg

Dieser Leitfaden dient als Einführung in eine Standardinstallation von IBM Multi-Cloud Data Encryption.

Produktübersicht

IBM Multi-Cloud Data Encryption (MDE) ist ein umfassendes Datensicherheitsprodukt auf der Basis von SPx®-Technologie, das die Verschlüsselung ruhender Daten mit den leistungsfähigen Schutzfunktionen eines Richtlinienbereitstellungsmanagers (Policy Provisioning Manager - PPM) kombiniert. Der PPM fungiert als zentrale Management-Server-Konsole und ermöglicht die Bereitstellung von Verschlüsselungsagenten, das Festlegen von Datenzugriffsrichtlinien sowie das Management der Schlüssellebensdauer, der Agentenaktualisierungen und der Benutzerzugriffsprotokollierung von bis zu 25.000 Agenten von einem einzelnen zentralen Standort aus.

1 Schritt 1: Auf die Software und die Dokumentation zugreifen



- Laden Sie das OVA-Paket (OVA - Open Virtual Appliance) für Multi-Cloud Data Encryption von Passport Advantage herunter.
- Lesen Sie die Releaseinformationen für Multi-Cloud Data Encryption, bevor Sie das Produkt installieren.
- Die vollständige Dokumentation finden Sie im IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/SSTD4E_2.3.0/doc/kc_welcome_mde23.html). Die Dokumentation wird auch mit dem Produkt ausgeliefert.

2 Schritt 2: Hardware- und Systemkonfiguration überprüfen



Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- a. Ein Betriebsserver mit einem lizenzierten Betriebssystem und einem unterstützten Hypervisor (VMware ESXi™) zum Bereitstellen und Ausführen von PPM (Policy Provisioning Manager).
- b. Gepacktes Basis-OVA.
- c. PPM-Installationsprogramm.
- d. Einer oder mehrere Zielservers mit einem unterstützten Agentenbetriebssystem (Red Hat®/CentOS 6.2+ oder 7.2+, AIX 7.1 oder 7.2 oder 7.2+ und Microsoft Windows Server® 2008 R2, Microsoft Windows Server® 2012 R2 oder Microsoft Windows Server® 2016).
- e. Browser: Google Chrome®, Microsoft Internet Explorer® 10+, Mozilla Firefox® ESR 52+.
- f. Netzzugriff zwischen PPM und allen Agenten.
- g. Von einer Zertifizierungsstelle (CA) signierte Zertifikate (Keystore, Truststore und CA-Zertifikatspaket) zum Herstellen einer sicheren Sitzung zwischen dem Management-Server (PPM) und allen Agenten.

Für Object Store Agent (OSA) gelten die folgenden zusätzlichen Voraussetzungen:

- S3-kompatibler Objektspeicher: Amazon Web Services S3 (AWS S3), IBM Cloud Object Storage (COS S3)
- Berechtigungsnachweise für den Objektspeicher: Benutzer-ID und geheimer Schlüssel (Kennwort)
- Eine Anwendung oder ein Dienstprogramm, die bzw. das die AWS S3 REST-API-Bibliothek oder die Boto Python-Library verwendet, um Daten an OSA zu verweisen.

Vollständige Informationen finden Sie unter *Planungsaspekte, Einstellungen für Serverzertifikate* und *Anhang: Beispielzertifikate einer Zertifizierungsstelle (CA)* in der Veröffentlichung *IBM Multi-Cloud Data Encryption Verwaltung*.

3 Schritt 3: IBM Multi-Cloud Data Encryption installieren



Installieren Sie MDE-PPM, die interne Datenbankkonfiguration und die Zertifikatskonfiguration.

Ersetzen Sie in diesem Beispiel das X in 'ibm_sw_mde_X.x.x-XX.bin' durch den Dateinamen, die Version und die Buildnummern.

- a. Stellen Sie das Basis-OVA für MDE im Hypervisor bereit. Im vorliegenden Beispiel wird er als "Management-Server-VM" bezeichnet.
- b. Melden Sie sich als Administrator (admin) an und legen Sie ein neues Kennwort fest.

Das Open Virtualization Archive (OVA) verwendet PAM-Standardkriterien, die vom Administrator konfiguriert werden können. Das PAM-Kennwort muss länger als 8 Zeichen sein und darf nicht mehr als 4 Zeichen aus dem vorherigen Kennwort enthalten.

- c. Notieren Sie die IP-Adresse der MDE-VM.
- d. Laden Sie `ibm-sw_mde_X.x.x-xx.bin` mit `scp` oder einer ähnlichen Methode auf MDE hoch.
- e. Definieren Sie die 'bin'-Datei als ausführbar. Verwenden Sie dazu den folgenden Befehl:

```
[admin@localhost]$ chmod +x ./ibm_sw_mde_X.x.x-XX.bin
```

- f. Führen Sie die 'bin'-Datei aus. Verwenden Sie dazu den folgenden Befehl:

```
[admin@localhost]$ ./ibm_sw_mde_X.x.x-XX.bin
```

- g. Wählen Sie "English" aus und drücken Sie die Eingabetaste.
- h. Lesen Sie die Seiten mit der Lizenzvereinbarung. Verwenden Sie die Tabulatortaste, um <OK> auszuwählen, und drücken Sie die Eingabetaste, um weiterzublättern.
- i. Wählen Sie <Yes> aus und drücken Sie die Eingabetaste, um die Lizenzvereinbarung zu akzeptieren.
- j. Wenn die Extraktion abgeschlossen ist, drücken Sie die Eingabetaste auf <OK>, um zur Befehlszeile zurückzukehren.
- k. Notieren Sie die Installationsposition der RPMs.
- l. Installieren Sie die RPMs als Rootbenutzer.

```
[admin@localhost]$ sudo yum -y install rpms/*.rpm
```

Der Management-Server (PPM) zwar ist jetzt installiert, aber noch nicht konfiguriert. Führen Sie erst nach Abschluss der Konfiguration einen Neustart aus.

Ein detaillierte Beschreibung der einzelnen Schritte finden Sie im Abschnitt *Produktinstallation* in der Veröffentlichung *IBM Multi-Cloud Data Encryption Verwaltung*.

4 Schritt 4: Standardsprache konfigurieren



Die unterstützten Sprachen wurden bei der RPM-Installation auf der Management-Server-VM installiert.

Installationsschritte:

- a. Führen Sie das Script `spsd-langsetup` wie folgt aus:

```
$ sudo /opt/securityfirst/spsd/bin/spsd-langsetup
```

- b. Zeigen Sie den aktuellen Standardsprachencode an. Ist kein Sprachencode festgelegt, ist dieser Wert leer.
- c. Zeigen Sie die Liste der verfügbaren Sprachencodes an.
- d. Geben Sie den neuen Standardsprachencode ein, zum Beispiel **de_DE**.
- e. Führen Sie das Script 'spsd-langsetup' erneut aus, um zu überprüfen, ob der Standardsprachencode festgelegt ist. In diesem Beispiel wird die Nachricht "Der aktuelle Standardwert ist: **de_DE**" angezeigt.

5 Schritt 5: Datenbank konfigurieren



Bevor MDE zum ersten Mal gestartet werden kann, muss eine interne oder externe Datenbank konfiguriert werden. Die interne Datenbank unterstützt nur PostgreSQL. Sie wird als vordefinierter Bestandteil des OVA ausgeliefert.

Gehen Sie wie folgt vor, um die Datenbank für die Arbeit mit MDE zu konfigurieren:

Führen Sie das Script `spsd-pgsetup` mit der Scriptoption `"--local"` aus. Mit der Option `"local"` wird eine neue, leere Datenbank auf dem internen lokalen PostgreSQL-Server konfiguriert. Führen Sie den Befehl wie folgt aus:

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --local
```

Informationen zum Installieren einer externen Datenbank finden Sie im Abschnitt *Datenbank konfigurieren* in der Veröffentlichung *IBM Multi-Cloud Data Encryption Verwaltung*.

6 Schritt 6: Zertifikate konfigurieren



Zertifikate werden verwendet, um eine sichere Kommunikationssitzung zwischen dem Management-Server (PPM) und Verschlüsselungsagenten sowie Web-Browsern einzurichten. Für PPM ist erforderlich, dass alle Zertifikate von einer Zertifizierungsstelle (Certificate Authority - CA) unterzeichnet sind. Die CA stellt einen Ausgangspunkt für das Vertrauen her, den alle Kommunikationsteilnehmer zum Verifizieren der Identität der anderen Teilnehmer verwenden.

- Das unterzeichnete CA-Zertifikat wird zusammen mit dem zugehörigen Schlüssel zu einem Java-Keystore zusammengefasst.
- Das von der CA zum Unterzeichnen der Agentenzertifikate verwendete Zertifikat (oder Zertifikatspaket) muss zu einem PPM-Truststore hinzugefügt werden.
- Im untenstehenden Beispiel für einen Einrichtungsprozess für ein PPM-Zertifikat werden alle drei Komponenten (Keystore, Truststore und CA-Zertifikatspaket) verwendet.

In diesem Beispiel wurden alle Zertifikatsdateien in das Verzeichnis `/etc/ppm/certs` auf der Management-Server-VM kopiert. In Klammern eingefasste Namen sind Beispielnamen.

Führen Sie das folgende Script aus, um einen Keystore, einen Truststore und ein CA-Paket zu konfigurieren:

Keystore:

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --ks /etc/ppm/certs/[ppm.jks] --  
kw password
```

Truststore:

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --ts /etc/ppm/certs/[trust.jks] --  
tw password
```

CA-Paket:

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --aca /etc/ppm/certs/  
[ca_bundle.pem]
```

Weitere Informationen zum Einrichten von Zertifikaten finden Sie unter *Einstellungen für Serverzertifikate* und *Anhang: Beispielzertifikate einer Zertifizierungsstelle (CA)* in der Veröffentlichung *IBM Multi-Cloud Data Encryption Verwaltung*.

7 Schritt 7: Neustart des Systems durchführen



Nachdem Sie PPM installiert, eine Datenbank konfiguriert, Zertifikate hinzugefügt und optional PKI festgelegt haben, können Sie nun die MDE-Management-Server-VM erneut starten.

8 Schritt 8: An der Konsole anmelden



Starten Sie die virtuelle Maschine nach der Bereitstellung über die Hypervisorschnittstelle. Sie müssen die IP-Adresse der virtuellen Maschine ermitteln.

Öffnen Sie die Management-Server-VM, melden Sie sich als Administrator (admin) an und zeigen Sie die IP-Adresse der MDE-Management-Server-VM an. Führen Sie dazu den Befehl "ip address" aus.

Geben Sie den folgenden Befehl auf einem unterstützten Browser ein, um auf die Managementkonsole zuzugreifen:

`https://<<ip-adresse des MDE-servers>>`

Unter dieser Adresse öffnet der Browser die Anmeldeseite von MDE, auf der Sie aufgefordert werden, sich anzumelden.

Die folgenden Standardberechtigungsanforderungen gelten für die erste Anmeldung. Sie müssen nach der Anmeldung geändert werden.

Benutzername: admin

Kennwort: admin

Wenn Sie die PKI-Clientauthentifizierung verwenden, wird das Dashboard möglicherweise sofort geöffnet, ohne dass die Anmeldeseite angezeigt wird. (Weitere Informationen finden Sie im Abschnitt *PKI-Einstellungen* in der Veröffentlichung *IBM Multi-Cloud Data Encryption Verwaltung*.)

Nach der Anmeldung können Sie mit der Verwendung von IBM Multi-Cloud Data Encryption beginnen, indem Sie einen Verschlüsselungsagenten bereitstellen.

Es gibt vier Typen von Verschlüsselungsagenten: Agenten des Typs 'Datei mit Richtlinie', Agenten des Typs 'Datenträger', Agenten des Typs 'Datenträger mit Richtlinie' und Agenten des Typs 'Objektspeicher'. Diese Agenten werden einem unterstützten Agentenbetriebssystem bereitgestellt. Weitere Informationen hierzu finden Sie im Abschnitt 'Voraussetzungen'. Genauere Informationen zur Agentenbereitstellung Sie im Abschnitt *Agentenbereitstellung und Agentenmanagement* in der Veröffentlichung *IBM Multi-Cloud Data Encryption Verwaltung*.

Weitere Informationen



Weitere Informationen finden Sie bei der Produktunterstützung für IBM Multi-Cloud Data Encryption unter <https://www.ibm.com/support/home/>.

