HITACHI
Inspire the Next

Encryption License Key

ユーザガイド

Hitachi Virtual Storage Platform One Block 23
Hitachi Virtual Storage Platform One Block 26
Hitachi Virtual Storage Platform One Block 28

4050-1J-U05-40

ストレージシステムを操作する場合は、必ずこのマニュアルを読み、操作手順、および指示事項をよく理解してから操作してください。

免責事項
このマニュアルの内容の一部または全部を無断で複製することはできません。
このマニュアルの内容については、将来予告なしに変更することがあります。
このマニュアルに基づいてソフトウェアを操作した結果、たとえ当該ソフトウェアがインストールされているお客様所有のコンピュータに何らかの障害が発生しても、当社は一切責任を負いかねますので、あらかじめご了承ください。
このマニュアルの当該ソフトウェアご購入後のサポートサービスに関する詳細は、弊社営業担当にお問い合わせください。
この製品は OpenSSL ツールキットを利用するために OpenSSL プロジェクト(http://www.openssl.org/)によって開発されたソフトウェアを含みます。

商標類
Microsoft は，米国 Microsoft Corporation 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。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
Windows は，米国 Microsoft Corporation 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。
Python は，Python Software Foundation の登録商標です。
その他記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

輸出時の注意
本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。
なお、不明な場合は、弊社担当営業にお問い合わせください。

発行
2025 年 1 月（4050-1J-U05-40）

目次

はじめに

このマニュアルでは、 Encryption License Key の機能概要について説明しています。

- 対象ストレージシステム
- マニュアルの参照と適合ファームウェアバージョン
- 対象読者
- このマニュアルの位置付け
- マニュアルで使用する記号について
- 「Thin Image Advanced」の表記について
- 発行履歴

対象ストレージシステム

このマニュアルでは、次に示すストレージシステムに対応する製品（プログラムプロダクト）を対象として記述しています。

Hitachi Virtual Storage Platform One Block 20

- Hitachi Virtual Storage Platform One Block 23
- Hitachi Virtual Storage Platform One Block 26
- Hitachi Virtual Storage Platform One Block 28

このマニュアルでは特に断りのない限り、上記モデルのストレージシステムを単に「ストレージシステム」または「本ストレージシステム」と称することがあります。

マニュアルの参照と適合ファームウェアバージョン

このマニュアルは、次の DKCMAIN ファームウェアバージョンに適合しています。

A3-04-01-XX

メモ

- このマニュアルは、上記バージョンのファームウェアをご利用の場合に最も使いやすくなるよう作成されていますが、上記バージョン未満のファームウェアをご利用の場合にもお使いいただけます。
- 各バージョンによるサポート機能については、別冊の『バージョン別追加サポート項目一覧』を参照ください。

対象読者

このマニュアルは、次の方を対象読者として記述しています。

- ストレージシステムを運用管理する方
- UNIX®コンピュータまたは Windows®コンピュータを使い慣れている方
- Web ブラウザを使い慣れている方

このマニュアルの位置付け

このマニュアルでは、主に Encryption License Key の機能、操作の準備、およびトラブルシューティングについて説明します。

詳細な操作方法や、操作上の注意事項などについては、次の管理ツールのマニュアルを参照してください。

管理ツール	参照マニュアル
REST API	『REST API リファレンスガイド』
VSP One Block Administrator	『VSP One Block Administrator ユーザガイド』
VSP One Block Administrator の API	『VSP One Block Administrator REST API リファレンスガイド』

管理ツール	参照マニュアル
RAID Manager	『RAID Manager コマンドリファレンス』

マニュアルで使用する記号について

このマニュアルでは、注意書きや補足情報を、次のとおり記載しています。

注意
データの消失・破壊のおそれや、データの整合性がなくなるおそれがある場合などの注意を示します。

メモ
解説、補足説明、付加情報などを示します。

ヒント
より効率的にストレージシステムを利用するのに役立つ情報を示します。

「Thin Image Advanced」の表記について

このマニュアルでは、Thin Image Advanced のことを、Thin Image または TI と表記することがあります。

発行履歴

マニュアル資料番号	発行年月	変更内容
4050-1J-U05-40	2025 年 1 月	適合 DKCMAIN ファームウェアバージョン：A3-04-01-XX • 鍵暗号化鍵の更新操作を追加した。 ◦ 1.1 Encryption License Key ◦ 3.8 鍵暗号化鍵の更新 ◦ 3.8.1 鍵暗号化鍵を更新する • ストレージシステム内の暗号化鍵の削除手順を修正した。 ◦ 3.7.1 ストレージシステム内の暗号化鍵を削除する • ロールを追加した。 ◦ 3.4 暗号化を有効にする
4050-1J-U05-30	2024 年 9 月	適合 DKCMAIN ファームウェアバージョン：A3-03-01-XX • VSP One Block Administrator で実行できる機能を修正した。 ◦ 1.1 Encryption License Key • 管理ツールでの機能ごとの操作可否を追加修正した。 ◦ 1.1 Encryption License Key • VSP One Block Administrator 接続をサポートした。 ◦ 1.1 Encryption License Key ◦ (1)暗号化鍵の一次バックアップと二次バックアップ ◦ 3 Encryption License Key の操作

マニュアル資料番号	発行年月	変更内容
4050-1J-U05-20	2024 年 5 月	適合 DKCMAIN ファームウェアバージョン：A3-02-21-XX • 鍵管理サーバとの接続をサポートした。 ◦ 1.1 Encryption License Key ◦ (1)暗号化鍵の一次バックアップと二次バックアップ ◦ (2)暗号化鍵の自動バックアップ ◦ 1.3.3 暗号化鍵のリストア機能 ◦ 1.3.4 鍵管理サーバを使用した暗号化鍵の操作 ◦ 2.1 システムの要件 ◦ 2.2 鍵管理サーバの要件 ◦ 2.2.1 鍵管理サーバのルート証明書の取得 ◦ 2.2.2 クライアント証明書の取得の流れ ◦ 2.2.3 証明書のアップロード ◦ 3 Encryption License Key の操作 ◦ 3.1 暗号化環境の設定 ◦ 3.1.1 鍵管理サーバの使用有無と暗号化環境の設定内容 ◦ 3.1.2 暗号化環境を設定する ◦ 3.2 暗号化鍵を作成する ◦ 3.3 暗号化鍵のバックアップ ◦ 3.3.1 管理ツールの操作端末内にファイルとして暗号化鍵をバックアップする ◦ 3.3.2 鍵管理サーバに接続して暗号化鍵をバックアップする ◦ 3.4 暗号化を有効にする ◦ 3.5 暗号化を無効にする ◦ 3.6 暗号化鍵のリストア ◦ 3.6.1 管理ツールの操作端末内にバックアップしたファイルから暗号化鍵をリストアする ◦ 3.6.2 鍵管理サーバに接続して暗号化鍵をリストアする ◦ 3.7 暗号化鍵の削除 ◦ 3.7.1 ストレージシステム内の暗号化鍵を削除する ◦ 3.8 鍵管理サーバを別サーバへ移行する ◦ 3.9 暗号化環境設定を初期化する ◦ 3.10 鍵管理サーバで使用する暗号化環境設定スクリプト ◦ 3.10.1 スクリプトの概要 ◦ 3.10.2 スクリプト実行環境設定 ◦ 3.10.3 初期設定スクリプトの実行方法 ◦ 3.10.4 初期化スクリプトの実行方法 ◦ 3.10.5 スクリプト実行結果の確認 ◦ 4.1 Encryption License Key 操作時のトラブルと対策 • セキュア通信プロトコルをサポートした。 ◦ 2.2 鍵管理サーバの要件 • パリティグループ作成時の暗号化有効設定にて RAID Manager の操作可否を修正した。 ◦ 1.1 Encryption License Key

マニュアル資料番号	発行年月	変更内容
4050-1J-U05-10	2024 年 3 月	適合 DKCMAIN ファームウェアバージョン：A3-02-01-XX ・ VSP One B20 で、通常パリティグループ、通常 VOL、DP-VOL 非サポートにより記載を修正した。 ◦ 1.4.1 データの暗号化 ◦ 1.4.3 データ暗号化鍵の変更
4050-1J-U05-00	2024 年 1 月	新規 適合 DKCMAIN ファームウェアバージョン：A3-01-01-XX

1

Encryption License Key の概要

ここでは、Encryption License Key の概要について説明します。

1.1 Encryption License Key

Encryption License Key を使用すると、ストレージシステム内のボリュームに格納されたデータを暗号化できます。データを暗号化すると、ストレージシステムまたはストレージシステム内のドライブを交換するとき、あるいは、これらが盗難に遭ったときに情報の漏えいを防ぐことができます。

Encryption License Key を使用するには、Encryption License Key プログラムプロダクトのライセンスキーが必要です。

Encryption License Key は、ボリュームに格納されたデータを暗号化できます。 データの暗号化は内部ボリュームの一部またはすべてに適用でき、データの入出力で処理時間や待ち時間に影響を与えることや、既存のアプリケーションやインフラストラクチャに損害を与えることがありません。Encryption License Key には、使用に際して簡単で安全な、鍵管理機能が備わっています。

Encryption License Key の操作は、REST API で実行します。一部機能は、VSP One Block Administrator でも実行できます。VSP One Block Administrator の操作は、『VSP One Block Administrator ユーザガイド』を参照してください。ただし、Encryption License Key に関する設定ができるのは、セキュリティ管理者（参照・編集）ロールを持ったユーザアカウントだけです。ユーザアカウントの詳細は、『システム管理者ガイド』を参照してください。

各管理ツールでの、機能ごとの操作可否を次に示します。

機能	REST API	VSP One Block Administrator	VSP One Block Administrator の API	RAID Manager
暗号化環境設定の編集	○	○	×	×
暗号化鍵の一覧表示/取得	○	○	×	×
暗号化環境設定編集での設定内容確認	○	○	×	×
暗号化鍵数表示/取得	○	○	×	×
暗号化鍵生成	○	×	×	×
管理ツールの操作端末内にファイルとして暗号化鍵をバックアップ※	○	○	×	×
鍵管理サーバに接続して暗号化鍵をバックアップ	○	×	×	×
管理ツールの操作端末内のファイルから暗号化鍵をリストア※	○	○	×	×
鍵管理サーバに接続して暗号化鍵をリストア	○	×	×	×
未使用暗号化鍵の削除および生成	○	×	×	×
鍵暗号化鍵の更新	○	×	×	×
パリティグループ作成時の暗号化有効設定	×	×	×	○
プール作成時の暗号化有効設定	×	○	○	×
鍵管理サーバ証明書の参照/登録/削除	○	○	×	×
鍵管理サーバ接続設定の参照/登録/編集/削除/優先度の変更/通信テスト	○	○	×	×

凡例

○：操作できる

×：操作できない

注※

ストレージシステムの暗号化環境が、鍵管理サーバと接続するように設定されている場合、管理ツールの操作端末内にファイルとしてバックアップできません。

1.2 暗号化の仕様

1.2.1 ハードウェアの仕様

暗号アルゴリズム

Advanced Encryption Standard (AES) 256 bit

暗号モード

XTS モード

暗号モジュール規格

モデル	説明
VSP One B20	FIPS 140-3 Level 1 準拠

1.2.2 暗号化できるボリューム

ボリューム種別

すべてのボリュームタイプ

エミュレーションタイプ

すべてのエミュレーションタイプ

内部／外部ボリューム

内部ボリュームのみ

既存のデータの暗号化

可能

関連概念

- 1.4.1 データの暗号化

1.2.3 格納データ暗号化で使用する鍵

格納データ暗号化において使用する鍵の属性

格納データ暗号化で使用する鍵は、属性「空き」（鍵種別が FREE）として生成し、用途に応じて各々の属性が設定されます。

- 空き：未使用鍵。格納データ暗号化において、生成され割り当て前の鍵
- DEK：データ暗号化鍵。格納したデータを暗号化するための鍵
- KEK：鍵暗号化鍵。格納データ暗号化において、ストレージシステム内に 1 つのみ存在する、属性が「KEK」以外の鍵を暗号化するための鍵

以降では、「DEK」を暗号化鍵と呼びます。

暗号化鍵の数

作成できる暗号化鍵の数は次のとおりです。下記に加えて、KEK が常に 1 つ存在します。

モデル	DEK の最大数	ストレージシステムごとの暗号化鍵の最大数
VSP One B20	984	4,096

暗号化鍵を設定する単位

- DEK：ドライブ単位に 1 つ

1.3 暗号化鍵の管理機能

格納データ暗号化で使用する鍵は、セキュリティ管理者（参照・編集）ロールを持ったユーザが REST API を使用して作成できます。

ストレージシステムごとに作成できる暗号化鍵の数は次のとおりです。

モデル	ストレージシステムごとに作成できる暗号化鍵の数
VSP One B20	4,096

ただし、初めて暗号化環境を設定したときに作成される暗号化鍵の数は次のとおりです。

モデル	初めて暗号化環境を設定したときに作成される暗号化鍵数
VSP One B20	4,096

データの有用性を確実にするため、Encryption License Key には暗号化鍵のバックアップとリストア機能があります。

関連概念

- 1.3.1 暗号化鍵の使用
- 1.3.2 暗号化鍵のバックアップ機能
- 1.3.3 暗号化鍵のリストア機能

1.3.1 暗号化鍵の使用

暗号化環境設定が完了している場合、次の操作および保守作業をしたときに暗号化鍵を使用します。

ドライブに関連する保守操作時

保守操作	使用される鍵数	備考
ドライブ増設	ドライブあたり 1 個	増設するドライブ数分必要となります。
ドライブ交換	ドライブあたり 1 個	交換するドライブ数分必要となります。
暗号化が有効なパリティグループの削除時	ドライブあたり 1 個	解除対象となるパリティグループに含まれるドライブ数分必要となります。

上記の操作および保守作業中に障害が発生した場合、回復のために上記の数以上の未使用鍵が使用される場合があります。

関連概念

- 1.3 暗号化鍵の管理機能

1.3.2 暗号化鍵のバックアップ機能

暗号化鍵のバックアップ機能について説明します。

関連概念

- 1.3 暗号化鍵の管理機能
- (1)　暗号化鍵の一次バックアップと二次バックアップ

(1)　暗号化鍵の一次バックアップと二次バックアップ

暗号化鍵のバックアップには、一次バックアップと二次バックアップがあります。

- 暗号化鍵の一次バックアップは、ストレージシステムによって自動的に行われます。 一次バックアップでは、暗号化鍵はストレージシステム内のキャッシュフラッシュメモリにバックアップされます。
- 暗号化鍵の二次バックアップは、REST API または VSP One Block Administrator を使用してユーザが実施します。このため、二次バックアップした暗号化鍵は、ユーザが責任を持って保管してください。二次バックアップは、一次バックアップが利用できなくなった場合、暗号化鍵をリストアするときに必要となります。二次バックアップを実施するには、専用の操作権限（セキュリティ管理者（参照・編集）ロール）が必要です。

注意
一次バックアップでバックアップした暗号化鍵が使用できず、かつ、二次バックアップでバックアップした暗号化鍵も使用できない場合は、データの復号化ができません。

暗号化鍵を作成したらすぐに二次バックアップを行ってください。また、データの有用性を確実にするためにも、定期的に（例えば週に一回）バックアップを行ってください。

二次バックアップには、管理ツールの操作端末にファイルとしてバックアップする方法と、鍵管理サーバに接続してバックアップする方法があります。

暗号化鍵を管理ツールの操作端末内にファイルとしてバックアップするときはパスワードを設定します。このパスワードは暗号化鍵をリストアするときに必要です。

鍵管理サーバに接続してバックアップしている場合､鍵管理サーバにバックアップできる鍵の数は、二次バックアップ、自動バックアップ合わせて一世代になります。バックアップ時に古い鍵は上書きされます。

暗号化鍵のバックアップは、作成済みの暗号化鍵に対して一括して実施されます。

作成済みの暗号化鍵がない状態では、暗号化鍵のバックアップはできません。

関連概念

- 1.3.2 暗号化鍵のバックアップ機能

(2)　暗号化鍵の自動バックアップ

鍵管理サーバを使用している場合は、暗号化鍵を作成後、自動的にバックアップされます。これを自動バックアップと言います。

鍵管理サーバに接続してバックアップしている場合､鍵管理サーバにバックアップできる鍵の数は、二次バックアップ、自動バックアップ合わせて一世代になります。バックアップ時に古い鍵は上書きされます。

鍵管理サーバを使用していない場合は、自動バックアップは実施されません。

1.3.3 暗号化鍵のリストア機能

不具合などによって既存の暗号化鍵が利用できなくなった場合、暗号化鍵は一次バックアップまたは二次バックアップからリストアされます。

注意
最新の暗号化鍵をリストアしてください。二次バックアップ後に暗号化鍵が変更されたなどの理由によって最新でない暗号化鍵はリストアできません。

- 一次バックアップからの暗号化鍵のリストアは、ストレージシステムによって自動的に行われます。
- 二次バックアップからの暗号化鍵のリストアは、ユーザが実施します。二次バックアップから最新の暗号化鍵のリストアするには、専用の操作権限（セキュリティ管理者（参照・編集）ロール）が必要です。二次バックアップから最新ではない暗号化鍵のリストアするには、専用の操作権限（セキュリティ管理者（参照・編集）ロールと保守（ベンダ専用）ロール）が必要です。
  二次バックアップからの暗号化鍵のリストアには、管理ツールの操作端末内にバックアップしたファイルからリストアする方法と、鍵管理サーバに接続してリストアする方法があります。

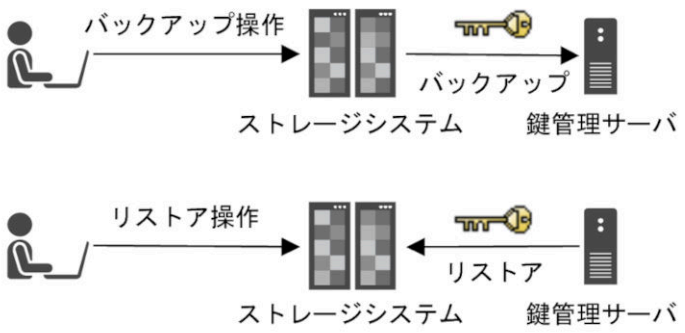
関連概念

- 1.3 暗号化鍵の管理機能

1.3.4 鍵管理サーバを使用した暗号化鍵の操作

暗号化鍵を管理するための規格である KMIP（Key Management Interoperability Protocol）に準じた鍵管理サーバで作成した暗号化鍵を使用できます。また、鍵管理サーバに暗号化鍵をバックアップでき、鍵管理サーバにバックアップした暗号化鍵から暗号化鍵をリストアできます。

暗号化鍵は、鍵管理サーバにバックアップされるときに別の暗号化鍵で暗号化され、その暗号化鍵とともに鍵管理サーバに格納されます。



関連概念

- 1.3 暗号化鍵の管理機能

関連タスク

- 3.3.2 鍵管理サーバに接続して暗号化鍵をバックアップする
- 3.6.2 鍵管理サーバに接続して暗号化鍵をリストアする

1.4 データの暗号化機能

データの暗号化機能について説明します。

関連概念

- 1.4.1 データの暗号化
- 1.4.2 暗号化の解除
- 1.4.3 データ暗号化鍵の変更

1.4.1 データの暗号化

Encryption License Key では、パリティグループごとにデータを暗号化できます。パリティグループ作成時に、暗号化設定を有効にします。そのパリティグループにボリュームを作成すると、そのボリュームに格納するデータが暗号化されます。

暗号化が無効なパリティグループの暗号化設定を有効に変更できません。パリティグループを一度削除して、暗号化を有効にしたパリティグループを新規作成してください。既存のパリティグループ内にボリュームが存在して、そのデータを暗号化する場合は、「既存のデータを暗号化する」を参照してください。

既存のデータを暗号化する

既存のデータを暗号化する場合は、データの移行が必要です。あらかじめ暗号化を設定したパリティグループを作成し、Volume Migration、または ShadowImage や TrueCopy などのコピー系プログラムプロダクトを使用してデータを移行します。データは仮想ボリューム単位で移行します。

Volume Migration を使用したデータの移行については、『Volume Migration ユーザガイド』を参照してください。コピー系プログラムプロダクトを使用したデータの移行については、ご使用になるコピー系プログラムプロダクトのマニュアルを参照してください。

関連概念

- 1.4 データの暗号化機能

1.4.2 暗号化の解除

Encryption License Key でパリティグループの暗号化を解除するには、暗号化が有効なパリティグループを削除します。暗号化が有効なパリティグループを削除すると、パリティグループを構成するドライブの暗号化鍵は削除され、新しい暗号化鍵が割り当てられます。

このため、暗号化の解除には注意が必要です。パリティグループ内の必要なデータは、暗号化を解除する前に責任を持ってバックアップしておいてください。あるいは、パリティグループの増設時や LDEV フォーマット機能を利用したフォーマット時など、パリティグループ全体をフォーマットする前に、暗号化を解除してください。

関連概念

- 1.4 データの暗号化機能

1.4.3 データ暗号化鍵の変更

暗号化したデータを別の暗号化鍵で暗号化する場合は、データの移行が必要です。あらかじめ別の暗号化鍵を設定したパリティグループを作成し、Volume Migration、または ShadowImage や TrueCopy などのコピー系プログラムプロダクトを使用してデータを移行します。データは仮想ボリューム単位で移行します。

Volume Migration を使用したデータの移行については、『Volume Migration ユーザガイド』を参照してください。コピー系プログラムプロダクトを使用したデータの移行については、ご使用になるコピー系プログラムプロダクトのマニュアルを参照してください。

データを移行後、移行元パリティグループを削除すると、そのパリティグループを構成するドライブに割り当てられた暗号化鍵は削除され、新しい暗号化鍵が割り当てられます。また、ドライブを交換すると、そのドライブに割り当てられた暗号化鍵は削除されます。交換または増設などによって新しいドライブを実装したときに、新しい暗号化鍵が割り当てられます。

関連概念

- 1.4 データの暗号化機能

1.5 監査ログ機能

監査ログ機能を使用して、ストレージシステム上の Encryption License Key に関する操作の履歴を取得できます。監査ログファイルには、暗号化鍵の操作やデータの暗号化の操作などの Encryption License Key に関する操作の履歴が記録されます。

監査ログおよび監査ログの履歴に関する詳細については、『監査ログ リファレンスガイド』を参照してください。

2

Encryption License Key を利用するための準備

ここでは、Encryption License Key を利用するための準備について説明します。

2.1 システムの要件

格納データ暗号化機能を使用して、データを暗号化するためのシステム要件を以下に示します。

項目	必要事項
ライセンスキー	Encryption License Key プログラムプロダクトのライセンスキーが必要です。
ロール	暗号化の設定および解除、暗号化鍵をバックアップおよびリストアするには、セキュリティ管理者（参照・編集）ロールが必要です。
ホストのプラットフォーム	すべてのプラットフォームがサポートされています。
DNS サーバ	鍵管理サーバに、IP アドレスではなくホスト名を指定して接続する場合は、ストレージシステムの管理ポートのネットワーク情報に、DNS サーバを設定してください。
データボリューム	すべてのボリュームタイプおよびすべてのエミュレーションタイプがサポートされています。 データを暗号化できるのは、ストレージシステムの内部ボリュームだけです。外部ボリュームは暗号化できません。

2.2 鍵管理サーバの要件

鍵管理サーバを使用する場合、鍵管理サーバは次の要件を満たしている必要があります。最新の検証済み鍵管理サーバ、および、そのファームウェアバージョンについては、「4.2 お問い合わせ先」へお問い合わせください。

- 前提プロトコル
  - Key Management Interoperability Protocol 1.0、1.1、1.2、1.3、1.4（KMIPv1.0、v1.1、v1.2、v1.3、v1.4）
- 前提製品

ベンダ	製品名
Thales/Gemalto	CipherTrust Manager k170v/k470v/k470/k570

- 証明書
  ルート証明書とクライアント証明書をストレージシステムにアップロードする必要があります。また、鍵管理サーバにサーバ証明書を設定する必要があります。
  これらの証明書については鍵管理サーバの管理者にお問い合わせください。証明書の管理については鍵管理サーバの管理者とご相談の上、適切に管理してください。ストレージシステムと鍵管理サーバ間の SSL/TLS 通信や証明書の要件については、『システム管理者ガイド』のストレージシステムと外部サーバ間の SSL/TLS 通信を参照ください。
  証明書には期限があります。期限が切れると鍵管理サーバと接続できなくなるため、証明書を準備するときは期限の設定にご注意ください。
  クライアント証明書は、PKCS#12 形式に変換する必要があります。また、PKCS#12 形式に変換する前のクライアント証明書は、鍵管理サーバの CA 局（Certificate Authority）によって署名されている必要があります。
  PKCS#12 形式のクライアント証明書に設定されたパスワードがわからない場合は、鍵管理サーバの管理者にお問い合わせください。
- その他

鍵管理サーバは最大 2 台登録できます。2 台登録する場合は、2 台でクラスタ化されている必要があります。鍵管理サーバは 2 台登録することを推奨します。

2.2.1 鍵管理サーバのルート証明書の取得

鍵管理サーバのルート証明書の取得方法については、各鍵管理サーバのマニュアルを参照してください。

2.2.2 クライアント証明書の取得の流れ

クライアント証明書を取得するには、クライアント証明書を作成するためのプログラムが必要です。クライアント証明書を作成するためのプログラムは、OpenSSL のホームページ（http://www.openssl.org/）からダウンロードしてください。ここでは、OpenSSL が C:¥openssl フォルダにインストールされているものとします。

クライアント証明書は、PKCS#12 形式に変換する必要があります。

以下に例として、OS に Windows を使用して秘密鍵と公開鍵を作成し、作成した公開鍵を鍵管理サーバの CA 局に署名してもらうことでクライアント証明書を取得する手順を説明します。

操作手順

1. 秘密鍵（.key ファイル）を作成します。
   秘密鍵を作成する方法については、『システム管理者ガイド』の秘密鍵を作成の操作手順を参照してください。
2. 公開鍵（.csr ファイル）を作成します。
   公開鍵を作成する方法については、『システム管理者ガイド』の公開鍵を作成の操作手順を参照してください。
3. 作成した公開鍵を鍵管理サーバの CA 局に署名してもらうことで証明書を取得します。この証明書をクライアント証明書として使用します。
   詳細については、各鍵管理サーバのマニュアルを参照してください。
4. Windows のコマンドプロンプト上で、カレントディレクトリを PKCS#12 形式のクライアント証明書ファイルを出力するフォルダがあるディレクトリに移動します。
5. 秘密鍵（.key ファイル）およびクライアント証明書をこのフォルダに移動し、次に示すコマンドを実行します。なお、この例では次の条件でコマンドを実行しています。
   ・PKCS#12 形式のクライアント証明書ファイルを出力するフォルダ：c:¥key
   ・秘密鍵のファイル名：client.key
   ・クライアント証明書のファイル名：client.crt
   OpenSSL をインストールした場合：

```
C:¥key>c:¥openssl¥bin¥openssl pkcs12 -export -in client.crt -inkey
client.key -out client.p12
```

6. 任意のパスワードを入力します。
   このパスワードは、PKCS#12 形式のクライアント証明書をストレージシステムにアップロードするときに使用します。
   PKCS#12 形式のクライアント証明書を作成するときに入力するパスワードは 0 文字以上 128 文字以下で、使用できる文字は次のとおりです。

   - 数字（0 から 9）
   - 英大文字（A から Z）

- 英小文字（a から z）
- 半角記号 31 種：！＃＄％＆'（）＊＋，－．／：；＜＝＞？＠［￥］＾＿｀｛｜｝～

この例では、client.p12 ファイルが c:¥key フォルダに作成されます。この client.p12 ファイルが PKCS#12 形式に変換されたクライアント証明書です。

2.2.3 証明書のアップロード

鍵管理サーバへの接続を設定するときに、鍵管理サーバのルート証明書および PKCS#12 形式のクライアント証明書をストレージシステムにアップロードする必要があります。証明書のアップロード操作については、「3.1.2 暗号化環境を設定する」を参照してください。

2.3 他のプログラムプロダクトとの併用

Encryption License Key と他のプログラムプロダクトとの併用について説明します。

2.3.1 Encryption License Key とコピー系プログラムプロダクトの併用

プライマリボリュームに暗号化を設定する場合は、セカンダリボリュームにも暗号化を設定してください。セカンダリボリュームに暗号化を設定しない場合、セカンダリボリュームのデータは暗号化されません。この場合、セカンダリボリュームのデータの機密性は保証できません。

2.3.2 Encryption License Key と Thin Image の併用

プライマリボリュームに暗号化を設定する場合、プールは暗号化を設定したプールボリュームだけで構成してください。暗号化を設定していないプールボリュームがある場合、プライマリボリュームの差分データは暗号化されていないデータとして格納されます。この場合、セカンダリボリュームのデータの機密性は保証できません。

プライマリボリュームの暗号化の状態とプールの暗号化の状態が異なる場合（例えば、プライマリボリュームには暗号化が設定されていないがプールは暗号化を設定したプールボリュームだけで構成されている、など）、セカンダリボリュームには暗号化されたデータと暗号化されていないデータが混在します。データの機密性を保つためにも、プライマリボリュームの暗号化の状態とプールの暗号化の状態は同じにしてください。

2.3.3 Encryption License Key と Universal Replicator の併用

プライマリボリュームに暗号化を設定する場合は、セカンダリボリュームにも暗号化を設定してください。セカンダリボリュームに暗号化を設定しない場合、セカンダリボリュームのデータは暗号化されません。この場合、セカンダリボリュームのデータの機密性は保証できません。

プライマリボリュームに暗号化を設定する場合、ジャーナルは暗号化を設定したジャーナルボリュームだけで構成してください。暗号化を設定していないジャーナルボリュームがある場合、プライマリボリュームのジャーナルは暗号化されていないデータとして格納されるため、データの機密性を保証できません。これはセカンダリボリュームについても同様です。

2.3.4 Encryption License Key と Volume Migration の併用

ソースボリュームに暗号化を設定する場合は、ターゲットボリュームにも暗号化を設定してください。ターゲットボリュームに暗号化を設定しない場合、ターゲットボリュームのデータは暗号化されません。この場合、ターゲットボリュームのデータの機密性は保証できません。

2.3.5 Encryption License Key と Dynamic Provisioning の併用

仮想ボリュームを経由してプールに書き込まれたデータを暗号化する場合は、暗号化を設定したプールボリュームだけで構成されたプールを使用してください。

2.4 Encryption License Key の使用を取りやめる場合

データを暗号化したあとに Encryption License Key の使用を取りやめる場合は、次の操作が必要になります。

注意
ライセンスキーを削除する前に手順 1 および手順 2 の操作が必要です。ライセンスキーを削除すると手順 1 および手順 2 の操作ができなくなります。

操作手順

1. 暗号化が有効なパリティグループをすべて削除してください。
   削除するパリティグループ内に必要なデータが含まれている場合は、削除前に必ずデータのバックアップまたはデータ移行を実施してください。
2. 暗号化環境設定を初期化してください。
3. Encryption License Key プログラムプロダクトのライセンスキーを削除してください。

3

Encryption License Key の操作

ここでは、REST API を使った、Encryption License Key（暗号化）の設定操作、前提条件、および注意事項について説明します。

REST API の詳細な操作方法については、『REST API リファレンスガイド』を参照してください。

3.1 暗号化環境の設定

3.1.1 鍵管理サーバの使用有無と暗号化環境の設定内容

鍵管理サーバの使用有無によって、設定する項目が異なります。

次の表で、鍵管理サーバの設定、暗号化環境に設定する内容を確認してください。

<table>
<tr><th colspan="3">暗号化環境</th><th>鍵管理サーバの設定
(POST kms-settings)</th><th colspan="3">暗号化環境の設定
(PATCH encryption-settings/instance)</th></tr>
<tr><th>暗号化</th><th colspan="2">鍵管理サーバ</th><th>各属性</th><th>暗号化環境を有効にする
(isEnabled)</th><th>鍵管理サーバを使用する
(usesKms)</th><th>ローカル鍵生成を禁止する
(prohibitsLocalKeyGeneration)</th></tr>
<tr><td rowspan="3">使用する</td><td colspan="2">使用しない</td><td>設定しない</td><td>有効</td><td>無効</td><td>無効</td></tr>
<tr><td rowspan="2">使用する</td><td>ローカル鍵生成を禁止しない</td><td rowspan="2">設定する</td><td rowspan="2">有効</td><td rowspan="2">有効</td><td>無効</td></tr>
<tr><td>ローカル鍵生成を禁止する</td><td>有効※</td></tr>
<tr><td>使用しない
（初期化）</td><td colspan="2">—</td><td>—</td><td>無効</td><td>無効</td><td>—</td></tr>
</table>

注※

「ローカル鍵生成を禁止する」を有効にした場合、設定が完了すると元に戻すことができません。有効に設定しても問題がないことをよく確認してください。

3.1.2 暗号化環境を設定する

鍵管理サーバを使用するには、鍵管理サーバへの接続設定やネットワークの設定が必要です。鍵管理サーバへの接続設定に必要な値については、各サーバの管理者にお問い合わせください。ネットワークの設定については、ネットワークの管理者に確認してください。

注意

鍵管理サーバにバックアップされる暗号化鍵はクライアント証明書と関連づけられて管理されます。このため、クライアント証明書を変更した場合、クライアント証明書を変更する前にバックアップした暗号化鍵をリストアできなくなります。クライアント証明書変更後は、必ず暗号化鍵をバックアップしてください。

注意

鍵管理サーバにバックアップされる暗号化鍵はクライアント証明書と関連づけられて管理されます。このため、クライアント証明書を紛失した場合、故障などによってコントローラを交換するとコントローラを交換する前にバックアップした暗号化鍵をリストアできなくなります。

また、鍵管理サーバへの接続設定のバックアップにはクライアント証明書は含まれません。このため、設定完了後は必ず鍵管理サーバへの接続設定をバックアップするとともに、鍵管理サーバの管理者と相談の上、クライアント証明書を別途保管してください。

メモ
鍵管理サーバは、最大 2 台登録できます。2 台登録する場合は、2 台でクラスタ化されている必要があります。鍵管理サーバは、2 台登録することを推奨します。

注意
「ローカル鍵生成を禁止する」を有効にした場合、設定が完了すると元に戻すことができません。有効にをしても問題がないことをよく確認してください。

注意
鍵管理サーバを使用する設定の場合、ストレージシステムの電源を ON にしたときに鍵管理サーバからバックアップした暗号化鍵を取得します。このとき、鍵管理サーバとの通信が確立されている必要があります。鍵管理サーバとの通信が確立されていない場合、ストレージシステムは起動しますが、すべてのボリュームが閉塞します。このため、ストレージシステムと鍵管理サーバが通信できることを確認してからストレージシステムの電源を ON にしてください。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール
- 鍵管理サーバに、IP アドレスではなくホスト名を指定して接続する場合は、ストレージシステムの管理ポートのネットワーク情報に、DNS サーバが設定されていること。
- 鍵管理サーバを使用する場合は、鍵管理サーバに登録されているクライアント証明書と鍵管理サーバのルート証明書を用意すること。それぞれの証明書については、鍵管理サーバの管理者に確認してください。

操作手順

鍵管理サーバを使用していない場合は、手順 4 のみ実施してください。

1. 鍵管理サーバを使用する場合、まずクライアント証明書とルート証明書のアップロードを実施します。
   リクエストライン：

```
POST <ベース URL>/v1/objects/kms-certificates
```

ヒント
クライアント証明書をアップロードする場合は、属性 `fileType` に `ClientCertFile` を、ルート証明書をアップロードする場合は、属性 `fileType` に `RootCertFile` を指定します。

2. 鍵管理サーバとの接続を設定します。
   リクエストライン：

```
POST ＜ベース URL ＞/v1/objects/kms-settings
```

3. 鍵管理サーバを使用する場合、鍵管理サーバとの通信テストを実施します。
   リクエストライン：

```
POST ＜ベース URL ＞/v1/objects/kms-settings/＜オブジェクト ID ＞/actions/
test-connectivity/invoke
```

4. 暗号化環境を有効に設定します。鍵管理サーバを使用するかどうかにより設定値が異なります。「3.1.1 鍵管理サーバの使用有無と暗号化環境の設定内容」を参照してください。
   暗号化環境設定を有効にすることで、暗号化の運用を開始できます。有効に設定すると、ストレージシステム内に暗号化鍵が作成されます。
   リクエストライン：

```
PATCH ＜ベース URL ＞/v1/objects/encryption-settings/instance
```

関連概念

- 3.1.1 鍵管理サーバの使用有無と暗号化環境の設定内容

3.2 暗号化鍵を作成する

暗号化鍵は、暗号化環境の設定が有効に設定された際に、自動で作成されます。ただし、次のような場合は、手動で暗号化鍵の作成が必要になります。

- 暗号化鍵の変更が必要になった場合
- ドライブ交換によって、未割り当ての鍵が不足した場合

ストレージシステムごとに作成できる暗号化鍵の数は次のとおりです。

モデル	ストレージシステムごとに作成できる暗号化鍵の数
VSP One B20	4,096

鍵管理サーバの使用有無により、暗号化鍵の生成場所やバックアップ方法が異なります。

鍵管理サーバの使用有無	鍵の生成場所	暗号化鍵のバックアップ方法
鍵管理サーバを使用している	鍵管理サーバ （鍵を使用するのは、ストレージシステム内）	自動的にバックアップされます。
鍵管理サーバを使用していない	ストレージシステム	手動でのバックアップが必要です。 「3.3.1 管理ツールの操作端末内にファイルとして暗号化鍵をバックアップする」を参照して、バックアップしてください。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

注意事項

- 暗号化鍵数には、作成可能な最大の暗号化鍵数を指定することを推奨します。
- 作成可能な最大の暗号化鍵数は、ストレージシステムごとに作成できる暗号化鍵の数（4,096）から、現在の暗号化鍵の数を引いた数が、その時点で作成可能な暗号化鍵の最大数になります。現在の暗号化鍵の数は、下記リクエストラインで確認できます。

```
GET ＜ベース URL ＞/v1/objects/encryption-key-counts/instance
```

操作手順

1. 暗号化鍵を作成します。
   リクエストライン：

```
POST ＜ベース URL ＞/v1/objects/encryption-keys
```

3.3 暗号化鍵のバックアップ

暗号化鍵のバックアップは、鍵管理サーバの使用有無により、次のように異なります。

- 鍵管理サーバを使用している場合
  - 鍵管理サーバへのバックアップは、自動的に一次バックアップ、二次バックアップが取得されます。手動での二次バックアップ操作は不要です。
  - 個別にバックアップを取り直したい場合や手動バックアップを取得するようにガイドされた場合は、鍵管理サーバに暗号鍵をバックアップしてください。
- 鍵管理サーバを使用していない場合
  - 暗号化鍵の一次バックアップは自動で取得されますが、二次バックアップは手動での取得操作が必要です。暗号化環境設定を有効化した後、または暗号化鍵を作成後は、暗号鍵を管理ツールの操作端末内にファイルとしてバックアップしてください。
  - 個別にバックアップを取り直したい場合や手動でバックアップを取得するようにガイドされた場合は、暗号鍵を管理ツールの操作端末内にファイルとしてバックアップしてください。

また、二次バックアップした暗号化鍵は、ユーザが責任を持って保管してください。

注意
一次バックアップでバックアップした暗号化鍵が使用できず、かつ、二次バックアップでバックアップした暗号化鍵も使用できない場合は、データの復号化ができません。

二次バックアップには、管理ツールの操作端末内にファイルとしてバックアップする方法と、鍵管理サーバに接続してバックアップする方法があります。

暗号化鍵を管理ツールの操作端末内にファイルとしてバックアップするときはパスワードを設定します。このパスワードは、暗号化鍵をリストアするときに必要です。

暗号化鍵のバックアップは、作成済みの暗号化鍵（DEK）に対して一括して実施されます。

作成済みの暗号化鍵がない状態では、暗号化鍵のバックアップはできません。

関連概念

- 1.3.2 暗号化鍵のバックアップ機能

関連タスク

- 3.3.1 管理ツールの操作端末内にファイルとして暗号化鍵をバックアップする
- 3.3.2 鍵管理サーバに接続して暗号化鍵をバックアップする

3.3.1 管理ツールの操作端末内にファイルとして暗号化鍵をバックアップする

鍵管理サーバを使用していない場合、暗号化鍵を管理ツールの操作端末内にファイルとしてバックアップできます。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

注意事項

保存した暗号化鍵ファイルとパスワードは、ユーザが責任を持って保管してください。

操作手順

1. 暗号化鍵をファイルとしてバックアップします。
   リクエストライン：

```
POST ＜ベース URL＞/v1/objects/encryption-keys/file/actions/backup/invoke
```

3.3.2 鍵管理サーバに接続して暗号化鍵をバックアップする

鍵管理サーバを使用している場合は、暗号化鍵を鍵管理サーバにバックアップできます。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 鍵管理サーバに、暗号化鍵をバックアップします。

```
POST ＜ベース URL＞/v1/objects/encryption-keys/kms/actions/backup/invoke
```

注意
鍵管理サーバにバックアップできる鍵の数は、自動バックアップと合わせて一世代になります。バックアップ時に古い鍵は上書きされます。

3.4 暗号化を有効にする

Encryption License Key では、パリティグループごとに暗号化の設定をします。暗号化を有効に設定できるのは、パリティグループ作成時のみです。

暗号化が無効なパリティグループに対して、後から暗号化を有効に設定できません。暗号化が無効なパリティグループに対して暗号化を設定したい場合は、その暗号化が無効なパリティグループを一度削除します。その後、暗号化が有効なパリティグループを作成します。ただし、前述の方法は、暗号化が無効なパリティグループにボリュームが作成されていない場合に限ります。

この手順は、RAID Manager で操作します。各コマンドの使用方法は『RAID Manager コマンドリファレンス』を参照してください。

前提条件

- 必要なロール：
  - ストレージ管理者（プロビジョニング）
  - セキュリティ管理者（参照・編集）ロール

操作手順

1. 暗号化が無効なパリティグループを削除します。
   コマンド：

```
raidcom delete parity_grp
```

2. 暗号化が有効なパリティグループを作成します。
   コマンド：

```
raidcom add parity_grp
```

ヒント
暗号化を有効にしたパリティグループを作成するには、-encryption オプションで enable を指定します。

3.5 暗号化を無効にする

暗号化を有効にしたパリティグループの暗号化設定を無効に変更できません。代わりに、暗号化が有効なパリティグループを一度削除した後に、暗号化が無効なパリティグループを作成することで、暗号化を無効にします。

ただし、前述の方法は、パリティグループにボリュームが存在しない場合に限ります。

この手順は、RAID Manager で操作します。各コマンドの使用方法は『RAID Manager コマンドリファレンス』を参照してください。

前提条件

- 必要なロール：ストレージ管理者（プロビジョニング）

操作手順

1. 暗号化が有効なパリティグループを削除します。
   コマンド：

```
raidcom delete parity_grp
```

2. 暗号化が無効なパリティグループを作成します。
   コマンド：

```
raidcom add parity_grp
```

3.6 暗号化鍵のリストア

一次バックアップでバックアップした暗号化鍵を含め、ストレージシステム内の暗号化鍵が使用できなくなった場合は、二次バックアップでバックアップした暗号化鍵をリストアします。

暗号化鍵のリストアは、バックアップ済みの暗号化鍵（未使用鍵、DEK を含む）のうち、鍵情報を紛失した暗号化鍵に対して一括して実施されます。ただし、ドライブの保守などのときに、削除された暗号化鍵、あるいは手動操作で明示的に削除した未使用鍵はリストアされません。

注意
最新の暗号化鍵をリストアしてください。最新の暗号化鍵を含まない二次バックアップはリストアできません。最新の暗号化鍵のバックアップがなく暗号鍵のリストアができない場合には、「4.2 お問い合わせ先」へお問い合わせください。

注意
暗号化鍵をリストアするには、暗号化鍵が設定されているパリティグループに属するプールボリュームがすべて閉塞状態である必要があります。また、暗号化鍵のリストア後は、暗号化鍵が設定されているパリティグループに属するプールボリュームをすべて回復する必要があります。

二次バックアップからの暗号化鍵のリストアは、管理ツールの操作端末内にバックアップしたファイルからリストアする方法と、鍵管理サーバに接続してリストアする方法があります。

関連タスク

- 3.6.1 管理ツールの操作端末内にバックアップしたファイルから暗号化鍵をリストアする
- 3.6.2 鍵管理サーバに接続して暗号化鍵をリストアする

3.6.1 管理ツールの操作端末内にバックアップしたファイルから暗号化鍵をリストアする

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 管理ツールの操作端末にバックアップしたファイルから、 暗号化鍵をリストアします。
   リクエストライン：

```
POST ＜ベース URL ＞/v1/objects/encryption-keys/file/actions/restore/invoke
```

関連概念

- 1.3.3 暗号化鍵のリストア機能
- 3.6 暗号化鍵のリストア

3.6.2 鍵管理サーバに接続して暗号化鍵をリストアする

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 鍵管理サーバから、 暗号化鍵をリストアします。
   リクエストライン：

```
POST ＜ベース URL ＞/v1/objects/encryption-keys/kms/actions/restore/
invoke
```

関連概念

- 1.3.3 暗号化鍵のリストア機能
- 1.3.4 鍵管理サーバを使用した暗号化鍵の操作
- 3.6 暗号化鍵のリストア

3.7 暗号化鍵の削除

暗号化鍵の削除は、次の場合に実施します。

- 暗号化環境設定の変更により、暗号化鍵の生成場所をストレージシステムから鍵管理サーバに変更する場合
- 鍵管理サーバを別サーバに移行した際に、過去に生成した暗号化鍵ではなく、新たに生成した暗号化鍵を使用する場合

メモ
暗号化鍵の削除後は、「3.2 暗号化鍵を作成する」の手順に従い、作成可能な最大数の暗号化鍵の生成を推奨します。

関連タスク

- 3.1 暗号化環境の設定
- 3.2 暗号化鍵を作成する
- 3.7.1 ストレージシステム内の暗号化鍵を削除する

3.7.1 ストレージシステム内の暗号化鍵を削除する

未使用鍵（属性が「空き」（鍵種別が FREE）の暗号化鍵）を削除します。ほかの属性の暗号化鍵は削除できません。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. ストレージシステム内の暗号化鍵を削除します。
   - リクエストの body で指定した暗号化鍵を削除する場合
     リクエストライン：

```
POST ＜ベース URL ＞/v1/services/encryption-key-service/actions/
delete/invoke
```

   - 鍵の ID を指定して削除する場合

リクエストライン：

```
DELETE ＜ベース URL ＞/v1/objects/encryption-keys/＜オブジェクト ID ＞
```

関連概念

- 3.7 暗号化鍵の削除

3.8 鍵暗号化鍵の更新

3.8.1 鍵暗号化鍵を更新する

REST API で鍵暗号化鍵を更新できます。鍵暗号化鍵を更新したらすぐに暗号化鍵のバックアップを行ってください。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 鍵暗号化鍵を更新します。
   リクエストライン：

```
POST ＜ベース URL ＞/v1/objects/encryption-keys/kek/actions/rekey/invoke
```

3.9 鍵管理サーバを別サーバへ移行する

鍵管理サーバを別サーバへ移行する場合は、プライマリサーバとセカンダリサーバの設定項目を、新しい鍵管理サーバに合わせて変更してください。鍵管理サーバの接続先を変更すると、新たに設定した鍵管理サーバに暗号化鍵のバックアップが行われます。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 移行後に使用する鍵管理サーバとの接続を設定します。
   リクエストライン：

```
PATCH ＜ベース URL ＞/v1/objects/kms-settings/＜オブジェクト ID ＞
```

メモ

鍵管理サーバ自体を変更する場合は、鍵管理サーバ移行フラグ `isMigration` を `true` に設定してください。移行先の鍵管理サーバに鍵暗号化鍵、暗号鍵のバックアップが登録されます。
鍵管理サーバ自体を変更しないで、IP アドレスやホスト名その他の設定を変更する場合は、鍵管理サーバ移行フラグ `isMigration` を `false` にして実行してください。鍵管理サーバには新たに鍵暗号化鍵、暗号鍵のバックアップは登録されません。

注意
鍵管理サーバを別サーバへ移行する設定作業の途中で、ストレージシステムの電源を OFF にしないでください。
上記の設定作業の途中でストレージシステムの電源を OFF にすると、電源を ON にしたときに、鍵管理サーバにバックアップした鍵暗号化鍵および暗号化鍵を取得できないため、データを復号化できなくなります。

注意
すべてのボリュームが閉塞し、SIM コード 661000 または 661001（鍵管理サーバからの暗号化鍵取得失敗）が報告されてた場合は、鍵管理サーバの移行を実施する前に、必ず以下の操作を実施してください。

1. 移行前の鍵管理サーバとの接続を回復させてください。
2. 鍵管理サーバとの接続テストが正常終了することを確認してください。
3. お問い合わせ先に連絡し、ストレージシステムの再起動を依頼してください。

3.10 暗号化環境設定を初期化する

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール
- 暗号化が有効なパリティグループが存在しないこと。

操作手順

1. 設定済みの暗号化環境設定を初期化します。
   リクエストライン：

```
PATCH ＜ベース URL ＞/v1/objects/encryption-settings/instance
```

ヒント
暗号化環境設定を初期化するには、属性 `isEnabled` および属性 `usesKms` に `false` を指定します。

2. 鍵管理サーバの設定を削除します。
   リクエストライン：

```
DELETE ＜ベース URL ＞/v1/objects/kms-settings/＜オブジェクト ID ＞
```

3.11 鍵管理サーバで使用する暗号化環境設定スクリプト

REST API を呼び出して、鍵管理サーバの環境構築、初期化を実施する際の参考情報として、Python で書かれたスクリプトを提供します。

3.11.1 スクリプトの概要

各種スクリプトファイルには、鍵管理サーバ証明書のアップロードや鍵管理サーバ設定の追加など、クライアントプログラムで必要な初期設定および初期化処理のコードが含まれています。

初期設定スクリプトの概要

鍵管理サーバの環境を構築するためのスクリプトです。

注意
鍵管理サーバが設定されていない状態で初期設定スクリプトを実行してください。
鍵管理サーバが設定されている状態で初期設定スクリプトを実行するとエラーになります。

- ESM にログインする。
- ストレージシステムにクライアント証明書をアップロードする。
- ストレージシステムにルート証明書をアップロードする。
- 証明書一覧を取得する。
- 鍵管理サーバを登録する。
- 暗号化環境設定を有効化する。
- ESM からログアウトする。

初期化スクリプトの概要

初期設定スクリプト実行時に、エラーが発生した場合など、行った設定を初期化するためのスクリプトです。

- ESM にログインする。
- 暗号化環境設定の状態を取得する。
- 暗号化環境設定を無効化する。
- 鍵管理サーバを削除する。
- 証明書一覧を取得する。
- ルート証明書とクライアント証明書を削除する。
- ESM からログアウトする。

スクリプトファイルの取得方法

各種スクリプトファイルは、下記の URL からダウンロードした kmip.zip ファイルを解凍して、取得してください。

- kmip.zip ファイルの URL

```
https://<サービス IP アドレス>/download/restapi/kmip.zip
```

- kmip.zip ファイルに格納されているファイル
  - setup_kms.py

    初期設定スクリプトファイルです。
  - init_kms.py

    初期化スクリプトファイルです。
  - block_storage_api.py

    リクエストラインを生成する関数を、BlockStorageAPI クラスとして定義したファイルです。
  - storage_param.py

ストレージシステムの情報を定義したファイルです。

3.11.2 スクリプト実行環境設定

- 各種スクリプトは、スクリプト言語の Python で作成されています。Python の公式サイト（https://www.python.org/）から Python をダウンロードし、動作環境を構築してください。
- このマニュアルに記載しているスクリプトでは、標準ライブラリ（json、sys、http.client、time、traceback）を使用します。
  また、標準ライブラリのほかに、サードパーティライブラリである Requests ライブラリを使用します。Requests ライブラリのダウンロードページ (https://pypi.org/project/requests/)から、最新版の Requests ライブラリをダウンロードしてください。
- 各種スクリプトは、Python3.11.0 および Requests2.31.0 の環境で動作確認しています。

Requests ライブラリのインストール方法

- オンライン環境の場合

  1. - proxy 環境下でインストールする場合：
       コマンドプロンプトを起動して、次のコマンドを実行してください。

       ```
       set https_proxy=プロキシサーバアドレス:プロキシサーバポート
       ```

     - proxy 環境を利用しない場合：
       本手順は、スキップしてください。
  2. コマンドプロンプトにて以下のコマンドを実行してください。

     ```
     pip install requests
     ```

- オフライン環境の場合

  1. 以下の Requests ライブラリのダウンロードページから 最新版の requests-X.XX.XX-py3-none-any.whl ファイルをダウンロードしてください。
     https://pypi.org/project/requests/#files
  2. ダウンロードしたインストールファイルを、記憶媒体などを用いてオフライン環境のフォルダにコピーしてください。
  3. コマンドプロンプトを起動して、コピーしたインストールファイルのフォルダに移動して、以下のコマンドを実行してください。コマンドの X の箇所は、ダウンロードした whl ファイルと同じにしてください。

     ```
     pip install requests-X.XX.XX-py3-none-any.whl
     ```

3.11.3 初期設定スクリプトの実行方法

鍵管理サーバの初期設定スクリプトについて説明します。

前提条件

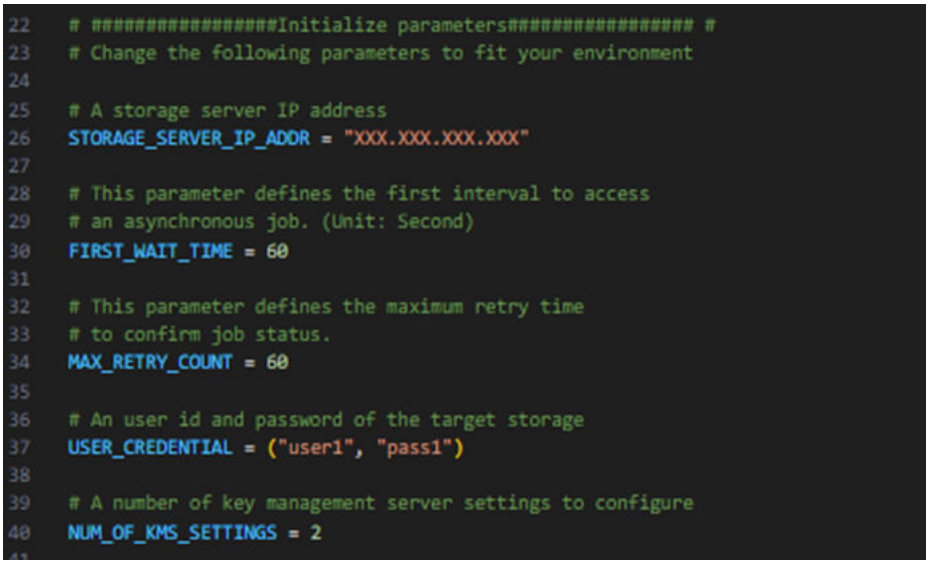
- Encryption License Key ライセンスがインストールされていること
- 暗号化が有効なパリティグループが作成されてないこと

パラメータの設定

初期設定スクリプト setup_kms.py の `Initialize parameters` にあるパラメータを必要に応じて、システムの環境や要件に合わせた設定に変更してください。次の表の設定例に記載している値は、入力例です。

パラメータ	設定例	説明
STORAGE_SERVER_IP_ADDR	"XXX.XXX.XXX.XXX"	ESM のサービス IP アドレスです。
FIRST_WAIT_TIME	60	非同期処理の実行結果を取得する 1 回目の間隔（秒）です。1～120 までの値を指定できます。通常は変更する必要はありません。
MAX_RETRY_COUNT	60	非同期処理の実行結果を取得する最大リトライ回数です。1～60 までの値を指定できます。通常は変更する必要はありません。
USER_CREDENTIAL	`("user1", "pass1")`	ストレージシステムでの認証に使用する認証情報です。設定値の例は、ユーザ ID が user1、パスワードが pass1 の場合の設定例です。ユーザには、セキュリティ管理者（参照・編集）ロールが必要です。
NUM_OF_KMS_SETTINGS	2	鍵管理サーバの設定台数です。1～2 までの値を指定できます。設定値の例は鍵管理サーバを 2 台設定し、クライアント証明書とルート証明書をそれぞれ 2 つずつアップロードする場合の例です。

下図に示す初期設定スクリプト setup_kms.py の 25 行目～40 行目のパラメータを、システムの環境や要件に合わせた設定に変更してください。



```
22  # ##################Initialize parameters################## #
23  # Change the following parameters to fit your environment
24
25  # A storage server IP address
26  STORAGE_SERVER_IP_ADDR = "XXX.XXX.XXX.XXX"
27
28  # This parameter defines the first interval to access
29  # an asynchronous job. (Unit: Second)
30  FIRST_WAIT_TIME = 60
31
32  # This parameter defines the maximum retry time
33  # to confirm job status.
34  MAX_RETRY_COUNT = 60
35
36  # An user id and password of the target storage
37  USER_CREDENTIAL = ("user1", "pass1")
38
39  # A number of key management server settings to configure
40  NUM_OF_KMS_SETTINGS = 2
```

鍵管理サーバの証明書設定

ストレージシステムへアップロードする鍵管理サーバのクライアント証明書とルート証明書の設定を説明します。

初期設定スクリプト setup_kms.py の `Initialize parameters` にあるパラメータを書き換えて設定してください。

証明書ファイルの格納先のパスはクライアント証明書とルート証明書ごとの共通の設定値を指定してください。それ以外のパラメータについては以下のとおりに設定してください。

- 鍵管理サーバを 1 台登録する場合：
  設定する証明書の設定値を設定してください。
  ［鍵管理サーバに割り当てる証明書のパラメータ設定値］
- 鍵管理サーバを 2 台登録する場合：
  設定する証明書の設定値をカンマ区切りで設定してください。
  ［鍵管理サーバ 1 台目に割り当てる証明書のパラメータ設定値,2 台目に割り当てる証明書のパラメータ設定値］

パラメータ	設定例	説明
CLIENT_CERT_FILE_PATH	"D:/cert/"	クライアント証明書ファイルの格納先のパスです。事前に鍵管理サーバのクライアント証明書ファイルを用意してください。
CLIENT_CERT_FILE_NAME_LIST	["clientCert1.p12", "clientCert2.p12"]	登録するクライアント証明書ごとのファイル名を指定してください。
CLIENT_CERT_FILE_NICKNAME_LIST	["clientCert1", "clientCert2"]	登録するクライアント証明書ごとのニックネームを 1～255 文字の半角英数字で指定してください。1 台目と 2 台目で重複したニックネームは指定できません。
CLIENT_CERT_FILE_PASSWORD_LIST	["clientCertPass1", "clientCertPass2"]	クライアント証明書ファイルのパスワードを 1～128 文字の半角英数記号で指定してください。パスワードなしのクライアント証明書の場合は""(空文字)と指定してください。
ROOT_CERT_FILE_PATH	"D:/cert/"	ルート証明書ファイルの格納先のパスです。事前に鍵管理サーバのルート証明書ファイルを用意してください。
ROOT_CERT_FILE_NAME_LIST	["rootCert1.pem", "rootCert2.pem"]	登録するルート証明書ごとのファイル名を指定してください。
ROOT_CERT_FILE_NICKNAME_LIST	["rootCert1", "rootCert2"]	ルート証明書のニックネームを 1～255 文字の半角英数字で指定してください。1 台目と 2 台目で重複したニックネームは指定できません。

下図に示す初期設定スクリプト setup_kms.py の 42 行目～61 行目のパラメータを、使用したい鍵管理サーバのクライアント証明書とルート証明書に合わせた値に変更してください。

鍵管理サーバの設定

使用する鍵管理サーバの情報の設定を説明します。

初期設定スクリプト setup_kms.py の `Initialize parameters` にあるパラメータを書き換えて設定してください。

鍵管理サーバの各パラメータの設定値は以下のとおりに設定してください。

- 設定する鍵管理サーバを 1 台登録する場合：
  設定する証明書の設定値を設定してください。
  ［鍵管理サーバのパラメータ設定値］
- 鍵管理サーバを 2 台登録する場合：
  設定する鍵管理サーバの設定値をカンマ区切りで設定してください。
  ［鍵管理サーバ 1 台目のパラメータ設定値,鍵管理サーバ 2 台目のパラメータ設定値］

パラメータ	設定例	説明
KMS_ID_LIST	`["0", "1"]`	登録する鍵管理サーバごとの鍵管理サーバ番号です。0～1 の値を指定します。鍵管理サーバを 1 台登録する場合は["0"]と指定し鍵管理サーバを 2 台登録する場合は["0","1"]または["1","0"]と指定してください。
INTRA_CLASS_PRIORITY_LIST	`[1, 2]`	鍵管理サーバがマルチマスタクラスタを組んでいる場合のクラスタ内の優先順位の設定です。鍵管理サーバを 1 台登録する場合は[1]と指定し鍵管理サーバを 2 台登録する場合は[1,2]もしくは[2,1]と指定してください。
KMS_SERVER_NAME_LIST	`["XXX.XXX.XXX.XXX", "XXX.XXX.XXX.XXX"]`	登録する鍵管理サーバごとの IP アドレスまたはホスト名 IPv4、IPv6 の IP アドレス、またはホスト名の形式で指定してください。
KMS_SERVER_PORT_LIST	`[5696, 5696]`	登録する鍵管理サーバごとのポート番号です。設定例で示している値はデフォルト値です。
NUM_OF_RETRIES_LIST	`[3, 3]`	登録する鍵管理サーバごとの通信に失敗した場合のリトライ回数です。1～50 の値を指定します。設定例で示している値はデフォルト値です。
RETRY_INTERVAL_LIST	`[10, 10]`	登録する鍵管理サーバごとの通信に失敗した場合のリトライ間隔（秒）です。1～60 の値を指定します。設定例で示している値はデフォルト値です。
TIMEOUT_LIST	`[120, 120]`	登録する鍵管理サーバごとの接続がタイムアウトするまでの時間（秒）です。10～999 の値を指定します。設定例で示している値はデフォルト値です。

下図に示す初期設定スクリプト setup_kms.py の 64 行目～82 行目のパラメータを、設定したい鍵管理サーバの情報に変更してください。

```
63  # A key management server id
64  KMS_ID_LIST = ["0", "1"]
65
66  # A key management server intro class priority
67  INTRA_CLASS_PRIORITY_LIST = [1, 2]
68
69  # A key management server name or IP address
70  KMS_SERVER_NAME_LIST = [ "XXX.XXX.XXX.XXX", "XXX.XXX.XXX.XXX" ]
71
72  # A key management server port number
73  KMS_SERVER_PORT_LIST = [5696, 5696]
74
75  # A number of retries
76  NUM_OF_RETRIES_LIST = [3, 3]
77
78  # A retry interval
79  RETRY_INTERVAL_LIST = [10, 10]
80
81  # A timeout
82  TIMEOUT_LIST =[120, 120]
83
84  ############################################################
```

証明書ファイルの保存

追加する鍵管理サーバごとに鍵管理サーバのルート証明書とクライアント証明書を、鍵管理サーバの証明書設定の CLIENT_CERT_FILE_PATH と ROOT_CERT_FILE_PATH で指定したパスに格納してください。

初期設定スクリプト setup_kms.py の実行

1. コマンドプロンプトを起動します。下記のコマンドを入力して、スクリプトファイルを格納したフォルダに移動してください。

```
cd スクリプトファイルを格納したフォルダのパス
```

2. コマンドプロンプトに下記のコマンドを入力して、スクリプトを実行してください。

```
python setup_kms.py
```

3.11.4 初期化スクリプトの実行方法

鍵管理サーバの初期化設定のコードについて説明します。

前提条件

- Encryption License Key ライセンスがインストールされていること
- 暗号化が有効なパリティグループが作成されてないこと

パラメータの設定

初期化スクリプト init_kms.py の Initialize parameters にあるパラメータを必要に応じて、システムの環境や要件に合わせた設定に変更してください。次の表の設定例に記載している値は、入力例です。

パラメータ	設定例	説明
STORAGE_SERVER_IP_ADDR	"XXX.XXX.XXX.XXX"	ESM のサービス IP アドレスです。
FIRST_WAIT_TIME	60	非同期処理の実行結果を取得する 1 回目の間隔（秒）です。1～120 までの値を指定できます。通常は変更する必要はありません。
MAX_RETRY_COUNT	60	非同期処理の実行結果を取得する最大リトライ回数です。1～60 までの値を指定できます。通常は変更する必要はありません。
USER_CREDENTIAL	("user1", "pass1")	ストレージシステムでの認証に使用する認証情報です。設定値の例は、ユーザ ID が user1、パスワードが pass1 の場合の設定例です。ユーザには、セキュリティ管理者（参照・編集）ロールが必要です。

下図に示す初期化スクリプト init_kms.py の 25 行目～37 行目のパラメータを、システムの環境や要件に合わせた設定に変更してください。

```
22  # ##################Initialize parameters################## #
23  # Change the following parameters to fit your environment
24
25  # A storage server IP address
26  STORAGE_SERVER_IP_ADDR = "XXX.XXX.XXX.XXX"
27
28  # This parameter defines the first interval to access
29  # an asynchronous job. (Unit: Second)
30  FIRST_WAIT_TIME = 60
31
32  # This parameter defines the maximum retry time
33  # to confirm job status.
34  MAX_RETRY_COUNT = 60
35
36  # An user id and password of the target storage
37  USER_CREDENTIAL = ("user1", "pass1")
38
39  ############################################################
```

初期化スクリプト init_kms.py の実行

1. コマンドプロンプトを起動します。下記のコマンドを入力して、スクリプトファイルを格納したフォルダに移動してください。

```
cd スクリプトファイルを格納したフォルダのパス
```

2. コマンドプロンプトに下記のコマンドを入力して、スクリプトを実行してください。

```
python init_kms.py
```

3.11.5 スクリプト実行結果の確認

コマンドプロンプトにてスクリプトを実行した際に、完了時にログが出力されます。必ず実行結果を確認してください。

- 正常終了した場合：
  以下のメッセージが出力されて、スクリプトが正常終了します。

```
Operation was completed.
```

- 異常終了した場合：
  以下のメッセージが出力されて、スクリプトが異常終了します。

```
An error occurred while running the script.
Please check the error message.
```

  指定したパラメータに間違いがあった場合、スクリプトを実行が中断され、スクリプトを実行したコマンドプロンプトにエラーメッセージが出力されます。 コマンドプロンプトに出力されたエラーメッセージを確認して、パラメータの設定を変更してください。

4

Encryption License Key のトラブルシューティング

ここでは、トラブルシューティングについて説明します。

4.1 Encryption License Key 操作時のトラブルと対策

Encryption License Key の操作中に発生したトラブルと対処方法について次に示します。

トラブル	対策
暗号化鍵の操作（バックアップ／リストア）が失敗した。	次のことを確認してください。 ・ Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか ・ セキュリティ管理者（参照・編集）ロールが割り当てられているか ・ 鍵管理サーバに接続してバックアップ／リストアしている場合、鍵管理サーバとの接続に問題はないか ・ 鍵管理サーバに接続してバックアップしている場合、鍵管理サーバがバックアップできる鍵の数を超えていないか ・ 鍵管理サーバに接続してバックアップ／リストアしている場合、鍵管理サーバ内の鍵の数が増えたことでタイムアウトが発生していないか ・ 鍵管理サーバに接続してバックアップ／リストアしている場合、ストレージシステムと鍵管理サーバの時刻が一致しているか ・ 最新の暗号化鍵をリストアしているか、二次バックアップ後に暗号化鍵が変更されていないか ・ ストレージシステムと鍵管理サーバとの SSL/TLS 通信や証明書の要件を満たしているか、『システム管理者ガイド』のストレージシステムと外部サーバ間の SSL/TLS 通信の記載を参照して、確認してください。 上記を確認後、再度暗号化鍵の操作（バックアップ／リストア）を実施してください。
暗号化鍵の作成操作が失敗した。	次のことを確認してください。 ・ Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか ・ セキュリティ管理者（参照・編集）ロールが割り当てられているか ・ 鍵管理サーバに接続して暗号化鍵を生成している場合、鍵管理サーバとの接続に問題はないか ・ 鍵管理サーバに接続して暗号化鍵を生成している場合、ストレージシステムと鍵管理サーバの時刻が一致しているか ・ ストレージシステムと鍵管理サーバとの SSL/TLS 通信や証明書の要件を満たしているか、『システム管理者ガイド』のストレージシステムと外部サーバ間の SSL/TLS 通信の記載を参照して、確認してください。 上記を確認後、暗号化鍵の一覧を参照し、暗号化鍵が作成されているかどうか確認してください。

トラブル	対策
	暗号化鍵の一覧参照手順は、『REST API リファレンスガイド』の暗号化鍵の一覧を取得するを参照してください。 ・ 暗号化鍵が作成されていた場合 暗号化鍵の作成は成功しています。暗号化鍵の外部バックアップを実施してください。 ・ 暗号化鍵が作成されていない場合 再度暗号化鍵の作成を実施してください。鍵管理サーバに接続していない場合は、暗号化鍵の作成が成功した後、手動で管理ツールの操作端末内に、ファイルとしてバックアップしてください。
暗号化鍵の削除に失敗した。	次のことを確認してください。 ・ Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか ・ セキュリティ管理者（参照・編集）ロールが割り当てられているか ・ 鍵管理サーバに接続して暗号化鍵を削除している場合、鍵管理サーバとの接続に問題はないか ・ 鍵管理サーバに接続して暗号化鍵を削除している場合、ストレージシステムと鍵管理サーバの時刻が一致しているか ・ ストレージシステムと鍵管理サーバとのSSL/TLS 通信や証明書の要件を満たしているか、『システム管理者ガイド』のストレージシステムと外部サーバ間の SSL/TLS 通信の記載を参照して、確認してください。 上記を確認後、暗号化鍵の一覧を参照して、暗号化鍵が削除されているかどうか確認してください。 暗号化鍵の一覧参照手順は、『REST API リファレンスガイド』の暗号化鍵の一覧を取得するを参照してください。 ・ 暗号化鍵が削除されていた場合 対処不要です。 ・ 暗号化鍵が削除されていない場合 再度暗号化鍵の削除を実施してください。
テスト通信に失敗した。	・ 鍵管理サーバとの接続設定が正しいか、次の項目を確認してください。 ◦ ホスト名 ◦ ポート番号 ◦ クライアント証明書ファイル ◦ ルート証明書ファイル ・ テスト通信に時間がかかっている場合は、次の項目を調整すれば、通信が成功することがあります。 ◦ タイムアウト ◦ リトライ間隔 ◦ リトライ回数 ・ ストレージシステムと鍵管理サーバの時刻が一致しているか

トラブル	対策
	• ストレージシステムと鍵管理サーバとの SSL/TLS 通信や証明書の要件を満たしているか、『システム管理者ガイド』のストレージシステムと外部サーバ間の SSL/TLS 通信の記載を参照して、確認してください。
暗号化環境設定に失敗した（暗号化の無効から有効への設定）。	次のことを確認してください。 • Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか • セキュリティ管理者（参照・編集）ロールが割り当てられているか • 鍵管理サーバに接続してバックアップ／リストアしている場合、鍵管理サーバとの接続に問題はないか • ストレージシステムと鍵管理サーバとの SSL/TLS 通信や証明書の要件を満たしているか、『システム管理者ガイド』のストレージシステムと外部サーバ間の SSL/TLS 通信の記載を参照して、確認してください。 • 鍵管理サーバに接続している場合、鍵管理サーバがバックアップできる鍵の数を超えていないか • 鍵管理サーバに接続している場合、ストレージシステムと鍵管理サーバの時刻が一致しているか 上記を確認後、暗号化環境設定の初期化を実行してください。暗号化環境設定の初期化が正常に終了したことを確認してから、再度暗号化環境設定を実施してください。
暗号化環境設定に失敗した（暗号化を有効に設定された状態で、鍵管サーバの使用有無の変更）。	次のことを確認してください。 • Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか • セキュリティ管理者（参照・編集）ロールが割り当てられているか • ストレージシステムと鍵管理サーバとの SSL/TLS 通信や証明書の要件を満たしているか、『システム管理者ガイド』のストレージシステムと外部サーバ間の SSL/TLS 通信の記載を参照して、確認してください。 • 鍵管理サーバに接続している場合、鍵管理サーバがバックアップできる鍵の数を超えていないか • 鍵管理サーバに接続している場合、ストレージシステムと鍵管理サーバの時刻が一致しているか 上記を確認後、鍵管理サーバと連携する設定状態（有効／無効）を確認してください。 • 設定が変更されていた場合 暗号化環境設定は成功しています。暗号化鍵の外部バックアップを実施してください。 • 設定が変更されていない場合 暗号化環境設定を再度実施してください。暗号化環境設定が成功した後、外部バックアップを実施してください。

トラブル	対策
	外部バックアップ先は、鍵管理サーバを使用するかどうかに応じて、鍵管理サーバまたはファイルになります。
暗号化鍵の操作が、次のどれかのエラーコードで失敗した。 • 36162-00204208 • 36162-00204209 • 36162-00204224	次の対策を実施してください。 • すべてのボリュームが閉塞し、SIM コード 661000、661001 が報告された場合 1. 鍵管理サーバとの接続を回復させて、接続テストが正常終了することを確認してください。 2. 「4.2 お問い合わせ先」に連絡して、ストレージシステムの再起動を依頼してください。 3. ストレージシステムの再起動後、閉塞していたすべてのボリュームが回復していることを確認してください。 • その他の場合 1. ストレージシステムの状態を確認し、ボリュームの閉塞部位があれば回復してください。 2. ボリュームの閉塞部位を回復後、失敗した暗号化鍵の操作を再度実施してください。
テスト通信は成功したが、エラーコード 36162-00204225 が表示された。	鍵管理サーバの設定に必要な機能が、接続している鍵管理サーバではサポートされていません。 「2.2 鍵管理サーバの要件」を確認して、鍵管理サーバのソフトウェアを最新にしてください。
SIM コード 660100 または 660200 が報告された。	未使用鍵（属性が「空き」（鍵種別が FREE）の暗号化鍵）の数が保守作業に必要なしきい値を下回っている可能性があります。 作成可能な最大数の暗号化鍵を作成しておくことを推奨します。
暗号化環境設定の初期化に失敗した。	次のことを確認してください。 • Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか • セキュリティ管理者（参照・編集）ロールが割り当てられているか • 鍵管理サーバに接続している場合、鍵管理サーバとの接続に問題はないか • 鍵管理サーバに接続している場合、ストレージシステムと鍵管理サーバの時刻が一致しているか • ストレージシステムと鍵管理サーバとの SSL/TLS 通信や証明書の要件を満たしているか、『システム管理者ガイド』のストレージシステムと外部サーバ間の SSL/TLS 通信の記載を参照して、確認してください。 上記を確認後、再度暗号化環境設定の初期化を実施してください。
鍵管理サーバの移行に失敗した。	次のことを確認してください。 • Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか

トラブル	対策
	• セキュリティ管理者（参照・編集）ロールが割り当てられているか • 鍵管理サーバに接続している場合、鍵管理サーバとの接続に問題はないか • 鍵管理サーバに接続している場合、ストレージシステムと鍵管理サーバの時刻が一致しているか • ストレージシステムと鍵管理サーバとのSSL/TLS 通信や証明書の要件を満たしているか、『システム管理者ガイド』のストレージシステムと外部サーバ間の SSL/TLS 通信の記載を参照して、確認してください。 • 鍵管理サーバに接続している場合、鍵管理サーバがバックアップできる鍵の数を超えていないか 上記を確認後、鍵管理サーバの設定を参照して、鍵管理サーバの設定が更新されているかどうか確認してください。 • 鍵管理サーバの設定が更新されていた場合 一度、鍵管理サーバ移行前の設定（鍵管理サーバ移行フラグ isMigration=false）に戻してから、再度鍵管理サーバの移行を実施してください。 • 鍵管理サーバの設定が更新されていない場合 鍵管理サーバの移行を再度実施してください。

4.2 お問い合わせ先

- 保守契約をされているお客様は、以下の連絡先にお問い合わせください。
  日立サポートサービス：http://www.hitachi-support.com/
- 保守契約をされていないお客様は、担当営業窓口にお問い合わせください。

A

このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報を示します。

A.1 操作対象リソースについて

このマニュアルで説明している機能を使用するときには、各操作対象のリソースが特定の条件を満たしている必要があります。

各操作対象のリソースの条件については『システム構築ガイド』を参照してください。

A.2 このマニュアルでの表記

このマニュアルで使用している表記を次の表に示します。

表記	製品名
Hitachi Virtual Storage Platform One Block 20	次の製品を区別する必要がない場合の表記です。 ・ Hitachi Virtual Storage Platform One Block 23 ・ Hitachi Virtual Storage Platform One Block 26 ・ Hitachi Virtual Storage Platform One Block 28
VSP One B20	Hitachi Virtual Storage Platform One Block 20

A.3 このマニュアルで使用している略語

このマニュアルで使用している略語を次の表に示します。

略語	フルスペル
LDEV	Logical DEVice
SIM	Service Information Message

A.4 KB（キロバイト）などの単位表記について

1KB（キロバイト）は 1,024 バイト、1MB（メガバイト）は 1,024KB、1GB（ギガバイト）は 1,024MB、1TB（テラバイト）は 1,024GB、1PB（ペタバイト）は 1,024TB です。

1block（ブロック）は 512 バイトです。

用語解説

（英字）

ALUA

（Asymmetric Logical Unit Access）
SCSI の非対称論理ユニットアクセス機能です。
ストレージ同士、またはサーバとストレージシステムを複数の冗長パスで接続している構成の場合に、どのパスを優先して使用するかをストレージシステムに定義して、I/O を発行できます。優先して使用するパスに障害が発生した場合は、他のパスに切り替わります。

bps

（bits per second）
データ転送速度の標準規格です。

CHAP

（Challenge Handshake Authentication Protocol）
認証方式のひとつ。ネットワーク上でやり取りされる認証情報はハッシュ関数により暗号化されるため、安全性が高いです。

CHB

（Channel Board）
詳しくは「チャネルボード」を参照してください。

CM

（Cache Memory（キャッシュメモリ））
詳しくは「キャッシュ」を参照してください。

CNA

（Converged Network Adapter）
HBA と NIC を統合したネットワークアダプタ。

CRC

（Cyclic Redundancy Check）
巡回冗長検査。コンピュータデータに対し、偶発的変化を検出するために設計された誤り訂正符号。

CSV

（Comma Separate Values）

データベースソフトや表計算ソフトのデータをファイルとして保存するフォーマットの 1 つで、主にアプリケーション間のファイルのやり取りに使われます。それぞれの値はコンマで区切られています。

CTG

（Consistency Group）
詳しくは「コンシステンシーグループ」を参照してください。

CU

（Control Unit（コントロールユニット））
主に磁気ディスク制御装置を指します。

CV

（Customized Volume）
任意のサイズが設定された可変ボリュームです。

DDP

（Dynamic Drive Protection）
パリティグループを構成する各ドライブの領域を複数の領域に分割して、各ドライブ内の分割された領域の 1 つを、スペア用の領域として使用します。これにより、リビルド I/O、または Correction I/O を分散できるため、リビルド時間が短縮できます。

DDP 用のパリティグループ

DDP 機能が有効なパリティグループのことです。

DKBN

（Disk Board NVMe）
NVMe ドライブとキャッシュメモリ間のデータ転送を制御するモジュールです。

DKC

（Disk Controller）
ストレージシステムを制御するコントローラが備わっているシャーシ（筐体）です。

DKU

各種ドライブを搭載するためのシャーシ（筐体）です。
DB(Drive Box)と同義語となります。

DP-VOL

詳しくは「仮想ボリューム」を参照してください。

ECC

（Error Check and Correct）
ハードウェアで発生したデータの誤りを検出し、訂正することです。

ENC

ドライブボックスに搭載され、コントローラシャーシまたは他のドライブボックスとのインターフェース機能を有します。

ESM

（Embedded Storage Manager）
Hitachi Virtual Storage Platform One Block 20 における管理系ソフトウェアです。

ESMOS

（Embedded Storage Manager Operating System）
ESM を動作させるための OS や OSS を含んだファームウェアです。

ExG

（External Group）
外部ボリュームを任意にグループ分けしたものです。詳しくは「外部ボリュームグループ」を参照してください。

Failover

故障しているものと機能的に同等のシステムコンポーネントへの自動的置換。
この Failover という用語は、ほとんどの場合、同じストレージデバイスおよびホストコンピュータに接続されているインテリジェントコントローラに適用されます。
コントローラのうちの 1 つが故障している場合、Failover が発生し、残っているコントローラがその I/O 負荷を引き継ぎます。

FC

（Fibre Channel）
ストレージシステム間のデータ転送速度を高速にするため、光ケーブルなどで接続できるようにするインターフェースの規格のことです。

FC-NVMe

Fibre Channel ネットワーク越しにホストとストレージ間で、NVMe-oF 通信プロトコルによる通信をするための NVMe over Fabrics 技術のひとつです。

FM

（Flash Memory（フラッシュメモリ））
詳しくは「フラッシュメモリ」を参照してください。

GID

（Group ID）
ホストグループを作成するときに付けられる 2 桁の 16 進数の識別番号です。

GUI

（Graphical User Interface）
コンピュータやソフトウェアの表示画面をウィンドウや枠で分け、情報や操作の対象をグラフィック要素を利用して構成するユーザインターフェース。マウスなどのポインティングデバイスで操作することを前提に設計されます。

HBA

（Host Bus Adapter）
詳しくは「ホストバスアダプタ」を参照してください。

I/O モード

global-active device ペアのプライマリボリュームとセカンダリボリュームが、それぞれに持つ I/O の動作です。

I/O レート

ドライブへの入出力アクセスが 1 秒間に何回行われたかを示す数値です。単位は IOPS（I/Os per second）です。

In-Band 方式

RAID Manager のコマンド実行方式の 1 つです。コマンドを実行すると、管理ツールの操作端末またはサーバから、ストレージシステムのコマンドデバイスにコマンドが転送されます。

Initiator

属性が RCU Target のポートと接続するポートが持つ属性です。

iSNS

（Internet Storage Naming Service）
iSCSI デバイスで使われる、自動検出、管理および構成ツールです。
iSNS によって、イニシエータおよびターゲット IP アドレスの特定リストで個々のストレージシステムを手動で構成する必要がなくなります。代わりに、iSNS は、環境内のすべての iSCSI デバイスを自動的に検出、管理および構成します。

LACP

（Link Aggregation Control Protocol）
複数回線を 1 つの論理的な回線として扱うための制御プロトコル。

LAN ボード

コントローラシャーシに搭載され、ストレージシステムの管理、UPS とのインターフェース機能を有するモジュールです。

LDEV

（Logical Device（論理デバイス））
RAID 技術では冗長性を高めるため、複数のドライブに分散してデータを保存します。この複数のドライブにまたがったデータ保存領域を論理デバイスまたは LDEV と呼びます。ストレージ内の LDEV は、LDKC 番号、CU 番号、LDEV 番号の組み合わせで区別します。LDEV に任意の名前を付けることもできます。
このマニュアルでは、LDEV（論理デバイス）を論理ボリュームまたはボリュームと呼ぶことがあります。

LDEV 名

LDEV 作成時に、LDEV に付けるニックネームです。あとから LDEV 名の変更もできます。

LDKC

（Logical Disk Controller）
複数の CU を管理するグループです。各 CU は 256 個の LDEV を管理しています。

LUN

（Logical Unit Number）
論理ユニット番号です。オープンシステム用のボリュームに割り当てられたアドレスです。オープンシステム用のボリューム自体を指すこともあります。

LUN セキュリティ

LUN に設定するセキュリティです。LUN セキュリティを有効にすると、あらかじめ決めておいたホストだけがボリュームにアクセスできるようになります。

LUN パス、LU パス

オープンシステム用ホストとオープンシステム用ボリュームの間を結ぶデータ入出力経路です。

LUSE ボリューム

オープンシステム用のボリュームが複数連結して構成されている、1 つの大きな拡張ボリュームのことです。ボリュームを拡張することで、ポート当たりのボリューム数が制限されているホストからもアクセスできるようになります。

MP ユニット

データ入出力を処理するプロセッサを含んだユニットです。データ入出力に関連するリソース（LDEV、外部ボリューム、ジャーナル）ごとに特定の MP ユニットを割り当てると、性能をチューニングできます。特定の MP ユニットを割り当てる方法と、ストレージシステムが自動的に選択した MP ユニットを割り当てる方法があります。MP ユニットに対して自動割り当ての設定を無効にすると、その MP ユニットがストレージシステムによって自動的にリソースに割り当てられることはないため、特定のリソース専用の MP ユニットとして使用できます。

MU

（Mirror Unit）
1 つのプライマリボリュームと 1 つのセカンダリボリュームを関連づける情報です。

Namespace

複数 LBA 範囲をまとめた、論理ボリュームの空間のことです。

Namespace Globally Unique Identifier

Namespace を識別するための、グローバルユニーク性を保証する 16Byte の識別情報です。
SCSI LU での NAA Format6 で表現される、WWN に類似する情報です。

Namespace ID

NVM サブシステム上に作成された Namespace を、NVM サブシステムの中でユニークに識別するための識別番号です。

NGUID

（Namespace Globally Unique Identifier）
詳しくは、「Namespace Globally Unique Identifier」を参照してください。

NQN

（NVMe Qualified Name）
NVMe-oF 通信プロトコルで、NVMe ホストまたは NVM サブシステムを特定するためのグローバルユニークな識別子です。

NSID

（Namespace ID）
Namespace を特定するための、4Byte の識別情報です。

NVM

（Non-Volatile Memory）
不揮発性メモリです。

NVMe

（Non-Volatile Memory Express）
PCI Express を利用した SSD の接続インタフェース、通信プロトコルです。

NVMe over Fabrics

NVMe-oF 通信プロトコルによる通信を、様々な種類のネットワークファブリックに拡張する NVMe のプロトコルです。

NVMe/TCP

TCP/IP ネットワーク越しにホストとストレージ間で、NVMe-oF 通信プロトコルによる通信をするための NVMe over Fabrics 技術のひとつです。

NVMe コントローラ

NVMe ホストからのコマンド要求を処理する、物理的または論理的な制御デバイスです。

NVM サブシステム

NVM のデータストレージ機能を提供する制御システムです。

NVM サブシステムポート

ホストとコントローラが、NVMe I/O をするための Fabric に接続する通信ポートです。

Out-of-Band 方式

RAID Manager のコマンド実行方式の 1 つです。コマンドを実行すると、クライアントまたはサーバから LAN 経由で ESM/RAID Manager サーバの中にある仮想コマンドデバイスにコマンドが転送されます。仮想コマンドデバイスからストレージシステムに指示を出し、ストレージシステムで処理が実行されます。

PCB

(Printed Circuit Board)
プリント基盤です。このマニュアルでは、コントローラボードやチャネルボード、ディスクボードなどのボードを指しています。

Point to Point

2 点を接続して通信するトポロジです。

Quorum ディスク

パスやストレージシステムに障害が発生したときに、global-active device ペアのどちらのボリュームでサーバからの I/O を継続するのかを決めるために使われます。外部ストレージシステムに設置します。

RAID

(Redundant Array of Independent Disks)
独立したディスクを冗長的に配列して管理する技術です。

RAID Manager

コマンドインタフェースでストレージシステムを操作するためのプログラムです。

RCU Target

属性が Initiator のポートと接続するポートが持つ属性です。

Read Hit 率

ストレージシステムの性能を測る指標の 1 つです。ホストがディスクから読み出そうとしていたデータが、どのくらいの頻度でキャッシュメモリに存在していたかを示します。単位はパーセントです。Read Hit 率が高くなるほど、ディスクとキャッシュメモリ間のデータ転送の回数が少なくなるため、処理速度は高くなります。

REST API

リクエストラインに simple を含まない REST API です。ストレージシステムの情報取得や構成変更することができます。

SAN

（Storage-Area Network）
ストレージシステムとサーバ間を直接接続する専用の高速ネットワークです。

SIM

（Service Information Message）
ストレージシステムのコントローラがエラーやサービス要求を検出したときに生成されるメッセージです。

SM

（Shared Memory）
詳しくは「シェアドメモリ」を参照してください。

SNMP

（Simple Network Management Protocol）
ネットワーク管理するために開発されたプロトコルの 1 つです。

SSL

（Secure Sockets Layer）
インターネット上でデータを安全に転送するためのプロトコルであり、Netscape Communications 社によって最初に開発されました。SSL が有効になっている 2 つのピア（装置）は、秘密鍵と公開鍵を利用して安全な通信セッションを確立します。どちらのピア（装置）も、ランダムに生成された対称キーを利用して、転送されたデータを暗号化します。

T10 PI

（T10 Protection Information）
SCSI で定義された保証コード基準の一つです。T10 PI では、512 バイトごとに 8 バイトの保護情報（PI）を追加して、データの検証に使用します。T10 PI にアプリケーションおよび OS を含めたデータ保護を実現する DIX（Data Integrity Extension）を組み合わせることで、アプリケーションからディスクドライブまでのデータ保護を実現します。

Target

ホストと接続するポートが持つ属性です。

UPS

（Uninterruptible Power System）
ストレージシステムが停電や、瞬停のときでも停止しないようにするために搭載してある予備の電源のことです。

URL

（Uniform Resource Locator）
リソースの場所や種類の両方を記載しているインターネット上の住所を記述する標準方式です。

UUID

（User Definable LUN ID）

ホストから論理ボリュームを識別するために、ストレージシステム側で設定する任意の ID です。

VDEV

（Virtual Device）
パリティグループ内にある論理ボリュームのグループです。VDEV 内に任意のサイズのボリューム（CV）を作成することもできます。

VLAN

（Virtual LAN）
スイッチの内部で複数のネットワークに分割する機能です（IEEE802.1Q 規定）。

VOLSER

（Volume Serial Number）
個々のボリュームを識別するために割り当てられる番号です。VSN とも呼びます。LDEV 番号や LUN とは無関係です。

VSP One Block Administrator

ストレージシステムの構成やリソースを操作するシンプルな GUI の管理ツールです。

VSP One Block Administrator の API

リクエストラインに simple を含む REST API です。
ストレージシステムの情報取得や構成変更することができます。

Windows

Microsoft® Windows® Operating System

Write Hit 率

ストレージシステムの性能を測る指標の 1 つです。ホストがディスクへ書き込もうとしていたデータが、どのくらいの頻度でキャッシュメモリに存在していたかを示します。単位はパーセントです。Write Hit 率が高くなるほど、ディスクとキャッシュメモリ間のデータ転送の回数が少なくなるため、処理速度は高くなります。

WWN

（World Wide Name）
ホストバスアダプタの ID です。ストレージ装置を識別するためのもので、実体は 16 桁の 16 進数です。

（ア行）

アクセス属性

ボリュームが読み書き可能になっているか（Read/Write）、読み取り専用になっているか（Read Only）、それとも読み書き禁止になっているか（Protect）どうかを示す属性です。

アクセスパス

ストレージシステム内の、データとコマンドの転送経路です。

エミュレーション

あるハードウェアまたはソフトウェアのシステムが、ほかのハードウェアまたはソフトウェアのシステムと同じ動作をすること（または同等に見えるようにすること）です。一般的には、

過去に蓄積されたソフトウェアの資産を役立てるためにエミュレーションの技術が使われます。

（カ行）

外部ストレージシステム

本ストレージシステムに接続されているストレージシステムです。

外部パス

本ストレージシステムと外部ストレージシステムを接続するパスです。外部パスは、外部ボリュームを内部ボリュームとしてマッピングしたときに設定します。複数の外部パスを設定することで、障害やオンラインの保守作業にも対応できます。

外部ボリューム

外部ボリュームグループに作成した LDEV のことです。マッピングした外部ストレージシステムのボリュームを実際にホストや他プログラムプロダクトから使用するためには、外部ボリュームグループに LDEV を作成する必要があります。

外部ボリュームグループ

外部ストレージシステムのボリュームをマッピングしている、本ストレージシステム内の仮想的なボリュームです。
外部ボリュームグループはパリティ情報を含みませんが、管理上はパリティグループと同じように取り扱います。

書き込み待ち率

ストレージシステムの性能を測る指標の 1 つです。キャッシュメモリに占める書き込み待ちデータの割合を示します。

仮想ボリューム

実体を持たない、仮想的なボリュームです。Dynamic Provisioning で使用する仮想ボリュームを DP-VOL とも呼びます。

監査ログ

ストレージシステムに対して行われた操作や、受け取ったコマンドの記録です。Syslog サーバへの転送設定をすると、監査ログは常時 Syslog サーバへ転送され、Syslog サーバから監査ログを取得・参照できます。

管理ツールの操作端末

ストレージシステムを操作するためのコンピュータです。

キャッシュ

チャネルとドライブの間にあるメモリです。中間バッファとしての役割があります。キャッシュメモリとも呼ばれます。

共用メモリ

詳しくは「シェアドメモリ」を参照してください。

クラスタ

ディスクセクターの集合体です。OS は各クラスタに対しユニークナンバーを割り当てし、それらがどのクラスタを使うかに応じて、ファイルの経過記録をとります。

形成コピー

ホスト I/O プロセスとは別に、プライマリボリュームとセカンダリボリュームを同期させるプロセスです。

更新コピー

形成コピー（または初期コピー）が完了したあとで、プライマリボリュームの更新内容をセカンダリボリュームにコピーして、プライマリボリュームとセカンダリボリュームの同期を保持するコピー処理です。

コピー系プログラムプロダクト

このストレージシステムに備わっているプログラムのうち、データをコピーするものを指します。ストレージシステム内のボリューム間でコピーするローカルコピーと、異なるストレージシステム間でコピーするリモートコピーがあります。

コマンドデバイス

ホストから RAID Manager コマンドを実行するために、ストレージシステムに設定する論理デバイスです。コマンドデバイスは、ホストから RAID Manager コマンドを受け取り、実行対象の論理デバイスに転送します。
Out-of-band 方式で接続された RAID Manager、もしくは内蔵 CLI を用いて設定してください。

コマンドデバイスセキュリティ

コマンドデバイスに適用されるセキュリティです。

コンシステンシーグループ

コピー系プログラムプロダクトで作成したペアの集まりです。コンシステンシーグループ ID を指定すれば、コンシステンシーグループに属するすべてのペアに対して、データの整合性を保ちながら、特定の操作を同時に実行できます。

（サ行）

サーバ証明書

サーバと鍵ペアを結び付けるものです。サーバ証明書によって、サーバは自分がサーバであることをクライアントに証明します。これによってサーバとクライアントは SSL を利用して通信できるようになります。サーバ証明書には、自己署名付きの証明書と署名付きの信頼できる証明書の 2 つの種類があります。

サブシステム NQN

NVM サブシステムに定義された NQN です。
NQN の詳細については、「NQN」を参照してください。

差分テーブル

コピー系プログラムプロダクトおよび Volume Migration で共有するリソースです。Volume Migration 以外のプログラムプロダクトでは、ペアのプライマリボリュームとセカンダリボリュームのデータに差分があるかどうかを管理するために使用します。Volume Migration では、ボリュームの移動中に、ソースボリュームとターゲットボリュームの差分を管理するために使用します。

シェアドメモリ

キャッシュ上に論理的に存在するメモリです。共用メモリとも呼びます。ストレージシステムの共通情報や、キャッシュの管理情報（ディレクトリ）などを記憶します。これらの情報を基

に、ストレージシステムは排他制御を行います。また、差分テーブルの情報もシェアドメモリで管理されており、コピーペアを作成する場合にシェアドメモリを利用します。

自己署名付きの証明書

自分自身で自分用の証明書を生成します。この場合、証明の対象は証明書の発行者と同じになります。ファイアウォールに守られた内部 LAN 上でクライアントとサーバ間の通信が行われている場合は、この証明書でも十分なセキュリティを確保できるかもしれません。

システムプールボリューム、システムプール VOL

プールを構成するプールボリュームのうち、1 つのプールボリュームがシステムプールボリュームとして定義されます。システムプールボリュームは、プールを作成したとき、またはシステムプールボリュームを削除したときに、優先順位に従って自動的に設定されます。なお、システムプールボリュームで使用可能な容量は、管理領域の容量を差し引いた容量になります。管理領域とは、プールを使用するプログラムプロダクトの制御情報を格納する領域です。

ジャーナルボリューム

Universal Replicator の用語で、プライマリボリュームからセカンダリボリュームにコピーするデータを一時的に格納しておくためのボリュームのことです。ジャーナルボリュームには、プライマリボリュームと関連づけられているマスタジャーナルボリューム、およびセカンダリボリュームと関連づけられているリストアジャーナルボリュームとがあります。

シュレッディング

ダミーデータを繰り返し上書きすることで、ボリューム内のデータを消去する処理です。

冗長パス

チャネルプロセッサの故障などによって LUN パスが利用できなくなったときに、その LUN パスに代わってホスト I/O を引き継ぐ LUN パスです。交替パスとも言います。

初期コピー

新規にコピーペアを作成すると、初期コピーが開始されます。初期コピーでは、プライマリボリュームのデータがすべて相手のセカンダリボリュームにコピーされます。初期コピー中も、ホストサーバからプライマリボリュームに対する Read／Write などの I/O 操作は続行できます。

署名付きの信頼できる証明書

証明書発行要求を生成したあとで、信頼できる CA 局に送付して署名してもらいます。CA 局の例としては VeriSign 社があります。

シリアル番号

ストレージシステムに一意に付けられたシリアル番号（装置製番）です。

スナップショットグループ

Thin Image Advanced で作成した複数のペアの集まりです。複数のペアに対して同じ操作を実行できます。

スナップショットデータ

Thin Image Advanced では、プライマリボリュームまたはセカンダリボリュームの更新後データを指します。Thin Image Advanced では、ペア分割状態のプライマリボリュームまたはセカンダリボリュームを更新すると、更新される部分の更新後データだけが、スナップショットデータとしてプールに格納されます。

正 VOL、正ボリューム

詳しくは「プライマリボリューム」を参照してください。

正サイト

通常時に、業務（アプリケーション）を実行するサイトを指します。

セカンダリボリューム

ペアとして設定された 2 つのボリュームのうち、コピー先のボリュームを指します。なお、プライマリボリュームとペアを組んでいるボリュームをセカンダリボリュームと呼びますが、Thin Image Advanced では、セカンダリボリューム（仮想ボリューム）ではなく、プールにデータが格納されます。

センス情報

エラーの検出によってペアがサスペンドされた場合に、正サイトまたは副サイトのストレージシステムが、適切なホストに送信する情報です。ユニットチェックの状況が含まれ、災害復旧に使用されます。

ソースボリューム

Volume Migration の用語で、別のパリティグループへと移動するボリュームを指します。

ゾーニング

ホストとリソース間トラフィックを論理的に分離します。ゾーンに分けることにより、処理は均等に分散されます。

（タ行）

ターゲットボリューム

Volume Migration の用語で、ボリュームの移動先となる領域を指します。

チャネルボード

ストレージシステムに内蔵されているアダプタの一種で、ホストコマンドを処理してデータ転送を制御します。

重複排除用システムデータボリューム（データストア）

容量削減の設定が重複排除および圧縮の仮想ボリュームが関連づけられているプール内で、重複データを格納するためのボリュームです。

重複排除用システムデータボリューム（フィンガープリント）

容量削減の設定が重複排除および圧縮の仮想ボリュームが関連づけられているプール内で、重複排除データの制御情報を格納するためのボリュームです。

ディスクボード

ストレージシステムに内蔵されているアダプタの一種で、キャッシュとドライブの間のデータ転送を制御します。

データ削減共有ボリューム

データ削減共有ボリュームは、Adaptive Data Reduction の容量削減機能を使用して作成する仮想ボリュームです。Thin Image Advanced ペアのボリュームとして使用できます。データ削減共有ボリュームは、Redirect-on-Write のスナップショット機能を管理するための制御データ（メタデータ）を持つボリュームです。

転送レート

ストレージシステムの性能を測る指標の 1 つです。1 秒間にディスクへ転送されたデータの大きさを示します。

同期コピー

ホストからプライマリボリュームに書き込みがあった場合に、リアルタイムにセカンダリボリュームにデータを反映する方式のコピーです。ボリューム単位のリアルタイムデータバックアップができます。優先度の高いデータのバックアップ、複写、および移動業務に適しています。

トポロジ

デバイスの接続形態です。Fabric、FC-AL、および Point-to-point の 3 種類があります。

ドライブボックス

各種ドライブを搭載するためのシャーシ（筐体）です。

（ナ行）

内部ボリューム

本ストレージシステムが管理するボリュームを指します。

（ハ行）

パリティグループ

同じ容量を持ち、1 つのデータグループとして扱われる一連のドライブを指します。パリティグループには、ユーザデータとパリティ情報の両方が格納されているため、そのグループ内の 1 つまたは複数のドライブが利用できない場合にも、ユーザデータにはアクセスできます。
場合によっては、パリティグループを RAID グループ、ECC グループ、またはディスクアレイグループと呼ぶことがあります。

パリティドライブ

RAID6 を構成するときに、1 つの RAID グループの中で 2 台のドライブがパリティドライブとなり、残りのドライブがデータドライブとなります。パリティドライブには複数台のデータドライブのデータから計算されたデータが記憶されます。これにより 1 つの RAID グループ内で 2 台のドライブが故障した場合でも、パリティドライブから再計算することでデータを損なわずにストレージシステムを使用できます。

非対称アクセス

global-active device でのクロスパス構成など、サーバとストレージシステムを複数の冗長パスで接続している場合で、ALUA が有効のときに、優先して I/O を受け付けるパスを定義する方法です。

非同期コピー

ホストから書き込み要求があった場合に、プライマリボリュームへの書き込み処理とは非同期に、セカンダリボリュームにデータを反映する方式のコピーです。複数のボリュームや複数のストレージシステムにわたる大量のデータに対して、災害リカバリを可能にします。

ピントラック

（pinned track）
物理ドライブ障害などによって読み込みや書き込みができないトラックです。固定トラックとも呼びます。

ファームウェア

ストレージシステムで、ハードウェアの基本的な動作を制御しているプログラムです。

ファイバチャネル

光ケーブルまたは銅線ケーブルによるシリアル伝送です。ファイバチャネルで接続された RAID のディスクは、ホストからは SCSI のディスクとして認識されます。

プール

プールボリューム（プール VOL）を登録する領域です。Dynamic Provisioning、および Thin Image Advanced がプールを使用します。

プールボリューム、プール VOL

プールに登録されているボリュームです。Dynamic Provisioning ではプールボリュームに通常のデータを格納し、Thin Image Advanced ではスナップショットデータをプールボリュームに格納します。

副 VOL、副ボリューム

詳しくは「セカンダリボリューム」を参照してください。

副サイト

主に障害時に、業務（アプリケーション）を正サイトから切り替えて実行するサイトを指します。

プライマリボリューム

ペアとして設定された 2 つのボリュームのうち、コピー元のボリュームを指します。

フラッシュメモリ

各プロセッサに搭載され、ソフトウェアを格納している不揮発性のメモリです。

ペア

データ管理目的として互いに関連している 2 つのボリュームを指します（例、レプリケーション、マイグレーション）。ペアは通常、お客様の定義によりプライマリもしくはソースボリューム、およびセカンダリもしくはターゲットボリュームで構成されます。

ペア状態

ペアオペレーション前後にボリュームペアに割り当てられた内部状態。ペアオペレーションが実行されている、もしくは結果として障害となっているときにペア状態は変化します。ペア状態はコピーオペレーションを監視し、およびシステム障害を検出するために使われます。

ペアテーブル

ペアを管理するための制御情報を格納するテーブルです。

ページ

DP の領域を管理する単位です。1 ページは 42MB です。

ポートモード

ストレージシステムのチャネルボードのポート上で動作する、通信プロトコルを選択するモードです。ポートの動作モードとも言います。

ホスト-Namespace パス

日立ストレージシステムで、Namespace セキュリティを使用する際に、ホスト NQN ごとに各 Namespace へのアクセス可否を決定するための設定です。

Namespace パスとも呼びます。

ホスト NQN

NVMe ホストに定義された NQN です。
NQN の詳細については、「NQN」を参照してください。

ホストグループ

ストレージシステムの同じポートに接続し、同じプラットフォーム上で稼働しているホストの集まりのことです。あるホストからストレージシステムに接続するには、ホストをホストグループに登録し、ホストグループを LDEV に結び付けます。この結び付ける操作のことを、LUN パスを追加するとも呼びます。

ホストグループ 0（ゼロ）

「00」という番号が付いているホストグループを指します。

ホストデバイス

ホストに提供されるボリュームです。HDEV（Host Device）とも呼びます。

ホストバスアダプタ

オープンシステム用ホストに内蔵されているアダプタで、ホストとストレージシステムを接続するポートの役割を果たします。それぞれのホストバスアダプタには、16 桁の 16 進数による ID が付いています。ホストバスアダプタに付いている ID を WWN（Worldwide Name）と呼びます。

ホストモード

オープンシステム用ホストのプラットフォーム（通常は OS）を示すモードです。

（マ行）

マイグレーションボリューム

HUS VM などの異なる機種のストレージシステムからデータを移行させる場合に使用するボリュームです。

マッピング

本ストレージシステムから外部ボリュームを操作するために必要な管理番号を、外部ボリュームに割り当てることです。

（ラ行）

ラック

電子機器をレールなどで棚状に搭載するフレームのことです。通常幅 19 インチで規定されるものが多く、それらを 19 型ラックと呼んでいます。搭載される機器の高さは EIA 規格で規定され、ボルトなどで機器を固定するためのネジ穴が設けられています。

リザーブボリューム

ShadowImage のセカンダリボリュームに使用するために確保されているボリューム、または Volume Migration の移動先として確保されているボリュームを指します。

リソースグループ

ストレージシステムのリソースを割り当てたグループを指します。リソースグループに割り当てられるリソースは、LDEV 番号、パリティグループ、外部ボリューム、ポートおよびホストグループ番号です。

リモートコマンドデバイス

外部ストレージシステムのコマンドデバイスを、本ストレージシステムの内部ボリュームとしてマッピングしたものです。リモートコマンドデバイスに対して RAID Manager コマンドを発行すると、外部ストレージシステムのコマンドデバイスに RAID Manager コマンドを発行でき、外部ストレージシステムのペアなどを操作できます。

リモートストレージシステム

ローカルストレージシステムと接続しているストレージシステムを指します。

リモートパス

リモートコピー実行時に、遠隔地にあるストレージシステム同士を接続するパスです。

リンクアグリゲーション

複数のポートを集約して、仮想的にひとつのポートとして使う技術です。
これによりデータリンクの帯域幅を広げるとともに、ポートの耐障害性を確保します。

レスポンスタイム

モニタリング期間内での平均の応答時間。あるいは、エクスポートツール 2 で指定した期間内でのサンプリング期間ごとの平均の応答時間。単位は、各モニタリング項目によって異なります。

ローカルストレージシステム

管理ツールの操作端末を接続しているストレージシステムを指します。

索引

る

日立ヴァンタラ株式会社
〒 244-0817 神奈川県横浜市戸塚区吉田町 292 番地