

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

관리자 안내서



참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, [105 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 2017, 2019.**

목차

제 1 장 소개.....	1
권한 부여된 사용 권한.....	1
문의처.....	1
관리자 안내서의 배경 및 목적.....	1
제 2 장 일반 개요.....	3
제품 개요.....	3
에이전트 유형.....	3
볼륨 에이전트.....	3
정책이 적용된 파일 에이전트.....	4
정책이 적용된 볼륨 에이전트.....	4
오브젝트 저장소 에이전트.....	5
에이전트 기능 매트릭스.....	5
제 3 장 계획 고려사항.....	7
선행 조건.....	7
최소 시스템 요구사항.....	7
인증서 요구사항.....	8
에이전트에 대한 파일 시스템 지원.....	8
네트워크 설정.....	9
네트워크 포트.....	9
OVA 구성.....	9
REST 인터페이스.....	9
제 4 장 제품 설치.....	11
설치 준비.....	11
Licensing.....	11
MDE OVA/VM 관리.....	11
MDE 설치.....	11
언어 설정.....	12
데이터베이스 설정.....	12
내부 데이터베이스.....	13
외부 데이터베이스.....	13
서버 인증서 설정.....	13
키 저장소, 신뢰 저장소 및 인증 기관.....	13
공개 키 인프라(PKI) 설정.....	14
최초 로그인 시작.....	14
제 5 장 MDE 그래픽 사용자 인터페이스(GUI).....	17
기본 제품 탐색.....	17
제품 대시보드.....	17
텍스트 상자 자동 완성.....	17
주의 알림.....	17
고급 특성.....	18
GUI 언어 설정.....	18
제 6 장 작업.....	21
작업 설명.....	21
다중 관리자 승인.....	22
작업 승인.....	22

작업 거부.....	22
작업 제외.....	22
작업 정보.....	22
제 7 장 MDE 관리 사용자 관리.....	25
관리 사용자 역할.....	25
제품 관리자 역할.....	25
보안 관리자 역할.....	25
관리 사용자 관리.....	25
새 관리 사용자 추가.....	25
관리 사용자 비밀번호 편집.....	26
관리 사용자 역할 편집.....	26
관리 사용자 상태 편집.....	26
관리 사용자 제거.....	27
사용자 계정 잠금.....	27
LDAP 디렉토리 목록.....	27
사용자 소스.....	28
제 8 장 이벤트.....	29
이벤트 로그.....	29
이벤트 세부사항.....	30
이벤트 내보내기.....	30
이벤트 전달.....	30
이벤트 인수.....	31
에이전트 이벤트.....	31
신뢰 가능한 이벤트.....	31
제 9 장 정책 적용 키 관리.....	33
키 추가.....	33
키 편집.....	33
키 로테이션.....	33
키 취소.....	35
키 폐기.....	35
자동 생성 키.....	35
외부 키 저장소.....	35
KMIP 키 저장소.....	36
하드웨어 보안 모듈(HSM).....	37
제 10 장 파일 레벨 정책 정의.....	39
선택자.....	39
경로 세트.....	40
데이터 유형.....	40
데이터 유형 행.....	41
데이터 유형 행 변수.....	41
프로세스.....	42
제 11 장 에이전트 프로비저닝 및 관리.....	43
에이전트 추가.....	43
ID.....	43
네트워크.....	44
정책이 제공된 파일, 정책이 적용된 볼륨 및 볼륨 에이전트 작성.....	44
볼륨.....	46
오브젝트 저장소 에이전트 작성.....	47
권한 부여된 사용자.....	50
에이전트 도구.....	51
검토 및 빌드.....	51
에이전트 활성화.....	52

에이전트 보기.....	52
에이전트 보고서.....	52
에이전트 설치.....	53
Linux용 에이전트 설치.....	53
AIX용 에이전트 설치.....	55
Windows용 에이전트 설치.....	55
정책 활성화.....	57
에이전트 편집.....	57
에이전트 정보 편집.....	58
인증서 추가/삭제.....	58
에이전트 도구.....	59
SU 데이터 액세스	59
정책 일시중단.....	60
정책 변경.....	60
에이전트 스냅샷.....	65
에이전트 편집 및 스냅샷 저장.....	65
스냅샷 관리.....	66
파일 에이전트 설치 제거.....	67
볼륨 에이전트 설치 제거.....	68
볼륨 에이전트 설치 제거.....	68
정책이 적용된 볼륨 에이전트 설치 제거.....	69
오브젝트 저장소 에이전트 설치 제거.....	69
MDE에서 에이전트 제거.....	70
에이전트 유틸리티.....	70
제 12 장 조작.....	73
제품 데이터 백업 및 복원.....	73
제품 데이터 백업.....	73
제품 데이터 복원.....	73
커널 업데이트.....	73
업그레이드.....	74
MDE 서버의 경우.....	74
에이전트 대상 VM의 경우.....	75
서비스 데이터.....	76
서비스 데이터 수집.....	76
PPM 로그에서 민감한 정보 제거.....	76
부록 A 샘플 에이전트 설치 프로세스.....	77
Red Hat / CentOS 프로세스.....	77
AIX 프로세스.....	78
Windows 서버 프로세스.....	78
부록 B 샘플 인증 기관(CA) 인증서.....	81
부록 C PKCS12 파일 작성을 위한 샘플 변환.....	85
부록 D 해야 할 작업과 하지 말아야 할 작업.....	87
지정된 키 변경.....	87
개요.....	87
배경.....	87
암호화된 백업을 사용하여 키 로테이션.....	87
개요.....	87
배경.....	87
부록 E 적절한 암호화.....	89
명령 옵션.....	89

감사 단계.....	89
암호화 단계.....	89
부록 F 에이전트 디버그 로깅.....	91
Linux 에이전트.....	91
Windows 에이전트.....	91
부록 G 비OVA 배치.....	93
부록 H 소프트웨어 버전 확인.....	95
부록 I 용어집	97
주의사항	105
상표.....	106
제품 문서의 이용 약관.....	107
개인정보처리방침 고려사항.....	107

제 1 장 소개

권한 부여된 사용 권한

이 소프트웨어의 사용은 라이선스 계약의 이용 약관으로 제한됩니다.

문의처

IBM Multi-Cloud Data Encryption(MDE)에 대한 추가 정보는 IBM 지원 센터 웹 사이트(<https://www.ibm.com/support/home/>)를 참조하십시오.

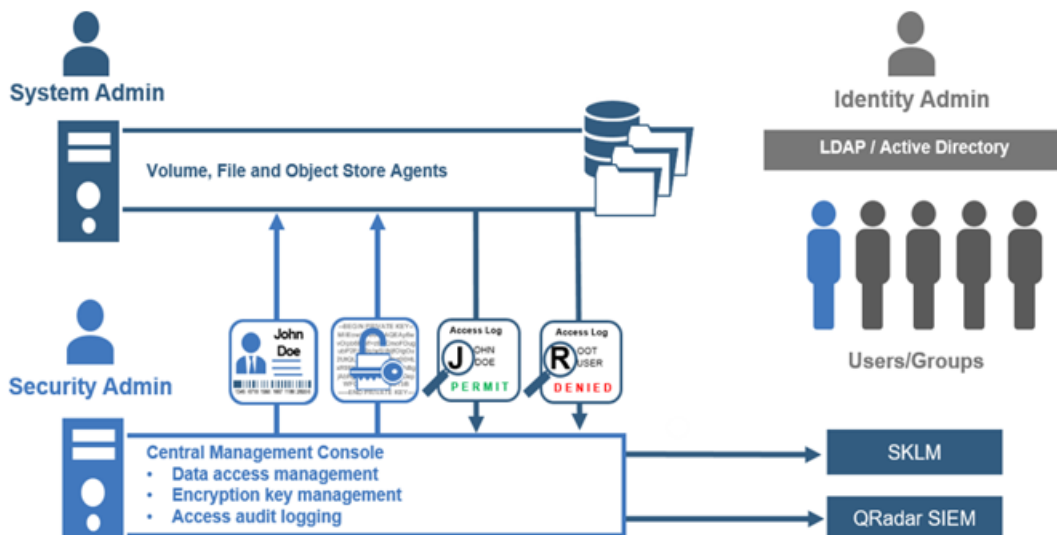
관리자 안내서의 배경 및 목적

관리자 안내서는 암호화 에이전트 프로비저닝과 관리, 정책 정의(액세스 및 암호화 제어), 정책 적용 키 관리 및 배치된 에이전트를 사용하는 선택된 서버에서의 저장 데이터(data at rest) 보호를 위한 MDE의 설치, 관리 및 사용에 대한 기본 참조서입니다. 이 문서는 관리 액세스 권한이 있으며 제품을 설치하고 관리하기 위한 자사 네트워크에 대해 잘 알고 있는 시스템 관리자로 작성되었습니다.

제 2 장 일반 개요

제품 개요

IBM Multi-Cloud Data Encryption(MDE)은 중앙 집중식 관리 콘솔로 작동하는 PPM(Policy Provisioning Manager)의 추가적인 강력한 보호 기능과 저장 데이터(data-at-rest) 암호화(에이전트를 통한)를 결합하는 SPx® 기술을 기반으로 하는 포괄적인 데이터 보안 제품입니다. MDE를 사용하면 단일 중앙 위치에서 최대 25,000개의 에이전트에 대해 에이전트 프로비저닝, 데이터 액세스 정책 설정(운영 및 암호화 액세스 정의), 관리(키 수명 주기, 에이전트 업데이트 및 사용자 액세스 로깅)가 가능합니다. MDE는 고유의 암호화 분할 기술을 사용하여 파일 시스템 레벨이나 볼륨 레벨에서 데이터를 암호화하는 에이전트를 지정하기 위한 융통성을 발휘하여 끊임 없고 안전한 시스템을 제공합니다. 이는 무차별적인 공격으로부터 데이터 암호화가 보다 강력하고 풀릴 수 없도록 하는 표준 암호화를 넘어서는 데이터 집중적인 보호를 제공합니다. 이는 보다 미세 조정된 액세스 정책을 정의함으로써 사용자 레벨에서 데이터 액세스를 제한하고 모니터링하며 감사하는 기능을 사용하여 보안을 한층 더 강화합니다.

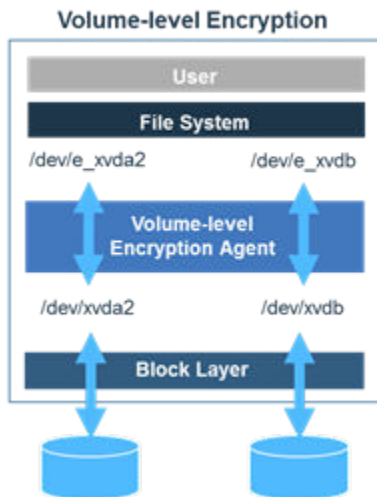


MDE는 별도의 관리 역할(제품 관리자 및 보안 관리자)을 사용하여 업무 분리를 제공합니다. 제품 관리자 역할은 MDE 제품 구성 및 유지보수에 필요한 권한으로 일임됩니다. 보안 관리자 역할은 에이전트를 프로비저닝하고 관리하는 데 필요한 권한으로 일임됩니다. 이 역할은 "7절: MDE 관리 사용자 관리"에서 더 자세하게 설명됩니다.

MDE는 정책 정의를 적용하는 데 사용되는 암호화 데이터 보호를 제공하는 네 개의 에이전트 유형 설치를 지원합니다.

에이전트 유형

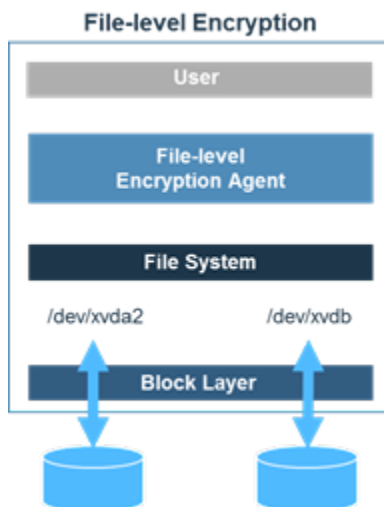
볼륨 에이전트



볼륨 에이전트에서는 액세스 정책 제어가 제한되는 볼륨 레벨 암호화를 제공합니다. 볼륨 레벨 암호화는 OS에서 블록 드라이버 구현을 통해 보호되고 사전 정의된 스토리지 디바이스의 양식으로 보안을 제공합니다.

전체 볼륨이 정의되고 암호화되어 단위로 보호됩니다. 데이터가 추가, 편집되거나 삭제될 때 볼륨 에이전트는 볼륨 내의 모든 데이터가 PPM 관리되는 암호화 키를 사용하여 암호화 방식으로 보호되는지 확인합니다.

정책이 적용된 파일 에이전트



정책이 적용된 파일 에이전트는 파일 레벨 암호화를 데이터 액세스 정책과 결합합니다. 파일 레벨 암호화는 파일 시스템 레벨에서 개별 파일 보호를 제공합니다. 파일 및 스토리지 환경 크기는 파일 시스템에 의해서만 제한되며 정책이 적용된 파일 에이전트에 의해서는 제한되지 않습니다. 보호된 데이터에 대한 위치는 해당 경로 정의에 대한 작업 그룹 키로 보호되며, 그 내부와 아래에 저장된 모든 개별 파일은 고유하고 예측 불가능한 초기화 벡터(IV)를 사용하여 별도로 암호화됩니다. 보호된 데이터는 NFS를 통해 마운트된 파일 시스템 또는 네트워크에 로컬일 수 있습니다.

고유 파일 레벨 키는 내부 키 관리 시스템으로 처리됩니다. 정책 기반 액세스 제어는 암호화 상에서 계층화되어 최소 권한의 액세스 제어 정의, 액세스 로깅 스펙 및 특정 시스템 기능에 대한 액세스 권한 제한(읽기/읽기-쓰기/복사/삭제)을 허용합니다. 해당 정책 제어는 표준 LDAP 또는 Active Directory 권한과 같이 작동합니다. 사용자에게 LDAP 또는 Active Directory의 데이터에 대한 권한이 없는 경우, 보안 관리자는 해당 액세스 제어를 겹쳐줄 수 없으며 데이터 액세스 권한을 부여할 수 없습니다.

기본적으로 모든 사용자는 정책이 적용되는 데이터 액세스에서 제외됩니다. 보안 관리자는 액세스 권한을 가지는 사용자를 정의해야 합니다. 이를 통해 보안 관리자는 시스템 관리자, 클라우드 공급업체 관리자 및 root 사용자가 보호된 데이터에 액세스하지 못하도록 제한할 수 있습니다.

정책이 적용된 볼륨 에이전트

정책이 적용된 볼륨 에이전트는 볼륨 에이전트의 볼륨 레벨 암호화 및 하나 이상의 보호된 파일 경로에 적용 및 강제 실행될 수 있는 파일 기반의 운영 액세스 제어 정책을 사용합니다.

오브젝트 저장소 에이전트

오브젝트 저장소 에이전트는 생성된 총 조각 수(N) 중 데이터를 다시 빌드하는 데 필요한 데이터 조각 수(M)를 결정하는 "M of N" 모델로 작동합니다. 라이선스에 따라 로컬 또는 원격 위치에 있을 수 있는 저장된 데이터 조각을 "공유"라고 합니다. 여러 공유를 사용하면 데이터 탄력성 및 결합 내구성에 대한 추가 옵션과 함께 데이터 흐름이 향상될 수 있습니다. 지원되는 M:N 분산형 공유 모델은 1:1, 2:3 또는 2:4입니다.

오브젝트 저장소 에이전트(OSA)는 오브젝트 스토리지로 전송되는 데이터를 암호화합니다. 데이터를 암호화 및 분할하여 오브젝트 스토리지에 파일이 전송될 때 파일의 통과 역할을 합니다. 오브젝트 저장소 에이전트를 통해 오브젝트 스토리지에서 검색된 파일은 검색시 해독됩니다. 오브젝트 스토리지의 저장된 파일은 암호화됩니다. 권한 부여된 사용자만 오브젝트 저장소 에이전트를 통해 데이터를 전송/수신할 수 있습니다.

에이전트 기능 매트릭스

에이전트 기능	볼륨 에이전트	정책이 적용된 볼륨 에이전트	정책이 적용된 파일 에이전트	오브젝트 저장소 에이전트
전체 볼륨 암호화	✓	✓		
지정된 보호된 디렉토리에서 개별적으로 파일 암호화			✓	
파일 레벨 정책		✓	✓	
파일 액세스 감사 로그		✓	✓	
사용자 데이터에 대한 관리자 액세스에 대해 보호			✓	
오브젝트 스토리지의 데이터 암호화				✓

제 3 장 계획 고려사항

선행 조건

IBM Multi-Cloud Data Encryption(MDE) 설치의 기본 OVA(Open Virtual Appliance)의 설치와 PPM(Provisioning Policy and Management) 설치 프로그램의 실행이 포함된 매우 간단한 프로세스입니다.

준비 과정에서 소프트웨어 설치 전에 설치 지시사항을 검토하는 것이 좋습니다. 다음은 IBM Multi-Cloud Data Encryption(MDE)의 성공적인 설치와 운영에 필요한 전제조건의 목록입니다.

1. PPM을 실행하고 배치하기 위한 라이선스가 있는 운영 체제 및 지원되는 하이퍼바이저(VMware ESXi™)가 포함된 운영 서버
2. 패키징된 기본 OVA
3. PPM 설치 프로그램
4. 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.
5. 브라우저: Google Chrome®, Microsoft Internet Explorer® 10+, Mozilla Firefox® ESR 52+.
6. PPM과 모든 에이전트 간의 네트워크 액세스
7. 관리 서버(PPM)와 모든 에이전트 간의 보안 세션을 확립하기 위한 인증 기관 서명이 있는 인증서(키 저장소, 신뢰 저장소 및 CA 인증서 번들).

자세한 내용은 인증서 요구사항 및 서버 인증서 설정을 참조하고 예제는 [81 페이지의 『부록 B 샘플 인증 기관\(CA\) 인증서』](#)의 내용을 참조하십시오.

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 키(비밀번호)
- AWS S3 REST API Library 또는 Boto Python Library를 활용하여 OSA 에이전트에 대한 데이터를 나타내는 애플리케이션 또는 유틸리티

중요한 참고사항: MDE, 외부 데이터베이스 및 에이전트가 NTP를 활용하여 좌표계 시간을 조정하도록 적극 권장합니다. 그러면 이벤트 / 감사 로그 시간소인이 제대로 순서화됩니다.

최소 시스템 요구사항

PPM VM 최소 시스템 요구사항

- CPU 4
- 8GB RAM
- 40GB의 사용 가능 스토리지
- 네트워크 액세스 필수

Linux 에이전트 최소 시스템 요구사항

- AES-NI가 사용되는 1개 코어 64비트 CPU @2GHz
 - (AES-NI가 지원되는 두 개의 코어 64비트 CPU @2GHz 권장)
 - 2GB RAM(4GB RAM 권장)

- 20GB의 사용 가능한 하드 디스크 공간
 - 300MB 이상의 로그 파일 공간 권장
- 네트워크 액세스 필수
- 설치/업데이트할 패키지: curl, openssl 및 nss(Red Hat / CentOS에서)
- 초기 에이전트 설치 중에 인터넷 액세스 또는 로컬 저장소 액세스
- 에이전트에 SSL 인증서가 필요함

Windows 에이전트 최소 시스템 요구사항

- AES-NI가 사용되는 1개 코어 64비트 CPU @2GHz - AES-NI가 사용되는 2개 코어 64비트 CPU @2GHz 권장
- 4GB RAM - 8GB RAM 권장
- 20GB의 사용 가능한 하드 디스크 공간 - 로그 파일 공간의 경우 300MB 이상이 권장됨
- 네트워크 액세스 필수
- 에이전트에 SSL 인증서가 필요함

참고: 에이전트를 작성하려면 SSL(자체 서명 또는 인증 기관) 인증서/키 쌍 파일이 필요합니다. 인증서는 에이전트와 MDE 서버 사이에서 보안 TLS 연결 설정에 사용됩니다.

인증서 요구사항

인증서는 PPM 서버와 에이전트 간에 보안 연결을 설정하는 데 필요합니다. 인증서 요구사항은 다음과 같습니다.

- PPM 서버에서는 에이전트가 제공한 인증서가 해당 에이전트(DNS 호스트 이름 또는 IP 주소)로 확인되어야 합니다.
- PPM 서버에서는 에이전트가 제공한 인증서에 클라이언트 인증 확장 키 사용 설정이 있어야 합니다.
- 에이전트에서는 PPM 서버가 제공한 인증서가 PPM 서버(DNS 호스트 이름 또는 IP 주소)로 확인되어야 합니다.
- 에이전트에서는 PPM 서버가 제공한 인증서에 서버 인증 확장 키 사용 설정이 있어야 합니다.

인증서가 유효 기간 내에 있는지 확인하려면 PPM 및 에이전트를 신뢰할 수 있는 시간 소스와 동기화해야 합니다. 배치된 각 에이전트마다 고유한 인증서가 필요합니다.

에이전트에 대한 파일 시스템 지원

볼륨 에이전트는 볼륨 레벨에서 암호화를 수행합니다. 정책이 적용된 파일 에이전트는 호스트 운영 체제의 지원되는 파일 시스템으로 또는 이 파일 시스템에서 작동됩니다. 정책이 적용된 파일 에이전트와 정책이 적용된 볼륨 에이전트는 다음의 파일 시스템을 지원합니다.

Linux 서버

- EXT3
- EXT4
- XFS(Red Hat / CentOS 6.5 이상에서)
- NFS(NFSv3, NFSv4)

Windows Server

- NTFS
- ReFS(Windows Server 2012 R2 이상에서)

AIX

- JFS2

네트워크 설정

이 태스크 정보

MDE에서는 MDE 서버와 에이전트 간의 안정적인 네트워크 연결을 요구합니다. 인터넷 프로토콜 IPv4 및 IPv6 이 지원됩니다. 정적 IP 지정 또는 정적 리스가 포함된 DHCP를 사용하면 이 요구사항이 충족됩니다. 또한 적절하게 작동하는 DNS 인프라 및 에코시스템 사이에서 호스트 이름 활용은 제대로 작동합니다.

네트워크 포트

기능	기본 포트	구성 가능
웹	443	예
데이터베이스	5432	예
외부 LDAP	없음	예
LDAP 디렉토리	없음	예
이메일 이벤트 전달	없음	예
Syslog 이벤트 전달	없음	예

OVA 구성

제공되는 MDE OVA는 MaxAuthTries가 1로 설정되어 미리 구성됩니다. MDE VM에 SSH를 통해 성공적으로 인증할 수 있도록 MaxAuthTries를 변경해야 하거나(권장되지 않음) 또는 SSH 클라이언트는 PubkeyAuthentication을 명령행이나 로컬 SSH 클라이언트 구성에서 "no"로 설정해야 합니다.

REST 인터페이스

MDE는 완전하게 프로그래밍된 REST 인터페이스를 지원합니다. 루트 REST URL은 다음과 같습니다.

`https://<Virtual Machine IP>/rest/`

중요 참고

REST API를 사용하여 관리자는 웹 인터페이스를 통해서는 액세스할 수 없는 고급 기능을 수행할 수 있습니다. 에이전트가 미지원 상태가 되도록 하는 방식으로 REST API가 잠재적으로 사용될 수 있으므로, 반드시 REST API 프로그래밍에 대해 잘 알고 있어야 합니다.

세부사항은 IBM Multi-Cloud Data Encryption(MDE) REST API 스펙 문서를 참조하십시오.

제 4 장 제품 설치

설치 준비

MDE 설치 프로세스에는 세 단계가 있습니다.

1. 선행 조건
2. MDE 기본 OVA(Open Virtual Appliance) 사용 가능
3. 지원되는 하이퍼바이저(VMware ESXi™)

Licensing

MDE의 경우 소프트웨어 라이선스 계약에서 제공되는 이상으로 에이전트를 실행하거나 구성하기 위한 고유 제품 라이선스가 필요하지 않습니다.

MDE OVA/VM 관리

최신 보안 패치와 소프트웨어 버전이 설치되도록 MDE OVA를 배치한 다음 시스템을 업데이트하십시오.

참고: 주기적으로 시스템을 업데이트하여 보안 패치와 최신 소프트웨어 버전을 받으십시오.

MDE 설치

이 태스크 정보

MDE 소프트웨어를 설치하려면 다음을 수행하십시오.

예제(ibm_sw_mde_X.x.x-XX.bin 파일)를 사용하여 사용 가능한 소프트웨어 버전에 대해 XX를 빌드 번호로 대체하고 root 사용자로 실행하십시오.

프로시저

1. MDE 기본 OVA를 하이퍼바이저에 배치하십시오. 이 예제에서는 이를 “MDE VM”이라고 합니다.
2. admin으로 로그인하고 새 비밀번호를 설정하십시오.

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

3. MDE VM의 IP 주소를 기록해 두십시오.
4. SCP 또는 유사한 파일 전송 방법을 사용하여 ibm_sw_mde_X.x.x-XX.bin을 MDE로 업로드하십시오.
5. 바이너리 파일을 실행 모드로 지정하십시오.

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

6. 바이너리 파일을 실행하십시오.

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

7. English를 선택하고 Enter를 누르십시오.
8. 라이선스 페이지를 읽고 <OK>로 탭한 다음 'Enter'를 눌러 계속 진행하십시오.
9. <Yes>를 선택하고 Enter를 눌러 라이선스 계약에 동의하십시오.

10. 추출이 완료되면 <OK>에서 Enter를 눌러 명령행으로 돌아가십시오.
11. RPM을 루트로 설치하십시오.

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

12. 이제 MDE가 설치되었지만 아직 구성되지는 않았습니다.

참고: 구성이 완료될 때까지는 MDE VM을 재부팅하지 마십시오.

언어 설정

이 태스크 정보

MDE는 VM 스크립트와 PPM GUI에 대해 다중 언어를 지원합니다. 제품을 실행하기 전에 기본 언어 환경 설정을 구성해야 합니다.

참고: 언어는 RPM을 통해 MDE VM에 설치됩니다. 설치 프로그램 바이너리 파일은 언어 RPM의 기본 제공 세트와 함께 제공됩니다. 초기 설치 이후에 언어를 더 추가할 수 있으며, 이를 적용하기 위해 PPM 서비스를 다시 시작해야 할 수 있습니다.

기본 언어를 구성하려면 아래의 단계를 따르십시오.

프로시저

1. spsd-langsetup 스크립트를 실행하십시오.

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

2. 현재 기본 언어 코드를 보십시오. 설정되어 있지 않으면 이는 공백입니다.

기본 언어 코드를 설정하십시오. 현재 기본값:

3. 사용 가능한 언어 코드의 목록을 보십시오. (아래의 목록은 사용자의 제품 버전에서 사용할 수 없는 예제를 표시할 수 있습니다.)

```
사용 가능한 언어 코드: en_US  
ja_JP  
ko_KR
```

4. 새 기본 언어 코드를 입력하십시오.

새 기본 언어 코드 입력: en_US
이제 기본 언어 코드는 en_US입니다.

5. spsd-langsetup 스크립트를 다시 실행하여 기본 언어 코드가 설정되어 있는지 검증하십시오.

기본 언어 코드를 설정하십시오. 현재 기본값은 en_US입니다.

데이터베이스 설정

이 태스크 정보

MDE는 내부 및 외부 데이터베이스 구성을 지원합니다. 두 경우 모두, MDE를 처음으로 시작하기 전에 구성된 데이터베이스와 MDE가 통신하도록 구성해야 합니다.

데이터베이스를 MDE와 연관시키려면 /etc/spsd/db.props 파일을 수정해야 합니다. root 사용자로 이 파일을 편집해야 합니다.

참고: spsd-pgsetup 스크립트를 실행하면 db.props 파일이 프롬프트에서 입력된 값으로 자동으로 수정됩니다.

아래에서 설명하는 대로 적합한 내부 또는 외부 데이터베이스에 연결하도록 파일 특성을 구성하십시오. 데이터베이스 특성 변경은 MDE가 다시 시작될 때까지 적용되지 않습니다.

중요 참고

db.props 수정 시 다음 제한조건을 준수하십시오.

- 특성 이름과 = 사이에 공백 없음
- =와 특성 값 사이에 공백 없음

내부 데이터베이스

현재 MDE는 내부 데이터베이스로서 PostgreSQL을 지원합니다.

내부 Postgres 데이터베이스

MDE OVA는 PostgreSQL 소프트웨어가 설치된 상태로 사전 패키징되어 제공됩니다. MDE에서 작동하도록 데이터베이스를 구성하려면 아래의 단계를 수행하십시오.

1. "--local" 스크립트 옵션을 지정하여 spsd-pgsetup 스크립트를 실행하십시오.

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

참고: "--local" 옵션은 내부 "로컬" PostgreSQL 서버에서 비어 있는 새 데이터베이스를 구성합니다.

이러한 설정을 적용한 후에는 서버 인증서 설정을 진행하십시오. 원격 대상에서 데이터베이스를 설정하려면 외부 데이터베이스를 진행하십시오.

외부 데이터베이스

현재 지원되는 유일한 외부 데이터베이스 서버는 PostgreSQL입니다. 이 프로세스를 실행하기 전에 다음 정보가 알려져 있는지 확인해야 합니다.

- 액세스 가능한 PostgreSQL 데이터베이스 서버의 이름(또는 IP 주소)
- 위의 PostgreSQL 서버가 청취하는 포트 번호
- 위의 서버에서 기존 데이터베이스의 이름
- 위의 데이터베이스의 소유자로서 정의된 기존 사용자의 이름
- 위의 데이터베이스 사용자의 비밀번호

MDE에서 작동하도록 데이터베이스를 구성하려면 spsd-pgsetup 스크립트를 실행하십시오. 이 명령에서 제공된 모든 값은 예제입니다.

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --host  
ext.postgres.svr1 --port 5432 --dbname policyDB --user policyDBuser  
--pass mypassword123
```

데이터베이스를 최신 스키마로 업그레이드하려면 "--upgrade" 스크립트 옵션으로 spsd-pgsetup 스크립트를 실행하십시오.

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

참고: "upgrade" 옵션을 지정하여 spsd-pgsetup 스크립트를 실행하면 데이터베이스 테이블이 PPM의 현재 버전으로 올바르게 구성되도록 합니다.

이러한 설정을 구성한 후에는 서버 인증서 설정을 진행하십시오.

서버 인증서 설정

키 저장소, 신뢰 저장소 및 인증 기관

인증서를 활용하여 웹 브라우저는 물론 관리 서버(PPM)와 에이전트 간의 보안 통신 세션을 확립할 수 있습니다. PPM에서는 모든 인증서를 인증 기관(CA)에서 서명하도록 요구합니다. CA는 기타 당사자의 ID 확인을 위해 통신 세션의 모든 관계자가 사용하는 신뢰 루트를 확립합니다.

- CA 서명된 인증서는 이에 대응되는 키와 함께 Java 키 저장소에 결합됩니다.
- 에이전트 인증서의 서명에 사용된 CA의 인증서(또는 인증서 번들)를 PPM 신뢰 저장소에 추가해야 합니다.
- 세 개의 모든 구성요소(키 저장소, 신뢰 저장소 및 CA 인증서 번들)는 아래의 PPM 인증서 설정 프로세스에서 사용됩니다.

인증 기관 인증서 프로세스의 샘플은 81 페이지의 『부록 B 샘플 인증 기관(CA) 인증서』의 내용을 참조하십시오.

서버 웹 인증서 키 저장소 및 웹 인증서 신뢰 저장소는 다음을 통해 구성됩니다.

spsd-certsetup - MDE VM의 /opt/securityfirst/spsd/bin 디렉토리에 있는 설치 스크립트

키 저장소와 신뢰 저장소 및 에이전트 CA 번들을 구성하려면 **굵은체**의 예제 입력을 참조하십시오.

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

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

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

참고

키 저장소, 신뢰 저장소 및 CA 번들 등의 서버 인증서 구성요소는 제공되지 않으며 설치 스크립트를 통해 생성되고 MDE VM에 업로드되어야 합니다. CAC(Common Access Card)가 인증에 사용되는 경우에는 PKI 설정을 사용해야 합니다.

공개 키 인프라(PKI) 설정

이 태스크 정보

PKI 구성은 PPM이 PPM 사용자 인증의 2차 방법을 제공할 수 있도록 합니다. 구성된 경우, PPM은 클라이언트 인증서를 웹 및 REST 세션에 대한 인증 방법으로 채택합니다.

이 인증서는 PPM이 신뢰하는 CA에 의해 서명되어야 합니다. PPM은 spsd-certsetup 스크립트에 정의된 규칙을 기반으로 하는 인증서를 검증합니다.

예제 입력은 **굵은체**입니다.

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --crl-on --ocsp-on --pols-on oids
```

```
x.x.x.x.x.x.x.x,Y.Y.Y.Y.Y.Y
```

참고

PKI는 키 저장소, 신뢰 저장소 및 CA 번들과 동일한 스크립트 실행에서 구성될 수 있습니다. 이는 교육용 값을 위해 여기서 나타나 있습니다.

MDE 설치, 데이터베이스 구성, 인증서 추가 및 PKI 설정(선택사항) 이후에는 이제 MDE VM을 재부팅할 수 있습니다.

최초 로그인 시작

이 태스크 정보

일단 배치와 구성이 완료되면, MDE 서버를 재부팅하거나 단순히 MDE 콘솔에서 "spsd" 서비스를 시작하여 웹 GUI를 시작하십시오. 가상 머신 콘솔이나 호스트 하이퍼바이저를 통해 가상 머신의 IP 주소나 호스트 이름을 검색해야 합니다.

지원되는 웹 브라우저를 열고 MDE 로그인 페이지에 도달하기 위한 URL로서 IP 주소나 호스트 이름을 입력하십시오.

https://<MDE Server IP>

이 시점에서는 사용 가능한 지원의 언어 목록에서 언어 설정을 변경할 수 있습니다.

Language English ▼



Please Sign In

User name

Password

Directory

Login

기본 신임 정보는 다음과 같습니다.

사용자 이름: admin
비밀번호: admin

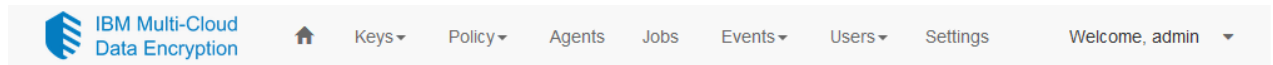
참고

- 최초 로그인 후에 기본 신임 정보를 변경해야 합니다.
- MDE는 Firefox, Chrome, Microsoft Edge 및 Internet Explorer 웹 브라우저의 대부분의 버전을 지원합니다.
- PKI 클라이언트 인증을 사용하는 경우, 이는 로그인 페이지를 우회하고 대시보드로 직접 이동할 수 있습니다.

제 5 장 MDE 그래픽 사용자 인터페이스(GUI)

기본 제품 탐색

MDE에는 페이지 맨 위 탐색 메뉴가 포함됩니다. 일부 메뉴 항목에는 하위 메뉴 목록이 포함됩니다. 각 메뉴 항목을 클릭하여 적절한 페이지로 이동하거나 하위 메뉴 목록을 표시하십시오.



- **홈 아이콘** - 제품 대시보드 홈 페이지에 대한 링크입니다.
- **키** - 키 관련 하위 메뉴 페이지 링크(외부 키 저장소 및 관리 키)가 포함된 메뉴입니다.
- **정책** - 정책 관련 하위 메뉴 페이지 링크(데이터 유형, 경로 세트, 프로세스 및 선택자)가 포함된 메뉴입니다.
- **에이전트** - 에이전트 페이지에 대한 링크입니다.
- **작업** - 작업 페이지에 대한 링크입니다.
- **이벤트** - 이벤트 관련 하위 메뉴 페이지 링크(전달 및 로그)가 포함된 메뉴입니다.
- **사용자** - 사용자 관련 하위 메뉴 페이지 링크(계정 및 LDAP 디렉토리)가 포함된 메뉴입니다.
- **설정** - 설정 페이지에 대한 링크입니다.

참고

MDE는 역할 기반 액세스 제어(RBAC)를 지원합니다. 즉, 일부 탐색 항목은 로그인된 사용자의 역할을 기반으로 사용 가능하지 않습니다. 따라서, 일부 탐색 항목은 모든 관리 사용자에게 대해 사용 가능하지 않을 수도 있습니다.

제품 대시보드

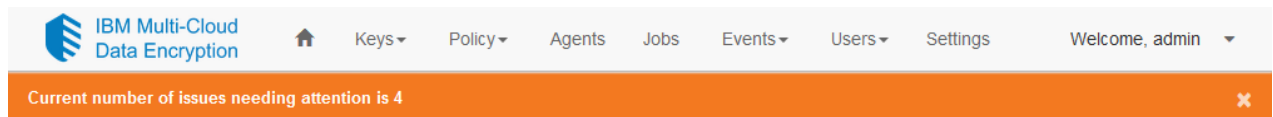
제품 홈 페이지는 기본 시작 대시보드 페이지입니다. 그 용도는 로그인된 관리자에게 최신 이벤트의 현재 상태에 대한 요약 보기를 제공하는 것입니다. 홈 페이지에는 최신 이벤트, 이벤트 경향 및 기타 요약 데이터가 포함되어 있습니다.

텍스트 상자 자동 완성

사용자 인터페이스 전체에 텍스트 입력 필드가 있습니다. 일부 텍스트 입력 필드는 입력된 문자의 자동 완성된 목록을 기반으로 일치 기준을 표시합니다. 자동 완성 제안 목록이 제공되기 전에 이러한 필드에 여러 문자가 필요할 수 있습니다.

주의 알림

처음 로그인 시에 사용자 인터페이스의 맨 위에는 해결해야 하는 조치를 표시하는 색상 배너가 있습니다.



배너의 텍스트를 클릭하면 관리자가 개별 항목이 표시된 “문제” 페이지로 경로 재지정됩니다.

- ▶ The current number of job approvals allows unilateral action. [Dismiss](#)
- ▶ The number of users having Product Administrator role is nearing the threshold of required approvals or required rejections. [Dismiss](#)
- ▶ The number of users having Security Administrator role is nearing the threshold of required approvals or required rejections. [Dismiss](#)
- ▶ One or more users are defined as having both Product Administrator and Security Administrator roles. [Dismiss](#)

개별 항목을 확장하면 문제점 해결 방법에 대한 세부사항이 제공됩니다.

- ▼ The current number of job approvals allows unilateral action. [Dismiss](#)
Summary It is best practice to require a minimum two administrators for job approval.
How to resolve Go to the "Advanced Properties" tab on the "Settings" page, and edit the "Number of approvals required to run a job" field. Note that it may also be wise to do this for number of rejectors as well, depending on company structure.
[Resolve](#)

일단 모든 현안이 해결되면 배너가 표시되지 않습니다. 그러나 관리자는 현재 페이지의 배너를 제거하도록 선택할 수 있습니다.

참고

새 “주의 요망” 문제를 발생시키는 새 조건이 발생할 수 있으며 배너가 다시 나타납니다.

고급 특성

제품 관리자는 제품 작동을 정의하는 고급 특성을 구성할 수 있습니다. 고급 특성은 설정 페이지를 통해 액세스가 가능합니다. 이러한 특성의 범위는 로컬 MDE 인스턴스로 지정되거나 잠재적으로 (고가용성(HA) 또는 다중 테넌트 기능의 레버리지를 활용하는 경우) MDE 에코시스템으로 지정됩니다.

Advanced Properties

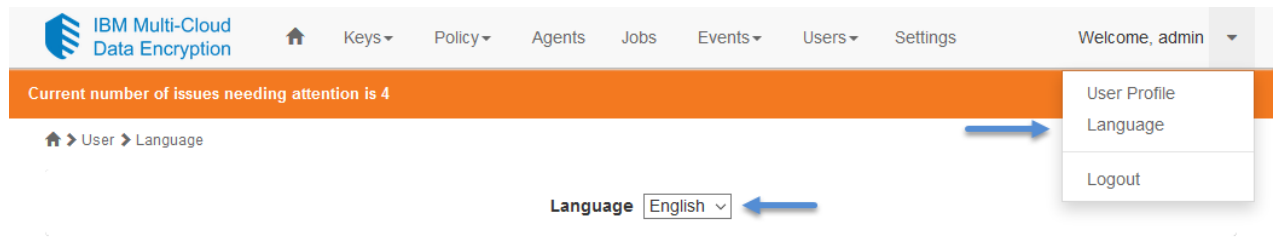
Property	Value	Description	Actions
com.securityfirstcorp.atlantis.bundles.haas.iterations	600000	Number of iterations used by REST API token hashing algorithm	Edit
com.securityfirstcorp.atlantis.jobs.requiredApprovers	1	Number of approvals required to run a job	Edit
com.securityfirstcorp.atlantis.jobs.requiredBuffers	2	The buffer number in between the number of users available and when we issue a warning	Edit
com.securityfirstcorp.atlantis.jobs.requiredRejectors	1	Number of rejections required to reject a job	Edit
events.maxLogLength	50000	Maximum number of entries in event log before rolling starts	Edit
com.securityfirstcorp.atlantis.bundles.userman.iterations	300000	Number of iterations used by user password hashing algorithm	Edit

특성을 편집하려면 제품 관리자가 “편집” 단추를 클릭해야 합니다. 적절히 변경하고 나면 “저장” 단추를 클릭하십시오. 이렇게 하면 작업이 작성됩니다.

GUI 언어 설정

GUI에서, 로그인 페이지나 홈 페이지에서 선택할 때 초기 설치 중에 설치된 지원 언어 중 하나로 변경할 수 있습니다.

- **로그인 페이지** - 페이지의 맨 위 오른쪽에 있습니다. 지원되는 언어의 목록을 보려면 풀다운 메뉴를 클릭하십시오.
- **홈 페이지** - 맨 위 오른쪽 풀다운 메뉴에 있습니다. 지원되는 언어의 목록을 보려면 “언어”를 선택하십시오.

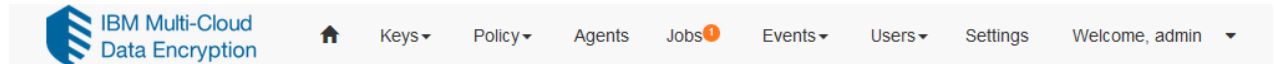


GUI에 표시된 언어는 다음 계층 구조에 의해 판별됩니다(첫 번째 제시된 설정이 사용됨):

1. PPM의 사용자 인터페이스를 통해 설정된 언어 쿠키의 값.
2. 사용자의 브라우저 언어 설정의 값.
3. PPM CLI script-langsetup을 통해 설정된 언어 코드의 값.
4. 처음 찾은 설치된 PPM 언어 팩.

제 6 장 작업

MDE는 실행 중인 태스크 승인 및 타이밍을 관리하기 위해 작업 시스템을 통합합니다. 다수의 기능은 확인되기 전에 승인 대기 위해 작업 시스템을 활용합니다. 작업이 작성되면 새 작업이 작업 페이지 목록에 추가됩니다.



관리자는 각 작업을 승인, 거부 또는 제외할 수 있습니다. 각 관리자는 작업별로 한 번만 조치를 수행합니다.

Type	State	Created	Started	Completed	Notes	Actions
User Create	Waiting	2017-09-22T23:21:01Z				Edit Note Approve Reject Abstain Show Info

작업 설명

작업	설명	범주	역할
고급 특성	고급 특성 수정	제품 관리	제품 관리자
키 저장소 수정	정책 적용 키 저장소의 위치/세부사항 변경	제품 설정	제품 관리자
키 로테이션	에이전트 에코시스템에서 키 세트 로테이션	키 관리	보안 관리자
키 취소	에이전트 에코시스템에서 키 세트 취소	키 관리	보안 관리자
키 폐기	에이전트 에코시스템에서 키 세트를 영구적으로 제거하여 데이터가 유실되도록 함	키 관리	보안 관리자
에이전트 추가	에코시스템에 새 에이전트를 프로비저닝 및 추가	에이전트 관리	보안 관리자
에이전트 삭제	MDE 관리에서 에이전트 제거	에이전트 관리	보안 관리자
에이전트 수정	에이전트 관련 정보 수정	에이전트 관리	보안 관리자
정책 업데이트	에이전트 관련 정책 수정	에이전트 관리	보안 관리자
새 관리 사용자 작성	새 MDE 관리자 작성	MDE 관리 사용자 관리	제품 관리자
관리 사용자 삭제	MDE 관리자 제거	MDE 관리 사용자 관리	제품 관리자
관리 사용자 역할 추가	MDE 관리자에 역할 추가	MDE 관리 사용자 관리	제품 관리자
관리 사용자 역할 제거	MDE 관리자에서 역할 제거	MDE 관리 사용자 관리	제품 관리자
관리 사용자 비밀번호 변경	MDE 관리자의 비밀번호 변경	MDE 관리 사용자 관리	제품 관리자
관리 사용자 상태 변경	MDE 관리 사용자 계정 사용 또는 사용 안함	MDE 관리 사용자 관리	제품 관리자

디렉토리 등록	MDE 관리 사용자에게 대한 LDAP 서버 디렉토리 구성	MDE 관리 사용자 관리	제품 관리자
디렉토리 삭제	MDE에서 LDAP 서버 디렉토리 제거	MDE 관리 사용자 관리	제품 관리자
디렉토리 업데이트	LDAP 서버 디렉토리 수정	MDE 관리 사용자 관리	제품 관리자

다중 관리자 승인

필수 승인자 및 거부자 수는 MDE 내에서 구성할 수 있습니다. 기본적으로 MDE는 단일 관리자 승인으로 구성됩니다. 둘 이상의 관리자가 작업 승인에 필수가 되도록 권장됩니다. 다중 관리자 승인은 한 명의 관리자가 MDE 자체 내 또는 모든 관리 에이전트 인스턴스에서 변경을 수행하지 못하도록 합니다.

User	Time	Actions	Required Approvals	Required Rejections	Notes
admin	2017-09-22T23:22:35Z	Approve	1	1	

중요 참고

관리자의 수는 “필수 승인” 또는 “필수 거부” 작업의 수를 충족하거나 이를 초과해야 합니다. 이러한 값을 변경하기 전에 필요한 수의 관리자가 있는지 확인하십시오.

승인 및 거부 임계값은 작업 유형으로 대체될 수 있습니다. 특성 변경 작업을 제외하고 시스템에서 정의한 각 작업 유형에는 고급 특성에 승인 및 거부 임계값이 있습니다. 이 임계값을 설정하면 시스템 기본값을 겹쳐씹니다. 특성이 설정되면 특성을 설정 해제할 수 없습니다.

특성 변경 작업은 고급 특성의 수정을 제어하므로 승인 및 거부 임계값이 없는 유일한 작업 유형입니다. 이 작업의 경우 승인 및 거부 임계값은 항상 시스템 기본값보다 더 높거나 다른 모든 작업 유형에 대해 정의된 가장 높은 겹쳐쓰기 값입니다. 이 조치는 특성 변경 프로세스를 통해 다른 작업 유형 임계값을 되돌릴 수 없도록 합니다.

작업 승인

작업을 승인하려면 적절한 권한이 있는 관리자가 작업 페이지를 탐색한 후 적절한 작업을 찾아서 "승인" 단추를 클릭해야 합니다. 일단 필요한 수의 관리자 승인에 도달하면 작업이 실행됩니다.

작업 거부

작업을 거부하려면 적절한 권한이 있는 관리자가 작업 페이지를 탐색한 후 적절한 작업을 찾아서 "거부" 단추를 클릭해야 합니다. 일단 필요한 수의 관리자 거부에 도달하면 작업이 영구적으로 취소됩니다.

작업 제외

작업에서 제외는 관리자에게 작업이 표시되지만 이를 승인하거나 거부하지 않는 것을 의미합니다. 제외는 "감사" 위치로 가장 적절하게 설명되며 관리자가 나중에 동일한 작업에서 다른 위치를 선택하지 못하도록 합니다.

작업 정보

MDE 내의 각 작업에는 이를 설명하는 서로 다른 정보가 있습니다. “정보 표시” 단추를 클릭할 수 있으며 작업 특정 정보가 표시됩니다. 추가로 다른 관리자별로 작업에서 수행하는 모든 조치(승인, 거부, 제외)가 조치를 수행한 관리자의 사용자 이름과 같이 표시됩니다.

User Create	Done	2017-09-22T23:22:36Z	2017-09-22T23:22:36Z	2017-09-22T23:22:36Z		<div>Hide Info</div>
-------------	------	----------------------	----------------------	----------------------	--	----------------------

User	Time	Actions	Required Approvals	Required Rejections	Notes
admin	2017-09-22T23:22:35Z	Approve	1	1	

Job Properties

User	ProductAdmin
------	--------------

제 7 장 MDE 관리 사용자 관리

관리 사용자 역할

MDE는 일반 정적 역할 기반 액세스 제어(RBAC) 설계를 사용합니다. MDE 내의 특정 기능은 특정 권한을 요구합니다. MDE 권한의 전체 세트는 두 개의 개별 역할인 제품 관리자와 보안 관리자로 그룹화됩니다. 각 역할의 추가 관리자는 언제든지 추가할 수 있습니다.

제품 관리자 역할

제품 관리자 역할은 MDE 제품 구성 및 유지보수에 필요한 권한으로 일임됩니다.

보안 관리자 역할

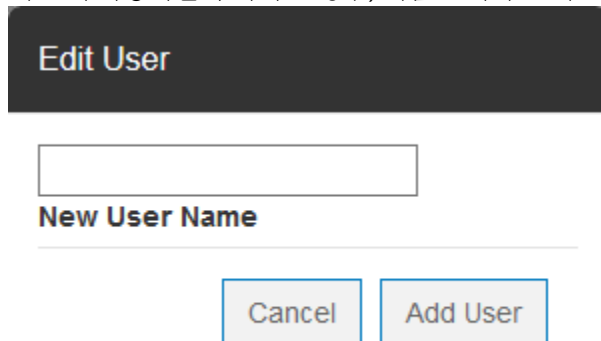
보안 관리자 역할은 에이전트를 프로비저닝하고 관리하는 데 필요한 권한으로 일임됩니다. 다음은 포함되지만 이로 한정되지는 않습니다. 정책 정의 및 스펙, 키 관리, 데이터 유형 정의, 에이전트 관리, 외부 키 저장소 구성, 정책에 대한 외부 그룹의 외부 LDAP 구성.

관리 사용자 관리

제품 관리자는 MDE 내에서 다른 관리 사용자를 추가, 수정, 제거하는 데 필요한 권한을 처리합니다.

새 관리 사용자 추가

새 관리 사용자를 추가하는 경우, 제품 관리자는 새 관리 사용자 이름을 입력하도록 프롬프트됩니다.



The screenshot shows a dark-themed dialog box titled "Edit User". Inside, there is a text input field labeled "New User Name". Below the input field are two buttons: "Cancel" and "Add User".

고유 사용자 이름을 채우고 작업이 이 관리 사용자를 MDE에 추가하도록 작성됩니다.

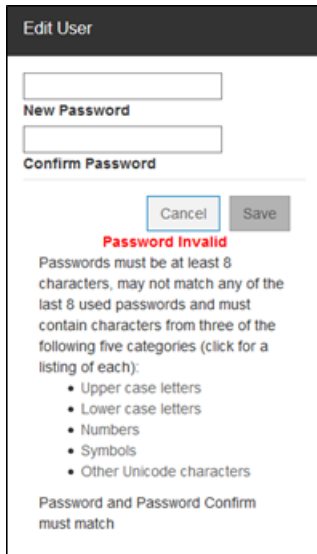
Type	State	Created	Started	Completed	Actions
Scheduler	Waiting	2019-03-20T16:14:01Z			Approve Reject Abstain Hide Info
<div><div>Approved None</div><div>Rejected None</div><div>Abstained None</div></div>					
Type : User Create		Frequency : Once		Starts : Upon approval	
Job Properties					
User				test	

사용자가 작성되려면 필수 제품 관리자 수가 작업을 승인해야 합니다.

새로 추가된 관리 사용자는 만료된 비밀번호를 사용하며 정의된 역할 없이 작성됩니다. 제품 관리자가 초기 비밀번호, 역할 및 상태를 편집해야 합니다. 업데이트할 때마다 작업을 생성합니다. 작업은 새 관리 사용자가 MDE에서 활성화되기 전에 승인되어야 합니다.

관리 사용자 비밀번호 편집

관리 사용자 비밀번호를 편집하려면 해당 사용자를 탐색한 후 "비밀번호 편집" 단추를 선택하십시오. 비밀번호 항목 대화 상자가 표시됩니다.



식별된 규칙을 준수하는 비밀번호를 입력하십시오. 입력한 후에 변경사항을 저장하면 작업이 작성됩니다.

비밀번호 변경사항을 적용하려면 필요한 수의 관리자가 작업을 승인해야 합니다.

참고: 새로 추가된 관리자에게 초기 로그인 시 비밀번호를 변경하라는 프롬프트가 표시됩니다.

관리 사용자 역할 편집

관리자의 역할을 편집하려면 사용자 행을 찾고 “역할 편집” 단추를 선택하십시오. 역할 항목 선택란이 인라인으로 표시됩니다.

편집을 수행 중인 관리자는 자신이 소유하는 것과 동일한 역할을 적용할 수 있습니다(예: 제품 관리자와 보안 관리자 역할을 모두 적용할 수 있는 초기 사용자인 “기본 제공 admin 사용자”). 그리고 동일한 역할이 부여된 사용자는 동일한 작업을 수행할 수 있습니다.

ProductAdmin	Disabled	<input type="checkbox"/> Product Administrator <input type="checkbox"/> Security Administrator	2017-09-22T23:25:40Z	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
--------------	----------	---	----------------------	---

원하는 역할을 선택하고 "변경사항 저장" 단추를 클릭하면 작업이 작성됩니다.

역할 변경사항이 적용되려면 필요한 수의 관리자가 작업을 승인해야 합니다.

관리 사용자 상태 편집

관리 사용자 상태를 편집하려면 영향을 받는 사용자를 탐색하고 "상태 편집" 단추를 선택하십시오. 상태 항목 드롭 다운이 인라인으로 표시됩니다.

ProductAdmin	Disable	None	2017-09-22T23:25:40Z	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
--------------	---------	------	----------------------	---

상태 값은 사용, 사용 안함 및 잠김입니다.

- **사용** - 관리자가 활성 상태이며 조치를 수행할 수 있습니다.
- **사용 안함** - 관리자가 비활성 상태이며 조치를 수행할 수 없습니다.
- **잠김** - 관리자가 잠금 상태이며 조치를 수행할 수 없습니다.

원하는 상태를 선택하고 “저장”을 클릭하십시오. 작업이 사용자 상태를 수정하기 위해 작성됩니다.

상태 변경사항이 적용되려면 필요한 수의 관리자가 작업을 승인해야 합니다.

관리 사용자 제거

관리자를 제거하려면 대상 사용자 행을 찾고 “삭제” 단추를 클릭하십시오. MDE에서 사용자를 제거하는 작업이 시작됩니다. 이 조치는 제품 관리자 역할이 있는 사용자만 수행할 수 있습니다.

Type	State	Created	Started	Completed	Notes	Actions
User Delete	Waiting	2017-09-22T23:37:05Z				<div>Edit Note</div> <div>Approve</div> <div>Reject</div> <div>Abstain</div> <div>Show Info</div>

사용자를 제거하려면 필요한 수의 관리자가 작업을 승인해야 합니다.

중요 참고

- 관리 사용자 제거는 영구적인 조치입니다.
- 필수 작업 승인 조건을 충족할 수 있도록 충분한 관리 사용자 수를 유지해야 합니다("다중 관리자 승인" 절 참조).
- 충분한 관리자가 없으면 작업을 정상적으로 승인할 수 없습니다.

사용자 계정 잠금

무차별 비밀번호 공격으로부터 시스템 및 사용자 계정을 보호하기 위해 10번 연속 실패한 로그인 시도 후에는 사용자 계정이 잠깁니다. 계정이 명시적으로 활성화되거나("관리 사용자 상태 편집" 절 참조) 서버 서비스가 다시 시작될 때까지 사용자 계정은 잠겨 있게 됩니다.

참고

- 서버 서비스를 다시 시작하려면 가상 머신 콘솔에서 **systemctl restart spsd**를 실행하십시오.
- 계정 잠금은 서버별로 이루어집니다. 클러스터의 한 서버에서 잠긴 계정은 클러스터 내의 다른 서버에서 자동으로 잠기지 않습니다.
- 계정 잠금 임계값은 사용자가 구성할 수 없습니다.

LDAP 디렉토리 목록

제품 관리자는 MDE 사용자 관리를 위해 LDAP 디렉토리를 구성할 수 있습니다. LDAP 디렉토리는 추가, 수정, 삭제할 수 있습니다. 각 조치는 적용 전에 승인을 위한 작업을 작성합니다.

LDAP 디렉토리를 추가/변경하는 경우에 사용 가능한 설정은 다음과 같습니다.

- **디렉토리 ID** - LDAP 디렉토리의 ID입니다.
- **유형** - LDAP 또는 Active Directory의 드롭 다운 옵션입니다.
- **바인드 DN** - LDAP 서버에 바인드하는 데 사용되는 전체 구별 이름입니다.

바인드 DN 샘플 구문은 다음과 같습니다.

```
uid=${username},ou=users,dc=company,dc=com
```

참고: “Active Directory” 유형을 선택하면 바인드 DN 정보가 필요하지 않으므로 바인드 DN 절이 회색 처리됩니다.

- **호스트** - LDAP 서버의 IP/호스트 이름입니다.
- **포트** - LDAP 서버의 포트입니다.
- **보안** - 보안 또는 비보안 LDAP 연결의 ID입니다.

• 조치 - 저장 또는 취소 선택

Directory ID	Type	Bind DN	Host	Port	Secure	Actions
LDAP1	LDAP	uid={\$username},ou=users,dc=company,dc=com	10.10.10.1	636	<input checked="" type="checkbox"/>	<div>Save</div> <div>Cancel</div>

사용자 소스

MDE는 내부 및 외부 정의 사용자를 동시에 지원할 수 있습니다. 외부 정의 사용자는 사용자 목록의 "디렉토리" 컬럼에 값을 표시합니다. 내부 정의 사용자는 해당 필드가 공백입니다.

Name	Status	Roles	Directory	PW Modified	Actions
admin	Enabled	Product Administrator, Security Administrator		2017-09-22T23:09:44Z	<div>Edit Password</div> <div>Edit Roles</div> <div>Delete</div>
ProductAdmin	Enabled	Product Administrator		2017-09-22T23:25:40Z	<div>Edit Password</div> <div>Edit Status</div> <div>Edit Roles</div> <div>Delete</div>
SecurityAdmin	Enabled	Security Administrator		2017-09-22T23:42:22Z	<div>Edit Password</div> <div>Edit Status</div> <div>Edit Roles</div> <div>Delete</div>

제 8 장 이벤트

MDE에는 이벤트 집계 및 전달 시스템이 포함됩니다. 이 시스템은 내부적으로 생성된 이벤트와 함께 관리 에이전트의 이벤트를 집계하고 이를 내부 이벤트 로그에 저장합니다. 또한 하나 이상의 수신자에게 이벤트를 전달하도록 이를 구성할 수도 있습니다.

이벤트 로그

MDE 이벤트 로그는 맨 위 레벨 메뉴 표시줄에서 이벤트 메뉴 항목을 선택하여 볼 수 있습니다.

[Home](#) > [Events](#) > [Logs](#)

☐ Show Redacted Events Reload Export CSV

Show 10 entries Search:

Sequence	ID	Message	Type	Severity	Timestamp	Source
16	PS000D0005	Requested action change-passw...	SYSTEM	INFO	2017-09-22T23:42:22Z	localhost
15	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:22Z	localhost
14	PS000D0005	Requested action change-user-st...	SYSTEM	INFO	2017-09-22T23:42:21Z	localhost
13	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:21Z	localhost
12	PS000D0005	Requested action change-user-ro...	SYSTEM	INFO	2017-09-22T23:42:21Z	localhost
11	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:21Z	localhost
10	PS000D0005	Requested action change-user-st...	SYSTEM	INFO	2017-09-22T23:36:47Z	localhost
9	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:36:47Z	localhost
8	PS000D0005	Requested action change-user-ro...	SYSTEM	INFO	2017-09-22T23:35:51Z	localhost
7	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:35:51Z	localhost

Showing 1 to 10 of 16 entries First Previous 1 2 Next Last

이 페이지는 단일 순차 목록으로 모든 이벤트를 표시합니다. 각 이벤트에는 아래에 정의된 대로 순서 번호, ID, 메시지, 유형, 심각도, 수신 시간소인 및 소스가 포함됩니다.

- **순서 번호** - 이벤트가 수신되는 순서에 대한 숫자 속성입니다. 이는 고유하며(동일한 이벤트가 반복되는 경우에도) 시간이 지남에 따라 증가됩니다.
- **ID** - 이벤트의 고유 ID입니다. 동일한 이벤트에 대한 다중 인스턴스는 공통 ID를 가집니다.
- **메시지** - 이벤트 중인 조건을 식별하는 설명 텍스트입니다. 일부 이벤트는 변수 삽입을 지원할 수도 있기 때문에 이벤트 ID가 공통되는 동안 텍스트가 조금 다를 수도 있습니다.
- **유형** - 이벤트가 시스템 조치에서 시작되는지 또는 사용자 조치에서 시작되는지 여부를 설명합니다. 유형은 다음과 같습니다.
 - **SYSTEM** - 자동화된 MDE 조치로 시작된 이벤트입니다.
 - **AUDIT** - 사용자 조치로 시작된 이벤트입니다.
- **심각도** - 이벤트의 인지 레벨에 대한 상대적 표시입니다. 심각도 범주는 다음과 같습니다.
 - **INFO** - 조치가 필요하지 않으며 정보 전용입니다.
 - **WARN** - 즉각적인 조치가 필요하지 않으며, 조건 모니터링을 권장합니다.

- **CRITICAL** - 즉각적인 조치가 필요합니다.
- 시간소인 - 이벤트 시작 시간에 대한 협정 세계시(UTC) 형식의 표시입니다.
- 소스 - 이벤트가 시작된 시스템(에이전트 또는 MDE)의 호스트 이름 또는 IP입니다.

MDE 이벤트 로그 크기는 고급 설정을 통해 구성이 가능합니다. 설정 크기 한계에 도달하면 가장 오래된 이벤트는 새 이벤트가 수신될 때 로테이션됩니다.

이벤트 세부사항

이벤트는 이벤트 메시지의 일부가 아닌 확장된 인수를 가질 수 있습니다. 이벤트가 있으면 이벤트는 이벤트 로그의 메시지 옆에 세부사항 링크를 표시합니다. 세부사항 단추를 클릭하면 확장된 인수가 표시됩니다.

34	P600140002	Agent 1 logged off: reason code 1005.	Details	Absolute process path:	2018-04-10T15:02:05Z	localhost
33	DEC2014	Read/write denied for user3 on /home/data/	Details	Decision: Deny	2018-04-10T15:01:19Z	cos5-file
32	DEC2010	Read denied for user4 on /home/data/	Details	Group name: user3	2018-04-10T15:01:19Z	cos5-file
31	DEC2011	Write permitted for user1 on /home/development/	Details	Operation: Read or Write	2018-04-10T15:01:19Z	cos5-file

이벤트 내보내기

MDE를 사용하여 관리자는 이벤트 페이지의 CSV 내보내기 단추에서 이벤트 목록을 CSV 파일 형식으로 내보낼 수 있습니다.

🏠 > Events > Logs

☐ Show Redacted Events

Reload Export CSV

"CSV 내보내기" 단추를 클릭하면 이벤트 파일이 클라이언트 머신으로 다운로드됩니다. 이벤트 파일의 각 행은 로그의 이벤트입니다.

이벤트 파일의 열은 이벤트 순서 번호, 이벤트 ID, 수정된 플래그, 이벤트 메시지 문자열(인수 누락), 이벤트 유형, 이벤트 심각도, 이벤트 인수, 이벤트 시간소인 및 이벤트 소스 등입니다.

이벤트 전달

수신된 모든 이벤트는 구성된 각 이벤트 수신자에 전달됩니다. 내부 이벤트 로그에 삽입될 때 이벤트는 병렬로 전달됩니다.

제품 또는 보안 관리자는 제품의 이벤트 수신자를 수정할 수 있습니다. 구성된 후에 작성되었거나 MDE로 수신된 모든 이벤트는 수신자에 전달됩니다. 지원되는 수신자 유형은 Syslog입니다.

🏠 > Events > Forwarding

Email Recipients

New Email Recipient

Email	Host	Port	Security	User	Password	Format	Actions
No Recipients							

Syslog Recipients

New Syslog Recipient

Host	Port	Format	Actions
No Recipients			

MDE는 전달되는 이벤트에 대해 다중 형식도 지원합니다. 지원되는 형식은 LEEF(Log Event Extended Format), CEF(Common Event Format), CADF(Cloud Auditing Data Federation) 이벤트 모델입니다.

이벤트 인수

일반 이벤트 메시지 문자열 외에도 이벤트 인수가 키/값 매개변수로 전송됩니다. 이러한 매개변수는 접두어 "spx"와 인수 이름이 연결된 문자열로 식별됩니다. 예를 들어, 이벤트에 사용자 이름이 포함되어 있으면 문자열 키/값 쌍은 "spxuser=user1"이 될 수 있습니다.

에이전트 이벤트

MDE는 각 관리(및 연결된) 에이전트에서 시스템 및 감사 이벤트를 집계합니다. 이러한 이벤트는 MDE 이벤트 로 그에 표시되며 구성된 모든 이벤트 수신자에게 전달됩니다.

참고

MDE, 외부 데이터베이스와 모든 에이전트가 NTP의 레버리지를 활용하여 시스템 시간을 조정하도록 적극 권장합니다. 그러면 이벤트 / 감사 로그 시간소인이 올바르게 순서화됩니다.

신뢰 가능한 이벤트

개별 에이전트에서 MDE로 전송된 이벤트는 실시간으로 처리됩니다. 이는 이벤트가 누락된 경우 MDE가 에이전트에 다시 연결하고 누락된 이벤트를 요청하며 이를 적절한 순서로 이벤트 로그에 삽입하도록 보장합니다.

제 9 장 정책 적용 키 관리

보안 관리자는 MDE 내에서 보안 스토리지를 위해 정책 적용 키를 정의할 수 있습니다. 해당 키는 데이터의 보안을 설정하고 암호 액세스 제어를 제공하기 위해 데이터 유형 및 볼륨에 연관 가능합니다.

🏠 > Keys > Managed Keys

Submit Rotation Job				New Key
ID	Name	Created	Notes	Actions
1	Key1	2017-09-22T23:49:12Z		Edit Submit Revocation Job
2	Key2	2017-09-22T23:49:17Z		Edit Submit Revocation Job
3	Key3	2017-09-22T23:49:23Z		Edit Submit Revocation Job

키 추가

새 키를 추가하는 경우, 고유 이름을 입력해야 합니다. 키 이름은 대소문자를 구분하지 않습니다. 키 값은 노출되지 않으며 사용자가 편집할 수 없습니다. 참고 필드는 선택사항입니다.

ID	Name	Created	Notes	Actions
	<input type="text"/>		<input type="text"/>	Save Cancel

참고

키 이름은 변경할 수 있지만 실제 키 값은 사용자가 수정할 수 없습니다.

키는 '키' 페이지 또는 에이전트 작성 마법사에서 작성할 수 있습니다. 에이전트 마법사에서 작성한 모든 "시스템 정의" 키는 자동 생성되므로 관리할 수 없습니다. 키는 '키' 페이지에서만 편집할 수 있습니다.

키 편집

키를 작성한 후에 보안 관리자는 키 이름을 수정할 수 있습니다. 키 이름을 변경해도 실제 기본 키 값은 변경되지 않습니다. 참고 필드도 수정할 수 있습니다.

키 로테이션

MDE를 사용하면 보안 관리자는 에이전트 에코시스템 내에서 키를 로테이션할 수 있습니다. 키 페이지에서 "키 로테이션 작업 제출" 단추를 클릭하십시오.

공개 키 업로드가 프롬프트됩니다. 이 키는 로테이션된 키에 대한 키 에스스로에 사용됩니다. 해당 키를 선택하고 키를 추가한 후 "다음"을 클릭하십시오.

중요 참고

SSL 키는 RSA 및 PEM 인코딩되어야 합니다.

Key Rotation



This wizard will assist you in selecting keys to be scheduled for rotation. Once the keys are selected, a job to rotate the keys will be queued for approval.

Upload Public Key

Browse...

No file selected.

Add Public Key

Public Key

Next

사용자가 작성한 모든 키 목록이 표시됩니다. 보안 관리자는 로테이션하려는 원하는 수 만큼의 키를 선택할 수 있습니다.

Key Rotation



Select one or more keys from the list of all keys:

☒ Key1

☐ Key2

☐ Key3

Back

Next

원하는 키를 선택하면 작업이 작성됩니다.

중요 참고

키가 둘 이상의 에이전트와 연관된 경우, 해당 키를 사용하는 모든 에이전트에 영향을 줍니다.

작업 승인 시, 영향을 받는 모든 에이전트에 키 로테이션이 통지됩니다. 작업은 영향을 받는 모든 에이전트가 키 로테이션 프로세스를 완료할 때까지 계속 실행됩니다. 영향 받는 에이전트 수에 따라 이 작업은 완료 시까지 시간이 더 소요될 수 있습니다.

참고

외부 키 저장소를 사용하는 경우, 이는 키 로테이션의 성공을 위해 **온라인** 상태여야 합니다. 오류가 발생하면 외부 키 저장소가 온라인 상태인지 확인하고 PPM 서버를 재부팅하거나 PPM 서비스(spsd)를 다시 시작하십시오.

키 취소

키 취소는 MDE에서 키를 제거하고 해당 키를 에스스로 배치합니다. 키 취소는 현재 활성 정책에 연관되지 않은 키에서만 수행될 수 있습니다. 키를 취소하기 전에 보안 관리자는 해당 키를 참조하는 정책을 제거해야 합니다.

에이전트 정책 연관의 키를 사용하는 경로를 제공하면 디스크의 데이터가 복호화되지 않기 때문에 데이터에 액세스해야 하는 경우 데이터는 해당 경로에 연관된 정책을 제거하기 전에 보호된 디렉토리에서 마이그레이션해야 합니다.

취소 완료 후에 보호된 경로에 남아 있는 모든 데이터에는 액세스할 수 없습니다. 취소된 키는 에스스로 저장되며 정상 PPM 조작에서는 제거됩니다.

경고

보안 관리자는 해당 키를 취소하기 전에 모든 에이전트로부터 대상 키를 분리시키기 위해 에이전트 정책을 업데이트해야 합니다. 경로 삭제에 대한 자세한 정보는 “에이전트 편집”에 관한 절을 참조하십시오.

키 폐기

키 폐기는 키 취소와 동일하게 작동하지만 키 폐기 조작이 완료되면 키는 에스스로 추가되지 않으며 데이터에는 영구적으로 액세스할 수 없습니다.

참고

이 기능은 REST API를 통해서만 사용할 수 있습니다. 세부사항은 REST API 문서를 참조하십시오.

자동 생성 키

보안 관리자가 정책 적용 키를 관리하지 않으려는 경우, MDE는 새로 작성된 각 정책에 대해 키를 자동 생성할 수 있습니다. 자동 생성 키는 항상 작성 시마다 고유하며 키 관리 페이지에는 표시되지 않습니다.

중요 참고

자동 생성 키는 로테이션하거나 취소할 수 없습니다. 키를 로테이션하거나 취소하는 기능이 필요하면 이름 지정된 키를 대신 사용하십시오.

외부 키 저장소

키는 내부 보안 데이터베이스 또는 외부 키 저장소의 두 위치 중 하나에 저장될 수 있습니다. MDE는 초기에 내부 보안 데이터베이스만 사용하도록 설정됩니다. 보안 관리자가 외부 키 저장소의 레버리지를 활용하려는 경우에는 이를 구성해야 합니다. 외부 키 저장소는 키 보호용으로만 사용됩니다. 외부 키 저장소의 키 관리는 MDE를 통해 이루어져야 합니다.

참고

외부 키 저장소의 설정에 대한 지시사항은 외부 키 저장소 공급업체가 제공합니다.

KMIP 키 저장소

이 태스크 정보

보안 관리자는 Java 키 저장소와 Java 신뢰 저장소를 업로드해야 합니다. 다음 단계에 따라 Java 키 저장소와 Java 신뢰 저장소를 작성하십시오.

프로시저

1. 클라이언트 인증서 파일 및 클라이언트 개인 키 파일을 PKCS12(Public Key Cryptography Standard #12) 형식으로 수집하십시오. 이후 단계에서 이는 "client.p12"라고 합니다. (클라이언트 인증서와 클라이언트 개인 키를 PKCS12 형식 파일로 결합하는 데 관한 샘플은 85 페이지의 [『부록 C PKCS12 파일 작성을 위한 샘플 변환』](#)의 내용을 참조하십시오.
2. 공용 CA 인증서 파일을 수집하십시오. 이후 단계에서 이는 "sklm_ca.pem"이라고 합니다.

```
[user@localhost]$ keytool -importkeystore -srckeystore client.p12 -keystore client.jks -storetype JKS
```

3. PKCS12 파일을 새 Java 키 저장소로 가져오십시오.

중요 참고

이 설정 중에 비밀번호를 확인합니다. 나중에 사용할 수 있도록 이 비밀번호를 보유하십시오.

```
[user@localhost]$ keytool -v -list -keystore client.jks
```

4. 파일에서 별명을 가져오십시오.
5. CA 인증서 파일을 새 Java 신뢰 저장소로 가져오십시오.

```
[user@localhost]$ keytool -import -trustcacerts -alias sklm  
-file sklm_ca.pem -keystore sklmtrust.jks
```

중요 참고

이 설정 중에 비밀번호를 확인합니다. 나중에 사용할 수 있도록 이 비밀번호를 보유하십시오.

6. 파일에서 별명을 가져오십시오.

```
keytool -v -list -keystore trust.jks
```

외부 키 저장소가 활성화되기 위해 파일링해야 하는 설정:

- **이름** - 외부 키 저장소에 대한 사용자 정의된 참조
- **상태** - 이는 MDE에 정의된 외부 키 저장소가 현재 활성 키 저장소를 겹쳐쓰도록 지시합니다. 상태가 활성화인 경우, MDE는 키 저장소를 사용하여 시작됩니다. 상태가 비활성인 경우에는 MDE가 더 이상 키 저장소를 사용하지 않습니다.
- **호스트** - 외부 키 저장소의 IP 주소입니다.
- **포트** - 외부 키 저장소의 포트 번호입니다.
- **클라이언트 키 저장소**
 - **키 저장소 별명** - 수집된 키 저장소 별명입니다.
 - **키 저장소 파일** - Java 키 저장소 파일입니다.
 - **클라이언트 키 저장소 비밀번호** - 키 저장소 작성 시의 비밀번호 설정입니다.
- **신뢰 저장소**
 - **신뢰 저장소 별명** - 수집된 신뢰 저장소 별명입니다.
 - **신뢰 저장소 파일** - Java 신뢰 저장소 파일입니다.
 - **신뢰 저장소 비밀번호** - 신뢰 저장소 작성 시의 비밀번호 설정입니다.

- **마스터임** - 모든 읽기/쓰기 조작에 대해 마스터 키 저장소로서 사용되는 외부 키 저장소를 식별합니다.
 - 정의된 첫 번째 키 저장소의 경우, 기본값은 “true”입니다.
 - 선택되지 않은 경우, 이는 “복제본” 키 저장소로서 간주되며 읽기 조작에만 사용됩니다.
 - 하나의 외부 키 저장소만 마스터로서 지정될 수 있습니다.

KMIP Keystore New KMIP KeyStore

Name	State	Host	Port	Client Keystore	Truststore	Is Master	Actions
<input type="text"/>	In: <input type="button" value="v"/>	<input type="text"/>	5696 <input type="button" value="v"/>	Alias <input type="text"/> Keystore Password <input type="text"/>	Alias <input type="text"/> Truststore Password <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
				Keystore Upload <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload"/>	Truststore Upload <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload"/>		

참고

현재 MDE는 외부 키 저장소 제품(KMIP용으로 구성된 IBM SKLM(Security Key Lifecycle Manager)을 지원 합니다.

하드웨어 보안 모듈(HSM)

이 태스크 정보

HSM을 외부 키 저장소로 사용할 때는 제조업체의 지시사항에 따라 써드파티 제품이 모두 구성되어 작동 중인지 확인해야 합니다.

HSM의 64비트 버전 클라이언트 소프트웨어가 PPM 제품 관리자에 의해 MDE PPM VM에 복사되어야 합니다. 통신을 설정하고 구성하기 위한 HSM 제조업체의 제품 지시사항을 사용하여 SDK 옵션에 따라 소프트웨어를 추출하고 설치해야 합니다.

HSM에서의 작동이 입증된 유틸리티나 클라이언트 소프트웨어와 함께 제공되는 유틸리티가 래퍼 키 작성에 사용됩니다. 래퍼 키는 PPM에서 사용할 수 있어야 하는 256-대칭 키입니다.

이 대칭 래퍼 키가 HSM에서 작성된 경우에는 핸들이 이에 지정됩니다. 이 핸들은 PPM GUI 페이지에서 HSM을 구성할 때 필요합니다. PPM은 정책 키의 래핑을 위해 이 핸들과 정책 키를 HSM에 전달하며, HSM은 PPM 데이터 베이스에 저장될 수 있도록 래핑된 키를 리턴합니다.

소프트웨어를 설치하고 구성한 후에는 PPM이 HSM과 통신할 수 있는지 확인하고 PPM VM을 재부팅하십시오.

외부 키 저장소 화면에서 새 HSM 키 저장소를 선택하십시오.

🏠 > Keys > External Keystores

HSM Keystore New HSM KeyStore

Name	State	HSM Token	Key Handle	HSM Password	Actions
No External Keystores					

KMIP Keystore New KMIP KeyStore

Name	State	Host	Port	Client Keystore	Truststore	Is Master	Actions
No External Keystores							

외부 키 저장소가 활성화되려면 다음의 설정을 채워야 합니다.

- **이름** - 외부 키 저장소에 대한 사용자 정의된 참조
- **상태** - 이는 키 저장소에 대해 원하는 상태를 설정함
- **HSM 토큰** - HSM은 파티션의 슬롯 번호를 사용함
- **키 핸들** - 정책 키를 래핑하는 데 사용될 키에 지정된 핸들
- **HSM 비밀번호** - 고객이 사용할 파티션과 연관된 비밀번호

HSM Keystore

[New HSM KeyStore](#)

Name	State	HSM Token	Key Handle	HSM Password	Actions
<input type="text"/>	Inactive <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

참고: 지원되는 HSM 제품: HSM 키 저장소용으로 구성된 SafeNet® Luna HSM.

제 10 장 파일 레벨 정책 정의

MDE를 사용하여 보안 관리자는 다양한 데이터에서 파일 레벨 제어(운영 및 암호화)를 정의할 수 있습니다. 아래 용어는 파일 레벨 데이터 제어 정의 시에 사용됩니다.

- **선택자** - 리소스(또는 경로 세트)에 대한 액세스가 허용되는 사람을 정의하는 순서가 지정되지 않은 사용자 및 그룹의 목록입니다. 선택사항으로, 정의된 프로세스는 선택자에 대한 다른 구성요소로서 식별될 수 있습니다.
- **경로 세트** - 정책에 의해 보호되는 파일 경로의 목록입니다.
- **데이터 유형** - 지정된 유형의 데이터에 지정된 액세스 정의 행의 순서화된 목록입니다. 각각의 행은 선택자, I/O(읽기/쓰기) 조작 및 정책 조치로 구성되어 있습니다.
- **프로세스** - 실행 파일에 대한 파일 경로입니다. 식별된 실행 파일의 액세스 제어를 정의하기 위해 선택자에서 사용됩니다. 보다 고급의 액세스 제어를 위한 선택사항입니다.

데이터 유형이 작성되면 하나 이상의 프로비저닝된 에이전트에 연관 가능합니다. 다음 절은 정책의 구성을 설명합니다.

선택자

선택자는 하나 이상의 선택자 행을 통해 사용자 및/또는 사용자 그룹 세트를 정의하는 정책 오브젝트입니다. 선택자를 새로 추가하는 경우, 보안 관리자는 저장 전에 이름을 제공해야 합니다. 선택자 행을 편집하여 선택자 참고 및 행을 언제든지 추가할 수 있습니다.

각 선택자 행에는 사용자, 그룹, 프로세스 필드가 포함됩니다. 저장하기 전에 필드 중 하나를 채워야 합니다.

- **사용자** - 대상 시스템 정의된 사용자의 축약형 이름입니다. 이는 대상 에이전트 운영 체제의 사용자와 일치됩니다. 이 필드는 선택사항입니다.
- **그룹** - 대상 시스템 또는 LDAP 정의된 사용자 그룹의 축약형 이름입니다. 이는 대상 에이전트 운영 체제의 사용자 그룹과 일치됩니다. 이 필드는 선택사항입니다.
- **프로세스** - 제품 정의된 프로세스 이름에 대한 참조입니다. 이는 대상 에이전트의 운영 체제에서 프로세스 파일 경로(및 선택적 해시 값)와 일치됩니다. 이 필드는 선택사항입니다.

🏠 > Policy > Selectors

Expand All Collapse All Search Enter Text Clear New Selector

Name: Selector1 Save Cancel Add New Row

Notes

User	Group	Process	Actions
<input type="text"/> user01	<input type="text"/>	<input type="text"/>	Delete Row

각 선택자 행의 값은 논리 AND 연산으로 결합됩니다. 단일 행에 여러 필드가 설정된 경우, 모든 필드는 일치하는 행에 대해 일치해야 합니다. 선택자는 정의된 임의의 행이 일치하는 경우에 일치합니다. 선택자 내에서 행 순서는 정책 일치 알고리즘에 영향을 주지 않습니다.

사용자	그룹	프로세스	에이전트 일치 작동
✓			사용자에 대해 일치
	✓		정의된 그룹의 사용자에 대해 일치

		✓	정의된 프로세스 경로에 대해 일치 및 잠재적으로 제공된 해시 값으로 제한
✓	✓		정의된 그룹의 구성원으로서 행동하는 경우에만 사용자에게 대해 일치
✓		✓	정의된 프로세스를 통해 행동하는 경우에만 사용자에게 대해 일치
	✓	✓	정의된 프로세스를 통해 행동하는 경우에만 정의된 그룹의 사용자에게 대해 일치
✓	✓	✓	정의된 그룹의 구성원으로서 행동하고 프로세스로 정의된 프로세스를 통해 행동하는 경우에만 사용자에게 대해 일치

참고

선택자 사용자 및/또는 그룹 확인은 파일 에이전트가 설치된 외부의 구성된 LDAP 서버 또는 Active Directory 서버에서 작동합니다.

경로 세트

경로 세트는 순서가 지정되지 않은 하나 이상의 파일 경로 행의 컬렉션입니다. 경로 세트를 추가할 때 보안 관리자는 경로 세트의 이름을 제공해야 합니다. 경로 세트에 행을 추가하려면 “경로 추가” 단추를 클릭하십시오. 각 행에는 파일 경로 및 참고가 포함됩니다.

🏠 > Policy > Path Sets

Expand All Collapse All

Search Enter Text Clear New Path Set

▶ Name: Pathset1 Save Cancel Add Path

Notes

Path	Notes	Actions
/protected		Delete Path

보안 관리자는 파일 경로를 제공해야 합니다. 보호는 제공된 경로에서 모든 하위 디렉토리를 포함하여 반복 순환됩니다. 참고 필드는 선택사항입니다.

데이터 유형

데이터 유형은 데이터에 대한 파일 레벨의 운영 및/또는 암호화 액세스 제어가 사용되도록 설정하는 데이터 유형 행 정의에 대한 순서화된 컬렉션입니다. 각 데이터 유형에는 이름, 정책 적용 키, 사용자 참고, 행에 대한 순서화된 목록이 포함됩니다.

- 이름 - 데이터 유형에 대한 사용자 정의된 참조
- 사용자 참고 - 보안 관리자 정의된 참고 필드

데이터 유형 행

각각의 데이터 유형 행에는 순서, 선택자, 조작 및 조치 필드가 포함되어 있습니다.

- 순서 - 각 정책 행이 검사되는 우선순위입니다. 첫 번째로 일치하는 행이 사용됩니다. 이 필드는 필수이지만 하나의 행만 있는 경우에는 표시되지 않습니다.
- 선택자 - 이전에 정의한 선택자의 선택사항입니다. 정책 행은 선택자에서 임의의 행이 일치하는 경우 일치합니다. 이 필드는 필수입니다. MDE는 임의의 사용자에게 대해 일치되는 "모두 선택" 선택자를 제공합니다.
- 조작 - 수행 가능한 파일 조작의 선택사항입니다. 옵션은 "읽기" 및 "읽기/쓰기"입니다. 이 필드는 필수입니다.
- 조치 - 조작에 연관되는 액세스 선택사항입니다. 옵션은 "허용", "거부", "허용, 로그", "거부, 로그"입니다. 이 필드는 필수입니다.

데이터 유형 행 변수

선택자, 조작, 조치 필드는 선택적으로 변수로 설정할 수 있습니다. 그러면 보안 관리자가 조치 작성 중에 완료되는 데이터 유형에 대한 템플릿을 작성할 수 있습니다. 사용 가능한 필드 설정은 편집할 수 있음, 편집해야 함, 편집할 수 없음입니다.

편집할 수 있음

이 필드는 에이전트 작성 중에 선택적으로 겹쳐줄 수 있습니다.

편집해야 함

이 필드는 에이전트 작성 중에 설정해야 합니다.

편집할 수 없음

이 필드는 데이터 유형 작성 중에 설정되며 에이전트 작성 중에는 변경할 수 없습니다.

Create/Edit Datatype

Name

Notes

Rules

Order	Selector	Operation	Actions	Delete
1 ▾	<div>Not Editable ▾</div> <div>Selector1 <input type="checkbox"/> Select All</div>	<div>Not Editable ▾</div> <div>Read or Write ▾</div>	<div>Not Editable ▾</div> <div>Permit ▾</div>	Delete
▲ 2	<div>Not Editable ▾</div> <div><input checked="" type="checkbox"/> Select All</div>	<div>Not Editable ▾</div> <div>Read or Write ▾</div>	<div>Not Editable ▾</div> <div>Deny, Log ▾</div>	Delete

[Add New Row](#)

[Save](#) [Cancel](#)

데이터 유형은 모든 행에 값 및/또는 변수 설정이 있을 때까지 저장할 수 없습니다.

프로세스

프로세스는 실행 파일에 대한 파일 시스템 경로를 식별합니다. 프로세스는 다음 필드로 구성되어 있습니다.

- **이름** - 프로세스의 이름입니다.
- **경로** - 파일 시스템 실행 파일에 대한 절대 경로입니다.
- **OS** - 운영 체제 유형(Linux, Windows, AIX)을 참조하는 데 사용되는 필드입니다.
- **버전** - 운영 체제 버전에 사용되는 필드입니다.
- **배포** - 운영 체제 배포 이름(Red Hat, CentOS, Windows, AIX)에 사용되는 필드입니다.

🏠 > Policy > Processes

Expand All Collapse All Search Clear New Process

▶ Name Processes1 Save Cancel Add Hash

Path	OS	Version	Distribution
<input type="text" value="/usr/bin/cat"/>	<input type="text" value="Linux"/>	<input type="text" value="6.7"/>	<input type="text" value="CentOS"/>

Hash	Actions
------	---------

프로세스는 파일 경로만으로 또는 프로세스 해시 값의 목록으로 정의될 수 있습니다. 하나 이상의 해시 값이 정의된 경우, 프로세스 일치는 나열된 해시로 제한됩니다.

참고

프로세스 해시 값은 에이전트 도구를 통해 생성되며 PPM에 복사되어야 합니다. 도구는 실행 파일의 현재 버전에 대한 해시 값을 출력합니다.

```
spxhash -p <path to executable>
```

예제:

```
[root@blkdr ~]# spxhash -p /usr/bin/vim
```

```
1202E81EF41273904A6DD381C35B2561F838F7E35B6B26959F8EEB646297A36A7C2
```


제 11 장 에이전트 프로비저닝 및 관리

MDE는 볼륨, 정책이 적용된 파일, 정책이 적용된 볼륨 및 오브젝트 저장소의 네 가지 에이전트 설치 유형을 지원합니다. 각 에이전트 유형은 서로 다른 데이터 보호 방법을 사용합니다.

- **볼륨** - 에이전트가 블록 디바이스 레벨에서 데이터를 보호함
- **정책이 적용된 파일** - 에이전트가 파일 레벨에서 데이터를 보호하고 파일 기반의 운영 액세스 제어 정책을 제공함
- **정책이 적용된 볼륨 에이전트** - 에이전트가 블록 디바이스 레벨에서 데이터를 보호하고 파일 기반의 운영 액세스 제어 정책도 제공함
- **오브젝트 저장소** - 에이전트가 오브젝트 저장소에 전송된 데이터를 보호함

에이전트 추가

에이전트를 추가하려면 보안 관리자가 MDE의 에이전트 페이지를 탐색하고 "에이전트 추가" 드롭 다운 목록을 클릭해야 합니다. 사용 가능한 에이전트 옵션이 나열됩니다.



에이전트 유형을 선택한 다음 에이전트를 작성할 수 있는 마법사가 열립니다.

참고: 프로세스 도중 이러한 구성요소를 작성할 수 없으므로 에이전트 추가 프로세스를 시작하기 전에 의도된 모든 정책 구성요소(선택자, 경로 세트, 키, 데이터 유형 및 프로세스)를 추가하는 것이 좋습니다.

에이전트를 프로비저닝하기 위한 6개의 섹션(에이전트 식별, 네트워크 정보, 정책, 볼륨, 권한 부여된 사용자 및 도구)이 있습니다. 모든 필수 섹션은 에이전트 추가 전에 완료되어야 합니다.

ID

ID 섹션에서는 보안 관리자가 이름, UUID, 운영 체제 및 Notes를 정의해야 합니다.

A screenshot of the 'Add File With Policy Agent' form. The form is divided into 'Required' and 'Optional' sections. Under 'Required', there are fields for 'Name *', 'UUID *' (with a refresh icon), and 'Operating System *' (a dropdown menu). There is also a 'Notes' text area. Under 'Optional', there are radio buttons for 'Policy', 'Authorized Users', and 'Tools'. A 'Next' button is at the bottom right.

- **이름** - 에이전트에 대한 사용자 정의된 참조입니다.
- **UUID** - MDE가 에이전트 식별에 사용하는 고유 ID입니다.
- **운영 체제** - 대상 에이전트의 운영 체제입니다.
- **참고** - 이 에이전트에 대한 보안 관리자 참고입니다.

필수 필드를 모두 입력하고 나면 **저장**을 클릭하여 다음 단계로 이동하십시오.

참고:

- MDE에서 UUID를 자동으로 채우지만, 필요한 경우 관리자가 대체할 수 있습니다.
- 필수 필드는 GUI에 표시되어 있습니다.
- 에이전트 이름은 고유하지 않습니다. 그러므로 여러 에이전트에 동일한 이름을 사용하는 경우 이벤트 로그 메시징이 메시지 소스를 잘못 표현할 수 있습니다.

네트워크

네트워크 단계에서는 보안 관리자가 MDE뿐 아니라 에이전트의 호스트 이름이나 IP 주소를 정의해야 하며 인증서가 MDE와 대상 에이전트 간의 보안 연결을 확립해야 합니다.

Subject	Fingerprint	Expiry	Private Key	Actions
No Certificates				

- **IP 주소**- 에이전트가 설치되는 서버의 IP 주소 또는 호스트 이름입니다.
- **MDE 피어 IP** - 대상 에이전트 서버 인스턴스에서 표시되는 MDE의 IP 주소 또는 호스트 이름입니다.

참고: MDE에서 MDE 피어 IP를 자동으로 채우지만, 필요한 경우 보안 관리자가 수정할 수 있습니다.

- **인증서** - MDE와 설치된 에이전트 간의 보안 연결 설정에 사용되는 업로드된 인증서의 목록입니다. 이 인증서는 에이전트와 MDE PPM 서버 간에 상호 인증된 TLS1.2 연결을 설정하는 데 사용됩니다.

인증서를 업로드하려면 보안 관리자가 **인증서 추가**를 클릭하고 원하는 인증서를 탐색한 후 열어야 합니다. 인증서는 새 에이전트-네트워크 화면에 표시됩니다.

참고: 키 저장소와 신뢰 저장소 인증서가 MDE에 업로드되지 않았으며 에이전트에 일치하는 인증서가 지정되지 않은 경우에는 에이전트와 PPM이 통신하지 않으며 에이전트가 데이터 암호화와 정책 적용을 수행하지 않습니다. 세부사항은 “서버 인증서 설정” 절을 참조하십시오.

필수 필드를 모두 입력하고 나면 **다음**을 클릭하여 다음 단계로 이동하십시오.

정책이 제공된 파일, 정책이 적용된 볼륨 및 볼륨 에이전트 작성

정책 단계에서는 보안 관리자가 대상 에이전트에서 파일 경로에 대한 운영 및 암호화 제어를 정의해야 합니다.

경로 추가

정책이 적용된 파일 및 정책이 적용된 볼륨 에이전트는 에이전트 정책에 경로 정의를 추가할 수 있습니다. 추가된 각 경로는 대상 에이전트에서 개별 파일 경로 또는 파일 경로 그룹을 보호합니다. 추가되는 경로 수는 보안 관리자가 정의합니다.

중요 참고

- 정책 적용 시에는 정책을 통해 보호되는 경로가 존재해야 하며, 그렇지 않으면 정책 적용에 실패합니다.
- 기존 파일과 서브디렉토리는 정책이 적용된 파일 에이전트의 설치 후에 사용 가능한 **spxconvert** 명령을 사용하여 수동으로 처리되어야 합니다. 파일이 암호화되지 않은 경우에도 정책은 적용됩니다.
- 설치 이후에 추가된 새 파일과 디렉토리는 정책을 통해 자동으로 암호화되고 보호됩니다.

Add File With Policy Agent

Required

- ✓ Agent Identity
- ✓ Network Information

Optional

- Policy
- Authorized Users
- Tools

[Add Path](#) [Back](#) [Next](#)

경로를 추가하려면 **경로 추가**를 클릭하십시오.

추가된 각 경로에는 파일 경로 또는 경로 세트, 키 및 데이터 유형의 항목이 필요합니다.

Add File With Policy Agent

Required

- ✓ Agent Identity
- ✓ Network Information

Optional

- Policy
- Authorized Users
- Tools

*** Required**

File Policy Path (or Path Set)*

[Delete](#)

Storage ☒ Local ☐ Network

Key ☐ System Defined ☒ User Defined

Name

Datatype*
(remember to fill out any empty values below)

Selector	Operation	Actions
Select All	Read or Write	Permit

[Add Path](#) [Back](#) [Next](#)

- **파일 정책 경로(또는 파일 세트)** - 식별된 데이터 유형 액세스 제어 정의로 보호되는 경로나 경로의 그룹을 식별합니다. 보호는 제공된 파일 경로에서 모든 하위 디렉토리를 포함하여 반복 순환됩니다.
- **스토리지** - 파일 경로의 위치를 식별합니다. 옵션은 로컬 또는 네트워크입니다. 네트워크를 선택한 경우 네트워크 스토리지를 올바르게 구성하려면 추가 매개변수를 입력해야 합니다. (아래 구성 정보 참조)
- **키** - 데이터 유형과 연관된 경로의 암호화에 사용되는 키입니다. 이전에 정의된 사용자 정의 키 또는 MDE 관리 시스템 정의 키를 사용할 수 있습니다. 이 필드는 정책이 적용된 파일 또는 정책이 적용된 볼륨 사용 여부에 따라 표시되거나 표시되지 않을 수 있습니다(참고 참조).
- **데이터 유형** - 사전 작성된 데이터 유형의 선택입니다. 선택하면 데이터 유형 정보가 인라인으로 추가됩니다. 변수가 있는 데이터 유형이 사용되면 변수는 저장 전에 입력해야 합니다.

참고:

- 경로 세트를 사용 중인 경우, 이는 새 에이전트를 추가하기 전에 작성되어야 합니다. 그렇지 않으면, 하나의 수동 경로가 정의될 수 있습니다.
- 사용되는 데이터 유형은 새 에이전트 추가 전에 작성되어야 합니다.
- 새 에이전트가 정책이 적용된 볼륨 유형인 경우, 보호가 볼륨 정책 정의를 통해 수행되기 때문에 경로 세트에는 정책 적용 키가 포함되지 않습니다.

로컬 스토리지 구성

파일 정책 경로를 정의할 때 로컬 스토리지를 사용하는 경우 **로컬 스토리지** 옵션을 선택하십시오. 이렇게 하면 에이전트는 정의된 절대 파일 경로(또는 경로 세트)를 보호합니다. 추가 매개변수는 필요하지 않습니다.

네트워크 스토리지 구성

파일 정책 경로를 정의할 때 네트워크 스토리지를 사용하는 경우 “네트워크 스토리지” 옵션을 선택하십시오. 이렇게 하면 에이전트는 정의된 절대 파일 경로로 정의된 네트워크 스토리지를 마운트합니다. 경로 세트는 네트워크 정의 스토리지와 함께 사용할 수 없습니다. 추가 매개변수가 필요합니다.

네트워크 스토리지에는 프로토콜, 호스트 이름/IP, 공유, 사용자 이름, 비밀번호 및 고급 마운트 옵션에 대한 정의가 필요합니다.

- **프로토콜** - 활용되는 네트워크 스토리지 유형을 식별합니다. 옵션은 NFSv4 및 NFSv3입니다.
- **호스트 이름/IP** - 네트워크 스토리지 시스템의 호스트 이름/IP
- **공유** - 네트워크 파일 시스템 내보내기 위치
- **사용자 이름** - (NFSv3의 경우 필수 아님) 네트워크 파일 시스템에 대한 인증 사용자 이름
- **비밀번호** - (NFSv3의 경우 필수 아님) 네트워크 파일 시스템에 대한 인증 비밀번호
- **고급 마운트 옵션** - NFS 정의에 적용할 선택으로 구분된 옵션

필수 필드를 모두 입력하고 나면 **다음**을 클릭하여 다음 단계로 이동하십시오.

볼륨

볼륨 추가

이 태스크 정보

볼륨 및 정책이 적용된 볼륨 에이전트 유형은 에이전트 정책에 하나 이상의 볼륨 정의를 추가할 수 있습니다. 추가되는 각 볼륨은 대상 에이전트에서 보호되는 새 블록 디바이스입니다.

Add Volume With Policy Agent

Required

✓ Agent Identity

✓ Network Information

Optional

☐ Policy

☒ **Volumes**

☐ Authorized Users

☐ Tools

Volumes

Device Label

Key

Autogenerate Key Required

Delete

Add Volume

Back

Next

볼륨을 추가하려면 **볼륨 추가**를 클릭하십시오. 추가된 각 볼륨에서는 정책 적용 키와 기본 디바이스 레이블의 항목이 필요합니다.

- **디바이스 레이블** - 보호 중인 디바이스를 식별합니다. 정책이 에이전트에 배치된 후에 디바이스 레이블은 `spxdevice` 명령을 실행하여 볼륨에 연관되어야 합니다(에이전트 설치 절 참조).
- **키** - 볼륨 암호화에 사용되는 키입니다. 이전에 정의된 키 또는 MDE 관리 자동 생성 키를 사용할 수 있습니다.

중요 참고

“자동 생성 키” 옵션을 사용하지 않는 한 추가된 정책 적용 키는 에이전트 추가 이전에 정의되어야 합니다. 정책 적용 키 관리 절을 참조하십시오.

필수 필드를 모두 입력하고 나면 **다음**을 클릭하여 다음 단계로 이동하십시오.

오브젝트 저장소 에이전트 작성

MDE 오브젝트 스토리지 에이전트(OSA)는 클라이언트와 백엔드 오브젝트 스토리지 사이의 중재자 역할을 수행합니다. 오브젝트 스토리지 클라이언트에서는 백업된 오브젝트 스토리지 신임 정보가 아니라 버킷 신임 정보를 사용하여 OSA에 연결합니다.

관리자가 하나 이상의 오브젝트 스토리지 제공자에 연결하도록 OSA를 구성할 수 있습니다. OSA에서는 OSA를 통해 구성된 백엔드 오브젝트 스토리지에 보낸 데이터를 암호화하고 정책을 적용합니다. 두 개 이상의 백엔드가 구성된 경우 데이터가 분할되고 데이터 조각이 각 백엔드에 전송됩니다.

프론트 엔드 인증서

오브젝트 저장소 클라이언트와 오브젝트 저장소 에이전트 사이의 보안 연결을 설정하려면 오브젝트 저장소 에이전트에서 인증서를 구성해야 합니다.

인증서를 업로드하려면 보안 관리자가 "인증서 추가" 단추를 클릭하고 원하는 인증서를 탐색한 후 열어야 합니다.

Add Object Store Agent
✕

Required

- ☒ Agent Identity
- ☒ Network Information

Optional

- ☒ **Front-End Certificates**
- ☐ Bucket Credentials
- ☐ Buckets
- ☐ Backends
- ☐ Authorized Users
- ☐ Tools

Front-End Certificate Add Certificate

Subject	CN=localhost,OU=Development,O=Security First Corp.,L=Rancho Santa Margarita,ST=California,C=US
Fingerprint	e9cf021f7092bec53ec27ba29467b2d3e70b2b2e1d5ed6acd738af363860b2bd
Expiry	2016-11-09T23:11:06Z
Private Key	False

Back
Next

필수 필드를 모두 입력하고 나면 "다음"을 클릭하여 다음 단계로 이동하십시오.

버킷 신임 정보

여러 오브젝트 스토리지 제공자와 통신하도록 MDE를 구성할 수 있습니다. 각 제공자는 버킷과 버킷 신임 정보를 구성해야 합니다.

Add Object Store Agent

Required

✓ Agent Identity

✓ Network Information

Optional

✓ Front-End Certificates

⊙ Bucket Credentials

○ Buckets

○ Backends

○ Authorized Users

○ Tools

* Required

QHW1UOGRU90BFNYZQ0CH

Delete

Key ID *

QHW1UOGRU90BFNYZQ0CH

API Key *

78dKnlcLBiUkQgl6OLjtBKqNoglZw54S6g5SSiik5JX0wOvZ0x0IIZoTa=PGKK3B

Protocol *

IBM S3

XH2BW34YV12A0REPF3TW

Delete

Key ID *

XH2BW34YV12A0REPF3TW

API Key *

3AoMJ9fXv3p1xpU8xoAqfSt=DoEaX=3iY7UOyVn3ovUAQ4ssKAbQQvAv1jmHPeXh

Protocol *

AMZ S3

New Credential

Back

Next

새 신임 정보 세트를 추가하려면 "새 신임 정보" 단추를 클릭하십시오.

버킷 신임 정보에는 키 ID, API 키 및 프로토콜의 정의가 필요합니다.

- **키 ID** – 오브젝트 저장소 액세스의 ID
- **API 키** – 키 ID와 상관시키기 위해 S3 API에 제공하는 문자열 비밀번호
- **프로토콜** – 오브젝트 스토리지 제공자(Swift, IBM S3 및 Amazon S3)와 통신하는 데 이용하는 프로토콜의 ID

MDE에서 키 ID와 API 키 쌍을 생성합니다. 원하는 경우 관리자가 이 생성된 값을 겹쳐쓸 수 있습니다. 관리자가 지원되는 오브젝트 스토리지 제공자 중에서 원하는 프로토콜을 선택해야 합니다.

필수 필드를 모두 입력하고 나면 "다음"을 클릭하여 다음 단계로 이동하십시오.

버킷

MDE에서 버킷 연관을 통해 오브젝트 스토리지 정책을 정의합니다. 각 버킷에는 이름, 로그 거부 및 정책 정의가 필요합니다.

Add Object Store Agent

Required

✓ Agent Identity

✓ Network Information

* Required

Bucket Name *

testBucket

Delete

Log Denials

☒

Policy

Key ID *	Access *	Log	Actions
XH2BW34YV12A0REPF3TW	Read or Write ▾	<input checked="" type="checkbox"/>	Delete
QHW1UOGRU90BFNYZQ0CH	Read or Write ▾	<input checked="" type="checkbox"/>	Delete
New Row			

New Bucket

Optional

✓ Front-End Certificates

✓ Bucket Credentials

⊙ Buckets

○ Backends

○ Authorized Users

○ Tools

Back

Next

- **이름** - 오브젝트 스토리지 버킷의 이름
- **로그 거부** - 선택란 선택사항. 선택하면 오브젝트 저장소 에이전트에서 액세스 거부에 관한 감사 로그를 작성합니다.
- **정책** - 버킷 액세스 제어의 정의. 정책은 여러 행으로 구성될 수 있습니다. 각 정책 정의 행에는 키 ID, 액세스, 로그가 필요합니다.
- **키 ID** - 사전 작성된 버킷 신임 정보 키 ID 항목.
- **액세스** - 읽기 또는 쓰기, 읽기 또는 쓰기 액세스 권한 중 선택사항.
- **로그** - 선택란 선택사항. 선택하면 오브젝트 스토리지 에이전트에서 제공된 행 동작의 액세스 허용에 관한 감사 로그를 작성합니다.

필수 필드를 모두 입력하고 나면 "다음"을 클릭하여 다음 단계로 이동하십시오.

백엔드

백엔드 연결 정보는 M:N 선택사항을 통해 정의합니다. 이 선택사항에 따라 오브젝트 스토리지 데이터의 보안 및 중복이 정의됩니다. N은 구성된 백엔드 오브젝트 스토리지 제공자 도는 "공유" 수를 나타냅니다. M은 데이터를 재구성하는 데 필요한 공유 수를 나타냅니다. 지원되는 구성은 1:1, 2:3, 2:4입니다.

Add Object Store Agent

Required

✓ Agent Identity

✓ Network Information

M:N 2:3

* Required

Optional

✓ Front-End Certificates

✓ Bucket Credentials

✓ Buckets

⊙ Backends

○ Authorized Users

○ Tools

Share 1 *

URL *

ID *

Key *

Protocol * IBM S3

Share 2 *

URL *

ID *

Key *

Protocol * IBM S3

Share 3 *

URL *

ID *

Key *

Protocol * IBM S3

Back

Next

각 공유에는 URL, ID, 키 및 프로토콜이 구성되어 있어야 합니다.

- **URL** – 오브젝트 스토리지 제공자의 액세스 URL
 - **ID** – 오브젝트 스토리지 제공자에 액세스하는 계정 사용자 ID.
 - **키** – 오브젝트 스토리지 제공자에 액세스하는 사용자 ID 계정.
 - **프로토콜** -- 오브젝트 스토리지 제공자(Swift, IBM S3 및 Amazon S3)와 통신하는 데 이용하는 프로토콜의 ID
- 필수 필드를 모두 입력하고 나면 "다음"을 클릭하여 다음 단계로 이동하십시오.

권한 부여된 사용자

사용자 단계에서 보안 관리자는 에이전트 설치 번들을 다운로드할 권한이 있는 MDE 사용자 계정을 정의해야 합니다.

사용자가 권한 부여된 사용자로서 나열되지 않으며 해당 사용자가 로그인하여 에이전트를 보는 경우, 해당 사용자는 에이전트 정보 페이지에서 다운로드 링크를 보지 못합니다.

필수 필드를 모두 입력하고 나면 **다음**을 클릭하여 다음 단계로 이동하십시오.

에이전트 도구

에이전트는 암호화된 형식으로 데이터를 전송하는 데 도움이 되는 특수 도구를 지원합니다. 도구에는 두 가지 유형, 즉 백업/복원 및 오브젝트 저장소가 있습니다.

도구는 에이전트 프로비저닝 중 또는 에이전트 정보 페이지에서 구성됩니다. 백업/복원 도구는 암호화된 데이터를 백업 및 복원할 때 사용됩니다. 이 도구에서는 연관된 키를 활용하여 암호화된 데이터를 백업하고 정책 키가 로테이션된 경우에도 나중에 암호화된 데이터를 복원할 수 있는 기능을 제공합니다. 백업/복원 도구는 선택사항이며 도구를 에이전트와 연관시킬 필요가 없습니다. 오브젝트 저장소 도구는 오브젝트 저장소 에이전트에 필요합니다.

에이전트 도구 매트릭스

도구 가용성은 에이전트 유형을 기반으로 하며 키를 연관시켜 활성화됩니다. 에이전트 유형별 도구 매트릭스는 다음과 같습니다.

도구 유형	블룸	정책이 적용된 블룸	정책이 적용된 파일	오브젝트 저장소
백업/복원	✓	✓	✓	
오브젝트 저장소				✓

도구 키 연관

키를 도구에 연관시키려면 원하는 도구 옆에 있는 텍스트 상자에 이전에 정의한 키 이름을 입력한 다음 목록에서 해당 키를 선택하십시오.

저장을 클릭하면 작업이 작성됩니다. 승인되면 구성된 도구를 에이전트에서 사용할 수 있게 됩니다.

참고: 자동 생성 키는 도구에서 지원되지 않습니다. 에이전트를 작성하기 전에 키를 정의해야 합니다.

필수 필드를 모두 입력하고 나면 **다음**을 클릭하여 다음 단계로 이동하십시오.

검토 및 빌드

이 태스크 정보

모든 프로비저닝 단계가 완료되면 사용자가 검토 화면으로 이동합니다.

프로비저닝 설정의 검토 페이지에 모든 구성 정보에 대한 전체 보기가 표시됩니다.

Add File With Policy Agent

Agent Build Summary

Identity

Name

fileAgent

UUID

c5bf0b5a-99b2-4dcc-8e82-2a559d5319c4

Type

File with Policy

Operating System

CentOS / Red Hat 7

Notes

Network

Back

Build

컨텐츠에서 완성도와 정확성을 검토한 후 **빌드**를 클릭하여 프로비저닝 프로세스를 완료하십시오. 에이전트를 추가하는 작업이 작성됩니다.

작업이 승인되면 에이전트가 작성되고 설치 패키지가 다운로드 및 설치 가능합니다.

에이전트 활성화

에이전트 빌드 작업이 승인되면 새로 작성된 에이전트가 MDE 내에서 활성화됩니다. 에이전트가 설치되면 구성된 MDE 피어 IP와 제공된 인증서를 사용하여 MDE에 대해 상호 인증된 TLS1.2 연결을 작성합니다.

에이전트는 초기 설치 및 후속 시작 시에 정책을 요청합니다. MDE는 구성된 정책 구성으로 응답합니다. 정책이 수신되면 이는 에이전트에서 적용됩니다.

에이전트 보기

이 태스크 정보

에이전트 페이지는 작성된 에이전트에 대한 요약 목록을 표시합니다.

Agents

Agent Report

Search

Name	Hostname or IP	Type	Notes	Actions
Agent1	1.1.1.1	Volume with Policy		<input type="button" value="Details"/> <input type="button" value="Delete Agent"/>

특정 에이전트에 대한 세부사항을 보려면 이름 열에서 에이전트 이름을 클릭하거나 조치 열에서 세부사항 단추를 클릭하십시오. 이는 프로비저닝 정보, 설치 번들 다운로드, 기타 유용한 정보를 표시하는 에이전트 세부사항 보기를 엽니다.

에이전트 보고서

MDE 보안 관리자가 에이전트 보고서를 작성할 수 있습니다. 이 보고서에는 총 에이전트 수, 유형 및 운영 체제별 에이전트 수, 보고서 생성 이후 30일 내에 로그인된 에이전트에 대한 정보가 포함되어 있습니다. 날짜는 UTC 시간인 PPM 시간을 기반으로 합니다. 데이터는 에이전트 유형에 따라 구분됩니다.

🏠 > Agents

Agent Report

Search

Enter Text

Clear

Add Agent

에이전트 설치

이 태스크 정보

에이전트에 필요한 모든 정보를 구성한 프로비저닝 단계는 대상 서버 인스턴스로 정책을 설치 및 배치합니다. 에이전트를 설치하려면 설치 패키지를 다운로드하고 이를 대상 시스템으로 복사한 후 콘텐츠를 언팩하고 설치 스크립트를 실행하십시오.

🏠 > Agents > Agent1

Agent Info

Edit Agent Info

Identity

Notes

Name

Agent1

UUID

dab30682-19ee-4763-84d8-12fe2ba91948

IP Address

1.1.1.1

Type

Volume with Policy

Operating System

CentOS / Red Hat 7

Network

MDE Peer IP

1.1.1.0

Certificates

Subject	Fingerprint	Expiry
CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US	ea584e4904fffa45a3416eccc753e0f0f655462929d4f1534f369cbccc38165f	2016-11

Browse...

No file selected.

Users

Download Tokens

Authorized Users

admin

Install Files Download URL

/rest/agents/1/install_bundle

Download Zip Bundle

Download Tar Bundle

ID	State
<div>Add Token</div>	

중요 참고

프로비저닝 정책에서 식별된 모든 사용자, 그룹 및 경로 또는 디바이스가 에이전트 시스템에 대해 작성, 연결 및 구성되었는지 확인하십시오.

Linux용 에이전트 설치

볼륨 에이전트, 정책이 적용된 파일 에이전트, 정책이 적용된 볼륨 에이전트 및 오브젝트 저장소 에이전트의 4가지 에이전트 유형이 있습니다. 에이전트 프로비저닝 중에 지정된 에이전트 유형을 사용하십시오.

Linux 볼륨 에이전트 디바이스 구성

이 태스크 정보

프로시저

1. PPM에서 볼륨을 작성(11.1.5절에서 사용된 디바이스 레이블 기억)
2. 에이전트 VM에서 “gettext” 패키지 설치
3. 에이전트 설치 - 세부사항은 77 페이지의 『부록 A 샘플 에이전트 설치 프로세스』의 내용을 참조하십시오.
4. 설치가 완료되면 에이전트 VM 재부팅
5. 루트로서 `spxdevice -e <label given in PPM> -m <mount point> -f <file system> -u <disk to use>` 명령 실행

```
spxdevice -e C0S6V0L -m /protected -f ext4 -u /dev/sdb
```

Linux 정책이 적용된 파일 에이전트 디바이스 구성

이 태스크 정보

프로시저

1. PPM에서 정책이 적용된 파일 에이전트 작성
2. 필수 사용자 작성
3. 모든 필수 서브디렉토리 작성
4. 디렉토리에서 적절한 권한 설정
5. 에이전트 VM에 “gettext” 패키지 설치
6. 에이전트 설치 - 세부사항은 77 페이지의 『부록 A 샘플 에이전트 설치 프로세스』의 내용을 참조하십시오.
7. 설치가 완료되면 에이전트 VM 재부팅
8. “`spxinfo -l`” 명령을 통해 파일 정책이 올바른지 검증

참고

경로 다음의 별표는 암호화 보류 중인 기존의 데이터가 있음을 표시합니다. 기존의 디렉토리 구조와 데이터에 대한 적절한 암호화를 수행하고 임의의 시점에 데이터의 상태를 판별하기 위해 MDE는 “`spxconvert`”라고 하는 명령행 유틸리티를 제공합니다.

해당 명령과 사용에 관한 자세한 설명은 89 페이지의 『부록 E 적절한 암호화』의 내용을 참조하십시오.

Linux 정책이 적용된 볼륨 에이전트 디바이스 구성

이 태스크 정보

프로시저

1. PPM에서 정책이 적용된 볼륨 에이전트 작성(사용된 디바이스 레이블 기억)
2. 에이전트 VM에 “gettext” 패키지 설치
3. 에이전트 설치 - 세부사항은 77 페이지의 『부록 A 샘플 에이전트 설치 프로세스』의 내용을 참조하십시오.
4. 설치가 완료되면 에이전트 VM 재부팅
5. 루트로서 `spxdevice -e <label given in PPM> -m <mount point> -f <file system> -u <disk to use>` 명령 실행

```
[root@localhost]# spxdevice -e COS6VOL -m /protected -f ext4 -u /dev/sdb
```

- 필수 서브디렉토리 및 사용자 작성
- 디렉토리에서 적절한 권한 설정
- 에이전트 VM 재부팅
- lsblk - 디스크 존재를 검증하는 데 사용되며 종종 최대 30초까지 걸립니다.
- “spxinfo -l” 명령을 통해 파일 정책이 올바른지 검증

참고

Linux에서는 볼륨 암호화가 전체 디바이스 또는 파티션에서 설정될 수 있습니다. 단일 파티션을 사용하려면 spxdevice -u 옵션을 사용할 때 비어 있는 파티션(예: /dev/sdb1)을 지정하기만 하면 됩니다.

Linux 오브젝트 저장소 에이전트 구성

이 태스크 정보

프로시저

- PPM에서 오브젝트 저장소 에이전트 작성
- 에이전트 설치 - 세부사항은 77 페이지의 『부록 A 샘플 에이전트 설치 프로세스』의 내용을 참조하십시오.
- 설치가 완료되면 에이전트 VM 재부팅

AIX용 에이전트 설치

AIX는 단일 에이전트 유형인 정책이 적용된 파일 에이전트를 지원합니다. 에이전트 프로비저닝 중에 지정된 에이전트 유형을 사용하십시오.

AIX 정책이 적용된 파일 에이전트 디바이스 구성

- PPM에서 정책이 적용된 파일 에이전트 작성
- 필수 사용자 작성
- 모든 필수 서브디렉토리 작성
- 디렉토리에서 적절한 권한 설정
- 에이전트 설치 - 세부사항은 77 페이지의 『부록 A 샘플 에이전트 설치 프로세스』의 내용을 참조하십시오.
- 설치가 완료되면 에이전트 VM 재부팅
- “spxinfo -l” 명령을 통해 파일 정책이 올바른지 검증

참고: 경로 다음의 별표는 암호화 보류 중인 기존의 데이터가 있음을 표시합니다. 기존의 디렉토리 구조와 데이터에 대한 적절한 암호화를 수행하고 임의의 시점에 데이터의 상태를 판별하기 위해 MDE는 “spxconvert”라고 하는 명령행 유틸리티를 제공합니다.

해당 명령과 사용에 관한 자세한 설명은 89 페이지의 『부록 E 적절한 암호화』의 내용을 참조하십시오.

Windows용 에이전트 설치

볼륨 에이전트, 정책이 적용된 파일 에이전트 및 정책이 적용된 볼륨 에이전트의 3가지 에이전트 유형이 있습니다. 에이전트 프로비저닝 중에 지정된 에이전트 유형을 사용하십시오.

Windows 볼륨 에이전트 디바이스 구성

이 태스크 정보

프로시저

- PPM에서 볼륨 작성(사용된 디바이스 레이블 기억)
- 에이전트 설치 - 세부사항은 77 페이지의 『부록 A 샘플 에이전트 설치 프로세스』의 내용을 참조하십시오.

3. 설치가 완료되면 에이전트 VM 재부팅

4. “spxdevice -e <label given at PPM> -d <disk number to use>”를 실행하여 전체 디스크에 연결. 관리자로 실행해야 합니다.

```
spxdevice -e PRODISK -d 1
```

5. 또는 “spxdevice -e <label given at PPM> -d <disk number to use> -m <drive letter> -f <file system>”을 실행하여 포맷되고 드라이브 이름으로 마운트될 전체 디스크에 연결

```
spxdevice -e PRODISK -d 1 -m E -f NTFS
```

6. 또는 “spxdevice -i <disk number to use>”를 실행하여 특정 파티션에 연결할 디스크 스테이징

```
spxdevice -i 1
```

7. 그 다음에는 “spxdevice -e <label given at PPM> -v <drive letter> -f <filesystem>”을 실행하여 특정 파티션에 연결하고 파일 시스템에서 해당 파티션 포맷

```
spxdevice -e PRODISK -v E -f NTFS
```

참고: Windows에서는 볼륨 암호화가 전체 디바이스 또는 파티션에서 설정될 수 있습니다.

- 전체 디스크 암호화의 경우, 디스크는 온라인 상태이고 초기화되어야 하며 디스크 공간은 포맷되지 않아야 합니다. 드라이브 이름을 사용할 수 있어야 합니다.
- 파티션 암호화의 경우, 백킹 디바이스는 정리된 디스크에서 “spxdevice -i <disk number>”를 통해 작성되어야 합니다. 그리고 드라이브 이름으로 RAW 파티션을 작성해야 합니다.

추가 옵션은 “spxdevice” 명령의 도움말을 참조하십시오.

Windows 정책이 적용된 파일 에이전트 디바이스 구성

이 태스크 정보

프로시저

1. PPM에서 정책이 적용된 파일 에이전트 작성
2. 필수 사용자 작성
3. 모든 필수 서브디렉토리 작성
4. 디렉토리에서 적절한 권한 설정
5. 에이전트 설치 - 세부사항은 77 페이지의 『부록 A 샘플 에이전트 설치 프로세스』의 내용을 참조하십시오.
6. spxinfo -l 명령을 통해 파일 정책이 올바른지 검증

참고

경로 다음의 별표는 암호화 보류 중인 기존의 데이터가 있음을 표시합니다. 기존의 디렉토리 구조와 데이터에 대한 적절한 암호화를 수행하고 임의의 시점에 데이터의 상태를 판별하기 위해 MDE는 “spxconvert”라고 하는 명령행 유틸리티를 제공합니다.

해당 명령과 사용에 관한 자세한 설명은 89 페이지의 『부록 E 적절한 암호화』의 내용을 참조하십시오.

참고

일단 정책이 검색되면 정책이 적용되므로, Windows에서는 관리자가 정책을 통해 대상 디렉토리를 작성할 권한이 있는지 확인하십시오.

Windows 정책이 적용된 볼륨 에이전트 디바이스 구성

이 태스크 정보

프로시저

1. PPM에서 정책이 적용된 볼륨 에이전트 작성(사용된 디바이스 레이블 기억)
2. 에이전트 설치 - 세부사항은 77 페이지의 『부록 A 샘플 에이전트 설치 프로세스』의 내용을 참조하십시오.
3. 설치가 완료되면 에이전트 VM 재부팅
4. “spxdevice -e <label given at PPM> -d <disk number to use>”를 실행하여 전체 디스크에 연결하십시오. 관리자로 실행해야 합니다.

PS C:\> spxdevice -e PRODISK -d 1

5. 또는 “spxdevice -e <label given at PPM> -d <disk number to use> -m <drive letter> -f <file system>”을 실행하여 포맷되고 드라이브 이름으로 마운트될 전체 디스크에 연결

PS C:\> spxdevice -e PRODISK -d 1 -m E -f NTFS

6. 또는 “spxdevice -I <disk number to use>”를 실행하여 특정 파티션에 연결할 디스크를 스테이징

PS C:\> spxdevice -i 1

7. 다음으로 “spxdevice -e <label given at PPM> -v <drive letter> -f <filesystem>”을 실행하여 특정 파티션에 연결하고 파일 시스템에서 해당 파티션을 포맷하십시오.

PS C:\> spxdevice -e PRODISK -v E -f NTFS

참고

Windows에서는 볼륨 암호화가 전체 디바이스 또는 파티션에서 설정될 수 있습니다.

- 전체 디스크 암호화의 경우, 디스크는 온라인 상태이고 초기화되어야 하며 디스크 공간은 포맷되지 않아야 합니다. 드라이브 이름을 사용할 수 있어야 합니다.
- 파티션 암호화의 경우, 백킹 디바이스는 정리된 디스크에서 “spxdevice -i <disk number>”를 통해 작성되어야 합니다. 그리고 드라이브 이름으로 RAW 파티션을 작성해야 합니다.

추가 옵션은 “spxdevice” 명령의 도움말을 참조하십시오.

8. 볼륨에 보호된 디렉토리 추가
9. 컴퓨터 다시 시작
10. spxinfo -l(모든 보호된 디렉토리 목록이 표시되어야 함)

참고

일단 볼륨이 연결되고 사용 가능하게 되면 정책이 적용되므로, Windows에서는 관리자가 정책을 통해 대상 디렉토리를 작성할 권한이 있는지 확인하십시오.

정책 활성화

각 에이전트에는 하나의 활성 정책만 있을 수 있습니다. 에이전트는 자체 정책을 지속적인 방법으로 저장하지 않습니다. 모든 에이전트 재부팅 시에 에이전트는 MDE에서 현재 활성화된 정책을 요청합니다. 에이전트가 MDE에 액세스할 수 없는 경우, 기본 액세스 거부가 에이전트에서 보호된 모든 디렉토리에 적용됩니다.

새 정책이 에이전트에 전송되면 에이전트는 정책이 성공적으로(또는 성공하지 않게) 적용 시 이벤트를 MDE에 전송합니다. 정책 활성화가 지속되는 경우 다음 위치에 있는 kernel_policy.log 파일을 참조하십시오.

- Linux/AIX: /var/log/spxagent/spx-policyagent
- Windows: C:\Windows\spxagent\PolicyAgent

에이전트 편집

에이전트가 성공적으로 프로비저닝되고 승인된 후에는 "에이전트 정보" 페이지에서 GUI를 통해 에이전트를 편집하여 해당 에이전트를 변경해야 합니다. 에이전트를 편집하려면 에이전트 세부사항을 보십시오. 에이전트의 정보 페이지에서는 에이전트의 섹션을 개별적으로 편집할 수 있습니다.

에이전트 정보 편집

“에이전트 정보 편집” 단추를 클릭하면 일부 에이전트 정보(이름, IP 주소, MDE 피어 IP 및 참고)를 수정할 수 있습니다.

[Edit Agent Info](#)

Agent Info

Identity

Notes

Name	Agent1
UUID	dab30682-19ee-4763-84d8-12fe2ba91948
IP Address	10.6.1.255
Type	Volume with Policy
Operating System	CentOS / Red Hat 7

Network

MDE Peer IP

10.6.1.105

Certificates

Subject	Fingerprint	Expir
CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US	ea584e4904fffa45a3416eccc753e0f0f655462929d4f1534f369cbccc38165f	2016-

[Browse...](#) No file selected.

MDE 피어 IP에 대한 변경은 MDE 내에서 즉시 적용되지만 에이전트가 이미 설치된 경우, 변경 적용 전에 새 설치 패키지가 작성되고 설치되어야 합니다.

참고

UUID, 운영 체제, 에이전트 유형은 초기 프로비저닝 후에는 편집할 수 없습니다.

인증서 추가/삭제

에이전트 인증서는 에이전트 정보 페이지의 인증서 섹션에서 해당 단추를 클릭하여 추가 및 삭제할 수 있습니다.

Network

MDE Peer IP

1.1.1.0

Certificates

Subject	Fingerprint	Expiry	
CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US	ea584e4904fffa45a3416eccc753e0f0f655462929d4f1534f369cbccc38165f	2016-11-15T14:32:08Z	Delete Certificate

[Browse...](#) No file selected.

[Add Certificate](#)

에이전트 인증서를 업데이트하려면 다음 단계를 수행하십시오.

1. 에이전트에 대한 새 인증서를 생성합니다.
2. 관리 콘솔을 통해 새 인증서를 PPM에 업로드합니다.
 - a. 에이전트 페이지에서 업데이트할 에이전트를 클릭하여 에이전트 정보 페이지를 표시합니다.
 - b. "인증서 추가" 단추를 클릭하고, 새 인증서 파일을 선택한 다음, "확인" 단추를 클릭합니다.

- c. 새 인증서가 표시됩니다.
3. 이전 인증서를 삭제합니다.
 - a. 에이전트 페이지에서 업데이트할 에이전트를 클릭하여 에이전트 정보 페이지를 표시합니다.
 - b. 삭제한 인증서를 판별합니다.
 - c. "인증서 삭제" 단추를 클릭합니다. 작업이 생성됩니다.
 - d. "닫기" 단추를 클릭합니다.
 - e. 작업 페이지에서 원하는 작업의 "승인" 단추를 클릭합니다.
4. 에이전트에서 인증서가 삭제되었는지 확인합니다.
 - a. 에이전트 페이지에서 업데이트할 에이전트를 클릭하여 에이전트 정보 페이지를 표시합니다.
 - b. 적절한 인증서가 남아있는지 확인합니다.

에이전트가 이미 설치된 경우, 인증서 변경을 적용하기 전에 새 설치 패키지를 작성하고 설치해야 합니다.

에이전트 도구

이제 에이전트 프로비저닝 중에 구성되지 않은 도구를 에이전트 정보 페이지에서 추가할 수 있습니다. 그리고 구성된 도구를 수정할 수 있습니다.

키 연관

키를 연관시키려면 도구 옆에 있는 텍스트 상자에 키 이름을 입력한 다음 목록에서 해당 키를 선택하십시오. "저장"을 클릭하면 작업이 작성됩니다. 승인되면 구성된 도구를 에이전트에서 사용할 수 있게 됩니다.

키 수정

키를 수정하려면 편집 단추를 클릭하고 도구 옆에 있는 텍스트 상자에 키 이름을 입력한 다음 목록에서 해당 키를 선택하십시오.

"저장"을 클릭하면 작업이 작성됩니다. 승인되면 구성된 도구를 에이전트에서 사용할 수 있게 됩니다.

Tools

SU 데이터 액세스

정책 액세스 제어를 적용할 때 기본 설정은 SU 데이터 액세스를 거부하는 것입니다. SU 데이터 액세스가 허용되는 시나리오가 있을 수 있습니다. 이 경우 에이전트 정보 페이지에서 설정을 수정할 수 있는 확인란이 있습니다.

Other Configuration

☒ Block access when su user substitution is in use

확인란을 전환하면 작업이 생성됩니다. 승인되면 SU 데이터 액세스 설정이 그에 따라 변경됩니다.

다음 표에서는 SU 데이터 액세스 제어를 보여줍니다.

에이전트 유형	운영 체제	SU 데이터 액세스 기본값	SU 데이터 액세스 구성 가능
볼륨	CentOS6/RedHat6	해당사항 없음	해당사항 없음
볼륨	CentOS7/RedHat7	해당사항 없음	해당사항 없음
볼륨	Windows	해당사항 없음	해당사항 없음
정책이 적용된 볼륨	CentOS6/RedHat6	차단됨	예
정책이 적용된 볼륨	CentOS7/RedHat7	차단됨	예
정책이 적용된 볼륨	Windows	해당사항 없음	해당사항 없음
정책이 적용된 파일	CentOS6/RedHat6	차단됨	예
정책이 적용된 파일	CentOS7/RedHat7	차단됨	예
정책이 적용된 파일	AIX	차단됨	예
정책이 적용된 파일	Windows	해당사항 없음	해당사항 없음
오브젝트 저장소	CentOS7/RedHat7	해당사항 없음	해당사항 없음

정책 일시중단

정책이 적용된 볼륨 에이전트 및 정책이 적용된 파일 에이전트는 정의된 활성 정책을 일시중단하는 기능을 지원합니다. 정책이 일시 중단되면 보호된 디렉토리에 대한 모든 조치가 거부됩니다. 활성 정책 일시중단은 활성 스냅샷 정의를 변경하지 않고 수행할 수 있습니다.

정책을 일시중단하려면 에이전트 정보 정책 섹션의 오른쪽 모서리에 있는 "활성 정책 일시중단" 단추를 클릭하십시오. 이렇게 하면 작업이 작성됩니다.

Suspend Active Policy Edit Master Policy Manage Snapshots

작업이 일시중단되면 정책이 즉시 일시중단되고 단추가 전환되어 "활성 정책 사용 재설정"을 표시합니다.

일시중단된 정책을 다시 사용하려면 "활성 정책 사용 재설정" 단추를 클릭하십시오. 작업이 작성됩니다. 작업을 승인한 후 마지막 활성 스냅샷 정책이 즉시 적용됩니다.

정책 변경

보호된 경로에 적용된 정책 수정, 새 보호된 경로 추가 또는 암호화된 볼륨 추가를 수행하여 정책을 변경할 수 있습니다.

정책을 변경해도 현재 데이터의 암호화 상태는 수정되지 않습니다. 이는 정책이 재배포된 후 작성되는 데이터 처리에만 영향을 줍니다.

중요 참고

활성 에이전트에서 볼륨 정책을 삭제하지 마십시오. 이 작업은 지원되지 않으며 대상 시스템이 불안정한 상태에 놓일 수 있습니다.

활성 에이전트에서 새 볼륨을 작성하고 이전 볼륨을 사용되지 않도록 둘 수 있습니다.

또는 새 에이전트를 작성하고 이를 배치할 수도 있습니다.

정책 편집

에이전트의 정책을 편집하면 파일 정책 경로, 경로 세트 및 데이터 유형 연관 또는 암호화된 볼륨을 수정할 수 있습니다.

데이터 유형을 편집 가능한 데이터 유형으로 변경하면 해당 필드에 대한 인라인 편집이 사용 가능합니다. 정책을 편집하려면 “마스터 정책 편집” 단추를 클릭하십시오.

Active Policy

[Edit Master Policy](#) [Manage Snapshots](#)

File Policy Path		Pathset1
Datatype	Datatype1	
Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Protected Volumes

Volume Policy Path	
Device Label	volume
Key	Key1

그림 1. 정책이 적용된 볼륨 에이전트 예제

그러면 마스터 정책 편집 페이지가 시작됩니다.

Edit Master Policy

File Policy Path (or Path Set)

Pathset1

☐ Autogenerate Key

Datatype

Datatype1

(remember to fill out any empty values below)

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Volume Policy Path

Device Label

volume

Key

Key1

☐ Autogenerate Key

Add Volume

Add Path

Save

Save and Snapshot

Save, Snapshot and Activate

Cancel

참고

마스터 정책을 편집해도 스냅샷은 수정되지 않습니다.

.

경로 추가

이 태스크 정보

정책 밑에 배치하려는 새 경로를 추가하려면 "경로 추가" 단추를 클릭하십시오.

Edit Master Policy

File Policy Path (or Path Set) **Pathset1**

☐ Autogenerate Key

Datatype


(remember to fill out any empty values below)

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Volume Policy Path

Device Label

Key ☐ Autogenerate Key



그러면 정책 입력에 대한 새 섹션이 열립니다(원래 프로비저닝과 유사).

File Policy Path (or Path Set) **Required**

☐ Autogenerate Key

Datatype **Required**

(remember to fill out any empty values below)

Selector	Operation	Actions
----------	-----------	---------

볼륨 추가

이 태스크 정보

암호화하려는 새 볼륨을 추가하려면 "볼륨 추가" 단추를 클릭하십시오.

Edit Master Policy

File Policy Path (or Path Set)

Pathset1

☐ Autogenerate Key

Datatype

Datatype1

(remember to fill out any empty values below)

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Volume Policy Path

Device Label

volume

Key

Key1

☐ Autogenerate Key

Add Volume

Add Path

그러면 입력을 위한 새 섹션이 열립니다(원래 프로비저닝과 유사).

Volume Policy Path

Delete

Device Label

Required

Key

☐ Autogenerate Key Required

Add Volume

Add Path

Save

Save and Snapshot

Save, Snapshot and Activate

Cancel

경로 삭제

이 태스크 정보

정책 보호에서 경로를 삭제하려면 원하는 경로에 대해 "삭제" 단추를 클릭하십시오. 일단 정책 구성의 저장, 스냅샷 찍기 및 활성화가 수행된 경우, 해당 경로는 액세스 제어 정책으로 더 이상 보호되지 않습니다. 디렉토리에 쓰여진 새 파일은 더 이상 암호화되지 않습니다. 기본 파일은 암호화된 상태를 유지하며 액세스 가능하지 않습니다.

참고: 데이터에 연속 액세스하려면 정책에서 경로를 삭제하기 전에 보호된 디렉토리에서 데이터를 복사/이동하십시오.

Edit Master Policy

File Policy Path (or Path Set) **Pathset1** Delete

☐ Autogenerate Key

Datatype

(remember to fill out any empty values below)

Selector	Operation	Actions
selector1	Read or Write	Permit

Volume Policy Path

Device Label

Key ☐ Autogenerate Key

Add Volume Add Path

Save Save and Snapshot Save, Snapshot and Activate Cancel

에이전트 스냅샷

에이전트 스냅샷은 정책 구성에 연관되는 에이전트의 영구적인 스토리지입니다. 스냅샷은 인덱스화되며 활성 또는 비활성 상태입니다. 에이전트별로 활성 스냅샷은 하나입니다. 이는 현재 에이전트에 적용되는 정책 구성입니다. 에이전트 정책 구성을 수정하려면 관리자는 원하는 변경을 반영하는 스냅샷을 새로 작성하고 새 스냅샷을 활성화해야 합니다.

에이전트 편집 및 스냅샷 저장

에이전트 정책 편집 완료 시에는 변경사항 취소, 변경사항 저장, 변경사항 저장 후 스냅샷 작성 또는 변경사항 저장 후 스냅샷 작성 및 이를 활성화할 수 있습니다.

Save Save and Snapshot Save, Snapshot and Activate Cancel

변경 취소

변경을 취소하면 수정 전에 있던 정책 구성으로 복귀됩니다.

변경사항 저장

변경사항을 저장하면 나중에 사용할 수 있도록 저장되지만 스냅샷은 작성되지 않기 때문에 변경사항은 에이전트에 적용할 수 없습니다.

저장 및 스냅샷

변경사항을 저장 및 스냅샷으로 작성하면 나중에 사용할 수 있도록 저장되고 나중에 보고 활성화할 수 있는 스냅샷이 작성됩니다.

저장, 스냅샷, 활성화

변경사항의 저장, 스냅샷 찍기 및 활성화를 수행하면 나중에 사용할 수 있도록 변경사항이 저장되고 볼 수 있는 스냅샷이 작성되며 해당 변경사항을 에이전트에 적용하는 작업이 즉시 작성됩니다.

참고: 에이전트가 PPM 서버와 통신할 수 있어야 스냅샷 변경 또는 업데이트가 적용됩니다. 생성된 작업은 PPM 과 에이전트 사이의 통신이 성공하거나 에이전트가 PPM 서버에서 제거될 때까지 계속 실행됩니다.

스냅샷 관리

에이전트와 연관된 모든 스냅샷은 에이전트 정보 보기의 "스냅샷 관리" 단추를 사용하여 볼 수 있습니다.

Active Policy

[Edit Master Policy](#) [Manage Snapshots](#)

File Policy Path	Pathset1	
Datatype	Datatype1	
Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

단추를 클릭하면 스냅샷 관리 대화 상자가 표시됩니다. 여기에서 보안 관리자는 스냅샷 세부사항을 보고 스냅샷을 활성화하며 스냅샷과 연관된 정책을 비활성화하고 스냅샷을 삭제할 수 있습니다.

Agent Snapshots

ID	State	Actions
1	Inactive	Activate Delete View Details
2	Active	Deactivate Policy View Details

[OK](#)

참고

활성 스냅샷을 변경해도 마스터 정책은 수정되지 않습니다.

세부사항 보기

이 단추는 스냅샷과 연관된 정책에 대한 요약 보기를 표시합니다.

Snapshot Detail

Notes

Protection Policy

File Policy Path /protected2

Datatype Datatype1

Selector	Operation	Key	Actions
<div>Back</div> <div>OK</div>			

스냅샷 활성화

스냅샷을 활성화하면 정책을 에이전트로 전송하는 작업이 작성됩니다. 승인되면, 스냅샷은 활성 상태로 변경되고 해당 정책은 에이전트에 있는 모든 정책을 겹쳐줍니다.

참고: 에이전트가 PPM 서버와 통신할 수 있어야 스냅샷 변경 또는 업데이트가 적용됩니다. 생성된 작업은 PPM과 에이전트 사이의 통신이 성공하거나 에이전트가 PPM 서버에서 제거될 때까지 계속 실행됩니다.

스냅샷 삭제

비활성 스냅샷은 삭제됩니다. 스냅샷을 삭제하면 MDE에서 이를 영구적으로 제거합니다.

파일 에이전트 설치 제거

이 태스크 정보

파일 에이전트를 제거하려는 경우, 이는 다음 단계를 통해 수행될 수 있습니다.

보호된 디렉토리에서 데이터를 복사하십시오. 그러면 정책 비활성화 이후에도 데이터가 액세스 불가능하지 않습니다.

다음 단계를 수행하여 에이전트 소프트웨어를 제거하십시오.

프로시저**1. Linux – 루트로 실행****a) spx-policyagent 서비스 중지**

- CentOS 7을 사용하여 실행

```
systemctl stop spx-policyagent
```

- CentOS 6을 사용하여 실행

```
service spx-policyagent stop
```

b) cd /opt/ibm/mde/spxagent/spx-fileagent/를 실행하십시오.**c) ./fileagent_uninstall.sh를 실행하십시오.****d) y를 입력하여 폐기 조치를 승인하십시오.**

- e) 재부팅하십시오.
- 2. AIX - 루트로 실행하십시오.
 - a) spx-policyagent 서비스를 중지하십시오.

```
stopsrc -s spx-policyagent
```

- b) 커널 모듈을 중지하십시오.

```
/opt/ibm/mde/spxagent/spx-fileagent/module/spx_kctrl_stop
```

- c) RPM을 제거하십시오.

```
rpm -e fileagent*
```

참고: 와일드카드 실행이 아니라 정확한 rpm 이름을 원하는 경우 다음을 사용하십시오.

```
rpm -qa | grep fileagent
```

- d) 재부팅하십시오.

- 3. Windows – 관리자로 실행하십시오.

- Windows GUI를 통해
 - 제어판의 프로그램 추가/제거로 이동
 - 설치 제거할 “FileAgent” 선택
 - 프롬프트가 표시되면 시스템 재부팅
- PowerShell CLI를 통해
 - msixexec /x <path to FileAgent.msi>
 - 프롬프트가 표시되면 시스템 재부팅

중요사항: 권한 부여된 사용자는 암호화된 위치와의 양방향 데이터 이동에 mv(이동) 명령을 사용하지 않아야 합니다. MDE 정책에서 문제가 발생할 수 있기 때문입니다.

우선 보호된(암호화된) 디렉토리 및 양방향으로 cp(복사) 명령을 사용하여 데이터를 백업하십시오.

볼륨 에이전트 설치 제거

볼륨 에이전트 설치 제거

- Linux – 루트로 실행합니다.

- 1. 보호된 볼륨의 마운트 해제

```
umount /dev/mapper/<e_volume>
```

- 2. spx-policyagent 서비스 중지

- CentOS 7을 사용하여 실행

```
systemctl stop spx-policyagent
```

- CentOS 6을 사용하여 실행

```
service spx-policyagent stop
```

- 3. cd /opt/ibm/mde/spxagent/spx-volumeagent/를 실행하십시오.

- 4. ./volumeagent_uninstall.sh를 실행하십시오.

- 5. y를 입력하여 폐기 조치를 승인하십시오.

6. Reboot

- Windows – 관리자로 실행
 - Windows GUI를 통해
 - 제어판의 프로그램 추가/제거로 이동
 - 설치 제거할 “VolumeAgent” 선택
 - 프롬프트가 표시되면 시스템 재부팅
 - PowerShell CLI를 통해
 - `msiexec/x <path to VolumeAgent.msi>`
 - 프롬프트가 표시되면 시스템 재부팅

정책이 적용된 볼륨 에이전트 설치 제거

이 태스크 정보

프로시저

1. Linux – 루트로 실행

a) 보호된 디렉토리의 마운트 해제

```
umount /dev/mapper/<e_volume>
```

b) spx-policyagent 서비스 중지

- CentOS 7을 사용하여 실행

```
systemctl stop spx-policyagent
```

- CentOS 6을 사용하여 실행

```
service spx-policyagent stop
```

c) `cd /opt/ibm/mde/spxagent/spx-hybridagent/`를 실행하십시오.

d) `./hybridagent_uninstall.sh`를 실행하십시오.

e) y를 입력하여 폐기 조치를 승인하십시오.

f) 재부팅하십시오.

2. Windows – 관리자로 실행

- Windows GUI를 통해
 - 제어판의 프로그램 추가/제거로 이동하십시오.
 - 설치 제거할 “HybridAgent”를 선택하십시오.
 - 프롬프트가 표시되면 시스템을 재부팅하십시오.
- PowerShell CLI를 통해
 - `msiexec /x <path to HybridAgent/msi>`를 실행하십시오.
 - 프롬프트가 표시되면 시스템을 재부팅하십시오.

오브젝트 저장소 에이전트 설치 제거

이 태스크 정보

모든 사용자 계정 및 권한은 에이전트가 PPM에서 삭제될 때까지 PPM에 저장되어 있습니다.

프로시저

1. Linux – 루트로 실행
2. spx-policyagent 서비스 중지

```
systemctl stop spx
```

3. **cd** /opt/ibm/mde/spxagent/spx-objectagent

```
./objectagent_uninstall.sh
```

4. "y"를 입력하여 폐기 조치 인지
5. 재부팅하십시오.

MDE에서 에이전트 제거

MDE에 의해 관리되는 에이전트는 MDE 사용자 인터페이스(GUI)를 사용하여 에코시스템에서 삭제될 수 있습니다.

에이전트를 제거하려면 "에이전트 삭제" 단추를 클릭하십시오. 그러면 작업이 작성됩니다. 작업이 승인되면 MDE에서 에이전트가 제거됩니다.

Name	Hostname or IP	Type	Notes	Actions
Agent1	1.1.1.1	Volume with Policy		Details Delete Agent

중요 참고

- MDE에서 에이전트를 제거하면 에이전트가 MDE에 연결할 수 없게 되기 때문에 다음에 에이전트를 다시 시작할 때 현재 보호 중인 데이터에 액세스할 수 없게 됩니다.
- 에이전트를 제거해도 데이터가 복호화되지 않습니다.

에이전트 유틸리티

MDE 에이전트에서 에이전트의 구성 및 중요한 정보의 보호를 지원하기 위해 여러 유틸리티를 제공합니다. 각각에 관한 자세한 정보는 "--help" 옵션으로 유틸리티를 실행하십시오.

유틸리티	기능	볼륨	정책이 적용된 볼륨	정책이 적용된 파일	오브젝트 저장소
spxbackup	식별된 데이터의 암호화된 백업을 작성합니다.	예	예	예	아니오
spxconvert	보호된 디렉토리에 있는 기존 데이터를 정의된 정책을 기반으로 암호화 해제됨에서 암호화됨으로 변환합니다.	아니오	아니오	예	아니오
spxdevice	디스크 볼륨/파티션을 정의된 디바이스 이름에 매핑합니다.	예	예	아니오	아니오

spxhash	표시된 프로세스의 버전별 해시를 생성합니다.	아니오	예	예	아니오
spximport	데이터를 이중 암호화하지 않고 암호화된 데이터를 디렉토리에 가져옵니다.	아니오	아니오	예 (Windows만 해당)	아니오
spxinfo	정의된 정책을 통해 보호한 디렉토리 나열	아니오	예	예	아니오
spxobject	오브젝트 저장소 나열	아니오	아니오	아니오	예
spxrestore	식별된 데이터의 암호화된 백업을 복원합니다.	예	예	예	아니오

제 12 장 조작

제품 데이터 백업 및 복원

MDE는 MDE PPM 데이터에 대한 특정 시점 백업을 수행하는 기능을 지원합니다. 이 특정 시점 백업은 MDE를 백업 콜렉션 시점의 상태로 되돌리기 위해 복원 가능합니다.

참고: 백업 또는 복원을 수행하기 전에 MDE VM에서 "systemctl stop spsd" 명령을 통해 MDE 서비스를 중지하십시오.

```
sudo systemctl stop spsd
```

제품 데이터 백업

이 태스크 정보

제품 백업은 MDE VM 내에서 실행되는 명령행 스크립트를 통해 수행됩니다.

백업 스크립트 spsd-backup은 MDE VM의 /opt/securityfirst/spsd/bin 디렉토리에 있습니다. 이는 자동으로 새 파일을 작성하고 이 백업이 작성된 시점의 시간소인으로 해당 이름을 지정합니다.

```
sudo /opt/securityfirst/spsd/bin/spsd-backup --help
사용법: spsd-backup [--nodb] [--help]-----
--nodb
데이터베이스 백업 안함      --help
이 도움말 표시
```

백업 실행:

```
sudo /opt/securityfirst/spsd/bin/spsd-backup
로컬 buildinfo 덤프로컬 spsd 특성 덤프로컬 PostgreSQL 데이터베이스 덤프완료 - 작성된 spsd-
backup-2017-04-04T144448-0700.tar.gz
```

제품 데이터 복원

이 태스크 정보

제품 복원은 MDE VM 내에서 실행되는 명령행 스크립트를 통해 수행됩니다.

복원 스크립트 spsd-restore는 /opt/securityfirst/spsd/bin 디렉토리에 있습니다.

```
sudo /opt/securityfirst/spsd/bin/spsd-restore --help
사용법: spsd-restore [--nodb] [--noprops] [--help] FILE-----
--nodb 데이터베이스에 쓰기 안함      --noprops 로컬 특성 작성 안함      --help
이 도움말 표시
```

복원 실행:

```
sudo /opt/securityfirst/spsd/bin/spsd-restore
spsd-backup-2017-04-04T144448-0700.tar.gz
```

참고: 백업 파일이 복원된 후에 MDE를 다시 시작하면 변경사항이 적용됩니다.

커널 업데이트

이 태스크 정보

Red Hat Enterprise Linux 7 또는 CentOS 7 운영 체제를 실행하는 에이전트에서 커널 업데이트가 필요한 경우 다음 지침을 따르십시오.

- OS/커널 업데이트가 동일한 릴리스 내에 있으면 새로운 커널이 자동으로 지원됩니다.
- OS/커널을 상위 버전(예: RHEL 7.2 -> 7.4)으로 업그레이드하는 경우 다음 단계를 실행하여 새 커널에 대한 지원을 구축하십시오.
 - 예: 에이전트 설치 번들이 /root/agent에 tar 압축 해제되었습니다.

```
cd /root/agent/spx-installer
./agent_setup.sh -d /root/agent
Reboot
```

Red Hat Enterprise Linux 6 또는 CentOS 6에서 실행되는 에이전트에는 이 단계가 필요하지 않습니다.

업그레이드

새 버전으로 MDE 제품을 업그레이드하려면 다음 단계를 수행하십시오.

참고: 이 단계는 MDE Open Virtualization Appliance에 적용됩니다. 비OVA 설치를 수행한 경우 디렉토리가 변경될 수 있습니다.

MDE 서버의 경우

이 태스크 정보

프로시저

1. 루트로서 PPM 정책 서비스를 중지하십시오.

```
systemctl stop spsd
```

2. MDE 데이터 백업:

```
/opt/securityfirst/spsd/bin/spsd-backup
```

3. 새 버전 MDE 바이너리 파일을 /home/admin 디렉토리로 이동하십시오.
4. 기존 rpms 디렉토리를 삭제하십시오.

```
rm -fr /home/admin/rpms
```

5. MDE 바이너리 파일에 대한 액세스 권한을 변경하십시오.

```
chmod +x /home/admin/ibm_sw_mde_X.x.x-XX.bin
```

6. 새 버전의 MDE 바이너리 파일을 실행하십시오.

```
/home/admin/ibm_sw_mde_X.x.x-XX.bin
```

7. RPM을 설치하십시오.

```
yum -y install /home/admin/rpms/*
```

8. 업그레이드 스크립트를 실행하십시오.

```
/opt/securityfirst/spsd/bin/spsd-pgsetup --upgrade
```

9. PPM 정책 서비스 백업 다시 시작:

```
systemctl start spsd
```


이전 버전에서 업그레이드

이 태스크 정보

정책이 작동하려면 다음 단계를 수행해야 합니다.

프로시저

1. 에이전트 정보 페이지로 이동
2. “마스터 정책 편집” 클릭
3. “저장, 스냅샷 찍기 및 활성화” 클릭
4. 작업 승인
5. 에이전트 VM으로 돌아가서 해당 디렉토리에 대한 권한이 있는 정책의 사용자로서 로그인하여 정책의 디렉토리에 대한 읽기/쓰기 조치의 수행을 시도한 후에 정의되지 않은 사용자가 허용되지 않음을 확인

에이전트 대상 VM의 경우

Linux/AIX 에이전트

이 태스크 정보

프로시저

1. 새 에이전트 디렉토리를 작성하고 새 에이전트 디렉토리로 변경

```
mkdir [agent_new_directory]
cd [agent_new_directory]
```

2. 개별적인 에이전트의 설치 번들을 다운로드하거나 "curl down" 실행

```
curl --header "Accept: application/x-tar" -u
username:password
https://<PPM IP address>/rest/agents/Agent ID #/install_bundle> install_bundle_name.tar
```

3. 설치 번들의 tar 압축 해제

```
tar xvf <install_bundle_name>.tar
```

4. setup.sh 스크립트를 실행하여 에이전트 재설치

```
./setup.sh
```

5. 에이전트 재부팅 프롬프트가 표시되면 예로 응답하십시오.
6. 원하는 경우, 이전 에이전트 디렉토리에서 이전 설치 프로그램 파일을 모두 삭제할 수 있습니다.

```
rm -rf [/previous Agent directory]
```

Windows 에이전트

이 태스크 정보

프로시저

1. 개별 에이전트의 설치 번들 다운로드
2. 설치 번들을 tar 압축 해제
3. .msi 설치 프로그램을 실행하여 새 에이전트 소프트웨어 설치
4. 에이전트 재부팅 프롬프트가 표시되면 "예"로 응답

서비스 데이터

서비스 데이터 수집

서비스 데이터 수집은 MDE VM 내에서 스크립트 실행을 통해 수행됩니다.

spsd-backup 스크립트는 MDE VM의 /opt/securityfirst/spsd/bin 디렉토리에 있습니다.

```
sudo /opt/securityfirst/spsd/bin/spsd-service --help
사용법:
spsd-service [OPTIONS]-----
  옵션:      --nodb 데이터베이스를
  덤프 안함   --norestore REST API에서 데이터를
  가져오기 안함 --nosys 시스템 데이터 가져오기 안함(/var/log,
  /proc 등)   --withcore spsd의 코어 덤프에서 가져오기   --help
이 도움말 표시
```

서비스 데이터 수집 실행:

```
sudo /opt/securityfirst/spsd/bin/spsd-service
```

PPM 로그에서 민감한 정보 제거

서비스 데이터가 PPM 논리적 경계를 벗어날 때 PPM 설치의 개인정보를 보호할 수 있도록 지원하기 위해 다음 MDE 디버그 로그에는 특수 태그 구문을 사용하여 태그 지정된 민감한 정보가 있습니다.

- bundleAll.log
- bundleWarnPlus.log
- debug.log
- warn.log

참고: 서비스 데이터 타르볼(위의 서비스 데이터 수집 프로세스 결과) 내부에서 이러한 로그는 로그 폴더에 있습니다.

태그 형식은 #<tagname>(<tagdata>)로 지정됩니다. 여기서 <tagdata>는 태그 지정될 데이터로 대체되고 <tagname>은 다음 중 하나입니다.

- user - MDE 사용자인 MDE가 통합된 외부 서비스 사용자인 상관없이 사용자 이름에 태그를 지정합니다. 예: #user(admin)
- group - 그룹 이름에 태그를 지정합니다. 예: #group(domainusers)
- email - 이메일 주소에 태그를 지정합니다. 예: #email(example@example.com)
- ip - IP 주소에 태그를 지정합니다. 예: #ip(192.168.0.5)
- host - 네트워크 호스트 이름에 태그를 지정합니다. 예: #host(dns.example.com)
- key - 공개 암호화 키 또는 관리되는 키 이름 같은 관련된 값에 태그를 지정합니다. 예: #key(HRKey2)
- cert - 연결 에이전트의 구별 이름과 같은 인증서 데이터에 태그를 지정합니다. 예: #cert(C=US, ST=UT, L=Provo, O=Example Corp., OU=architecture, CN=docserver4)
- 지문 - 인증서 지문에 태그를 지정합니다. 예: #fingerprint(41:1A:B9:89:DB:77:90:77:39:D0:DF:5E:98:90:B7:17)

bundleAll.log에서 #user 태그가 지정된 데이터를 제거하는 이 예제에서처럼 프로세스를 사용하여 서비스 데이터에서 태그를 제거할 수 있습니다.

```
gunzip spsd-service-2018-01-24T141620-0800.tar.gz
tar xf spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
sed -i '/\#user/c\REDACTED' logs/bundleAll.log
tar --delete --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
tar --append --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
gzip spsd-service-2018-01-24T141620-0800.tar
```

부록 A 샘플 에이전트 설치 프로세스

다음 절에서는 에이전트 설치 번들 설치를 위한 일반적인 프로세스에 대해 설명합니다. 이는 단순히 예제 방법으로 설치 지시에서는 지원되지 않습니다.

Red Hat / CentOS 프로세스

이 태스크 정보

CURL을 통해 설치 번들 전송:

프로시저

1. 대상 시스템에 로그인
2. MDE 서버와의 유효한 네트워크 연결 확인
3. 정책에서 식별되는 모든 사용자, 그룹 및 경로 또는 디바이스가 작성되어 시스템에 접속 및 구성되었는지 확인
4. MDE에 로그인
5. MDE 내에서 대상 시스템에 대해 에이전트 프로비저닝
6. MDE 내에서 에이전트 세부사항 확인 및 다운로드 URL 기록

Users

Authorized Users admin

Install Files Download URL/rest/agents/1/install_bundle

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. 대상 시스템에서 에이전트 다운로드용 디렉토리를 작성하고 해당 디렉토리로 변경
8. 다음의 curl 명령을 사용하여 tar 번들 다운로드:

```
[user@localhost]$ curl -k --header "Accept: application/x-tar" -u admin:admin https://<PPM IP>/<Download URL> > package.tar
```

PPM 정의 사용자 사용 예제:

```
[user@localhost]$ curl -k --header "Accept: application/x-tar" -u admin:admin-password https://1.1.1.10/rest/agents/1/install_bundle > package.tar
```

PPM LDAP 정의 사용자 사용 예제:

```
[user@localhost]$ curl -k --header "X-Directory: tenant1" --header "Accept: application/x-tar" -u john:secret https://1.1.1.10/rest/agents/1/install_bundle > package.tar
```

(디렉토리 ID는 "tenant1", 사용자는 "john" 및 비밀번호는 "secret"라고 가정)

9. 대상 시스템에서 패키지를 tar 압축 해제:

```
[user@localhost]$ tar -xf package.tar
```

10. 대상 시스템에서 루트로 설치 스크립트 실행

```
[user@localhost]$ ./setup.sh
```

11. 설치 스크립트가 완료되면 에이전트가 설치되고 정책은 MDE에서 다운로드되며 적용됩니다.

AIX 프로세스

이 태스크 정보

설치 번들 전송:

1. 대상 시스템에 로그인
2. MDE 서버와의 유효한 네트워크 연결 확인
3. 정책에서 식별되는 모든 사용자, 그룹 및 경로 또는 디바이스가 작성되어 시스템에 접속 및 구성되었는지 확인
4. MDE에 로그인
5. MDE 내에서 대상 시스템에 대해 에이전트 프로비저닝
6. MDE 내에서 에이전트 세부사항 확인 및 다운로드 URL 기록

Users

Authorized Users admin

Install Files Download URL/rest/agents/1/install_bundle

Download Zip Bundle

Download Tar Bundle

7. 대상 시스템에서 에이전트 다운로드용 디렉토리를 작성하고 해당 디렉토리로 변경
8. 대상 시스템에 번들 전송
9. 대상 시스템에서 패키지를 tar 압축 해제:

```
[user@localhost]$ tar -xf package.tar
```

10. 대상 시스템에서 루트로 설치 스크립트 실행.

```
[user@localhost]$ ./setup.sh
```

11. 설치 스크립트가 완료되면 에이전트가 설치되고 정책은 MDE에서 다운로드되며 적용됩니다.

Windows 서버 프로세스

이 태스크 정보

설치 번들 전송:

프로시저

1. 대상 시스템에 로그인
2. MDE 서버와의 유효한 네트워크 연결 확인
3. 정책에서 식별되는 모든 사용자, 그룹 및 경로 또는 디바이스가 작성되어 시스템에 접속 및 구성되었는지 확인
4. MDE에 로그인
5. MDE 내에서 대상 시스템에 대해 에이전트 프로비저닝
6. MDE 내에서 에이전트 세부사항 확인 및 다운로드 URL 기록

Users

Authorized Users admin

Install Files Download URL /rest/agents/1/install_bundle

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. "Zip 번들 다운로드"를 클릭하여 에이전트 소프트웨어에 대한 zip 파일 번들을 로컬 시스템으로 다운로드
8. 대상 시스템에 설치 번들 전송
9. 대상 시스템에서 zip 파일 번들 콘텐츠 추출
10. 설치 번들의 msi 파일 실행

FileAgent-<version>.msi

예제:

PS C:\> FileAgent-4.2.11-0030.msi

11. 설치 스크립트가 완료되고 에이전트가 올바르게 설치되면 정책이 적용됩니다.

참고: 재부팅해야 합니다. 요청된 재부팅 프롬프트를 무시하려면 재부팅 안함 옵션을 지정하여 명령을 실행하십시오. **msiexec /i <agent_filename_version.msi> NO_REBOOT_PROMPT=1**

부록 B 샘플 인증 기관(CA) 인증서

이 태스크 정보

MDE에서는 인증 기관이 서명한 인증서가 관리 서버(PPM)와 에이전트 간에 보안 세션을 확립하도록 요구합니다. 이에에는 다음이 필요합니다.

- 키 저장소
- 신뢰 저장소
- CA 인증서 번들

내부 회사 RSA 기반 인증 기관이나 써드파티 인증 기관을 사용하여 인증서에 서명할 수 있습니다. 아래의 Linux 예제에서는 다음 항목이 작성됩니다.

- 인증서 서명 요청(CSR)이 작성되고 서명을 위해 인증 기관에 전송됩니다. 서명된 인증서와 키가 결합되어 키 저장소가 작성됩니다.
- 신뢰 저장소는 인증 기관의 인증서 번들을 사용하여 작성됩니다.
- 에이전트 인증서가 작성되었습니다. 이 인증서는 PPM 및 에이전트 간의 통신에 필요합니다.

이 예제는 사용자의 편의를 위해 제공되며, 서명되는 인증서를 생성할 때는 해당 인증 기관에 따라야 합니다. 대괄호 [name.pem] 내의 이름은 회사 또는 써드파티 인증서를 사용할 때 상이하거나 변경될 수 있는 파일 이름을 표시합니다.

키 저장소를 작성하려면 CSR을 내부 회사 인증 기관 또는 써드파티 인증 기관에 제출해야 합니다.

프로시저

1. 다음 정보를 포함하는 OpenSSL 구성 파일(즉, ppm.cnf)을 작성하십시오.

```
[req]
default_bits          = 4096
distinguished_name     = req_distinguished_name
req_extensions        = v3_req
prompt                = no

[req_distinguished_name]
C           = your_country
ST          = your_state_or_province
L           = your_locale_(city)
O           = your_organization
OU          = your_org_unit_(department)
CN          = your_ppm_host.your_domain

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints      = CA:FALSE
extendedKeyUsage      = serverAuth
subjectAltName        = @alt_names

[alt_names]
DNS.1              = your_ppm_host.your_domain
IP.1               = your_ppm_ip_address
```

조직의 정보를 반영하도록 [req_distinguished_name] 및 [alt_names] 섹션을 업데이트해야 합니다.

2. PPM CSR을 작성하십시오.

```
openssl req -out [csr.pem] -new -newkey rsa:2048 -keyout [key.pem] -outform pem
```

3. CSR [csr.pem]을 인증 기관(CA)에서 서명해야 합니다.
4. CA로부터 서명된 인증서가 수신되면 확장 키 사용 및 제목 대체 이름이 있는지 확인하십시오.

```
openssl x509 -in [signed cert] -noout -text
```

5. 서명된 인증서와 키(2단계의 키)를 결합하십시오.

```
a. openssl pkcs12 -export -out [ppm.p12] -inkey [key.pem] -in [signed-cert] -name ppm
b. keytool -importkeystore -srckeystore [ppm.p12] -keystore [ppm.jks] -storetype JKS
```

신뢰 저장소를 작성하려면 CSR 서명에 사용되는 인증 기관의 인증서가 필요합니다. 이를 CA 인증서 번들이라고도 합니다. 아래의 “ca_bundle.crt”를 이 인증서의 실제 이름으로 대체하십시오.

- a. 인증 기관(CA) 인증서 번들을 사용하여 신뢰 저장소를 작성하십시오. CA 인증서 번들에 다중 인증서가 있는 경우 각 인증서를 분리하여 개별적으로 신뢰 저장소에 가져와야 합니다.

```
a. keytool -import -trustcacerts -file [ca_bundle-1.crt] -alias CA1 -keystore [trust.jks]
b. keytool -import -trustcacerts -file [ca_buncle-2.crt] -alias CA2 -keystore [trust.jks]
c. continue for each certificate in bundle
```

- b. 최종 *.jks 및 [ca_bundle.crt] 파일을 보안 디렉토리(예: /etc/ppm/certs)의 PPM 서버에 복사하십시오. 이 위치는 spsd-certsetup 스크립트를 사용하여 웹과 에이전트 특성 파일을 업데이트할 때 지정됩니다. (아래의 관리 서버 설정 참조)

MDE 에이전트 인증서도 필수입니다.

- a. 다음 정보를 포함하는 OpenSSL 구성 파일(즉, host01.cnf)을 작성하십시오.

```
[req]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no

[req_distinguished_name]
C = your_country
ST = your_state_or_province
L = your_locale_(city)
O = your_organization
OU = your_org_unit_(department)
CN = your_agent_host.your_domain

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
extendedKeyUsage = clientAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = your_agent_host.your_domain
IP.1 = your_agent_ip_address
```

조직의 정보를 반영하도록 [req_distinguished_names] 및 [alt_names] 섹션을 업데이트해야 합니다.

- b. MDE 에이전트 CSR을 작성하십시오.

```
a. openssl req -out [host01.csr] -nodes -sha256 -newkey rsa:2048 -keyout [host01.key] -config [host01.cnf]
```

- c. 인증 기관(CA)이 서명한 CSR을 요청하십시오.

- d. CA로부터 서명된 인증서가 수신되면 확장 키 사용 및 제목 대체 이름이 있는지 확인하십시오.

```
a. openssl x509 -in [signed-agent] -noout -text
```

- e. 에이전트 인증서가 PPM 인증서와 다른 CA에 의해 서명된 경우 CA_bundle 인증서를 PPM 신뢰 저장소로 가져와야 합니다. 위 PPM 인증서 작성 프로세스의 5단계를 참조하십시오.

- f. 서명된 인증서와 키를 결합하십시오.

```
a. cat [signed-agent] [host01.key] > [host01.pem]
```


g. MDE에서 이 호스트에 대한 에이전트를 작성할 때 [host01.pem] 인증서/키 쌍을 사용하십시오.

a. [host01.pem] is uploaded using a browser during the PPM agent creation.

PPM 에이전트 작성 중에 액세스될 수 있도록 [host01.pem]을 워크스테이션 또는 공유 자원에 복사하십시오.
에이전트가 설치되는 호스트마다 이 프로세스를 수행하십시오.

관리 서버 설정

관리 서버 설정에는 정책 에이전트를 구성하기 전에 업데이트된 인증서가 있어야 합니다. 이를 위해서는 회사의 키 저장소와 신뢰 저장소 및 CA 인증서 번들을 업로드한 후에 서버에서 제공된 스크립트(/opt/securityfirst/spsd/bin/spsd-certsetup)를 실행해야 합니다(관리자 안내서의 서버 인증서 설정 절 참조). 또한 spsd 서비스를 다시 시작하거나 관리 서버(PPM)를 재부팅해야 합니다. 그렇지 않으면 에이전트가 MDE 관리 서버와 통신할 수 없습니다.

인증서가 업데이트되지 않고 에이전트가 구성된 경우, 인증서 업데이트 스크립트를 실행한 후에 에이전트 정보 페이지에서 에이전트 인증서를 업데이트하면 에이전트와 MDE 관리 서버 간의 통신이 복원됩니다.

부록 C PKCS12 파일 작성을 위한 샘플 변환

이 태스크 정보

다음 단계를 사용하여 클라이언트 개인 키와 클라이언트 인증서를 하나의 PKCS12(Public Key Cryptography Standard #12) 파일로 결합하십시오.

```
[user@localhost]$ openssl pkcs12 -export -out ppmclient.p12 -inkey client_key.pem -in client_cert.pem  
-name ppmclient
```

```
[user@localhost]$ keytool -v -list -keystore ppmclient.p12 -storetype pkcs12
```

부록 D 해야 할 작업과 하지 말아야 할 작업

지정된 키 변경

개요

보호된 디렉토리 내에 데이터가 있고 해당 디렉토리 및 연관된 키를 수정하려고 합니다.

배경

디렉토리 내의 데이터는 데이터 작성 시(또는 해당 디렉토리로 이동 시) 정의되는 키를 사용하여 암호화됩니다. 정책 키를 변경해도 기존의 데이터가 새 키로 마이그레이션되지 않습니다.

정책이 에이전트에 적용되고 활성화되면 보호된 디렉토리의 키 값을 수정하는 것은 잠재적으로 매우 위험합니다. 엄격하게 금지되지는 않지만 키 값을 수정하면 데이터가 유실될 수 있습니다.

해야 할 작업:

관리자가 임의 키에서 다른 키로 전체 디렉토리를 마이그레이션하려는 경우, 우선 데이터를 해당 디렉토리에서 이동해야 합니다. 디렉토리가 비면 정책을 통해 연관된 키 값을 변경하고 적용할 수 있습니다. 그런 다음, 데이터를 해당 디렉토리로 다시 이동할 수 있고 데이터는 새 키로 암호화됩니다.

하지 말아야 할 작업:

정책에 연관된 키 값을 수정하지 말고 디렉토리에서 데이터를 우선 마이그레이션하지 않은 상태로 정책을 활성화하십시오. 우수 사례 방법이 그 다음에 수행되지 않으면 디렉토리에 원래 있던 데이터는 계속 원래 키를 사용하여 암호화됩니다. 정책을 새 키로 수정하면 데이터는 액세스할 수 없게 됩니다. 또한, 원래 키가 로테이션되는 경우, 정책을 원래 키 값으로 다시 수정할 수 없기 때문에 데이터는 영구적으로 액세스할 수 없습니다.

암호화된 백업을 사용하여 키 로테이션

개요

보호된 디렉토리의 데이터를 백업하려고 합니다.

배경

암호화된 형식으로 데이터를 백업하면 해당 데이터는 백업 시에 키 값에 연결됩니다. 백업 조작 수행 후에 키가 로테이션되면 적절하게 복원할 수 없습니다.

키는 데이터가 아니라 보호된 위치에 연관되어야 합니다. 이를 통해 복원 시에 의도치 않은 데이터 액세스 문제가 방지됩니다.

해야 할 작업:

디렉토리 내의 데이터는 데이터 작성 시(또는 해당 디렉토리로 이동 시) 정의되는 키를 사용하여 암호화됩니다. 키를 로테이션하기 전에 데이터를 백업하는 것이 좋은 방법입니다. 에이전트 유틸리티 “spx-backup”을 사용하여 이 작업을 수행할 수 있습니다. 그러면 보호된 디렉토리를 기반으로 하지 않고 키 로테이션의 영향을 받지 않는 키가 있는 데이터를 백업합니다.

하지 말아야 할 작업:

보호된 디렉토리를 암호화된 양식(예: 디스크 이미지 또는 VM 스냅샷)으로 복사할 때 주의하십시오. 완료되면 데이터는 원래 키가 로테이션된 후 액세스할 수 없게 됩니다.

부록 E 적절한 암호화

기존의 디렉토리 구조와 데이터에 대한 암호화를 허용하고 임의의 시점에 데이터의 상태를 판별할 수 있도록 MDE는 "spxconvert"라고 하는 명령행 유틸리티를 제공합니다.

이 기능은 기존 데이터를 암호화할 수 있음은 물론 PCI(Payment Card Industry) 또는 HIPAA(Health Insurance Portability and Accountability Act) 등의 감사를 거칠 때도 유용합니다.

참고: 이 기능은 파일 에이전트에서만 작동되며 공식 데이터 마이그레이션이 필요한 볼륨은 커버하지 않습니다.

명령 옵션

spxconvert 사용법: (매개변수는 대괄호 []와 함께 표시되며 유형을 포함함)

-h (-?, ?) '이 도움말 대화 상자 인쇄'

-a '암호화된 파일 감사 수행'

-p [STR] '경로 감사'

-e [STR] '경로의 비보호 파일 암호화'

-c '사전/사후 파일 변환의 모든 체크섬 덤프'

-v '상세 - 추가된 정보에 대한 추가 인쇄'

감사 (-a)

기본적으로 감사는 정책 디렉토리의 모두에 대해 수행됩니다. -p 옵션을 사용하여 이를 단일 디렉토리로 좁힐 수 있습니다. 감사는 암호화되지 않은 디렉토리에 대해 임의의 파일을 인쇄하며, 암호화된 디렉토리 내의 총 파일 수에 대한 파일 개수를 인쇄합니다.

암호화 (-e)

지정된 디렉토리의 비보호 파일을 변환합니다. 완료 시에 일치되지 않는 체크섬의 파일이 사용자에게 표시됩니다. 선택적 -c 플래그는 해당 충돌만이 아니라 완료 시에 모든 파일에 대한 체크섬을 인쇄합니다. 시스템 캐시가 변환 이후에 플러시되어야 하므로, 체크섬은 성능을 위해 완료 시에만 인쇄될 수 있습니다. 각 파일 이후에 캐시를 플러시하면 성능에 막대한 부정적인 영향을 줄 수 있습니다.

감사 단계

1. 암호화 보류 중인 항목이 있는 경우 표시:

spxinfo -l

1. 데이터에 관한 세부 정보 표시:

spxconvert -a -v

1. 특정 디렉토리에 관한 세부 정보 표시:

spxconvert -p -v <path>

암호화 단계

1. 암호화 보류 중인 항목 표시:

spxinfo -l

1. 암호화 전에 모든 체크섬 표시:

spxconvert -c -p <path>

1. 특정 경로의 파일 암호화:

spxconvert -p -v <path>

1. 암호화 이후 특정 경로의 모든 체크섬 표시:

spxconvert -c -p <path>

부록 F 에이전트 디버그 로깅

기본적으로 정책 에이전트는 로깅에서 누락된 디버그 레벨 메시지로 작동됩니다. 에이전트의 로그에서 디버그 레벨 메시지를 캡처하기 위해, 에이전트의 시스템 관리자는 해당 기능을 작동시킨 후에 디버그 레벨 메시지의 캡처가 시작될 수 있도록 에이전트를 다시 시작해야 합니다.

유효값은 1 - 6입니다. 그러나 기본값은 '4'이며 '4' 미만의 값을 설정하면 유용한 정보가 누락될 수 있습니다.

중요 참고

- 디버그 레벨 로깅을 사용하면 민감한 시스템 정보가 노출될 수 있습니다.
- 디버그 메시징의 특성 때문에 에이전트 로그 파일의 파일 크기가 엄청나게 증가될 수 있습니다.

Linux 에이전트

이 태스크 정보

/etc/sysconfig/spx-policyagent에 있는 구성 파일을 찾아서 디버깅을 사용으로 설정하고 쓰기 가능 플래그를 설정하십시오(**chmod +w /etc/sysconfig/spx-policyagent**).

따옴표 없이 "**LOG_LEVEL=6**"을 파일의 맨 아래에 추가하십시오.

Windows 에이전트

이 태스크 정보

HKLM\SYSTEM\CurrentControlSet\Services\Spx Policy Agent\log level에 있는 레지스트리 키를 찾아서 디버깅을 사용으로 설정하고 값을 '6'으로 설정하십시오.

부록 G 비OVA 배치

다음은 PPM 배치에 맞게 비OVA 환경을 설정하는 방법에 관한 예제 지시사항입니다. 이 지시사항은 제공된 PPM OVA를 배치하지 않고, 대신 PPM 소프트웨어를 배치할 고유 RHEL 또는 CentOS 7.x 환경을 작성하는 경우에만 해당됩니다.

모든 PPM 노드에 이 패키지를 설치하십시오.

참고: 이 설정은 하나의 예제일 뿐입니다. 이 지시사항이 올바르지 않게 되는 환경별 요구사항이 많이 있습니다. 추가 도움은 지원 센터에 문의하십시오.

1. java 1.8 및 postgresql 9.2를 설치하십시오.

참고: initdb 프로세스 중에 비밀번호를 입력하도록 프롬프트됩니다. 이 비밀번호는 postgres “superuser” 비밀번호입니다.

```
yum install -y postgresql-server java-1.8.0-openjdk-headless
passwd postgres
su - postgres
initdb --auth=md5 -W
exit
```

2. 방화벽 정책을 설치하십시오.

아래 예에서는 iptables를 사용하여 방화벽 정책을 설치하는 방법을 보여줍니다. 다른 방법도 마찬가지로 잘 작동하며 사이트 환경 설정에 따라 사용할 수 있습니다. 예: `yum install -y iptables iptables-services`

다음 두 명령에서는 firewalld가 설치되어 사용으로 설정되었다고 가정합니다. firewalld가 설치되지 않은 경우에도 해당 명령을 실행해도 무방합니다.

```
systemctl stop firewalld
systemctl disable firewalld
```

IP 테이블 방화벽 서비스 시작 및 플러시

```
systemctl start iptables.service
iptables -F
```

iptables 서비스 사용 설정 - 선택적 단계 - 로컬 소프트웨어 기반 방화벽이 필요하지 않으면 건너뛸 수 있습니다.

```
systemctl enable iptables.service
```

기본 방화벽 정의 - 선택적 단계 - 로컬 소프트웨어 기반 방화벽이 필요하지 않으면 건너뛸 수 있습니다.

```
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --
update --seconds 60 --hitcount 4 --name DEFAULT --rsource -j LOG --log-prefix
"SSH BruteForce: "
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --
update --seconds 60 --hitcount 4 --name DEFAULT --rsource -m recent --set --name
ssh --rsource
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
service iptables save
```

3. Keepalive, HAProxy 및 PSMisc 패키지를 설치하십시오.

```
yum install -y haproxy keepalived psmisc
```

4. Zookeeper를 다운로드하십시오.

참고: wget이 설치되지 않은 경우 설치하십시오.

```
yum install -y wget
wget http://apache.claz.org/zookeeper/zookeeper-3.4.10/zookeeper-3.4.10.tar.gz
```

```
mkdir /home/admin
mv zookeeper-3.4.10.tar.gz /home/admin
```

5. 신뢰할 수 있는 네트워크 시간 소스를 설치하고 구성하십시오.

이 예에서는 NTP 구성을 표시하지만, 기타 신뢰할 수 있는 시간 소스도 똑같이 잘 작동하며 사이트 환경 설정에 따라 사용할 수 있습니다.

```
yum install -y ntp
sed -i "/server\ [0-9].rhel/ s/rhel/us/" /etc/ntp.conf
sed -i "/server\ [0-9].centos/ s/centos/us/" /etc/ntp.conf
systemctl stop chronyd
systemctl disable chronyd
systemctl start ntpd
systemctl enable ntpd
```

6. EPRL(Extra Packages for Enterprise Linux) 저장소 설치

```
yum install -y epel-release
```

7. 예측할 수 없는 난수 생성기를 설치하십시오(EPEL 필요).

```
yum install -y haveged
```

8. 서비스 데이터 컬렉션의 net-tools를 설치하십시오.

```
yum install -y net-tools
```

부록 H 소프트웨어 버전 확인

다음 명령을 확인하여 소프트웨어 버전을 확인하십시오.

PPM 버전

PPM VM 셸에서 다음 명령을 실행하십시오.

```
cat /etc/ppm/buildinfo/release
```

Linux 에이전트 버전

Linux CLI에서 다음 명령을 실행하십시오.

```
yum list policyagent
```

AIX 에이전트 버전

AIX CLI에서 다음 명령을 실행하십시오.

```
rpm -qa | grep fileagent
```

Windows 에이전트 버전

Windows에서 **프로그램 추가/제거**로 이동하십시오. 스크롤하여 에이전트 이름을 찾으십시오.

에이전트 유형	Windows의 에이전트 이름
정책이 적용된 파일	FileAgent
볼륨	VolumeAgent
정책이 적용된 볼륨	HybridAgent

부록 I 용어집

용어	정의
가상 머신(VM, Virtual Machine)	컴퓨터 아키텍처 및 실제 또는 가상 컴퓨터 기능을 기반으로 하는 컴퓨터 시스템의 에뮬레이션입니다.
고가용성(HA, High Availability)	시스템 조작은 중복(이중 전원 공급, CPU, 드라이브, 소프트웨어 등)으로 인해 구성요소가 실패해도 계속됩니다.
공개 키 인프라(PKI, Public Key Infrastructure)	디지털 인증서를 작성, 관리, 배포, 사용, 저장 및 취소하고 공개 키 암호화를 관리하는 데 필요한 역할, 정책 및 프로시저 세트입니다.
그래픽 사용자 인터페이스(GUI, Graphical User Interface)	사용자가 텍스트 기반 인터페이스 및 입력되는 명령과는 다르게 그래픽 아이콘을 사용하여 MDE와 상호작용하도록 허용하는 사용자 인터페이스 유형입니다.
도메인 이름 서비스(DNS, Domain Name Service)	도메인 이름을 IP 주소로 변환하는 인터넷 서비스입니다.
도메인 이름(DN, Domain Name)	전체적으로 고유하며 IP 대상 정보에 링크되는 인터넷 자원 이름입니다.
명령행 인터페이스(CLI, Command Line Interface)	사용자가 텍스트 행(명령행) 양식으로 애플리케이션에 대해 명령을 실행하는 상호작용의 유형입니다.
보호된(Protected)	처리된 모든 데이터입니다.
볼륨 에이전트(Volume Agent)	볼륨 에이전트는 대상 시스템에서 하나 이상의 보호된 볼륨의 연관과 볼륨 정책 정의를 적용합니다.
선택자(Selector)	데이터, 경로 세트 및 기타 정책 관련 기능에 액세스할 수 있는 OS 정의된 사용자 및 그룹입니다.
신뢰 저장소(Truststore)	신뢰 저장소에는 SSL 연결에서 서버에 의한 인증서 확인에 사용되는 신뢰할 수 있는 인증 기관(CA)의 인증서가 저장됩니다.
암호화 액세스 제어(Cryptographic Access Controls)	다른 암호화 방법을 사용하여 사용자 액세스를 분리하는 기능입니다.
에이전트(Agent)	보안 우선 암호화 및 액세스 제어 소프트웨어를 실행하는 관리 서버입니다.
역할 기반 액세스 제어(RBAC, Role Based Access Control)	엔터프라이즈 내에서 개별 사용자의 역할을 기반으로 컴퓨터 또는 네트워크에 대한 액세스를 제어하는 방법입니다. 이 컨텍스트에서 액세스는 개별 사용자가 특정 태스크(예: 파일 보기, 작성 또는 수정)를 수행하는 기능입니다.
오브젝트 저장소 에이전트(Object Store Agent)	오브젝트 저장소 에이전트는 전송될 데이터를 암호화하고 분할하여 클라우드, 온 프레미스 또는 이 모두에서 확장성이 높고 효율적인 오브젝트 스토리지에 안전하게 저장합니다.
인증 기관(Certificate Authority)	디지털 인증서를 서명하기 위한 신뢰 조직입니다. CA는 제출된 인증서 요청의 적법성과 ID를 검증합니다. 요청 검증에 성공하는 경우, CA는 서명된 인증서를 발행합니다.

인증서 폐기 목록(CRL, Certificate Revocation List)	대응되는 인증서를 발행한 인증 기관(CA)이 취소한 인증서의 게시된 목록입니다.
자동 생성 키(Auto-Generated Keys)	정책 적용 키는 MDE가 작성 및 관리합니다. 이는 자동 생성 키에 의해 정책 작성 중에 표시됩니다.
정책이 적용된 볼륨 에이전트(Volume with Policy Agent)	이는 볼륨 에이전트에 대한 볼륨 정책 보호의 레버리지를 활용하며, 파일 기반의 운영 액세스 제어 정책이 하나 이상의 보호된 파일 경로에 대해 적용되고 강제 실행되도록 허용합니다. 이를 하이브리드 에이전트라고도 합니다.
초기화 벡터(IV, Initialization Vector)	세션에서 한 번만 채택되는 데이터 암호화의 비밀 키와 함께 사용될 수 있는 임의의 또는 예측 불가능한 난수입니다.
키 로테이션(Key Rotation)	에이전트 환경 내에서 정책 적용 키를 마이그레이션하면 데이터 액세스에 대한 변경이 사용자에게 표시되지 않습니다.
키 저장소(Keystore)	정책 적용 키에 대해 구성된 스토리지 위치입니다.
키 취소(Key Revocation)	에이전트 환경에서 정책 적용 키를 제거하면 암호화 데이터 액세스 제한이 복구 가능하게 됩니다. 이 조치로 인해 데이터는 임시로 읽을 수 없습니다.
키 폐기(Key Shredding)	에이전트 환경에서 정책 적용 키를 제거하면 암호화 데이터 액세스 제한이 복구 불가능하게 됩니다. 이 조치로 인해 데이터는 영구적으로 읽을 수 없습니다.
파일 에이전트(File Agent)	파일 에이전트는 파일 기반의 운영 액세스 정책 정의 및 하나 이상의 보호된 파일 경로를 강제 적용합니다. 각 보호된 파일 경로는 자체적으로 운영 및 암호화 액세스 제어를 포함할 수 있습니다.
하이퍼바이저(Hypervisor)	가상 머신 모니터라고도 합니다. 하이퍼바이저 또는 가상 머신 모니터(VMM)는 가상 머신을 작성, 실행, 관리하는 일종의 컴퓨터 소프트웨어, 펌웨어 또는 하드웨어입니다. 하이퍼바이저가 하나 이상의 가상 머신을 실행하는 컴퓨터를 호스트 머신이라고 하며 각 가상 머신은 게스트 머신이라고 합니다. VMware 하이퍼바이저는 ESXi 호스트라고도 합니다.
협정 세계시(UTC, Coordinated Universal Time)	세계에서 클럭 및 시간을 규정하는 기본 <u>시간 표준</u> 입니다.
AES-NI(Advanced Encryption Standard New Instructions)	2001년에 미국 NIST(National Institute of Standards and Technology)에서 제정한 전자 데이터의 암호화 스펙이며, SPx 기반 제품이 사용하는 암호화 프로토콜입니다.
AWS(Amazon Web Services) S3	데이터를 저장하고 검색하는 단순 스토리지 서비스로서 확장 가능성이 높고 저렴한 오브젝트 스토리지입니다.
CADF(Cloud Auditing Data Federation)	SIEM(Security Information and Event Management) 시스템에 전달되는 공통 이벤트 형식 구문 유형입니다.
CEF(Comma Event Format)	SIEM(Security Information and Event Management) 시스템에 전달되는 공통 이벤트 형식 구문 유형입니다.

CRLDP(Certificate Revocation List Distribution Point)	이름, (선택사항으로) 취소 사유 및 CRL 발행자 이름이 포함된 발행 CA에 의한 취소된 인증서 관련 정보가 보관되는 인증서 내의 시작점 필드입니다.
CSV(Comma Separated Value)	섬표를 필드 구분 기호로 사용하고 리턴을 레코드 구분 기호로 사용하는 데이터 형식입니다.
CURL	CURL은 다양한 프로토콜을 사용하여 데이터를 전송하기 위한 라이브러리와 명령행 도구를 제공하는 컴퓨터 소프트웨어 프로젝트입니다.
DER(Distinguished Encoding Rules)	DER은 ITU-T X.690, 2002, 스펙에 정의된 ASN.1 인코딩 규칙 중 하나입니다. 데이터 구조에 대한 인코딩 규칙은 컴퓨터 간의 전송 시에 스트림의 바이트가 구성되는 방법을 규정하는 전송 구문을 제공합니다.
DHCP(Dynamic Host Configuration Protocol)	해당 IP 주소 및 관련 구성 정보(예: 서브넷 마스크 및 기본 게이트웨이)를 IP(Internet Protocol)에 자동으로 제공하는 클라이언트/서버 프로토콜입니다.
HIPAA(Health Insurance Portability and Accountability Act)	HIPAA 개인정보 보호 규정에서는 제공자와 조직에게 PHI(Protected Health Information)의 기밀성과 보안성을 보장하도록 요구합니다.
HTTP(Hypertext Transfer Protocol)	월드 와이드 웹에 대한 데이터 통신의 기반이 되는 애플리케이션 프로토콜입니다.
IBM Cloud Object Storage(COS S3)	저장 데이터 및 고가용성을 제공하는, 백업, 아카이브, 비디오 파일 및 이미지 파일과 같은 많은 양의 데이터를 보유하는 스토리지 플랫폼입니다.
Java 키 저장소(JKS, Java KeyStore)	Java 키 저장소(JKS)는 보안 인증서(권한 부여 인증서 또는 공개 키 인증서) 및 대응되는 개인 키의 저장소입니다. JDK(Java Development Kit)는 키 저장소에서 키와 인증서를 관리하기 위한 도구(keytool)를 제공합니다. jks 확장자는 Java 특정 파일 형식입니다.
LDAP(Lightweight Directory Access Protocol)	네트워크에서 분산 디렉토리 정보에 액세스 및 이를 유지보수하는 개방형의 공급업체에 중립적인 산업 표준 프로토콜입니다. 네트워크에서 누구든지 조직, 개인 및 기타 리소스(예: 파일 및 디바이스)를 찾을 수 있도록 하는 소프트웨어 프로토콜입니다.
LEEF(Log Event Extended Format)	LEEF는 QRadar에 대해 읽기 가능하고 손쉽게 처리되는 이벤트가 포함된 IBM Security QRadar의 사용자 정의된 이벤트 형식입니다. 이는 이벤트 페이로드에 대한 다수의 사전정의된 이벤트 속성을 지원합니다.
LVM(Logical Volume Manager)	디바이스 매퍼 Linux 커널 프레임워크를 사용하여 그룹으로 스토리지 디바이스를 수집하며 필요하면 결합된 공간의 LU(Logical Unit)를 할당하는 스토리지 디바이스 관리자입니다. 대부분의 Linux 배포자는 LVM을 인지합니다.
M of N(M:N)	작성된 총 조각(공유) 수(N) 중 데이터를 다시 빌드하는 데 필요한 데이터 조각 수(M)를 결정하는 모델입니다.
NTFS(NT File System)	Windows NT 운영 체제에서 Microsoft에 의해 개발되고 파일 레벨 보안, 압축 및 감사를 지원한 하드 디스크의 파일을 저장하고 검색하는 데 사용되는 전용 파일 시스템입니다.

NTP(Network Time Protocol)	컴퓨터 시스템 간에 클럭 동기화를 위한 네트워킹 프로토콜입니다.
OCSP(Online Certificate Status Protocol)	X.509 디지털 인증서의 폐기 상태를 가져오는 데 사용된 내부 프로토콜입니다.
OID(Object Identifier)	전역적으로 모호하지 않은 지속적 이름으로 오브젝트나 개념의 이름을 지정하기 위한 ID 표준화 메커니즘입니다.
OVA(Open Virtualization Archive)	tar 아카이브 파일입니다. 이는 하나의 파일로 zip 또는 압축된 모든 OVF 파일입니다.
PCI(Payment Card Industry)	사기를 줄이기 위해 카드 소지자 데이터와 관련하여 제어성과 보안성을 높이기 위한 표준입니다.
PEM	X.509 v3 표준으로 정의된 구문 및 콘텐츠가 포함된 보안 인증서에 대해 광범위하게 사용되는 인코딩 형식입니다.
PKCS12(Public Key Cryptography Standard #12)	다수의 암호화 오브젝트를 단일 파일로서 저장하기 위한 아카이브 파일 형식을 정의하는 공개 키 암호화 표준입니다. 이는 일반적으로 X.509 인증서에서 개인 키를 번들링하고 신뢰 체인의 모든 멤버를 번들링하는 데 사용됩니다. 이는 암호화되고 서명될 수 있습니다.
PostgreSQL	PostgreSQL(발음: “post-gress-Q-L”)은 전세계의 지원자 팀에 의해 개발된 오픈 소스 RDBMS(Relational DataBase Management System)입니다. PostgreSQL은 회사 또는 기타 민간 기업의 통제를 받지 않으며 소스 코드는 무료로 사용이 가능합니다.
ReFS	Windows Server 2012에서 도입되었으며 데이터 가용성, 확장성과 데이터 무결성을 최대화하도록 설계된 Microsoft의 새 파일 시스템입니다.
REST API(Representational State Transfer Application Program Interface)	RESTful 웹 서비스라고도 하는 RESTful API는 종종 웹 서비스 개발에서 사용되는 통신에 대한 아키텍처 스타일과 접근 방법인 REST(Representational State Transfer) 기술을 기반으로 합니다.
RSA	공개 및 개인 키를 사용하여 데이터를 보호하는 RSA(Rivest, Shamir, and Adelman)에 의해 개발된 공개 키 암호화입니다.
scp(Secure Copy Protocol)	scp 명령은 SSH(Secure Shell) 프로토콜을 통해 시스템 간에 파일을 전송하기 위해 Linux에서 사용됩니다.
SSH(Secure Socket Shell)	관리자에게 원격 컴퓨터 액세스에 대한 보안 설정된 방법을 제공하는 네트워크 프로토콜입니다. SSH는 이 프로토콜을 구현하는 유틸리티 스위트를 의미하기도 합니다.
SSL(Secure Sockets Layer)	대칭 키를 교환하기 위해 비대칭 키를 활용하여 인터넷상의 데이터 통신을 암호화하는 암호화 프로토콜입니다. 인증 기관 및 공개 키 인프라는 인증서를 생성, 서명하고 이의 유효성을 관리함은 물론 인증서와 소유자의 검증을 허용하는 데 필요합니다.
TLS(Transport Layer Security)	컴퓨터 네트워크 상에서 안전한 통신을 제공하는 암호화 프로토콜입니다.

UUID(Unique Identifier)	UUID(Unique Identifier)는 소프트웨어 구성에서 사용되는 ID 표준입니다. UUID(128비트 숫자)는 인터넷에서 일부 오브젝트 또는 엔티티를 고유하게 식별하는데 사용됩니다.
VMware ESXi™	실제 또는 가상 컴퓨터 기능과 컴퓨터 아키텍처를 기반으로 하는 특정 컴퓨터 시스템의 에뮬레이션입니다.

공지사항[r]

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

본 자료는 다른 언어로도 제공될 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, 3IFC

한국 아이.비.엠 주식회사

대표전화서비스: 02-3781-7114

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, 3IFC

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.

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.

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. 샘플 프로그램은 어떠한 종류의 보증 없이 "현상태대로" 제공됩니다. IBM은 귀하의 샘플 프로그램 사용과 관련되는 손해에 대해 책임을 지지 않습니다. 이 정보를 보는 방법에 따라 일부 이미지와 삽화가 나타나지 않을 수도 있습니다.

상표[r]

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, 서비스 표, 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[r]

해당되는 책의 사용에 대한 권한은 다음의 이용 약관에 따라 부여됩니다.

적용: 본 이용 약관은 IBM 웹 사이트의 모든 이용 약관에 추가됩니다.

개인적 사용: 모든 소유권 공지사항을 표시하는 경우에 한해 귀하는 개인적이며 비상업적 용도로 이 책을 복제할 수 있습니다. IBM의 명시적인 동의 없이 이 책 또는 그 일부를 배포 또는 전시하거나 2차적 저작물을 만들 수 없습니다.

상업적 사용: 모든 소유권 공지사항을 표시하는 경우에 한해 귀하는 이 책을 귀하의 기업집단 내에서만 복제, 배포하고 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 권한에서 명시적으로 부여된 경우를 제외하면, 이 책이나 이 책에 포함된 정보, 데이터, 소프트웨어 또는 기타 지적 재산권에 대해 어떠한 권한, 라이선스 또는 권리도 명시적으로 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[r]

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 고 객인 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.

제품 번호: 5737-C67

미국에서 인쇄됨

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.



SC43-5058-01

