

IBM Multi-Cloud Data Encryption
Powered by SPx[®]
バージョン 2.2

リリース・ノート

IBM

IBM Multi-Cloud Data Encryption
Powered by SPx[®]
バージョン 2.2

リリース・ノート

IBM

注記

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

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。

© Copyright Security First Corp. 2018

© Copyright International Business Machines Corporation 2018

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
Release Notes

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

リリース・ノート	1	バージョン 1.0.1-2 - 日付: 2017 年 3 月 3 日 . . .	12
バージョン 2.2 - 日付: 2018 年 5 月 25 日 - 改訂:		特記事項	15
2018 年 6 月 4 日	1	商標	17
バージョン 2.1.0.2 - 日付: 2018 年 3 月 23 日 . . .	3	製品資料に関するご使用条件	17
バージョン 2.1.0.1* - 日付: 2018 年 1 月 5 日 . . .	5	プライバシー・ポリシーに関する考慮事項	18
バージョン 2.1.1-1 - 日付: 2017 年 9 月 28 日 . . .	7		
バージョン 1.0.1-3 - 日付: 2017 年 3 月 24 日 . . .	11		

リリース・ノート

バージョン 2.2 – 日付: 2018 年 5 月 25 日 – 改訂: 2018 年 6 月 4 日

リリースの特色

- オブジェクト・ストア・エージェント (OSA)。
- Linux ポリシー・エージェントについて、切り替え可能な「su」のブロックが追加されました。
- すべてのポリシー・エージェントに対してポリシー中断オプションが追加されました。
- 保護データのバックアップ/リストア・ツールが追加されました。

解決された問題

以前のリリース以降に解決された既知の問題は以下のとおりです。

- Windows エージェント用のポリシー・パスを含むプロセスで、大/小文字の区別がなくなりました。
- パス・セット・ポリシー・オブジェクトを使用してポリシー・スナップショットを更新する機能が修正されました。
- Firefox および Internet Explorer における Policy Provisioning Manager (PPM) のタイムアウトに関する問題が解決しました。
- ダッシュボードのイベント・グラフが正しく表示されない問題。

必要なアクション

以前のリリースの必須アクションに加えて、以下のアクションを行います。

- RedHat/CentOS 7 システム上で実行されるファイル/ポリシー・エージェントのアップグレード時に、以前のソフトウェアの完全な削除を要求するパッチが実装されました。ソフトウェアがアンインストールされ、システムがリブートされたら、新しいエージェント・ソフトウェアの通常インストールに従ってください。

注: このプロセス中は、すべての保護データが暗号化状態のままになります。ただし、アクセス・ポリシーは適用されません。このプロセス中は、アップグレードの完了後にポリシーを適用できるようになるまで、データが変更されないことが重要です。

- Unicode 文字は、パーセントでエンコードされた形式に変換されるため、パーセントでのエンコードで拡張されてもファイル・パスの長さが 250 文字を超えないことを確認してください。
- OSA の構成プロセスは、他の使用可能なエージェントと同じですが、以下の点が異なります。
 - エージェントは、ローカル構成のポリシーを使用し、その後、ポリシーは PPM に格納されます。ポリシーのスナップショットは、OSA では使用できません。

- エージェントが正常に動作するには、「ツール鍵」が割り当てられている必要があります。これは、エージェントの作成中、またはその後の構成中に割り当てることができます。
- OSA のデプロイ後に以下の操作を行う必要があります。
 - /etc/spx-osa ディレクトリーの spx-osa.conf ファイルを変更して、REST API 通信用の SSL 証明書を指定する必要があります。
 - エージェントからオブジェクト・ストアへの通信を保護するために、REST API 用の SSL 証明書を指定する必要があります。これは、PPM からエージェントへの通信に使用される証明書とは別のものです。
 - 構成ファイルで証明書を指定し、その証明書をエージェント・システムにインストールしたら、サービスを再始動します。
 - 新しく使用できるようになったコマンド・ライン・ユーティリティー `spxobject` を使用すると、エージェント・ポリシーの構成 (M:N、共有エンドポイント URL、ローカル・アカウント、および許可の設定など) を実行できます。
 - 共有には、オブジェクト・ストア・アカウントの API アクセスと秘密鍵が必要です。
 - 各共有の `-auth` は、それぞれのクラウド・サービスに相関する必要があります (例: Amazon AWS S3 = `S3_AMAZ4`)
 - エンド・ユーザーは、構成で指定されたローカル・アカウント ID と鍵のみを使用して操作を行います。
 - ほとんどのユーティリティーでは、ローカル・アカウントの `-auth` タイプに「`S3_AMZ4`」を使用する必要があります

既知の問題

以前のリリースの既知の問題に加えて、以下の問題があります。

- OSA では、250 文字を超える長さのファイル名を持つオブジェクトのアップロードに失敗します。
- OSA では、マルチパート・アップロードがサポートされません。
- CloudBerry S3 ユーティリティーを使用した、括弧文字を含む名前のファイルの OSA へのアップロードは正常に実行されません。それらの文字を削除するか、異なるアプリケーションを使用してください。
- OSA では、v4 署名のハッシュ処理が原因で、Minio MC ユーティリティーがサポートされません。
- OSA が管理するオブジェクト・ファイルの S3 ユーティリティーを使用した名前の変更はサポートされません。
- OSA ローカル・クラウド・アカウント構成をリストすると、エンドポイント URL 列に誤って「Bucket」と表示されます。
- `spxobject` コマンド・ラインのヘルプで、正しくない `-ac` コマンド入力に対して、誤って `-ag` とリストされます。
- Linux ポリシー・エージェント上の `spxbackup/spxrestore` コマンド・ユーティリティーで、使用できないフラグである `-P`、`-f`、および `-c` のヘルプがリストされます。
- `spxobject -m:n` を実行すると、限定的な成功/失敗メッセージが返されます。

- `fstab` にマウントされている iSCSI ディスクがある場合、Linux ファイル・エージェントが、誤って `/etc/fstab` 内の LVM を変更します。ポリシー・エージェントのインストール前に、`fstab` にマウントされている iSCSI ディスクがないことを確認してください。
- ユーザー・ロールの変更時に、PPM ユーザー管理イベントが正しく報告されません。
- ユーザー・パスワードの変更時に、PPM ユーザー管理イベントが正しく報告されません。
- 新しいユーザーの作成時に、PPM ユーザー管理イベントが正しく報告されません。
- 一部のイベント・ログ・メッセージが、PPM ダッシュボードに表示されないか、正しく表示されません。

バージョン 2.1.0.2 – 日付: 2018 年 3 月 23 日

リリースの特色

- セキュリティー強化
 - ホスト証明書の検証
 - アカウントのログイン試行失敗によるロックアウト
- サーバーのパフォーマンス向上
 - REST 呼び出しの改善
 - データベース処理の最適化
- ロギング・メッセージの改善とクリーンアップ
- ジョブ承認の分離
- 管理サーバーの非対話式インストール
- エージェントの保護ディレクトリーの保存リスト

解決された問題

以前のリリース以降に解決された既知の問題は以下のとおりです。

- Windows 版のボリューム・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、4096 より小さいディスク割り振りサイズをサポートできます。
- Windows ファイル・エージェントで、DB2 データベースと PostgreSQL データベースをサポートできます。
- 重複する管理ユーザー名を作成できません。これを試行するとジョブが失敗します。
- Windows SPx ポリシー・エージェント・サービスが予期せず停止した場合に、Microsoft Office 製品を使用してリモート共有経由でファイルが編集およびアクセスされていても、データの破損が発生しなくなりました。
 - サーバーのリブート後にサービスが正しく開始されなくても、データを変更できます。
- PPM GUI の問題:
 - 拡張設定を使用することで、予期される入力タイプを保存できます。

- 管理サーバーのパフォーマンスが向上し、最大 5000 エージェントに対応できるようになりました。

必要なアクション

以前のリリースの必須アクションに加えて、以下のアクションを行います。

- エージェント・ソフトウェアで「ハイブリッド」と言及されているものは、すべて「ボリューム/ポリシー」エージェントを指します。
- ポリシーの更新時に、ポリシー更新ジョブが処理および実行されるようにするには、エージェントが実行されている必要があります。ジョブの実行は、エージェントがオンラインになり、管理サーバーへの通信が正常に行われるまで、またはエージェントが管理サーバーから削除されるまで続きます。
- ボリューム/ポリシー・エージェントと同じディレクトリー・レベルのネットワーク共有にポリシーを付加すると、共有リソースが使用不可になります。ポリシー・パスは、ネットワーク共有ディレクトリーのレベルよりも上のパスに設定してください。
- 証明書に関するホスト検証が可能になりました。
 - 管理サーバーとエージェントの両方の証明書が、管理サーバーのトラストストアにある認証局によって署名されていること、サーバーおよびクライアント認証の拡張鍵用途属性を含んでいること、および目的のホストの特定の DNS 名および/または IP アドレスを含んでいることを確認してください。
- アカウントのログイン失敗によるロックアウトは、アカウントに対するログイン試行の失敗回数が 10 回に到達すると適用されます。アカウントがロックアウトされると、そのアカウントの状況が「ロック済み」に設定され、別の管理者による対処が必要になります。
 - 管理サーバーに管理者アカウントが 1 つしかない場合に、そのアカウントがロックされると、サーバーをリブートしなければアカウントのロックを解除できません。
- ジョブ承認の分離により、特定のジョブ・アクションに必要な承認数をより細かく制御できるようになりました。ジョブに対するジョブ承認の必要数が、サーバー上で必要なロールを担うことができる管理者の総数以下になるようにすることが重要です。

既知の問題

以前のリリースの既知の問題に加えて、以下の問題があります。

- システムに多数のポリシー・オブジェクトが含まれている場合に、データ・タイプ・ポリシー編集オプション「編集可能」や「編集の必要あり」を使用すると、ポリシー行が重複する可能性があります。
- セレクターのユーザー名とグループ名にスペースを含めることはできません。
 - 現時点では、問題の発生を防ぐために、スペースの代わりにアンダースコアを使用したグループまたは名前を作成する必要があります。
- Windows 版のファイル/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、ピリオド (.) を含むパスを使用できません。

- ネットワーク共有パスと同じディレクトリー・レベルにポリシーを適用すると、ネットワーク共有パスが正しく機能しません。ポリシーはターゲットの親ディレクトリーに適用してください。
- MariaDB のバックアップ・ユーティリティ「`mariabackup`」は、CentOS 6/7 ボリューム・エージェントおよびボリューム/ポリシー・エージェントでサポートされています。ファイル・エージェントはサポートされていません。
- NFS を通じてエクスポートされた RHEL/CentOS ファイル・エージェントが管理する保護ディレクトリーには、ポリシー内の特定のユーザー名を通じて定義された許可ユーザーだけがアクセスできます。グループ名はサポートされていません。
- Windows エージェント用のポリシー・パスを含むプロセスでは、大/小文字が区別され、Windows Server OS 環境で指定されたものと同じ大/小文字の区別に従う必要があります。
 - 例えば、「`C:\Windows\System32`」と「`C:\Windows\system32`」は同じではありません。後者を使用すると、パスの大/小文字の区別が異なるために、アクセスが拒否されます。
- RHEL/CentOS ファイル・エージェントが管理するシステムに、新規の論理ボリューム・マネージャー (LVM) 物理ボリューム (PV) を追加する場合は、`/etc/lvm/lvm.conf` ファイルのグローバル・フィルター行のデバイス・パスを `/dev/mapper` に変更します。例えば、


```
global_filter = [ "a|/dev/fileagent/*|" "r|.*)" ]
```

 は以下のように変更します。


```
global_filter = [ "a|/dev/mapper/*|" "r|.*)" ]
```
- Windows の「ボリューム・シャドー・コピー」はサポートされていません。
- CentOS 7 ファイル・エージェントでは、IBM Spectrum Protect (SP) による別の場所へのデータ復元がサポートされていません。
 - データ復元を正常に行うには、バックアップ用の十分なスペースがあることを確認し、元のファイル・システムをアンマウントして、バックアップ・ファイル・システムを元のデータと同じ場所にマウントします。この操作を行った後は、サービスを再始動する必要があります。
- `spsd-clustersetup` スクリプトを使用するときは、応答ファイルを通じて入力を受け付けてください。非対話式インストールには資料で示したフラグを使用しないでください。

バージョン 2.1.0.1* – 日付: 2018 年 1 月 5 日

リリースの特色

- スペイン語、ドイツ語、フランス語、イタリア語、ポルトガル語、日本語、韓国語、ロシア語、中国語、および中国語 (台湾) に対するグローバル化・サポート
- GUI 検証の改善
- エージェントの状況の報告
- ジョブのクラスター化
- DB 暗号化ポリシーのスナップショット

- ボリュームのパーティショニング (Windows)

*バージョン番号は新しい IBM のバージョン管理を反映して変更されました

解決された問題

以前のリリース以降に解決された既知の問題は以下のとおりです。

- RHEL / CentOS 7.4 のカーネルが、このリリースでサポートされるようになりました。
- Windows Server 2008R2 版のボリューム・エージェントで、異なるバージョンの鍵で暗号化されたデータをシステムにロードしても、ブルー・スクリーン・エラーが発生しなくなりました。
- Windows 版のボリューム・エージェントおよびボリューム/ポリシー・エージェントが、Active Directory ドメイン・コントローラーにインストールできるようになりました。
- ポリシー・オブジェクト (パス・セット、セレクター、データ・タイプなど) のすべての名前入力フィールドに、フィールド検証が適用されました。
- 絶対的な開始時刻と相対的な終了時刻を指定して作成/スケジュールされるジョブが、サポートされるようになりました。
- 一度に 50 件を超える数の、バッチで実行されて完了するスケジュール済みジョブが、完了するようになりました。
- QRadar などのアプリケーションに転送されるイベント・ログ・メッセージが向上しました。

必要なアクション

以前のリリースの必須アクションに加えて、以下のアクションを行います。

- Windows でボリューム・エージェントまたはボリューム/ポリシー・エージェント上にストレージを準備するときは、**spxdevice** コマンドを使用する前に、まずディスクをオンラインにして、既存のファイル・システム、パーティション、他の割り振りスペースなしで初期化する必要があります。
- **spsd-certsetup** で対話式実行が行われなくなりました。また、新しく提供されたコマンド引数を使用して、すべてのオプションをインラインで設定する必要があります。詳しくは、**spsd-certsetup --help** を実行してヘルプ・メニューを表示するか、管理者ガイドを参照してください。

既知の問題

以前のリリースの以前からの既知の問題に加えて、以下の問題があります。

- Web ブラウザーとして Firefox や Internet Explorer を使用する場合、「LDAP ポート」がアルファ文字を受け入れます。
- Windows 版のボリューム・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、4096 より小さいディスク割り振りサイズをサポートできません。
- Windows ファイル・エージェントは、現時点では DB2 データベースと PostgreSQL データベースをサポートできません。

- パス・セット・ポリシー・オブジェクトを使用して、ポリシー・スナップショットを更新することはできません。追加のパスには、手動パスを使用してください。
- 重複する管理ユーザー名を作成できます。
- ユーザー名が内部/OSGI と外部 (LDAP、Active Directory、クライアント証明書) の両方に存在するときは、ユーザー名間で競合が発生します。
- ディレクトリーに既存のファイルがある場合、以降に削除されても、spxinfo -l により、ディレクトリーの暗号化が保留中であると誤って報告されます。このメッセージは、spxconvert の実行か、システムのリブートまでは消去されません。
- SPx ポリシー・エージェント・サービスが予期せず停止したときに、Microsoft Office 製品を使用してリモート共有経由でファイルが編集およびアクセスされていた場合、データの破損が発生する可能性があります。
- PPM サーバーが AWS にデプロイされている場合、データ・タイプ・ポリシー編集オプション「May Edit」や「Must Edit」を使用しないでください。
- GUI を使用して新しいポリシー・オブジェクトを作成しているとき、対応するページのロード中に「新規セクター」、「新規データ・タイプ」、「新規プロセス」、または「新規パス・セット」のボタンをクリックすると、エラー・メッセージが表示され、新しいオブジェクトが作成されません。これを回避するには、項目を作成する前に、ページが完全にロードするまで待機してください。
- PPM GUI の問題:
 - PPM サーバーのブラウザー UI ナビゲーション・バーが、予期するとおりに省略表示されません。
 - ユーザー・アカウントの作成中に「Esc」を押すと、余分な行が残されます。
 - データ・タイプ行を削除しても、行の順序が更新されません。
 - 拡張設定を使用すると、どのような文字列も保存できます。

バージョン 2.1.1-1 – 日付: 2017 年 9 月 28 日

リリースの特色

- 10,000 件までのジョブのジョブ・スケジュールのプログラマチック (REST API) サポート。
- セキュリティー強化
- ロギング強化
- プロセス経由でのポリシー適用
- ファイル・エージェントのその場でのデータ暗号化
- UI の向上
- 「su」機能と「sudo」機能を制限するための追加機能。ポリシーの下でデータにアクセスするには、ユーザー・セッションがログイン・セッションと一致する必要があります。
- CA 証明書サポートの更新

解決された問題

以前のリリース以降に解決された既知の問題は以下のとおりです。

- アンインストール・プロセスが更新されました。最新情報については、「管理者ガイド」を参照してください。
- Active Directory/LDAP で UGLR 手法が不要になりました。
- RHEL 6.2 以降用のファイル・エージェントで、カーネル・パニックおよびデータ損失のリスクなしに複数のディスクがサポートされるようになりました。
- アーカイブ・ロギング時に DB2database データベースが DB2 トランザクション・ログを暗号化しない問題が解決しました。

必要なアクション

以前のリリースの必須アクションに加えて、以下のアクションを行います。

- Btrfs は Red Hat で非推奨になりました(<https://access.redhat.com/solutions/197643>)。この変更により、ファイル・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 Btrfs をサポートしなくなります。
- 保護されたディレクトリーに既にデータが存在していた場合、そのデータが削除された場合でも、管理者はそのディレクトリーに対して `spxconvert` を実行する必要があります。
- Windows Defender Device Guard の検証はまだ進行中です。検証が完了するまでは、Windows エージェントは、Windows Defender Device Guard で構成された Server 2016 システムと連携しません。(<https://docs.microsoft.com/en-us/windows/device-security/device-guard/device-guard-deployment-guide>)
- Windows Server 2008R2 をサポートするには、SHA2 ハッシュをサポートするためのパッチ KB3033929 をインストールする必要があります。(<https://www.microsoft.com/en-us/download/details.aspx?id=46148>)
- ボリューム/ポリシー・エージェントで `spxdevice` を使用する場合は、`-m` フラグを指定する必要があります。ボリューム・エージェントの場合はこのフラグを使用する必要はありません。
- ディスクを無効にするための `spxdevice` コマンドでは、Linux でリブート後にディスク状態を維持するために追加の管理アクションが必要となります。Windows 環境の場合は追加アクションは必要ありません。
- Windows 版のボリューム・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、複数パーティション・ディスクで固有の暗号鍵がサポートされません。暗号鍵はディスク全体に割り当てられます。
- プロセスを使用したポリシー適用
 - プロセスはポリシー適用に対する追加の意思決定レイヤーとして機能するものであり、オプションです。プロセスを使用するには、プロセス・ポリシーを作成し、セレクター・ポリシーに関連付ける必要があります。
 - プロセスを使用した意思決定エンジンは次のようになります。<操作> が <ユーザー> によって実行されるものであり、<グループ> に属していて、<プロセス> を使用している場合、このステートメント true になります。それ以外の場合、このステートメントは false です。
 - プロセス・ポリシーを作成するには、そのプロセス (実行可能ファイル) のパスを入力し、「OS」、「バージョン」、「配布」の各オプションを入力する必要があります。

- プロセスをさらに明細に指定するために、エージェントでコマンド・ユーティリティー `spxhash` を使用して、プロセスに関連付けるハッシュを生成できます。これにより、プロセスの特定のバージョン (複数可) のみがポリシーに対して有効になります。
- 暗号化されたストレージにアプリケーションが依存している場合は、ストレージが利用可能な状態になってからアプリケーションがストレージへのアクセスを試行するように、アプリケーションを遅延スタートアップさせてください。
 - ボリューム・エージェントの場合は、ボリュームが `/dev/mapper/e_<label>` で使用可能であることを確認してください。
 - ファイル/ポリシー・エージェントの場合は、コマンド「`spxinfo -l`」を使用して、ポリシーでアクティブになっていてシステムで使用可能な、保護されたディレクトリーをリストしてください。
 - ボリューム/ポリシー・エージェントは、ボリュームが使用可能であること、および保護されたディレクトリーがポリシーでアクティブになっていてシステムで使用可能であることの両方を確認する必要があります。

既知の問題

- RHEL / CentOS 7.4 のカーネルはこのリリースではサポートされていません。
- Windows 版のボリューム・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 Active Directory ドメイン・コントローラーにはインストールできません。
- Windows Server 2016 のセキュア・ブート機能は、このリリースではサポートされていません。
- システムのリブート実行時に Windows 版のボリューム・エージェントで部分的に割り振り解除されたディスクのマウントが失敗することがあります。この問題を緩和するには、暗号化ボリューム上の完全割り振り済みパーティションを使用してください。
- Windows Server 2008 R2 版のボリューム・エージェントでは、別のバージョンの鍵で暗号化されたデータをシステムにロードすると、ブルー・スクリーン・エラーが発生します。
- 保護されたディレクトリー・パスでは NFS はサポートされません。
- エージェントの管理は、PPM サーバーにアクティブに接続しているエージェントの数が 3900 を超える場合はサポートされません。
- Web ブラウザーの解像度を、より小さいサイズに変更すると、UI エlementが正しく表示ないことがあります。
- Web GUI はアイドル・セッションを自動的にログアウトするように設計されています。アイドル状態のアクティビティーが原因でセッションが終了した場合は、ブラウザーを最新表示して、GUI にログインし直してください。
- 使用可能な作成済みユーザー数よりも多い数に管理者承認のしきい値が設定された場合に警告が表示されません。この値を調整するときは注意してください。
- ポリシー・オブジェクト (パス・セット、セレクター、データ・タイプなど) のすべての名前入力フィールドで、英数字 Unicode 文字およびダッシュ (-) とアンダースコア () が受け入れられます。
- セレクター作成中にいずれかのセレクター行で「キャンセル」ボタンをクリックすると、保存していない変更はすべて破棄されます。また、名前が入力されてい

ない空のセクターのあるセクター行で「保存」ボタンをクリックすると、エラーになります。セクター・ポリシー行は一度に 1 行ずつ作成してください。

- 保護されたディレクトリー内でサイズの大きなファイルを操作すると、アクションの完了にさらに時間を要することになります。
- エージェントの作成中に無効な鍵を入力し、ユーザーが「戻る」をクリックして「ポリシー」タイトルを再入力すると、エージェント構成に無効な鍵が保存されてしまいます。
- ジョブの承認時に「作成」列のタイム・スタンプが変わることがあります。
- OS/LDAP に存在しないグループに属するユーザーが正しくログに記録されません。
- Internet Explorer 11 では、無効な LDAP ユーザー・ログインの場合のエラー・プロンプトが正しく表示されません。
- 現在、ポリシー・スナップショットの削除に関連するアクションは監査されていません。
- 「ログを確認して、再試行してください。」というエラー・プロンプトは、ユーザー入力が無効な場合を示しています。入力が有効であり、許容される値であることを確認してから、再試行してください。
 - 詳細なログ・メッセージは、PPM サーバーの /opt/securityfirst/spsd/ にある「bundleAll.log」ファイルで確認できます。
- 503 エラーが発生した場合は、少し待ってからアクションを再試行してください。
- REST を使用してユーザーを作成する場合、正常に完了するためには、作成、ロール、状況について個別の呼び出しが必要です。
- PPM を HA 構成で使用しているときは、ジョブを作成したノードがオフになり、別のノードでジョブが承認されると、ジョブが正常に完了した場合でも、ログにエラー・メッセージが示されます。
- SafeNet KeySecure の認証局で署名されたエージェント証明書は現在サポートされていません。
- Gemalto Luna HSM v5.4 は、このバージョンの PPM ではサポートされていません。今後のリリースでサポートされる予定です。
- QRadar などのアプリケーションに転送されたイベント・ログの場合、アクションが実行されているかどうかを判別するために、イベントの詳細を調べなければならないことがあります。
- 2 番目の鍵ストアを追加するジョブは、最初の試行時には失敗します。再試行すると、成功します。
- 絶対的な開始時刻と相対的な終了時刻を指定して作成/スケジュールされるジョブはサポートされません。
- スケジュール済みジョブは、一度に 50 件を超える数のジョブがバッチで実行されて完了する場合は、完了に失敗します。
- マルチノード・クラスター・セットアップでは、ジョブ・スケジュールは部分的にサポートされます。スケジュール済みジョブが実行されるのは、承認要求を登録したノードであり、かつ、そのジョブのタイマーを有するノードがアクティブ

な場合のみです。このノードがオフラインになった場合、別のクラスター・ノードでそのタイマーを復元するための高可用性メカニズムはないため、ジョブの実行がスキップされます。

- これは、ジョブの実行中に稼働中のノードに障害が発生したときにジョブを再開するという高可用性メカニズムとは無関係のコンセプトです。

バージョン 1.0.1-3 – 日付: 2017 年 3 月 24 日

リリースの特色

- このリリースではパスワードが覆い隠されます。

必要なアクション

以前のリリースの必須アクションに加えて、以下のアクションを行います。

- 以下の項目は、Red Hat Enterprise Linux (RHEL) バージョン 6 オペレーティング・システムを対象とするすべてのエージェント・タイプに関連しており、エージェントのインストールの前に実行する必要があります。
 - OpenSSL バージョン 1.0.1e-30.el6 以降が必要です (パッケージ名: openssl-1.0.1e-30.el6.x86_64)
 - Device Mapper バージョン 1.02.117 以降が必要です (パッケージ名: device-mapper-1.02.117-7.el6.x86_64)
 - 以下のようにして、/usr/sbin/depmod へのシンボリック・リンクを作成します (root として実行)。
 - `ln -s /sbin/depmod /usr/sbin/depmod`
- yum オペレーティング・システムのリポジトリを使用できるようにしている場合は、エージェントのインストール時に従属パッケージが自動的にインストールされます。ターゲットのエージェント・システムで yum オペレーティング・システムのリポジトリを使用できるようにしていない場合は、エージェントをインストールする前に以下の従属パッケージを手動でインストールする必要があります。
 - net-snmp-utils

既知の問題

以前のリリースの問題に加えて、以下の問題があります。

- Linux リリース 6.2 から 6.X において、エージェントのインストール先のターゲット・サーバーに curl を介してエージェント・ソフトウェアをダウンロードする場合に SSL エラー (35) が指摘されています。これを防ぐには、必ず最新バージョンの curl をオプション --tlsv1.2 を指定して使用してください。
- Windows ポリシーの入力では大/小文字が区別されます。例えば、User1 と user1 は同じではありません。
- すべての Windows ファイル・システムのパスは、大文字のドライブ名の後に続ける必要があります。また、パスでは、ディレクトリーの分離に円記号 (¥) 文字を使用する必要があります。注: C:¥test は有効な Windows ファイル・システムのパスです。C:/test は無効な Windows ファイル・システムのパスです。

初期リリースの機能

以下のオペレーティング・システムのファイル/ポリシー・エージェントのサポート:

- RHEL (6.2 以降および 7.2 以降)
- CentOS (6.2 以降および 7.2 以降)
- Windows Server 2012R2

以下のオペレーティング・システムのボリューム・エージェントのサポート:

- RHEL (6.2 以降および 7.2 以降)
- CentOS (6.2 以降および 7.2 以降)
- Windows Server 2012R2

以下のオペレーティング・システムのボリューム/ポリシー・エージェントのサポート:

- RHEL (6.2 以降および 7.2 以降)
- CentOS (6.2 以降および 7.2 以降)
- Windows Server 2012R2

必要なアクション

- エージェントの「package.tar」バンドルの抽出時に、最適な操作を行うために、必ずそのバンドルを固有の新規ディレクトリーに配置してください。
- インストールの手順について MDE クイック・スタート・ガイドで概説されている手順に従ってください。
- ファイル・エージェントでは、保護されたディレクトリーがエージェント VM に空の状態に既に存在し、かつすべてのユーザーとグループが既に存在している必要があります。
- データベースの実装では、ボリューム・エージェントまたはボリューム/ポリシー・エージェントを使用することがベスト・プラクティスです。

既知の問題

- RHEL 6.2 以降用のファイル・エージェントは、単一のデバイス (ディスク) のみをサポートします。複数のディスクを使用することは、カーネル・パニックおよびデータ損失のリスクがあります。
- DB2 とともにファイル・エージェント RHEL (6.2 以降および 7.2 以降) を使用する場合、アーカイブ・ロギングの構成時にデータベースで DB2 トランザクション・ログが暗号化されません。
- Active Directory または LDAP を使用する Windows 外部グループのサポートでは、「UGLR」方法を実装する必要があります。
- 鍵の廃棄は手動で実行できます。
 - ただし、鍵を廃棄する前に VM のスナップショットがあり、そのスナップショットに戻ると、鍵が使用可能になります。
- Linux のアンインストールの手順では、以下のステップに従う必要があります。

- IFA エージェントの場合:
 - 保護されたディレクトリーが空であることを確認します。
 - GUI を介して PPM 管理サーバーからエージェントを削除します。
 - 最後に「spxuninstall.sh」を実行します。
 - CENTOS 6 エージェントでは、「spxuninstall.sh」ファイルに使用のための実行権が付与されている必要があります。
- Linux IVA エージェントの場合:
 - </dev/mapper/e_volume> をアンマウントします。
 - cd /opt/ibm/mde/spxagent/spx-volumeagent/
 - ./uninstall_blockfiler.sh
 - y を入力して破壊アクションを確認します。
 - cd /opt/ibm/mde/spxagent/spx-policyagent/
 - ./policy_uninstall.sh
 - リブート
- Linux IVFA エージェントの場合:
 - ボリューム・ステップを実行します。
 - spxuninstall.sh
 - リブートします。
- Windows IVFA は、始動時にポリシーを適切に実行しない場合があります。これが発生した場合、サービス「secFirst Policy Agent」を再始動します。

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を提供し、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せんが、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検証できません。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をお願いします。

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ます、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を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。

© (お客様の会社名) (西暦年), 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](http://www.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を提供され、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