IBM Multi-Cloud Data Encryption Powered by SPx®

バージョン 2.2

管理者ガイド

IBM

IBM Multi-Cloud Data Encryption Powered by SPx®

バージョン 2.2

管理者ガイド

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、 111 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。

本書は、IBM Multi-Cloud Data Encryption (プロダクト番号 5737-C67) バージョン 2.2、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

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
Administrator Guide

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

概要

使用許諾権

本ソフトウェアの使用は、ご使用条件の条項に制限されています。

POC

IBM Multi-Cloud Data Encryption (MDE) に関する追加情報については、IBM サポート Web サイト (https://www.ibm.com/support/home/) を参照してください。

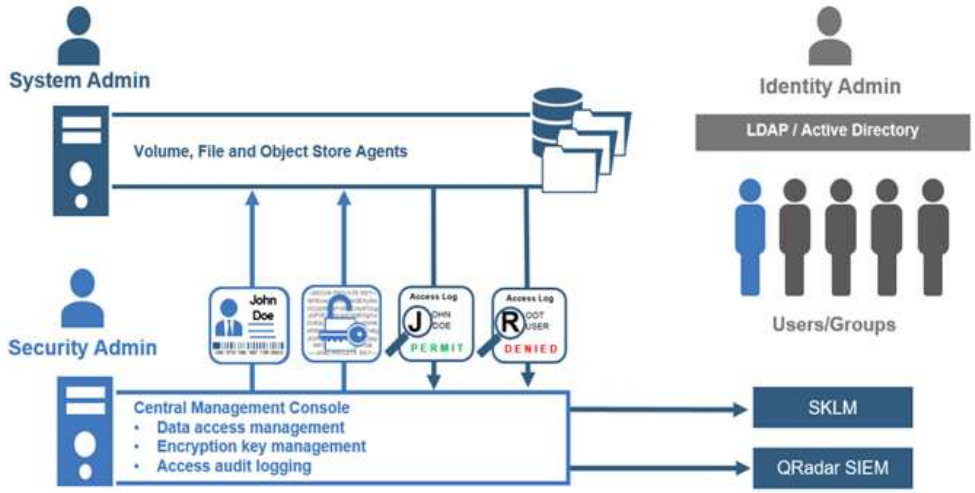
本管理者ガイドの背景と目的

本管理者ガイドは、デプロイされたエージェントを使用する選択されたサーバーで、暗号化エージェントのプロビジョニングと管理、ポリシーの定義 (アクセスと暗号の制御)、ポリシー実施鍵の管理、および保存データのセキュリティー保護のために MDE をインストール、管理、および使用するための主要解説書です。本書は、製品をインストールおよび管理するための管理アクセス権と企業ネットワークの知識を備えた、システム管理者を対象にしています。

一般概要

システム概要

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 箇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。

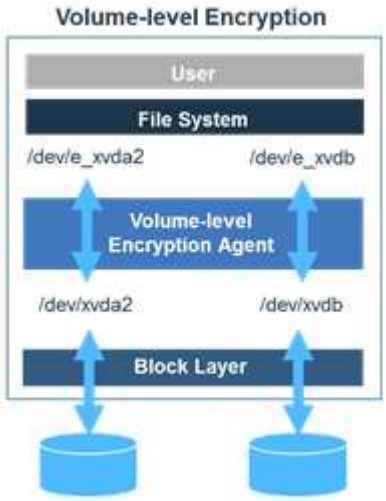


MDE は、製品管理者とセキュリティー管理者という別々の管理者ロールによる職務分離を提供します。製品管理者ロールには、MDE 製品の構成と保守に必要となる権限が付与されます。セキュリティー管理者ロールには、エージェントのプロビジョニングと管理に必要となる権限が付与されます。これらのロールについては、セクション 7「MDE 管理ユーザーの管理」で詳しく説明します。

MDE は 4 つのエージェント・タイプのインストールをサポートしていて、これらによって、ポリシー定義を適用するために使用する暗号データ保護を提供します。

エージェントのタイプ

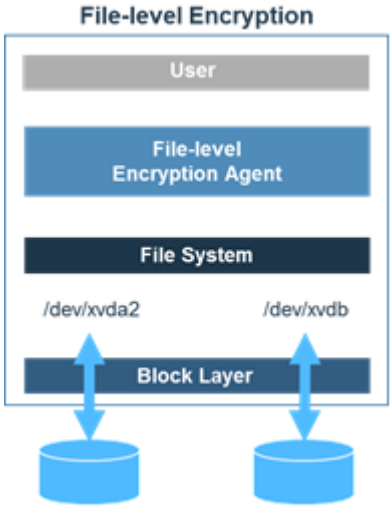
ボリューム・エージェント (Volume Agent)



ボリューム・エージェントは、アクセス・ポリシー制御が制限されたボリューム・レベルの暗号化を提供します。ボリューム・レベルの暗号化は、OS へのブロック・ドライバーの実装により、保護される事前定義のストレージ・デバイスの形態でセキュリティーを提供します。

ボリューム全体が 1 つの単位として定義されて暗号化によって保護されます。データが追加、編集、または削除されると、ボリューム・エージェントは、ボリューム内のすべてのデータが PPM 管理暗号鍵で暗号的に保護されるようにします。

ファイル/ポリシー・エージェント



ファイル/ポリシー・エージェントは、ファイル・レベルの暗号化をデータ・アクセス・ポリシーと組み合わせます。ファイル・レベルの暗号化によって、ファイル・システム・レベルで個別のファイル保護を提供します。ファイルおよびストレージ

環境のサイズは、ファイル・システムによってのみ制限されます。ファイル/ポリシー・エージェントによって制限されることはありません。保護データの場所は、そのパス定義に対応したワークグループ鍵によって保護され、その場所内およびその場所の下に保存されている個別のファイルはすべて、固有で予測できない初期設定ベクトル (IV) を使用して個別に暗号化されます。

固有のファイル・レベルの鍵は、内部の鍵管理システムによって処理されます。ポリシー・ベースのアクセス制御は暗号化の上に階層化されるため、最小特権のアクセス制御の定義、アクセス・ロギングの指定、および特定のシステム機能に対するアクセス権 (読み取り、読み取り/書き込み、コピー、削除など) の制限が可能です。これらのポリシー制御が、標準の LDAP や Active Directory の権限と連携して機能します。ユーザーが LDAP または Active Directory 内のデータに対する権限を持っていない場合、セキュリティー管理者がこれらのアクセス制御を上書きしてデータ・アクセスを許可することはできません。

デフォルトでは、すべてのユーザーが、ポリシーの対象となっているデータへのアクセスから除外されます。どのユーザーがアクセス権を持つかを、セキュリティー管理者が定義する必要があります。これにより、セキュリティー管理者は、システム管理者、クラウド・ベンダー管理者、および root ユーザーによる、保護データへのアクセスを制限できます。

ボリューム/ポリシー・エージェント

ボリューム/ポリシー・エージェントは、ボリューム・エージェントのボリューム・レベルの暗号化と、1 つ以上の保護対象ファイル・パスに適用および実施できるファイル・ベース操作のアクセス制御ポリシーを利用します。

オブジェクト・ストア・エージェント

オブジェクト・ストア・エージェントの動作は、「M of N」モデルを基盤としています。このモデルは、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。保管されるデータの断片 (保管場所はライセンスに応じてローカルの場合とリモートの場合がある) は「共有」と呼ばれます。複数の共有を使用することで、データ・フローが改善されるとともに、データ回復やフォールト・トレランスのために選択できる方法が増えます。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。

オブジェクト・ストア・エージェント (OSA) は、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ます。このエージェントは、ファイルがオブジェクト・ストレージに送信される際にパススルーとして機能し、途中でデータを暗号化して分割します。オブジェクト・ストレージからオブジェクト・ストア・エージェントを通じて取得されるファイルは、取得時に暗号化解除されます。オブジェクト・ストレージに保管されたファイルは暗号化されています。オブジェクト・ストア・エージェントを通じてデータを送受信できるのは、許可されたユーザーだけです。

エージェント機能のマトリックス

エージェント機能	ボリューム・エージェント (Volume Agent)	ボリューム/ポリシー・エージェント	ファイル/ポリシー・エージェント	オブジェクト・ストア・エージェント
ボリューム全体の暗号化	X	X		
指定された保護対象ディレクトリー内のファイルの個別暗号化			X	
ファイル・レベルのポリシー		X	X	
ファイル・アクセスの監査ログ		X	X	
ユーザー・データに対する管理者アクセスからの保護			X	
オブジェクト・ストレージ内のデータの暗号化				X

計画に関する考慮事項

前提条件

IBM Multi-Cloud Data Encryption (MDE) のインストールは簡単なプロセスであり、ベース Open Virtual Appliance (OVA) のインストールと、ポリシーのプロビジョニングおよび管理 (PPM) インストーラーの実行が含まれます。

準備では、ソフトウェアのインストール前にインストール手順を全体を通して確認することをお勧めします。以下に、IBM Multi-Cloud Data Encryption のインストールと運用を成功させるための前提条件のリストを示します。

1. ライセンス交付を受けたオペレーティング・システムおよびサポートされるハイパーバイザー (VMware ESXi™) がインストールされた、PPM をデプロイおよび実行するための運用サーバー
2. パッケージ化されたベース OVA
3. PPM インストーラー
4. サポートされるエージェント・オペレーティング・システム (Red Hat®/CentOS 6.2 以降または 7.2 以降、Microsoft Windows Server® 2008 R2、Microsoft Windows Server® 2012 R2、または Microsoft Windows Server® 2016) がインストールされた 1 つ以上のターゲット・サーバー
5. ブラウザー: Google Chrome®、Internet Explorer® 10 以降、Microsoft® Edge、Firefox® ESR 52 以降
6. PPM とすべてのエージェント間のネットワーク・アクセス
7. 管理サーバー (PPM) およびすべてのエージェントの間でセキュア・セッションを確立するための認証局署名済み証明書 (鍵ストア、トラストストア、および CA 証明書バンドル) (詳しくは、『証明書に関する要件』と『サーバー証明書の設定』を、例については、『付録 *B*』を参照)。

オブジェクト・ストア・エージェント (OSA) の場合、追加の要件は次のとおりです。

- S3 互換オブジェクト・ストレージ: アマゾン ウェブ サービス S3 (AWS S3)、IBM Cloud Object Storage (COS S3)
- オブジェクト・ストレージ資格情報: ユーザー ID と秘密鍵 (パスワード)
- AWS S3 REST API ライブラリーまたは Boto Python ライブラリーを使用して OSA エージェントに対するデータを指すアプリケーションまたはユーティリティー

重要な注記

MDE、外部データベース、およびエージェントで NTP を利用してシステム時刻を調整することを強くお勧めします。これにより、イベント/監査ログのタイム・スタンプが適切に順序付けられます。

最小システム要件

PPM VM の最小システム要件

- CPU 4
- 8 GB RAM
- 40 GB の使用可能なストレージ
- ネットワーク・アクセスが必要

エージェントの最小システム要件

- AES-NI が有効な 1 コア 64 ビット CPU (2 GHz)
  - (AES-NI が有効な 2 コア 64ビット CPU (2 GHz) を推奨)
  - 2 GB RAM (4 GB RAM を推奨)
- 20 GB の使用可能なハード・ディスク・スペース
  - ログ・ファイル・スペース用に 300 MB 以上を推奨
- ネットワーク・アクセスが必要
- 以下のパッケージが Red Hat / CentOS 上でインストール/更新されていること: curl、openssl、および nss
- 初期エージェント・インストール時のインターネット・アクセスまたはローカル・リポジトリーへのアクセス
- エージェントには SSL 証明書が必要

注記

エージェントの作成前に、**SSL (**自己署名または認証局**)** 証明書/鍵ペア・ファイルが必要です。この証明書は、エージェントと **MDE** サーバー間にセキュアな **TLS** 接続を確立するために使用されます。

証明書に関する要件

PPM サーバーとすべてのエージェントの間にセキュア接続を確立するために必要となる証明書は、以下の条件を満たしている必要があります。

- PPM サーバーでは、エージェントによって提示される証明書が、そのエージェント (DNS ホスト名または IP アドレス) に解決される必要があります。
- PPM サーバーでは、エージェントによって提示される証明書に、「クライアント認証 (Client Authentication)」拡張鍵用途が設定されている必要があります。
- エージェントでは、PPM サーバーによって提示される証明書が、その PPM サーバー (DNS ホスト名または IP アドレス) に解決される必要があります。
- エージェントでは、PPM サーバーによって提示される証明書に、「サーバー認証 (Server Authentication)」拡張鍵用途が設定されている必要があります。

証明書の有効期限が超過しないようにするために、PPM とエージェントは、信頼できる時間ソースに同期されている必要があります。

デプロイされたエージェントごとに固有の証明書が必要です。

エージェントのファイル・システム・サポート

ボリューム・エージェントは、ボリューム・レベルで暗号化を実行します。ファイル/ポリシー・エージェントは、ホスト・オペレーティング・システムのサポートされるファイル・システムとともに作動するか、サポートされるファイル・システム上で作動します。ファイル/ポリシー・エージェントおよびボリューム/ポリシー・エージェントは、以下のファイル・システムをサポートします。

Linux サーバー

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

Windows Server

- NTFS
- ReFS (Windows Server 2012 R2 以降)

ネットワークのセットアップ

このタスクについて

MDE では、MDE PPM サーバーとエージェント間に一貫性のあるネットワーク接続が必要です。インターネット・プロトコル IPv4 および IPv6 がサポートされています。静的 IP 割り当てまたは静的リースの DHCP を使用すると、この要求が満たされます。また、適切に動作する DNS インフラストラクチャーを使用し、エコシステム全体でホスト名を使用することも有効です。

ネットワーク・ポート

機能	デフォルト・ポート	構成可否
Web	443	はい
データベース	5432	はい
外部 LDAP	なし	はい
LDAP ディレクトリー	なし	はい
E メール・イベント転送	なし	はい
Syslog イベント転送	なし	はい

OVA の構成

提供される MDE OVA は事前構成されており、MaxAuthTries が 1 に設定されています。SSH を介して MDE VM に対して認証を成功させるためには、MaxAuthTries を変更するか (推奨されません)、コマンド・ラインまたはローカル SSH クライアント構成を使用して SSH クライアントで PubkeyAuthentication を「no」に設定する必要があります。

REST インターフェース

MDE は、完全なプログラマチック REST インターフェースをサポートしています。ルート REST URL は、次のとおりです。

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

重要な注記

> REST API を使用すると、管理者は、Web インターフェースではアクセスできない高度な機能を実行できます。エージェントがサポートされない状態になるような方法で REST API が使用される可能性があります。そのため、REST API プログラミングの知識を把握している必要があります。

詳しくは、IBM Multi-Cloud Data Encryption (MDE) の REST API 仕様の資料を参照してください。

製品のインストール

インストールの準備

MDE のインストール・プロセスには、次の 3 つのステップがあります。

1. 前提条件
2. 使用可能な MDE ベース Open Virtual Appliance (OVA)
3. サポートされるハイパーバイザー (VMware ESXi™)

ライセンス登録

MDE では、ソフトウェアご使用条件で指定されたもの以外のエージェントの実行または構成のための固有の製品ライセンスは必要ありません。

MDE のインストール

このタスクについて

MDE ソフトウェアをインストールするには、以下の手順を実行します。

サンプルのファイル ibm_sw_mde_X.x.x-XX.bin を使用して、XX を使用可能なソフトウェアのバージョンのビルド番号に置き換え、root ユーザーとして操作します。

手順

1. MDE ベース OVA をハイパーバイザーにデプロイします。この例では、これを「MDE VM」と呼びます。
2. 管理者としてログインし、新規パスワードを設定します。

   MDE VM では、管理者による構成が可能な PAM 標準基準が使用されます。PAM パスワードには 8 文字を超える文字列を指定する必要があり、以前のパスワードと同じ文字を 5 文字以上含めることができません。
3. MDE VM の IP アドレスをメモします。
4. SCP または類似のファイル転送方式を使用して ibm_sw_mde_X.x.x-XX.bin を MDE にアップロードします。
5. bin ファイルを実行可能にします。

   ```
   [admin@localhost]$ chmod +x ./ibm_sw_mde_X.x.x-XX.bin
   ```
6. bin ファイルを実行します。

   ```
   [admin@localhost]$ ./ibm_sw_mde_X.x.x-XX.bin
   ```
7. 「English」を選択して Enter キーを押します。
8. ライセンス・ページを読んで <OK> にタブ移動し、Enter キーを押して先に進みます。

9. <Yes> を選択し、Enter キーを押してご使用条件に同意します。
10. 抽出が完了したら、<OK> で Enter キーを押してコマンド・ラインに戻ります。
11. RPM を root としてインストールします。

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

12. MDE はこれでインストールされましたが、まだ構成されていません。

    注: 構成が完了するまで MDE VM をリブートしないでください。

言語のセットアップ

このタスクについて

MDE は、VM スクリプトと PPM GUI 用に複数の言語をサポートします。この製品を実行する前に、デフォルトの言語設定を構成する必要があります。

注: 言語は、RPM によって MDE VM にインストールされます。インストーラー・バイナリーには、複数の言語 RPM が組み込まれています。他の言語は初期インストールの後に追加でき、追加した言語を有効にするために PPM サービスの再始動が必要になる場合があります。

デフォルト言語を構成するには、以下のステップに従ってください。

手順

1. spsd-langsetup スクリプトを実行します。

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

2. 現在のデフォルトの言語コードを確認します。何も設定されていない場合は、ブランクになっています。

   ```
   デフォルトの言語コードを設定します。
   現在のデフォルト:
   ```

3. 使用可能な言語コードのリストを確認します。(以下のリストは、ご使用のバージョンの製品で使用できないサンプルを示している場合があります。)

   ```
   使用可能な言語コード:
   en_US
   ja_JP
   ko_KR
   ```

4. 新しいデフォルトの言語コードを入力してください。

   ```
   新しいデフォルトの言語コード en_US を入力します。
   デフォルトの言語コードが en_US になります。
   ```

5. spsd-langsetup スクリプトを再実行して、デフォルトの言語コードが設定されていることを確認します。

   ```
   デフォルトの言語コードを設定します。
   現在のデフォルトは en_US です。
   ```

データベースのセットアップ

このタスクについて

MDE は内部データベース構成も外部データベース構成もサポートします。いずれの場合も、MDE を初めて開始する前に、構成されたデータベースと通信するように MDE を構成する必要があります。

データベースを MDE に関連付けるには、MDE VM の /etc/securityfirst/atlantis/props.d/db.props ファイルを変更する必要があります。このファイルは、root ユーザーとして編集する必要があります。

注**:** spsd-pgsetup スクリプトを実行すると、プロンプトに入力された値によって db.props ファイルが自動的に変更されます。

後述の説明に従って、適切な内部データベースまたは外部データベースに接続するようにファイル・プロパティーを構成します。MDE を再始動するまで、データベース・プロパティーの変更は有効になりません。

重要な注記

db.props を変更するときに、次の制約に従ってください。

- プロパティー名と = の間にスペースを配置できません。
- = とプロパティー値の間にスペースを配置できません。

内部データベース

現在、MDE は、内部データベースとして PostgreSQL をサポートしています。

内部 **Postgres** データベース

MDE OVA には、PostgreSQL ソフトウェアがインストール済みの状態でプリパッケージされています。MDE で機能するようにこのデータベースを構成するには、以下の手順に従ってください。

1. 「--local」スクリプト・オプションを指定して spsd-pgsetup スクリプトを実行します。

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

注**:** この「--local」オプションにより、内部の「ローカル」 PostgreSQL サーバーに新しい空のデータベースが構成されます。

これらの設定を適用したら、『サーバー証明書の設定』に進みます。リモート・ターゲットにデータベースをセットアップしようとしている場合は、『外部データベース』に進みます。

外部データベース

現在、サポートされている外部データベース・サーバーは PostgreSQL のみです。このプロセスを実行する前に、必ず以下の情報を確認しておいてください。

- アクセス可能な PostgreSQL データベース・サーバーの名前 (または IP アドレス)
- 上記の PostgreSQL サーバーが listen しているポート番号
- 上記サーバー上の既存のデータベースの名前
- 上記データベースの所有者として定義されている既存ユーザーの名前
- 上記のデータベース・ユーザーのパスワード

MDE で機能するようにこのデータベースを構成するには、spsd-pgsetup スクリプトを実行します。以下の例は、このコマンドで指定されるすべての値を示しています。

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

データベースを最新のスキーマにアップグレードするには、「-upgrade」スクリプト・オプションを指定して spsd-pgsetup スクリプトを実行します。

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

注: 「upgrade」オプションを指定して spsd-pgsetup スクリプトを実行すると、PPM の現行バージョンに合わせてデータベース表が適切に構成されます。

これらの設定を構成したら、『サーバー証明書の設定』に進みます。

サーバー証明書の設定

鍵ストア、トラストストア、および認証局

証明書は、管理サーバー (PPM) とエージェントおよび Web ブラウザーとの間でセキュア通信セッションを確立するために使用します。PPM は、すべての証明書が認証局 (CA) によって署名されていることを必要とします。CA によって、通信セッションのすべての参加者が相手方の身元を確認するために使用する信頼のルートが確立されます。

- CA 署名済み証明書とその対応する鍵の組み合わせが、Java 鍵ストアに格納されます。
- エージェント証明書の署名に使用された CA からの証明書 (または証明書バンドル) が、PPM トラストストアに追加されている必要があります。
- 3 つの構成要素 (鍵ストア、トラストストア、およびCA 証明書バンドル) すべてが、下の PPM 証明書のセットアップ・プロセスで使用されます。

認証局証明書プロセスのサンプルについては、『付録 *B*』を参照してください。

サーバーの Web 証明書鍵ストアおよび Web 証明書トラストストアは、以下を使用して構成されます。

MDE VM の /opt/securityfirst/spsd/bin ディレクトリーにあるセットアップ・スクリプトの spsd-certsetup。

鍵ストアとトラストストアとエージェントCA バンドルを構成するための入力例 (太字):

$ 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

注記

鍵ストア、トラストストア、CA バンドルなどのサーバー証明書構成要素は提供されないため、セットアップ・スクリプトを使用して生成し、MDE VM にアップロードする必要があります。Common Access Card (CAC) を認証に使用する場合は、PKI 設定を有効にする必要があります。

公開鍵基盤 (PKI) の設定

このタスクについて

PKI 構成を使用すると、PPM で 2 次的な PPM ユーザー認証方式が提供されます。これを構成すると、PPM は Web セッションおよび REST セッションの認証方式としてクライアント証明書を受け入れます。

この証明書は、PPM によって信頼された CA によって署名されている必要があります。PPM は、spsd-certsetup スクリプトに定義されたルールに基づいてこの証明書を検証します。

太字で示された入力例:

$ 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.Y

注記

PKI は、鍵ストア、トラストストア、および CA バンドルと同じスクリプトを実行して構成できます。説明用の値を示すためにここに抜粋しています。

MDE のインストール、データベースの構成、証明書の追加、およびオプションでの PKI のセットアップが済んだら、MDE VM をリブートできます。

開始と初回ログイン

このタスクについて

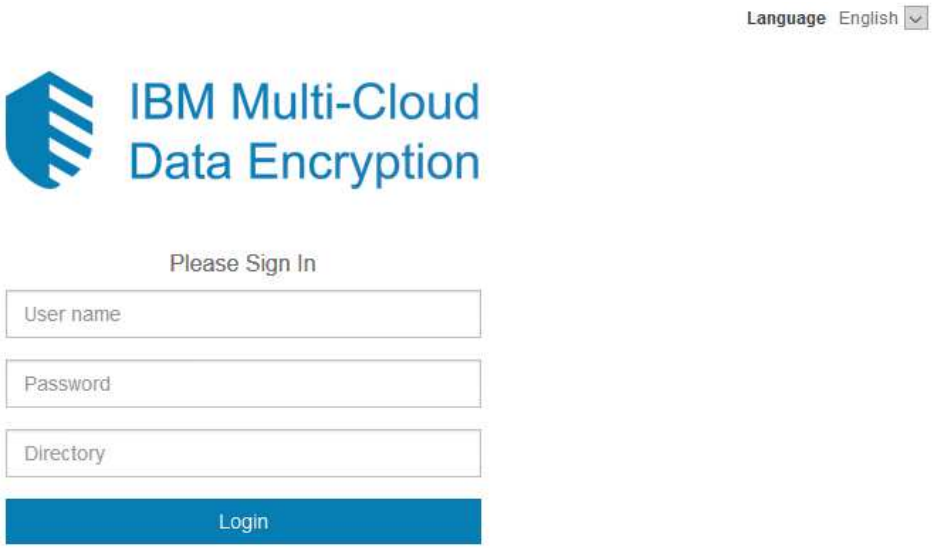
デプロイメントと構成が完了したら、MDE サーバーをリブートするか、単に MDE コンソールからサービス「spsd」を開始して Web GUI を開始します。仮想マシ

ン・コンソールまたはホスト・ハイパーバイザーを通じて、仮想マシンの IP アドレスまたはホスト名を取得する必要があります。

サポートされる Web ブラウザーを開き、IP アドレスまたはホスト名を URL として入力し、MDE ログイン・ページにアクセスします。

```
https://<MDE Server IP>
```

この時点で、使用可能なサポート言語のリストから言語設定を変更できます。



デフォルトの資格情報は次のとおりです。

ユーザー名: admin
パスワード: admin

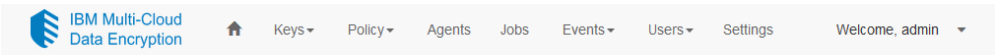
注記

- 初回ログイン後に、デフォルトの資格情報を変更する必要があります。
- MDE は Firefox、Chrome、Microsoft Edge、および Internet Explorer の各 Web ブラウザーの大部分のバージョンをサポートしています。
- PKI クライアント認証を使用すると、ログイン・ページがバイパスされ、ダッシュボードに直接移動する場合があります。

MDE のグラフィカル・ユーザー・インターフェース (GUI)

基本的な製品ナビゲーション

MDE はページ上部のナビゲーション・メニューを備えています。一部のメニュー項目にはサブメニュー・リストがあります。各メニュー項目をクリックすると、該当するページにナビゲートするか、サブメニュー・リストが表示されます。



- ホーム・アイコン - 製品「ダッシュボード」ホーム・ページへのリンク。
- 「鍵」 – 鍵関連のサブメニュー・ページ・リンク「外部鍵ストア (External Keystores)」および「管理対象鍵」が含まれたメニュー。
- 「ポリシー」 - ポリシー関連のサブメニュー・ページ・リンク「データ・タイプ」、「パス・セット」、「プロセス」、および「セレクター」が含まれたメニュー。
- 「エージェント」 – 「エージェント」ページへのリンク。
- 「ジョブ」 – 「ジョブ」ページへのリンク。
- 「イベント」 – イベント関連のサブメニュー・ページ・リンク「転送」および「ログ」が含まれたメニュー。
- 「ユーザー」 – ユーザー関連のサブメニュー・ページ・リンク「アカウント」および「LDAP ディレクトリー」が含まれたメニュー。
- 「設定」 – 「設定」ページへのリンク。

注記

MDE はロール・ベースのアクセス制御 (RBAC) をサポートしており、一部のナビゲーション項目は、ログイン・ユーザーのロールに基づいて使用できなくなります。そのため、一部のナビゲーション項目を使用できない管理ユーザーが存在する場合があります。

テキスト・ボックスのオートコンプリート

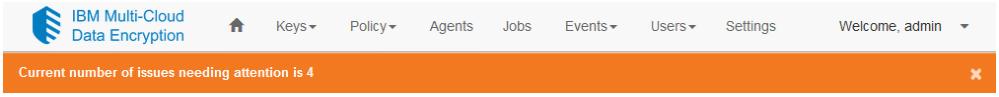
ユーザー・インターフェースのさまざまな場所で、テキスト入力フィールドが表示されます。一部のテキスト入力フィールドには、入力文字のオートコンプリートに基づいて一致基準が表示されます。オートコンプリートの推奨リストを表示するには、これらのフィールドに複数の文字が必要になる場合があります。

製品ダッシュボード

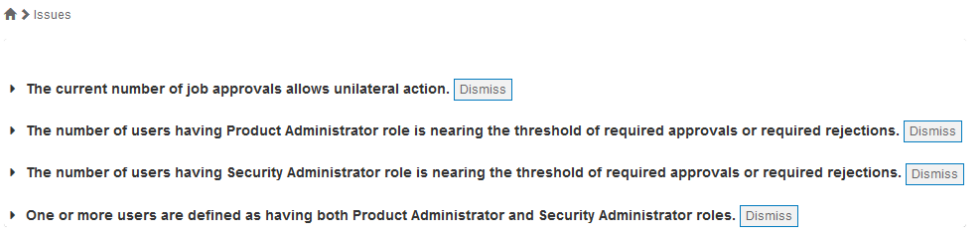
製品ホーム・ページは、メインのランディング・ダッシュボード・ページです。ログインしている管理者に対して、最近のイベントの現在の状況についてのサマリー・ビューを表示することを目的としています。ホーム・ページには、最近のイベント、イベントの傾向、およびその他のサマリー・データが表示されます。

重要通知

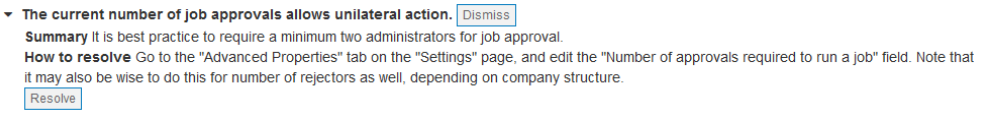
初回ログイン時に、ユーザー・インターフェースの上部に、解決する必要のあるアクションを示すカラー・バナーが表示されます。



バナー内のテキストをクリックすると、管理者は、個々の項目が表示される「問題」ページにリダイレクトされます。



個々の項目を展開すると、その問題を解決する方法の詳細が表示されます。



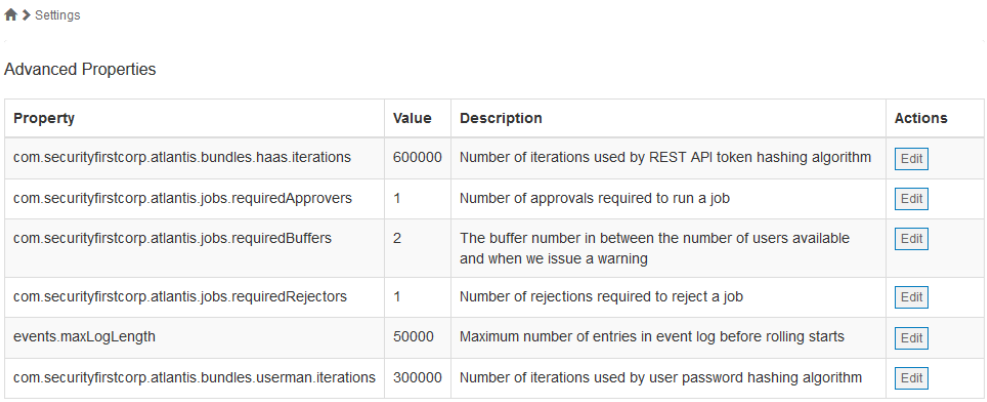
未解決の問題がすべて解決されると、バナーは表示されなくなりますが、管理者は現行ページのバナーを非表示にするように選択できます。

注記

新しい「要対処」問題が作成される新たな状況が生じると、バナーが再表示されます。

拡張プロパティー

製品管理者は、製品の動作を定義する拡張プロパティーを構成できます。拡張プロパティーには、設定ページを使用してアクセスできます。これらのプロパティーの範囲は、ローカルのインスタンスに設定されるか、高可用性 (HA) またはマルチテナント機能を使用する場合は MDE エコシステムに設定されることがあります。

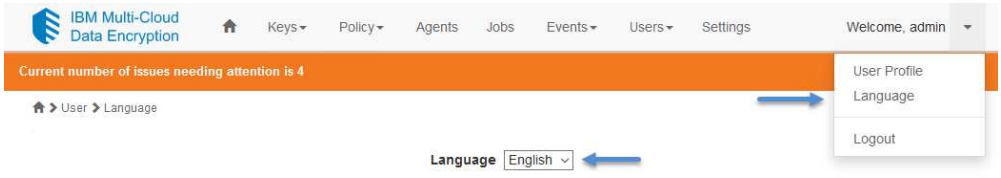


プロパティーを編集するには、製品管理者は「編集」ボタンをクリックします。適切な変更を行ったら、「保存」ボタンをクリックすると、ジョブが作成されます。

GUI 言語設定

初期インストール時にログイン・ページまたはホーム・ページから言語を選択するときに、GUI からインストール済みのサポート対象言語のいずれかに変更できます。

- ログイン・ページ - ページの右上にあります。プルダウン・メニューをクリックして、サポート対象言語のリストを表示します。
- ホーム・ページ - 右上のプルダウン・メニューにある「言語」を選択して、サポート対象言語のリストを表示します。

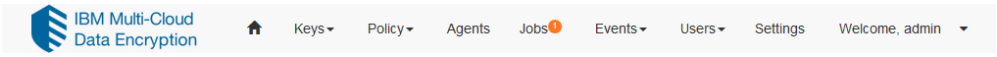


GUI に表示される言語は、以下の階層によって決まります (最初に出現する設定が使用されます)。

1. PPM のユーザー・インターフェースを介して設定された言語 Cookie の値。
2. ユーザーのブラウザーの言語設定の値。
3. PPM CLI script-langsetup を介して設定された言語コードの値。
4. 最初に検出されたインストールされている PPM 言語パック。

ジョブ

MDE には、実行タスクの承認とタイミングを管理するジョブ・システムが組み込まれています。多くの機能は、確認される前に、ジョブ・システムを使用して承認を待ちます。ジョブが作成されると、「ジョブ」ページのリストに新規ジョブが追加されます。



管理者は各ジョブを承認、拒否、または辞退できます。各管理者は、ジョブごとに 1 回のみアクションを実行できます。

ジョブの説明

ジョブ	説明	カテゴリー	役割
拡張プロパティー	拡張プロパティーを変更する	製品管理	製品管理者
鍵ストアの変更	ポリシー実施鍵ストアの場所/詳細を変更する	製品設定	製品管理者
鍵のローテーション	エージェント・エコシステム内で鍵のセットをローテーションする	鍵管理	セキュリティー管理者
鍵の取り消し	エージェント・エコシステムの鍵のセットを取り消す	鍵管理	セキュリティー管理者
鍵の廃棄	鍵のセットをエージェント・エコシステムから完全に削除する。これにより、データが失われる。	鍵管理	セキュリティー管理者
エージェントの追加	エコシステムに新規エージェントをプロビジョニングおよび追加する	エージェント管理	セキュリティー管理者
エージェントの削除	MDE 管理からエージェントを削除する	エージェント管理	セキュリティー管理者

エージェントの変更	エージェントに関連する情報を変更する	エージェント管理	セキュリティー管理者
ポリシーの更新	エージェントに関連付けられたポリシーを変更する	エージェント管理	セキュリティー管理者
新規管理ユーザーの作成	新規 MDE 管理者を作成する	MDE 管理ユーザーの管理	製品管理者
管理ユーザーの削除	MDE 管理者を削除する	MDE 管理ユーザーの管理	製品管理者
管理ユーザーのロールの追加	MDE 管理者にロールを追加する	MDE 管理ユーザーの管理	製品管理者
管理ユーザーのロールの削除	MDE 管理者からロールを削除する	MDE 管理ユーザーの管理	製品管理者
管理ユーザーのパスワードの変更	MDE 管理者のパスワードを変更する	MDE 管理ユーザーの管理	製品管理者
管理ユーザーの状況の変更	MDE 管理ユーザー・アカウントを有効または無効にする	MDE 管理ユーザーの管理	製品管理者
ディレクトリーの登録	MDE 管理ユーザーの LDAP サーバー・ディレクトリーを構成する	MDE 管理ユーザーの管理	製品管理者
ディレクトリーの削除	MDE から LDAP サーバー・ディレクトリーを削除する	MDE 管理ユーザーの管理	製品管理者
ディレクトリーの更新	LDAP サーバー・ディレクトリーを変更する	MDE 管理ユーザーの管理	製品管理者

複数管理者の承認

承認者と拒否者の必要数を MDE 内に構成できます。デフォルトでは、MDE は 1 人の管理者の承認に対応するように構成されます。ジョブ承認に複数の管理者が必要となるように設定することを強くお勧めします。複数管理者の承認により、1 人の管理者が MDE 自体での変更や管理対象エージェント・インスタンスへの変更を有効にするのを防ぎます。

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

重要な注記

管理者ユーザーの数は、「ジョブの必須の承認数」または「必須の拒否数」に対応する数以上にする必要があります。これらの値を変更する前に、必要な数の管理者ユーザーが存在することを確認してください。

承認および拒否のしきい値はジョブ・タイプによってオーバーライドできます。システム定義の各ジョブ・タイプ (「プロパティー変更 (Property Change)」ジョブを除く) には、「拡張プロパティー」に承認しきい値と拒否しきい値の両方があり、これらを設定すると、システム・デフォルトがオーバーライドされます。一度設定したプロパティーを設定解除することはできません。

「プロパティー変更 (Property Change)」ジョブは、「拡張プロパティー」の変更を制御するジョブであるため、承認および拒否のしきい値がない唯一のジョブ・タイプです。このジョブについては、承認および拒否のしきい値が、システム・デフォルトと、他のジョブ・タイプに定義された最も大きいオーバーライド値のうちの、より高いほうの値に設定されます。このアクションにより、プロパティー変更プロセスを通じて他のジョブ・タイプのしきい値が無効化されないようにすることができます。

ジョブの承認

ジョブを承認するには、適切な権限を持つ管理者が「ジョブ」ページにナビゲートし、該当するジョブを見つけて、「承認」ボタンをクリックする必要があります。必要な数の管理者承認に達すると、ジョブが実行されます。

ジョブの拒否

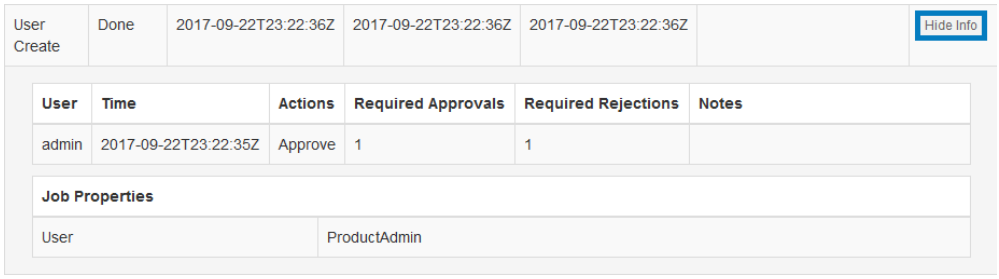
ジョブを拒否するには、適切な権限を持つ管理者が「ジョブ」ページにナビゲートし、該当するジョブを見つけて、「拒否」ボタンをクリックする必要があります。必要な数の管理者拒否に達すると、ジョブが永久にキャンセルされます。

ジョブの辞退

ジョブの辞退は、管理者がジョブを確認したが、そのジョブを承認または拒否したくないことを示します。辞退は、「監査」の見解と見なすのが最も適切である場合があり、管理者が将来に同じジョブで異なる見解を選択するのを防ぎます。

ジョブの情報

MDE 内の各ジョブには、そのジョブを説明するさまざまな情報が付属します。「情報の表示」ボタンをクリックすると、ジョブ固有の情報が表示されます。また、ジョブに対してさまざまな管理者が実行したアクション (承認、拒否、辞退) が、そのアクションを実行した管理者のユーザー名とともに表示されます。


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

MDE 管理ユーザーの管理

管理ユーザーのロール

MDE では、フラットで静的なロール・ベースのアクセス制御 (RBAC) 設計を利用しています。MDE 内の特定の機能には、特定の権限が必要です。 MDE のすべての権限セットが、製品管理者とセキュリティー管理者の 2 つの異なるロールにグループ化されます。各ロールの管理者をいつでも追加できます。

製品管理者ロール

製品管理者ロールには、MDE 製品の構成と保守に必要となる権限が付与されます。

セキュリティー管理者ロール

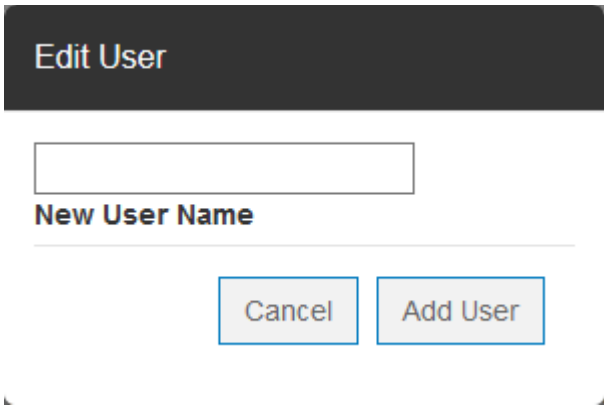
セキュリティー管理者ロールには、エージェントのプロビジョニングと管理に必要となる権限が付与されます。これらには、ポリシーの定義と指定、鍵の管理、データベースの定義、エージェントの管理、外部鍵ストアの構成、および外部ポリシー・グループの外部 LDAP の構成が含まれますが、これらに限定されません。

管理ユーザーの管理

製品管理者は、MDE 内で他の管理ユーザーを追加、変更、および削除するために必要となる権限を持ちます。

新規管理ユーザーの追加

新規管理ユーザーを追加するときに、製品管理者に対して、新規管理ユーザーの名前を入力するように求めるプロンプトが出されます。



固有のユーザー名を入力すると、ジョブが作成されてこの管理ユーザーが MDE に追加されます。ユーザーを作成するには、必要数の製品管理者がジョブを承認する必要があります。

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

新規に追加される管理ユーザーは、有効期限切れのパスワードで作成され、ロールは定義されていません。製品管理者は、パスワード、ロール、および状況を編集する必要があり、これによりジョブが生成されます。新規管理ユーザーが MDE でアクティブになるためには、ジョブが承認される必要があります。

ProductAdmin	Disabled	None		Never	Edit Password Edit Status Edit Roles Delete

管理ユーザーのパスワードの編集

管理ユーザーのパスワードを編集するには、該当するユーザーにナビゲートして「パスワードの編集」ボタンを選択します。パスワード入力ダイアログが表示されます。

指定されたルールに準拠しているパスワードを入力します。入力したら、変更を保存するとジョブが作成されます。

Type	State	Created	Started	Completed	Notes	Actions
User Password Change	waiting	2017-02-28T18:07:28.926Z			Edit Note	Approve Reject Abstain Show Info

パスワードの変更を有効にするには、必要数の管理ユーザーがジョブを承認する必要があります。

注記

ジョブが承認され、新規管理ユーザーとパスワードが追加されたら、新規に追加された管理者は初回ログイン時にパスワードを変更する必要があります。

管理ユーザーのロールの編集

管理ユーザーのロールを編集するには、ユーザー行を見つけて、「ロールの編集」ボタンを選択します。ロール入力チェック・ボックスがインラインで表示されます。

編集を実行する管理ユーザーは、製品管理者ロールとセキュリティー管理者ロールの両方を適用できる初期ユーザーである「組み込み管理ユーザー」など、その管理ユーザーが所有するロールと同じロールを適用できます。これにより、同じロールを与えられたユーザーは同じことができるようになります。

必要なロールを選択して「Save Changes」ボタンをクリックすると、ジョブが作成されます。

ロールの変更を有効にするには、必要数の管理者ユーザーがジョブを承認する必要があります。

管理ユーザーの状況の編集

管理ユーザーの状況を編集するには、該当するユーザーにナビゲートして「状況の編集」ボタンを選択します。状況入力ドロップダウンがインラインで表示されます。

状況値は、「enabled」、「disabled」、および「locked」です。

- 「**enabled**」 – 管理ユーザーはアクティブになっており、アクションを実行できます。
- 「**disabled**」 – 管理ユーザーは非アクティブになっており、アクションを実行できません。

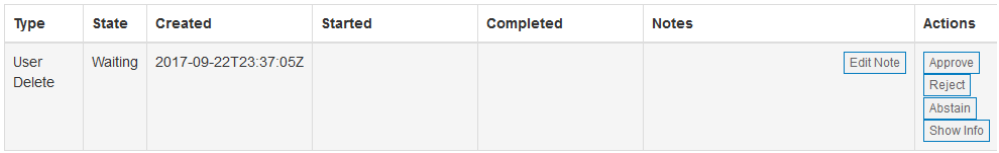
- 「**locked**」 – 管理ユーザーはロックされており、アクションを実行できません。

必要な状況を選択して「保存」をクリックすると、ユーザー状況を変更するためのジョブが作成されます。

状況の変更を有効にするには、必要数の管理ユーザーがジョブを承認する必要があります。

管理ユーザーの削除

管理ユーザーを削除するには、ターゲット・ユーザー行を見つけて、「削除」ボタンをクリックします。MDE からユーザーを削除するためのジョブが開始されます。このアクションは、製品管理者ロールを持つユーザーのみが実行できます。



ユーザーを削除するには、必要数の管理ユーザーがジョブを承認する必要があります。

重要な注記

- 管理ユーザーの削除は永久的なアクションです。
- 必要なジョブ承認数の条件を満たす、十分な管理ユーザーを維持する必要があります (『複数管理者の承認』セクションを参照)。
- 十分な管理ユーザーがいない場合、ジョブは正常に受け入れられません。

ユーザー・アカウントのロックアウト

システムおよびユーザー・アカウントをブルート・フォース・パスワード攻撃から保護するために、ユーザー・アカウントの連続ログイン試行回数が 10 回に到達すると、そのユーザー・アカウントがロックされます。ユーザー・アカウントのロックは、アカウントが明示的に有効化されるか (『管理ユーザーの状況の編集』のセクション参照)、サーバー・サービスが再始動されるまで解除されません。

注記

- サーバー・サービスを再始動するには、仮想マシンのコンソールで **systemctl restart spsd** を実行します。
- アカウントのロックアウトはサーバー・ベースで行われます。クラスター内の 1 つのサーバーでロックアウトされたアカウントが、そのクラスター内の他のサーバーで自動的にロックアウトされることはありません。
- アカウントのロックアウトのしきい値をユーザーが構成することはできません。

LDAP ディレクトリーのリスト

製品管理者は、MDE ユーザー管理用に LDAP ディレクトリーを構成できます。LDAP ディレクトリーを追加、変更、または削除できます。各アクションでジョブが作成され、ジョブを有効にするには承認が必要です。

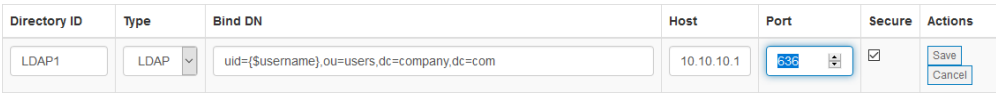
LDAP ディレクトリーを追加または変更する場合、使用できる設定は次のとおりです。

- 「ディレクトリー **ID**」 – LDAP ディレクトリーの ID。
- 「タイプ」 - LDAP または Active Directory のドロップダウン・オプション。
- 「バインド **DN**」 – LDAP サーバーにバインドするために使用する完全識別名。
  - バインド DN のサンプル構文は、次のとおりです。
    uid={$username},ou=users,dc=company,dc=com

注記

LDAP タイプを Active Directory に変更する前に、バインド DN は設定する必要があります。

- 「ホスト」 – LDAP サーバーの IP/ホスト名。
- 「ポート」 – LDAP サーバーのポート。
- 「セキュア」 – セキュアまたは非セキュアな LDAP 接続の ID。
- 「アクション」 - 「保存」または「キャンセル」を選択。



ユーザーのソース

MDE では、内部定義ユーザーと外部定義ユーザーを同時にサポートできます。外部定義ユーザーでは、「ユーザー・リスト」の「ディレクトリー」列に値が表示されます。内部定義ユーザーでは、そのフィールドは空白になります。

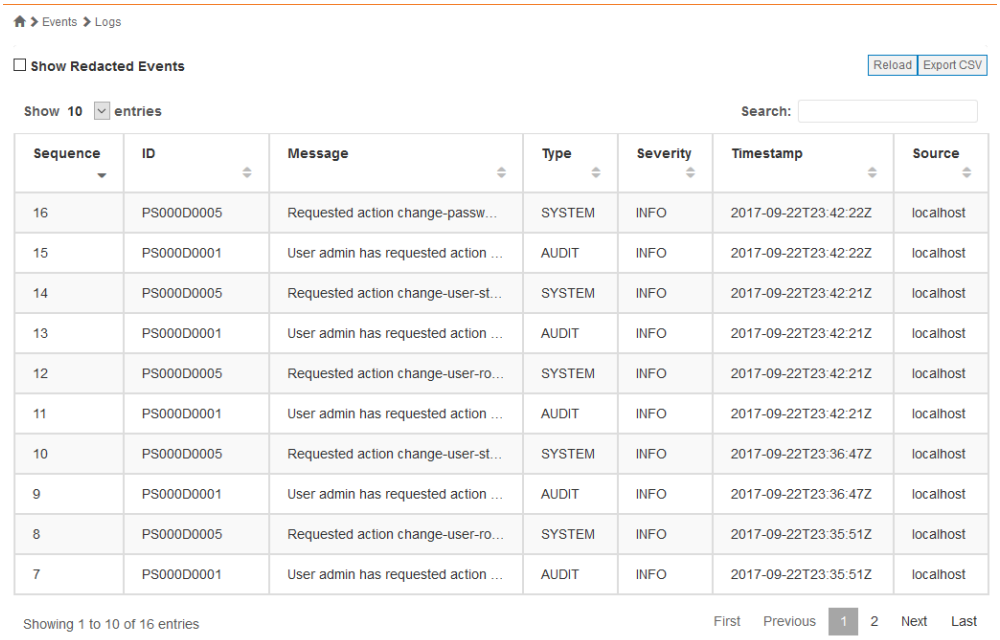
Name	Status	Roles	Directory	PW Modified	Actions
admin	Enabled	Product Administrator, Security Administrator		2017-09-22T23:09:44Z	Edit Password Edit Roles Delete
ProductAdmin	Enabled	Product Administrator		2017-09-22T23:25:40Z	Edit Password Edit Status Edit Roles Delete
SecurityAdmin	Enabled	Security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

イベント

MDE 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。このシステムにより、管理対象エージェントからのイベントは内部的に生成されたイベントとともに集約されて、内部イベント・ログに保存されます。また、1 つ以上の宛先にイベントを転送するようにシステムを構成できます。

イベント・ログ

MDE のイベント・ログは、最上位のメニュー・バーにある「イベント」メニュー項目を選択すると表示できます。



このページには、単一の順次リストに、すべてのイベントが表示されます。イベントごとに、以下のように定義されているシーケンス番号、ID、メッセージ、タイプ、重大度、受信タイム・スタンプ、およびソースが表示されます。

- **Sequence number** – イベントを受信した順序に基づいた番号。この値は (同じイベントが繰り返された場合でも) 固有であり、時間とともに増加します。
- **ID** – イベントの固有の ID。同じイベントの複数のインスタンスに、共通の ID が割り当てられます。
- **Message** – イベントが発生した状態を示す説明テキスト。一部のイベントでは変数の挿入がサポートされているため、イベント ID が共通の場合でも、テキストが若干異なることがあります。
- **Type** – イベント発生原因がシステム・アクションなのかユーザー・アクションなのかを示します。タイプは、次のとおりです。
  - **SYSTEM** - 自動化された MDE アクションによって発生したイベント。

  - **AUDIT** - ユーザー・アクションによって発生したイベント。
- **Severity** – イベント認識レベルの相対表示。重大度のカテゴリーは次のとおりです。
  - **INFO** – アクションは不要です。単なる通知メッセージです。
  - **WARN** – 即時アクションは不要です。状態のモニターをお勧めします。
  - **CRITICAL** – 即時アクションが必要です。
- **Timestamp** – 協定世界時 (UTC) 形式でのイベント発生時刻の表示。
- **Source** – イベントが発生したシステム (エージェントまたは MDE) のホスト名または IP。

MDE イベント・ログのサイズは、「Advanced Settings」で構成できます。設定されているサイズ制限に達した場合、新規イベントを受信すると、最も古いイベントがローテーションにより削除されます。

イベントの詳細

イベントには、イベント・メッセージに含まれない拡張引数が存在する場合があります。これが存在する場合、そのイベントのイベント・ログのメッセージ列に「詳細」リンクが表示されます。この「詳細」ボタンをクリックすると、拡張引数が表示されます。

イベントのエクスポート

MDE では、管理者は、「イベント」ページの「CSV のエクスポート」ボタンを使用してイベント・リストを CSV ファイル・フォーマットでエクスポートできます。

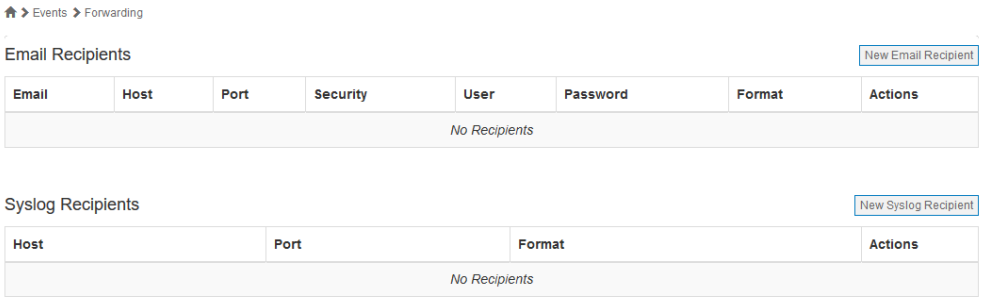
「CSV のエクスポート」ボタンをクリックすると、イベント・ファイルがクライアント・マシンにダウンロードされます。イベント・ファイル内の各行が、ログ内のイベントです。

イベント・ファイルの列は、イベント・シーケンス番号、イベント ID、編集済みフラグ、イベント・メッセージ文字列 (引数を含まない)、イベント・タイプ、イベント重大度、イベント引数、イベント・タイム・スタンプ、イベント・ソースです。

イベントの転送

受信したすべてのイベントが、構成されている各イベント宛先に転送されます。イベントは、内部イベント・ログへの挿入と並行して転送されます。

製品管理者またはセキュリティー管理者は、製品のイベント宛先を変更できます。構成すると、MDE によって作成または受信されたイベントが宛先に転送されます。サポートされる宛先タイプは、E メールと Syslog です。



また、MDE は、転送対象のイベントに対して複数のフォーマットをサポートしています。サポートされるフォーマットは、Log Event Extended Format (LEEF)、Common Event Format (CEF)、および Cloud Auditing Data Federation (CADF) イベント・モデルです。

イベント引数

通常のイベント・メッセージ・ストリングに加えて、イベント引数もキー/値パラメーターの形で送信されます。これらのパラメーターは、プレフィックス「spx」と引数名を連結させたストリングによって識別されます。例えば、イベントにユーザー名が含まれている場合、キー/値ペアのストリングは「spxuser=user1」のようになります。

エージェント・イベント

MDE では、各管理対象 (および接続された) エージェントのシステム・イベントと監査イベントが集約されます。これらのイベントは MDE イベント・ログに表示され、構成されているイベント宛先に転送されます。

注記

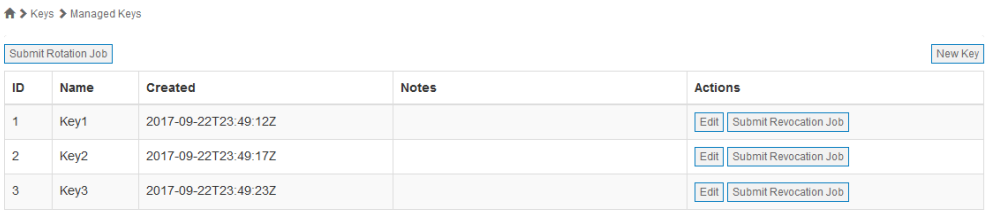
MDE、外部データベース、およびすべてのエージェントで **NTP** を利用してシステム時刻を調整することを強くお勧めします。これにより、イベント/監査ログのタイム・スタンプが適切に順序付けられます。

確実なイベント

個々のエージェントから MDE に送信されるイベントは、リアルタイムで処理されます。これは、イベントが欠落している場合に MDE がエージェントと通信し、欠落しているイベントを要求して、イベント・ログに適切な順序で挿入することを意味します。

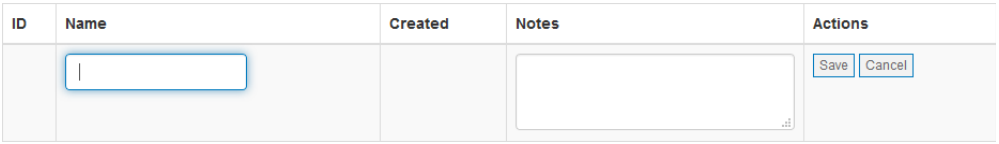
ポリシー実施鍵の管理

セキュリティー管理者は、MDE 内のセキュア・ストレージに対してポリシー実施鍵を定義できます。これらの鍵をデータ・タイプとボリュームに関連付けることで、データをセキュリティー保護し、暗号化アクセス制御を提供できます。



鍵の追加

新規の鍵を追加する場合、固有の名前を入力する必要があります。鍵名には大/小文字の区別がありません。鍵値は公開されず、ユーザーが編集することはできません。メモ・フィールドはオプションです。



注記

鍵名は変更できますが、実際の鍵値をユーザーが変更することはできません。

鍵は「鍵」ページで追加するか、データ・タイプまたはデータ・タイプ行を定義するときに追加できます。鍵は、「鍵」ページでのみ編集できます。

鍵の編集

鍵の作成後、セキュリティー管理者は鍵の名前を変更できます。鍵名を変更しても、実際の基盤となる鍵値は変更されません。また、メモ・フィールドを変更できます。

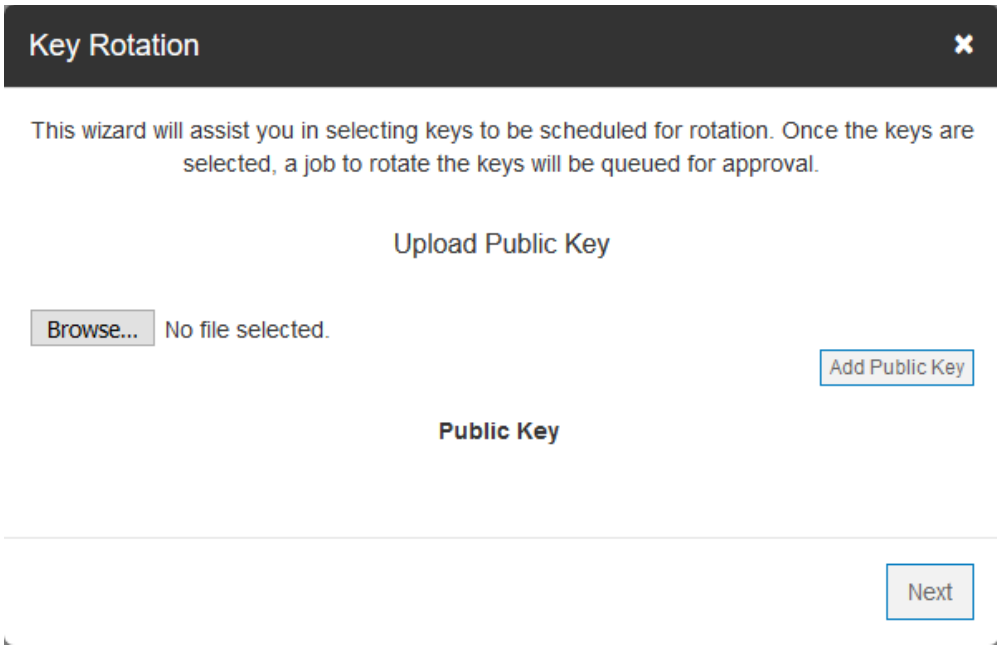
鍵のローテーション

MDE では、セキュリティー管理者はエージェント・エコシステム内で鍵をローテーションできます。「鍵」ページで、「鍵ローテーション・ジョブの実行依頼 (Submit Key Rotation Job)」ボタンをクリックします。

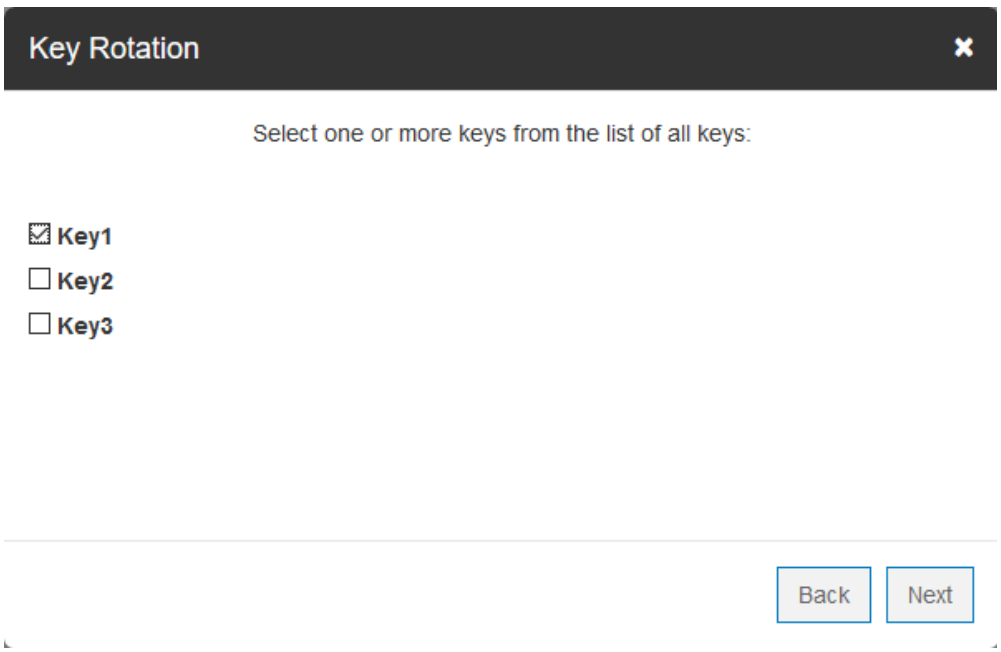
公開鍵をアップロードするように求めるプロンプトが出されます。この鍵を使用して、ローテーションされる鍵の鍵エスクローが暗号化されます。該当する鍵を選択し、鍵を追加して、「次へ」をクリックします。

重要な注記

SSL 鍵は、RSA および PEM でエンコードされている必要があります。



鍵を手動で選択する場合、作成されたすべての鍵のリストが表示されます。セキュリティー管理者は、任意の数の鍵をローテーションに選択できます。



必要な鍵を選択すると、ジョブが作成されます。

重要な注記

鍵が複数のエージェントに関連付けられている場合、その鍵を使用するすべてのエージェントが影響を受けます。

ジョブの承認時に、影響を受けるすべてのエージェントに鍵ローテーションが通知されます。影響を受けるすべてのエージェントが鍵ローテーション・プロセスを完了するまで、ジョブは引き続き実行されます。影響を受けるエージェントの数に応じて、このジョブの完了に時間がかかる場合があります。

注記

外部鍵ストアを使用する場合、鍵ローテーションを成功させるには、外部鍵ストアがオンラインになっている必要があります。エラーが発生した場合は、外部鍵ストアがオンラインであることを確認し、PPM サーバーをリブートするか、PPM サービス (spsd) を再始動してください。

鍵の取り消し

鍵の取り消しにより、MDE から鍵が削除されて、その鍵がエスクローに配置されます。鍵の取り消しは、アクティブなポリシーに現在関連付けられていない鍵でのみ実行できます。鍵の取り消しの前に、セキュリティー管理者はその鍵を参照しているポリシーを削除する必要があります。

鍵を利用するパスをエージェント・ポリシーの関連付けから削除しても、ディスク上のデータは暗号化解除されないため、データにアクセスできる必要がある場合は、そのパスに関連付けられたポリシーを削除する前に、保護対象のディレクトリーからデータを移動する必要があります。

取り消しが完了すると、保護対象のパスに残っているデータはアクセス不能になります。取り消された鍵はエスクローに保存され、通常の PPM 操作から削除されます。

警告

セキュリティー管理者は、エージェント・ポリシーを更新して、すべてのエージェントからターゲット鍵の関連付けを解除してから、その鍵を取り消す必要があります。パスの削除について詳しくは、『エージェントの編集』のセクションを参照してください。

鍵の廃棄

鍵の廃棄は鍵の取り消しと同じように機能しますが、鍵廃棄操作が完了した後で鍵はエスクローに配置されず、データが永久にアクセス不能になります。

注記

この機能は REST API 経由でのみ使用可能です。詳しくは、REST API の資料を参照してください。

自動生成鍵

セキュリティー管理者がポリシー実施鍵を管理することを希望しない場合は、新規で作成した各ポリシーに対して MDE によって鍵を自動生成できます。自動生成鍵は、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。

重要な注記

自動生成鍵は、ローテーションすることも取り消すこともできません。鍵のローテーションまたは取り消しの機能が必要な場合は、代わりに名前付きの鍵を使用してください。

外部鍵ストア

鍵は、内部のセキュアなデータベースまたは外部鍵ストアの 2 つの場所のいずれかに保管できます。MDE は、最初は内部のセキュアなデータベースのみを使用するようにセットアップされています。セキュリティー管理者が外部鍵ストアを利用する予定であれば、外部鍵ストアを構成する必要があります。外部鍵ストアは、鍵の保護にのみ使用されます。外部鍵ストアの鍵管理は、MDE によって行う必要があります。

注記

外部鍵ストアのセットアップ手順は、外部鍵ストアのベンダーから提供されています。

KMIP 鍵ストア

このタスクについて

セキュリティー管理者は、Java 鍵ストアと Java トラストストアをアップロードする必要があります。Java 鍵ストアと Java トラストストアを作成するには、以下の手順を実行します。

手順

1. クライアント証明書ファイルとクライアント秘密鍵ファイルを PKCS12 (Public Key Cryptography Standard #12) フォーマットで収集します。以降の手順では、これを「client.p12」と呼んでいます (クライアント証明書とクライアント

秘密鍵を 1 つの PKCS12 形式のファイルに結合する場合の例については、『付録 *C*: PKCS12 ファイルを作成するための変換のサンプル』を参照してください)。

2. 公開 CA 証明書ファイルを収集します。以降の手順では、このファイルを「sklm_ca.pem」と呼んでいます。

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

3. 以下のようにして、PKCS12 ファイルを新規の Java 鍵ストアにインポートします。

   重要な注記

   この手順で、パスワードが求められます。以降で使用するために、このパスワードを保持してください。

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

4. 以下のようにして、ファイルから別名を取得します。
5. 以下のようにして、CA 証明書ファイルを新規の Java トラストストアにインポートします。

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

   重要な注記

   この手順で、パスワードが求められます。以降で使用するために、このパスワードを保持してください。

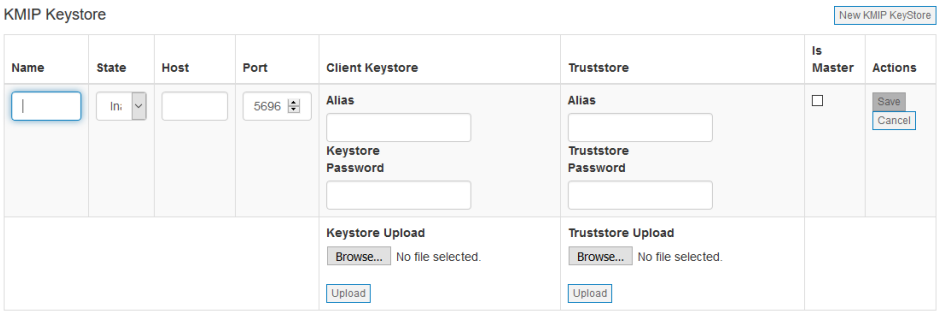
6. 以下のようにして、ファイルから別名を取得します。 **keytool -v -list -keystore trust.jks**

   外部鍵ストアをアクティブにするために入力する必要がある設定は、次のとおりです。

   - 「名前」 – 外部鍵ストアの、ユーザー定義の参照。
   - 「状態」 **-** これにより、MDE に対して、定義した外部鍵ストアによって現在のアクティブな鍵ストアをオーバーライドする必要があることを指示します。「状態」が「*active*」の場合、MDE はこの鍵ストアの使用を開始します。「状態」が「*inactive*」の場合、MDE は鍵ストアを使用しなくなります。
   - 「ホスト」 **-** 外部鍵ストアの IP アドレス。
   - 「ポート」 **-** 外部鍵ストアのポート番号。
   - 「クライアント鍵ストア」
     - 「**Keystore Alias**」 – 収集した鍵ストア別名。
     - 「**Keystore File**」 – Java 鍵ストア・ファイル。
     - 「**Client Keystore Password**」 – 鍵ストアの作成時にセットアップしたパスワード。
   - 「トラストストア」

- 「**Truststore Alias**」 – 収集したトラストストア別名。
- 「**Truststore File**」 - Java トラストストア・ファイル。
- 「**Truststore Password**」 - トラストストアの作成時にセットアップしたパスワード。

• 「マスター」 - すべての読み取り操作と書き込み操作のマスター鍵ストアとして使用される外部鍵ストアを識別します。
  - デフォルトでは、最初に定義された鍵ストアについてこれが「true」になります。
  - これを選択しない場合、「クローン」鍵ストアとして扱われ、読み取り操作にのみ使用されます。
  - マスターとして指定できる外部鍵ストアは 1 つのみです。



注記

現在、MDE がサポートしている外部鍵ストア製品は、KMIP 用に構成された IBM Security Key Lifecycle Manager (SKLM) です。

ハードウェア・セキュリティー・モジュール (HSM)

このタスクについて

HSM を外部鍵ストアとして使用する場合、そのサード・パーティー製品が製造元の説明に従って完全に構成済みであり、作動可能な状態であることを確認する必要があります。

HSM の 64 ビット・バージョンのクライアント・ソフトウェアは、PPM 製品管理者が MDE VM にコピーする必要があります。このソフトウェアは、通信のセットアップと構成を行うために、HSM の製造元の製品説明を使用して SDK オプションとともに抽出し、インストールする必要があります。

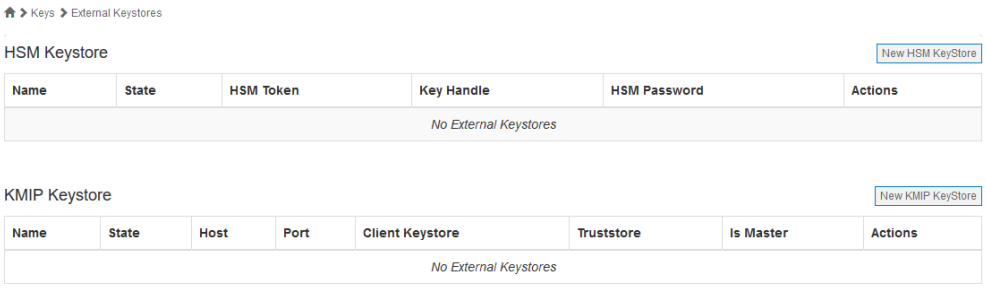
クライアント・ソフトウェアに付属のユーティリティー、または HSM で機能することが実証されているユーティリティーを使用して、ラッパー鍵を作成します。 ラッパー鍵は、PPM を使用して作業するために必要な 256 対称鍵です。

この対称ラッパー鍵を HSM 上に作成すると、その鍵にハンドルが割り当てられます。このハンドルは、PPM GUI ページで HSM を構成する際に必要になります。

PPM は、ポリシーの鍵をラップするためにこのハンドルとポリシーの鍵を HSM に渡し、HSM は、ラップされた鍵を PPM データベースに保管するために返却します。

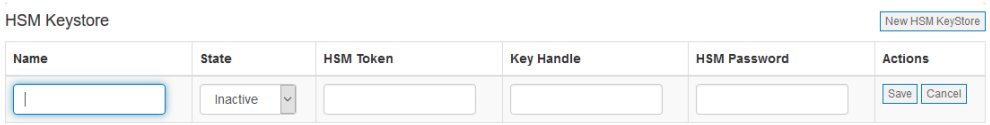
ソフトウェアのインストールと構成が済んだら、PPM が HSM と通信できることを確認し、PPM VM をリブートします。

「外部鍵ストア (External Keystores)」画面から「新規 HSM 鍵ストア (New HSM Keystore)」を選択します。



外部鍵ストアをアクティブにするには、以下の設定を入力する必要があります。

- 「名前」 – 外部鍵ストアの、ユーザー定義の参照。
- 「状態」 - これによって鍵ストアに意図した状態を設定します。
- 「**HSM** トークン」 - HSM はパーティションのスロット番号を使用します。
- 「鍵ハンドル」 - これは、ポリシーの鍵をラップするために使用される鍵に割り当てられるハンドルです。
- 「**HSM** パスワード」 - これは、お客様が使用するパーティションに関連付けられたパスワードです。



注: サポートされる HSM 製品: HSM 鍵ストアとして構成された SafeNet® Luna HSM。

ファイル・レベルのポリシー定義

MDE では、セキュリティー管理者はさまざまなタイプのデータにファイル・レベルの制御 (操作および暗号) を定義できます。ファイル・レベルのデータ制御を定義する際に、以下の用語を使用します。

- セレクター - 任意のリソース (またはパス・セット) へのアクセスが許可されるユーザーを定義する、ユーザーとグループの順不同リスト。オプションで、定義済みプロセスをセレクターの別の構成要素として識別できます。
- パス・セット - ポリシーによって保護されるファイル・パスのリスト。
- データ・タイプ - 指定のタイプのデータに割り当てられる、アクセス定義行の番号付きリスト。各行はセレクター、入出力 (読み取り/書き込み) 操作、およびポリシー・アクションで構成されます。
- プロセス - 実行可能ファイルのファイル・パス。識別された実行可能ファイルとともにアクセス制御を定義するために、セレクター内で使用されます。より高度なアクセス制御のためのオプション。

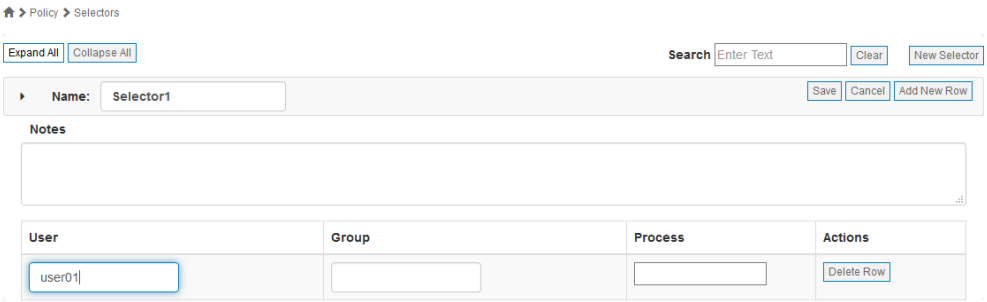
データ・タイプを作成したら、それをプロビジョニングされた 1 つ以上のエージェントに関連付けできます。以下のセクションでは、ポリシーの構成について説明します。

セレクター

セレクターは、1 つ以上のセレクター行を使用して 1 組のユーザーまたはユーザー・グループ (あるいはこの両方) を定義するポリシー・オブジェクトです。新規セレクターを追加する際、セキュリティー管理者は保存前に名前を指定する必要があります。セレクターを編集することで、セレクターのメモと行をいつでも追加できます。

各セレクター行には、ユーザー・フィールド、グループ・フィールド、プロセス・フィールドが含まれています。必ずこれらのフィールドのいずれかにデータを設定してから保存してください。

- 「ユーザー」 - ターゲット・システム定義のユーザーの短縮名。これは、ターゲット・エージェントのオペレーティング・システム内のユーザーと突き合わせられます。このフィールドはオプションです。
- 「グループ」 – ターゲット・システム定義または LDAP 定義のユーザー・グループの短縮名。これは、ターゲット・エージェントのオペレーティング・システム内のユーザー・グループと突き合わせられます。このフィールドはオプションです。
- 「プロセス」 - 製品によって定義されたプロセス名の参照。これは、ターゲット・エージェントのオペレーティング・システム内のプロセス・ファイル・パス (およびオプションのハッシュ値) と突き合わせられます。このフィールドはオプションです。



各セレクター行の値は、論理 AND 演算を使用して結合されます。単一行に複数のフィールドが設定されている場合、突き合わせる行のすべてのフィールドが一致している必要があります。セレクターは、定義された行のいずれかが一致する場合に一致します。セレクター内の行の順序は、ポリシー・マッチング・アルゴリズムに影響しません。

ユーザー	グループ	プロセス	エージェントの突き合わせ動作
X			ユーザーに対して突き合わせ
	X		定義されたグループ内のいずれかのユーザーに対して突き合わせ
		X	定義されたプロセス・パスに対して突き合わせし、指定されたハッシュ値に限定される可能性あり
X	X		定義されたグループのメンバーとして動作する場合にのみ、ユーザーに対して突き合わせ
X		X	定義されたプロセスを通じて動作する場合にのみ、ユーザーに対して突き合わせ
	X	X	定義されたプロセスを通じて動作する場合にのみ、定義されたグループ内のいずれかのユーザーに対して突き合わせ

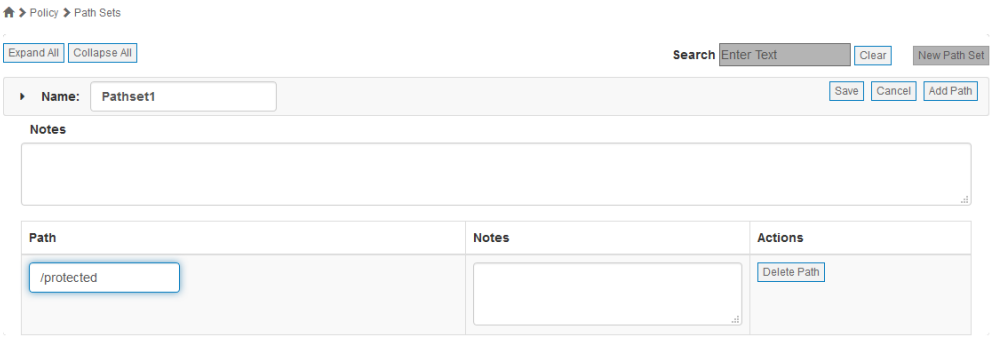
X	X	X	定義されたグループのメンバーとして動作し、定義されたプロセスを通じてプロセスとともに動作する場合にのみ、ユーザーに対して突き合わせ

注記

セレクターのユーザーおよびグループ (またはそのいずれか) の解決は、ファイル・エージェントがインストールされた構成済みの外部 LDAP サーバーまたは Active Directory サーバーと連動して機能します。

パス・セット

パス・セットは、1 つ以上の順不同ファイル・パス行のコレクションです。パス・セットを追加する際、セキュリティー管理者はパス・セットに名前を指定する必要があります。パス・セットに行を追加するには、「パスの追加」ボタンをクリックします。各行にはファイル・パスとメモが含まれています。



セキュリティー管理者は、ファイル・パスを指定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。

データ・タイプ

データ・タイプは、データのファイル・レベルの操作や暗号化アクセス制御を可能にする、データ・タイプ行定義の順序付きコレクションです。各データ・タイプに名前、ポリシー実施鍵、ユーザー・メモ、および行の順序付きリストが含まれています。

- 「名前」 - データ・タイプへのユーザー定義の参照。
- 「ユーザー・メモ **(User Notes)**」 - セキュリティー管理者が定義するメモ・フィールド。

データ・タイプ行

各データ・タイプ行には、順序、セレクター、操作、およびアクションの各フィールドが含まれています。

- 「順序」 - 各ポリシー行をチェックする際の優先順位。最初に一致した行が使用されます。このフィールドは必須ですが、存在する行が 1 行のみの場合は表示されません。
- 「セレクター」 - 以前に定義されたセレクターの選択。ポリシー行は、セレクター内のいずれかの行が一致する場合に一致します。このフィールドは必須です。MDE では、すべてのユーザーに対して一致する「すべて選択」セレクターを使用できます。
- 「操作」 - 実行できるファイル操作の選択。オプションは「読み取り」と「読み取り/書き込み」です。このフィールドは必須です。
- 「アクション」 - 操作に関連付けるアクセス・アクションの選択。オプションは「permit」、「deny」、「permit, log」、および「deny, log」です。このフィールドは必須です。

データ・タイプ行の変数

必要に応じて、「セレクター」フィールド、「操作」フィールド、および「アクション」フィールドを可変にするように設定できます。これにより、セキュリティー管理者はエージェント作成時に指定するデータ・タイプのテンプレートを作成できます。使用可能なフィールド設定は、「編集可能」、「編集の必要あり」および「編集不可」です。

「編集可能」

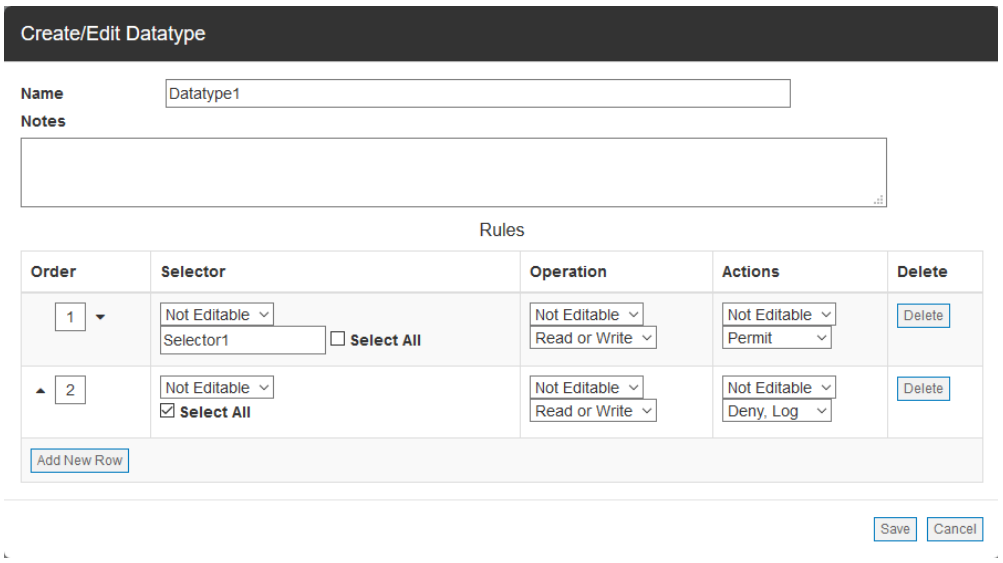
このフィールドは、必要に応じて、エージェント作成時に上書きできます。

「編集の必要あり」

このフィールドは、エージェント作成時に設定する必要があります。

「編集不可」

このフィールドは、データ・タイプ作成時に設定する必要があり、エージェント作成時に変更することはできません。



すべての行に値または変数設定を指定するまで、データ・タイプを保存することはできません。

プロセス

プロセスは、実行可能ファイルへのファイル・システム・パスを識別します。プロセスは以下のフィールドで構成されます。

- 「名前」 - プロセスの名前
- 「パス」 - ファイル・システムの実行可能ファイルへの絶対パス
- 「**OS**」 - オペレーティング・システムのタイプ (Linux、Windows) を参照するために使用するフィールド。
- 「バージョン」 - オペレーティング・システムのバージョンを入力するために使用するフィールド。
- 「配布」 - オペレーティング・システムのディストリビューション名 (Red Hat、CentOS、Windows) を入力するために使用するフィールド。

プロセスは、単なるファイル・パスとして定義することもプロセス・ハッシュ値のリストによって定義することもできます。1 つ以上のハッシュ値を定義する場合、プロセスの突き合わせ対象はリストされたハッシュに限定されます。

注記

プロセス・ハッシュ値はエージェント・ツールによって生成され、この値を PPM にコピーする必要があります。このツールは、現行バージョンの実行可能ファイルのハッシュ値を出力します。

spxhash -p <path to executable>

例:

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

1202E81EF41273904A6DD381C35B2561F838F7E35B6B26959F8EEB646297A36A7C2

エージェントのプロビジョニングと管理

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・ストアの 4 つのタイプのエージェント・インストールをサポートしています。エージェントのタイプごとに、異なる方式のデータ保護を使用できます。

- ボリューム - エージェントはデータをブロック・デバイス・レベルで保護する
- ファイル/ポリシー - エージェントはデータをファイル・レベルで保護し、ファイル・ベース操作のアクセス制御ポリシーを提供する
- ボリューム/ポリシー - エージェントはデータをブロック・デバイス・レベルで保護し、ファイル・ベース操作のアクセス制御ポリシーも提供する
- オブジェクト・ストア - エージェントはオブジェクト・ストレージに送信されるデータを保護する

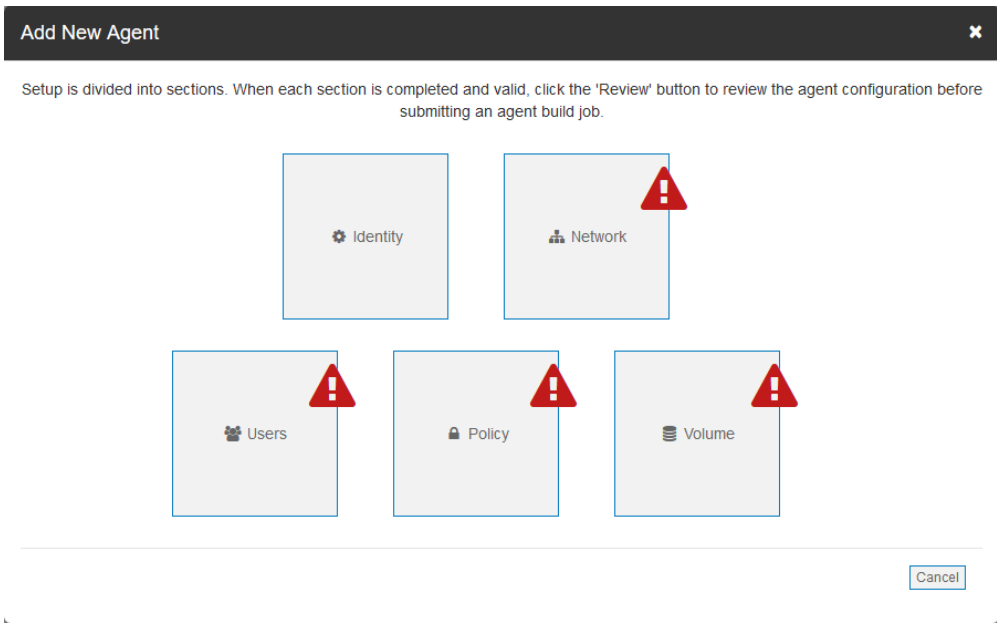
エージェントの追加

エージェントを追加するには、セキュリティー管理者は MDE の「エージェント」ページにナビゲートして「エージェントの追加」ボタンをクリックする必要があります。これにより、ダイアログが起動して新規エージェントをプロビジョニングするために必要な手順が示されます。

注記

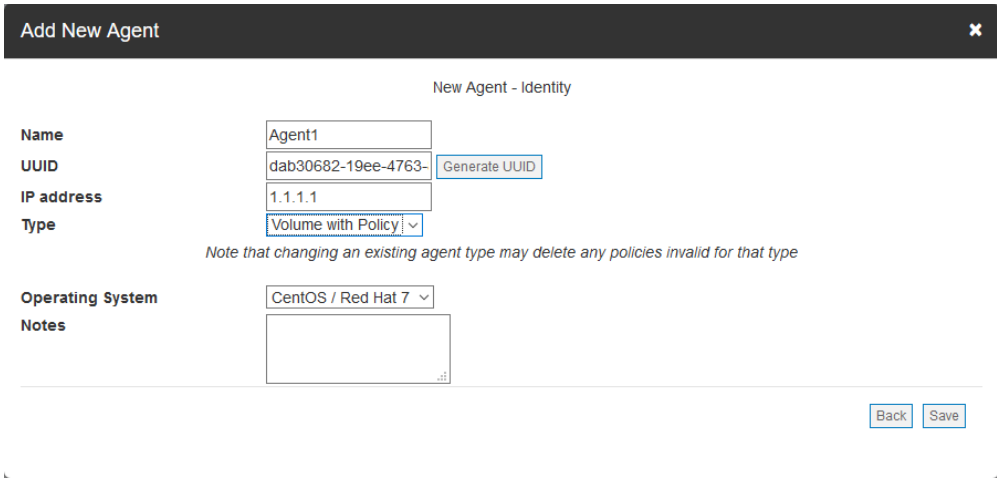
エージェントの追加プロセスを開始する前に、対象のポリシー構成要素 (セレクター、パス・セット、鍵、データ・タイプ、およびプロセス) をすべて追加することをお勧めします。これらの構成要素はプロセス中に作成できないためです。

エージェントのプロビジョニングには、「ID」、「ネットワーク」、「ユーザー」、「ポリシー」、「ボリューム」、および「ツール」の 6 つのセクションがあります。 エージェントのタイプによっては、「ポリシー」セクションと「ボリューム」セクションは表示される場合も表示されない場合もあります。エージェントを追加するためには、必要なすべてのセクションを完了する必要があります。



ID

「ID」セクションでは、セキュリティー管理者はエージェントの名前、タイプ、IP アドレス、オペレーティング・システム、メモを定義し、固有 ID (UUID) を指定または生成する必要があります



- 「名前」 - エージェントに対するユーザー定義の参照。
- 「**UUID**」 – エージェントを特定するために MDE が使用する固有 ID。
- 「**IP** アドレス」 - エージェントがインストールされているサーバーの IPv4 アドレス。
- 「タイプ」 – ボリューム、ファイル/ポリシー、ボリューム/ポリシー、またはオブジェクト・ストアの選択。
- 「オペレーティング・システム」 – ターゲット・エージェントのオペレーティング・システム。

- 「メモ」 – このエージェントに関するセキュリティー管理者のメモ。

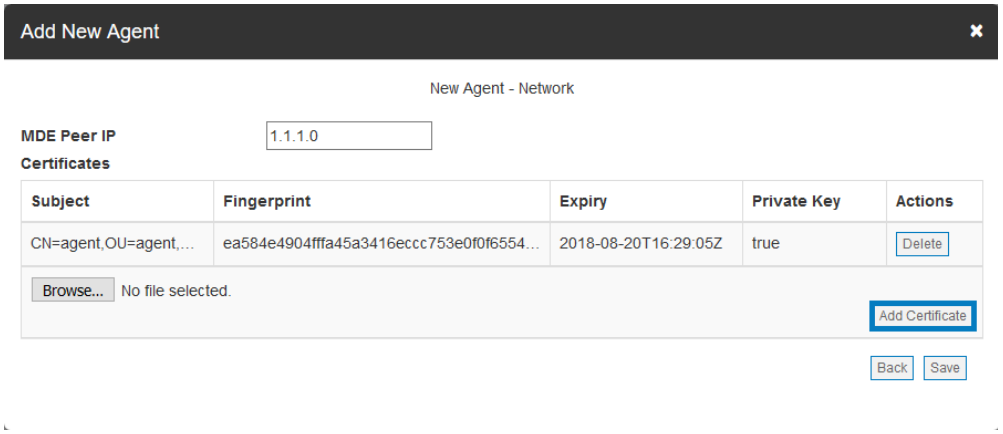
必要なすべてのフィールドに入力したら、「保存」をクリックしてメインのプロビジョニング・ダイアログに戻ります。

注記

- セキュリティー管理者が UUID を指定することを希望しない場合は、MDE によって生成できます。
- 必須のフィールドは、GUI で示されます。
- エージェントの名前は固有ではありません。このため、複数のエージェントに同じ名前を使用する場合は、イベント・ログのメッセージの通報源が誤って表される場合があります。

ネットワーク

ネットワーク・ステップでは、セキュリティー管理者は MDE のホスト名または IP アドレス、および MDE とターゲット・エージェント間にセキュアな接続を確立するために必要となる証明書を定義する必要があります。



- 「**MDE Peer IP**」 – ターゲット・エージェント・サーバー・インスタンスから見た MDE の IP アドレス。
- 「証明書」 – MDE とインストールされたエージェント間にセキュアな接続を確立するために使用する、アップロードされた証明書のリスト。この証明書を使用して、エージェントと MDE PPM サーバー間に相互認証の TLS1.2 接続を確立します。

証明書をアップロードするには、セキュリティー管理者は「証明書の追加」ボタンをクリックし、該当する証明書にナビゲートして開く必要があります。これにより、「新規エージェント - ネットワーク」画面に表示されます。

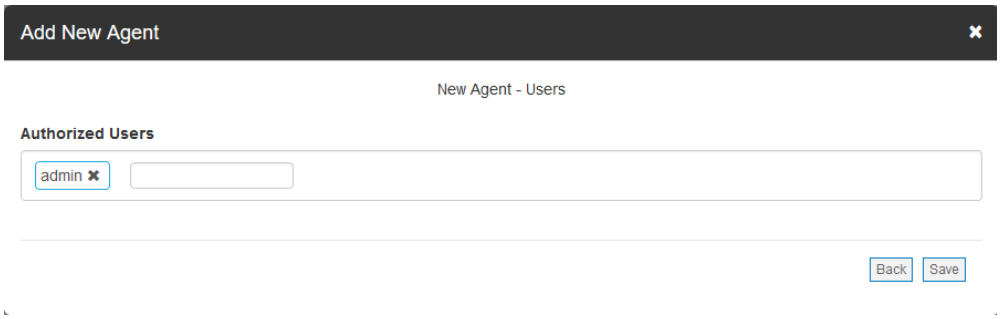
注記

鍵ストア証明書とトラストストア証明書が MDE にアップロードされておらず、エージェントに一致する証明書が割り当てられていない場合、エージェントと PPM は通信せず、エージェントはデータの暗号化もポリシーの実施も行いません。詳しくは、『サーバー証明書の設定』セクションを参照してください。

必要なすべてのフィールドに入力したら、「保存」をクリックしてメインのプロビジョニング・ダイアログに戻ります。

ユーザー

ユーザー・ステップでは、セキュリティー管理者は、エージェント・インストール・バンドルをダウンロードする特権を持つ MDE ユーザー・アカウントを定義する必要があります。ユーザーが許可されたユーザーとしてリストされていない場合に、そのユーザーがログインしてエージェントを表示した場合、そのユーザーには「エージェント情報」ページにダウンロード・リンクは表示されません。



ポリシー

ポリシー・ステップでは、セキュリティー管理者は、ターゲット・エージェントのファイル・パスに対する操作制御と暗号制御を定義する必要があります。

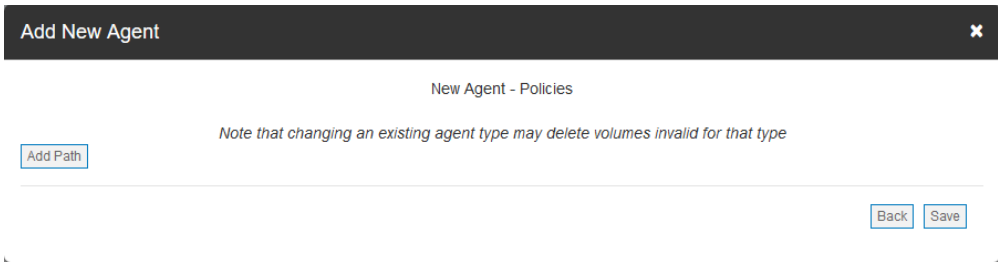
パスの追加

このタスクについて

ファイル/ポリシー・エージェントおよびボリューム/ポリシー・エージェントでは、エージェント・ポリシーにパス定義を追加できます。追加された各パスにより、ターゲット・エージェントの個々のファイル・パスまたはファイル・パス・グループが保護されます。追加するパスの数は、セキュリティー管理者が定義します。

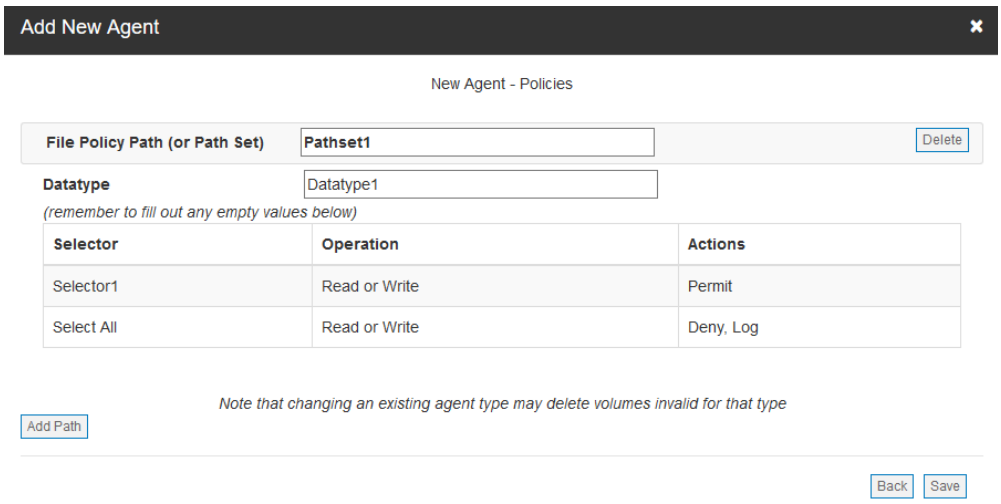
重要な注記

- ポリシー適用時にポリシーによって保護されたパスが存在している必要があります。そうでないと、ポリシー適用は失敗します。
- 既存のファイルとサブディレクトリーは、ファイル/ポリシー・エージェントのインストール後に使用可能になる **spxconvert** コマンドを使用して手動で処理する必要があります。ファイルが暗号化されていない場合でも、ポリシーは有効になります。
- インストール後に追加された新しいファイルとディレクトリーは自動的に暗号化され、ポリシーによって保護されます。



パスを追加するには、「パスの追加」ボタンをクリックします。

追加するパスごとに、ファイル・パスまたはパス・セット、およびデータ・タイプの入力が必要です。



- 「ファイル・ポリシー・パス」**(**または「パス・セット」**)** – 指定のデータ・タイプ・アクセス制御定義によって保護するパスまたはパス・グループを指定します。保護は、指定されたファイル・パスからサブディレクトリーまで再帰的に行われます。
- 「鍵」 **-** データ・タイプに関連付けられたパスを暗号化するために使用する鍵。以前に定義した鍵または MDE で管理される自動生成鍵を使用できます。ファイル/ポリシーとボリューム/ポリシーのいずれを使用するかに応じて、このフィールドは表示される場合も表示されない場合もあります (注記を参照)。

- 「データ・タイプ」 – 事前作成されたデータ・タイプの選択。選択すると、データ・タイプ情報がインラインで追加されます。変数が含まれたデータ・タイプを使用する場合は、保存する前に変数を入力する必要があります。

注記

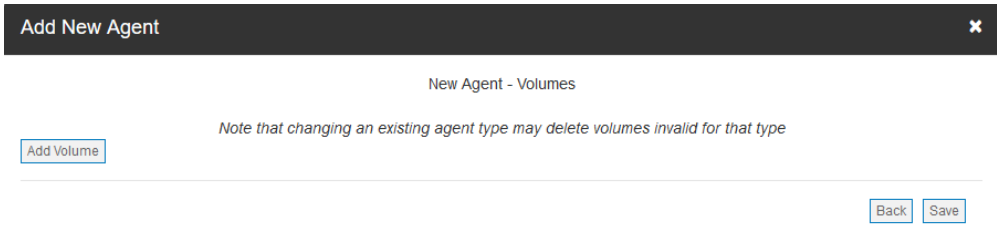
- パス・セットを使用する場合、新規エージェントを追加する前にパス・セットを作成する必要があります。それ以外の場合は、単一の手動パスを定義できます。
- 使用するデータ・タイプは、新規エージェントを追加する前に作成する必要があります。
- 新規エージェントがボリューム/ポリシー・タイプの場合、保護はボリューム・ポリシー定義によって実行されるため、パス・セットにポリシー実施鍵は含まれません。

ボリューム

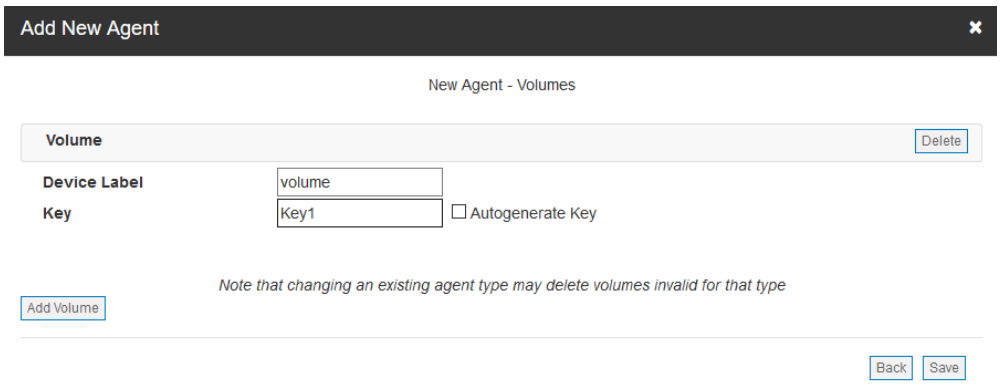
ボリュームの追加

このタスクについて

ボリューム・エージェント・タイプおよびボリューム/ポリシー・エージェント・タイプでは、エージェント・ポリシーに 1 つ以上のボリューム定義を追加できます。追加した各ボリュームは、ターゲット・エージェント上の新しい保護対象ブロック・デバイスになります。



ボリュームを追加するには、「ボリュームの追加」ボタンをクリックします。追加するボリュームごとに、基本のデバイス・ラベルおよびポリシー実施鍵の入力が必要になります。



- 「デバイス・ラベル」 – 保護対象のデバイスを指定します。エージェントにポリシーをデプロイしたら、spxdevice コマンドを実行してデバイス・ラベルをボリュームに関連付ける必要があります (セクション『エージェントのインストール』を参照)。
- 「鍵」 – ボリュームを暗号化するために使用する鍵。以前に定義した鍵または MDE で管理される自動生成鍵を使用できます。

重要な注記

「鍵の自動生成」オプションを使用する場合を除き、追加するポリシー実施鍵はエージェントの追加前に定義する必要があります。セクション『ポリシー実施鍵の管理』を参照してください。

エージェントのツール

エージェントでは、データを暗号化された形で転送するための専用のツールがサポートされています。バックアップ/リストア、送受信、およびオブジェクト・ストアの 3 つのタイプのツールがあります。

ツールの構成は、エージェントのプロビジョニング時、または「エージェント情報」ページで行います。バックアップ/リストア・ツールは、暗号化されたデータのバックアップおよびリストアに使用されます。これは、関連付けられている鍵を利用して、暗号化されたデータをバックアップし、後で、そのポリシー鍵がローテーションされても、その暗号化されたデータをリストアできるようにします。送受信ツールは、暗号化されたデータに鍵を関連付けて、ユーザーがその暗号化されたデータを暗号化解除できるようにします。バックアップ/リストア・ツールと送受信ツールはオプションで、ツールをエージェントに関連付ける必要はありません。オブジェクト・ストア・ツールは、オブジェクト・ストア・エージェントには必須です。

エージェントとツールのマトリックス

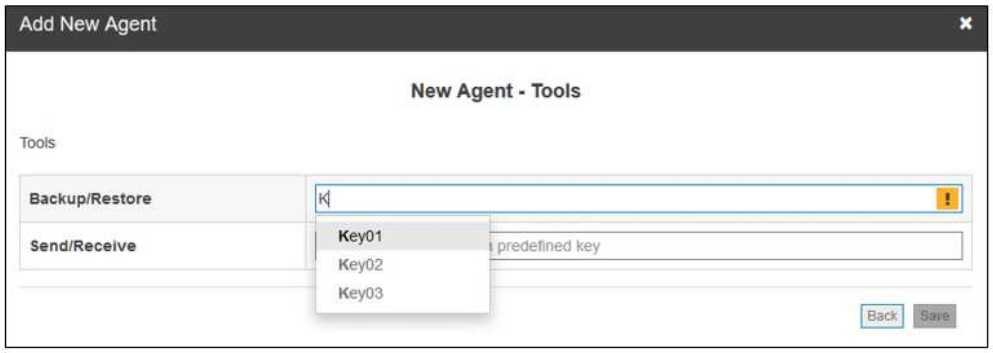
ツールを使用できるかどうかはエージェントのタイプによって異なり、鍵を関連付けることによってツールが有効化されます。エージェント・タイプごとのツールのマトリックスを以下に示します。

ツール・タイプ	ボリューム	ポリシー付きボリューム	ポリシー付きファイル	オブジェクト・ストア
バックアップ/リストア	X	X	X	
送信/受信	X	X	X	
オブジェクト・ストア				X

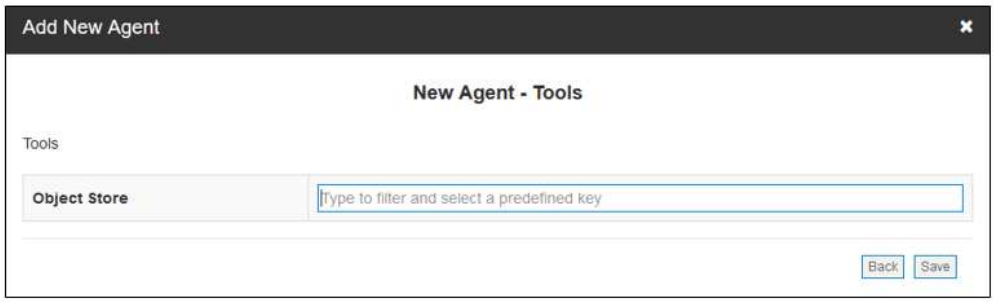
ツールと鍵の関連付け

鍵をツールに関連付けるには、使用するツールの横にあるテキスト・ボックスに、以前に定義した鍵名の最初の数文字を入力し、表示されたリストから該当する鍵を

選択します。「保存」をクリックするとジョブが作成されます。ジョブが承認されると、構成されたツールをエージェントで使用できるようになります。



For the Object Store Agent, it will display one available tool:

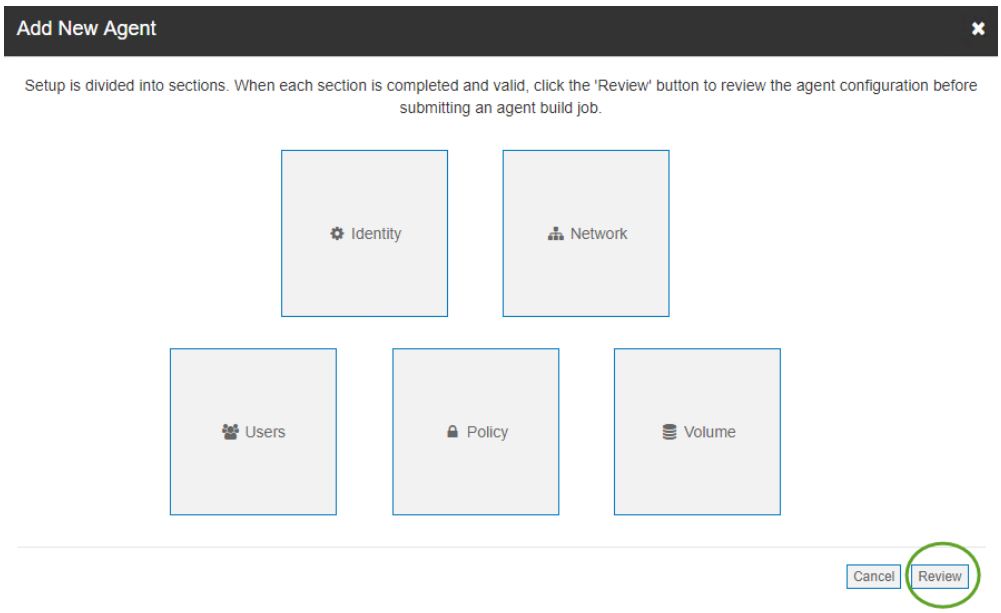


注: ツールでは自動生成鍵がサポートされていません。エージェントを作成する前に、鍵を定義しておく必要があります。

レビューとビルド

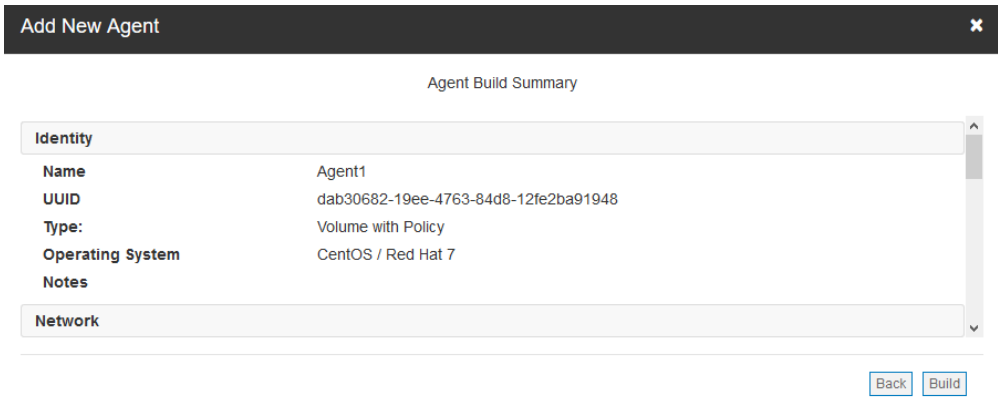
このタスクについて

必要なすべてのボリュームとパスを入力したら、「保存」をクリックしてメインのプロビジョニング・ページに戻ります。すべてのプロビジョニング手順が完了すると、プロビジョニング手順のボックスの表示がクリアされて「レビュー」ボタンが使用可能になります。



追加の変更を行うか、「レビュー」をクリックして次の手順に進みます。

プロビジョニング・セットアップのレビュー・ページには、すべての構成情報の完全なビューが表示されます。



内容が完全かつ正確かどうかをレビューし、「ビルド」をクリックしてプロビジョニング・プロセスを完了します。「ビルド」ボタンをクリックすると、エージェントを追加するためのジョブが作成されます。

ジョブが承認されると、エージェントが作成されて、インストール・パッケージをダウンロードしてインストールできるようになります。

エージェントのアクティブ化

エージェント・ビルド・ジョブが承認されると、新規作成されたエージェントが MDE 内でアクティブになります。エージェントがインストールされると、構成された MDE ピア IP と指定された証明書を使用して MDE への相互認証 TLS1.2 接続が作成されます。

エージェントは、初回インストール時と以降の開始時にポリシーを要求します。MDE は、設定されているポリシー構成で応答します。ポリシーは、受信されるとエージェントで適用されます。

エージェントの表示

このタスクについて

「エージェント」ページには、作成したエージェントのサマリー・リストが表示されます。

特定のエージェントの詳細を表示するには、「名前」列にあるエージェント名をクリックするか、「アクション」列の「詳細」ボタンをクリックします。エージェント詳細表示ページが開いて、プロビジョニング情報、インストール・バンドルのダウンロード、およびその他の役立つ情報が表示されます。

エージェント・レポート

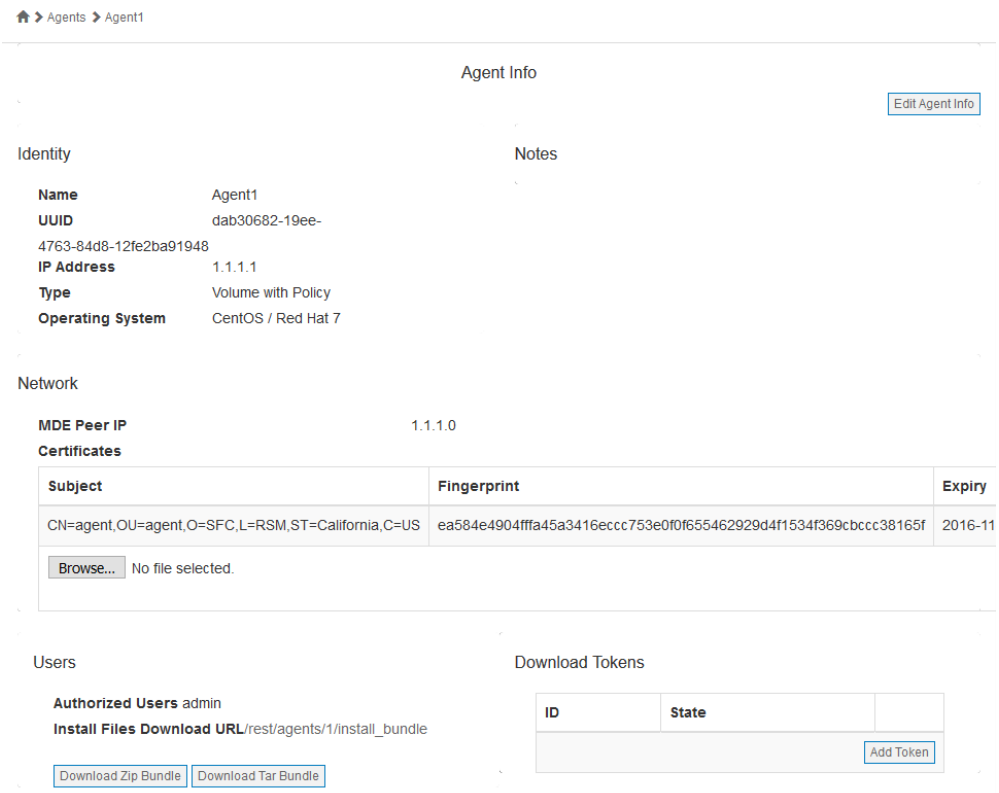
MDE のセキュリティー管理者はエージェント・レポートを作成できます。このレポートには、エージェントの総数、タイプおよびオペレーティング・システムごとのエージェント数、およびレポート生成から 30 日以内にログインしたエージェントに関する情報が含まれます。日付は、UTC 時間である PPM 時間に基づきます。データはエージェント・タイプに細分されます。

エージェントのインストール

このタスクについて

プロビジョニング手順で、ターゲット・サーバー・インスタンスにエージェントをインストールしてポリシーをデプロイするために必要となるすべての情報を構成し

ました。エージェントをインストールするには、インストール・パッケージをダウンロードしてターゲット・システムにコピーし、コンテンツをアンパックして、セットアップ・スクリプトを実行します。



重要な注記

プロビジョニング・ポリシーに指定されているすべてのユーザー、グループ、およびパスまたはデバイスが作成されており、エージェント・システムに接続されて構成されていることを確認します。

Linux 用のエージェントのインストール

エージェント・タイプには、ボリューム・エージェント、ポリシー付きファイル・エージェント、ポリシー付きボリューム・エージェント、およびオブジェクト・ストア・エージェントの 4 つがあります。エージェント・プロビジョニング中に指定したエージェント・タイプを使用してください。

Linux 用ボリューム・エージェントのデバイス構成

このタスクについて

手順

1. ボリュームを PPM で作成します (セクション 11.1.5 で使用したデバイス・ラベルを記憶します)。
2. エージェント VM に「gettext」パッケージをインストールします。

3. エージェントをインストールします。詳しくは『付録 *A*』を参照してください。
4. インストールが完了したら、エージェント VM をリブートします。
5. root として spxdevice -e <PPM で指定したラベル> -m <マウント・ポイント> -f <ファイル・システム> -u <使用するディスク> を実行します。

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

Linux 用ファイル/ポリシー・エージェントのデバイス構成

このタスクについて

手順

1. ファイル/ポリシー・エージェントを PPM で作成します。
2. 必要なユーザーを作成します。
3. 必要なサブディレクトリーを作成します。
4. ディレクトリーに適切な権限を設定します。
5. エージェント VM に「gettext」パッケージをインストールします。
6. エージェントをインストールします。詳しくは『付録 *A*』を参照してください。
7. インストールが完了したら、エージェント VM をリブートします。
8. コマンド「spxinfo -l」を使用してファイル・ポリシーが適切であることを確認します。

   注記

パスの横のアスタリスクは、暗号化が保留になっている既存のデータがあることを示しています。既存のディレクトリー構造とデータに対して適切に暗号化を行い、データの状況を随時判別できるよう、MDE には「spxconvert」というコマンド・ライン・ユーティリティーが用意されています。 このコマンドの詳しい説明と使用法については、『付録 *E:* 暗号化の実施』を参照してください。

Linux 用ボリューム/ポリシー・エージェントのデバイス構成

このタスクについて

手順

1. ボリューム/ポリシー・エージェントを PPM で作成します (使用したデバイス・ラベルを記憶します)。
2. エージェント VM に「gettext」パッケージをインストールします。
3. エージェントをインストールします。詳しくは『付録 *A*』を参照してください。
4. インストールが完了したら、エージェント VM をリブートします。
5. root として spxdevice -e <PPM で指定したラベル> -m <マウント・ポイント> -f <ファイル・システム> -u <使用するディスク> を実行します。

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

6. 必要なサブディレクトリーとユーザーを作成します。
7. ディレクトリーに適切な権限を設定します。
8. エージェント VM をリブートします。
9. lsblk – これを使用してディスクが存在することを確認します。この操作には最大 30 秒かかる場合があります。
10. コマンド「spxinfo -l」を使用してファイル・ポリシーが適切であることを確認します。

注記

Linux では、ボリュームの暗号化はデバイス全体でもパーティションでもセットアップできます。単一のパーティションを使用する場合は、spxdevice -u オプションの使用時に単に空のパーティション (例えば、/dev/sdb1) を指定します。

Linux オブジェクト・ストア・エージェントの構成

このタスクについて

手順

1. オブジェクト・ストア・エージェントを PPM で作成します。
2. エージェントをインストールします。PPM については『付録 *A*』を参照してください。
3. インストールが完了したら、エージェント VM をリブートします。
4. オブジェクト・ストア・エージェントの SSL 証明書をシステムに作成またはコピーして、/etx/spx-osa/ に配置します。
5. /etc/spx-osa/spx-osa.conf を編集して、certfile、keyfile、および chainfile を該当する証明書名で更新します。
6. spxobject -m:n <m>:<n> を root として実行します。

```
[root@localhost]# spxobject -m:n 2:3
```

7. すべての共有について spxobject -ac -id <cloud id> -key <cloud key> -url <cloud url> -auth <auth type> -share id> を root として実行します。

```
[root@localhost]# spxobject -ac -id APIUSER1 -key APIKEY1 -url
s3.us-south.objectstorage.softlayer.net -auth S3_IBM4 -share 1
[root@localhost]# spxobject -ac -id APIUSER2 -key APIKEY2 -url
s3.us-south.objectstorage.softlayer.net -auth S3_IBM4 -share 2
[root@localhost]# spxobject -ac -id APIUSER3 -key APIKEY3 -url
s3.us-east-1.amazonaws.com -auth S3_AMZ4 -share 3
```

8. オブジェクト・ストア・エージェントとの通信用にローカルの API ID/鍵を作成します。

```
[root@localhost]# cat /dev/urandom | tr -dc 'A-Z0-9' | fold -w 20
| head -n 1 && cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold -w 40
| head -n 1
```

9. spxobject -ag -id <local id> -key <local key> -auth <auth type> を root として実行します。

```
[root@localhost]# spxobject -ag -id APILOCALUSER1 -key
APILOCALKEY1 -auth S3_IBM4
```

10. spxobject -ap -id <local id> -b <bucket> -perms <perm> を root として実行します。

```
[root@localhost]# spxobject -ap -id APILOCALUSER1 -b MyBucket1
-perms RW
```

Windows 用のエージェントのインストール

エージェント・タイプには、ボリューム・エージェント、ファイル/ポリシー・エージェント、およびボリューム/ポリシー・エージェントの 3 つがあります。エージェント・プロビジョニング中に指定したエージェント・タイプを使用してください。

Windows 用ボリューム・エージェントのデバイス構成

このタスクについて

手順

1. ボリュームを PPM で作成します (使用したデバイス・ラベルを記憶します)。
2. エージェントをインストールします。詳しくは『付録 *A*』を参照してください。
3. インストールが完了したら、エージェント VM をリブートします。
4. 「spxdevice -e <PPM で指定したラベル> -d <使用するディスク番号>」を実行して、ディスク全体に接続します。必ず管理者として実行してください。

   PS C:¥> spxdevice -e PRODISK -d 1
5. または、「spxdevice -e <PPM で指定したラベル> -d <使用するディスク番号> -m <ドライブ名> -f <ファイル・システム>」を実行してディスク全体に接続します。このディスクは、ドライブ名を使用してフォーマットされ、マウントされます。

   PS C:¥> spxdevice -e PRODISK -d 1 -m E -f NTFS
6. あるいは、「spxdevice -i <使用するディスク番号>」を実行してディスクをステージングして、特定のパーティションに接続します。

   PS C:¥> spxdevice -e PRODISK -i 1
7. 次に、「spxdevice -e <PPM で指定したラベル> -v <ドライブ名> -f <ファイル・システム>」を実行して特定のパーティションに接続し、ファイル・システムを使用してそのパーティションをフォーマットします。

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

   注記

Windows では、ボリュームの暗号化はデバイス全体でもパーティションでもセットアップできます。

- ディスク全体を暗号化する場合、そのディスクはオンラインかつ初期化済みでなければならず、ディスク・スペースはフォーマットされていてはなりません。ドライブ名が使用可能でなければなりません。
- パーティションを暗号化する場合、「spxdevice -i <ディスク番号>」を使用してクリーン・ディスク上にバッキング・デバイスを作成しなければなりません。その後に、ドライブ名を指定して RAW パーティションを作成する必要があります。

その他のオプションについては、「spxdevice」コマンドのヘルプを参照してください。

Windows 用ファイル/ポリシー・エージェントのデバイス構成

このタスクについて

手順

1. ファイル/ポリシー・エージェントを PPM で作成します。
2. 必要なユーザーを作成します。
3. 必要なサブディレクトリーを作成します。
4. ディレクトリーに適切な権限を設定します。
5. エージェントをインストールします。詳しくは『付録 *A*』を参照してください。
6. コマンド spxinfo -l を使用して、ファイル・ポリシーが適切であることを確認します。

注記

パスの横のアスタリスクは、暗号化が保留になっている既存のデータがあることを示しています。既存のディレクトリー構造とデータに対して適切に暗号化を行い、データの状況を随時判別できるよう、MDE には「spxconvert」というコマンド・ライン・ユーティリティーが用意されています。

このコマンドの詳しい説明と使用法については、『付録 *E:* 暗号化の実施』を参照してください。

注記

Windows では、ポリシーを使用してターゲット・ディレクトリーを作成する許可が管理ユーザーにあることを確認してください。ポリシーが取得されるとそのポリシーが適用されるためです。

Windows 用ボリューム/ポリシー・エージェントのデバイス構成

このタスクについて

手順

1. ボリューム/ポリシー・エージェントを PPM で作成します (使用したデバイス・ラベルを記憶します)。

2. エージェントをインストールします。詳しくは『付録 *A*』を参照してください。
3. インストールが完了したら、エージェント VM をリブートします。
4. 「spxdevice -e <PPM で指定したラベル> -d <使用するディスク番号>」を実行して、ディスク全体に接続します。必ず管理者として実行してください。

   PS C:¥> spxdevice -e PRODISK -d 1
5. または、「spxdevice -e <PPM で指定したラベル> -d <使用するディスク番号> -m <ドライブ名> -f <ファイル・システム>」を実行してディスク全体に接続します。このディスクは、ドライブ名を使用してフォーマットされ、マウントされます。

   PS C:¥> spxdevice -e PRODISK -d 1 -m E -f NTFS
6. あるいは、「spxdevice -I <使用するディスク番号>」を実行してディスクをステージングして、特定のパーティションに接続します。

   PS C:¥> spxdevice -i 1
7. 次に、「spxdevice -e <PPM で指定したラベル> -v <ドライブ名> -f <ファイル・システム>」を実行して特定のパーティションに接続し、ファイル・システムを使用してそのパーティションをフォーマットします。

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

   注記

Windows では、ボリュームの暗号化はデバイス全体でもパーティションでもセットアップできます。

- ディスク全体を暗号化する場合、そのディスクはオンラインかつ初期化済みでなければならず、ディスク・スペースはフォーマットされていてはなりません。ドライブ名が使用可能でなければなりません。
- パーティションを暗号化する場合、「spxdevice -i <ディスク番号>」を使用してクリーン・ディスク上にバッキング・デバイスを作成しなければなりません。その後に、ドライブ名を指定して RAW パーティションを作成する必要があります。

その他のオプションについては、「spxdevice」コマンドのヘルプを参照してください。

8. 保護対象のディレクトリーをボリュームに追加します。
9. コンピューターを再起動します。
10. spxinfo -l (保護対象のすべてのディレクトリーのリストが表示されます)

    注記

Windows では、ポリシーを使用してターゲット・ディレクトリーを作成する許可が管理ユーザーにあることを確認してください。ボリュームが接続されて使用可能になるとそのポリシーが有効になるためです。

アクティブ・ポリシー

エージェントごとに 1 つのアクティブ・ポリシーのみ設定できます。エージェントには、ポリシーは永続的な方法では保存されません。エージェントのリブートごとに、エージェントは、MDE から現在アクティブなポリシーを要求します。MDE にエージェントがアクセスできない場合、そのエージェントの保護対象のすべてのディレクトリーに対して、デフォルトのアクセス拒否が適用されます。

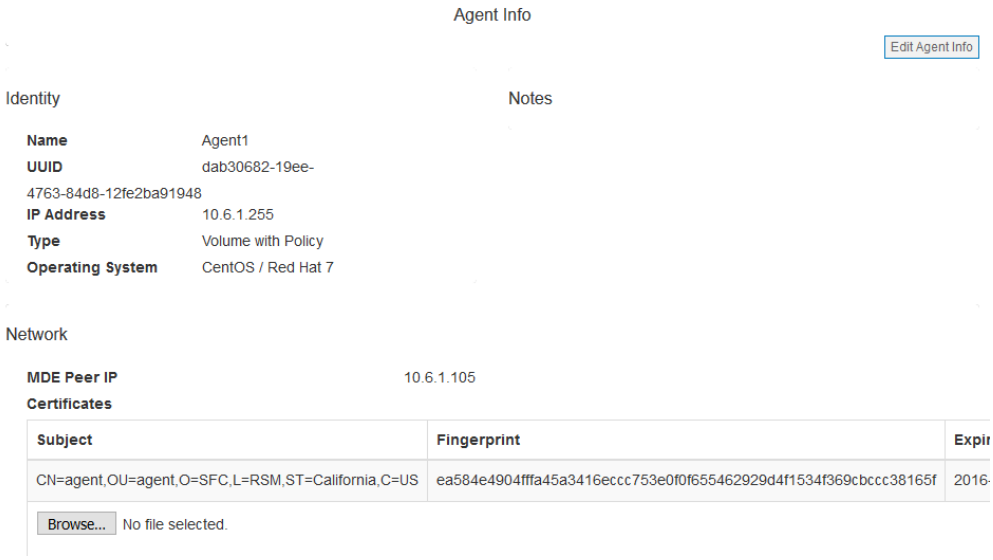
新しいポリシーがエージェントに送信された場合、ポリシーの適用が成功 (または失敗) すると、エージェントは MDE にイベントを送信します。ポリシーのアクティブ化が続く場合は、/var/log/spxagent/spx-policyagent ディレクトリーの kernel_policy.log ファイルを参照してください。

エージェントの編集

エージェントが正常にプロビジョンされて承認されたら、そのエージェントに対するすべての変更は、「エージェント情報」ページの GUI を使用してエージェントを編集することで実行する必要があります。エージェントを編集するには、エージェント詳細を表示します。「エージェント情報」ページでは、エージェントの各セクションを個別に編集できます。

エージェント情報の編集

「エージェント情報の編集」ボタンをクリックすると、一部のエージェント情報 (名前、IP アドレス、MDE ピア IP、メモ) を変更できるようになります。



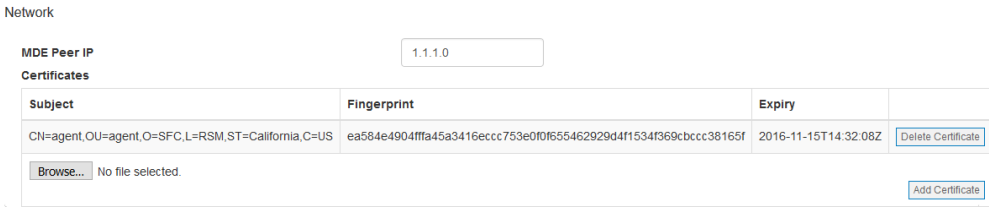
MDE ピア IP の変更は MDE 内で即座に行われますが、エージェントが既にインストールされている場合は、変更を有効にする前に、新規インストール・パッケージを作成してインストールする必要があります。

注記

初期プロビジョニング後に、UUID、オペレーティング・システム、およびエージェント・タイプを編集することはできません。

証明書の追加と削除

「エージェント情報」ページの「証明書」セクションにある該当するボタンをクリックすると、エージェント証明書を追加および削除できます。



エージェント証明書を更新するには、以下の手順を実行します。

1. エージェントの新規証明書を生成します。
2. 管理コンソールを通じて PPM に新規証明書をアップロードします。
   a. 「エージェント」ページで、更新するエージェントをクリックして、「エージェント情報」ページを表示します。
   b. 「証明書の追加」ボタンをクリックし、新規証明書のファイルを選択して、「OK」ボタンをクリックします。
   c. 新規証明書が表示されます。
3. 以前の証明書を削除します。
   a. 「エージェント」ページで、更新するエージェントをクリックして、「エージェント情報」ページを表示します。
   b. 削除する証明書を特定します。
   c. 「証明書の削除」ボタンをクリックすると、ジョブが作成されます。
   d. 「閉じる」ボタンをクリックします。
   e. 「ジョブ」ページで、該当するジョブの「承認」ボタンをクリックします。
4. 証明書がエージェントから削除されたことを確認します。
   a. 「エージェント」ページで、更新するエージェントをクリックして、「エージェント情報」ページを表示します。
   b. 適切な証明書が残っていることを確認します。

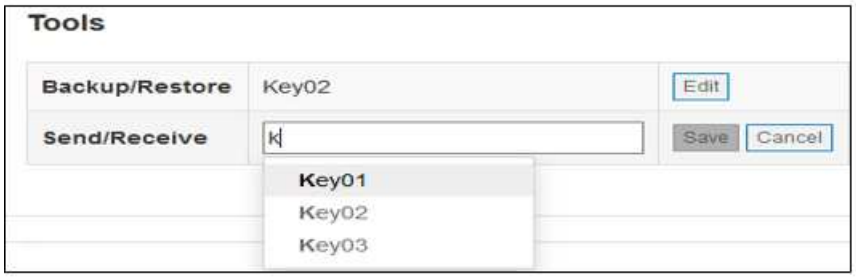
エージェントが既にインストールされている場合は、証明書の変更を有効にする前に、新規インストール・パッケージを作成してインストールする必要があります。

エージェントのツール

エージェントのプロビジョニング時に構成されなかったツールを、「エージェント情報」ページで追加できるようになりました。また、構成済みのツールを変更することもできます。

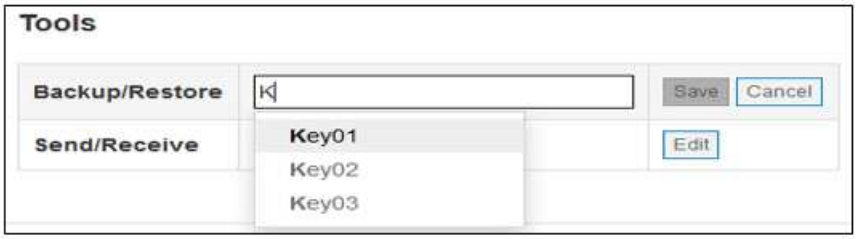
鍵の関連付け

鍵を関連付けるには、ツールの横にあるテキスト・ボックスに鍵名を入力し、表示されたリストから鍵を選択します。「保存」をクリックするとジョブが作成されます。ジョブが承認されると、構成されたツールをエージェントで使用できるようになります。



鍵の変更

鍵を変更するには、「編集」ボタンをクリックして、ツールの横にあるテキスト・ボックスに鍵名を入力し、表示されたリストから鍵を選択します。「保存」をクリックするとジョブが作成されます。ジョブが承認されると、構成されたツールをエージェントで使用できるようになります。



SU データ・アクセス

ポリシーによるアクセス制御を適用する場合、デフォルト設定では SU データ・アクセスが拒否されます。ただし、SU データ・アクセスが許可されるシナリオが存在する場合もあります。その場合は、「エージェント情報」ページに、この設定を変更できるチェック・ボックスがあります。

このチェック・ボックスを切り替えるとジョブが作成されます。ジョブが承認されると、SU データ・アクセスの設定がそれに合わせて変更されます。

以下の表に、SU データ・アクセスの制御内容を示します。

エージェント・タイプ	オペレーティング・システム	**SU** データ・アクセスのデフォルト	**SU** データ・アクセスが構成可能かどうか
ボリューム	CentOS6/RedHat6	該当しない	該当しない
ボリューム	CentOS7/RedHat7	該当しない	該当しない
ボリューム	Windows	該当しない	該当しない
ポリシー付きボリューム	CentOS6/RedHat6	ブロック済み	はい
ポリシー付きボリューム	CentOS7/RedHat7	ブロック済み	はい
ポリシー付きボリューム	Windows	該当しない	該当しない
ポリシー付きファイル	CentOS6/RedHat6	ブロック済み	はい
ポリシー付きファイル	CentOS7/RedHat7	ブロック済み	はい
ポリシー付きファイル	Windows	該当しない	該当しない
オブジェクト・ストア	CentOS7/RedHat7	該当しない	該当しない

ポリシーの中断

ボリューム/ポリシー・エージェントおよびファイル/ポリシー・エージェントでは、定義済みのアクティブ・ポリシーを中断する機能がサポートされています。ポリシーが中断されると、保護されたディレクトリーに対するすべてのアクションが拒否されます。アクティブ・ポリシーの中断は、アクティブなスナップショット定義を変更せずに行うことができます。

ポリシーを中断するには、「エージェント情報」のポリシー・セクションの右隅にある「アクティブ・ポリシーの中断」ボタンをクリックします。これにより、ジョブが作成されます。

ジョブが承認されると、ポリシーが直ちに中断され、ボタンの表示が「アクティブ・ポリシーの再有効化」に切り替わります。

中断されたポリシーを再有効化するには、「アクティブ・ポリシーの再有効化」ボタンをクリックします。これによりジョブが作成されます。ジョブが承認されると、最新のアクティブなスナップショット・ポリシーが直ちに有効化されます。

ポリシーの変更

ポリシーを変更するには、保護パスに適用されているポリシーを変更するか、新しい保護パスを追加するか、または暗号化ボリュームを追加します。

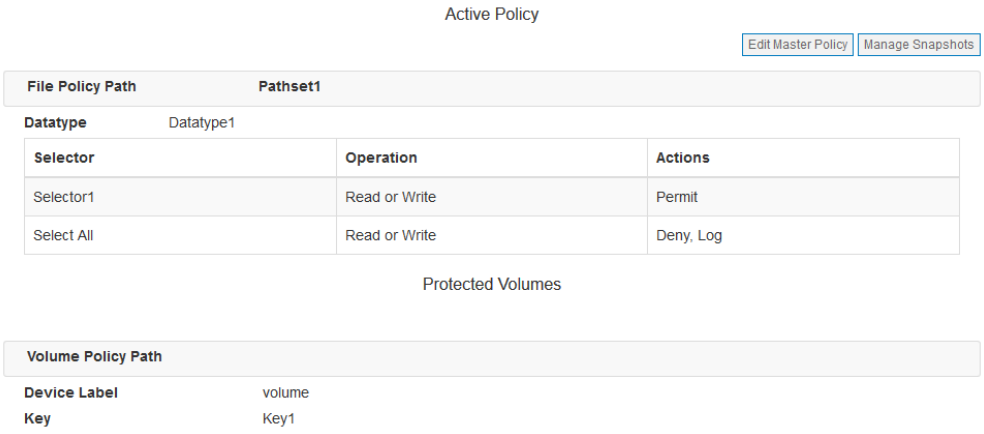
ポリシーの変更によって、現在のデータの暗号化状況は変更されません。ポリシーを再デプロイした後で作成されたデータの処理にのみ影響します。

重要な注記

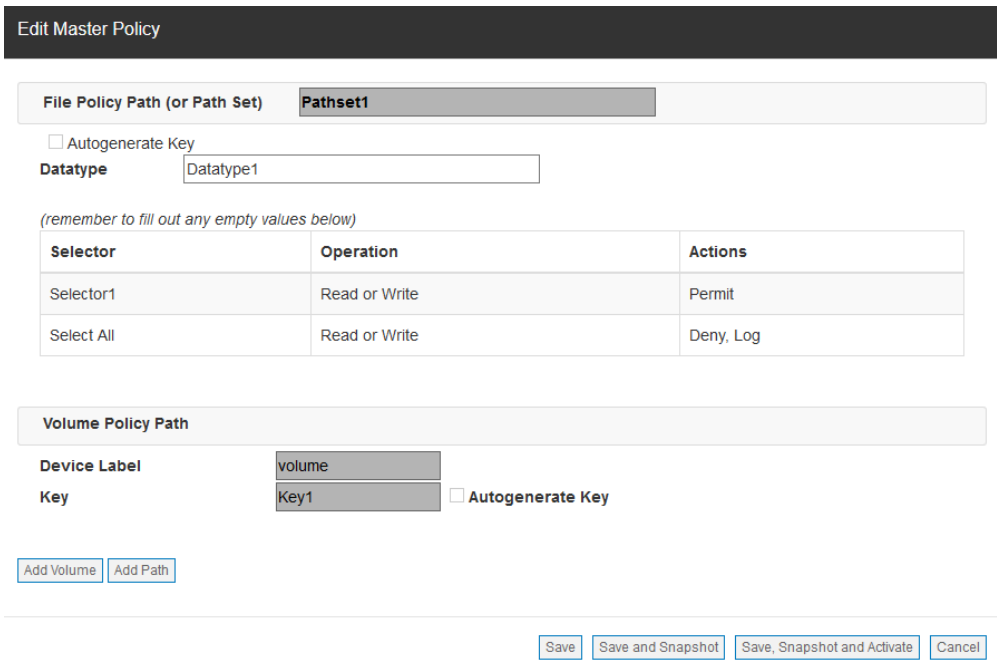
> アクティブなエージェントからボリューム・ポリシーを削除しないでください。削除はサポートされておらず、それを行うとターゲット・システムが一定しない状態になる可能性があります。
>
> アクティブなエージェントに新規ボリューム・ポリシーを作成して、古いボリュームを未使用のままにできます。
>
> または、新規エージェントを作成してデプロイすることもできます。

ポリシーの編集

エージェントのポリシーを編集することにより、ファイル・ポリシー・パス、パス・セットとデータ・タイプの関連付け、または暗号化ボリュームを変更できます。データ・タイプを変更して編集可能なデータ・タイプにすると、これらのフィールドのインライン編集が可能になります。ポリシーを編集するには、「マスター・ポリシーの編集」ボタンをクリックします。



これにより、「マスター・ポリシーの編集」ページが起動します。



注記

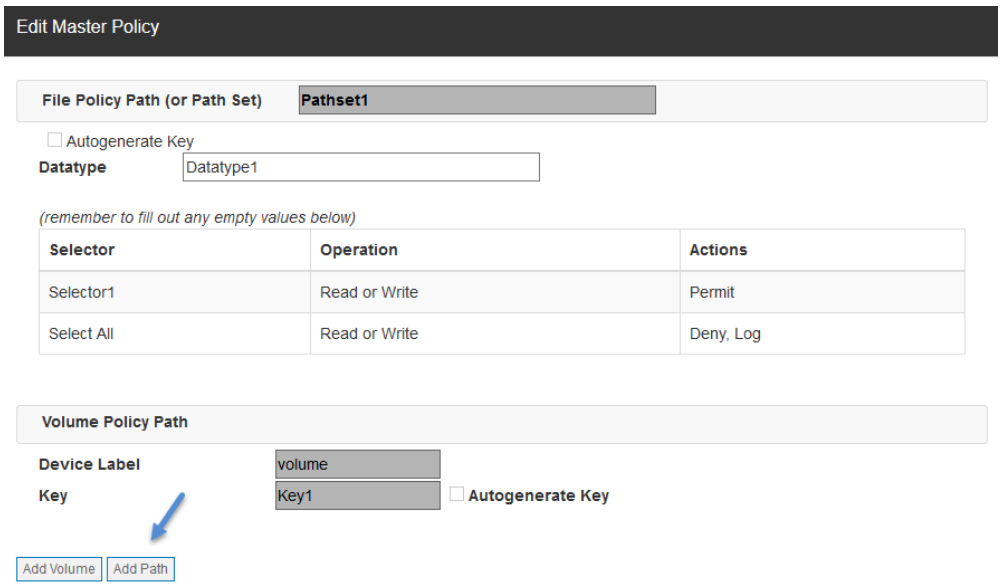
マスター・ポリシーを編集しても、スナップショットは変更されません。

•

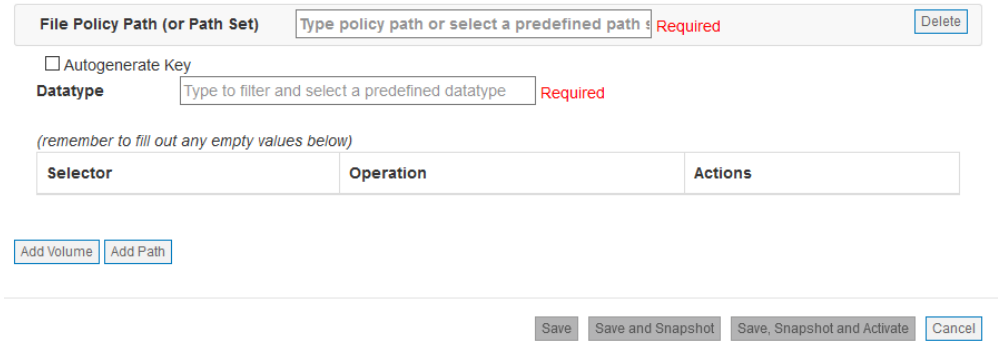
パスの追加

このタスクについて

ポリシーの下に配置する新規パスを追加するには、「パスの追加」ボタンをクリックします。



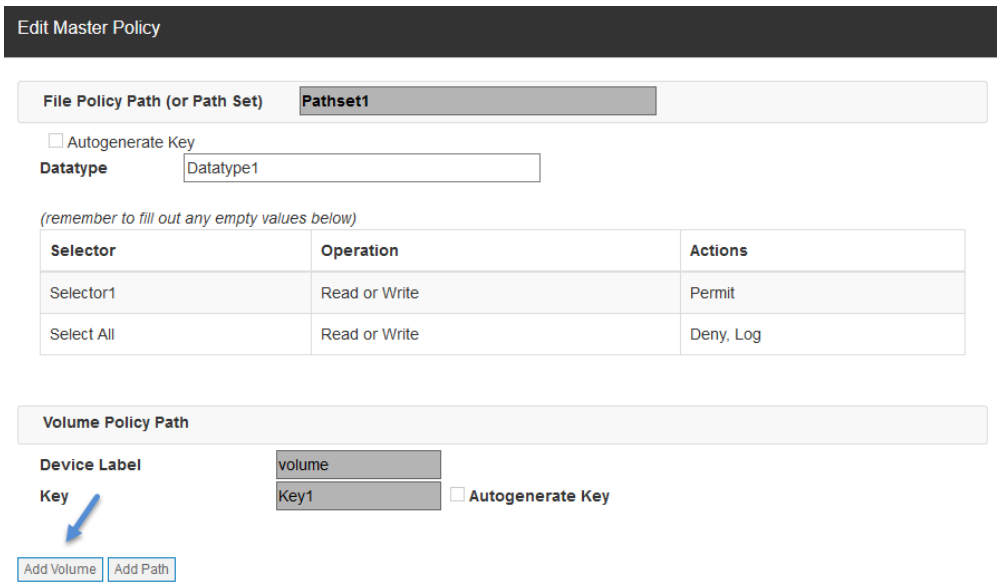
これにより、ポリシー入力用の新規セクションが開きます (最初のプロビジョニングと同様)。



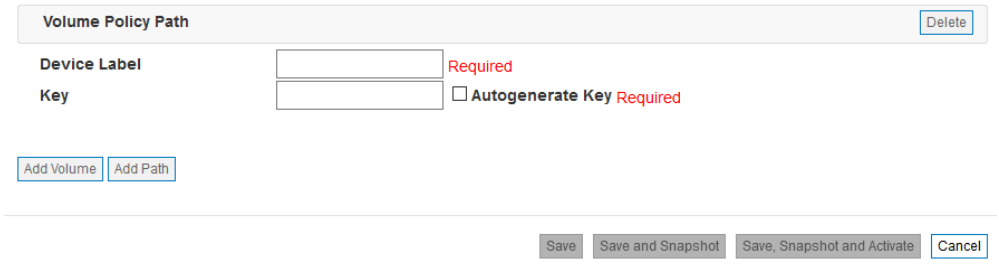
ボリュームの追加

このタスクについて

暗号化する新規ボリュームを追加するには、「ボリュームの追加」ボタンをクリックします。



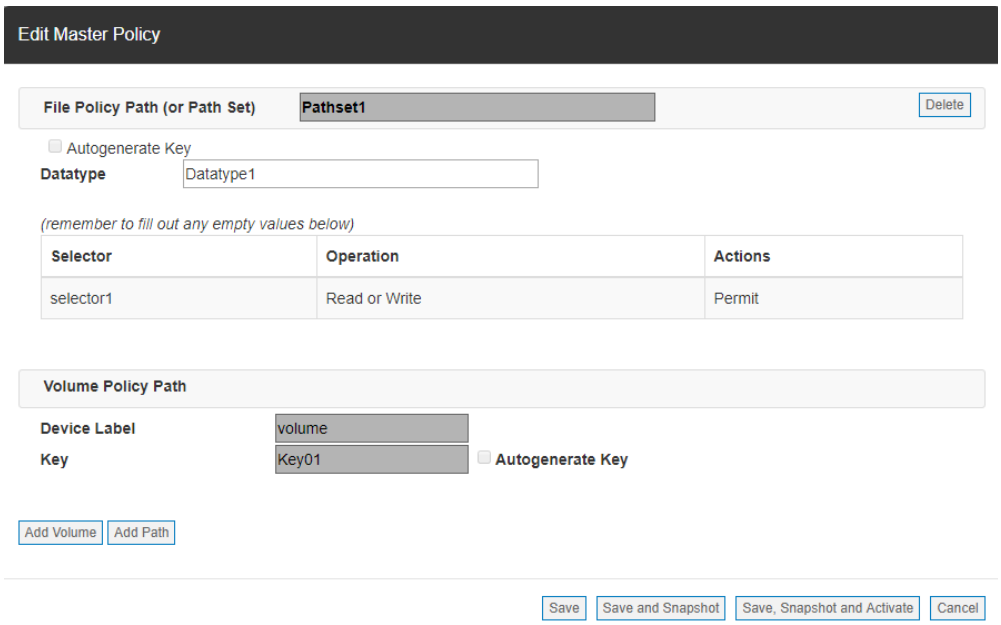
これにより、入力用の新規セクションが開きます (最初のプロビジョニングと同様)。



パスの削除

このタスクについて

ポリシー保護からパスを削除するには、目的のパスの「削除」ボタンをクリックします。そのポリシー構成が保存され、スナップショットが作成されてからアクティブ化されると、そのパスはアクセス制御ポリシーによって保護されなくなります。ディレクトリーに書き込まれた新規ファイルは暗号化されなくなります。既存のファイルは暗号化状態のままになり、アクセスできなくなります。

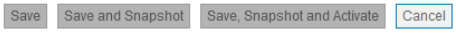


エージェント・スナップショット

エージェント・スナップショットは、エージェントに関連付けられたポリシー構成の永続ストレージです。スナップショットは索引付けされて、アクティブまたは非アクティブの状態になります。エージェントごとに、アクティブなスナップショットは 1 つのみです。これが、エージェントに現在適用されているポリシー構成です。エージェントのポリシー構成を変更するには、管理者は必要な変更を反映した新規スナップショットを作成して、新規スナップショットをアクティブ化する必要があります。

エージェントの編集の保存とスナップショット

エージェント・ポリシーの編集が完了したら、変更をキャンセルするか、変更を保存するか、変更を保存してスナップショットを作成するか、または変更を保存してスナップショットを作成してからアクティブ化できます。



変更のキャンセル

変更をキャンセルすると、変更前に適用されていたポリシー構成に戻ります。

変更の保存

変更を保存すると、今後の使用のために変更が保存されますが、スナップショットは作成されないため、変更をエージェントに適用できません。

保存とスナップショット作成

変更を保存してスナップショットを作成すると、今後の使用のために変更が保存されて、後で表示およびアクティブ化できるスナップショットが作成されます。

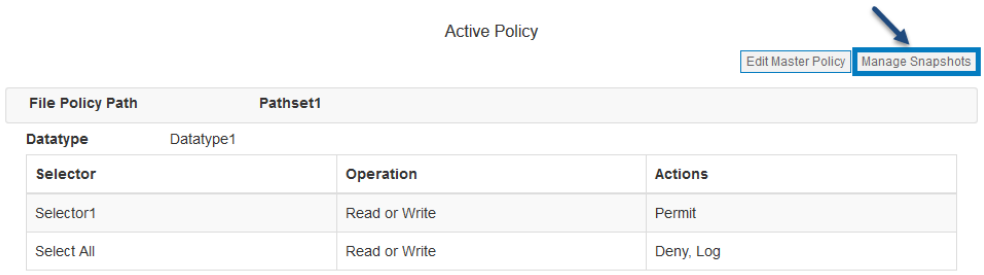
保存、スナップショット作成、およびアクティブ化

変更を保存してスナップショットを作成し、アクティブ化すると、今後の使用のために変更が保存されて、表示可能なスナップショットが作成され、これらの変更をエージェントに適用するジョブが即座に作成されます。

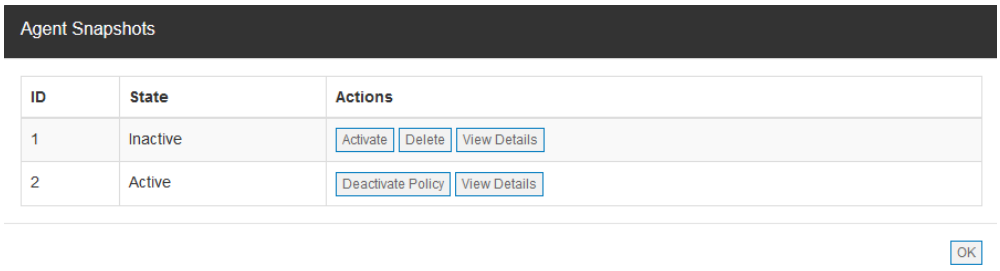
注: スナップショットに対する変更または更新は、エージェントが PPM サーバーと通信できるようになるまで適用されません。作成されたジョブは、PPM とエージェントの間の正常な通信またはエージェントが PPM サーバーから削除されるまで、引き続き実行されます。

スナップショットの管理

「エージェント情報」ビューの「スナップショットの管理」ボタンで、エージェントに関連付けられたすべてのスナップショットを表示できます。



このボタンをクリックすると、スナップショット管理ダイアログが表示されます。ここから、セキュリティー管理者は、スナップショットの詳細の表示、スナップショットのアクティブ化、スナップショットに関連付けられたポリシーの非アクティブ化、およびスナップショットの削除を行うことができます。

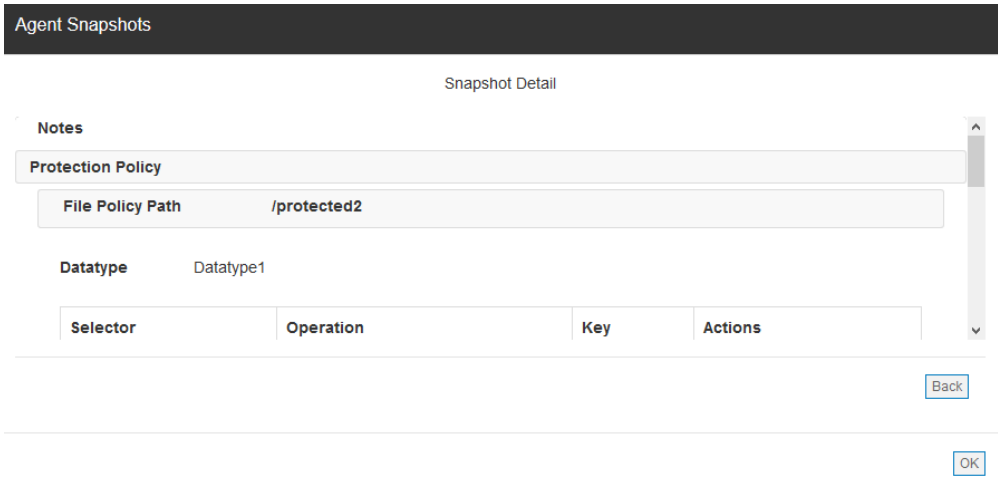


注記

アクティブ・スナップショットを変更しても、マスター・ポリシーは変更されません。

詳細の表示

このボタンで、スナップショットに関連付けられたポリシーのサマリー・ビューが表示されます。



「Activate Snapshot」

スナップショットをアクティブ化すると、ポリシーをエージェントに送信するジョブが作成されます。承認されると、スナップショットがアクティブ状態に移行し、そのポリシーによってエージェントに配置されているポリシーが上書きされます。

注: スナップショットに対する変更または更新は、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適用されません。作成されたジョブは、PPM とエージェントの間の正常な通信またはエージェントが PPM サーバーから削除されるまで、引き続き実行されます。

「Delete Snapshot」

非アクティブなスナップショットを削除できます。スナップショットを削除すると、MDE から完全に削除されます。

ファイル・エージェントのアンインストール

このタスクについて

ファイル・エージェントを削除する必要がある場合は、以下のステップを使用して実行できます。

保護対象ディレクトリーのデータをコピーします。これにより、ポリシーを非アクティブ化した後でデータがアクセス不能にならないようにします。

エージェント・ソフトウェアを削除するには、以下のステップを実行します。

手順

1. Linux – root として実行します。
2. spx-policyagent サービスを停止します。
   - CentOS 7 を使用している場合、以下を実行します。

     systemctl stop spx-policyagent
   - CentOS 6 を使用している場合、以下を実行します。

     service spx-policyagent stop
3. cd/opt/ibm/mde/spxagent/spx-fileagent/
4. ./fileagent_uninstall.sh
5. 「y」を入力して破壊アクションを確認します。
6. cd/opt/ibm/mde/spxagent/spx-policyagent/
7. ./policyagent_uninstall.sh
8. リブートします。
9. Windows – 管理者として実行します。
10. Windows GUI を使用する場合
    - 「コントロール パネル」の「プログラムの追加と削除」にナビゲートします。
    - 「FileAgent」を選択してアンインストールします。
    - プロンプトが出されたらシステムをリブートします。
11. PowerShell CLI を使用する場合
    - msiexec /x <FileAgent.msi へのパス>
    - プロンプトが出されたらシステムをリブートします。

    重要な注記

- 許可されたユーザーは、**mv (移動)** コマンドを使用して、暗号化された場所との間でデータを移動しないでください。そうした場合、**MDE** ポリシーに問題が発生する可能性があるためです。
  - まず、保護対象 **(暗号化された)** ディレクトリーとの間で **cp (コピー)** コマンドを使用してデータをバックアップします。
- ディレクトリーがポリシーによって保護されている場合、アンインストールの実行は完了しません。

ボリューム・エージェントのアンインストール

ボリューム・エージェントのアンインストール

1. Linux - root として実行します。
1. 保護ボリュームをアンマウントします。
- Unmount/dev/mapper/<e_volume>
1. spx-policyagent サービスを停止します。

- CentOS 7 を使用している場合、以下を実行します。

systemctl stop spx-policyagent

- CentOS 6 を使用している場合、以下を実行します。

service spx-policyagent stop

1. cd/opt/ibm/mde/spxagent/spx-volumeagent/
2. ./volumeagent_uninstall.sh
3. 「y」を入力して破壊アクションを確認します。
4. cd/opt/ibm/mde/spxagent/spx-policyagent/
5. ./policyagent_uninstall.sh
6. リブート

1. Windows – 管理者として実行します。

1. Windows GUI を使用する場合

- 「コントロール パネル」の「プログラムの追加と削除」にナビゲートします。
- アンインストール対象として「VolumeAgent」を選択します。
- プロンプトが出されたら、システムをリブートします。

1. PowerShell CLI を使用する場合

- msiexec/x <VolumeAgent.msi のパス>
- プロンプトが出されたら、システムをリブートします。

ボリューム/ポリシー・エージェントのアンインストール

このタスクについて

手順

1. Linux – root として実行します。
2. 保護されているディレクトリーをアンマウントします。
   - Unmount /dev/mapper/<e_volume>
3. spx-policyagent サービスを停止します。
   - CentOS 7 を使用している場合、以下を実行します。

   systemctl stop spx-policyagent
   - CentOS 6 を使用している場合、以下を実行します。

   service spx-policyagent stop
4. cd /opt/ibm/mde/spxagent/spx-hybridagent/
5. ./hybridagent_uninstall.sh
6. 「y」を入力して破壊アクションを確認します。
7. cd /opt/ibm/mde/spxagent/spx-policyagent/
8. ./policyagent_uninstall.sh
9. リブートします。
10. Windows – 管理者として実行します。

11. Windows GUI を使用する場合
    - 「コントロール パネル」の「プログラムの追加と削除」にナビゲートします。
    - 「HybridAgent」を選択してアンインストールします。
    - プロンプトが出されたらシステムをリブートします。
12. PowerShell CLI を使用する場合
    - msiexec /x <HybridAgent/msi へのパス>
    - プロンプトが出されたらシステムをリブートします。
    -

オブジェクト・ストア・エージェントのアンインストール

このタスクについて

エージェントが PPM から削除されない限り、すべてのユーザー・アカウントと権限は PPM に保管されたままになります。

手順

1. Linux – root として実行します。
2. spx-policyagent サービスを停止します。

   ```
   systemctl stop spx-objectagent
   ```
3. cd /opt/ibm/mde/spxagent/spx-objectagent
4. ./objectagent_uninstall.sh
5. 「y」を入力して破壊アクションを確認します。
6. cd /opt/ibm/mde/spxagent/spx-policyagent/
7. ./policyagent_uninstall.sh
8. リブートします。

MDE からのエージェントの削除

MDE によって管理されているエージェントを、MDE ユーザー・インターフェース (GUI) を使用してエコシステムから削除できます。

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

重要な注記

- MDE からエージェントを削除すると、エージェントが MDE に接続できなくなり、エージェントの次回の再始動時に現在保護されているデータにアクセスできなくなります。
- エージェントの削除によって、データは暗号化解除されません。

-

操作

製品データのバックアップとリストア

MDE は、MDE PPM データのポイント・イン・タイム・バックアップを実行する機能をサポートしています。このポイント・イン・タイム・バックアップをリストアして MDE をバックアップ収集時の状態に戻すことができます。

注記

バックアップまたはリストアを実行する前に、MDE VM で「systemctl stop spsd」コマンドを使用して MDE サービスを停止してください。

[admin@localhost]$ sudo systemctl stop spsd

製品データのバックアップ

このタスクについて

製品のバックアップは、MDE VM 内で実行されるコマンド・ライン・スクリプトによって行われます。

バックアップ・スクリプト spsd-backup は MDE VM の /opt/securityfirst/spsd/bin ディレクトリーにあります。このスクリプトによって自動的に新規ファイルが作成され、このバックアップ作成時のタイム・スタンプ付きの名前が指定されます。

[admin@localhost]$ sudo /opt/securityfirst/spsd/bin/spsd-backup --help

使用方法: spsd-backup [--nodb] [--help]

--nodb　　データベースをバックアップしない

--help　　このヘルプを表示する

バックアップを実行するには、次のようにします。

[admin@localhost]$ sudo /opt/securityfirst/spsd/bin/spsd-backup

ローカルのビルド情報をダンプしています

ローカルの spsd プロパティーをダンプしています

ローカルの PostgreSQL データベース a をダンプしています

完了 - spsd-backup-2017-04-04T144448-0700.tar.gz を作成しました (Done - created spsd-backup-2017-04-04T144448-0700.tar.gz)

製品データのリストア

このタスクについて

製品のリストアは、MDE VM 内で実行されるコマンド・ライン・スクリプトによって行われます。

リストア・スクリプト spsd-restore は /opt/securityfirst/spsd/bin ディレクトリーにあります。

[admin@localhost]$ sudo /opt/securityfirst/spsd/bin/spsd-restore --help

使用方法: spsd-restore [--nodb] [--noprops] [--help] FILE

--nodb　　データベースに書き込まない

--noprops　ローカル・プロパティーに書き込まない

--help　　このヘルプを表示する

リストアを実行するには、次のようにします。

[admin@localhost]$ sudo /opt/securityfirst/spsd/bin/spsd-restore spsd-backup-2017-04-04T144448-0700.tar.gz

注記

バックアップ・ファイルをリストアすると、MDE の次回の開始時に変更が適用されます。

カーネルの更新

このタスクについて

Red Hat Enterprise Linux 7 または CentOS 7 のオペレーティング・システムを実行するエージェントでカーネルを更新する必要がある場合は、以下のガイドラインに従ってください。

- OS/カーネルの更新が同じリリース内で行われる場合は、新規カーネルが自動的にサポートされます。
- OS/カーネルの更新によってリリースが上がる場合は (RHEL 7.2 から 7.4 になる場合など)、以下の手順を実行して新規カーネルのサポートを作成します。
  - 例: エージェントのインストール・バンドルが /root/agent に untar された場合

```
cd /root/agent/spx-installer
./agent/setup.sh -d /root/agent -k 1
リブート
```

これらの手順は、Red Hat Enterprise Linux 6 または CentOS 6 を実行するエージェントでは不要です。

アップグレード

MDE 製品を新規バージョンにアップグレードするには、以下の手順を実行します。

MDE サーバーの場合

このタスクについて

手順

1. root として PPM ポリシー・サービスを停止します。

   systemctl stop spsd
2. 以下を入力して MDE データをバックアップします。

   /opt/ibm/spsd/bin/spsd-backup
3. 新規バージョンの MDE bin ファイルを「/home/admin」ディレクトリーに移動します。
4. MDE bin ファイルへのアクセス許可を変更します。

   chmod +x /home/admin/ ibm_sw_mde_X.x.x-XX.bin
5. 新規バージョンの MDE bin ファイルを実行します。

   /home/admin/ibm_sw_mde_X.x.x-XX.bin
6. RPM をインストールします。

   yum -y install /home/admin rpms/*
7. アップグレード・スクリプトを実行します。

   /opt/ibm/spsd/bin/spsd-pgsetup --upgrade
8. 以下を入力して PPM ポリシー・サービスのバックアップをもう一度開始します。

   systemctl start spsd

前のバージョンからのアップグレード

このタスクについて

ポリシーが機能できるようにするには、以下のステップを実行する必要があります。

手順

1. 「エージェント情報」ページにナビゲートします。
2. 「マスター・ポリシーの編集」をクリックします。
3. 「保存、スナップショット作成、およびアクティブ化」をクリックします。
4. ジョブを承認します

5. エージェント VM に戻り、ポリシー内ディレクトリーに対して読み取り/書き込みアクションの実行を試み、そのディレクトリーに対する権限を持つポリシー内ユーザーとしてログインし、さらに、定義されていないユーザーに許可が与えられていないことを確認します。

エージェント・ターゲット VM の場合

Linux エージェント

このタスクについて

手順

1. 新規のエージェント・ディレクトリーを作成し、その新規エージェント・ディレクトリーに移動します。

   mkdir [agent_new_directory]

   cd [agent_new_directory]
2. それぞれのエージェントのインストール・バンドルをダウンロードするか、curl でダウンロードします。

   curl -k --header "Accept: application/x-tar" -u <*username*>:<*password*>https://<*PPM IP address*>/rest/agents/<*Agent ID #*>/install_bundle > <*install_bundle_name*>.tar
3. インストール・バンドルを untar します。

   tar xvf <install_bundle_name>.tar
4. setup.sh スクリプトを実行し、エージェントを再インストールします。

   ./setup.sh
5. プロンプトが出されたら、yes と応答してエージェントをリブートします。
6. 必要であれば、前のエージェント・ディレクトリーから前のインストーラー・ファイルをすべて削除できます。

   rm -rf [/previous Agent directory]

Windows エージェント

このタスクについて

手順

1. それぞれのエージェントのインストール・バンドルをダウンロードします。
2. インストール・バンドルを unzip します。
3. .msi インストーラーを実行して、新しいエージェント・ソフトウェアをインストールします。
4. プロンプトが出されたら、yes と応答してエージェントをリブートします。

サービス・データ

サービス・データの収集

サービス・データの収集は、MDE VM 内で実行されるスクリプトによって行われます。

spsd-service スクリプトは MDE VM の /opt/securityfirst/spsd/bin ディレクトリーにあります。

[admin@localhost]$ sudo /opt/securityfirst/spsd/bin/spsd-service –-help

使用方法: spsd-service [オプション]

オプション:

--nodb　　データベースをダンプしない

--norest　REST API からデータをプルしない

--nosys　　システム・データ (/var/log、/proc など) をプルしない

--withcore　spsd のコア・ダンプをプルインする

--help　　このヘルプを表示する

サービス・データの収集を実行するには、次のようにします。

[admin@localhost]$ sudo /opt/securityfirst/spsd/bin/spsd-service

PPM ログからの機密情報の削除

サービス・データが PPM の論理境界を超える場合に、PPM のインストール済み環境のプライバシーを保護できるように、以下の MDE デバッグ・ログでは、特殊なタグ構文を使用して、機密情報にタグが付けられます。

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

注**:** これらのログは、サービス・データの tarball (前述のサービス・データ収集プロセスで作成されるもの) 内の logs フォルダーに作成されます。

タグの形式は #<tagname>(<tagdata>) です。ここで <tagdata> はタグ付け対象データに置き換えられ、<tagname> は以下のいずれかになります。

- user - ユーザー名にタグ付けする場合。MDE ユーザーまたは MDE の統合先外部サービスのユーザーのいずれか。*例: #user(admin)*
- group - グループ名にタグ付けする場合。*例: #group(domainusers)*

- email - E メール・アドレスにタグ付けする場合。*例: #email (example@example.com)*
- ip - IP アドレスにタグ付けする場合。*例: #ip(192.168.0.5)*
- host - ネットワーク・ホスト名にタグ付けする場合。*例: #host(dns.example.com)*
- key - 公開暗号化鍵または関連する値 (管理対象鍵名など) にタグ付けする場合。*例: #key(HRKey2)*
- cert - 証明書データ (接続元エージェントの識別名など) にタグ付けする場合。*例: #cert(C=US, ST=UT, L=Provo, O=Example Corp., OU=architecture, CN=docserver4)*
- fingerprint - 証明書のフィンガープリントにタグ付けする場合。*例: #fingerprint(41:1A:B9:89:DB:77:90:77:39:D0:DF:5E:98:90:B7:17)*

サービス・データからタグを削除するには、以下の例のようなプロセスを使用します。この例のプロセスは、#user タグが付いたデータを bundleAll.log から削除します。

```
[admin@localhost]$ gunzip spsd-service-2018-01-24T141620-0800.tar.gz
[admin@localhost]$ tar xf spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
[admin@localhost]$ sed -i '/¥#user/c¥REDACTED' logs/bundleAll.log
[admin@localhost]$ tar --delete --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
[admin@localhost]$ tar --append --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
[admin@localhost]$ gzip spsd-service-2018-01-24T141620-0800.tar
```

付録 A. サンプルのエージェント・インストール・プロセス

以下のセクションでは、エージェント・インストール・バンドルの一般的なインストール・プロセスの概要を示します。これらは方法の例にすぎず、サポートされているインストール手順ではありません。

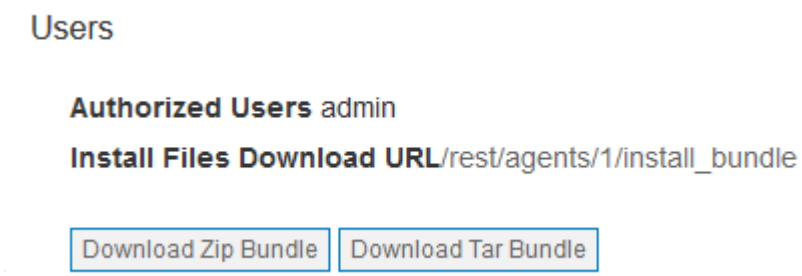
Red Hat / CentOS のプロセス

このタスクについて

CURL によるインストール・バンドルの転送

手順

1. ターゲット・システムにログインします。
2. MDE サーバーとの有効なネットワーク接続を確認します。
3. ポリシーに指定されているすべてのユーザー、グループ、およびパスまたはデバイスが作成されており、システムに接続されて構成されていることを確認します。
4. MDE にログインします。
5. MDE 内で、ターゲット・システムに対してエージェントをプロビジョニングします。
6. MDE 内で、エージェントの詳細を表示してダウンロード URL をメモします。



7. ターゲット・システムから、エージェントのダウンロード用のディレクトリーを作成し、そのディレクトリーに移動します。
8. 次の curl コマンドを使用して tar バンドルをダウンロードします。

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

   PPM 定義ユーザーを使用した例:

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

PPM LDAP 定義ユーザーを使用した例:

[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

*(*ディレクトリー *ID* が「*tenant1*」、ユーザーが「*john*」、パスワードが「*secret*」であると想定*)*

9. ターゲット・システムから、パッケージを untar します。

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

10. ターゲット・システムから、セットアップ・スクリプトを root として実行します。

    [user@localhost]$ ./setup.sh

11. セットアップ・スクリプトが完了すると、エージェントがインストールされ、ポリシーが MDE からダウンロードされて適用されます。

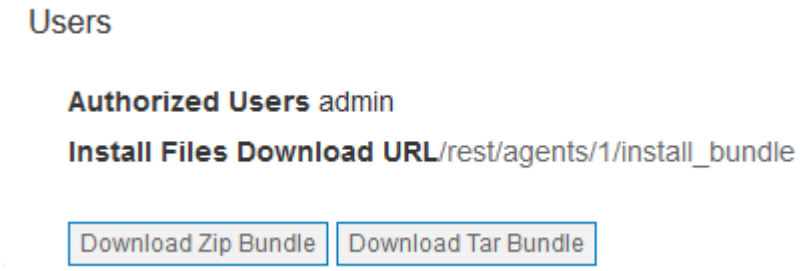
Windows Server のプロセス

このタスクについて

インストール・バンドルの転送

手順

1. ターゲット・システムにログインします。
2. MDE サーバーとの有効なネットワーク接続を確認します。
3. ポリシーに指定されているすべてのユーザー、グループ、およびパスまたはデバイスが作成されており、システムに接続されて構成されていることを確認します。
4. MDE にログインします。
5. MDE 内で、ターゲット・システムに対してエージェントをプロビジョニングします。
6. MDE 内で、エージェントの詳細を表示してダウンロード URL をメモします。



7. 「Zip バンドルのダウンロード」をクリックして、エージェント・ソフトウェアの zip ファイル・バンドルをローカル・システムにダウンロードします。
8. インストール・バンドルをターゲット・システムに転送します。
9. ターゲット・システムで、zip ファイル・バンドルのコンテンツを解凍します。
10. インストール・バンドルの msi ファイルを実行します。

    FileAgent-<version>.msi

    例:

    PS C:¥> FileAgent-4.2.11-0030.msi
11. セットアップ・スクリプトが完了してエージェントが正しくインストールされると、ポリシーが適用されます。

    注**:** リブートが必要です。リブート要求プロンプトをバイパスするには、以下のようにリブートなしオプションを指定してコマンドを実行します。**msiexec /i <agent_filename_version.msi> NO_REBOOT_PROMPT=1**

付録 B. サンプルの認証局 (CA) 証明書

このタスクについて

MDE では、管理サーバー (PPM) とエージェント間のセキュア・セッションを確立するために、認証局が署名した証明書が必要になります。これには以下が必要です。

- 鍵ストア
- トラストストア
- CA 証明書バンドル

証明書への署名には、社内の RSA ベースの認証局またはサード・パーティー認証局を使用できます。下記の Linux のサンプルでは、以下の項目が作成されます。

- 証明書署名要求 (CSR) が作成され、認証局に送信されて署名を受けます。署名された証明書と鍵を結合して鍵ストアが作成されます。
- 認証局の証明書バンドルを使用してトラストストアが作成されます。
- エージェント証明書が作成されます。これらの証明書は、PPM とエージェントの間の通信に必要です。

このサンプルは便宜的に用意されたものです。署名を受ける証明書を生成するときは、ご使用の認証局に従ってください。大括弧で囲まれた名前 [name.pem] はファイル名を表しますが、これは会社の証明書やサード・パーティーの証明書を使用する場合には、異なっていたり変更されていたりする可能性があります。

鍵ストアを作成するには、CSR を社内の認証局またはサード・パーティーの認証局に送信する必要があります。

手順

1. 以下の情報を含む OpenSSL 構成ファイル (ppm.cnf) を作成します。

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

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

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

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

[req_distinguished_name] および [alt_names] の各セクションは、組織の情報に合わせて更新する必要があります。

2. PPM CSR を作成します。

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

3. CSR [csr.pem] は認証局 (CA) の署名を受ける必要があります。
4. 署名済みの証明書を CA から受け取ったら、拡張鍵用途とサブジェクト代替名が含まれていることを確認します。

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

5. 署名済み証明書と鍵 (ステップ 2 の鍵) を結合します。

```
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
```

トラストストアを作成するには、認証局が CSR への署名に使用する、認証局の証明書が必要です。これは、CA 証明書バンドルとも呼ばれます。以下の「ca_bundle.crt」を、この証明書の実際の名前に置き換えてください。

a. 認証局 (CA) 証明書バンドルを使用してトラストストアを作成します。CA 証明書バンドル内に複数の証明書がある場合は、それらを分割してトラストストアに個別にインポートする必要があります。

```
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. 結果として得られた *.jks ファイルと [ca_bundle.crt] ファイルを PPM サーバーのセキュア・ディレクトリー (すなわち、/etc/ppm/certs) 内にコピーします。この場所は、spsd-certsetup スクリプトを使用して Web およびエージェントのプロパティー・ファイルを更新するときに指定されます。(以下の『管理サーバーのセットアップ』を参照してください。)

MDE エージェントの証明書も必要です。

a. 以下の情報を含む OpenSSL 構成ファイル (host01.cnf) を作成します。

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

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

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

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

[reg_distinguished_names] および [alt_names] の各セクションは、組織の情報に合わせて更新する必要があります。

b. MDE エージェントの CSR を作成します。

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

c. 認証局 (CA) が署名した CSR を要求します。

d. 署名済みの証明書を CA から受け取ったら、拡張鍵用途とサブジェクト代替名が含まれていることを確認します。

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

e. エージェント証明書の署名が PPM 証明書とは異なる CA によって行われている場合は、CA_bundle 証明書を PPM トラストストアにインポートする必要があります。前述の PPM 証明書作成プロセス (CSR) のステップ 5 を参照してください。

f. 署名済み証明書と鍵を結合します。

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

g. MDE でこのホストのエージェントを作成するときに、この [host01.pem] 証明書/鍵のペアを使用します。

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

[host01.pem] をご使用のワークステーションまたは共有リソースにコピーし、PPM エージェントの作成中にアクセスできるようにします。

エージェントをインストールする各ホストに対してこのプロセスを実行します。

管理サーバーのセットアップ

管理サーバーのセットアップでは、ポリシー・エージェントの構成前に証明書を更新しておく必要があります。そのためには、会社の鍵ストアとトラストストアおよび CA 証明書バンドルのアップロード後に、提供されたスクリプト (/opt/securityfirst/spsd/bin/spsd-certsetup) をそのサーバーで実行する必要があります (「管理者ガイド」の『サーバー証明書の設定』セクションを参照)。また、spsd サービスの再始動または管理サーバー (PPM) のリブートも必要です。この操作を行わないと、エージェントが MDE 管理サーバーと通信できなくなります。

証明書が更新されておらず、エージェントは構成済みである場合、証明書更新スクリプトを実行してから「エージェント情報」ページでエージェント証明書を更新すると、エージェントと MDE 管理サーバーの間の通信が復元されます。

付録 C. PKCS12 ファイルを作成するための変換のサンプル

このタスクについて

以下の手順を使用して、クライアント秘密鍵とクライアント証明書を単一の PKCS12 (Public Key Cryptography Standard #12) ファイルに結合します。

```
[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
```

付録 D. 実行する操作と実行してはならない操作

割り当てられている鍵の変更

概要

保護されているディレクトリーにデータがあり、そのディレクトリーに関連付けられている鍵を変更する必要があるとします。

背景

ディレクトリー内のデータは、データ作成時 (またはそのディレクトリーへの移動時) に定義された鍵によって暗号化されています。ポリシーの鍵を変更した場合、既存のデータは新しい鍵に移行されません。

ポリシーがエージェントに適用されておりアクティブになっている場合、保護されているディレクトリーの鍵値を変更するのは非常に危険である可能性があります。完全に禁止されてはいませんが、鍵値を変更するとデータ損失を招く可能性があります。

実行

管理者が 1 つの鍵から別の鍵にディレクトリー全体を移行することを希望する場合は、まずデータをそのディレクトリーから移動する必要があります。ディレクトリーが空になったら、ポリシーによって関連付けられている鍵値を変更して適用できます。その後で、データをそのディレクトリーに戻すと、新しい鍵を使用してデータが暗号化されます。

実行してはならない操作

最初にディレクトリーからデータを移動することなく、ポリシーに関連付けられている鍵値を変更してポリシーをアクティブ化することは行わないでください。ベスト・プラクティスの手順に従わなかった場合、ディレクトリー内にもともと存在していたデータが引き続き元の鍵で暗号化されます。新しい鍵へのポリシーの変更を行うと、データがアクセス不能になります。また、元の鍵がローテーションされている場合、ポリシーを元の鍵値に戻す方法がないため、データが永久にアクセス不能になります。

暗号化バックアップでの鍵のローテーション

概要

保護されているディレクトリーのデータをバックアップする必要があるとします。

背景

暗号化形式のバックアップ・データでは、バックアップ時にデータが鍵値に関連付けられます。バックアップ操作を実行した後で鍵がローテーションされている場合は、適切にリストアできません。

鍵をデータにではなく保護されている場所に関連付ける必要があります。これにより、リストア時に意図しないデータ・アクセスの問題が発生しません。

実行

ディレクトリー内のデータは、データ作成時 (またはそのディレクトリーへの移動時) に定義された鍵によって暗号化されています。データをバックアップするには、バックアップ・プロセス前 (またはバックアップ・プロセス中) に、保護されているディレクトリーのデータを保護されていない領域にコピーすることをお勧めします。保護されているディレクトリーのデータをコピーすると、データは暗号化解除されます。別の保護されているディレクトリーをバックアップ場所に指定できるため、データが保護されないのはバックアップ操作中のみになります。

実行してはならない操作

保護されているディレクトリーをその暗号化形式でコピーしないでください (ディスク・イメージ、VM スナップショットなど)。これを行った場合、元の鍵がローテーションされると、データがアクセス不能になります。

付録 E. 暗号化の実施

既存のディレクトリー構造およびデータの暗号化を可能にし、いつでもデータの状況の判別を行えるようにするために、MDE には「spxconvert」というコマンド・ライン・ユーティリティーが用意されています。

この機能は、既存のデータを暗号化できるだけでなく、Payment Card Industry (PCI) や医療保険の積算と責任に関する法律 (HIPAA) などの監査を実行する場合にも役立ちます。

この機能は、ファイル/ポリシー・エージェントでのみ機能し、正式なデータ・マイグレーションを必要とするボリュームは対象外です。

注記

この機能は、ファイル・エージェントでのみ機能し、正式なデータ・マイグレーションを必要とするボリュームは対象外です。

コマンド・オプション

spxconvert の使用法: (パラメーターは大括弧 [ ] で示され、タイプが含まれています)

-h (-?, ?) 「このヘルプ・ダイアログを印刷する」

-a 「暗号化されたファイル監査の実行」

-p [STR] 「監査パス」

-e [STR] 「パス内の無保護のファイルを暗号化」

-c 「ファイル変換の前/後のすべてのチェックサムをダンプ」

-v 「詳細 - 追加情報の追加出力」

監査 (-a)

デフォルトでは、監査はポリシー・ディレクトリー内のすべてに対して実行されます。-p オプションを使用して、これを単一のディレクトリーに絞り込むことができます。監査により、暗号化されていないディレクトリーのファイルがすべて出力され、暗号化されたディレクトリー内のファイル総数に対するファイル数が出力されます。

暗号化 (-e)

指定されたディレクトリー内の無保護のファイルを変換します。完了すると、チェックサムが一致しないファイルがユーザーに表示されます。オプションの -c フラグを指定すると、完了時に、矛盾するファイルだけでなく、すべてのファイルのチェ

ックサムを出力します。変換後にシステム・キャッシュをフラッシュする必要があるため、チェックサムが出力できるのは、パフォーマンスの完了時のみです。各ファイルの後にキャッシュをフラッシュすると、パフォーマンスに多大な悪影響を与えます。

監査の手順

1. 以下を実行して、暗号化が保留の項目があるかどうかを表示します。

spxinfo -l

1. 以下を実行して、データに関する詳細情報を表示します。

spxconvert -a -v

1. 以下を実行して、特定のディレクトリーに関する詳細情報を表示します。

spxconvert -p -v <*path*>

暗号化の手順

1. 以下を実行して、暗号化が保留の項目を表示します。

spxinfo -l

1. 以下を実行して、暗号化前のチェックサムをすべて表示します。

spxconvert -c -p <*path*>

1. 以下を実行して、特定のパスにあるすべてのファイルを暗号化します。

spxconvert -p -v <*path*>

1. 以下を実行して、暗号化後の特定のパス上のチェックサムをすべて表示します。

spxconvert -c -p <*path*>

付録 F. エージェントのデバッグ・ロギング

デフォルトでは、ポリシー・エージェントは、デバッグ・レベル・メッセージをロギングから除外して作動します。エージェントのログにデバッグ・レベル・メッセージをキャプチャーするには、エージェントのシステム管理者がその機能を有効にしてから、デバッグ・レベル・メッセージのキャプチャーを開始するためにエージェントを再始動する必要があります。

有効な値は 1 から 6 です。ただし、デフォルト値は「4」であり、「4」より小さい値を設定すると、有用な情報が省略される場合があります。

重要な注記

- デバッグ・レベル・ロギングを有効にすると、機密性の高いシステム情報が開示される可能性があります。
- デバッグ・メッセージングの性質上、エージェント・ログ・ファイルのファイル・サイズが大幅に増加する場合があります。

Linux エージェント

このタスクについて

/etc/sysconfig/spx-policyagent にある構成ファイルを見つけてデバッグを有効にし、書き込み可能フラグ (**chmod +w /etc/sysconfig/spx-policyagent**) を設定します。

ファイルの末尾に引用符なしで「**LOG_LEVEL=6**」を付加します。

Windows エージェント

このタスクについて

HKLM¥SYSTEM¥CurrentControlSet¥Services¥Spx Policy Agent¥log level にあるレジストリー・キーを見つけてデバッグを有効にし、値を「**6**」に設定します。

付録 G. 用語集

用語	定義
Advanced Encryption Standard New Instructions (AES-NI)	2001 年に米国連邦情報・技術局 (NIST) によって確立された電子データの暗号化の仕様。SPx ベースの製品で使用される暗号化プロトコル。
エージェント (Agent)	Security First の暗号化とアクセス制御ソフトウェアを実行する、管理対象サーバー。
アマゾン ウェブ サービス (Amazon Web Services) (AWS) S3	データの格納と取得を行う、拡張性が高く安価な簡素ストレージ・サービス。
自動生成鍵 (Auto-Generated Key)	MDE によって作成されて管理されるポリシー実施鍵。これらの鍵は、ポリシー作成時に鍵の自動生成によって示される。
認証局 (Certificate Authority)	デジタル証明書に署名するために信頼されている組織。CA は、実行依頼された認証要求の識別情報と正当性を検査する。要求の検査が成功すると、CA は署名付き証明書を発行する。
証明書失効リスト (Certificate Revocation List、CRL)	対応する証明書を発行した認証局 (CA) によって取り消された証明書の公開リスト。
証明書失効リスト配布ポイント (Certificate Revocation List Distribution Point、CRLDP)	発行元 CA によって取り消された証明書に関する情報 (名前、オプションで取り消し理由、および CRL 発行者名を含む) を保持する、証明書内の開始点フィールド。
Cloud Auditing Data Federation (CADF)	Security Information and Event Management (SIEM) システムに転送される共通イベント・フォーマット構文タイプ。
Comma Event Format (CEF)	Security Information and Event Management (SIEM) システムに転送される共通イベント・フォーマット構文タイプ。
コンマ区切り値 (Comma Separated Value、CSV)	コンマをフィールド区切り文字として使用し、改行をレコード区切り文字として使用するデータ・フォーマット。
コマンド・ライン・インターフェース (Command Line Interface、CLI)	ユーザーがアプリケーションに対してコマンドをテキスト行の形式 (コマンド・ライン) で発行する対話のタイプ。
協定世界時 (Coordinated Universal Time、UTC)	全世界で時計と時刻を調整するために使用されている、主要な 時刻標準。
暗号化アクセス制御 (Cryptographic Access Control)	さまざまな暗号化の素材を使用することでユーザー・アクセスを分離する機能。

CURL	CURL は、さまざまなプロトコルを使用してデータを転送するためのライブラリーおよびコマンド・ライン・ツールを提供するコンピューター・ソフトウェア・プロジェクトである。
識別エンコード規則 (Distinguished Encoding Rules、DER)	DER は、ITU-T X.690, 2002 仕様で定義されている ASN.1 エンコード規則の 1 つである。データ構造に対するエンコード規則は、ストリーム内のバイトをコンピューター間で送信するときの編成方法を制御する転送構文を提供する。
ドメイン・ネーム (Domain Name、DN)	全世界的に固有であり IP 宛先情報に関連付けられている、インターネット・リソース名。
ドメイン・ネーム・サービス (Domain Name Service、DNS)	ドメイン・ネームを IP アドレスに変換するインターネット・サービス。
動的ホスト構成プロトコル (Dynamic Host Configuration Protocol、DHCP)	インターネット・プロトコル (IP) ホストに対して、その IP アドレスおよびその他の関連する構成情報 (サブネット・マスク、デフォルト・ゲートウェイなど) を提供する、クライアント/サーバー・プロトコル。
ファイル・エージェント (File Agent)	ファイル・エージェントは、ファイル・ベース操作のアクセス・ポリシー定義および 1 つ以上の保護ファイル・パスの関連付けを実施する。各保護ファイル・パスに固有の操作アクセス制御と暗号化アクセス制御を設定することが可能。
グラフィカル・ユーザー・インターフェース (Graphical User Interface、GUI)	テキスト・ベースのインターフェースと入力したコマンドではなく、グラフィカルなアイコンを使用してユーザーが MDE と対話できるようにするタイプのユーザー・インターフェース。
医療保険の積算と責任に関する法律 (Health Insurance Portability and Accountability Act、HIPAA)	HIPAA プライバシー規定では、プロバイダーと組織が保護医療情報 (PHI) の機密性とセキュリティーを確保することを求めている。
高可用性 (High Availability、HA)	冗長性 (予備電源装置、CPU、ドライブ、ソフトウェアなど) により、コンポーネントに障害が発生した場合でもシステム操作を続行。
Hypertext Transfer Protocol (HTTP)	World Wide Web でのデータ通信の基盤となっているアプリケーション・プロトコル。

ハイパーバイザー (Hypervisor)	仮想マシン・モニターとも呼ばれる。ハイパーバイザーまたは仮想マシン・モニター (VMM) は、仮想マシンを作成、実行、および管理するコンピューター・ソフトウェア、ファームウェア、またはハードウェアの一部である。ハイパーバイザーが 1 つ以上の仮想マシンを実行しているコンピューターはホスト・マシンと呼ばれ、各仮想マシンはゲスト・マシンと呼ばれる。また、VMware ハイパーバイザーは ESXi Host と呼ばれる。
IBM Cloud Object Storage (COS S3)	バックアップ、アーカイブ、ビデオ・ファイル、イメージ・ファイルなどの大容量のデータを保持し、保存データと高可用性の機能を提供するストレージ・プラットフォーム。
初期設定ベクトル (Initialization Vector、IV)	データ暗号化で秘密鍵とともに使用できる、セッションで一度だけ使用される任意または予測不能の乱数。
Java 鍵ストア (Java KeyStore、JKS)	Java 鍵ストア (JKS) は、セキュリティー証明書 (許可証明書または公開鍵証明書のいずれか) とそれに対応する秘密鍵のリポジトリーである。Java Development Kit (JDK) には、鍵ストア内の鍵および証明書を管理するツール (keytool) が用意されている。jks 拡張子は、Java 固有のファイル・フォーマットである。
鍵の取り消し (Key Revocation)	エージェント環境からのポリシー実施鍵の削除であり、暗号データ・アクセス制限はリカバリー可能である。このアクションにより、データが一時的に読み取り不能になる。
鍵のローテーション (Key Rotation)	エージェント環境内でのポリシー実施鍵の移行であり、データ・アクセスに対するユーザー側からは見えない変更である。
鍵の廃棄 (Key Shredding)	エージェント環境からのポリシー実施鍵の削除であり、暗号データ・アクセス制限はリカバリー不能になる。このアクションにより、データが永久的に読み取り不能になる。
鍵ストア (Keystore)	ポリシー実施鍵の構成された保管場所。
Lightweight Directory Access Protocol (LDAP)	分散されたディレクトリーの情報をネットワーク経由でアクセスおよび保守するための、ベンダーに依存しないオープンな業界標準プロトコル。このソフトウェア・プロトコルを使用すると、ユーザーがネットワーク内の組織、個人、およびその他のリソース (ファイル、デバイスなど) を見つけることが可能。

Log Event Extended Format (LEEF)	LEEF は、IBM Security QRadar 用にカスタマイズされたイベント・フォーマットであり、QRadar の簡単に処理される読み取り可能イベントを含む。このフォーマットでは、イベント・ペイロードに対していくつかの事前定義イベント属性がサポートされている。
論理ボリューム・マネージャー (Logical Volume Manager、LVM)	デバイス・マッパー Linux カーネル・フレームワークを使用して複数のストレージ・デバイスをグループ化し、必要に応じて結合スペースから論理装置を割り振るストレージ・デバイス・マネージャー。ほとんどの Linux ディストリビューションは LVM 対応である。
M of N (M:N)	作成されたデータの断片 (共有) 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) を決定するモデル。
NT ファイル・システム (NT File System、NTFS)	Windows NT オペレーティング・システムで Microsoft により開発され、ファイル・レベルのセキュリティー、圧縮、および監査をサポートするハード・ディスクでのファイルの保管および検索に使用される専有ファイル・システム。
Network Time Protocol (NTP)	コンピューター・システム間で刻時同期を行うためのネットワーク・プロトコル。
オブジェクト ID (Object Identifier、OID)	グローバルに一義的な永続名を使用して、オブジェクトまたは概念を命名するための ID 標準化メカニズム。
オブジェクト・ストア・エージェント (Object Store Agent)	オブジェクト・ストア・エージェントは、送信するデータを暗号化し、分割して、拡張性が高く効率的なオブジェクト・ストレージ (クラウド、オンプレミス、またはその両方) に安全に格納する。
オンライン証明書状況プロトコル (Online Certificate Status Protocol、OCSP)	X.509 デジタル証明書の失効状況を取得するために使用される内部プロトコル。
Open Virtualization Archive (OVA)	tar アーカイブ・ファイル。すべての OVF ファイルが単一ファイルに zip されるか、圧縮されるか、またはその両方が行われたもの。
Payment Card Industry (PCI)	不正を削減するためにカード所有者のデータの制御とセキュリティーを強化する規格。
PEM	X.509 v3 標準によって定義されている構文とコンテンツを使用したセキュリティー証明書用に広く使用されているエンコード形式。

PostgreSQL	PostgreSQL (発音は「post-gress-Q-L」) は、ボランティアの世界的なチームが開発したオープン・ソースのリレーショナル・データベース管理システム (DBMS) である。PostgreSQL は、どの企業や他の民間団体によっても管理されず、ソース・コードは無料で使用可能。
保護されています (Protected)	処理されているデータ。
Public Key Cryptography Standard #12 (PKCS12)	多数の暗号化オブジェクトを単一ファイルとして保管するためのアーカイブ・ファイル・フォーマットを定義する公開鍵暗号規格。一般に、秘密鍵をその X.509 証明書にバンドルしたり、トラスト・チェーンのすべてのメンバーをバンドルしたりするために使用される。暗号化と署名が可能。
公開鍵基盤 (PKI)	デジタル証明書の作成、管理、配布、使用、保管、取り消し、および公開鍵暗号化の管理に必要なロール、ポリシー、およびプロシージャーのセット。
ReFS	Windows Server 2012 で導入され、データの可用性、拡張容易性、およびデータ保全性を最大化するように設計された Microsoft の新しいファイル・システム。
Representational State Transfer アプリケーション・プログラム・インターフェース (Representational State Transfer Application Program Interface、REST API)	RESTful API (RESTful Web サービスとも呼ばれる) は、Representational State Transfer (REST) テクノロジー (Web サービス開発でよく使用される通信に対するアーキテクチャー・スタイルとアプローチ) に基づいている。
ロール・ベースのアクセス制御 (Role Based Access Control、RBAC)	企業内の個々のユーザーのロールに基づいてコンピューターまたはネットワーク・リソースへのアクセスを規制する手法。このコンテキストでは、アクセスとは、個々のユーザーがファイルの表示、作成、変更などの特定のタスクを実行できること。
RSA	公開鍵と秘密鍵を使用してデータを保護する、Rivest、Shamir、および Adelman (RSA) によって開発された公開鍵暗号方式。
セキュア・コピー・プロトコル (Secure Copy Protocol、scp)	scp コマンドは、セキュア・シェル (SSH) プロトコルを介してシステム間でファイルを転送するために Linux で使用される。
Secure Socket Layer (SSL)	対称鍵を交換するために非対称鍵を使用して、インターネットを介したデータ通信を暗号化する暗号プロトコル。証明書と所有者の検査、および証明書の生成、署名、その有効期間の管理を可能にするためには、認証局および公開鍵のインフラストラクチャーが必要である。

Secure Socket Shell (SSH)	リモート・コンピューターにアクセスするためのセキュアな方法を管理者に提供するネットワーク・プロトコル。また、SSH は、このプロトコルを実装するユーティリティーのスイートも指す。
セレクター (Selector)	データ、パス・セット、およびその他のポリシー関連機能にアクセスできる、OS 定義のユーザーおよびグループ。
Transport Layer Security (TLS)	コンピューター・ネットワークを介した安全な通信を提供する暗号プロトコル。
トラストストア (Truststore)	トラストストアは、SSL 接続のサーバーによる証明書の検査に使用される、信頼できる認証局 (CA) からの証明書を保管する。
固有 ID (Unique Identifier、UUID)	Universally Unique Identifier (UUID) は、ソフトウェア構築に使用される ID 標準のこと。UUID (128 ビット値) は、インターネット上のオブジェクトまたはエンティティーを一意に識別するために使用される。
仮想マシン (Virtual Machine、VM)	実際のコンピューターまたは仮想コンピューターのコンピューター・アーキテクチャーと機能に基づいた、コンピューター・システムのエミュレーション。
VMware ESXi™	実際のコンピューターまたは仮想コンピューターのコンピューター・アーキテクチャーと機能に基づいた、特定のコンピューター・システムのエミュレーション。
ボリューム・エージェント (Volume Agent)	ボリューム・エージェントは、ターゲット・システム上でボリューム・ポリシー定義および 1 つ以上の保護ボリュームの関連付けを実施する。
ボリューム/ポリシー・エージェント (Volume with Policy Agent)	このエージェントは、ボリューム・エージェントのボリューム・ポリシー保護を利用し、1 つ以上の保護ファイル・パスに対してファイル・ベース操作のアクセス制御ポリシーを適用および施行できるようにする。ハイブリッド・エージェントとも呼ばれる。

特記事項**[r]**

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 U.S.A.

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。

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。

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。本書をご覧になる方法によっては、一部の画像や図が表示されない場合があります。

商標**[r]**

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 **[r]**

これらの資料は、以下の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**[r]**

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。

プロダクト番号: 5737-C67

Printed in the USA

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