

## Guía de inicio rápido

*Esta guía sirve de iniciación a una instalación típica de IBM Multi-Cloud Data Encryption.*

### Visión general del producto

IBM Multi-Cloud Data Encryption (MDE) es un producto completo para la seguridad de los datos que está basado en la tecnología SPx® y que combina el cifrado de datos almacenados con las potentes funciones de protección de un Policy Provisioning Manager (PPM). PPM hace de consola de servidor de gestión que permite proporcionar agentes de cifrado, valores de política de acceso a datos, gestión de ciclo de vida de claves, actualizaciones de agente y registro de accesos de usuario hasta 25.000 agentes desde una única ubicación central.

### 1 Paso 1: Acceder al software y la documentación



- Descargue OVA para Multi-Cloud Data Encryption desde Passport Advantage.
- Revise las Notas del release para Multi-Cloud Data Encryption antes de la instalación.
- Para obtener la documentación completa, consulte el IBM Knowledge Center ([https://www.ibm.com/support/knowledgecenter/SSTD4E\\_2.3.0/doc/kc\\_welcome\\_mde23.html](https://www.ibm.com/support/knowledgecenter/SSTD4E_2.3.0/doc/kc_welcome_mde23.html)). La documentación también se incluye con el producto.

### 2 Paso 2: Evaluar la configuración de hardware y del sistema



Asegúrese de que se cumplen los requisitos siguientes:

- a. Servidor operativo con sistema operativo bajo licencia e hipervisor soportado (VMware ESXi™) para desplegar y ejecutar PPM.
- b. OVA base empaquetado
- c. Programa de instalación de PPM
- d. Uno o más servidores de destino con sistema operativo de agente soportado (Red Hat® / CentOS 6.2+ o 7.2+, AIX 7.1 o 7.2, y Microsoft Windows Server® 2008 R2, Microsoft Windows Server® 2012 R2 o Microsoft Windows Server® 2016.
- e. Navegadores: Google Chrome®, Microsoft Internet Explorer® 10+, Mozilla Firefox® ESR 52+.
- f. Acceso de red entre PPM y todos los agentes.
- g. Certificados firmados de autoridad de certificado (almacén de claves, de confianza y paquete de certificados CA) para sesión segura entre Servidor de gestión (PPM) y todos los agentes.

Para Object Store Agent (OSA), los siguientes son requisitos adicionales:

- Almacenamiento de objetos compatible con S3: Amazon Web Services S3 (AWS S3), IBM Cloud Object Storage (COS S3)
- Credenciales del almacenamiento de objetos: ID de usuario y clave secreta (contraseña)
- Una aplicación o programa de utilidad que aprovecha la biblioteca de la API de REST AWS S3 o la biblioteca de Boto Python para apuntar datos al agente de OSA

Para obtener información completa, consulte las secciones *Consideraciones sobre la planificación*, *Valores de certificado de servidor* y el *Apéndice II: Certificados de muestra de entidad emisora* en la publicación *IBM Multi-Cloud Data Encryption, Guía del administrador*.

### 3 Paso 3: Instalar IBM Multi-Cloud Data Encryption



Instale MDE PPM, la configuración de la base de datos interna y la configuración de certificado.

En el archivo de ejemplo `ibm_sw_mde_X.x.x-XX.bin`, sustituya X por el nombre de archivo, la versión y los números de nivel de compilación.

- a. Despliegue el paquete OVA base de MDE en el hipervisor. En este ejemplo, se llama "VM del Servidor de gestión".
- b. Inicie una sesión como administrador y establezca una contraseña nueva.

Los OVA utilizan criterios estándar de PAM que el administrador puede configurar. La contraseña de PAM debe tener más de 8 caracteres y no puede contener 5 de los caracteres de la contraseña anterior.

- c. Anote la dirección IP de la máquina virtual de MDE.
- d. Cargue `ibm-sw_mde_X.x.x-xx.bin` en MDE mediante `scp` o un método parecido.
- e. Convierta el archivo `bin` en ejecutable.

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

- f. Ejecute el archivo `bin`.

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

- g. Seleccione "English" y pulse Intro.
- h. Lea las páginas del Acuerdo de licencia utilizando la tecla de tabulación <Aceptar>, pulse Intro para avanzar.
- i. Seleccione <Yes> y pulse Intro para aceptar el Acuerdo de licencia.
- j. Una vez completada la extracción, pulse Intro en <Aceptar> para volver a la línea de mandatos.
- k. Anote la ubicación de instalación de `rpm`.
- l. Instale los RPM como usuario `root`.

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

El servidor de gestión (PPM) está ahora instalado, pero no configurado. No rearranque hasta completar la configuración.

Para conocer los pasos detallados, consulte la sección *Instalación del producto* en la publicación *IBM Multi-Cloud Data Encryption, Guía del administrador*.

### 4 Paso 4: Configurar el idioma predeterminado



Los idiomas soportados se han instalado durante la instalación de RPM en la máquina virtual del Servidor de gestión, descrita más arriba.

Pasos de instalación:

- a. Ejecute el script `spsd-langsetup`:

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

- b. Vea el código de idioma predeterminado actual. Si no hay ninguno establecido, se muestra en blanco.
- c. Vea la lista de códigos de idioma disponibles.
- d. Escriba el nuevo código de idioma predeterminado: **en\_US** (ejemplo).
- e. Vuelva a ejecutar el script `spsd-language` para comprobar que el código de idioma predeterminado esté establecido. De acuerdo con el ejemplo, muestra "El valor predeterminado actual es: **en\_US**".

### 5 Paso 5: Configurar la base de datos



Es necesario configurar una base de datos interna o externa antes de iniciar MDE por primera vez. La base de datos interna solamente es compatible con PostgreSQL y se entrega en el paquete de OVA.

Para configurar la base de datos para que trabaje con MDE:

Ejecute el script `spsd-pgsetup` con la opción de script `"--local"`. La opción `local` configura una nueva base de datos vacía en el servidor `--local` de PostgreSQL.

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

Si instala una base de datos externa, consulte la sección, *Configuración de base de datos* en la publicación *IBM Multi-Cloud Data Encryption, Guía del administrador*.

## 6 Paso 6: Configurar certificados



Se utilizan certificados para establecer una sesión de comunicación segura entre el Servidor de gestión (PPM) y los agentes de cifrado y navegadores web. PPM necesita que todos los certificados estén firmados por una entidad emisora de certificados. La entidad emisora de certificados establece una raíz de confianza que es utilizada por todos los participantes en la sesión de comunicación para verificar la identidad del interlocutor.

- El certificado firmado de la entidad emisora y la clave correspondiente se combinan en un almacén de claves Java.
- El certificado (o paquete de certificados) de la entidad emisora que se utiliza para firmar los certificados del agente debe añadirse al almacén de confianza de PPM.
- Los tres componentes (almacén de claves, almacén de confianza y paquete de certificados de entidad emisora) se utilizan en el proceso de configuración de certificados de PPM, descrito más abajo.

En este ejemplo, todos los archivos de certificado se han copiado en /etc/ppm/certs en la vm del servidor de gestión. Los nombres entre corchetes son nombres de ejemplo.

Para configurar un almacén de claves, un almacén de confianza y un paquete de entidad emisora de certificados, ejecute:

Para el almacén de claves:

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

Para el almacén de confianza:

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

Para el paquete de entidad emisora de certificados:

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

Para obtener más información sobre la configuración de certificados, consulte las secciones *Valores de certificado de servidor* y el *Apéndice: Certificados de muestra de entidad emisora* en la publicación *IBM Multi-Cloud Data Encryption, Guía del administrador*.

## 7 Paso 7: Rearrancar



Después de instalar PPM, configurar una base de datos, añadir certificados y opcionalmente establecer valores de PKI, ahora puede rearrancar la máquina virtual del Servidor de gestión de MDE.

## 8 Paso 8: Iniciar sesión en la consola



Una vez desplegada, inicie la máquina virtual mediante la interfaz del hipervisor. Necesitará obtener la dirección IP de la máquina virtual.

Abra la VM del servidor de gestión, inicie la sesión como administrador y visualice la dirección IP de la VM del servidor de gestión de MDE ejecutando el mandato “ip address”.

Para acceder a la consola de gestión, especifique lo siguiente en un navegador soportado:

`https://<<dirección IP de servidor de MDE>>`

Este enlace dirige el navegador hasta la página de inicio de sesión de MDE, donde podrá iniciar una sesión.

Estas son las credenciales predeterminadas para el primer inicio de sesión y se deben cambiar tras iniciar la sesión:

Nombre de usuario: admin

Contraseña: admin

Observe que cuando se utiliza la autenticación de cliente de PKI, puede aparecer el panel de control sin pasar por la página de inicio de sesión. (Consulte la sección *Valores de infraestructura de clave pública (PKI)* en la publicación *IBM Multi-Cloud Data Encryption, Guía del administrador*.

Después de iniciar la sesión, está preparado para utilizar IBM Multi-Cloud Data Encryption mediante el suministro de un Agente de cifrado.

Hay cuatro tipos de Agentes de cifrado: Archivo con agente de política, Agente de volumen, Volumen con agente de política y Agente de almacén de objetos. Estos agentes se suministran a un sistema operativo de agente soportado (vea Requisitos previos). Para obtener información específica sobre el suministro de agentes, consulte la sección *Suministro y gestión de agentes* en la publicación *IBM Multi-Cloud Data Encryption, Guía del administrador*.

## Más información



Para obtener más información, consulte Soporte de producto para IBM Multi-Cloud Data Encryption, en <https://www.ibm.com/support/home/>.

