

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

Häufig gestellte Fragen (FAQ)



Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter [„Bemerkungen“ auf Seite 13](#) 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 .**

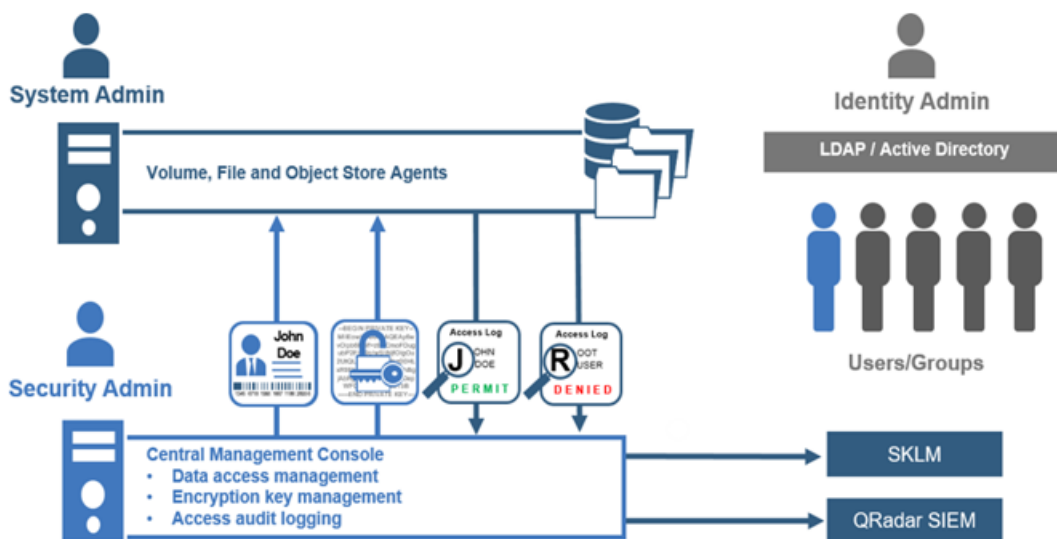
Inhaltsverzeichnis

Kapitel 1. Übersicht.....	1
Kapitel 2. MDE - Häufig gestellte Fragen (FAQ).....	3
Allgemeine häufig gestellte Fragen.....	3
Frage: Was ist IBM Multi-Cloud Data Encryption (MDE)?	3
Frage: Welche Betriebssysteme werden von IBM Multi-Cloud Data Encryption (MDE) un-	
terstützt?	3
Frage: Welche Dateisysteme werden von MDE-Agenten unterstützt?	3
Frage: Müssen für IBM Multi-Cloud Data Encryption (MDE) bestimmte Voraussetzungen	
erfüllt sein?.....	3
Frage: Welche Browser werden von IBM Multi-Cloud Data Encryption (MDE) unterstützt?	3
Frage: Wird IBM Multi-Cloud Data Encryption (MDE) im FIPS-Modus ausgeführt?	4
Frage: Muss ich meine Daten verschlüsseln, wenn ich Multi-Cloud Data Encryption (MDE)	
verwende und ich die Daten an ein fernes System sende? Benötige ich weiterhin eine	
VPN-Verbindung zu dem fernen System?	4
Frage: Was bedeutet die Aussage, dass IBM Multi-Cloud Data Encryption (MDE) die Si-	
cherheit auf Bitebene in die Daten integriert?.....	4
Frage: Wie wird die Integrität der Daten mit IBM Multi-Cloud Data Encryption (MDE) si-	
chergestellt?	4
Häufig gestellte Fragen zu PPM (Policy, Provisioning and Management)	4
Frage: Wozu dient Policy, Provisioning and Management (PPM)?	4
Frage: Warum verwendet Policy, Provisioning and Management (PPM) rollenbasierte Zu-	
griffssteuerung?	4
Frage: Was sind Prozesse in der PPM-Konsole? Wofür werden sie verwendet?	5
Frage: Was ist ein Selektor in der PPM-Konsole und wie wird er verwendet?	5
Frage: Was ist eine Pfadgruppe in der PPM-Konsole? Wofür wird sie verwendet?	5
Frage: Was ist ein Datentyp in der PPM-Konsole und wie wird er verwendet?	5
Frage: Was ist ein Agent in der PPM-Konsole und wie wird er verwendet?	5
Frage: Wann sollte der Agent des Typs 'Datenträger' eingesetzt werden? Wie funktioniert	
dieser Schutz?	6
Frage: Wann sollte der Agent des Typs 'Datei mit Richtlinie' eingesetzt werden? Wie funk-	
tioniert dieser Schutz?	6
Frage: Wann sollte der Agent des Typs 'Datenträger mit Richtlinie' eingesetzt werden?	
Wie funktioniert dieser Schutz?	6
Frage: Wann sollte der Agent des Typs 'Objektspeicher' eingesetzt werden? Wie funk-	
tioniert dieser Schutz?	6
Frage: Was ist ein Job in der PPM-Konsole und wie wird er verwendet?	7
Frage: In welchen Fällen muss für IBM Multi-Cloud Data Encryption eine externe Post-	
greSQL-Datenbank verwendet werden?	7
Zertifikate - Häufig gestellte Fragen.....	7
Frage: Welche Voraussetzungen gelten für PPM-Serverzertifikate?.....	7
Frage: Welche Voraussetzungen gelten für Agentenzertifikate?	7
Frage: Unterstützt PPM NAT- (NAT, Network Address Translation) oder PAT-Verbindungen	
(PAT, Port Address Translation)?.....	7
Frage: Wie werden PPM-Serverzertifikate für einen PPM-Server in einer NAT-Netzkonfigu-	
ration (Network Address Translation) oder einer PAT-Netzkonfiguration (Port Address	
Translation) konfiguriert?	8
Frage: Wie werden Agentenzertifikate konfiguriert, wenn sich ein Agent in einer NAT-	
Netzkonfiguration (Network Address Translation) oder in einer PAT-Netzkonfiguration	
(Port Address Translation) befindet?	8

Frage: Welche Voraussetzungen gelten für PPM-Serverzertifikate in einer Hochverfügbarkeitskonfiguration (HA-Konfiguration)?	8
Häufig gestellte Fragen zu Schlüsseln und zur Verarbeitung von Schlüsseln	8
Frage: Welche Operationen zum Verarbeiten von Schlüsseln kann IBM Multi-Cloud Data Encryption ausführen?	8
Frage: Warum sollten Schlüssel turnusmäßig gewechselt (rotiert) werden?	8
Frage: Warum sollten Schlüssel widerrufen werden?	8
Frage: Warum sollten Schlüssel geschreddert werden?	9
Frage: Verwaltet IBM Multi-Cloud Data Encryption die Schlüssel für mich?	9
Häufig gestellte Fragen zur Installation und Konfiguration	9
Frage: Wie wirkt sich die Verwendung von IBM Multi-Cloud Data Encryption (MDE) auf Endbenutzer (d. h. Benutzer ohne Verwaltungsaufgaben) aus?	9
Frage: Kann ein MDE-Agent auf einem Docker-Host installiert werden und alle Lese-/Schreibenanforderungen von Anwendungen in Docker-Containern verarbeiten?	9
Häufig gestellte Fragen zur Konfiguration	9
Frage: Kann ich HTML-Dateien mit IBM Multi-Cloud Data Encryption (MDE) verschlüsseln?	9
Häufig gestellte Fragen zum Betrieb	9
Frage: Kann ich sicher sein, dass meine Daten mit IBM Multi-Cloud Data Encryption (MDE) geschützt sind?	10
Frage: Welche Vorsichtsmaßnahmen werden empfohlen, bevor Änderungen an einer Produktionsimplementierung von IBM Multi-Cloud Data Encryption (MDE) vorgenommen werden?	10
Frage: Kann ich Ereignisse aus IBM Multi-Cloud Data Encryption (MDE) an andere SIEM-Korrelationsanwendungen (SIEM - Security Information and Event Management) weiterleiten?	10
Fragen: Ist Groß-/Kleinschreibung wichtig?	10
Frage: Was bedeutet die Operationsreihenfolge und warum ist diese wichtig?	10
Frage: Ich habe einen Snapshotaktivierungsjob übergeben und er ist immer noch aktiv. Wann wird er beendet?	10
Häufig gestellte Fragen zur Hochverfügbarkeit	11
Frage: Wann ist Hochverfügbarkeit für eine MDE-Bereitstellung erforderlich?	11
Frage: Sind für eine MDE-Bereitstellung mit Hochverfügbarkeit Einrichtungen für den Lastausgleich erforderlich?	11
Häufig gestellte Fragen zur Multi-Tenant-Funktionalität	11
Frage: Wozu dient die Multi-Tenant-Funktion?	11
Bemerkungen	13
Marken	14
Bedingungen für die Nutzung dieser Produktdokumentation	15
Hinweise zur Datenschutzrichtlinie	16

Kapitel 1. Übersicht

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-Attacken macht. Der Schutz wird darüber hinaus durch die Möglichkeit erweitert, den Datenzugriff durch die Definition differenzierter Zugriffsrichtlinien auf Benutzerebene einzuschränken, zu überwachen und zu prüfen.



MDE ermöglicht eine Trennung von Aufgaben durch zwei 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. Abbildung 1 stellt diese Rollen dar, die im Abschnitt "Management von Benutzern mit Verwaltungsaufgaben in MDE" der Veröffentlichung "Verwaltung" eingehender beschrieben werden.

Vier Agententypen sind verfügbar, die implementiert werden können, um die Richtliniendefinitionen von geschützten oder verschlüsselten Daten durchzusetzen. Agenten des Typs 'Datenträger' setzen die Datenträgersrichtliniendefinition und die Zuordnung eines oder mehrerer geschützter Datenträger durch. Agenten des Typs 'Datei mit Richtlinie' setzen dateibasierte operative Zugriffsrichtliniendefinitionen und die Zuordnung eines oder mehrerer geschützter Dateipfade durch, wobei jeder geschützte Dateipfad über eigene operative und Zugriffssteuerungsrichtlinien verfügen kann, die in differenzierten Richtlinienspezifikationen definiert sind. Agenten des Typs 'Datenträger mit Richtlinie' nutzen den Datenträgersrichtlinienschutz eines Datenträgeragenten und ermöglichen die Anwendung und Durchsetzung von dateibasierten operativen Zugriffssteuerungsrichtlinien für einen oder mehrere geschützte Dateipfade. Agenten des Typs 'Objektspeicher' verschlüsseln Daten, die an einen oder mehrere cloudbasierte Objektspeicher gesendet werden, und führen für diese Daten kryptografisches Datensplitting durch.

Kapitel 2. MDE - Häufig gestellte Fragen (FAQ)

Allgemeine häufig gestellte Fragen

Frage: Was ist IBM Multi-Cloud Data Encryption (MDE)?

Antwort: MDE ermöglicht die Bereitstellung von Agenten und von Richtlinien (Definition des operativen Zugriffs und des Verschlüsselungszugriffs) sowie das Management (Lebenszyklusaktualisierungen und Benutzerprotokollierung) von bis zu 25.000 Agenten von einer einzelnen zentralen Position aus. MDE unterstützt die Bereitstellung der folgenden vier Agententypen: Datenträger, Datei mit Richtlinie, Datenträger mit Richtlinie und Objektspeicher. Diese Agenten sind leicht zu installieren und für den Endbenutzer nahtlos zu verwenden. Sie geben Administratoren die Möglichkeit, die Software zu konfigurieren und bereitzustellen, die zum Erfüllen von Konformitätsanforderungen für die IT-Umgebungen erforderlich ist.

Frage: Welche Betriebssysteme werden von IBM Multi-Cloud Data Encryption (MDE) unterstützt?

Antwort: MDE unterstützt zum gegenwärtigen Zeitpunkt die folgenden Betriebssysteme:

- Red Hat® Enterprise Linux 6.2-Kernelversion 2.6.32-220 und nachfolgende Releases
- Red Hat® Enterprise Linux 7.2+-Kernelversionen
- CentOS 6.2-Kernelversion 2.6.32-220 und nachfolgende Releases
- CentOS 7.2-Kernelversion und nachfolgende Releases
- Microsoft Windows Server® 2008R2
- Microsoft Windows Server® 2012
- Microsoft Windows Server® 2012R2
- Microsoft Windows Server® 2016

Frage: Welche Dateisysteme werden von MDE-Agenten unterstützt?

Antwort: MDE unterstützt die folgenden Dateisysteme:

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

Frage: Müssen für IBM Multi-Cloud Data Encryption (MDE) bestimmte Voraussetzungen erfüllt sein?

Antwort: MDE wird als Open Virtualization Archive (OVA) ausgeliefert, das problemlos in VMware ESXi™ oder Microsoft Hyper-V bereitgestellt werden kann und das in den meisten anderen Hypervisoren ausgeführt werden kann.

Frage: Welche Browser werden von IBM Multi-Cloud Data Encryption (MDE) unterstützt?

Antwort: MDE kann mit Mozilla Firefox, Google Chrome™, Microsoft Internet Explorer und Microsoft Edge ausgeführt werden.

Frage: Wird IBM Multi-Cloud Data Encryption (MDE) im FIPS-Modus ausgeführt?

Antwort: Ja, MDE entspricht dem Standard FIPS 140.2 (FIPS - Federal Information Processing Standard) der im Datenblatt des Produkts beschrieben wird.

Frage: Muss ich meine Daten verschlüsseln, wenn ich Multi-Cloud Data Encryption (MDE) verwende und ich die Daten an ein fernes System sende? Benötige ich weiterhin eine VPN-Verbindung zu dem fernen System?

Antwort: MDE ist dafür ausgelegt, Daten sicher an ferne Standorte (einschließlich öffentlicher Cloud-Sites) zu schreiben, sofern das Programm Zugriff auf die Speicherposition der Datei hat. Für die Verbindung zu dem fernen Standort ist jedoch möglicherweise ein VPN (Virtual Private Network) erforderlich.

Frage: Was bedeutet die Aussage, dass IBM Multi-Cloud Data Encryption (MDE) die Sicherheit auf Bitebene in die Daten integriert?

Antwort: Das auf der SPx-Technologie basierende Produkt MDE kombiniert die Verschlüsselung, das randomisierte oder schlüsselbasierte Datensplitting auf Bitebene, die Authentifizierung (Integritätsprüfung), die Fehlertoleranz und ein COI-Framework zu einem Prozess, der identifizierbare Daten und Informationen in völlig zufällige und nicht verwendbare binäre Elemente umwandelt. Das Ergebnis dieser MDE-Operation ist, dass das Informationszusicherungselement tief in der Struktur der Daten verankert ist. Sicherheit, Datenausfallsicherheit, Vertrauensbeziehungen und ein Framework für die gemeinsame Informationsnutzung sind mit den Daten durchsetzt und durchdringen die Daten. Dadurch werden diese Elemente untrennbar miteinander verbunden. Der Schutz der Daten und Informationen wird ab dem Zeitpunkt ihrer Erstellung während des gesamten Lebenszyklus bis zum Zeitpunkt der Zerstörung der Daten oder ihrer öffentlichen Freigabe sichergestellt. Der Schutz bleibt mit den Daten verbunden, wenn sie ruhen (d. h., wenn sie in den Speicher geschrieben werden) und wenn auf die Daten zugegriffen wird.

Frage: Wie wird die Integrität der Daten mit IBM Multi-Cloud Data Encryption (MDE) sichergestellt?

Antwort: Die Integrität der Daten wird mithilfe von Nachrichtenauthentifizierungs-codes sichergestellt, die übereinstimmen müssen, damit die Daten gelesen werden können.

Häufig gestellte Fragen zu PPM (Policy, Provisioning and Management)

Frage: Wozu dient Policy, Provisioning and Management (PPM)?

Antwort: PPM verwaltet die Bereitstellung von Agenten (Datenschutzmodell), Richtlinien (Definition des operativen Zugriffs und des Verschlüsselungszugriffs) und der Verwaltung (Lebenszyklusaktualisierungen und Benutzerprüfungen) von bis zu 25.000 Agenten von einer einzelnen zentralen Position aus. Das Produkt unterstützt die Bereitstellung der folgenden vier Datenverschlüsselungsagententypen: Datenträger, Datei mit Richtlinie, Datenträger mit Richtlinie und Objektspeicher. Der Agent des Typs 'Datenträger' schützt die Daten auf der Ebene der Blockeinheit. Der Agent des Typs 'Datei mit Richtlinie' schützt die Daten auf Dateiebene und stellt dateibasierte operative Zugriffssteuerung bereit. Der Agent des Typs 'Datenträger mit Richtlinie' schützt die Daten auf der Ebene der Blockeinheit und stellt dateibasierte operative Zugriffssteuerung bereit. Agenten des Typs 'Objektspeicher' verschlüsseln Daten, die an einen oder mehrere cloudbasierte Objektspeicher gesendet werden, und führen für diese Daten kryptografisches Datensplitting durch.

Frage: Warum verwendet Policy, Provisioning and Management (PPM) rollenbasierte Zugriffssteuerung?

Antwort: PPM nutzt ein flaches, auf statischen Rollen basierendes Zugriffssteuerungsdesign (RBAC - Role-based Access Control). Für die Funktionalität innerhalb von PPM sind bestimmte Berechtigungen erforderlich.

derlich. Es gibt zwei verschiedene Rollen: Produktadministrator und Sicherheitsadministrator. Diese beiden Rollen haben zwar einige Berechtigungen gemeinsam; die Trennung der Rollen gibt dem IT-Führungspersonal jedoch die Möglichkeit, die Verwaltungsaufgaben grundlegend aufzuteilen. Dadurch kann ein verbrecherischer Mitarbeiter die IT-Umgebung des Unternehmens nicht sabotieren. Zusätzliche Rollen der verschiedenen Typen können hinzugefügt werden, um eine größere oder komplexere IT-Umgebung zu unterstützen. Darüber hinaus kann ein Kunde mit dem Programm die Anzahl der für das Genehmigen oder Ablehnen eines Jobs erforderlichen Administratoren definieren. Daher werden die von Administratoren getätigten Genehmigungen und Ablehnungen für jede Gruppe von Rollen durch PPM verfolgt, damit sichergestellt ist, dass sich ausreichend viele Administratoren für eine Ausführung oder eine Ablehnung ausgesprochen haben. Wenn die erforderliche Anzahl an Administratoren den Job genehmigt, wird er ausgeführt. Wenn die erforderliche Anzahl an Administratoren den Job ablehnt (diese Anzahl kann sich von der für die Genehmigung erforderliche Anzahl unterscheiden) wird der Job abgebrochen. Dies ermöglicht die detaillierte Steuerung von administrativen und sicherheitsbezogenen Tasks. Die Reihenfolge der Genehmigungen und Ablehnungen wird protokolliert, sodass sie geprüft und die Einhaltung von Vorschriften verifiziert werden kann.

Frage: Was sind Prozesse in der PPM-Konsole? Wofür werden sie verwendet?

Antwort: Prozesse, die auch als "Prozess über Richtlinie" bezeichnet werden, bestehen aus einer Liste von Prozessen oder Anwendungen, denen die Zugriffssteuerung für die von IBM Multi-Cloud Data Encryption geschützten Daten zugewiesen wird. Prozesse sind an einen Selektor gebunden und ermöglichen die Zugriffssteuerung für Prozesse durch Benutzer auf einem Zielsystem.

Frage: Was ist ein Selektor in der PPM-Konsole und wie wird er verwendet?

Antwort: Ein Selektor ist eine ungeordnete Liste mit Benutzern, Gruppen und Prozessen. Mit einem Selektor, der in einem Datentyp kombiniert ist, hat der Sicherheitsadministrator eine einfache Möglichkeit, Objektgruppen mit Entitäten zu identifizieren, die gemeinsamen Zugriff auf die von MDE geschützten Daten haben sollen. Ein Selektor kann einen optionalen Benutzer, ein optionales Feld für eine Gruppe zusammen mit der Gruppenquelle (intern oder extern, falls mit LDAP definiert) oder einen optionalen "Prozess über Richtlinie" enthalten.

Frage: Was ist eine Pfadgruppe in der PPM-Konsole? Wofür wird sie verwendet?

Antwort: Eine Pfadgruppe ist eine ungeordnete Liste mit den durch eine MDE-Richtlinie geschützten (oder - abhängig von der Richtlinie - den möglicherweise vom Schutz durch eine Richtlinie ausgeschlossenen) Dateipfaden. Mit einer Pfadgruppe hat der Sicherheitsadministrator eine einfache Möglichkeit, Sammlungen mit Dateipfaden anzugeben oder aufzulisten, die von MDE geschützt werden sollen. Bei der Angabe einer Pfadgruppe muss der Sicherheitsadministrator einen Namen für die Pfadsammlung erstellen. Der Schutz erfolgt rekursiv vom angegebenen Pfad ausgehend für alle Unterverzeichnisse. Das Hinweisfeld ist optional.

Frage: Was ist ein Datentyp in der PPM-Konsole und wie wird er verwendet?

Antwort: Ein Datentyp ist eine geordnete Liste der Zugriffsdefinitionszeilen, die einem bestimmten Typ von Daten zugeordnet sind. Jede Zeile besteht aus einem Selektor, einer E/A-Operation, einer Aktionsdefinition und einem zugeordneten Schlüssel. Beim Erstellen eines Agenten wird der Datentyp einem Dateipfad (oder einer Pfadgruppe) zugeordnet um die operative Zugriffssteuerung und die Verschlüsselungszugriffsteuerung für die Daten zu definieren.

Frage: Was ist ein Agent in der PPM-Konsole und wie wird er verwendet?

Antwort: PPM unterstützt vier Typen von Agenten, von denen unterschiedliche Arten des Schutzes bereitgestellt werden. Die Agententypen sind 'Datenträger', 'Datei mit Richtlinie', 'Datenträger mit Richtlinie' und 'Objektspeicher'. Der Agent des Typs 'Datenträger' schützt die Daten auf der Ebene des Datenträgers. Der Agent des Typs 'Datei mit Richtlinie' schützt die Daten auf Dateiebene und stellt dateibasierte operative Zugriffssteuerung sowie optional eine Verschlüsselungszugriffssteuerung bereit. Der Agent des Typs 'Datenträger mit Richtlinie' schützt die Daten auf Datenträgerebene und stellt dateibasierte operative Zu-

griffssteuerung bereit. Agenten des Typs 'Objektspeicher' verschlüsseln Daten, die an einen oder mehrere cloudbasierte Objektspeicher gesendet werden, und führen für diese Daten kryptografisches Datensplitting durch.

Frage: Wann sollte der Agent des Typs 'Datenträger' eingesetzt werden? Wie funktioniert dieser Schutz?

Antwort: Der Agent des Typs 'Datenträger' bietet der IT Schutz von ruhenden Daten (Data at Rest) in Form eines geschützten, vordefinierten Datenträgers. Bei der Bereitstellung erstellt der Datenträger eine Gruppe von Schlüsseln, die auf den gesamten Datenträger angewendet werden und die den Datenträger als einzelne Einheit durch Verschlüsselung schützen. Beim Speichern und/oder Bearbeiten, Hinzufügen oder Löschen von Daten und Dateien werden die Verschlüsselungsalgorithmen aufgerufen, um sicherzustellen, dass alle Daten auf dem Datenträger ordnungsgemäß gesichert sind. Ein Datenträger kann in eine oder mehrere Partitionen aufgeteilt werden, wobei die einzelnen Partitionen auf ähnliche Weise geschützt sind. Der Datenträgerschutz ist an besten für Benutzergruppen geeignet, die mittlere bis große Datenmengen offen gemeinsam nutzen wollen.

Frage: Wann sollte der Agent des Typs 'Datei mit Richtlinie' eingesetzt werden? Wie funktioniert dieser Schutz?

Antwort: Ein Agent des Typs 'Datei mit Richtlinie' bietet der IT extrem leistungsfähigen, individuellen Schutz auf Dateibasis. Bei der Bereitstellung eines Dateiagenten wird das Verzeichnis der höchsten Ebene als Speicherort der geschützten Daten identifiziert. Jede in diesem Verzeichnis gespeicherte Datei wird einzeln mit einer Gruppe von Schlüsseln geschützt, während Zugriffsteuerungsdateien für Benutzer, Gruppen und Prozesse über in PPM definierte Richtlinien verwaltet werden. Darüber hinaus kann ein Sicherheitsadministrator einen Verschlüsselungsschlüssel definieren, der so auf Benutzer, Gruppen und Prozesse angewendet werden kann, dass die ausgewählten Dateien gegenüber anderen Benutzern, Gruppen und Prozessen, die ebenfalls Zugriff auf dieses Verzeichnis haben, durch Verschlüsselung geschützt sind. Beim Zugriff auf Dateien kann eine Option ausgewählt werden, mit der jeder Zugriff (Lesen, Schreiben oder beide) zu Prüfungs- und Überwachungszwecken protokolliert wird. Es gibt keine Beschränkung der Dateigröße oder der Größe der Speicherumgebung mit Dateischutz - wenn mehr Speicherplatz benötigt wird, wächst der Speicherplatz mit der Größe der in ihm enthaltenen Dateien. Der Dateischutz mit Richtlinie ist am besten für den Schutz einzelner, gemeinsam oder privat genutzter Dateien geeignet.

Frage: Wann sollte der Agent des Typs 'Datenträger mit Richtlinie' eingesetzt werden? Wie funktioniert dieser Schutz?

Antwort: Beim Agent des Typs 'Datenträger mit Richtlinie' wird die Dateizugriffsteuerung für Benutzer und Gruppen zum geschützten Datenträger (oder der geschützten Partition) hinzugefügt. Bei der Bereitstellung erstellt der Datenträgeragent eine Gruppe von Schlüsseln, die auf den gesamten Datenträger angewendet werden und die den Datenträger als einzelne Einheit durch Verschlüsselung schützen. Beim Speichern und/oder Bearbeiten, Hinzufügen oder Löschen von Dateien werden die Verschlüsselungsalgorithmen verwendet, um sicherzustellen, dass alle Daten auf dem Datenträger ordnungsgemäß gesichert sind. Ein Sicherheitsadministrator kann mithilfe von PPM Richtlinien für die Dateizugriffsteuerung für Benutzer, Gruppen oder Prozesse erstellen. Beim Zugriff auf Dateien kann eine Option ausgewählt werden, mit der jeder Zugriff (Lesen, Schreiben oder beide) zu Prüfungs- und Überwachungszwecken protokolliert wird. Der Datenträgerschutz mit Richtlinien ist an besten für Benutzergruppen geeignet, die die Dateizugriffsteuerung benötigen und die darüber hinaus mittlere bis große Datenmengen gemeinsam nutzen wollen.

Frage: Wann sollte der Agent des Typs 'Objektspeicher' eingesetzt werden? Wie funktioniert dieser Schutz?

Antwort: Ein Agent des Typs 'Objektspeicher' ermöglicht das Speichern von Daten im hoch skalierbaren, effizienten Objektspeicher lokal oder in der Cloud. Die Daten werden vom Kunden kontrolliert und sind stets privat und verfügbar. Der Zugriff wird vom Eigner des Objektspeicher gesteuert. Daten, die über den Agenten des Typs 'Objektspeicher' gesendet werden, werden lokal verschlüsselt und während der Über-

tragung zusätzlich mithilfe des TLS-Protokolls (Transport Layer Security) geschützt. So wird sichergestellt, dass die Daten vom lokalen Standort bis zum S3-kompatiblen Cloudspeicher gesichert sind. 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.

Frage: Was ist ein Job in der PPM-Konsole und wie wird er verwendet?

Antwort: PPM enthält ein Jobsystem, auf das über die GUI zugegriffen werden kann, um die Genehmigung, die Ablaufsteuerung und die Ausführung der einzelnen Bereitstellungs-, Richtlinien- und Verwaltungstasks im Zusammenhang mit den geschützten Daten und der Steuerung des Zugriffs auf die Daten zu verwalten und zu verfolgen. Wenn ein Administrator eine Task eingibt, wird ein Job erstellt. Der neue Job wird zur Liste der Jobs hinzugefügt, die auf der Seite 'Jobs' angezeigt werden. Administratoren mit der entsprechenden Berechtigung haben die Möglichkeit, die einzelnen Jobs zu genehmigen, abzuweisen oder auf eine Aktion zu verzichten.

Frage: In welchen Fällen muss für IBM Multi-Cloud Data Encryption eine externe PostgreSQL-Datenbank verwendet werden?

Antwort: Eine externe Postgres-Datenbank wird in allen Produktionsumgebungen dringend empfohlen. Eine interne Datenbank wird nur in sehr kleinen Installationen (wenige Agenten, wenige Benutzergruppen) oder in Test- oder Qualitätssicherungsinstallationen mit geringen Wachstumsaussichten empfohlen. Darüber hinaus ist eine Postgres-Datenbank erforderlich, wenn MDE in einer Hochverfügbarkeitskonfiguration bereitgestellt wird.

Zertifikate - Häufig gestellte Fragen

Frage: Welche Voraussetzungen gelten für PPM-Serverzertifikate?

Antwort: Die PPM-Serverzertifikate müssen die folgenden Elemente aufweisen:

- Erweiterte Schlüsselattribute für die Serverauthentifizierung.
- Einen Abschnitt für den alternativen Namen des Subjekts, der den vollständig qualifizierten Domänenname (Fully Qualified Domain Name, FQDN) für den PPM-Server angibt.

Frage: Welche Voraussetzungen gelten für Agentenzertifikate?

Antwort: Jedes Agentenzertifikat muss die folgenden Elemente aufweisen:

- Erweiterte Schlüsselattribute für die Clientauthentifizierung.
- Einen Abschnitt für den alternativen Namen des Subjekts, der den vollständig qualifizierten Domänenname (Fully Qualified Domain Name, FQDN) für den Agenten angibt.

Frage: Unterstützt PPM NAT- (NAT, Network Address Translation) oder PAT-Verbindungen (PAT, Port Address Translation)?

Antwort: Ja. Der PPM-Server muss über den Agenten erreichbar sein, damit die Kommunikation hergestellt werden kann, da der Agent die Kommunikationssitzung zum PPM-Server initiiert. Sobald die Kommunikation hergestellt wurde, bleibt sie geöffnet. Der Agent sendet über diese Verbindung Ereignisdaten an den PPM-Server. Der PPM-Server wiederum sendet über diese Verbindung Richtlinienaktualisierungen an den Agenten.

Frage: Wie werden PPM-Serverzertifikate für einen PPM-Server in einer NAT-Netzkonfiguration (Network Address Translation) oder einer PAT-Netzkonfiguration (Port Address Translation) konfiguriert?

Antwort: Die PPM-Serverzertifikate müssen die folgenden Elemente aufweisen:

- Erweitere Schlüsselattribute für die Serverauthentifizierung.
- Einen Abschnitt für den alternativen Namen des Subjekts, der den vollständig qualifizierten Domänenname (Fully Qualified Domain Name, FQDN) für den PPM-Server angibt.
- Einen Abschnitt für den alternativen Namen des Subjekts, der die externe IP-Adresse angibt.

Frage: Wie werden Agentenzertifikate konfiguriert, wenn sich ein Agent in einer NAT-Netzkonfiguration (Network Address Translation) oder in einer PAT-Netzkonfiguration (Port Address Translation) befindet?

Antwort: Die Agentenzertifikate müssen die folgenden Elemente aufweisen:

- Erweitere Schlüsselattribute für die Clientauthentifizierung.
- Einen Abschnitt für den alternativen Namen des Subjekts, der den vollständig qualifizierten Domänenname (Fully Qualified Domain Name, FQDN) für den PPM-Server angibt.
- Einen Abschnitt für den alternativen Namen des Subjekts, der die externe IP-Adresse angibt.

Frage: Welche Voraussetzungen gelten für PPM-Serverzertifikate in einer Hochverfügbarkeitskonfiguration (HA-Konfiguration)?

Antwort: Die PPM-Serverzertifikate müssen die folgenden Elemente aufweisen:

- Erweitere Schlüsselattribute für die Serverauthentifizierung.
- Einen Abschnitt für den alternativen Namen des Subjekts, der den vollständig qualifizierten Domänenname (Fully Qualified Domain Name, FQDN) für den PPM-Server angibt, aus dem der PPM-Cluster besteht, sowie den FQDN, der der virtuellen PPM-IP-Adresse zugeordnet ist.

Häufig gestellte Fragen zu Schlüsseln und zur Verarbeitung von Schlüsseln

Frage: Welche Operationen zum Verarbeiten von Schlüsseln kann IBM Multi-Cloud Data Encryption ausführen?

Antwort: Ein Sicherheitsadministrator kann Verschlüsselungsschlüssel definieren, um Daten in Policy Provisioning Manager (PPM) zu sichern. Diese Schlüssel können Datentypen, Datentypzeilen und Datenträgern zugeordnet werden. Zu den Optionen für das Verarbeiten von Schlüsseln gehören das Erstellen, das turnusmäßige Wechseln, das Widerrufen und das Schreddern oder Löschen von Schlüsseln.

Frage: Warum sollten Schlüssel turnusmäßig gewechselt (rotiert) werden?

Antwort: Die regelmäßige Schlüsselrotation ist im Allgemeinen erforderlich, um sicherzustellen, dass die Daten ausreichend gegen unbefugten Zugriff geschützt sind. Bei der Schlüsselrotation werden die aktuellen Schlüssel durch neue Schlüssel ersetzt. Wegen der Funktionsweise der Verschlüsselung ist dafür eine Rechenoperation mit Verschlüsselungsalgorithmen erforderlich. Die regelmäßige Schlüsselrotation wird von vielen Experten für IT-Abteilungen in Unternehmen empfohlen, besonders für solche Abteilungen, die mit der Cloud interagieren. Heutzutage gibt es Standards, die eine regelmäßige Rotation fordern, wie beispielsweise PCI-DSS. Bei der PPM-Schlüsselrotation werden Datensätze mit Zeitmarken erstellt, die zu Prüfzwecken zum Nachweis der Konformität protokolliert werden.

Frage: Warum sollten Schlüssel widerrufen werden?

Antwort: Wird ein Schlüssel mit Policy Provisioning Manager (PPM) widerrufen, wird der Zugriff auf geschützte Daten vorübergehend inaktiviert. Schlüssel werden normalerweise widerrufen, wenn der Datenschutz fraglich ist oder wenn der Zugriff auf geschützte Daten abgelehnt werden muss. Wird derselbe Schlüssel später erneut verteilt, kann auf die Daten wieder zugegriffen werden.

Frage: Warum sollten Schlüssel geschreddert werden?

Antwort: Beim Schreddern von Schlüsseln wird der Zugriff auf geschützte Daten dauerhaft inaktiviert. Verwenden Sie diese Option nur, wenn die Daten nicht mehr gebraucht werden.

Frage: Verwaltet IBM Multi-Cloud Data Encryption die Schlüssel für mich?

Antwort: Wenn ein Sicherheitsadministrator die Verschlüsselungsschlüssel nicht manuell verwalten will, kann Policy Provisioning Manager (PPM) für jede neu erstellte Richtlinie automatisch einen Schlüssel erstellen. Automatisch generierte Schlüssel sind bei ihrer Erstellung immer eindeutig; sie werden auf der Seite für die Schlüsselverwaltung nicht angezeigt.

Häufig gestellte Fragen zur Installation und Konfiguration

Frage: Wie wirkt sich die Verwendung von IBM Multi-Cloud Data Encryption (MDE) auf Endbenutzer (d. h. Benutzer ohne Verwaltungsaufgaben) aus?

Antwort: Benutzern ohne Verwaltungsaufgaben wird die Sicherheit und Hochverfügbarkeit von IBM Multi-Cloud Data Encryption (MDE) bereitgestellt, ohne dass die Benutzer einen Unterschied gegenüber dem normalen Betrieb bemerken. Wenn sich Dateien in einem verwalteten (geschützten) Verzeichnis befinden, hat dies keine Auswirkung darauf, wie Benutzer auf Dateien zugreifen, in Dateien schreiben und Dateien speichern können.

Frage: Kann ein MDE-Agent auf einem Docker-Host installiert werden und alle Lese-/Schreibanforderungen von Anwendungen in Docker-Containern verarbeiten?

Antwort: Ja. Sowohl der Agent des Typs 'Datei mit Richtlinie' als auch der Agent des Typs 'Datenträger' können für den Schutz der Daten eingesetzt werden.

- Der Agent des Typs 'Datei mit Richtlinie' kann dazu verwendet werden, den Docker-Datenträgerpfad zu schützen, der sicherstellt, dass die vom Container verwendeten Anwendungsdaten geschützt sind.
- Der Agent des Typs 'Datenträger' kann dazu verwendet werden, den Docker-Container-Pfad zu schützen. Er verschlüsselt den gesamten Container und dessen gesamte Ein-/Ausgabe effektiv. Wenn der Docker-Datenträger außerhalb des Docker-Container-Pfads gespeichert ist, kann ein weiterer Datenträger konfiguriert werden, um den externen Docker-Datenträger zu schützen.
- Ein zentraler Aspekt ist, dass auf dem Docker-Host ein unterstützter Kernel unter Red Hat 7.2+ (3.10-*) ausgeführt werden muss.

Häufig gestellte Fragen zur Konfiguration

Frage: Kann ich HTML-Dateien mit IBM Multi-Cloud Data Encryption (MDE) verschlüsseln?

Antwort: Gegenwärtig wird nicht empfohlen, HTML-Dateien zu schützen. Websites zeigen aktive HTML-Dateien an, die möglicherweise nicht ordnungsgemäß dargestellt werden, wenn sie verschlüsselt sind.

Häufig gestellte Fragen zum Betrieb

Frage: Kann ich sicher sein, dass meine Daten mit IBM Multi-Cloud Data Encryption (MDE) geschützt sind?

Antwort: Der MDE-Schutz ist auch dann aktiv, wenn auf eine geschützte Datei zugegriffen wird, während der Service gestoppt ist.

Frage: Welche Vorsichtsmaßnahmen werden empfohlen, bevor Änderungen an einer Produktionsimplementierung von IBM Multi-Cloud Data Encryption (MDE) vorgenommen werden?

Antwort: Kleinere Änderungen können während des Systembetriebs mithilfe des Befehlszeilenbefehls 'spxconfig' oder über die GUI vorgenommen werden. Für größere Änderungen ist jedoch eine detaillierte Vorbereitung erforderlich, zu der auch empfohlene Sicherungen gehören. Vor dem Implementieren von Änderungen sollten Sie die gesamte Produktdokumentation lesen, um sich mit dem Produktionsumfeld vertraut zu machen.

Frage: Kann ich Ereignisse aus IBM Multi-Cloud Data Encryption (MDE) an andere SIEM-Korrelationsanwendungen (SIEM - Security Information and Event Management) weiterleiten?

Antwort: Ja. MDE enthält ein Ereignisaggregations- und Ereignisweiterleitungssystem. Dieses System aggregiert Ereignisse aus verwalteten Agenten sowie intern generierte Ereignissen und speichert die Ereignisse in einem internen Ereignisprotokoll. Das Ereignisprotokoll kann über das Administratordashboard angezeigt werden und kann so konfiguriert werden, dass es Ereignisse an einen oder mehrere Empfänger weiterleitet.

Fragen: Ist Groß-/Kleinschreibung wichtig?

Antwort: Ja, Groß-/Kleinschreibung ist sehr wichtig.

- Beim Erstellen von Selektoren muss bei Feldern für Benutzer und Gruppen die Groß-/Kleinschreibung beachtet werden.
- Beim Erstellen einer Pfadgruppe unter Windows muss der Laufwerksbuchstabe groß geschrieben und beim Verzeichnisnamen die Groß-/Kleinschreibung beachtet werden.
- Beim Erstellen von Agenten des Typs 'Datenträger' oder 'Datenträger mit Richtlinie' muss für die Datenträgerbezeichnung die Groß-/Kleinschreibung beachtet werden.
- Die Beachtung der Groß-/Kleinschreibung sollte immer für einen Wert oder ein Feld angenommen werden.

Frage: Was bedeutet die Operationsreihenfolge und warum ist diese wichtig?

Antwort: Sie ist wichtig, da das Erstellen und Bereitstellen eines Agenten in einer bestimmten Reihenfolge durchgeführt werden muss, damit der Vorgang erfolgreich ist.

- Vor dem Bereitstellen eines Dateiagenten muss der Zieldatenträger online, initialisiert und mit erstellten Verzeichnissen mit den entsprechenden Berechtigungen formatiert sein.
- Vor dem Bereitstellen von Agenten des Typs 'Datenträger' muss der Datenträger vorhanden, online und initialisiert, jedoch nicht formatiert sein.
- Vor dem Bereitstellen von Agenten des Typs 'Datenträger mit Richtlinie' muss der Datenträger vorhanden, online und initialisiert, jedoch nicht formatiert sein. Definierte Selektoren müssen in den lokalen Hierarchien des Zielsystems oder LDAP- oder Active Directory-Hierarchien vorhanden sein.

Frage: Ich habe einen Snapshotaktivierungsjob übergeben und er ist immer noch aktiv. Wann wird er beendet?

Antwort: Snapshotänderungen oder -aktualisierungen treten erst dann in Kraft, wenn der Agent mit dem PPM-Server kommunizieren kann. Der erstellte Job wird so lange ausgeführt, bis der Agent erfolgreich mit dem PPM-Server kommunizieren kann oder der Agent vom PPM-Server entfernt wird.

Häufig gestellte Fragen zur Hochverfügbarkeit

Frage: Wann ist Hochverfügbarkeit für eine MDE-Bereitstellung erforderlich?

Antwort: Eine MDE-Bereitstellung mit Hochverfügbarkeit (High Availability - HA) sollte in IT-Umgebungen verwendet werden, wenn für deren Datenzugriffs- und Schutzmanagementservices eine Verfügbarkeit von annähernd 100 % erforderlich ist. Falls für die PPM-Instanz Wartungsarbeiten erforderlich werden oder falls die Instanz fehlschlägt oder versehentlich inaktiviert wird, wird die Hot Backup-Instanz sofort aktiviert und setzt den Betrieb fort.

Frage: Sind für eine MDE-Bereitstellung mit Hochverfügbarkeit Einrichtungen für den Lastausgleich erforderlich?

Antwort: Ja. Zwei Einrichtungen für den Lastausgleich (Lastausgleichscluster) müssen zwischen den Agenten und den PPM-Servern eingerichtet werden. An jeder Position, an der mindestens zwei PPM-Server bereitgestellt sind, ist ein Lastausgleichscluster erforderlich. Die Einrichtungen für den Lastausgleich kommunizieren untereinander über ein lokales Teilnetz und stellen eine virtuelle IP-Adresse (d. h. eine variable IP-Adresse) bereit, die von den Agenten und Administratoren für den Zugriff auf die PPM-Server verwendet wird. Für PPM mit Hochverfügbarkeit sind verschiedene Szenarios möglich: eine einzelner Standort, mehrere Rechenzentren usw. Jedes Szenario umfasst spezielle Bereitstellungsoptionen und Konfigurationen.

Häufig gestellte Fragen zur Multi-Tenant-Funktionalität

Frage: Wozu dient die Multi-Tenant-Funktion?

Antwort: Die Multi-Tenant-Funktionalität von PPM gibt IT-Anbietern die Möglichkeit, die PPM-Steuerung nach Benutzern zu untergliedern. Dadurch erhält jeder Benutzer eine eigene, isolierte Anmeldung bei PPM mit eigenen Administratoren, Richtlinien, Dashboards, Jobs, Ereignissen usw. innerhalb der IT-Umgebung. Kunden können Speicherplatz und sogar Verzeichnisse gemeinsam nutzen; ihre geschützten Dateien und Datenträger sind jedoch individuell durch Verschlüsselung voneinander geschützt. Dadurch können mehrere Nutzer (Tenants) oder Kunden denselben Speicherplatz gemeinsam nutzen, während die Daten der einzelnen Nutzer voneinander getrennt und für andere Nutzer und Kunden nicht sichtbar sind.

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 dieser Dokumentation 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 Programmiertechniken 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 Servicenamen 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 Servicenamen 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>.



Teilenummer CC0LSEN

GC43-5032-00



(1P) P/N: CC0LSEN

