

IBM Multi-Cloud Data Encryption
Powered by SPx[®]
Version 2.3

Verwaltung



Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „[Bemerkungen](#)“ auf Seite 115 gelesen werden.

Diese Ausgabe bezieht sich auf Version 2.3 von IBM Multi-Cloud Data Encryption (Produktnummer 5737-C67) und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuauflage geändert wird.

© Copyright IBM Corporation and others 2017, 2019

© **Copyright International Business Machines Corporation 2017, 2019.**

Inhaltsverzeichnis

Kapitel 1. Einführung.....	1
Autorisierte Nutzungsberechtigung.....	1
Kontaktadresse.....	1
Hintergrund und Zweck des Handbuchs 'Verwaltung'.....	1
Kapitel 2. Allgemeine Übersicht.....	3
Produktübersicht	3
Agententypen.....	3
Datenträgeragent.....	3
Agent vom Typ 'Datei mit Richtlinie'	4
Agent vom Typ 'Datenträger mit Richtlinie'.....	5
Agent vom Typ 'Objektspeicher'.....	5
Agentenfunktionsmatrix.....	5
Kapitel 3. Planungsaspekte.....	7
Voraussetzungen.....	7
Systemmindestvoraussetzungen.....	7
Zertifikatsanforderungen.....	8
Dateisystemunterstützung für Agenten	8
Netzkonfiguration.....	9
Netzports	9
OVA-Konfiguration	9
REST-Schnittstelle.....	9
Kapitel 4. Produktinstallation.....	11
Installation vorbereiten.....	11
Lizenzierung.....	11
Verwaltung der MDE-OVA und der VM.....	11
MDE installieren.....	11
Sprachkonfiguration.....	12
Datenbanksetup.....	13
Interne Datenbank.....	13
Externe Datenbank.....	13
Einstellungen für Serverzertifikate.....	14
Keystore, Truststore und Zertifizierungsstelle (CA).....	14
PKI-Infrastruktur - Einstellungen.....	14
Starten und erste Anmeldung	15
Kapitel 5. Grafische Benutzerschnittstelle (GUI) von MDE.....	17
Grundlegende Navigation im Produkt.....	17
Produktdashboard.....	17
Automatische Vervollständigung in Textfeldern.....	17
Zu beachtende Benachrichtigungen.....	17
Erweiterte Eigenschaften.....	18
GUI-Spracheinstellung.....	19
Kapitel 6. Jobs.....	21
Jobbeschreibungen.....	21
Genehmigung durch mehrere Administratoren.....	22
Jobgenehmigung.....	23

Jobablehnung.....	23
Jobverzicht.....	23
Jobinformationen.....	23
Kapitel 7. Management von Benutzern mit Verwaltungsaufgaben in MDE.....	25
Rollen für Benutzer mit Verwaltungsaufgaben.....	25
Produktadministratorrolle.....	25
Sicherheitsadministratorrolle.....	25
Management von Benutzern mit Verwaltungsaufgaben.....	25
Neuen Benutzer mit Verwaltungsaufgaben hinzufügen	25
Kennwort für einen Benutzer mit Verwaltungsaufgaben bearbeiten.....	26
Rolle für Benutzer mit Verwaltungsaufgaben bearbeiten.....	26
Status für Benutzer mit Verwaltungsaufgaben bearbeiten.....	27
Benutzer mit Verwaltungsaufgaben entfernen	27
Benutzerkontosperrung.....	27
LDAP-Verzeichnisliste	28
Benutzerquelle.....	28
Kapitel 8. Ereignisse.....	29
Ereignisprotokoll.....	29
Ereignisdetails.....	30
Ereignisexport.....	30
Ereignisweiterleitung.....	30
Ereignisargumente.....	31
Agentenereignisse.....	31
Zuverlässige Ereignisse.....	31
Kapitel 9. Management von Richtliniendurchsetzungsschlüsseln.....	33
Schlüssel hinzufügen.....	33
Schlüssel bearbeiten.....	33
Schlüsselrotation	33
Schlüsselwiderruf.....	35
Schlüsselschredderung.....	36
Automatisch generierte Schlüssel.....	36
Externer Keystore.....	36
KMIP-Keystores.....	36
Hardware Security Modules (HSM).....	38
Kapitel 10. Richtliniendefinition auf Dateiebene.....	41
Selektoren.....	41
Pfadgruppen.....	42
Datentypen.....	43
Datentypzeile.....	43
Variablen für Datentypzeilen.....	43
Prozesse.....	44
Kapitel 11. Agentenbereitstellung und Agentenmanagement.....	47
Agenten hinzufügen	47
Identität	47
Netz	48
Agenten des Typs 'Datei mit Richtlinie', 'Datenträger mit Richtlinie' und 'Datenträger' erstellen. ...	49
Datenträger.....	51
Objektspeicheragent erstellen.....	52
Berechtigte Benutzer	55
Agententools.....	56
Prüfen und Build erstellen.....	57
Agentenaktivierung.....	57

Agenten anzeigen.....	58
Agentenbericht.....	58
Agenten installieren.....	58
Agenten für Linux installieren.....	59
Agenten für AIX installieren.....	61
Agenten für Windows installieren.....	61
Aktive Richtlinie	64
Agenten bearbeiten.....	64
Agenteninfo bearbeiten.....	64
Zertifikate hinzufügen/löschen.....	65
Agententools.....	65
Datenzugriff über SU.....	66
Richtlinie aussetzen.....	67
Richtlinienänderungen.....	67
Agentensnapshots.....	71
Agentenbearbeitungen und Snapshots speichern.....	71
Snapshots verwalten.....	72
Dateiagenten deinstallieren	73
Datenträgeragenten deinstallieren.....	74
Datenträgeragenten deinstallieren	74
Agenten vom Typ 'Datenträger mit Richtlinie' deinstallieren	75
Agent vom Typ 'Objektspeicher' deinstallieren.....	76
Agenten aus MDE entfernen	76
Agentendienstprogramme.....	76
Kapitel 12. Operationen.....	79
Sicherung und Wiederherstellung von Produktdaten	79
Sicherung von Produktdaten	79
Wiederherstellung von Produktdaten	79
Kernelaktualisierung.....	80
Upgrade	80
Für den MDE-Server.....	80
Für die Ziel-VM von Agenten.....	81
Servicedaten.....	82
Servicedaten erfassen.....	82
Schutzwürdige Informationen aus PPM-Protokollen entfernen.....	82
Anhang A. Beispiele für Agenteninstallationsprozesse.....	85
Red Hat-/CentOS-Prozess.....	85
AIX-Prozess.....	86
Windows Server-Prozess.....	86
Anhang B. Beispielzertifikate einer Zertifizierungsstelle (CA).....	89
Anhang C. Beispielkonvertierung zum Erstellen einer PKCS12-Datei.....	93
Anhang D. Empfehlungen und Warnungen.....	95
Zugeordnete Schlüssel ändern.....	95
Übersicht.....	95
Hintergrund.....	95
Schlüsselrotation mit verschlüsselten Sicherungen.....	95
Übersicht.....	95
Hintergrund	95
Anhang E. Verschlüsselung an der Position.....	97
Befehlsoptionen.....	97

<i>Auditschritte</i>	97
<i>Verschlüsselungsschritte</i>	97
Anhang F. Debugprotokollierung für Agenten	99
Linux-Agenten.....	99
Windows-Agenten.....	99
Anhang G. Nicht-OVA-Bereitstellung	101
Anhang H. Prüfung der Softwareversion	103
Anhang I. Glossar	105
Bemerkungen	115
Marken.....	116
Bedingungen für die Nutzung dieser Produktdokumentation.....	117
Hinweise zur Datenschutzrichtlinie.....	118

Kapitel 1. Einführung

Autorisierte Nutzungsberechtigung

Die Verwendung dieser Software ist auf die Bedingungen der Lizenzvereinbarung beschränkt.

Kontaktadresse

Weitere Informationen zu IBM Multi-Cloud Data Encryption (MDE) finden Sie auf der IBM Support-Website unter <https://www.ibm.com/support/home/>.

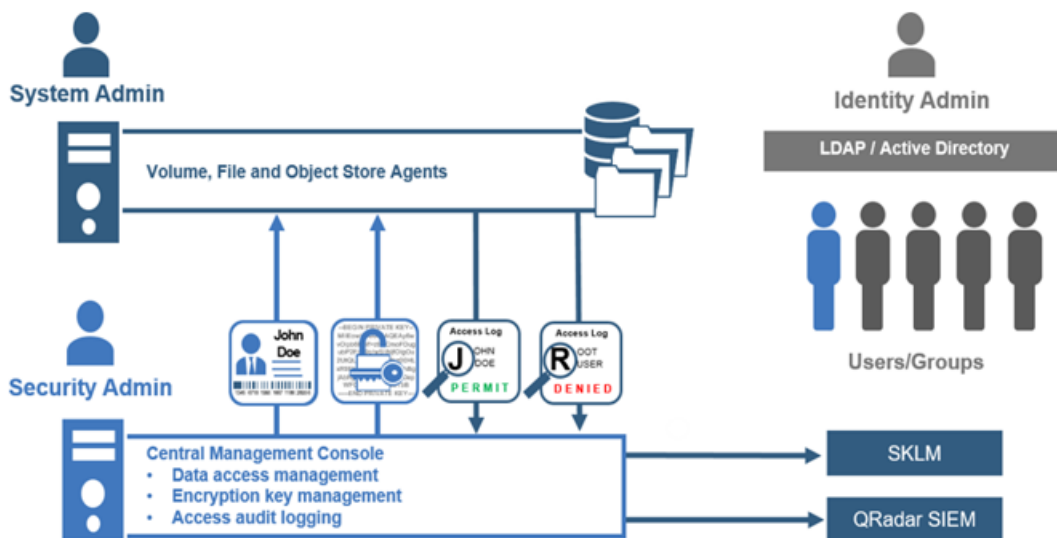
Hintergrund und Zweck des Handbuchs 'Verwaltung'

Das Handbuch 'Verwaltung' ist die primäre Informationsreferenz für die Installation, Verwaltung und Verwendung von MDE im Hinblick auf die Bereitstellung und Verwaltung von Verschlüsselungsagenten, die Richtliniendefinition (Zugriffs- und Verschlüsselungssteuerung), die Schlüsselverwaltung für die Richtliniendurchsetzung sowie im Hinblick auf den Schutz von ruhenden Daten (Data at Rest) auf ausgewählten Servern, die bereitgestellte Agenten verwenden. Dieses Dokument ist für Systemadministratoren gedacht, die über Verwaltungszugriff sowie über entsprechende Kenntnisse über das Unternehmensnetz verfügen, um das Produkt installieren und verwalten zu können.

Kapitel 2. Allgemeine Übersicht

Produktübersicht

IBM Multi-Cloud Data Encryption (MDE) ist ein umfassendes Datensicherheitsprodukt auf der Basis von SPx®-Technologie, das die Verschlüsselung ruhender Daten (durch Agenten) mit den leistungsfähigen Schutzfunktionen eines Richtlinienbereitstellungsmanagers (Policy Provisioning Manager - PPM) kombiniert, der als zentrale Managementkonsole fungiert. MDE ermöglicht die Bereitstellung von Agenten und von Einstellungen für Datenzugriffsrichtlinien (Definition des operativen Zugriffs und des Verschlüsselungszugriffs) sowie das Management (Schlüssellebensdauer, Agentenaktualisierungen und Benutzerzugriffsprotokollierung) von bis zu 25.000 Agenten über eine einzelne zentrale Position. MDE stattet ein sicheres System nahtlos mit flexibler Funktionalität für die Zuordnung von Agenten aus, die Daten auf Dateisystemebene oder Datenträgerebene mit einer einzigartigen kryptografischen Datensplitting-Technologie verschlüsseln. Das Produkt bietet einen datenzentrierten Schutz, der über die Standardverschlüsselung hinausgeht und die Datenverschlüsselung wesentlich robuster und widerstandsfähiger gegen Brute-Force-Angriffe macht. Der Schutz wird darüber hinaus durch die Möglichkeit erweitert, den Datenzugriff auf Benutzerebene durch die Definition differenzierter Zugriffsrichtlinien einzuschränken, zu überwachen und durch einen Audit zu prüfen.

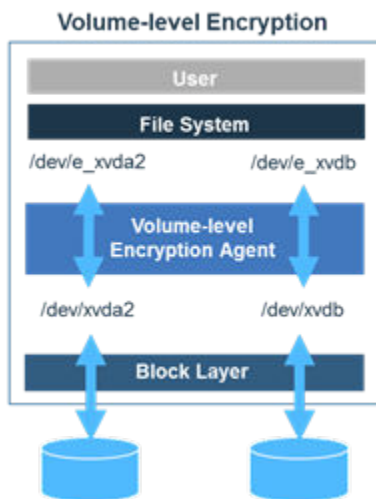


MDE ermöglicht eine Trennung von Aufgaben durch separate Administratorrollen: Produktadministrator und Sicherheitsadministrator. Der Produktadministratorrolle sind die Berechtigungen anvertraut, die zur Konfiguration und Verwaltung des MDE-Produkts erforderlich sind. Der Sicherheitsadministratorrolle sind die Berechtigungen anvertraut, die zur Bereitstellung und Verwaltung der Agenten erforderlich sind. Diese Rollen sind in Abschnitt 7 ('Management von Benutzern mit Verwaltungsaufgaben in MDE') eingehender beschrieben.

MDE unterstützt die Installation von vier Agententypen, die den Datenverschlüsselungsschutz bereitstellen, durch den die Richtliniendefinitionen durchgesetzt werden.

Agententypen

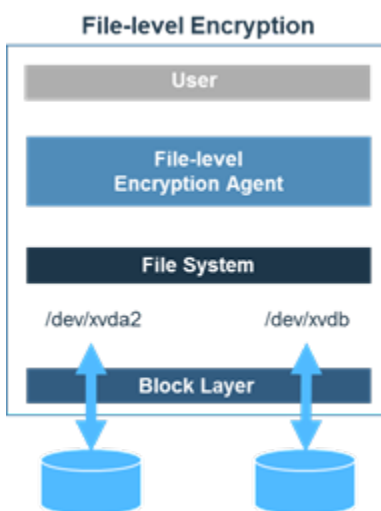
Datenträgeragent



Der Datenträgeragent stellt eine Verschlüsselung auf Datenträgerebene mit Richtliniensteuerelementen für eingeschränkten Zugriff bereit. Die Verschlüsselung auf Datenträgerebene stellt Sicherheit in Form einer geschützten, vordefinierten Speichereinheit durch eine Blocktreiberimplementierung im Betriebssystem bereit.

Ein gesamter Datenträger wird als Einheit definiert und durch Verschlüsselungsverfahren geschützt. Wenn Daten hinzugefügt, bearbeitet oder gelöscht werden, stellt der Datenträgeragent sicher, dass alle Daten auf dem Datenträger durch Verschlüsselung mit einem von PPM verwalteten Verschlüsselungsschlüssel gesichert werden.

Agent vom Typ 'Datei mit Richtlinie'



Der Agent vom Typ 'Datei mit Richtlinie' kombiniert die Verschlüsselung auf Dateiebene mit einer Datenzugriffsrichtlinie. Die Verschlüsselung auf Dateiebene stellt den Schutz einzelner Dateien auf der Dateisystemebene bereit. Die Datei- und Speicherumgebungsgrößen werden nur durch das Dateisystem und nicht durch den Agenten vom Typ 'Datei mit Richtlinie' begrenzt. Die Position für die geschützten Daten wird durch den Arbeitsgruppenschlüssel für diese Pfaddefinition geschützt und alle einzelnen Dateien, die in oder unter diesem Datenpfad gespeichert werden, werden separat mithilfe eines eindeutigen und nicht vorhersagbaren Initialisierungsvektors (IV) verschlüsselt. Geschützte Daten können lokal im Dateisystem vorhanden sein oder über NFS aus dem Netz angehängt werden.

Die eindeutigen Schlüssel der Dateiebene werden von einem internen Schlüsselmanagementsystem verwaltet. Die richtlinienbasierte Zugriffssteuerung ist auf die Verschlüsselung aufgesetzt und ermöglicht es, den Zugriff mit den Mindestberechtigungen zu definieren, die Zugriffsprotokollierung anzugeben und Zugriffsberechtigungen auf bestimmte Systemfunktionen wie Lesen/Lesen-Schreiben/Kopieren/Löschen einzuschränken. Diese Richtliniensteuerelemente funktionieren in Verbindung mit Standardberechtigungen

gen von LDAP oder Active Directory. Wenn ein Benutzer keine Berechtigungen für die Daten in LDAP oder Active Directory hat, kann der Sicherheitsadministrator diese Zugriffssteuerungsdefinitionen nicht überschreiben und den Datenzugriff nicht zulassen.

Standardmäßig werden alle Benutzer vom Zugriff auf die Daten, die durch eine Richtlinie geschützt werden, ausgeschlossen. Der Sicherheitsadministrator muss definieren, wer Zugriff haben soll. Dadurch kann der Sicherheitsadministrator Systemadministratoren, Administratoren von Cloud-Anbietern und Rootbenutzern den Zugriff auf geschützte Daten verwehren.

Agent vom Typ 'Datenträger mit Richtlinie'

Ein Agent vom Typ 'Datenträger mit Richtlinie' verwendet die Verschlüsselung auf Datenträgerebene eines Datenträgeragenten und die Richtlinien für die dateibasierte operative Zugriffssteuerung, die für einen oder mehrere geschützte Dateipfade angewendet und durchgesetzt werden kann.

Agent vom Typ 'Objektspeicher'

Ein Agent des Typs "Objektspeicher" greift auf ein Modell mit dem Konzept "M von N" zurück, das festlegt, wie viele Datenteile für das erneute Erstellen der Daten (M) aus der Gesamtanzahl der erstellten Datenteile (N) benötigt werden. Diese gespeicherten Datenteile, die sich je nach Lizenz an lokalen oder fernen Speicherorten befinden können, werden als "Shares" bezeichnet. Die Verwendung mehrerer Shares ermöglicht neben den hinzugefügten Optionen für Datenausfallsicherheit und Fehlertoleranz für einen verbesserten Datenfluss. Unterstützung des Modells "M von N" mit verteilten Shares besteht für 1:1, 2:3 oder 2:4.

Ein Agent des Typs "Objektspeicher" (Object Store Agent, OSA) verschlüsselt Daten, die an den Objektspeicher gesendet werden. Er fungiert als "Durchlauf" für Dateien, während sie an den Objektspeicher übertragen werden, und verschlüsselt und splittet Daten bei diesem Prozess. Dateien, die vom Objektspeicher über einen solchen Agenten abgerufen werden, werden beim Abrufen entschlüsselt. Die Dateien, die im Objektspeicher residieren, werden verschlüsselt. Nur berechtigte Benutzer können Daten über einen Agenten des Typs "Objektspeicher" senden/empfangen.

Agentenfunktionsmatrix

Agentenfeature	Datenträgeragent	Agent vom Typ 'Datenträger mit Richtlinie'	Agent vom Typ 'Datei mit Richtlinie'	Agent vom Typ 'Objektspeicher'
Gesamten Datenträger verschlüsseln	✓	✓		
Einzelne Dateien in vorgesehenen geschützten Verzeichnissen verschlüsseln			✓	
Richtlinie auf Dateiebene		✓	✓	
Auditprotokolle für Dateizugriffe		✓	✓	
Schutz gegen Administratorzugriff auf Benutzerdaten			✓	

Verschlüsselung von Daten im Ob- jektspeicher				✓
---	--	--	--	---

Kapitel 3. Planungsaspekte

Voraussetzungen

Die Installation von IBM Multi-Cloud Data Encryption (MDE) ist ein einfacher Prozess, der die Installation eines Basis-OVA (OVA - Open Virtual Archive) und die Ausführung eines PPM-Installationsprogramms (PPM - Provisioning Policy and Management) umfasst.

Zur Vorbereitung vor der Installation der Software empfiehlt es sich, die Installationsanweisungen vollständig zu prüfen. Nachfolgend finden Sie eine Liste der Voraussetzungen, die eine erfolgreiche Installation und Ausführung von IBM Multi-Cloud Data Encryption ermöglichen.

1. Ein Betriebsserver mit einem lizenzierten Betriebssystem und einem unterstützten Hypervisor (VMware ESXi™) zum Bereitstellen und Ausführen von PPM (Policy Provisioning Manager).
2. Gepacktes Basis-OVA.
3. PPM-Installationsprogramm.
4. Einer oder mehrere Zielserver mit einem unterstützten Agentenbetriebssystem (Red Hat®/CentOS 6.2+ oder 7.2+, AIX 7.1 oder 7.2 und Microsoft Server® 2008 R2, Microsoft Windows Server® 2012 R2 oder Microsoft Windows Server® 2016).
5. Browser: Google Chrome®, Microsoft Internet Explorer® 10+, Mozilla Firefox® ESR 52+.
6. Netzzugriff zwischen PPM und allen Agenten.
7. Durch eine Zertifizierungsstelle (CA) signierte Zertifikate (Keystore, Truststore und CA-Zertifikatsbundle) zur Einrichtung einer sicheren Sitzung zwischen Management Server (PPM) und allen Agenten.

Weitere Details finden Sie in den Abschnitten 'Zertifikatsvoraussetzungen' und 'Einstellungen für Serverzertifikate'; ein Beispiel finden Sie unter [Anhang B, „Beispielzertifikate einer Zertifizierungsstelle \(CA\)“](#), auf Seite 89.

Für einen Agenten des Typs "Objektspeicher" (Object Store Agent, OSA) gelten die folgenden zusätzlichen Voraussetzungen:

- Mit S3 kompatibler Objektspeicher: Amazon Web Services S3 (AWS S3), IBM Cloud Object Storage (COS S3)
- Objektspeicherberechtigungsnachweise: Benutzer-ID und geheimer Schlüssel (Kennwort)
- Eine Anwendung oder ein Dienstprogramm, das eine AWS S3-REST-API-Bibliothek oder eine Boto Python-Bibliothek für Datenverweise auf den OSA-Agenten nutzt.

Wichtiger Hinweis: Es wird dringend empfohlen, NTP (Network Time Protocol) für die Koordination der Systemzeiten für MDE, externe Datenbanken und Agenten zu nutzen. Dadurch wird die ordnungsgemäße Reihenfolge von Ereignis-/Auditprotokollzeitmarken sichergestellt.

Systemmindestvoraussetzungen

Systemmindestvoraussetzungen für die PPM-VM

- CPU 4
- 8 GB RAM
- 40 GB verfügbarer Speicherplatz
- Netzzugriff erforderlich

Systemmindestvoraussetzungen für Linux-Agenten

- Eine Core-64-Bit-CPU @2GHz mit aktivierter AES-NI
 - (empfohlen 2 Core-64-Bit-CPU's @2GHz mit aktivierter AES-NI)
 - 2 GB RAM (empfohlen: 4 GB RAM)
- 20 GB verfügbarer Festplattenspeicherplatz
 - 300 MB oder mehr für den Protokolldateispeicherplatz empfohlen
- Netzzugriff erforderlich
- Installation / Aktualisierung der folgenden Pakete: curl, openssl und nss unter Red Hat / CentOS
- Internetzugriff oder Zugriff auf ein lokales Repository bei der ersten Agenteninstallation
- Ein SSL-Zertifikat ist für Agenten erforderlich.

Systemmindestvoraussetzungen für Windows-Agenten

- 1 Core-64-Bit-CPU @2GHz mit aktivierter AES-NI - empfohlen sind 2 Core-64-Bit-CPU's @2GHz mit aktivierter AES-NI
- 4 GB RAM - empfohlen sind 8 GB RAM
- 20 GB verfügbarer Festplattenspeicherplatz - 300 MB oder mehr sind für den Protokolldateispeicherplatz empfohlen
- Netzzugriff erforderlich
- Ein SSL-Zertifikat ist für Agenten erforderlich.

Anmerkung: Erfordert ein SSL-Zertifikat (selbst signiert oder von der Zertifizierungsstelle (CA) signiert) / eine Schlüsselpaardatei vor der Erstellung von Agenten. Das Zertifikat wird zum Herstellen einer sicheren TLS-Verbindung zwischen dem Agenten und dem MDE-Server verwendet.

Zertifikatsanforderungen

Um eine sichere Verbindung zwischen dem PPM-Server und den Agenten herzustellen, sind Zertifikate erforderlich. Dabei gelten die folgenden Voraussetzungen für die Zertifikate:

- Für den PPM-Server ist es erforderlich, dass das von einem Agenten bereitgestellte Zertifikat für diesen Agent aufgelöst wird (DNS-Hostname oder IP-Adresse).
- Für den PPM-Server ist es erforderlich, dass für das von einem Agenten bereitgestellte Zertifikat die erweiterte Schlüsselnutzung für die Clientauthentifizierung festgelegt ist.
- Für den Agenten ist es erforderlich, dass das vom PPM-Server bereitgestellte Zertifikat für den PPM-Server aufgelöst wird (DNS-Hostname oder IP-Adresse).
- Für den Agenten ist es erforderlich, dass für das vom PPM-Server bereitgestellte Zertifikat die erweiterte Schlüsselnutzung für die Clientauthentifizierung festgelegt ist.

Der PPM-Server und der Agent sollten mit einer verlässlichen Zeitquelle synchronisiert werden, um sicherzustellen, dass die Zertifikate im Gültigkeitszeitraum liegen.

Für jeden bereitgestellten Agenten ist ein eindeutiges Zertifikat erforderlich.

Dateisystemunterstützung für Agenten

Datenträgeragenten führen die Verschlüsselung auf Datenträgerebene durch. Die Agenten vom Typ 'Datei mit Richtlinie' operieren entweder mit oder in unterstützten Dateisystemen des Hostbetriebssystems. Der Agent vom Typ 'Datei mit Richtlinie' und der Agent vom Typ 'Datenträger mit Richtlinie' unterstützen die folgenden Dateisysteme:

Linux-Server

- EXT3
- EXT4
- XFS (unter Red Hat / CentOS 6.5 oder neuer)
- NFS (NFSv3, NFSv4)

Windows-Server

- NTFS
- ReFS (unter Windows Server 2012 R2 oder neuer)

AIX

- JFS2

Netzkonfiguration

Informationen zu diesem Vorgang

MDE erfordert eine konsistente Netzverbindung zwischen MDE-PPM-Servern und Agenten. Es werden die Internetprotokolle IPv4 und IPv6 unterstützt. Die Verwendung von statischen IP-Adresszuordnungen oder von DHCP mit statischen Leases würde diese Anforderung erfüllen. Außerdem würde eine ordnungsgemäß arbeitende DNS-Infrastruktur oder die Nutzung von Hostnamen im gesamten Systemumfeld funktionieren.

Netzports

Funktion	Standardport	Konfigurierbar
Web	443	Ja
Datenbank	5432	Ja
Externes LDAP	Keiner	Ja
LDAP-Verzeichnisse	Keiner	Ja
E-Mail-Ereignisweiterleitung	Keiner	Ja
Syslog-Ereignisweiterleitung	Keiner	Ja

OVA-Konfiguration

Das bereitgestellte MDE-OVA (Open Virtualization Archive) ist mit dem Wert 1 für die Einstellung 'MaxAuthTries' vorkonfiguriert. Für eine erfolgreiche Authentifizierung über SSH bei der MDE-VM muss entweder die Einstellung von MaxAuthTries geändert werden (nicht empfohlen) oder auf den SSH-Clients muss die Einstellung 'PubkeyAuthentication' auf den Wert "no" über die Befehlszeile oder in der lokalen SSH-Clientkonfiguration gesetzt werden.

REST-Schnittstelle

MDE unterstützt eine vollständige programmgesteuerte REST-Schnittstelle. Die Rootadresse der REST-URL sieht wie folgt aus:

<https://<IP-Adresse der virtuellen Maschine>/rest/>

Kritischer Hinweis

Die REST-API bietet einem Administrator die Möglichkeit, erweiterte Funktionen auszuführen, die über die Webschnittstelle nicht zugänglich sind. Die REST-API kann potenziell in einer Weise verwendet werden, die einen Agenten in einen nicht unterstützten Status versetzt; daher sind Programmierkenntnisse über die REST-API wichtig.

Weitere Details finden Sie im Dokument zur REST-API-Spezifikation für IBM Multi-Cloud Data Encryption (MDE).

Kapitel 4. Produktinstallation

Installation vorbereiten

Der Installationsprozess für MDE umfasst drei Schritte:

1. Voraussetzungen
2. Verfügbares MDE Basis-OVA (Open Virtual Archive)
3. Unterstützter Hypervisor (VMware ESXi™)

Lizenzierung

MDE erfordert außer der in der Softwarelizenzvereinbarung bereitgestellten Lizenz keine weitere eindeutige Produktlizenz für die Ausführung oder Konfiguration von Agenten.

Verwaltung der MDE-OVA und der VM

Nach dem Bereitstellen der MDE-OVA (Open Virtualization Appliance), müssen Sie das System aktualisieren, um sicherzustellen, dass die aktuellen Sicherheitskorrekturen und Softwareversionen installiert sind.

Anmerkung: Sie sollten das System in regelmäßigen Abständen aktualisieren, um die Sicherheitskorrekturen und die neuesten Softwareversionen zu erhalten.

MDE installieren

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um die MDE-Software zu installieren:

Ersetzen Sie im Beispiel im Dateinamen 'ibm_sw_mde_X.x.x-XX.bin' die Buildnummer XX durch die Version der verfügbaren Software und führen Sie die Prozedur als Rootbenutzer aus.

Vorgehensweise

1. Stellen Sie das MDE-Basis-OVA in Ihrem Hypervisor bereit. In diesem Beispiel wird dies als "MDE-VM" bezeichnet.
2. Melden Sie sich als 'admin' an und legen Sie ein neues Kennwort fest.
Die MDE-VM verwendet PAM-Standardkriterien, die von einem Administrator konfiguriert werden können. Das PAM-Kennwort muss länger als 8 Zeichen sein und darf keine 5 Zeichen aus dem vorherigen Kennwort enthalten.
3. Notieren Sie sich die IP-Adresse der MDE-VM.
4. Laden Sie die Datei ibm_sw_mde_X.x.x-XX.bin in MDE mit SCP oder einer ähnlichen Dateiübertragungsmethode hoch.
5. Machen Sie die Bin-Datei ausführbar.

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

6. Führen Sie die Bin-Datei aus.

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

7. Wählen Sie 'English' aus und drücken Sie die Eingabetaste.
8. Lesen Sie die Lizenzseiten, navigieren Sie mit der Tabulatortaste zu <OK> und drücken Sie die Eingabetaste, um fortzufahren.
9. Wählen Sie <Yes> aus und drücken Sie die Eingabetaste, um die Lizenzvereinbarung zu akzeptieren.
10. Wenn die Extraktion abgeschlossen ist, drücken Sie die Eingabetaste auf <OK>, um zur Befehlszeile zurückzukehren.
11. Installieren Sie die RPMs als Rootbenutzer.

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

12. MDE ist jetzt installiert, jedoch noch nicht konfiguriert.

Anmerkung: Starten Sie die MDE-VM erst erneut, wenn die Konfiguration abgeschlossen ist.

Sprachkonfiguration

Informationen zu diesem Vorgang

MDE unterstützt mehrere Sprachen für die VM-Scripts und die grafische PPM-Benutzerschnittstelle (GUI). Sie müssen eine Einstellung für die Standardsprache konfigurieren, bevor Sie das Produkt ausführen.

Anmerkung: Sprachen werden über RPM in der MDE-VM installiert. Das Installationsprogramm wird mit einer integrierten Gruppe von Sprach-RPMs bereitgestellt. Weitere Sprachen können nach der Erstinstallation hinzugefügt werden. In diesem Fall kann ein Neustart des PPM-Service erforderlich sein, damit die Änderung wirksam wird.

Führen Sie die folgenden Schritte aus, um die Standardsprache zu konfigurieren:

Vorgehensweise

1. Führen Sie das Script 'spsd-langsetup' aus.

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

2. Zeigen Sie den aktuellen Standardsprachencode an. Wenn keiner festgelegt ist, ist das Feld leer.

Legen Sie den Standardsprachencode fest. Der aktuelle Standardwert ist:

3. Zeigen Sie die Liste der verfügbaren Sprachencodes an. (Die folgende Liste zeigt Beispiele, die in Ihrer Version des Produkts möglicherweise nicht verfügbar sind.)

```
Verfügbare Sprachencodes:  
en_US  
ja_JP  
ko_KR
```

4. Geben Sie den neuen Standardsprachencode ein.

Geben Sie den neuen Standardsprachencode ein: en_US
Der Standardsprachencode ist: en_US

5. Führen Sie das Script 'spsd-langsetup' erneut aus, um zu prüfen, ob der Standardsprachencode festgelegt ist.

Legen Sie den Standardsprachencode fest. Der aktuelle Standardwert ist: en_US

Datenbanksetup

Informationen zu diesem Vorgang

MDE unterstützt die Konfiguration einer internen oder einer externen Datenbank. In beiden Fällen müssen Sie MDE für die Kommunikation mit der konfigurierten Datenbank konfigurieren, bevor Sie MDE zum ersten Mal starten.

Um eine Datenbank für MDE zuzuordnen, müssen Sie die MDE-VM-Datei `/etc/spsd/db.props` ändern. Sie müssen diese Datei als Rootbenutzer bearbeiten.

Anmerkung: Die Verwendung des Scripts 'spsd-pgsetup' ändert automatisch die Datei 'db.props' mit den in die Eingabeaufforderung eingegebenen Werten.

Konfigurieren Sie die Dateieigenschaften für die Verbindung zur entsprechenden internen oder externen Datenbank wie nachfolgend beschrieben. Änderungen an Datenbankeigenschaften werden erst nach einem Neustart von MDE wirksam.

Kritischer Hinweis

Wenn Sie die Datei 'db.props' ändern, beachten Sie die folgenden Einschränkungen:

- **Keine Leerzeichen zwischen Eigenschaftsname und =**
- **Keine Leerzeichen zwischen = und Eigenschaftswert**

Interne Datenbank

Gegenwärtig unterstützt MDE PostgreSQL als interne Datenbank.

Interne Postgres-Datenbank

Das MDE-OVA (Open Virtualization Archive) wird mit einer vordefinierten PostgreSQL-Software geliefert. Zur Konfiguration der Datenbank für die Arbeit mit MDE führen Sie die folgenden Schritte aus:

1. Führen Sie das Script 'spsd-pgsetup' mit der Option "--local" aus.

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

Anmerkung: Die Option "--local" konfiguriert eine neue, leere Datenbank auf dem internen "lokalen" PostgreSQL-Server.

Nach der Anwendung dieser Einstellungen fahren Sie mit den Serverzertifikatseinstellungen fort. Wenn Sie planen, die Datenbank auf einem fernen Ziel einzurichten, fahren Sie mit 'Externe Datenbank' fort.

Externe Datenbank

Gegenwärtig ist PostgreSQL der einzige unterstützte externe Datenbankserver. Sie müssen sicherstellen, dass die folgenden Informationen bekannt sind, bevor Sie diesen Prozess ausführen:

- Der Name (oder die IP-Adresse) eines zugänglichen PostgreSQL-Datenbankservers.
- Die Portnummer, über die der obige PostgreSQL-Server empfangsbereit ist.
- Der Name einer vorhandenen Datenbank auf dem obigen Server.
- Der Name eines vorhandenen Benutzers, der als Eigner der obigen Datenbank definiert ist.
- Das Kennwort des obigen Datenbankbenutzers.

Führen Sie das Script 'spsd-pgsetup' aus, um die Datenbank für die Arbeit mit MDE zu konfigurieren. Alle in diesem Befehl bereitgestellten Werte sind beispielhaft:

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

Führen Sie das Script 'spsd-pgsetup' mit der Option "--upgrade" aus, um ein Upgrade der Datenbank auf das letzte Schema durchzuführen.

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

Anmerkung: Die Ausführung des Scripts 'spsd-pgsetup' mit der Option 'upgrade' stellt sicher, dass die Datenbanktabellen ordnungsgemäß für die aktuelle Version von PPM konfiguriert sind.

Nach dem Konfigurieren dieser Einstellungen fahren Sie mit den Einstellungen für Serverzertifikate fort.

Einstellungen für Serverzertifikate

Keystore, Truststore und Zertifizierungsstelle (CA)

Mithilfe von Zertifikaten wird eine sichere Kommunikationssitzung zwischen dem Management-Server (PPM) und den Agenten sowie den Web-Browsern eingerichtet. Für PPM ist es erforderlich, dass alle Zertifikate durch eine Zertifizierungsstelle (CA, Certificate Authority) signiert sind. Die Zertifizierungsstelle richtet eine Vertrauensbasis ein, mit deren Hilfe alle Teilnehmer an der Kommunikationssitzung die Identität der anderen Partei verifizieren können.

- Das CA-signierte Zertifikat wird zusammen mit dem entsprechenden Schlüssel in einem Java-Keystore kombiniert.
- Das Zertifikat (oder Zertifikatsbundle) von der Zertifizierungsstelle, das zum Signieren der Agentenzertifikate verwendet wird, muss zum PPM-Truststore hinzugefügt werden.
- Alle drei Komponenten (Keystore, Truststore und CA-Zertifikatsbundle) werden im nachfolgenden Prozess zur PPM-Zertifikatskonfiguration verwendet.

In Anhang B, „Beispielzertifikate einer Zertifizierungsstelle (CA)“, auf Seite 89 finden Sie ein Beispiel für die Verarbeitung des CA-Zertifikats.

Der Webzertifikatskeystore des Servers und der Webzertifikatstruststore werden über das Setup-Script 'spsd-certsetup' konfiguriert, das sich im Verzeichnis /opt/securityfirst/spsd/bin der MDE-VM befindet.

Das folgende, in **Fett** hervorgehobene Beispiel zeigt Eingaben zur Konfiguration des Keystores, des Truststores und des CA-Bundles für Agenten:

```
$ 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
```

Hinweis

Serverzertifikatskomponenten wie Keystore, Truststore und CA-Bundle werden nicht bereitgestellt und müssen mithilfe des Setup-Scripts generiert und in die MDE-VM hochgeladen werden. Wenn eine Common Access Card (CAC) für die Authentifizierung verwendet wird, müssen PKI-Einstellungen aktiviert werden.

PKI-Infrastruktur - Einstellungen

Informationen zu diesem Vorgang

Durch die PKI-Konfiguration (PKI - Public Key Infrastructure) kann PPM eine zweite Methode der PPM-Benutzerauthentifizierung bereitstellen. Bei entsprechender Konfiguration akzeptiert PPM Clientzertifikate als Authentifizierungsmethode für Web- und REST-Sitzungen.

Dieses Zertifikat muss von einer Zertifizierungsstelle (CA) signiert sein, der PPM vertraut. PPM validiert das Zertifikat nach den Regeln, die im Script 'spsd-certsetup' definiert sind.

Ein Beispiel für die Eingabe in **Fettdruck**:

```
$ 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
```

Hinweis

PKI kann in derselben Scriptausführung wie der Keystore, der Truststore und das CA-Bundle konfiguriert werden. Zu Demonstrationszwecken wird dieser Schritt hier separat behandelt.

Nach der Installation von MDE, der Konfiguration einer Datenbank, dem Hinzufügen von Zertifikaten und der optionalen Einrichtung von PKI können Sie die MDE-VM jetzt erneut starten.

Starten und erste Anmeldung

Informationen zu diesem Vorgang

Nach Abschluss der Bereitstellung und Konfiguration starten Sie den MDE-Server erneut oder starten nur den Service "spsd" über die MDE-Konsole, um die Web-GUI zu starten. Sie müssen die IP-Adresse oder den Hostnamen der virtuellen Maschine über die VM-Konsole oder den Host-Hypervisor abrufen.

Öffnen Sie einen unterstützten Web-Browser und geben Sie die IP-Adresse oder den Hostnamen als URL ein, um zur MDE-Anmeldeseite zu gelangen.

```
https://<IP-Adresse des MDE-Servers>
```

An diesem Punkt können Sie die Spracheinstellung über die verfügbare Liste der unterstützten Sprachen ändern.



Please Sign In

User name

Password

Directory

Login

Die Standardberechtigungs-nachweise sind folgende:

Benutzername: admin
Kennwort: admin

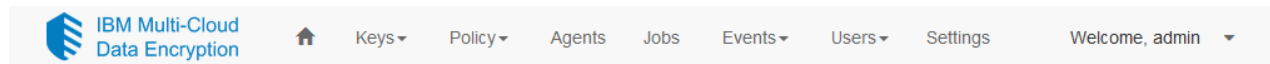
Hinweis

- Die Standardberechtigungs-nachweise müssen bei der ersten Anmeldung geändert werden.
- MDE unterstützt die meisten Versionen der Web-Browser Firefox, Chrome, Microsoft Edge und Internet Explorer.
- Bei Verwendung der PKI-Clientauthentifizierung kann die Anmeldeseite übersprungen und direkt zum Dashboard navigiert werden.

Kapitel 5. Grafische Benutzerschnittstelle (GUI) von MDE

Grundlegende Navigation im Produkt

MDE enthält ein Navigationsmenü im oberen Bereich der Seiten. Einige Menüelemente enthalten Untermenülisten. Klicken Sie auf das gewünschte Menüelement, um zu der entsprechenden Seite zu navigieren oder die Untermenüliste anzuzeigen.



- **Symbol für Homepage:** Ein Link zur Startseite des Produktdashboards.
- **Schlüssel:** Ein Menü, das schlüsselbezogene Untermenüseitenlinks enthält: Externe Keystores und Verwaltungste Schlüsselschlüssel.
- **Richtlinie:** Ein Menü, das richtlinienbezogene Untermenüseitenlinks enthält: Datentypen, Pfadgruppen und Selektoren.
- **Agenten:** Ein Link zur Seite 'Agenten'.
- **Jobs:** Ein Link zur Seite 'Jobs'.
- **Ereignisse:** Ein Menü, das ereignisbezogene Untermenüseitenlinks enthält: Weiterleitung und Protokolle.
- **Benutzer:** Ein Menü, das benutzerbezogene Untermenüseitenlinks enthält: Konten und LDAP-Verzeichnisse.
- **Einstellungen:** Ein Link zur Seite 'Einstellungen'.

Hinweis

MDE unterstützt eine rollenbasierte Zugriffssteuerung (RBAC), sodass je nach der Rolle des angemeldeten Benutzers einige Navigationselemente nicht verfügbar sind. Das heißt, dass einige Navigationselemente möglicherweise nicht für alle Benutzer mit Verwaltungsaufgaben verfügbar sind.

Produktdashboard

Die Startseite des Produkts ist die Hauptzielseite des Dashboards. Sie ist dazu gedacht, eine Zusammenfassungsansicht über den aktuellen Status der letzten Ereignisse für den angemeldeten Administrator bereitzustellen. Die Startseite enthält die zuletzt empfangenen Ereignisse, Ereignistrends und andere zusammengefasste Daten.

Automatische Vervollständigung in Textfeldern

In der gesamten Benutzerschnittstelle befinden sich Texteingabefelder. In einigen Texteingabefeldern werden Entsprechungen zur automatischen Vervollständigung für die bereits eingegebenen Zeichen angezeigt. In diese Felder müssen mehrere Zeichen eingegeben werden, bevor ein Vorschlag zur automatischen Vervollständigung eingeblendet wird.

Zu beachtende Benachrichtigungen

Nach der ersten Anmeldung wird im Kopf der Benutzerschnittstelle ein farbiges Banner angezeigt, das auf Probleme hinweist, die Aufmerksamkeit erfordern.

Durch Klicken auf das Banner wird der Administrator zur Seite “Probleme” geführt, auf der einzelne Elemente angezeigt werden.

Home
 >
 Issues

▶ 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

Durch Erweitern eines Elements werden Details zur Behebung des Problems eingeblendet.

▼ 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

Wenn alle offenen Probleme behoben wurden, wird das Banner nicht angezeigt. Allerdings kann der Administrator das Banner für die aktuelle Seite ausblenden.

Hinweis

Es können neue Bedingungen auftreten, die neue Probleme, die “Aufmerksamkeit erfordern”, erstellen, sodass das Banner erneut angezeigt wird.

Erweiterte Eigenschaften

Der Produktadministrator ist berechtigt, erweiterte Eigenschaften zu konfigurieren, die das Produktverhalten definieren. Auf die erweiterten Eigenschaften kann über die Seite 'Einstellungen' zugegriffen werden. Diese Eigenschaften gelten entweder für die lokale Instanz oder potenziell für das gesamte MDE-Umfeld, wenn Hochverfügbarkeitsfunktionalität (HA) oder die Multi-Tenant-Funktionalität genutzt wird.

Home
 >
 Settings

Advanced Properties

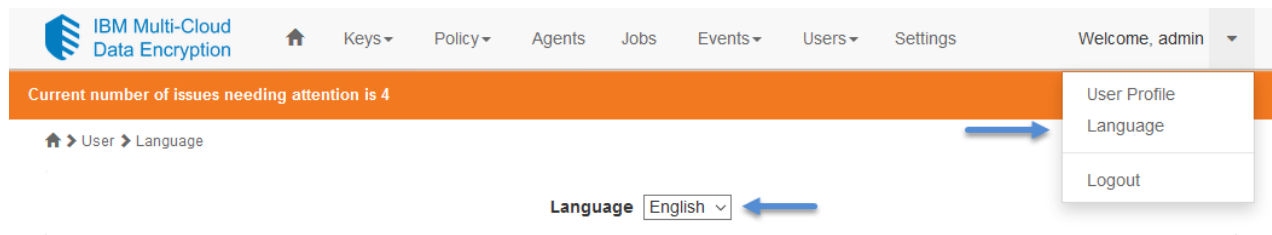
Property	Value	Description	Actions
com.securityfirstcorp.atlantis.bundles.haas.iterations	600000	Number of iterations used by REST API token hashing algorithm	<div>Edit</div>
com.securityfirstcorp.atlantis.jobs.requiredApprovers	1	Number of approvals required to run a job	<div>Edit</div>
com.securityfirstcorp.atlantis.jobs.requiredBuffers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

Zur Bearbeitung einer Eigenschaft muss der Produktadministrator auf die Schaltfläche “Bearbeiten” klicken. Nach Abschluss der gewünschten Änderungen klickt er auf die Schaltfläche “Speichern”. Dadurch wird ein Job erstellt.

GUI-Spracheinstellung

Über die grafische Benutzerschnittstelle (GUI) können Sie eine der unterstützten Sprachen ändern, die während der Erstinstallation installiert wurden, wenn Sie die entsprechende Auswahl auf der Anmeldeseite oder Startseite angeben.

- **Anmeldeseite:** In der rechten oberen Ecke der Seite. Klicken Sie auf das Pulldown-Menü, um eine Liste der unterstützten Sprachen einzublenden.
- **Homepage:** Wählen Sie im Pulldown-Menü in der rechten oberen Ecke die Option “Sprache” aus, um eine Liste der unterstützten Sprachen einzublenden.

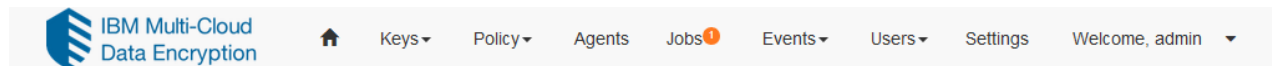


Die in der grafischen Benutzerschnittstelle angezeigte Sprache wird durch die folgende Hierarchie festgelegt (erste vorhandene Einstellung wird verwendet):

1. Der Wert des Sprachencookies, das über die Benutzerschnittstelle von PPM gesetzt wurde.
2. Der Wert der Spracheinstellung im Browser des Benutzers.
3. Der Wert des Sprachencodes, der über die PPM-Befehlszeilenschnittstelle 'script-langsetup' festgelegt wurde.
4. Das erste gefundene installierte PPM-Sprachenpaket.

Kapitel 6. Jobs

MDE nutzt ein Jobsystem, um die Genehmigung und den zeitlichen Ablauf für die Ausführung von Tasks zu verwalten. Viele Funktionen verwenden das Jobsystem, um auf eine Genehmigung zu warten, bevor eine Bestätigung erfolgt. Wenn ein Job erstellt wird, wird ein neuer Job der Liste auf der Seite 'Jobs' hinzugefügt.



Administratoren haben für jeden Job die Optionen, ihn zu genehmigen, ihn abzulehnen oder auf ihn zu verzichten. Jeder Administrator kann die Aktion nur einmal pro Job ausführen.

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

Jobbeschreibungen

Job	Beschreibung	Kategorie	Rolle
Erweiterte Eigenschaft-ten	Erweiterte Eigenschaft ändern	Produktmanagement	Produktadministrator
Keystore ändern	Position/Details des Keystores für die Richtliniendurchsetzung ändern	Produkteinstellungen	Produktadministrator
Schlüsselrotation	Gruppe von Schlüsseln im Agentenumfeld rotieren	Schlüsselmanagement	Sicherheitsadministrator
Schlüsselwiderruf	Gruppe von Schlüsseln aus dem Agentenumfeld widerrufen	Schlüsselmanagement	Sicherheitsadministrator
Schlüsselschredderung	Gruppe von Schlüssel permanent aus dem Agentenumfeld entfernen, sodass die Daten verloren sind.	Schlüsselmanagement	Sicherheitsadministrator
Agent hinzufügen	Neuen Agenten im System bereitstellen und hinzufügen	Agentenmanagement	Sicherheitsadministrator
Agent löschen	Agenten aus dem MDE-Management entfernen	Agentenmanagement	Sicherheitsadministrator
Agent ändern	Informationen zu einem Agenten ändern	Agentenmanagement	Sicherheitsadministrator
Richtlinienaktualisierung	Richtlinie ändern, die einem Agenten zugeordnet ist	Agentenmanagement	Sicherheitsadministrator

Neuen Benutzer mit Verwaltungsaufgaben erstellen	Neuen MDE-Administrator erstellen	Management von Benutzern mit Verwaltungsaufgaben in MDE	Produktadministrator
Benutzer mit Verwaltungsaufgaben löschen	MDE-Administrator entfernen	Management von Benutzern mit Verwaltungsaufgaben in MDE	Produktadministrator
Rolle für Benutzer mit Verwaltungsaufgaben hinzufügen	Rolle einem MDE-Administrator hinzufügen	Management von Benutzern mit Verwaltungsaufgaben in MDE	Produktadministrator
Rolle für Benutzer mit Verwaltungsaufgaben entfernen	Rolle von einem MDE-Administrator entfernen	Management von Benutzern mit Verwaltungsaufgaben in MDE	Produktadministrator
Kennwort für Benutzer mit Verwaltungsaufgaben ändern	Kennwort eines MDE-Administrators ändern	Management von Benutzern mit Verwaltungsaufgaben in MDE	Produktadministrator
Status für Benutzer mit Verwaltungsaufgaben ändern	MDE-Konto für Benutzer mit Verwaltungsaufgaben aktivieren oder inaktivieren	Management von Benutzern mit Verwaltungsaufgaben in MDE	Produktadministrator
Verzeichnisregistrierung	LDAP-Serververzeichnis für MDE-Benutzer mit Verwaltungsaufgaben konfigurieren	Management von Benutzern mit Verwaltungsaufgaben in MDE	Produktadministrator
Verzeichnislöschung	LDAP-Serververzeichnis aus MDE entfernen	Management von Benutzern mit Verwaltungsaufgaben in MDE	Produktadministrator
Verzeichnisaktualisierung	LDAP-Serververzeichnis ändern	Management von Benutzern mit Verwaltungsaufgaben in MDE	Produktadministrator

Genehmigung durch mehrere Administratoren

Die erforderliche Anzahl von Genehmigern und Ablehnern kann in MDE konfiguriert werden. Standardmäßig ist MDE für die Genehmigung durch einen einzelnen Administrator konfiguriert. Es wird ausdrücklich empfohlen, zwei oder mehr Administratoren für die Jobgenehmigung erforderlich zu machen. Bei Genehmigung durch mehrere Administratoren wird verhindert, dass ein einzelner Administrator eine Änderung in MDE selbst oder an verwalteten Agenteninstanzen durchführt.

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

Kritischer Hinweis

Die Anzahl der Benutzer mit Verwaltungsaufgaben (Administratoren) muss größer-gleich der Anzahl der erforderlichen Genehmigungen bzw. erforderlichen Ablehnungen für einen Job sein. Stellen Sie sicher, dass die erforderliche Anzahl von Benutzern mit Verwaltungsaufgaben vorhanden ist, bevor diese Werte geändert werden.

Die Schwellenwerte für die Genehmigung oder Zurückweisung können je nach Jobtyp überschrieben werden. Alle durch das System definierte Jobtypen (mit Ausnahme des Jobs 'Änderung von Produkteigen-

schaft') verfügen unter "Erweiterte Eigenschaften" sowohl über einen Schwellenwert für die Genehmigung als auch einen Schwellenwert für die Zurückweisung, die, wenn sie festgelegt sind, den Systemstandard überschreiben. Sobald eine Eigenschaft festgelegt ist, kann diese Einstellung nicht rückgängig gemacht werden.

Der Job 'Änderung von Produkteigenschaft' ist der einzige Jobtyp ohne Schwellenwerte für Genehmigung und Zurückweisung, da dieser die Änderung der erweiterten Eigenschaften steuert. Für diesen Job werden diese Schwellenwerte immer der höhere Wert des Systemstandards oder der höchste Überschreibungswert sein, der für alle anderen Jobtypen definiert ist. Durch diese Aktion wird sichergestellt, dass kein anderer Schwellenwert für einen Jobtyp durch eine Eigenschaftsänderung gefährdet werden kann.

Jobgenehmigung

Zum Genehmigen eines Jobs muss ein Administrator mit den entsprechenden Berechtigungen zur Seite 'Jobs' navigieren, den betreffenden Job herausuchen und auf die Schaltfläche "Genehmigen" klicken. Wenn die erforderliche Anzahl von Administratorgenehmigungen erreicht ist, wird der Job ausgeführt.

Jobablehnung

Zum Ablehnen eines Jobs muss ein Administrator mit den entsprechenden Berechtigungen zur Seite 'Jobs' navigieren, den betreffenden Job herausuchen und auf die Schaltfläche "Ablehnen" klicken. Wenn die erforderliche Anzahl von Administratorablehnungen erreicht ist, wird der Job dauerhaft abgebrochen.

Jobverzicht

Durch Verzichten auf einen Job wird angegeben, dass ein Administrator den Job gesehen hat, diesen jedoch weder genehmigen noch ablehnen möchte. Ein Verzicht lässt vielleicht am besten als Prüfposition ("Audit") beschreiben. Er verhindert, dass der Administrator zu einem späteren Zeitpunkt eine andere Position für denselben Job auswählt.

Jobinformationen

Jeder Job in MDE hat unterschiedliche Informationen, die ihn beschreiben. Durch Klicken auf die Schaltfläche "Info anzeigen" können jobspezifische Informationen angezeigt werden. Darüber hinaus werden alle Aktionen (Genehmigen, Ablehnen, Verzichten), die von anderen Administratoren für den Job ausgeführt wurden, zusammen mit dem Benutzernamen des Administrators, der die Aktion ausgeführt hat, angezeigt.

User Create	Done	2017-09-22T23:22:36Z	2017-09-22T23:22:36Z	2017-09-22T23:22:36Z		Hide Info
User	Time	Actions	Required Approvals	Required Rejections	Notes	
admin	2017-09-22T23:22:35Z	Approve	1	1		
Job Properties						
User		ProductAdmin				

Kapitel 7. Management von Benutzern mit Verwaltungsaufgaben in MDE

Rollen für Benutzer mit Verwaltungsaufgaben

MDE nutzt ein flaches, auf statischen Rollen basierendes Zugriffssteuerungsdesign (RBAC). Bestimmte Funktionen in MDE erfordern bestimmte Berechtigungen. Der gesamte Satz der MDE-Berechtigungen ist in zwei verschiedene Rollen gruppiert: Produktadministrator und Sicherheitsadministrator. Jeder Rolle können zu jeder Zeit weitere Administratoren hinzugefügt werden.

Produktadministratorrolle

Der Produktadministratorrolle sind die Berechtigungen anvertraut, die zur Konfiguration und Verwaltung des MDE-Produkts erforderlich sind.

Sicherheitsadministratorrolle

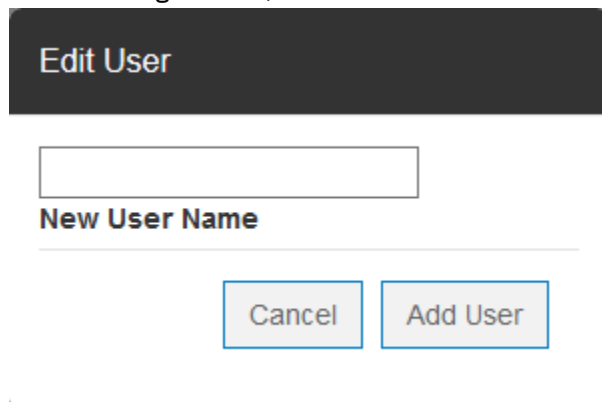
Der Sicherheitsadministratorrolle sind die Berechtigungen anvertraut, die zur Bereitstellung und Verwaltung der Agenten erforderlich sind. Diese Berechtigungen umfassen zum Beispiel Richtliniendefinitionen und -spezifikationen, das Schlüsselmanagement, Datentypdefinitionen, das Agentenmanagement, die Konfiguration externer Keystores sowie die externe LDAP-Konfiguration externer Gruppen für Richtlinien.

Management von Benutzern mit Verwaltungsaufgaben

Ein Produktadministrator besitzt die Berechtigungen, die erforderlich sind, um andere Benutzer mit Verwaltungsaufgaben (Administratoren) in MDE hinzuzufügen, zu ändern und zu entfernen.

Neuen Benutzer mit Verwaltungsaufgaben hinzufügen

Beim Hinzufügen eines neuen Benutzers mit Verwaltungsaufgaben (Administrator) wird ein Produktadministrator aufgefordert, den Benutzernamen des neuen Benutzers mit Verwaltungsaufgaben einzugeben.



Edit User

New User Name

Cancel Add User

Geben Sie einen eindeutigen Benutzernamen ein. Es wird ein Job erstellt, um diesen Benutzer mit Verwaltungsaufgaben zu MDE hinzuzufügen.

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> <div> <div>Type : User Create</div> <div>Frequency : Once</div> <div>Starts : Upon approval</div> </div> <div> <div>Job Properties</div> <div>User</div> <div>test</div> </div>					

Damit der Benutzer erstellt wird, muss die erforderliche Anzahl von Produktadministratoren den Job genehmigen.

Ein neu hinzugefügter Benutzer mit Verwaltungsaufgaben wird mit einem abgelaufenen Kennwort und ohne definierte Rolle erstellt. Ein Produktadministrator muss das Anfangskennwort, die Rolle und den Status bearbeiten. Jede diese Aktualisierungen generiert einen Job. Die Jobs müssen genehmigt werden, bevor der neue Benutzer mit Verwaltungsaufgaben in MDE aktiv werden kann.

Kennwort für einen Benutzer mit Verwaltungsaufgaben bearbeiten

Zum Bearbeiten des Kennworts eines Benutzers mit Verwaltungsaufgaben (Administrator) navigieren Sie zu dem entsprechenden Benutzer und wählen die Schaltfläche “Kennwort bearbeiten” aus. Ein Dialog zur Kennworteingabe wird angezeigt.

The screenshot shows a dialog box titled "Edit User". It contains two input fields for "New Password" and "Confirm Password". Below these fields are "Cancel" and "Save" buttons. A red error message "Password Invalid" is displayed, followed by a detailed password policy: "Passwords must be at least 8 characters, may not match any of the last 8 used passwords and must contain characters from three of the following five categories (click for a listing of each):". The categories listed are: Upper case letters, Lower case letters, Numbers, Symbols, and Other Unicode characters. At the bottom, it states "Password and Password Confirm must match".

Geben Sie ein Kennwort ein, das den angegebenen Regeln entspricht. Speichern Sie nach der Eingabe die Änderungen. Es wird ein Job erstellt.

Damit die Kennwortänderung wirksam wird, muss die erforderliche Anzahl von Benutzern mit Verwaltungsaufgaben den Job genehmigen.

Anmerkung: Der neu hinzugefügte Administrator wird bei seiner ersten Anmeldung dazu aufgefordert, sein Kennwort zu ändern.

Rolle für Benutzer mit Verwaltungsaufgaben bearbeiten

Zum Bearbeiten der Rolle eines Benutzers mit Verwaltungsaufgaben suchen Sie die Benutzerzeile und wählen die Schaltfläche “Rollen bearbeiten” aus. Es werden Kontrollkästchen eingeblendet.

Der Benutzer mit Verwaltungsaufgaben, der eine Bearbeitung vornimmt, kann die gleiche Rolle, die er selbst hat, anwenden. Zum Beispiel kann der integrierte Benutzer “admin”, der der erste Benutzer ist, die Rolle des Produktadministrators und die Rolle des Sicherheitsadministrators anwenden. Ein Benutzer, der die gleichen Rollen hat, kann dies selbst ebenfalls tun.

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"/>
--------------	----------	---	--	----------------------	---

Wählen Sie die gewünschten Rollen aus und klicken Sie auf die Schaltfläche “Änderungen speichern”. Es wird ein Job erstellt.

Damit die Rollenänderung wirksam wird, muss die erforderliche Anzahl von Benutzern mit Verwaltungsaufgaben den Job genehmigen.

Status für Benutzer mit Verwaltungsaufgaben bearbeiten

Zum Bearbeiten des Status eines Benutzers mit Verwaltungsaufgaben navigieren Sie zu dem betreffenden Benutzer und wählen die Schaltfläche “Status bearbeiten” aus. Eine Dropdown-Liste für die Statuseingabe wird eingeblendet.

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

Statuswerte: Aktiviert, Inaktiviert und Gesperrt.

- **Aktiviert:** Der Benutzer mit Verwaltungsaufgaben ist aktiv und kann Aktionen ausführen.
- **Inaktiviert:** Der Benutzer mit Verwaltungsaufgaben ist inaktiv und kann keine Aktionen ausführen.
- **Gesperrt:** Der Benutzer mit Verwaltungsaufgaben ist gesperrt und kann keine Aktionen ausführen.

Wählen Sie den gewünschten Status aus und klicken Sie auf “Speichern”. Es wird ein Job zur Änderung des Benutzerstatus erstellt.

Damit die Statusänderung wirksam wird, muss die erforderliche Anzahl von Benutzern mit Verwaltungsaufgaben den Job genehmigen.

Benutzer mit Verwaltungsaufgaben entfernen

Zum Entfernen eines Benutzers mit Verwaltungsaufgaben (Administrators) suchen Sie die Zielbenutzerzeile und klicken Sie auf die Schaltfläche “Löschen”. Es wird ein Job gestartet, um den Benutzer aus MDE zu entfernen. Diese Aktion kann nur von einem Benutzer mit der Produktadministratorrolle ausgeführt werden.

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

Damit der Benutzer entfernt wird, muss die erforderliche Anzahl von Benutzern mit Verwaltungsaufgaben den Job genehmigen.

Kritischer Hinweis

- Das Entfernen eines Benutzers mit Verwaltungsaufgaben ist eine Aktion mit permanentem Ergebnis.
- Es müssen ausreichend Benutzer mit Verwaltungsaufgaben beibehalten werden, um die Bedingung der erforderlichen Jobgenehmigungen erfüllen zu können. Siehe Abschnitt “Genehmigung durch mehrere Administratoren”.
- Jobs können nicht erfolgreich akzeptiert werden, wenn nicht ausreichend Benutzer mit Verwaltungsaufgaben vorhanden sind.

Benutzerkontosperrung

Um das System und Benutzerkonten vor Brute-Force-Angriffen auf Kennwörter zu schützen, werden Benutzerkonten nach zehn (10) aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen gesperrt. Das

entsprechende Benutzerkonto bleibt so lange gesperrt, bis das Konto wieder explizit aktiviert (siehe Abschnitt zum Bearbeiten des Status des Benutzers mit Verwaltungsaufgaben) oder der Server-Service erneut gestartet wird.

Hinweis

- Um den Server-Service erneut zu starten, führen Sie **systemctl restart spsd** in der Konsole der virtuellen Maschine aus.
- Die Kontosperrung erfolgt auf Pro-Server-Basis. Ein Konto, das auf einem Server in einem Cluster gesperrt ist, ist nicht automatisch auf den anderen Servern im Cluster gesperrt.
- Der Schwellenwert für die Kontosperrung kann nicht vom Benutzer konfiguriert werden.

LDAP-Verzeichnisliste

Ein Produktadministrator kann LDAP-Verzeichnisse für das MDE-Benutzermanagement konfigurieren. LDAP-Verzeichnisse können hinzugefügt, geändert oder gelöscht werden. Jede Aktion erstellt einen Job zur Genehmigung, bevor sie wirksam wird.

Beim Hinzufügen/Ändern eines LDAP-Verzeichnisses sind die folgenden Einstellungen verfügbar:

- **Verzeichnis-ID:** Die Identität des LDAP-Verzeichnisses.
- **Typ:** Eine Dropdown-Liste mit Optionen für LDAP oder Active Directory.
- **Binde-DN:** Der vollständige Distinguished Name (DN), der für die Bindung an den LDAP-Server verwendet wird.

Beispiel für die Syntax einer Binde-DN:

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

Anmerkung: Wenn Sie den Typ 'Active Directory' auswählen, wird der Abschnitt 'Binde-DN' ausgeblendet dargestellt, da diese Informationen nicht erforderlich sind.

- **Host:** Die IP-Adresse oder der Hostname des LDAP-Servers.
- **Port:** Der Port des LDAP-Servers.
- **Sicher:** Die Angabe einer sicheren oder nicht sicheren LDAP-Verbindung.
- **Aktionen:** Wählen Sie 'Speichern' oder 'Abbrechen' aus.

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>

Benutzerquelle

MDE kann intern und extern definierte Benutzer gleichzeitig unterstützen. Für extern definierte Benutzer wird ein Wert in der Spalte "Verzeichnis" der Benutzerliste angezeigt. Für intern definierte Benutzer bleibt dieses Feld leer.

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>

Kapitel 8. Ereignisse

MDE enthält ein System für Ereignisaggregation und -weiterleitung. Das System aggregiert Ereignisse aus verwalteten Agenten zusammen mit intern generierten Ereignissen und speichert die Ereignisse in einem internen Ereignisprotokoll. Darüber hinaus kann es so konfiguriert werden, dass Ereignisse an einen oder mehrere Empfänger weitergeleitet werden.

Ereignisprotokoll

Das MDE-Ereignisprotokoll kann angezeigt werden, indem das Menüelement 'Ereignisse' in der Menüleiste der höchsten Ebene ausgewählt wird.

[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

Diese Seite zeigt alle Ereignisse in einer einzelnen sequenziellen Liste an. Jedes Ereignis hat eine Folgennummer (Sequenz), eine ID, eine Nachricht, einen Typ, eine Wertigkeit, eine Empfangszeitmarke und eine Quelle, wie nachfolgend beschrieben:

- **Folgennummer (Sequenz):** Eine Nummer, die in der Reihenfolge, in der das Ereignis empfangen wird, zugeordnet wird. Sie ist eindeutig (selbst wenn dasselbe Ereignis wiederholt wird) und wird im Zeitverlauf inkrementiert.
- **ID:** Eine eindeutige Kennung des Ereignisses. Mehrere Instanzen desselben Ereignisses haben eine gemeinsame ID.
- **Nachricht:** Ein beschreibender Text, der die Bedingung angibt, die das Ereignis ausgelöst hat. Einige Ereignisse unterstützen eine Variableneinfügung, sodass auch bei gleicher Ereignis-ID der Text geringfügig abweichen kann.
- **Typ:** Beschreibt, ob das Ereignis durch eine Systemaktion oder eine Benutzeraktion verursacht wurde. Der Typ ist wie folgt:

- **SYSTEM:** Ereignisse, die aus einer automatisierten MDE-Aktion stammen.
- **AUDIT:** Ereignisse, die aus einer Benutzeraktion stammen.
- **Wertigkeit:** Relative Angabe des erforderlichen Aufmerksamkeitsgrads für das Ereignis. Folgende Kategorien sind für die Wertigkeit verfügbar:
 - **INFO:** Keine Aktion erforderlich, nur zu Informationszwecken.
 - **WARN:** Keine sofortige Aktion erforderlich; eine Überwachung der Bedingung wird empfohlen.
 - **KRITISCH:** Sofortige Aktion erforderlich.
- **Zeitmarke:** Der Zeitpunkt in koordinierter Weltzeit (UTC-Format), zu dem das Ereignis aufgetreten ist.
- **Quelle:** Der Hostname oder die IP-Adresse des Systems (Agent oder MDE), von dem Ereignis stammt.

Die Größe des MDE-Ereignisprotokolls kann über die erweiterten Einstellungen konfiguriert werden. Wenn die festgelegte Größenbegrenzung erreicht wird, werden jeweils die ältesten Ereignisse aus dem Protokoll entfernt, wenn neue Ereignisse empfangen werden.

Ereignisdetails

Ein Ereignis kann über weitere Argumente verfügen, die nicht Teil der Ereignisnachricht sind. Falls vorhanden, wird für das Ereignis in der Nachrichtenspalte des Ereignisprotokolls ein Link "Details" angezeigt. Durch das Klicken auf diesen Link werden die erweiterten Argumente angezeigt.

34	PS00140002	Agent 1 logged off. reason code 1006.	Details		2018-04-10T15:02:05Z	localhost
33	DEC02014	Read/write denied for user3 on /home/data/	Details	Absolute process path: Decision: Deny Group name: user3 Operation: Read or Write	2018-04-10T15:01:19Z	cos5-file
32	DEC02010	Read denied for user4 on /home/data/	Details		2018-04-10T15:01:19Z	cos5-file
31	DEC02011	Write permitted for user1 on /home/development/	Details	AUDIT	INFO	2018-04-10T15:01:19Z

Ereignisexport

MDE ermöglicht einem Administrator über die Schaltfläche 'CSV exportieren' auf der Seite 'Ereignisse' den Export der Ereignisliste in ein CSV-Dateiformat.

🏠 > Events > Logs

☐ Show Redacted Events

Reload Export CSV

Durch Klicken auf die Schaltfläche "CSV exportieren" wird die Ereignisdatei auf die Clientmaschine heruntergeladen. Jede Zeile in der Ereignisdatei stellt ein Ereignis aus dem Protokoll dar.

Die Ereignisdatei enthält die folgenden Spalten: Ereignisfolgennummer, Ereignis-ID, Flag 'Redigiert', Ereignisnachrichtenzeichenfolge (mit ausgeschlossenen Argumenten), Ereignistyp, Ereigniswertigkeit, Ereignisargumente, Ereigniszeitmarke und Ereignisquelle.

Ereignisweiterleitung

Jedes empfangene Ereignis wird an jeden konfigurierten Ereignisempfänger weitergeleitet. Ereignisse werden parallel nach Einfügung in das interne Ereignisprotokoll weitergeleitet.

Ein Produkt- oder Sicherheitsadministrator kann die Ereignisempfänger des Produkts ändern. Nach der Konfiguration wird jedes Ereignis, das von MDE erstellt oder empfangen wird, an die Empfänger weitergeleitet. Der unterstützte Empfängertyp ist 'Syslog'.

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			

MDE unterstützt außerdem mehrere Formate für die weitergeleiteten Ereignisse. Unterstützte Formate: Log Event Extended Format (LEEF), Common Event Format (CEF) und Ereignismodelle von Cloud Auditing Data Federation (CADF).

Ereignisargumente

Neben der normalen Ereignisnachrichtenzeichenfolge werden Ereignisargumente als Schlüssel/Wert-Parameter gesendet. Diese Parameter werden durch die verknüpfte Zeichenfolge des Präfix mit "spx" und dem Argumentname angegeben. Wenn beispielsweise ein Ereignis einen Benutzernamen enthält, lautet das Schlüssel/Wert-Paar der Zeichenfolge "spxuser=user1".

Agentenereignisse

MDE aggregiert System- und Auditereignisse aus jedem verwalteten (und verbundenen) Agenten. Diese Ereignisse werden im MDE-Ereignisprotokoll angezeigt und an alle konfigurierten Ereignisempfänger weitergeleitet.

Hinweis

Es wird dringend empfohlen, NTP (Network Time Protocol) für die Koordination der Systemzeiten für MDE, externe Datenbanken und alle Agenten zu nutzen. Dadurch wird die ordnungsgemäße Reihenfolge von Ereignis-/Auditprotokollzeitmarken sichergestellt.

Zuverlässige Ereignisse

Die Ereignisse, die von einem einzelnen Agenten an MDE gesendet werden, werden in Echtzeit verarbeitet. Dies stellt sicher, dass ein Ereignis, das verpasst wird, von MDE erneut vom Agenten angefordert und in das Ereignisprotokoll in der richtigen Reihenfolge (Sequenz) eingefügt wird.

Kapitel 9. Management von Richtliniendurchsetzungsschlüsseln

Ein Sicherheitsadministrator kann Richtliniendurchsetzungsschlüssel für sichere Speicherung in MDE definieren. Diese Schlüssel können Datentypen und Datenträgern zugeordnet werden, um Daten zu schützen und eine Verschlüsselungszugriffssteuerung bereitzustellen.

🏠 > 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

Schlüssel hinzufügen

Beim Hinzufügen eines neuen Schlüssels muss ein eindeutiger Name eingegeben werden. Schlüsselnamen sind nicht von der Groß-/Kleinschreibung abhängig. Der Schlüsselwert wird nicht zugänglich gemacht und kann von einem Benutzer nicht bearbeitet werden. Das Feld für Hinweise ist optional.

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

Hinweis

Schlüsselnamen können geändert werden, jedoch kann der tatsächliche Schlüsselwert von einem Benutzer nicht geändert werden.

Schlüssel können auf der Seite 'Schlüssel' oder beim Ausführen des Assistenten für das Erstellen von Agenten erstellt werden. Alle vom System definierten Schlüssel, die beim Ausführen des Assistenten für das Erstellen von Agenten erstellt werden, werden automatisch generiert und können nicht verwaltet werden. Schlüssel können nur auf der Seite 'Schlüssel' bearbeitet werden.

Schlüssel bearbeiten

Nach der Erstellung eines Schlüssels kann der Sicherheitsadministrator den Namen des Schlüssels ändern. Das Ändern des Schlüsselnamens ändert jedoch nicht die tatsächlichen zugrunde liegenden Schlüsselwerte. Darüber hinaus kann das Feld für Hinweise geändert werden.

Schlüsselrotation

MDE ermöglicht es dem Sicherheitsadministrator, Schlüssel innerhalb des Agentenumfelds zu rotieren. Klicken Sie auf der Seite 'Schlüssel' auf die Schaltfläche "Rotationsjob übergeben".

Sie werden aufgefordert, einen öffentlichen Schlüssel hochzuladen. Dieser Schlüssel wird zur Verschlüsselung des Schlüssel-Escrow für den rotierten Schlüssel verwendet. Wählen Sie einen geeigneten Schlüssel aus, fügen Sie den Schlüssel hinzu und klicken Sie auf “Weiter”.

Kritischer Hinweis

Der SSL-Schlüssel muss RSA- und PEM-codiert sein.

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

Eine Liste aller vom Benutzer erstellten Schlüssel wird angezeigt. Der Sicherheitsadministrator kann eine beliebige Anzahl von Schlüsseln für die Rotation auswählen.

Key Rotation



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

☒ Key1

☐ Key2

☐ Key3

Back

Next

Nach der Auswahl der gewünschten Schlüssel wird ein Job erstellt.

Kritischer Hinweis

Wenn ein Schlüssel mehr als einem Agenten zugeordnet wird, sind alle Agenten, die diesen Schlüssel verwenden, betroffen.

Nach der Jobgenehmigung werden alle betroffenen Agenten von der Schlüsselrotation benachrichtigt. Der Job wird weiter ausgeführt, bis alle betroffenen Agenten den Schlüsselrotationsprozess abgeschlossen haben. Abhängig von der Anzahl der betroffenen Agenten kann die Ausführung dieses Jobs längere Zeit in Anspruch nehmen.

Hinweis

Wenn ein externer Keystore verwendet wird, muss er **online** sein, damit die Schlüsselrotation erfolgreich ausgeführt werden kann. Wenn ein Fehler auftritt, stellen Sie sicher, dass der externe Keystore online ist. Starten Sie den PPM-Server oder den PPM-Service (spsd) erneut.

Schlüsselwiderruf

Durch Schlüsselwiderruf wird ein Schlüssel aus MDE entfernt und der betreffende Schlüssel in den Escrow-Speicher versetzt. Der Schlüsselwiderruf kann nur für einen Schlüssel durchgeführt werden, der zurzeit keiner aktiven Richtlinie zugeordnet ist. Vor dem Widerruf eines Schlüssels muss der Sicherheitsadministrator Richtlinien entfernen, die auf diesen Schlüssel verweisen.

Durch Entfernen des Pfads, der den Schlüssel aus der Agentenrichtlinienzuordnung verwendet, werden die Daten auf der Platte nicht entschlüsselt. Wenn also der Zugriff auf die Daten erhalten bleiben soll, müssen die Daten aus dem geschützten Verzeichnis herausmigriert werden, bevor die Richtlinie entfernt wird, die diesem Pfad zugeordnet ist.

Nach Abschluss des Widerrufs sind alle Daten, die in dem geschützten Pfad verblieben sind, nicht mehr zugänglich. Der widerrufene Schlüssel wird im Escrow-Speicher hinterlegt und aus dem normalen PPM-Betrieb entfernt.

WARNUNG

Der Sicherheitsadministrator muss die Agentenrichtlinie aktualisieren, um die Zuordnung des betreffenden Schlüssels von allen Agenten aufzuheben, bevor dieser Schlüssel widerrufen wird. Weitere Informationen zum Löschen eines Pfads finden Sie im Abschnitt "Agenten bearbeiten".

Schlüsselschredderung

Die Schlüsselschredderung funktioniert ähnlich wie der Schlüsselwiderruf. Allerdings wird der Schlüssel nach Abschluss der Schlüsselschredderoperation nicht im Escrow-Speicher hinterlegt, sodass die Daten permanent unzugänglich werden.

Hinweis

Diese Funktion ist nur über die REST-API verfügbar. Weitere Informationen finden Sie in der Dokumentation zur REST-API.

Automatisch generierte Schlüssel

Wenn ein Sicherheitsadministrator die Richtliniendurchsetzungsschlüssel nicht verwalten möchte, kann MDE einen Schlüssel für jede neu erstellte Richtlinie automatisch generieren. Automatisch generierte Schlüssel sind immer eindeutig, wenn sie erstellt werden, und sind auf der Schlüsselmanagementseite nicht sichtbar.

Kritischer Hinweis

Automatisch generierte Schlüssel können nicht rotiert oder widerrufen werden. Wenn es erforderlich ist, dass Schlüssel rotieren oder widerrufen werden können, verwenden Sie stattdessen benannte Schlüssel.

Externer Keystore

Schlüssel können an einer von zwei Positionen gespeichert werden: in einer sicheren Datenbank oder in einem externen Keystore. MDE ist zu Anfang nur zur Verwendung der internen sicheren Datenbank konfiguriert. Wenn der Sicherheitsadministrator die Nutzung eines externen Keystores plant, muss ein Keystore konfiguriert werden. Externe Keystore werden nur zum Schützen von Schlüsseln verwendet. Das Schlüsselmanagement für externe Keystore muss in MDE erfolgen.

Hinweis

Anweisungen zur Einrichtung eines externen Keystores werden vom Anbieter des externen Keystores bereitgestellt.

KMIP-Keystores

Informationen zu diesem Vorgang

Ein Sicherheitsadministrator muss einen Java-Keystore und einen Java-Truststore hochladen. Führen Sie die folgenden Schritte aus, um einen Java-Keystore und einen Java-Truststore zu erstellen:

Vorgehensweise

1. Erfassen Sie die Clientzertifikatsdatei und eine Datei mit privatem Clientschlüssel im PKCS12-Format (Public Key Cryptography Standard #12). Diese Datei wird für spätere Schritte "client.p12" genannt. (In [Anhang C, „Beispielkonvertierung zum Erstellen einer PKCS12-Datei“](#), auf Seite 93 finden Sie ein

Beispiel für das Kombinieren eines Clientzertifikats und eines privaten Clientschlüssels in einer Datei im PKCS12-Format.)

2. Erfassen Sie eine öffentliche CA-Zertifikatsdatei. Für spätere Schritte soll diese Datei den Namen "sklm_ca.pem" erhalten.

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

3. Importieren Sie die PKCS12-Datei in einen neuen Java-Keystore:

Kritischer Hinweis

Während dieses Schritts werden Sie zur Eingabe eines Kennworts aufgefordert. Behalten Sie dieses Kennwort für später.

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

4. Rufen Sie den Alias aus der Datei ab:
5. Importieren Sie die CA-Zertifikatsdatei in einen neuen Java-Truststore:

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

Kritischer Hinweis

Während dieses Schritts werden Sie zur Eingabe eines Kennworts aufgefordert. Behalten Sie dieses Kennwort für später.

6. Rufen Sie den Alias aus der Datei ab:

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

Die Einstellungen, die ausgefüllt werden müssen, damit der externe Keystore aktiv ist:

- **Name:** Die benutzerdefinierte Referenz für den externen Keystore.
- **Zustand:** Diese Einstellung teilt MDE mit, dass der definierte externe Keystore den aktuellen aktiven Keystore überschreiben soll. Wenn der Zustand *aktiv* ist, beginnt MDE mit der Verwendung des Keystores. Wenn der Zustand *inaktiv* ist, verwendet MDE den Keystore nicht mehr.
- **Host:** Die IP-Adresse des externen Keystores.
- **Port:** Die Portnummer des externen Keystores.
- **Client-Keystore**
 - **Keystore-Alias:** Der erfasste Keystore-Alias.
 - **Keystore-Datei:** Die Java-Keystore-Datei.
 - **Client-Keystore-Kennwort:** Das Kennwort, das bei der Keystore-Erstellung eingerichtet wurde.
- **Truststore**
 - **Truststore-Alias:** Der erfasste Truststore-Alias.
 - **Truststore-Datei:** Die Java-Truststore-Datei.
 - **Truststore-Kennwort:** Das Kennwort, das bei der Truststore-Erstellung eingerichtet wurde.
- **Ist Master:** Gibt den externen Keystore als Master-Keystore für alle Lese- und Schreiboperationen an.
 - Hat standardmäßig den Wert "true" für den ersten definierten Keystore.
 - Wenn nicht ausgewählt, wird er als "Klon-Keystore" behandelt und nur für Leseoperationen verwendet.
 - Nur ein externer Keystore kann als Master angegeben werden.

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="password"/>	Alias <input type="text"/> Truststore Password <input type="password"/>	<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"/>		

Hinweis

Gegenwärtig unterstützt MDE ein externes Keystore-Produkt: IBM Security Key Lifecycle Manager (SKLM) mit einer Konfiguration für KMIP.

Hardware Security Modules (HSM)

Informationen zu diesem Vorgang

Bei Verwendung eines HSM (Hardware Security Module, Hardwaresicherheitsmodul) als externen Keystore, müssen Sie sicherstellen, dass das Drittanbieterprodukt entsprechend den Anweisungen des Herstellers vollständig konfiguriert und einsatzbereit gemacht wurde.

Die 64-Bit-Version der HSM-Client-Software muss vom PPM-Produktadministrator in die MDE-VM kopiert werden. Die Software muss extrahiert und zusammen mit der SDK-Option entsprechend den Produktanweisungen des HSM-Herstellers zur Einrichtung und Konfiguration der Kommunikation installiert werden.

Ein Dienstprogramm, das mit der Client-Software bereitgestellt wird, oder ein Dienstprogramm, das geprüftermaßen mit HSM funktioniert, wird zum Erstellen eines Wrapper-Schlüssels verwendet. Ein Wrapper-Schlüssel ist ein symmetrischer 256-Bit-Schlüssel, der zur Verwendung mit PPM verfügbar sein muss.

Wenn dieser symmetrische Wrapper-Schlüssel in den HSM erstellt wird, wird ihm ein Handle (interne Kennung) zugeordnet. Dieses Handle wird für die Konfiguration des HSM auf der grafischen Benutzerschnittenseite von PPM benötigt. PPM übergibt dieses Handle und den Richtlinienschlüssel an das HSM zum Verpacken des Richtlinienschlüssels in einen Wrapper und HSM geben den in einen Wrapper verpackten Schlüssel zurück, sodass er in der PPM-Datenbank gespeichert werden kann.

Stellen Sie nach der Installation und Konfiguration der Software sicher, dass PPM mit dem HSM kommunizieren kann, und starten Sie die PPM-VM erneut.

Wählen Sie in der Anzeige für externe Keystore die Option 'Neuer HSM-Keystore' aus.

[Home](#) > [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							

Die folgenden Einstellungen müssen angegeben werden, damit ein externer Keystore aktiv ist:

- **Name:** Die benutzerdefinierte Referenz für den externen Keystore.

- **Zustand:** Dieses Feld legt den gewünschten Status für den Keystore fest.
- **HSM-Token:** HSM verwenden die Slotnummer der Partition.
- **Schlüsselhandle:** Dies ist das Handle, das dem Schlüssel zugeordnet wird, das zum Packen des Richtlinienschlüssels in einen Wrapper verwendet wird.
- **HSM-Kennwort:** Dies ist das Kennwort, das der Partition zugeordnet wird, die der Kunde verwenden wird.

HSM Keystore
New HSM KeyStore

Name	State	HSM Token	Key Handle	HSM Password	Actions
<input style="width: 100%;" type="text"/>	Inactive ▼	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="margin-right: 5px;" type="button" value="Save"/> <input type="button" value="Cancel"/>

Anmerkung: Unterstütztes HSM-Produkt: SafeNet® Luna HSM konfiguriert für einen HSM-Keystore.

Kapitel 10. Richtliniendefinition auf Dateiebene

MDE bietet dem Sicherheitsadministrator die Möglichkeit, eine Steuerung (für den operativen Zugriff und den Verschlüsselungszugriff) für verschiedene Typen von Daten zu definieren. Die nachfolgenden Begriffe werden bei der Definition der Datensteuerung auf Dateiebene verwendet.

- **Selektoren:** Eine ungeordnete Liste von Benutzern und Gruppen, die definieren, welchen Benutzern der Zugriff auf eine Ressource (oder Pfadgruppe) erteilt wird. Optional kann ein definierter Prozess als weitere Komponente für einen Selektor angegeben werden.
- **Pfadgruppen:** Eine Liste von Dateipfaden, die durch die Richtlinie geschützt werden sollen.
- **Datentypen:** Eine geordnete Liste von Zugriffsdefinitionszeilen, die einem angegebenen Typ von Daten zugeordnet werden. Jede Zeile besteht aus einem Selektor, einer E/A-Operation (Lese-/Schreiboperation) und einer Richtlinienaktion.
- **Prozesse:** Ein Dateipfad zu einer ausführbaren Datei. Wird in einem Selektor verwendet, um Zugriffssteuerungselemente mit einer identifizierten ausführbaren Datei zu definieren. Für eine erweiterte Zugriffssteuerung optional.

Sobald ein Datentyp erstellt ist, kann er einem oder mehreren bereitgestellten Agenten zugeordnet werden. In den folgenden Abschnitten wird die Konfiguration einer Richtlinie beschrieben.

Selektoren

Ein Selektor ist ein Richtlinienobjekt, das eine Gruppe von Benutzern und/oder Benutzergruppen durch eine oder mehrere Selektorzeilen definiert. Beim Hinzufügen eines neuen Selektors muss der Sicherheitsadministrator vor dem Speichern einen Namen angeben. Einem Selektor können jederzeit Hinweise und Zeilen durch Bearbeiten des Selektors hinzugefügt werden.

Jede Selektorzeile enthält die folgenden Felder: Benutzer, Gruppe, Prozess. Eines der Felder muss vor dem Speichern gefüllt werden.

- **Benutzer (User):** Der Kurzname eines auf dem Zielsystem definierten Benutzers. Dieses Feld wird mit einem Benutzer im Zielbetriebssystem des Agenten abgeglichen. Dieses Feld ist optional.
- **Gruppe (Group)** Der Kurzname einer im Zielsystem oder in LDAP definierten Benutzergruppe. Dieses Feld wird mit einer Benutzergruppe im Zielbetriebssystem des Agenten abgeglichen. Dieses Feld ist optional.
- **Prozess (Process):** Eine Referenz auf einen produktdefinierten Prozessnamen. Dieses Feld wird mit dem Prozessdateipfad (und optionalen Hashwerten) im Zielbetriebssystem des Agenten abgeglichen. Dieses Feld ist optional.

Policy > Selectors

Expand All Collapse All Search Enter Text Clear New Selector

Name: Selector1 Save Cancel Add New Row

Notes

User	Group	Process	Actions
user01			Delete Row

Die Werte in jeder Selektorzeile werden durch eine logische UND-Operation kombiniert. Wenn mehrere Felder in einer Zeile festgelegt werden, müssen alle Felder übereinstimmen, damit die Zeile überein-

stimmt. Ein Selektor stimmt überein, wenn eine der definierten Zeilen übereinstimmt. Die Reihenfolge der Zeilen in einem Selektor hat keine Auswirkungen auf den Richtlinienabgleichsalgorithmus.

Benutzer	Gruppe	Prozess	Abgleichverhalten des Agenten
✓			Gleicht Benutzer ab.
	✓		Gleicht beliebigen Benutzer in der definierten Gruppe ab.
		✓	Gleicht den definierten Prozesspfad ab und schränkt potenziell auf angegebene Hashwerte ein.
✓	✓		Gleicht Benutzer nur ab, wenn dieser als Mitglied der definierten Gruppe fungiert.
✓		✓	Gleicht Benutzer nur ab, wenn dieser über den definierten Prozess agiert.
	✓	✓	Gleicht mit einem beliebigen Benutzer in der definierten Gruppe nur ab, wenn dieser über den definierten Prozess agiert.
✓	✓	✓	Gleicht Benutzer nur ab, wenn dieser als Mitglied der definierten Gruppe fungiert und über den definierten Prozess mit einem Prozess agiert.

Hinweis

Die Auflösung von Selektorbenutzern und/oder -gruppen funktioniert in Verbindung mit dem konfigurierten externen LDAP- oder Active Directory Server, auf dem der Dateiaгент installiert ist.

Pfadgruppen

Eine Pfadgruppe ist eine Zusammenstellung aus einer oder mehreren ungeordneten Dateipfadzeilen. Beim Hinzufügen einer Pfadgruppe muss der Sicherheitsadministrator einen Namen für die Pfadgruppe angeben. Klicken Sie zum Hinzufügen der Pfadgruppe auf die Schaltfläche "Pfad hinzufügen". Jede Zeile enthält einen Dateipfad und Hinweise.

🏠 > Policy > Path Sets

Expand All Collapse All

Search

▶ Name:

Notes

Path	Notes	Actions
<input type="text" value="/protected"/>	<div style="border: 1px solid #ccc; height: 30px; width: 100%;"></div>	<input type="button" value="Delete Path"/>

Der Sicherheitsadministrator muss einen Dateipfad angeben. Der Schutz erfolgt rekursiv vom angegebenen Pfad aus bis hinunter in alle vorhandenen Unterverzeichnisse. Das Feld für Hinweise ist optional.

Datentypen

Ein Datentyp ist eine geordnete Gruppe von Datentypzeilendefinitionen, die eine Steuerung des operativen Datenzugriffs und/oder des Verschlüsselungsdatenzugriffs auf Dateiebene ermöglichen. Jeder Datentyp enthält einen Namen, einen Richtliniendurchsetzungsschlüssel, Benutzerhinweise und eine geordnete Liste von Zeilen.

- **Name:** Die benutzerdefinierte Referenz auf den Datentyp.
- **Benutzerhinweise:** Das Feld mit den vom Sicherheitsadministrator definierten Hinweisen.

Datentypzeile

Jede Datentypzeile enthält die folgenden Felder: Reihenfolge, Selektor, Operation und Aktion.

- **Reihenfolge:** Die Priorität, in der jede Richtlinienzeile geprüft wird. Die erste übereinstimmende Zeile wird verwendet. Dieses Feld ist erforderlich, aber es wird nicht angezeigt, wenn nur eine Zeile vorhanden ist.
- **Selektor:** Eine Auswahl zuvor definierter Selektoren. Die Richtlinienzeile stimmt überein, wenn beliebige der Zeilen im Selektor übereinstimmen. Dieses Feld ist erforderlich. MDE stellt einen Selektor "Alles auswählen" bereit, der eine Übereinstimmung mit jedem Benutzer bedeutet.
- **Operation:** Eine Auswahl von Dateioperationen, die ausgeführt werden können. Die Optionen sind "Lesen" und "Lesen/Schreiben". Dieses Feld ist erforderlich.
- **Aktion:** Eine Auswahl von Zugriffsaktionen, die der Operation zugeordnet werden. Die Optionen sind "Zulassen", "Verweigern", "Zulassen, Protokollieren" und "Verweigern, Protokollieren". Dieses Feld ist erforderlich.

Variablen für Datentypzeilen

Die Felder 'Selektor', 'Operation' und 'Aktion' können optional als variabel festgelegt werden. Dies gibt Sicherheitsadministratoren die Möglichkeit, Vorlagen für einen Datentyp zu erstellen, die bei der Agentenerstellung ausgefüllt werden. Die verfügbaren Feldeinstellungen sind: 'Bearbeiten möglich', 'Bearbeiten erforderlich' und 'Bearbeiten nicht möglich'.

Bearbeiten möglich

Dieses Feld kann optional bei der Agentenerstellung überschrieben werden.

Bearbeiten erforderlich

Dieses Feld muss bei der Agentenerstellung festgelegt werden.

Bearbeiten nicht möglich

Dieses Feld muss bei der Datentyperstellung festgelegt werden und kann bei der Agentenerstellung nicht geändert werden.

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>	<div>Delete</div>
▴ 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>	<div>Delete</div>

Add New Row

Save

Cancel

Ein Datentyp kann erst gespeichert werden, wenn alle Zeilen Werte und/oder eine variable Einstellung enthalten.

Prozesse

Ein Prozess gibt einen Dateisystempfad zu einer ausführbaren Datei an. Ein Prozess besteht aus den folgenden Feldern:

- **Name:** Der Name des Prozesses.
- **Pfad:** Der absolute Pfad zu einer ausführbaren Datei im Dateisystem.
- **Betriebssystem:** Ein Feld, das zur Angabe des Betriebssystemtyps (Linux, Windows, AIX) verwendet wird.
- **Version:** Ein Feld, das zur Angabe der Betriebssystemversion verwendet wird.
- **Distribution:** Ein Feld, das zur Angabe der Betriebssystemdistribution (Red Hat, CentOS, Windows, AIX) verwendet wird.

🏠 > Policy > Processes

Expand All Collapse All

Search

Clear

New Process

▸ Name

Save Cancel Add Hash

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

Hash

Actions

44 IBM Multi-Cloud Data EncryptionPowered by SPx®: Verwaltung

Ein Prozess kann nur als Dateipfad oder mit einer Liste von Prozesshashwerten definiert werden. Wenn ein oder mehrere Hashwerte definiert werden, wird der Prozessabgleich auf die aufgelisteten Hashwerte begrenzt.

Hinweis

Prozesshashwerte werden durch ein Agententool generiert und müssen in PPM kopiert werden. Das Tool gibt einen Hashwert für die aktuelle Version der ausführbaren Datei aus.

`spxhash -p <Pfad zur ausführbaren Datei>`

Beispiel:

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

```
1202E81EF41273904A6DD381C35B2561F838F7E35B6B26959F8EEB646297A36A7C2
```


Kapitel 11. Agentenbereitstellung und Agentenmanagement

MDE unterstützt vier Typen von Agenteninstallationen: 'Datenträger', 'Datei mit Richtlinie', 'Datenträger mit Richtlinie' und 'Objektspeicher'. Jeder Agententyp ermöglicht eine andere Methode von Datenschutz.

- **Datenträger:** Der Agent schützt Daten auf der Blockeinheitenebene.
- **Datei mit Richtlinie:** Der Agent schützt Daten auf Dateiebene und stellt dateibasierte operative Richtlinien für die Zugriffssteuerung bereit.
- **Datenträger mit Richtlinie:** Der Agent schützt Daten auf Blockeinheitenebene und stellt zudem dateibasierte operative Richtlinien für die Zugriffssteuerung bereit.
- **Objektspeicher:** Der Agent schützt an den Objektspeicher gesendete Daten.

Agenten hinzufügen

Zum Hinzufügen eines Agenten muss ein Sicherheitsadministrator zur Seite 'Agenten' in MDE navigieren und auf die Dropdown-Liste "Agent hinzufügen" klicken. Die verfügbaren Agentenoptionen werden aufgelistet.

🏠 > Agents

Agent Report

Search

Enter Text

Clear

Add Agent

File with Policy
Volume
Volume with Policy
Object Store

Wenn Sie den Agententyp auswählen, wird ein Assistent geöffnet, in dem sie den Agenten erstellen können.

Anmerkung: Es wird empfohlen, alle vorgesehenen Richtlinienkomponenten (Selektoren, Pfadgruppen, Schlüssel, Datentypen und Prozesse) hinzuzufügen, bevor mit dem Prozess zum Hinzufügen von Agenten begonnen wird, da diese Komponenten nicht während des Prozesses erstellt werden können.

Die Bereitstellung eines Agenten umfasst sechs Abschnitte: Agentenidentität, Netzinformationen, Richtlinie, Datenträger, berechtigte Benutzer und Tools. Alle erforderlichen Abschnitte müssen ausgefüllt werden, bevor der Agent hinzugefügt werden kann.

Identität

Im Abschnitt 'Identität' muss der Sicherheitsadministrator einen Namen, eine eindeutige Kennung (UUID), das Betriebssystem und Hinweise definieren.

Add File With Policy Agent

Required

☒ Agent Identity

☐ Network Information

Optional

☐ Policy

☐ Authorized Users

☐ Tools

* Required

Name *

UUID *

9a5db4d2-0bd2-430b-841d-4cc122a152dd

Operating System *

Notes

Next

- **Name:** Eine benutzerdefinierte Referenz für den Agenten.
- **UUID:** Eine eindeutige ID, die MDE zum Identifizieren des Agenten verwendet.
- **Betriebssystem:** Das Betriebssystem des Zielagenten.
- **Hinweise:** Die Hinweise des Sicherheitsadministrators für diesen Agenten.

Wenn Sie Eingaben in alle erforderlichen Felder vorgenommen haben, klicken Sie auf **Speichern**, um mit dem nächsten Schritt fortzufahren.

Anmerkung:

- MDE füllt die UUID automatisch aus, der Sicherheitsadministrator kann sie jedoch bei Bedarf ersetzen.
- Die erforderlichen Felder sind in der grafischen Benutzerschnittstelle (GUI) gekennzeichnet.
- Die Namen für Agenten sind nicht eindeutig; wenn derselbe Name für mehrere Agenten verwendet wird, wird daher die Nachrichtenquelle in den Ereignisprotokollnachrichten möglicherweise nicht korrekt dargestellt.

Netz

Im Schritt für die Netzkonfiguration muss der Sicherheitsadministrator den Hostnamen oder die IP-Adresse des Agenten und von MDE sowie die Zertifikate definieren, die zur Herstellung einer sicheren Verbindung zwischen MDE und dem Zielagenten benötigt werden.

- **IP-Adresse:** Die IP-Adresse oder der Hostname des Servers, auf dem der Agent installiert wird.
- **MDE-Peer-IP:** Die IP-Adresse oder der Hostname von MDE aus der Perspektive der Instanz des Zielagentenservers.

Anmerkung: MDE füllt die MDE-Peer-IP automatisch aus, der Sicherheitsadministrator kann sie jedoch bei Bedarf ändern.

- **Zertifikate:** Eine Liste der hochgeladenen Zertifikate, die zum Herstellen einer sicheren Verbindung zwischen MDE und dem installierten Agenten verwendet werden. Dieses Zertifikat wird zum Herstellen einer gegenseitig authentifizierten TLS1.2-Verbindung zwischen dem Agenten und dem MDE-PPM-Server verwendet.

Zum Hochladen eines Zertifikats muss der Sicherheitsadministrator auf **Zertifikat hinzufügen** klicken, zum gewünschten Zertifikat navigieren und dieses öffnen. Es wird in der Anzeige “Neuer Agent - Netz” angezeigt.

Anmerkung: Der Agent und PPM kommunizieren nicht und der Agent verschlüsselt keine Daten und setzt keine Richtlinien durch, wenn das Keystore- und das Truststore-Zertifikat nicht in MDE hochgeladen wurden und dem Agenten das entsprechende Zertifikat nicht zugeordnet ist. Weitere Details finden Sie im Abschnitt “Einstellungen für Serverzertifikate”.

Wenn Sie Eingaben in alle erforderlichen Felder vorgenommen haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

Agenten des Typs 'Datei mit Richtlinie', 'Datenträger mit Richtlinie' und 'Datenträger' erstellen.

Im Schritt für die Richtlinie muss der Sicherheitsadministrator die Steuerelemente für den operativen Zugriff und den Verschlüsselungszugriff für Dateipfade auf dem Zielagenten definieren.

Pfad hinzufügen

Agenten vom Typ 'Datei mit Richtlinie' und 'Datenträger mit Richtlinie' können der Agentenrichtlinie eine Pfaddefinition hinzufügen. Jeder hinzugefügte Pfad schützt einen einzelnen Dateipfad oder eine Gruppierung von Dateipfaden auf dem Zielagenten. Die Anzahl der hinzugefügten Pfade wird durch den Sicherheitsadministrator definiert.

Kritischer Hinweis

- **Pfade, die durch eine Richtlinie geschützt werden, müssen bei Anwendung der Richtlinie vorhanden sein, andernfalls schlägt die Richtlinienanwendung fehl.**
- **Vorhandene Dateien und Unterverzeichnisse müssen manuell mit dem Befehl 'spxconvert' verarbeitet werden, der nach der Installation des Agenten vom Typ 'Datei mit Richtlinie' verfügbar ist. Die Richtlinie ist in Kraft, auch wenn die Dateien nicht verschlüsselt werden.**
- **Neue Dateien und Verzeichnisse, die nach der Installation hinzugefügt werden, werden durch die Richtlinie automatisch verschlüsselt und geschützt.**

Add File With Policy Agent

Required

- ✓ Agent Identity
- ✓ Network Information

Optional

- ☒ Policy
- ☐ Authorized Users
- ☐ Tools

Buttons: Add Path, Back, Next

Klicken Sie auf 'Pfad hinzufügen', um einen Pfad hinzuzufügen.

Für jeden hinzuzufügenden Pfad müssen der Dateipfad oder die Pfadgruppe, der Schlüssel und ein Datentyp eingegeben werden.

Add File With Policy Agent

Required

✓ Agent Identity

✓ Network Information

Optional

○ Policy

○ Authorized Users

○ Tools

* Required

File Policy Path (or Path Set) *

/home/data

Delete

Storage

☒ Local

☐ Network

Key

☐ System Defined

☒ User Defined

Name

User Defined Key

Datatype *

testDT

(remember to fill out any empty values below)

Selector	Operation	Actions
Select All	Read or Write	Permit

Add Path

Back

Next

- **Dateirichtlinienpfad (oder Pfadgruppe):** Gibt den Pfad oder die Gruppe von Pfaden an, die durch die angegebene Zugriffssteuerungsdefinition für den Datentyp geschützt werden soll. Der Schutz erfolgt rekursiv vom angegebenen Dateipfad in alle vorhandenen Unterverzeichnisse.
- **Speicher:** Identifiziert die Position des Dateipfads. Gültige Optionen sind 'Lokal' oder 'Netz'. Wenn 'Netz' ausgewählt ist, müssen zusätzliche Parameter eingegeben werden, um den Netzspeicher korrekt zu konfigurieren. (Siehe die Konfigurationsinformationen weiter unten.)
- **Schlüssel:** Der Schlüssel, der zum Verschlüsseln von Pfaden, die dem Datentyp zugeordnet sind, verwendet wird. Jeder zuvor definierte benutzerdefinierte Schlüssel oder jeder durch MDE verwaltete, vom System generierte Schlüssel kann verwendet werden. Dieses Feld kann sichtbar oder nicht sichtbar sein, je nachdem, ob 'Datei mit Richtlinie' oder 'Datenträger mit Richtlinie' verwendet wird (siehe Hinweis).
- **Datentyp:** Auswahl eines zuvor erstellten Datentyps. Nach der Auswahl werden die Datentypinformationen in der Ansicht hinzugefügt. Wenn ein Datentyp mit Variablen verwendet wird, müssen die Variablen vor dem Speichern eingegeben werden.

Anmerkung:

- Wenn eine Pfadgruppe verwendet wird, muss diese erstellt sein, bevor der neue Agent hinzugefügt wird. Andernfalls kann ein einzelner manueller Pfad definiert werden.
- Der verwendete Datentyp muss erstellt worden sein, bevor der neue Agent hinzugefügt wird.
- Wenn der neue Agent vom Typ 'Datenträger mit Richtlinie' ist, enthalten Pfadgruppen keine Richtlinien-durchsetzungsschlüssel, da der Schutz durch die Datenträgerschlüsseldefinition erfolgt.

Konfiguration des lokalen Speichers

Wenn Sie lokalen Speicher für die Definition des Dateirichtlinienpfads verwenden, müssen Sie die Option **Lokaler Speicher** auswählen. Dadurch wird der Agent angewiesen, den definierten absoluten Dateipfad (oder die Pfadgruppe) zu schützen. Es sind keine weiteren Parameter erforderlich.

Konfiguration des Netzspeichers

Wenn Sie Netzspeicher für die Definition des Dateirichtlinienpfads verwenden, müssen Sie die Option 'Netzspeicher' auswählen. Dadurch wird der Agent angewiesen, den definierten Netzspeicher an den definierten absoluten Dateipfad anzuhängen (mount). Pfadgruppen können mit definierten Netzspeicher nicht verwendet werden. Es sind zusätzliche Parameter erforderlich.

Für den Netzspeicher müssen die folgenden Elemente definiert werden: Protokoll, Hostname/IP-Adresse, Freigabe, Benutzername, Kennwort und erweiterte Mountoptionen.

- **Protokoll:** Identifiziert den Typ des verwendeten Netzspeichers. Die folgenden Optionen sind gültig: NFSv4, NFSv3.
- **Hostname/IP-Adresse:** Der Hostname oder die IP-Adresse des Netzspeichersystems.
- **Freigabe:** Die Exportposition des Netzdateisystems.
- **Benutzername:** Der Authentifizierungsbenutzername für das Netzdateisystem (für NFSv3 nicht erforderlich).
- **Kennwort:** Das Authentifizierungskennwort für das Netzdateisystem (für NFSv3 nicht erforderlich).
- **Erweiterte Mountoptionen:** Eine durch Kommas getrennte Liste der für die NFS-Definition anzuwendenden Optionen.

Wenn Sie Eingaben in alle erforderlichen Felder vorgenommen haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

Datenträger

Datenträger hinzufügen

Informationen zu diesem Vorgang

Agenten vom Typ 'Datenträger' und 'Datenträger mit Richtlinie' können der Agentenrichtlinie eine oder mehrere Datenträgerdefinitionen hinzufügen. Jeder Datenträger, der hinzugefügt wird, ist eine neue geschützte Blockeinheit auf dem Zielagenten.

The screenshot shows a window titled "Add Volume With Policy Agent". On the left, under "Required", "Agent Identity" and "Network Information" are checked. Under "Optional", "Volumes" is selected with a radio button. The "Volumes" section on the right contains a table with two columns: "Device Label" and "Key". There is an "Add Volume" button below the table and a "Delete" button in the top right corner of the table area. A checkbox "Autogenerate Key Required" is also present. At the bottom right are "Back" and "Next" buttons.

Klicken Sie auf **Datenträger hinzufügen**, um einen Datenträger hinzuzufügen. Für jeden hinzugefügten Datenträger muss ein zugrunde liegender Einheitenkennsatz und ein Richtliniendurchsetzungsschlüssel eingegeben werden.

- **Einheitenkennsatz:** Gibt die Einheit an, die geschützt wird. Wenn eine Richtlinie auf einem Agenten bereitgestellt wurde, muss der Einheitenkennsatz dem Datenträger mithilfe des Befehls 'spxdevice' zugeordnet werden (siehe Abschnitt *Agenten installieren*).
- **Schlüssel:** Der Schlüssel, der zum Verschlüsseln des Datenträgers verwendet wird. Jeder zuvor definierte Schlüssel oder durch MDE verwaltete, automatisch generierte Schlüssel kann verwendet werden.

Kritischer Hinweis

Wenn nicht die Option “Schlüssel automatisch generieren” verwendet wird, muss der Richtliniendurchsetzungsschlüssel definiert werden, bevor der Agent hinzugefügt wird. Weitere Informationen finden Sie im Abschnitt *Management von Richtliniendurchsetzungsschlüsseln*.

Wenn Sie Eingaben in alle erforderlichen Felder vorgenommen haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

Objektspeicheragent erstellen

Der MDE-Objektspeicheragent (Object Storage Agent - OSA) wird als Vermittler zwischen einem Client und dem Back-End-Objektspeicher verwendet. Anstelle der Berechtigungsnachweise für den Back-End-Objektspeicher verwenden Objektspeicherclients Bucket-Berechtigungsnachweise, um die Verbindung zum OSA herzustellen.

Administratoren können den OSA so konfigurieren, dass er Verbindungen zu einem oder mehreren Objektspeicherprovidern herstellt. Der OSA verschlüsselt die Daten, die über den OSA an den konfigurierten Back-End-Objektspeicher gesendet werden, und setzt die Richtlinien für diese Daten durch. Sind mehrere Back-Ends konfiguriert, werden die Daten aufgeteilt und Teile der Daten werden an die einzelnen Back-Ends gesendet.

Front-End-Zertifikate

Für Objektspeicheragenten muss ein Zertifikat konfiguriert werden, mit dem eine sichere Verbindung zwischen dem Objektspeicherclient und dem Objektspeicheragenten hergestellt wird.

Zum Hochladen eines Zertifikats muss der Sicherheitsadministrator auf die Schaltfläche “Zertifikat hinzufügen” klicken, zum gewünschten Zertifikat navigieren und dieses öffnen.

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

Wenn Sie Eingaben in alle erforderlichen Felder vorgenommen haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

Bucket-Berechtigungsnachweise

MDE kann für die Kommunikation mit mehreren Objektspeicherprovidern konfiguriert werden. Für jeden Provider müssen ein Bucket und die Bucket-Berechtigungsnachweise konfiguriert werden.

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 *

78dKnlcLBiUkQgl6OLjtBKqNoglZw54S6g5SSiik5JX0wOvZ0xoIIZoTa=PGKK3B

Protocol *

IBM S3

XH2BW34YV12A0REPF3TW

Delete

Key ID *

XH2BW34YV12A0REPF3TW

API Key *

3AoMJ9fXv3p1xpU8xoAqfSt=DoEaX=3iY7UOyVn3ovUAQ4ssKAbQQvAv1jmHPeXh

Protocol *

AMZ S3

New Credential

Back

Next

Klicken Sie auf die Schaltfläche 'Neuer Berechtigungsnachweis', um einen neuen Berechtigungsnachweis hinzuzufügen.

Für Bucket-Berechtigungsnachweise müssen die Schlüssel-ID, der API-Schlüssel und das Protokoll definiert werden.

- **Schlüssel-ID** – Die Kennung des Zugriffsobjekts für den Objektspeicher.
- **API-Schlüssel** – Ein Zeichenfolgekennwort das der S3-API bereitgestellt wird, um mit der Schlüssel-ID zu korrelieren.
- **Protokoll** – Die Kennung des Protokolls, das für die Kommunikation mit dem Objektspeicherprovider (Swift, IBM S3 und Amazon S3) verwendet wird.

MDE generiert das Paar aus Schlüssel-ID und API-Schlüssel. Administratoren können diese generierten Werte bei Bedarf überschreiben. Ein Administrator muss das gewünschte Protokoll aus den unterstützten Objektspeicherprovidern auswählen.

Wenn Sie Eingaben in alle erforderlichen Felder vorgenommen haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

Buckets

MDE definiert die Objektspeicherrichtlinie über die Zuordnung von Buckets. Für jedes Bucket müssen der Name, die Angabe, ob Verweigerungen protokolliert werden sollen, und die Richtlinie definiert werden.

Agentenbereitstellung und Agentenmanagement 53

Add Object Store Agent

Required

✓ Agent Identity

✓ Network Information

Optional

✓ Front-End Certificates

✓ Bucket Credentials

⊙ Buckets

○ Backends

○ Authorized Users

○ Tools

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

Back

Next

- **Name** – Der Name des Objektspeicherbuckets.
- **Verweigerungen protokollieren** – Eine Kontrollkästchenauswahl. Wird das Kontrollkästchen ausgewählt, erstellt der Objektspeicheragent Prüfprotokolle für Zugriffsverweigerungen.
- **Richtlinie** – Die Definition der Bucketzugriffssteuerungen. Die Richtlinie kann aus mehreren Zeilen bestehen. Für jede Zeile der Richtliniendefinition sind die Schlüssel-ID, der Zugriff und das Protokoll erforderlich.
- **Schlüssel-ID** – Der Eintrag einer vordefinierten Schlüssel-ID für den Bucket-Berechtigungsnachweis.
- **Zugriff** – Die Auswahl der Zugriffsberechtigung 'Lesen oder Schreiben', 'Lesen' oder 'Schreiben'.
- **Protokoll** – Eine Kontrollkästchenauswahl. Wird das Kontrollkästchen ausgewählt, erstellt der Objektspeicheragent Prüfprotokolle für Zugriffsberechtigungen des angegebenen Zeilenverhaltens.

Wenn Sie Eingaben in alle erforderlichen Felder vorgenommen haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

Back-Ends

Back-End-Verbindungsinformationen werden über eine M:N-Auswahl definiert. Diese Auswahl definiert die Redundanz und Sicherheit der Objektspeicherdaten. N steht für die Anzahl der konfigurierten Back-End-Objektspeicherprovider, die auch als 'Freigaben' bezeichnet werden. M steht für die Anzahl der Freigaben, die erforderlich sind, um die Daten wiederherzustellen. Die unterstützten Konfigurationen sind 1:1, 2:3 und 2:4.

54 IBM Multi-Cloud Data EncryptionPowered by SPx®: Verwaltung

Add Object Store Agent

Required

☒ Agent Identity
☒ Network Information

Optional

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

M:N 2:3

* Required

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

Für jede Freigabe müssen die URL, die ID, der Schlüssel und das Protokoll definiert werden.

- **URL** – Die Zugriffs-URL für den Objektspeicherprovider.
- **ID** – Die Benutzer-ID des Kontos für den Zugriff auf den Objektspeicherprovider.
- **Schlüssel** – Der Kontoschlüssel der Benutzer ID für den Zugriff auf den Objektspeicherprovider.
- **Protokoll** – Die Kennung des Protokolls, das für die Kommunikation mit dem Objektspeicherprovider (Swift, IBM S3 und Amazon S3) verwendet wird.

Wenn Sie Eingaben in alle erforderlichen Felder vorgenommen haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

Berechtigte Benutzer

Im Schritt für Benutzer muss der Sicherheitsadministrator die MDE-Benutzerkonten definieren, die über die Berechtigungen zum Herunterladen des Agenteninstallationsbundles verfügen.

Wenn ein Benutzer nicht als berechtigter Benutzer aufgeführt ist und sich dieser Benutzer anmeldet und den Agenten anzeigt, werden diesem Benutzer die Download-Links auf der Seite 'Agenteninfo' nicht angezeigt.

Add File With Policy Agent

Required

☒ Agent Identity
 ☒ Network Information

Optional

☒ Policy
 ☒ **Authorized Users**
☐ Tools

Authorized Users

Back

Next

Wenn Sie Eingaben in alle erforderlichen Felder vorgenommen haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

Agententools

Agenten unterstützen spezialisierte Tools, die bei der Übertragung von Daten in einem verschlüsselten Format helfen. Es gibt zwei Typen von Tools: Sichern/Wiederherstellen und Objektspeicher.

Tools werden entweder während der Agentenbereitstellung oder auf der Seite "Agenteninfo" konfiguriert. Das Tool "Sichern/Wiederherstellen" wird zur Sicherung und Wiederherstellung verschlüsselter Daten verwendet. Es nutzt einen zugeordneten Schlüssel zur Sicherung verschlüsselter Daten und bietet die Möglichkeit, die verschlüsselten Daten zu einem späteren Zeitpunkt wiederherzustellen, auch wenn der Richtlinien Schlüssel turnusmäßig gewechselt wurde. Das Tool zum Sichern/Wiederherstellen ist optional mit keinerlei Anforderung für die Zuordnung eines Tools zu einem Agenten. Das Tool für den Objektspeicher wird für den Agenten "Objektspeicher" benötigt.

Matrix für Agententools

Die Verfügbarkeit von Tools basiert auf dem Agententyp und wird durch die Zuordnung eines Schlüssels ermöglicht. Die Toolmatrix nach Agententyp sieht folgendermaßen aus:

Tooltyp	Datenträger	Datenträger mit Richtlinie	Datei mit Richtlinie	Objektspeicher
Sichern/Wiederherstellen	✓	✓	✓	
Objektspeicher				✓

Zuordnung zwischen Tools und Schlüsseln

Um einem Tool einen Schlüssel zuzuordnen, geben sie zunächst einen zuvor definierten Schlüsselnamen in das Textfeld neben dem gewünschten Tool ein und wählen Sie dann den entsprechenden Schlüssel aus der Liste aus.

Klicken Sie auf **Speichern**. Dadurch wird ein Job erstellt. Sobald das konfigurierte Tool genehmigt wurde, wird es für den Agenten aktiviert.

Anmerkung: Automatisch generierte Schlüssel werden für Tools nicht unterstützt. Schlüssel müssen vor der Erstellung des Agenten definiert werden.

Wenn Sie Eingaben in alle erforderlichen Felder vorgenommen haben, klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

Prüfen und Build erstellen

Informationen zu diesem Vorgang

Nach Abschluss aller Bereitstellungsschritte wird der Benutzer an die Anzeige 'Prüfen' weitergeleitet.

Auf der Seite zum Prüfen der Bereitstellungsconfiguration wird eine vollständige Ansicht aller Konfigurationsinformationen angezeigt.

Prüfen Sie den Inhalt auf Vollständigkeit und Richtigkeit und klicken Sie auf **Erstellen**, um den Bereitstellungsprozess abzuschließen. Ein Job zum Hinzufügen des Agenten wird erstellt.

Nach der Genehmigung des Jobs wird der Agent erstellt und das Installationspaket ist zum Download und zur Installation verfügbar.

Agentenaktivierung

Nach der Genehmigung des Agentenbuild-Jobs ist der neu erstellte Agent in MDE aktiv. Sobald der Agent installiert ist, verwendet er die für MDE konfigurierte Peer-IP-Adresse und die bereitgestellten Zertifikate, um eine gegenseitig authentifizierte TLS1.2-Verbindung zu MDE zu erstellen.

Der Agent fordert eine Richtlinie bei der Erstinstallation und dem nachfolgenden Start an. MDE antwortet mit der konfigurierten Richtlinienkonfiguration. Wenn die Richtlinie empfangen wurde, wird sie auf dem Agenten durchgesetzt.

Agenten anzeigen

Informationen zu diesem Vorgang

Auf der Seite 'Agenten' wird eine Zusammenfassung der erstellten Agenten angezeigt.

🏠 > 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"/>

Zum Anzeigen der Details für einen bestimmten Agenten klicken Sie auf den Namen des Agenten in der Spalte 'Name' oder auf die Schaltfläche 'Details' in der Spalte 'Aktionen'. Dadurch wird eine Ansichtsseite für Agentendetails geöffnet, die Bereitstellungsinformationen, Downloads von Installationspaketen und weitere nützliche Informationen anzeigt.

Agentenbericht

Der MDE-Sicherheitsadministrator kann einen Agentenbericht erstellen. Dieser Bericht enthält die folgenden Informationen: Gesamtzahl Agenten, Agentenanzahlen nach Typ und Betriebssystem sowie Agenten, die sich innerhalb von 30 Tagen ab der Berichtsgenerierung angemeldet haben. Das Datum basiert auf der PPM-Zeit, die als UTC-Zeit angegeben wird. Die Daten werden nach Agententyp aufgeschlüsselt.

🏠 > Agents

Agent Report

Search

Agenten installieren

Informationen zu diesem Vorgang

Im Bereitstellungsschritt wurden alle Informationen konfiguriert, die für die Agenteninstallation und die Bereitstellung einer Richtlinie auf einer Zielserverinstanz erforderlich sind. Zum Installieren des Agenten laden Sie das Installationspaket herunter, kopieren es auf das Zielsystem, entpacken den Inhalt und führen das Setup-Script aus.

Agent Info Edit Agent Info

Identity

Name Agent1
UUID dab30682-19ee-4763-84d8-12fe2ba91948
IP Address 1.1.1.1
Type Volume with Policy
Operating System CentOS / Red Hat 7

Notes

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

Authorized Users admin
Install Files Download URL /rest/agents/1/install_bundle

Download Zip Bundle
Download Tar Bundle

Download Tokens

ID	State
Add Token	

Kritischer Hinweis

Stellen Sie sicher, dass alle Benutzer, Gruppen und Pfade oder Einheiten, die in der Bereitstellungsrichtlinie angegeben werden, im Agentensystem erstellt, angehängt und konfiguriert werden.

Agenten für Linux installieren

Es gibt vier Typen von Agenten: 'Datenträger', 'Datei mit Richtlinie', 'Datenträger mit Richtlinie' und 'Objektspeicher'. Verwenden Sie den bei der Agentenbereitstellung vorgesehenen Agententyp.

Einheitenkonfiguration für Linux-Datenträgeragenten

Informationen zu diesem Vorgang

Vorgehensweise

1. Erstellen Sie einen Datenträger in PPM (merken Sie sich den Einheitenkennsatz, der in Abschnitt 11.1.5 verwendet wird).
2. Installieren Sie das Paket "gettext" auf Ihrer Agenten-VM.
3. Installieren Sie den Agenten (Details siehe [Anhang A, „Beispiele für Agenteninstallationsprozesse“](#), auf Seite 85).
4. Starten Sie die Agenten-VM erneut, wenn die Installation abgeschlossen ist.

5. Führen Sie als Rootbenutzer den folgenden Befehl aus: `spxdevice -e <in PPM angegebener Kennsatz> -m <Mountpunkt> -f <Dateisystem> -u <zu verwendende Platte>`

```
spxdevice -e COS6VOL -m /protected -f ext4 -u /dev/sdb
```

Einheitenkonfiguration für Linux-Agenten vom Typ 'Datei mit Richtlinie'

Informationen zu diesem Vorgang

Vorgehensweise

1. Erstellen Sie einen Agenten vom Typ 'Datei mit Richtlinie' in PPM.
2. Erstellen Sie alle erforderlichen Benutzer.
3. Erstellen Sie alle erforderlichen Unterverzeichnisse.
4. Legen Sie die richtigen Berechtigungen für Verzeichnisse fest.
5. Installieren Sie das Paket "gettext" auf Ihrer Agenten-VM.
6. Installieren Sie den Agenten (Details siehe [Anhang A, „Beispiele für Agenteninstallationsprozesse“](#), auf Seite 85).
7. Starten Sie die Agenten-VM erneut, wenn die Installation abgeschlossen ist.
8. Prüfen Sie mit dem Befehl "spxinfo -l", ob die Dateirichtlinie korrekt ist.

Hinweis

Ein Stern neben einem Pfad gibt an, dass es zuvor vorhandene Daten gibt, deren Verschlüsselung ansteht. Zur Durchführung der Verschlüsselung an der Position für zuvor vorhandene Verzeichnisstrukturen und Daten sowie zur Bestimmung des Status von Daten zu einem beliebigen Zeitpunkt stellt MDE ein Befehlszeilendienstprogramm mit dem Namen "spxconvert" bereit.

In [Anhang E, „Verschlüsselung an der Position“](#), auf Seite 97 finden Sie eine detaillierte Beschreibung des Befehls und seiner Verwendung.

Einheitenkonfiguration für Linux-Agenten vom Typ 'Datenträger mit Richtlinie'

Informationen zu diesem Vorgang

Vorgehensweise

1. Erstellen Sie einen Agenten vom Typ 'Datenträger mit Richtlinie' in PPM (merken Sie sich den verwendeten Einheitenkennsatz).
2. Installieren Sie das Paket "gettext" auf Ihrer Agenten-VM.
3. Installieren Sie den Agenten (Details siehe [Anhang A, „Beispiele für Agenteninstallationsprozesse“](#), auf Seite 85).
4. Starten Sie die Agenten-VM erneut, wenn die Installation abgeschlossen ist.
5. Führen Sie als Rootbenutzer den folgenden Befehl aus: `spxdevice -e <in PPM angegebener Kennsatz> -m <Mountpunkt> -f <Dateisystem> -u <zu verwendende Platte>`

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

6. Erstellen Sie erforderliche Unterverzeichnisse und Benutzer.
7. Legen Sie die richtigen Berechtigungen für Verzeichnisse fest.
8. Starten Sie die Agenten-VM erneut.
9. lsblk – Prüfen Sie mit diesem Befehl, ob die Platte vorhanden ist. Dies kann manchmal bis zu 30 Sekunden dauern.
10. Prüfen Sie mit dem Befehl "spxinfo -l", ob die Dateirichtlinie korrekt ist.

Hinweis

Unter Linux kann die Datenträgerverschlüsselung auf ganzen Einheiten oder in Partitionen eingerichtet werden. Zur Verwendung einer einzelnen Partition geben Sie einfach eine leere Partition (z. B. /dev/sdb1) an, wenn Sie die Option 'spxdevice -u' verwenden.

Konfiguration von Agenten des Typs 'Objektspeicher' unter Linux

Informationen zu diesem Vorgang

Vorgehensweise

1. Erstellen Sie einen Agenten vom Typ 'Objektspeicher' in PPM.
2. Installieren Sie den Agenten (Details siehe [Anhang A, „Beispiele für Agenteninstallationsprozesse“](#), auf Seite 85).
3. Starten Sie die Agenten-VM erneut, wenn die Installation abgeschlossen ist.

Agenten für AIX installieren

AIX unterstützt nur einen einzelnen Agententyp: den Typ 'Datei mit Richtlinie'. Verwenden Sie den bei der Agentenbereitstellung vorgesehenen Agententyp.

Einheitenkonfiguration für AIX-Agenten vom Typ 'Datei mit Richtlinie'

1. Erstellen Sie einen Agenten vom Typ 'Datei mit Richtlinie' in PPM.
2. Erstellen Sie alle erforderlichen Benutzer.
3. Erstellen Sie alle erforderlichen Unterverzeichnisse.
4. Legen Sie die richtigen Berechtigungen für Verzeichnisse fest.
5. Installieren Sie den Agenten (Details siehe [Anhang A, „Beispiele für Agenteninstallationsprozesse“](#), auf Seite 85).
6. Starten Sie die Agenten-VM erneut, wenn die Installation abgeschlossen ist.
7. Prüfen Sie mit dem Befehl “spxinfo -l”, ob die Dateirichtlinie korrekt ist.

Anmerkung: Ein Stern neben einem Pfad gibt an, dass es zuvor vorhandene Daten gibt, deren Verschlüsselung ansteht. Zur Durchführung der Verschlüsselung an der Position für zuvor vorhandene Verzeichnisstrukturen und Daten sowie zur Bestimmung des Status von Daten zu einem beliebigen Zeitpunkt stellt MDE ein Befehlszeilendienstprogramm mit dem Namen “spxconvert” bereit.

In [Anhang E, „Verschlüsselung an der Position“](#), auf Seite 97 finden Sie eine detaillierte Beschreibung des Befehls und seiner Verwendung.

Agenten für Windows installieren

Es gibt drei Typen von Agenten: 'Datenträger', 'Datei mit Richtlinie' und 'Datenträger mit Richtlinie'. Verwenden Sie den bei der Agentenbereitstellung vorgesehenen Agententyp.

Einheitenkonfiguration für Windows-Datenträgeragenten

Informationen zu diesem Vorgang

Vorgehensweise

1. Erstellen Sie einen Datenträger in PPM (merken Sie sich den verwendeten Einheitenkennsatz).
2. Installieren Sie den Agenten (Details siehe [Anhang A, „Beispiele für Agenteninstallationsprozesse“](#), auf Seite 85).
3. Starten Sie die Agenten-VM erneut, wenn die Installation abgeschlossen ist.

4. Führen Sie den Befehl “spxdevice -e <in PPM vergebener Kennsatz> -d <zu verwendende Plattenadresse>” aus, um die gesamte Platte anzuhängen. Dieser Befehl muss unter Administratorberechtigungen ausgeführt werden.

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

5. Oder führen Sie den Befehl 'spxdevice -e <in PPM vergebener Kennsatz> -d <zu verwendende Plattenadresse> -m <Laufwerksbuchstabe> -f <Dateisystem>' aus, um die gesamte Platte anzuhängen, die formatiert und mit einem Laufwerksbuchstaben angehängt wird.

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

6. Alternativ können Sie den Befehl “spxdevice -i <zu verwendende Plattenadresse>” ausführen, um die Platte zum Anhängen an eine bestimmte Partition bereitzustellen.

```
spxdevice -i 1
```

7. Führen Sie als Nächstes den Befehl “spxdevice -e <in PPM vergebener Kennsatz> -v <Laufwerksbuchstabe> -f <Dateisystem>” aus, um den Datenträger an eine bestimmte Partition anzuhängen und die Partition mit einem Dateisystem zu formatieren.

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

Anmerkung: Unter Windows kann die Datenträgerverschlüsselung auf ganzen Einheiten oder in Partitionen eingerichtet werden.

- Für die Verschlüsselung einer gesamten Platte muss die Platte online und initialisiert sein und der Plattenspeicher darf nicht formatiert sein. Es müssen Laufwerksbuchstaben verfügbar sein.
- Für eine Partitionsverschlüsselung muss die Sicherungseinheit mit dem Befehl “spxdevice -i <Plattenadresse>” auf einer reinen Platte erstellt werden. Anschließend muss eine unformatierte Partition (RAW) mit einem Laufwerksbuchstaben erstellt werden.

In der Hilfe zum Befehl “spxdevice” finden Sie Informationen zu weiteren Optionen.

Einheitenkonfiguration für Windows-Agenten vom Typ 'Datei mit Richtlinie'

Informationen zu diesem Vorgang

Vorgehensweise

1. Erstellen Sie einen Agenten vom Typ 'Datei mit Richtlinie' in PPM.
2. Erstellen Sie alle erforderlichen Benutzer.
3. Erstellen Sie alle erforderlichen Unterverzeichnisse.
4. Legen Sie die richtigen Berechtigungen für Verzeichnisse fest.
5. Installieren Sie den Agenten (Details siehe [Anhang A, „Beispiele für Agenteninstallationsprozesse“](#), auf Seite 85).
6. Prüfen Sie mit dem folgenden Befehl, ob die Dateirichtlinie korrekt ist: `spxinfo -l`

Hinweis

Ein Stern neben einem Pfad gibt an, dass es zuvor vorhandene Daten gibt, deren Verschlüsselung ansteht. Zur Durchführung der Verschlüsselung an der Position für zuvor vorhandene Verzeichnisstrukturen und Daten sowie zur Bestimmung des Status von Daten zu einem beliebigen Zeitpunkt stellt MDE ein Befehlszeilendienstprogramm mit dem Namen “spxconvert” bereit.

In [Anhang E, „Verschlüsselung an der Position“](#), auf Seite 97 finden Sie eine detaillierte Beschreibung des Befehls und seiner Verwendung.

Hinweis

Stellen Sie unter Windows durch eine Richtlinie sicher, dass ein Benutzer mit Verwaltungsaufgaben berechtigt ist, die Zielrichtlinien zu erstellen, da die Richtlinie gilt, sobald sie abgerufen wurde.

Einheitenkonfiguration für Windows-Agenten vom Typ 'Datenträger mit Richtlinie'

Informationen zu diesem Vorgang

Vorgehensweise

1. Erstellen Sie einen Agenten vom Typ 'Datenträger mit Richtlinie' in PPM (merken Sie sich den verwendeten Einheitenkennsatz).
2. Installieren Sie den Agenten (Details siehe [Anhang A, „Beispiele für Agenteninstallationsprozesse“](#), auf Seite 85).
3. Starten Sie die Agenten-VM erneut, wenn die Installation abgeschlossen ist.
4. Führen Sie den Befehl "spxdevice -e <in PPM vergebener Kennsatz> -d <zu verwendende Plattenadresse>" aus, um die gesamte Platte anzuhängen. Dieser Befehl muss unter Administratorberechtigungen ausgeführt werden.

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

5. Oder führen Sie den Befehl "spxdevice -e <in PPM vergebener Kennsatz> -d <zu verwendende Plattenadresse> -m <Laufwerksbuchstabe> -f <Dateisystem>" aus, um die gesamte Platte anzuhängen, die formatiert und mit einem Laufwerksbuchstaben angehängt wird.

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

6. Alternativ können Sie den Befehl "spxdevice -I <zu verwendende Plattenadresse>" ausführen, um die Platte zum Anhängen an eine bestimmte Partition bereitzustellen.

PS C:\> spxdevice -i 1

7. Führen Sie als Nächstes den Befehl "spxdevice -e <in PPM vergebener Kennsatz> -v <Laufwerksbuchstabe> -f <Dateisystem>" aus, um den Datenträger an eine bestimmte Partition anzuhängen und die Partition mit einem Dateisystem zu formatieren.

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

Hinweis

Unter Windows kann die Datenträgerverschlüsselung auf ganzen Einheiten oder in Partitionen eingerichtet werden.

- Für die Verschlüsselung einer gesamten Platte muss die Platte online und initialisiert sein und der Plattenspeicher darf nicht formatiert sein. Es müssen Laufwerksbuchstaben verfügbar sein.
- Für eine Partitionsverschlüsselung muss die Sicherungseinheit mit dem Befehl "spxdevice -i <Plattenadresse>" auf einer reinen Platte erstellt werden. Anschließend muss eine unformatierte Partition (RAW) mit einem Laufwerksbuchstaben erstellt werden.

In der Hilfe zum Befehl "spxdevice" finden Sie Informationen zu weiteren Optionen.

8. Fügen Sie ein oder mehrere geschützte Verzeichnisse auf dem Datenträger hinzu.
9. Starten Sie den Computer neu.
10. spxinfo -l (sollte eine Liste aller geschützten Verzeichnisse anzeigen)

Hinweis

Stellen Sie unter Windows durch eine Richtlinie sicher, dass ein Benutzer mit Verwaltungsaufgaben berechtigt ist, die Zielrichtlinien zu erstellen, da die Richtlinie gilt, sobald der Datenträger angehängt und verfügbar ist.

Aktive Richtlinie

Jeder Agent kann nur eine aktive Richtlinie haben. Agenten speichern ihre Richtlinie nicht in persistenter Weise. Bei jedem Agentenneustart fordert der Agent die zurzeit aktive Richtlinie aus MDE an. Wenn MDE für den Agenten nicht zugänglich ist, wird der Standardverweigerungszugriff auf alle geschützten Verzeichnisse auf dem Agenten angewendet.

Wenn eine neue Richtlinie an den Agenten gesendet wird, sendet der Agent ein Ereignis an MDE, sobald die Richtlinie erfolgreich (oder nicht erfolgreich) angewendet wurde. Wenn die Problem mit der Richtlini-enaktivierung bestehen bleiben, prüfen Sie die Datei 'kernel_policy.log' an den folgenden Positionen:

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

Agenten bearbeiten

Nach der erfolgreichen Bereitstellung und Genehmigung eines Agenten müssen alle Änderungen an diesem Agenten durch eine Bearbeitung über die grafische Benutzerschnittstelle (GUI) auf der Seite “Agenteninfo” vorgenommen werden. Zum Bearbeiten eines Agenten zeigen Sie die Details des Agenten an. Auf der Seite “Agenteninfo” können Abschnitte des Agenten unabhängig voneinander bearbeitet werden.

Agenteninfo bearbeiten

Durch Klicken auf die Schaltfläche “Agenteninfo bearbeiten” können einige Agenteninformationen geändert werden: Name, IP-Adresse, MDE-Peer-IP-Adresse und Hinweise.

Agent Info

Edit 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	ea584e4904ffa45a3416eccc753e0f0f655462929d4f1534f369cbccc38165f	2016-

Browse...

No file selected.

Änderungen an der MDE-Peer-IP-Adresse werden in MDE unverzüglich wirksam, wenn der Agent jedoch bereits installiert war, muss ein neues Installationspaket erstellt und installiert werden, bevor die Änderungen wirksam werden.

Hinweis

UUID, Betriebssystem und Agententyp sind nach der Erstbereitstellung nicht bearbeitbar.

Zertifikate hinzufügen/löschen

Agentenzertifikate können durch Klicken auf die entsprechenden Schaltflächen im Abschnitt für Zertifikate der Seite mit den Agenteninfos hinzugefügt und gelöscht werden.

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](#)

Führen Sie die folgenden Schritte aus, um ein Agentenzertifikat zu aktualisieren:

1. Generieren Sie ein neues Zertifikat für den Agenten.
2. Laden Sie das neue Zertifikat nach PPM über die Managementkonsole hoch.
 - a. Klicken Sie auf der Seite "Agenten" auf den zu aktualisierenden Agenten, um die Seite "Agenteninfo" anzuzeigen.
 - b. Klicken Sie auf die Schaltfläche "Zertifikat hinzufügen", wählen Sie die neue Zertifikatsdatei aus und klicken Sie auf die Schaltfläche "OK".
 - c. Das neue Zertifikat sollte angezeigt werden.
3. Löschen Sie das alte Zertifikat.
 - a. Klicken Sie auf der Seite "Agenten" auf den zu aktualisierenden Agenten, um die Seite "Agenteninfo" anzuzeigen.
 - b. Bestimmen Sie das Zertifikat, das gelöscht werden soll.
 - c. Klicken Sie auf die Schaltfläche "Zertifikat löschen" und es wird ein Job erstellt.
 - d. Klicken Sie auf die Schaltfläche "Schließen".
 - e. Klicken Sie auf der Seite "Jobs" für den gewünschten Job auf die Schaltfläche "Genehmigen".
4. Stellen Sie sicher, dass das Zertifikat von dem Agenten gelöscht wurde.
 - a. Klicken Sie auf der Seite "Agenten" auf den zu aktualisierenden Agenten, um die Seite "Agenteninfo" anzuzeigen.
 - b. Stellen Sie sicher, dass das richtige Zertifikat noch vorhanden ist.

Wenn der Agent bereits installiert war, muss ein neues Installationspaket erstellt und installiert werden, bevor die Zertifikatsänderungen wirksam werden.

Agententools

Die Tools, die während der Agentenbereitstellung nicht konfiguriert wurden, können nun auf der Seite "Agenteninfo" hinzugefügt werden. Außerdem können konfigurierte Tools geändert werden.

Schlüssel zuordnen

Um einen Schlüssel zuzuordnen, geben Sie den Schlüsselnamen in das Textfeld neben dem Tool ein und wählen Sie den Schlüssel aus der Liste aus. Klicken Sie auf "Speichern" und ein Job wird erstellt. Sobald das konfigurierte Tool genehmigt wurde, wird es für den Agenten aktiviert.

Add File With Policy Agent

Required

☒ Agent Identity
☒ Network Information

Backup/Restore

Type to filter and select a predefined key

Optional

☒ Policy
☒ Authorized Users
☒ Tools

Back
Next

Schlüssel ändern

Um einen Schlüssel zu ändern, klicken Sie auf die Schaltfläche "Bearbeiten", geben Sie den Schlüsselnamen in das Textfeld neben dem Tool ein und wählen Sie den Schlüssel aus der Liste aus.

Klicken Sie auf “Speichern” und ein Job wird erstellt. Sobald das konfigurierte Tool genehmigt wurde, wird es für den Agenten aktiviert.

Tools

Backup/Restore

User Defined Key

Save
Cancel

Datenzugriff über SU

Beim Anwenden von Zugriffssteuerungen für Richtlinien ist die Standardeinstellung, den Datenzugriff über SU zu verweigern. Es kann jedoch Szenarien geben, in denen ein solcher Zugriff erlaubt ist. Ist dies der Fall, gibt es auf der Seite "Agenteninfo" ein entsprechendes Kontrollkästchen, über das die Einstellung geändert werden kann.

Other Configuration

☒ Block access when su user substitution is in use

Durch das Umschalten des Kontrollkästchens wird ein Job erstellt. Nach der Genehmigung wird die Einstellung für den Datenzugriff über SU entsprechend geändert.

Die folgende Tabelle enthält die Zugriffssteuerungen für den Datenzugriff über SU:

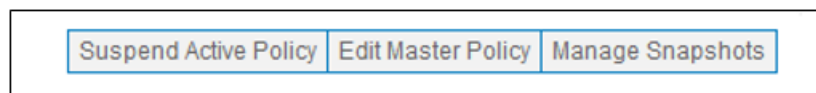
Agententyp	Betriebssystem	Datenzugriff über SU - Standard	Datenzugriff über SU - Konfigurierbar
Datenträger	CentOS6/RedHat6	n. z.	n. z.
Datenträger	CentOS7/RedHat7	n. z.	n. z.
Datenträger	Windows	n. z.	n. z.
Datenträger mit Richtlinie	CentOS6/RedHat6	Geblockt	Ja
Datenträger mit Richtlinie	CentOS7/RedHat7	Geblockt	Ja
Datenträger mit Richtlinie	Windows	n. z.	n. z.

Datei mit Richtlinie	CentOS6/RedHat6	Geblockt	Ja
Datei mit Richtlinie	CentOS7/RedHat7	Geblockt	Ja
Datei mit Richtlinie	AIX	Geblockt	Ja
Datei mit Richtlinie	Windows	n. z.	n. z.
Objektspeicher	CentOS7/RedHat7	n. z.	n. z.

Richtlinie aussetzen

Die Agenten 'Datenträger mit Richtlinie' und 'Datei mit Richtlinie' unterstützen die Möglichkeit, eine definierte aktive Richtlinie auszusetzen. Wenn eine Richtlinie ausgesetzt wird, werden alle Aktionen für die geschützten Verzeichnisse verweigert. Das Aussetzen einer aktiven Richtlinie kann ohne eine Änderung der aktiven Snapshotdefinition erfolgen.

Um eine Richtlinie auszusetzen, klicken Sie in der rechten Ecke des Abschnitts mit den Agenteninfos auf die Schaltfläche "Aktive Richtlinie aussetzen"; dadurch wird ein Job erstellt.



Sobald der Job genehmigt wurde, wird die Richtlinie sofort ausgesetzt und die Schaltfläche wird so umgeschaltet, dass "Aktive Richtlinie wieder aktivieren" angezeigt wird.

Um die ausgesetzte Richtlinie wieder zu aktivieren, klicken Sie auf die Schaltfläche "Aktive Richtlinie wieder aktivieren"; daraufhin wird ein Job erstellt. Nachdem der Job genehmigt wurde, tritt die letzte aktive Snapshotrichtlinie in Kraft.

Richtlinienänderungen

Richtlinienänderungen können entweder durch Ändern einer Richtlinie, die auf einen geschützten Pfad angewendet wird, durch Hinzufügen eines neuen geschützten Pfads oder durch Hinzufügen eines verschlüsselten Datenträgers vorgenommen werden.

Änderungen an einer Richtlinie ändern nicht den Verschlüsselungsstatus der aktuellen Daten. Sie wirken sich nur auf die Verarbeitung von Daten aus, die nach der erneuten Bereitstellung der Richtlinie erstellt werden.

Kritischer Hinweis

Löschen Sie keine Datenträgerrichtlinie von einem aktiven Agenten. Dies wird nicht unterstützt, da es das Zielsystem in einen inkonstanten Status versetzen könnte.

Sie können einen neuen Datenträger auf einem aktiven Agenten erstellen und den alten Datenträger ungenutzt beibehalten.

Alternativ können Sie einen neuen Agenten erstellen und bereitstellen.

Richtlinie bearbeiten

Durch Bearbeiten der Richtlinie eines Agenten können der Dateirichtlinienpfad oder die Pfadgruppe und die Datentypzuordnung oder verschlüsselte Datenträger geändert werden.

Wenn der Datentyp in einen bearbeitbaren Datentyp geändert wird, ist eine integrierte Bearbeitung dieser Felder verfügbar. Klicken Sie zum Bearbeiten der Richtlinie auf die Schaltfläche "Hauptrichtlinie bearbeiten".

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

Abbildung 1. Beispiel für Agent vom Typ 'Datenträger mit Richtlinie'

Dadurch wird die Seite 'Hauptrichtlinie bearbeiten' geöffnet.

Edit Master Policy

File Policy Path (or Path Set)	Pathset1	
<input type="checkbox"/> 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
<input type="checkbox"/> Autogenerate Key	

Add Volume
Add Path

Save
Save and Snapshot
Save, Snapshot and Activate
Cancel

Hinweis

Durch das Bearbeiten der Hauptrichtlinie werden keine Snapshots geändert.

•

Pfad hinzufügen

Informationen zu diesem Vorgang

Klicken Sie auf die Schaltfläche “Pfad hinzufügen”, um einen Pfad unter der Richtlinie hinzuzufügen.

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



Dadurch wird ein neuer Abschnitt für die Eingabe der Richtlinie geöffnet (ähnlich wie bei der ursprünglichen Bereitstellung).

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

☐ Autogenerate Key

Datatype **Required**

(remember to fill out any empty values below)

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

Datenträger hinzufügen

Informationen zu diesem Vorgang

Klicken Sie zum Hinzufügen eines neuen Datenträgers auf die Schaltfläche “Datenträger hinzufügen”.

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

Dadurch wird ein neuer Abschnitt für die Eingabe geöffnet (ähnlich wie bei der ursprünglichen Bereitstellung).

Volume Policy Path Delete

Device Label Required

Key ☐ Autogenerate Key Required

Add Volume Add Path

Save Save and Snapshot Save, Snapshot and Activate Cancel

Pfad löschen

Informationen zu diesem Vorgang

Zum Löschen eines Pfads aus dem Richtlinienchutz klicken Sie auf die Schaltfläche “Löschen” für den beabsichtigten Pfad. Wenn die Richtlinienkonfiguration gespeichert wurde, ein Snapshot von ihr erstellt und sie aktiviert wurde, wird der Pfad nicht mehr durch die Zugriffssteuerungsrichtlinie geschützt. Neue Dateien, die in das Verzeichnis geschrieben werden, werden nicht mehr verschlüsselt. Vorhandene Dateien bleiben im verschlüsselten Status und sind nicht zugänglich.

Anmerkung: Um den ununterbrochenen Zugriff auf Ihre Daten sicherzustellen, sollten Sie die Daten aus dem geschützten Verzeichnispfad kopieren bzw. versetzen, bevor Sie den Pfad aus der Richtlinie löschen.

Edit Master Policy

File Policy Path (or Path Set)

☐ 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

Agentensnapshots

Agentensnapshots sind der permanente Speicher von zugeordneten Richtlinienkonfigurationen für Agenten. Snapshots werden indexiert und haben den Status 'Aktiv' oder 'Inaktiv'. Es ist nur ein aktiver Snapshot pro Agent vorhanden. Dies ist die Richtlinienkonfiguration, die zurzeit auf den Agenten angewendet wird. Zum Ändern der Agentenrichtlinienkonfiguration muss der Administrator einen neuen Snapshot erstellen, der die gewünschten Änderungen abbildet, und den neuen Snapshot aktivieren.

Agentenbearbeitungen und Snapshots speichern

Wenn Sie die Bearbeitung einer Agentenrichtlinie abgeschlossen haben, können Sie die Änderungen abbrechen, die Änderungen speichern, die Änderungen speichern und einen Snapshot der Änderungen erstellen oder die Änderungen speichern, einen Snapshot der Änderungen erstellen und die Änderungen aktivieren.

Änderungen abbrechen

Durch das Abbrechen der Änderungen wird die Richtlinienkonfiguration wiederhergestellt, die vor den Änderungen vorhanden war.

Änderungen speichern

Durch das Speichern von Änderungen werden diese Änderungen zur künftigen Verwendung gespeichert, jedoch wird kein Snapshot erstellt, sodass die Änderungen nicht auf den Agenten angewendet werden können.

Speichern und Snapshot erstellen

Durch Speichern und Erstellen eines Snapshots der Änderungen werden diese Änderungen zur künftigen Verwendung gespeichert und ein Snapshot erstellt, der zu einem späteren Zeitpunkt angezeigt und aktiviert werden kann.

Speichern, Snapshot erstellen und aktivieren

Durch Speichern, Erstellen eines Snapshots und Aktivieren der Änderungen werden diese Änderungen zur künftigen Verwendung gespeichert, ein Snapshot erstellt, der zu einem späteren Zeitpunkt angezeigt werden kann, und sofort ein Job erstellt, um diese Änderungen auf den Agenten anzuwenden.

Anmerkung: Snapshotänderungen oder -aktualisierungen werden erst wirksam, wenn der Agent mit dem PPM-Server kommunizieren kann. Der erstellte Job bleibt so lange aktiv, bis eine erfolgreiche Kommunikation zwischen PPM und dem Agenten hergestellt wurde oder der Agent vom PPM-Server entfernt wird.

Snapshots verwalten

Alle Snapshots, die einem Agenten zugeordnet sind, können über die Schaltfläche “Snapshots verwalten” der Ansicht für Agenteninfos angezeigt werden.

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

Durch Klicken auf die Schaltfläche wird ein Dialog für die Snapshotverwaltung geöffnet. Über diesen Dialog kann ein Sicherheitsadministrator Snapshotdetails anzeigen, einen Snapshot aktivieren, die einem Snapshot zugeordnete Richtlinie inaktivieren und einen Snapshot löschen.

Agent Snapshots

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

[OK](#)

Hinweis

Durch Ändern des aktiven Snapshots wird die Hauptrichtlinie nicht geändert.

Details anzeigen

Mit dieser Schaltfläche wird eine Zusammenfassungsansicht der Richtlinie angezeigt, die dem Snapshot zugeordnet ist.

Notes

Protection Policy

File Policy Path /protected2

Datatype Datatype1

Selector	Operation	Key	Actions

Back

OK

Snapshot aktivieren

Durch Aktivieren eines Snapshots wird ein Job zum Senden der Richtlinie an den Agenten erstellt. Sobald der Snapshot genehmigt ist, geht er in den aktiven Status über und die zugehörige Richtlinie überschreibt jede andere Richtlinie, die im Agenten vorhanden ist.

Anmerkung: Snapshotänderungen oder -aktualisierungen werden erst wirksam, wenn der Agent mit dem PPM-Server kommunizieren kann. Der erstellte Job bleibt so lange aktiv, bis eine erfolgreiche Kommunikation zwischen PPM und dem Agenten hergestellt wurde oder der Agent vom PPM-Server entfernt wird.

Snapshot löschen

Ein inaktiver Snapshot kann gelöscht werden. Durch das Löschen wird der Snapshot permanent aus MDE entfernt.

Dateiagenten deinstallieren

Informationen zu diesem Vorgang

Wenn Sie einen Dateiagenten entfernen möchten, können Sie dazu die folgenden Schritte ausführen:

Kopieren Sie die Daten aus den geschützten Verzeichnissen heraus. Dies stellt sicher, dass die Daten nach der Inaktivierung der Richtlinie nicht unzugänglich sind.

Führen Sie die folgenden Schritte aus, um die Agentensoftware zu entfernen:

Vorgehensweise

1. Linux – Führen Sie die Prozedur als Rootbenutzer aus.

a) Stoppen Sie den Service 'spx-policyagent'.

- Führen Sie unter CentOS 7 folgenden Befehl aus:

```
systemctl stop spx-policyagent
```

- Führen Sie unter CentOS 6 folgenden Befehl aus:

```
service spx-policyagent stop
```

- b) Führen Sie den Befehl `cd /opt/ibm/mde/spxagent/spx-fileagent/` aus.
 - c) Führen Sie den Befehl `./fileagent_uninstall.sh` aus.
 - d) Geben Sie `y` ein, um die Deinstallationsaktion zu bestätigen.
 - e) Starten Sie das System neu.
2. AIX - Führen Sie die Prozedur als Rootbenutzer aus.
- a) Stoppen Sie den Service 'spx-policyagent'.

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

- b) Stoppen Sie die Kernelmodule.

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

- c) Entfernen Sie den RPM.

```
rpm -e fileagent*
```

Anmerkung: Führen Sie den folgenden Befehl aus, wenn Sie den genauen RPM-Namen anstelle des Platzhalters verwenden wollen:

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

- d) Starten Sie das System neu.

3. Windows – Führen Sie die Prozedur als Administrator aus.

- Über die grafische Benutzeroberfläche von Windows:
 - Navigieren Sie zu 'Programme hinzufügen/entfernen' in der Systemsteuerung.
 - Wählen Sie "FileAgent" für die Deinstallation aus.
 - Starten Sie das System erneut, wenn Sie dazu aufgefordert werden.
- Über die PowerShell-Befehlszeilenschnittstelle (CLI)
 - `msiexec /x <Pfad zu FileAgent.msi>`
 - Starten Sie das System erneut, wenn Sie dazu aufgefordert werden.

Wichtig: Berechtigte Benutzer sollten nicht den Befehl 'mv' (move) verwenden, um Daten in die verschlüsselte Position oder aus der verschlüsselten Position zu versetzen, da dies zu Problemen mit der MDE-Richtlinie führen kann.

Sichern Sie die Daten zuerst mit dem Befehl 'cp' (copy) aus/in geschützten (verschlüsselten) Verzeichnissen.

Datenträgeragenten deinstallieren

Datenträgeragenten deinstallieren

- Linux – Führen Sie die Prozedur als Rootbenutzer aus.

1. Hängen Sie den geschützten Datenträger ab.

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

2. Stoppen Sie den Service 'spx-policyagent'.

- Führen Sie unter CentOS 7 folgenden Befehl aus:

```
systemctl stop spx-policyagent
```


- Führen Sie unter CentOS 6 folgenden Befehl aus:

```
service spx-policyagent stop
```

3. Führen Sie den Befehl `cd /opt/ibm/mde/spxagent/spx-volumeagent/` aus.
 4. Führen Sie den Befehl `./volumeagent_uninstall.sh` aus.
 5. Geben Sie `y` ein, um die Deinstallationsaktion zu bestätigen.
 6. Führen Sie einen Warmstart durch.
- Windows – Führen Sie die Prozedur als Administrator aus.
 - Über die grafische Benutzeroberfläche von Windows:
 - Navigieren Sie zu 'Programme hinzufügen/entfernen' in der Systemsteuerung.
 - Wählen Sie "VolumeAgent" für die Deinstallation aus.
 - Starten Sie das System erneut, wenn Sie dazu aufgefordert werden.
 - Über die PowerShell-Befehlszeilenschnittstelle (CLI)
 - `msiexec/x <Pfad zu VolumeAgent.msi>`
 - Starten Sie das System erneut, wenn Sie dazu aufgefordert werden.

Agenten vom Typ 'Datenträger mit Richtlinie' deinstallieren

Informationen zu diesem Vorgang

Vorgehensweise

1. Linux – Führen Sie die Prozedur als Rootbenutzer aus.

- a) Hängen Sie das geschützte Verzeichnis ab.

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

- b) Stoppen Sie den Service 'spx-policyagent'.

- Führen Sie unter CentOS 7 folgenden Befehl aus:

```
systemctl stop spx-policyagent
```

- Führen Sie unter CentOS 6 folgenden Befehl aus:

```
service spx-policyagent stop
```

- c) Führen Sie den Befehl `cd /opt/ibm/mde/spxagent/spx-hybridagent/` aus.
 - d) Führen Sie den Befehl `./hybridagent_uninstall.sh` aus.
 - e) Geben Sie `y` ein, um die Deinstallationsaktion zu bestätigen.
 - f) Starten Sie das System neu.
2. Windows – Führen Sie die Prozedur als Administrator aus.
 - Über die grafische Benutzeroberfläche von Windows:
 - Navigieren Sie zu 'Programme hinzufügen/entfernen' in der Systemsteuerung.
 - Wählen Sie "HybridAgent" für die Deinstallation aus.
 - Starten Sie das System erneut, wenn Sie dazu aufgefordert werden.
 - Über die PowerShell-Befehlszeilenschnittstelle (CLI)
 - Führen Sie den Befehl `msiexec /x <Pfad zu Hybridagent/msi>` aus.
 - Starten Sie das System erneut, wenn Sie dazu aufgefordert werden.

Agent vom Typ 'Objektspeicher' deinstallieren

Informationen zu diesem Vorgang

Alle Benutzerkonten und -berechtigungen werden so lange in PPM gespeichert, bis der Agent aus PPM gelöscht wird.

Vorgehensweise

1. Linux – Führen Sie die Prozedur als Rootbenutzer aus.
2. Stoppen Sie den Service 'spx-policyagent'.

```
systemctl stop spx
```

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

```
./objectagent_uninstall.sh
```

4. Geben Sie 'y' ein, um die Deinstallationsaktion zu bestätigen.
5. Starten Sie das System neu.

Agenten aus MDE entfernen

Ein von MDE verwalteter Agent kann aus dem Systemumfeld über die MDE-Benutzerschnittstelle (GUI) entfernt werden.

Klicken Sie zum Löschen eines Agenten auf die Schaltfläche 'Agent löschen'. Dadurch wird ein Job erstellt. Sobald der Job genehmigt wurde, wird der Agent aus MDE gelöscht.

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

Kritischer Hinweis

- Durch das Entfernen eines Agenten aus MDE kann der Agent keine Verbindung mehr zu MDE herstellen, sodass die zurzeit geschützten Daten beim nächsten Neustart des Agenten unzugänglich werden.
- Durch das Entfernen eines Agenten werden die Daten nicht entschlüsselt.

Agentendienstprogramme

Die MDE-Agenten stellen eine Reihe von Dienstprogrammen bereit, die Sie bei der Konfiguration eines Agenten und beim Schutz sensibler Daten unterstützen. Weitere Informationen zu einem Dienstprogramm erhalten Sie, wenn Sie das gewünschte Dienstprogramm mit der Option “--help” ausführen.

Dienstprogramm	Funktion	Datenträger	Datenträger mit Richtlinie	Datei mit Richtlinie	Objektspeicher
spxbackup	Erstellt eine verschlüsselte Sicherung der angegebenen Daten.	Ja	Ja	Ja	Nein

spxconvert	Konvertiert vorhandene Daten in einem geschützten Verzeichnis auf der Basis der definierten Richtlinie vom nicht verschlüsselten zum verschlüsselten Status.	Nein	Nein	Ja	Nein
spxdevice	Ordnet einen Plattendatenträger oder eine Partition einem definierten Einheitenamen zu.	Ja	Ja	Nein	Nein
spxhash	Generiert einen versionsspezifischen Hash eines angegebenen Prozesses.	Nein	Ja	Ja	Nein
spximport	Importiert verschlüsselte Daten in ein Verzeichnis, ohne die Daten doppelt zu verschlüsseln.	Nein	Nein	Ja (Nur Windows)	Nein
spxinfo	Listet die über eine bestimmte Richtlinie geschützten Verzeichnisse auf.	Nein	Ja	Ja	Nein
spxobject	Listet den Objektspeicher auf.	Nein	Nein	Nein	Ja
spxrestore	Stellt eine verschlüsselte Sicherung der angegebenen Daten wieder her.	Ja	Ja	Ja	Nein

Kapitel 12. Operationen

Sicherung und Wiederherstellung von Produktdaten

MDE unterstützt die Möglichkeit einer zeitpunktbezogenen Sicherung von MDE-PPM-Daten. Diese zeitpunktbezogene Sicherung kann wiederhergestellt werden, um MDE auf den Status zum Zeitpunkt der Sicherungserfassung zurückzusetzen.

Anmerkung: Stoppen Sie vor der Durchführung einer Sicherung oder Wiederherstellung den MDE-Service durch den Befehl “systemctl stop spsd” in der MDE-VM.

```
sudo systemctl stop spsd
```

Sicherung von Produktdaten

Informationen zu diesem Vorgang

Produktsicherungen werden durch ein Befehlszeilenscript durchgeführt, das innerhalb der MDE-VM ausgeführt wird.

Das Sicherungsscript 'spsd-backup' befindet sich in der MDE-VM im Verzeichnis /opt/securityfirst/spsd/bin. Es erstellt automatisch eine neue Datei und versieht den Namen der Datei mit einer Zeitmarke des Zeitpunkts, zu dem die Sicherung erstellt wurde.

```
sudo /opt/securityfirst/spsd/bin/spsd-backup --help
Syntax: spsd-backup [--nodb] [--help]
-----
--nodb Datenbank nicht sichern
--help Diese Hilfe anzeigen
```

Führen Sie eine Sicherung wie folgt aus:

```
sudo /opt/securityfirst/spsd/bin/spsd-backup
Speicherauszug der lokalen Buildinformationen wird erstellt
Speicherauszug der lokalen Buildinformationen wird erstellt
Speicherauszug der lokalen Buildinformationen wird erstellt
Sicherung abgeschlossen - erstellt wurde: spsd-backup-2017-04-04T144448-0700.tar.gz
```

Wiederherstellung von Produktdaten

Informationen zu diesem Vorgang

Die Produktwiederherstellung wird durch ein Befehlszeilenscript durchgeführt, das innerhalb der MDE-VM ausgeführt wird.

Das Wiederherstellungsscript 'spsd-restore' befindet sich im Verzeichnis /opt/securityfirst/spsd/bin.

```
sudo /opt/securityfirst/spsd/bin/spsd-restore --help
Syntax: spsd-restore [--nodb] [--noprops] [--help] Dateiname
-----
--nodb Datenbank nicht schreiben
--noprops Lokale Eigenschaften nicht schreiben
--help Diese Hilfe anzeigen
```

Führen Sie eine Wiederherstellung wie folgt aus:

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

Anmerkung: Nach der Wiederherstellung einer Sicherungsdatei werden die Änderungen beim nächsten Start von MDE angewendet.

Kernelaktualisierung

Informationen zu diesem Vorgang

Wenn für einen Agenten, der unter Red Hat Enterprise Linux 7 oder CentOS 7 ausgeführt wird, eine Kernelaktualisierung erforderlich ist, befolgen Sie folgende Richtlinien:

- Wenn die Betriebssystem-/Kernelaktualisierung im selben Release erfolgt, wird der neue Kernel automatisch unterstützt.
- Wenn die Betriebssystem-/Kernelaktualisierung für ein höheres Release erfolgt (z. B. RHEL 7.2 -> 7.4), führen Sie die folgenden Schritte aus, um Unterstützung für den neuen Kernel zu erhalten:
 - Beispiel: Das Agenteninstallationspaket wurde in '/root/agent' gespeichert.

```
cd /root/agent/spx-installer
./agent_setup.sh -d /root/agent
Führen Sie einen Warmstart durch.
```

Diese Schritte sind nicht für Agenten erforderlich, die unter Red Hat Enterprise Linux 6 oder CentOS 6 ausgeführt werden.

Upgrade

Führen Sie die folgenden Schritte aus, um ein Upgrade des MDE-Produkts auf eine neue Version durchzuführen.

Anmerkung: Diese Schritte gelten für MDE Open Virtualization Appliance (OVA). Wenn eine Nicht-OVA-Installation durchgeführt wurde, sind die Verzeichnisse möglicherweise unterschiedlich.

Für den MDE-Server

Informationen zu diesem Vorgang

Vorgehensweise

1. Stoppen Sie als Rootbenutzer den PPM-Richtlinienservice.

```
systemctl stop spsd
```

2. Sichern Sie die MDE-Daten:

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

3. Versetzen Sie die neue Version der MDE-Bin-Datei in das Verzeichnis /home/admin.
4. Löschen Sie das vorhandene RPM-Verzeichnis.

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

5. Ändern Sie die Zugriffsberechtigung für die MDE-Bin-Datei.

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

6. Führen Sie die MDE-Bin-Datei der neuen Version aus.

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

7. Installieren Sie die RPMs.

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

8. Führen Sie das Upgrade-Script aus.

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

9. Starten Sie den PPM-Richtlinienservice erneut:

```
systemctl start spsd
```

Upgrade von vorheriger Version durchführen

Informationen zu diesem Vorgang

Die folgenden Schritte müssen ausgeführt werden, um die Funktion der Richtlinie zu ermöglichen:

Vorgehensweise

1. Navigieren Sie zur Seite "Agenteninfo".
2. Klicken Sie auf "Haupttrichtlinie bearbeiten".
3. Klicken Sie auf "Speichern, Snapshot erstellen und aktivieren".
4. Genehmigen Sie den Job.
5. Kehren Sie zur Agenten-VM zurück und versuchen Sie, eine Lese-/Schreibaktion für ein Verzeichnis in der Richtlinie auszuführen, indem Sie als Benutzer in der Richtlinie angemeldet sind, der Zugriffsberechtigungen für dieses Verzeichnis hat. Prüfen Sie außerdem, ob kein nicht definierter Benutzer zugelassen wird.

Für die Ziel-VM von Agenten

Linux-/AIX-Agenten

Informationen zu diesem Vorgang

Vorgehensweise

1. Erstellen Sie ein neues Agentenverzeichnis und wechseln Sie in das neue Agentenverzeichnis.

```
mkdir [neues_Agentenverzeichnis]  
cd [neues_Agentenverzeichnis]
```

2. Laden Sie das Installationsbundle für den betreffenden Agenten herunter (bzw. verwenden Sie den Befehl 'curl').

```
curl --header "Accept: application/x-tar" -u  
benutzername:kennwort  
https://<IP-Adresse von PPM>/rest/agents/Agenten-ID #/install_bundle> Name_des_Installations-  
bundles.tar
```

3. Dekomprimieren Sie das Installationsbundle.

```
tar xvf <Name_des_Installationsbundles>.tar
```

4. Führen Sie das Script 'setup.sh' aus, um den Agenten erneut zu installieren.

```
./setup.sh
```

5. Geben Sie yes ('ja') bei der entsprechenden Eingabeaufforderung ein, um den Agenten neu zu starten.

6. Sie können bei Bedarf alle vorherigen Installationsdateien aus dem vorherigen Agentenverzeichnis löschen.

```
rm -rf [/vorheriges_Agentenverzeichnis]
```

Windows-Agenten

Informationen zu diesem Vorgang

Vorgehensweise

1. Laden Sie das Installationsbundle des betreffenden Agenten herunter.
2. Dekomprimieren Sie das Installationsbundle.
3. Führen Sie die .msi-Installationsdatei aus, um die neue Agentensoftware zu installieren.
4. Geben Sie 'yes' ('ja') bei entsprechender Eingabeaufforderung ein, um den Agenten neu zu starten.

Servicedaten

Servicedaten erfassen

Die Servicedatenerfassung erfolgt durch ein Script, das in der MDE-VM ausgeführt wird.

Das Script 'spsd-service' befindet sich in der MDE-VM im Verzeichnis '/opt/securityfirst/spsd/bin'.

```
sudo /opt/securityfirst/spsd/bin/spsd-service --help
Syntax: spsd-service [OPTIONEN]
-----
OPTIONEN:
--nodb Speicherauszug der Datenbank nicht erstellen
--norest Keine Daten aus der REST-API extrahieren
--nosys Keine Systemdaten extrahieren (/var/log, /proc usw.)
--withcore Kernspeicherauszug von SPSP extrahieren
--help Diese Hilfe anzeigen
```

Gehen Sie wie folgt vor, um eine Servicedatenerfassung auszuführen:

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

Schutzwürdige Informationen aus PPM-Protokollen entfernen

Um den Datenschutz einer PPM-Installation zu gewährleisten, wenn Servicedaten die logischen PPM-Grenzen verlassen, sind in den folgenden MDE-Debugprotokollen schutzwürdige Informationen mit Tags versehen, die eine spezielle Syntax aufweisen:

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

Anmerkung: In einer TAR-Datei mit Service-Daten (dem Ergebnis des obigen Servicedatenerfassungsprozesses) können sich diese Protokolle im Protokollordner befinden.

Die Tags sind als #<Tagname>(<Tagdaten>) formatiert, wobei <Tagdaten> mit den Daten ersetzt wird, die in Tags eingeschlossen werden sollen, und <Tagname> für Folgendes stehen kann:

- user: Zum Kennzeichnen von Benutzernamen, ganz gleich, ob es sich dabei um MDE-Benutzer oder Benutzer eines externen Service handelt, mit dem MDE integriert wird. *Beispiel: #user(admin)*
- group: Zum Kennzeichnen von Gruppennamen. *Beispiel: #group(domainusers)*

- email: Zum Kennzeichnen von E-Mail-Adressen. *Beispiel: #email(example@example.com)*
- ip: Zum Kennzeichnen von IP-Adressen. *Beispiel: #ip(192.168.0.5)*
- host: Zum Kennzeichnen von Netzhostenamen. *Beispiel: #host(dns.example.com)*
- key: Zum Kennzeichnen von **öffentlichen** Verschlüsselungsschlüssel oder einem zugehörigen Wert, wie ein verwalteter Schlüsselname. *Beispiel: #key(HRKey2)*
- cert: Zum Kennzeichnen von Zertifikatsdaten, wie ein definierter Name eines Verbindungsagenten. *Beispiel: #cert(C=US, ST=UT, L=Provo, O=Example Corp., OU=architecture, CN=docserver4)*
- fingerprint: Zum Kennzeichnen von Zertifikatsfingerabdrücken. *Beispiel: #fingerprint(41:1A:B9:89:DB:77:90:77:39:D0:DF:5E:98:90:B7:17)*

Tags können mithilfe eines Prozesses aus Servicedaten entfernt werden, bei dem mit #user gekennzeichnete Daten aus der Datei 'bundleAll.log' entfernt werden:

```
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
```


Anhang A. Beispiele für Agenteninstallationsprozesse

In den folgenden Abschnitten wird der allgemeine Prozess zur Installation des Agenteninstallationsbundes skizziert. Dabei handelt es sich lediglich um Beispielmethoden und nicht um unterstützte Installationsanweisungen.

Red Hat-/CentOS-Prozess

Informationen zu diesem Vorgang

Installationsbundle mithilfe von CURL übertragen:

Vorgehensweise

1. Melden Sie sich am Zielsystem an.
2. Stellen Sie sicher, dass eine gültige Netzverbindung zum MDE-Server besteht.
3. Stellen Sie sicher, dass alle Benutzer, Gruppen und Pfade oder Einheiten, die in der Richtlinie angegeben werden, im System erstellt, angehängt und konfiguriert sind.
4. Melden Sie sich bei MDE an.
5. Stellen Sie in MDE einen Agenten für das Zielsystem bereit.
6. Zeigen Sie in MDE die Agentendetails an und notieren Sie die Download-URL.

Users

Authorized Users admin

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

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. Erstellen Sie auf dem Zielsystem ein Verzeichnis für den Agenten-Download und wechseln Sie in dieses Verzeichnis.
8. Laden Sie das TAR-Bundle mit dem folgenden curl-Befehl herunter:

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

Beispiel mit einem definierten PPM-Benutzer:

```
[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
```

Beispiel mit einem in LDAP definierten PPM-Benutzer:

```
[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
```

(Bei Verwendung der Verzeichniskennung "tenant1" mit Benutzer "john" und Kennwort "secret")

9. Dekomprimieren Sie das Paket auf dem Zielsystem:

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

10. Führen Sie das Setup-Script auf dem Zielsystem als Rootbenutzer aus:

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

11. Wenn die Ausführung des Setup-Skripts abgeschlossen ist, ist der Agent installiert und die Richtlinie wird von MDE heruntergeladen und in Kraft gesetzt.

AIX-Prozess

Informationen zu diesem Vorgang

Installationsbundle übertragen

1. Melden Sie sich am Zielsystem an.
2. Stellen Sie sicher, dass eine gültige Netzverbindung zum MDE-Server besteht.
3. Stellen Sie sicher, dass alle Benutzer, Gruppen und Pfade oder Einheiten, die in der Richtlinie angegeben werden, im System erstellt, angehängt und konfiguriert sind.
4. Melden Sie sich bei MDE an.
5. Stellen Sie in MDE einen Agenten für das Zielsystem bereit.
6. Zeigen Sie die Agentendetails in MDE an und notieren Sie die Download-URL

Users

Authorized Users admin

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

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. Erstellen Sie auf dem Zielsystem ein Verzeichnis für den Agenten-Download und wechseln Sie in dieses Verzeichnis.
8. Übertragen Sie das Bundle auf das Zielsystem.
9. Dekomprimieren Sie das Paket auf dem Zielsystem wie folgt:

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

10. Führen Sie das Setup-Skript auf dem Zielsystem als Rootbenutzer aus:

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

11. Wenn die Ausführung des Setup-Skripts abgeschlossen ist, ist der Agent installiert und die Richtlinie wird von MDE heruntergeladen und in Kraft gesetzt.

Windows Server-Prozess

Informationen zu diesem Vorgang

Installationsbundle übertragen

Vorgehensweise

1. Melden Sie sich am Zielsystem an.
2. Stellen Sie sicher, dass eine gültige Netzverbindung zum MDE-Server besteht.

3. Stellen Sie sicher, dass alle Benutzer, Gruppen und Pfade oder Einheiten, die in der Richtlinie angegeben werden, im System erstellt, angehängt und konfiguriert sind.
4. Melden Sie sich bei MDE an.
5. Stellen Sie in MDE einen Agenten für das Zielsystem bereit.
6. Zeigen Sie in MDE die Agentendetails an und notieren Sie die Download-URL.

Users

Authorized Users admin

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

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. Klicken Sie auf “ZIP-Bundle herunterladen”, um das ZIP-Dateibundle für die Agentensoftware auf das lokale System herunterzuladen.
8. Übertragen Sie das Installationsbundle auf das Zielsystem.
9. Extrahieren Sie auf dem Zielsystem den Inhalt des ZIP-Dateibundles.
10. Führen Sie die MSI-Datei des Installationsbundles aus.

FileAgent-<Version>.msi

Beispiel:

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

11. Sobald die Ausführung des Setup-Skripts abgeschlossen und der Agent ordnungsgemäß installiert ist, wird die Richtlinie wirksam.

Anmerkung: Es muss ein Warmstart durchgeführt werden. Um die angeforderte Eingabeaufforderung für einen Warmstart zu umgehen, können Sie den Befehl ohne Option für einen Warmstart ausführen:
msiexec /i <Agentendateiname_Version.msi> NO_REBOOT_PROMPT=1

Anhang B. Beispielzertifikate einer Zertifizierungsstelle (CA)

Informationen zu diesem Vorgang

MDE erfordert Zertifikate, die von einer Zertifizierungsstelle (CA, Certificate Authority) signiert sind, um eine sichere Sitzung zwischen dem Management-Server (PPM) und Agenten einzurichten. Die folgenden Elemente sind erforderlich:

- Keystore
- Truststore
- CA-Zertifikatsbundle

Zum Signieren von Zertifikaten kann eine interne RSA-basierte Zertifizierungsstelle (CA) des Unternehmens oder eine Zertifizierungsstelle eines anderen Anbieters verwendet werden. Im folgenden Linux-Beispiel werden die folgenden Elemente erstellt:

- Eine Zertifikatssignieranforderung (CSR, Certificate Signing Request) wird erstellt und zum Signieren an die Zertifizierungsstelle gesendet. Das signierte Zertifikat und der Schlüssel werden zum Erstellen eines Keystores kombiniert.
- Ein Truststore wird mit dem Zertifikatsbundle der Zertifizierungsstelle erstellt.
- Ein Agentenzertifikat wird erstellt. Solche Zertifikate sind für die Kommunikation zwischen PPM und Agenten erforderlich.

Dieses Beispiel wird nur aus Gründen der Benutzerfreundlichkeit bereitgestellt. Sie sollten sich an Ihre Zertifizierungsstelle (CA) halten, wenn Sie Zertifikate generieren, die signiert werden müssen. Namen in eckigen Klammern [name.pem] stellen Dateinamen dar, die anders lauten oder geändert werden können, wenn Sie Zertifikate des Unternehmens oder eines Drittanbieters verwenden.

Zum Erstellen eines Keystores müssen Sie eine Zertifikatssignieranforderung (CSR) an eine interne Zertifizierungsstelle des Unternehmens oder an eine Zertifizierungsstelle eines Drittanbieters übergeben.

Vorgehensweise

1. Erstellen Sie eine OpenSSL-Konfigurationsdatei (z. B. ppm.cnf), die die folgenden Informationen enthält:

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

[req_distinguished_name]
C      = Ihr_Land
ST     = Ihr_Bundesland
L      = Ihre_Ländereinstellung_(Stadt)
O      = Ihre_Organisation
OU     = Ihre_Organisationseinheit_(Abteilung)
CN     = Ihr_PPM-Host.Ihre_Domäne

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

[alt_names]
DNS.1      = Ihr_PPM-Host.Ihre_Domäne
IP.1       = Ihre_PPM-IP-Adresse
```

Sie müssen die Abschnitte [req_distinguished_name] und [alt_names] mit den Informationen für Ihre Organisation aktualisieren.

2. Erstellen Sie eine PPM-Zertifikatssignieranforderung.

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

3. Die Zertifikatssignieranforderung [csr.pem] muss von der Zertifizierungsstelle (CA) signiert werden.
4. Stellen Sie nach dem Empfang des signierten Zertifikats von der Zertifizierungsstelle sicher, dass die erweiterte Schlüsselnutzung und alternative Namen für das Subjekt vorhanden sind.

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

5. Kombinieren Sie das signierte Zertifikat und den Schlüssel (Schlüssel aus Schritt 2).

```
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
```

Zum Erstellen eines Truststores benötigen Sie das Zertifikat der Zertifizierungsstelle, das sie zum Signieren von Zertifikatssignieranforderungen (CSRs) verwendet. Dies wird auch als CA-Zertifikatsbundle bezeichnet. Ersetzen Sie nachfolgend "ca_bundle.crt" durch den tatsächlichen Namen dieses Zertifikats.

- a. Erstellen Sie den Truststore mit dem Zertifikatsbundle der Zertifizierungsstelle. Wenn mehrere Zertifikate im Zertifikatsbundle der Zertifizierungsstelle vorhanden sind, müssen Sie getrennt und einzeln in ein Truststore importiert werden.

```
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. Kopieren Sie die resultierenden Dateien *.jks und [ca_bundle.crt] auf den PPM-Server in ein sicheres Verzeichnis (d. h. /etc/ppm/certs). Diese Position wird angegeben, wenn Sie die Web- und Agenteneigenschaftendateien mit dem Script 'spsd-certsetup' aktualisieren. (Siehe Management-Server-Konfiguration weiter unten.)

Es ist zudem ein MDE-Agentenzertifikat erforderlich.

- a. Erstellen Sie eine OpenSSL-Konfigurationsdatei (z. B. host01.cnf), die die folgenden Informationen enthält:

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

[req_distinguished_name]
C = Ihr_Land
ST = Ihr_Bundesland
L = Ihre_Ländereinstellung_(Stadt)
O = Ihre_Organisation
OU = Ihre_Organisationseinheit_(Abteilung)
CN = Ihr_Agentenhost.Ihre_Domäne

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

[alt_names]
DNS.1 = Ihr_Agentenhost.Ihre_Domäne
IP.1 = Ihre_Agenten-IP-Adresse
```


Sie müssen die Abschnitte [req_distinguishd_name] und [alt_names] mit den Informationen für Ihre Organisation aktualisieren.

- b. Erstellen Sie eine Zertifikatssignieranforderung (CSR) für den MDE-Agenten.

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

- c. Fordern Sie eine Zertifikatssignieranforderung an, die von einer Zertifizierungsstelle (CA) signiert ist.

- d. Stellen Sie nach dem Empfang des signierten Zertifikats von der Zertifizierungsstelle sicher, dass die erweiterte Schlüsselnutzung und alternative Namen für den Betreff vorhanden sind.

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

- e. Wenn das Agentenzertifikat von einer anderen Zertifizierungsstelle signiert wurde als das PPM-Zertifikat, dann muss das Zertifikatsbundle der Zertifizierungsstelle in den PPM-Truststore importiert werden. Informationen hierzu finden Sie in Schritt 5 im Erstellungsprozess für das Zertifikat weiter oben.

- f. Kombinieren Sie das signierte Zertifikat und den Schlüssel.

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

- g. Verwenden Sie das Zertifikat/Schlüssel-Paar [host01.pem] beim Erstellen eines Agenten für diesen Host in MDE.

```
a. [host01.pem] wird mit einem Browser während der PPM-Agentenerstellung  
hochgeladen.
```

Kopieren Sie die Datei [host01.pem] auf Ihre Workstation oder auf eine gemeinsam genutzte Ressource, sodass sie während der PPM-Agentenerstellung zugänglich ist.

Befolgen Sie diesen Prozess für jeden Host, auf dem ein Agent installiert wird.

Management-Server-Konfiguration

Für die Management-Server-Konfiguration müssen die Zertifikate aktualisiert werden, bevor Richtlini-agenten konfiguriert werden. Dazu muss das bereitgestellte Script (/opt/securityfirst/spsd/bin/spsd-certsetup) auf dem Server ausgeführt werden, nachdem der Keystore und der Truststore Ihres Unternehmens und ein CA-Zertifikatsbundle hochgeladen wurden. (Informationen finden Sie im Handbuch 'Verwaltung' im Abschnitt 'Einstellungen für Serverzertifikate'.) Außerdem muss der Service 'spsd' erneut gestartet oder der Management-Server (PPM) erneut gestartet werden. Ohne diese Aktion können Agenten nicht mit dem MDE-Management-Server kommunizieren.

Wenn Zertifikate nicht aktualisiert wurden und ein Agent konfiguriert wurde, kann die Kommunikation zwischen dem Agenten und dem MDE-Management-Server wiederhergestellt werden, indem das Zertifikatsaktualisierungsscript ausgeführt und anschließend das Agentenzertifikat auf der Seite 'Agenteninfo' aktualisiert wird.

Anhang C. Beispielkonvertierung zum Erstellen einer PKCS12-Datei

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um den privaten Clientschlüssel und das Clientzertifikat in einer einzelnen PKCS12-Datei (PKCS12 - Public Key Cryptography Standard #12) zu kombinieren:

```
[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
```

Anhang D. Empfehlungen und Warnungen

Zugeordnete Schlüssel ändern

Übersicht

Sie haben Daten in einem geschützten Verzeichnis und wollen den Schlüssel ändern, der diesem Verzeichnis zugeordnet ist.

Hintergrund

Daten in einem Verzeichnis werden mit dem Schlüssel verschlüsselt, der bei der Datenerstellung (oder beim Versetzen der Daten in dieses Verzeichnis) definiert ist. Durch das Ändern eines Richtlinienschlüssels werden die vorher vorhandenen Daten nicht auf den neuen Schlüssel migriert.

Wenn eine Richtlinie auf einen Agenten angewendet wurde und aktiv ist, kann es potenziell sehr gefährlich sein, die Schlüsselwerte der geschützten Verzeichnisse zu ändern. Obwohl es nicht streng verboten ist, kann das Ändern eines Schlüsselwerts zu Datenverlust führen.

Empfehlung

Wenn der Administrator ein ganzes Verzeichnis von einem Schlüssel auf einen anderen migrieren möchte, müssen die Daten in diesem Verzeichnis zunächst an eine andere Position versetzt werden. Wenn das Verzeichnis leer ist, kann der durch eine Richtlinie zugeordnete Schlüsselwert geändert und angewendet werden. Anschließend können die Daten in dieses Verzeichnis zurückversetzt werden und die Daten werden mit dem neuen Schlüssel verschlüsselt.

Warnung

Ändern Sie den Schlüsselwert, der der Richtlinie zugeordnet ist, nicht und aktivieren Sie die Richtlinie nicht, ohne zuvor die Daten aus dem Verzeichnis herauszuversetzen. Wenn die bewährten Verfahrensweisen nicht befolgt werden, werden die ursprünglich im Verzeichnis vorhandenen Daten weiterhin mit dem ursprünglichen Schlüssel verschlüsselt. Sobald die Richtlinie in einen neuen Schlüssel geändert wird, ist kein Zugriff auf die Daten mehr möglich. Wenn außerdem der ursprüngliche Schlüssel rotiert wird, werden die Daten dauerhaft unzugänglich, da es keine Möglichkeit gibt, die Richtlinie in den ursprünglichen Schlüsselwert zurückzuändern.

Schlüsselrotation mit verschlüsselten Sicherungen

Übersicht

Sie wollen eine Sicherung von Daten in einem geschützten Verzeichnis erstellen.

Hintergrund

Sicherungsdaten in ihrem verschlüsselten Format sind an den Schlüsselwert der Daten zum Zeitpunkt der Sicherung gebunden. Wenn der Schlüssel nach der Durchführung der Sicherungsoperation rotiert wird, kann die Sicherung nicht ordnungsgemäß wiederhergestellt werden.

Schlüssel sollten einer geschützten Speicherposition und nicht bestimmten Daten zugeordnet sein. Dadurch lassen sich unerwünschte Datenzugriffsprobleme bei einer Wiederherstellung vermeiden.

Empfehlung

Daten in einem Verzeichnis werden mit dem Schlüssel verschlüsselt, der bei der Datenerstellung (oder beim Versetzen der Daten in dieses Verzeichnis) definiert ist. Es ist ein bewährtes Verfahren, die Daten vor dem Rotieren des Schlüssels zu sichern. Zum Ausführen dieser Aktion kann das Agentendienstprogramm 'spx-backup' verwendet werden. Dieses Dienstprogramm sichert die Daten mit einem Schlüssel, der nicht auf dem geschützten Verzeichnis basiert und der von der Schlüsselrotation nicht beeinflusst wird.

Warnung

Gehen Sie vorsichtig vor, wenn Sie das geschützte Verzeichnis in seiner verschlüsselten Form (d. h. als Plattenimage oder VM-Snapshot) kopieren. Wenn Sie dies tun, können die Daten unzugänglich werden, sobald der ursprüngliche Schlüssel rotiert wird.

Anhang E. Verschlüsselung an der Position

Um die Verschlüsselung in zuvor vorhandenen Verzeichnisstrukturen und Daten zu ermöglichen und den Status von Daten zu einem beliebigen Zeitpunkt zu ermitteln, stellt MDE ein Befehlszeilendienstprogramm mit dem Namen "spxconvert" bereit.

Diese Funktion kann nicht nur zuvor vorhandene Daten verschlüsseln, sondern sie ist auch nützlich, wenn ein Audit durchzuführen ist, wie zum Beispiel im Rahmen des Standards Payment Card Industry (PCI) oder des Health Insurance Portability and Accountability Act (HIPAA).

Anmerkung: Diese Funktion arbeitet nur mit Dateiagenten und deckt keine Datenträger ab, die eine formale Datenmigration erfordern.

Befehlsoptionen

Syntax für den Befehl **spxconvert**: (Parameter werden durch eckige Klammern [] angegeben, die den Typ enthalten)

- h (-?, ?) 'Diesen Hilfedialog ausgeben'
- a 'Audit verschlüsselter Dateien durchführen'
- p [STR] 'Auditpfad'
- e [STR] 'Alle ungeschützten Dateien im Pfad verschlüsseln'
- c 'Auszug aller Kontrollsummen vorheriger/nachträglicher Dateikonvertierungen ausgeben'
- v 'Verbose - Ausführliche Ausgabe mit zusätzlichen Informationen'

Audit (-a)

Standardmäßig wird der Audit für alle Verzeichnisse in der Richtlinie durchgeführt. Dies kann durch die Option -p auf ein einzelnes Verzeichnis eingegrenzt werden. Ein Audit gibt alle Dateien für ein Verzeichnis aus, die nicht verschlüsselt sind, und gibt die Gesamtzahl der Dateien in einem Verzeichnis aus, die verschlüsselt sind.

Encrypt (-e)

Konvertiert alle nicht geschützten Dateien im angegebenen Verzeichnis. Nach Abschluss werden dem Benutzer alle Dateien mit nicht übereinstimmenden Kontrollsummen angezeigt. Durch das optionale Flag -c werden Kontrollsummen für alle Dateien nach Abschluss ausgegeben, nicht nur für Dateien im Konfliktstatus. Kontrollsummen können aus Leistungsgründen nur nach Abschluss ausgegeben werden, da der Systemcache nach der Konvertierung geleert werden muss. Die Leerung (Flush) des Cache nach jeder Datei hätte eine beträchtliche negative Auswirkung auf die Leistung.

Auditschritte

1. Zeigen Sie an, ob Elemente vorhanden sind, deren Verschlüsselung ansteht:

spxinfo -l

1. Zeigen Sie ausführliche Informationen zu Daten an:

spxconvert -a -v

1. Zeigen Sie ausführliche Informationen zu einem bestimmten Verzeichnis an:

spxconvert -p -v <Pfad>

Verschlüsselungsschritte

1. Zeigen Sie Elemente an, deren Verschlüsselung ansteht:

spxinfo -l

1. Zeigen Sie alle Kontrollsummen vor der Verschlüsselung an:

spxconvert -c -p <Pfad>

1. Verschlüsseln Sie alle Dateien in einem bestimmten Pfad:

spxconvert -p -v <Pfad>

1. Zeigen Sie alle Kontrollsummen für einen bestimmten Pfad nach der Verschlüsselung an:

spxconvert -c -p <Pfad>

Anhang F. Debugprotokollierung für Agenten

Richtlinienagenten arbeiten standardmäßig so, dass Nachrichten der Debugstufe von der Protokollierung ausgeschlossen werden. Wenn Nachrichten der Debugstufe im Protokoll des Agenten erfasst werden sollen, muss der Systemadministrator des Agenten die Funktion aktivieren und dann den Agenten erneut starten, damit die Erfassung von Nachrichten der Debugstufe beginnt.

Gültige Werte sind 1-6. Der Standardwert ist jedoch '4' und durch die Einstellung eines Werts kleiner '4' wird möglicherweise jede nützliche Information ausgeschlossen.

Kritischer Hinweis

- Durch die Aktivierung der Protokollierung der Debugstufe können sensible Systeminformationen offengelegt werden.
 - Aufgrund der Spezifik von Debugnachrichten können Agentenprotokolldateien drastisch anwachsen.

Linux-Agenten

Informationen zu diesem Vorgang

Aktivieren Sie das Debugging, indem Sie die Konfigurationsdatei im Verzeichnis **/etc/sysconfig/spx-policyagent** lokalisieren und das Flag für Beschreibbarkeit (**chmod +w /etc/sysconfig/spx-policyagent**) festlegen.

Hängen Sie am Ende der Datei die Angabe **"LOG_LEVEL=6"** ohne Anführungszeichen an.

Windows-Agenten

Informationen zu diesem Vorgang

Aktivieren Sie das Debugging, indem Sie den Registrierungsschlüssel unter **HKLM\SYSTEM\CurrentControlSet\Services\Spx Policy Agent\log level** aufsuchen und den Wert auf **'6'** setzen.

Anhang G. Nicht-OVA-Bereitstellung

Die folgenden Anweisungen enthalten Beispiele dafür, wie eine Nicht-OVA-Umgebung (OVA - Open Virtualization Appliance) für die PPM-Bereitstellung konfiguriert wird. Diese Anweisungen gelten nur, wenn Sie nicht die bereitgestellte PPM-OVA bereitstellen, sondern stattdessen eine eigene RHEL- oder CentOS 7.x-Umgebung erstellen, in der die PPM-Software bereitgestellt wird.

Installieren Sie diese Pakete auf allen PPM-Knoten.

Anmerkung: Dies ist nur eine Beispielkonfiguration. Es gibt viele umgebungsspezifische Anforderungen, die dazu führen, dass diese Anweisungen ungültig werden. Wenden Sie sich an den Support, um weitere Unterstützung anzufordern.

1. Installieren Sie Java 1.8 und PostgreSQL 9.2.

Anmerkung: Während des 'initdb'-Prozesses werden Sie zur Eingabe eines Kennworts aufgefordert. Dabei handelt es sich um das 'postgres'-Kennwort "superuser".

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

2. Installieren Sie die Firewallrichtlinien.

Im nachfolgenden Beispiel wird dargestellt, wie die Firewallrichtlinien mit 'iptables' installiert werden. Andere Methoden können jedoch ebenso gut arbeiten und können entsprechend den Präferenzen Ihrer Site verwendet werden. Beispiel: `yum install -y iptables iptables-services`

Für die nächsten beiden Befehle wird angenommen, dass die Firewall installiert und aktiv ist. Ist die Firewall nicht installiert, ist die Ausführung dieser Befehle unschädlich.

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

Starten Sie den Firewall-Service 'iptables' und leeren Sie ihn.

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

Aktivieren Sie den 'iptables'-Service. Dies ist ein optionaler Schritt. Er kann übersprungen werden, wenn keine lokale softwarebasierte Firewall erforderlich ist.

```
systemctl enable iptables.service
```

Definieren Sie eine Basisfirewall. Dies ist ein optionaler Schritt. Er kann übersprungen werden, wenn keine lokale softwarebasierte Firewall erforderlich ist.

```
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. Installieren Sie die Pakete 'Keepalived', 'HAProxy' und 'PSMisc' wie folgt:

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

4. Laden Sie Zookeeper herunter.

Anmerkung: Wenn 'wget' nicht installiert ist, müssen Sie es wie folgt installieren:

```
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. Installieren und konfigurieren Sie eine zuverlässige Quelle für die Zeit im Netz.

In diesem Beispiel wird die NTP-Konfiguration dargestellt; andere zuverlässige Zeitquellen können jedoch ebenso gut arbeiten und können entsprechend den Präferenzen Ihrer Site verwendet werden.

```
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. Installieren Sie das Repository mit den zusätzlichen Paketen für Enterprise Linux (Extra Packages for Enterprise Linux - EPEL).

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

7. Installieren Sie den Generator für unvorhersehbare Zufallszahlen (EPEL ist erforderlich).

```
yum install -y haveged
```

8. Installieren Sie die Netztools (net-tools) für die Erfassung der Servicedaten.

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

Anhang H. Prüfung der Softwareversion

Führen Sie die folgenden Befehle aus, um die Softwareversion zu überprüfen.

PPM-Version

Führen Sie in der PPM-VM-Shell den folgenden Befehl aus:

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

Version des Linux-Agenten

Führen Sie in der Linux-CLI den folgenden Befehl aus:

```
yum list policyagent
```

Version des AIX-Agenten

Führen Sie in der AIX-CLI den folgenden Befehl aus:

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

Version des Windows-Agenten

Navigieren Sie zu **Programme hinzufügen/entfernen** in der Windows-Systemsteuerung. Blättern Sie und suchen Sie den Agentennamen.

Agententyp	Agentenname unter Windows
Datei mit Richtlinie	FileAgent
Datenträger	VolumeAgent
Datenträger mit Richtlinie	HybridAgent

Anhang I. Glossar

Begriff	Definition
Advanced Encryption Standard New Instructions (AES-NI)	Eine Spezifikation für die Verschlüsselung elektronischer Daten, definiert vom U.S. National Institute of Standards and Technology (NIST) im Jahr 2001; ein Verschlüsselungsprotokoll, das von SPx-basierten Produkten verwendet wird.
Agent	Ein verwalteter Server, der die Verschlüsselungs- und Zugriffssteuerungssoftware von Security First ausführt.
Amazon Web Services (AWS) S3	Ein einfacher Speicherservice zum Speichern und Abrufen von Daten, der hoch skalierbar ist und einen kosteneffizienten Objektspeicher darstellt.
Automatisch generierte Schlüssel	Richtliniendurchsetzungsschlüssel, die durch MDE erstellt und verwaltet werden. Diese werden während der Richtlinienerstellung durch die Bezeichnung 'Schlüssel automatisch generieren' angegeben.
Zertifizierungsstelle	Eine vertrauenswürdige Organisation, die digitale Zertifikate signiert. Die Zertifizierungsstelle (CA, Certificate Authority) prüft die Identität und die Legitimität der übergebenen Zertifikatsanforderung. Wenn die Verifizierung der Anforderung erfolgreich ist, stellt die Zertifizierungsstelle Zertifikate aus.
Zertifikatswiderrufsliste (Certificate Revocation List, CRL)	Eine veröffentlichte Liste von Zertifikaten, die durch die Zertifizierungsstelle (CA), die sie ausgegeben hatte, widerrufen wurden.
Distributionspunkt für Zertifikatswiderrufsliste (CRLDP)	Ein Feld für den Ausgangspunkt im Zertifikat, das Informationen zu dem widerrufenen Zertifikat von der ausstellenden Zertifizierungsstelle enthält, die den Namen, optional Gründe für den Widerruf und den CRL-Ausstellernamen umfassen.
Cloud Auditing Data Federation (CADF)	Ein allgemeiner Ereignisformatsyntaxtyp, der an ein System für Sicherheitsinformationen und Ereignismanagement (Security Information and Event Management - SIEM) weitergeleitet wird.
Common Event Format (CEF)	Ein allgemeiner Ereignisformatsyntaxtyp, der an ein System für Sicherheitsinformationen und Ereignismanagement (Security Information and Event Management - SIEM) weitergeleitet wird.
Comma Separated Value (CSV)	Ein Datenformat, bei dem ein Komma als Feldtrennzeichen und ein Rückführzeichen als Datensatzbegrenzer verwendet wird.
Befehlszeilenschnittstelle (CLI)	Ein Typ von Interaktion, bei dem der Benutzer Befehle an die Anwendung in Form von Textzeilen (Befehlszeilen) sendet.

Coordinated Universal Time (UTC)	Der primäre <u>Zeitstandard</u> , nach dem Systemuhren und Zeitangaben reguliert werden.
Verschlüsselte Zugriffskontrolle (Cryptographic Access Controls)	Die Möglichkeit, den Benutzerzugriff durch die Nutzung von Verschlüsselungsmaterial zu trennen.
CURL	CURL ist ein Computer-Software-Projekt, das eine Bibliothek und ein Befehlszeilentool zur Übertragung von Daten über verschiedene Protokolle bereitstellt.
Distinguished Encoding Rules (DER)	DER ist eine der ASN.1-Codierungsregeln, die in der Spezifikation ITU-T X.690, 2002, definiert sind. Eine Codierungsregel für Datenstrukturen stellt eine Übertragungssyntax bereit, die steuert, wie Byte in einem Datenstrom beim Senden zwischen Computern organisiert werden.
Domänenname (DN)	Ein Internetressourcenname, der universell eindeutig und mit IP-Zielinformationen verknüpft ist.
Domain Name Service (DNS)	Ein Internet-Service, der Domännennamen in IP-Adressen übersetzt.
Dynamic Host Configuration Protocol (DHCP)	Ein Client/Server-Protokoll, das einen Internet Protocol-Host (IP-Host) automatisch mit seiner IP-Adresse und anderen zugehörigen Konfigurationsinformationen wie Teilnetzmaske und Standardgateway versorgt.
Dateiagent	Ein Dateiagent setzt dateibasierte operative Zugriffsrichtliniendefinitionen und die Zuordnung eines oder mehrerer geschützter Dateipfade durch. Jeder geschützte Dateipfad kann eine eigene operative Zugriffssteuerung und eine eigene Verschlüsselungszugriffsteuerung haben.
Grafische Benutzerschnittstelle (GUI)	Ein Typ von Benutzerschnittstelle (UI), der Benutzern die Interaktion mit MDE über grafische Symbole ermöglicht und nicht durch textbasierte Schnittstellen und durch Eingabe von Befehlen.
Health Insurance Portability and Accountability Act (HIPAA)	Die HIPAA-Datenschutzbestimmung verlangt von Anbietern und Organisationen, dass sie die Vertraulichkeit und Sicherheit geschützter Diagnoseinformationen (PHI, Protected Health Information) sicherstellen.
Hochverfügbarkeit (High Availability - HA)	Der Systembetrieb wird durch Redundanz (redundante Stromversorgungssysteme, CPUs, Laufwerke, Software usw.) auch dann fortgesetzt, wenn Komponenten ausfallen.
Hypertext Transfer Protocol (HTTP)	Ein Anwendungsprotokoll, das die Basis der Datenübertragung für das World Wide Web darstellt.

Hypervisor	Wird auch als VM-Monitor bezeichnet. Ein Hypervisor bzw. ein VM-Monitor (VMM) ist eine Computer-Software, Firmware oder Hardware, die virtuelle Maschinen erstellt, ausführt und verwaltet. Ein Computer, auf dem ein Hypervisor eine oder mehrere virtuelle Maschinen ausführt, wird als Hostmaschine bezeichnet. Jede virtuelle Maschine wird hierbei als Gastmaschine bezeichnet. Der VMware-Hypervisor wird auch als ESXi-Host bezeichnet.
IBM Cloud Object Storage (COS S3)	Eine Speicherplattform zum Speichern von großen Datenmengen wie z. B. Sicherungen, Archiven, Videodateien und Imagedateien für die Bereitstellung von ruhenden Daten und hoher Verfügbarkeit.
Initialisierungsvektor (IV)	Eine beliebige und unvorhersehbare Zufallszahl, die zusammen mit einem geheimen Schlüssel zur Datenverschlüsselung verwendet werden kann und die nur einmal in einer Sitzung verwendet wird.
Java-Keystore (JKS)	Ein Java-Keystore (JKS) ist ein Repository für Sicherheitszertifikate, d. h. Autorisierungszertifikate oder Zertifikate für öffentlichen Schlüssel, sowie für die entsprechenden privaten Schlüssel. Das Java Development Kit (JDK) stellt ein Tool (keytool) zum Verwalten von Schlüsseln und Zertifikaten im Keystore bereit. Dateien mit der Erweiterung 'jks' haben ein Java-spezifisches Dateiformat.
Schlüsselwiderruf	Das Entfernen von Richtliniendurchsetzungsschlüsseln aus einer Agentenumgebung, die eine behebbare Einschränkung des Datenzugriffs auf verschlüsselte Daten zur Folge hat. Diese Aktion macht die Daten vorübergehend unzugänglich.
Schlüsselrotation	Die Migration von Richtliniendurchsetzungsschlüsseln in einer Agentenumgebung, die eine für keinen Benutzer sichtbare Änderung am Datenzugriff zur Folge hat.
Schlüsselschredderung	Das Entfernen von Richtliniendurchsetzungsschlüsseln aus einer Agentenumgebung, die eine nicht behebbare Einschränkung des Datenzugriffs auf verschlüsselte Daten zur Folge hat. Diese Aktion macht Daten permanent unzugänglich.
Keystore	Die konfigurierte Speicherposition von Richtliniendurchsetzungsschlüsseln.
Lightweight Directory Access Protocol (LDAP)	Ein offenes, anbieterneutrales Protokoll des Industriestandards für den Zugriff und die Verwaltung verteilter Verzeichnisinformationen über ein Netz. Mithilfe dieses Softwareprotokolls können beliebige Benutzer Organisationen, Einzelpersonen und andere Ressourcen wie Dateien und Einheiten in einem Netz lokalisieren.

Log Event Extended Format (LEEF)	LEEF ist ein angepasstes Ereignisformat für IBM Security QRadar, das lesbare und leicht verarbeitbare Ereignisse für QRadar enthält. Es unterstützt mehrere vordefinierte Ereignisattribute für die Ereignisnutzdaten.
Logical Volume Manager (LVM)	Ein Speichereinheitenmanager, der ein Linux-Kernel-Framework zur Einheitenzuordnung (Device Mapper) nutzt, um Speichereinheiten zu Gruppen zusammenzufassen, und logische Einheiten aus dem kombinierten Speicherbereich nach Bedarf zuordnet. Die meisten Linux-Distributionen sind für LVM eingerichtet.
M of N (M:N)	Ein Modell, das festlegt, wie viele Datenteile für das erneute Erstellen der Daten (M) aus der Gesamtanzahl der erstellten Datenteile - oder 'Shares' - (N) benötigt werden.
NT File System (NTFS)	Ein von Microsoft in Windows NT entwickeltes proprietäres Dateisystem, das zum Speichern und Abrufen von Dateien auf einer Festplatte verwendet wird und Sicherheits-, Komprimierungs und Auditfunktionen auf Dateiebene unterstützt.
Network Time Protocol (NTP)	Ein Netzprotokoll für die Systemzeitsynchronisation zwischen Computersystemen.
Objekt-ID (OID)	Ein standardisierter Kennungsmechanismus zur Benennung von Objekten oder Konzepten mit einem global unzweideutigen und persistenten Namen.
Agent vom Typ 'Objektspeicher'	Mit diesem Agenten können Daten verschlüsselt und gesplittet werden (kryptografisches Datensplitting), die an einen hoch skalierbaren, effizienten Objektspeicher gesendet und dort sicher gespeichert werden - in der Cloud und/oder lokal.
Online Certificate Status Protocol (OCSP)	Ein internes Protokoll zum Abrufen des Widerrufsstatus von digitalen X.509-Zertifikaten.
Open Virtualization Archive (OVA)	Eine TAR-Archivdatei. Diese eine komprimierte Datei enthält sämtliche OVA-Dateien.
Payment Card Industry (PCI)	Ein Standard zur Verbesserung der Kontrolle und Sicherheit für Karteninhaberdaten zur Verringerung von Betrugsfällen.
PEM	Ein häufig genutztes Codierformat für Sicherheitszertifikate, dessen Syntax und Inhalt durch X.509-Standards der Version 3 definiert sind.
PostgreSQL	PostgreSQL (sprich "post-gress-Q-L" ist ein quell-offenes Managementsystem für relationale Datenbanken (DBMS), das von einem weltweit tätigen Team von Freiwilligen entwickelt wird. PostgreSQL wird durch kein Unternehmen oder private Entität kontrolliert und der Quellcode ist kostenlos verfügbar.
Geschützt	Alle Daten, die verarbeitet wurden.

Public Key Cryptography Standard 12 (PKCS12)	Ein auf einem öffentlichen Schlüssel basierender Verschlüsselungsstandard, der ein Archivdateiformat zum Speichern vieler Verschlüsselungsobjekte in Form einer einzelnen Datei definiert. Der Standard wird häufig verwendet, um einen privaten Schlüssel mit dem zugehörigen X.509-Zertifikat zusammenzupacken oder alle Mitglieder einer Zertifikatskette zu bündeln. Er kann verschlüsselt und signiert werden.
Public Key Infrastructure (PKI)	Eine Gruppe von Rollen, Richtlinien und Prozeduren, die erforderlich sind, um digitale Zertifikate erstellen, verwalten, verteilen, verwenden, speichern und widerrufen sowie die Verschlüsselung mit öffentlichem Schlüssel verwalten zu können.
ReFS	Das neue Dateisystem von Microsoft, das mit Windows Server 2012 eingeführt wurde und darauf ausgelegt ist, die Datenverfügbarkeit, Skalierbarkeit und Datenintegrität zu maximieren.
Representational State Transfer Application Program Interface (REST API)	Eine REST-konforme API, die auch als REST-konformer Web-Service bezeichnet wird, basiert auf der REST-Technologie (REST - Representational State Transfer), einem Architekturstil und -ansatz für die Kommunikation, der häufig in der Web-Service-Entwicklung genutzt wird.
Rollenbasierte Zugriffssteuerung (RBAC - Role Based Access Control)	Eine Methode zur Regulierung des Zugriffs auf Computer- und Netzressourcen auf der Basis der Rollen einzelner Benutzer in einem Unternehmen. In diesem Kontext meint Zugriff die Fähigkeit eines Einzelbenutzers, eine bestimmte Task auszuführen, wie zum Beispiel das Anzeigen, Erstellen oder Ändern einer Datei.
RSA	Eine von Rivest, Shamir und Adelman (RSA) entwickelte Public-Key-Verschlüsselung, bei der ein öffentlicher und ein privater Schlüssel für den Schutz von Daten verwendet werden.
Secure Copy Protocol (SCP)	Der Befehl 'scp' wird unter Linux für das Übertragen von Dateien zwischen Systemen über das SSH-Protokoll (Secure Shell) verwendet.
Secure Socket Layer (SSL)	Ein Verschlüsselungsprotokoll, das die Datenkommunikation über das Internet mithilfe eines asymmetrischen Schlüssels verschlüsselt, um symmetrische Schlüssel auszutauschen. Eine Zertifizierungsstelle (CA) und eine Infrastruktur öffentlicher Schlüssel sind erforderlich, um die Überprüfung von Zertifikaten und Eignern zu ermöglichen und Zertifikate zu generieren und zu signieren sowie die Gültigkeit von Zertifikaten zu verwalten.
Secure Socket Shell (SSH)	Ein Netzprotokoll, das Administratoren ein sicheres Verfahren für den Zugriff auf einen fernen Computer bietet. SSH bezeichnet außerdem eine Reihe von Dienstprogrammen, die dieses Protokoll implementieren.

Selektor	Im Betriebssystem definierte Benutzer und Gruppen, die auf Daten, Pfadgruppen und andere richtlinienbezogene Komponenten zugreifen können.
Transport Layer Security (TLS)	Ein Verschlüsselungsprotokoll, das eine sichere Kommunikation über ein Computernetz ermöglicht.
Truststore	Ein Truststore speichert Zertifikate aus einer vertrauenswürdigen Zertifizierungsstelle (CA), die zur Prüfung von Zertifikaten durch den Server in einer SSL-Verbindung verwendet wird.
Eindeutige ID (UUID)	Universally Unique Identifier (UUID) ist ein Kennungsstandard, der in der Softwareerstellung verwendet wird. Eine UUID (128-Bit-Nummer) wird verwendet, um ein Objekt oder eine Entität im Internet eindeutig zu identifizieren.
Virtuelle Maschine (VM)	Eine Emulation eines Computersystems, die auf der Computerarchitektur und den Funktionen eines realen oder hypothetischen Computers basiert.
VMware ESXi™	Eine Emulation eines bestimmten Computersystems, die auf der Computerarchitektur und den Funktionen eines realen oder hypothetischen Computers basiert.
Datenträgeragent	Ein Datenträgeragent setzt die Datenträgerrichtliniendefinition und die Zuordnung eines oder mehrerer geschützter Datenträger auf einem Zielsystem durch.
Agent vom Typ 'Datenträger mit Richtlinie'	Dieser Typ von Agent nutzt den Datenträgerrichtlinienschutz eines Datenträgeragenten und ermöglicht die Anwendung und Durchsetzung von dateibasierten operativen Zugriffssteuerungsrichtlinien für einen oder mehrere geschützte Dateipfade. Wird auch als Hybridagent bezeichnet.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

IBM stellt dieses Material möglicherweise auch in anderen Sprachen zur Verfügung. Für den Zugriff auf das Material in einer anderen Sprache kann eine Kopie des Produkts oder der Produktversion in der jeweiligen Sprache erforderlich sein.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für die in diesem Handbuch beschriebenen Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing

IBM Europe, Middle East & Africa

Tour Descartes

2, avenue Gambetta

92066 Paris La Defense

France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht. Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Director of Licensing

IBM Corporation

North Castle Drive, MD-NC119

Armonk, NY 10504-1785 U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellsprache geschrieben sind und Programmier Techniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher

kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis) und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen. Abhängig von der Art der Anzeige dieser Informationen werden bestimmte Abbildungen und Illustrationen möglicherweise nicht angezeigt.

Marken

SPx und Security First Corp sind Marken oder eingetragene Marken der Security First Corp. in den USA und/oder anderen Ländern. Weitere Produkt- und Servicennamen können Marken oder Servicemarken von Security First Corp. oder anderen Herstellern sein.

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicennamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

The Apache Software Foundation (ASF) owns all Apache-related trademarks, service marks, and graphic logos on behalf of our Apache project communities, and the names of all Apache projects are trademarks of the ASF.

Node.JS ist eine eingetragene Marke von Joyent, Inc., a Delaware Corporation; 345 California Street; Suite 2000; San Francisco, California, 94104.

Unicode und das Unicode-Logo sind eingetragene Marken von Unicode, Inc. in den USA und/oder anderen Ländern.

Die CentOS-Marken sind Marken von Red Hat, Inc. ("Red Hat").

"Red Hat", Red Hat Linux, das Red Hat "Shadowman"-Logo und die aufgelisteten Produkte sind Marken oder eingetragene Marken von Red Hat Inc. in den USA und anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Bedingungen für die Nutzung dieser Produktdokumentation[r]

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Anwendbarkeit: Diese Bedingungen sind eine Ergänzung der Nutzungsbedingungen auf der IBM Website.

Persönliche Nutzung: Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM nicht weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Kommerzielle Nutzung: Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Berechtigungen: Abgesehen von den hier gewährten Berechtigungen werden keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum gewährt. IBM behält sich das Recht vor, die hierin gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden. Sie dürfen diese Informationen nur in Übereinstimmung mit allen

anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.

Hinweise zur Datenschutzrichtlinie

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden. Dieses Softwareangebot verwendet keine Cookies oder andere Technologien zur Erfassung personenbezogener Daten.

Wenn es die für dieses Softwareangebot bereitgestellten Konfigurationen Ihnen als Kunde ermöglichen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in den Schwerpunkten der IBM Online-Datenschutzerklärung unter <http://www.ibm.com/privacy>, in der IBM Online-Datenschutzerklärung unter <http://www.ibm.com/privacy/details> im Abschnitt "Cookies, Web Beacons und sonstige Technologien" und auf der Seite "IBM Software Products and Software-as-a-Service Privacy Statement" unter <http://www.ibm.com/software/info/product-privacy>.

Produktnummer: 5737-C67

Gedruckt in den USA

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. IBM stellt dieses Material möglicherweise auch in anderen Sprachen zur Verfügung. Für den Zugriff auf das Material in einer anderen Sprache kann eine Kopie des Produkts oder der Produktversion in der jeweiligen Sprache erforderlich sein.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für die in diesem Handbuch beschriebenen Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

*IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France*

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA*

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingun-

gen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können unter Umständen von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellsprache geschrieben sind und Programmier Techniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis) und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corporation abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_.

Wird dieses Dokument als Softcopy (Book) angezeigt, sind Fotografien oder Farabbildungen möglicherweise nicht sichtbar.

Marken

SPx und Security First Corp sind Marken oder eingetragene Marken der Security First Corp. in den USA und/oder anderen Ländern. Weitere Produkt- und Servicennamen können Marken oder Servicemarken von Security First Corp. oder anderen Herstellern sein.

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicennamen können Marken von IBM oder anderen

Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

The Apache Software Foundation (ASF) owns all Apache-related trademarks, service marks, and graphic logos on behalf of our Apache project communities, and the names of all Apache projects are trademarks of the ASF.

Node.JS ist eine eingetragene Marke von Joyent, Inc., a Delaware Corporation; 345 California Street; Suite 2000; San Francisco, California, 94104.

Unicode und das Unicode-Logo sind eingetragene Marken von Unicode, Inc. in den USA und/oder anderen Ländern.

Die CentOS-Marken sind Marken von Red Hat, Inc. ("Red Hat").

"Red Hat", Red Hat Linux, das Red Hat "Shadowman"-Logo und die aufgelisteten Produkte sind Marken oder eingetragene Marken von Red Hat Inc. in den USA und anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Bedingungen für die Nutzung dieser Produktdokumentation

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt:

Anwendbarkeit

Diese Bedingungen sind eine Ergänzung der Nutzungsbedingungen auf der IBM Website.

Persönliche Nutzung

Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM nicht weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Kommerzielle Nutzung

Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Rechte

Abgesehen von den hier gewährten Berechtigungen werden keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum gewährt.

IBM behält sich das Recht vor, die hierin gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine aus-

drückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.

Hinweise zur Datenschutzrichtlinie

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen (“Softwareangebote”), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden. Dieses Softwareangebot verwendet keine Cookies oder andere Technologien zur Erfassung personenbezogener Daten.

Wenn es die für dieses Softwareangebot bereitgestellten Konfigurationen Ihnen als Kunde ermöglichen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in den Schwerpunkten der IBM Online-Datenschutzerklärung unter <http://www.ibm.com/privacy>, in der IBM Online-Datenschutzerklärung unter <http://www.ibm.com/privacy/details> im Abschnitt “Cookies, Web Beacons und sonstige Technologien” und auf der Seite “IBM Software Products and Software-as-a-Service Privacy Statement” unter <http://www.ibm.com/software/info/product-privacy>.



SC43-5052-01

