IBM Multi-Cloud Data Encryption Powered by SPx®

バージョン 2.2

よくあるご質問 (FAQ)

IBM

IBM Multi-Cloud Data Encryption Powered by SPx®

バージョン **2.2**

よくあるご質問 **(FAQ)**

IBM

注記

本書および本書で紹介する製品をご使用になる前に、 15 ページの『特記事項』に記載されている情報をお読みください。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM Multi-Cloud Data Encryption Powered by SPx®
Version 2.2
Frequently Asked Questions (FAQ)

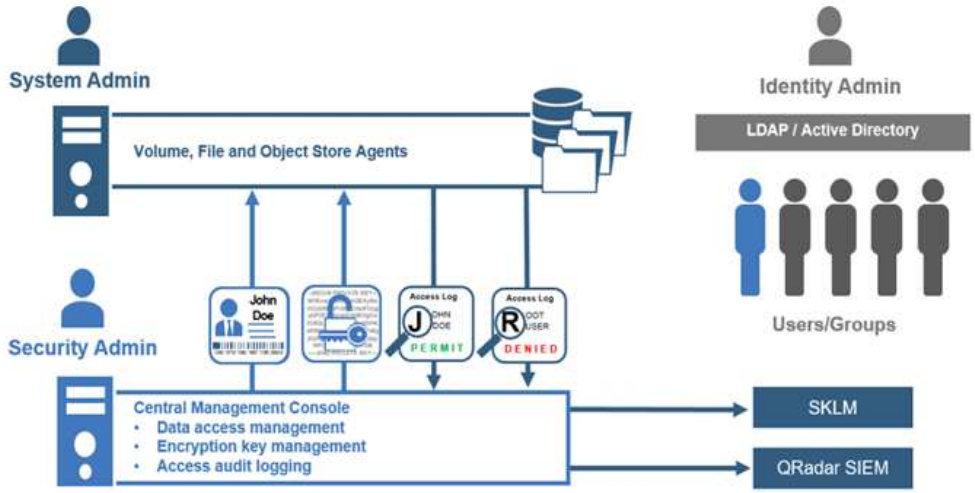
発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

概説

IBM Multi-Cloud Data Encryption (MDE) は SPx® テクノロジーを採用した包括的なデータ・セキュリティー製品であり、保存データの暗号化 (エージェントを使用) と、一元管理コンソールとして機能する Policy Provisioning Manager (PPM) の追加の強力な保護機能を組み合わせたものです。MDE では、最大 25,000 エージェントについて、中央の 1 カ所からエージェントのプロビジョニング、データ・アクセス・ポリシーの設定 (操作および暗号化のアクセス定義)、および管理 (鍵のライフサイクル、エージェントの更新、およびユーザー・アクセスのロギング) が可能です。MDE は、固有の暗号分割テクノロジーを使用してファイル・システム・レベルまたはボリューム・レベルでデータを暗号化するエージェントを柔軟に割り当てることができる、シームレスでセキュアなシステムを提供します。このテクノロジーによって、データ暗号化をより強固にしてブルート・フォース・アタックを寄せ付けない、標準の暗号化を超えるデータ中心の保護を提供しています。MDE では、詳細なアクセス・ポリシーを定義することによって、データ・アクセスをユーザー・レベルで制限、モニター、および監査できることで、保護をさらに 1 歩先に進めます。



MDE では、製品管理者およびセキュリティー管理者という別々の管理者役割を使用して職務を分離します。製品管理者役割には、MDE 製品の構成と保守に必要な権限が委託されます。セキュリティー管理者役割には、エージェントのプロビジョンおよび管理に必要な権限が委託されます。図 1 は、これらの役割を示しています。詳細については、セクション 7『MDE 管理ユーザーの管理』で説明します。

次の 4 つのタイプのエージェントをデプロイして、保護データまたは暗号データのポリシー定義を実施できます。(1) ボリューム・エージェント。ボリューム・ポリシー定義と、1 つ以上の保護ボリュームの関連付けを実施します。(2) ファイル/ポリシー・エージェント。ファイル・ベースの操作アクセス・ポリシー定義と、1 つ以上の保護ファイルのパスの関連付けを実施します。保護ファイルのパスはそれぞれ、非常に細かいポリシー指定を通じて定義された独自の操作ポリシーとアクセス制御ポリシーを持つことができます。(3) ボリューム/ポリシー・エージェント。ボ

リューム・エージェントのボリューム・ポリシー保護を活用し、ファイル・ベースの操作アクセス制御ポリシーを 1 つ以上の保護ファイルのパスに適用して実施することを許可します。(4) オブジェクト・ストア・エージェント。1 つ以上のクラウド・ベースのオブジェクト・ストレージに送信されるデータを暗号化し、暗号的に分割します。

MDE - よくあるご質問 (FAQ)

一般的な FAQ

Q: IBM Multi-Cloud Data Encryption (MDE) とは、どのような製品ですか?

A: MDE は、中心となる単一の場所から、エージェント、ポリシー (操作アクセスおよび暗号化アクセスの定義)、および最大で 25,000 件までのエージェントの管理 (ライフサイクル更新およびユーザー監査) をプロビジョニングできる機能を導入し、使用可能にする製品です。MDE は、ボリューム、ファイル/ポリシー、ボリューム/ポリシー、およびオブジェクト・ストアという 4 つのタイプのエージェントのデプロイをサポートしています。これらのエージェントは、簡単にインストールすることができ、エンド・ユーザーに対してシームレスであり、管理者に IT 環境のコンプライアンス要件を満たすようにソフトウェアを構成してデプロイする機能を提供します。

Q: IBM Multi-Cloud Data Encryption (MDE) では、どのようなオペレーティング・システムがサポートされますか?

A: MDE は現在、次のオペレーティング・システムがサポートされています。

- Red Hat® Enterprise Linux 6.2 カーネル・バージョン 2.6.32-220 以降のリリース
- Red Hat® Enterprise Linux 7.2 以降のカーネル・バージョン
- CentOS 6.2 カーネル・バージョン 2.6.32-220 以降のリリース
- CentOS 7.2 カーネル・バージョン以降のリリース
- Microsoft Windows Server® 2008R2
- Microsoft Windows Server® 2012
- Microsoft Windows Server® 2012R2
- Microsoft Windows Server® 2016

Q: MDE では、どのようなファイル・システムがサポートされていますか?

A: MDE では、次のファイル・システムがサポートされています。

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

Q: IBM Multi-Cloud Data Encryption (MDE) には、必要な前提条件がありますか?

A: MDE は、VMware ESXi™ または Microsoft Hyper-V に簡単にデプロイでき、他のほとんどのハイパーバイザーでも実行可能な、OVA として提供されます。

Q: IBM Multi-Cloud Data Encryption (MDE) では、どのブラウザーがサポートされますか?

A: MDE は、Firefox、Chrome™、または Microsoft Internet Explorer で実行できます。

Q: IBM Multi-Cloud Data Encryption (MDE) は、FIPS モードで実行されますか?

A: はい。MDE は、製品データシートに示されているように、FIPS 140.2 準拠の標準に従っています。

Q: Multi-Cloud Data Encryption (MDE) の使用時に、データをリモート・システムに送信するときに暗号化する必要はありますか? また、リモート・システムには、引き続き VPN 接続する必要がありますか?

A:MDE は、ファイルの場所へのアクセス権がある限り、パブリック・クラウド・サイトを含むリモート・サイトに安全にデータを書き込むように設計されています。ただし、リモート・サイトへの接続に VPN が必要になる場合もあります。

Q: 「IBM Multi-Cloud Data Encryption (MDE) は『データにセキュリティーをビット・レベルで組み入れる』」とは、どのような意味ですか?

A: SPx テクノロジーを採用した MDE は、暗号化、ビット・レベルでランダム化してキー付けしたデータ分割、認証 (保全性の検査)、フォールト・トレランス、および COI フレームワークを組み合わせることにより、識別可能なデータおよび情報を、完全にランダムで使用できない 2 進エレメントに変換するプロセスを作成します。MDE を操作すると、Information Assurance (IA) エレメントがデータの構造そのものに組み入れられます。セキュリティー、データ回復、信頼性、および情報共有フレームワークのすべてがデータが注ぎ込まれ、データにしっかり張り付き、不可欠なものとなります。データおよび情報は、その作成時からデータ破棄/パブリック・リリースまでのライフサイクルと通して、確実に保護されます。データは、保存される (ストレージに書き込まれる) ときも、アクセスされるときも、常に保護されます。

Q: IBM Multi-Cloud Data Encryption (MDE) でデータの保全性が維持される仕組みを説明してください。

A:データの保全性は、データの読み取り時に照合する必要があるメッセージ認証コードを使用して保証されます。

ポリシー、プロビジョニング、および管理に関する FAQ

Q: ポリシー、プロビジョニング、および管理 (PPM) には、どのような目的がありますか?

A: PPM は、エージェント (データ保護モデル)、ポリシー (操作アクセスおよび暗号化アクセスの定義)、および最大で 25,000 件までのエージェントの管理 (ライフサイクル更新およびユーザー監査) のプロビジョニングを、1 箇所から集中的に管理します。これは、ボリューム、ファイル/ポリシー、ボリューム/ポリシー、およびオブジェクト・ストアという 4 つのタイプのデータ暗号化エージェントのデプロイをサポートしています。ボリュームは、ブロック・デバイス・レベルでデータを保護します。ファイル/ポリシーは、ファイル・レベルでデータを保護し、ファイル・ベースの操作アクセス制御を提供します。ボリューム/ポリシーは、ファイル・ベースの操作アクセス制御と共にブロック・デバイス・レベルでデータを保護します。オブジェクト・ストアは、1 つ以上のクラウド・ベースのオブジェクト・ストレージに送信されるデータを暗号化し、暗号的に分割します。

Q: ポリシー、プロビジョニング、および管理 (PPM) で役割ベースのアクセス制御が使用される理由は何ですか?

A: PPM は、フラットで静的な役割ベースのアクセス制御 (RBAC) 設計を活用しています。PPM 内の機能を使用するには、特定の許可が必要です。役割には、製品管理者とセキュリティー管理者の 2 つの異なるタイプがあります。共通の権限はいくつかありますが、役割を分離することで、IT リーダーは管理任務を明確に分離することができ、従業員の不正による IT 環境の破壊を防ぎます。各タイプにさらに役割を追加することで、より大規模な、またはより複雑な IT 環境を適切にサポートすることができます。また、顧客はジョブの承認に必要な管理者の数と、ジョブの拒否に必要な管理者の数をプログラムで定義できます。そうすることで、PPM が役割のセットごとに管理者の承認と拒否を追跡し、実行または拒否に十分な承認があることを確認します。必要な数の管理者がジョブを承認すると、ジョブは実行されます。必要な数の管理者がジョブを拒否すると (この数は、承認の数と異なる場合があります)、ジョブはキャンセルされます。これにより、管理関連のタスクとセキュリティー関連のタスクを正確に管理できるようになります。一連の承認や拒否は、監査およびコンプライアンスの目的で両方とも追跡され、ログに記録されます。

Q: ポリシー、プロビジョニング、および管理 (PPM) コンソールの「プロセス」とは、どのようなものですか? また、これは何のために使用されますか?

A: 「ポリシー経由のプロセス」とも呼ばれる「プロセス」は、IBM Multi-Cloud Data Encryption によって保護されているデータへのアクセス制御が割り当てられているプロセスまたはアプリケーションのリストです。プロセスはセレクターに関連付けられて、ターゲット・システム上のユーザー経由でプロセスのアクセス制御を提供します。

Q: ポリシー、プロビジョニング、および管理 (PPM) コンソールの「Selector」(セレクター) とは、どのようなものですか? また、これは何のために使用されますか?

A: セレクターとは、ユーザー、グループ、およびプロセスの順不同リストのことです。データ・タイプに結合されることで、セキュリティー管理者に対して、MDE で保護されたデータを共有するエンティティー、または MDE で保護されたデータに対して共通のアクセス権を持つエンティティーのコレクションを簡単に識別する方法を提供します。「セレクター」は、オプションの「ユーザー」、オプションのグループ・ソース (内部または LDAP が定義されている場合は外部) 付き「グループ」フィールド、あるいはオプションの「ポリシー経由のプロセス」から構成される場合があります。

Q: ポリシー、プロビジョニング、および管理 (PPM) コンソールの「パス・セット」とは、どのようなものですか? また、これは何のために使用されますか?

A: パス・セットとは、MDE ポリシーで保護されるファイル・パス (ポリシーによっては、ポリシー保護から除外されるファイル・パス) の順不同リストのことです。これにより、セキュリティー管理者は、MDE で保護されるファイル・パスのコレクションを簡単に指定またはリストできます。「Path Set」を指定するとき、セキュリティー管理者は、パスのコレクションの名前を作成する必要があります。保護は、指定されたパスからサブディレクトリーまで再帰的に行われます。「メモ」フィールドはオプションです。

Q: ポリシー、プロビジョニング、および管理 (PPM) コンソールの「Datatype」(データ・タイプ) とは、どのようなものですか? また、これは何のために使用されますか?

A: データ・タイプとは、指定のタイプのデータに割り当てられたアクセス定義行の番号付きリストのことです。各行は、セレクター、入出力操作、アクション定義、および関連する鍵から構成されます。エージェントの作成時、データ・タイプはファイル・パス (またはパス・セット)に関連付けられ、データに対する操作アクセス制御および暗号化アクセス制御が定義されます。

Q: ポリシー、プロビジョニング、および管理 (PPM) コンソールの「Agent」(エージェント) とは、どのようなものですか? また、これは何のために使用されますか?

A: PPM は、それぞれ異なるタイプの保護を提供する 4 つのエージェント・タイプをサポートしています。これらは、ボリューム、ファイル/ポリシー、ボリューム/ポリシー、およびオブジェクト・ストアです。ボリュームは、ボリューム・レベルでデータを保護します。ファイル/ポリシーは、ファイル・レベルでデータを保護し、ファイル・ベースの操作アクセス制御、およびオプションの暗号化アクセス制御を提供します。ボリューム/ポリシーは、ボリューム・レベルでデータを保護し、ファイル・ベースの操作アクセス制御を提供します。オブジェクト・ストアは、1 つ以上のクラウド・ベースのオブジェクト・ストレージに送信されるデータを暗号化し、暗号的に分割します。

Q: ボリューム・エージェントはいつ使用すべきですか? また、このタイプの保護はどのように機能しますか?

A: ボリューム・エージェントには、保存データの安全保護機能が、保護された定義済みボリュームという形で IT に対して用意されています。ボリューム・エージェントは、デプロイメント時に一連の鍵を作成します。これらの鍵はボリューム全体に適用されるため、ボリュームは 1 つのユニットとして暗号化されて保護されます。データやファイルが保管、編集、追加、削除されると、ボリューム内のすべてのデータが適切に保護されるように暗号化アルゴリズムが呼び出されます。1 つのボリュームを 1 つ以上のパーティションに分割して、各パーティションを同じように保護できます。ボリューム保護は、中程度の量から大量のデータを開放的に共有するユーザー・グループに最適です。

Q: ファイル/ポリシー・エージェントはいつ使用すべきですか? また、このタイプの保護はどのように機能しますか?

A: ファイル/ポリシー・エージェントには、非常に強力な個々のファイル・レベルの保護機能が IT に対して用意されています。ファイル・エージェントをデプロイするときは、保護データの場所として最上位ディレクトリーが特定されます。このディレクトリーに保管される各ファイルは、一連の鍵により個々に保護されます。一方、ユーザー、グループ、およびプロセスに対するファイルへのアクセス制御は、PPM で定義されたポリシーを通じて管理されます。セキュリティー管理者は、ユーザー、グループ、またはプロセスに適用可能な暗号鍵を定義して、ディレクトリーへのアクセスを共有する他のユーザーから、選択されたファイルを暗号化して保護することもできます。ファイル・アクセス時に監査および追跡の目的で各アクセス (読み取り、書き込み、またはその両方) をログに記録することを許可するオプションを選択できます。ファイル保護の対象となるファイルのサイズやストレージ環境のサイズに制限はありません。スペース使用率は、ディレクトリー内のファイルのサイズに従って拡大し成長します。ポリシーによるファイル保護は、共有されるか、個人的に利用される個々のファイルを保護する場合に最適です。

Q: ボリューム/ポリシー・エージェントはいつ使用すべきですか? また、このタイプの保護はどのように機能しますか?

A: ボリューム/ポリシー・エージェントは、保護対象のボリューム (またはパーティション) に、ユーザーおよびグループのファイル・アクセス制御を追加します。ボリューム・エージェントは、デプロイメント時に一連の鍵を作成します。これらの鍵はボリューム全体に適用されるため、ボリュームは 1 つのユニットとして暗号化されて保護されます。ファイルが保管、編集、追加、削除されると、ボリューム内のすべてのデータが適切に保護されるように暗号化アルゴリズムが使用されます。セキュリティー管理者は、PPM を使用して、ユーザー、グループ、およびプロセスのファイル・アクセス制御ポリシーを定義できます。ファイル・アクセス時に監査および追跡の目的で各アクセス (読み取り、書き込み、またはその両方) をログに記録することを許可するオプションを選択できます。ポリシーによるボリューム保護は、中程度の量から大量のデータを共有するだけではなく、ファイル・アクセス制御も必要とするユーザー・グループに最適です。

Q: オブジェクト・ストア・エージェントはいつ使用すべきですか? また、どのように機能しますか?

A: オブジェクト・ストア・エージェントには、拡張性が高く、効率的なオブジェクト・ストレージ (オンプレミスまたはクラウド) にデータを格納する機会が用意されています。データは顧客が制御し、常に専用で使用できます。アクセスは、オブジェクト・ストレージの所有者によって制御されます。オブジェクト・ストア・エージェント経由で送信されるデータは、ローカルで暗号化され、さらに送信中も Transport Layer Security (TLS) プロトコルによって保護されます。これにより、オンプレミスから S3 対応のクラウド・ストレージに至るまで、データの安全性が確保されます。オブジェクト・ストア・エージェントは、「M of N」モデルを基盤として動作します。これは、作成されたデータの断片の総数 (N) のうち、そのデータを再構築するために必要な断片の数 (M) を決定します。格納されるデータの断片 (ライセンスに応じてローカルまたはリモートの場所に存在) は、「共有」と呼ばれます。複数の共有を使用すると、データ・フローが向上し、データ回復とフォールト・トレランスのオプションが追加されます。サポートされる M of N 分散共有モデルは、1:1、2:3、または 2:4 です。

Q: ポリシー、プロビジョニング、および管理 (PPM) コンソールの「job」(ジョブ) とは、どのようなものですか? また、これは何のために使用されますか?

A: PPM には、GUI から利用可能なジョブ・システムが組み込まれています。このシステムにより、各種のデプロイメント、ポリシー、および保守タスク (保護データと、それにアクセス可能な主体に関するタスク) の承認、時間調整、および実行を管理および追跡できます。管理者がタスクを入力すると、ジョブが作成され、この新しいジョブが「jobs」ページに表示されるリストに追加されます。各ジョブの承認、拒否、または保留を選択できるのは、権限を持つ管理者です。

Q: IBM Multi-Cloud Data Encryption では、どのようなときに外部 PostgreSQL データベースを使用する必要がありますか?

A: 外部 Postgres データベースは、すべての実稼働環境で使用することを強くお勧めします。内部データベースが推奨されるのは、拡張の可能性がほとんどない非常に小規模なインストール済み環境 (エージェント、ユーザー、グループの数が非常に少ない、または単にテストや QA セットアップ用) に限られます。Postgres データベースは、MDE を高可用性 (HA) 構成でデプロイするときも必要です。

証明書の FAQ

Q: PPM サーバー証明書の要件はどのようなものですか?

A: PPM サーバー証明書には、次の要素が含まれている必要があります。

- 「サーバー認証」を指定する拡張鍵属性
- PPM サーバーの完全修飾ドメイン名 (FQDN) を指定する「Subject Alternative Name」セクション

Q: エージェント証明書の要件はどのようなものですか?

A: 各エージェント証明書には、次の要素が含まれている必要があります。

- 「クライアント認証」を指定する拡張鍵属性
- エージェントの完全修飾ドメイン名 (FQDN) を指定する「Subject Alternative Name」セクション

Q: PPM はネットワーク・アドレス変換 (NAT) 接続やポート・アドレス変換 (PAT) 接続をサポートしますか?

A: はい。通信を確立するためには、エージェントが PPM サーバーに到達できる必要があります。エージェントが PPM サーバーへの通信セッションを開始するためです。通信が確立されると、その通信は開いたままになります。エージェントは、この接続を使用して、PPM サーバーにイベント・データを送信します。PPM サーバーは、この接続を使用して、エージェントにポリシーの更新を送信します。

Q: ネットワーク・アドレス変換 (NAT) やポート・アドレス変換 (PAT) のネットワーク構成内にある PPM サーバーの PPM サーバー証明書をどのように構成すればよいですか?

A: PPM サーバー証明書には、次の要素が含まれている必要があります。

- 「サーバー認証」を指定する拡張鍵属性
- PPM サーバーの完全修飾ドメイン名 (FQDN) を指定する「Subject Alternative Name」セクション
- 外部向き IP アドレスを指定する「Subject Alternative Name」セクション

Q: エージェントがネットワーク・アドレス変換 (NAT) やポート・アドレス変換 (PAT) のネットワーク構成内にあるときは、エージェント証明書をどのように構成すればよいですか?

A: エージェント証明書には、次の要素が含まれている必要があります。

- 「クライアント認証」を指定する拡張鍵属性
- PPM サーバーの完全修飾ドメイン名 (FQDN) を指定する「Subject Alternative Name」セクション
- 外部向き IP アドレスを指定する「Subject Alternative Name」セクション

Q: 高可用性 (HA) 構成での PPM サーバー証明書の要件はどのようなものですか?

A: PPM サーバー証明書には、次の要素が含まれている必要があります。

- 「サーバー認証」を指定する拡張鍵属性
- PPM クラスターを構成する PPM サーバーの完全修飾ドメイン名 (FQDN)、および PPM 仮想 IP アドレスに関連付けられている FQDN を指定する「Subject Alternative Name」セクション

鍵および鍵の処理に関する FAQ

Q: IBM Multi-Cloud Data Encryption では、どのような鍵処理操作を実行できますか?

A: セキュリティー管理者は、Policy Provisioning Manager (PPM) 内でデータを保護するための暗号鍵を定義できます。これらの鍵は、データ・タイプ、データ・タイプ行、およびボリュームに関連付けることができます。鍵処理操作には、作成、ローテーション、取り消し、および破棄が含まれます。

Q: 鍵をローテーションする必要があるのはなぜですか?

A: 通常、鍵のローテーションは、データを無許可アクセスから十分に保護するために定期的に行う必要があります。鍵のローテーションとは、現在の鍵を真新しい鍵に置き換えることです。暗号化の性質上、暗号化アルゴリズムを使用した計算が必要になります。多くの専門家は、企業の IT ショップ、特にクラウドと対話する企業の IT ショップで、鍵のローテーションを定期的に行うことを推奨しています。現在では、PCI-DSS など、定期的なローテーションを要求する標準があります。PPM で鍵をローテーションすると、タイムスタンプが付いたデータ・レコードが作成されます。このレコードは、コンプライアンス準拠を証明するために、監査目的でログに記録されます。

Q: 鍵を取り消す必要があるのはなぜですか?

A: Policy Provisioning Manager (PPM) で鍵を取り消すと、保護データへのアクセスが一時的に無効になります。通常、鍵を取り消すのは、データ保護に問題が発生

したときや、保護データへのアクセスを拒否する必要があるときです。後で同じ鍵を再配布すると、データに再度アクセスできるようになります。

Q: 鍵を廃棄する必要があるのはなぜですか?

A: 鍵を廃棄すると、保護データへのアクセスが完全に無効になります。このオプションは、データが不要にならない限り、選択しないでください。

Q: IBM Multi-Cloud Data Encryption では、鍵が自動的に管理されますか?

A: セキュリティー管理者が暗号鍵を手動で管理したくない場合は、Policy Provisioning Manager (PPM) が、ポリシーが新規作成されるたびに鍵を自動生成できます。自動生成された鍵は、作成時に常に固有であり、鍵管理ページには表示されません。

インストールとセットアップに関する FAQ

Q: IBM Multi-Cloud Data Encryption (MDE) は、エンド・ユーザー (管理者以外のユーザー) にどのような影響を与えますか?

A:管理者以外のユーザーは、通常運用時との違いに気付くことなく、IBM Multi-Cloud Data Encryption (MDE) のセキュリティーと高可用性の恩恵を享受できます。管理対象 (保護対象) ディレクトリー内のファイルにアクセスする場合でも、通常どおり、ファイルに対してアクセス、書き込み、保管を行うことができます。

Q: MDE エージェントを Docker ホストにインストールして、Docker コンテナーのアプリケーションからのすべての読み取り/書き込み要求を処理できますか?

A: はい。ファイル/ポリシー・エージェントとボリューム・エージェントの両方を使用して、データを保護できます。

- ファイル/ポリシー・エージェントを使用して、コンテナーが使用するアプリケーション・データが保護されるようにするために、Docker ボリューム・パスを保護できます。
- ボリューム・エージェントを使用して、Docker コンテナー・パスを保護できます。これは、コンテナー全体とそのすべての入出力を効率よく暗号化します。Docker ボリュームが Docker コンテナー・パスの外部に格納される場合、外部の Docker ボリュームを保護するために追加のボリュームを構成できます。
- Docker ホストで重要な点は、Red Hat 7.2 以降でサポートされているカーネル (3.10-*) が実行されている必要があることです。

構成に関する FAQ

Q: IBM Multi-Cloud Data Encryption (MDE) で HTML ファイルを暗号化できますか?

A:現時点では、HTML ファイルの保護は推奨されません。Web サイトに表示されるアクティブ HTML ファイルは、暗号化すると正しく表示されない場合があります。

操作に関する FAQ

Q: IBM Multi-Cloud Data Encryption (MDE) でデータが保護されていることを知るには、どのようにすればよいですか?

A:MDE による保護は、サービスが停止している場合でも、保護ファイルへのアクセスがあった場合でもアクティブです。

Q: 実稼働環境に実装された IBM Multi-Cloud Data Encryption (MDE) を変更するときは、事前にどのような準備が必要ですか?

A:軽微な変更は、システム稼働中に「spxconfig」コマンド・ラインまたは GUI から行うことができます。ただし、重大な変更を行う場合は、綿密な準備と推奨バックアップが必要になります (変更を行う前に、すべての製品資料を参照して製品エコシステムを確認してください)。

Q: IBM Multi-Cloud Data Encryption (MDE) のイベントを他の SIEM (Security Information and Event Management) 相関アプリケーションに転送できますか?

A: はい。本製品には、イベント集約および転送システムが組み込まれています。このシステムは、内部的に生成されたイベントと共に管理対象エージェントのイベントを集約して、内部イベント・ログに保管します。このログは、管理者ダッシュボードで表示でき、イベントを 1 つ以上の受信者に転送するように構成できます。

Q: 大/小文字の区別 (大文字化) は重要ですか?

A: はい。大/小文字の区別は大変重要です。

- セレクターを作成するとき、「ユーザー」フィールドと「グループ」フィールドには大/小文字の区別はありません。
- Windows を使用してパス・セットを作成するとき、ドライブ名は大文字にする必要があり、ディレクトリー名は大/小文字が区別されます。
- ボリュームまたはポリシー付きボリューム・エージェントを作成するとき、ボリューム・ラベルは大/小文字が区別されます。
- 値やフィールドについては、大/小文字の区別を常に想定する必要があります。

Q: 操作の順序とは何ですか？ なぜ重要なのですか?

A: これが重要なのは、エージェントの作成とデプロイを正常に実行するためには特定の順序が必要であるためです。

- ファイル・エージェントをデプロイするには、ターゲット・ボリュームをオンラインにし、初期化し、作成したディレクトリーと適切な許可を使用してフォーマットする必要があります。
- ボリューム・エージェントをデプロイするには、ボリュームが存在し、オンラインであり、初期化されているが、フォーマットはされていない必要があります。
- ポリシー付きボリューム・エージェントをデプロイするには、ボリュームが存在し、オンラインであり、初期化されているが、フォーマットはされていない必要があります。定義されているセレクターが、ターゲット・マシンのローカルまたは LDAP / AD 階層に存在する必要があります。

Q: スナップショットのアクティブ化ジョブを実行して、まだ実行中です。いつ完了しますか?

A: スナップショットの変更や更新は、エージェントが PPM サーバーと通信できるようになるまで反映されません。作成されたジョブは、PPM とエージェントとの間の通信が成功するか、エージェントが PPM サーバーから削除されるまで実行中のままになります。

高可用性に関する FAQ

Q: IBM Multi-Cloud Data Encryption (MDE) デプロイメントの高可用性が必要になるのは、どのようなときですか?

A: 高可用性 (HA) MDE デプロイメントは、データ・アクセスおよび保護管理サービスに対して 100% に近い可用性が必要な IT 環境で使用する必要があります。PPM インスタンスで保守が必要になるか、障害が発生するか、誤ってオフラインになった場合は、ホット・バックアップ・インスタンスに即時に切り替わり、操作が再開されます。

Q: 高可用性 (HA) IBM Multi-Cloud Data Encryption デプロイメントでは、ロード・バランサーは必要ですか?

A: はい。2 つのロード・バランサー (ロード・バランサー・クラスター) をエージェントと PPM サーバーとの間に配置する必要があります。2 つ以上の PPM サーバーがデプロイされている場所では、それぞれロード・バランサー・クラスターが必要です。これらのロード・バランサーは、ローカル・サブネット上で相互に通信し、仮想 IP アドレス (別名: 浮動 IP アドレス) を提供します。このアドレスは、エージェントおよび管理者が PPM サーバーにアクセスする際に使用されます。PPM HA には、単一の場所、複数のデータセンターなど、多くのシナリオがあり、それぞれに独自のデプロイメント・オプションおよび構成があります。

マルチテナンシーに関する FAQ

Q: マルチテナンシー機能には、どのような目的がありますか?

A: PPM のマルチテナンシー機能を使用すると、IT プロバイダーは、PPM の制御を顧客別に区分化できます。従って、それぞれの顧客は IT 環境内で PPM ログイン、管理者、ポリシー、ダッシュボード、ジョブ、イベントなどを分離された形で独自に所有できます。顧客はストレージだけではなくディレクトリーも共有する可能性がありますが、各顧客の保護ファイルおよび保護ボリュームは個々に暗号化され、互いから保護されます。これにより、複数のテナントや顧客が同じストレージ・スペースを安全に共有して活用できる同時に、各テナントのデータは分離され、他のテナントや顧客が見ることはありません。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

この資料の他の言語版を IBM から入手できる場合があります。ただし、これを入手するには、本製品または当該言語版製品を所有している必要がある場合があります。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。

国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

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

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。 IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

(C) (お客様の会社名) (年).このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用可能性

このご使用条件は、IBM Web サイトのすべてのご利用条件に追加して適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権利　ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項をご確認ください。この「ソフトウェア・オファリング」は、Cookie もしくはその他のテクノロジーを使用して個人情報を収集することはありません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

プログラム番号: 5737-C67

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21