

IBM Multi-Cloud Data Encryption
SPx[®] 기반
버전 2.3

자주 묻는 질문(*FAQ*)



참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에 [11 페이지의 『주의사항』](#)의 정보를 읽으십시오.

이 개정판은 새 개정판에서 별도로 명시하지 않는 한 IBM Multi-Cloud Data Encryption 버전 2.3(제품 번호 5737-C67) 및 모든 후속 릴리스와 수정에 적용됩니다.

© 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.

© **Copyright International Business Machines Corporation .**

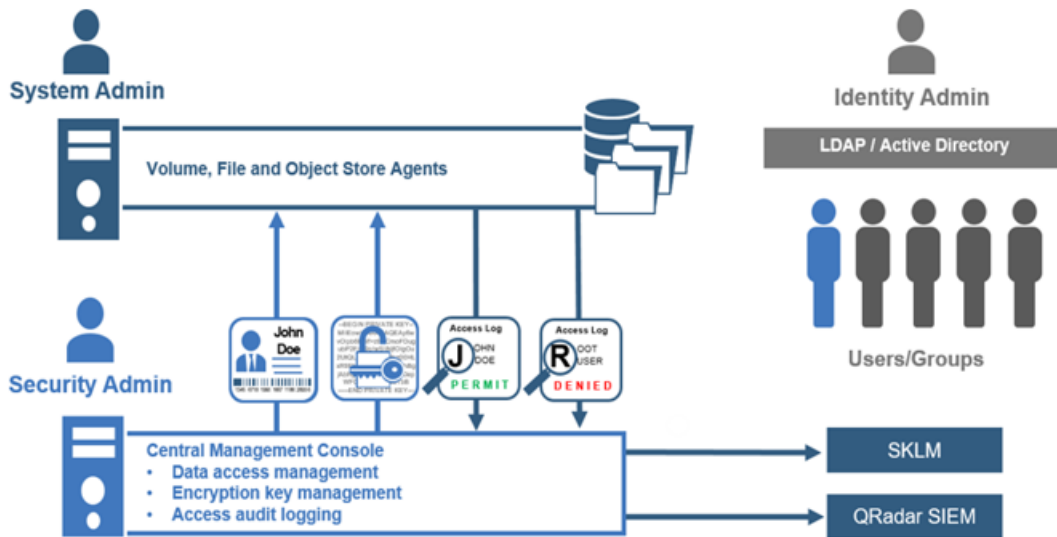
목차

| | |
|---|---|
| 제 1 장 개요..... | 1 |
| 제 2 장 MDE - 자주 묻는 질문(FAQ)..... | 3 |
| 일반 FAQ..... | 3 |
| Q: IBM Multi-Cloud Data Encryption(MDE)은 무엇입니까?..... | 3 |
| Q: IBM Multi-Cloud Data Encryption(MDE)에서 지원되는 운영 체제는 무엇입니까?..... | 3 |
| Q: MDE 에이전트에서 지원하는 파일 시스템은 무엇입니까?..... | 3 |
| Q: IBM Multi-Cloud Data Encryption(MDE)에 사전 설치 소프트웨어가 필요합니까? | 3 |
| Q: IBM MDE(Multi-Cloud Data Encryption)에서 지원되는 브라우저는 무엇입니까?..... | 3 |
| Q: IBM Multi-Cloud Data Encryption(MDE)이 FIPS 모드로 실행됩니까?..... | 3 |
| Q: Multi-Cloud Data Encryption(MDE) 사용 시에 원격 시스템으로 데이터를 전송할 때 암호화해야 합니까? 원격 시스템에 대해 VPN 연결이 계속 필요합니까? | 4 |
| Q: IBM Multi-Cloud Data Encryption(MDE)이 "비트 레벨에서 데이터에 보안을 접목"한다는 것은 무슨 말입니까?..... | 4 |
| Q: 데이터 무결성이 IBM Multi-Cloud Data Encryption(MDE)으로 유지보수되는 방법을 설명해 주십 시오..... | 4 |
| 정책, 프로비저닝, 관리 FAQ..... | 4 |
| Q: 정책, 프로비저닝, 관리(PPM)의 목적은 무엇입니까?..... | 4 |
| Q: 정책, 프로비저닝, 관리(PPM)가 역할 기반 액세스 제어를 사용하는 이유가 무엇입니까?..... | 4 |
| Q: 정책, 프로비저닝 및 관리(PPM) 콘솔에서 프로세스란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?..... | 4 |
| Q: 정책, 프로비저닝, 관리(PPM) 콘솔에서 선택자란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?..... | 4 |
| Q: 정책, 프로비저닝 및 관리(PPM) 콘솔에서 경로 세트란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?..... | 5 |
| Q: 정책, 프로비저닝, 관리(PPM) 콘솔에서 데이터 유형이란 무엇입니까? 그리고, 어떤 용도로 사용됩니 까?..... | 5 |
| Q: 정책, 프로비저닝, 관리(PPM) 콘솔에서 에이전트란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?..... | 5 |
| Q: 볼륨 에이전트를 언제 사용해야 합니까? 그리고 작동 방식은 어떻게 됩니까?..... | 5 |
| Q: 정책이 적용된 파일 에이전트를 언제 사용해야 합니까? 그리고 작동 방식은 어떻게 됩니까?..... | 5 |
| Q: 정책이 적용된 볼륨 에이전트를 언제 사용해야 합니까? 그리고 작동 방식은 어떻게 됩니까?..... | 5 |
| Q: 오브젝트 저장소 에이전트를 반드시 사용해야 하는 경우는 언제입니까? 그리고, 작동 방식은 어떻게 됩니까?..... | 6 |
| Q: 정책, 프로비저닝, 관리(PPM) 콘솔에서 작업이란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?..... | 6 |
| Q: IBM Multi-Cloud Data Encryption의 경우, 외부 PostgreSQL 데이터베이스를 사용하는 시기는 언제입니까? | 6 |
| 인증서 FAQ..... | 6 |
| Q: PPM 서버 인증서의 요구사항은 무엇입니까?..... | 6 |
| Q: 에이전트 인증서에 대한 요구사항은 무엇입니까?..... | 6 |
| Q: PPM에서 NAT(네트워크 주소 변환) 또는 PAT(포트 주소 변환) 연결을 지원합니까?..... | 6 |
| Q: NAT(Network Address Translation) 또는 PAT(Port Address Translation) 네트워크 구성에서 PPM 서버의 PPM 서버 인증서를 어떻게 구성합니까?..... | 6 |
| Q: 에이전트가 NAT(Network Address Translation) 또는 PAT(Port Address Translation) 네트워 크 구성으로 되어 있는 경우 에이전트 인증서를 어떻게 구성합니까?..... | 7 |
| Q:고가용성(HA) 구성에서 PPM 서버 인증서에 대한 요구사항은 무엇입니까?..... | 7 |
| 키 및 키 처리 FAQ..... | 7 |
| Q: IBM Multi-Cloud Data Encryption이 수행할 수 있는 키 처리 조작은 무엇입니까?..... | 7 |
| Q: 키를 로테이션해야 하는 이유는 무엇입니까?..... | 7 |
| Q: 키를 취소해야 하는 이유는 무엇입니까?..... | 7 |
| Q: 키를 폐기해야 하는 이유는 무엇입니까?..... | 7 |
| Q: IBM Multi-Cloud Data Encryption이 키를 관리합니까?..... | 7 |
| 설치 및 설정 FAQ..... | 7 |

| | |
|---|-----------|
| Q: IBM Multi-Cloud Data Encryption(MDE)이 일반 사용자(예: 관리자가 아닌 사용자)에게 주는 영향은 무엇입니까? | 8 |
| Q: MDE 에이전트를 Docker 호스트에 설치하고 이를 통해 Docker 컨테이너에 있는 애플리케이션의 모든 읽기/쓰기 요청을 처리할 수 있습니까? | 8 |
| 구성 FAQ | 8 |
| Q: IBM Multi-Cloud Data Encryption(MDE)를 사용하여 HTML 파일을 암호화할 수 있습니까? | 8 |
| 운영 FAQ | 8 |
| Q: IBM Multi-Cloud Data Encryption(MDE)으로 데이터가 보호되는지 여부를 확인하는 방법은 무엇입니까? | 8 |
| Q: IBM Multi-Cloud Data Encryption(MDE) 프로덕션 구현을 변경하기 전에 수행해야 하는 예방책은 무엇입니까? | 8 |
| Q: IBM Multi-Cloud Data Encryption(MDE)에서 다른 SIEM(Security Information and Event Management) 상관 애플리케이션으로 이벤트를 전송할 수 있습니까? | 8 |
| Q: 대소문자 구분이 중요합니까? | 8 |
| Q: 조작 순서는 무엇을 의미하고 왜 중요합니까? | 9 |
| Q: 스냅샷 활성화 작업을 제출했고 이 작업이 아직도 실행 중입니다. 이 작업은 언제 완료됩니까? | 9 |
| 고가용성 FAQ | 9 |
| Q: IBM Multi-Cloud Data Encryption(MDE) 배치에 대해 고가용성이 필요한 시기는 언제입니까? | 9 |
| Q: 고가용성(HA) IBM Multi-Cloud Data Encryption 배치에 로드 밸런서가 필요합니까? | 9 |
| 다중 테넌트 FAQ | 9 |
| Q: 다중 테넌트 기능의 용도는 무엇입니까? | 9 |
| 주의사항 | 11 |
| 상표 | 12 |
| 제품 문서의 이용 약관 | 13 |
| 개인정보처리방침 고려사항 | 13 |

제 1 장 개요

IBM Multi-Cloud Data Encryption(MDE)은 중앙 관리 콘솔로 작동하는 PPM(Policy Provisioning Manager)의 강력한 보호 기능과 저장 데이터(data-at-rest) 암호화를 결합하는 SPx® 기술을 기반으로 하는 포괄적인 데이터 보안 제품입니다. MDE를 사용하면 단일 중앙 집중식 위치에서 최대 25,000개의 에이전트에 대해 에이전트 프로 비저닝, 데이터 액세스 정책 설정(운영 및 암호화 액세스 정의) 및 관리(키 수명 주기, 에이전트 업데이트 및 사용자 액세스 로깅)가 가능합니다. MDE는 고유 암호 분할 기술을 사용하여 파일 시스템 레벨이나 볼륨 레벨에서 데이터를 암호화하는 에이전트를 지정하는 유연성을 완벽한 보안 시스템에 제공합니다. 또한 무차별 대입 공격이 통하지 않도록 데이터 암호화를 더 견고하게 만들어 표준 암호화보다 뛰어난 데이터 중심 보호를 제공합니다. 세분화된 액세스 정책을 정의하여 사용자 레벨에서 데이터 액세스를 제한하고 모니터링하고 감사하는 기능으로 한 차원 더 높은 보호 조치를 수행합니다.



MDE는 개별 관리자 역할(제품 관리자와 보안 관리자)을 업무 분리를 위해 제공합니다. 제품 관리자 역할은 MDE 제품을 구성하고 유지보수하는 데 필요한 권한을 위임받습니다. 보안 관리자 역할은 에이전트를 프로비저닝하고 관리하는 데 필요한 권한을 위임받습니다. 그림 1은 이러한 역할을 보여주며, 이는 7절: MDE 관리자 관리에서 자세히 논의됩니다.

보호되거나 암호화된 데이터의 정책 정의를 적용하는 네 가지 에이전트 유형을 배치할 수 있습니다. 볼륨 에이전트는 하나 이상의 보호된 볼륨의 볼륨 정책 정의 및 연관을 적용합니다. 정책이 적용된 파일 에이전트는 보호된 각 파일 경로가 세분화된 정책 스펙을 통해 정의된 대로 고유 운영 및 액세스 제어 정책을 포함할 수 있는 하나 이상의 보호된 파일 경로의 파일 기반 운영 액세스 정책 정의 및 연관을 적용합니다. 정책이 적용된 볼륨 에이전트에서는 볼륨 에이전트의 볼륨 정책 보호를 활용하고 파일 기반 운영 액세스 제어 정책을 하나 이상의 보호 파일 경로에 적용하고 강제할 수 있습니다. 그리고 오브젝트 저장소 에이전트는 하나 이상의 클라우드 기반 오브젝트 스토리지로 전송되는 데이터를 암호화하고 암호화된 방식으로 분할합니다.

제 2 장 MDE - 자주 묻는 질문(FAQ)

일반 FAQ

Q: IBM Multi-Cloud Data Encryption(MDE)은 무엇입니까?

A: MDE는 단일 중앙 집중식 위치에서 최대 25,000개의 에이전트에 대해 에이전트 프로비저닝, 정책(운영 및 암호화 액세스 정의) 및 관리(수명 주기 업데이트 및 사용자 감사)를 도입하고 사용 가능하게 합니다. MDE는 네 가지 에이전트 유형, 즉 볼륨, 정책이 적용된 파일, 정책이 적용된 볼륨, 오브젝트 저장소의 배치를 지원합니다. 해당 에이전트는 설치하기가 쉬우며 일반 사용자에게 끊임 없이 제공되고 관리자에게는 IT 환경 준수 요구사항을 충족하는 소프트웨어 구성 및 배치 기능을 제공합니다.

Q: IBM Multi-Cloud Data Encryption(MDE)에서 지원되는 운영 체제는 무엇입니까?

A: MDE는 현재 다음 운영 체제를 지원합니다.

- Red Hat® Enterprise Linux 6.2 커널 버전 2.6.32-220 및 후속 릴리스
- Red Hat® Enterprise Linux 7.2+ 커널 버전
- CentOS 6.2 커널 버전 2.6.32-220 및 후속 릴리스
- CentOS 7.2 커널 버전 및 후속 릴리스
- Microsoft Windows Server® 2008R2
- Microsoft Windows Server® 2012
- Microsoft Windows Server® 2012R2
- Microsoft Windows Server® 2016

Q: MDE 에이전트에서 지원하는 파일 시스템은 무엇입니까?

A: MDE는 다음 파일 시스템을 지원합니다.

- EXT3
- EXT4
- XFS(Red Hat®/CentOS 6.5 이상)
- NTFS
- ReFS

Q: IBM Multi-Cloud Data Encryption(MDE)에 사전 설치 소프트웨어가 필요합니까?

A: MDE는 VMware ESXi™ 또는 Microsoft Hyper-V에서 쉽게 배치되는 OVA로 제공되며 대부분의 다른 하이퍼바이저에서도 실행됩니다.

Q: IBM MDE(Multi-Cloud Data Encryption)에서 지원되는 브라우저는 무엇입니까?

A: MDE는 Mozilla Firefox, Google Chrome™, Microsoft Internet Explorer 및 Microsoft Edge에서 실행할 수 있습니다.

Q: IBM Multi-Cloud Data Encryption(MDE)이 FIPS 모드로 실행됩니까?

A: 예, MDE는 제품 데이터시트에 지정된 대로 FIPS 140.2 준수 표준을 준수합니다.

**Q: Multi-Cloud Data Encryption(MDE) 사용 시에 원격 시스템으로 데이터를 전송할 때 암호화해야
합니까? 원격 시스템에 대해 VPN 연결이 계속 필요합니까?**

A: MDE는 파일 위치에 액세스할 수 있는 경우 퍼블릭 클라우드 사이트를 비롯한 원격 사이트에 보안 상태로 데이터를 쓰도록 설계됩니다. 그러나 원격 사이트에 연결하려면 VPN이 필요할 수도 있습니다.

**Q: IBM Multi-Cloud Data Encryption(MDE)이 "비트 레벨에서 데이터에 보안을 접목"한다는 것은
무슨 말입니까?**

A: SPx 기술을 사용하는 MDE는 암호화, 비트 레벨에서 무작위로 키 입력된 데이터를 분할, 인증(무결성 검사), 결합 내구성, COI 프레임워크를 식별 가능한 데이터로 변환하는 프로세스로 결합하고 정보는 순수한 무작위의 사용 불가능한 2진 요소로 결합합니다. MDE 조작의 결과는 정보 보증(IA) 요소가 데이터의 기본으로 접목됩니다. 보안, 데이터 탄력성, 신뢰, 정보 공유 프레임워크 모두는 분리할 수 없게 되어 데이터에 포함됩니다. 데이터 및 정보 보호는 데이터 폐기 및/또는 공개 릴리스 수명 주기를 통해 작성 시점부터 보증됩니다. 데이터는 마지막으로 스토리지에 기록될 때까지 액세스될 때마다 보호됩니다.

**Q: 데이터 무결성이 IBM Multi-Cloud Data Encryption(MDE)으로 유지보수되는 방법을 설명해 주
십시오.**

A: 데이터 무결성은 읽어야 하는 데이터에 일치하는 메시지 인증 코드를 사용하여 보장됩니다.

정책, 프로비저닝, 관리 FAQ

Q: 정책, 프로비저닝, 관리(PPM)의 목적은 무엇입니까?

A: PPM은 단일 중앙 집중식 위치에서 최대 25,000개의 에이전트에 대해 에이전트 프로비저닝(데이터 보호 모델), 정책(운영 및 암호화 액세스 정의) 및 관리(수명 주기 업데이트 및 사용자 감사)를 관리합니다. 이는 네 가지 데이터 암호화 에이전트 유형, 즉 볼륨, 정책이 적용된 파일, 정책이 적용된 볼륨, 오브젝트 저장소의 배치를 지원합니다. 볼륨은 블록 디바이스 레벨에서 데이터를 보호합니다. 정책이 적용된 파일은 파일 레벨에서 데이터를 보호하고 파일 기반의 운영 액세스 제어를 제공합니다. 정책이 적용된 볼륨은 파일 기반 운영 액세스 제어를 같이 사용하여 블록 디바이스 레벨에서 데이터를 보호합니다. 오브젝트 저장소는 하나 이상의 클라우드 기반 오브젝트 스토리지로 전송되는 데이터를 암호화하고 암호화된 방식으로 분할합니다.

Q: 정책, 프로비저닝, 관리(PPM)가 역할 기반 액세스 제어를 사용하는 이유가 무엇입니까?

A: PPM은 일반 및 정적 역할 기반 액세스 제어(RBAC) 설계를 사용합니다. PPM 내의 기능에는 특정 권한이 필요합니다. 제품 관리자와 보안 관리자의 두 개별 역할이 있습니다. 공통되는 권한은 몇 개 없지만 역할 분할은 IT 담당자에게 관리 업무를 엄격하게 분할하도록 하여 사보타주 IT 환경에서 올바르게 많은 직원을 제거할 수 있습니다. 각 유형에 대한 추가 역할은 대형의 또는 더 복잡한 IT 환경을 적절하게 지원하도록 추가될 수 있습니다. 또한, 고객은 작업 승인에 필요한 몇 명의 관리자와 작업 거부에 필요한 몇 명의 관리자를 프로그래밍 방식으로 정의할 수도 있습니다. 따라서, 각 역할 세트에 대해 관리자 승인 및 거부가 PPM으로 추적되어 실행에 대한 충분한 승인이나 거부가 가능합니다. 요청된 관리자 수가 작업을 승인하면 실행됩니다. 필요한 수의 관리자가 작업을 거부하면(승인과 다를 수 있음) 작업이 취소됩니다. 이를 통해 관리 및 보안 관련 태스크가 정밀하게 제어됩니다. 승인 및/또는 거부의 순서 모두 추적되고 감사 및 준수를 위해 로깅됩니다.

Q: 정책, 프로비저닝 및 관리(PPM) 콘솔에서 프로세스란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?

A: 프로세스는 "정책을 통한 프로세스"라고도 하며 IBM Multi-Cloud Data Encryption으로 보호되는 데이터에 대한 액세스 제어가 지정되는 프로세스 또는 애플리케이션의 목록입니다. 프로세스는 선택자와 연결되어 대상 시스템에서 사용자를 통해 프로세스에 대한 액세스 제어를 제공합니다.

Q: 정책, 프로비저닝, 관리(PPM) 콘솔에서 선택자란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?

A: 선택자는 순서가 지정되지 않은 사용자, 그룹 및 프로세스의 목록입니다. 이는 데이터 유형과 결합하여 보안 관리자에게 공유하거나 MDE로 보호되는 데이터에 대한 공통 액세스 권한을 가진 엔티티 컬렉션을 식별하는 간단한 방법을 제공합니다. 선택자는 그룹 소스(내부 또는 LDAP가 정의된 경우는 외부) 또는 선택적 "정책을 통한 프로세스"와 함께 선택적 사용자, 선택적 그룹 필드로 구성될 수 있습니다.

Q: 정책, 프로비저닝 및 관리(PPM) 콘솔에서 경로 세트란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?

A: 경로 세트는 MDE 정책으로 보호(또는 정책에 따라 정책 보호에서 잠재적으로 제외)되는 순서가 지정되지 않은 파일 경로 목록입니다. 이는 보안 관리자에게 MDE로 보호되는 파일 경로에 대한 컬렉션을 지정 또는 나열하는 간단한 방법을 제공합니다. 경로 세트를 지정하는 경우 보안 관리자는 경로 컬렉션의 이름을 작성해야 합니다. 보호는 제공된 경로에서부터 아래로 모든 하위 디렉토리를 통해 재귀적으로 적용됩니다. 참고 필드는 선택사항입니다.

Q: 정책, 프로비저닝, 관리(PPM) 콘솔에서 데이터 유형이란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?

A: 데이터 유형은 지정한 데이터 유형에 지정된 액세스 정의 행에 대해 순서가 지정된 목록입니다. 각 행은 선택자, I/O 조작, 조치 정의, 연관된 키로 구성됩니다. 에이전트를 작성할 때 데이터 유형은 파일 경로(또는 경로 세트)와 연관되어 데이터의 운영 및 암호화 액세스 제어를 정의합니다.

Q: 정책, 프로비저닝, 관리(PPM) 콘솔에서 에이전트란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?

A: PPM은 네 가지 유형의 에이전트를 지원하며, 각각은 서로 다른 유형의 보호를 제공합니다. 지원되는 에이전트는 볼륨, 정책이 적용된 파일, 정책이 적용된 볼륨 및 오브젝트 저장소입니다. 볼륨은 볼륨 레벨에서 데이터를 보호합니다. 정책이 적용된 파일은 파일 레벨에서 데이터를 보호하며 파일 기반의 운영 액세스 제어 및 선택적 암호화 액세스 제어를 제공합니다. 정책이 적용된 볼륨은 볼륨 레벨에서 데이터를 보호하며 파일 기반의 운영 액세스 제어를 제공합니다. 오브젝트 저장소는 하나 이상의 클라우드 기반 오브젝트 스토리지로 전송되는 데이터를 암호화하고 암호화된 방식으로 분할합니다.

Q: 볼륨 에이전트를 언제 사용해야 합니까? 그리고 작동 방식은 어떻게 됩니까?

A: 볼륨 에이전트는 IT에 사전 정의된 보호 볼륨 양식으로 저장 데이터에 대한 보안을 제공합니다. 배치 시에 볼륨 에이전트는 전체 볼륨에 적용되어 이를 단일 단위로 암호화를 사용하여 보호하는 키 세트를 작성합니다. 데이터 및 파일이 저장 및/또는 편집, 추가 또는 삭제되기 때문에 암호화 알고리즘은 볼륨 내의 모든 데이터가 제대로 보안 설정되도록 호출됩니다. 볼륨은 하나 이상의 파티션으로 분할될 수 있으며 이들 각각의 파티션은 유사하게 보호됩니다. 볼륨 보호는 소량에서 대량의 데이터를 광범위하게 공유하려는 사용자 그룹에 가장 적합합니다.

Q: 정책이 적용된 파일 에이전트를 언제 사용해야 합니까? 그리고 작동 방식은 어떻게 됩니까?

A: 정책이 적용된 파일 에이전트는 IT에 매우 강력한 개별 파일 레벨 보호를 제공합니다. 파일 에이전트가 배치되면 최상위 레벨 디렉토리는 보호된 데이터의 위치로 식별됩니다. 이 안에 저장되는 각 파일은 키 세트를 사용하여 개별적으로 보호되며 사용자, 그룹, 프로세스에 대한 파일 액세스 제어는 PPM 정의 정책으로 관리됩니다. 또한, 보안 관리자는 사용자, 그룹 또는 프로세스에 적용할 수 있는 암호화 키를 정의하여 선택 파일이 디렉토리를 공유하는 다른 사용자, 그룹 또는 프로세스에서 암호화되어 보호될 수 있도록 합니다. 파일에 액세스되면, 감사 및 추적을 위해 각 액세스(읽기 또는 쓰기 또는 둘 다)가 로깅될 수 있도록 허용하는 옵션이 선택될 수도 있습니다. 파일 크기 또는 파일 보호가 포함된 스토리지 환경 크기에는 제한이 없으며 공간 활용도는 포함된 파일 크기별로 확장됩니다. 정책을 사용하는 파일 보호는 공유 또는 개인적으로 사용되는 개별 파일 보호에 가장 적합합니다.

Q: 정책이 적용된 볼륨 에이전트를 언제 사용해야 합니까? 그리고 작동 방식은 어떻게 됩니까?

A: 정책이 적용된 볼륨 에이전트는 보호 볼륨(또는 파티션)에 사용자 및 그룹 파일 액세스 제어를 추가합니다. 배치 시에 볼륨 에이전트는 전체 볼륨에 적용되어 이를 단일 단위로 암호화를 사용하여 보호하는 키 세트를 작성합니다. 파일이 저장 및/또는 편집, 추가 또는 삭제되기 때문에 암호화 알고리즘은 볼륨 내의 모든 데이터가 제대로 보안 설정되도록 사용됩니다. 보안 관리자는 PPM을 사용하여 사용자, 그룹, 프로세스에 대한 파일 액세스 제어 정책을 정의할 수도 있습니다. 파일에 액세스되면, 감사 및 추적을 위해 각 액세스(읽기 또는 쓰기 또는 둘 다)가 로깅될 수 있도록 허용하는 옵션이 선택될 수도 있습니다. 정책을 사용하는 볼륨 보호는 소량에서 대량의 데이터를 공유뿐만 아니라 파일 액세스 제어도 필요한 사용자 그룹에 가장 적합합니다.

Q: 오브젝트 저장소 에이전트를 반드시 사용해야 하는 경우는 언제입니까? 그리고, 작동 방식은 어떻게 됩니까?

A: 오브젝트 저장소 에이전트에서는 온프레미스이거나 클라우드에 있거나에 관계없이 확장성이 높고 효율적인 오브젝트 스토리지에 데이터를 저장할 수 있습니다. 데이터는 고객이 제어하며 항상 개인용으로 사용 가능합니다. 액세스 권한은 오브젝트 스토리지 소유자가 제어합니다. 오브젝트 저장소 에이전트를 통해 전송되는 데이터는 로컬로 암호화되며 TLS(Transport Layer Security) 프로토콜을 사용하여 전송 중 추가로 보호됩니다. 그러면 S3 가능 클라우드 스토리지를 통해 온프레미스에서 데이터를 보호합니다. 오브젝트 저장소 에이전트는 "M:N" 모델에서 작동하며, 이 모델은 작성한 총 조각 수(N) 중 데이터를 다시 빌드하는 데 필요한 데이터 조각 수(M)를 결정합니다. 라이선스에 따라 로컬 또는 원격 위치에 있을 수 있는 저장된 데이터 조각을 "공유"라고 합니다. 여러 공유를 사용하면 데이터 탄력성 및 결함 내구성에 대한 추가 옵션과 함께 데이터 흐름이 향상될 수 있습니다. 지원되는 M:N 분산형 공유 모델은 1:1, 2:3 또는 2:4입니다.

Q: 정책, 프로비저닝, 관리(PPM) 콘솔에서 작업이란 무엇입니까? 그리고, 어떤 용도로 사용됩니까?

A: PPM은 GUI에서 액세스 가능한 작업 시스템을 통합하여 보호된 데이터 및 이에 액세스할 수 있는 사용자 및 항목에 관련된 승인, 타이밍, 다양한 배치 실행, 정책 및 유지보수 태스크를 관리 및 추적합니다. 관리자가 태스크를 입력하면 작업이 작성되고 새 작업은 작업 페이지에 표시되는 목록에 추가됩니다. 권한이 있는 관리자는 각 작업을 승인, 거부 또는 제외합니다.

Q: IBM Multi-Cloud Data Encryption의 경우, 외부 PostgreSQL 데이터베이스를 사용하는 시기는 언제입니까?

A: 외부 Postgres 데이터베이스는 모든 제품 환경에 대해 매우 권장됩니다. 내부 데이터베이스는 성장 가능성이 적은 매우 작은(소수의 에이전트, 소수의 사용자 및 그룹 또는 단순한 테스트 또는 QA 설정) 설치에 대해서만 권장됩니다. 또한, Postgres 데이터베이스는 고가용성(HA) 구성에서 배치 시에 필요합니다.

인증서 FAQ

Q: PPM 서버 인증서의 요구사항은 무엇입니까?

- A:** PPM 서버 인증서에는 다음 요소가 포함되어야 합니다.
- "서버 인증"을 지정하는 확장 키 속성
 - PPM 서버 FQDN(완전 규정된 도메인 이름)을 지정하는 제목 대체 이름 섹션

Q: 에이전트 인증서에 대한 요구사항은 무엇입니까?

- A:** 각 에이전트 인증서에는 다음 요소가 포함되어야 합니다.
- "클라이언트 인증"을 지정하는 확장 키 속성
 - 에이전트 FQDN(Fully Qualified Domain Name)을 지정하는 제목 대체 이름 섹션

Q: PPM에서 NAT(네트워크 주소 변환) 또는 PAT(포트 주소 변환) 연결을 지원합니까?

A: 예. 에이전트가 PPM 서버에 대한 통신 세션을 시작하기 때문에 통신이 설정되려면 PPM 서버가 에이전트에서 연결할 수 있어야 합니다. 통신이 설정되면 열린 상태로 유지됩니다. 에이전트는 이 연결을 사용하여 이벤트 데이터를 PPM 서버로 보냅니다. PPM 서버는 이 연결을 사용하여 에이전트에 정책 업데이트를 보냅니다.

Q: NAT(Network Address Translation) 또는 PAT(Port Address Translation) 네트워크 구성에서 PPM 서버의 PPM 서버 인증서를 어떻게 구성합니까?

- A:** PPM 서버 인증서에는 다음 요소가 포함되어야 합니다.
- "서버 인증"을 지정하는 확장 키 속성
 - PPM 서버 FQDN(완전 규정된 도메인 이름)을 지정하는 제목 대체 이름 섹션

- 나가는 방향의 IP 주소를 지정하는 제목 대체 이름 섹션

Q: 에이전트가 NAT(Network Address Translation) 또는 PAT(Port Address Translation) 네트워크 구성으로 되어 있는 경우 에이전트 인증서를 어떻게 구성합니까?

A: 에이전트 인증서에는 다음 요소가 포함되어야 합니다.

- "클라이언트 인증"을 지정하는 확장 키 속성
- PPM 서버 FQDN(완전 규정된 도메인 이름)을 지정하는 제목 대체 이름 섹션
- 나가는 방향의 IP 주소를 지정하는 제목 대체 이름 섹션

Q: 고가용성(HA) 구성에서 PPM 서버 인증서에 대한 요구사항은 무엇입니까?

A: PPM 서버 인증서에는 다음 요소가 포함되어야 합니다.

- "서버 인증"을 지정하는 확장 키 속성
- PPM 가상 IP 주소와 연관되는 FQDN 및 PPM 클러스터를 구성하는 PPM 서버 FQDN(Fully Qualified Domain Name)을 지정하는 제목 대체 이름 섹션입니다.

키 및 키 처리 FAQ

Q: IBM Multi-Cloud Data Encryption이 수행할 수 있는 키 처리 조작은 무엇입니까?

A: 보안 관리자는 PPM(Policy Provisioning Manager) 내에서 데이터를 보안 설정하는 암호화 키를 정의할 수 있습니다. 해당 키는 데이터 유형, 데이터 유형 행, 볼륨과 연관될 수 있습니다. 키 처리 조작에는 작성, 로테이션, 취소, 폐기가 포함됩니다.

Q: 키를 로테이션해야 하는 이유는 무엇입니까?

A: 주기적인 키 로테이션은 일반적으로 권한없는 액세스로부터 데이터를 충분히 보호하기 위해 필요합니다. 키 로테이션은 현재 키를 새 키로 바꾸는 것으로, 암호화의 특성으로 인해 암호화 알고리즘을 사용하는 계산이 필요합니다. 많은 전문가가 엔터프라이즈 IT 샵(특히, 클라우드와 상호작용하는 경우)에서는 주기적으로 키를 로테이션하도록 권장합니다. 요즘은 PCI-DSS와 같이 주기적인 로테이션이 필요한 표준이 있습니다. PPM 키 로테이션은 감사용으로 로깅되는 시간소인된 데이터 레코드를 작성하여 준수를 표시합니다.

Q: 키를 취소해야 하는 이유는 무엇입니까?

A: PPM(Policy Provisioning Manager)을 사용하여 키를 취소하면 임시로 보호된 데이터에 액세스할 수 없게 됩니다. 키는 일반적으로 데이터 보호에 문제가 있는 경우 또는 보호된 데이터에 대한 액세스가 거부되는 인스턴스에서 취소됩니다. 나중에 데이터는 동일한 키가 재분배되면 다시 사용 가능해질 수도 있습니다.

Q: 키를 폐기해야 하는 이유는 무엇입니까?

A: 키를 폐기하면 보호된 데이터에 영구적으로 액세스할 수 없게 됩니다. 데이터가 더 이상 필요하지 않은 경우를 제외하고는 이 옵션을 선택하지 마십시오.

Q: IBM Multi-Cloud Data Encryption이 키를 관리합니까?

A: 보안 관리자가 암호화 키를 수동으로 관리하지 않으려는 경우, PPM(Policy Provisioning Manager)은 새로 작성된 각 정책에 대해 키를 자동 생성할 수 있습니다. 자동 생성된 키는 항상 작성 시마다 고유하며 키 관리 페이지에는 표시되지 않습니다.

설치 및 설정 FAQ

Q: IBM Multi-Cloud Data Encryption(MDE)이 일반 사용자(예: 관리자가 아닌 사용자)에게 주는 영향은 무엇입니까?

A: 관리자가 아닌 사용자는 정상 조작에서 아무 차이점도 느끼지 못하면서 IBM Multi-Cloud Data Encryption(MDE)의 보안 및 고가용성을 사용할 수 있습니다. 관리(보호된) 디렉토리의 파일에 액세스해도 파일 액세스, 쓰기 또는 저장 기능에는 아무런 영향도 없습니다.

Q: MDE 에이전트를 Docker 호스트에 설치하고 이를 통해 Docker 컨테이너에 있는 애플리케이션의 모든 읽기/쓰기 요청을 처리할 수 있습니까?

A: 네, 정책이 적용된 파일 에이전트와 볼륨 에이전트 모두를 사용하여 데이터를 보호할 수 있습니다.

- 정책이 적용된 파일 에이전트를 사용하여 Docker 볼륨 경로를 보호하면 컨테이너에서 사용하는 애플리케이션 데이터를 보호할 수 있습니다.
- 볼륨 에이전트는 Docker 컨테이너 경로를 보호하는 데 사용할 수 있습니다. 이 에이전트는 전체 컨테이너와 모든 I/O를 효과적으로 암호화합니다. Docker 볼륨이 Docker 컨테이너 경로 외부에 저장되는 경우, 외부 Docker 볼륨을 보호하도록 추가 볼륨을 구성할 수 있습니다.
- Docker 호스트의 핵심은 Red Hat 7.2+(3.10-*)에서 지원되는 커널을 실행해야 한다는 것입니다.

구성 FAQ

Q: IBM Multi-Cloud Data Encryption(MDE)를 사용하여 HTML 파일을 암호화할 수 있습니까?

A: 이 시점에서는 HTML 파일 보호가 권장되지 않습니다. 웹 사이트에는 암호화 시에 제대로 표시되지 않을 수도 있는 활성 HTML 파일이 표시됩니다.

운영 FAQ

Q: IBM Multi-Cloud Data Encryption(MDE)으로 데이터가 보호되는지 여부를 확인하는 방법은 무엇입니까?

A: MDE 보호는 서비스가 중단되고 모든 보호 파일에 액세스하는 경우에도 활성화됩니다.

Q: IBM Multi-Cloud Data Encryption(MDE) 프로덕션 구현을 변경하기 전에 수행해야 하는 예방책은 무엇입니까?

A: 시스템이 작동 중인 동안 'spxconfig' 명령행이나 GUI를 통해 사소한 수정은 가능합니다. 그렇지만 중요한 변경의 경우 자세한 예방책 및 권장되는 백업이 필요합니다. (변경 구현 전에 프로덕션 에코시스템에 대한 모든 제품 문서를 참조하십시오.)

Q: IBM Multi-Cloud Data Encryption(MDE)에서 다른 SIEM(Security Information and Event Management) 상환 애플리케이션으로 이벤트를 전송할 수 있습니까?

A: 예, 여기에는 이벤트 집계 및 전달 시스템이 포함됩니다. 이 시스템은 관리 에이전트의 이벤트와 내부적으로 생성된 이벤트를 집계하고 이를 관리자 대시보드를 통해 볼 수 있는 내부 이벤트 로그에 저장하며 하나 이상의 수신자에게 이벤트를 전달하도록 구성할 수 있습니다.

Q: 대소문자 구분이 중요합니까?

A: 예, 대소문자 구분은 매우 중요합니다.

- 선택자를 작성할 때 사용자 필드 및 그룹 필드에서는 대소문자를 구분합니다.

- Windows를 사용하여 경로 세트를 작성할 때 드라이브 이름은 대문자여야 하고 디렉토리 이름은 대소문자를 구분합니다.
- 볼륨 에이전트 또는 정책이 적용된 볼륨 에이전트를 작성할 때 볼륨 레이블은 대소문자를 구분합니다.
- 값 또는 필드의 대소문자 구분을 항상 가정해야 합니다.

Q: 조작 순서는 무엇을 의미하고 왜 중요합니까?

- A:** 성공을 보장하기 위해서 에이전트 작성 및 배치를 특정 순서로 수행해야 하기 때문에 순서가 중요합니다.
- 파일 에이전트를 배치하기 전에 대상 볼륨은 온라인 상태이고 초기화되며 생성된 디렉토리로 포맷되고 적절한 권한이 지정되어야 합니다.
 - 볼륨 에이전트를 배치하기 전에 볼륨이 존재해야 하며 온라인 상태이고 초기화되어야 하지만 포맷은 되지 않아야 합니다.
 - 정책이 적용된 볼륨 에이전트를 배치하기 전에 볼륨이 존재해야 하며 온라인 상태이고 초기화되어야 하지만 포맷은 되지 않아야 합니다. 정의된 선택자가 대상 시스템의 로컬 또는 LDAP/AD 계층 구조에 있어야 합니다.

Q: 스냅샷 활성화 작업을 제출했고 이 작업이 아직도 실행 중입니다. 이 작업은 언제 완료됩니까?

- A:** 에이전트가 PPM 서버와 통신할 수 있을 때까지 스냅샷 변경 또는 업데이트가 적용되지 않습니다. 생성된 작업은 PPM과 에이전트 사이의 통신이 성공하거나 에이전트가 PPM 서버에서 제거될 때까지 계속 실행됩니다.

고가용성 FAQ

Q: IBM Multi-Cloud Data Encryption(MDE) 배치에 대해 고가용성이 필요한 시기는 언제입니까?

- A:** 고가용성(HA) MDE 배치는 데이터 액세스 및 거의 100%의 가용성에 육박하는 보호 관리 서비스가 필요한 IT 환경에서 사용되어야 합니다. PPM 인스턴스에 유지보수가 필요하거나 실패 또는 실수로 오프라인이 되는 경우, 핫 백업 인스턴스가 즉시 사용되어 조작을 재개합니다.

Q: 고가용성(HA) IBM Multi-Cloud Data Encryption 배치에 로드 밸런서가 필요합니까?

- A:** 예. 두 개의 로드 밸런서(로드 밸런서 클러스터)가 에이전트와 PPM 서버 사이에 있어야 합니다. 로드 밸런서 클러스터는 둘 이상의 PPM 서버가 배치되는 각 위치에 필요합니다. 로드 밸런서는 로컬 서브넷에서 이들 사이에서 통신하고 에이전트와 관리자가 PPM 서버 액세스에 사용하는 가상 IP 주소("부동 IP 주소"라고도 함)를 제공합니다. PPM HA에 해당하는 시나리오는 단일 위치, 다중 데이터 센터 등과 같이 다양하며 이들 각각은 자체적인 배치 옵션 및 구성을 포함합니다.

다중 테넌트 FAQ

Q: 다중 테넌트 기능의 용도는 무엇입니까?

- A:** PPM의 다중 테넌트 기능은 IT 제공자에게 고객별로 PPM 제어를 구분하는 기능을 제공합니다. 따라서, 각 고객은 IT 환경 내에 자체적으로 격리된 PPM 로그인, 관리자, 정책, 대시보드, 작업, 이벤트 등을 포함합니다. 고객은 스토리지뿐만 아니라 디렉토리도 공유할 수 있지만 보호된 파일 및 볼륨은 서로 개별적으로 암호화되어 보호됩니다. 이를 사용하면 다중 테넌트 또는 고객이 동일한 스토리지 공간을 안전하게 공유하고 활용할 수 있으며 각 테넌트의 데이터는 분리되고 다른 테넌트나 고객에게 표시되지 않습니다.

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다. 본 자료는 IBM에서 다른 언어로 제공할 수 있습니다. 그러나 자료에 접근하기 위해서는 해당 언어로 된 제품 또는 제품 버전의 사본이 필요할 수 있습니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이선스까지 부여하는 것은 아닙니다. 라이선스에 대한 의문사항은 다음으로 문의하십시오.

07326

서울특별시 영등포구

국제금융로 10, 31FC

한국 아이.비.엠 주식회사

대표전화서비스: 02-3781-7114

2바이트 문자 세트(DBCS) 정보에 관한 라이선스 문의는 한국 IBM에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다.

IBM은 타인의 권리 침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 책을 "현상태대로" 제공합니다.

일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 정보에서 언급되는 비IBM의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(i) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (ii) 교환된 정보의 상호 이용을 목적으로 본 프로그램에 관한 정보를 얻고자 하는 라이선스 사용자는 다음 주소로 문의하십시오.

07326

서울특별시 영등포구

국제금융로 10, 31FC

한국 아이.비.엠 주식회사

대표전화서비스: 02-3781-7114

이러한 정보는 해당 조건(예를 들면, 사용료 지불 등)하에서 사용될 수 있습니다.

이 정보에 기술된 라이선스가 부여된 프로그램 및 프로그램에 대해 사용 가능한 모든 라이선스가 부여된 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이선스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

본 문서에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 다른 운영 환경에서 얻어진 결과는 상당히 다를 수 있습니다. 일부 성능은 개발 단계의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한 일부 성능은 추정을 통해 추측되었을 수도 있으므로 실제 결과는 다를 수 있습니다. 이 책의 사용자는 해당 데이터를 본인의 특정 환경에서 검증해야 합니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품들을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능의 정확성, 호환성 또는 기타 청구에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지 없이 변경될 수 있습니다.

여기에 나오는 모든 IBM의 가격은 IBM이 제시하는 현 소매가이며 통지 없이 변경될 수 있습니다. 실제 판매가는 다를 수 있습니다.

이 정보는 계획 수립 목적으로만 사용됩니다. 이 정보는 기술된 제품이 GA(General Availability)되기 전에 변경될 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

저작권 라이선스:

이 정보에는 여러 운영 플랫폼에서의 프로그래밍 기법을 보여주는 원어로 된 샘플 응용프로그램이 들어 있습니다. 귀하는 이러한 샘플 프로그램의 작성 기준이 된 운영 플랫폼의 응용프로그램 프로그래밍 인터페이스(API)에 부합하는 응용프로그램을 개발, 사용, 판매 또는 배포할 목적으로 추가 비용 없이 이들 샘플 프로그램을 어떠한 형태로든 복사, 수정 및 배포할 수 있습니다. 이러한 샘플 프로그램은 모든 조건하에서 완전히 테스트된 것은 아닙니다. 따라서 IBM은 이들 샘플 프로그램의 신뢰성, 서비스 가능성 또는 기능을 보증하거나 진술하지 않습니다. 본 샘플 프로그램은 일체의 보증 없이 "현상태대로" 제공됩니다. IBM은 귀하의 샘플 프로그램 사용과 관련되는 손해에 대해 책임을 지지 않습니다.

이러한 샘플 프로그램 또는 파생 제품의 각 사본이나 그 일부에는 반드시 다음과 같은 저작권 표시가 포함되어야 합니다.

© (귀하의 회사명) (연도). 이 코드의 일부는 IBM Corp.의 샘플 프로그램에서 파생됩니다. © Copyright IBM Corp. _enter the year or years_.

이 정보를 소프트웨어로 확인하는 경우에는 사진과 컬러 삽화가 제대로 나타나지 않을 수도 있습니다.

상표

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

IBM, IBM 로고 및 ibm.com은 전세계 여러 국가에 등록된 International Business Machines Corp.의 상표 또는 등록상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. IBM 상표에 대한 현재 목록은 "저작권 및 상표 정보"의 웹 사이트(<http://www.ibm.com/legal/copytrade.shtml>)에서 제공됩니다.

Adobe, Adobe 로고, PostScript 및 PostScript 로고는 미국 및/또는 기타 국가에서 사용되는 Adobe Systems Incorporated의 등록상표 또는 상표입니다.

Apache Software Foundation(ASF)는 Apache 프로젝트 커뮤니티를 대신하여 모든 Apache 관련 상표, 서비스표, 그래픽 로고를 소유하며, 모든 Apache 프로젝트의 이름은 ASF의 상표입니다.

Node.JS는 Joyent, Inc.의 등록상표입니다(CORPORATION DELAWARE 345 California Street; Suite 2000 San Francisco CALIFORNIA 94104).

Unicode 및 Unicode 로고는 미국 또는 기타 국가에서 사용되는 Unicode, Inc.의 등록상표입니다.

CentOS 마크는 Red Hat, Inc.("Red Hat")의 상표입니다.

"Red Hat", Red Hat Linux, Red Hat "Shadowman" 로고 및 나열된 제품은 미국 또는 기타 국가에서 사용되는 Red Hat, Inc.의 상표 또는 등록상표입니다.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

Java 및 모든 Java 기반 상표와 로고는 Oracle 및/또는 그 계열사의 상표 또는 등록상표입니다.

제품 문서의 이용 약관

다음 이용 약관에 따라 이 책을 사용할 수 있습니다.

적용성

본 이용 약관은 IBM 웹 사이트의 모든 이용 약관에 추가됩니다.

개인적 사용

모든 소유권 사항을 표시하는 경우에 한하여 귀하는 이 책을 개인적, 비상업적 용도로 복제할 수 있습니다. IBM의 명시적인 동의 없이는 이 책 또는 그 일부를 배포 또는 전시하거나 2차적 저작물을 만들 수 없습니다.

상업적 사용

모든 소유권 사항을 표시하는 경우에 한하여 귀하는 이 책을 귀하 기업집단 내에서만 복제, 배포 및 전시할 수 있습니다. 귀하의 기업집단 외에서는 IBM의 명시적인 동의 없이 이 책의 2차적 저작물을 만들거나 이 책 또는 그 일부를 복제, 배포 또는 전시할 수 없습니다.

권한

본 허가에서 명시적으로 부여된 경우를 제외하고, 이 책이나 이 책에 포함된 정보, 데이터, 소프트웨어 또는 기타 지적 재산권에 대한 어떠한 허가나 라이선스 또는 권한도 명시적 또는 묵시적으로 부여되지 않습니다.

IBM은 이 책의 사용이 IBM의 이익을 해친다고 판단하거나 위에서 언급된 지시사항이 준수되지 않는다고 판단하는 경우 언제든지 부여한 허가를 철회할 수 있습니다.

귀하는 미국 수출법 및 관련 규정을 포함하여 모든 적용 가능한 법률 및 규정을 철저히 준수하는 경우에만 본 정보를 다운로드, 송신 또는 재송신할 수 있습니다.

IBM은 이 책의 내용에 대해 어떠한 보증도 제공하지 않습니다. 타인의 권리 침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여 (단 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 현 상태대로 제공합니다.

개인정보처리방침 고려사항

SaaS(Software as a Service) 솔루션을 포함한 IBM 소프트웨어 제품(이하 "소프트웨어 오퍼링")은 제품 사용 정보를 수집하거나 최종 사용자의 경험을 개선하는 데 도움을 주거나 최종 사용자와의 상호 작용을 조정하거나 그 외의 용도로 쿠키나 기타 다른 기술을 사용할 수 있습니다. 많은 경우에 있어서, 소프트웨어 오퍼링은 개인 식별 정보를 수집하지 않습니다. IBM의 일부 소프트웨어 오퍼링은 귀하가 개인 식별 정보를 수집하도록 도울 수 있습니다. 본 소프트웨어 오퍼링이 쿠키를 사용하여 개인 식별 정보를 수집할 경우, 본 오퍼링의 쿠키 사용에 대한 특정 정보가 다음에 규정되어 있습니다. 본 소프트웨어 오퍼링은 개인 식별 정보를 수집하기 위해 쿠키 및 기타 다른 기술을 사용하지 않습니다.

본 소프트웨어 오퍼링에 배치된 구성이 쿠키 및 기타 기술을 통해 최종 사용자의 개인 식별 정보 수집 기능을 고객 귀하에게 제공하는 경우, 귀하는 통지와 동의를 위한 요건을 포함하여 이러한 정보 수집과 관련된 법률 자문을 스스로 구해야 합니다.

이러한 목적의 쿠키를 포함한 다양한 기술의 사용에 대한 자세한 정보는 IBM 개인정보처리방침(<http://www.ibm.com/privacy/kr/ko>), IBM 온라인 개인정보처리방침(<http://www.ibm.com/privacy/details/kr/ko>) 및 "쿠키, 웹 비콘 및 기타 기술" 및 "IBM 소프트웨어 제품 및 SaaS(Software-as-a Service) 개인정보처리방침"(<http://www.ibm.com/software/info/product-privacy>) 부분을 참조하십시오.



부품 번호 CC0LSEN

GC43-5038-00



(1P) P/N: CC0LSEN

