

빠른 시작 안내서

이 안내서를 사용하면 일반 *IBM Multi-Cloud Data Encryption* 설치를 시작할 수 있습니다.

제품 개요

IBM Multi-Cloud Data Encryption(MDE)은 PPM(Policy Provisioning Manager)의 강력한 보호 기능과 저장 데이터 암호화를 결합하는 SPx® 기술을 기반으로 하는 포괄적인 데이터 보안 제품입니다. PPM은 단일 중앙 위치에서 최대 25,000개의 에이전트에 대해 암호화 에이전트의 프로비저닝, 데이터 액세스 정책 설정, 키 라이프사이클 관리, 에이전트 업데이트 및 사용자 액세스 로깅을 가능하게 하는 관리 서버 콘솔의 역할을 합니다.

1 단계 1: 소프트웨어 및 문서 액세스



- Passport Advantage®에서 Multi-Cloud Data Encryption에 대한 OVA를 다운로드하십시오.
- 설치 전에 Multi-Cloud Data Encryption에 대한 릴리스 정보를 검토하십시오.
- 전체 문서는 IBM Knowledge Center(https://www.ibm.com/support/knowledgecenter/SSTD4E_2.3.0/doc/kc_welcome_mde23.html)를 참조하십시오. 문서는 제품과도 함께 제공됩니다.

2 단계 2: 하드웨어 및 시스템 구성 평가



다음 요구사항이 충족되는지 확인하십시오.

- a. PPM을 실행하고 배치하기 위한 라이선스가 있는 운영 체제 및 지원되는 하이퍼바이저(VMware ESXi™)가 포함된 운영 서버
- b. 패키징된 기본 OVA
- c. PPM 설치 프로그램
- d. 지원되는 에이전트 운영 체제(Red Hat®/CentOS 6.2+ 또는 7.2+, AIX 7.1 또는 7.2 및 Microsoft Windows Server® 2008 R2, Microsoft Windows Server® 2012 R2 또는 Microsoft Windows Server® 2016)가 포함된 하나 이상의 대상 서버.
- e. 브라우저: Google Chrome®, Microsoft Internet Explorer® 10+, Mozilla Firefox® ESR 52+.
- f. PPM과 모든 에이전트 간의 네트워크 액세스
- g. 관리 서버(PPM)와 모든 에이전트 간의 보안 세션을 확립하기 위한 인증 기관에서 서명한 인증서(키 저장소, 신뢰 저장소 및 CA 인증서 번들).

오브젝트 저장소 에이전트(OSA)의 경우 추가 요구사항은 다음과 같습니다.

- S3 호환 가능 오브젝트 스토리지: Amazon Web Services S3(AWS S3), IBM Cloud Object Storage(COS S3)
- 오브젝트 스토리지 신임 정보: 사용자 ID 및 비밀번호(비밀번호)
- AWS S3 REST API Library 또는 Boto Python Library를 활용하여 OSA 에이전트에 대한 데이터를 나타내는 애플리케이션 또는 유틸리티

전체 정보는 *IBM Multi-Cloud Data Encryption* 관리자 안내서의 계획 고려사항, 서버 인증서 설정 및 부록: 샘플 인증 기관(CA) 인증서 절을 참조하십시오.

3 단계 3: IBM Multi-Cloud Data Encryption 설치



MDE PPM, 내부 데이터베이스 구성 및 인증서 설정을 설치하십시오.

예제(ibm_sw_mde_X.x.x-XX.bin 파일)를 사용하여 X를 파일 이름, 버전, 빌드 번호로 대체하십시오.

- MDE 기반 OVA를 하이퍼바이저에 배치하십시오. 이 예제에서 이는 "관리 서버 VM"이라고 합니다.
- admin으로 로그인한 후 비밀번호를 새로 설정하십시오.

OVA에서는 관리자가 구성할 수 있는 PAM 표준 기준을 사용합니다. PAM 비밀번호는 9자 이상이어야 하고 이전 비밀번호의 5자가 포함될 수 없습니다.

- MDE VM의 IP 주소를 기록해 두십시오.
- scp 또는 유사한 방법으로 ibm-sw_mde_X.x.x-xx.bin을 MDE로 업로드하십시오.
- 바이너리 파일을 실행 가능하도록 설정하십시오.

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

- 바이너리 파일을 실행하십시오.

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

- "English"를 선택하고 Enter를 누르십시오.
- 라이선스 페이지를 읽고 <OK>로 탭한 다음 Enter를 눌러 계속 진행하십시오.
- <Yes>를 선택하고 Enter를 눌러 라이선스 계약에 동의하십시오.
- 추출이 완료되면 <OK>에서 Enter를 눌러 명령행으로 돌아가십시오.
- rpm 설치 위치를 기록해 두십시오.
- RPM을 루트로 설치하십시오.

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

이제 관리 서버(PPM)가 설치되었지만 아직 구성되지는 않았습니다. 구성이 완료될 때까지는 재부팅하지 마십시오.

자세한 단계는 *IBM Multi-Cloud Data Encryption* 관리자 안내서의 제품 설치 절을 참조하십시오.

4 단계 4: 기본 언어 구성



지원 언어는 관리 서버 VM에 rpm 설치 시에 설치되었습니다.

설치 단계:

- spsd-langsetup 스크립트를 실행하십시오.

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

- 현재 기본 언어 코드를 보십시오. 설정된 언어 코드가 없는 경우에는 공백입니다.
- 사용 가능한 언어 코드 목록을 보십시오.
- 새 기본 언어 코드(예: **en_US**)를 입력하십시오.
- spsd-language 스크립트를 다시 실행하여 기본 언어 코드가 설정되었는지 유효성 검증하십시오. 예제에서와 같이 "현재 기본값: **en_US**"로 표시됩니다.

5 단계 5: 데이터베이스 구성



MDE를 처음으로 시작하기 전에 내부 또는 외부 데이터베이스를 구성해야 합니다. 내부 데이터베이스는 PostgreSQL만 지원하며 OVA에서 사전 패키지로 제공됩니다.

MDE에서 작동하도록 데이터베이스를 구성하려면 다음을 수행하십시오.

""--local" 스크립트 옵션을 지정하여 spsd-pgsetup 스크립트를 실행하십시오. 이 로컬 옵션은 내부 "--local" PostgreSQL Server에서 새로운 빈 데이터베이스를 구성합니다.

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

외부 데이터베이스를 설치하는 경우 *IBM Multi-Cloud Data Encryption* 관리자 안내서의 데이터베이스 설정 절을 참조하십시오.

6 단계 6: 인증서 구성



인증서는 관리 서버(PPM)와 암호화 에이전트 및 웹 브라우저 사이에서 보안 통신 세션을 설정하는 데 사용됩니다. PPM의 경우, 모든 인증서는 인증 기관(CA)에서 서명해야 합니다. CA는 통신 세션의 모든 관계자가 다른 파티의 ID를 검증하는 데 사용하는 신뢰 루트를 설정합니다.

- CA 서명 인증서와 해당 키는 java 키 저장소에 결합됩니다.
- 에이전트 인증서의 서명에 사용된 CA의 인증서(또는 인증서 번들)를 PPM 신뢰 저장소에 추가해야 합니다.
- 이 세 구성요소(키 저장소, 신뢰 저장소, CA 인증서 번들)는 아래 PPM 설정 프로세스에서 사용됩니다.

이 예제에서 모든 인증서 파일은 관리 서버 vm의 /etc/ppm/certs를 복사되었습니다. 대괄호로 표시된 이름은 예제 이름입니다.

키 저장소, 신뢰 저장소 및 CA 번들을 구성하려면 다음을 실행하십시오.

키 저장소의 경우:

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

신뢰 저장소의 경우:

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

CA 번들의 경우:

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

인증서 설정에 관한 자세한 정보는 *IBM Multi-Cloud Data Encryption* 관리자 안내서의 서버 인증서 설정 및 부록: 샘플 인증 기관(CA) 인증서 절을 참조하십시오.

7 단계 7: 재부팅



PPM 설치, 데이터베이스 구성, 인증서 추가, 선택적으로 PKI 설정 후에 이제 MDE 관리 서버 VM을 재부팅할 수 있습니다.

8 단계 8: 콘솔에 로그인



배치되고 나면 하이퍼바이저 인터페이스를 통해 가상 머신을 시작하십시오. 가상 머신의 IP를 검색해야 합니다.

관리 서버 VM을 열고 admin으로 로그인한 후 “ip address” 명령을 실행하여 MDE 관리 서버 VM의 IP 주소를 표시하십시오.

관리 콘솔에 액세스하려면 지원되는 브라우저에서 다음을 입력하십시오.

`https://<<MDE Server IP>>`

그러면 브라우저가 로그인하도록 프롬프트되는 MDE 로그인 페이지로 연결됩니다.

첫 번째 로그인에 대한 기본 신임 정보는 다음과 같으며 로그인 후에 변경해야 합니다.

사용자 이름: admin

비밀번호: admin

PKI 클라이언트 인증 사용 시 대시보드가 로그인 페이지를 생략한 채로 표시될 수 있습니다. (*IBM Multi-Cloud Data Encryption* 관리자 안내서의 공개 키 인프라(PKI) 설정을 참조하십시오.

로그인한 후에는 암호화 에이전트를 프로비저닝하여 IBM Multi-Cloud Data Encryption을 사용할 준비가 됩니다.

암호화 에이전트에는 네 가지 유형, 즉 정책이 적용된 파일 에이전트, 볼륨 에이전트, 정책이 적용된 볼륨 에이전트 및 오브젝트 저장소 에이전트가 있습니다. 이러한 에이전트는 지원되는 에이전트 운영 체제(전제조건 참조)로 프로비저닝됩니다. 에이전트 프로비저닝에 관한 구체적인 정보는 *IBM Multi-Cloud Data Encryption* 관리자 안내서의 에이전트 프로비저닝 및 관리 절을 참조하십시오.

자세한 정보



자세한 정보는 IBM Multi-Cloud Data Encryption 제품 지원(<https://www.ibm.com/support/home/>)을 참조하십시오.

IBM® Multi-Cloud Data Encryption, Version 2.3 Licensed Materials - Property of IBM. © Copyright IBM Corporation and others 2017, 2019. US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

SPx 및 Security First Corp는 전세계 여러 국가에서 등록된 Security First Corp.의 상표 또는 등록 상표입니다. 기타 제품 또는 서비스 이름은 Security First Corp. 또는 타사의 상표입니다.

IBM, IBM 로고 및 ibm.com®은 전세계 여러 국가에 등록된 International Business Machines Corp.의 상표 또는 등록상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다.

현재 IBM 상표 목록은 웹 "[저작권 및 상표 정보](http://www.ibm.com/legal/copytrade.shtml)"(www.ibm.com/legal/copytrade.shtml)에 있습니다.

문서 번호: GC43-5056-01

