

Hitachi Virtual Storage Platform One SDS Block

オペレーションガイド

著作権

All Rights Reserved. Copyright (C) 2024, 2025, Hitachi Vantara, Ltd.

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。

商標類

AIX は、世界の多くの国で登録された International Business Machines Corporation の商標です。

Amazon Web Services、AWS、Powered by AWS ロゴ、Amazon EC2、Amazon S3、AWS CloudFormation、AWS Marketplace は、Amazon.com, Inc. またはその関連会社の商標です。

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

Red Hat is registered trademarks of Red Hat, Inc. in the United States and other countries.

UNIX は、The Open Group の登録商標です。

Microsoft Edge、Windows、Azure は、マイクロソフト グループの企業の商標です。

Google Chrome、Google Cloud および関連するサービスは、Google LLC の商標です。

その他記載の会社名、商品名は、それぞれの会社の商標または登録商標です。

輸出時の注意

本製品および本製品に関するライセンスを輸出される場合には、外国為替および外国貿易法の規制なら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、弊社営業担当にお問い合わせください。

発行

2025 年 8 月 (4048-1J-U20-31)

目次

はじめに.....	21
マニュアルの参照と適合ソフトウェアバージョン.....	22
対象読者.....	22
マニュアルで使用する記号について.....	22
単位表記について.....	23
ストレージシステムの表記について.....	23
発行履歴.....	24
 1.VSP One SDS Block の概要.....	41
1.1 VSP One SDS Block とは.....	42
1.1.1 ユーザーデータの保護方式<<Bare metal>>.....	42
1.1.2 ユーザーデータの保護方式<<Cloud>>.....	45
1.2 システムの構成<<Bare metal>>.....	47
1.3 システムの構成<<Cloud for AWS>>.....	52
1.4 システムの構成<<Cloud for Google Cloud>>.....	59
1.5 システムの構成<<Cloud for Microsoft Azure>>.....	65
 2.運用・管理・保守の概要(ユースケース索引).....	73
2.1 運用環境を構成するには.....	74
2.2 ユーザー登録とセキュリティ対策をするには.....	76
2.3 ボリュームをコンピュートノードに提供するには.....	77
2.4 運用状況を監視するには.....	79
2.5 リソース情報を確認するには.....	80
2.6 設定を確認するには.....	83
2.7 リソースを追加・削除・変更するには.....	86
2.8 設定を変更するには.....	93
 3.運用環境を構成する.....	97
3.1 構成ファイルの管理.....	98
3.1.1 構成ファイルを管理する<<Bare metal>>.....	98
3.1.2 構成ファイルを管理する<<Cloud for AWS>>.....	99
3.1.3 構成ファイルを管理する<<Cloud for Google Cloud>>.....	101
3.1.4 構成ファイルを管理する<<Cloud for Microsoft Azure>>.....	103

3.1.5 構成ファイルをエクスポートする《Bare metal》	105
3.1.6 構成ファイルをエクスポートする《Cloud for AWS》	107
3.1.7 構成ファイルをエクスポートする《Cloud for Google Cloud》	111
3.1.8 構成ファイルをエクスポートする《Cloud for Microsoft Azure》	113
3.1.9 VM 構成ファイルを Terraform の作業ディレクトリーへ配置する 《Cloud for Google Cloud》	116
3.2 コントローラーノードの設置と管理操作	117
3.2.1 コントローラーノードの設置《Bare metal》	117
3.2.2 コントローラーノードの設置《Cloud for AWS》	118
3.2.3 コントローラーノードの設置《Cloud for Google Cloud》	119
3.2.4 コントローラーノードの設置《Cloud for Microsoft Azure》	120
3.2.5 VSP One SDS Block Administrator について	122
3.2.6 コンソールインターフェイスについて《Bare metal》	122
3.2.7 コンソールインターフェイスについて《Cloud》	123
3.3 コンピュートノードの設置	123
3.3.1 コンピュートノードを設置する《Bare metal》	123
(1) コンピュートノード設置に当たっての注意事項《Bare metal》	125
(2) NVMe/TCP 接続時のシステム構成《Bare metal》	125
3.3.2 コンピュートノードを設置する《Cloud for AWS》	127
(1) コンピュートノード設置に当たっての注意事項《Cloud for AWS》	128
3.3.3 コンピュートノードを設置する《Cloud for Google Cloud》	128
(1) コンピュートノード設置に当たっての注意事項《Cloud for Google Cloud》	130
3.3.4 コンピュートノードを設置する《Cloud for Microsoft Azure》	130
(1) コンピュートノード設置に当たっての注意事項《Cloud for Microsoft Azure》	132
3.3.5 タスクをスケジュールする(コンピュートノードの OS が Windows の場合)	132
3.4 空状態にあるストレージプールの拡張	141
3.4.1 空状態にあるストレージプールを拡張する《Bare metal》	141
3.4.2 空状態にあるストレージプールを拡張する《Cloud》	143
3.5 ログイン時・CLI Basic 認証時に表示するメッセージを設定する	146
3.6 許可リストの設定	148
3.6.1 許可リストを設定する《Bare metal》	148
3.6.2 許可リストを設定する《Cloud》	149
4. ライセンスを管理する	151
4.1 ライセンス管理の概要	152
4.1.1 ライセンス管理の概要《Bare metal》	152
4.1.2 ライセンス管理の概要《Cloud》	156
4.2 ライセンスの登録	164
4.2.1 ライセンスを登録する《Bare metal》	164
4.2.2 ライセンスを登録する《Cloud》	165
4.3 ライセンスの削除	166
4.3.1 ライセンスを削除する《Bare metal》	166
4.3.2 ライセンスを削除する《Cloud》	166
4.4 ライセンス情報の取得	167
4.4.1 取得できるライセンス情報《Bare metal》	167
4.4.2 取得できるライセンス情報《Cloud》	168
4.4.3 ライセンス情報の一覧を取得する	168
4.4.4 ライセンス情報を個別に取得する	169
4.5 ライセンスの設定値の編集	169
4.5.1 ライセンスの警告しきい値を編集する《Bare metal》	169
4.5.2 ライセンスの設定値を編集する《Cloud》	170

4.6 ライセンス設定情報の取得.....	170
4.6.1 取得できるライセンスの設定情報<<Bare metal>>.....	171
4.6.2 取得できるライセンスの設定情報<<Cloud>>.....	171
4.6.3 ライセンスの設定情報を取得する.....	171
5.時刻設定を管理する.....	173
5.1 時刻の同期設定について<<Bare metal>>.....	174
5.2 ストレージクラスターの時刻設定を取得する.....	174
6.イベントログを管理する.....	177
6.1 イベントログについて.....	178
6.2 イベントログの取得.....	180
6.2.1 取得できるイベントログ情報.....	180
6.2.2 イベントログの一覧を取得する.....	180
6.2.3 イベントログを個別に取得する.....	181
6.3 イベントログの Syslog 転送設定の編集.....	181
6.3.1 イベントログの Syslog 転送設定を編集する<<Bare metal>>.....	181
6.3.2 イベントログの Syslog 転送設定を編集する<<Cloud>>.....	183
6.4 イベントログの SMTP 転送設定の編集.....	184
6.4.1 イベントログの SMTP 転送設定を編集する<<Bare metal>>.....	184
6.4.2 イベントログの SMTP 転送設定を編集する<<Cloud>>.....	189
6.5 イベントログの設定を取得する.....	194
6.6 Syslog 転送されるイベントログを監視する.....	195
6.7 Syslog 転送時のイベントログの構造.....	195
6.8 E メール形式.....	197
6.9 SNMP を利用する.....	198
6.9.1 SNMP マネージャーと環境の要件.....	199
6.9.2 SNMP アクセスコントロールを設定する.....	199
6.9.3 SNMP アクセスコントロールを取得する.....	201
6.9.4 標準 MIB について.....	201
6.9.5 拡張 MIB の取り込み.....	202
6.9.6 トラップ受信後の障害ハードウェアの特定.....	205
7.監査ログを管理する.....	207
7.1 監査ログの概要.....	208
7.2 監査ログをコントローラーノードにダウンロードする.....	209
7.3 監査ログの Syslog 転送設定の編集.....	209
7.3.1 監査ログの Syslog 転送設定を編集する<<Bare metal>>.....	209
7.3.2 監査ログの Syslog 転送設定を編集する<<Cloud>>.....	211
7.4 監査ログの Syslog 転送設定を取得する.....	212
7.5 Syslog サーバーへ転送される監査ログを監視する.....	212
8.ドライブを管理する.....	213
8.1 ドライブ管理の概要.....	214
8.2 ドライブ情報の取得.....	214
8.2.1 取得できるドライブ情報<<Bare metal>>.....	214

8.2.2 取得できるドライブ情報<<Cloud>>	214
8.2.3 ドライブの情報の一覧を取得する	215
8.2.4 ドライブの情報を個別に取得する	215
8.3 ドライブの減設	216
8.3.1 ドライブを減設する<<Bare metal>>	216
8.3.2 ドライブを減設する<<Cloud for Google Cloud>>	219
8.3.3 ドライブを減設する<<Cloud for Microsoft Azure>>	221
8.4 ドライブの交換	224
8.4.1 ドライブを交換する<<Bare metal>>	224
8.4.2 ドライブを交換する<<Cloud for AWS>>	227
8.4.3 ドライブを交換する<<Cloud for Google Cloud>>	233
8.4.4 ドライブを交換する<<Cloud for Microsoft Azure>>	236
8.5 ドライブを再組み入れする<<Bare metal>>	238
9. ドライブを増設する	241
9.1 ドライブ増設の概要	242
9.2 ドライブを挿入する<<Bare metal>>	244
9.3 ドライブを作成する<<Cloud for AWS>>	244
9.4 ドライブを作成する<<Cloud for Google Cloud>>	247
9.5 ドライブを作成する<<Cloud for Microsoft Azure>>	249
9.6 ストレージプールを拡張する	250
10. ストレージノードを管理する	255
10.1 ストレージノード管理の概要	256
10.2 ストレージノード情報の取得	256
10.2.1 取得できるストレージノード情報<<Bare metal>>	256
10.2.2 取得できるストレージノード情報<<Cloud>>	257
10.2.3 ストレージノード情報の一覧を取得する	258
10.2.4 ストレージノード情報を個別に取得する	258
11. ストレージノード増設の準備と手順	259
11.1 ストレージノードの増設<<Bare metal>>	260
11.1.1 増設用ストレージノードを準備する<<Bare metal>>	261
11.1.2 システム要件ファイルを更新する<<Bare metal>>	262
11.1.3 構成ファイルを編集する<<Bare metal>>	263
11.1.4 ストレージノードを増設する<<Bare metal>>	263
11.1.5 追加した論理容量が使用できることを確認する<<Bare metal>>	267
11.1.6 増設したストレージノードの設定を行う<<Bare metal>>	268
11.2 ストレージノードの増設<<Cloud for AWS>>	270
11.2.1 ストレージノードを増設する<<Cloud for AWS>>	271
11.2.2 追加した論理容量が使用できることを確認する<<Cloud for AWS>>	275
11.2.3 増設したストレージノードの設定を行う<<Cloud for AWS>>	275
11.3 ストレージノードの増設<<Cloud for Google Cloud>>	276
11.3.1 ストレージノードを増設する<<Cloud for Google Cloud>>	278
11.3.2 追加した論理容量が使用できることを確認する<<Cloud for Google Cloud>>	282
11.3.3 増設したストレージノードの設定を行う<<Cloud for Google Cloud>>	283
11.4 ストレージノードの増設<<Cloud for Microsoft Azure>>	283
11.4.1 ストレージノードを増設する<<Cloud for Microsoft Azure>>	285

11.4.2 追加した論理容量が使用できることを確認する<<Cloud for Microsoft Azure>>	288
11.4.3 増設したストレージノードの設定を行う<<Cloud for Microsoft Azure>>	289
12.ストレージノード減設の条件と手順.....	291
12.1 ストレージノードの減設<<Bare metal>>	292
12.1.1 ストレージノード減設の条件を確認する<<Bare metal>>	293
12.1.2 ストレージノードを減設する<<Bare metal>>	297
12.2 ストレージノードの減設<<Cloud for AWS>>	299
12.2.1 ストレージノード減設の条件を確認する<<Cloud for AWS>>	300
12.2.2 ストレージノードを減設する<<Cloud for AWS>>	302
12.3 ストレージノードの減設<<Cloud for Google Cloud>>	307
12.3.1 ストレージノード減設の条件を確認する<<Cloud for Google Cloud>>	307
12.3.2 ストレージノードを減設する<<Cloud for Google Cloud>>	309
12.4 ストレージノードの減設<<Cloud for Microsoft Azure>>	313
12.4.1 ストレージノード減設の条件を確認する<<Cloud for Microsoft Azure>>	314
12.4.2 ストレージノードを減設する<<Cloud for Microsoft Azure>>	316
12.5 ストレージノードの減設処理を中止する.....	318
13.ストレージノードを保守する.....	321
13.1 ストレージノード保守の原因と対処.....	322
13.1.1 ストレージノード保守の原因と対処<<Bare metal>>	322
13.1.2 ストレージノード保守の原因と対処<<Cloud for AWS>>	327
13.1.3 ストレージノード保守の原因と対処<<Cloud for Google Cloud>>	331
13.1.4 ストレージノード保守の原因と対処<<Cloud for Microsoft Azure>>	335
13.2 ストレージノードの保守回復.....	338
13.2.1 ストレージノードを保守回復する<<Bare metal>>	339
13.2.2 ストレージノードを保守回復する<<Cloud for AWS>>	342
13.2.3 ストレージノードを保守回復する<<Cloud for Google Cloud>>	346
13.2.4 ストレージノードを保守回復する<<Cloud for Microsoft Azure>>	349
13.3 ストレージノードの保守閉塞.....	352
13.3.1 ストレージノードの保守閉塞の条件を確認する<<Bare metal>>	352
13.3.2 ストレージノードの保守閉塞の条件を確認する<<Cloud>>	357
13.3.3 ストレージノードを保守閉塞する<<Bare metal>>	361
13.3.4 ストレージノードを保守閉塞する<<Cloud for AWS>>	363
13.3.5 ストレージノードを保守閉塞する<<Cloud for Google Cloud>>	364
13.3.6 ストレージノードを保守閉塞する<<Cloud for Microsoft Azure>>	365
13.4 ストレージノードの交換.....	367
13.4.1 ストレージノードを交換する<<Bare metal>>	367
13.4.2 ストレージノードを交換する<<Cloud for AWS>>	374
13.4.3 ストレージソフトウェアのバージョンが混在している場合のストレージノード交換<<Cloud for AWS>>	379
13.4.4 ストレージノードを交換する<<Cloud for Google Cloud>>	381
13.4.5 ストレージノードを交換する<<Cloud for Microsoft Azure>>	389
13.5 ストレージノードの自動回復機能の設定.....	394
13.5.1 ストレージノードの自動回復機能を設定する<<Bare metal>>	394
13.5.2 ストレージノードの自動回復機能を設定する<<Cloud>>	399
13.6 ストレージノードの自動回復機能の情報取得.....	402
13.6.1 ストレージノードの自動回復機能の情報を取得する<<Bare metal>>	402
13.6.2 ストレージノードの自動回復機能の情報を取得する<<Cloud>>	403

13.7 クラウドプラットフォームのメンテナンスについて <<Cloud for Google Cloud>>	403
13.8 クラウドプラットフォームのメンテナンスについて <<Cloud for Microsoft Azure>>	404
14. ドライブデータ再配置を管理する <<Bare metal>>	407
14.1 ドライブデータ再配置の概要 <<Bare metal>>	408
14.2 ドライブデータ再配置の起動契機と動作可能な条件 <<Bare metal>>	408
14.3 ドライブデータ再配置完了までの時間(目安) <<Bare metal>>	409
14.4 ドライブデータ再配置の状態を確認する <<Bare metal>>	411
14.5 ドライブデータ再配置を中断する <<Bare metal>>	411
14.6 ドライブデータ再配置を再開する <<Bare metal>>	413
15. コンピュートノードの接続を管理する	415
15.1 コンピュートノードの情報を登録する	416
15.2 コンピュートノード情報の一覧を取得する	417
15.3 コンピュートノード情報を個別に取得する	417
15.4 コンピュートノードの情報を編集する	418
15.5 コンピュートノードの情報を削除する	419
15.6 コンピュートノードのイニシエーター情報を登録する	421
15.6.1 iSCSI 接続している場合	421
15.6.2 NVMe/TCP 接続している場合 <<Bare metal>>	423
15.6.3 FC 接続している場合 <<Bare metal>>	424
15.7 コンピュートノードのイニシエーター情報の取得	425
15.7.1 取得できるコンピュートノードのイニシエーター情報	425
15.7.2 コンピュートノードのイニシエーター情報の一覧を取得する	425
15.7.3 コンピュートノードのイニシエーター情報を個別に取得する	425
15.8 コンピュートノードのイニシエーター情報を削除する	426
15.9 コンピュートノードのパス情報を登録する	427
15.10 コンピュートノードのパス情報の取得	430
15.10.1 取得できるコンピュートノードのパス情報 <<Bare metal>>	430
15.10.2 取得できるコンピュートノードのパス情報 <<Cloud>>	430
15.10.3 コンピュートノードのパス情報の一覧を取得する	430
15.10.4 コンピュートノードのパス情報を個別に取得する <<Bare metal>>	431
15.10.5 コンピュートノードのパス情報を個別に取得する <<Cloud>>	432
15.11 コンピュートノードのパス情報の削除	432
15.11.1 コンピュートノードのパス情報を削除する <<Bare metal>>	432
15.11.2 コンピュートノードのパス情報を削除する <<Cloud>>	434
15.12 ボリュームとコンピュートノードの接続	435
15.12.1 ボリュームをコンピュートノードに接続する <<Bare metal>>	435
15.12.2 ボリュームをコンピュートノードに接続する <<Cloud>>	437
15.13 ボリュームとコンピュートノードの接続情報の取得	439
15.13.1 取得できるボリュームとコンピュートノードの接続情報 <<Bare metal>>	439
15.13.2 取得できるボリュームとコンピュートノードの接続情報 <<Cloud>>	440
15.13.3 ボリュームとコンピュートノードの接続情報の一覧を取得する	440
15.13.4 ボリュームとコンピュートノードの接続情報を個別に取得する	441
15.14 ボリュームとコンピュートノードの接続解除	441
15.14.1 ボリュームとコンピュートノードの接続を解除する <<Bare metal>>	441
15.14.2 ボリュームとコンピュートノードの接続を解除する <<Cloud>>	443

15.15 複数のボリュームとコンピュータノードの接続解除.....	445
15.15.1 複数のボリュームとコンピュータノードの接続を解除する <<Bare metal>>.....	445
15.15.2 複数のボリュームとコンピュータノードの接続を解除する <<Cloud>>.....	446
16. コンピュータポートを管理する.....	449
16.1 コンピュータポートの情報の取得.....	450
16.1.1 取得できるコンピュータポートの情報 <<Bare metal>>.....	450
16.1.2 取得できるコンピュータポートの情報 <<Cloud>>.....	451
16.1.3 コンピュータポートの情報の一覧を取得する.....	451
16.1.4 コンピュータポートの情報を個別に取得する.....	451
16.2 コンピュータポート設定の編集.....	452
16.2.1 コンピュータポートの設定を編集する <<Bare metal>>.....	452
16.2.2 コンピュータポートの設定を編集する <<Cloud>>.....	455
16.3 コンピュータポートのプロトコルを変更する <<Bare metal>>.....	458
17. ボリュームを管理する.....	461
17.1 ボリューム管理の概要.....	462
17.1.1 ボリュームとストレージプール.....	463
17.1.2 Quality of Service(QoS)機能について.....	466
17.2 ボリュームの容量削減機能の概要.....	468
17.3 ボリュームの容量削減機能を有効にする.....	473
17.4 ボリュームの作成.....	474
17.4.1 ボリュームを作成する <<Bare metal>>.....	474
17.4.2 ボリュームを作成する <<Cloud>>.....	477
17.5 ボリュームを削除する.....	479
17.6 ボリュームを拡張する.....	481
17.7 ボリューム情報の一覧の取得.....	483
17.7.1 取得できるボリュームの一覧情報 <<Bare metal>>.....	484
17.7.2 取得できるボリュームの一覧情報 <<Cloud>>.....	485
17.7.3 ボリューム情報の一覧を取得する.....	486
17.8 ボリューム情報の個別取得.....	486
17.8.1 取得できるボリュームの個別情報 <<Bare metal>>.....	487
17.8.2 取得できるボリュームの個別情報 <<Cloud>>.....	488
17.8.3 ボリュームの情報を個別に取得する.....	490
17.9 ボリュームの設定を編集する.....	490
17.10 ボリュームが稼働するアベイラビリティゾーンを確認する <<Cloud>>.....	492
18. スナップショットを使用したボリュームのバックアップと復元.....	495
18.1 スナップショットの概要.....	496
18.2 スナップショットの取得準備をする.....	504
18.3 スナップショットを取得する.....	506
18.4 スナップショットを削除する.....	508
18.5 スナップショットからのボリューム復元.....	509
18.5.1 スナップショットからボリュームを復元する <<Bare metal>>.....	509
18.5.2 スナップショットからボリュームを復元する <<Cloud>>.....	513
18.6 ボリュームに対する P-VOL 情報を取得する.....	516
18.7 ボリュームに対する S-VOL 情報の一覧を取得する.....	517

19.ユーザーを管理する.....	519
19.1 ユーザー管理の概要.....	520
19.2 ユーザー情報の一覧を取得する.....	525
19.3 ユーザーの詳細情報を取得する.....	526
19.4 ユーザーを作成する.....	527
19.5 ユーザー情報を編集する.....	528
19.6 ユーザーを削除する.....	529
19.7 自身のパスワードを変更する.....	530
19.8 ユーザーをユーザーグループに追加する.....	531
19.9 ユーザーをユーザーグループから削除する.....	532
19.10 ユーザーグループの一覧を取得する.....	532
19.11 ユーザーグループの詳細情報を取得する.....	533
19.12 ユーザーグループを作成する.....	534
19.13 ユーザーグループ情報を編集する.....	534
19.14 ユーザーグループを削除する.....	535
19.15 外部認証サーバーを利用する.....	536
19.15.1 外部認証サーバー利用の概要.....	536
19.15.2 外部認証サーバー利用の操作.....	543
19.16 外部認証サーバーの設定を取得する.....	545
19.17 外部認証サーバーのルート証明書を取得する.....	545
20.セッションを管理する.....	547
20.1 セッション管理の概要.....	548
20.2 セッション情報の取得.....	548
20.2.1 取得できるセッション情報.....	548
20.2.2 セッションの一覧を取得する.....	549
20.2.3 セッション情報を取得する.....	549
20.3 セッションを生成する.....	549
20.4 セッションを削除する.....	550
21.ユーザー認証設定を編集する.....	551
21.1 ユーザー認証設定を編集する.....	552
21.2 ユーザー認証設定を取得する.....	554
22.運用管理を SSL/TLS 通信で行う.....	555
22.1 TLS とは.....	556
22.2 SSL/TLS 通信の設定の流れ.....	556
22.3 サーバー証明書を更新するときの注意事項.....	557
22.4 OpenSSL のインストール.....	558
22.5 秘密鍵を作成する.....	558
22.6 秘密鍵を暗号化する.....	559
22.7 証明書署名要求を作成する.....	559
22.8 署名付き証明書を取得する.....	562
22.9 秘密鍵のパスフレーズの確認と解除.....	563

22.10 ルート証明書をインポートする.....	564
22.10.1 REST API でルート証明書を扱う方法.....	564
22.10.2 CLI プログラムにルート証明書をインストールする方法.....	564
22.10.3 ブラウザーにルート証明書をインポートする方法.....	565
22.11 SSL/TLS 通信の署名付き証明書をインポートする.....	565
22.12 SSL/TLS 通信のクライアント要件.....	567
22.12.1 SSL/TLS 通信のクライアント要件 <<Bare metal>>.....	567
22.12.2 SSL/TLS 通信のクライアント要件 <<Cloud>>.....	569
22.13 サーバー証明書に関する警告メッセージが表示されたときの対処.....	571
23.CHAP 認証を利用する.....	573
23.1 CHAP ユーザーを作成して CHAP 認証を設定する.....	574
23.2 CHAP ユーザー情報の一覧を取得する.....	576
23.3 CHAP ユーザー情報を個別に取得する.....	576
23.4 CHAP ユーザー情報を編集する.....	577
23.5 CHAP ユーザーを削除する.....	577
23.6 ターゲット動作のコンピュートポートの認証設定を取得する.....	578
23.7 ターゲット動作のコンピュートポートの認証設定を編集する.....	579
23.8 CHAP ユーザーに対してコンピュートポートへのアクセスを許可する.....	580
23.9 コンピュートポートへのアクセスを許可した CHAP ユーザー情報の取得.....	581
23.9.1 取得できるコンピュートポートへのアクセスを許可した CHAP ユーザー情報.....	581
23.9.2 コンピュートポートへのアクセスを許可した CHAP ユーザー情報の一覧を取得する.....	581
23.9.3 コンピュートポートへのアクセスを許可した CHAP ユーザー情報を個別に取得する.....	582
23.10 CHAP ユーザーに対してコンピュートポートへのアクセス許可を解除する.....	582
24.システムの性能情報・容量情報を取得する.....	585
24.1 ストレージシステムの性能情報と容量情報.....	586
24.2 管理ポートの性能情報の取得.....	586
24.2.1 取得できる管理ポートの性能情報.....	586
24.2.2 管理ポートの性能情報(低解像度)の一覧を取得する.....	586
24.2.3 管理ポートの性能情報(高解像度)の一覧を取得する.....	586
24.2.4 管理ポートの性能情報を個別に取得する.....	587
24.3 ドライブの性能情報の取得.....	587
24.3.1 取得できるドライブの性能情報.....	587
24.3.2 ドライブの性能情報(低解像度)の一覧を取得する.....	588
24.3.3 ドライブの性能情報(高解像度)の一覧を取得する.....	588
24.3.4 ドライブの性能情報を個別に取得する.....	589
24.4 ストレージノード間ポートの性能情報の取得.....	589
24.4.1 取得できるストレージノード間ポートの性能情報.....	589
24.4.2 ストレージノード間ポートの性能情報(低解像度)の一覧を取得する.....	590
24.4.3 ストレージノード間ポートの性能情報(高解像度)の一覧を取得する.....	590
24.4.4 ストレージノード間ポートの性能情報を個別に取得する.....	590
24.5 ストレージプールの容量情報の取得.....	591
24.5.1 取得できるストレージプールの容量情報.....	591
24.5.2 ストレージプールの容量情報(低解像度)の一覧を取得する.....	591
24.5.3 ストレージプールの容量情報(低解像度)を個別に取得する.....	591
24.6 ストレージプールの性能情報の取得.....	592

24.6.1 取得できるストレージプールの性能情報.....	592
24.6.2 ストレージプールの性能情報(低解像度)の一覧を取得する.....	593
24.6.3 ストレージプールの性能情報(低解像度)を個別に取得する.....	593
24.7 コンピュートポートの性能情報の取得.....	593
24.7.1 取得できるコンピュートポートの性能情報<<Bare metal>>.....	593
24.7.2 取得できるコンピュートポートの性能情報<<Cloud>>.....	594
24.7.3 コンピュートポートの性能情報(低解像度)の一覧を取得する.....	594
24.7.4 コンピュートポートの性能情報(高解像度)の一覧を取得する.....	594
24.7.5 コンピュートポートの性能情報を個別に取得する.....	595
24.8 ストレージクラスターの性能情報(低解像度)を取得する.....	595
24.9 ストレージノードの性能情報の取得.....	596
24.9.1 取得できるストレージノードの性能情報.....	596
24.9.2 ストレージノードの性能情報の一覧を取得する.....	597
24.9.3 ストレージノードの性能情報を個別に取得する.....	597
24.10 ボリュームの容量情報の取得.....	598
24.10.1 取得できるボリュームの容量情報.....	598
24.10.2 ボリュームの容量情報(低解像度)の一覧を取得する.....	598
24.10.3 ボリュームの容量情報(低解像度)を個別に取得する.....	598
24.11 ボリュームの性能情報の取得.....	599
24.11.1 取得できるボリュームの性能情報.....	599
24.11.2 ボリュームの性能情報の一覧を取得する.....	599
24.11.3 ボリュームの性能情報を個別に取得する.....	600
24.12 ジャーナルの性能情報の取得.....	600
24.12.1 取得できるジャーナルの性能情報.....	600
24.12.2 ジャーナルの性能情報の一覧を取得する.....	601
24.12.3 ジャーナルの性能情報を個別に取得する.....	601
25.ネットワーク設定の情報を取得する.....	603
25.1 ストレージクラスターのネットワーク情報の取得.....	604
25.1.1 取得できるストレージクラスターのネットワーク情報<<Bare metal>>.....	604
25.1.2 取得できるストレージクラスターのネットワーク情報<<Cloud>>.....	604
25.1.3 ストレージクラスターのネットワーク情報を取得する.....	604
25.2 管理ポートの情報の取得.....	604
25.2.1 取得できる管理ポート情報<<Bare metal>>.....	604
25.2.2 取得できる管理ポート情報<<Cloud>>.....	605
25.2.3 管理ポートの情報の一覧を取得する.....	606
25.2.4 管理ポートの情報を個別に取得する.....	606
25.3 ストレージノード間ポートの情報の取得.....	606
25.3.1 取得できるストレージノード間ポート情報<<Bare metal>>.....	606
25.3.2 取得できるストレージノード間ポート情報<<Cloud>>.....	607
25.3.3 ストレージノード間ポートの情報の一覧を取得する.....	607
25.3.4 ストレージノード間ポートの情報を個別に取得する.....	608
25.4 ストレージノードのネットワーク設定の取得.....	608
25.4.1 取得できるストレージノードのネットワーク設定.....	608
25.4.2 ストレージノードのネットワーク設定の一覧を取得する.....	608
25.4.3 ストレージノードのネットワーク設定を個別に取得する.....	608
26.ストレージプールを管理する.....	611
26.1 ストレージプール管理の概要.....	612

26.2 ストレージプールの容量情報.....	612
26.3 ストレージプールの容量状態.....	614
26.4 ストレージプールのリビルド領域について.....	614
26.5 ストレージプールの情報の取得.....	617
26.5.1 取得できるストレージプールの情報<<Bare metal>>.....	617
26.5.2 取得できるストレージプールの情報<<Cloud>>.....	619
26.5.3 ストレージプールの情報の一覧を取得する.....	621
26.5.4 ストレージプールの情報を個別に取得する.....	621
26.6 ストレージプールの設定を編集する.....	622
26.7 リビルド領域の不足に対処する.....	624
26.8 ライセンスの使用量を確認するためにストレージプールの容量を試算する<<Cloud for AWS>>.....	625
26.8.1 ストレージノード数、ドライブ数、およびドライブ障害数を指定して論理容量を試算する<<Cloud for AWS>>.....	625
26.8.2 追加するストレージノード数、ドライブ数、またはドライブ障害数を指定して論理容量を試算する<<Cloud for AWS>>.....	626
27.ストレージクラスターの情報を取得する.....	629
27.1 ストレージクラスターの情報の取得.....	630
27.1.1 取得できるストレージクラスターの情報<<Bare metal>>.....	630
27.1.2 取得できるストレージクラスターの情報<<Cloud>>.....	631
27.1.3 ストレージクラスターの情報を取得する.....	632
27.2 フォールトドメイン情報の一覧の取得.....	633
27.2.1 取得できるフォールトドメインの一覧情報<<Bare metal>>.....	633
27.2.2 取得できるフォールトドメインの一覧情報<<Cloud>>.....	633
27.2.3 フォールトドメイン情報の一覧を取得する.....	634
27.3 フォールトドメイン情報の個別取得.....	634
27.3.1 取得できるフォールトドメインの個別情報<<Bare metal>>.....	635
27.3.2 取得できるフォールトドメインの個別情報<<Cloud>>.....	635
27.3.3 フォールトドメイン情報を個別に取得する.....	636
27.4 ヘルスステータスを取得する.....	636
27.5 クラスターマスターノード(プライマリー)かを確認する.....	637
28.プロテクションドメインを管理する.....	639
28.1 プロテクションドメイン情報の一覧を取得する.....	640
28.2 プロテクションドメイン情報を個別に取得する.....	640
28.3 内部処理 I/O のリソース使用率を変更する.....	641
29.ストレージコントローラーを管理する.....	643
29.1 機能の概要.....	644
29.2 ストレージコントローラーの容量状態.....	644
29.3 ストレージコントローラーの情報の取得.....	645
29.3.1 取得できるストレージコントローラーの情報.....	645
29.3.2 ストレージコントローラー情報の一覧を取得する.....	646
29.3.3 ストレージコントローラー情報を個別に取得する.....	646
29.4 ストレージコントローラーの設定を編集する.....	647

30.リビルド(データ再構築)の状態を確認する.....	649
30.1 リビルドの概要.....	650
30.2 リビルドが動作可能な条件.....	651
30.3 リビルド完了までの時間(目安).....	651
30.4 リビルドの状態を確認する.....	655
31.共通情報を取得する.....	657
31.1 API のバージョン・名称を取得する.....	658
31.2 ジョブの情報の取得.....	658
31.2.1 取得できるジョブの情報.....	658
31.2.2 ジョブの情報の一覧を取得する.....	658
31.2.3 ジョブの情報を個別に取得する.....	659
31.3 モデルを確認する.....	659
32.ストレージソフトウェアアップデートの要件と手順.....	661
32.1 ストレージソフトウェアアップデートの概要.....	662
32.2 参考事項・制限事項.....	664
32.2.1 ソフトウェアアップデートの対象.....	665
32.2.2 ソフトウェアアップデートが制限されるケース.....	665
32.2.3 ソフトウェアアップデート中に制限される操作.....	666
32.2.4 ソフトウェアアップデート中の動作.....	666
32.2.5 ソフトウェアアップデート後に必要な操作.....	667
32.3 ストレージソフトウェアをアップグレードする《Bare metal》.....	668
32.4 ストレージソフトウェアをアップグレードする《Cloud for AWS》.....	673
32.5 ストレージソフトウェアをアップグレードする《Cloud for Google Cloud》.....	679
32.6 ストレージソフトウェアをアップグレードする《Cloud for Microsoft Azure》.....	684
32.7 ストレージソフトウェアをダウングレードする《Bare metal》.....	688
32.8 ストレージソフトウェアをダウングレードする《Cloud for AWS》.....	706
32.8.1 ダウングレード時の VM 構成ファイルを作成する《Cloud for AWS》.....	716
32.9 ストレージソフトウェアをダウングレードする《Cloud for Google Cloud》.....	721
32.10 ストレージソフトウェアをダウングレードする《Cloud for Microsoft Azure》.....	726
32.11 ソフトウェアアップデートを中止する.....	731
32.12 転送済みのソフトウェアアップデートファイルの情報を取得する.....	732
33.ストレージクラスターを起動/停止する.....	733
33.1 ストレージクラスターの起動/停止の概要.....	734
33.2 ストレージクラスターの起動.....	734
33.2.1 ストレージクラスターを起動する《Bare metal》.....	734
33.2.2 ストレージクラスターを起動する《Cloud for AWS》.....	736
33.2.3 ストレージクラスターを起動する《Cloud for Google Cloud》.....	738
33.2.4 ストレージクラスターを起動する《Cloud for Microsoft Azure》.....	740
33.3 ストレージクラスターを強制起動する.....	742
33.4 ストレージクラスターの停止.....	743
33.4.1 ストレージクラスターを停止する《Bare metal》.....	743
33.4.2 ストレージクラスターを停止する《Cloud》.....	744
33.5 ストレージクラスターの強制停止.....	746

33.5.1 ストレージクラスターを強制停止する《Bare metal》	746
33.5.2 ストレージクラスターを強制停止する《Cloud》	749
33.6 ストレージクラスターの再起動	751
33.6.1 ストレージクラスターを再起動する《Bare metal》	751
33.6.2 ストレージクラスターを再起動する《Cloud》	753
34.ストレージクラスターの構成情報を変更・設定する《Bare metal》	755
34.1 構成情報の変更・設定の概要《Bare metal》	756
34.2 管理ネットワーク変更時の運用の注意《Bare metal》	757
34.3 構成情報の変更・設定のために VSSB 構成ファイルを編集する《Bare metal》	759
34.4 構成情報を変更・設定する《Bare metal》	761
35.認証チケットを管理する	767
35.1 認証チケットを発行する	768
35.2 認証チケットを破棄する	768
36.構成情報をバックアップする《Bare metal》《Cloud for AWS》	771
36.1 構成バックアップ・構成リストアの概要《Bare metal》《Cloud for AWS》	772
36.2 構成バックアップを行う《Bare metal》《Cloud for AWS》	773
37.ストレージソフトウェアをアンインストールする	781
37.1 ストレージソフトウェアのアンインストールの概要	782
37.2 スタックを削除する《Cloud for AWS》	784
37.3 VPC ファイアウォール上のルールを削除する《Cloud for Google Cloud》	784
37.4 ストレージクラスターを削除する《Cloud for Google Cloud》	785
37.5 ストレージクラスターを削除する《Cloud for Microsoft Azure》	787
37.6 構成バックアップファイルを削除する《Bare metal》《Cloud for AWS》	787
38.コンソールインターフェイスの操作	789
38.1 コンソールインターフェイスの概要	790
38.2 ログインとログアウト	790
38.2.1 ログイン操作とログアウト操作《Bare metal》	790
38.2.2 ログイン操作とログアウト操作《Cloud》	792
38.3 コンソールトップメニュー画面について	793
38.4 「Show storage cluster information」画面について	793
38.5 コンソールインターフェイスの留意事項	794
39.マルチテナンシーを構成する《Bare metal》	795
39.1 マルチテナンシーの概要《Bare metal》	796
39.2 VPS に関する設定について《Bare metal》	799
39.3 テナント共通の設定《Bare metal》	802
39.4 システム管理者向けの設定《Bare metal》	803
39.5 VPS を作成する《Bare metal》	804

39.6 VPS の利用状況を確認する <<Bare metal>>	805
39.7 VPS の情報の取得 <<Bare metal>>	806
39.7.1 取得できる VPS の情報 <<Bare metal>>	806
39.7.2 VPS の情報の一覧を取得する <<Bare metal>>	807
39.7.3 VPS の情報を個別に取得する <<Bare metal>>	807
39.8 VPS の設定を編集する <<Bare metal>>	808
39.9 VPS を削除する <<Bare metal>>	808
39.10 性能低下・操作不可の監視と対処 <<Bare metal>>	810
39.11 リソース不足・性能問題発生時の対処 <<Bare metal>>	811
40.スペアノードを管理する <<Bare metal>>	815
40.1 スペアノードの概要 <<Bare metal>>	816
40.2 スペアノード切り換えの概要 <<Bare metal>>	818
40.3 スペアノードを準備する <<Bare metal>>	822
40.4 スペアノードを利用するための BMC アカウントを準備する <<Bare metal>>	823
40.5 ストレージクラスターに BMC 接続検証用ルート証明書をインポートする <<Bare metal>>	824
40.6 ストレージクラスターから BMC 接続検証用ルート証明書を取得する <<Bare metal>>	825
40.7 ストレージクラスターから BMC 接続検証用ルート証明書を削除する <<Bare metal>>	826
40.8 ストレージノードの BMC 情報を登録・編集する <<Bare metal>>	826
40.9 ストレージノードの BMC 情報の取得 <<Bare metal>>	828
40.9.1 取得できるストレージノードの BMC 情報 <<Bare metal>>	828
40.9.2 ストレージノードの BMC 情報の一覧を取得する <<Bare metal>>	828
40.9.3 ストレージノードの BMC 情報を個別に取得する <<Bare metal>>	828
40.10 スペアノードの情報を登録する <<Bare metal>>	829
40.11 スペアノードの情報を編集する <<Bare metal>>	830
40.12 スペアノードの情報の取得 <<Bare metal>>	832
40.12.1 取得できるスペアノードの情報 <<Bare metal>>	832
40.12.2 スペアノードの情報を一覧で取得する <<Bare metal>>	833
40.12.3 スペアノードの情報を個別に取得する <<Bare metal>>	833
40.13 スペアノードの情報を削除する <<Bare metal>>	833
40.14 スペアノード機能の設定を確認する <<Bare metal>>	834
41.キャッシュ保護付きライトバックモードを管理する.....	837
41.1 キャッシュ保護付きライトバックモードの概要.....	838
41.2 キャッシュ保護付きライトバックモードの有効化.....	839
41.2.1 キャッシュ保護付きライトバックモードを有効にする <<Bare metal>>.....	839
41.2.2 キャッシュ保護付きライトバックモードを有効にする <<Cloud>>.....	841
41.3 キャッシュ保護用メタデータの冗長度の確認.....	844
41.3.1 キャッシュ保護用メタデータの冗長度を確認する <<Bare metal>>.....	844
41.3.2 キャッシュ保護用メタデータの冗長度を確認する <<Cloud>>.....	845
42.格納データ暗号化を利用する.....	847
42.1 格納データ暗号化の概要.....	848
42.2 暗号化環境の設定を編集する.....	851
42.3 暗号化環境の設定の情報を取得する.....	852

42.4 ストレージプールの暗号化の設定を編集する.....	852
42.5 暗号化鍵を作成する.....	853
42.6 暗号化鍵を削除する.....	854
42.7 暗号化鍵の情報の取得.....	855
42.7.1 取得できる暗号化鍵の情報<<Bare metal>>.....	855
42.7.2 取得できる暗号化鍵の情報<<Cloud>>.....	855
42.7.3 暗号化鍵の情報の一覧を取得する.....	856
42.7.4 暗号化鍵の情報を個別に取得する.....	856
42.8 暗号化鍵の個数を取得する.....	857
43.Universal Replicator を利用する.....	859
43.1 Universal Replicator の概要.....	860
43.2 Universal Replicator 利用時の留意事項.....	860
44.容量バランスを管理する.....	863
44.1 容量バランスの概要.....	864
44.2 容量バランスの発動条件.....	867
44.3 ストレージクラスターの容量バランスの設定を編集する.....	869
44.4 ストレージクラスターの容量バランスの設定を取得する.....	870
44.5 ストレージコントローラーの容量バランスの設定を編集する.....	870
44.6 ストレージコントローラーの容量バランスの設定を取得する.....	871
44.7 ストレージノードの容量バランスの設定を編集する.....	871
44.8 ストレージノードの容量バランスの情報の取得.....	872
44.8.1 取得できるストレージノードの容量バランスの情報.....	872
44.8.2 ストレージノードの容量バランスの情報を一覧で取得する.....	872
44.8.3 ストレージノードの容量バランスの情報を個別に取得する.....	873
45.メタデータのドライブ書き込み削減モードを管理する.....	875
45.1 メタデータのドライブ書き込み削減モードの概要.....	876
45.2 メタデータのドライブ書き込み削減モードを有効にする.....	877
45.3 メタデータのドライブ書き込み削減モードを無効にする.....	878
付録 A 容量設計(HPEC 4D+1P の場合)<<Bare metal>>.....	881
A.1 容量設計の考え方(1):物理容量(HPEC 4D+1P の場合)<<Bare metal>>.....	882
A.2 容量設計の考え方(2):論理容量(HPEC 4D+1P の場合)<<Bare metal>>.....	882
A.3 容量設計方法(1)-1 物理容量から論理容量(HPEC 4D+1P の場合)<<Bare metal>>.....	884
A.4 容量設計方法(2) 論理容量から物理容量(HPEC 4D+1P の場合)<<Bare metal>>.....	885
付録 B 容量設計(HPEC 4D+2P の場合).....	887
B.1 容量設計の考え方(1):物理容量(HPEC 4D+2P の場合).....	888
B.2 容量設計の考え方(2):論理容量(HPEC 4D+2P の場合).....	888
B.3 容量設計方法(1)-1 物理容量から論理容量(HPEC 4D+2P の場合).....	890
B.4 容量設計方法(2) 論理容量から物理容量(HPEC 4D+2P の場合).....	890

付録 C 容量設計(Mirroring の場合).....	893
C.1 容量設計の考え方(1):物理容量(Mirroring の場合).....	894
C.2 容量設計の考え方(2):論理容量(Mirroring の場合).....	894
C.3 容量設計方法(1)-1 物理容量から論理容量(Mirroring の場合).....	896
C.4 容量設計方法(2) 論理容量から物理容量(Mirroring の場合).....	896
付録 D 増設時の容量設計.....	899
D.1 容量増設の方法.....	900
D.2 ストレージノード増設時の容量設計(HPEC 4D+1P の場合)≪Bare metal≫.....	900
D.3 ドライブ増設時の容量設計(HPEC 4D+1P の場合)≪Bare metal≫.....	901
D.4 ストレージノード増設時の容量設計(HPEC 4D+2P の場合).....	902
D.5 ドライブ増設時の容量設計(HPEC 4D+2P の場合).....	902
D.6 ストレージノード増設時の容量設計(Mirroring の場合).....	903
D.7 ドライブ増設時の容量設計(Mirroring の場合).....	904
付録 E ALUA 構築ガイドライン.....	905
E.1 必要な事前設定.....	906
E.1.1 VMware ESXi.....	906
E.1.2 Microsoft Windows.....	906
E.1.3 Linux.....	907
E.2 ALUA の設定手順.....	907
E.2.1 VMware ESXi(NMP の場合).....	907
E.2.2 Microsoft Windows(MPIO の場合).....	907
E.2.3 Linux 系(Device Mapper の場合).....	907
付録 F ANA 構築ガイドライン.....	909
F.1 必要な事前設定.....	910
F.1.1 VMware ESXi.....	910
F.1.2 Linux.....	910
F.2 ANA の設定手順.....	910
F.2.1 VMware ESXi(HPP の場合).....	910
F.2.2 Linux 系(Native NVMe Multipath の場合).....	910
付録 G スナップショット操作の処理時間≪Bare metal≫.....	913
G.1 スナップショット操作の処理時間(目安)≪Bare metal≫.....	914
付録 H ハードウェア交換の条件≪Bare metal≫.....	917
H.1 ハードウェア交換の条件≪Bare metal≫.....	918
付録 I 容量削減機能が有効なボリュームの削除時間.....	921
I.1 容量削減機能が有効なボリュームの削除時間(目安).....	922
付録 J ストレージコントローラーへの容量割り付けの処理時間.....	923
J.1 ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安).....	924

J.2 ストレージコントローラーへの容量割り付けの処理時間(論理容量)(目安).....	925
用語解説.....	927



はじめに

このマニュアルには、Virtual Storage Platform One SDS Block(以降、VSP One SDS Block)のセットアップ後の運用方法、操作方法に関する情報と手順を記載しています。

- マニュアルの参照と適合ソフトウェアバージョン
- 対象読者
- マニュアルで使用する記号について
- 単位表記について
- ストレージシステムの表記について
- 発行履歴

マニュアルの参照と適合ソフトウェアバージョン

このマニュアルは、VSP One SDS Block ソフトウェアバージョン 01.18.0x.xx に適合しています。

このマニュアルは、VSP One SDS Block の Bare metal モデル、および Cloud モデルを対象としています。

- マニュアル内で<<Bare metal>>と記述があるのは、Bare metal モデルに適用される内容です。
- マニュアル内で<<Cloud>>と記述があるのは、Cloud モデルに適用される内容です。クラウドプラットフォームによって内容が異なる場合、以下のように示しています。
 - <<Cloud for AWS>>AWS 向け Cloud モデルの内容です。本文中では「Cloud モデル for AWS」とも表記しています。
 - <<Cloud for Google Cloud>>Google Cloud 向け Cloud モデルの内容です。本文中では「Cloud モデル for Google Cloud」とも表記しています。
 - <<Cloud for Microsoft Azure>>Microsoft Azure 向け Cloud モデルの内容です。本文中では「Cloud モデル for Microsoft Azure」とも表記しています。

モデルの確認方法は「モデルを確認する」を参照してください。



メモ

VSP One SDS Block が出力するメッセージやイベントログ、一部の GUI などに、製品名が Virtual Storage Software Block と表示されることがあります。VSP One SDS Block に置き換えてお読みください。

対象読者

このマニュアルは、VSP One SDS Block のシステム管理者や利用者を対象としています。

対象読者には、以下の知識やスキルが必要です。

- ネットワークに関する知識
- Windows および Linux に関する知識
- VSP One SDS Block の REST API と CLI に関する知識
- ハイパーバイザー型の仮想環境に関する知識
- 物理サーバーの運用管理に関する知識
- Amazon Web Services (AWS)に関する知識
- Google Cloud に関する知識
- Microsoft Azure に関する知識

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、コマンドの書式を次の記号を使って記述しています。

記号	説明
<>	この記号で囲まれている項目は可変値であることを示します。
	複数の項目の区切りとして、「または」の意味を示します。

記号	説明
[]	この記号で囲まれている項目は省略してもよいことを示します。 (例) [a b] 何も指定しないか、a または b を指定します。
{ }	この記号で囲まれている項目のうち、どれか 1 つを必ず指定することを示します。 (例) { a b } a または b を指定します。

このマニュアルでは、注意書きや補足情報を、以下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。

単位表記について

このマニュアルでは、単位表記を以下のように記載しています。

1KB(キロバイト)、1MB(メガバイト)、1GB(ギガバイト)、1TB(テラバイト)は、それぞれ 1,000 バイト、1,000² バイト、1,000³ バイト、1,000⁴ バイトです。

1KiB(キビバイト)、1MiB(メビバイト)、1GiB(ギビバイト)、1TiB(テビバイト)は、それぞれ 1,024 バイト、1,024² バイト、1,024³ バイト、1,024⁴ バイトです。

ストレージシステムの表記について

このマニュアルでは、ストレージシステムを以下のように表記しています。

- Hitachi Virtual Storage Platform One SDS Block を「VSP One SDS Block」と表記
- Hitachi Virtual Storage Platform 5000 シリーズを「VSP 5000 シリーズ」と表記
- Hitachi Virtual Storage Platform One Block 23, Block 26, Block 28 を「VSP One B20」と表記
- Hitachi Virtual Storage Platform E1090 を「VSP E1090」と表記
- Hitachi Virtual Storage Platform E1090H を「VSP E1090H」と表記

発行履歴

マニュアル資料番号	発行年月	変更内容
4048-1J-U20-31	2025 年 8 月	- 適合 VSP One SDS Block ソフトウェアバージョン： 01.18.0x.xx - 格納データ暗号化のサポート範囲拡大による見直しをした。 2.1 運用環境を構成するには 2.4 運用状況を監視するには 2.5 リソース情報を確認するには 2.6 設定を確認するには 2.7 リソースを追加・削除・変更するには 2.8 設定を変更するには 3.4.2 空状態にあるストレージプールを拡張する 《Cloud》 4.1.1 ライセンス管理の概要《Bare metal》 4.1.2 ライセンス管理の概要《Cloud》 4.2.1 ライセンスを登録する《Bare metal》 4.2.2 ライセンスを登録する《Cloud》 9.6 ストレージプールを拡張する 32.8 ストレージソフトウェアをダウングレードする 《Cloud for AWS》 42 格納データ暗号化を利用する - 取得情報を追加した。 24.13 ストレージプールの性能情報の一覧を取得する 24.14 ストレージプールの性能情報を個別に取得する 24.19 ストレージノードの性能情報の一覧を取得する 24.20 ストレージノードの性能情報を個別に取得する 24.23 ボリュームの性能情報の一覧を取得する 24.24 ボリュームの性能情報を個別に取得する 24.25 ジャーナルの性能情報の一覧を取得する 24.26 ジャーナルの性能情報を個別に取得する - VSP E1090、VSP E1090H の対応で説明を見直した。 19.1 ユーザー管理の概要 32.5 ストレージソフトウェアをダウングレードする 《Bare metal》 32.6 ストレージソフトウェアをダウングレードする 《Cloud》 「VSP」の名称を「VSP ファミリー」に変更した。 - 説明を追加した。

マニュアル資料番号	発行年月	変更内容
		32.3 ストレージソフトウェアをアップグレードする 《Bare metal》 32.4 ストレージソフトウェアをアップグレードする 《Cloud》 32.5 ストレージソフトウェアをダウングレードする 《Bare metal》 32.6 ストレージソフトウェアをダウングレードする 《Cloud》 - 新規バージョンの追加により、ソフトウェアアップデート関連の記述を追加した。 32.1 ストレージソフトウェアアップデートの概要 - Universal Replicator 関連の説明を追加・変更した。 19.1 ユーザー管理の概要 32.5 ストレージソフトウェアをダウングレードする 《Bare metal》 32.6 ストレージソフトウェアをダウングレードする 《Cloud》 34.1 構成情報の変更・設定の概要《Bare metal》 34.3 構成情報の変更・設定のために VSSB 構成ファイルを編集する《Bare metal》 34.4 構成情報を変更・設定する《Bare metal》 43.1 Universal Replicator の概要 - VSP One SDS Block Administrator のサーバー証明インポートのサポートに伴う記載を追加した。 2.2 ユーザー登録とセキュリティ対策をするには 22.11 SSL/TLS 通信の署名付き証明書をインポートする - Universal Replicator 性能改善により内容の追加、見直しをした。 32.4 ストレージソフトウェアをダウングレードする 45.メタデータのドライブ書き込み削減モードを管理する - NVMe Drive Direct Attach のサポートに伴い、記載を追記した。 8.3 ドライブを減設する《Bare metal》 8.4.1 ドライブを交換する《Bare metal》 32.5 ストレージソフトウェアをダウングレードする 《Bare metal》 - Google Cloud のサポートに伴い、記載を追加・変更した。 - 本マニュアル全体 - Microsoft Azure のサポートに伴い、記載を追加・変更した。 - 本マニュアル全体 - 注意事項と手順を追加した。 3.5 ログイン時・CLI Basic 認証時に表示するメッセージを設定する

マニュアル資料番号	発行年月	変更内容
		- 補足説明を修正した。 14.2 ドライブデータ再配置の起動契機と動作可能な条件<<Bare metal>> - 連携可能な外部認証サーバーのバージョンを見直した。 19.15.1 外部認証サーバー利用の概要 - キャッシュ保護付きライトバックモードの一部の機能変更により、節と項を削除した。 41.3 キャッシュ保護付きライトバックモードの無効化 41.3.1 キャッシュ保護付きライトバックモードを無効にする<<Bare metal>> 41.3.2 キャッシュ保護付きライトバックモードを無効にする<<Cloud>> - キャッシュ保護付きライトバックモードの一部の機能変更により、説明を変更した。 13.3.1 ストレージノードの保守閉塞の条件を確認する<<Bare metal>> 13.3.2 ストレージノードの保守閉塞の条件を確認する<<Cloud>> 32.7 ストレージソフトウェアをダウングレードする<<Bare metal>> 32.8 ストレージソフトウェアをダウングレードする<<Cloud for AWS>> 41.1 キャッシュ保護付きライトバックモードの概要 41.2.1 キャッシュ保護付きライトバックモードを有効にする<<Bare metal>> 41.2.2 キャッシュ保護付きライトバックモードを有効にする<<Cloud>> 41.3.1 キャッシュ保護用メタデータの冗長度を確認する<<Bare metal>> 41.3.2 キャッシュ保護用メタデータの冗長度を確認する<<Cloud>> - 一部のバージョン混在時の注意を追加した。 32.2.4 ソフトウェアアップデート中の動作 - ボリューム削除時のストレージプール使用論理容量について注意を追加した。 17.5 ボリュームを削除する - AWS の構成バックアップリスト対応で記載を見直した。 1.1.2 ユーザーデータの保護方式<<Cloud>> 3.4.1 空状態にあるストレージプールを拡張する<<Bare metal>> 3.4.2 空状態にあるストレージプールを拡張する<<Cloud>> 3.5 ログイン時・CLI Basic 認証時に表示するメッセージを設定する 3.6.1 許可リストを設定する<<Bare metal>>

マニュアル資料番号	発行年月	変更内容
		3.6.2 許可リストを設定する<<Cloud>> 4.2.1 ライセンスを登録する<<Bare metal>> 4.2.2 ライセンスを登録する<<Cloud>> 4.3.1 ライセンスを削除する<<Bare metal>> 4.3.2 ライセンスを削除する<<Cloud>> 4.5.1 ライセンスの警告しきい値を編集する<<Bare metal>> 6.3.1 イベントログの Syslog 転送設定を編集する<<Bare metal>> 6.3.2 イベントログの Syslog 転送設定を編集する<<Cloud>> 6.4.1 イベントログの SMTP 転送設定を編集する<<Bare metal>> 6.4.2 イベントログの SMTP 転送設定を編集する<<Cloud>> 6.9.2 SNMP アクセスコントロールを設定する 7.3.1 監査ログの Syslog 転送設定を編集する<<Bare metal>> 7.3.2 監査ログの Syslog 転送設定を編集する<<Cloud>> 8.3.1 ドライブを減設する<<Bare metal>> 8.4.1 ドライブを交換する<<Bare metal>> 8.4.2 ドライブを交換する<<Cloud for AWS>> 9.6 ストレージプールを拡張する 11.1.6 増設したストレージノードの設定を行う<<Bare metal>> 11.2.3 増設したストレージノードの設定を行う<<Cloud for AWS>> 12.1.2 ストレージノードを減設する<<Bare metal>> 12.2.2 ストレージノードを減設する<<Cloud for AWS>> 13.2.1 ストレージノードを保守回復する<<Bare metal>> 13.2.2 ストレージノードを保守回復する<<Cloud for AWS>> 13.4.1 ストレージノードを交換する<<Bare metal>> 13.4.2 ストレージノードを交換する<<Cloud for AWS>> 13.5.1 ストレージノードの自動回復機能を設定する<<Bare metal>> 13.5.2 ストレージノードの自動回復機能を設定する<<Cloud>> 15.1 コンピュートノードの情報を登録する 15.4 コンピュートノードの情報を編集する 15.5 コンピュートノードの情報を削除する 15.6.1 iSCSI 接続している場合

マニュアル資料番号	発行年月	変更内容
		15.6.2 NVMe/TCP 接続している場合<<Bare metal>> 15.6.3 FC 接続している場合<<Bare metal>> 15.8 コンピュートノードのイニシエーター情報を削除する 15.9 コンピュートノードのパス情報を登録する 15.11.1 コンピュートノードのパス情報を削除する<<Bare metal>> 15.11.2 コンピュートノードのパス情報を削除する<<Cloud>> 15.12.1 ボリュームをコンピュートノードに接続する<<Bare metal>> 15.12.2 ボリュームをコンピュートノードに接続する<<Cloud>> 15.14.1 ボリュームとコンピュートノードの接続を解除する<<Bare metal>> 15.14.2 ボリュームとコンピュートノードの接続を解除する<<Cloud>> 15.15.1 複数のボリュームとコンピュートノードの接続を解除する<<Bare metal>> 15.15.2 複数のボリュームとコンピュートノードの接続を解除する<<Cloud>> 16.2.1 コンピュートポートの設定を編集する<<Bare metal>> 16.2.2 コンピュートポートの設定を編集する<<Cloud>> 16.3 コンピュートポートのプロトコルを変更する<<Bare metal>> 17.4.1 ボリュームを作成する<<Bare metal>> 17.4.2 ボリュームを作成する<<Cloud>> 17.5 ボリュームを削除する 17.6 ボリュームを拡張する 17.9 ボリュームの設定を編集する 18.1 スナップショットの概要 18.4 スナップショットを削除する 19.4 ユーザーを作成する 19.5 ユーザー情報を編集する 19.6 ユーザーを削除する 19.7 自身のパスワードを変更する 19.8 ユーザーをユーザーグループに追加する 19.9 ユーザーをユーザーグループから削除する 19.12 ユーザーグループを作成する 19.13 ユーザーグループ情報を編集する 19.14 ユーザーグループを削除する 19.15.2 外部認証サーバー利用の操作

マニュアル資料番号	発行年月	変更内容
		◦ 21.1 ユーザー認証設定を編集する ◦ 22.11 SSL/TLS 通信の署名付き証明書をインポートする ◦ 23.1 CHAP ユーザーを作成して CHAP 認証を設定する ◦ 23.4 CHAP ユーザー情報を編集する ◦ 23.5 CHAP ユーザーを削除する ◦ 23.7 ターゲット動作のコンピュータポートの認証設定を編集する ◦ 23.8 CHAP ユーザーに対してコンピュータポートへのアクセスを許可する ◦ 23.10 CHAP ユーザーに対してコンピュータポートへのアクセス許可を解除する ◦ 26.6 ストレージプールの設定を編集する ◦ 28.3 内部処理 I/O のリソース使用率を変更する ◦ 29.4 ストレージコントローラーの設定を編集する ◦ 32.3 ストレージソフトウェアをアップグレードする<<Bare metal>> ◦ 32.4 ストレージソフトウェアをアップグレードする<<Cloud for AWS>> ◦ 32.8 ストレージソフトウェアをダウングレードする<<Cloud for AWS>> ◦ 34.4 構成情報を変更・設定する<<Bare metal>> ◦ 36 構成情報をバックアップする<<Bare metal>> <<Cloud for AWS>> ◦ 36.1 構成バックアップ・構成リストアの概要<<Bare metal>> <<Cloud for AWS>> ◦ 36.2 構成バックアップを行う<<Bare metal>> <<Cloud for AWS>> ◦ 37.1 ストレージソフトウェアのアンインストールの概要 ◦ 37.5 構成バックアップファイルを削除する<<Bare metal>> <<Cloud for AWS>> ◦ 39.1 マルチテナンシーの概要<<Bare metal>> ◦ 40.1 スペアノードの概要<<Bare metal>> ◦ 42.1 格納データ暗号化の概要 ◦ 42.2 暗号化環境の設定を編集する ◦ 42.4 ストレージプールの暗号化の設定を編集する ◦ 44.3 ストレージクラスターの容量バランスの設定を編集する ◦ 44.5 ストレージコントローラーの容量バランスの設定を編集する ◦ 44.7 ストレージノードの容量バランスの設定を編集する ・ AWS 環境におけるコントローラーノードレスのサポートに伴い、項を削除した。

マニュアル資料番号	発行年月	変更内容
		◦ 3.2.8 VSP One SDS Block インストーラーについて 《Cloud for AWS》 ◦ 22.10.3 VSP One SDS Block インストーラーにルート証明書をインストールする方法《Cloud for AWS》 • AWS 環境におけるコントローラーノードレスのサポートに伴い、項を追加した。 ◦ 13.4.3 ストレージソフトウェアのバージョンが混在している場合のストレージノード交換《Cloud for AWS》 • AWS 環境におけるコントローラーノードレスのサポートに伴い、記載を変更した。 ◦ 3.1.6 構成ファイルをエクスポートする《Cloud for AWS》 ◦ 3.2.2 コントローラーノードの設置《Cloud for AWS》 ◦ 8.4.2 ドライブを交換する《Cloud for AWS》 ◦ 9.3 ドライブを作成する《Cloud for AWS》 ◦ 10.2.2 取得できるストレージノード情報《Cloud》 ◦ 11.2.1 ストレージノードを増設する《Cloud for AWS》 ◦ 12.2.2 ストレージノードを減設する《Cloud for AWS》 ◦ 13.4.2 ストレージノードを交換する《Cloud for AWS》 ◦ 22.10 ルート証明書をインポートする ◦ 22.12.2 SSL/TLS 通信のクライアント要件 《Cloud》 ◦ 22.13 サーバー証明書に関する警告メッセージが表示されたときの対処 ◦ 27.2.2 取得できるフォールトドメインの一覧情報 《Cloud》 ◦ 27.3.2 取得できるフォールトドメインの個別情報 《Cloud》 ◦ 32.4 ストレージソフトウェアをアップグレードする 《Cloud for AWS》 ◦ 32.8 ストレージソフトウェアをダウングレードする 《Cloud for AWS》 ◦ 36.2 構成バックアップを行う《Bare metal》《Cloud for AWS》 • サーバー証明書更新時の注意を追加した。 ◦ 22.3 サーバー証明書を更新するときの注意事項 • AWS CLI コマンドについてのメモを追加した。 ◦ 3.1.6 構成ファイルをエクスポートする《Cloud for AWS》 • ストレージノード交換時の EC2 インスタンスについて、注意を追加した。

マニュアル資料番号	発行年月	変更内容
		13.4.2 ストレージノードを交換する「Cloud for AWS」 - KB の参照先を見直した。 - E.1.1 VMware ESXi - ホストからの I/O 停止について手順を追加した。 45.2 メタデータのドライブ書き込み削減モードを有効にする 45.3 メタデータのドライブ書き込み削減モードを無効にする
4048-1J-U20-21	2025 年 6 月	- 適合 VSP One SDS Block ソフトウェアバージョン：01.17.0x.xx - キャッシュ保護付きライトバックモードの一部の機能変更により削除した。 41.3 キャッシュ保護付きライトバックモードを無効にする - キャッシュ保護付きライトバックモードの一部の機能変更により、説明を変更した。 13.3 ストレージノードの保守閉塞の条件を確認する 32.4 ストレージソフトウェアをダウングレードする 41.1 キャッシュ保護付きライトバックモードの概要 41.2 キャッシュ保護付きライトバックモードを有効にする 41.3 キャッシュ保護用メタデータの冗長度を確認する
4048-1J-U20-20	2024 年 12 月	- 適合 VSP One SDS Block ソフトウェアバージョン：01.17.0x.xx - コンピュータネットワークの IPv6 アドレスサポートに関する記載を追加した。 32.4 ストレージソフトウェアをダウングレードする - サポートする外部認証サーバーとバージョンを追加した。 19.1 ユーザー管理の概要 19.15 外部認証サーバーを利用する - FC 接続のサポートに伴い、記載を追加・変更した。 1.2 システムの構成 3.3 コンピュートノードを設置する 3.3.1 コンピュートノード設置に当たっての注意事項 11.4 構成ファイルを編集する「Bare metal」 13.2 ストレージノードを保守回復する 15.3 コンピュートノード情報を個別に取得する 15.6 コンピュートノードのイニシエーター情報を登録する 15.6.3 FC 接続している場合「Bare metal」 15.7 コンピュートノードのイニシエーター情報の一覧を取得する

マニュアル資料番号	発行年月	変更内容
		15.8 コンピュートノードのイニシエーター情報を個別に取得する 15.9 コンピュートノードのイニシエーター情報を削除する 15.11 コンピュートノードのパス情報の一覧を取得する 15.12 コンピュートノードのパス情報を個別に取得する 15.13 コンピュートノードのパス情報を削除する 15.14 ボリュームをコンピュートノードに接続する 15.15 ボリュームとコンピュートノードの接続情報の一覧を取得する 15.16 ボリュームとコンピュートノードの接続情報を個別に取得する 15.17 ボリュームとコンピュートノードの接続を解除する 15.18 複数のボリュームとコンピュートノードの接続を解除する 16.1 コンピュートポートの情報の一覧を取得する 16.2 コンピュートポートの情報を個別に取得する 16.3 コンピュートポートの設定を編集する 16.4 コンピュートポートのプロトコルを変更する 《Bare metal》 17.8 ボリューム情報を個別に取得する 23.1 CHAP ユーザーを作成して CHAP 認証を設定する 23.6 ターゲット動作のコンピュートポートの認証設定を取得する 23.7 ターゲット動作のコンピュートポートの認証設定を編集する 23.8 CHAP ユーザーに対してコンピュートポートへのアクセスを許可する 23.9 コンピュートポートへのアクセスを許可した CHAP ユーザー情報の一覧を取得する 23.10 コンピュートポートへのアクセスを許可した CHAP ユーザー情報を個別に取得する 23.11 CHAP ユーザーに対してコンピュートポートへのアクセス許可を解除する 24.15 コンピュートポートの性能情報(低解像度)の一覧を取得する 24.16 コンピュートポートの性能情報(高解像度)の一覧を取得する 24.17 コンピュートポートの性能情報を個別に取得する 32.4 ストレージソフトウェアをダウングレードする 33.5 ストレージクラスターを停止する 33.6 ストレージクラスターを強制停止する

マニュアル資料番号	発行年月	変更内容
		◦ 34.1 構成情報の変更・設定の概要<<Bare metal>> ◦ 34.3 構成情報の変更・設定のために VSSB 構成ファイルを編集する<<Bare metal>> ◦ 34.4 構成情報を変更・設定する<<Bare metal>> ◦ 39.3 テナント共通の設定<<Bare metal>> ◦ 40.2 スペアノード切り換えの概要<<Bare metal>> ◦ 40.3 スペアノードを準備する<<Bare metal>> ◦ H.1 ハードウェア交換の条件<<Bare metal>> ・ 用語表現などを見直した。 ◦ 13.6 ストレージノードの自動回復機能を設定する ◦ 40.2 スペアノード切り換えの概要<<Bare metal>> ・ マルチテナンシー機能の外部認証サポートに伴い、説明を追加した。 ◦ 32.4 ストレージソフトウェアをダウングレードする ◦ 39.1 マルチテナンシーの概要<<Bare metal>> ◦ 39.4 システム管理者向けの設定<<Bare metal>> ◦ 39.5 VPS を作成する<<Bare metal>> ・ 「ホワイトリスト」を「許可リスト」に修正した。 ◦ 2.2 ユーザー登録とセキュリティ対策をするには ◦ 2.6 設定を確認するには ◦ 2.8 設定を変更するには ◦ 3.2 コントローラーノードの設置と管理操作 ◦ 3.6 許可リストを設定する ◦ 19.1 ユーザー管理の概要 ◦ 34.2 管理ネットワーク変更時の運用の注意<<Bare metal>> ◦ 39.3 テナント共通の設定<<Bare metal>> ・ 説明を見直した。 ◦ 22.1 TLS とは ◦ 22.8 署名付き証明書を取得する ・ 説明を見直した。 ◦ 8.2 ドライブの情報の一覧を取得する ◦ 8.3 ドライブの情報を個別に取得する ・ イベントログの説明を追加した。 ◦ 13.6 ストレージノードの自動回復機能を設定する ・ セッション生成数の上限について説明を追加した。 ◦ 20.1 セッション管理の概要 ・ 前提条件について説明を追加した。 ◦ 20.2 セッションの一覧を取得する ・ Universal Replicator 関連の説明を追加・変更した。 ◦ 2.1 運用環境を構成するには ◦ 11.5 ストレージノードを増設する<<Bare metal>> ◦ 12.1 ストレージノード減設の概要

マニュアル資料番号	発行年月	変更内容
		◦ 12.2 ストレージノード減設の条件を確認する ◦ 15.14 ボリュームをコンピュータノードに接続する ◦ 15.17 ボリュームとコンピュータノードの接続を解除する ◦ 16.4 コンピュータポートのプロトコルを変更する 《Bare metal》 ◦ 17.3 ボリュームの容量削減機能を有効にする ◦ 17.4 ボリュームを作成する ◦ 17.5 ボリュームを削除する ◦ 17.6 ボリュームを拡張する ◦ 18.2 スナップショットの取得準備をする ◦ 18.3 スナップショットを取得する ◦ 18.5 スナップショットからボリュームを復元する ◦ 19.1 ユーザー管理の概要 ◦ 20.1 セッションの管理の概要 ◦ 22.3 サーバー証明書を更新するときの注意事項 ◦ 22.12 SSL/TLS 通信のクライアント要件 ◦ 32.2.5 ソフトウェアアップデート後に必要な操作 ◦ 32.3 ストレージソフトウェアをアップグレードする ◦ 32.4 ストレージソフトウェアをダウングレードする ◦ 34.1 構成情報の変更・設定の概要《Bare metal》 ◦ 34.3 構成情報の変更・設定のために VSSB 構成ファイルを編集する《Bare metal》 ◦ 34.4 構成情報を変更・設定する《Bare metal》 ◦ 36.1 構成バックアップ・構成リストアの概要 ◦ 36.2 構成バックアップを行う ◦ 39.1 マルチテナンシーの概要《Bare metal》 ◦ 41.1 キャッシュ保護付きライトバックモードの概要 ◦ 41.3 キャッシュ保護付きライトバックモードを無効にする ◦ 43 Universal Replicator を利用する ◦ 43.1 Universal Replicator の概要 ◦ 43.2 Universal Replicator 利用時の留意事項 ◦ 用語解説 • ロケーター LED がサポートされていない構成の場合について説明を追加した。 ◦ 8.4 ドライブを減設する《Bare metal》 ◦ 8.5 ドライブを交換する《Bare metal》 • 新規バージョンの追加により、ソフトウェアアップデート関連の記述を追加した。 ◦ 32.1 ストレージソフトウェアアップデートの概要 • VSP One SDS Block Administrator のパスワード変更画面のサポートに伴い、説明を追記した。 ◦ 2.7 リソースを追加・削除・変更するには

マニュアル資料番号	発行年月	変更内容
		◦ 19.7 自身のパスワードを変更する • 適用可能サーバ種の拡大サポートに伴う記載を追加した。 ◦ 3.2.2 コンソールインターフェイスについて<<Bare metal>> ◦ 3.6 許可リストを設定する ◦ 13.2 ストレージノードを保守回復する ◦ 13.4 ストレージノードを保守閉塞する ◦ 33.5 ストレージクラスターを停止する ◦ 33.6 ストレージクラスターを強制停止する ◦ 38.1 コンソールインターフェイスの概要 ◦ 38.2 ログインとログアウト ◦ 38.5 コンソールインターフェイスの留意事項 • タイトルを見直した。 ◦ 14 ドライブデータ再配置を管理する<<Bare metal>> • 注意事項を追加した。 ◦ 40.1 スペアノードの概要<<Bare metal>> ◦ 40.2 スペアノード切り換えの概要<<Bare metal>> ◦ 40.3 スペアノードを準備する<<Bare metal>> ◦ 40.4 スペアノードを利用するための BMC アカウントを準備する<<Bare metal>> ◦ 40.8 ストレージノードの BMC 情報を登録・編集する<<Bare metal>> ◦ 40.11 スペアノードの情報を登録する<<Bare metal>> ◦ 40.12 スペアノードの情報を編集する<<Bare metal>> ◦ 40.16 スペアノード機能の設定を確認する<<Bare metal>> • 容量バランスの機能追加により説明を独立させて新しい章とした。 ◦ 2.6 設定を確認するには ◦ 2.8 設定を変更するには ◦ 10 ストレージノードを管理する ◦ 10.1 ストレージノード管理の概要 ◦ 19.1 ユーザー管理の概要 ◦ 39.11 性能低下・操作不可の監視と対処<<Bare metal>> ◦ 44 容量バランスを管理する • 前提条件を見直した。 ◦ 41.2 キャッシュ保護付きライトバックモードを有効にする ◦ 41.3 キャッシュ保護付きライトバックモードを無効にする • 説明を追加した。

マニュアル資料番号	発行年月	変更内容
		◦ 40.2 スペアノード切り換えの概要<<Bare metal>> ・ ロール説明を見直した。 ◦ 19.2 ユーザー情報の一覧を取得する ◦ 20.3 セッション情報を取得する ・ 手順説明を一部見直した。 ◦ 22.7 証明書署名要求を作成する ・ リビルド処理時間の前提条件を追加した。 ◦ 30.3 リビルド完了までの時間(目安) ・ ライセンスが無効状態のときに実施できる操作を見直した。 ◦ 4.1 ライセンス管理の概要 ◦ 33.5 ストレージクラスターを停止する ・ 手順説明を一部見直した。 ◦ 8.6 ドライブを交換する<<Cloud>> ◦ 9.3 ドライブを作成する<<Cloud>> ◦ 11.6 ストレージノードを増設する<<Cloud>> ◦ 12.3 ストレージノードを減設する ◦ 13.5.2 ストレージノードを交換する<<Cloud>> ◦ 32.3 ストレージソフトウェアをアップグレードする ・ 注意事項を追加した。 ◦ 40.16 スペアノード機能の設定を確認する<<Bare metal>> ・ メモを追加した。 ◦ 6.1 イベントログについて ・ 説明を追加した。 ◦ 39.1 マルチテナンシーの概要<<Bare metal>> ・ 説明を追加した。 ◦ 3.6 許可リストを設定する ・ 説明を追加した。 ◦ 32.1 ストレージソフトウェアアップデートの概要 ・ 説明を追加した。 ◦ 21.1 ユーザー認証設定を編集する ◦ 21.2 ユーザー認証設定を取得する ・ 説明を見直した。 ◦ 3.3 コンピュートノードを設置する ・ 手順番号を一部見直した。 ◦ 3.3 コンピュートノードを設置する ・ 手順説明を見直した。 ◦ 11.3 システム要件ファイルを更新する<<Bare metal>> ◦ 13.5.1 ストレージノードを交換する<<Bare metal>> ◦ 32.3 ストレージソフトウェアをアップグレードする ◦ 32.4 ストレージソフトウェアをダウングレードする ・ 説明を一部見直した。

マニュアル資料番号	発行年月	変更内容
		3.1.3 構成ファイルをエクスポートする<<Cloud>> - 手順説明を一部見直した。 8.6 ドライブを交換する<<Cloud>> - 外部認証サーバーに関する説明を見直した。 19.15 外部認証サーバーを利用する 32.2.5 ソフトウェアアップデート後に必要な操作 - 一部説明を見直した。 13.5.1 ストレージノードを交換する<<Bare metal>> 13.6 ストレージノードの自動回復機能を設定する 15.6.3 FC 接続している場合<<Bare metal>> - スペアノード切り換えが動作する条件を追加した。 40.2 スペアノード切り換えの概要<<Bare metal>> 40.3 スペアノードを準備する<<Bare metal>> - インスタンスタイプについて説明を追加した。 17.2 ボリュームの容量削減機能の概要 32.4.1 ダウングレード時の VM 構成ファイルを作成する<<Cloud>> 41.2 キャッシュ保護付きライトバックモードを有効にする - 手順を追加した。 19.15 外部認証サーバーを利用する - 手順説明ほかを見直した。 15.10 コンピュートノードのパス情報を登録する 16.3 コンピュートポートの設定を編集する 23.1 CHAP ユーザーを作成して CHAP 認証を設定する 23.6 ターゲット動作のコンピューポートの認証設定を取得する 23.7 ターゲット動作のコンピューポートの認証設定を編集する 23.8 CHAP ユーザーに対してコンピューポートへのアクセスを許可する 23.9 コンピュートポートへのアクセスを許可した CHAP ユーザー情報の一覧を取得する 23.10 コンピュートポートへのアクセスを許可した CHAP ユーザー情報を個別に取得する 23.11 CHAP ユーザーに対してコンピューポートへのアクセス許可を解除する - ストレージノードの自動回復機能に関し、説明の追加と用語の見直しを行った。 13.6 ストレージノードの自動回復機能を設定する 13.7 ストレージノードの自動回復機能の情報を取得する - 説明を追加した。 21.1 ユーザー認証設定を編集する

マニュアル資料番号	発行年月	変更内容
		- 説明を追加した。 - A.1 容量設計の考え方(1):物理容量(HPEC 4D+1P の場合)≪Bare metal≫ - A.3 容量設計方法(1)-1 物理容量から論理容量(HPEC 4D+1P の場合)≪Bare metal≫ - B.1 容量設計の考え方(1):物理容量(HPEC 4D+2P の場合) - B.3 容量設計方法(1)-1 物理容量から論理容量(HPEC 4D+2P の場合) - C.1 容量設計の考え方(1):物理容量(Mirroring の場合) - C.3 容量設計方法(1)-1 物理容量から論理容量(Mirroring の場合)
4048-1J-U20-10	2024 年 9 月	- 適合 VSP One SDS Block ソフトウェアバージョン : 01.16.0x.xx - Universal Replicator の VSP One B20 のサポートに伴い、記載を変更・追加した。 19.1 ユーザー管理の概要 32.4 ストレージソフトウェアをダウングレードする - 説明文を一部見直した。 17.5 ボリュームを削除する - オーバープロビジョニングについての説明を追加した。 17.1.1 ボリュームとストレージプール 17.4 ボリュームを作成する 17.6 ボリュームを拡張する - ユーザー認証設定における lockoutSeconds のシステムの初期値を変更した。 21.1 ユーザー認証設定を編集する - パスワード入力に関する説明を削除・追加した。 3.1.3 構成ファイルをエクスポートする ≪Cloud≫ 11.6 ストレージノードを増設する ≪Cloud≫ 13.5.2 ストレージノードを交換する ≪Cloud≫ - 操作手順内で説明のマスターコマンドオプションのうち、--password の説明を削除した。 34.3 構成情報の変更・設定のために VSSB 構成ファイルを編集する ≪Bare metal≫ - 説明を追加した。 10.4 ストレージノードの容量管理の概要 - 説明を追加した。 32.1 ストレージソフトウェアアップデートの概要 32.4 ストレージソフトウェアをダウングレードする - CLI パスワードオプション非表示化に伴い、説明を変更した。 23.1 CHAP ユーザーを作成して CHAP 認証を設定する

マニュアル資料番号	発行年月	変更内容
		- 格納データ暗号化機能を Cloud モデルにてサポートしたことにより、説明を見直した。 2.1 運用環境を構成するには 2.4 運用状況を監視するには 2.5 リソース情報を確認するには 2.6 設定を確認するには 2.7 リソースを追加・削除・変更するには 2.8 設定を変更するには 3.4 ストレージプールを拡張する 4.1 ライセンス管理の概要 9.4 ストレージプールを拡張する 26.5 ストレージプールの情報の一覧を取得する 26.6 ストレージプールの情報を個別に取得する 32.4 ストレージソフトウェアをダウングレードする 36.1 構成バックアップ・構成リストアの概要 42 格納データ暗号化を利用する - 説明を見直した。 32.4 ストレージソフトウェアをダウングレードする 32.4.1 ダウングレード時の VM 構成ファイルを作成する<<Cloud>> - 構成ファイルの説明を見直した。 1.2 システムの構成 3.1 構成ファイルを管理する - コンピュータノードの OS に関する記述を見直した。 3.3 コンピュータノードを設置する 3.3.1 コンピュータノード設置に当たっての注意事項 - ルート追加の説明を見直した。 1.2 システムの構成 3.3 コンピュータノードを設置する - 注意事項を追加した。 33.5 ストレージクラスターを停止する - 記載を見直した。 3.1.1 構成ファイルのエクスポート 14.2 ドライブデータ再配置の起動契機と動作可能な条件<<Bare metal>> 39.5 VPS を作成する<<Bare metal>> - メモを追加した。 42.5 暗号化鍵を作成する - 取得情報を追加した。 8.2 ボリューム情報の一覧を取得する 8.3 ボリューム情報を個別に取得する - ストレージシステムの表記について説明を追加した。 - ストレージシステムの表記について

マニュアル資料番号	発行年月	変更内容
		- targetInformation の説明を追加した。 42.7 暗号化鍵の情報の一覧を取得する 42.8 暗号化鍵の情報を個別に取得する - 説明の追加・見直しを行った。 36.1 構成バックアップ・構成リストアの概要<<Bare metal>> - コマンド説明を見直した。 36.2 構成バックアップを行う<<Bare metal>> - 注意事項を追加した。 3.1.3 構成ファイルをエクスポートする<<Cloud>> 8.6 ドライブを交換する<<Cloud>> 9.3 ドライブを作成する<<Cloud>> 11.6 ストレージノードを増設する<<Cloud>> 12.3 ストレージノードを減設する 13.5.2 ストレージノードを交換する<<Cloud>> 32.3 ストレージソフトウェアをアップグレードする 32.4 ストレージソフトウェアをダウングレードする 32.4.1 ダウングレード時の VM 構成ファイルを作成する<<Cloud>> - 記述・語句を追加・削除した。 13.3 ストレージノードの保守閉塞の条件を確認する 16.1 コンピュートポートの情報の一覧を取得する 16.2 コンピュートポートの情報を個別に取得する 32.4 ストレージソフトウェアをダウングレードする - 用語解説
4048-1J-U20-00	2024 年 8 月	新規(適合 VSP One SDS Block ソフトウェアバージョン : 01.15.0x.xx)

VSP One SDS Block の概要

- 1.1 VSP One SDS Block とは
- 1.2 システムの構成<<Bare metal>>
- 1.3 システムの構成<<Cloud for AWS>>
- 1.4 システムの構成<<Cloud for Google Cloud>>
- 1.5 システムの構成<<Cloud for Microsoft Azure>>

1.1 VSP One SDS Block とは

VSP One SDS Block は、複数の汎用サーバーから、1つの仮想的なストレージシステムを構築し、機能させるストレージソフトウェア製品です。

VSP One SDS Block のストレージシステムは、以下のような運用管理の特長を有する高性能・高信頼・大容量のブロックストレージサービスを提供します。

- ・ 汎用サーバー(x86 サーバー)を用いることによって、導入コストを抑えることができます。
- ・ 初期導入、スケールアウト/スケールインが迅速に行えます。
- ・ 複数のストレージノードを1つのストレージシステムとして一元管理できます。
- ・ リソースの稼働状態やその時点で作成可能な最大ボリューム容量や I/O 性能などが容易に把握できます。
- ・ VSP One SDS Block の REST API は、Hitachi Storage Advisor Embedded の REST API と互換です。このため、日立ストレージ製品の管理経験がある管理者は、学習なしで VSP One SDS Block のストレージ管理が行えます。

1.1.1 ユーザーデータの保護方式《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

VSP One SDS Block では、ユーザーデータの保護方式として、HPEC(Hitachi Polyphase Erasure Coding)、Mirroring がサポートされます。HPEC は、ストレージノード間ネットワーク帯域が狭い SDS システム向けに開発した日立独自のデータ保護方式です。HPEC では、ユーザーデータはローカルドライブに格納します。Mirroring はユーザーデータのコピーを別のストレージノードに格納するデータ保護方式です。

HPEC 4D+1P、HPEC 4D+2P、または Mirroring Duplication を選択し、セットアップ作業時に設定します。

ユーザーデータの保護方式については、ストレージコントローラーの冗長度およびクラスターマスターノードの冗長度の設定との組み合わせに制限があります。詳細は、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「VSP One SDS Block がサポートする耐障害性に関する設定と各機能の説明」を参照してください。



メモ

HPEC 4D+1P と HPEC 4D+2P、Mirroring Duplication のそれぞれの容量設計に関しては、このマニュアルの「容量設計(HPEC 4D+1P の場合)《Bare metal》」、「容量設計(HPEC 4D+2P の場合)」、または「容量設計(Mirroring の場合)」を参照してください。



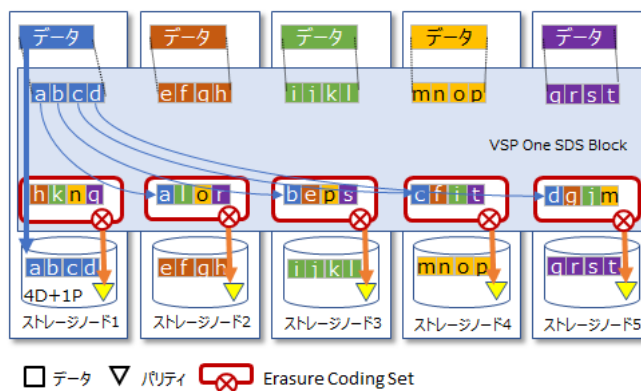
注意

許容される障害数を超える障害が発生した場合、VSP One SDS Block の再インストールまたは構成バックアップファイルからの構成リストアが必要になります。許容される障害数を超える障害の発生に備えて、他の媒体へのユーザーデータのバックアップ、VSP One SDS Block の構成バックアップファイルを取得しておくことを強くお勧めします。VSP One SDS Block の再インストールや構成バックアップファイルからの構成リストアによってユーザーデータはリストアされません。

HPEC 4D+1P (4 データ+1 パリティ)

容量効率、性能を重視する場合に適した方式です。

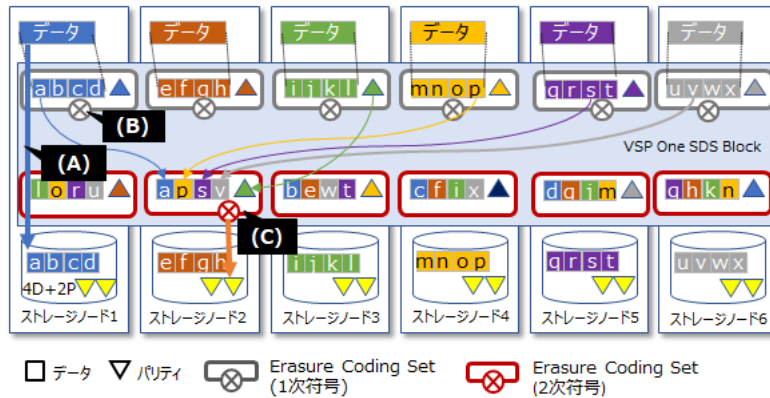
- 異なる 5 つ以上のストレージノードに、ユーザーデータとユーザーデータのパリティを格納して冗長化します。
- ストレージノードは最低 5 台必要です。
- ユーザーが利用可能な容量は、最大で物理容量の 60～75%です。
ただし、リビルド領域ポリシー(rebuildCapacityPolicy)を"Fixed"(デフォルト値)に設定している場合は、各ストレージノードの物理容量からリビルド領域の容量を除いた容量の 60～75%になります。リビルド領域については「ストレージプールのリビルド領域について」を参照してください。
- リード性能は HPEC 4D+2P と同等ですが、ライト性能は HPEC 4D+2P より優れています。
- 許容される障害数は 1 です。
ここでいう障害数とは、障害が発生しているストレージノード数とドライブ数の合計値です。
ただし、以下の場合の障害数は 1 と数えます。
 - 障害が発生したストレージノード内でドライブの障害が発生している場合
 - 同一ストレージノード内で複数のドライブ障害が発生している場合



HPEC 4D+2P (4 データ+2 パリティ)

許容される障害数を重視する場合に適した方式です。

- 異なる 6 つ以上のストレージノードに、ユーザーデータとユーザーデータのパリティを格納して冗長化します。
- ストレージノードは最低 6 台必要です。
- ユーザーが利用可能な容量は、最大で物理容量の 50～65%です。
ただし、リビルド領域ポリシー(rebuildCapacityPolicy)を"Fixed"(デフォルト値)に設定している場合は、各ストレージノードの物理容量からリビルド領域の容量を除いた容量の 50～65%になります。リビルド領域については「ストレージプールのリビルド領域について」を参照してください。
- リード性能は HPEC 4D+1P と同等ですが、ライト性能は 4D+1P の 60%ほどになります。
- 許容される障害数は 2 です。
ここでいう障害数とは、障害が発生しているストレージノード数とドライブ数の合計値です。
ただし、以下の場合の障害数は 1 と数えます。
 - 障害が発生したストレージノード内でドライブの障害が発生している場合
 - 同一ストレージノード内で複数のドライブ障害が発生している場合



- (A) データをローカルに格納し、リード時のネットワーク通信を削減
- (B) 1次符号化：符号化することで2冗長化のためのデータ通信量を削減
- (C) 2次符号化：データ格納容量を削減し、EC(Erasure Coding)同等の容量効率とする

Mirroring Duplication (1 データ+1 コピーデータ)

性能を重視する場合に適した方式です。

- 異なる2つのストレージノードに、ユーザーデータとユーザーデータのコピーデータを格納して冗長化します。
- ストレージノードは最低3台必要です。
- ユーザーが利用可能な容量は、最大で物理容量の40～48%です。
ただし、リビルド領域ポリシー(rebuildCapacityPolicy)を"Fixed"(デフォルト値)に設定している場合は、各ストレージノードの物理容量からリビルド領域の容量を除いた容量の40～48%になります。リビルド領域については「ストレージプールのリビルド領域について」を参照してください。
- リード性能はHPEC 4D+1P、4D+2Pと同等ですが、ライト性能はHPEC 4D+1Pより優れています。また、ストレージノードやドライブの障害時性能についても、HPECと比較して優れています。
- 許容される障害数は1です。
ここでいう障害数とは、障害が発生しているストレージノード数とドライブ数の合計値です。ただし、以下の場合の障害数は1と数えます。
 - 障害が発生したストレージノード内でドライブの障害が発生している場合
 - 同一ストレージノード内で複数のドライブ障害が発生している場合
 また、障害数が2以上の場合でも、以下のいずれかのケースを除いて、障害は許容されます。
 - [条件1] 冗長化されたストレージコントローラーに属する両ストレージノードでストレージノードまたはドライブの障害が発生したケース
ストレージコントローラーについては、このマニュアルの「ストレージノードの容量管理とストレージコントローラー」を参照してください。

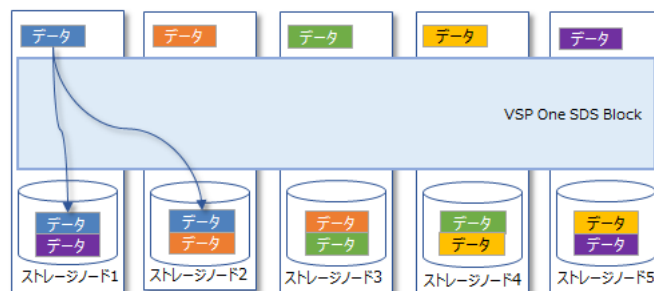


注意

下記の期間においては、[条件1]を満たさない場合でも障害が許容されない場合があります。

- ストレージノード増設後、ドライブデータ再配置が完了するまでの間
- ストレージノード減設中

- [条件 2] 2 つ以上のクラスターマスターノードで障害が発生したケース
クラスターマスターノードについては、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「クラスターマスターノードの冗長化」を参照してください。



1.1.2 ユーザーデータの保護方式<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

VSP One SDS Block では、ユーザーデータの保護方式として、HPEC(Hitachi Polyphase Erasure Coding)、Mirroring がサポートされます。HPEC は、ストレージノード間ネットワーク帯域が狭い SDS システム向けに開発した日立独自のデータ保護方式です。HPEC では、ユーザーデータはローカルドライブに格納します。Mirroring はユーザーデータのコピーを別のストレージノードに格納するデータ保護方式です。

HPEC 4D+2P または Mirroring Duplication を選択し、セットアップ作業時に設定します。

ユーザーデータの保護方式については、ストレージコントローラーの冗長度およびクラスターマスターノードの冗長度の設定との組み合わせに制限があります。詳細は、ご使用のクラウドプラットフォームに対応した「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「VSP One SDS Block がサポートする耐障害性に関する設定と各機能の説明」を参照してください。



メモ

HPEC 4D+2P、Mirroring Duplication の容量設計に関しては、このマニュアルの「容量設計(HPEC 4D+2P の場合)」または「容量設計(Mirroring の場合)」を参照してください。



注意

<<Cloud for AWS>>許容される障害数を超える障害が発生した場合、VSP One SDS Block の再インストールまたは構成バックアップファイルからの構成リストアが必要になります。許容される障害数を超える障害の発生に備えて、他の媒体へのユーザーデータのバックアップ、VSP One SDS Block の構成バックアップファイルを取得しておくことを強くお勧めします。VSP One SDS Block の再インストールや構成バックアップファイルからの構成リストアによってユーザーデータはリストアされません。

<<Cloud for Google Cloud>>許容される障害数を超える障害が発生した場合、VSP One SDS Block の再インストールが必要になります。VSP One SDS Block の再インストールによってユーザーデータはリストアされません。

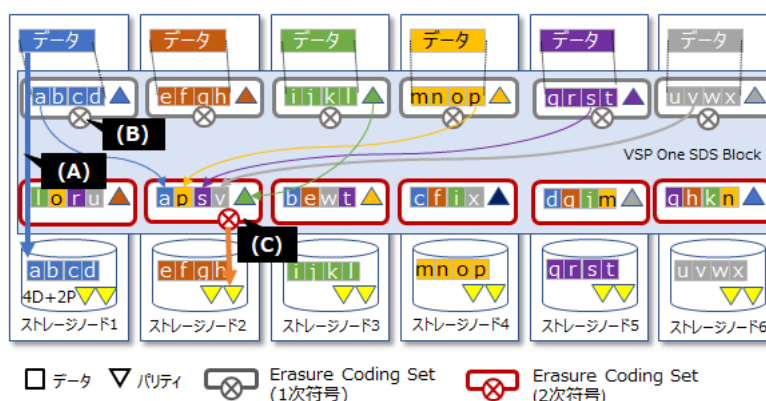
<<Cloud for Microsoft Azure>>許容される障害数を超える障害が発生した場合、VSP One SDS Block の再インストールが必要になります。VSP One SDS Block の再インストールによってユーザーデータはリストアされません。

HPEC 4D+2P (4 データ+2 パリティ)

許容される障害数を重視する場合に適した方式です。

- 異なる 6 つ以上のストレージノードに、ユーザーデータとユーザーデータのパリティを格納して冗長化します。
- ストレージノードは最低 6 台必要です。
- ユーザーが利用可能な容量は、最大で物理容量の 50～65%です。
ただし、リビルド領域ポリシー(rebuildCapacityPolicy)を"Fixed"(デフォルト値)に設定している場合は、各ストレージノードの物理容量からリビルド領域の容量を除いた容量の 50～65%になります。リビルド領域については「ストレージプールのリビルド領域について」を参照してください。
- リード性能は HPEC 4D+1P と同等ですが、ライト性能は 4D+1P の 60%ほどになります。
- 許容される障害数は 2 です。
ここでいう障害数とは、障害が発生しているストレージノード数とドライブ数の合計値です。ただし、以下の場合の障害数は 1 と数えます。

- 障害が発生したストレージノード内でドライブの障害が発生している場合
- 同一ストレージノード内で複数のドライブ障害が発生している場合



- (A)データをローカルに格納し、リード時のネットワーク通信を削減
- (B)1次符号化：符号化することで2冗長化のためのデータ通信量を削減
- (C)2次符号化：データ格納容量を削減し、EC(Erasure Coding)同等の容量効率とする

Mirroring Duplication (1 データ+1 コピーデータ)

性能を重視する場合に適した方式です。

- 異なる 2 つのストレージノードに、ユーザーデータとユーザーデータのコピーデータを格納して冗長化します。
- ストレージノードは最低 3 台必要です。
- ユーザーが利用可能な容量は、最大で物理容量の 40～48%です。
ただし、リビルド領域ポリシー(rebuildCapacityPolicy)を"Fixed"(デフォルト値)に設定している場合は、各ストレージノードの物理容量からリビルド領域の容量を除いた容量の 40～48%になります。リビルド領域については「ストレージプールのリビルド領域について」を参照してください。
- リード性能は 4D+2P と同等です。また、ストレージノードやドライブの障害時性能についても、4D+2P と比較して優れています。

- ・ 許容される障害数は1です。
ここでいう障害数とは、障害が発生しているストレージノード数とドライブ数の合計値です。
ただし、以下の場合の障害数は1と数えます。
 - ・ 障害が発生したストレージノード内でドライブの障害が発生している場合
 - ・ 同一ストレージノード内で複数のドライブ障害が発生している場合
 また、障害数が2以上の場合でも、以下のいずれかのケースを除いて、障害は許容されます。
 - [条件1] 冗長化されたストレージコントローラーに属する両ストレージノードでストレージノードまたはドライブの障害が発生したケース
ストレージコントローラーについては、このマニュアルの「ストレージノードの容量管理とストレージコントローラー」を参照してください。

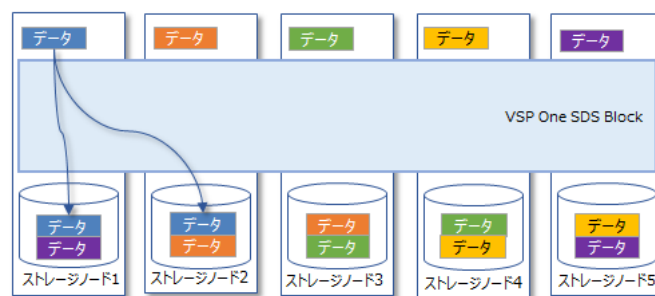


注意

下記の期間においては、[条件1]を満たさない場合でも障害が許容されない場合があります。

- ・ ストレージノード増設後、ドライブデータ再配置が完了するまでの間
- ・ ストレージノード減設中

- [条件2] 2つ以上のクラスターマスターノードで障害が発生したケース
クラスターマスターノードについては、ご使用のクラウドプラットフォームに対応した「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「クラスターマスターノードの冗長化」を参照してください。



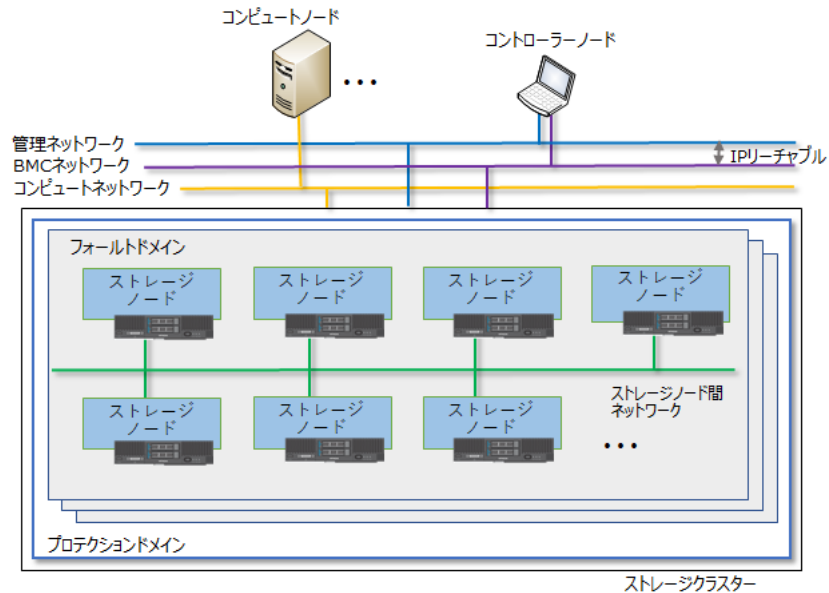
1.2 システムの構成《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

VSP One SDS Block によって構築されるシステムは、ストレージノードとコンピュータノードが分離している分離型の Software Defined Storage(SDS)です。

VSP One SDS Block のストレージシステムは、複数のストレージノードから構成されます。ストレージノードは複数のドライブから構成されます。

運用に当たっては、ストレージシステムにアクセスするアプリケーションが動作するコンピュータノードの登録とストレージシステムの管理操作を行うためのコントローラーノードなどの設置が必要です。



コントローラーノード、コンピュータノード、ストレージノード

- コントローラーノード
VSP One SDS Block への管理操作をするためのアクセス用ノードです。詳細は「コントローラーノードの設置と管理操作」を参照してください。
- コンピュータノード
ユーザーのアプリケーションが動作し、ストレージノードにユーザーデータの入出力を行うノードです。詳細は「コンピュータノードを設置する<<Bare metal>>」を参照してください。
- ストレージノード
VSP One SDS Block を構成する物理サーバーです。

ネットワーク

- 管理ネットワーク
コントローラーノードとストレージノード間のネットワークです。VSP One SDS Block に対する管理操作や、外部サービス(SNMP マネージャー、NTP など)と連携するための通信に利用します。ストレージノードの管理ポートと接続します。管理ポートの接続に非冗長化、冗長化のどちらかの構成を構築することができます。冗長化を構築する場合は、複数ポートを用いたストレージノードのチーミング機能を必須で有効にしてください。詳細な仕様は、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。
- コンピュータネットワーク
コンピュータノードとストレージノードの間のネットワークです。ユーザーデータが送受信されます。ストレージノードのコンピュータポートと接続します。このネットワークでは iSCSI、FC、または NVMe/TCP プロトコルを使用します。
- ストレージノード間ネットワーク
ストレージノード間のネットワークです。ストレージノード間のデータ保護、容量バランス時のユーザーデータのやりとり、ストレージノード間における管理情報の通信が行われます。ストレージノードのチーミング機能によって複数のポートを用いた冗長化構成とします。チーミング機能の詳細な仕様は、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

- **BMC ネットワーク**
ストレージノードの BMC とコントローラーノードを接続するネットワークです。BMC をコントローラーノードから操作するために使用されます。ストレージノードの BMC ポートと接続します。BMC ネットワークは管理ネットワークと通信可能である必要があります。

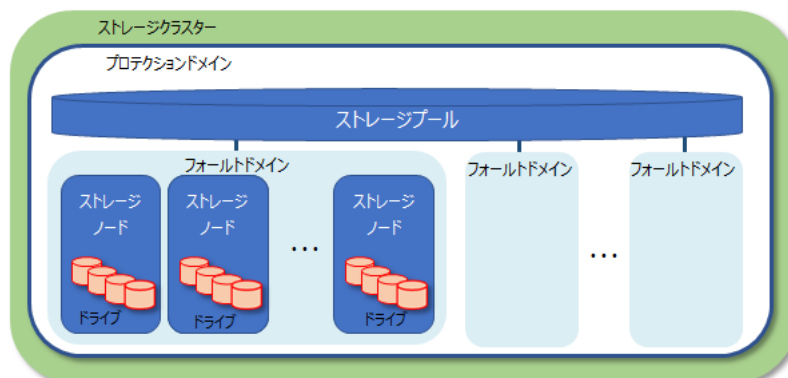
ストレージノードの役割

ストレージクラスター内のストレージノードは、役割によって以下のように呼びます。

- **クラスターマスターノード(プライマリー)**
ストレージクラスター全体を管理する役割を持つストレージノードです。
ストレージクラスターの代表 IP アドレスが割り当てられます。
 - ユーザーや管理アプリケーションと連携するためのインターフェイス機能を持ちます。
 - ストレージクラスター内のストレージノードを統括して制御します。ユーザーや管理アプリケーションはクラスターマスターノード(プライマリー)に対して操作するだけで各ストレージノードを制御できます。
- **クラスターマスターノード(セカンダリー)**
クラスターマスターノード(プライマリー)に障害が発生した場合にプライマリーになる役割を持つストレージノードです。
- **クラスターワーカーノード**
クラスターマスターノード(プライマリー)から制御されるストレージノードです。

プロテクションドメインとフォールトドメイン

プロテクションドメインは、データ保証形式と内部処理 I/O のリソース使用率を設定する単位です。プロテクションドメイン内にはストレージプールが 1 つ存在し、プロテクションドメインには 1 つ以上のフォールトドメインがあります。



フォールトドメインは、同じ電源系統やネットワークスイッチなどのハードウェアを共有するストレージノードのグループです。フォールトドメインを複数設定し、フォールトドメインごとに電源系統やネットワークスイッチなどのハードウェアを分離させることによって、あるフォールトドメイン内でハードウェア障害が発生した場合でも、別のフォールトドメインが正常であればストレージシステムの運用が続けられるようになります。

VSP One SDS Block は、フォールトドメインをまたがって冗長化されるよう、ユーザーデータ、ストレージコントローラーを自動配置します。ただし、クラスターマスターノードの配置は、フォールトドメインごとに 1 ノード(クラスターマスターノードが計 3 ノードの場合)または 1~2 ノード(クラスターマスターノードが計 5 ノードの場合)になるよう、導入時に手動で行う必要があります。詳しくは、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップ

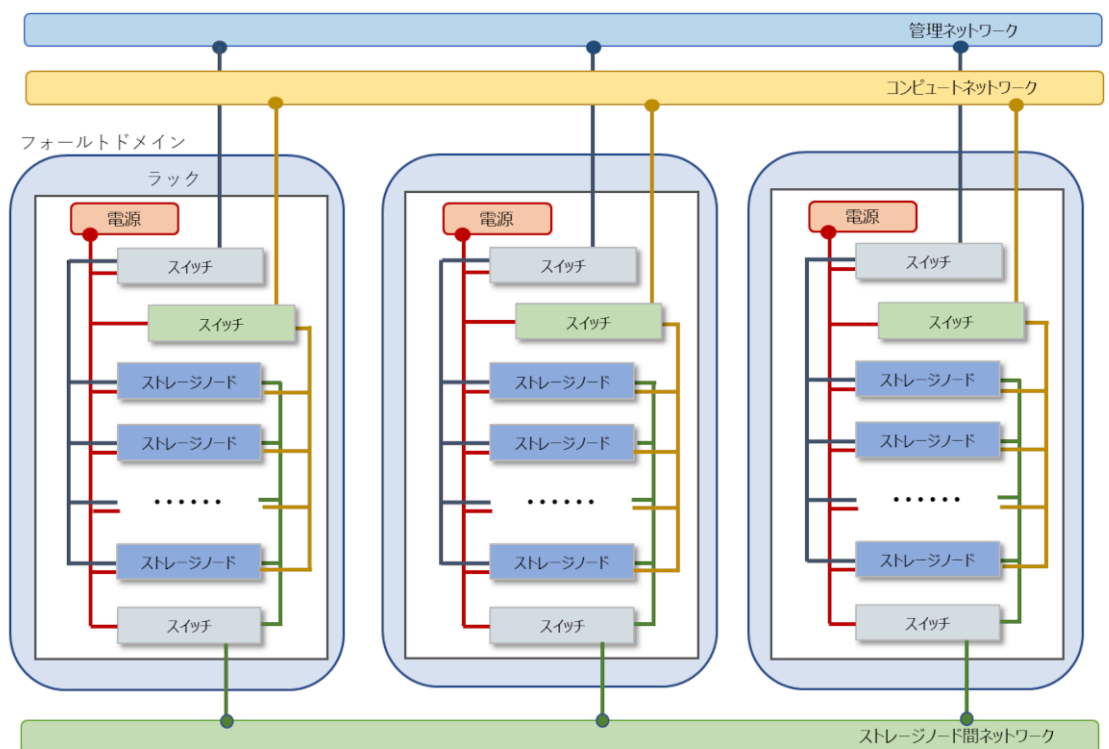
ップガイド」の「VSP One SDS Block がサポートする耐障害性に関する設定と各機能の説明」を参照してください。

ただし、複数フォールトドメイン構成の場合でも、他のフォールトドメインとの間で共有する電源系統やネットワークスイッチなどのハードウェアが1つでもあると、そのハードウェアに障害が発生した場合は、複数のフォールトドメインが同時障害となり、運用が停止するおそれがあります。

フォールトドメインごとに電源系統やネットワークスイッチなどのハードウェアが分離できない場合は、分離できていないハードウェアに障害が発生した場合に備えて、冗長構成をとっておく必要があります。

フォールトドメインは、VSP One SDS Block のセットアップ時に設定します。設定方法など詳しくは、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

以下の図に関し、BMC ネットワークについてもその他ネットワークと同様にハードウェアを分離させてください。



構成ファイル

VSP One SDS Block には次の構成ファイルがあります。構成ファイルの詳細については、「構成ファイルを管理する<<Bare metal>>」を参照してください。

構成ファイル	説明
SystemConfigurationFile.csv	VSP One SDS Block の自体の構成を記載するファイル(VSSB 構成ファイル)

このファイルは以下の場合に使用されます。

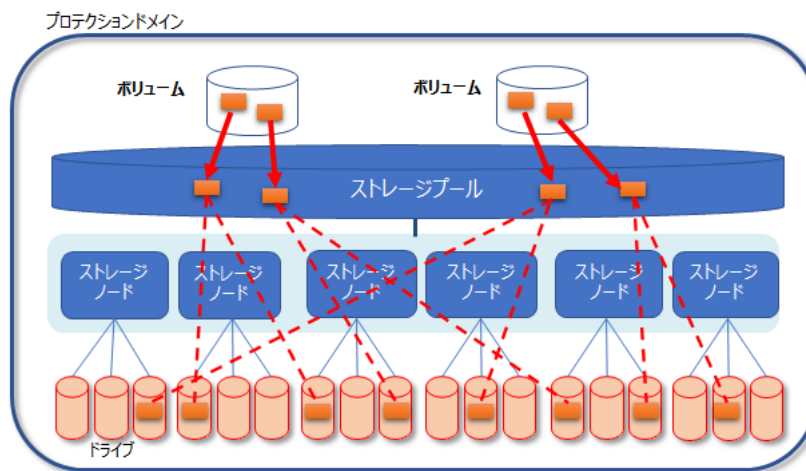
- ・ ストレージクラスター構築時

- ・ ストレージノード増設時
- ・ ストレージノード交換時
- ・ 構成情報の変更・設定時

ストレージプールとボリューム

複数のドライブをまとめた論理的なユーザーデータ格納領域をストレージプールといいます。ユーザーは、ストレージプールを対象にストレージ容量を管理すればよく、ドライブやその物理的な境界を意識せずに済みます。

ストレージプールは、既存のストレージノードにドライブを増設したり、別途ストレージノードを追加したりすることで拡張できます。



ボリュームは、ユーザーデータの読み書きが行われる論理デバイスです。ボリュームはストレージコントローラーによって管理され、ユーザーデータはボリュームに関連付けられたストレージプールに書き込まれます。

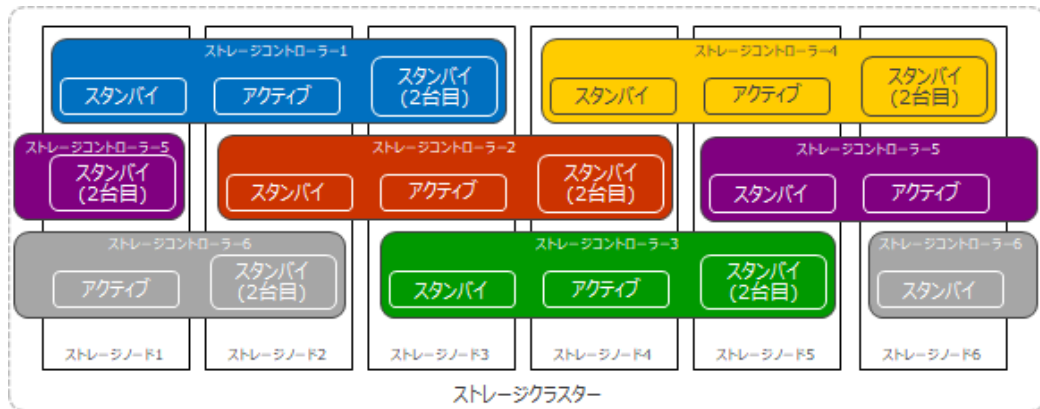
ストレージノードの容量管理とストレージコントローラー

ストレージコントローラーは、ストレージノードの容量やボリュームを管理する VSP One SDS Block の一部のプロセスです。

各ストレージノードの容量は、ストレージコントローラーによって管理されます。また、ストレージコントローラーは、システムの構成や使用状況を監視しています。

ストレージコントローラーが管理する容量をまとめたものが、ストレージプールの全体容量になります。

ストレージコントローラーは、ストレージノードと同数存在します。1つのストレージコントローラーは複数のストレージノードにまたがって配置されており、ストレージノード障害に耐えられるように冗長化されています(下図は3重化の例)。



ストレージコントローラーの冗長度としては、OneRedundantStorageNode(2 重化)とTwoRedundantStorageNodes(3 重化)の 2 つが存在し、ユーザーデータの保護方式の設定から自動的に決定されます。

詳しくは、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

また、ストレージコントローラーの管理については、このマニュアルの「ストレージコントローラーを管理する」を参照してください。

1.3 システムの構成《Cloud for AWS》

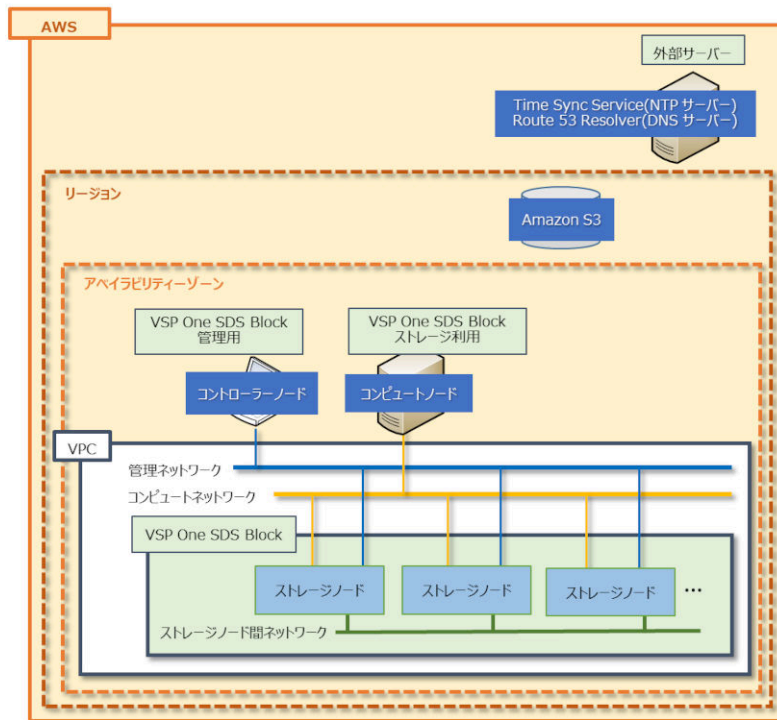
この項での記述内容は Cloud モデル for AWS に適用されます。

VSP One SDS Block によって構築されるシステムは、ストレージノードとコンピューターノードが分離している分離型の Software Defined Storage(SDS)です。

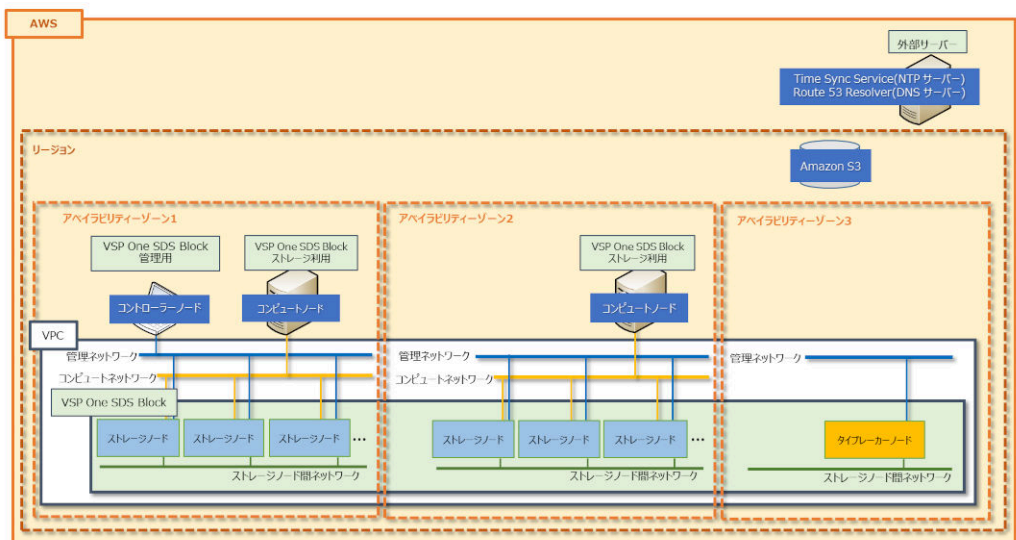
VSP One SDS Block のストレージシステムは、複数のストレージノードから構成されます。ストレージノードは複数のドライブから構成されます。

運用に当たっては、ストレージシステムにアクセスするアプリケーションが動作するコンピューターノードの登録とストレージシステムの管理操作を行うためのコントローラーノードなどの設置が必要です。

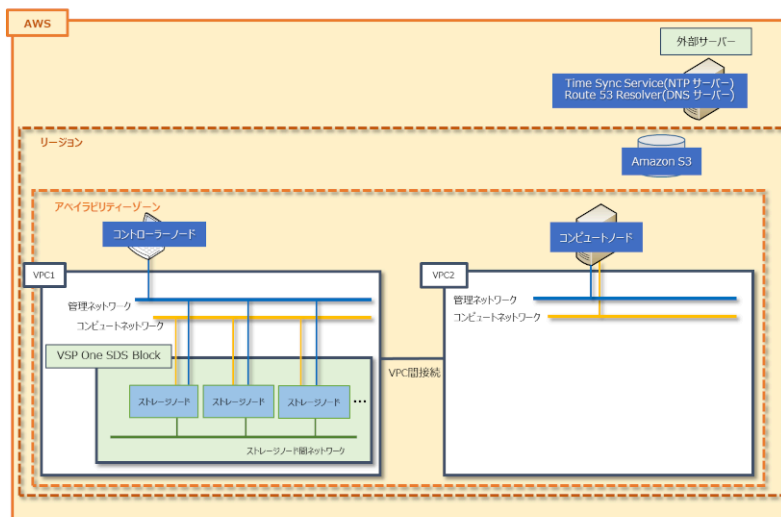
コンピュータノードをVSP One SDS Blockと同一のVPC に構築した場合(Single-AZ構成)



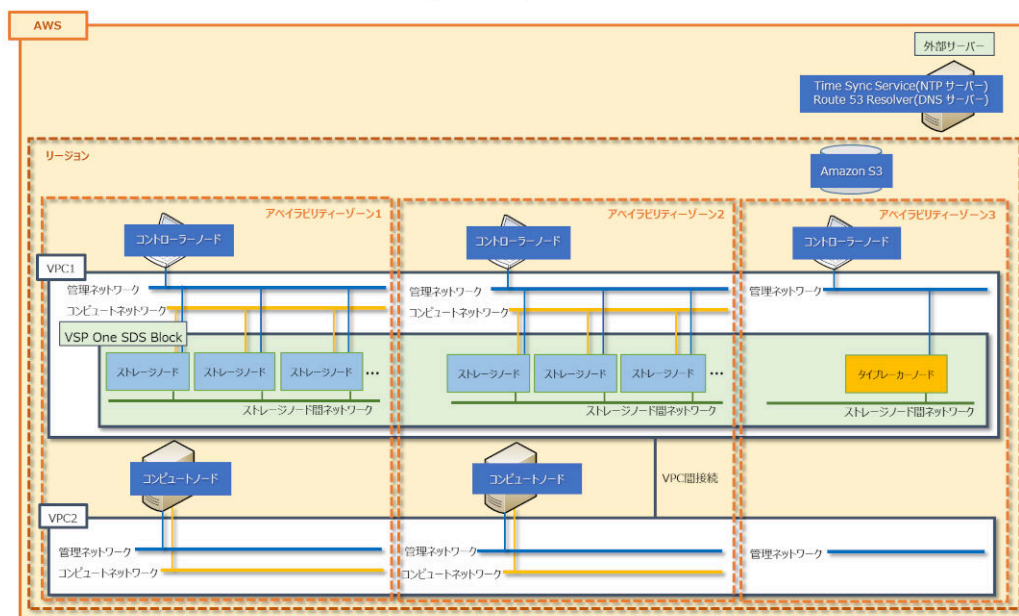
コンピュータノードをVSP One SDS Block と同一のVPCに構築した場合(Multi-AZ構成)



コンピュータノードをVSP One SDS Block とは別のVPC に構築した場合 (Single-AZ構成)



コンピュータノードをVSP One SDS Block とは別のVPC に構築した場合 (Multi-AZ構成)



メモ

コンピュータノードを VSP One SDS Block とは別のサブネットに設置する場合は「コンピュータノードを設置する「Cloud」」に記載のとおり、以下が必要になります。

- Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「コンピュータノードの設置に関する補足事項」に記載の手順を実施すること
- コンピュータノードのコンピュータネットワーク用サブネットヘルート(経路)を追加すること

コントローラーノード、コンピュータノード、ストレージノード

- コントローラーノード
VSP One SDS Block への管理操作をするためのアクセス用ノードです。詳細は「コントローラーノードの設置と管理操作」を参照してください。
- コンピュータノード

ユーザーのアプリケーションが動作し、ストレージノードにユーザーデータの入出力を行うノードです。詳細は「コンピュータノードを設置する<<Cloud>>」を参照してください。

- ストレージノード

VSP One SDS Block を構成する仮想サーバー(EC2 インスタンス)です。

- タイブレーカーノード

Multi-AZ 構成において、クラスターマスターノードの役割のみを持つストレージノードです。ストレージコントローラーは配置されません。また、コンピュータポートもドライブも持ちません。

ネットワーク

- 管理ネットワーク

コントローラーノードとストレージノード間のネットワークです。VSP One SDS Block に対する管理操作や、外部サービス(SNMP マネージャーなど)と連携するための通信に利用します。ストレージノードの管理ポートと接続します。

- コンピュータネットワーク

コンピュータノードとストレージノードの間のネットワークです。ユーザーデータが送受信されます。ストレージノードのコンピュータポートと接続します。このネットワークでは iSCSI プロトコルを使用します。

- ストレージノード間ネットワーク

ストレージノード間のネットワークです。ストレージノード間のデータ保護、容量バランス時のユーザーデータのやりとり、ストレージノード間における管理情報の通信が行われます。ストレージノードのストレージノード間ポートと接続します。

ストレージノードの役割

ストレージクラスター内のストレージノードは、役割によって以下のように呼びます。

- クラスターマスターノード(プライマリー)

ストレージクラスター全体を管理する役割を持つストレージノードです。

- ユーザーや管理アプリケーションと連携するためのインターフェイス機能を持ちます。

- ストレージクラスター内のストレージノードを統括して制御します。ユーザーや管理アプリケーションはクラスターマスターノード(プライマリー)に対して操作するだけで各ストレージノードを制御できます。

- クラスターマスターノード(セカンダリー)

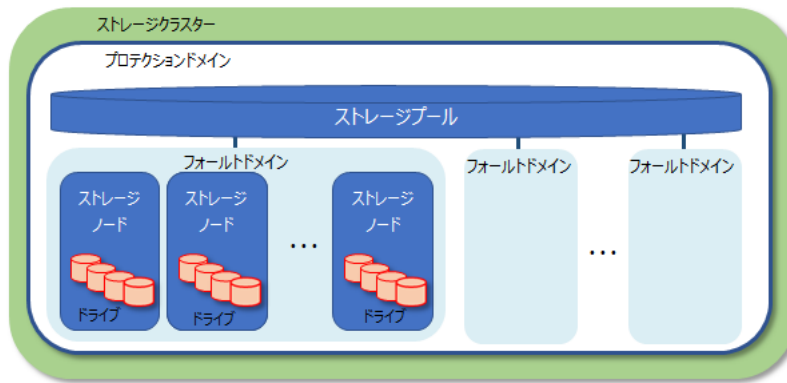
クラスターマスターノード(プライマリー)に障害が発生した場合にプライマリーになる役割を持つストレージノードです。

- クラスターワーカーノード

クラスターマスターノード(プライマリー)から制御されるストレージノードです。

プロテクションドメインとフォールトドメイン

プロテクションドメインは、データ保証形式と内部処理 I/O のリソース使用率を設定する単位です。プロテクションドメイン内にはストレージプールが 1 つ存在し、プロテクションドメインには 1 つ以上のフォールトドメインがあります。



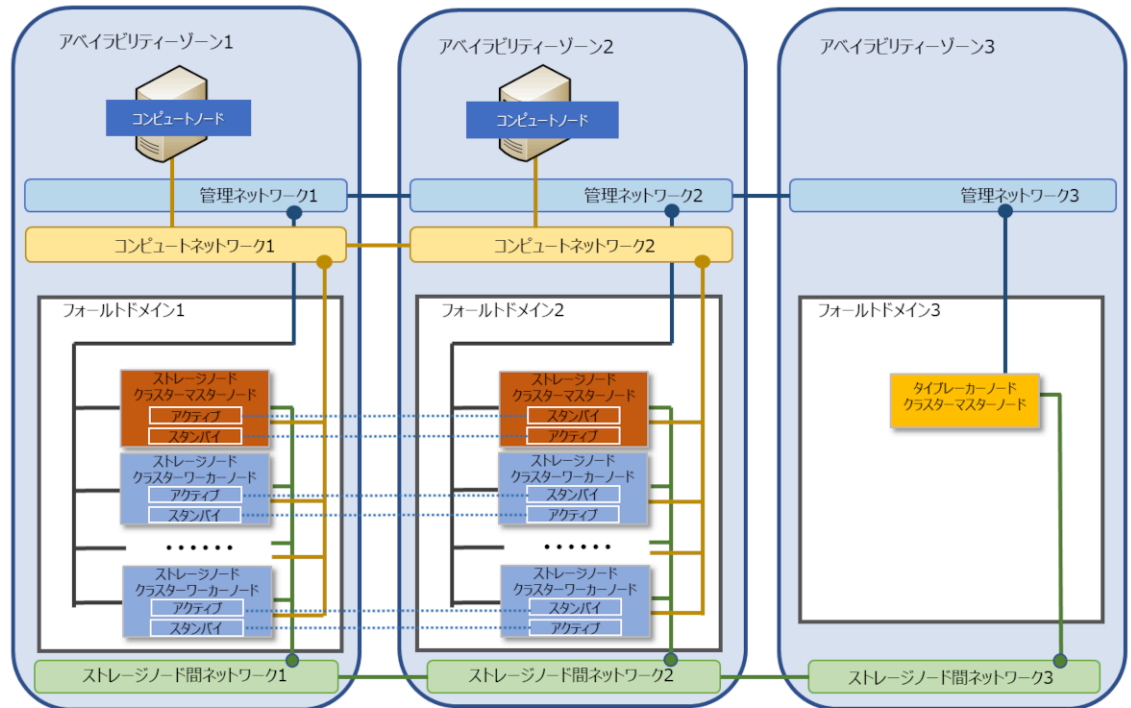
フォールトドメインは、単一のアベイラビリティゾーンに設置されているストレージノードのグループです。Single-AZ 構成の場合、クラスターを構築するストレージノードは、単一のアベイラビリティゾーンにのみ設置可能であるため、フォールトドメイン数は 1 となります。Multi-AZ 構成の場合、1 つのフォールトドメイン内のストレージノードがまとまって異常になっても、別のフォールトドメインが正常であればストレージの運用を継続できます。

VSP One SDS Block は、フォールトドメインをまたがって冗長化されるよう、ユーザーデータ、ストレージコントローラーを自動配置します。ただし、クラスターマスターノードの配置は、フォールトドメインごとに 1 ノード(クラスターマスターノードが計 3 ノードの場合)または 1~2 ノード(クラスターマスターノードが計 5 ノードの場合)になるよう、導入時に手動で行う必要があります。詳しくは、Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「VSP One SDS Block がサポートする耐障害性に関する設定と各機能の説明」を参照してください。

ただし、複数フォールトドメイン構成の場合でも、他のフォールトドメインとの間で共有する電源系統やネットワークスイッチなどのハードウェアが 1 つでもあると、そのハードウェアに障害が発生した場合は、複数のフォールトドメインが同時障害となり、運用が停止するおそれがあります。

フォールトドメインごとに電源系統やネットワークスイッチなどのハードウェアが分離できない場合は、分離できていないハードウェアに障害が発生した場合に備えて、冗長構成をとっておく必要があります。

フォールトドメインは、VSP One SDS Block のセットアップ時に設定します。設定方法など詳しくは、Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。



構成ファイル

VSP One SDS Block には次の構成ファイルがあります。構成ファイルの詳細については、「構成ファイルを管理する<<Cloud>>」を参照してください。

構成ファイル	説明
SystemConfigurationFile.csv ¹	VSP One SDS Block の自体の構成を記載するファイル
VMConfigurationFile.yml ²	VSP One SDS Block のストレージノードに構築する仮想マシンの構成を定義するファイル
VMConfigurationFile_Duplication.yml ²	ユーザーデータの保護方式が Mirroring Duplication の場合に必要となるファイル
VMConfigurationFile_4D2P.yml ²	Single-AZ 構成、かつユーザーデータの保護方式が HPEC 4D+2P の場合に必要となるファイル
VMConfigurationFile_node01.yml ²	Single-AZ 構成の場合に必要な VSP One SDS Block のストレージノードに構築する仮想マシンの構成を定義するファイル
VMConfigurationFile_nodeNN.yml ²	VSP One SDS Block のストレージノードに構築する仮想マシンの構成を定義するファイル
NetworkResourceConfigurationFile_Duplication.yml ²	ユーザーデータの保護方式が Mirroring Duplication の場合に必要となるファイル
NetworkResourceConfigurationFile_4D2P.yml ²	Single-AZ 構成、かつユーザーデータの保護方式が HPEC 4D+2P の場合に必要となるファイル
IamResourceConfigurationFile.yml ²	VSP One SDS Block のストレージノードに構築する仮想マシンの構成を定義するファイル
VMConfigurationFile_nodeTB.yml ²	Multi-AZ 構成の場合に必要なファイル
1. VSSB 構成ファイル	

構成ファイル	説明
2. VM 構成ファイル	

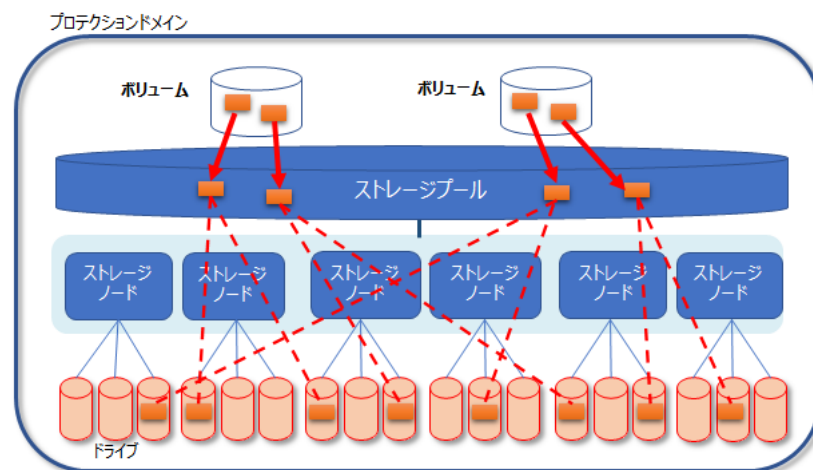
これらのファイルは、VSP One SDS Block の構成を定義するファイルであり、以下の場合に使用されます。

- ・ ドライブ増設時
- ・ ドライブ交換時
- ・ ストレージノード増設時
- ・ ストレージノード交換時
- ・ ソフトウェアアップデート時

ストレージプールとボリューム

複数のドライブをまとめた論理的なユーザーデータ格納領域をストレージプールといいます。ユーザーは、ストレージプールを対象にストレージ容量を管理すればよく、ドライブやその物理的な境界を意識せずに済みます。

ストレージプールは、既存のストレージノードにドライブを増設したり、別途ストレージノードを追加したりすることで拡張できます。



ボリュームは、ユーザーデータの読み書きが行われる論理デバイスです。ボリュームはストレージコントローラーによって管理され、ユーザーデータはボリュームに関連付けられたストレージプールに書き込まれます。

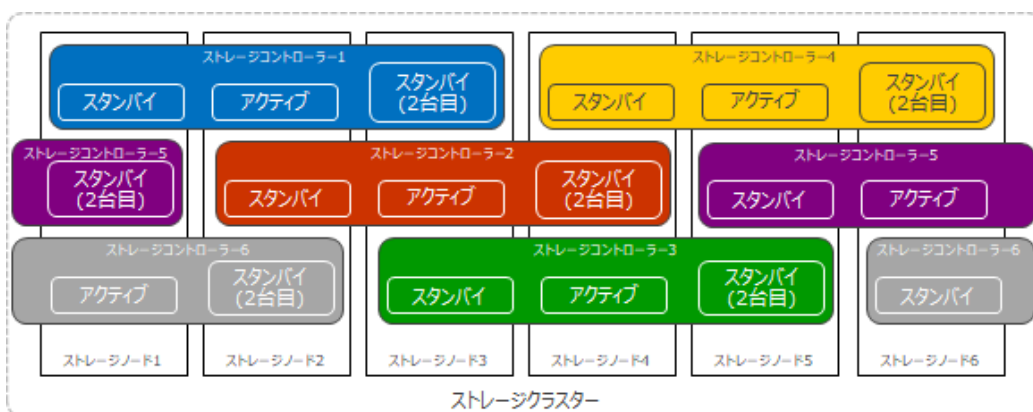
ストレージノードの容量管理とストレージコントローラー

ストレージコントローラーは、ストレージノードの容量やボリュームを管理する VSP One SDS Block の一部のプロセスです。

各ストレージノードの容量は、ストレージコントローラーによって管理されます。また、ストレージコントローラーは、システムの構成や使用状況を監視しています。

ストレージコントローラーが管理する容量をまとめたものが、ストレージプールの全体容量になります。

ストレージコントローラーは、ストレージノードと同数存在します。1つのストレージコントローラーは複数のストレージノードにまたがって配置されており、ストレージノード障害に耐えられるように冗長化されています(下図は3重化の例)。



ストレージコントローラーの冗長度としては、OneRedundantStorageNode(2重化)とTwoRedundantStorageNodes(3重化)の2つが存在し、ユーザーデータの保護方式の設定から自動的に決定されます。

詳しくは、Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

また、ストレージコントローラーの管理については、このマニュアルの「ストレージコントローラーを管理する」を参照してください。

1.4 システムの構成<<Cloud for Google Cloud>>

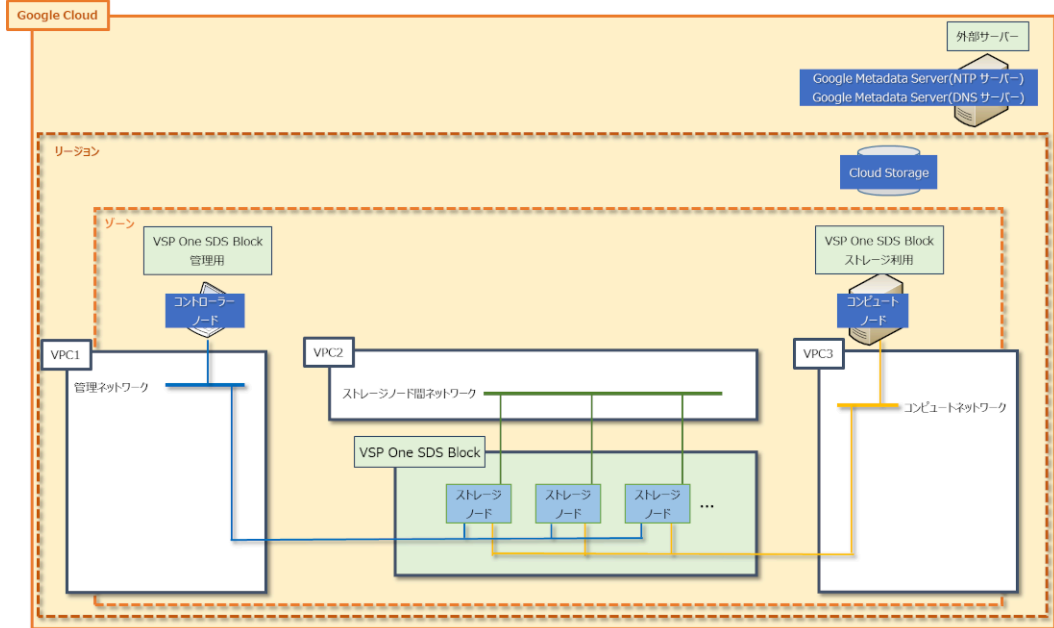
この項での記述内容は Cloud モデル for Google Cloud に適用されます。

VSP One SDS Block によって構築されるシステムは、ストレージノードとコンピューターノードが分離している分離型の Software Defined Storage(SDS)です。

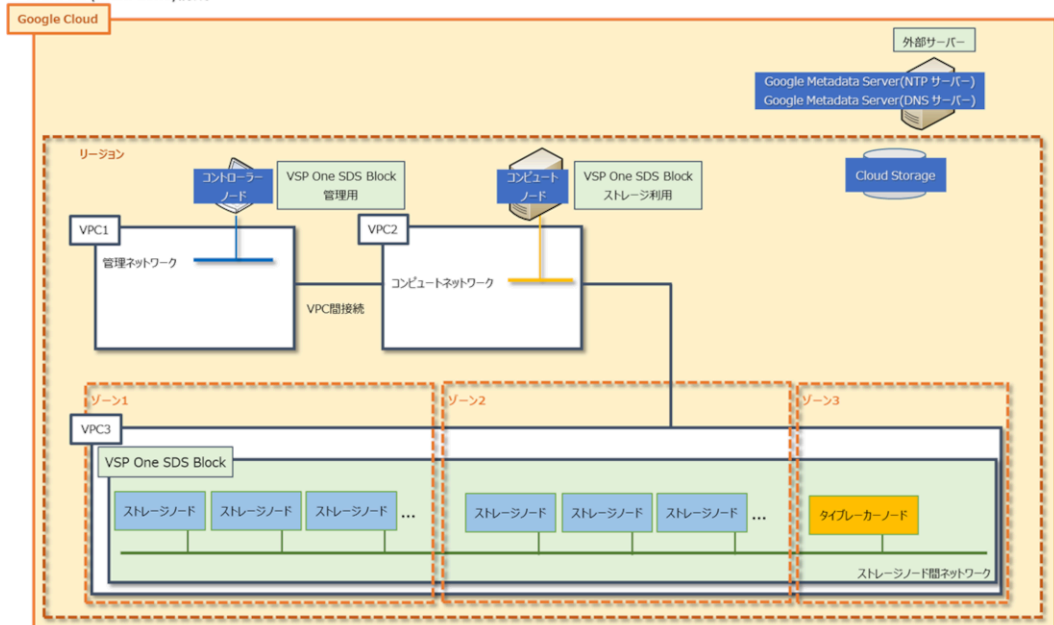
VSP One SDS Block のストレージシステムは、複数のストレージノードから構成されます。ストレージノードは複数のドライブから構成されます。

運用に当たっては、ストレージシステムにアクセスするアプリケーションが動作するコンピューターノードの登録とストレージシステムの管理操作を行うためのコントローラーノードなどの設置が必要です。

<Single-AZ (Single-Zone)構成>



<Multi-AZ (Multi-Zone)構成>



メモ

コンピュータノードを VSP One SDS Block とは別のサブネットに設置する場合は「コンピュータノードを設置する《Cloud for Google Cloud》」に記載のとおり、以下が必要になります。

- Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「サブネットを作成する」に記載の手順を実施すること
- コンピュータノードのコンピュータネットワーク用サブネットヘルート(経路)を追加すること

コントローラーノード、コンピュータノード、ストレージノード

- コントローラーノード

VSP One SDS Block への管理操作をするためのアクセス用ノードです。詳細は「コントローラーノードの設置と管理操作」を参照してください。

- コンピュータノード

ユーザーのアプリケーションが動作し、ストレージノードにユーザーデータの入出力を行うノードです。詳細は「コンピュータノードを設置する<<Cloud>>」を参照してください。

- ストレージノード

VSP One SDS Block を構成する仮想サーバー(Compute Engine インスタンス)です。

- タイブレーカーノード

Multi-AZ (Multi-Zone)構成において、クラスターマスターノードの役割のみを持つストレージノードです。ストレージコントローラーは配置されません。また、コンピュータポートもドライブも持ちません。

ネットワーク

- 管理ネットワーク

コントローラーノードとストレージノード間のネットワークです。VSP One SDS Block に対する管理操作や、外部サービス(SNMP マネージャーなど)と連携するための通信に利用します。ストレージノードの管理ポートと接続します。

- コンピュータネットワーク

コンピュータノードとストレージノードの間のネットワークです。ユーザーデータが送受信されます。ストレージノードのコンピュータポートと接続します。このネットワークでは iSCSI プロトコルを使用します。

- ストレージノード間ネットワーク

ストレージノード間のネットワークです。ストレージノード間のデータ保護、容量バランス時のユーザーデータのやりとり、ストレージノード間における管理情報の通信が行われます。ストレージノードのストレージノード間ポートと接続します。

ストレージノードの役割

ストレージクラスター内のストレージノードは、役割によって以下のように呼びます。

- クラスターマスターノード(プライマリー)

ストレージクラスター全体を管理する役割を持つストレージノードです。

- ユーザーや管理アプリケーションと連携するためのインターフェイス機能を持ちます。

- ストレージクラスター内のストレージノードを統括して制御します。ユーザーや管理アプリケーションはクラスターマスターノード(プライマリー)に対して操作するだけで各ストレージノードを制御できます。

- クラスターマスターノード(セカンダリー)

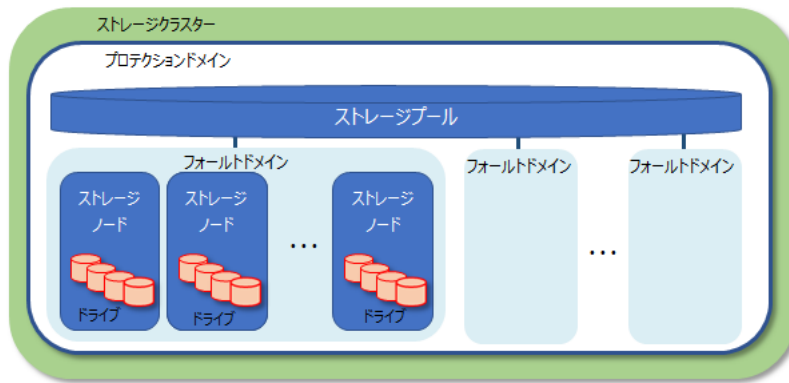
クラスターマスターノード(プライマリー)に障害が発生した場合にプライマリーになる役割を持つストレージノードです。

- クラスターワーカーノード

クラスターマスターノード(プライマリー)から制御されるストレージノードです。

プロテクションドメインとフォールトドメイン

プロテクションドメインは、データ保証形式と内部処理 I/O のリソース使用率を設定する単位です。プロテクションドメイン内にはストレージプールが 1 つ存在し、プロテクションドメインには 1 つ以上のフォールトドメインがあります。



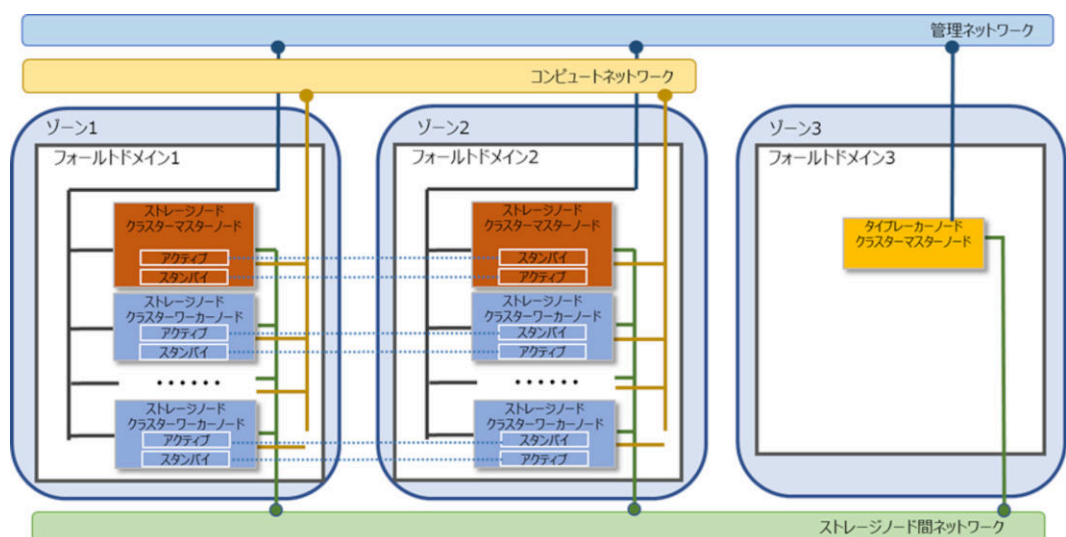
フォールトドメインは、単一のアベイラビリティゾーンに設置されているストレージノードのグループです。Single-AZ (Single-Zone)構成の場合、クラスターを構築するストレージノードは、単一のゾーンにのみ設置可能であるため、フォールトドメイン数は1となります。Multi-AZ (Multi-Zone)構成の場合、1つのフォールトドメイン内のストレージノードがまとまって異常になっても、別のフォールトドメインが正常であればストレージの運用を継続できます。

VSP One SDS Block は、フォールトドメインをまたがって冗長化されるよう、ユーザーデータ、ストレージコントローラーを自動配置します。ただし、クラスターマスターノードの配置は、フォールトドメインごとに1ノード(クラスターマスターノードが計3ノードの場合)または1~2ノード(クラスターマスターノードが計5ノードの場合)になるよう、導入時に手動で行う必要があります。詳しくは、Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「VSP One SDS Block がサポートする耐障害性に関する設定と各機能の説明」を参照してください。

ただし、複数フォールトドメイン構成の場合でも、他のフォールトドメインとの間で共有する電源系統やネットワークスイッチなどのハードウェアが1つでもあると、そのハードウェアに障害が発生した場合は、複数のフォールトドメインが同時障害となり、運用が停止するおそれがあります。

フォールトドメインごとに電源系統やネットワークスイッチなどのハードウェアが分離できない場合は、分離できていないハードウェアに障害が発生した場合に備えて、冗長構成をとっておく必要があります。

フォールトドメインは、VSP One SDS Block のセットアップ時に設定します。設定方法など詳しくは、Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。



構成ファイル

VSP One SDS Block には次の構成ファイルがあります。構成ファイルの詳細については、「構成ファイルを管理する <<Cloud for Google Cloud>>」を参照してください。

構成ファイル	説明
SystemConfigurationFile.csv ¹	VSP One SDS Block の自体の構成を記載するファイル
main.tf ²	ストレージクラスターデプロイ用テンプレートファイル
variable.tf ²	ストレージクラスターデプロイ用変数定義ファイル
backend.auto.tfvars ²	バックエンド指定ファイル
terraform.tfvars ²	ストレージクラスターの構成に関わる変数定義ファイル
1. VSSB 構成ファイル 2. VM 構成ファイル	

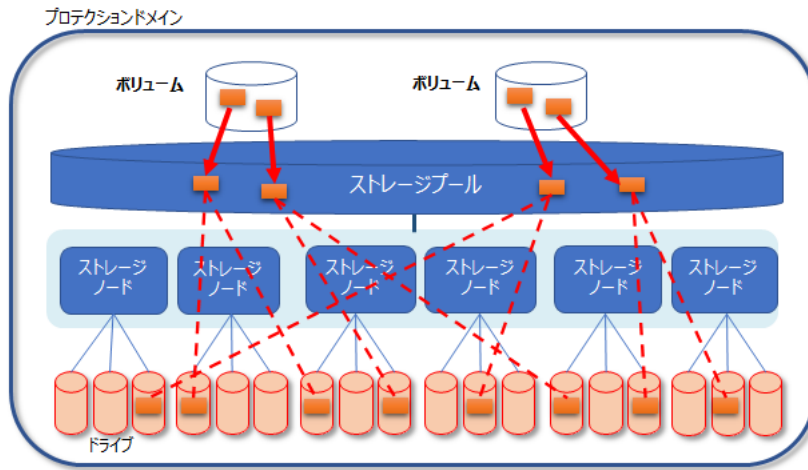
これらのファイルは、VSP One SDS Block の構成を定義するファイルであり、以下の場合に使用されます。

- ・ ストレージクラスター構築時
- ・ ドライブ増設時
- ・ ドライブ交換時
- ・ ドライブ減設時
- ・ ストレージノード増設時
- ・ ストレージノード交換時
- ・ ソフトウェアアップデート時

ストレージプールとボリューム

複数のドライブをまとめた論理的なユーザーデータ格納領域をストレージプールといいます。ユーザーは、ストレージプールを対象にストレージ容量を管理すればよく、ドライブやその物理的な境界を意識せずに済みます。

ストレージプールは、既存のストレージノードにドライブを増設したり、別途ストレージノードを追加したりすることで拡張できます。



ボリュームは、ユーザーデータの読み書きが行われる論理デバイスです。ボリュームはストレージコントローラーによって管理され、ユーザーデータはボリュームに関連付けられたストレージプールに書き込まれます。

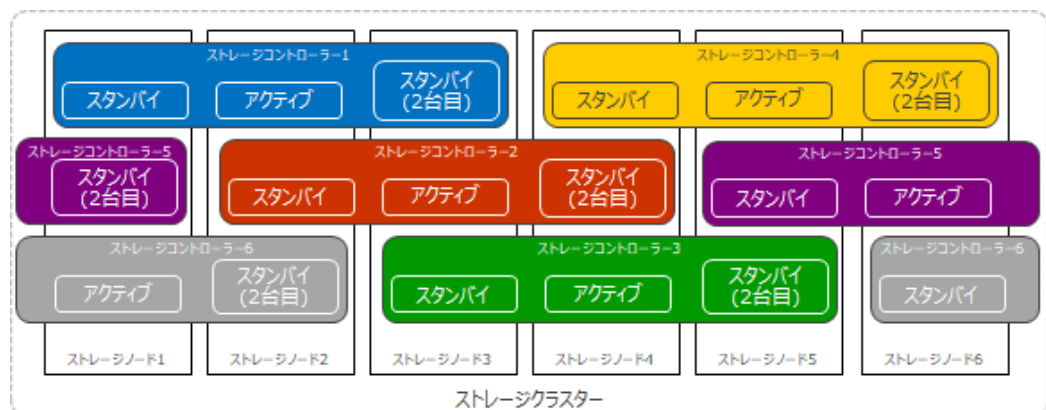
ストレージノードの容量管理とストレージコントローラー

ストレージコントローラーは、ストレージノードの容量やボリュームを管理する VSP One SDS Block の一部のプロセスです。

各ストレージノードの容量は、ストレージコントローラーによって管理されます。また、ストレージコントローラーは、システムの構成や使用状況を監視しています。

ストレージコントローラーが管理する容量をまとめたものが、ストレージプールの全体容量になります。

ストレージコントローラーは、ストレージノードと同数存在します。1つのストレージコントローラーは複数のストレージノードにまたがって配置されており、ストレージノード障害に耐えられるように冗長化されています(下図は3重化の例)。



ストレージコントローラーの冗長度としては、OneRedundantStorageNode(2重化)とTwoRedundantStorageNodes(3重化)の2つが存在し、ユーザーデータの保護方式の設定から自動的に決定されます。

詳しくは、Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

また、ストレージコントローラーの管理については、このマニュアルの「ストレージコントローラーを管理する」を参照してください。

1.5 システムの構成《Cloud for Microsoft Azure》

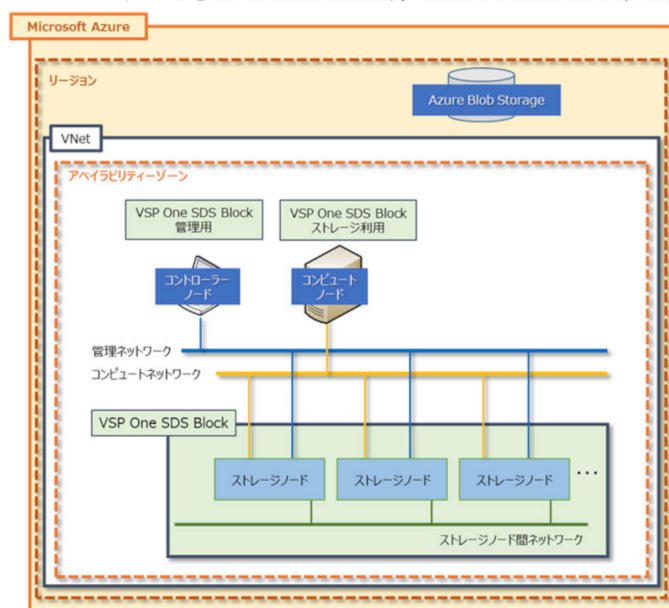
この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

VSP One SDS Block によって構築されるシステムは、ストレージノードとコンピューターノードが分離している分離型の Software Defined Storage(SDS)です。

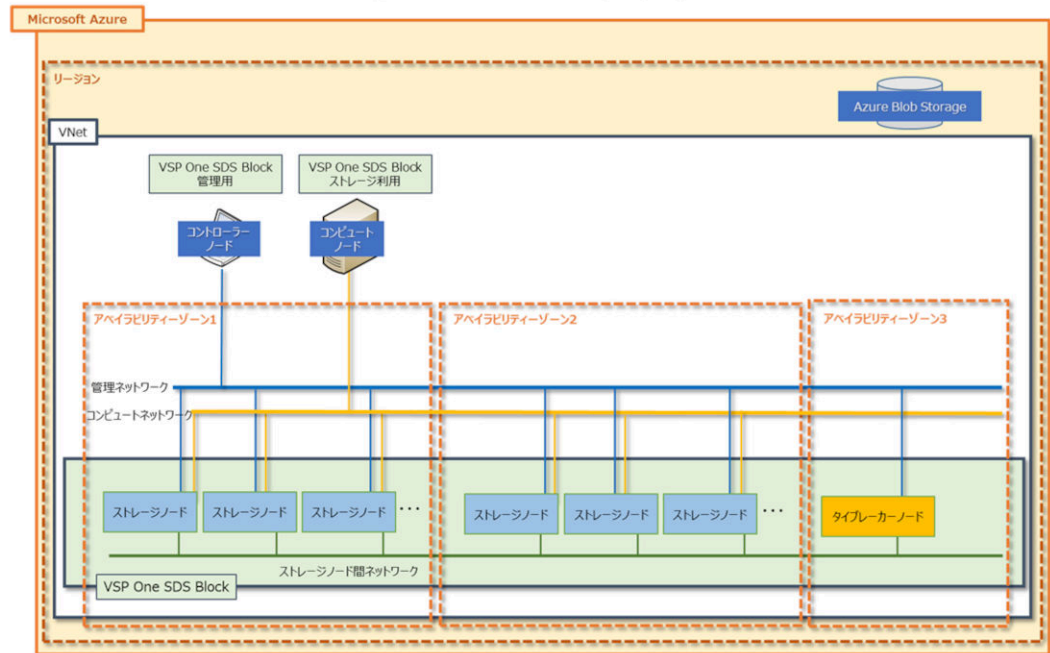
VSP One SDS Block のストレージシステムは、複数のストレージノードから構成されます。ストレージノードは複数のドライブから構成されます。

運用に当たっては、ストレージシステムにアクセスするアプリケーションが動作するコンピューターノードの登録とストレージシステムの管理操作を行うためのコントローラーノードなどの設置が必要です。

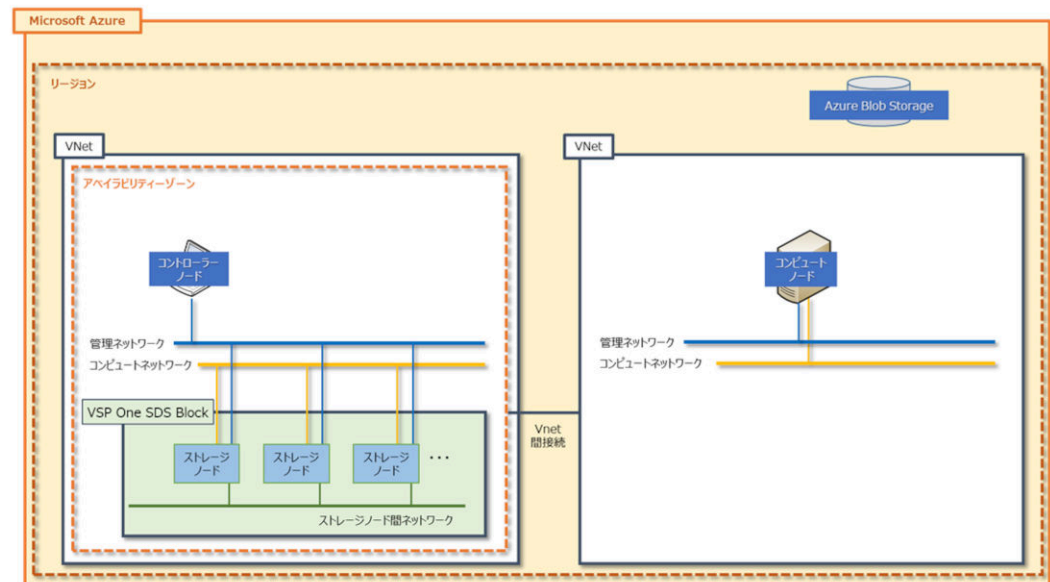
<コンピューターノードをVSP One SDS Block と同一のAzure Virtual Network(VNet)に構築する場合>



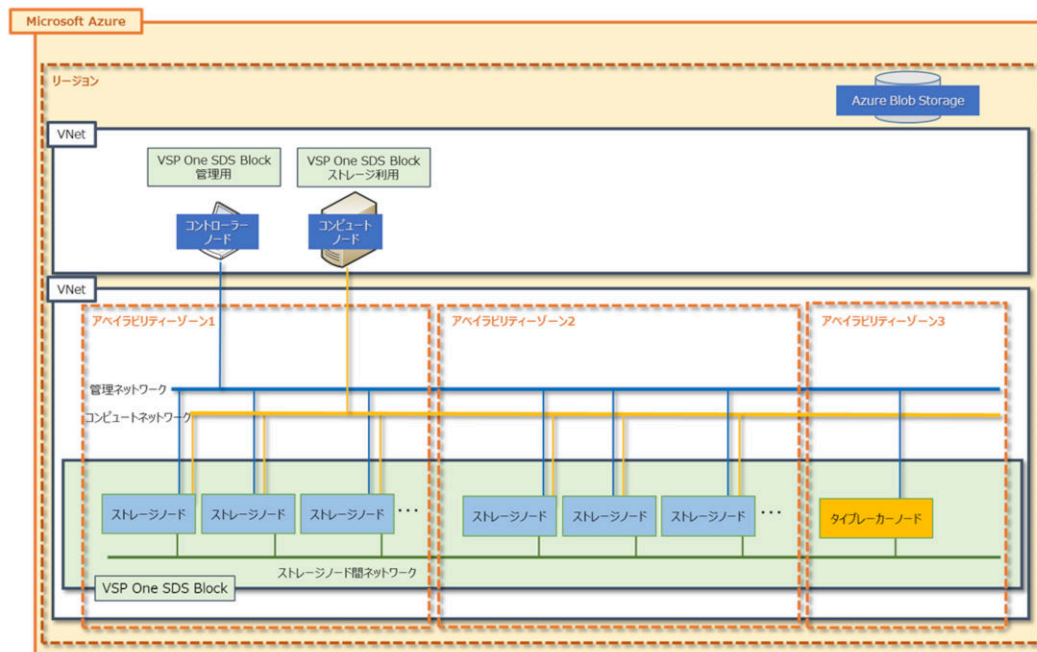
<コンピュートノードをVSP One SDS Blockと同一のAzure Virtual Network(VNet)に構築する場合>



<コンピュートノードをVSP One SDS Blockとは別のAzure Virtual Network(VNet)に構築する場合>



<コンピュートノードをVSP One SDS Blockとは別のAzure Virtual Network(VNet)に構築する場合>



メモ

- 以下の場合には、ネットワークセキュリティグループの設定のため、ストレージクラスター構築時にパラメーターの指定が必要になります。
 - コントローラーノードを VSP One SDS Block とは別の仮想ネットワークに設置する場合
 - コンピュートノードを VSP One SDS Block のコンピュートネットワーク用サブネットとは別のサブネットに設置する場合

詳細は Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージクラスターを構築する」を参照してください。

ストレージクラスター構築後にネットワークセキュリティグループの設定変更が必要になった場合は、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージクラスターの設定値を変更する」を参照してください。

- VSP One SDS Block とは別のサブネットにコントローラーノード、コンピュートノードを設置する場合は、必要に応じてサブネットにルートテーブルを設定してください。

コントローラーノード、コンピュートノード、ストレージノード

- コントローラーノード
VSP One SDS Block への管理操作をするためのアクセス用ノードです。詳細は「コントローラーノードの設置と管理操作」を参照してください。
- コンピュートノード
ユーザーのアプリケーションが動作し、ストレージノードにユーザーデータの入出力を行うノードです。詳細は「コンピュートノードを設置する<<Cloud>>」を参照してください。
- ストレージノード
VSP One SDS Block を構成する仮想サーバー(Azure VM インスタンス)です。
 - タイブレーカーノード
Multi-AZ 構成において、クラスターマスターノードの役割のみを持つストレージノードです。ストレージコントローラーは配置されません。また、コンピュートポートもドライブも持ちません。

ネットワーク

- 管理ネットワーク
コントローラーノードとストレージノード間のネットワークです。VSP One SDS Block に対する管理操作や、外部サービス(SNMP マネージャーなど)と連携するための通信に利用します。ストレージノードの管理ポートと接続します。
- コンピュートネットワーク
コンピューターノードとストレージノードの間のネットワークです。ユーザーデータが送受信されます。ストレージノードのコンピューターポートと接続します。このネットワークでは iSCSI プロトコルを使用します。
- ストレージノード間ネットワーク
ストレージノード間のネットワークです。ストレージノード間のデータ保護、容量バランス時のユーザーデータのやりとり、ストレージノード間における管理情報の通信が行われます。ストレージノードのストレージノード間ポートと接続します。

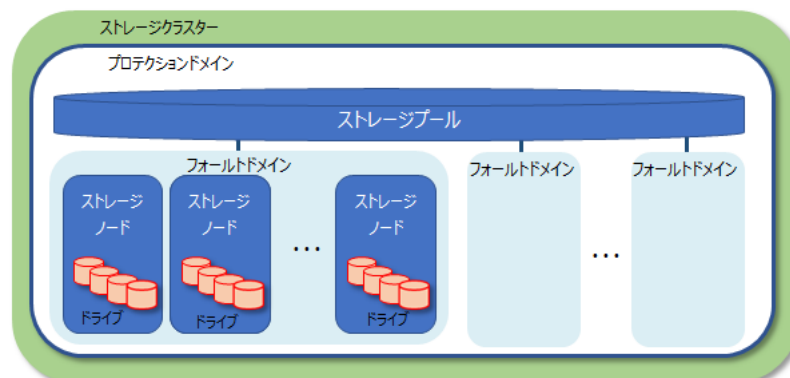
ストレージノードの役割

ストレージクラスター内のストレージノードは、役割によって以下のように呼びます。

- クラスターマスターノード(プライマリー)
ストレージクラスター全体を管理する役割を持つストレージノードです。
 - ユーザーや管理アプリケーションと連携するためのインターフェイス機能を持ちます。
 - ストレージクラスター内のストレージノードを統括して制御します。ユーザーや管理アプリケーションはクラスターマスターノード(プライマリー)に対して操作するだけで各ストレージノードを制御できます。
- クラスターマスターノード(セカンダリー)
クラスターマスターノード(プライマリー)に障害が発生した場合にプライマリーになる役割を持つストレージノードです。
- クラスターワーカーノード
クラスターマスターノード(プライマリー)から制御されるストレージノードです。

プロテクションドメインとフォールトドメイン

プロテクションドメインは、データ保証形式と内部処理 I/O のリソース使用率を設定する単位です。プロテクションドメイン内にはストレージプールが 1 つ存在し、プロテクションドメインには 1 つ以上のフォールトドメインがあります。



フォールトドメインは、単一のアベイラビリティーゾーンに設置されているストレージノードのグループです。Single-AZ 構成の場合、クラスターを構築するストレージノードは、単一のアベイラビリティーゾーンにのみ設置可能であるため、フォールトドメイン数は 1 となります。Multi-AZ 構

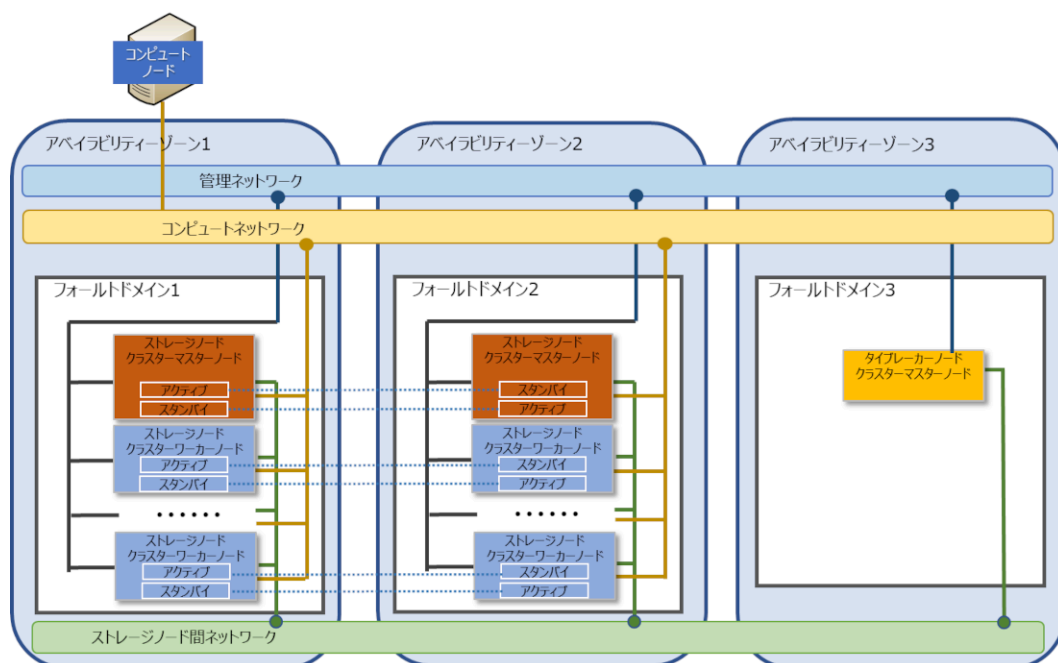
成の場合、1つのフォールトドメイン内のストレージノードがまとまって異常になっても、別のフォールトドメインが正常であればストレージの運用を継続できます。

VSP One SDS Block は、フォールトドメインをまたがって冗長化されるよう、ユーザーデータ、ストレージコントローラーを自動配置します。ただし、クラスターマスターノードの配置は、フォールトドメインごとに1ノード(クラスターマスターノードが計3ノードの場合)または1~2ノード(クラスターマスターノードが計5ノードの場合)になるよう、導入時に手動で行う必要があります。詳しくは、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「VSP One SDS Block がサポートする耐障害性に関する設定と各機能の説明」を参照してください。

ただし、複数フォールトドメイン構成の場合でも、他のフォールトドメインとの間で共有する電源系統やネットワークスイッチなどのハードウェアが1つでもあると、そのハードウェアに障害が発生した場合は、複数のフォールトドメインが同時障害となり、運用が停止するおそれがあります。

フォールトドメインごとに電源系統やネットワークスイッチなどのハードウェアが分離できない場合は、分離できていないハードウェアに障害が発生した場合に備えて、冗長構成をとっておく必要があります。

フォールトドメインは、VSP One SDS Block のセットアップ時に設定します。設定方法など詳しくは、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。



構成ファイル

VSP One SDS Block には次の構成ファイルがあります。構成ファイルの詳細については、「構成ファイルを管理する <<Cloud for Microsoft Azure>>」を参照してください。

構成ファイル	説明
SystemConfigurationFile.csv ¹	VSP One SDS Block の自体の構成を記載するファイル
VMConfigurationFile.json ²	ストレージクラスターデプロイ用テンプレートファイル

構成ファイル	説明
VMConfigurationFile.parameters.json ²	ストレージクラスターデプロイ用変数定義ファイル
1. VSSB 構成ファイル 2. VM 構成ファイル	

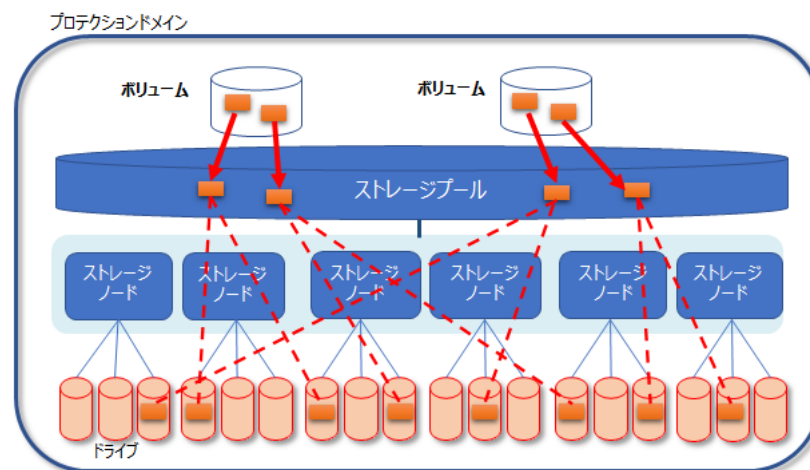
これらのファイルは、VSP One SDS Block の構成を定義するファイルであり、以下の場合に使用されます。

- ・ ドライブ増設時
- ・ ドライブ交換時
- ・ ストレージノード増設時
- ・ ストレージノード交換時
- ・ ソフトウェアアップデート時

ストレージプールとボリューム

複数のドライブをまとめた論理的なユーザーデータ格納領域をストレージプールといいます。ユーザーは、ストレージプールを対象にストレージ容量を管理すればよく、ドライブやその物理的な境界を意識せずに済みます。

ストレージプールは、既存のストレージノードにドライブを増設したり、別途ストレージノードを追加したりすることで拡張できます。



ボリュームは、ユーザーデータの読み書きが行われる論理デバイスです。ボリュームはストレージコントローラーによって管理され、ユーザーデータはボリュームに関連付けられたストレージプールに書き込まれます。

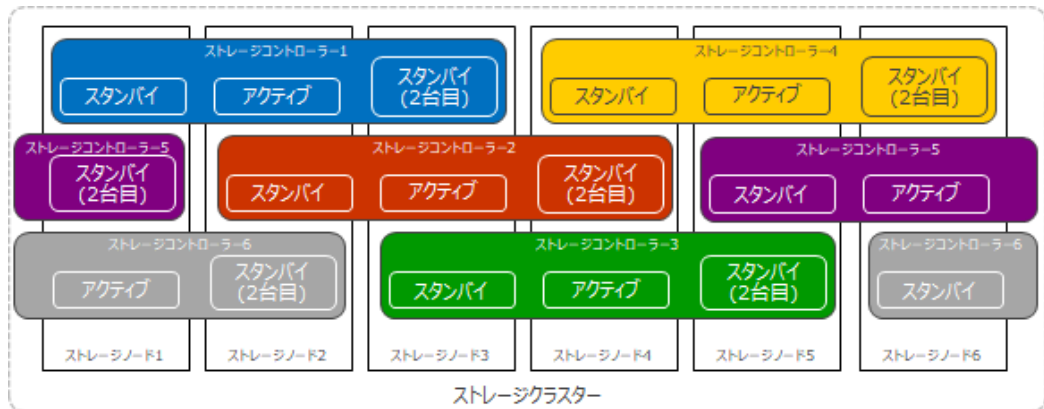
ストレージノードの容量管理とストレージコントローラー

ストレージコントローラーは、ストレージノードの容量やボリュームを管理する VSP One SDS Block の一部のプロセスです。

各ストレージノードの容量は、ストレージコントローラーによって管理されます。また、ストレージコントローラーは、システムの構成や使用状況を監視しています。

ストレージコントローラーが管理する容量をまとめたものが、ストレージプールの全体容量になります。

ストレージコントローラーは、ストレージノードと同数存在します。1つのストレージコントローラーは複数のストレージノードにまたがって配置されており、ストレージノード障害に耐えられるように冗長化されています(下図は3重化の例)。



ストレージコントローラーの冗長度としては、OneRedundantStorageNode(2重化)とTwoRedundantStorageNodes(3重化)の2つが存在し、ユーザーデータの保護方式の設定から自動的に決定されます。

詳しくは、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

また、ストレージコントローラーの管理については、このマニュアルの「ストレージコントローラーを管理する」を参照してください。

運用・管理・保守の概要(ユースケース索引)

- 2.1 運用環境を構成するには
- 2.2 ユーザー登録とセキュリティ対策をするには
- 2.3 ボリュームをコンピュータノードに提供するには
- 2.4 運用状況を監視するには
- 2.5 リソース情報を確認するには
- 2.6 設定を確認するには
- 2.7 リソースを追加・削除・変更するには
- 2.8 設定を変更するには

2.1 運用環境を構成するには

セットアップ終了後、運用を開始する前に以下のような環境構築を行います。

下表の列「GUI 可能操作」では、VSP One SDS Block Administrator を使って行える操作を○印で示しています。

≪Bare metal≫

区分	参照先	GUI 可能操 作
構成ファイルを管理する	3.1.1 構成ファイルを管理する≪Bare metal≫	
コントローラーノードを設置する	3.2.1 コントローラーノードの設置≪Bare metal≫	
コンピュートノードを設置する	3.3.1 コンピュートノードを設置する≪Bare metal≫	
ライセンスを登録する	4.2.1 ライセンスを登録する≪Bare metal≫	
時刻設定を確認する	5 時刻設定を管理する	
ユーザーデータを暗号化する	42 格納データ暗号化を利用する	
ストレージプールを拡張する	3.4.1 空状態にあるストレージプールを拡張する≪Bare metal≫	
ログイン時・CLI Basic 認証時に表示するメッセージを設定する	3.5 ログイン時・CLI Basic 認証時に表示するメッセージを設定する	
iSNS サーバーを利用する	16.2.1 コンピュートポートの設定を編集する≪Bare metal≫	
マルチテナンシーを構成する	39 マルチテナンシーを構成する≪Bare metal≫	
スペアノードを利用する	40 スペアノードを管理する≪Bare metal≫	○*
キャッシュ保護付きライトバックモードを利用する	41 キャッシュ保護付きライトバックモードを管理する	
Universal Replicator を利用する	43 Universal Replicator を利用する	
* スペアノード情報の参照・登録・編集・削除、BMC 接続情報の参照・更新が可能		

≪Cloud for AWS≫

区分	参照先	GUI 可能操 作
構成ファイルを管理する	3.1.2 構成ファイルを管理する≪Cloud for AWS≫	
コントローラーノードを設置する	3.2.2 コントローラーノードの設置≪Cloud for AWS≫	
コンピュートノードを設置する	3.3.2 コンピュートノードを設置する≪Cloud for AWS≫	
ライセンスを登録する	4.2.2 ライセンスを登録する≪Cloud≫	
時刻設定を確認する	5 時刻設定を管理する	
ユーザーデータを暗号化する	42 格納データ暗号化を利用する	
ストレージプールを拡張する	3.4.2 空状態にあるストレージプールを拡張する≪Cloud≫	
ログイン時・CLI Basic 認証時に表示するメッセージを設定する	3.5 ログイン時・CLI Basic 認証時に表示するメッセージを設定する	

区分	参照先	GUI 可能操 作
iSNS サーバーを利用する	16.2.2 コンピュートポートの設定を編集する<<Cloud>>	
キャッシュ保護付きライトバックモードを利用する	41 キャッシュ保護付きライトバックモードを管理する	
Universal Replicator を利用する	43 Universal Replicator を利用する	

<<Cloud for Google Cloud>>

区分	参照先	GUI 可能操 作
構成ファイルを管理する	3.1.3 構成ファイルを管理する<<Cloud for Google Cloud>>	
コントローラーノードを設置する	3.2.3 コントローラーノードの設置<<Cloud for Google Cloud>>	
コンピューターノードを設置する	3.3.3 コンピューターノードを設置する<<Cloud for Google Cloud>>	
ライセンスを登録する	4.2.2 ライセンスを登録する<<Cloud>>	
時刻設定を確認する	5 時刻設定を管理する	
ユーザーデータを暗号化する	42 格納データ暗号化を利用する	
ストレージプールを拡張する	3.4.2 空状態にあるストレージプールを拡張する<<Cloud>>	
ログイン時・CLI Basic 認証時に表示するメッセージを設定する	3.5 ログイン時・CLI Basic 認証時に表示するメッセージを設定する	
iSNS サーバーを利用する	16.2.2 コンピュートポートの設定を編集する<<Cloud>>	
キャッシュ保護付きライトバックモードを利用する	41 キャッシュ保護付きライトバックモードを管理する	
Universal Replicator を利用する	43 Universal Replicator を利用する	

<<Cloud for Microsoft Azure>>

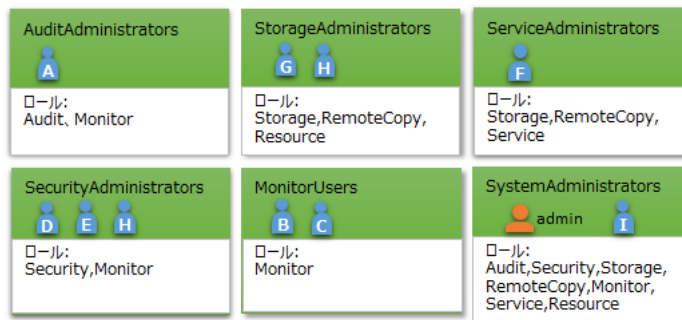
区分	参照先	GUI 可能操 作
構成ファイルを管理する	3.1.4 構成ファイルを管理する<<Cloud for Microsoft Azure>>	
コントローラーノードを設置する		
コンピューターノードを設置する	3.3.4 コンピューターノードを設置する<<Cloud for Microsoft Azure>>	
ライセンスを登録する	4.2.2 ライセンスを登録する<<Cloud>>	
時刻設定を確認する	5 時刻設定を管理する	
ユーザーデータを暗号化する	42 格納データ暗号化を利用する	
ストレージプールを拡張する	3.4.2 空状態にあるストレージプールを拡張する<<Cloud>>	
ログイン時・CLI Basic 認証時に表示するメッセージを設定する	3.5 ログイン時・CLI Basic 認証時に表示するメッセージを設定する	
iSNS サーバーを利用する	16.2.2 コンピュートポートの設定を編集する<<Cloud>>	

区分	参照先	GUI 可能操 作
キャッシュ保護付きライトバックモードを利用する	41 キャッシュ保護付きライトバックモードを管理する	
Universal Replicator を利用する	43 Universal Replicator を利用する	

2.2 ユーザー登録とセキュリティ対策をするには

ストレージシステムのセキュリティ対策のため、ユーザー登録とロールによる権限割り当てのほか、いくつかのセキュリティ対策に関する手段が用意されています。

(ユーザーの登録例)



AuditAdministrators や StorageAdministrators などは、ユーザーグループ名です。ユーザー(A～I)の操作権限は、所属したユーザーグループのロールによって規定されます。

下表の列「GUI 可能操作」では、VSP One SDS Block Administrator を使って行える操作を○印で示しています。

＜＜Bare metal＞＞

区分	参照先	GUI 可能操 作
ユーザー登録と操作権限の割り当て	19.4 ユーザーを作成する	
	19.12 ユーザーグループを作成する	
	19.8 ユーザーをユーザーグループに追加する	
	19.15 外部認証サーバーを利用する	
ユーザー認証設定を編集する	21.1 ユーザー認証設定を編集する	
運用管理を SSL/TLS 通信で行う	22 運用管理を SSL/TLS 通信で行う	○*
CHAP 認証を利用する	23.1 CHAP ユーザーを作成して CHAP 認証を設定する	
	23.8 CHAP ユーザーに対してコンピュータポートへのアクセスを許可する	
許可リストを設定する	3.6.1 許可リストを設定する＜＜Bare metal＞＞	
* サーバー証明書のインポートが可能		

＜＜Cloud＞＞

区分	参照先	GUI 可能操 作
ユーザー登録と操作権限の割り当て	19.4 ユーザーを作成する	
	19.12 ユーザーグループを作成する	
	19.8 ユーザーをユーザーグループに追加する	
	19.15 外部認証サーバーを利用する	
ユーザー認証設定を編集する	21.1 ユーザー認証設定を編集する	
運用管理を SSL/TLS 通信で行う	22 運用管理を SSL/TLS 通信で行う	○*
CHAP 認証を利用する	23.1 CHAP ユーザーを作成して CHAP 認証を設定する	
	23.8 CHAP ユーザーに対してコンピュータポートへのアクセスを許可する	
許可リストを設定する	3.6.2 許可リストを設定する<<Cloud>>	
* サーバー証明書のインポートが可能		

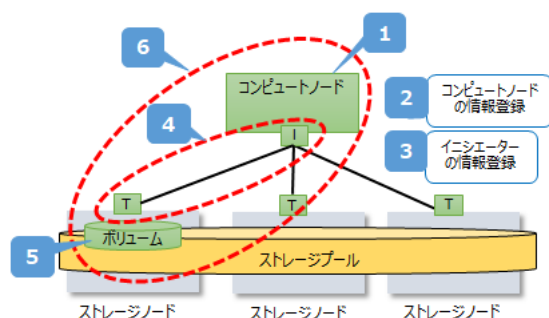
2.3 ボリュームをコンピュータノードに提供するには

ストレージシステムを利用するコンピュータノードは、以下の情報登録が必要です。

- ・ 設置するコンピュータノードの要件などの確認
- ・ コンピュータノードの情報登録
- ・ コンピュータノードのイニシエーター情報の登録
- ・ コンピュータノードのパス情報の登録

また、コンピュータノードからストレージシステムを利用するには、ユーザーデータが格納されるボリュームをストレージプールに作成します。

作成したボリュームを、コンピュータノードから扱えるようにするには、ボリュームとコンピュータノード間のパスを設定します。



下表の列「GUI 可能操作」では、VSP One SDS Block Administrator を使って行える操作を○印で示しています。

<<Bare metal>>

区分	操作手順の実施順と参照先	GUI 可能操 作
ボリュームをコンピュータノードに提供する	(1) 「 3.3.1 コンピュータノードを設置する<<Bare metal>> 」	○
	(2) 「 15.1 コンピュータノードの情報を登録する 」	
	(3) 「 15.6 コンピュータノードのイニシエーター情報を登録する 」	
	(4) 「 15.9 コンピュータノードのパス情報を登録する 」	
	(5) 「 17.4.1 ボリュームを作成する<<Bare metal>> 」	○
	(6) 「 15.12.1 ボリュームをコンピュータノードに接続する<<Bare metal>> 」	○

<<Cloud for AWS>>

区分	操作手順の実施順と参照先	GUI 可能操 作
ボリュームをコンピュータノードに提供する	(1) 「 3.3.2 コンピュータノードを設置する<<Cloud for AWS>> 」	○
	(2) 「 15.1 コンピュータノードの情報を登録する 」	
	(3) 「 15.6 コンピュータノードのイニシエーター情報を登録する 」	
	(4) 「 15.9 コンピュータノードのパス情報を登録する 」	
	(5) 「 17.4.2 ボリュームを作成する<<Cloud>> 」	○
	(6) 「 15.12.2 ボリュームをコンピュータノードに接続する<<Cloud>> 」	○

<<Cloud for Google Cloud>>

区分	操作手順の実施順と参照先	GUI 可能操 作
ボリュームをコンピュータノードに提供する	(1) 「 3.3.3 コンピュータノードを設置する<<Cloud for Google Cloud>> 」	○
	(2) 「 15.1 コンピュータノードの情報を登録する 」	
	(3) 「 15.6 コンピュータノードのイニシエーター情報を登録する 」	
	(4) 「 15.9 コンピュータノードのパス情報を登録する 」	
	(5) 「 17.4.2 ボリュームを作成する<<Cloud>> 」	○
	(6) 「 15.12.2 ボリュームをコンピュータノードに接続する<<Cloud>> 」	○

<<Cloud for Microsoft Azure>>

区分	操作手順の実施順と参照先	GUI 可能操作
ボリュームをコンピュータノードに提供する	(1) 「 3.3.4 コンピュータノードを設置する<<Cloud for Microsoft Azure>> 」	
	(2) 「 15.1 コンピュータノードの情報を登録する 」	○
	(3) 「 15.6 コンピュータノードのイニシエーター情報を登録する 」	
	(4) 「 15.9 コンピュータノードのパス情報を登録する 」	
	(5) 「 17.4.2 ボリュームを作成する<<Cloud>> 」	○
	(6) 「 15.12.2 ボリュームをコンピュータノードに接続する<<Cloud>> 」	○

2.4 運用状況を監視するには

ストレージシステムの運用状況は、ログ、性能、容量、内部動作などによって監視します。

下表の列「GUI 可能操作」では、VSP One SDS Block Administrator を使って行える操作を○印で示しています。

<<Bare metal>>

区分	参照先	GUI 可能操作
ログを監視する	6.2 イベントログの取得	○
	6.3.1 イベントログの Syslog 転送設定を編集する<<Bare metal>>	
	6.4.1 イベントログの SMTP 転送設定を編集する<<Bare metal>>	
	6.6 Syslog 転送されるイベントログを監視する	
	7.2 監査ログをコントローラーノードにダウンロードする	
	7.5 Syslog サーバーへ転送される監査ログを監視する	
	6.9 SNMP を利用する	
性能を監視する (VSP One SDS Block Administrator では 32 個まで。 また高解像度のみ取得できます。)	24.3 ドライブの性能情報の取得	○
	24.2 管理ポートの性能情報の取得	○
	24.4 ストレージノード間ポートの性能情報の取得	○
	24.6 ストレージプールの性能情報の取得	
	24.7 コンピュータポートの性能情報の取得	○
	24.8 ストレージクラスターの性能情報(低解像度)を取得する	
	24.9 ストレージノードの性能情報の取得	○
容量を監視する	24.11 ボリュームの性能情報の取得	○
	24.5 ストレージプールの容量情報の取得	○
	24.10 ボリュームの容量情報の取得	○

区分	参照先	GUI 可能 操作
内部動作を監視する	20.2 セッション情報の取得	
	31.2 ジョブの情報の取得	○
	30 リビルド(データ再構築)の状態を確認する	○
	14 ドライブデータ再配置を管理する<<Bare metal>>	○
マルチテナンシーを構成している場合	39.10 性能低下・操作不可の監視と対処<<Bare metal>>	
	39.11 リソース不足・性能問題発生時の対処<<Bare metal>>	
暗号化鍵の使用状況を監視する	42.1 格納データ暗号化の概要	

<<Cloud>>

区分	参照先	GUI 可能 操作
ログを監視する	6.2 イベントログの取得	○
	6.3.2 イベントログの Syslog 転送設定を編集する<<Cloud>>	
	6.4.2 イベントログの SMTP 転送設定を編集する<<Cloud>>	
	6.6 Syslog 転送されるイベントログを監視する	
	7.2 監査ログをコントローラーノードにダウンロードする	
	7.5 Syslog サーバーへ転送される監査ログを監視する	
	6.9 SNMP を利用する	
性能を監視する (VSP One SDS Block Administrator では 32 個まで。 また高解像度のみ取得できます。)	24.3 ドライブの性能情報の取得	○
	24.2 管理ポートの性能情報の取得	○
	24.4 ストレージノード間ポートの性能情報の取得	○
	24.6 ストレージプールの性能情報の取得	
	24.7 コンピュートポートの性能情報の取得	○
	24.8 ストレージクラスターの性能情報(低解像度)を取得する	
	24.9 ストレージノードの性能情報の取得	○
	24.11 ボリュームの性能情報の取得	○
容量を監視する	24.5 ストレージプールの容量情報の取得	○
	24.10 ボリュームの容量情報の取得	○
内部動作を監視する	20.2 セッション情報の取得	
	31.2 ジョブの情報の取得	○
	30 リビルド(データ再構築)の状態を確認する	○
暗号化鍵の使用状況を監視する	42.1 格納データ暗号化の概要	

2.5 リソース情報を確認するには

ストレージシステムを構成する各種リソースの情報が確認できます。

下表の列「GUI 可能操作」では、VSP One SDS Block Administrator を使って行える操作を○印で示しています。

≪Bare metal≫

区分	参照先	GUI 可能操 作
ストレージクラスターの情報を確認する	27.1 ストレージクラスターの情報の取得	○
	28.1 プロテクションドメイン情報の一覧を取得する	
	28.2 プロテクションドメイン情報を個別に取得する	○
	27.2 フォールトドメイン情報の一覧の取得	○
	27.3 フォールトドメイン情報の個別取得	○
	27.4 ヘルスステータスを取得する	○
	27.5 クラスターマスターノード(プライマリー)かを確認する	
	31.1 API のバージョン・名称を取得する	
	4.4 ライセンス情報の取得	○
ドライブの情報を確認する	8.2 ドライブ情報の取得	○
コンピュートノードの情報を確認する	15.2 コンピュートノード情報の一覧を取得する	○
	15.3 コンピュートノード情報を個別に取得する	○
	15.7 コンピュートノードのイニシエーター情報の取得	○
	15.10 コンピュートノードのパス情報の取得	○
	15.13 ボリュームとコンピュートノードの接続情報の取得	○
ストレージコントローラーの情報を確認する	29.3 ストレージコントローラーの情報の取得	○
ユーザーの情報を確認する	19.2 ユーザー情報の一覧を取得する	
	19.3 ユーザーの詳細情報を取得する	
	19.10 ユーザーグループの一覧を取得する	
	19.11 ユーザーグループの詳細情報を取得する	
ネットワークの情報を確認する	25.1 ストレージクラスターのネットワーク情報の取得	
	25.2 管理ポートの情報の取得	○
	25.3 ストレージノード間ポートの情報の取得	○
	16.1 コンピュートポートの情報の取得	○
	25.4 ストレージノードのネットワーク設定の取得	
ボリュームの情報を確認する	17.7 ボリューム情報の一覧の取得	○
	17.8 ボリューム情報の個別取得	○
	18.6 ボリュームに対する P-VOL 情報を取得する	○
	18.7 ボリュームに対する S-VOL 情報の一覧を取得する	○
ストレージノードの情報を確認する	10.2 ストレージノード情報の取得	○
ストレージプールの情報を確認する	26.5 ストレージプールの情報の取得	○

区分	参照先	GUI 可能操 作
モデルを確認する	31.3 モデルを確認する	○
VPS の情報を確認する	39.7 VPS の情報の取得<<Bare metal>>	○
スベアノードの情報を確認する	40.12 スベアノードの情報の取得<<Bare metal>>	○
BMC 情報を確認する	40.9 ストレージノードの BMC 情報の取得<<Bare metal>>	○
暗号化鍵の情報を確認する	42.7 暗号化鍵の情報の取得	
	42.8 暗号化鍵の個数を取得する	

<<Cloud>>

区分	参照先	GUI 可能操 作
ストレージクラスターの情報を確認する	27.1 ストレージクラスターの情報の取得	○
	28.1 プロテクションドメイン情報の一覧を取得する	
	28.2 プロテクションドメイン情報を個別に取得する	○
	27.2 フォールトドメイン情報の一覧の取得	○
	27.3 フォールトドメイン情報の個別取得	○
	27.4 ヘルスステータスを取得する	○
	27.5 クラスタマスターノード(プライマリー)かを確認する	
	31.1 API のバージョン・名称を取得する	
	4.4 ライセンス情報の取得	○
ドライブの情報を確認する	8.2 ドライブ情報の取得	○
コンピュータノードの情報を確認する	15.2 コンピュータノード情報の一覧を取得する	○
	15.3 コンピュータノード情報を個別に取得する	○
	15.7 コンピュータノードのイニシエーター情報の取得	○
	15.10 コンピュータノードのバス情報の取得	
	15.13 ボリュームとコンピュータノードの接続情報の取得	○
ストレージコントローラーの情報を確認する	29.3 ストレージコントローラーの情報の取得	○
ユーザーの情報を確認する	19.2 ユーザー情報の一覧を取得する	
	19.3 ユーザーの詳細情報を取得する	
	19.10 ユーザーグループの一覧を取得する	
	19.11 ユーザーグループの詳細情報を取得する	
ネットワークの情報を確認する	25.1 ストレージクラスターのネットワーク情報の取得	
	25.2 管理ポートの情報の取得	○
	25.3 ストレージノード間ポートの情報の取得	○
	16.1 コンピュータポートの情報の取得	○
	25.4 ストレージノードのネットワーク設定の取得	○

区分	参照先	GUI 可能操 作
ボリュームの情報を確認する	17.7 ボリューム情報の一覧の取得	○
	17.8 ボリューム情報の個別取得	○
	18.6 ボリュームに対する P-VOL 情報を取得する	○
	18.7 ボリュームに対する S-VOL 情報の一覧を取得する	○
ストレージノードの情報を確認する	10.2 ストレージノード情報の取得	○
ストレージプールの情報を確認する	26.5 ストレージプールの情報の取得	
モデルを確認する	31.3 モデルを確認する	○
暗号化鍵の情報を確認する	42.7 暗号化鍵の情報の取得	
	42.8 暗号化鍵の個数を取得する	

2.6 設定を確認するには

VSP One SDS Block の動作に関する設定内容を確認できます。

下表の列「GUI 可能操作」では、VSP One SDS Block Administrator を使って行える操作を○印で示しています。

≪Bare metal≫

区分	参照先	GUI 可 能操作
ログの Syslog 転送設定を確認する	6.5 イベントログの設定を取得する	
	7.4 監査ログの Syslog 転送設定を取得する	
ライセンス情報を確認する	4.4 ライセンス情報の取得	○
ライセンス設定を確認する	4.6 ライセンス設定情報の取得	○
時刻設定を確認する	5.2 ストレージクラスターの時刻設定を取得する	
容量バランスの設定を確認する	44.4 ストレージクラスターの容量バランスの設定を取得する	
	44.6 ストレージコントローラーの容量バランスの設定を取得する	
	44.8 ストレージノードの容量バランスの情報の取得	
ストレージノードの自動回復機能の設定を確認する	13.6.1 ストレージノードの自動回復機能の情報を取得する ≪Bare metal≫	
ユーザー認証設定を確認する	21.2 ユーザー認証設定を取得する	
CHAP 設定を確認する	23.2 CHAP ユーザー情報の一覧を取得する	
	23.3 CHAP ユーザー情報を個別に取得する	
	23.6 ターゲット動作のコンピュータポートの認証設定を取得する	

区分	参照先	GUI 可能操作
	23.9 コンピュートポートへのアクセスを許可した CHAP ユーザー情報の取得	
許可リストの設定を確認する	3.6.1 許可リストを設定する<<Bare metal>>	
外部認証サーバーの設定を取得する	19.16 外部認証サーバーの設定を取得する	
構成ファイルをエクスポートする	3.1.5 構成ファイルをエクスポートする<<Bare metal>>	
スベアノード機能の設定を確認する	40.14 スベアノード機能の設定を確認する<<Bare metal>>	
暗号化環境の設定を確認する	42.3 暗号化環境の設定の情報を取得する	
	26.5 ストレージプールの情報の取得	

<<Cloud for AWS>>

区分	参照先	GUI 可能操作
ログの Syslog 転送設定を確認する	6.5 イベントログの設定を取得する	
	7.4 監査ログの Syslog 転送設定を取得する	
ライセンス情報を確認する	4.4 ライセンス情報の取得	○
ライセンス設定を確認する	4.6 ライセンス設定情報の取得	○
時刻設定を確認する	5.2 ストレージクラスターの時刻設定を取得する	
容量バランスの設定を確認する	44.4 ストレージクラスターの容量バランスの設定を取得する	
	44.6 ストレージコントローラーの容量バランスの設定を取得する	
	44.8 ストレージノードの容量バランスの情報の取得	
ストレージノードの自動回復機能の設定を確認する	13.6.2 ストレージノードの自動回復機能の情報を取得する<<Cloud>>	
ユーザー認証設定を確認する	21.2 ユーザー認証設定を取得する	
CHAP 設定を確認する	23.2 CHAP ユーザー情報の一覧を取得する	
	23.3 CHAP ユーザー情報を個別に取得する	
	23.6 ターゲット動作のコンピューポートの認証設定を取得する	
	23.9 コンピュートポートへのアクセスを許可した CHAP ユーザー情報の取得	
許可リストの設定を確認する	3.6.2 許可リストを設定する<<Cloud>>	
外部認証サーバーの設定を取得する	19.16 外部認証サーバーの設定を取得する	
構成ファイルをエクスポートする	3.1.6 構成ファイルをエクスポートする<<Cloud for AWS>>	
暗号化環境の設定を確認する	42.3 暗号化環境の設定の情報を取得する	
	26.5 ストレージプールの情報の取得	

<<Cloud for Google Cloud>>

区分	参照先	GUI 可能操作
ログの Syslog 転送設定を確認する	6.5 イベントログの設定を取得する	
	7.4 監査ログの Syslog 転送設定を取得する	
ライセンス情報を確認する	4.4 ライセンス情報の取得	○
ライセンス設定を確認する	4.6 ライセンス設定情報の取得	○
時刻設定を確認する	5.2 ストレージクラスターの時刻設定を取得する	
容量バランスの設定を確認する	44.4 ストレージクラスターの容量バランスの設定を取得する	
	44.6 ストレージコントローラーの容量バランスの設定を取得する	
	44.8 ストレージノードの容量バランスの情報の取得	
ストレージノードの自動回復機能の設定を確認する	13.6.2 ストレージノードの自動回復機能の情報を取得する<<Cloud>>	
ユーザー認証設定を確認する	21.2 ユーザー認証設定を取得する	
CHAP 設定を確認する	23.2 CHAP ユーザー情報の一覧を取得する	
	23.3 CHAP ユーザー情報を個別に取得する	
	23.6 ターゲット動作のコンピュートポートの認証設定を取得する	
	23.9 コンピュートポートへのアクセスを許可した CHAP ユーザー情報の取得	
許可リストの設定を確認する	3.6.2 許可リストを設定する<<Cloud>>	
外部認証サーバーの設定を取得する	19.16 外部認証サーバーの設定を取得する	
構成ファイルをエクスポートする	3.1.7 構成ファイルをエクスポートする<<Cloud for Google Cloud>>	
暗号化環境の設定を確認する	42.3 暗号化環境の設定の情報を取得する	
	26.5 ストレージプールの情報の取得	

<<Cloud for Microsoft Azure>>

区分	参照先	GUI 可能操作
ログの Syslog 転送設定を確認する	6.5 イベントログの設定を取得する	
	7.4 監査ログの Syslog 転送設定を取得する	
ライセンス情報を確認する	4.4 ライセンス情報の取得	○
ライセンス設定を確認する	4.6 ライセンス設定情報の取得	○
時刻設定を確認する	5.2 ストレージクラスターの時刻設定を取得する	
容量バランスの設定を確認する	44.4 ストレージクラスターの容量バランスの設定を取得する	
	44.6 ストレージコントローラーの容量バランスの設定を取得する	
	44.8 ストレージノードの容量バランスの情報の取得	

区分	参照先	GUI 可能操作
ストレージノードの自動回復機能の設定を確認する	13.6.2 ストレージノードの自動回復機能の情報を取得する<<Cloud>>	
ユーザー認証設定を確認する	21.2 ユーザー認証設定を取得する	
CHAP 設定を確認する	23.2 CHAP ユーザー情報の一覧を取得する	
	23.3 CHAP ユーザー情報を個別に取得する	
	23.6 ターゲット動作のコンピュートポートの認証設定を取得する	
	23.9 コンピュートポートへのアクセスを許可した CHAP ユーザー情報の取得	
許可リストの設定を確認する	3.6.2 許可リストを設定する<<Cloud>>	
外部認証サーバーの設定を取得する	19.16 外部認証サーバーの設定を取得する	
構成ファイルをエクスポートする	3.1.8 構成ファイルをエクスポートする<<Cloud for Microsoft Azure>>	
暗号化環境の設定を確認する	42.3 暗号化環境の設定の情報を取得する	
	26.5 ストレージプールの情報の取得	

2.7 リソースを追加・削除・変更するには

各リソースに対して、実行できる追加・削除・変更などの一覧です。

下表の列「GUI 可能操作」では、VSP One SDS Block Administrator を使って行える操作を○印で示しています。

<<Bare metal>>

区分	参照先	GUI 可能操作
ストレージクラスター	<起動・停止・再起動> 33 ストレージクラスターを起動/停止する	
	<ソフトウェアアップデート> 32 ストレージソフトウェアアップデートの要件と手順	
	<ソフトウェアアンインストール> 37 ストレージソフトウェアをアンインストールする	
	<ライセンス> 4 ライセンスを管理する	
ドライブ	9 ドライブを増設する	○
	8.3.1 ドライブを減設する<<Bare metal>>	○
	8.4.1 ドライブを交換する<<Bare metal>>	○
	8.5 ドライブを再組み入れする<<Bare metal>>	○
ユーザー/ユーザーグループ	19.4 ユーザーを作成する	
	19.5 ユーザー情報を編集する	
	19.6 ユーザーを削除する	

区分	参照先	GUI 可能操作
	19.7 自身のパスワードを変更する	○ ¹
	19.8 ユーザーをユーザーグループに追加する	
	19.9 ユーザーをユーザーグループから削除する	
	19.12 ユーザーグループを作成する	
	19.13 ユーザーグループ情報を編集する	
	19.14 ユーザーグループを削除する	
セッション	20.3 セッションを生成する	
	20.4 セッションを削除する	
コンピュータポート	16.2.1 コンピュータポートの設定を編集する<<Bare metal>>	
ボリューム	17.4.1 ボリュームを作成する<<Bare metal>>	○
	17.9 ボリュームの設定を編集する	○ ²
	17.2 ボリュームの容量削減機能の概要	
	17.3 ボリュームの容量削減機能を有効にする	
	17.5 ボリュームを削除する	○
	17.6 ボリュームを拡張する	○
	18.2 スナップショットの取得準備をする	
	18.3 スナップショットを取得する	
	18.4 スナップショットを削除する	○
	18.5.1 スナップショットからボリュームを復元する<<Bare metal>>	
	15.12.1 ボリュームをコンピュータノードに接続する<<Bare metal>>	○
	15.14.1 ボリュームとコンピュータノードの接続を解除する<<Bare metal>>	○
	15.15.1 複数のボリュームとコンピュータノードの接続を解除する<<Bare metal>>	
ストレージノード	11.1 ストレージノードの増設<<Bare metal>>	
	12.1 ストレージノードの減設<<Bare metal>>	
	13 ストレージノードを保守する	○ ³
コンピュータノード	15.1 コンピュータノードの情報を登録する	○
	15.4 コンピュータノードの情報を編集する	○
	15.5 コンピュータノードの情報を削除する	○
	15.6 コンピュータノードのイニシエーター情報を登録する	○
	15.8 コンピュータノードのイニシエーター情報を削除する	○
	15.9 コンピュータノードのパス情報を登録する	○
	15.11.1 コンピュータノードのパス情報を削除する<<Bare metal>>	
	15.12.1 ボリュームをコンピュータノードに接続する<<Bare metal>>	○

区分	参照先	GUI 可能操作
	15.14.1 ボリュームとコンピュータノードの接続を解除する 《Bare metal》	○
	15.15.1 複数のボリュームとコンピュータノードの接続を解除する 《Bare metal》	○
構成情報	34 ストレージクラスターの構成情報を変更・設定する 《Bare metal》	
認証チケット	35.1 認証チケットを発行する	
	35.2 認証チケットを破棄する	
マルチテナンシー	39.10 性能低下・操作不可の監視と対処 《Bare metal》	
	39.11 リソース不足・性能問題発生時の対処 《Bare metal》	
スペアノード	40.10 スペアノードの情報を登録する 《Bare metal》	○
	40.11 スペアノードの情報を編集する 《Bare metal》	○
	40.13 スペアノードの情報を削除する 《Bare metal》	○
BMC 情報	40.4 スペアノードを利用するための BMC アカウントを準備する 《Bare metal》	
	40.5 ストレージクラスターに BMC 接続検証用ルート証明書をインポートする 《Bare metal》	
	40.6 ストレージクラスターから BMC 接続検証用ルート証明書を取得する 《Bare metal》	
	40.7 ストレージクラスターから BMC 接続検証用ルート証明書を削除する 《Bare metal》	
	40.8 ストレージノードの BMC 情報を登録・編集する 《Bare metal》	○
暗号化鍵	42.5 暗号化鍵を作成する	
	42.6 暗号化鍵を削除する	
1. 初めてログインする場合、またはパスワードの有効期限が切れている場合のみ可能 2. 通常ボリュームのみ可能 3. ストレージノードの保守閉塞とストレージノードの保守回復のみ可能		

《Cloud for AWS》

区分	参照先	GUI 可能操作
ストレージクラスター	<起動・停止・再起動> 33 ストレージクラスターを起動/停止する	
	<ソフトウェアアップデート> 32 ストレージソフトウェアアップデートの要件と手順	
	<ソフトウェアアンインストール> 37 ストレージソフトウェアをアンインストールする	
	<ライセンス> 4 ライセンスを管理する	
ドライブ	9 ドライブを増設する	○

区分	参照先	GUI 可能操作
	8.4.2 ドライブを交換する<<Cloud for AWS>>	○
ユーザー/ユーザーグループ	19.4 ユーザーを作成する	
	19.5 ユーザー情報を編集する	
	19.6 ユーザーを削除する	
	19.7 自身のパスワードを変更する	○ ¹
	19.8 ユーザーをユーザーグループに追加する	
	19.9 ユーザーをユーザーグループから削除する	
	19.12 ユーザーグループを作成する	
	19.13 ユーザーグループ情報を編集する	
	19.14 ユーザーグループを削除する	
セッション	20.3 セッションを生成する	
	20.4 セッションを削除する	
コンピュートポート	16.2.2 コンピュートポートの設定を編集する<<Cloud>>	
ボリューム	17.4.2 ボリュームを作成する<<Cloud>>	○
	17.9 ボリュームの設定を編集する	○ ²
	17.2 ボリュームの容量削減機能の概要	
	17.3 ボリュームの容量削減機能を有効にする	
	17.5 ボリュームを削除する	○
	17.6 ボリュームを拡張する	○
	18.2 スナップショットの取得準備をする	
	18.3 スナップショットを取得する	
	18.4 スナップショットを削除する	○
	18.5.2 スナップショットからボリュームを復元する<<Cloud>>	
	15.12.2 ボリュームをコンピュートノードに接続する<<Cloud>>	○
	15.14.2 ボリュームとコンピュートノードの接続を解除する<<Cloud>>	○
	15.15.2 複数のボリュームとコンピュートノードの接続を解除する<<Cloud>>	
ストレージノード	11.2 ストレージノードの増設<<Cloud for AWS>>	
	12.2 ストレージノードの減設<<Cloud for AWS>>	
	13 ストレージノードを保守する	○ ³
コンピュートノード	15.1 コンピュートノードの情報を登録する	○
	15.4 コンピュートノードの情報を編集する	○
	15.5 コンピュートノードの情報を削除する	○
	15.6 コンピュートノードのイニシエーター情報を登録する	○
	15.8 コンピュートノードのイニシエーター情報を削除する	○
	15.9 コンピュートノードのパス情報を登録する	○
	15.11.2 コンピュートノードのパス情報を削除する<<Cloud>>	

区分	参照先	GUI 可能操作
	15.12.2 ボリュームをコンピュータノードに接続する<<Cloud>>	○
	15.14.2 ボリュームとコンピュータノードの接続を解除する<<Cloud>>	○
	15.15.2 複数のボリュームとコンピュータノードの接続を解除する<<Cloud>>	○
認証チケット	35.1 認証チケットを発行する	
	35.2 認証チケットを破棄する	
暗号化鍵	42.5 暗号化鍵を作成する	
	42.6 暗号化鍵を削除する	
1. 初めてログインする場合、またはパスワードの有効期限が切れている場合のみ可能 2. 通常ボリュームのみ可能 3. ストレージノードの保守閉塞とストレージノードの保守回復のみ可能		

<<Cloud for Google Cloud>>

区分	参照先	GUI 可能操作
ストレージクラスター	<起動・停止・再起動> 33 ストレージクラスターを起動/停止する	
	<ソフトウェアアップデート> 32 ストレージソフトウェアアップデートの要件と手順	
	<ソフトウェアアンインストール> 37 ストレージソフトウェアをアンインストールする	
	<ライセンス> 4 ライセンスを管理する	
ドライブ	9 ドライブを増設する	○
	8.3.2 ドライブを減設する<<Cloud for Google Cloud>>	○
	8.4.3 ドライブを交換する<<Cloud for Google Cloud>>	○
ユーザー/ユーザーグループ	19.4 ユーザーを作成する	
	19.5 ユーザー情報を編集する	
	19.6 ユーザーを削除する	
	19.7 自身のパスワードを変更する	○ ¹
	19.8 ユーザーをユーザーグループに追加する	
	19.9 ユーザーをユーザーグループから削除する	
	19.12 ユーザーグループを作成する	
	19.13 ユーザーグループ情報を編集する	
セッション	20.3 セッションを生成する	
	20.4 セッションを削除する	
コンピュータポート	16.2.2 コンピュータポートの設定を編集する<<Cloud>>	

区分	参照先	GUI 可能操作
ボリューム	17.4.2 ボリュームを作成する<<Cloud>>	○
	17.9 ボリュームの設定を編集する	○ ²
	17.2 ボリュームの容量削減機能の概要	
	17.3 ボリュームの容量削減機能を有効にする	
	17.5 ボリュームを削除する	○
	17.6 ボリュームを拡張する	○
	18.2 スナップショットの取得準備をする	
	18.3 スナップショットを取得する	
	18.4 スナップショットを削除する	○
	18.5.2 スナップショットからボリュームを復元する<<Cloud>>	
	15.12.2 ボリュームをコンピュータノードに接続する<<Cloud>>	○
	15.14.2 ボリュームとコンピュータノードの接続を解除する<<Cloud>>	○
	15.15.2 複数のボリュームとコンピュータノードの接続を解除する<<Cloud>>	
ストレージノード	11.3 ストレージノードの増設<<Cloud for Google Cloud>>	
	12.3 ストレージノードの減設<<Cloud for Google Cloud>>	
	13 ストレージノードを保守する	○ ³
コンピュータノード	15.1 コンピュータノードの情報を登録する	○
	15.4 コンピュータノードの情報を編集する	○
	15.5 コンピュータノードの情報を削除する	○
	15.6 コンピュータノードのイニシエーター情報を登録する	○
	15.8 コンピュータノードのイニシエーター情報を削除する	○
	15.9 コンピュータノードのパス情報を登録する	○
	15.11.2 コンピュータノードのパス情報を削除する<<Cloud>>	
	15.12.2 ボリュームをコンピュータノードに接続する<<Cloud>>	○
	15.14.2 ボリュームとコンピュータノードの接続を解除する<<Cloud>>	○
	15.15.2 複数のボリュームとコンピュータノードの接続を解除する<<Cloud>>	○
認証チケット	35.1 認証チケットを発行する	
	35.2 認証チケットを破棄する	
暗号化鍵	42.5 暗号化鍵を作成する	
	42.6 暗号化鍵を削除する	
1. 初めてログインする場合、またはパスワードの有効期限が切れている場合のみ可能 2. 通常ボリュームのみ可能 3. ストレージノードの保守閉塞とストレージノードの保守回復のみ可能		

<<Cloud for Microsoft Azure>>

区分	参照先	GUI 可能操作
ストレージクラスター	＜起動・停止・再起動＞ 33 ストレージクラスターを起動/停止する	
	＜ソフトウェアアップデート＞ 32 ストレージソフトウェアアップデートの要件と手順	
	＜ソフトウェアアンインストール＞ 37 ストレージソフトウェアをアンインストールする	
	＜ライセンス＞ 4 ライセンスを管理する	
ドライブ	9 ドライブを増設する	○
	8.4.4 ドライブを交換する<<Cloud for Microsoft Azure>>	○
ユーザー/ユーザーグループ	19.4 ユーザーを作成する	
	19.5 ユーザー情報を編集する	
	19.6 ユーザーを削除する	
	19.7 自身のパスワードを変更する	○ ¹
	19.8 ユーザーをユーザーグループに追加する	
	19.9 ユーザーをユーザーグループから削除する	
	19.12 ユーザーグループを作成する	
	19.13 ユーザーグループ情報を編集する	
	19.14 ユーザーグループを削除する	
セッション	20.3 セッションを生成する	
	20.4 セッションを削除する	
コンピュータポート	16.2.2 コンピュータポートの設定を編集する<<Cloud>>	
ボリューム	17.4.2 ボリュームを作成する<<Cloud>>	○
	17.9 ボリュームの設定を編集する	○ ²
	17.2 ボリュームの容量削減機能の概要	
	17.3 ボリュームの容量削減機能を有効にする	
	17.5 ボリュームを削除する	○
	17.6 ボリュームを拡張する	○
	18.2 スナップショットの取得準備をする	
	18.3 スナップショットを取得する	
	18.4 スナップショットを削除する	○
	18.5.2 スナップショットからボリュームを復元する<<Cloud>>	
	15.12.2 ボリュームをコンピュータノードに接続する<<Cloud>>	○
	15.14.2 ボリュームとコンピュータノードの接続を解除する<<Cloud>>	○
	15.15.2 複数のボリュームとコンピュータノードの接続を解除する<<Cloud>>	
ストレージノード	11.4 ストレージノードの増設<<Cloud for Microsoft Azure>>	
	12.4 ストレージノードの減設<<Cloud for Microsoft Azure>>	

区分	参照先	GUI 可能操作
	13 ストレージノードを保守する	○ ³
コンピュータノード	15.1 コンピュータノードの情報を登録する	○
	15.4 コンピュータノードの情報を編集する	○
	15.5 コンピュータノードの情報を削除する	○
	15.6 コンピュータノードのイニシエーター情報を登録する	○
	15.8 コンピュータノードのイニシエーター情報を削除する	○
	15.9 コンピュータノードのパス情報を登録する	○
	15.11.2 コンピュータノードのパス情報を削除する<<Cloud>>	
	15.12.2 ボリュームをコンピュータノードに接続する<<Cloud>>	○
	15.14.2 ボリュームとコンピュータノードの接続を解除する<<Cloud>>	○
	15.15.2 複数のボリュームとコンピュータノードの接続を解除する<<Cloud>>	○
認証チケット	35.1 認証チケットを発行する	
	35.2 認証チケットを破棄する	
暗号化鍵	42.5 暗号化鍵を作成する	
	42.6 暗号化鍵を削除する	
1. 初めてログインする場合、またはパスワードの有効期限が切れている場合のみ可能 2. 通常ボリュームのみ可能 3. ストレージノードの保守閉塞とストレージノードの保守回復のみ可能		

2.8 設定を変更するには

VSP One SDS Block の動作に関する設定内容を変更できます。

<<Bare metal>>

区分	参照先
ログの設定を編集する	6.3.1 イベントログの Syslog 転送設定を編集する<<Bare metal>>
	6.4.1 イベントログの SMTP 転送設定を編集する<<Bare metal>>
	7.3.1 監査ログの Syslog 転送設定を編集する<<Bare metal>>
ライセンスの警告しきい値を編集する	4.5.1 ライセンスの警告しきい値を編集する<<Bare metal>>
時刻設定を確認し必要に応じて変更する	5.1 時刻の同期設定について<<Bare metal>>
容量バランスの設定を変更する	44.3 ストレージクラスターの容量バランスの設定を編集する
	44.5 ストレージコントローラーの容量バランスの設定を編集する

区分	参照先
	44.7 ストレージノードの容量バランスの設定を編集する
ストレージノードの自動回復機能を設定する	13.5.1 ストレージノードの自動回復機能を設定する ≪Bare metal≫
セキュリティ設定を変更する	21.1 ユーザー認証設定を編集する
	23.1 CHAP ユーザーを作成して CHAP 認証を設定する
	23.8 CHAP ユーザーに対してコンピュートポートへのアクセスを許可する
	23.4 CHAP ユーザー情報を編集する
	23.5 CHAP ユーザーを削除する
	23.10 CHAP ユーザーに対してコンピュートポートへのアクセス許可を解除する
	3.6.1 許可リストを設定する ≪Bare metal≫
構成情報を変更する	34 ストレージクラスターの構成情報を変更・設定する ≪Bare metal≫
内部処理 I/O によるストレージノード間ネットワークの利用を制御する	28.3 内部処理 I/O のリソース使用率を変更する
ストレージコントローラーの設定を編集する	29.4 ストレージコントローラーの設定を編集する
ストレージプールの設定を変更する	26.6 ストレージプールの設定を編集する
暗号化環境の設定を編集する	42.2 暗号化環境の設定を編集する
ストレージプールの暗号化の設定を編集する	42.4 ストレージプールの暗号化の設定を編集する

≪Cloud≫

区分	参照先
ログの設定を編集する	6.3.2 イベントログの Syslog 転送設定を編集する ≪Cloud≫
	6.4.2 イベントログの SMTP 転送設定を編集する ≪Cloud≫
	7.3.2 監査ログの Syslog 転送設定を編集する ≪Cloud≫
ライセンスの設定値を編集する	4.5.2 ライセンスの設定値を編集する ≪Cloud≫
容量バランスの設定を変更する	44.3 ストレージクラスターの容量バランスの設定を編集する
	44.5 ストレージコントローラーの容量バランスの設定を編集する
	44.7 ストレージノードの容量バランスの設定を編集する
ストレージノードの自動回復機能を設定する	13.5.2 ストレージノードの自動回復機能を設定する ≪Cloud≫
セキュリティ設定を変更する	21.1 ユーザー認証設定を編集する
	23.1 CHAP ユーザーを作成して CHAP 認証を設定する
	23.8 CHAP ユーザーに対してコンピュートポートへのアクセスを許可する
	23.4 CHAP ユーザー情報を編集する

区分	参照先
	23.5 CHAP ユーザーを削除する
	23.10 CHAP ユーザーに対してコンピュータポートへのアクセス許可を解除する
	3.6.2 許可リストを設定する<<Cloud>>
内部処理 I/O によるストレージノード間ネットワークの利用を制御する	28.3 内部処理 I/O のリソース使用率を変更する
ストレージコントローラーの設定を編集する	29.4 ストレージコントローラーの設定を編集する
ストレージプールの設定を変更する	26.6 ストレージプールの設定を編集する
暗号化環境の設定を編集する	42.2 暗号化環境の設定を編集する
ストレージプールの暗号化の設定を編集する	42.4 ストレージプールの暗号化の設定を編集する

運用環境を構成する

- 3.1 構成ファイルの管理
- 3.2 コントローラーノードの設置と管理操作
- 3.3 コンピュートノードの設置
- 3.4 空状態にあるストレージプールの拡張
- 3.5 ログイン時・CLI Basic 認証時に表示するメッセージを設定する
- 3.6 許可リストの設定

3.1 構成ファイルの管理

保守作業に使用する構成ファイルについて説明します。

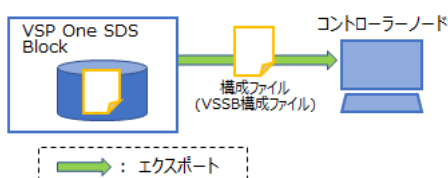
3.1.1 構成ファイルを管理する《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

構成ファイル(VSSB 構成ファイル: SystemConfigurationFile.csv)は、保守作業に使用します。保守作業の実施に当たっては、構成ファイルのエクスポートによって現在の構成情報が記載された構成ファイルを取得し、実施する保守作業に合わせて内容を更新し、保守作業での入力情報として使用します。

保守作業を実施すると、VSP One SDS Block 内部の状態は更新されます。

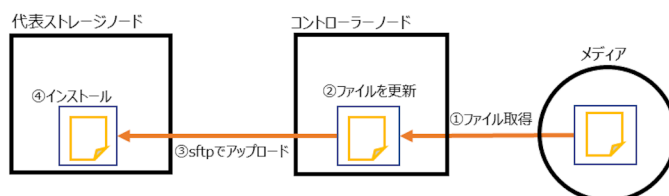
保守作業は構成ファイル(VSSB 構成ファイル)を使用して実現します。保守作業によって更新された構成情報は、VSP One SDS Block に反映され保持されます。



以下に、各操作における構成ファイルの管理概念を示します。

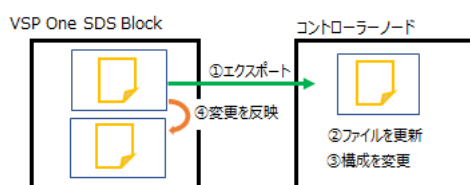
インストール時の管理

製品メディア同梱のテンプレート、またはサポートセンターから入手したテンプレートを基に構成ファイルを作成します。インストール作業の実施によって VSP One SDS Block 内部に構成情報が保持されます。



ストレージノード増設時の管理

ストレージノード増設では、最新の構成情報を VSP One SDS Block から取り出すことから作業を開始します。ストレージノードの増設処理によって、VSP One SDS Block 内部の構成情報が自動的に更新されます。



ストレージノード交換時の管理

構成ファイルに関する操作は不要です。

ドライブ保守時の管理

構成ファイルに関する操作は不要です。

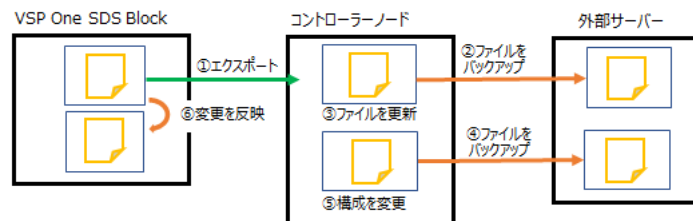
ソフトウェアアップデート時の管理

構成ファイルに関する操作は不要です。

構成情報の変更・設定時の管理

最新の構成情報を VSP One SDS Block から取り出すことから作業を開始します。構成情報の変更・設定処理によって、VSP One SDS Block 内部の情報が自動的に更新されます。

構成情報の変更・設定前後の構成ファイルはトラブルシュートの際に使用しますので、構成情報の変更・設定処理が正常終了するまでは外部サーバーに保存しておきます。



3.1.2 構成ファイルを管理する《Cloud for AWS》

この項での記述内容は Cloud モデル for AWS に適用されます。

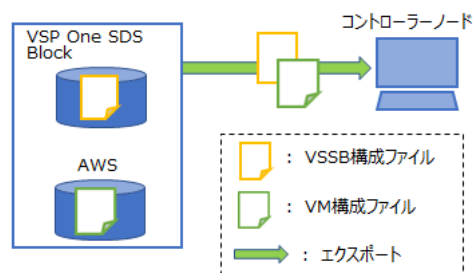
構成ファイルは、保守作業に使用します。保守作業の実施に当たっては、構成ファイルのエクスポートによって現在の構成情報が記載された構成ファイルを取得し、実施する保守作業に合わせて内容を更新し、保守作業での入力情報として使用します。

構成ファイル	
VSSB 構成ファイル	VM 構成ファイル
SystemConfigurationFile.csv	Single-AZ 構成の場合 - VMConfigurationFile.yml - VMConfigurationFile_Duplication.yml* - VMConfigurationFile_4D2P.yml* - VMConfigurationFile_node01.yml - VMConfigurationFile_nodeNN.yml - NetworkResourceConfigurationFile_Duplication.yml* - NetworkResourceConfigurationFile_4D2P.yml* - IamResourceConfigurationFile.yml Multi-AZ 構成の場合 - VMConfigurationFile.yml - VMConfigurationFile_Duplication.yml* - VMConfigurationFile_nodeTB.yml - VMConfigurationFile_nodeNN.yml - NetworkResourceConfigurationFile_Duplication.yml* - IamResourceConfigurationFile.yml

構成ファイル	
VSSB 構成ファイル	VM 構成ファイル
* ユーザーデータの保護方式が Mirroring Duplication の場合は、VMConfigurationFile_Duplication.yml と NetworkResourceConfigurationFile_Duplication.yml を使用します。ユーザーデータの保護方式が HPEC 4D+2P の場合は、VMConfigurationFile_4D2P.yml と NetworkResourceConfigurationFile_4D2P.yml を使用します。	

保守作業を実施すると、VSP One SDS Block 内部の状態は更新されます。

このモデルでは、AWS と連携し保守作業を実現します。保守作業は構成ファイル(VSSB 構成ファイルと VM 構成ファイル)を使用して実施します。保守作業によって更新された構成情報は、AWS と VSP One SDS Block の両方に反映され保持されます。構成ファイルのエクスポートでは AWS と VSP One SDS Block から構成情報を取得します。



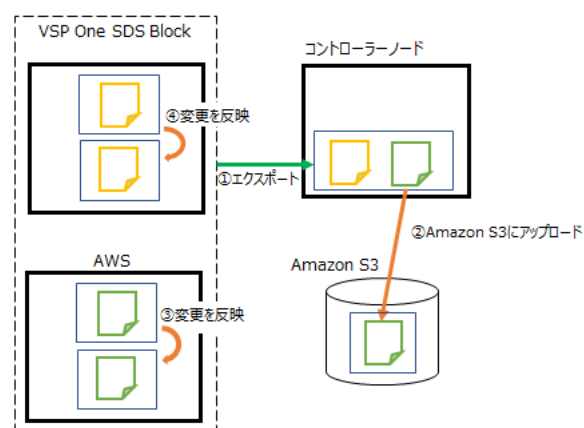
以下に、各操作における構成ファイルの管理概念を示します。

インストール時の管理

インストール時に構成ファイルは使用しません。

ストレージノード増設時の管理

ストレージノード増設処理後の構成情報を VSP One SDS Block から取り出すことから作業を開始します。ストレージノードの増設処理によって、VSP One SDS Block 内部および AWS の構成情報が自動的に更新されます。また、ストレージノードの増設作業時に VM 構成ファイルは Amazon S3 に格納して使用します。

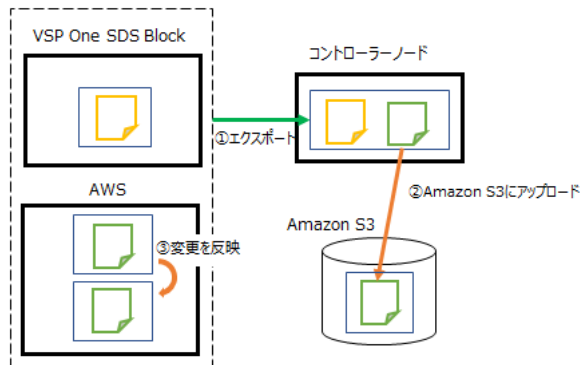


ストレージノード交換時の管理

ストレージノード増設時の場合と同じです。

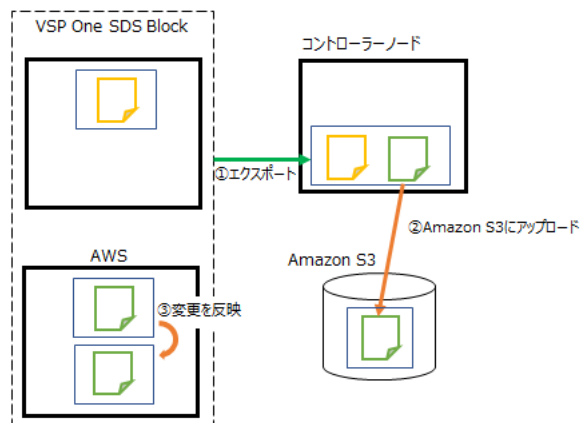
ドライブ保守時の管理

最新の構成情報を VSP One SDS Block から取り出すことから作業を開始します。ドライブの増設処理または交換処理によって、VSP One SDS Block 内部および AWS の構成情報が自動的に更新されます。また、ドライブの増設または交換作業時に VM 構成ファイルは Amazon S3 に格納して使用します。



ソフトウェアアップデート時の管理

ソフトウェアアップデートでは、アップデートを実施したあとに、アップデート後の VM 構成ファイルを AWS に登録する必要があります。そのため、構成ファイルをコントローラーノードにエクスポートし、VM 構成ファイルを AWS のスタックに適用します。



構成情報の変更・設定時の管理

Cloud モデル for AWS では構成情報の変更・設定の機能はサポートしていません。

3.1.3 構成ファイルを管理する《Cloud for Google Cloud》

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

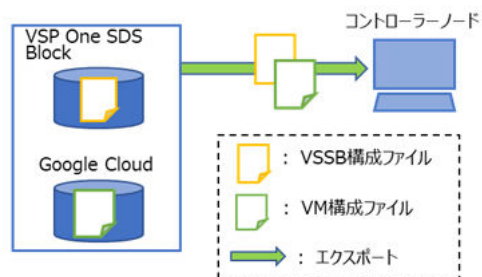
構成ファイル(VM 構成ファイル)は、保守作業に使用します。保守作業の実施に当たっては、構成ファイルのエクスポートによって保守作業の入力となる構成ファイルを取得し、そのまま保守作業の入力情報として使用します。

構成ファイル(VM 構成ファイル)
• main.tf

構成ファイル(VM 構成ファイル)
• variable.tf • backend.auto.tfvars • terraform.tfvars

保守作業を実施すると、VSP One SDS Block 内部の状態は更新されます。

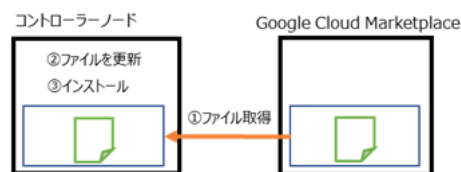
このモデルでは、Google Cloud と連携し保守作業を実現します。保守作業は構成ファイル(VM 構成ファイル)を使用して実施します。保守作業によって更新された構成情報は、Google Cloud と VSP One SDS Block の両方に反映されます。構成ファイルのエクスポートでは Google Cloud と VSP One SDS Block から構成情報を取得します。VSP One SDS Block から取得した構成情報 (VSSB 構成ファイル)は、保守作業に使用しません。



以下に、各操作における構成ファイルの管理概念を示します。

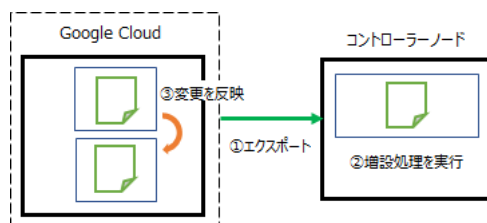
インストール時の管理

Google Cloud Marketplace から入手したテンプレートを基に構成ファイル(VM 構成ファイル)を作成します。インストール作業の実施によって VSP One SDS Block 内部に構成情報が保持されます。



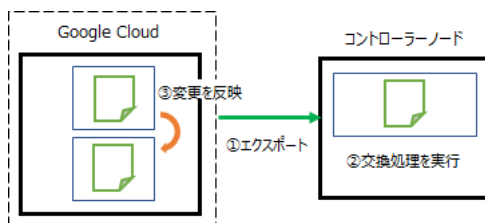
ストレージノード増設時の管理

ストレージノード増設処理用の構成情報を VSP One SDS Block から取り出すことから作業を開始します。ストレージノードの増設処理によって、VSP One SDS Block 内部および Google Cloud の構成情報が自動的に更新されます。



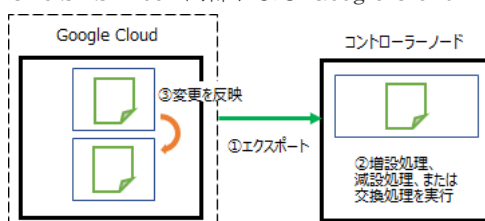
ストレージノード交換時の管理

ストレージノード交換処理用の構成情報を VSP One SDS Block から取り出すことから作業を開始します。ストレージノードの交換処理によって、VSP One SDS Block 内部および Google Cloud の構成情報が自動的に更新されます。



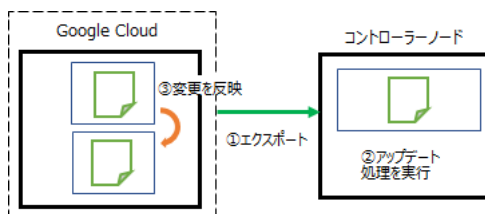
ドライブ保守時の管理

ドライブ増設処理用、減設処理用、または交換処理用の構成情報を VSP One SDS Block から取り出すことから作業を開始します。ドライブの増設処理、減設処理、または交換処理によって、VSP One SDS Block 内部および Google Cloud の構成情報が自動的に更新されます。



ソフトウェアアップデート時の管理

ソフトウェアアップデートでは、アップデートを実施したあとに、アップデート後の VM 構成ファイルを Google Cloud に登録する必要があります。そのため、構成ファイルをコントローラーノードにエクスポートし、VM 構成ファイルを Google Cloud のクラウドリソースに適用します。



構成情報の変更・設定時の管理

Cloud モデル for Google Cloud では構成情報の変更・設定の機能はサポートしていません。

3.1.4 構成ファイルを管理する<<Cloud for Microsoft Azure>>

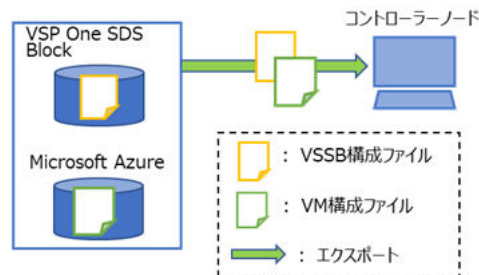
この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

構成ファイル(VM 構成ファイル)は、保守作業に使用します。保守作業の実施に当たっては、構成ファイルのエクスポートによって保守作業の入力となる構成ファイルを取得し、そのまま保守作業の入力情報として使用します。

構成ファイル(VM 構成ファイル)	
• VMConfigurationFile.json • VMConfigurationFile.parameters.json	

保守作業を実施すると、VSP One SDS Block 内部の状態は更新されます。

このモデルでは、Microsoft Azure と連携し保守作業を実現します。保守作業は構成ファイル(VM 構成ファイル)を使用して実施します。保守作業によって更新された構成情報は、Microsoft Azure と VSP One SDS Block の両方に反映されます。構成ファイルのエクスポートでは Microsoft Azure と VSP One SDS Block から構成情報を取得します。VSP One SDS Block から取得した構成情報(VSSB 構成ファイル)は、保守作業に使用しません。



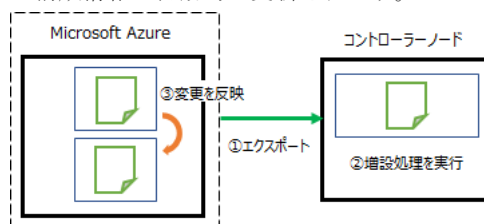
以下に、各操作における構成ファイルの管理概念を示します。

インストール時の管理

インストール時に構成ファイルは使用しません。

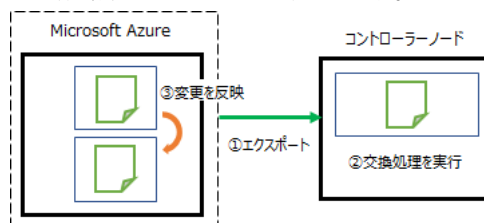
ストレージノード増設時の管理

ストレージノード増設処理用の構成情報を VSP One SDS Block から取り出すことから作業を開始します。ストレージノードの増設処理によって、VSP One SDS Block 内部および Microsoft Azure の構成情報が自動的に更新されます。



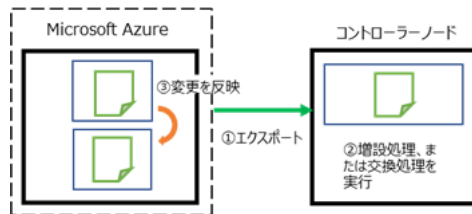
ストレージノード交換時の管理

ストレージノード交換処理用の構成情報を VSP One SDS Block から取り出すことから作業を開始します。ストレージノードの交換処理によって、VSP One SDS Block 内部および Microsoft Azure の構成情報が自動的に更新されます。



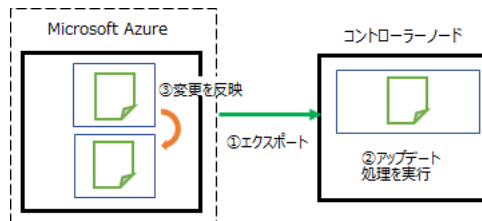
ドライブ保守時の管理

ドライブ増設処理用または交換処理用の構成情報を VSP One SDS Block から取り出します。ドライブの増設処理または交換処理によって、VSP One SDS Block 内部および Microsoft Azure の構成情報が自動的に更新されます。



ソフトウェアアップデート時の管理

ソフトウェアアップデートでは、アップデートを実施したあとに、アップデート後の VM 構成ファイルを Microsoft Azure に登録する必要があります。そのため、構成ファイルをコントローラーノードにエクスポートし、VM 構成ファイルを Microsoft Azure のストレージクラスターを構成するデプロイに適用します。



構成情報の変更・設定時の管理

Cloud モデル for Microsoft Azure では構成情報の変更・設定の機能はサポートしていません。

3.1.5 構成ファイルをエクスポートする《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

保守作業を実施する際には、VSP One SDS Block の現在の構成を構成ファイルとして VSP One SDS Block から取り出す操作を行います。この操作を構成ファイルのエクスポートといいます。

構成ファイルをエクスポートすると、エクスポートコマンドを実行した際のカレントディレクトリに ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz が格納されます。

ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz を解凍することで SystemConfigurationFile.csv を取得できます。

構成ファイルのエクスポートは、コントローラーノードにログインして操作します。



注意

- 構成ファイルのエクスポート実施中は、実施中に構成が変更されないように、最大 5 分、構成変更に関する操作は実行できません。構成変更に関する操作は、構成ファイルのエクスポートが完了するのを待ってから実行してください。
- 構成ファイルは下記の操作によって変更されます。構成ファイルをエクスポートして保守作業を実施する場合は、保守作業の流れの中で、構成ファイルのエクスポートを実施し、最新の状態にしておいてください。なお、下記の操作にかかわらず、構成ファイルは常に最新のものをエクスポートして使用するようにしてください。
 - ストレージノード保守(ストレージノード増設、ストレージノード減設)
 - VSP One SDS Block の構成情報の変更・設定

前提条件

- 実行に必要なロール : Service

- 本機能では、ストレージクラスターの代表 IP アドレスまたはクラスターマスターノード(プライマリ)の管理ネットワーク用の IP アドレスが必要になります。
- 下記の操作を先行して実施している場合、エクスポート操作が先行する操作と競合するためにエラーになることがあります。先行する操作を中断するか、完了するまでお待ちください。
 - ストレージノードの減設
 - ストレージソフトウェアのアップデート
- 下記の処理が動作中の場合は、完了するまでしばらく時間を置いてからエクスポート操作を実施してください。
 - ストレージプールの容量バランス処理
KARS16028-I にて開始、KARS16029-I にて完了を示しています。詳細は「Hitachi Virtual Storage Platform One SDS Block メッセージリファレンス」を参照してください。
 - ドライブデータ再配置処理
KARS07010-I にて開始、KARS07011-I にて完了を示しています。詳細はこのマニュアルの「ドライブデータ再配置の状態を確認する <<Bare metal>>」または「Hitachi Virtual Storage Platform One SDS Block メッセージリファレンス」を参照してください。
 - リビルド処理
KARS07000-I にて開始、KARS07001-I にて完了を示しています。詳細はこのマニュアルの「リビルドの状態を確認する」または「Hitachi Virtual Storage Platform One SDS Block メッセージリファレンス」を参照してください。
- コントローラーノード上に REST API/CLI の使用環境が構築済みであること
コントローラーノードの構築については、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「コントローラーノードを構築する」と「VSP One SDS Block の CLI プログラムをインストールする」を参照してください。
- コントローラーノード上に tar.gz 形式のファイルの解凍に必要なソフトウェアがインストールされていること

操作手順

1. コントローラーノードにログインします。
2. 構成ファイルの作成を行います。
パラメーターを指定せずにコマンドを実行します。
REST API : POST /v1/objects/configuration-file/actions/create/invoke
CLI : configuration_file_create
ジョブが完了するまで最大で約 5 分掛かります。
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの ID を指定してジョブの state を確認します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
4. 作成した構成ファイルをダウンロードします。
REST API : GET /v1/objects/configuration-file/download
CLI : configuration_file_download



注意

以下の外部要因によって構成ファイルのダウンロードに掛かる時間が長くなることがあります。
ダウンロードに掛かる時間が長い場合は、これらの項目に問題がないことを確認してください。

- ・ ネットワークの通信状況(コントローラーノードとストレージノード間の通信状況)
- ・ サーバーの性能状況(ストレージノードの温度上昇による性能低下など)

5. 取得した `ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` を解凍し、以下のファイルが含まれていることを確認します。

- ・ VSSB 構成ファイル(SystemConfigurationFile.csv)



注意

構成ファイルを解凍する際、解凍先のディレクトリーに既存の VSSB 構成ファイルが存在すると、既存の VSSB 構成ファイルが上書きされてしまう可能性があります。意図しない上書きを防ぐには、既存の VSSB 構成ファイルが存在するディレクトリーではなく、別のディレクトリーに構成ファイルを解凍してください。また、解凍する際に `tar` コマンドを使用する場合、`tar` コマンドに `--keep-old-files` や `--skip-old-files` 等のオプションを指定することで意図しない上書きを防ぐことができます。

以上でエクスポートの手順は完了です。



メモ

エクスポートされた VSSB 構成ファイル(SystemConfigurationFile.csv)のファイル末尾には改行コードはありません。

3.1.6 構成ファイルをエクスポートする《Cloud for AWS》

この項での記述内容は Cloud モデル for AWS に適用されます。

保守作業を実施する際には、VSP One SDS Block の現在または保守作業後の構成を構成ファイルとして VSP One SDS Block から取り出す操作を行います。この操作を、構成ファイルのエクスポートといいます。

構成ファイルをエクスポートすると、エクスポートコマンドを実行した際のカレントディレクトリーに `ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` が格納されます。

`ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` を解凍すると、以下のファイルが取り出されます。

Single-AZ 構成の場合

- ・ SystemConfigurationFile.csv
- ・ VMConfigurationFile.yml
- ・ VMConfigurationFile_Duplication.yml*
- ・ VMConfigurationFile_4D2P.yml*
- ・ IamResourceConfigurationFile.yml
- ・ NetworkResourceConfigurationFile_Duplication.yml*
- ・ NetworkResourceConfigurationFile_4D2P.yml*
- ・ VMConfigurationFile_node01.yml
- ・ VMConfigurationFile_nodeNN.yml

Multi-AZ 構成の場合

- ・ SystemConfigurationFile.csv
- ・ VMConfigurationFile.yml

- VMConfigurationFile_Duplication.yml
- IamResourceConfigurationFile.yml
- NetworkResourceConfigurationFile_Duplication.yml
- VMConfigurationFile_nodeTB.yml
- VMConfigurationFile_nodeNN.yml

* 4つのファイルのうちユーザーデータの保護方式が **Mirroring Duplication** の場合は VMConfigurationFile_Duplication.yml と NetworkResourceConfigurationFile_Duplication.yml が取り出せます。ユーザーデータの保護方式が **HPEC 4D+2P** の場合は VMConfigurationFile_4D2P.yml と NetworkResourceConfigurationFile_4D2P.yml が取り出せます。

構成ファイルのエクスポートは、コントローラーノードにログインして操作します。



注意

- 構成ファイルのエクスポート実施中は、実施中に構成が変更されないように、最大 5 分、構成情報に関する操作は実行できません。構成変更に関する操作は、構成ファイルのエクスポートが完了するのを待ってから実行してください。
- 構成ファイルは下記の操作によって変更されます。構成ファイルをエクスポートして保守操作を実施する場合は、保守作業の流れの中で、構成ファイルのエクスポートを実施し、最新の状態にしておいてください。なお、下記の操作にかかわらず、構成ファイルは常に最新のものをエクスポートして使用するようになっています。
 - ストレージノード保守(ストレージノード増設、ストレージノード減設、ストレージノード交換)
 - ドライブ保守(ドライブ増設、ドライブ交換)
- エクスポートは、コマンドを実行したディレクトリーに構成ファイルを出力するため、実行ディレクトリーに対して実行ユーザーの **Write** 権限が付与されていない場合はファイルが書き込めず失敗します。そのため、実行ディレクトリーに実行ユーザーの **Write** 権限を付与するか、実行ユーザーの **Write** 権限があるディレクトリーで実行してください。
- 構成ファイルのエクスポートで出力された構成ファイルは編集しないでください。編集した場合、予期しないエラーが発生するおそれがあります。オプションで指定する値を間違えた場合は、正しい値を指定して構成ファイルのエクスポートを再度実行し、最新の構成ファイルを取得しなおしてください。
- 保守作業の中で構成ファイルをエクスポートする際、必ず各保守作業の手順に従って構成ファイルをエクスポートしてください。前の手順が完了する前に構成ファイルをエクスポートするなど手順と異なる順番で実施すると、内容が正しくない構成ファイルがエクスポートされることがあります。これらを使用して保守作業を継続した場合、予期しないエラーが発生したり、保守作業の結果が不正となったりするおそれがあります。
上記の要因で保守作業の結果が不正となった場合は、すべてのストレージノードに対しダンプログファイルを採取し、サポートセンターに連絡してください。

前提条件

- 実行に必要なロール : **Service**
- 本機能では、ロードバランサーの IP アドレスまたはクラスターマスターノード(プライマリー)の管理ネットワーク用の IP アドレスが必要になります。
- 下記の操作を先行して実施している場合、エクスポート操作が先行する操作と競合するためにエラーになることがあります。先行する操作を中断するか、完了するまでお待ちください。
 - ストレージノードの減設
 - ストレージソフトウェアのアップデート
- 下記の処理が動作中の場合は、完了するまでしばらく時間を置いてからエクスポート操作を実施してください。

- ・ ストレージプールの容量バランス処理
KARS16028-I にて開始、KARS16029-I にて完了を示しています。詳細は「Hitachi Virtual Storage Platform One SDS Block メッセージリファレンス」を参照してください。
- ・ リビルド処理
KARS07000-I にて開始、KARS07001-I にて完了を示しています。詳細はこのマニュアルの「リビルドの状態を確認する」または「Hitachi Virtual Storage Platform One SDS Block メッセージリファレンス」を参照してください。
- ・ コントローラーノード上に REST API/CLI の使用環境が構築済みであること
コントローラーノードの構築については、Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「コントローラーノードを構築する」と「VSP One SDS Block の CLI プログラムをインストールする」を参照してください。
- ・ コントローラーノード上に tar.gz 形式のファイルの解凍に必要なソフトウェアがインストールされていること

操作手順

1. コントローラーノードにログインします。
2. エクスポートする VM 構成ファイルを格納するため、Amazon S3 バケットにフォルダーを作成します。



注意

VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。

既存のフォルダーを使用する場合は、フォルダーの作成は不要です。

以降の手順で使用するため、AWS マネジメントコンソールから Amazon S3 バケットのフォルダーを選択して Amazon S3 バケットの URL(https)をコピーし、記録しておきます。

3. 構成ファイルを作成します。

クラスターマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。コマンド実行時には、手順 2 で記録した Amazon S3 バケットの URL(https)を `templateS3Url` パラメーターに指定してください。

ジョブが完了するまで最大で約 5 分掛かります。

REST API : `POST /v1/objects/configuration-file/actions/create/invoke`

CLI : `configuration_file_create`

コマンド実行後に表示されるジョブの ID を確認します。



メモ

AMI ID を指定して構成ファイルの作成を行う場合は、以下の AWS CLI コマンドを実行することで、事前に AMI ID の存在を確認できます。

```
aws ec2 describe-images --image-ids <指定する AMI ID>
```

4. ジョブの ID を指定してジョブの state を確認します。

REST API : `GET /v1/objects/jobs/<jobId>`

CLI : `job_show`

state が "Succeeded" になっていたらジョブは完了です。

5. 作成した構成ファイルをダウンロードします。

クラスターマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。

REST API : `GET /v1/objects/configuration-file/download`

CLI : `configuration_file_download`



注意

以下の外部要因によって構成ファイルのダウンロードに掛かる時間が長くなることがあります。ダウンロードに掛かる時間が長い場合は、これらの項目に問題がないことを確認してください。

- AWS の負荷状況
- ネットワークの通信状況(コントローラーノード、ストレージノード、AWS との相互間の通信状況)
- EC2 インスタンスの性能状況

6. 取得した ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz を解凍し、以下のファイルが含まれていることを確認します。

```
tar -xzf ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz
```

Single-AZ 構成の場合

- VSSB 構成ファイル
 - SystemConfigurationFile.csv
- VM 構成ファイル
 - VMConfigurationFile.yml
 - VMConfigurationFile_Duplication.yml*
 - VMConfigurationFile_4D2P.yml*
 - IamResourceConfigurationFile.yml
 - NetworkResourceConfigurationFile_Duplication.yml*
 - NetworkResourceConfigurationFile_4D2P.yml*
 - VMConfigurationFile_node01.yml
 - VMConfigurationFile_nodeNN.yml

Multi-AZ 構成の場合

- VSSB 構成ファイル
 - SystemConfigurationFile.csv
- VM 構成ファイル
 - VMConfigurationFile.yml
 - VMConfigurationFile_Duplication.yml
 - IamResourceConfigurationFile.yml
 - NetworkResourceConfigurationFile_Duplication.yml
 - VMConfigurationFile_nodeTB.yml
 - VMConfigurationFile_nodeNN.yml

* 4 つのファイルのうちユーザーデータの保護方式が Mirroring Duplication の場合は VMConfigurationFile_Duplication.yml と

NetworkResourceConfigurationFile_Duplication.yml が含まれていることを確認します。ユーザーデータの保護方式が HPEC 4D+2P の場合は VMConfigurationFile_4D2P.yml と NetworkResourceConfigurationFile_4D2P.yml が取り出せます。



注意

構成ファイルを解凍する際、解凍先のディレクトリーに既存の構成ファイルが存在すると、既存の構成ファイルが上書きされてしまう可能性があります。意図しない上書きを防ぐには、既存の構成ファイルが存在するディレクトリーではなく、別のディレクトリーに構成ファイルを解凍してください。また、解凍する際に `tar` コマンドを使用する場合、`tar` コマンドに`"--keep-old-files"`や`"--skip-old-files"`等のオプションを指定することで意図しない上書きを防ぐことができます。

以上でエクスポートの手順は完了です。

3.1.7 構成ファイルをエクスポートする《Cloud for Google Cloud》

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

保守作業を実施する際には、VSP One SDS Block の現在または保守作業用の構成を構成ファイルとして VSP One SDS Block から取り出す操作を行います。この操作を、構成ファイルのエクスポートといいます。

構成ファイルをエクスポートすると、エクスポートコマンドを実行した際のカレントディレクトリーに `ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` が格納されます。`ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` を解凍すると、以下のファイルが取り出されます。

- `SystemConfigurationFile.csv`*
- `main.tf`
- `variable.tf`
- `backend.auto.tfvars`
- `terraform.tfvars`

* 保守作業では、`SystemConfigurationFile.csv` は使用しません。

構成ファイルのエクスポートは、コントローラーノードにログインして操作します。



注意

- 構成ファイルのエクスポート実施中は、実施中に構成が変更されないように、最大 5 分、構成変更に関する操作は実行できません。構成変更に関する操作は、構成ファイルのエクスポートが完了するのを待ってから実行してください。
- 構成ファイルは下記の操作によって変更されます。構成ファイルをエクスポートして保守操作を実施する場合は、保守作業の流れの中で、構成ファイルのエクスポートを実施し、最新の状態にしておいてください。なお、下記の操作にかかわらず、構成ファイルは常に最新のものをエクスポートして使用するようにしてください。
 - ストレージノード保守(ストレージノード増設、ストレージノード減設、ストレージノード交換)
 - ドライブ保守(ドライブ増設、ドライブ減設、ドライブ交換)
- 構成ファイルのエクスポートで出力された構成ファイルは、マニュアルによる指示がない限り編集しないでください。編集した場合、予期しないエラーが発生するおそれがあります。パラメーターで指定する値を間違えた場合は、正しい値を指定して構成ファイルのエクスポートを再度実行し、最新の構成ファイルを取得しなおしてください。
- 保守作業の中で構成ファイルをエクスポートする際、必ず各保守作業の手順に従って構成ファイルをエクスポートしてください。前の手順が完了する前に構成ファイルをエクスポートするなど手順と異なる順番で実施すると、内容が正しくない構成ファイルがエクスポートされることがあります。これらを使用して保守作業を継続した場合、予期しないエラーが発生したり、保守作業の結果が不正となったりするおそれがあります。
上記の要因で保守作業の結果が不正となった場合は、すべてのストレージノードに対しダンプログファイルを採取し、サポートセンターに連絡してください。

前提条件

- 実行に必要なロール : Service
- 本機能では、ロードバランサーの IP アドレスまたはクラスターマスターノード(プライマリー)の管理ネットワーク用の IP アドレスが必要になります。
- 下記の操作を先行して実施している場合、エクスポート操作が先行する操作と競合するためにエラーになることがあります。先行する操作を中断するか、完了するまでお待ちください。
 - ストレージノードの増設
 - ストレージノードの減設
 - ストレージノードの交換
 - ストレージノードの保守回復
 - ストレージソフトウェアのアップデート
- 下記の処理が動作中の場合は、完了するまでしばらく時間を置いてからエクスポート操作を実施してください。
 - ストレージプールの容量バランス処理
KARS16028-I にて開始、KARS16029-I にて完了を示しています。詳細は「Hitachi Virtual Storage Platform One SDS Block メッセージリファレンス」を参照してください。
 - リビルド処理
KARS07000-I にて開始、KARS07001-I にて完了を示しています。詳細はこのマニュアルの「リビルドの状態を確認する」または「Hitachi Virtual Storage Platform One SDS Block メッセージリファレンス」を参照してください。
- コントローラーノード上に REST API/CLI の使用環境が構築済みであること
- コントローラーノード上に tar.gz 形式のファイルの解凍に必要なソフトウェアがインストールされていること

操作手順

1. コントローラーノードにログインします。
2. 構成ファイルを作成します。

クラスターマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。
ジョブが完了するまで最大で約 5 分掛かります。

REST API : POST /v1/objects/configuration-file/actions/create/invoke

CLI : configuration_file_create

コマンド実行後に表示されるジョブの ID を確認します。



メモ

ジョブが完了した際にイベントログの追加情報が Cloud Storage にアップロードされることがあります。イベントログのアクションで "Error message file" の参照が指示されている場合、メッセージに記載されている Error Message File のパスを基に追加情報を Cloud Storage から取得してください。

アップロード先の Cloud Storage のディレクトリーは、ストレージクラスター構築の際に terraform.tfvars ファイルの gsUri で指定したディレクトリーです。

gsUri の情報は terraform output で gsUri のキーを確認してください。

terraform output

3. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4. 作成した構成ファイルをダウンロードします。

クラスターマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。

REST API : GET /v1/objects/configuration-file/download

CLI : configuration_file_download



注意

以下の外部要因によって構成ファイルのダウンロードに掛かる時間が長くなることがあります。ダウンロードに掛かる時間が長い場合は、これらの項目に問題がないことを確認してください。

- Google Cloud の負荷状況
- ネットワークの通信状況(コントローラーノード、ストレージノード、Google Cloud との相互間の通信状況)
- Compute Engine インスタンスの性能状況

5. 取得した ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz を解凍し、以下のファイルが含まれていることを確認します。

```
tar -xzf ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz
```

- VSSB 構成ファイル
 - SystemConfigurationFile.csv
- VM 構成ファイル
 - main.tf
 - variable.tf
 - backend.auto.tfvars
 - terraform.tfvars



注意

構成ファイルを解凍する際、解凍先のディレクトリーに既存の構成ファイルが存在すると、既存の構成ファイルが上書きされてしまう可能性があります。意図しない上書きを防ぐには、既存の構成ファイルが存在するディレクトリーではなく、別のディレクトリーに構成ファイルを解凍してください。また、解凍する際に tar コマンドを使用する場合、tar コマンドに"--keep-old-files"や"--skip-old-files"等のオプションを指定することで意図しない上書きを防ぐことができます。

以上でエクスポートの手順は完了です。

3.1.8 構成ファイルをエクスポートする<<Cloud for Microsoft Azure>>

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

保守作業を実施する際には、VSP One SDS Block の現在または保守作業用の構成を構成ファイルとして VSP One SDS Block から取り出す操作を行います。この操作を、構成ファイルのエクスポートといいます。

構成ファイルをエクスポートすると、エクスポートコマンドを実行した際のカレントディレクトリーに ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz が格納されます。

ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz を解凍すると、以下のファイルが取り出されます。

- SystemConfigurationFile.csv*
- VMConfigurationFile.json
- VMConfigurationFile.parameters.json
- Checksum*

* 保守作業では、SystemConfigurationFile.csv および Checksum は使用しません。

構成ファイルのエクスポートは、コントローラーノードにログインして操作します。



注意

- 構成ファイルのエクスポート実施中は、実施中に構成が変更されないように、最大 5 分、構成変更に関する操作は実行できません。構成変更に関する操作は、構成ファイルのエクスポートが完了するのを待ってから実行してください。
- 構成ファイルは下記の操作によって変更されます。構成ファイルをエクスポートして保守操作を実施する場合は、保守作業の流れの中で、構成ファイルのエクスポートを実施し、最新の状態にしておいてください。なお、下記の操作にかかわらず、構成ファイルは常に最新のものをエクスポートして使用するようになっています。
 - ストレージノード保守(ストレージノード増設、ストレージノード減設、ストレージノード交換)
 - ドライブ保守(ドライブ増設、ドライブ減設、ドライブ交換)
- 構成ファイルのエクスポートで出力された構成ファイルは、マニュアルによる指示がない限り編集しないでください。また、ストレージノードの増設や交換のためにエクスポートを行った場合は、ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz の解凍も行わないでください。解凍/編集した場合、予期しないエラーが発生するおそれがあります。パラメーターで指定する値を間違えた場合は、正しい値を指定して構成ファイルのエクスポートを再度実行し、最新の構成ファイルを取得しなおしてください。
- 保守作業の中で構成ファイルをエクスポートする際、必ず各保守作業の手順に従って構成ファイルをエクスポートしてください。前の手順が完了する前に構成ファイルをエクスポートするなど手順と異なる順番で実施すると、内容が正しくない構成ファイルがエクスポートされることがあります。これらを使用して保守作業を継続した場合、予期しないエラーが発生したり、保守作業の結果が不正となったりするおそれがあります。
上記の要因で保守作業の結果が不正となった場合は、すべてのストレージノードに対しダンプログファイルを採取し、サポートセンターに連絡してください。

前提条件

- 実行に必要なロール : Service
- 本機能では、ロードバランサーの IP アドレスまたはクラスターマスターノード(プライマリー)の管理ネットワーク用の IP アドレスが必要になります。
- 下記の操作を先行して実施している場合、エクスポート操作が先行する操作と競合するためにエラーになることがあります。先行する操作を中断するか、完了するまでお待ちください。
 - ストレージノードの増設
 - ストレージノードの減設
 - ストレージノードの交換
 - ストレージノードの保守回復
 - ストレージソフトウェアのアップデート
- 下記の処理が動作中の場合は、完了するまでしばらく時間を置いてからエクスポート操作を実施してください。
 - ストレージプールの容量バランス処理
KARS16028-I にて開始、KARS16029-I にて完了を示しています。詳細は「Hitachi Virtual Storage Platform One SDS Block メッセージリファレンス」を参照してください。

- リビルド処理
 KARS07000-Iにて開始、KARS07001-Iにて完了を示しています。詳細はこのマニュアルの「リビルドの状態を確認する」または「Hitachi Virtual Storage Platform One SDS Block メッセージリファレンス」を参照してください。
- コントローラーノード上に REST API/CLI の使用環境が構築済みであること
- コントローラーノード上に tar.gz 形式のファイルの解凍に必要なソフトウェアがインストールされていること

操作手順

1. コントローラーノードにログインします。
2. 構成ファイルを作成します。
 クラスタマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。
 ジョブが完了するまで最大で約 5 分掛かります。
 REST API : POST /v1/objects/configuration-file/actions/create/invoke
 CLI : configuration_file_create
 コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの ID を指定してジョブの state を確認します。
 REST API : GET /v1/objects/jobs/<jobId >
 CLI : job_show
 state が"Succeeded"になっていたらジョブは完了です。
4. 作成した構成ファイルをダウンロードします。
 クラスタマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。
 REST API : GET /v1/objects/configuration-file/download
 CLI : configuration_file_download



注意

以下の外部要因によって構成ファイルのダウンロードに掛かる時間が長くなることがあります。
 ダウンロードに掛かる時間が長い場合は、これらの項目に問題がないことを確認してください。

- Microsoft Azure の負荷状況
- ネットワークの通信状況(コントローラーノード、ストレージノード、Microsoft Azure との相互間の通信状況)
- Azure VM インスタンスの性能状況

5. 取得した ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz を解凍し、以下のファイルが含まれていることを確認します。

```
tar -xzf ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz
```

- VSSB 構成ファイル
 - SystemConfigurationFile.csv
- VM 構成ファイル
 - VMConfigurationFile.json
 - VMConfigurationFile.parameters.json
- その他のファイル
 - Checksum



注意

構成ファイルを解凍する際、解凍先のディレクトリーに既存の構成ファイルが存在すると、既存の構成ファイルが上書きされてしまう可能性があります。意図しない上書きを防ぐには、既存の構成ファイルが存在するディレクトリーではなく、別のディレクトリーに構成ファイルを解凍してください。また、解凍する際に `tar` コマンドを使用する場合、`tar` コマンドに `"--keep-old-files"` や `"--skip-old-files"` 等のオプションを指定することで意図しない上書きを防ぐことができます。

以上でエクスポートの手順は完了です。

3.1.9 VM 構成ファイルを Terraform の作業ディレクトリーへ配置する 《Cloud for Google Cloud》

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

Terraform の各コマンドを実行するために、構成ファイルのエクスポートによって取得した VM 構成ファイルを Terraform の作業ディレクトリーへ配置します。

Terraform の作業ディレクトリーとは `terraform` のコマンドを実行するディレクトリーを指します。作業ディレクトリーには `terraform` の構成ファイル (VM 構成ファイル) やパッケージ等が格納されます。任意のディレクトリーを作業ディレクトリーとすることが可能です。ただし、既存の Terraform の作業ディレクトリー以外を作業ディレクトリーにすると、`terraform` 実行前の初期化によって新しくパッケージがインストールされるので、容量に注意してください。

前提条件

- 構成ファイルのエクスポートを実行して
`ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` を取得していること

操作手順

1. Terraform の作業ディレクトリーへ移動します。

```
cd <Terraform の作業ディレクトリー>
```



メモ

ここで移動する作業ディレクトリーはまだ作業ディレクトリーとして使用していない新規のディレクトリーでも問題ありません。

2. `ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` を解凍し、取得した以下のファイルを Terraform の作業ディレクトリーに配置します。

```
tar xzvf <ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz へのパス>
```

- VSSB 構成ファイル
 - `SystemConfigurationFile.csv`
- VM 構成ファイル
 - `main.tf`
 - `variable.tf`
 - `backend.auto.tfvars`
 - `terraform.tfvars`



注意

すでに作業ディレクトリーとして使用しているディレクトリーを作業ディレクトリーとして使用する場合、既存の構成ファイルが上書きされてしまう可能性があります。解凍する際に、tar コマンドに"--keep-old-files"や"--skip-old-files"などのオプションを指定することで意図しない上書きを防ぐことができます。

3. Terraform の作業ディレクトリーの初期化を行います。

```
terraform init -backend-config="backend.auto.tfvars"
```

以下のメッセージが出力されることを確認してください。

```
Terraform has been successfully initialized!
```



メモ

すでに作業ディレクトリーとして使用しているディレクトリーを作業ディレクトリーとして使用する場合、本手順はスキップできます。

4. VSP One SDS Block のクラウドリソースを Terraform が認識していることを確認します。

```
terraform show
```

VSP One SDS Block を構成するクラウドリソースが表示されることを確認してください。



メモ

VSP One SDS Block を構成するクラウドリソースは、リソース名のプレフィックスにストレージクラスター名がついています。

3.2 コントローラーノードの設置と管理操作

VSP One SDS Block の構築と管理をするためのコントローラーノードについて説明します。

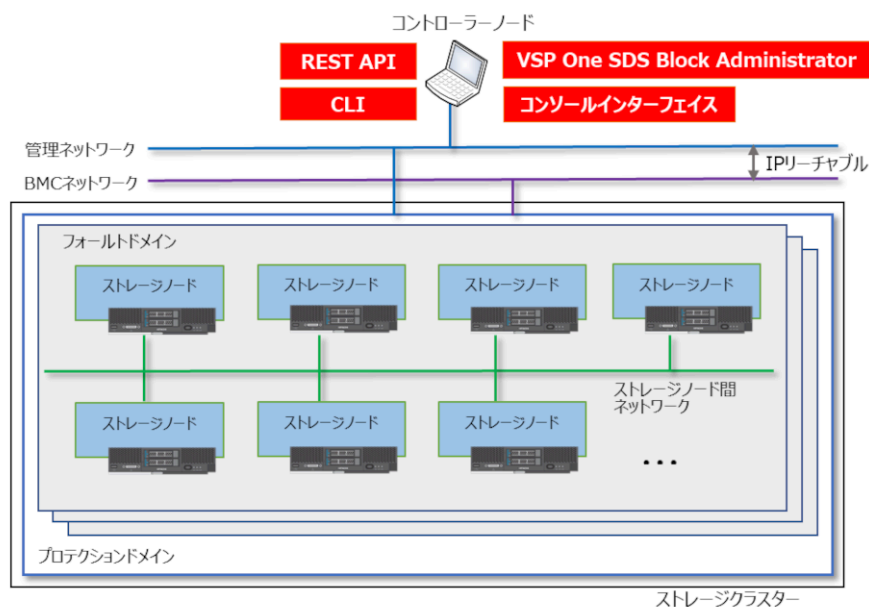
3.2.1 コントローラーノードの設置<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

コントローラーノードは、VSP One SDS Block の構築と管理をするためのノードです。以下の操作をするために必要です。

- REST API 操作
- CLI 操作
- VSP One SDS Block Administrator 操作
- コンソールインターフェイス操作

コントローラーノードは複数台設置できます。不正な管理操作を防ぐために、コントローラーノードの IP アドレスまたは IP アドレスの範囲(CIDR 表記)を許可リストに設定できます。詳しくは「許可リストを設定する」を参照してください。



REST API、CLI は、コントローラーノードの OS が Windows であればコマンドプロンプト、Linux であればターミナル端末などのコマンド実行が可能なコンソールから実行します。



メモ

- REST API と CLI での時刻指定と時刻表示は、すべて UTC になります。
- I/O 高負荷時は、REST API の応答、ジョブの処理時間、VSP One SDS Block Administrator 操作などの管理操作において、I/O 低負荷時に比べて時間を要することがあります。
- REST API や CLI コマンド、VSP One SDS Block Administrator 操作を同時に複数実行すると、1 つのみ実行したときと比較して応答に時間を要したり、KARS15020-E、KARS15588-E が返されたりすることがあります。KARS15020-E、KARS15588-E が返された場合は、時間を置いてから同じ操作を再度実行してください。
- ボリューム情報の一覧を取得するといった、複数リソースについて応答する REST API や VSP One SDS Block Administrator 操作などの管理操作において、対象のリソース数が多くなると、少ないときに比べて応答に時間を多く要することがあります。

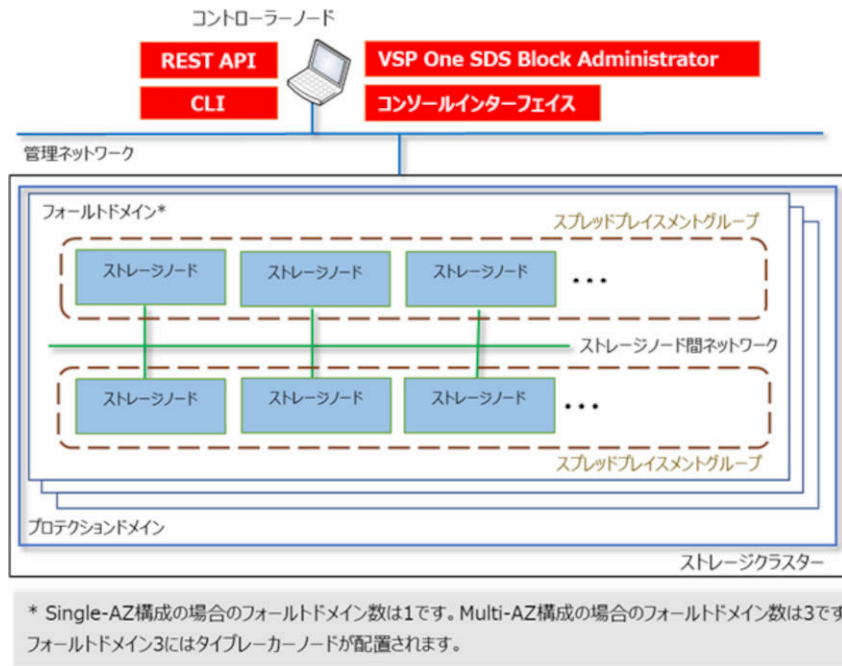
3.2.2 コントローラーノードの設置<<Cloud for AWS>>

この項での記述内容は Cloud モデル for AWS に適用されます。

コントローラーノードは、VSP One SDS Block の構築と管理をするためのノードです。以下の操作をするために必要です。

- REST API 操作
- CLI 操作
- VSP One SDS Block Administrator 操作
- コンソールインターフェイス操作

コントローラーノードは複数台設置できます。不正な管理操作を防ぐために、コントローラーノードの IP アドレスまたは IP アドレスの範囲(CIDR 表記)を許可リストに設定できます。詳しくは「許可リストを設定する」を参照してください。



ヒント

スプレッドプレイスメントグループについては、Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ユーザーデータおよび管理機能の耐障害性に関する設定(Single-AZ 構成)」または「ユーザーデータおよび管理機能の耐障害性に関する設定(Multi-AZ 構成)」を参照してください。

REST API を操作する curl などや CLI は、コントローラーノードの OS が Windows であればコマンドプロンプト、Linux であればターミナル端末などのコマンド実行が可能なコンソールから実行します。



メモ

- REST API と CLI での時刻指定と時刻表示は、すべて UTC になります。
- I/O 高負荷時は、REST API の応答、ジョブの処理時間、VSP One SDS Block Administrator 操作などの管理操作において、I/O 低負荷時に比べて時間を要することがあります。
- REST API や CLI コマンド、VSP One SDS Block Administrator 操作を同時に複数実行すると、1 つのみ実行したときと比較して応答に時間を要したり、KARS15020-E、KARS15588-E が返されたりすることがあります。KARS15020-E、KARS15588-E が返された場合は、時間を置いてから同じ操作を再度実行してください。
- ボリューム情報の一覧を取得するといった、複数リソースについて応答する REST API や VSP One SDS Block Administrator 操作などの管理操作において、対象のリソース数が多くなると、少ないときに比べて応答に時間を多く要することがあります。

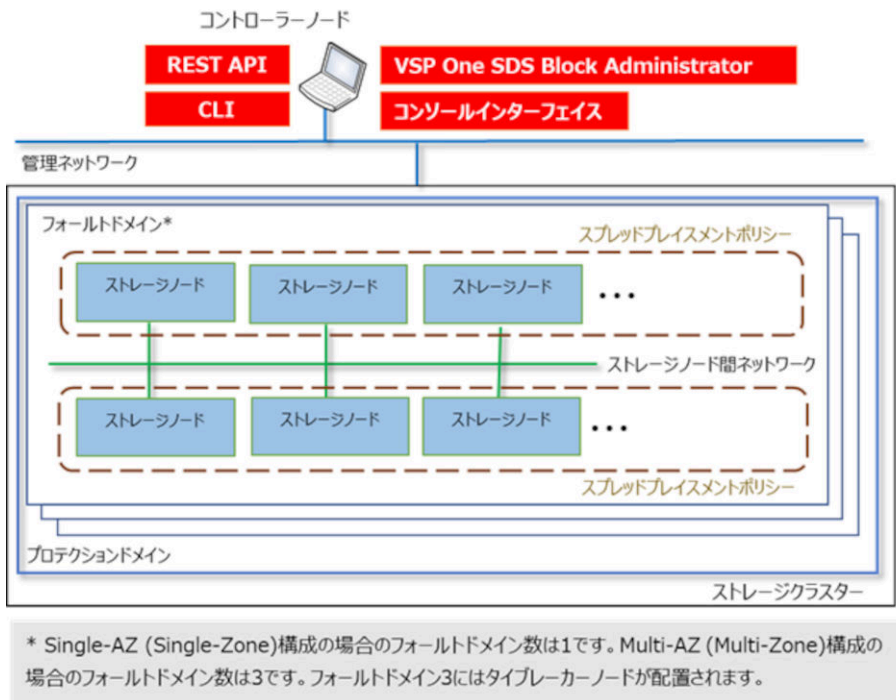
3.2.3 コントローラーノードの設置<<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

コントローラーノードは、VSP One SDS Block の構築と管理をするためのノードです。以下の操作をするために必要です。

- REST API 操作
- CLI 操作
- VSP One SDS Block Administrator 操作
- コンソールインターフェイス操作

コントローラーノードは複数台設置できます。不正な管理操作を防ぐために、コントローラーノードの IP アドレスまたは IP アドレスの範囲(CIDR 表記)を許可リストに設定できます。詳しくは「許可リストを設定する」を参照してください。



ヒント

スプレッドプレースメントポリシーについては、Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ユーザーデータおよび管理機能の耐障害性に関する設定 (Single-Zone 構成)」または「ユーザーデータおよび管理機能の耐障害性に関する設定 (Multi-Zone 構成)」を参照してください。

REST API を操作する curl などや CLI は、コントローラーノードの OS が Windows であればコマンドプロンプト、Linux であればターミナル端末などのコマンド実行が可能なコンソールから実行します。



メモ

- REST API と CLI での時刻指定と時刻表示は、すべて UTC になります。
- I/O 高負荷時は、REST API の応答、ジョブの処理時間、VSP One SDS Block Administrator 操作などの管理操作において、I/O 低負荷時に比べて時間を要することがあります。
- REST API や CLI コマンド、VSP One SDS Block Administrator 操作を同時に複数実行すると、1 つのみ実行したときと比較して応答に時間を要したり、KARS15020-E、KARS15588-E が返されたりすることがあります。KARS15020-E、KARS15588-E が返された場合は、時間を置いてから同じ操作を再度実行してください。
- ボリューム情報の一覧を取得するといった、複数リソースについて応答する REST API や VSP One SDS Block Administrator 操作などの管理操作において、対象のリソース数が多くなると、少ないときに比べて応答に時間を多く要することがあります。

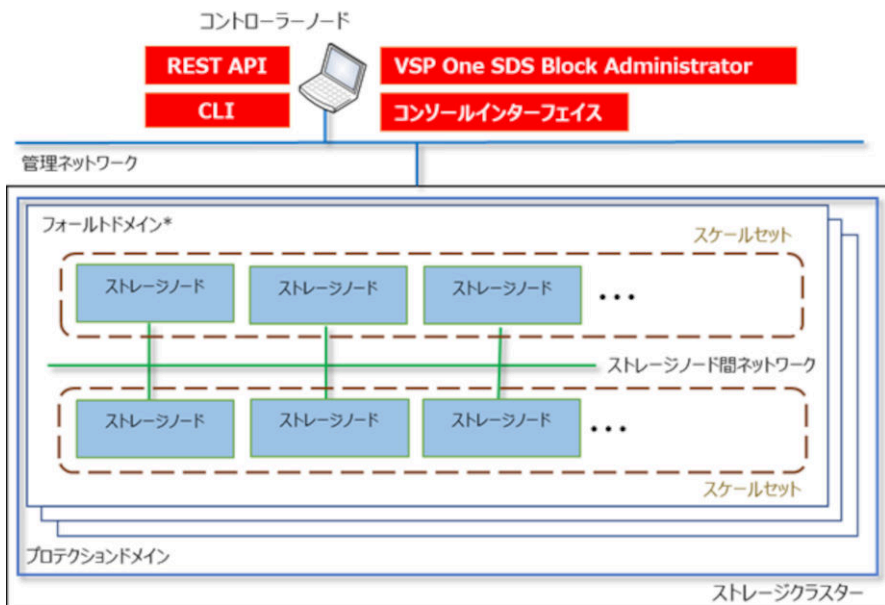
3.2.4 コントローラーノードの設置《Cloud for Microsoft Azure》

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

コントローラーノードは、VSP One SDS Block の構築と管理をするためのノードです。以下の操作をするために必要です。

- REST API 操作
- CLI 操作
- VSP One SDS Block Administrator 操作
- コンソールインターフェイス操作

コントローラーノードは複数台設置できます。不正な管理操作を防ぐために、コントローラーノードの IP アドレスまたは IP アドレスの範囲(CIDR 表記)を許可リストに設定できます。詳しくは「許可リストを設定する」を参照してください。



* Single-AZ構成の場合のフォールトドメイン数は1です。Multi-AZ構成の場合のフォールトドメイン数は3です。フォールトドメイン3にはタイブレーカーノードが配置されます。



ヒント

スケールセットについては、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ユーザーデータおよび管理機能の耐障害性に関する設定(Single-AZ 構成)」または「ユーザーデータおよび管理機能の耐障害性に関する設定(Multi-AZ 構成)」を参照してください。

REST API を操作する curl などや CLI は、コントローラーノードの OS が Windows であればコマンドプロンプト、Linux であればターミナル端末などのコマンド実行が可能なコンソールから実行します。



メモ

- REST API と CLI での時刻指定と時刻表示は、すべて UTC になります。
- I/O 高負荷時は、REST API の応答、ジョブの処理時間、VSP One SDS Block Administrator 操作などの管理操作において、I/O 低負荷時に比べて時間を要することがあります。
- REST API や CLI コマンド、VSP One SDS Block Administrator 操作を同時に複数実行すると、1つのみ実行したときと比較して応答に時間を要したり、KARS15020-E、KARS15588-E が返されたりすることがあります。KARS15020-E、KARS15588-E が返された場合は、時間を置いてから同じ操作を再度実行してください。
- ボリューム情報の一覧を取得するといった、複数リソースについて応答する REST API や VSP One SDS Block Administrator 操作などの管理操作において、対象のリソース数が増えると、少ないときに比べて応答に時間を多く要することがあります。

3.2.5 VSP One SDS Block Administrator について

VSP One SDS Block の VSP One SDS Block Administrator は、シンプルなナビゲーションと高速なレスポンスで、VSP One SDS Block が管理するストレージシステムの全体構成や状態、各種リソースの情報などが容易に確認できるソフトウェアです。また、ボリューム・ドライブ・ストレージノード・コンピュートノードに関する各種操作やダンプログファイルの操作などが行えます。

操作方法や VSP One SDS Block Administrator を利用するブラウザの要件など、詳しくは「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」を参照してください。



注意

- Web ブラウザーの「更新」は使用しないでください。これを使用すると、意図しない画面が表示されることがあります。意図しない画面が表示された場合は、ブラウザを閉じてから、再度ログインしてください。
- 画面の表示倍率設定によっては、ボタンがクリックできない状態になるなど、画面が正常に表示されない場合があります。その場合は、Web ブラウザーのズーム機能の拡大縮小によって調整してください。
- VSP One SDS Block Administrator の画面を複数のウインドウで表示したり、VSP One SDS Block Administrator の画面を含むタブが非アクティブになると、性能情報のチャート表示などの画面で、更新間隔が長くなる可能性があります。以下を行うことによって、改善できることがあります。
 - タブやウインドウの数をできる限り減らす
 - 性能情報のチャート表示を含む画面は、できる限り各ウインドウのアクティブタブで表示する
- "Waiting for available socket..."と Web ブラウザーに表示されて、動作が遅くなった場合は、Web ブラウザーを再起動すると回復する可能性があります。
- "Loading..."が画面左上に表示された状態から遷移しない場合は、ネットワークが正常に動作していない可能性があります。ネットワークが正常に動作しているか確認し、タブをいったん閉じ、開き直してから VSP One SDS Block Administrator を使用してください。
- アイコンが非表示や正しく表示されない場合(例えば、アイコンが□で表示されている場合など)、ネットワークが正常に動作していない可能性があります。ネットワークが正常に動作しているか確認し、タブをいったん閉じ、開き直してから VSP One SDS Block Administrator を使用してください。
- 操作アイコンボタンが表示されない場合、適切な権限がユーザーに付与されていることを確認してください。適切な権限をユーザーに付与されている場合には、ネットワークが正常に動作していない可能性があります。ネットワークが正常に動作しているか確認し、タブをいったん閉じ、開き直してから VSP One SDS Block Administrator を使用してください。
- Volumes 画面の表示などで対象のリソース数が多くなると、リソース数が少ないときに比べて画面の表示に要する時間が長くなる場合があります。

3.2.6 コンソールインターフェイスについて《Bare metal》

ここでの記述内容は Bare metal モデルに適用されます。

VSP One SDS Block では、VSP One SDS Block の保守操作において BMC のリモートコンソールを使用したコンソールインターフェイスを使用します。コンソールインターフェイスを使用する操作には以下があります。

- ストレージクラスターの構築
- ストレージノードの増設
- ストレージノードの交換
- VSP One SDS Block の構成情報の変更
- スペアノードの構築

また、コンソールインターフェイスは、障害などによって VSP One SDS Block Administrator や REST API などが使用できない状況で、トラブルシュートに必要な機能を提供します。

コンソールインターフェイスは、BMC の Web インターフェイス画面および BMC のリモートコンソールを使用して操作します。BMC の Web インターフェイス画面および BMC のリモートコンソールへの接続方法は、ストレージノードとして使用する物理サーバーのベンダーが提供する BMC のユーザーガイドを参照して確認してください。

ストレージクラスター構築、ストレージノード増設、ストレージノード交換におけるコンソールインターフェイスの操作方法に関しては、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

それ以外のケースにおけるコンソールインターフェイスの操作方法に関しては、このマニュアルの「コンソールインターフェイスの操作」を参照してください。また、「コンソールインターフェイスの操作」に記載の操作をする際にはコンソールインターフェイスの使用を許可されたユーザーを使用する必要があります。ユーザーの管理の詳細については「ユーザーを管理する」を参照してください。

3.2.7 コンソールインターフェイスについて<<Cloud>>

ここでの記述内容は Cloud モデルに適用されます。

コンソールインターフェイスは、障害などによって VSP One SDS Block Administrator や REST API などが使用できない状況で、トラブルシュートに必要な機能を提供します。

コンソールインターフェイスの操作方法に関しては、このマニュアルの「コンソールインターフェイスの操作」を参照してください。また、「コンソールインターフェイスの操作」に記載の操作をする際にはコンソールインターフェイスの使用を許可されたユーザーを使用する必要があります。ユーザーの管理の詳細については「ユーザーを管理する」を参照してください。

3.3 コンピュートノードの設置

この節では、コンピュートノードの設置について説明します。

3.3.1 コンピュートノードを設置する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

コンピュートノードは、ユーザーのアプリケーションが動作し、ストレージノードにユーザーデータの入出力を行うノードです。コンピュートノードは、コンピュートネットワークを介してストレージシステムに接続します。

接続完了後は、このマニュアルの「タスクをスケジュールする(コンピュートノードの OS が Windows の場合)」に従ってタスクのスケジューリングを行ったあと、「コンピュートノードの情報を登録する」に従ってコンピュートノードの情報を登録します。

コンピュートノードの要件は下表のとおりです。

なお、ALUA の有効化の方法は、このマニュアルの「ALUA 構築ガイドライン」を参照してください。他の項目については、各 OS のマニュアルを参照してください。

■iSCSI または FC 接続の場合

項目	要件
OS ¹	- Windows Server(64 ビット) - Red Hat Enterprise Linux(64 ビット) - VMware ESXi
ALUA のサポートと有効化	Asymmetric Logical Unit Access(ALUA)がサポートされていること。かつ、ALUA が有効化されていること。
SCSI Timeout 設定	SCSI Timeout 設定値が 120 秒以上であること ²
マルチパス設定(Linux Device Mapper - Multipath)	以下をすべて満たすこと。 - no_path_retry の設定値が 6 以上であること - polling_interval の設定値が 30 以上であること - fast_io_fail_tmo の設定値が off 以外 ³ であること - dev_loss_tmo の設定値が OS 最大値 ⁴ であること - failback の設定値が immediate であること ⁵ - path_checker の設定値が readsector0 であること ⁶ - hardware_handler の設定値が 0 であること ⁷
コンピュータネットワークのネットワークインターフェイスの MTU サイズ	iSCSI の場合、VSSB 構成ファイルの ComputeNWMTUSize の設定値と同じであること ⁸
- サポートバージョンはサポートセンターにお問い合わせください。 - SCSI Timeout 設定値は、SCSI コマンドの無応答が発生したと OS が判断するまでの時間です。OS は、SCSI コマンドの無応答を検出すると、障害発生パスに対してリカバリー処理を実施します。リカバリー処理によって障害発生パスが復旧しない場合、当該パスを閉塞して別のパスに切り替わります。リカバリー処理中は、当該パスに対する I/O 動作が停止します。そのため、アプリケーション層のタイムアウト設計は、SCSI Timeout 設定値に加えて、リカバリー処理の時間を考慮する必要があります。 - fast_io_fail_tmo のデフォルト値は 5 です。off に設定するとパス障害発生時に dev_loss_tmo 秒経過するまでパス切り替えが発生せず、期待どおり動作しません。 - お使いのディストリビューションによって最大値が異なります。お使いのディストリビューションのマニュアルを参照して最大値を確認してください。 - パスグループのフェイルバックポリシー(failback)を immediate(即時フェイルバック)に設定してください。本設定を行わない場合、パス障害から復旧した際に、I/O 発行先が非優先パスのままとなり、手動でのパス切り替え作業が必要になります。 - VSP One SDS Block でストレージノード障害が発生した場合、readsector0 以外の値が設定されていると、パスが誤閉塞する可能性があります。そのため、必ず readsector0 を設定してください。 0 以外の値が設定されていると、コンピュータノードの OS のバージョンによっては、マルチパスが期待どおり動作しないことがあります。 - FC 接続の場合は、ComputeNWMTUSize の設定値は使用されないため、設定値と同じである必要はありません。	

■NVMe/TCP 接続の場合

項目	要件
OS ¹	- Red Hat Enterprise Linux(64 ビット) - VMware ESXi
NVMe Timeout 設定	NVMe Timeout 設定値が 120 秒以上であること ²
マルチパス設定	以下をすべて満たすこと。 Native NVMe Multipath が有効であること ³

項目	要件
	- NVMe デバイスの I/O ポリシー設定が round-robin であること - ctrl_loss_tmo の設定値が-1 であること⁴
- サポートバージョンはサポートセンターにお問い合わせください。 - NVMe Timeout 設定値は、NVMe コマンドの無応答が発生したと OS が判断するまでの時間です。OS は、NVMe コマンドの無応答を検出すると、障害発生パスに対してリカバリー処理を実施します。リカバリー処理によって障害発生パスが復旧しない場合、当該パスを閉塞して別のパスに切り替えます。リカバリー処理中は、当該パスに対する I/O 動作が停止します。そのため、アプリケーション層のタイムアウト設計は、NVMe Timeout 設定値に加えて、リカバリー処理の時間を考慮する必要があります。 - Native NVMe Multipath を有効にすると、すべてのボリュームに対して Asymmetric Namespace Access(ANA)が適用されます。ANA の詳細については「ANA 構築ガイドライン」を参照してください。 - ctrl_loss_tmo を-1 に設定すると、パス損失が発生した場合に永続的にパス検出を再試行するようになります。	

VSP One SDS Block における VMware vStorage APIs for Array Integration(VAAI)機能についてのサポート状況は以下のとおりです。

VAAI 機能	概要	サポート状況
Block Zeroing	新しい仮想マシンの作成時に実行されるフォーマット(ゼロ書き)処理をストレージ側で行うことによって、仮想マシンのプロビジョニングを高速化します。また、シンプロビジョニング機能と連携することで、従来、仮想マシンの作成時に確保されていたブロック領域を解放することが可能となり、容量の効率化を実現します。	サポート
Hardware Assisted Locking	複数の ESXi ホストで 1 つの VMFS ボリュームを共有する環境において、vMotion や仮想マシンのパワーオンを実施した場合に、SCSI リザーブの衝突が発生し、性能が劣化するという問題を回避し、効率のよい排他ロック機能を提供します。	サポート
Full Copy	VMware ESXi 上で実施されるボリューム間のコピー処理をストレージ側へオフロードすることで、仮想マシンのクローニングや Storage vMotion の処理時間を短縮します。	サポートしていません

(1) コンピュートノード設置に当たっての注意事項<<Bare metal>>

ここでの記述内容は Bare metal モデルに適用されます。

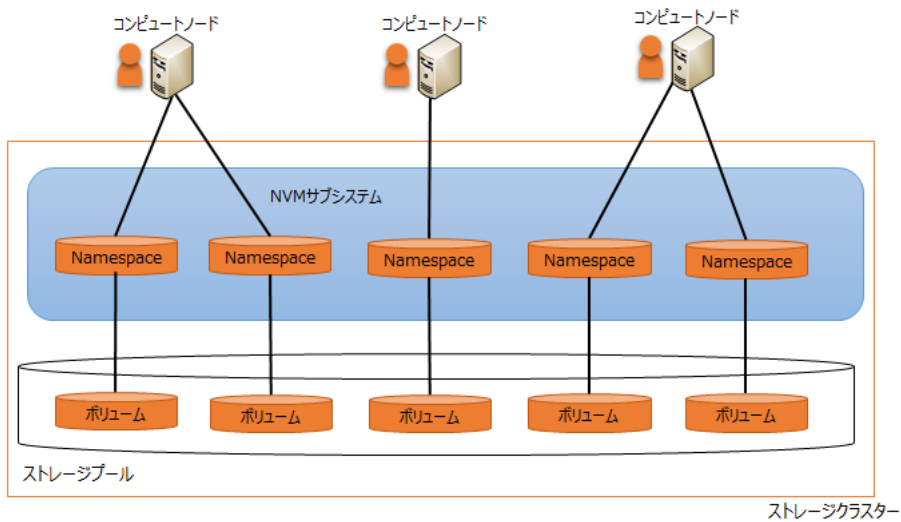
- iSCSI 接続または NVMe/TCP 接続で利用する場合、コンピュートノードにおいて Digest 設定を有効にすることで、Data Digest 機能と Header Digest 機能が使用できます。これらの機能を使用すると、通信路上のデータの信頼性は向上しますが、性能は低下します。低下の割合は、ホストやネットワークなどの環境に依存します。用途に合わせて、本機能を使用するかどうかを選択してください。
- FC 接続で利用する場合、ストレージノード障害が発生すると、障害が発生したストレージノードに対するパスで SCSI コマンドの無応答が発生することがあります。その際、障害発生パスから別のパスに切り替わるまで、SCSI Timeout 設定値に加え、無応答となった SCSI コマンドの破棄など、リカバリー処理の時間が必要になります。

(2) NVMe/TCP 接続時のシステム構成<<Bare metal>>

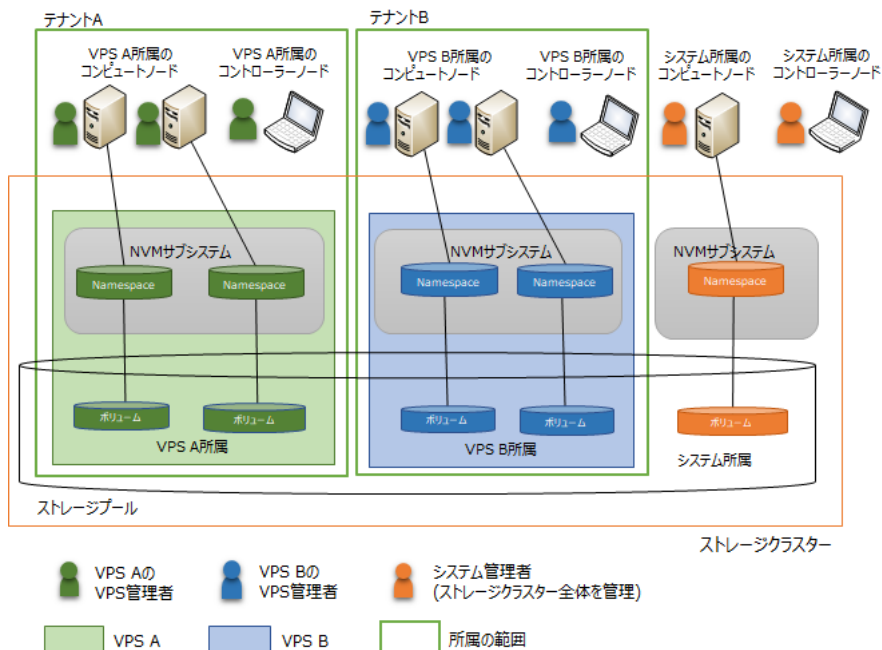
ここでの記述内容は Bare metal モデルに適用されます。

コンピュータノードとストレージ間を NVMe/TCP で接続する場合、VSP One SDS Block ではストレージ(ターゲット)側の NVMe デバイス制御情報(NVM サブシステムおよび Namespace)を自動で作成します。

NVMe/TCP 接続時のシステム構成の一例を以下に示します。



また、マルチテナンシーを構成してる場合のシステム構成の一例を以下に示します。



NVM サブシステムは、VPS 外(システム所属)として1つ、また VPS ごとに1つずつ作成されます。各所属の1つ目のコンピュータノードを登録したときに自動で作成され、各所属の最後のコンピュータノードを削除したときに NVM サブシステムも自動で削除されます。



メモ

マルチテナンシーを構成していない場合は NVM サブシステムはストレージクラスター内に1つだけ作成されます。マルチテナンシー機能については「マルチテナンシーを構成する<<Bare metal>>」を参照してください。

Namespace はボリューム単位に1つずつ、NVM サブシステム上に作成されます。各ボリュームに対する1つ目のボリュームパスを設定したときに自動で作成され、各ボリュームに対する最後のボリュームパスを削除したときに Namespace も自動で削除されます。

ボリュームパスの設定と削除については「ボリュームをコンピュータノードに接続する<<Bare metal>>」、「ボリュームとコンピュータノードの接続を解除する<<Bare metal>>」をそれぞれ参照してください。

3.3.2 コンピュータノードを設置する<<Cloud for AWS>>

この項での記述内容は Cloud モデル for AWS に適用されます。

コンピュータノードは、ユーザーのアプリケーションが動作し、ストレージノードにユーザーデータの入出力を行うノードです。コンピュータノードは、コンピュータネットワークを介してストレージシステムに接続します。

接続完了後は、このマニュアルの「タスクをスケジュールする(コンピュータノードの OS が Windows の場合)」に従ってタスクのスケジュールを行ったあと、「コンピュータノードの情報を登録する」に従ってコンピュータノードの情報を登録します。

コンピュータノードの要件は下表のとおりです。

なお、ALUA の有効化の方法は、このマニュアルの「ALUA 構築ガイドライン」を参照してください。他の項目については、各 OS のマニュアルを参照してください。

項目	要件
OS ¹	- Windows Server(64 ビット) - Red Hat Enterprise Linux(64 ビット) - Amazon Linux - SUSE Linux Enterprise Server - Oracle Linux
ALUA のサポートと有効化	Asymmetric Logical Unit Access(ALUA)がサポートされていること。かつ、ALUA が有効化されていること。
SCSI Timeout 設定	SCSI Timeout 設定値が 120 秒以上であること ²
マルチパス設定(Linux Device Mapper - Multipath)	以下をすべて満たすこと。 - no_path_retry の設定値が 6 以上であること - polling_interval の設定値が 30 以上であること - fast_io_fail_tmo の設定値が off 以外 ³ であること - dev_loss_tmo の設定値が OS 最大値 ⁴ であること - failback の設定値が immediate であること ⁵ - path_checker の設定値が readsector0 であること ⁶ - hardware_handler の設定値が 0 であること ⁷
コンピュータネットワークのネットワークインターフェイスの MTU サイズ	9000 以上であること
1. サポートバージョンはサポートセンターにお問い合わせください。 2. SCSI Timeout 設定値は、SCSI コマンドの無応答が発生したと OS が判断するまでの時間です。OS は、SCSI コマンドの無応答を検出すると、障害発生パスに対してリカバリー処理を実施します。リカバリー処理によって障害発生パスが復旧しない場合、当該パスを閉塞して別のパスに切り替わります。リカバリー処理中は、当該パスに対する I/O 動作が停止します。そのため、アプリケーション層のタイムアウト設計は、SCSI Timeout 設定値に加えて、リカバリー処理の時間を考慮する必要があります。 3. fast_io_fail_tmo のデフォルト値は 5 です。off に設定するとパス障害発生時に dev_loss_tmo 秒経過するまでパス切り替えが発生せず、期待どおり動作しません。	

項目	要件
4.	お使いのディストリビューションによって最大値が異なります。お使いのディストリビューションのマニュアルを参照して最大値を確認してください。
5.	パスグループのフェイルバックポリシー(failback)を immediate(即時フェイルバック)に設定してください。本設定を行わない場合、パス障害から復旧した際に、I/O 発行先が非優先パスのままとなり、手動でのパス切り替え作業が必要になります。
6.	VSP One SDS Block でストレージノード障害が発生した場合、readsector0 以外の値が設定されていると、パスが誤閉塞する可能性があります。そのため、必ず readsector0 を設定してください。
7.	0 以外の値が設定されていると、コンピュータノードの OS のバージョンによっては、マルチパスが期待どおり動作しないことがあります。

コンピュータノードとして使用する EC2 インスタンスには、以下のように少なくとも 2 個のネットワークインターフェイスを割り当てる必要があります。

- 管理ネットワークに接続されたネットワークインターフェイス
- コンピュータネットワークに接続されたネットワークインターフェイス

それぞれのネットワークインターフェイスのセキュリティグループの設定は、Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「コンピュータノードのセキュリティグループ設定例」を参照してください。



メモ

- コンピュータノードを VSP One SDS Block のコンピュータネットワーク用サブネットとは別のサブネットに設置する場合、またはコンピュータノードを VSP One SDS Block の VPC とは別の VPC に設置する場合は、以下を実施してください。
 - Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」にある「コンピュータノードの設置に関する補足事項」の手順を実施したあとに、本節記載の手順を実施してください。
 - コンピュータノードの OS にログイン後、必要に応じてコンピュータポートからコンピュータネットワーク用サブネットへのルート(経路)を追加してください。
- コンピュータノードとストレージクラスターとの通信がアベイラビリティゾーンをまたいだ場合、アベイラビリティゾーン間の通信が発生します。通信料については AWS の Web サイトをご確認ください。

(1) コンピュータノード設置に当たっての注意事項<<Cloud for AWS>>

ここでの記述内容は Cloud モデル for AWS に適用されます。

- コンピュータノードにおいて Digest 設定を有効にすることで、Data Digest 機能と Header Digest 機能が使用できます。これらの機能を使用すると、通信路上のデータの信頼性は向上しますが、性能は低下します。低下の割合は、ホストやネットワークなどの環境に依存します。用途に合わせて、本機能を使用するかどうかを選択してください。
- AWS Nitro System ベースのインスタンスタイプだけをサポートします。Xen システムベースのインスタンスタイプはサポートしません。AWS Nitro System ベースのインスタンスタイプの詳細は、以下の Web サイトを参照してください。
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#ec2-nitro-instances>

3.3.3 コンピュータノードを設置する<<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

コンピュータノードは、ユーザーのアプリケーションが動作し、ストレージノードにユーザーデータの入出力を行うノードです。コンピュータノードは、コンピュータネットワークを介してストレージシステムに接続します。

接続完了後は、このマニュアルの「タスクをスケジュールする(コンピュータノードの OS が Windows の場合)」に従ってタスクのスケジュールを行ったあと、「コンピュータノードの情報を登録する」に従ってコンピュータノードの情報を登録します。

コンピュータノードの要件は下表のとおりです。

なお、ALUA の有効化の方法は、このマニュアルの「ALUA 構築ガイドライン」を参照してください。他の項目については、各 OS のマニュアルを参照してください。

項目	要件
OS ¹	- Windows Server(64 ビット) - Red Hat Enterprise Linux(64 ビット)
ALUA のサポートと有効化	Asymmetric Logical Unit Access(ALUA)がサポートされていること。かつ、ALUA が有効化されていること。
SCSI Timeout 設定	SCSI Timeout 設定値が 120 秒以上であること ²
マルチパス設定(Linux Device Mapper - Multipath)	以下をすべて満たすこと。 - no_path_retry の設定値が 6 以上であること - polling_interval の設定値が 30 以上であること - fast_io_fail_tmo の設定値が off 以外 ³ であること - dev_loss_tmo の設定値が OS 最大値 ⁴ であること - failback の設定値が immediate であること ⁵ - path_checker の設定値が readsector0 であること ⁶ - hardware_handler の設定値が 0 であること ⁷
コンピュータネットワークのネットワークインターフェイスの MTU サイズ	仮想ネットワーク作成用テンプレートの VM 構成ファイル(terraform.tfvars)に記載されている computeNetworkMtu の設定値と同じであること 仮想ネットワーク作成用テンプレートの VM 構成ファイル(terraform.tfvars)は、クラウド構成ファイルパッケージ(hsds-terraform-template-files-<version>-<number>.zip)を解凍し、VNetConfigurationFile フォルダーから入手してください。
- サポートバージョンはサポートセンターにお問い合わせください。 - SCSI Timeout 設定値は、SCSI コマンドの無応答が発生したと OS が判断するまでの時間です。OS は、SCSI コマンドの無応答を検出すると、障害発生パスに対してリカバリー処理を実施します。リカバリー処理によって障害発生パスが復旧しない場合、当該パスを閉塞して別のパスに切り替わります。リカバリー処理中は、当該パスに対する I/O 動作が停止します。そのため、アプリケーション層のタイムアウト設計は、SCSI Timeout 設定値に加えて、リカバリー処理の時間を考慮する必要があります。 - fast_io_fail_tmo のデフォルト値は 5 です。off に設定するとパス障害発生時に dev_loss_tmo 秒経過するまでパス切り替えが発生せず、期待どおり動作しません。 - お使いのディストリビューションによって最大値が異なります。お使いのディストリビューションのマニュアルを参照して最大値を確認してください。 - パスグループのフェイルバックポリシー(failback)を immediate(即時フェイルバック)に設定してください。本設定を行わない場合、パス障害から復旧した際に、I/O 発行先が非優先パスのままとなり、手動でのパス切り替え作業が必要になります。 - VSP One SDS Block でストレージノード障害が発生した場合、readsector0 以外の値が設定されていると、パスが誤閉塞する可能性があります。そのため、必ず readsector0 を設定してください。	

項目	要件
7.0 以外の値が設定されていると、コンピュータノードの OS のバージョンによっては、マルチパスが期待どおり動作しないことがあります。	

コンピュータノードとして使用する Compute Engine インスタンスには、以下のように少なくとも 2 個のネットワークインターフェイスを割り当てる必要があります。

- 管理ネットワークに接続されたネットワークインターフェイス
- コンピュータネットワークに接続されたネットワークインターフェイス

それぞれのネットワークインターフェイスの Cloud Next Generation Firewall の設定は、Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「コンピュータノードの Cloud Next Generation Firewall 設定例」を参照してください。



メモ

- コンピュータノードを VSP One SDS Block のコンピュータネットワーク用サブネットとは別のサブネットに設置する場合は、以下を実施してください。
 - Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」にある「サブネットを作成する」の手順を実施したあとに、本節記載の手順を実施してください。
 - コンピュータノードの OS にログイン後、必要に応じてコンピュータポートからコンピュータネットワーク用サブネットへのルート(経路)を追加してください。
- コンピュータノードとストレージクラスターとの通信がゾーンをまたいだ場合、ゾーン間の通信が発生します。通信料については Google Cloud の Web サイトをご確認ください。

(1) コンピュータノード設置に当たっての注意事項<<Cloud for Google Cloud>>

ここでの記述内容は Cloud モデル for Google Cloud に適用されます。

コンピュータノードにおいて Digest 設定を有効にすることで、Data Digest 機能と Header Digest 機能が使用できます。これらの機能を使用すると、通信路上のデータの信頼性は向上しますが、性能は低下します。低下の割合は、ホストやネットワークなどの環境に依存します。用途に合わせて、本機能を使用するかどうかを選択してください。

3.3.4 コンピュータノードを設置する<<Cloud for Microsoft Azure>>

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

コンピュータノードは、ユーザーのアプリケーションが動作し、ストレージノードにユーザーデータの入出力を行うノードです。コンピュータノードは、コンピュータネットワークを介してストレージシステムに接続します。

接続完了後は、このマニュアルの「タスクをスケジュールする(コンピュータノードの OS が Windows の場合)」に従ってタスクのスケジュールを行ったあと、「コンピュータノードの情報を登録する」に従ってコンピュータノードの情報を登録します。

コンピュータノードの要件は下表のとおりです。

なお、ALUA の有効化の方法は、このマニュアルの「ALUA 構築ガイドライン」を参照してください。他の項目については、各 OS のマニュアルを参照してください。

項目	要件
OS ¹	- Windows Server(64 ビット) - Red Hat Enterprise Linux(64 ビット)
ALUA のサポートと有効化	Asymmetric Logical Unit Access(ALUA)がサポートされていること。かつ、ALUA が有効化されていること。
SCSI Timeout 設定	SCSI Timeout 設定値が 120 秒以上であること ²
マルチパス設定(Linux Device Mapper - Multipath)	以下をすべて満たすこと。 - no_path_retry の設定値が 6 以上であること - polling_interval の設定値が 30 以上であること - fast_io_fail_tmo の設定値が off 以外 ³ であること - dev_loss_tmo の設定値が OS 最大値 ⁴ であること - failback の設定値が immediate であること ⁵ - path_checker の設定値が readsector0 であること ⁶ - hardware_handler の設定値が 0 であること ⁷
コンピュータネットワークのネットワークインターフェイスの MTU サイズ	VM 構成ファイルの computeMtuSize の設定値と同じであること

1. サポートバージョンはサポートセンターにお問い合わせください。

2. SCSI Timeout 設定値は、SCSI コマンドの無応答が発生したと OS が判断するまでの時間です。OS は、SCSI コマンドの無応答を検出すると、障害発生パスに対してリカバリー処理を実施します。リカバリー処理によって障害発生パスが復旧しない場合、当該パスを閉塞して別のパスに切り替わります。リカバリー処理中は、当該パスに対する I/O 動作が停止します。そのため、アプリケーション層のタイムアウト設計は、SCSI Timeout 設定値に加えて、リカバリー処理の時間を考慮する必要があります。

3. fast_io_fail_tmo のデフォルト値は 5 です。off に設定するとパス障害発生時に dev_loss_tmo 秒経過するまでパス切り替えが発生せず、期待どおり動作しません。

4. お使いのディストリビューションによって最大値が異なります。お使いのディストリビューションのマニュアルを参照して最大値を確認してください。

5. パスグループのフェイルバックポリシー(failback)を immediate(即時フェイルバック)に設定してください。本設定を行わない場合、パス障害から復旧した際に、I/O 発行先が非優先パスのままとなり、手動でのパス切り替え作業が必要になります。

6. VSP One SDS Block でストレージノード障害が発生した場合、readsector0 以外の値が設定されていると、パスが誤閉塞する可能性があります。そのため、必ず readsector0 を設定してください。

7. 0 以外の値が設定されていると、コンピュータノードの OS のバージョンによっては、マルチパスが期待どおり動作しないことがあります。

コンピュータノードとして使用する Azure VM インスタンスには、以下のように少なくとも 2 個のネットワークインターフェイスを割り当てる必要があります。

- 管理ネットワークに接続されたネットワークインターフェイス
- コンピュータネットワークに接続されたネットワークインターフェイス

それぞれのネットワークインターフェイスのネットワークセキュリティグループの設定は、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「コンピュータノードのネットワークセキュリティグループ設定例」を参照してください。



メモ

- コンピュートノードを VSP One SDS Block のコンピュータネットワーク用サブネットとは別のサブネットに設置する場合は、以下を実施してください。
- ネットワークセキュリティグループの設定のため、ストレージクラスター構築時にパラメーターを指定します。詳細は Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージクラスターを構築する」を参照してください。
ストレージクラスター構築後にネットワークセキュリティグループの設定を変更する場合は、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージクラスターの設定値を変更する」を参照してください。
- 必要に応じてサブネットにルートテーブルを設定してください。
- コンピュートノードの OS にログイン後、必要に応じてコンピュータポートからコンピュータネットワーク用サブネットへのルート(経路)を追加してください。
- コンピュートノードとストレージクラスターとの通信がアベイラビリティゾーンをまたいだ場合、アベイラビリティゾーン間の通信が発生します。ただし、Microsoft Azure では通信料は発生しません。

(1) コンピュートノード設置に当たっての注意事項《Cloud for Microsoft Azure》

ここでの記述内容は Cloud モデル for Microsoft Azure に適用されます。

コンピュータノードにおいて Digest 設定を有効にすることで、Data Digest 機能と Header Digest 機能が使用できます。これらの機能を使用すると、通信路上のデータの信頼性は向上しますが、性能は低下します。低下の割合は、ホストやネットワークなどの環境に依存します。用途に合わせて、本機能を使用するかどうかを選択してください。

3.3.5 タスクをスケジュールする(コンピュータノードの OS が Windows の場合)

VSP One SDS Block では Windows のマルチパス I/O の制限に抵触しないようにストレージ側でパス数を絞っています。

この制限に対する運用を簡易化するために Windows 搭載のコンピュータノード(ホスト)へのタスク導入が必須になります。Windows 搭載のコンピュータノードでは、下記の手順に従ってタスクスケジューラを登録してください。説明には Windows 10 の画面を使用しています。

タスクスケジューラは、初回設定、および再起動による再実行が行われるように登録します。タスクスケジューラによって周期的にデバイスの更新を行うことで、障害や容量バランス処理後の構成情報に追従することが可能となります。

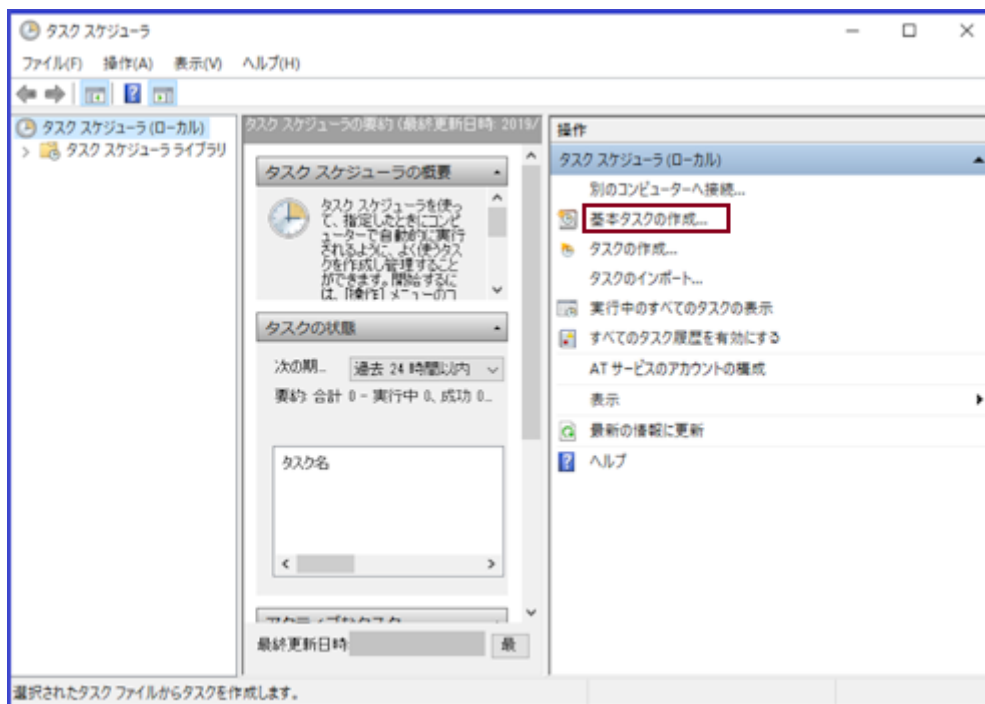


注意

メンテナンスによるコンピュータノードのログアウト、または予期せぬシャットダウンから、ログインまたは起動した際にも、タスクが再実行されるよう、下記の手順に従ってタスクをスケジュールしてください。

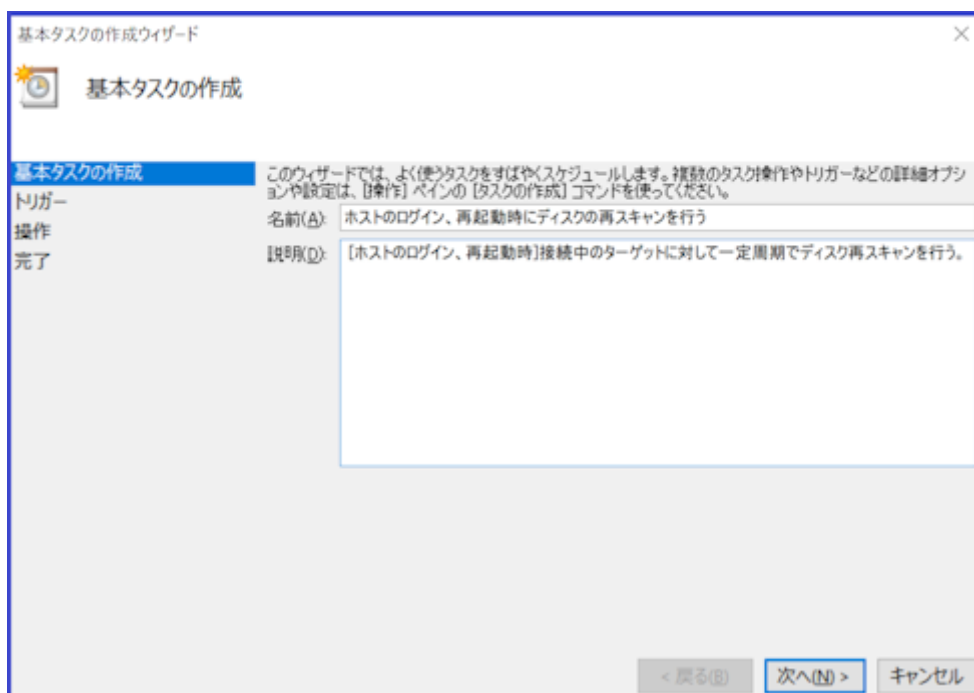
操作手順

1. スタートメニューから[Windows 管理ツール]>[タスク スケジューラ]を選択します。
「タスク スケジューラ」画面が表示されます。



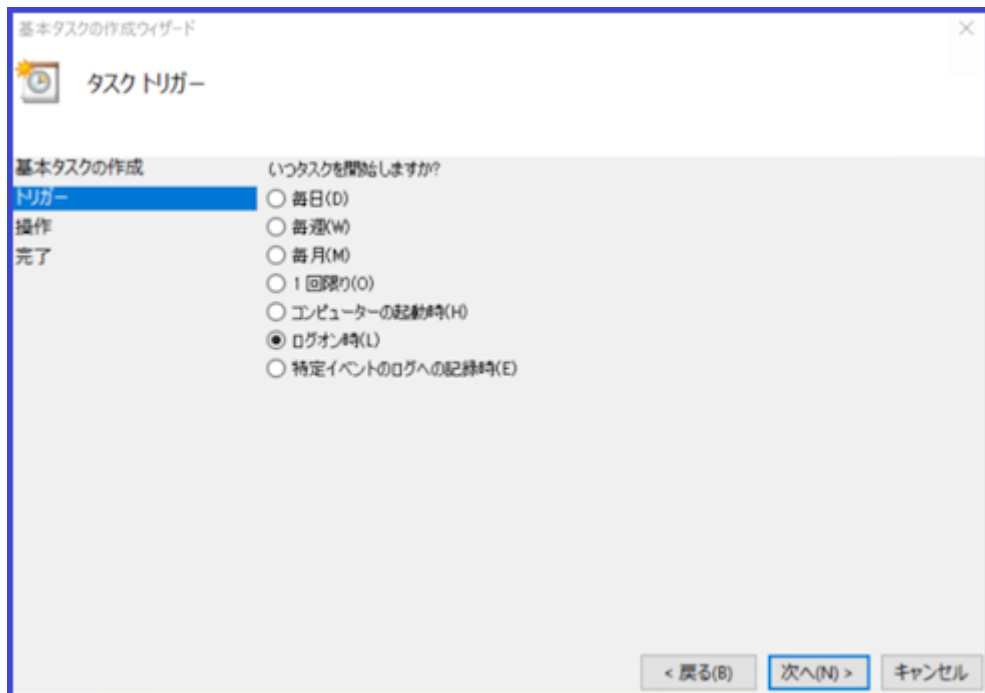
- 画面左の[タスク スケジューラ ライブラリ]を選択し、画面右の操作メニューから[基本タスクの作成]をクリックします。

「基本タスクの作成ウィザード(基本タスクの作成)」画面が表示されます。

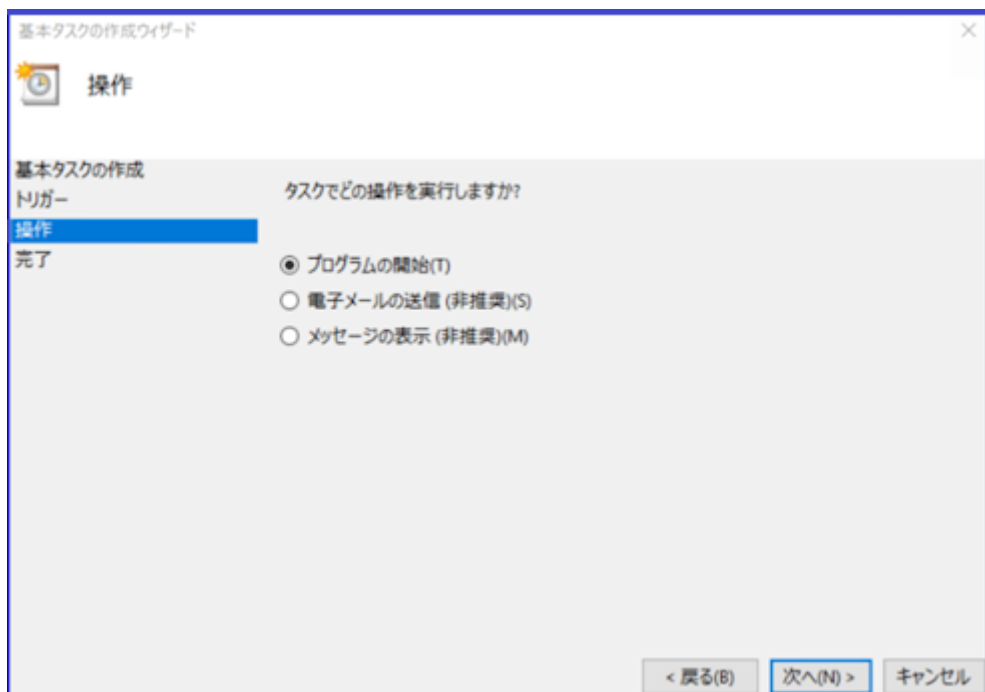


- タスクの[名前]と[説明]を入力し、[次へ]をクリックします。

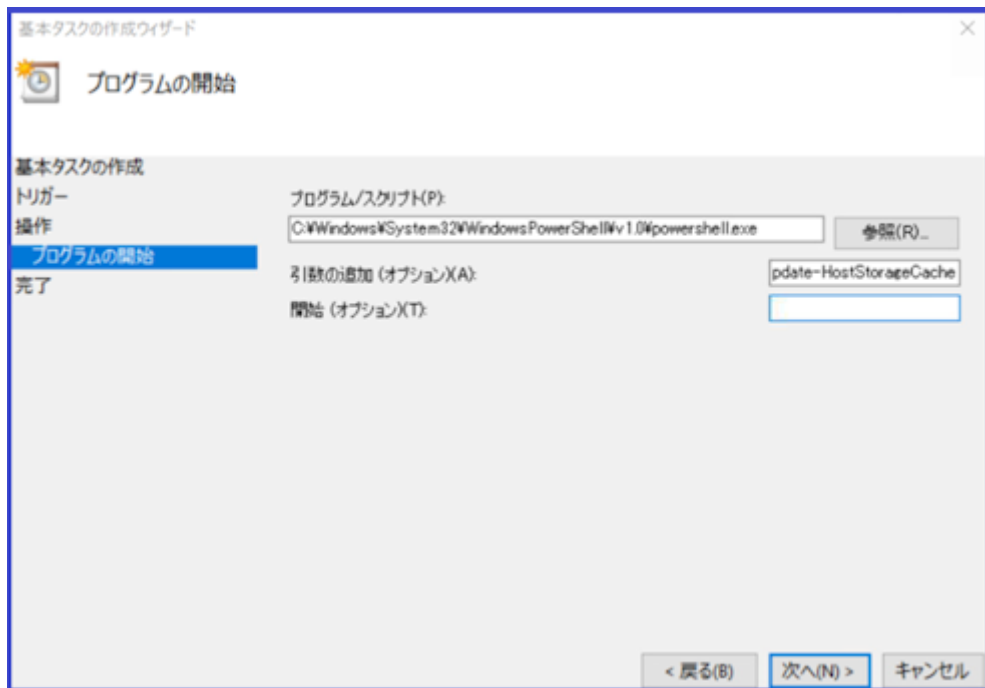
「基本タスクの作成ウィザード(タスク トリガー)」画面が表示されます。



4. 「ログオン時」を選択し、[次へ]をクリックします。
「基本タスクの作成ウィザード(操作)」画面が表示されます。



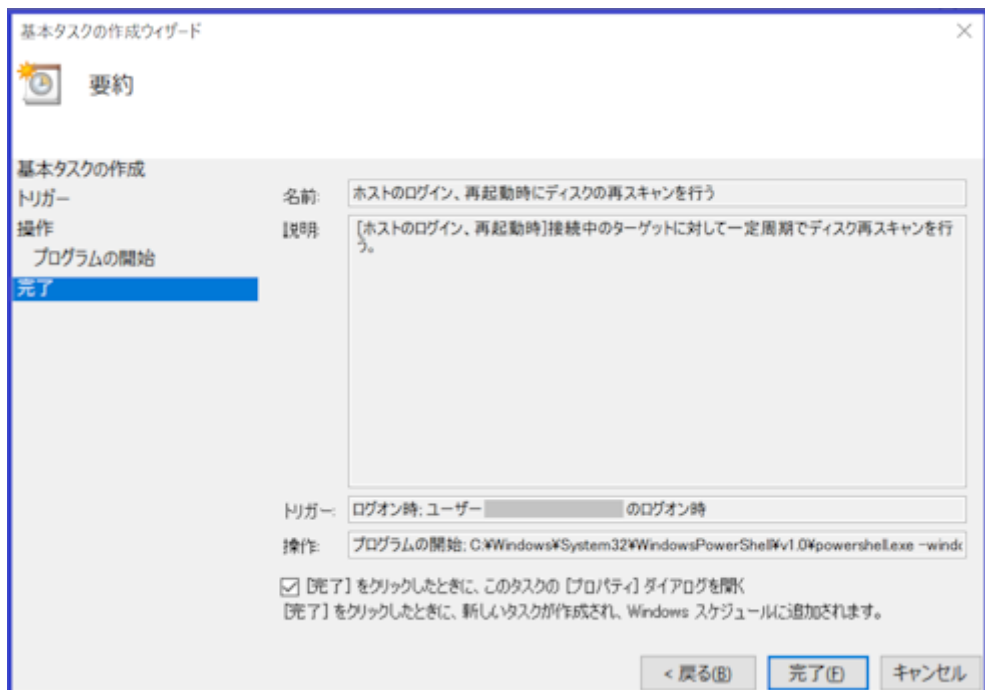
5. 「プログラムの開始」を選択し、[次へ]をクリックします。
「基本タスクの作成ウィザード(プログラムの開始)」画面が表示されます。



6. 以下の設定し、[次へ]をクリックします。

- ・ プログラム/スクリプト：C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
- ・ 引数の追加：-Windowstyle Hidden Update-HostStorageCache

「基本タスクの作成ウィザード(要約)」画面が表示されます。



7. 内容を確認し、[[完了] をクリックしたときに、このタスクの [プロパティ] ダイアログを開く]にチェックを付けてから[完了]をクリックします。

タスクのプロパティ画面が表示されます。

プロパティの設定値は、運用に合わせた設定を行ってください。以下に参考として、設定例を記します。

[全般]タブにて、セキュリティ オプションの設定を行います。

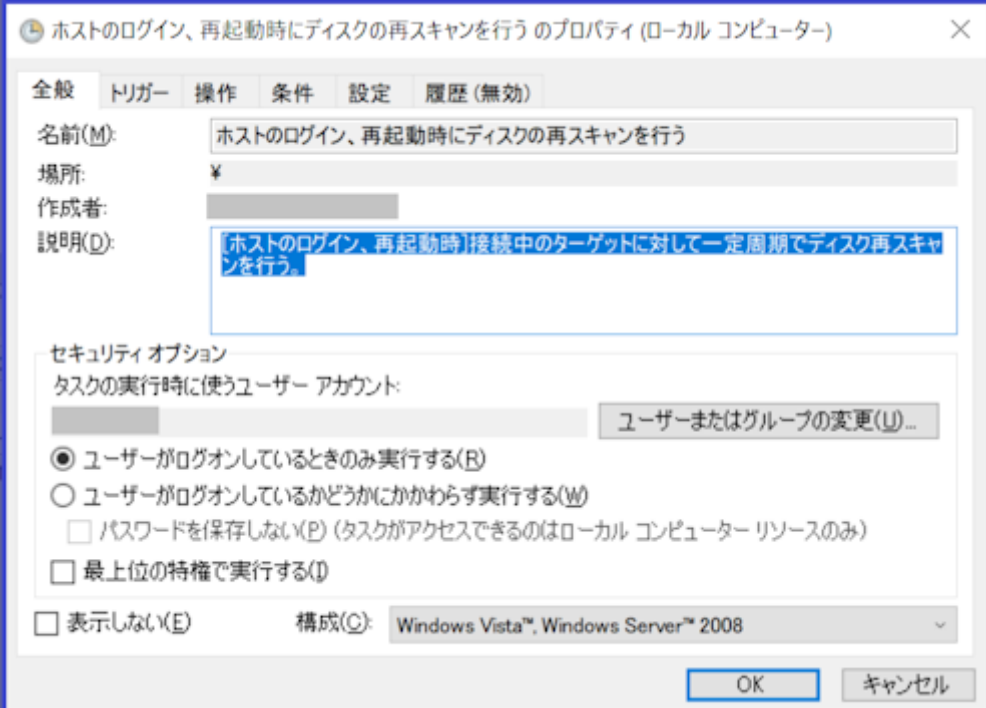
運用方法によって[ユーザーがログオンしているときのみ実行する]か[ユーザーがログオンしているかどうかにかかわらず実行する]かのどちらかを選択してください。

直前に指定しているユーザーがログイン中にのみボリュームへアクセスする場合は、[ユーザーがログオンしているときのみ実行する]を選択してください。

[ユーザーがログオンしているときのみ実行する]を設定すると、ログアウト中にストレージ側の更新に追従できず、アクセスロスとなる可能性があります。

直前に指定しているユーザーがログアウト中にもボリュームへアクセスする場合は、[ユーザーがログオンしているかどうかにかかわらず実行する]を選択し、[パスワードを保存しない(P) (タスクがアクセスできるのはローカル コンピューター リソースのみ)]にチェックを入れてください。

[最上位の特権で実行する]はチェック不要です。[表示しない]はチェック不要です。構成には、デフォルト値を設定してください。



ホストのログイン、再起動時にディスクの再スキャンを行うのプロパティ (ローカル コンピューター)

全般 トリガー 操作 条件 設定 履歴 (無効)

名前(M): ホストのログイン、再起動時にディスクの再スキャンを行う

場所: *

作成者:

説明(D): ホストのログイン、再起動時]接続中のターゲットに対して一定周期でディスク再スキャンを行う。

セキュリティ オプション

タスクの実行時に使うユーザー アカウント:

ユーザーまたはグループの変更(U)...

☒ ユーザーがログオンしているときのみ実行する(R)

☐ ユーザーがログオンしているかどうかにかかわらず実行する(W)

☐ パスワードを保存しない(P) (タスクがアクセスできるのはローカル コンピューター リソースのみ)

☐ 最上位の特権で実行する(I)

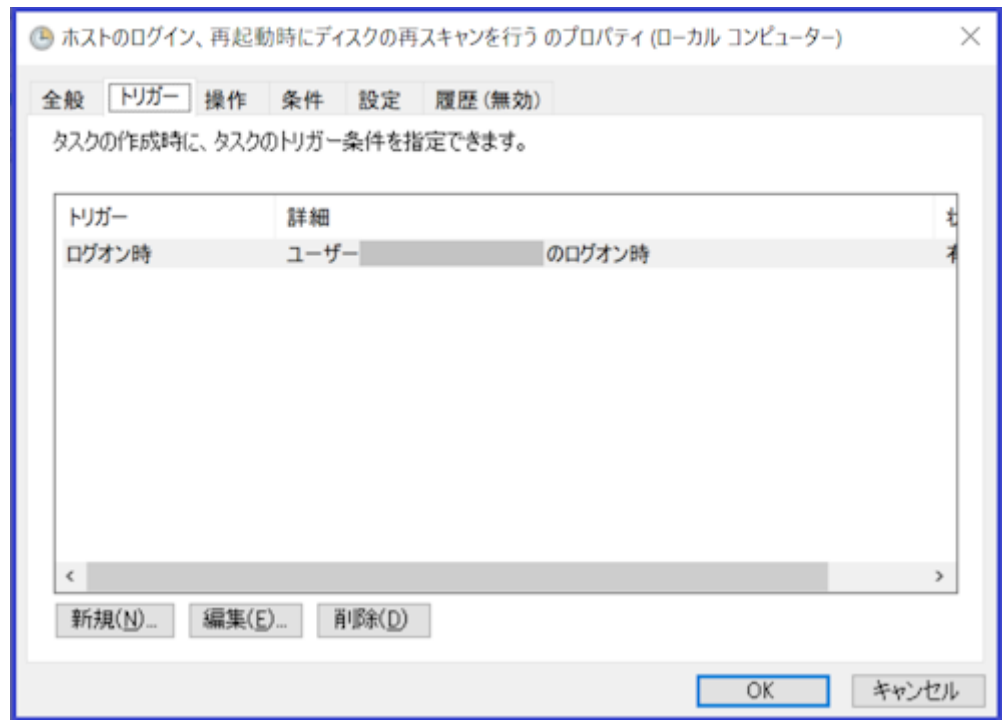
☐ 表示しない(E) 構成(C): Windows Vista™, Windows Server™ 2008

OK キャンセル

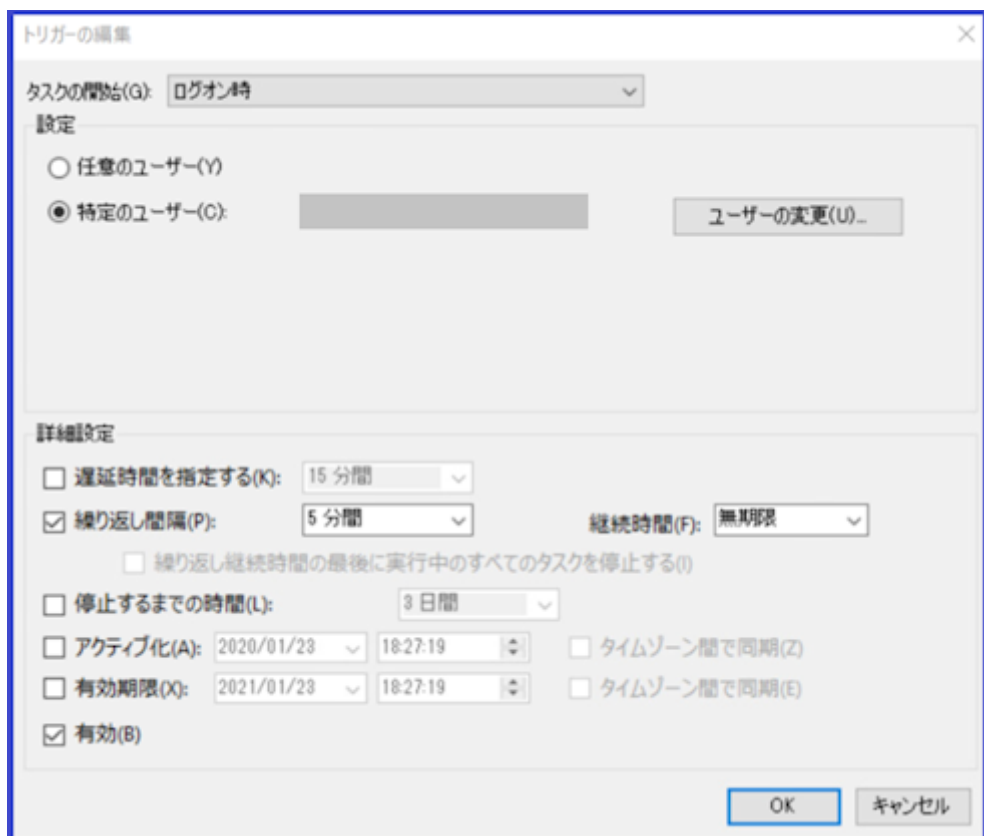


メモ

[トリガー]タブに指定されているユーザーは、必要に応じて[編集]をクリックし、コンピュートノードとして使用している Windows ホストサーバーのログインユーザーを指定してください。



8. [トリガー]タブを選択し、トリガーを選択し[編集]をクリックします。
「トリガーの編集」画面が表示されます。



9. 以下を設定し、[OK]をクリックします。

- ・ 繰り返し間隔：5 分間
- ・ 継続時間：無期限

その他の設定値は、運用に合わせた設定を行ってください。

タスクのプロパティ画面に戻ります。

10. [OK]をクリックします。

「タスク スケジューラ」画面に戻ります。

11. 続けて初回実行するタスクを作成します。作成したタスクを選択し、画面右の操作メニューから[エクスポート]をクリックして、タスクを保存します。

エクスポートするタスクの保存先は任意です。



12. エクスポートしたタスクをインポートします。画面右の操作メニューから[タスクのインポート]をクリックし、手順 11 で保存したタスクを開きます。このスケジューラは、現在ログイン中の状態のままタスクを実行させるトリガーとなります。



「タスクの作成」画面が表示されます。

タスクの作成

全般 トリガー 操作 条件 設定

名前(M): ホストのログイン、再起動後にディスク再スキャンを行うスケジュール

場所: ¥

作成者:

説明(D): [ログイン、再起動時]接続中のターゲットが認証しているディスクに対する一定周期のディスク再スキャンを行う。

セキュリティ オプション

タスクの実行時に使うユーザー アカウント:

ユーザーまたはグループの変更(U)...

☒ ユーザーがログオンしているときのみ実行する(B)

☐ ユーザーがログオンしているかどうかにかかわらず実行する(W)

☐ パスワードを保存しない(P) (タスクがアクセスできるのはローカル コンピューター リソースのみ)

☐ 最上位の特権で実行する(I)

☐ 表示しない(E) 構成(C): Windows Vista™, Windows Server™ 2008

OK キャンセル

13. [全般]タブで[名前]と[説明]を変更します。

タスクの作成

全般 トリガー 操作 条件 設定

名前(M): タスクの作成、変更時にディスクの再スキャンを行う

場所: ¥

作成者:

説明(D): [タスクの作成、変更時]接続中のターゲットに対して一定周期でディスク再スキャンを行う。

セキュリティ オプション

タスクの実行時に使うユーザー アカウント:

ユーザーまたはグループの変更(U)...

☒ ユーザーがログオンしているときのみ実行する(B)

☐ ユーザーがログオンしているかどうかにかかわらず実行する(W)

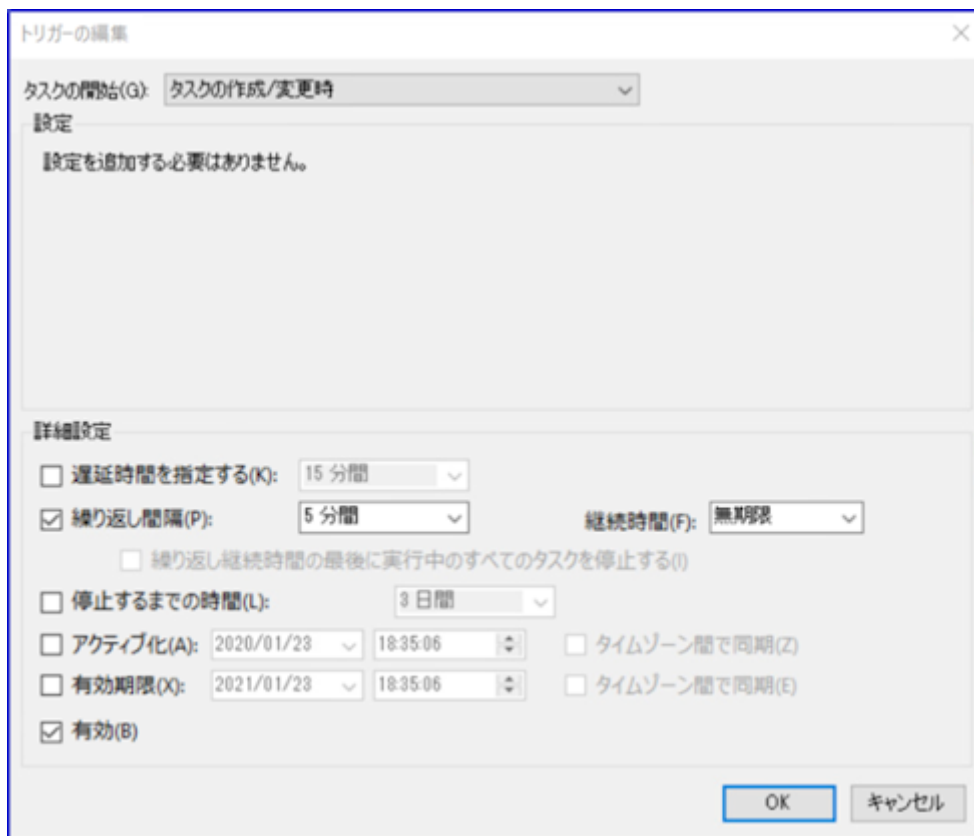
☐ パスワードを保存しない(P) (タスクがアクセスできるのはローカル コンピューター リソースのみ)

☐ 最上位の特権で実行する(I)

☐ 表示しない(E) 構成(C): Windows Vista™, Windows Server™ 2008

OK キャンセル

14. [トリガー]タブを選択し、手順 13 で変更したトリガーを選択し[編集]をクリックします。
「トリガーの編集」画面が表示されます。



15. 以下のように設定し、[OK]をクリックします。

- ・ タスクの開始：タスクの作成/変更時
- ・ 繰り返し間隔：5 分間
- ・ 継続時間：無期限

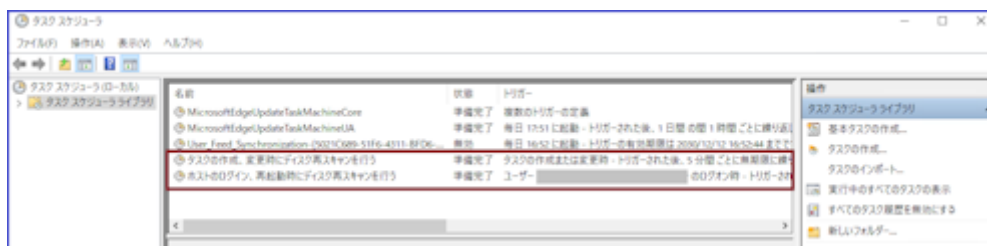
「タスクの作成」画面に戻ります。

16. [OK]をクリックします。

初回実行のスケジューラが開始します。

「タスク スケジューラ」画面に戻ります。

「タスク スケジューラ ライブラリ」を選択し、作成したタスクが表示され、「状態」が「準備完了」になっていることを確認してください。



17. 「タスク スケジューラ」画面を閉じます。



メモ

Windows 搭載のコンピュータノードを、コンピュータネットワークから切断する場合には、作成したタスクスケジューラを削除してください。「タスク スケジューラ」画面で、削除するタスクを選択し、画面右の操作メニューから[削除]をクリックします。

3.4 空状態にあるストレージプールの拡張

ストレージプールが空の状態にあるときに行うストレージプールの拡張について説明します。

3.4.1 空状態にあるストレージプールを拡張する《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

ストレージクラスターの構築を行うと、VSSB 構成ファイル(SystemConfigurationFile.csv)で指定した名称でストレージプールが作成されます。この時点で、ストレージプールは空の状態にあります。そこで、ストレージプールの拡張を実施します。



注意

格納データ暗号化を利用する場合は、本手順の前に「格納データ暗号化の概要」の暗号化環境の設定を有効にする手順およびストレージプールの暗号化の設定を有効にする手順を実施していることを確認してください。本手順を実施後に、暗号化環境の設定およびストレージプールの暗号化の設定を変更することはできません。

この操作の実行には Storage ロールが必要です。Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「初期ユーザーを作成する」に記載の手順が完了している場合、ServiceAdministrators にユーザーが作成されています。ServiceAdministrators には Service ロールと Storage ロールが設定されているため、ServiceAdministrators に作成したユーザーでストレージプールの拡張が行えます。コマンド実行時の認証情報として、そのユーザーのユーザー ID とパスワードを使って、以下の手順を実施してください。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- ストレージプールの拡張を実行すると、内部処理によってストレージノードの CPU の使用率が上昇して、一時的にホスト I/O の性能が低下することがあります。

前提条件

- 実行に必要なロール：Storage

操作手順

- 拡張前のストレージプールの論理容量、ストレージプールの空き容量、ストレージプールの ID、ストレージプールのリビルド領域ポリシーと許容されるドライブ障害数を確認します。
CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。
REST API : GET /v1/objects/pools
CLI : pool_list
- 運用に合わせて必要に応じてリビルド領域ポリシーと許容されるドライブ障害数を変更します。
詳細は「ストレージプールの設定を編集する」を参照してください。



注意

ストレージプールを拡張してからリビルド領域ポリシーを変更しても、リビルド領域を十分確保できない可能性があります。そのため、リビルド領域ポリシーを変更する場合は、ストレージプールを拡張する前に変更してください。

3. 拡張対象のドライブが搭載されたストレージノードの **status** を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

ストレージノードの **status** が "Ready" または "RemovalFailed" のとき、次の手順に進みます。

4. ドライブの ID を確認します。

REST API : GET /v1/objects/drives

CLI : drive_list



ヒント

ストレージプールに組み込まれていないドライブは、**status** が "Offline" のドライブです。ドライブの **status** はドライブ情報から取得できます。

5. ストレージプールを拡張します。

ストレージプールの ID とストレージプールに追加するドライブの ID を指定してコマンドを実行します。

CLI を使う場合はストレージプールの ID の代わりに名前が指定できます。

REST API : POST /v1/objects/pools/<id>/actions/expand/invoke

CLI : pool_expand

コマンド実行後に表示されるジョブの ID を確認します。



注意

他の操作を行う場合は、ストレージプールの拡張後、手順 7 に記載の確認操作が終わってからにしてください。

6. ジョブの ID を指定してジョブの **state** を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。ジョブの完了から約 2 分以内に、内部処理であるストレージコントローラーへの容量割り付け処理が実行されます。この処理の終了によって、追加した容量が使用できるようになります。

ストレージコントローラーへの容量割り付けの処理時間は、このマニュアルの「ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安)」を参照してください。

7. イベントログを取得して、手順 5 で指定したドライブがストレージプールの容量として使用できるようになったことを確認します。

REST API : GET /v1/objects/event-logs

CLI : event_log_list

イベントログ KARS16020-I が、ストレージノードの数だけ出力されるまでお待ちください。それまでは、他の操作が実施できないことがあります。

イベントログ KARS16020-I が、ストレージノードの数だけ出力されたら、指定どおりにストレージプールが拡張できています。

ただし、イベントログ KARS16020-I が、ストレージノードの数だけ出力されるまでの間に、ストレージノードに障害が発生していた場合、ストレージプールの拡張ができていない場合がありますので「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対応してください。

また、イベントログ KARS16046-I が出力された場合は、指定されたドライブの容量またはドライブの数が不足しているため、ユーザーが利用可能な容量である論理容量が構成できていません。

論理容量を構成するためには「容量設計(HPEC 4D+1P の場合)≪Bare metal≫」、「容量設計(HPEC 4D+2P の場合)」または「容量設計(Mirroring の場合)」を参照して必要な容量を算出し、「ドライブを増設する」に従ってストレージプールを拡張してください。



注意

キャッシュ保護付きライトバックモードの状態が有効だった場合、論理容量を構成するためには各ストレージノードで 3 台以上のドライブに対してストレージプール拡張を実行する必要があります。また、キャッシュ保護付きライトバックモードの状態を無効から有効に変更する場合は、変更する前に各ストレージノードで 3 台以上のドライブに対してストレージプール拡張を実行しておく必要があります。詳細は「キャッシュ保護付きライトバックモードを有効にする ≪Bare metal≫」を参照してください。

8. 拡張後のストレージプールの情報を取得します。

REST API : GET /v1/objects/pools

CLI : pool_list

拡張前に比べて拡張後のストレージプールの論理容量とストレージプールの空き容量が拡張されたことを確認します。

9. 構成情報のバックアップを行います。

「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

3.4.2 空状態にあるストレージプールを拡張する ≪Cloud≫

この項での記述内容は Cloud モデルに適用されます。

ストレージクラスターの構築を行うとストレージプールが作成されます。この時点で、ストレージプールは空の状態にあります。そこで、ストレージプールの拡張を実施します。



注意

格納データ暗号化を利用する場合は、本手順の前に「格納データ暗号化の概要」の暗号化環境の設定を有効にする手順およびストレージプールの暗号化の設定を有効にする手順を実施していることを確認してください。本手順を実施後に、暗号化環境の設定およびストレージプールの暗号化の設定を変更することはできません。

この操作の実行には Storage ロールが必要です。ご使用のクラウドプラットフォームに対応した「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「初期ユーザーを作成する」に記載の手順が完了している場合、ServiceAdministrators にユーザーが作成されています。ServiceAdministrators には Service ロールと Storage ロールが設定されているため、ServiceAdministrators に作成したユーザーでストレージプールの拡張が行えます。コマンド実行時の認証情報として、そのユーザーのユーザー ID とパスワードを使って、以下の手順を実施してください。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- ストレージプールの拡張を実行すると、内部処理によってストレージノードの CPU の使用率が上昇して、一時的にホスト I/O の性能が低下することがあります。



メモ

Multi-AZ (Multi-Zone)構成の場合、タイプブレーカーノードにはドライブが存在しないため、手順 3 と 7 での確認対象にタイプブレーカーノードを含める必要はありません。

前提条件

- 実行に必要なロール : **Storage**

操作手順

1. 拡張前のストレージプールの論理容量、ストレージプールの空き容量、ストレージプールの ID、ストレージプールのリビルド領域ポリシーと許容されるドライブ障害数を確認します。
CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。
REST API : GET /v1/objects/pools
CLI : pool_list
2. 運用に合わせて必要に応じてリビルド領域ポリシーと許容されるドライブ障害数を変更します。
詳細は「ストレージプールの設定を編集する」を参照してください。



注意

- ストレージプールを拡張してからリビルド領域ポリシーを変更しても、リビルド領域を十分確保できない可能性があります。そのため、リビルド領域ポリシーを変更する場合は、ストレージプールを拡張する前に変更してください。
- <<Cloud for AWS>>ベースライセンスとして **Floating** を適用している場合、以下に注意してください。
 - 許容されるドライブ障害数の変更によって **AWS License Manager** のライセンスの契約容量を超過する場合があります。許容されるドライブ障害数の変更ができるかどうか「ライセンスの使用量を確認するためにストレージプールの容量を試算する<<Cloud>>」を参照して、ストレージプール拡張後のストレージプールの容量を計算し、ストレージプールの論理容量が **AWS License Manager** のライセンスの契約容量に収まるかを確認してください。なお、必要なライセンスの契約容量は、ストレージプールの論理容量を **TiB** 単位に切り上げて計算してください。
複数のストレージクラスターで **AWS License Manager** のライセンスを共有している場合は、ストレージクラスターそれぞれのストレージプールの論理容量を先に **TiB** 単位に切り上げてから、それらを合計した値が、**AWS License Manager** のライセンスの契約容量に収まるかを確認してください。
(例) 2 つのストレージクラスターがあって、それぞれのストレージプールの論理容量が 31.3[TiB]と 47.7[TiB]の場合、それぞれの値を整数値に切り上げて 32[TiB]と 48[TiB]としてから、それらを合計して 80[TiB]と計算します。
契約容量が不足する場合、**AWS Marketplace** 上でライセンスの契約を更新してください。
 - リビルド領域ポリシーは**"Fixed"**から変更できません。

3. 拡張対象のドライブが搭載されたストレージノードの **status** を確認します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
ストレージノードの **status** が**"Ready"**または**"RemovalFailed"**のとき、次の手順に進みます。
4. ドライブの ID を確認します。
REST API : GET /v1/objects/drives
CLI : drive_list



ヒント

ストレージプールに組み込まれていないドライブは、status が"Offline"のドライブです。ドライブの status はドライブ情報から取得できます。

5. ストレージプールを拡張します。

ストレージプールの ID とストレージプールに追加するドライブの ID を指定してコマンドを実行します。

CLI を使う場合はストレージプールの ID の代わりに名前が指定できます。

REST API : POST /v1/objects/pools/<id >/actions/expand/invoke

CLI : pool_expand

コマンド実行後に表示されるジョブの ID を確認します。



注意

他の操作を行う場合は、ストレージプールの拡張後、手順 7 に記載の確認操作が終わってからにしてください。

6. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。ジョブの完了から約 2 分以内に、内部処理であるストレージコントローラーへの容量割り付け処理が実行されます。この処理の終了によって、追加した容量が使用できるようになります。

ストレージコントローラーへの容量割り付けの処理時間は、このマニュアルの「ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安)」を参照してください。

7. イベントログを取得して、手順 5 で指定したドライブがストレージプールの容量として使用できるようになったことを確認します。

REST API : GET /v1/objects/event-logs

CLI : event_log_list

イベントログ KARS16020-I が、ストレージノードの数だけ出力されるまでお待ちください。それまでは、他の操作が実施できないことがあります。

イベントログ KARS16020-I が、ストレージノードの数だけ出力されたら、指定どおりにストレージプールが拡張できています。

ただし、イベントログ KARS16020-I が、ストレージノードの数だけ出力されるまでの間に、ストレージノードに障害が発生していた場合、ストレージプールの拡張ができていない場合がありますので「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対応してください。

また、イベントログ KARS16046-I が出力された場合は、指定されたドライブの容量またはドライブの数が不足しているため、ユーザーが利用可能な容量である論理容量が構成できていません。

論理容量を構成するためには「容量設計(HPEC 4D+2P の場合)」または「容量設計(Mirroring の場合)」を参照して必要な容量を算出し、「ドライブを増設する」に従ってストレージプールを拡張してください。



メモ

- ・ キャッシュ保護付きライトバックモードの状態が有効だった場合、論理容量を構成するためには各ストレージノードで 3 台以上のドライブに対してストレージプール拡張を実行する必要があります。また、キャッシュ保護付きライトバックモードの状態を無効から有効に変更する場合は、変更する前に各ストレージノードで 3 台以上のドライブに対してストレージプール拡

張を実行しておく必要があります。詳細は「キャッシュ保護付きライトバックモードを有効にする<<Cloud>>」を参照してください。

- <<Cloud for AWS>>ベースライセンスとして **Floating** を適用している場合、ドライブの増設によって **AWS License Manager** のライセンスの契約容量を超過する場合があります。増設手順を実施する前に「ライセンスの使用量を確認するためにストレージプールの容量を試算する<<Cloud>>」を参照して、ドライブ増設後のストレージプールの容量を計算し、ストレージプールの論理容量が **AWS License Manager** のライセンスの契約容量に収まるかを確認してください。なお、必要なライセンスの契約容量は、ストレージプールの論理容量を **TiB** 単位に切り上げて計算してください。

8. 拡張後のストレージプールの情報を取得します。

REST API : GET /v1/objects/pools

CLI : pool_list

拡張前に比べて拡張後のストレージプールの論理容量とストレージプールの空き容量が拡張されたことを確認します。

9. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

3.5 ログイン時・CLI Basic 認証時に表示するメッセージを設定する

VSP One SDS Block Administrator のログイン画面、コンソールインターフェースのログイン時、および CLI Basic 認証時の警告バナーに表示するメッセージが設定できます。

設定に必要なロールは **Security** です。設定されているメッセージを取得するときは、ロールによる実行制限はありません。



メモ

<<Cloud>>コンソールインターフェースでは、ログイン状態でない場合、接続後に以下の操作手順で設定するメッセージを含むログインプロンプトが表示されます。ただし、使用するシリアルコンソールによっては接続後にログインプロンプトが表示されないことがあります。そのときは、コンソール上で「Ctrl」+「U」を入力してから「Enter」キーを押すことでログインプロンプトが表示されます。

前提条件

- 設定に必要なロール : **Security**

操作手順

1. メッセージを設定します。

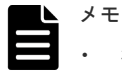
メッセージ本文を指定してコマンドを実行します。削除する場合は空文字を指定します。

最大文字数は 6,144 です。使用できる文字種は、ASCII printable characters です。

REST API : PATCH /configuration/login-message

CLI : login_message_set

コマンド実行後に表示されるジョブの ID を確認します。



メモ

- ・ コンソールインターフェイスの画面サイズは文字数単位で 80 × 24 です。画面サイズを考慮したメッセージを設定してください。文字数が多い場合や改行が多い場合、メッセージの表示が切れることがあります。
- ・ メッセージの設定は、1 分周期で実施される内部処理によってコンソールインターフェイスに反映され、イベントログ KARS20069-I が出力されます。このため、反映が終わるまで一定の時間を要します。
- ・ 以下の操作を実施した場合、イベントログは出力されません。
 - ログイン画面・CLI Basic 認証時の警告バナーに表示するメッセージを設定したが、メッセージの内容に変更がない場合

2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

3. メッセージが正しく設定できたかを確認します。

REST API : GET /configuration/login-message

CLI : login_message_show

設定されているメッセージが表示されます。何も表示されない場合は設定されていません。

4. <<Cloud>>VM インスタンスのシリアルコンソールに接続します。
5. <<Cloud>>ログインプロンプトが表示されたら「Enter」キーを押してログインプロンプトを再表示させ、手順 1 で設定したメッセージが表示されることを確認します。



メモ

使用するシリアルコンソールによっては、接続後にログインプロンプトが表示されないことがあります。そのときは、コンソール上で「Ctrl」+「U」を入力してから「Enter」キーを押してください。この操作を行わない場合、使用するコンソールによっては、手順 1 で設定したメッセージが反映されないままログインプロンプトが表示されることがあります。

6. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



メモ

認証が不要な CLI とセッション認証による CLI の場合は、メッセージが設定されている場合でも表示はされません。

7. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



メモ

認証が不要な CLI とセッション認証による CLI の場合は、メッセージが設定されている場合でも表示はされません。

3.6 許可リストの設定

不正な管理操作を防ぐための、許可リストの設定について説明します。

3.6.1 許可リストを設定する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

不正な管理操作を防ぐために、コントローラーノードの IP アドレスまたは IP アドレスの範囲 (CIDR 表記) を許可リストに設定できます。最大で 10 件設定できます。



注意

- 許可リスト設定時または変更時には、一時的に、REST API、CLI または VSP One SDS Block Administrator の操作はできなくなります。約 30 秒待ってから操作してください。
- VMware vCenter Server Plugin を使用する場合は、VMware vCenter Server の IP アドレスまたは IP アドレスの範囲 (CIDR 表記) を許可リストに設定してください。設定していない場合、VMware vCenter Server から情報の参照ができなくなります。
- コンソールインターフェイスの操作は許可リスト設定では制限できません。コンソールインターフェイスの操作を制限する場合、ストレージノードごとの BMC が提供するセキュリティー設定を使用して制限を行ってください。詳細は、ストレージノードとして使用する物理サーバーのベンダーが提供する BMC のユーザーガイドを参照して確認してください。

前提条件

- 設定に必要なロール：Security

操作手順

1. 許可リスト設定を編集します。

許可リストの有効/無効と、許可リストに設定するコントローラーノードの IP アドレス (IPv4) または IP アドレス (IPv4) の範囲 (CIDR 表記) を指定してコマンドを実行します。

設定内容は上書きされます。

REST API : PATCH /v1/objects/web-server-access-setting

CLI : web_server_access_setting_set

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

3. 正しく設定できたかを確認します。

REST API : GET /v1/objects/web-server-access-setting

CLI : web_server_access_setting_show

コマンド実行後のレスポンスに設定内容が表示されます。

4. 構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

3.6.2 許可リストを設定する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

不正な管理操作を防ぐために、以下の IP アドレスまたは IP アドレスの範囲(CIDR 表記)を許可リストに設定できます。

- コントローラーノード
- ロードバランサー
- <<Cloud for Google Cloud>>ヘルスチェックプローブ
- <<Cloud for Microsoft Azure>>ヘルスチェックプローブ

最大で 10 件設定できます。



注意

- 許可リスト設定時または変更時には、一時的に、REST API、CLI または VSP One SDS Block Administrator の操作はできなくなります。約 30 秒待ってから操作してください。
- VMware vCenter Server Plugin を使用する場合は、VMware vCenter Server の IP アドレスまたは IP アドレスの範囲(CIDR 表記)を許可リストに設定してください。設定していない場合、VMware vCenter Server から情報の参照ができなくなります。
- ヘルスチェックプローブとは、ロードバランサーの正常状態を検出する機能です。
 - <<Cloud for Google Cloud>>ロードバランサーは、ヘルスチェックプローブの固有のアドレスを使用しているため、ヘルスチェックプローブの IP アドレス(IPv4)の範囲(CIDR 表記)も許可リストに設定してください。ヘルスチェックプローブのアドレスは、Google Cloud のドキュメントを参照してください。
 - <<Cloud for Microsoft Azure>>ロードバランサーは、ヘルスチェックプローブの固有のアドレスを使用しているため、ヘルスチェックプローブの IP アドレス(IPv4)も許可リストに設定してください。ヘルスチェックプローブのアドレスは、Microsoft Azure のドキュメントを参照してください。

前提条件

- 設定に必要なロール : Security

操作手順

1. 許可リスト設定を編集します。

許可リストの有効/無効と、許可リストに設定する上記のリソースの IP アドレス(IPv4)または IP アドレス(IPv4)の範囲(CIDR 表記)を指定してコマンドを実行します。

設定内容は上書きされます。

REST API : PATCH /v1/objects/web-server-access-setting

CLI : web_server_access_setting_set

コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。
3. 正しく設定できたかを確認します。

REST API : GET /v1/objects/web-server-access-setting

CLI : web_server_access_setting_show

コマンド実行後のレスポンスに設定内容が表示されます。
4. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする《Bare metal》《Cloud for AWS》」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

ライセンスを管理する

- 4.1 ライセンス管理の概要
- 4.2 ライセンスの登録
- 4.3 ライセンスの削除
- 4.4 ライセンス情報の取得
- 4.5 ライセンスの設定値の編集
- 4.6 ライセンス設定情報の取得

4.1 ライセンス管理の概要

ライセンス管理の概要について説明します。

4.1.1 ライセンス管理の概要<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

VSP One SDS Block の利用にはライセンスが必要です。ストレージクラスターを構築すると、VSP One SDS Block のベースライセンスの Trial ライセンスが登録された状態でストレージクラスターが構築されます。Trial ライセンスの有効期間は 60 日です。有効期間後も VSP One SDS Block を継続して利用するには、Trial ライセンス以外のベースライセンスの登録が必要です。



メモ

個別の付加価値機能を有効にするには、対象とする付加価値機能のプログラムプロダクトライセンスの登録が必要です。

ライセンスの発行と登録

ライセンスの発行および登録に当たっては、営業担当またはサポートセンターに連絡し、ライセンスキーを購入してください。ライセンスキーを購入する際には、ストレージクラスターの ID、対象となるプログラムプロダクト、ライセンスの種類の提示が必要になります。また、ライセンスの種類によって、契約容量や契約期間の提示が必要になります。

ストレージクラスターの ID は「ストレージクラスターの情報を取得する」に記載のコマンドか、VSP One SDS Block Administrator の Storage Cluster Information アイコンから取得できます。



注意

- ストレージクラスターを再構築すると、再構築前に発行されたライセンスキーは新しいストレージクラスターでは使用できません。その際は、営業担当またはサポートセンターに連絡して、新しいストレージクラスターの ID に対応したライセンスキーの再発行を依頼してください。
- 一度登録したライセンスキーを再度指定してライセンスを登録することはできません。ライセンスを削除する際には注意してください。

ライセンスの区分と種類

VSP One SDS Block の各プログラムプロダクトにはライセンスがあります。プログラムプロダクトは基本機能と個別の付加価値機能の区分に分類されます。それに対するライセンスとして、基本機能を有効にするベースライセンスと、個別の付加価値機能を有効にするプログラムプロダクトライセンスがあります。各プログラムプロダクトには、利用できる容量や期間が異なる数種類のライセンスがあります。個別の付加価値機能を有効にするには、対象とする付加価値機能のプログラムプロダクトライセンスのみではなく、前提としてベースライセンスが必要です。

区分	種類
ベースライセンス	Trial
	Perpetual*
	Subscription
プログラムプロダクトライセンス	Trial*
	Perpetual
	Subscription*

区分	種類
* 現在は提供されていません。	

ベースライセンスにおけるライセンスの種類

種類	有効期間	従量課金	容量制限	説明
Trial	あり	なし	なし	ストレージクラスターを構築した際にインストールされるライセンスの種類です。有効期間が 60 日のため、有効期間後も継続して使用するには、ライセンスの種類のうち Perpetual または Subscription のライセンス登録が必要です。
Perpetual	なし	なし	あり	指定容量(ストレージプールに登録できる容量)の使用権を買い取って、永続的に使用できます。 既存のベースライセンスのライセンスの種類が Perpetual だったとき、新たに登録できるベースライセンスのライセンスの種類は、Perpetual または Subscription です。 Subscription ライセンスをあとから登録した場合は、Subscription ライセンスの有効期間を超えるか、Subscription ライセンスを削除すると Perpetual ライセンスに戻ります。
Subscription	あり	なし	あり	使用する期間を決めて、指定容量(ストレージプールに登録できる容量)を使用できます。 既存のベースライセンスのライセンスの種類が Subscription だったとき、新たに登録できるベースライセンスのライセンスの種類は、Perpetual または Subscription です。

プログラムプロダクトライセンスにおけるライセンスの種類

現在、提供しているプログラムプロダクトライセンスのライセンス種類は下記のみです。

種類	有効期間	従量課金	容量制限	説明
Perpetual	なし	なし	なし	ストレージプールに登録できる容量の制限なしで、個別の機能を永続的に使用できます。ただし、ベースライセンスの容量制限を超えて使用することはできません。 ベースライセンスのライセンスの種類が Trial 以外のとき、このライセンスが登録できます。

プログラムプロダクトごとのライセンスの提供状況

プログラムプロダクト名	ライセンスの区分	ライセンスの種類	ライセンスの提供有無	説明
Hitachi SDS Core Base	ベースライセンス	Trial	○ (構築時にインストール済み)	VSP One SDS Block 使用有効期間、ストレージプールの使用可能容量を管理するライセンスです。ストレージクラスターの構築を行うと、有効期間 60 日、従量課金なし、容量制限なしの
		Perpetual	×	
		Subscription	○	

プログラムプロダクト名	ライセンスの区分	ライセンスの種類	ライセンスの提供有無	説明
				Trial ライセンスが自動で適用されます。 Perpetual については現在は提供されていません。
Data At Rest Encryption	プログラムプロダクトライセンス	Perpetual	○	格納データ暗号化を有効にするためのライセンスです。格納データ暗号化の詳細はこのマニュアルの「格納データ暗号化の概要」を参照してください。 暗号化環境の設定を有効にしている場合、このライセンスは削除できません。

ライセンスの有効期間

ベースライセンスが Trial、または Subscription の場合、ライセンスの有効期間の起点は、VSP One SDS Block をセットアップまたはライセンスを登録した日時です。また、有効期間の終点は、最終日の 23 時 59 分になります。例えば、契約期間が 1 年の Subscription ライセンスを August 5 2020 13:00 に登録すると、August 5 2021 23:59 までライセンスは有効です。

ライセンスの容量

Perpetual と Subscription ライセンスにおける容量とは「ストレージプールの情報の一覧を取得する」または「ストレージプールの情報を個別に取得する」で得られる totalCapacity[MiB](ストレージプールの論理容量)です。totalCapacity については「ストレージプールの容量情報」を参照してください。

ライセンスの status と statusSummary

ライセンスの status は、そのライセンスが有効であるかどうかを示すものです。また、statusSummary は、エラー状態であるかどうかを示すものです。status と statusSummary は「ライセンス情報の一覧を取得する」または「ライセンス情報を個別に取得する」に記載の操作で得られます。

status	説明	statusSummary
Active	ライセンスが有効な状態です。 - ライセンスを登録するとそのライセンスは"Active"になります。 - 既存の"Active"なライセンスが有効期間中に、有効期間が重なる別の種類のライセンスが登録されると、有効期間が重なっている間、既存のライセンスは"Overwritten"になります。	Normal
Warning	ライセンスは有効ですが、使用容量または使用期間が以下の状態にあります。 Perpetual の場合 - 警告しきい値 ≤ 使用容量 ≤ 契約容量 Subscription の場合(以下のどちらか) - 警告しきい値 ≤ 使用容量 ≤ 契約容量 - 警告しきい値 ≤ 使用期間 ≤ 契約期間	Warning

status	説明	statusSummary
	原因がいずれかであるかは「ライセンス情報の一覧を取得する」または「ライセンス情報を個別に取得する」で得られる cause で判別できます。 "Warning"になった際は、警告のイベントログが出力されます。ユーザーが警告しきい値を変更したり、警告しきい値の原因を取り除いたりすることで"Active"になります。	
GracePeriod	使用容量または使用期間が以下の状態にあります。 Perpetual の場合 - 契約容量 < 使用容量 Subscription の場合(以下のどちらか) - 契約容量 < 使用容量 - 契約期間 < 使用期間 原因がいずれかであるかは「ライセンス情報の一覧を取得する」または「ライセンス情報を個別に取得する」で得られる cause で判別できます。 "GracePeriod"になった際は、警告のイベントログが出力されます。 "GracePeriod"のまま 30 日を超過すると、"Invalid"になります。 "GracePeriod"の状態中に、日数追加や容量追加のライセンスが登録されると"Active"になります。	Error
Invalid	ライセンスが無効な状態です。エラーのイベントログが通知されます。"Invalid"のときでも I/O は可能です。 "Invalid"状態のときはストレージクラスターに対する管理操作が基本的に制限され、実施できません。ただし、次の操作は"Invalid"状態時でも実施できます。 - ライセンスを登録・解除する操作 - ユーザー管理の操作 - ストレージクラスター内の各リソースの情報取得 - ストレージクラスターの停止 - ダンプログファイルの採取	Error



メモ

上記以外の status として、"Overwritten"があります。status が"Overwritten"になるのは、競合するライセンスがほかに存在するために当該ライセンスが一時的に無効になっている状態です。

既存の有効なライセンスよりあとに、有効期間が重なるライセンスを登録したとき、既存のライセンスは"Overwritten"になります。また、あとから登録したライセンスは"Active"になります。あとから登録したライセンスの有効期間が切れたり、削除されたりした場合、既存のライセンスは"Overwritten"から"Active"になります。このとき、既存のライセンスが有効期間切れや容量超過であったときは、既存のライセンスは"Overwritten"が終わったあと"GracePeriod"になります。

例えば、600TiB を使用している状況にあるとき、500TiB の Perpetual ライセンスを登録すると、その Perpetual ライセンスは"GracePeriod"になります。この状況で、600TiB の Subscription ライセンスを登録すると、Perpetual ライセンスは"Overwritten"になり、Subscription ライセンスは"Active"になります。

警告しきい値の設定

ライセンスの有効期間の残り日数や使用容量の警告しきい値は、デフォルトでそれぞれ 30 日、80% に設定されています。ライセンスの有効期間の残り日数が警告しきい値以下、または使用容量が警告しきい値以上になると、イベントログで警告通知を受け取ることができます。警告しきい値の設定を変更する場合は「ライセンスの警告しきい値を編集する<<Bare metal>>」を参照してください。

4.1.2 ライセンス管理の概要<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

VSP One SDS Block の利用にはライセンスが必要です。各クラウドプラットフォームの Marketplace で選択する料金モデルによって、ストレージクラスター構築時のベースライセンスが異なります。

- BYOL(Bring Your Own License)を選択した場合：
VSP One SDS Block のベースライセンスの Trial ライセンスが登録された状態でストレージクラスターが構築されます。Trial ライセンスの有効期間は 60 日です。有効期間後も VSP One SDS Block を継続して利用するには、Trial ライセンス以外のベースライセンスの登録が必要です。
- <<Cloud for AWS>>Usage Pricing を選択した場合：
VSP One SDS Block のベースライセンスの Utility ライセンスが登録された状態でストレージクラスターが構築されます。Utility ライセンスのベースライセンスには有効期間がないため、継続して利用できます。
- <<Cloud for AWS>>Contract を選択した場合：
VSP One SDS Block のベースライセンスの Floating ライセンスが登録された状態でストレージクラスターが構築されます。AWS Marketplace 上での契約に応じて一定の容量が、一定の期間だけ利用できます。



メモ

- 個別の付加価値機能を有効にするには、対象とする付加価値機能のプログラムプロダクトライセンスの登録が必要です。
- 利用可能なライセンスは、VSP One SDS Block をご利用になる地域で異なります。ご利用の地域で利用可能なライセンスは、サポートセンターにお問い合わせください。

ライセンスの発行と登録

ライセンスの発行および登録に当たっては、営業担当またはサポートセンターに連絡し、ライセンスキーを購入してください。ライセンスキーを購入する際には、ストレージクラスターの ID、対象となるプログラムプロダクト、ライセンスの種類の提示が必要になります。また、ライセンスの種類によって、契約容量や契約期間の提示が必要になります。

<<Cloud for AWS>>ベースライセンスとして Floating を適用する場合、ライセンスの契約は AWS Marketplace 上で行います。また、ライセンスの購入はストレージクラスター構築前に必要です。

ストレージクラスターの ID は「ストレージクラスターの情報を取得する」に記載のコマンドか、VSP One SDS Block Administrator の Storage Cluster Information アイコンから取得できます。



注意

- ストレージクラスターを再構築すると、再構築前に発行されたライセンスキーは新しいストレージクラスターでは使用できません。その際は、営業担当またはサポートセンターに連絡して、新しいストレージクラスターの ID に対応したライセンスキーの再発行を依頼してください。
- 一度登録したライセンスキーを再度指定してライセンスを登録することはできません。ライセンスを削除する際には注意してください。

ライセンスの区分と種類

VSP One SDS Block の各プログラムプロダクトにはライセンスがあります。プログラムプロダクトは基本機能と個別の付加価値機能の区分に分類されます。それに対するライセンスとして、基本

機能を有効にするベースライセンスと、個別の付加価値機能を有効にするプログラムプロダクトライセンスがあります。各プログラムプロダクトには、利用できる容量や期間が異なる数種類のライセンスがあります。個別の付加価値機能を有効にするには、対象とする付加価値機能のプログラムプロダクトライセンスのみではなく、前提としてベースライセンスが必要です。

区分	種類
ベースライセンス	Trial
	Perpetual*
	Subscription
	Utility
	Floating
プログラムプロダクトライセンス	Trial*
	Perpetual
	Subscription*
* 現在は提供されていません。	

ベースライセンスにおけるライセンスの種類

種類	有効期間	従量課金	容量制限	説明
Trial	あり	なし	なし	ストレージクラスターを構築した際にインストールされるライセンスの種類です。有効期間が 60 日のため、有効期間後も継続して使用するには、ライセンスの種類のうち Perpetual または Subscription のライセンス登録が必要です。
Perpetual	なし	なし	あり	指定容量(ストレージプールに登録できる容量)の使用権を買い取って、永続的に使用できます。 既存のベースライセンスのライセンスの種類が Perpetual だったとき、新たに登録できるベースライセンスのライセンスの種類は、Perpetual または Subscription です。 Subscription ライセンスをあとから登録した場合は、Subscription ライセンスの有効期間を超えるか、Subscription ライセンスを削除すると Perpetual ライセンスに戻ります。
Subscription	あり	なし	あり	使用する期間を決めて、指定容量(ストレージプールに登録できる容量)を使用できます。 既存のベースライセンスのライセンスの種類が Subscription だったとき、新たに登録できるベースライセンスのライセンスの種類は、Perpetual または Subscription です。
«Cloud for AWS»Utility	なし	あり	なし	AWS Marketplace で VSP One SDS Block の Usage Pricing を選択してストレージクラスターを構築した際にインストールされるベースライセンスのライセンスの種類です。Utility ライセンスには有効期間と使用容量に制限がないため、継続的に使用できます。ただし、使用容量に対して従量制で課金されます。このライセンスからほかのライセンスの種類への移行はできません。

種類	有効期間	従量課金	容量制限	説明
«Cloud for AWS»Floating*	あり	なし	あり	AWS Marketplace で VSP One SDS Block の Contract を選択してストレージクラスターを構築した際にインストールされるベースライセンスのライセンスの種類です。Floating ライセンスでは、AWS Marketplace 上での契約に応じて、容量と期間について一定の使用権が得られます。使用できる容量や期間を超過した場合は、猶予期間(30 日)のあと、イベントログ通知とともに構成変更が禁止されます。構成変更できるようにするためには、AWS 上での契約容量の追加や契約期間の延長のための再契約が必要になります。 Floating ライセンスの契約は AWS Marketplace 上で行います。 このライセンスからほかのライセンスの種類への移行はできません。
* «Cloud for AWS»Floating ライセンスでは、契約期間と契約容量については、AWS License Manager のライセンスで管理されます。 AWS License Manager のライセンスは契約と運用上の留意事項があります。詳細は「Contract 製品のライセンス」を参照してください。				

プログラムプロダクトライセンスにおけるライセンスの種類

現在、提供しているプログラムプロダクトライセンスのライセンス種類は下記のみです。

種類	有効期間	従量課金	容量制限	説明
Perpetual	なし	なし	なし	ストレージプールに登録できる容量の制限なしで、個別の機能を永続的に使用できます。ただし、ベースライセンスの容量制限を超えて使用することはできません。 ベースライセンスのライセンスの種類が Trial 以外のとき、このライセンスが登録できます。

プログラムプロダクトごとのライセンスの提供状況

プログラムプロダクト名	ライセンスの区分	ライセンスの種類	ライセンスの提供有無	説明
Hitachi SDS Core Base	ベースライセンス	Trial	○ (構築時にインストール済み)	料金モデルに BYOL を選択した場合、VSP One SDS Block 使用有効期間、ストレージプールの使用可能容量を管理するライセンスです。ストレージクラスターの構築を行うと、有効期間 60 日、従量課金なし、容量制限なしの Trial ライセンスが自動で適用されます。 Perpetual については現在は提供されていません。 «Cloud for AWS»AWS Marketplace で VSP One SDS Block の Usage Pricing を選択してストレージクラスターの構築を行うと、有効期間なし、従
		Perpetual	×	
		Subscription	○	
		«Cloud for AWS»Utility	○ (構築時にインストール済み)	
		«Cloud for AWS»Floating	○ (構築時にインストール済み)	

プログラムブ ロダクト名	ライセンスの 区分	ライセンスの 種類	ライセンスの提供 有無	説明
				量課金あり、容量制限なしの Utility ライセンスが自動で適用 されます。 ≪Cloud for AWS≫AWS Marketplace で VSP One SDS Block の Contract を選択してス トレージクラスターの構築を行 うと、AWS Marketplace 上での 契約に応じて、容量と期間につ いて一定の使用権がある Floating ライセンスが自動で適 用されます。
Data At Rest Encryption	プログラムプロ ダクトライセン ス	Perpetual	○	格納データ暗号化を有効にする ためのライセンスです。格納デ ータ暗号化の詳細はこのマニ ュアルの「格納データ暗号化の概 要」を参照してください。 暗号化環境の設定を有効にして いる場合、このライセンスは削 除できません。

ライセンスの有効期間

ベースライセンスが Trial、または Subscription の場合、ライセンスの有効期間の起点は、VSP One SDS Block をセットアップまたはライセンスを登録した日時です。また、有効期間の終点は、最終日の 23 時 59 分になります。例えば、契約期間が 1 年の Subscription ライセンスを August 5 2020 13:00 に登録すると、August 5 2021 23:59 までライセンスは有効です。

≪Cloud for AWS≫ベースライセンスが Floating の場合、ライセンスの有効期間の起点と終点は、AWS License Manager のライセンスによって決まります。ベースライセンスが Utility の場合、有効期間はありません。

ライセンスの容量

以下のライセンスにおける容量とは「ストレージプールの情報の一覧を取得する」または「ストレージプールの情報を個別に取得する」で得られる totalCapacity[MiB](ストレージプールの論理容量)です。totalCapacity については「ストレージプールの容量情報」を参照してください。

Perpetual ライセンス、Subscription ライセンス、Utility ライセンス、Floating ライセンス

≪Cloud for AWS≫ライセンスの従量課金

ベースライセンスが Utility の場合、使用した容量に対して従量制で課金されます。課金対象はストレージプールの論理容量になります。ストレージクラスターの起動時と、以降 1 時間ごとに AWS へ課金情報が送信されます。仮に、AWS への課金情報の送信に 2 時間以上失敗すると、VSP One SDS Block のライセンスの status が "Invalid" になります。



メモ

- ・ ストレージプールの論理容量については、このマニュアルの「ストレージプールの容量情報」に記載されている totalCapacity[MiB]を参照してください。

- ・ ストレージクラスターの再起動などで AWS へ課金情報が複数回送信される場合があります。その場合は、1 時間以内の同じ時間帯で最初に送信された課金情報が AWS に適用されます。

《Cloud for AWS》Contract 製品のライセンス

Contract 製品の AWS License Manager のライセンスは、以下の特徴があります。

- ・ AWS License Manager のライセンスは、初回の VSP One SDS Block のストレージクラスター構築時に契約する
- ・ AWS License Manager のライセンスを契約すると一定の容量と期間の使用権が得られる
- ・ AWS License Manager のライセンスは AWS アカウントに対して 1 つだけ契約が可能
(ストレージクラスターごとに個別にライセンスを契約することは不可。また、同一の AWS アカウントで複数のストレージクラスターを構築する場合、ライセンスの契約容量が共有される)

このため、最初のストレージクラスターを構築する前には以下の点に留意する必要があります。

- ・ ストレージクラスターの構築前に、AWS License Manager のライセンスの契約期間と契約容量を決めておくこと
- ・ ストレージクラスターを単体または複数で運用するかを決めた上で、使用する最大容量を算出して契約容量とすること



注意

AWS License Manager のライセンスを一度契約したあとにライセンスの契約容量を追加しようとする、そのライセンスの契約開始までさかのぼって再契約が必要になる場合があります。そのため、将来のストレージプールの論理容量の追加を考慮して、ライセンスの契約容量を決定してください。



メモ

- ・ AWS License Manager のライセンスの契約容量は、VSP One SDS Block のストレージプールの論理容量が対象となります。容量設計に関しては、「容量設計(HPEC 4D+2P の場合)」または「容量設計(Mirroring の場合)」を参照してください。
- ・ AWS License Manager のライセンスで必要となる契約容量は、VSP One SDS Block のストレージプールの論理容量を TiB 単位に切り上げて計算してください。
同一の AWS アカウントで複数のストレージクラスターを構築する場合は、それぞれのストレージクラスターが必要とするストレージプールの論理容量を TiB 単位に切り上げてから、それらを合計し、その値をライセンスの契約容量としてください。
(例) 2 つのストレージクラスターがあつて、それぞれのストレージプールの論理容量が 31.3[TiB]と 47.7[TiB]の場合、それぞれの値を整数値に切り上げて 32[TiB]と 48[TiB]としてから、それらを合計して 80[TiB]と計算します。

ストレージクラスターの運用開始後、AWS License Manager のライセンス違反については以下の点に留意してください。

- ・ AWS License Manager のライセンスのライセンス違反には、以下の 3 つの要因があります。
 - 契約期間の超過
 - 契約容量の超過
 - VSP One SDS Block と AWS License Manager 間の通信が 60 分不通AWS License Manager のライセンス違反が発生した場合、それぞれ以下のとおり VSP One SDS Block が制限されます。
<契約期間の超過の場合>
- ・ AWS License Manager のライセンス : VSP One SDS Block のストレージクラスター構築、ストレージノード増設、ストレージノード交換ができなくなります。

- Floating ライセンス：status が GracePeriod に移行し猶予期間(30 日)に入ります。
<契約容量の超過の場合>
- AWS License Manager のライセンス：制限はありません。
- Floating ライセンス：status が GracePeriod に移行し猶予期間(30 日)に入ります。
<VSP One SDS Block と AWS License Manager 間の通信が 60 分不通になった場合>
- AWS License Manager のライセンス：通信が不通となった VSP One SDS Block の容量使用権(ストレージクラスターで利用できるストレージプールの論理容量)が回収されます。
- Floating ライセンス：status が GracePeriod に移行し猶予期間(30 日)に入ります。
- AWS License Manager のライセンスの使用量は、ユーザー責任で管理が必要です。複数のストレージクラスターで使用する場合には、ストレージクラスターごとのストレージプールの使用量を管理してください。
- ストレージプールの論理容量が変化する VSP One SDS Block の構成変更を実施する際には、AWS License Manager のライセンスの契約容量を超過しないよう、容量を試算したあとに構成変更を実施してください。
なお、構成変更により AWS License Manager のライセンス違反が発生する場合に備えて、VSP One SDS Block は構成変更を失敗させる機能があります。この機能は、設定により許可、不許可を設定できます。デフォルトは不許可です。設定については「ライセンスの設定値を編集する<<Cloud>>」を参照してください。
構成変更の結果ライセンス違反が発生すると、VSP One SDS Block の Floating ライセンスの Status が GracePeriod に遷移します。その場合は AWS License Manager のライセンス違反状態を解消してください。



メモ

- ドライブやストレージノードの増設、許容されるドライブ障害数の変更によるストレージプールの論理容量の試算は「ライセンスの使用量を確認するためにストレージプールの容量を試算する<<Cloud>>」を参照してください。
- 必要なライセンスの契約容量は、ストレージプールの論理容量を TiB 単位に切り上げて計算してください。複数のストレージクラスターで AWS License Manager のライセンスを共有している場合は、ストレージクラスターそれぞれのストレージプールの論理容量を先に TiB 単位に切り上げてから、それらを合計した値が、AWS License Manager のライセンスの契約容量に収まるかを確認してください。
(例) 2 つのストレージクラスターがあつて、それぞれのストレージプールの論理容量が 31.3[TiB]と 47.7[TiB]の場合、それぞれの値を整数値に切り上げて 32[TiB]と 48[TiB]としてから、それらを合計して 80[TiB]と計算します。
契約容量が不足する場合、AWS Marketplace 上でライセンスの契約を更新してください。

AWS License Manager のライセンスの管理については以下の点に留意してください。

- 以下の場合、AWS License Manager のライセンスから VSP One SDS Block に与えられている容量使用権が、AWS License Manager に返却されます。
 - ストレージクラスターの停止時
 - 障害などで VSP One SDS Block と AWS License Manager 間の通信が 60 分不通になった場合
返却された容量使用権は以下のタイミングで再度確保されます。
 - 停止したストレージクラスターの起動後
 - VSP One SDS Block と AWS License Manager 間の不通が解消されたあと
- VSP One SDS Block は、AWS License Manager に対して 15 分周期でライセンスの契約期間と契約容量の問い合わせを行います。問い合わせ結果を VSP One SDS Block が管理する

Floating ライセンスの情報に反映します。そのため、契約容量の追加や契約期間の延長の再契約、またはほかのストレージクラスターの状況が変化したなど、AWS License Manager のライセンス情報が変化した場合は、VSP One SDS Block の管理する Floating ライセンスの情報を更新するまでに最大で 15 分時間が掛かることがあります。



メモ

ストレージプールの論理容量が変化する VSP One SDS Block の構成変更を実施した場合、容量使用権が AWS License Manager に返却されますが、構成変更の処理の中で再度確保されます。

ライセンスの status と statusSummary

ライセンスの status は、そのライセンスが有効であるかどうかを示すものです。また、statusSummary は、エラー状態であるかどうかを示すものです。status と statusSummary は「ライセンス情報の一覧を取得する」または「ライセンス情報を個別に取得する」に記載の操作で得られます。

status	説明	statusSummary
Active	ライセンスが有効な状態です。 - ライセンスを登録するとそのライセンスは"Active"になります。 - 既存の"Active"なライセンスが有効期間中に、有効期間が重なる別の種類のライセンスが登録されると、有効期間が重なっている間、既存のライセンスは"Overwritten"になります。	Normal
Warning	ライセンスは有効ですが、使用容量または使用期間が以下の状態にあります。 Perpetual の場合 - 警告しきい値 ≤ 使用容量 ≤ 契約容量 Subscription の場合(以下のどちらか) - 警告しきい値 ≤ 使用容量 ≤ 契約容量 - 警告しきい値 ≤ 使用期間 ≤ 契約期間 ≪Cloud for AWS≫Floating の場合(以下のどちらか) - 警告しきい値 ≤ 使用容量 ≤ 契約容量* - 警告しきい値 ≤ 使用期間 ≤ 契約期間 原因がいずれかであるかは「ライセンス情報の一覧を取得する」または「ライセンス情報を個別に取得する」で得られる cause で判別できます。 "Warning"になった際は、警告のイベントログが出力されます。ユーザーが警告しきい値を変更したり、警告しきい値の原因を取り除いたりすることで"Active"になります。	Warning
GracePeriod	使用容量または使用期間が以下の状態にあります。 Perpetual の場合 - 契約容量 < 使用容量 Subscription の場合(以下のどちらか) - 契約容量 < 使用容量 - 契約期間 < 使用期間 ≪Cloud for AWS≫Floating の場合(以下のどちらか) - 契約容量* < 使用容量 - 契約期間 < 使用期間 原因がいずれかであるかは「ライセンス情報の一覧を取得する」または「ライセンス情報を個別に取得する」で得られる cause で判別できます。 "GracePeriod"になった際は、警告のイベントログが出力されます。	Error

status	説明	statusSummary
	"GracePeriod"のまま 30 日を超過すると、"Invalid"になります。 "GracePeriod"の状態中に、日数追加や容量追加のライセンスが登録されると"Active"になります。 ≪Cloud for AWS≫ベースライセンスが Floating の場合、"Active"にするためには AWS Marketplace 上でライセンス契約を更新する必要があります。 ≪Cloud for AWS≫ベースライセンスが Floating の場合、VSP One SDS Block が AWS License Manager との通信に失敗した場合も "GracePeriod"になります。 ≪Cloud for AWS≫ベースライセンスが Floating の場合、契約期間の超過が原因で AWS License Manager のライセンスが無効のときは、ストレージクラスターの構築、ストレージノードの増設、ストレージノードの交換はできません。	
Invalid	ライセンスが無効な状態です。エラーのイベントログが通知されます。"Invalid"のときでも I/O は可能です。 "Invalid"状態のときはストレージクラスターに対する管理操作が基本的に制限され、実施できません。ただし、次の操作は"Invalid"状態時でも実施できます。 ・ ライセンスを登録・解除する操作 ・ ユーザー管理の操作 ・ ストレージクラスター内の各リソースの情報取得 ・ ストレージクラスターの停止 ・ ダンプログファイルの採取	Error
* ≪Cloud for AWS≫ベースライセンスが Floating の場合、契約容量は以下の計算式で求められます。 AWS License Manager 上のライセンスの最大容量 - AWS License Manager 上のライセンスの総使用量 + 自身のストレージクラスターが確保した AWS License Manager 上のライセンスの使用量		



メモ

上記以外の status として、"Overwritten"があります。status が"Overwritten"になるのは、競合するライセンスがほかに存在するために当該ライセンスが一時的に無効になっている状態です。

既存の有効なライセンスよりあとに、有効期間が重なるライセンスを登録したとき、既存のライセンスは"Overwritten"になります。また、あとから登録したライセンスは"Active"になります。あとから登録したライセンスの有効期間が切れたり、削除されたりした場合、既存のライセンスは"Overwritten"から"Active"になります。このとき、既存のライセンスが有効期間切れや容量超過であったときは、既存のライセンスは"Overwritten"が終わったあと"GracePeriod"になります。

例えば、600TiB を使用している状況にあるとき、500TiB の Perpetual ライセンスを登録すると、その Perpetual ライセンスは"GracePeriod"になります。この状況で、600TiB の Subscription ライセンスを登録すると、Perpetual ライセンスは"Overwritten"になり、Subscription ライセンスは"Active"になります。

ライセンスの設定値の編集

ライセンスの有効期間の残り日数や使用容量の警告しきい値は、デフォルトでそれぞれ 30 日、80% に設定されています。ライセンスの有効期間の残り日数が警告しきい値以下、または使用容量が警告しきい値以上になると、イベントログで警告通知を受け取ることができます。

≪Cloud for AWS≫ベースライセンスが Floating の場合、構成変更による AWS License Manager のライセンス違反発生時の備えとして、構成変更による AWS License Manager のライセンス違反時における、構成変更の許可・不許可(デフォルト。構成変更は失敗になる)についての設定もできます。

ライセンスの設定値を変更する場合は「ライセンスの設定値を編集する<<Cloud>>」を参照してください。

4.2 ライセンスの登録

ライセンスの登録方法について説明します。

4.2.1 ライセンスを登録する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ライセンスを登録します。

プログラムプロダクトライセンスは、ベースライセンスが Trial 以外の場合のみ登録できます。



注意

- ストレージクラスターを再構築すると、再構築前に発行されたライセンスキーは新しいストレージクラスターでは使用できません。その際は、営業担当に連絡して、新しいストレージクラスターの ID に対応したライセンスキーの再発行を依頼して、再発行されたライセンスキーを指定してライセンスを登録してください。
- 同じプログラムプロダクトのライセンスを追加で登録する場合、登録済みのライセンスより発行時刻が古いライセンスキーは指定できません。新しいライセンスキーの再発行を依頼して、再発行されたライセンスキーを指定してライセンスを登録してください。

前提条件

- 実行に必要なロール：Storage

操作手順

1. 営業担当に連絡してライセンスキーを購入します。

ライセンスキーを購入する際には、ストレージクラスターの ID、ライセンスの種類の提示が必要になります。また、ライセンスの種類によって、契約容量や契約期間の提示が必要になります。

ストレージクラスターの ID は「ストレージクラスターの情報を取得する」に記載のコマンドか、VSP One SDS Block Administrator の Storage Cluster Information アイコンから取得できます。

2. ライセンスを登録します。

ライセンスキーを指定してコマンドを実行します。

REST API : POST /v1/objects/licenses

CLI : license_install

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

affectedResources に削除されたライセンスと追加されたライセンスの両方が表示されます。

state が"Succeeded"になっていたらジョブは完了です。

4. 構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

4.2.2 ライセンスを登録する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ライセンスを登録します。

プログラムプロダクトライセンスは、ベースライセンスが Trial 以外の場合のみ登録できます。



注意

- ・ ストレージクラスターを再構築すると、再構築前に発行されたライセンスキーは新しいストレージクラスターでは使用できません。その際は、営業担当に連絡して、新しいストレージクラスターの ID に対応したライセンスキーの再発行を依頼して、再発行されたライセンスキーを指定してライセンスを登録してください。
- ・ 同じプログラムプロダクトのライセンスを追加で登録する場合、登録済みのライセンスより発行時刻が古いライセンスキーは指定できません。新しいライセンスキーの再発行を依頼して、再発行されたライセンスキーを指定してライセンスを登録してください。



メモ

<<Cloud for AWS>>ベースライセンスが Utility または Floating の場合、ライセンス登録の必要はありません。

前提条件

- ・ 実行に必要なロール : Storage

操作手順

1. 営業担当に連絡してライセンスキーを購入します。

ライセンスキーを購入する際には、ストレージクラスターの ID、ライセンスの種類の提示が必要になります。また、ライセンスの種類によって、契約容量や契約期間の提示が必要になります。

ストレージクラスターの ID は「ストレージクラスターの情報を取得する」に記載のコマンドか、VSP One SDS Block Administrator の Storage Cluster Information アイコンから取得できます。

2. ライセンスを登録します。

ライセンスキーを指定してコマンドを実行します。

REST API : POST /v1/objects/licenses

CLI : license_install

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

affectedResources に削除されたライセンスと追加されたライセンスの両方が表示されます。state が "Succeeded" になっていたらジョブは完了です。

4. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

4.3 ライセンスの削除

ライセンスの削除方法について説明します。

4.3.1 ライセンスを削除する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ライセンスを削除します。ただし、以下に注意してください。

- ライセンスを削除することで、ベースライセンスがなくなるような場合、ライセンスの削除はできません。
- 暗号化環境の設定を有効にしている場合、Data At Rest Encryption のプログラムプロダクトライセンスは削除できません。
- 一度登録したライセンスキーを再度指定してライセンスを登録することはできません。ライセンスを削除する際には注意してください。

前提条件

- 実行に必要なロール：Storage

操作手順

1. 削除するライセンスの ID を確認します。

REST API : GET /v1/objects/licenses

CLI : license_list

2. ライセンスを削除します。

ライセンスの ID を指定してコマンドを実行します。

REST API : DELETE /v1/objects/licenses/<id >

CLI : license_uninstall

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4. 構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

4.3.2 ライセンスを削除する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ライセンスを削除します。ただし、以下に注意してください。

- ライセンスを削除することで、ベースライセンスがなくなるような場合、ライセンスの削除はできません。

- 暗号化環境の設定を有効にしている場合、Data At Rest Encryption のプログラムプロダクトライセンスは削除できません。
- 一度登録したライセンスキーを再度指定してライセンスを登録することはできません。ライセンスを削除する際には注意してください。

前提条件

- 実行に必要なロール：Storage

操作手順

1. 削除するライセンスの ID を確認します。
REST API : GET /v1/objects/licenses
CLI : license_list
2. ライセンスを削除します。
ライセンスの ID を指定してコマンドを実行します。
REST API : DELETE /v1/objects/licenses/<id >
CLI : license_uninstall
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの ID を指定してジョブの state を確認します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
4. ≪Cloud for AWS≫構成情報のバックアップを行います。
「構成情報をバックアップする≪Bare metal≫≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

4.4 ライセンス情報の取得

ライセンスの情報が一覧または個別に取得できます。

4.4.1 取得できるライセンス情報≪Bare metal≫

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : ライセンスの ID(uuid)
- programProductName : プログラムプロダクトの名前
- status : ライセンスの状態
- statusSummary : ライセンスの状態のサマリー
- cause : ライセンスの状態のサマリーが"Warning"または"Error"になっている原因
- keyType : ライセンスキーの種別
- permittedCapacityInTiB : ライセンスで許可する全ストレージプールの総論理容量(容量制限がない場合は null)[TiB]

- `totalPoolCapacityInGiB` : 全ストレージプールの総論理容量(容量制限がない場合は `null`)[GiB]
- `remainingDays` : 残日数(有効期限がない場合は `null`)
- `checkedOutLicenseUsageInTiB` : `null`
- `capacityRate` : ライセンスの許可容量(`permittedCapacityInTiB`)に対する全ストレージプールの総論理容量(`totalPoolCapacityInGiB`)の割合[%]。容量制限がない場合は `null`

4.4.2 取得できるライセンス情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- `id` : ライセンスの ID(uuid)
- `programProductName` : プログラムプロダクトの名前
- `status` : ライセンスの状態
- `statusSummary` : ライセンスの状態のサマリー
- `cause` : ライセンスの状態のサマリーが"Warning"または"Error"になっている原因
- `keyType` : ライセンスキーの種別
- `permittedCapacityInTiB` : ライセンスで許可する全ストレージプールの総論理容量(容量制限がない場合は `null`)[TiB]
 <<Cloud for AWS>> ライセンスの状態のサマリーが"Normal"でも、AWS License Manager と一時的に接続できないときは 0 が出力されます。
- `totalPoolCapacityInGiB` : 全ストレージプールの総論理容量(容量制限がない場合は `null`)[GiB]
- `remainingDays` : 残日数(有効期限がない場合は `null`)
- `checkedOutLicenseUsageInTiB` :
 <<Cloud for AWS>> ベースライセンスが `Floating` の場合、ストレージクラスターが確保した AWS License Manager 上のライセンスの使用量[TiB]。Floating 以外のベースライセンスの場合は `null`
 <<Cloud for Microsoft Azure>> `null`
 <<Cloud for Google Cloud>> `null`
- `capacityRate` : ライセンスの許可容量(`permittedCapacityInTiB`)に対する全ストレージプールの総論理容量(`totalPoolCapacityInGiB`)の割合[%]。容量制限がない場合は `null`
 <<Cloud for AWS>> ベースライセンスが `Floating` の場合で、ライセンスの許可容量(`permittedCapacityInTiB`)に対して全ストレージプールの総論理容量が上回るときは、-1 が出力されます。

4.4.3 ライセンス情報の一覧を取得する

ライセンスの情報を一覧で取得します。

前提条件

- 実行に必要なロール : `Storage`、`RemoteCopy`、`Monitor`、または `Resource`

操作手順

1. ライセンス情報の一覧を取得します。
 REST API : `GET /v1/objects/licenses`
 CLI : `license_list`

4.4.4 ライセンス情報を個別に取得する

指定した ID のライセンス情報を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 取得するライセンスの ID を確認します。
REST API : GET /v1/objects/licenses
CLI : license_list
2. ライセンス情報を取得します。
ライセンスの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/licenses/<id >
CLI : license_show

4.5 ライセンスの設定値の編集

ライセンスの設定値を編集します。

4.5.1 ライセンスの警告しきい値を編集する《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

ライセンスの警告しきい値が編集できます。

VSP One SDS Block のシステムの初期値(セットアップ後のデフォルト値)は以下のとおりです。

- warningThresholdSetting : ライセンスの警告しきい値設定(警告日数、警告容量率[%])
 - remainingDays : 30[日]
 - totalPoolCapacityRate : 80[%]
- overcapacityAllowed : null

前提条件

- 実行に必要なロール : Storage

操作手順

1. ライセンスの設定を編集します。
警告までの日数と警告までの容量率を指定してコマンドを実行します。
REST API : PATCH /v1/objects/license-setting
CLI : license_setting_set
コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの ID を指定してジョブの state を確認します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

3. 構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

4.5.2 ライセンスの設定値を編集する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ライセンスの設定値が編集できます。

VSP One SDS Block のシステムの初期値(セットアップ後のデフォルト値)は以下のとおりです。

- warningThresholdSetting : ライセンスの警告しきい値設定(警告日数、警告容量率[%])
 - remainingDays : 30[日]
 - totalPoolCapacityRate : 80[%]
- overcapacityAllowed :
 - <<Cloud for AWS>>ベースライセンスが Floating の場合、AWS License Manager のライセンス違反時に構成変更を許可するか不許可とするかの設定。デフォルトは false(不許可)。
 - Floating 以外のベースライセンスの場合は null
 - <<Cloud for Microsoft Azure>>null
 - <<Cloud for Google Cloud>>null

前提条件

- 実行に必要なロール : Storage

操作手順

1. ライセンスの設定を編集します。

警告までの日数と警告までの容量率を指定してコマンドを実行します。

警告までの日数と警告までの容量率を指定してコマンドを実行します。

<<Cloud for AWS>>ベースライセンスが Floating の場合、AWS License Manager のライセンス違反時に構成変更を許可するか不許可とするかが指定できます。なお、構成変更を許可にした状態でライセンス違反が発生すると、ライセンスの Status が GracePeriod に遷移して、すぐにライセンスの更新が必要となります。

REST API : PATCH /v1/objects/license-setting

CLI : license_setting_set

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4.6 ライセンス設定情報の取得

ライセンスの設定情報を取得します。

4.6.1 取得できるライセンスの設定情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が取得できます。

- warningThresholdSetting : ライセンスの警告しきい値設定(警告日数、警告容量率[%])
 - remainingDays : 警告日数[日]
 - totalPoolCapacityRate : 警告容量率[%]
- overcapacityAllowed : null

4.6.2 取得できるライセンスの設定情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が取得できます。

- warningThresholdSetting : ライセンスの警告しきい値設定(警告日数、警告容量率[%])
 - remainingDays : 警告日数[日]
 - totalPoolCapacityRate : 警告容量率[%]
- overcapacityAllowed :
 - <<Cloud for AWS>>ベースライセンスが Floating の場合、AWS License Manager のライセンス違反時に構成変更を許可するか不許可とするかの設定。Floating 以外のベースライセンスの場合は null
 - <<Cloud for Google Cloud>>null
 - <<Cloud for Microsoft Azure>>null

4.6.3 ライセンスの設定情報を取得する

ライセンスについて設定情報を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. ライセンスの設定情報を取得します。
REST API : GET /v1/objects/license-setting
CLI : license_setting_show

時刻設定を管理する

- 5.1 時刻の同期設定について<<Bare metal>>
- 5.2 ストレージクラスターの時刻設定を取得する

5.1 時刻の同期設定について《Bare metal》

この節での記述内容は Bare metal モデルに適用されます。

ストレージクラスター内の時刻は、セットアップ時や「ストレージクラスターの構成情報を変更・設定する《Bare metal》」で設定した NTP サーバーとタイムゾーンに従って同期しています。



注意

ストレージクラスターを構成するコンポーネント*の時刻は、NTP などを使用して同期してください。複数の NTP サーバーを使用する場合、NTP サーバー同士の時刻も同期するようにしてください。時刻を同期することによって、時刻ずれに起因する不具合が生じるリスクを避けることができます。また、障害などが発生した場合の原因特定が容易になります。

* BMC(ストレージノード、スペアノード)、ストレージノード、コンピュータノード、コントローラーノード、ネットワーク機器など

NTP サーバーの時刻を変更する場合

NTP サーバーの時刻を変更する場合は、以下の手順に従って、必ずストレージクラスターを停止してから実施してください。

- ①ストレージクラスターを停止する
- ②NTP サーバーの時刻を変更する
- ③ストレージクラスターを構成する他のコンポーネント*の時刻を、変更後の時刻と同期するように設定する
- ④ストレージクラスターを起動する

* BMC、ストレージノード、コンピュータノード、コントローラーノード、ネットワーク機器など

Windows タイムサービスを NTP サーバーとして使用する場合

Windows Server の Windows タイムサービスをストレージシステムの NTP サーバーとして使用する場合は、ネットワーク上の他の NTP サーバーと時刻を同期できるように設定する必要があります。設定方法は、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

5.2 ストレージクラスターの時刻設定を取得する

ストレージクラスターの時刻設定について、以下の情報を取得します。

- systemTime : ストレージクラスターの UTC 時刻
- ntpServerNames :
 - 《Cloud for AWS》NTP サーバーの一覧(優先度順)
 - 《Cloud for Google Cloud》NTP サーバーの一覧(優先度順)
 - 《Cloud for Microsoft Azure》空文字
- timezone : ストレージクラスターのタイムゾーン

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. 時刻設定を取得します。

REST API : GET /v1/objects/storage-time-setting

CLI : storage_time_setting_show

イベントログを管理する

- 6.1 イベントログについて
- 6.2 イベントログの取得
- 6.3 イベントログの Syslog 転送設定の編集
- 6.4 イベントログの SMTP 転送設定の編集
- 6.5 イベントログの設定を取得する
- 6.6 Syslog 転送されるイベントログを監視する
- 6.7 Syslog 転送時のイベントログの構造
- 6.8 E メールの形式
- 6.9 SNMP を利用する

6.1 イベントログについて

ストレージクラスターの稼働中に、ユーザーへの通知が必要な事象が発生すると、VSP One SDS Block はその事象からイベントログを作成します。ユーザーは、イベントログを調べることで、発生した事象の内容を把握できます。

イベントログの最大保持数は 864,000 件です。最大保持容量を超えた場合は、最も古いログから上書きされます。

イベントログは、設定によって、Syslog サーバーと SMTP サーバーのどちらにも転送できます。ただし、Syslog サーバーと SMTP サーバーへの転送設定は、それぞれのコマンドを別々に実行する必要があります。SMTP サーバーに転送されたイベントログは、E メールで送信されます。

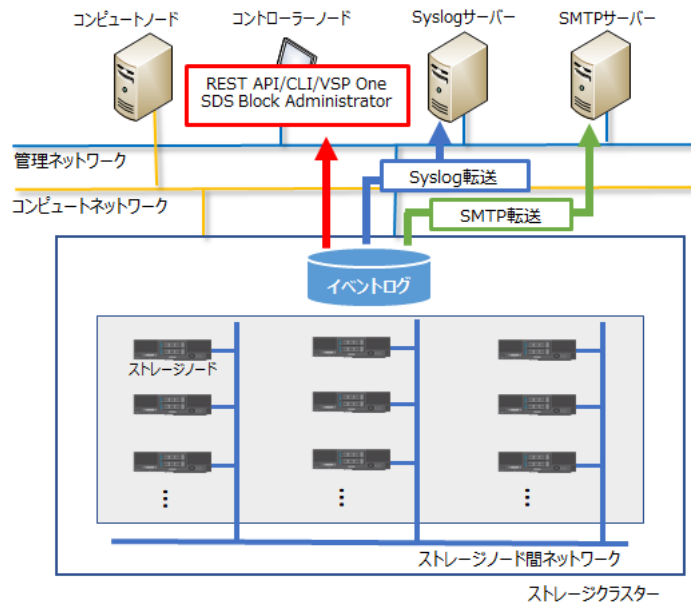
Syslog サーバーまたは SMTP サーバーに転送されるイベントログは、イベントログ設定で転送設定を実施したあとに作成されたイベントログです。イベントログ設定で転送設定を実施する前に作られたイベントログは転送されません。

SMTP サーバーに転送されるイベントログは、Severity(イベントの重大度)が、"Critical"、"Error"、"Warning"のイベントログです。対象となるイベントログの発生から、E メールが送信されるまでの時間は約 1 分 20 秒です。



メモ

- ストレージクラスターの再起動時やストレージノードの保守回復時には、障害発生前に発行されたイベントログが再発行されることがあります。
また、イベントログは、ストレージクラスターにて何らかの処理を実行中に発行されます。しかし、処理の実行中に障害が発生した場合は、処理を他の正常なストレージノードに引き渡して再実行するため、同一のイベントログが発行されることがあります。
- <<Cloud for AWS>>Syslog サーバーまたは SMTP サーバーにはイベントログを受信可能なように、Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「コントローラーノードのセキュリティーグループ設定例」を参考に、セキュリティーグループの設定を実施してください。
- <<Cloud for Google Cloud>>Syslog サーバーまたは SMTP サーバーにはイベントログを受信可能なように、Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「コントローラーノードの Cloud Next Generation Firewall 設定例」を参考に、Cloud Next Generation Firewall の設定を実施してください。
- <<Cloud for Microsoft Azure>>Syslog サーバーまたは SMTP サーバーにはイベントログを受信可能なように、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「コントローラーノードのネットワークセキュリティーグループ設定例」を参考に、ネットワークセキュリティーグループの設定を実施してください。
- クラスターマスターノード(プライマリー)の閉塞時には、閉塞処理と他の正常なストレージノードへの引き渡し処理が同時に動くため、障害検出のイベントログが、処理の再開または回復のイベントログよりもあとに発行されることがあります。



Syslog サーバーと SMTP サーバーの要件

- Syslog サーバー：Rsyslog 8 をサポートします。
 - SMTP サーバー：SMTP サーバーの要件は以下のとおりです。
 - STARTTLS をサポートしていること
 - SMTP 認証をサポートしていること
 - SMTP 認証の方式として、CRAM-MD5、PLAIN、または LOGIN のうち、少なくとも 1 つをサポートしていること
 - TLS1.2 に対応していること
 ストレージシステムが SMTP サーバーとの接続に使用している SMTP クライアントは TLS1.2 のみを使用しますが、SMTP サーバーの設定においても、脆弱なプロトコルバージョン(SSL2.0、SSL3.0、TLS1.0、TLS1.1)を無効化することをお勧めします。
 - TLS の暗号スイートとして、次の(1)～(6)のうち 1 つ以上をサポートしていること
 - (1) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
 - (2) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 - (3) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - (4) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - (5) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - (6) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- 暗号スイートの要件を満たさない場合、SMTP サーバーとの TLS 接続に失敗します。
- SMTP サーバーが上記の暗号スイートをサポートしているかどうかは、使用する SMTP サーバーのマニュアルを参照してください。
- 使用する暗号スイートの鍵交換方式(DHE, ECDHE)に応じて、SMTP サーバーに鍵交換(DHE, ECDHE)の設定が必要な場合があります。具体的な設定方法については、使用する SMTP サーバーのマニュアルを参照してください。
- SMTP サーバーに設定するサーバー証明書が RSA 証明書か ECC 証明書かによって、使用可能な暗号スイートが異なります。RSA 証明書の場合は上記の(1)～(4)が、ECC 証明書の場合

合は上記の(5)、(6)が使用可能です。SMTP サーバーへのサーバー証明書の設定方法については、使用する SMTP サーバーのマニュアルを参照してください。

・ストレージシステムが SMTP サーバーとの接続に使用している SMTP クライアントは、上記の暗号スイートのみを使用しますが、上記以外で脆弱な暗号スイートについては、SMTP サーバーの設定において無効化することをお勧めします。脆弱な暗号スイートとは、RFC7540 Appendix A. TLS 1.2 Cipher Suite Black List に示される暗号スイート(Cipher Suite)を指します。

- SMTP サーバーに複数のサーバー証明書を設定する場合は、ストレージシステムにインポートする 1 つのルート証明書ですべてのサーバー証明書の信頼性を証明できるように、サーバー証明書を発行していること
(VSP One SDS Block にインポートする SMTP 以外の機能の証明書に関しては対象外です。)
- VSP One SDS Block が提供する SMTP クライアントは、下位互換性のために安全でない再ネゴシエーションを許可しています。
SMTP サーバーとの TLS 接続に当たっては、RFC5746 に対応した SMTP サーバーの使用を推奨します。

6.2 イベントログの取得

イベントログが一覧または個別に取得できます。

6.2.1 取得できるイベントログ情報

以下の情報が一覧または個別に取得できます。

- ・ id : イベントの ID(uuid)
- ・ time : イベントを検出した日時
- ・ timeInMicroseconds : イベントを検出した日時に対する、1970 年 1 月 1 日 0 時 0 分 0 秒 0 マイクロ秒からの経過時間(マイクロ秒)
- ・ category : イベントのカテゴリ(ドライブ、ストレージプールなど)
- ・ eventName : イベントの一意な名前
- ・ messageId : メッセージ ID
- ・ severity : イベントの重大度
- ・ message : イベントの説明
- ・ solution : 発生したイベントへの推奨される対処法
- ・ nodeLocation : イベントが発生したストレージノードの情報
- ・ eventType : 常に null
- ・ severityLevel : 常に null

6.2.2 イベントログの一覧を取得する

イベントログの一覧を取得します。

前提条件

- ・ 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. イベントログの一覧を取得します。

REST API : GET /v1/objects/event-logs

CLI : event_log_list



メモ

イベントログの最大保持数は 864,000 件ですが、コマンドの実行で一度に取得できるイベントログは最大 1,000 件です。範囲指定のためのパラメーター(`startTime` または `endTime`)なしでコマンドを実行すると最新の 1,000 件が取得されます。それより前のイベントログを取得するには、`startTime` または `endTime` を指定してコマンドを実行します。

6.2.3 イベントログを個別に取得する

指定した ID のイベントログについての情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. イベントの ID を確認します。

REST API : GET /v1/objects/event-logs

CLI : event_log_list

2. イベントログを取得します。

イベントの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/event-logs/<id >

CLI : event_log_show

6.3 イベントログの Syslog 転送設定の編集

イベントログの Syslog 転送設定の編集について説明します。

6.3.1 イベントログの Syslog 転送設定を編集する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

イベントログの Syslog 転送設定を編集します。Syslog サーバーは 2 つまで設定できます。Syslog サーバーに転送されるイベントログの構造は「Syslog 転送時のイベントログの構造」を参照してください。



注意

DNS サーバーを利用している場合、ストレージノードは、DNS サーバーにおいて設定された時間(DNS TTL)だけ、DNS への問い合わせ結果をキャッシュしています。このため、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL の間、ストレージノードが古い IP アドレスにアクセスする場合があります。したがって、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL で設定された時間が経過したあとに Syslog 転送設定を実行してください。



メモ

イベントログの Syslog 転送を設定すると、ネットワークの経路の確立のために、VSP One SDS Block から、設定した Syslog サーバーに対して、定期的に ICMP echo request を送信します。

前提条件

- 実行に必要なロール : Security

操作手順

1. イベントログの Syslog 転送を設定します。

イベントログの Syslog 転送設定のパラメーターを指定してコマンドを実行します。

REST API : PATCH /v1/objects/event-log-setting

CLI : event_log_setting_set

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

3. 構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

4. Syslog サーバー側で、VSP One SDS Block からのイベントログを受信できるように設定します。

使用する Syslog サーバーのマニュアルを参照し、必要に応じて以下を設定します。

- Syslog 送信元 IP アドレス : Syslog 転送において、VSP One SDS Block から送信する IP パケットの送信元 IP アドレスは、以下のようになります。
 - ストレージクラスターの代表 IP アドレスを設定していない場合 :
クラスターマスターノード(プライマリー)の管理ネットワーク用の IP アドレスになります。
 - ストレージクラスターの代表 IP アドレスを設定している場合 :
ストレージクラスターの代表 IP アドレスまたはクラスターマスターノード(プライマリー)の管理ネットワーク用の IP アドレスになります。
クラスターマスターノード(プライマリー)は、ストレージノードの障害などによって、別のストレージノードに変更する可能性があるため、Syslog サーバーでは、ストレージクラスターの代表 IP アドレスとすべてのストレージノードの管理ネットワーク用の IP アドレスからの Syslog メッセージを受信できるように設定することをお勧めします。
- Syslog 送信元ポート番号 : 手順 1 で設定したポート番号
- 通信プロトコル : 手順 1 で設定した通信プロトコル

5. イベントログが正しく Syslog サーバーに転送されるかを確認します。

手順 1 で実施したイベントログの Syslog 転送設定を同じ入力値で再度実施します。

VSP One SDS Block の Syslog サーバー設定と Syslog サーバー側の受信設定が正しく実施されていれば、イベントログの Syslog 転送設定のジョブ起動を示す以下のイベントログが Syslog

サーバーに転送されます。以下のイベントログが転送されなかった場合は、設定またはネットワークを見直してください。

- ・ イベントログ名 : Start of job
- ・ イベントの説明 : The job has started. JobId=[jobId],Operation=event_log_setting_set

6.3.2 イベントログの Syslog 転送設定を編集する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

イベントログの Syslog 転送設定を編集します。Syslog サーバーは 2 つまで設定できます。Syslog サーバーに転送されるイベントログの構造は「Syslog 転送時のイベントログの構造」を参照してください。



注意

DNS サーバーを利用している場合、ストレージノードは、DNS サーバーにおいて設定された時間(DNS TTL)だけ、DNS への問い合わせ結果をキャッシュしています。このため、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL の間、ストレージノードが古い IP アドレスにアクセスする場合があります。したがって、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL で設定された時間が経過したあとに Syslog 転送設定を実行してください。



メモ

イベントログの Syslog 転送を設定すると、ネットワークの到達性を確認するために、VSP One SDS Block から、設定した Syslog サーバーに対して、定期的に ICMP echo request を送信します。

前提条件

- ・ 実行に必要なロール : Security

操作手順

1. イベントログの Syslog 転送を設定します。
イベントログの Syslog 転送設定のパラメーターを指定してコマンドを実行します。
REST API : PATCH /v1/objects/event-log-setting
CLI : event_log_setting_set
コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの ID を指定してジョブの state を確認します。
REST API : GET /v1/objects/jobs/<jobId>
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
3. <<Cloud for AWS>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
4. Syslog サーバー側で、VSP One SDS Block からのイベントログを受信できるように設定します。
使用する Syslog サーバーのマニュアルを参照し、必要に応じて設定してください。
 - ・ Syslog 送信元 IP アドレス :

VSP One SDS Block からの Syslog 転送ではロードバランサーを通過しないため、送信元 IP アドレスは各ストレージノードの管理ネットワーク用の IP アドレスのままになります。したがって、送信元 IP アドレスを登録する場合は、ロードバランサーに付与した IP アドレスではなく、各クラスターマスターノードの管理ネットワーク用の IP アドレスをすべて設定してください。

- Syslog 送信元ポート番号：手順 1 で設定したポート番号を設定してください。
- 通信プロトコル：手順 1 で設定した通信プロトコルを設定してください。

5. イベントログが正しく Syslog サーバーに転送されるかを確認します。

手順 1 で実施したイベントログの Syslog 転送設定を同じ入力値で再度実施します。

VSP One SDS Block の Syslog サーバー設定と Syslog サーバー側の受信設定が正しく実施されていれば、イベントログの Syslog 転送設定のジョブ起動を示す以下のイベントログが Syslog サーバーに転送されます。以下のイベントログが転送されなかった場合は、設定またはネットワークを見直してください。

- イベントログ名：Start of job
- イベントの説明：The job has started. JobId=[jobId],Operation=event_log_setting_set

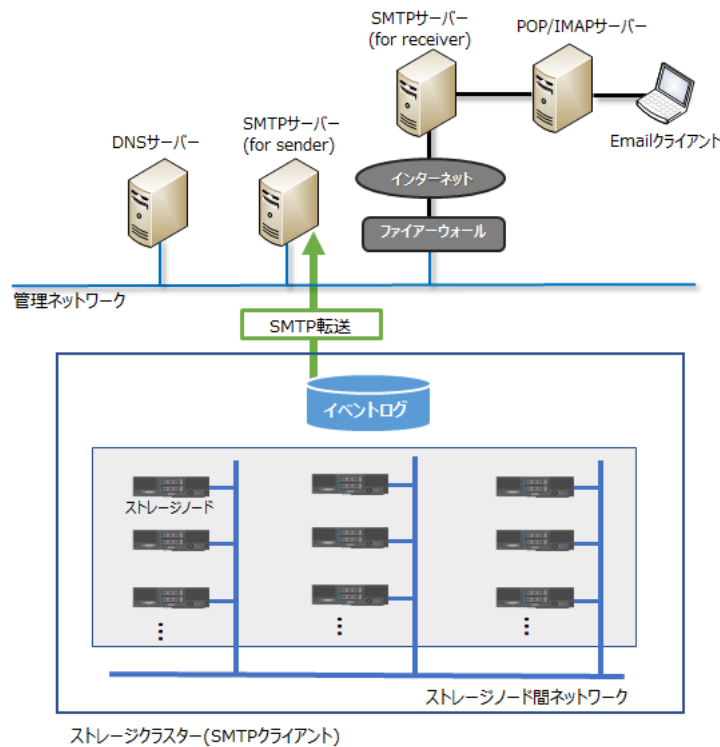
6.4 イベントログの SMTP 転送設定の編集

イベントログの SMTP 転送設定の編集について説明します。

6.4.1 イベントログの SMTP 転送設定を編集する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

VSP One SDS Block は SMTP クライアントとして機能し、イベントログの情報を含んだ E メールを送信用 SMTP サーバーに転送します。メールサービスに必要な SMTP サーバー、POP/IMAP サーバーはユーザーが用意する必要があります。下図はメールサービスに必要な構成の一例であり、運用によってはリレーのためのほかの SMTP サーバーなど、その他の構成要素が存在する場合があります。



SMTP 転送を利用するためには、イベントログの SMTP 転送設定を編集します。送信用 SMTP サーバーのサーバー証明書の信頼性を証明するためのルート証明書をストレージクラスターにインポートします。これによって、送信用 SMTP サーバーと TLS を利用して通信できます。証明書ファイルは PEM 形式または DER 形式をサポートしています。

送信用 SMTP サーバーを経由して送信される E メール形式は「Eメールの形式」を参照してください。

SMTP サーバーに転送されるイベントログは、Severity(イベントの重大度)が、"Critical"、"Error"、"Warning"のイベントログです。対象となるイベントログの発生から、Eメールが送信されるまでの時間は約 1 分 20 秒です。



メモ

クラスターマスターノード(プライマリー)は、ストレージノードの障害などによって、別のストレージノードに変更されることがあります。このような場合でも E メールが受信できるよう、送信元 IP アドレスを登録する際は、ストレージクラスターの代表 IP アドレスとすべてのストレージノードの管理ネットワーク用の IP アドレスを設定してください。

前提条件

- 実行に必要なロール : Security

操作手順

1. 送信用 SMTP サーバーのサーバー証明書の信頼性を証明するためのルート証明書を、ストレージクラスターにインポートします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

証明書ファイルと送信用 SMTP サーバーの識別番号を指定してコマンドを実行します。

REST API : POST /v1/objects/smtp-server-root-certificates/<targetServer >/actions/import/
invoke

CLI : smtp_server_root_certificate_import

コマンド実行後に表示されるジョブの ID を確認します。



メモ

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される次のフィールドがサポートされます。

- 基本制限(Basic Constraints)
- キー使用法(Key Usage)
- サブジェクトキー識別子(Subject Key Identifier)
- 機関キー識別子(Authority Key Identifier)
- 証明書ポリシー(Certificate Policies)
- サブジェクト代替名(Subject Alternative Name)
- 名前の制限(Name Constraints)
- ポリシーの制限(Policy Constraints)
- 拡張キー使用法(Extended Key Usage)
- ポリシー禁止(Inhibit anyPolicy)

2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

送信用 SMTP サーバーとの TLS 通信設定が有効になっている場合、ルート証明書は即時適用されます。

3. イベントログの SMTP 転送を設定します。

イベントログ転送先の E メール通知設定のパラメーターを指定してコマンドを実行します。

REST API : PATCH /v1/objects/event-log-setting

CLI : event_log_setting_set

コマンド実行後に表示されるジョブの ID を確認します。



注意

- DNS サーバーを利用している場合、ストレージノードは、DNS サーバーにおいて設定された時間(DNS TTL)だけ、DNS への問い合わせ結果をキャッシュしています。このため、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL の間、ストレージノードが古い IP アドレスにアクセスする場合があります。したがって、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL で設定された時間が経過したあとに SMTP 転送設定を実行してください。
- SMTP サーバーの設定によっては、問題のある送信元 E メールアドレスを含む E メールをブロックするためのフィルターやルールが設定されていることがあります。そのため、SMTP 転送設定の送信元 E メールアドレスには、受信可能なアドレスを設定してください。例えば、SMTP サーバーが送信元 E メールアドレスに含まれるドメインの名前解決をできない場合に、E メールをブロックする場合があります。この場合、SMTP 転送設定の送信元 E メールアドレスのドメイン部分に以下のような設定をすることで、E メールを受信できるようになる場合があります。
 - ストレージクラスターの代表 IP アドレスに対応する FQDN(ストレージクラスターの代表 IP アドレスを設定している場合のみ)
 - クラスターマスターノードのいずれかの管理ネットワーク用の IP アドレスに対応する FQDN

4. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

5. イベントログの SMTP 転送設定が正しくできたことを確認します。

SMTP 転送設定と送信用 SMTP サーバー側の設定が正しく実施できていれば、イベントログの SMTP 転送設定のジョブ起動を示すイベントログの E メール(件名=VSSB-Report KARS10603-D)が送信されます。E メールは即時送信されますが、ネットワークの状況によって遅延することがあります。E メールクライアントが E メールを受信できなかった場合は次の手順に進みます。

6. イベントログの一覧を取得します。

REST API : GET /v1/objects/event-logs

CLI : event_log_list

7. 以下のイベントログがあった場合は、それぞれの対処を実施します。

メッセージ ID	対処方法
KARS10650-W	イベントログのメッセージの Detailed Information に記載されている詳細なエラー原因を確認し、SMTP 転送の設定内容または送信用 SMTP サーバーの設定を確認・修正してから、SMTP 転送を設定してください。
KARS10652-W	ルート証明書をインポートしてから、SMTP 転送を設定してください。
KARS10651-W	期限切れや不正なルート証明書がインポートされていないかを確認し、正しいルート証明書をインポートしてから、SMTP 転送を設定してください。

上記のイベントログがなかった場合は、VSP One SDS Block は送信用 SMTP サーバーへの Eメールの転送に成功しています。そのため、VSP One SDS Block が SMTP クライアントとして検知できない以下の原因が考えられます。

- SMTP 転送の設定で指定した送信用 SMTP サーバーの設定の中で、別の SMTP サーバーへリレーするための設定に問題がある
- SMTP 転送の設定で指定した送信用 SMTP サーバーの設定の中で、POP/IMAP サーバーへ転送するための設定に問題がある
- POP/IMAP サーバー、リレー用の SMTP サーバー、E メールクライアント、その他の構成要素の設定に問題がある
- それぞれの構成要素間のネットワークに問題がある

VSP One SDS Block が SMTP クライアントとして実行する主な処理とエラー時に通知するイベントログは以下のとおりです。手順 7 で、SMTP 転送のエラーを示すイベントログがなかった場合、以下の処理は成功しています。E メールクライアントが E メールを受信できない場合に、その原因を切り分けるための参考にしてください。

処理	エラー時のイベントログ
SMTP 転送の設定の smtpServerName にホスト名を指定している場合、ホスト名の名前解決を実行する。	KARS10650-W (Detailed information = Connection to the SMTP server is not established.)
送信用 SMTP サーバーと TCP コネクションを確立する。	KARS10650-W (Detailed information = Connection to the SMTP server is not established.)

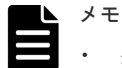
処理	エラー時のイベントログ
SMTP プロトコルの EHLO コマンドを TCP プロトコル上で送信しその応答を確認する。	KARS10650-W (Detailed information = Connection to the SMTP server is not established.)
SMTP プロトコルの STARTTLS コマンドで、送信用 SMTP サーバーが TLS 通信可能であることを確認する。	KARS10650-W (Detailed information = STARTTLS feature is not available in the SMTP server.)
送信用 SMTP サーバーが TLS1.2 をサポートしていることを VSP One SDS Block が確認する。	KARS10650-W (Detailed information = TLS1.2 is not available in the SMTP server.)
送信用 SMTP サーバーが要件を満たす暗号スイートに対応していることを VSP One SDS Block が確認する。 [サポート対象暗号スイート]	KARS10650-W (Detailed information = Connection to the SMTP server is not established.)
• TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	
VSP One SDS Block にインポートしたルート証明書を使用して、送信用 SMTP サーバーのサーバー証明書を検証する。	KARS10651-W
SMTP プロトコルの EHLO コマンドを TLS プロトコル上で送信しその応答を確認する。	KARS10650-W (Detailed information = Connection to the SMTP server is not established.)
SMTP プロトコルの AUTH コマンドで、SMTP 転送の設定の smtpAuthAccount と smtpAuthPassword を送信して、送信用 SMTP サーバーから認証を受ける。	KARS10650-W (Detailed information = Authentication feature is not available in the SMTP server.) または KARS10650-W (Detailed information = Authentication is failed.)
SMTP プロトコルの MAIL FROM コマンドで、SMTP 転送の設定の fromAddress を送信して、送信用 SMTP サーバーに送信元アドレスの情報を伝える。	KARS10650-W (Detailed information = Sender address is not accepted in the SMTP server.)
SMTP プロトコルの RCPT TO コマンドで、SMTP 転送の設定の toAddress1,toAddress2,toAddress3 を送信して、送信用 SMTP サーバーに送信先アドレスの情報を伝える。	KARS10650-W (Detailed information = Recipient address is not accepted in the SMTP server.)
SMTP プロトコルの DATA コマンドで、送信用 SMTP サーバーに E メールタイトルと本文の情報を送信する。	KARS10650-W (Detailed information = Sent data is not accepted in the SMTP server.)
SMTP プロトコルの QUIT コマンドを送信する。	なし



注意

VSP One SDS Block の SMTP 転送機能では、エラーを示すイベントログ(KARS10650-W、KARS10651-W、KARS10652-W)を通知した場合、その後問題が解決するまで同一のメッセージ ID のイベントログを通知することを抑止しています。E メールクライアントが E メールを受信できない場合に、その原因を切り分けるため、再び同一のメッセージ ID のイベントログを通知するようにするためには次の手順を実施してください。

1. イベントログの SMTP 転送の設定で、isEnabled を"false"を指定して設定してください。
isEnabled 以外で指定が必須のパラメーターには、指定可能な任意の値を指定してください。
REST API : PATCH /v1/objects/event-log-setting
CLI : event_log_setting_set
2. ジョブの ID を指定してジョブの state を確認します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていれば、SMTP 転送の設定の構成情報の変更・設定は完了しています。VSP One SDS Block が SMTP クライアントとして構成情報どおりの動作となるまで約 20 秒待ったあと、操作手順の手順 3 以降の操作によって、再びイベントログの SMTP 転送の設定をしてください。



メモ

- ・ クラスタマスターノード(プライマリー)の閉塞があった場合には、タイミングによって、送信済み E メールと同一の E メールが送信されることがあります。
- ・ 送信先 E メールアドレス 1~3 に、同一のメールアドレスを設定した場合、SMTP サーバーの設定によっては同じ E メールが重複して送信されます。
- ・ 送信用 SMTP サーバーのサーバー証明書の信頼性を検証するためのルート証明書は、以下のコマンドで取得できます。
クラスタマスターノード(プライマリー)に対してのみ実行できます。
送信用 SMTP サーバーの識別番号を指定してコマンドを実行します。
ルート証明書は DER 形式のファイルとして取得します。
REST API : GET /v1/objects/smtp-server-root-certificates/<targetServer >/download
CLI : smtp_server_root_certificate_download

8. 構成情報のバックアップを行います。

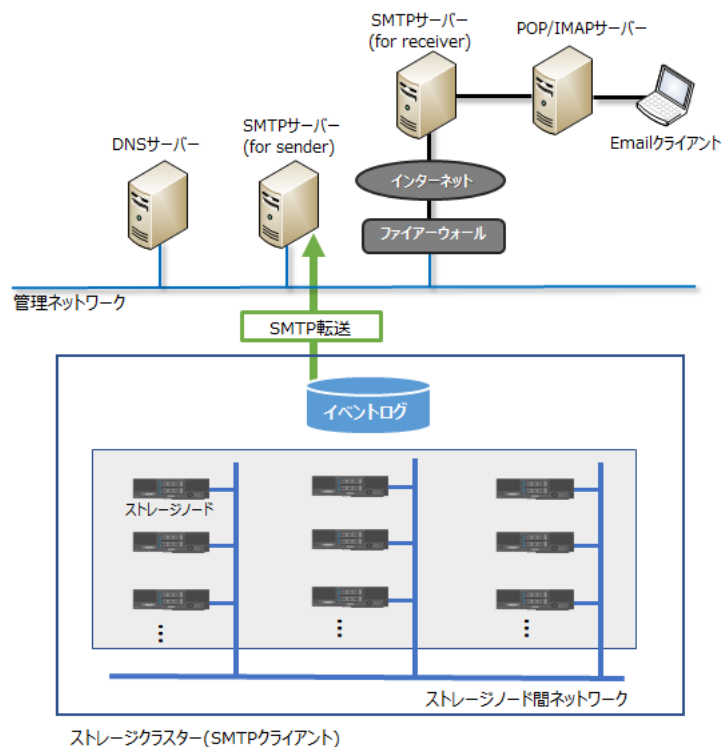
「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

6.4.2 イベントログの SMTP 転送設定を編集する <<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

VSP One SDS Block は SMTP クライアントとして機能し、イベントログの情報を含んだ E メールを送信用 SMTP サーバーに転送します。メールサービスに必要な SMTP サーバー、POP/IMAP サーバーはユーザーが用意する必要があります。下図はメールサービスに必要な構成の一例であり、運用によってはリレーのためのほかの SMTP サーバーなど、その他の構成要素が存在する場合があります。



SMTP 転送を利用するためには、イベントログの SMTP 転送設定を編集します。送信用 SMTP サーバーのサーバー証明書の信頼性を証明するためのルート証明書をストレージクラスターにインポートします。これによって、送信用 SMTP サーバーと TLS を利用して通信できます。証明書ファイルは PEM 形式または DER 形式をサポートしています。

送信用 SMTP サーバーを経由して送信される E メールの形式は「Eメールの形式」を参照してください。

SMTP サーバーに転送されるイベントログは、Severity(イベントの重大度)が、"Critical"、"Error"、"Warning"のイベントログです。対象となるイベントログの発生から、Eメールが送信されるまでの時間は約 1 分 20 秒です。



メモ

VSP One SDS Block からの SMTP 転送ではロードバランサーを通過しないため、送信元 IP アドレスは各ストレージノードの管理ネットワーク用の IP アドレスのままになります。したがって、送信元 IP アドレスを登録する場合は、ロードバランサーに付与した IP アドレスではなく、各クラスターマスターノードの管理ネットワーク用の IP アドレスをすべて設定してください。

前提条件

- 実行に必要なロール：Security

操作手順

1. 送信用 SMTP サーバーのサーバー証明書の信頼性を証明するためのルート証明書を、ストレージクラスターにインポートします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

証明書ファイルと送信用 SMTP サーバーの識別番号を指定してコマンドを実行します。

REST API : POST /v1/objects/smtp-server-root-certificates/<targetServer >/actions/import/
invoke

CLI : smtp_server_root_certificate_import

コマンド実行後に表示されるジョブの ID を確認します。



メモ

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される次のフィールドがサポートされます。

- 基本制限(Basic Constraints)
- キー使用法(Key Usage)
- サブジェクトキー識別子(Subject Key Identifier)
- 機関キー識別子(Authority Key Identifier)
- 証明書ポリシー(Certificate Policies)
- サブジェクト代替名(Subject Alternative Name)
- 名前の制限(Name Constraints)
- ポリシーの制限(Policy Constraints)
- 拡張キー使用法(Extended Key Usage)
- ポリシー禁止(Inhibit anyPolicy)

2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

送信用 SMTP サーバーとの TLS 通信設定が有効になっている場合、ルート証明書は即時適用されます。

3. イベントログの SMTP 転送を設定します。

イベントログ転送先の E メール通知設定のパラメーターを指定してコマンドを実行します。

REST API : PATCH /v1/objects/event-log-setting

CLI : event_log_setting_set

コマンド実行後に表示されるジョブの ID を確認します。



注意

- DNS サーバーを利用している場合、ストレージノードは、DNS サーバーにおいて設定された時間(DNS TTL)だけ、DNS への問い合わせ結果をキャッシュしています。このため、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL の間、ストレージノードが古い IP アドレスにアクセスする場合があります。したがって、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL で設定された時間が経過したあとに SMTP 転送設定を実行してください。
- SMTP サーバーの設定によっては、問題のある送信元 E メールアドレスを含む E メールをブロックするためのフィルターやルールが設定されていることがあります。そのため、SMTP 転送設定の送信元 E メールアドレスには、受信可能なアドレスを設定してください。例えば、SMTP サーバーが送信元 E メールアドレスに含まれるドメインの名前解決をできない場合に、E メールをブロックする場合があります。この場合、SMTP 転送設定の送信元 E メールアドレスのドメイン部分に以下のような設定をすることで、E メールを受信できるようになる場合があります。
 - ロードバランサーの IP アドレスに対応する FQDN(ロードバランサーを使用している場合のみ)
 - クラスタマスターノードのいずれかの管理ネットワーク用の IP アドレスに対応する FQDN

4. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

5. イベントログの SMTP 転送設定が正しくできたことを確認します。

SMTP 転送設定と送信用 SMTP サーバー側の設定が正しく実施できていれば、イベントログの SMTP 転送設定のジョブ起動を示すイベントログの E メール(件名=VSSB-Report KARS10603-D)が送信されます。E メールは即時送信されますが、ネットワークの状況によって遅延することがあります。E メールクライアントが E メールを受信できなかった場合は次の手順に進みます。

6. イベントログの一覧を取得します。

REST API : GET /v1/objects/event-logs

CLI : event_log_list

7. 以下のイベントログがあった場合は、それぞれの対処を実施します。

メッセージ ID	対処方法
KARS10650-W	イベントログのメッセージの Detailed Information に記載されている詳細なエラー原因を確認し、SMTP 転送の設定内容または送信用 SMTP サーバーの設定を確認・修正してから、SMTP 転送を設定してください。
KARS10652-W	ルート証明書をインポートしてから、SMTP 転送を設定してください。
KARS10651-W	期限切れや不正なルート証明書がインポートされていないかを確認し、正しいルート証明書をインポートしてから、SMTP 転送を設定してください。

上記のイベントログがなかった場合は、VSP One SDS Block は送信用 SMTP サーバーへの Eメールの転送に成功しています。そのため、VSP One SDS Block が SMTP クライアントとして検知できない以下の原因が考えられます。

- SMTP 転送の設定で指定した送信用 SMTP サーバーの設定の中で、別の SMTP サーバーへリレーするための設定に問題がある
- SMTP 転送の設定で指定した送信用 SMTP サーバーの設定の中で、POP/IMAP サーバーへ転送するための設定に問題がある
- POP/IMAP サーバー、リレー用の SMTP サーバー、E メールクライアント、その他の構成要素の設定に問題がある
- それぞれの構成要素間のネットワークに問題がある

VSP One SDS Block が SMTP クライアントとして実行する主な処理とエラー時に通知するイベントログは以下のとおりです。手順 7 で、SMTP 転送のエラーを示すイベントログがなかった場合、以下の処理は成功しています。E メールクライアントが E メールを受信できない場合に、その原因を切り分けるための参考にしてください。

処理	エラー時のイベントログ
SMTP 転送の設定の smtpServerName にホスト名を指定している場合、ホスト名の名前解決を実行する。	KARS10650-W (Detailed information = Connection to the SMTP server is not established.)
送信用 SMTP サーバーと TCP コネクションを確立する。	KARS10650-W (Detailed information = Connection to the SMTP server is not established.)

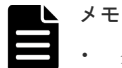
処理	エラー時のイベントログ
SMTP プロトコルの EHLO コマンドを TCP プロトコル上で送信しその応答を確認する。	KARS10650-W (Detailed information = Connection to the SMTP server is not established.)
SMTP プロトコルの STARTTLS コマンドで、送信用 SMTP サーバーが TLS 通信可能であることを確認する。	KARS10650-W (Detailed information = STARTTLS feature is not available in the SMTP server.)
送信用 SMTP サーバーが TLS1.2 をサポートしていることを VSP One SDS Block が確認する。	KARS10650-W (Detailed information = TLS1.2 is not available in the SMTP server.)
送信用 SMTP サーバーが要件を満たす暗号スイートに対応していることを VSP One SDS Block が確認する。 [サポート対象暗号スイート] • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	KARS10650-W (Detailed information = Connection to the SMTP server is not established.)
VSP One SDS Block にインポートしたルート証明書を使用して、送信用 SMTP サーバーのサーバー証明書を検証する。	KARS10651-W
SMTP プロトコルの EHLO コマンドを TLS プロトコル上で送信しその応答を確認する。	KARS10650-W (Detailed information = Connection to the SMTP server is not established.)
SMTP プロトコルの AUTH コマンドで、SMTP 転送の設定の smtpAuthAccount と smtpAuthPassword を送信して、送信用 SMTP サーバーから認証を受ける。	KARS10650-W (Detailed information = Authentication feature is not available in the SMTP server.) または KARS10650-W (Detailed information = Authentication is failed.)
SMTP プロトコルの MAIL FROM コマンドで、SMTP 転送の設定の fromAddress を送信して、送信用 SMTP サーバーに送信元アドレスの情報を伝える。	KARS10650-W (Detailed information = Sender address is not accepted in the SMTP server.)
SMTP プロトコルの RCPT TO コマンドで、SMTP 転送の設定の toAddress1,toAddress2,toAddress3 を送信して、送信用 SMTP サーバーに送信先アドレスの情報を伝える。	KARS10650-W (Detailed information = Recipient address is not accepted in the SMTP server.)
SMTP プロトコルの DATA コマンドで、送信用 SMTP サーバーに E メールタイトルと本文の情報を送信する。	KARS10650-W (Detailed information = Sent data is not accepted in the SMTP server.)
SMTP プロトコルの QUIT コマンドを送信する。	なし



注意

VSP One SDS Block の SMTP 転送機能では、エラーを示すイベントログ(KARS10650-W、KARS10651-W、KARS10652-W)を通知した場合、その後問題が解決するまで同一のメッセージ ID のイベントログを通知することを抑止しています。E メールクライアントが E メールを受信できない場合に、その原因を切り分けるため、再び同一のメッセージ ID のイベントログを通知するようにするためには次の手順を実施してください。

1. イベントログの SMTP 転送の設定で、isEnabled を"false"を指定して設定してください。
isEnabled 以外で指定が必須のパラメーターには、指定可能な任意の値を指定してください。
REST API : PATCH /v1/objects/event-log-setting
CLI : event_log_setting_set
2. ジョブの ID を指定してジョブの state を確認します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていれば、SMTP 転送の設定の構成情報の変更・設定は完了しています。VSP One SDS Block が SMTP クライアントとして構成情報どおりの動作となるまで約 20 秒待ったあと、操作手順の手順 3 以降の操作によって、再びイベントログの SMTP 転送の設定をしてください。



メモ

- ・ クラスタマスターノード(プライマリー)の閉塞があった場合には、タイミングによって、送信済み E メールと同一の E メールが送信されることがあります。
- ・ 送信先 E メールアドレス 1~3 に、同一のメールアドレスを設定した場合、SMTP サーバーの設定によっては同じ E メールが重複して送信されます。
- ・ 送信用 SMTP サーバーのサーバー証明書の信頼性を検証するためのルート証明書は、以下のコマンドで取得できます。
クラスタマスターノード(プライマリー)に対してのみ実行できます。
送信用 SMTP サーバーの識別番号を指定してコマンドを実行します。
ルート証明書は DER 形式のファイルとして取得します。
REST API : GET /v1/objects/smtp-server-root-certificates/<targetServer >/download
CLI : smtp_server_root_certificate_download

8. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

6.5 イベントログの設定を取得する

イベントログの Syslog 転送と E メール通知の設定を取得します。以下の情報が得られます。

- ・ syslogForwardingSetting : イベントログの Syslog 転送設定
- ・ emailReportSetting : イベントログの E メール通知設定

前提条件

- ・ 実行に必要なロール : Security

操作手順

1. イベントログの設定を取得します。
REST API : GET /v1/objects/event-log-setting
CLI : event_log_setting_show

6.6 Syslog 転送されるイベントログを監視する

ネットワーク障害などによってイベントログが Syslog サーバーに転送されない場合があります。その場合、VSP One SDS Block 内のイベントログを確認します。

操作手順

1. Syslog サーバーで受信したイベントログの「メッセージ通番」を確認します。
「メッセージ通番」は、イベントに付けられた通し番号であるため、「メッセージ通番」を確認することで、イベントログがすべて転送されているかを確認できます。もし、転送されたイベントログの「メッセージ通番」が連続していなかった場合は、ネットワーク障害などによって Syslog サーバーに転送できていないイベントログがあることになります。その場合は、次の手順でイベントログを確認してください。
2. 「メッセージ通番」抜けが、Syslog サーバーで受信したイベントログにあった場合、その前後のイベントログの Date and time を確認します。
3. 「イベントログの一覧を取得する」を参照して、イベントログの一覧を取得します。
4. 取得したイベントログの一覧から、手順 2 で確認した時間の間に発生したイベントログを確認します。

6.7 Syslog 転送時のイベントログの構造

Syslog サーバーに転送されるイベントログの情報は、1 件当たり以下のような構造をしています。改行コードは挿入されません。

```
<130>1△2018-10-04T13:03:30.0+09:00△MyStorageCluster△Storage△-△-△  
-△  
1234567890,edd6c079-f278-41a4-a8c4-ec39565afac2,StoragePool,  
Storage Device access failed,KARS12345-I,Critical,  
"Storage Device access Error threshold exceeded,  
id=a01d4f9d-c384-465a-b906-02d5d6db99f8, S/N=naa.5000c50030222d2b",  
2499952a-6c85-480e-b7df-4cbd2137eb69,Informational,Building-A,VSSB:25300
```

ヘッダー部
構造化データ部
メッセージ部

ヘッダー部

ヘッダー部の例を示します。例中の△はスペースを表しています。例中の番号は下表の番号に対応しています。

```
<130>1△2018-10-04T13:03:30.0+09:00△MyStorageCluster△Storage△-△-△  
1 2 3 4 5 6 7
```

番号	項目	説明
1	Priority	・ <130> : イベントの severity が Critical の場合 ・ <131> : イベントの severity が Error の場合 ・ <132> : イベントの severity が Warning の場合 ・ <134> : イベントの severity が Info の場合
2	Version	"1"固定です。

番号	項目	説明
3	Date and time	"YYYY-MM-DDThh:mm:ss.s±hh:mm"の形式で出力されます (YYYY : 年、MM : 月、DD : 日、hh : 時、mm : 分、ss.s : 秒)。 日時は、UTC(協定世界時)表示です。 "±hh:mm"は、UTC と発生日時との時差です。"+"は発生日時が UTC より hh:mm だけ進んでいることを意味し、 "-"は発生日時が UTC より hh:mm だけ遅れていることを意味します。 2019-03-20T23:06:58.0Z のように、日時のあとに"Z"が付いている場合は、UTC と同じ日時であることを意味します。
4	Storage cluster name	ストレージクラスター名です。
5	Program name	"Storage"固定です。
6	Process name	"-"固定です。
7	Message name	"-"固定です。

構造化データ部

構造化データ部の例を示します。例中の△はスペースを表しています。例中の番号は下表の番号に対応しています。

8

番号	項目	説明
8	Structured data	"-"固定です。

メッセージ部

メッセージ部の例を示します。例中の△はスペースを表しています。例中の番号は下表の番号に対応しています。

1234567890,edd6c079-f278-41a4-a8c4-ec39565afac2,StoragePool,
Storage Device access failed,KARS12345-I,Critical,
"Storage Device access Error threshold exceeded",
id=a01d4f9d-c384-465a-b906-02d5d6db99f8, S/N=naa.5000c50030222d2b",
2499952a-6c85-480e-b7df-4cbd2137eb69,Informational,Building-A,VSSB:25300



メモ

メッセージ部の先頭には、BOM(Byte Order Mark)として、固定で"%xEF.BB.BF"が挿入されます。

番号	項目	説明
9	メッセージ通番	イベントに付けられた通番です。(範囲 : 0000000001～9999999999)
10	イベントの ID	イベントの ID です。
11	イベントのカテゴリ	ドライブ、ストレージプールなど、イベントのカテゴリを示します。
12	イベントの一意な名前	イベントの一意な名前です。
13	メッセージ ID	メッセージの ID です。

番号	項目	説明
14	イベントの重大度	イベントの重大度です。 • Info : 情報レベル • Warning : 警告レベル。すぐには問題にならないが、後に大きな障害につながる可能性があるイベントです。 • Error : 障害レベル。対応が必要となるイベントです。 • Critical : 致命的な障害レベル。早急な対応が必須となるイベントです。
15	イベントの説明	イベントの説明です。
16	イベントが発生したストレージノードの情報	イベントが発生したストレージノードの情報です。
17	イベントタイプ	イベントタイプです。この項目は将来使用するために予約された項目であり、"Informational"が固定で出力されます。
18	ロケーション名	装置の設置場所など、イベントの出力元ロケーションです。
19	型名 : 製番	型名と製番です。

6.8 E メールの形式

SMTP サーバーを介して送信される E メール の形式は以下のとおりです。

項目	形式と内容
E メール のタイトル	VSSB-Report <Message ID>
ヘッダー 情報	<pre>----- This is a notification report of the VSSB. This is automatically sent to the registered addresses. Please refer to the reported event and take action if required. -----</pre> Storage cluster name : ストレージクラスターのニックネーム Storage cluster version : ストレージクラスターのバージョン Timezone : タイムゾーン Date and time : 採取日時(yyyy/MM/dd hh:mm:ss.fff) Severity : イベントの重大度 Message ID : メッセージの ID Description : イベントログ本文 Action : 対処方法 Event ID : イベントの ID <pre>----- The followings show the events that occurred before and after the reported event. Note that * is marked at the beginning of the line corresponding to the reported event. -----</pre>
イベント ログの一 覧	E メールにて転送された当該イベントログとその前後に発生したイベントログが表示されます。 当該イベントログの前には、当該イベントログの発生 30 分前までに発生したイベントログが最大で 50 件表示されます。

項目	形式と内容
	当該イベントログの後ろには、当該イベントログの発生から 1 分後まで発生したイベントログが最大で 50 件表示されます。当該イベントログの後ろに表示されたイベントログは、たとえ E メール転送の対象になるものであったとしても、E メールにて通知されることはありません。 形式：<採取日時> <Severity> <Message ID> <イベントログ本文> <イベントログの ID> 例：20xx/12/10 17:40:33.145 Info KARS08100-I The storage cluster started. aace3c10-9aa6-45ef-84d9-b2b4e32a242c 当該イベントログには、先頭に*が表示されます。 例：* 20xx/12/10 17:40:33.238 Error KARS08103-E The storage node, storage_node_uuid_1234567890 was blocked. fc1f2299-d0fc-42ed-96f9-c310b029443a

6.9 SNMP を利用する

VSP One SDS Block には SNMP エージェント機能が備わっており、ユーザーが用意し管理ネットワークに接続した SNMP マネージャーに、VSP One SDS Block ストレージクラスターで発生した障害情報(イベントログ)を SNMP プロトコルによって発報します。

また、SNMP プロトコルを使用して、システムの構成や稼働状態が確認できます。

管理対象の機器に関する障害情報を検知した VSP One SDS Block は、トラップというメッセージを使用して、SNMP マネージャーからの要求がなくても障害情報を SNMP マネージャーに発報します。

SNMP の利用に当たっては「SNMP アクセスコントロールを設定する」を参照して、SNMP の有効/無効、SNMP トラップの発報先、SNMP でのリクエスト許可、システムグループ情報などを設定します。

SNMP プロトコルには、管理情報の構造とそのデータベースについて、MIB(Management Information Base)と呼ばれる標準があります。

《Bare metal》障害が発生したハードウェアの情報は、MIB によって定義されます。MIB には標準 MIB と拡張 MIB があります。

《Cloud for AWS》障害が発生した EC2 インスタンスや EBS ボリュームの情報は、MIB によって定義されます。MIB には標準 MIB と拡張 MIB があります。

《Cloud for Google Cloud》障害が発生した Compute Engine インスタンスや Google Cloud Hyperdisk ボリュームの情報は、MIB によって定義されます。MIB には標準 MIB と拡張 MIB があります。

《Cloud for Microsoft Azure》障害が発生した Azure VM インスタンスや Azure マネージドディスクボリュームの情報は、MIB によって定義されます。MIB には標準 MIB と拡張 MIB があります。

SNMP マネージャーに発報される障害情報は、イベントログのうち、Severity(イベントの重大度)が、"Critical"、"Error"、"Warning"のイベントログからの情報です。

また、SNMP マネージャーに発報される障害情報は、SNMP の設定を実施したあとに作成されたイベントログに基づきます。SNMP 設定を実施する前に作られたイベントログは対象になりません。

障害情報が通知された場合の対処方法は、障害情報中のメッセージ ID を基に「Hitachi Virtual Storage Platform One SDS Block メッセージリファレンス」を参照してください。

6.9.1 SNMP マネージャーと環境の要件

SNMP の各機能を使用するためにユーザーが用意する SNMP マネージャーと環境についての要件は以下のとおりです。

《Bare metal》

項目		要件
通信プロトコル		UDP がサポートされていること
通信ポート	SNMP コマンド	宛先 Port161 に Get 送信できること
	SNMP Trap	宛先 Port162 のパケットを受信できること
SNMP バージョン		v2c をサポートしていること
受信する Trap の送信元 IP アドレスの設定		イベントログの SNMP 転送設定における送信元 IP アドレスは、以下のようになります。 - ストレージクラスターの代表 IP アドレスを設定していない場合： クラスターマスターノード(プライマリー)の管理ネットワーク用の IP アドレスになります。 - ストレージクラスターの代表 IP アドレスを設定している場合： ストレージクラスターの代表 IP アドレスまたはクラスターマスターノード(プライマリー)の管理ネットワーク用の IP アドレスになります。 クラスターマスターノード(プライマリー)は、ストレージノードの障害などによって、別のストレージノードに変更されることがあります。このような場合でも Trap が受診できるよう、送信元 IP アドレスを登録する際は、ストレージクラスターの代表 IP アドレスとすべてのストレージノードの管理ネットワーク用の IP アドレスを設定してください。

《Cloud》

項目		要件
通信プロトコル		UDP がサポートされていること
通信ポート	SNMP コマンド	宛先 Port161 に Get 送信できること
	SNMP Trap	宛先 Port162 のパケットを受信できること
SNMP バージョン		v2c をサポートしていること
受信する Trap の送信元 IP アドレスの設定		VSP One SDS Block からの SNMP 転送ではロードバランサーを通過しないため、送信元 IP アドレスは各ストレージノードの管理ネットワーク用の IP アドレスのままになります。したがって、送信元 IP アドレスを登録する場合は、ロードバランサーに付与した IP アドレスではなく、各クラスターマスターノードの管理ネットワーク用の IP アドレスをすべて設定してください。

6.9.2 SNMP アクセスコントロールを設定する

SNMP のアクセスコントロールを設定します。コマンド実行時に指定を省略したパラメーターの設定情報は削除されます。

SNMP 設定編集のパラメーターの community、storageSystemName(CLI:storage_system_name)、contact、location の設定では、以下に従ってください。

- 文字数：最大 180
- 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(! # \$ ' () + - . @ _ ` { } ~)
または、1 文字目と最後の文字種は上記と同じ、中間の文字には上記文字種に加えて Space が使用できます。



注意

DNS サーバーを利用している場合、ストレージノードは、DNS サーバーにおいて設定された時間(DNS TTL)だけ、DNS への問い合わせ結果をキャッシュしています。このため、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL の間、ストレージノードが古い IP アドレスにアクセスする場合があります。したがって、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL で設定された時間が経過したあとに SNMP 設定の編集を実行してください。

前提条件

- 実行に必要なロール：Security

操作手順

1. SNMP のアクセスコントロールを設定します。
SNMP 設定編集のパラメーターを指定してコマンドを実行します。
REST API : PATCH /v1/objects/snmp-setting
CLI : snmp_setting_set
コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
3. ≪Bare metal≫構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
4. ≪Cloud for AWS≫構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
5. 手順 1 の設定が正しく設定できており、かつトラップの発報先設定の指定があった場合は、設定確認のトラップが発報されます。以下のイベントログが転送されなかった場合は、設定またはネットワークを見直してください。
 - メッセージ ID : KARS10607-I
 - SNMP setting complete. JobId=[JobId]

6.9.3 SNMP アクセスコントロールを取得する

SNMP のアクセスコントロールを取得します。以下の情報が得られます。

- isSNMPAgentEnabled : SNMP の有効/無効
- snmpVersion : SNMP のバージョン
- sendingTrapSetting : SNMP トラップの発報先設定
- requestAuthenticationSetting : SNMP でのリクエスト許可の設定
- systemGroupInformation : システムグループ情報

前提条件

- 実行に必要なロール : Security

操作手順

1. SNMP のアクセスコントロールを取得します。

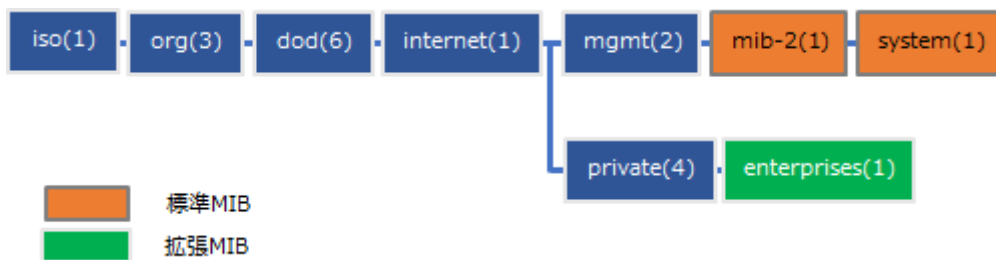
REST API : GET /v1/objects/snmp-setting

CLI : snmp_setting_show

6.9.4 標準 MIB について

VSP One SDS Block の標準 MIB の構造を以下に示します。標準 MIB では system グループのみをサポートしています。

VSP One SDS Block の拡張 MIB については「拡張 MIB の取り込み」を参照してください。



System グループの構造と内容は以下のとおりです。

OID	名称	内容	R/W 属性	備考
1	sysDescr	製品名称	R	
2	sysObjectID	拡張 MIB の先頭 OID	R	
3	sysUpTime	SNMP エージェントの稼働時間*	R	
4	sysContact	連絡先	R/W	
5	sysName	システム名称	R/W	
6	sysLocation	設置場所	R/W	
7	sysServices	提供サービス	R	
8	sysORLastChange	—	—	非サポート
9	sysORTable	—	—	非サポート
* SNMP エージェントのリスタートでリセットされます。				

6.9.5 拡張 MIB の取り込み

SNMP コマンド(Get など)やトラップで受信したデータを参照するためには、SNMP マネージャーに VSP One SDS Block の拡張 MIB ファイルを取り込む必要があります。

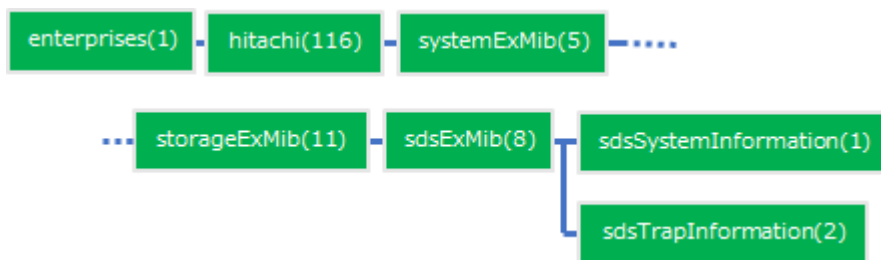
拡張 MIB ファイルは以下の名称です。

- ファイル名 : sdsExMib -<version>-<number>.mib

拡張 MIB ファイルは製品メディアから取得します。

ストレージソフトウェアのアップデートを行った場合は、アップデートしたストレージソフトウェアのバージョンと、上記のファイル名の<version>が一致したファイルを入手してください。

VSP One SDS Block の拡張 MIB の構成は以下のとおりです。



メモ

クラウドプラットフォーム上の VM インスタンスの情報を取得するには、以下の手順を実施します。
コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

≪Cloud for AWS≫

```
aws ec2 describe-instances ¥  
--instance-ids <sdsStorageNodeServerSerialNumber>
```

≪Cloud for Google Cloud≫

```
gcloud compute instances list ¥  
--filter="id~<sdsStorageNodeServerSerialNumber>"
```

≪Cloud for Microsoft Azure≫

```
az vm list --query "[?vmId=='<sdsStorageNodeServerSerialNumber>']"
```

OI D	名称	内容	R/W 属性	備考
1	sdsSystemInformation(1)	VSP One SDS Block のシステム情報	R	
2	sdsTrapInformation(2)	SNMP トラップ情報	—	R/W 不可

sdsSystemInformation

O I D	名称	説明	備考
1	sdsProductName	製品名称	固定 : VSSB
2	sdsSoftwareVersion	稼働中のソフトウェアバージョン	ストレージソフトウェアのバージョン
3	sdsExMibVersion	稼働中のソフトウェアが対応している拡張 MIB のバージョン	ストレージノードの拡張 MIB のバージョン。 このバージョンは、ストレージソフトウェアのバージョンと異なります。
4	sdsStorageNodeIdTable	ストレージクラスター内のストレージノードの ID の一覧	ストレージノードの ID の配列
5	sdsStorageNodeInformationTable	<<Bare metal>>ストレージクラスター内のストレージノードのハードウェア情報 <<Cloud>>ストレージノードが動作している VM インスタンスの情報	sdsStorageNodeInformationTable の表を参照してください。

sdsStorageNodeInformationTable<<Bare metal>>

O I D	名称	説明	設定内容
1	sdsStorageNodeNickName	ストレージノードのノード名称	ストレージノードのノード名称
2	sdsStorageNodeServerModel	ストレージノードのサーバーモデル	ストレージノードのサーバーモデル
3	sdsStorageNodeServerSerialNumber	ストレージノードのシリアル番号	ストレージノードのシリアル番号

sdsStorageNodeInformationTable<<Cloud for AWS>>

O I D	名称	説明	設定内容
1	sdsStorageNodeNickName	ストレージノードのノード名称	ストレージノードのノード名称
2	sdsStorageNodeServerModel	ストレージノードが動作している VM インスタンスのモデル名	ストレージノードが動作している EC2 インスタンスのモデル名
3	sdsStorageNodeServerSerialNumber	ストレージノードのシリアル番号	ストレージノードが動作している EC2 インスタンスの ID

sdsStorageNodeInformationTable<<Cloud for Google Cloud>>

OID	名称	説明	設定内容
1	sdsStorageNodeNickName	ストレージノードのノード名称	ストレージノードのノード名称
2	sdsStorageNodeServerModel	ストレージノードが動作している VM インスタンスのマシンタイプ	ストレージノードが動作している Compute Engine インスタンスのマシンタイプ
3	sdsStorageNodeServerSerialNumber	ストレージノードのシリアル番号	ストレージノードが動作している Compute Engine インスタンスの ID

sdsStorageNodeInformationTable<<Cloud for Microsoft Azure>>

OID	名称	説明	設定内容
1	sdsStorageNodeNickName	ストレージノードのノード名称	ストレージノードのノード名称
2	sdsStorageNodeServerModel	ストレージノードが動作している VM インスタンスのサイズ	ストレージノードが動作している Azure VM インスタンスのサイズ
3	sdsStorageNodeServerSerialNumber	ストレージノードのシリアル番号	ストレージノードが動作している Azure VM インスタンスの ID

sdsTrapInformation

OID	名称	説明	設定内容
1	sdsInternalID	装置製番	システムの ID
2	sdsEventLog	イベントログ	sdsEventLog の表を参照してください。

sdsEventLog

OID	名称	説明	設定内容
1	sdsDateAndTime	イベントを検出した日時	YYYY/MM/DD hh:mm:ss.msec
2	sdsSeverity	イベントの重大度	"Critical"、"Error"、 "Warning"のいずれか
3	sdsMessageId	メッセージ ID	イベントのメッセージ ID
4	sdsEventName	イベント名称	イベントの一意な名前
5	sdsEventMessage	イベント内容の詳細メッセージ	イベントの説明
6	sdsCategory	障害カテゴリー	イベントのカテゴリー

OID	名称	説明	設定内容
7	sdsID	イベントの個別 ID	イベントの ID
8	sdsNodeLocation	イベントログを登録したストレージノードの ID	ストレージノードの ID

6.9.6 トラップ受信後の障害ハードウェアの特定

トラップを受信してから障害発生したハードウェアの部位を特定するまでの手順は以下のとおりです。

Cloud モデルの場合は、VM インスタンスを特定するまでの手順となります。

操作手順

1. トラップで受信した情報からハードウェア障害が発生しているストレージノードの ID を確認します。障害が発生しているストレージノードの ID は `sdsEventMessage` から特定します。
(ただし、すべてのトラップがハードウェア障害起因で発生するわけではなく、`sdsEventMessage` にストレージノードの ID が含まれていないケースもあります。)
2. SNMP コマンドを使用してストレージノードの ID のリストを取得します。
3. ストレージノードの ID のリストから、手順 1 で確認した ID と一致するものを検索します。
4. 検索したストレージノードの Entry 番号(X)を使用してストレージノードの情報を参照します。

(例)

ストレージノードのノード名称の OID : 1.3.6.1.4.1.116.3.11.8.1.5.X.1

ストレージノードのサーバーモデルの OID : 1.3.6.1.4.1.116.3.11.8.1.5.X.2

ストレージノードのサーバーシリアル番号の OID : 1.3.6.1.4.1.116.3.11.8.1.5.X.3

5. 手順 4 の結果から障害が発生したサーバーを特定します。

監査ログを管理する

- 7.1 監査ログの概要
- 7.2 監査ログをコントローラーノードにダウンロードする
- 7.3 監査ログの Syslog 転送設定の編集
- 7.4 監査ログの Syslog 転送設定を取得する
- 7.5 Syslog サーバーへ転送される監査ログを監視する

7.1 監査ログの概要

監査ログは、ストレージクラスターに対して実行された操作内容を記録したものです。監査ログからは「いつ」「誰が」「何をした」かが確認でき、これによって法規制、業界基準、社内規定などの監査基準に準拠しているかどうかを調査できます。

監査ログの最大保持数は 750,000 件です。最大保持容量を超えた場合は、最も古いログから上書きされます。



注意

監査ログの syslog 転送設定をしている場合は、監査ログの未転送件数が、最大件数の 750,000 件の 70%と 100%に達したときに、イベントログ(KARS10613-W、KARS10614-W)による注意喚起がされます。監査ログの syslog 転送設定をしていない場合は、注意喚起のイベントログは発行されません。このため、監査ログを保持する必要がある場合には、定期的に監査ログをダウンロードして回収する必要があります。

監査ログは、クラスターマスターノード(プライマリー)に格納されており、次の方法で取得できます。

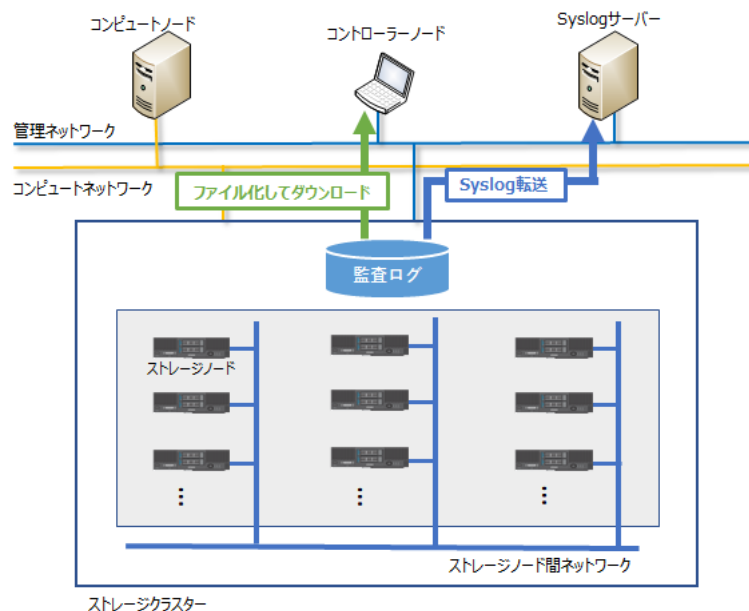
- ・ 監査ログファイルを作成し、コントローラーノードにダウンロードする
- ・ 監査ログを Syslog サーバーへ転送するよう設定し、転送先の Syslog サーバーから監査ログを取得する

Syslog サーバーへ転送される監査ログは、Syslog 転送設定を実施後に作成された監査ログです。Syslog 転送設定を実施する前に作成された監査ログは Syslog サーバーには転送されません。

サポートされる Syslog サーバーは以下です。

- ・ Rsyslog 8

監査ログの構造などについては「Hitachi Virtual Storage Platform One SDS Block 監査ログリファレンス」を参照してください。



7.2 監査ログをコントローラーノードにダウンロードする

監査ログファイルを作成し、コントローラーノードにダウンロードします。

前提条件

- 実行に必要なロール : Audit または Security

操作手順

1. 監査ログファイルを作成します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : POST /v1/objects/audit-logs/actions/create-file/invoke

CLI : audit_log_create_file

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

3. 監査ログファイルをダウンロードします。

監査ログファイルは REST API または CLI を実行したカレントディレクトリーに zip 形式でダウンロードされます。

REST API : GET /v1/objects/audit-logs/download

CLI : audit_log_download

CLI を実行したときの監査ログファイルの名称は "download-auditlog.zip" になります。

7.3 監査ログの Syslog 転送設定の編集

監査ログの Syslog 転送設定の編集方法について説明します。

7.3.1 監査ログの Syslog 転送設定を編集する <<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

監査ログの Syslog 転送を設定します。Syslog サーバーは 2 つまで設定できます。

監査ログの最大件数は 750,000 件です。Syslog サーバーへの転送を有効にした場合、未転送の監査ログが最大件数の 70% と 100% に達すると、イベントログと監査ログでユーザーに通知されます。



メモ

- DNS サーバーを利用している場合、ストレージノードは、DNS サーバーにおいて設定された時間(DNS TTL)だけ、DNS への問い合わせ結果をキャッシュしています。このため、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL の間、ストレージノードが古い IP アドレスにアクセスする場合があります。したがって、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL で設定された時間が経過したあとに Syslog 転送設定を実行してください。

- 監査ログの Syslog 転送を設定すると、ネットワークの到達性を確認するために、VSP One SDS Block から、設定した Syslog サーバーに対して、定期的に ICMP echo request を送信します。
 - 監査ログの Syslog 転送設定における送信元 IP アドレスは、以下のようになります。
 - ストレージクラスターの代表 IP アドレスを設定していない場合：
クラスターマスターノード(プライマリー)の管理ネットワーク用の IP アドレスになります。
 - ストレージクラスターの代表 IP アドレスを設定している場合：
ストレージクラスターの代表 IP アドレスまたはクラスターマスターノード(プライマリー)の管理ネットワーク用の IP アドレスになります。クラスターマスターノード(プライマリー)は、ストレージノードの障害などによって、別のストレージノードに変更されることがあります。このような場合でも監査ログが受信できるよう、送信元 IP アドレスを登録する際は、ストレージクラスターの代表 IP アドレスとすべてのストレージノードの管理ネットワーク用の IP アドレスを設定してください。
-

前提条件

- 実行に必要なロール : Security

操作手順

1. 監査ログの Syslog 転送を設定します。

監査ログの設定パラメーターを指定してコマンドを実行します。

locationName(CLI : --location_name)パラメーターを指定する場合は、以下に従ってください。

- 文字数 : 1~180
- 使用可能文字 : 数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(! # \$ ' () + - . @ _ ` { } ~)

REST API : PATCH /v1/objects/audit-log-setting

CLI : audit_log_setting_set

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

3. Syslog サーバー側で VSP One SDS Block から監査ログを受信できるように設定します。

使用する Syslog サーバーのマニュアルを参照し、必要に応じて以下を設定します。

- Syslog 送信元 IP アドレス : クラスターマスターノード(プライマリー)の管理ポートの IP アドレス
- Syslog 送信元ポート番号 : 手順 1 で設定したポート番号
- 通信プロトコル : 手順 1 で設定した通信プロトコル

4. 監査ログが正しく Syslog サーバーに転送されるかを確認します。

手順 1 で実施した監査ログの Syslog 転送設定を同じ入力値で再度実施します。

VSP One SDS Block の Syslog サーバー設定と Syslog サーバー側の受信設定が正しく実施されていれば、監査ログの Syslog 転送設定のジョブ起動を示す以下の監査ログが Syslog サーバーに転送されます。転送されない場合は設定またはネットワークを見直してください。

- Audit event : JOB STARTED FOR audit_log_setting_set

5. 構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

7.3.2 監査ログの Syslog 転送設定を編集する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

監査ログの Syslog 転送を設定します。Syslog サーバーは 2 つまで設定できます。

監査ログの最大件数は 750,000 件です。Syslog サーバーへの転送を有効にした場合、未転送の監査ログが最大件数の 70%と 100%に達すると、イベントログと監査ログでユーザーに通知されます。



メモ

- DNS サーバーを利用している場合、ストレージノードは、DNS サーバーにおいて設定された時間(DNS TTL)だけ、DNS への問い合わせ結果をキャッシュしています。このため、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL の間、ストレージノードが古い IP アドレスにアクセスする場合があります。したがって、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL で設定された時間が経過したあとに Syslog 転送設定を実行してください。
- 監査ログの Syslog 転送を設定すると、ネットワークの到達性を確認するために、VSP One SDS Block から、設定した Syslog サーバーに対して、定期的に ICMP echo request を送信します。
- VSP One SDS Block からの Syslog 転送ではロードバランサーを通過しないため、送信元 IP アドレスは各ストレージノードの管理ネットワーク用の IP アドレスのままになります。したがって、送信元 IP アドレスを登録する場合は、ロードバランサーに付与した IP アドレスではなく、各クラスターマスターノードの管理ネットワーク用の IP アドレスをすべて設定してください。

前提条件

- 実行に必要なロール : Security

操作手順

1. 監査ログの Syslog 転送を設定します。

監査ログの設定パラメーターを指定してコマンドを実行します。

locationName(CLI : --location_name)パラメーターを指定する場合は、以下に従ってください。

- 文字数 : 1~180
- 使用可能文字 : 数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(! # \$ ' () + - . @ _ ` { } ~)

REST API : PATCH /v1/objects/audit-log-setting

CLI : audit_log_setting_set

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

3. Syslog サーバー側で VSP One SDS Block から監査ログを受信できるように設定します。

使用する Syslog サーバーのマニュアルを参照し、必要に応じて以下を設定します。

- Syslog 送信元 IP アドレス : クラスターマスターノード(プライマリー)の管理ポートの IP アドレス
- Syslog 送信元ポート番号 : 手順 1 で設定したポート番号
- 通信プロトコル : 手順 1 で設定した通信プロトコル

4. 監査ログが正しく Syslog サーバーに転送されるかを確認します。

手順 1 で実施した監査ログの Syslog 転送設定を同じ入力値で再度実施します。

VSP One SDS Block の Syslog サーバー設定と Syslog サーバー側の受信設定が正しく実施されていれば、監査ログの Syslog 転送設定のジョブ起動を示す以下の監査ログが Syslog サーバーに転送されます。転送されない場合は設定またはネットワークを見直してください。

- Audit event : JOB STARTED FOR audit_log_setting_set

5. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

7.4 監査ログの Syslog 転送設定を取得する

監査ログを転送する Syslog サーバーについての設定を取得します。以下の情報が得られます。

- locationName : ロケーション情報
- index : Syslog サーバーの識別番号
- isEnabled : Syslog サーバーに監査ログを転送するかどうかの設定
- serverName : Syslog サーバーのホスト名または IP アドレス(IPv4)
- port : Syslog サーバーのポート番号
- transportProtocol : 通信プロトコル

前提条件

- 実行に必要なロール : Security

操作手順

1. Syslog サーバーについての設定を取得します。

REST API : GET /v1/objects/audit-log-setting

CLI : audit_log_setting_show

7.5 Syslog サーバーへ転送される監査ログを監視する

ネットワーク障害などによって監査ログが Syslog サーバーに転送されない場合があります。その場合、監査ログをダウンロードして参照します。

操作手順

1. Syslog サーバーで受信した監査ログの Serial number を確認します。

Serial number に抜けがない場合、すべての監査ログが Syslog サーバーに転送されています。Serial number に抜けがある場合、ネットワーク障害などによって Syslog サーバーに転送できていない監査ログがあります。その場合は、次の手順で監査ログを確認します。

2. 「監査ログをコントローラーノードにダウンロードする」を参照して、監査ログをダウンロードします。Syslog サーバーで抜けていた Serial number の監査ログを確認します。

ドライブを管理する

- 8.1 ドライブ管理の概要
- 8.2 ドライブ情報の取得
- 8.3 ドライブの減設
- 8.4 ドライブの交換
- 8.5 ドライブを再組み入れする《Bare metal》

8.1 ドライブ管理の概要

ストレージノードを構成するドライブについて、情報取得や構成変更など、以下の操作を行います。

項目	説明
ドライブ情報の取得	ドライブの状態や固有情報などを取得できます。ドライブ情報は一覧取得する方法とドライブの ID を指定して取得することができます。
ドライブの増設	ストレージプールの容量拡張のためなどに行うドライブを増設する操作です。「ドライブを増設する」を参照してください。
ドライブの減設	障害ドライブを減設する操作です。
ドライブの交換	障害ドライブを別のドライブと交換する操作です。
ドライブの再組み入れ	閉塞ドライブを再利用して回復させる操作です。



メモ

《Bare metal》ドライブのファームウェアアップデートは、サーバーベンダーのマニュアルに従って実施してください。

8.2 ドライブ情報の取得

ドライブの情報が一覧または個別に取得できます。

8.2.1 取得できるドライブ情報《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : ドライブの ID(uuid)
- wwid : ドライブの WWID(WWN)
- statusSummary : ドライブの状態のサマリー
- status : ドライブの状態
- typeCode : ドライブ種別を示すコード(ドライブのモデル名)
- serialNumber : ドライブのシリアルナンバー
- storageNodeId : ストレージノードの ID(uuid)
- deviceFileName : ドライブに対応するデバイスファイル名
- vendorName : ベンダー名
- firmwareRevision : ファームウェアリビジョン
- locatorLedStatus : ロケータ LED の点消灯状態
- driveType : ドライブの種別
- driveCapacity : ドライブの容量[GB]

8.2.2 取得できるドライブ情報《Cloud》

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : ドライブの ID(uuid)
- wwid :
 - ◀Cloud for AWS▶ 常に"N/A"
 - ◀Cloud for Google Cloud▶ ドライブの固有情報
 - ◀Cloud for Microsoft Azure▶ ドライブの固有情報
- statusSummary : ドライブの状態のサマリー
- status : ドライブの状態
- typeCode : ドライブ種別を示すコード(ドライブのモデル名)
- serialNumber :
 - ◀Cloud for AWS▶ EBS のボリューム ID からハイフンを除いた値
 - ◀Cloud for Google Cloud▶ ディスク名
 - ◀Cloud for Microsoft Azure▶ ディスク名
- storageNodeId : ストレージノードの ID(uuid)
- deviceFileName : ドライブに対応するデバイスファイル名
- vendorName : ベンダー名
- firmwareRevision : 常に"N/A"
- locatorLedStatus : 常に"N/A"
- driveType : ドライブの種別
- driveCapacity : ドライブの容量[GB]

8.2.3 ドライブの情報の一覧を取得する

各ドライブの情報を一覧で取得します。



メモ

ドライブの種類によって、typeCode、serialNumber、vendorName の出力結果に空白が含まれることがあります。また、有効な値を取得できず、vendorName、firmwareRevision に"N/A"が出力されることがあります。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ドライブの一覧を取得します。

REST API : GET /v1/objects/drives

CLI : drive_list

8.2.4 ドライブの情報を個別に取得する

指定した ID のドライブ情報を取得します。



メモ

ドライブの種類によって、typeCode、serialNumber、vendorName の出力結果に空白が含まれることがあります。また、有効な値を取得できず、vendorName、firmwareRevision に"N/A"が出力されることがあります。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ドライブの ID を確認します。
REST API : GET /v1/objects/drives
CLI : drive_list
2. ドライブの情報を取得します。
ドライブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/drives/<id >
CLI : drive_show

8.3 ドライブの減設

ドライブの減設方法について説明します。

8.3.1 ドライブを減設する <<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ドライブの減設は、障害ドライブの減設を目的に行います。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ドライブを減設する <<Bare metal>> <<Cloud for Google Cloud>> <<Cloud for Microsoft Azure>>」

前提条件

- 実行に必要なロール : Storage

操作手順

1. 減設対象の障害ドライブの ID と、障害ドライブが搭載されたストレージノードの ID を確認します。
また、減設対象の障害ドライブの WWID を記録します。WWID はサーバーから障害ドライブを抜き取る際に使用します。
クエリーパラメーター status に "Blockage" を指定してコマンドを実行します。
REST API : GET /v1/objects/drives
CLI : drive_list
2. 障害ドライブが搭載されているストレージノードの status を確認します。
障害ドライブが搭載されたストレージノードの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/storage-nodes/<id >
CLI : storage_node_show

ストレージノードの status が"Ready"または"RemovalFailed"のとき、次の手順に進みます。

3. 抜き取るドライブのロケーター LED を点灯させます。

operationType(CLI の場合 : operation_type)に"TurnOn"を指定してコマンドを実行します。

REST API : POST /v1/objects/drives/<id >/actions/control-locator-led/invoke

CLI : drive_control_locator_led

コマンド実行後に表示されるジョブの ID を確認します。



注意

ドライブの減設操作中に発生したストレージノード障害によって、REST API、CLI または VSP One SDS Block Administrator で表示されるロケーター LED の点消灯状態が、物理ドライブのロケーター LED の点消灯状態と不一致になることがあります。ストレージノード障害から回復後に、REST API、CLI または VSP One SDS Block Administrator で表示されるロケーター LED の点消灯状態が更新されて不一致が解消されます。



メモ

- 「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載の構成でない場合、ロケーター LED の操作ができないことがあります。この場合は、手順 5 のメモに記載されている方法でドライブの位置を確認してください。
- ドライブを NVMe Drive Direct Attach で構成している場合、「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載されている構成でもロケーター LED 操作は VSP One SDS Block からできません。
日立アドバンストサーバ HA8000V シリーズを使用している場合、ロケーター LED の点消灯は iLO で操作します。具体的な操作方法是ハードウェアのマニュアルを参照してください。
日立アドバンストサーバ HA8000V シリーズ以外の物理サーバーを使用している場合、ロケーター LED の操作方法是、サーバーベンダーのマニュアルを参照してください。

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

5. サーバーからロケーター LED が点灯しているドライブを見つけ出し、抜き取るドライブの搭載位置を確認します。

上記を実施した上で、サーバーから障害ドライブを抜き取ります。

サーバーベンダーのマニュアルを参照して実施してください。



注意

ドライブの減設操作中に発生した障害によって、点灯させたロケーター LED が消灯してしまうことがあります。その場合は手順 3 から再度実施してください。

ドライブの減設操作を中断してストレージノードの再起動を伴う保守操作を実施した場合、点灯させたロケーター LED が消灯してしまうことがあります。その場合は手順 3 から再度実施してください。



メモ

- ロケーター LED が点灯できない場合は、以下の方法で抜き取るドライブの搭載位置を確認します。

手順 1 で記録した障害ドライブの WWID と、増設時に記録したドライブの WWN または EUI の値が一致するドライブを見つけます。また、WWN または EUI と関連付けて記録したドライブの搭載位置を確認します。

- ドライブ増設時に記録した値が WWN だった場合、手順 1 で記録した WWID の右 16 桁部分の、最終 1〜3 桁ほどに差異が生じることがあります。

6. キャッシュ保護付きライトバックモードの状態を確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

- "Disabled"または"Enabling"だった場合は、手順 8 に進みます。
 - "Enabled"または"Disabling"だった場合は、次の手順に進みます。
7. 「キャッシュ保護用メタデータの冗長度を確認する<<Bare metal>>」を参照し、キャッシュ保護用メタデータの冗長度が低下していないことを確認します。
- 冗長度が低下していない場合は、次の手順に進みます。
- 冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。イベントログ KARS06596-E が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 7 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

8. 「リビルドの状態を確認する」を参照して、リビルドが動作中かどうか、またリビルドでエラーが発生していないかどうかを確認します。

リビルドが動作中でなく、かつエラーが発生していないときは、次の手順に進みます。

リビルドが動作中のとき、またはリビルドでエラーが発生しているときは「リビルドの状態を確認する」を参照して対処してください。



メモ

次の手順に進む前にドライブの一覧を取得して、減設対象の障害ドライブが存在することを確認してください。減設対象の障害ドライブが存在しない場合は手順 12 へ進みます。減設対象の障害ドライブの確認方法は手順 1 を参照してください。

9. 障害ドライブを減設します。

手順 1 で確認した障害ドライブの ID を指定してコマンドを実行します。

REST API : POST /v1/objects/drives/<id >/actions/remove/invoke

CLI : drive_remove

コマンド実行後に表示されるジョブの ID を確認します。

10. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

11. ドライブの一覧を取得して、減設対象の障害ドライブが削除されていることを確認します。

手順 9 を実施後、ドライブが削除されるまでには 1 分程度の時間を要することがあります。

REST API : GET /v1/objects/drives

CLI : drive_list

12. 構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

8.3.2 ドライブを減設する <<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

ドライブの減設は、障害ドライブの減設を目的に行います。



注意

- ドライブを減設すると、減設対象の Google Cloud Hyperdisk ボリュームは削除されます。
- ドライブを減設したあとには「ドライブを交換する <<Cloud for Google Cloud>>」に戻り、各ストレージノードのドライブ数が同じになるようにドライブを作成してください。
- 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - 構成ファイルのエクスポート
 - ドライブの減設
 - ドライブの増設
 - ドライブの交換

ドライブの減設では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作して行います。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ドライブを減設する <<Bare metal>> <<Cloud for Google Cloud>> <<Cloud for Microsoft Azure>>」

前提条件

- 実行に必要なロール : Storage

操作手順の留意事項

- Terraform は実行可能な環境から実行してください。
- script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておくと、結果の確認やエラー発生時の対応に有効です。

操作手順

1. コントローラーノードにログインします。

2. 減設対象の障害ドライブの ID を確認します。
クエリーパラメーター `status` に"Blockage"を指定してコマンドを実行します。
REST API : GET /v1/objects/drives
CLI : `drive_list`
3. 障害ドライブが搭載されているストレージノードの `status` を確認します。
障害ドライブが搭載されたストレージノードの ID を指定して、コマンドを実行します。
REST API : GET /v1/objects/storage-nodes/<id >
CLI : `storage_node_show`
ストレージノードの `status` が"Ready"または"RemovalFailed"のとき、次の手順に進みます。
4. 「構成ファイルをエクスポートする<<Cloud for Google Cloud>>」を参照し、VSP One SDS Block からドライブ減設用の構成ファイルを取得します。
構成ファイルをエクスポートする際は、`exportFileType` パラメーターに"ReplaceDrive"を指定してください。
また、`driveId` パラメーターには減設対象の障害ドライブの ID を指定してください。
`recoverSingleDrive` パラメーターの指定は不要です。
最新状態の構成ファイルを使用するために、ドライブ減設用の構成ファイルは必ず取得してください。



注意

構成ファイルのエクスポートで取得した構成ファイルは編集しないでください。編集するとドライブ減設に失敗することがあります。設定値を間違えたときは、正しい値を設定して構成ファイルのエクスポートを再度実行してください。

5. 「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する<<Cloud for Google Cloud>>」を参照し、ドライブ減設用の構成ファイルを配置します。
6. ドライブ減設用の構成ファイルを使用して、ドライブ減設を行います。
減設するドライブに誤りがないかを確認するため、以下のコマンドを実行します。

```
terraform plan
```

7. `terraform plan` での確認に問題がなければ、実際のドライブ減設を行うため以下のコマンドを実行します。

```
terraform apply
```

コマンドの実行後、[Enter a value:]と表示されたら[yes]を入力します。

8. キャッシュ保護付きライトバックモードの状態を確認します。
REST API : GET /v1/objects/storage
CLI : `storage_show`
キャッシュ保護付きライトバックモードの状態(`writeBackModeWithCacheProtection`)によって以下の対応を行います。
 - "Disabled"または"Enabling"だった場合は、手順 10 に進みます。
 - "Enabled"または"Disabling"だった場合は、次の手順に進みます。
9. 「キャッシュ保護用メタデータの冗長度を確認する<<Cloud>>」を参照し、キャッシュ保護用メタデータの冗長度が低下していないことを確認します。
冗長度が低下していない場合は、次の手順に進みます。
冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。
イベントログ `KARS06596-E` が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 9 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

10. 「リビルドの状態を確認する」を参照して、リビルドが動作中かどうか、またリビルドでエラーが発生していないかどうかを確認します。

リビルドが動作中でなく、かつエラーが発生していないときは、次の手順に進みます。

リビルドが動作中のとき、またはリビルドでエラーが発生しているときは「リビルドの状態を確認する」を参照して対処してください。



メモ

次の手順に進む前にドライブの一覧を取得して、減設対象の障害ドライブが存在することを確認してください。減設対象の障害ドライブが存在しない場合は、以上で手順は終了です。減設対象の障害ドライブの確認方法は、手順 2 を参照してください。

11. 障害ドライブを減設します。

手順 2 で確認した障害ドライブの ID を指定してコマンドを実行します。

REST API : POST /v1/objects/drives/<id >/actions/remove/invoke

CLI : drive_remove

コマンド実行後に表示されるジョブの ID を確認します。

12. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

13. ドライブの一覧を取得して、減設対象の障害ドライブが削除されていることを確認します。

手順 11 を実施後、ドライブが削除されるまでには 1 分程度の時間を要することがあります。

REST API : GET /v1/objects/drives

CLI : drive_list

8.3.3 ドライブを減設する ≪Cloud for Microsoft Azure≫

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ドライブの減設は、障害ドライブの減設を目的に行います。



注意

- ドライブを減設すると、減設対象の Azure マネージドディスクボリュームは削除されます。
- ドライブを減設したあとには「ドライブを交換する ≪Cloud for Microsoft Azure≫」に戻り、各ストレージノードのドライブ数が同じになるようにドライブを作成してください。
- 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - 構成ファイルのエクスポート
 - ドライブの減設
 - ドライブの増設

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ドライブを減設する <<Bare metal>> <<Cloud for Google Cloud>> <<Cloud for Microsoft Azure>>」

前提条件

- ・ 実行に必要なロール : Storage
- ・ コントローラーノードで Azure CLI が実行できること

操作手順の留意事項

- ・ 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。
- ・ script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておく、結果の確認やエラー発生時の対応に有効です。

操作手順

1. コントローラーノードにログインします。
2. 減設対象の障害ドライブの ID と障害ドライブが搭載されたストレージノードの ID を確認します。
また、減設対象の障害ドライブのシリアルナンバーを記録します。障害ドライブを特定する際に使用します。
クエリーパラメーター status に"Blockage"を指定してコマンドを実行します。
REST API : GET /v1/objects/drives
CLI : drive_list
3. 障害ドライブが搭載されているストレージノードの status を確認します。
障害ドライブが搭載されたストレージノードの ID を指定して、コマンドを実行します。
REST API : GET /v1/objects/storage-nodes/<id >
CLI : storage_node_show
ストレージノードの status が"Ready"または"RemovalFailed"のとき、次の手順に進みます。
4. Azure ポータルにアクセスして、ディスクの画面に移動します。
ディスクの検索ボックスに障害ドライブのシリアルナンバーを入力して、減設対象のディスクを確認します。ディスク名は記録してください。手順 5 で使用します。
(例) ディスク名は、以下のように表示されます。
<ClusterName>_SN02_UserDataDisk01_disk
5. 次の Azure CLI を実行し、減設対象のディスクをデタッチします。

```
az vm disk detach --resource-group <リソースグループ名> ¥  
--vm-name <障害ストレージノードの Azure VM インスタンス名> ¥  
--name <デタッチ対象のディスク名>
```

Azure ポータルまたは Azure CLI で減設対象のディスクがデタッチされていることを確認してください。

6. 次の Azure CLI を実行し、デタッチしたディスクを削除します。

```
az disk delete --name <削除対象のディスク名> ¥  
--resource-group <リソースグループ名>
```

Azure ポータルまたは Azure CLI で減設対象のディスクが削除されていることを確認してください。

7. キャッシュ保護付きライトバックモードの状態を確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

- "Disabled"または"Enabling"だった場合は、手順 9 に進みます。
 - "Enabled"または"Disabling"だった場合は、次の手順に進みます。
8. 「キャッシュ保護用メタデータの冗長度を確認する<<Cloud>>」を参照し、キャッシュ保護用メタデータの冗長度が低下していないことを確認します。
- 冗長度が低下していない場合は、次の手順に進みます。
- 冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。イベントログ KARS06596-E が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 8 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

9. 「リビルドの状態を確認する」を参照して、リビルドが動作中かどうか、またリビルドでエラーが発生していないかどうかを確認します。
- リビルドが動作中でなく、かつエラーが発生していないときは、次の手順に進みます。
- リビルドが動作中のとき、またはリビルドでエラーが発生しているときは「リビルドの状態を確認する」を参照して対処してください。



メモ

次の手順に進む前にドライブの一覧を取得して、減設対象の障害ドライブが存在することを確認してください。減設対象の障害ドライブが存在しない場合は、以上で手順は終了です。

減設対象の障害ドライブの確認方法は、手順 2 を参照してください。

10. 障害ドライブを減設します。

手順 2 で確認した障害ドライブの ID を指定してコマンドを実行します。

REST API : POST /v1/objects/drives/<id >/actions/remove/invoke

CLI : drive_remove

コマンド実行後に表示されるジョブの ID を確認します。

11. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

12. ドライブの一覧を取得して、減設対象の障害ドライブが削除されていることを確認します。

手順 10 を実施後、ドライブが削除されるまでには 1 分程度の時間を要することがあります。

REST API : GET /v1/objects/drives

8.4 ドライブの交換

ドライブの交換方法について説明します。

8.4.1 ドライブを交換する《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

障害ドライブを別のドライブと交換します。

ドライブ自動回復機能に関する注意事項

Bare metal モデルではドライブの応答遅延に伴うドライブ障害から、ドライブの自動復旧を行うドライブ自動回復機能があります。ドライブ自動回復機能が動作する条件を満たしている場合、ドライブを交換する必要はありません。ドライブの自動回復が完了するまでお待ちください。

ドライブの自動回復を待つか、ドライブを交換するかの判断方法は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ドライブの Health Status に "Alerting"発生時の対処」を参照してください。

以下の場合、ドライブ自動回復は動作しません。この節の説明に従ってドライブを交換してください。

- ドライブの障害要因がドライブの応答遅延ではない場合
ドライブの障害要因がドライブの応答遅延の場合、イベントログ KARS05012-E が出力されます。
- リビルド領域の確保状態が"Sufficient"以外であり、リビルドが動作できない場合
ただし、リビルド領域の確保状態が"Sufficient"以外の場合でも、障害が発生したドライブによってはリビルドが動作可能な場合があります。この場合はリビルド完了後にドライブ自動回復も動作します。リビルド領域の確保状態の詳細や確認方法については「ストレージプールを管理する」を参照してください。
- リビルド可能な領域が確保されていない場合
- ドライブ自動回復処理中にドライブ障害が発生した場合
- キャッシュ保護用メタデータの冗長度低下なしの状態に戻せない場合

ドライブ自動回復機能は常に有効であり、無効には設定できません。

ドライブの応答遅延に伴うドライブ障害とドライブの自動回復が繰り返す場合など、応答遅延が頻発するドライブを交換する場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「応答遅延が頻発するドライブを交換したい場合の対処」を参照して対処してください。



メモ

ドライブ自動回復が動作したドライブのデータは、リビルドによって他のドライブに再構築されています。この場合、回復したドライブの領域はリビルド用の空き領域として確保され、リビルドやストレージプール拡張など、ドライブのデータ配置が変更となるイベントが発生するまで当該ドライブに対するアクセスは発生しません。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ドライブを交換する <<Bare metal>>」

前提条件

- ・ 実行に必要なロール：Storage

操作手順

1. 減設対象の障害ドライブの ID と、障害ドライブが搭載されたストレージノードの ID を確認します。
また、減設対象の障害ドライブの WWID を記録します。WWID はサーバーから障害ドライブを抜き取る際に使用します。
クエリーパラメーター status に"Blockage"を指定してコマンドを実行します。
REST API : GET /v1/objects/drives
CLI : drive_list
2. 障害ドライブが搭載されているストレージノードの status を確認します。
障害ドライブが搭載されたストレージノードの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/storage-nodes/<id >
CLI : storage_node_show
status が"Ready"または"RemovalFailed"のとき、次の手順に進みます。
3. 抜き取るドライブのロケーター LED を点灯させます。
operationType(CLI の場合：operation_type)に"TurnOn"を指定してコマンドを実行します。
REST API : POST /v1/objects/drives/<id >/actions/control-locator-led/invoke
CLI : drive_control_locator_led
コマンド実行後に表示されるジョブの ID を確認します。



注意

ドライブの交換操作中に発生したストレージノード障害によって、REST API、CLI、または VSP One SDS Block Administrator で表示されるロケーター LED の点消灯状態が、物理ドライブのロケーター LED の点消灯状態と不一致になることがあります。ストレージノード障害から回復後に、REST API、CLI、または VSP One SDS Block Administrator で表示されるロケーター LED の点消灯状態が更新されて不一致が解消されます。



メモ

- ・ 「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載の構成でない場合、ロケーター LED の操作ができないことがあります。この場合は、手順 5 のメモに記載されている方法でドライブの位置を確認してください。
- ・ ドライブを NVMe Drive Direct Attach で構成している場合、「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載されている構成でもロケーター LED 操作は VSP One SDS Block からできません。
日立アドバンストサーバ HA8000V シリーズを使用している場合、ロケーター LED の点消灯は iLO で操作します。具体的な操作方法はハードウェアのマニュアルを参照してください。

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

5. サーバーからロケータ LED が点灯しているドライブを見つけ出し、抜き取るドライブの搭載位置を確認します。

上記を実施した上で、サーバーから障害ドライブを抜き取ります。

サーバーベンダーのマニュアルを参照して実施してください。



注意

ドライブの交換操作中に発生した障害によって、点灯させたロケータ LED が消灯してしまうことがあります。その場合は手順 3 から再度実施してください。

ドライブの交換操作を中断してストレージノードの再起動を伴う保守操作を実施した場合、点灯させたロケータ LED が消灯してしまうことがあります。その場合は手順 3 から再度実施してください。



メモ

- ・ ロケータ LED が点灯できない場合は、以下の方法で抜き取るドライブの搭載位置を確認します。
手順 1 で記録した障害ドライブの WWID と、増設時に記録したドライブの WWN または EUI の値が一致するドライブを見つけます。また、WWN または EUI と関連付けて記録したドライブの搭載位置を確認します。
- ・ ドライブ増設時に記録した値が WWN だった場合、手順 1 で記録した WWID の右 16 桁部分の、最終 1~3 桁ほどに差異が生じることがあります。

6. 「ドライブを増設する」の「ドライブを挿入する <<Bare metal>>」から「ストレージプールを拡張する」の手順 5 までは実施します。増設するドライブは手順 5 で抜き取った障害ドライブではなく、新規ドライブにしてください。



注意

複数のドライブを同時に交換する場合は、手順 1 から 6(物理ドライブ減設および増設操作)については、1 ドライブずつ実施してください。すべてのドライブで手順 6 が完了したら、手順 7 以降を実施してください。

7. キャッシュ保護付きライトバックモードの状態を確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

- ・ "Disabled"または"Enabling"だった場合は、手順 9 に進みます。
- ・ "Enabled"または"Disabling"だった場合は、次の手順に進みます。

8. 「キャッシュ保護用メタデータの冗長度を確認する <<Bare metal>>」を参照し、キャッシュ保護用メタデータの冗長度が低下していないことを確認します。

冗長度が低下していない場合は、次の手順に進みます。

冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。イベントログ **KARS06596-E** が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 8 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

9. 「リビルドの状態を確認する」を参照して、リビルドが動作中かどうか、またリビルドでエラーが発生していないかどうかを確認します。

リビルドが動作中でなく、かつエラーが発生していないときは、次の手順に進みます。リビルドが動作中のとき、またはリビルドでエラーが発生しているときは「リビルドの状態を確認する」を参照して対処してください。



メモ

次の手順に進む前にドライブの一覧を取得して、減設対象の障害ドライブが存在することを確認してください。減設対象の障害ドライブが存在しない場合は手順 13 へ進みます。減設対象の障害ドライブの確認方法は手順 1 を参照してください。

10. 障害ドライブを減設します。

手順 1 で確認した障害ドライブの ID を指定してコマンドを実行します。

REST API : POST /v1/objects/drives/<id >/actions/remove/invoke

CLI : drive_remove

コマンド実行後に表示されるジョブの ID を確認します。

11. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

12. ドライブの一覧を取得して、減設対象の障害ドライブが削除されていることを確認します。

手順 10 を実施後、ドライブが削除されるまでには 1 分程度の時間を要することがあります。

REST API : GET /v1/objects/drives

CLI : drive_list

13. 構成情報のバックアップを行います。

「構成情報をバックアップする《Bare metal》《Cloud for AWS》」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

8.4.2 ドライブを交換する《Cloud for AWS》

この項での記述内容は Cloud モデル for AWS に適用されます。

障害ドライブを別のドライブと交換します。



注意

- 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - 構成ファイルのエクスポート
 - ドライブの増設
 - ドライブの交換
- EBS 暗号化を利用している場合は、AWS を操作するアカウントやコントローラーノードに設定する IAM ロールに、AWS Key Management Service へアクセスするための権限を追加する必要があります。詳細は、AWS のユーザーガイドを参照してください。

ドライブの交換では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作を行います。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ドライブを交換する <<Cloud>>」

前提条件

- 実行に必要なロール：Storage

操作手順の留意事項

- 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。¥記号を含めてコピーアンドペーストしても正しく動作します。
- 本手順では AWS CLI を使用して実施していますが、CloudFormation のスタックのステータスや動作状況は AWS マネジメントコンソールの AWS CloudFormation コンソールからも確認できます。
- script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておくと、結果の確認やエラー発生時の対応に有効です。

操作手順

1. コントローラーノードにログインします。
2. 交換対象の障害ドライブの ID と、障害ドライブが搭載されたストレージノードの ID を確認します。

また、交換対象の障害ドライブのシリアルナンバーを記録します。障害ドライブを特定する際に使用します。

status"Blockage"をクエリーパラメーターで指定して、コマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

3. 障害ドライブが搭載されているストレージノードの status を確認します。

障害ドライブが搭載されたストレージノードの ID を指定して、コマンドを実行します。

REST API : GET /v1/objects/storage-nodes/<id >

CLI : storage_node_show

ストレージノードの status が"Ready"または"RemovalFailed"のとき、次の手順に進みます。

4. AWS マネジメントコンソールにアクセスして、EC2 の画面に移動します。

画面左側のナビゲーションペインからボリュームをクリックしてください。

5. ボリュームの検索ボックスに障害ドライブのシリアルナンバー("vol"の文字列の後ろにハイフンを追記したもの)を入力して、交換対象のドライブ番号を確認します。

確認したドライブ番号は記録してください。手順 11 で使用します。

(例) ドライブの番号が 1 の場合、以下のように表示されます。

<構築時にパラメーターで指定した ClusterName>_SN02_UserDataDisk01

6. 「構成ファイルをエクスポートする《Cloud for AWS》」を参照し、VSP One SDS Block からドライブ交換用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、exportFileType パラメーターに"ReplaceDrive"を指定してください。

また、driveId パラメーターに手順 2 で確認した交換対象の障害ドライブの ID を指定してください。

最新状態の構成ファイルを使用するために、必ず取得してください。

複数のドライブを交換する場合は手順 6～21 を繰り返します。



注意 構成ファイルのエクスポートで取得した構成ファイルは編集しないでください。編集するとドライブ交換に失敗することがあります。設定値を間違えたときは、正しい値を設定して構成ファイルのエクスポートを再度実行してください。

7. 構成ファイルのエクスポートで取得した構成ファイル一式を手順 6 で templateS3Url パラメーターで指定した Amazon S3 バケットに格納します。

Amazon S3 にファイルを格納する方法として、例えば AWS CLI を用いて Amazon S3 にファイルをコピーする方法があります。詳細は Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「Amazon S3 の操作例」を参照してください。



注意 VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。

8. 次の AWS CLI を実行して変更セットを作成します。複数のドライブを交換する場合は手順 6～17 を繰り返します。

```
aws cloudformation create-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <任意の変更セット名*> ¥
--template-url <Amazon S3 に格納した VMConfigurationFile.yml の URL (https)> ¥
--include-nested-stacks ¥
--capabilities CAPABILITY_NAMED_IAM
```

*使用可能文字などは以下の Web サイトを参照してください。

<https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-change-set.html>

9. 次の AWS CLI を実行して変更セットを表示します(1 階層目)。

```
aws cloudformation describe-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 8 で指定した変更セット名>
```

以下の事項を確認します。

- "Status"が"CREATE_COMPLETE"であること

"Status"が"CREATE_IN_PROGRESS"の場合はしばらく待ってから再度実行してください。

- "Changes"の項目数が 1 個であること
- "Changes"内の"ResourceChange"について
 - "Action"が"Modify"であること
 - 次の手順のため、"ChangeSetId"の値を記録します。

10. 次の AWS CLI を実行して変更セットを表示します(2 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 9 で記録した"ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
 - "Action"が"Modify"であること
 - "LogicalResourceId"が"StorageNodeXX"であること(XX は障害ドライブが搭載されたストレージノードの番号)
 - 次の手順のため、各項目の"ChangeSetId"の値を記録します。

11. 次の AWS CLI を実行して各ストレージノードのスタックの変更セットを表示します(3 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 10 で記録した"ChangeSetId">
```

RemoveDriveNodeNumber で指定したストレージノードの場合、以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
 - "Action"が"Remove"である項目の"LogicalResourceId"が"VolumeAttachmentXX"、または"UserDataDiskXX"であること(XX は指定した障害ドライブの番号)
- 上記以外の"Changes"内の各項目の"ResourceChange"について、"Action"がすべて"Modify"であることを確認します。

12. 次の AWS CLI を実行して、作成した変更セットを実行します。

```
aws cloudformation execute-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 8 で指定した変更セット名>
```

13. 次の AWS CLI を実行して、変更セットの実行結果を確認します。

wait stack-update-complete を実行すると、変更セットの実行が完了するまで待つことができます。

```
aws cloudformation wait stack-update-complete ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

実行が完了したら、describe-stacks を実行して、StackStatus が"UPDATE_COMPLETE"であることを確認してください。

```
aws cloudformation describe-stacks ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

14. 「構成ファイルをエクスポートする《Cloud for AWS》」を参照し、VSP One SDS Block からドライブ交換用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、`exportFileType` パラメーターに"ReplaceDrive"を指定してください。

また、`RecoverSingleDrive` パラメーターに"true"を指定してください。

最新状態の構成ファイルを使用するために、必ず取得してください。



注意 構成ファイルのエクスポートで取得した構成ファイルは編集しないでください。編集するとドライブ交換に失敗することがあります。設定値を間違えたときは、正しい値を設定して構成ファイルのエクスポートを再度実行してください。

15. 構成ファイルのエクスポートで取得した構成ファイル一式を手順 14 で `templateS3Url` パラメーターで指定した Amazon S3 バケットに格納します。

Amazon S3 にファイルを格納する方法として、例えば AWS CLI を用いて Amazon S3 にファイルをコピーする方法があります。詳細は Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「Amazon S3 の操作例」を参照してください。



注意 VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。

16. 次の AWS CLI を実行して変更セットを作成します。

```
aws cloudformation create-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <任意の変更セット名*> ¥
--template-url <Amazon S3 に格納した VMConfigurationFile.yml の
URL(https)> ¥
--include-nested-stacks ¥
--capabilities CAPABILITY_NAMED_IAM
```

*使用可能文字などは以下の Web サイトを参照してください。

<https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-change-set.html>

17. 次の AWS CLI を実行して変更セットを表示します(1 階層目)。

```
aws cloudformation describe-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 16 で指定した変更セット名>
```

以下の事項を確認します。

- "Status"が"CREATE_COMPLETE"であること
- "Status"が"CREATE_IN_PROGRESS"の場合はしばらく待ってから再度実行してください。
- "Changes"の項目数が 1 個であること
- "Changes"内の"ResourceChange"について
 - "Action"が"Modify"であること
 - 次の手順のため、"ChangeSetId"の値を記録します。

18. 次の AWS CLI を実行して変更セットを表示します(2 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 17 で記録した"ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
 - "Action"が"Modify"であること
 - "LogicalResourceId"が"StorageNodeXX"であること(XX は障害ドライブが搭載されたストレージノードの番号)
 - 次の手順のため、各項目の"ChangeSetId"の値を記録します。

19. 次の AWS CLI を実行して各ストレージノードのスタックの変更セットを表示します(3 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 18 で記録した"ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
 - "Action"が"Add"である項目の"LogicalResourceId"が"VolumeAttachmentXX"、または"UserDataDiskXX"であること(XX は指定した障害ドライブの番号)
 - 他の項目の"Action"がすべて"Modify"であること

20. 次の AWS CLI を実行して、作成した変更セットを実行します。

```
aws cloudformation execute-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 16 で指定した変更セット名>
```

21. 次の AWS CLI を実行して、変更セットの実行結果を確認します。

wait stack-update-complete を実行すると、変更セットの実行が完了するまで待つことができます。

```
aws cloudformation wait stack-update-complete ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

実行が完了したら、describe-stacks を実行して、StackStatus が"UPDATE_COMPLETE"であることを確認してください。

```
aws cloudformation describe-stacks ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

22. ドライブの一覧を取得して、新規ドライブが追加されたことを確認します。

REST API : GET /v1/objects/drives

CLI : drive_list



ヒント

新規ドライブは、status が"Offline"のドライブです。ドライブの status はドライブ情報から取得できます。

23. 「ストレージプールを拡張する」の手順 5 までを実施します。

24. キャッシュ保護付きライトバックモードの状態を確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

- "Disabled"または"Enabling"だった場合は、手順 26 に進みます。

- "Enabled"または"Disabling"だった場合は、次の手順に進みます。
25. 「キャッシュ保護用メタデータの冗長度を確認する<<Cloud>>」を参照し、キャッシュ保護用メタデータの冗長度が低下していないことを確認します。
- 冗長度が低下していない場合は、次の手順に進みます。
- 冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。イベントログ KARS06596-E が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 25 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

26. 「リビルドの状態を確認する」を参照して、リビルドが動作中かどうか、またリビルドでエラーが発生していないかどうかを確認します。
- リビルドが動作中でなく、かつエラーが発生していないときは、次の手順に進みます。リビルドが動作中のとき、またはリビルドでエラーが発生しているときは「リビルドの状態を確認する」を参照して対処してください。



メモ

次の手順に進む前にドライブの一覧を取得して、減設対象の障害ドライブが存在することを確認してください。減設対象の障害ドライブが存在しない場合は、以上で手順は終了です。減設対象の障害ドライブの確認方法は、手順 2 を参照してください。

27. 障害ドライブを減設します。
- 手順 2 で確認した障害ドライブの ID を指定してコマンドを実行します。
- REST API : POST /v1/objects/drives/<id >/actions/remove/invoke
- CLI : drive_remove
- コマンド実行後に表示されるジョブの ID を確認します。
28. ジョブの state を確認します。
- ジョブの ID を指定してコマンドを実行します。
- REST API : GET /v1/objects/jobs/<jobId >
- CLI : job_show
- state が"Succeeded"になっていたらジョブは完了です。
29. ドライブの一覧を取得して、減設対象の障害ドライブが削除されていることを確認します。
- 手順 27 を実施後、ドライブが削除されるまでには 1 分程度の時間を要することがあります。
- REST API : GET /v1/objects/drives
- CLI : drive_list
30. 構成情報のバックアップを行います。
- 「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
- ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

8.4.3 ドライブを交換する<<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

障害ドライブを別のドライブと交換します。



注意

次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。

- ストレージノードの増設
- ストレージノードの交換
- 構成ファイルのエクスポート
- ドライブの減設
- ドライブの増設
- ドライブの交換

ドライブの交換では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラノード上から操作して行います。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ドライブを交換する<<Cloud>>」

前提条件

- 実行に必要なロール：Storage

操作手順の留意事項

- Terraform は実行可能な環境から実行してください。
- script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておく、結果の確認やエラー発生時の対応に有効です。

操作手順

1. 「ドライブを減設する<<Cloud for Google Cloud>>」の手順 1 から 7 を実施します。

複数のドライブを交換する場合は、「ドライブを交換する<<Cloud for Google Cloud>>」の手順 1 から 5 を 1 ドライブずつ実施し、交換するドライブの台数分だけ繰り返してください。

2. 「構成ファイルをエクスポートする<<Cloud for Google Cloud>>」を参照し、VSP One SDS Block からドライブ交換用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、exportFileType パラメーターに"ReplaceDrive"を指定してください。

また、recoverSingleDrive パラメーターに"true"を指定してください。

driveId パラメーターの指定は不要です。

最新状態の構成ファイルを使用するために、ドライブ交換用の構成ファイルは必ず取得してください。



注意

構成ファイルのエクスポートで取得した構成ファイルは編集しないでください。編集するとドライブ交換に失敗することがあります。設定値を間違えたときは、正しい値を設定して構成ファイルのエクスポートを再度実行してください。

3. 「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する<<Cloud for Google Cloud>>」を参照し、ドライブ交換用の構成ファイルを配置します。
4. ドライブ交換用の構成ファイルを使用して、ドライブ交換を行います。

交換するドライブに誤りがないかを確認するため、以下のコマンドを実行します。

```
terraform plan
```

5. terraform plan での確認に問題がなければ、実際のドライブ交換を行うため以下のコマンドを実行します。

```
terraform apply
```

コマンドの実行後、[Enter a value:]と表示されたら[yes]を入力します。

6. 「ストレージプールを拡張する」の手順 5 までを実施します。
7. キャッシュ保護付きライトバックモードの状態を確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

- "Disabled"または"Enabling"だった場合は、手順 9 に進みます。
 - "Enabled"または"Disabling"だった場合は、次の手順に進みます。
8. 「キャッシュ保護用メタデータの冗長度を確認する<<Cloud>>」を参照し、キャッシュ保護用メタデータの冗長度が低下していないことを確認します。
冗長度が低下していない場合は、次の手順に進みます。
冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。
イベントログ KARS06596-E が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 8 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

9. 「リビルドの状態を確認する」を参照して、リビルドが動作中かどうか、またリビルドでエラーが発生していないかどうかを確認します。
リビルドが動作中でなく、かつエラーが発生していないときは、次の手順に進みます。リビルドが動作中のとき、またはリビルドでエラーが発生しているときは「リビルドの状態を確認する」を参照して対処してください。



メモ

次の手順に進む前にドライブの一覧を取得して、減設対象の障害ドライブが存在することを確認してください。減設対象の障害ドライブが存在しない場合は、以上で手順は終了です。
減設対象の障害ドライブの確認方法は「ドライブを減設する<<Cloud for Google Cloud>>」の手順 2 を参照してください。

10. 障害ドライブを減設します。

障害ドライブの ID を指定してコマンドを実行します。

REST API : POST /v1/objects/drives/<id>/actions/remove/invoke

CLI : drive_remove

コマンド実行後に表示されるジョブの ID を確認します。

11. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

12. ドライブの一覧を取得して、減設対象の障害ドライブが削除されていることを確認します。
手順 10 を実施後、ドライブが削除されるまでには 1 分程度の時間を要することがあります。

REST API : GET /v1/objects/drives

CLI : drive_list

8.4.4 ドライブを交換する《Cloud for Microsoft Azure》

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

障害ドライブを別のドライブと交換します。



注意

次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。

- ・ ストレージノードの増設
- ・ ストレージノードの交換
- ・ 構成ファイルのエクスポート
- ・ ドライブの減設
- ・ ドライブの増設
- ・ ドライブの交換

ドライブの交換では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作して行います。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ドライブを交換する《Cloud》」

前提条件

- ・ 実行に必要なロール : Storage
- ・ コントローラーノードで Azure CLI が実行できること

操作手順の留意事項

- ・ 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。
- ・ script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておく、結果の確認やエラー発生時の対応に有効です。

操作手順

1. 「ドライブを減設する《Cloud for Microsoft Azure》」の手順 1 から 6 を実施します。
複数のドライブを交換する場合は、「ドライブを減設する《Cloud for Microsoft Azure》」の手順 5 と 6 を 1 ドライブずつ実施し、交換するドライブの台数分だけ繰り返してください。

2. 「構成ファイルをエクスポートする<<Cloud for Microsoft Azure>>」を参照し、VSP One SDS Block からドライブ交換用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、**exportFileType** パラメーターに"ReplaceDrive"を指定してください。

最新状態の構成ファイルを使用するために、ドライブ交換用の構成ファイルは必ず取得してください。



注意

パラメーターで指定する値を間違えた場合は、正しい値を指定して構成ファイルのエクスポートを再度実行し、最新の構成ファイルを取得しなおしてください。

3. エクスポートした ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz を解凍します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、ジョブが失敗するおそれがあります。

4. ドライブ交換用の構成ファイルを使用して、次のコマンドを実行します。

```
az deployment group create ¥
--name mainTemplate ¥
--resource-group <ストレージクラスター用リソースグループ名> ¥
--template-file VMConfigurationFile.json ¥
--parameters VMConfigurationFile.parameters.json
```

5. 実行結果を確認します。

Azure CLI がエラーになっていないこと、または Azure ポータルでストレージクラスター用リソースグループの画面へ移動し、デプロイが成功していることを確認してください。

6. ドライブの一覧を取得して、新規ドライブが追加されたことを確認します。

REST API : GET /v1/objects/drives

CLI : drive_list



ヒント

新規ドライブは、status が"Offline"のドライブです。ドライブの status はドライブ情報から取得できます。

7. 「ストレージプールを拡張する」の手順 5 までを実施します。

8. キャッシュ保護付きライトバックモードの状態を確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

- "Disabled"または"Enabling"だった場合は、手順 10 に進みます。
- "Enabled"または"Disabling"だった場合は、次の手順に進みます。

9. 「キャッシュ保護用メタデータの冗長度を確認する<<Cloud>>」を参照し、キャッシュ保護用メタデータの冗長度が低下していないことを確認します。

冗長度が低下していない場合は、次の手順に進みます。

冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。イベントログ KARS06596-E が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 9 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

10. 「リビルドの状態を確認する」を参照して、リビルドが動作中かどうか、またリビルドでエラーが発生していないかどうかを確認します。

リビルドが動作中でなく、かつエラーが発生していないときは、次の手順に進みます。リビルドが動作中のとき、またはリビルドでエラーが発生しているときは「リビルドの状態を確認する」を参照して対処してください。



メモ

次の手順に進む前にドライブの一覧を取得して、減設対象の障害ドライブが存在することを確認してください。減設対象の障害ドライブが存在しない場合は、以上で手順は終了です。

減設対象の障害ドライブの確認方法は、「ドライブを減設する <<Cloud for Microsoft Azure>>」の手順 2 を参照してください。

11. 障害ドライブを減設します。

障害ドライブの ID を指定してコマンドを実行します。

REST API : POST /v1/objects/drives/<id >/actions/remove/invoke

CLI : drive_remove

コマンド実行後に表示されるジョブの ID を確認します。

12. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

13. ドライブの一覧を取得して、減設対象の障害ドライブが削除されていることを確認します。

手順 11 を実施後、ドライブが削除されるまでには 1 分程度の時間を要することがあります。

REST API : GET /v1/objects/drives

CLI : drive_list

8.5 ドライブを再組み入れする <<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ドライブの再組み入れは、閉塞したドライブの再利用を目的に行います。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ドライブを再組み入れする <<Bare metal>>」

前提条件

- ・ 実行に必要なロール : Storage

操作手順

1. 「ドライブを減設する<<Bare metal>>」の手順 1 から手順 11 までを実施します。
2. 「ドライブを増設する」の「ドライブを挿入する<<Bare metal>>」の手順すべてと「ストレージプールを拡張する」の手順 1 から手順 8 までを実施します。

増設するドライブは手順 1 で抜き取った閉塞ドライブを使用します。

再組み入れが成功したら「ドライブを挿入する<<Bare metal>>」の手順 1 で記録した情報に当該ドライブが再組み入れ済みであることを関連付けて記録しておいてください。

記録した情報は、ドライブ閉塞時にドライブ再組み入れとドライブ交換のどちらの保守手順を実施するか判定に使用します。



注意

- 複数のドライブを同時に再組み入れする場合は、1 ドライブずつ手順 1 と 2 を実施してください。
 - 抜き取ったドライブを再度挿入する際は、20 秒ほど待ってから実施してください。
-

ドライブを増設する

- 9.1 ドライブ増設の概要
- 9.2 ドライブを挿入する<<Bare metal>>
- 9.3 ドライブを作成する<<Cloud for AWS>>
- 9.4 ドライブを作成する<<Cloud for Google Cloud>>
- 9.5 ドライブを作成する<<Cloud for Microsoft Azure>>
- 9.6 ストレージプールを拡張する

9.1 ドライブ増設の概要

ストレージプールの容量を追加するためにドライブを増設します。

ストレージプールの容量の追加には、全ストレージノードへのドライブ増設が必要です。必要なドライブ容量は構成によって異なります。「増設時の容量設計」を参照して必要な容量を準備してください。



注意

- 増設するドライブの既存データは失われてしまいます。注意してください。
- ドライブ増設後、増設したドライブに対して自動でユーザーデータを移動することがあります。ユーザーデータの移動中は、ホスト I/O 性能が低下することがあります。
- スペアノードを登録済みの場合、スペアノードに対してもドライブを増設してください。

ドライブ増設の要件<<Bare metal>>

増設するドライブは「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載してあるハードウェアから選択してください。その他のドライブ増設の要件は以下のとおりです。

項目	要件	備考
増設対象のドライブを搭載したストレージノードの status	"Ready"または"RemovalFailed"であること	
ユーザーデータドライブの最大数 (ストレージノード 1 台当たり)	24	ストレージノードとして使用するサーバーによって台数の上限は異なります。
ドライブの種類	SSD(SAS または NVMe)であること	
ドライブの容量	ドライブ 1 台当たりの必要容量を満たしていること HPEC 4D+1P の場合 : 249[GiB]以上 HPEC 4D+2P の場合 : 298[GiB]以上 Mirroring Duplication の場合 : 201[GiB]以上	下記を超えるドライブを搭載しても、システムでは使用されません。 HPEC 4D+1P の場合 : 124[TiB] HPEC 4D+2P の場合 : 148[TiB] Mirroring Duplication の場合 : 198[TiB]

ドライブ増設の要件<<Cloud>>

Cloud モデルにおけるドライブ増設の要件は以下のとおりです。



注意

<<Cloud for AWS>>ベースライセンスとして Floating を適用している場合、ドライブの増設によって AWS License Manager のライセンスの契約容量を超過する場合があります。増設手順を実施する前に「ライセンスの使用量を確認するためにストレージプールの容量を試算する<<Cloud for AWS>>」を参照して、ドライブ増設後のストレージプールの容量を計算し、ストレージプールの論理容量が AWS License Manager のライセンスの契約容量に収まるかを確認してください。なお、必要なライセンスの契約容量は、ストレージプールの論理容量を TiB 単位に切り上げて計算してください。

複数のストレージクラスターで AWS License Manager のライセンスを共有している場合は、ストレージクラスターそれぞれのストレージプールの論理容量を先に TiB 単位に切り上げてから、それらを合計した値が、AWS License Manager のライセンスの契約容量に収まるかを確認してください。

(例) 2つのストレージクラスターがあって、それぞれのストレージプールの論理容量が 31.3[TiB]と 47.7[TiB]の場合、それぞれの値を整数値に切り上げて 32[TiB]と 48[TiB]としてから、それらを合計して 80[TiB]と計算します。

契約容量が不足する場合、AWS Marketplace 上でライセンスの契約を更新してください。

項目	要件	備考
増設対象のドライブを搭載したストレージノードの status	"Ready"または"RemovalFailed"であること	
ユーザーデータドライブの最大数(ストレージノード 1 台当たり)	24	
ストレージノード 1 台当たりのユーザーデータドライブの台数	すべてのストレージノード*で同じ台数であること	* Multi-AZ (Multi-Zone)構成のタイブレーカーノードを除きます。
ドライブの種類	<<Cloud for AWS>>SSD(gp3)であること <<Cloud for Google Cloud>>SSD(hd-balanced)であること <<Cloud for Microsoft Azure>>SSD(Premium SSD v2)であること	
ドライブの性能と容量	初回構築時と同一の性能、容量であること	初回構築時の設定からドライブの性能と容量は変更できません。

ドライブ増設の手順

ドライブ増設の操作手順の実施順と参照先を以下に示します。



メモ

<<Bare metal>>複数のストレージノードにドライブを増設する場合は、「ドライブを挿入する<<Bare metal>>」をストレージノードの数だけ繰り返し実施したあと、増設したすべてのドライブ情報を確認した上で「ストレージプールを拡張する」を実施してください。

モデル	操作手順の実施順と参照先
Bare metal モデル	1. 「 9.2 ドライブを挿入する<<Bare metal>> 」 2. 「 9.6 ストレージプールを拡張する 」
Cloud モデル for AWS	1. 「 9.3 ドライブを作成する<<Cloud for AWS>> 」 2. 「 9.6 ストレージプールを拡張する 」
Cloud モデル for Google Cloud	1. 「 9.4 ドライブを作成する<<Cloud for Google Cloud>> 」 2. 「 9.6 ストレージプールを拡張する 」
Cloud モデル for Microsoft Azure	1. 「 9.5 ドライブを作成する<<Cloud for Microsoft Azure>> 」 2. 「 9.6 ストレージプールを拡張する 」

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ドライブを増設する」

9.2 ドライブを挿入する《Bare metal》

この節での記述内容は Bare metal モデルに適用されます。

増設するドライブをストレージノードに挿入します。

前提条件

- ・ 実行に必要なロール : Security、Storage、Monitor、Service、または Resource

操作手順

1. 増設するすべてのドライブ(現物)の搭載位置、ドライブ(現物)の形名、ドライブ(現物)に貼り付けられているラベルに記載された WWN または EUI を関連付けて記録しておいてください。
記録した情報は、ドライブ減設時やドライブ交換時に使用します。また、格納データ暗号化を有効化する場合暗号化鍵の情報を監査するときにも使用します。
2. 増設するドライブをストレージノードに挿入します。
サーバーベンダーのマニュアルを参照して実施してください。



メモ

ドライブ増設を行うストレージノードで、ユーザーデータドライブがディスクコントローラーに接続されている場合は、以下の点を確認してください。
ユーザーデータドライブはユーザーデータドライブのみが接続されるディスクコントローラーとの結線を確認した上で、任意のドライブスロットに搭載してください。このとき、ユーザーデータドライブを接続するディスクコントローラーが複数枚の場合、障害点および負荷を分散するため、各ディスクコントローラーに接続されるユーザーデータドライブ数が均等になるようにユーザーデータドライブを接続するようお勧めします。

3. ドライブの一覧を取得してドライブが増設されたことを確認します。
ドライブを増設したストレージノードの ID をクエリーパラメーターで指定してコマンドを実行します。

REST API : GET /v1/objects/drives
CLI : drive_list

増設したドライブが確認できるまでには、1 分程度の時間を要することがあります。増設したドライブが確認できなかった場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ドライブが認識されない場合の対処」に従って対処してください。

9.3 ドライブを作成する《Cloud for AWS》

この節での記述内容は Cloud モデル for AWS に適用されます。



注意

- ・ 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ・ ストレージノードの増設
 - ・ ストレージノードの交換
 - ・ 構成ファイルのエクスポート
 - ・ ドライブの増設

- ドライブの交換
- EBS 暗号化を利用している場合は、AWS を操作するアカウントやコントローラーノードに設定する IAM ロールに、AWS Key Management Service へアクセスするための権限を追加する必要があります。詳細は、AWS のユーザーガイドを参照してください。



メモ

ベースライセンスとして Floating を適用している場合、「ドライブ増設の要件《Cloud》」を参照してドライブ増設後のストレージプールの論理容量が AWS License Manager のライセンスの契約容量に収まるかを確認してください。

ドライブの増設では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作を行います。

前提条件

- 実行に必要なロール：Security、Storage、Monitor、Service、または Resource

操作手順の留意事項

- 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。¥記号を含めてコピーアンドペーストしても正しく動作します。
- 本手順では AWS CLI を使用して実施していますが、CloudFormation のスタックのステータスや動作状況は AWS マネジメントコンソールの AWS CloudFormation コンソールからも確認できます。
- script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておく、結果の確認やエラー発生時の対応に有効です。

操作手順

1. コントローラーノードにログインします。
2. 次の AWS CLI を実行して、現在のストレージノード 1 台当たりのドライブの数を確認します。

```
aws cloudformation describe-stacks ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--query Stacks[0].Parameters
```

"ParameterKey"が"DriveCount"である項目の"ParameterValue"の値を確認します。

3. 「構成ファイルをエクスポートする《Cloud for AWS》」を参照し、VSP One SDS Block からドライブ増設用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、exportFileType パラメーターに"AddDrives"を指定してください。

また、numberOfDrives パラメーターには、既存のドライブ数と増設するドライブ数をあわせた合計値を指定してください。

最新状態の構成ファイルを使用するために、ドライブ増設用の構成ファイルは必ず取得してください。



注意 構成ファイルのエクスポートで取得した構成ファイルは編集しないでください。編集するとドライブ増設に失敗することがあります。設定値を間違えたときは、正しい値を設定して構成ファイルのエクスポートを再度実行してください。

4. 構成ファイルのエクスポートで取得した構成ファイル一式を手順 3 で templateS3Url パラメーターで指定した Amazon S3 バケットに格納します。

Amazon S3 にファイルを格納する方法として、例えば AWS CLI を用いて Amazon S3 にファイルをコピーする方法があります。詳細は Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「Amazon S3 の操作例」を参照してください。



注意

VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。

5. 次の AWS CLI を実行して変更セットを作成します。

```
aws cloudformation create-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <任意の変更セット名*> ¥
--template-url ¥
<Amazon S3 に格納した VMConfigurationFile.yml の URL(https)> ¥
--include-nested-stacks ¥
--capabilities CAPABILITY_NAMED_IAM
```

*使用可能文字などは以下の Web サイトを参照してください。

<https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-change-set.html>

6. 次の AWS CLI を実行して変更セットを表示します(1 階層目)。

```
aws cloudformation describe-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 5 で指定した変更セット名>
```

以下の事項を確認します。

- "Status"が"CREATE_COMPLETE"であること
"Status"が"CREATE_IN_PROGRESS"の場合はしばらく待ってから再度実行してください。
- "Changes"の項目数が 1 個であること
- "Changes"内の"ResourceChange"について
 - "Action"が"Modify"であること
 - "LogicalResourceId"が以下の値であること
 - HPEC 4D+2P の場合 : "StorageCluster4D2P"であること
 - Mirroring Duplication の場合 : "StorageClusterDuplication"であること
 - 次の手順のため、"ChangeSetId"の値を記録します。

7. 次の AWS CLI を実行して変更セットを表示します(2 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 6 で記録した"ChangeSetId">
```

以下の事項を確認します。

- "Changes"の項目数が 1 つであること
- "ResourceChange"の項目数がストレージノードのノード数*だけあること
* Multi-AZ 構成の場合、タイブレーカーノードは容量を持たない(ドライブが存在しない)ため、ストレージノード数の対象には含みません。
- 次の手順のため、各項目の"ChangeSetId"の値を記録します。

8. 次の AWS CLI を実行して各ストレージノードのスタックの変更セットを表示します(3 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 7 で記録した "ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
 - "Action"が"Add"である項目の"LogicalResourceId"が"VolumeAttachmentXX"、または"UserDataDiskXX"であること(XX は作成されるドライブ番号)
 - 他の項目の"Action"がすべて"Modify"であること("Remove"がないこと)
9. 次の AWS CLI を実行して、作成した変更セットを実行します。

```
aws cloudformation execute-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 5 で指定した変更セット名>
```

10. 次の AWS CLI を実行して、変更セットの実行結果を確認します。

wait stack-update-complete を実行すると、変更セットの実行が完了するまで待つことができます。

```
aws cloudformation wait stack-update-complete ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

実行が完了したら、describe-stacks を実行して、StackStatus が"UPDATE_COMPLETE"であることを確認してください。

```
aws cloudformation describe-stacks ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

11. ドライブの一覧を取得して、増設対象のストレージノードでドライブが増設されたことを確認します。

各ストレージノードの ID をクエリーパラメーターで指定して、コマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

増設したドライブが確認できるまでには、1 分程度の時間を要することがあります。増設したドライブが確認できなかった場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ドライブが認識されない場合の対処」に従って対処してください。

9.4 ドライブを作成する<<Cloud for Google Cloud>>

この節での記述内容は Cloud モデル for Google Cloud に適用されます。



注意

次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。

- ストレージノードの増設
- ストレージノードの交換
- 構成ファイルのエクスポート
- ドライブの減設
- ドライブの増設
- ドライブの交換

ドライブの増設では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作して行います。

前提条件

- 実行に必要なロール : Security、Storage、Monitor、Service、または Resource

操作手順の留意事項

- Terraform は実行可能な環境から実行してください。
- script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておく、結果の確認やエラー発生時の対応に有効です。

操作手順

1. コントローラーノードにログインします。
2. 「構成ファイルをエクスポートする<<Cloud for Google Cloud>>」を参照し、VSP One SDS Block からドライブ増設用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、`exportFileType` パラメーターに "AddDrives" を指定してください。

また、`numberOfDrives` パラメーターには、既存のドライブ数と増設するドライブ数をあわせた合計値を指定してください。

最新状態の構成ファイルを使用するために、ドライブ増設用の構成ファイルは必ず取得してください。



注意

構成ファイルのエクスポートで取得した構成ファイルは編集しないでください。編集するとドライブ増設に失敗することがあります。設定値を間違えたときは、正しい値を設定して構成ファイルのエクスポートを再度実行してください。

3. 「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する<<Cloud for Google Cloud>>」を参照し、ドライブ作成用の構成ファイルを配置します。

4. ドライブ増設用の構成ファイルを使用して、ドライブ作成を行います。

作成するドライブ数に誤りがないかを確認するため、以下のコマンドを実行します。

```
terraform plan
```

5. `terraform plan` での確認に問題がなければ、実際のドライブ作成を行うため以下のコマンドを実行します。

```
terraform apply
```

コマンドの実行後、[Enter a value:]と表示されたら[yes]を入力します。

6. ドライブの一覧を取得して、増設対象のストレージノードでドライブが増設されたことを確認します。

各ストレージノードの ID をクエリーパラメーターで指定して、コマンドを実行します。

REST API : GET /v1/objects/drives

CLI : `drive_list`

増設したドライブが確認できるまでには、1 分程度の時間を要することがあります。増設したドライブが確認できなかった場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ドライブが認識されない場合の対処」に従って対処してください。

9.5 ドライブを作成する《Cloud for Microsoft Azure》

この節での記述内容は Cloud モデル for Microsoft Azure に適用されます。



注意

次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。

- ストレージノードの増設
- ストレージノードの交換
- 構成ファイルのエクスポート
- ドライブの減設
- ドライブの増設
- ドライブの交換

ドライブの増設では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作して行います。

前提条件

- 実行に必要なロール：Security、Storage、Monitor、Service、または Resource

操作手順の留意事項

- 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。
- script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておくと、結果の確認やエラー発生時の対応に有効です。

操作手順

1. コントローラーノードにログインします。
2. Azure CLI または Azure ポータルから現在のストレージノード 1 台当たりのドライブの数を確認します。
3. 「構成ファイルをエクスポートする《Cloud for Microsoft Azure》」を参照し、VSP One SDS Block からドライブ増設用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、`exportFileType` パラメーターに "AddDrives" を指定してください。

また、`numberOfDrives` パラメーターには、既存のドライブ数と増設するドライブ数をあわせた合計値を指定してください。

最新状態の構成ファイルを使用するために、ドライブ増設用の構成ファイルは必ず取得してください。



注意

パラメーターで指定する値を間違えた場合は、正しい値を指定して構成ファイルのエクスポートを再度実行し、最新の構成ファイルを取得しなおしてください。

4. エクスポートした `ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` を解凍します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、ジョブが失敗するおそれがあります。

5. ドライブ増設用の構成ファイルを使用して、次のコマンドを実行します。

```
az deployment group create ¥
--name mainTemplate ¥
--resource-group <ストレージクラスター用リソースグループ名> ¥
--template-file VMConfigurationFile.json ¥
--parameters VMConfigurationFile.parameters.json
```

6. 実行結果を確認します。

Azure CLI がエラーになっていないこと、または Azure ポータルでストレージクラスター用リソースグループの画面へ移動し、デプロイが成功していることを確認してください。

7. ドライブの一覧を取得して、増設対象のストレージノードでドライブが増設されたことを確認します。

各ストレージノードの ID をクエリーパラメーターで指定して、コマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

増設したドライブが確認できるまでには、1 分程度の時間を要することがあります。増設したドライブが確認できなかった場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ドライブが認識されない場合の対処」に従って対処してください。

9.6 ストレージプールを拡張する

ストレージプールを拡張します。



注意

- ストレージプールの拡張を実行すると、内部処理によってストレージノードの CPU の使用率が上昇して、一時的にホスト I/O の性能が低下することがあります。
- 格納データ暗号化を利用する場合は、「格納データ暗号化の概要」の暗号化環境の設定を有効にする手順およびストレージプールの暗号化の設定を有効にする手順を実施していることを確認してください。ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」に従ってセットアップが完了していれば、暗号化環境の設定を有効にする手順およびストレージプールの暗号化の設定を有効にする手順を実施しています。本手順を実施後に、暗号化環境の設定およびストレージプールの暗号化の設定を変更することはできません。



メモ

≪Cloud≫Multi-AZ (Multi-Zone)構成の場合、タイブレーカーノードにはドライブが存在しないため、手順 6 での確認対象にタイブレーカーノードを含める必要はありません。

前提条件

- 実行に必要なロール : Storage

操作手順

1. 拡張前のストレージプールの論理容量、ストレージプールの空き容量、ストレージプールの ID を確認します。

CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

2. ドライブの一覧を取得して、ストレージプールに追加するドライブの ID を確認します。

REST API : GET /v1/objects/drives

CLI : drive_list



ヒント

ストレージプールに組み込まれていないドライブは、status が"Offline"のドライブです。ドライブの status はドライブ情報から取得できます。

3. ストレージプールのリビルド領域ポリシーと許容されるドライブ障害数を変更する場合は「ストレージプールの設定を編集する」を参照し、操作を行ってください。



注意

- ストレージプールの設定を編集するにはユーザーデータの冗長度が低下していないことが必要です。ユーザーデータの冗長度が低下している場合は、回復操作を実施したあとにストレージプールの設定の編集をしてください。
- ストレージプールを拡張してからリビルド領域ポリシーを変更しても、リビルド領域を十分確保できない可能性があります。そのため、リビルド領域ポリシーを変更する場合は、ストレージプールを拡張する前に変更してください。
- <<Cloud for AWS>> ベースライセンスとして Floating を適用している場合、以下に注意してください。
 - 許容されるドライブの障害数の変更によって AWS License Manager のライセンスの契約容量を超過する場合があります。以降の手順を実施する前に「ライセンスの使用量を確認するためにストレージプールの容量を試算する<<Cloud>>」を参照して、許容されるドライブの障害数の変更後のストレージプールの容量を計算し、ストレージプールの論理容量が AWS License Manager のライセンスの契約容量に収まるかを確認してください。
なお、必要なライセンスの契約容量は、ストレージプールの論理容量を TiB 単位に切り上げて計算してください。
複数のストレージクラスターで AWS License Manager のライセンスを共有している場合は、ストレージクラスターそれぞれのストレージプールの論理容量を先に TiB 単位に切り上げてから、それらを合計した値が、AWS License Manager のライセンスの契約容量に収まるかを確認してください。
(例) 2 つのストレージクラスターがあって、それぞれのストレージプールの論理容量が 31.3[TiB]と 47.7[TiB]の場合、それぞれの値を整数値に切り上げて 32[TiB]と 48[TiB]としてから、それらを合計して 80[TiB]と計算します。
契約容量が不足する場合、AWS Marketplace 上でライセンスの契約を更新してください。
 - リビルド領域ポリシーは"Fixed"から変更できません。

4. ストレージプールを拡張します。

ストレージプールの ID とストレージプールに追加するすべてのドライブの ID を指定してコマンドを実行します。

CLI を使う場合はストレージプールの ID の代わりに名前が指定できます。

REST API : POST /v1/objects/pools/<id >/actions/expand/invoke

CLI : pool_expand

コマンド実行後に表示されるジョブの ID を確認します。



注意

他の操作を行う場合は、ストレージプールの拡張後、手順 6 に記載の確認操作が終わってからにしてください。

5. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



メモ

ドライブを増設したストレージノード上のストレージコントローラーの容量不足が原因で、`rebuildStatus` が "Error" になっていた場合、次に実行されるストレージコントローラーへの容量割り付け処理の前にリビルド処理が実施されます。このリビルド処理の結果、新たにストレージコントローラーへ割り当てる容量がなくなった場合、ストレージコントローラーへの容量割り付け処理は実施されません。また、ストレージプールのリビルド領域が不足しており、追加したドライブ容量がリビルド領域として補充された場合もストレージコントローラーへの容量割り付け処理は実施されません。この結果として、ストレージプールの容量も増加されないため、手順 6 のイベントログも出力されず、ストレージプールの論理容量とストレージプールの空き容量も本手順実施前と変わりません。ただし、ストレージプールのリビルド領域ポリシーが "Variable" の場合は、ストレージコントローラーの容量割り付け処理が実施されなくても、ストレージプールの論理容量と空き容量が増える場合があります。

続けて、内部処理であるストレージコントローラーへの容量割り付け処理が実行されます。これら処理の終了によって、追加した容量が使用できるようになります。

ストレージコントローラーへの容量割り付けの処理時間は、このマニュアルの「ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安)」を参照してください。

6. イベントログを取得して、手順 4 で指定したドライブがストレージプールの容量として使用できるようになったことを確認します。

REST API : `GET /v1/objects/event-logs`

CLI : `event_log_list`

イベントログ `KARS16022-I` または `KARS16081-I` が、既存のストレージノードの数だけ出力されるまでお待ちください。それまでは、他の操作が実施できないことがあります。

イベントログ `KARS16022-I` または `KARS16081-I` が、既存のストレージノードの数だけ出力されたら、指定どおりにストレージプールが拡張できています。

ただし、イベントログ `KARS16022-I` または `KARS16081-I` が、既存のストレージノードの数だけ出力されるまでの間に、ストレージノードに障害が発生していた場合、ストレージプールの拡張ができていない場合がありますので、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対応してください。

また、イベントログ `KARS16046-I` が出力された場合は、指定されたドライブの容量またはドライブの数が不足しているため、ユーザーが利用可能な容量である論理容量の拡張ができていません。論理容量を拡張するためには「増設時の容量設計」を参照して必要な容量を算出し、「ドライブを増設する」に従ってストレージプールを拡張してください。



注意

キャッシュ保護付きライトバックモードの状態が有効だった場合、論理容量を構成するためには各ストレージノードで 3 台以上のドライブに対してストレージプール拡張を実行する必要があります。また、キャッシュ保護付きライトバックモードの状態を無効から有効に変更する場合は、変更する前に各ストレージノードで 3 台以上のドライブに対してストレージプール拡張を実行しておく必要があります。詳細は「キャッシュ保護付きライトバックモードの有効化」を参照してください。

7. 拡張後のストレージプールの情報を取得します。

REST API : `GET /v1/objects/pools`

CLI : `pool_list`

拡張前に比べて拡張後のストレージプールの論理容量とストレージプールの空き容量が拡張されたことを確認します。

8. ストレージコントローラーの管理下にあるユーザーデータの移動を確認します。

ストレージプールの拡張後、ユーザーデータの量が均等になるよう、ユーザーデータの移動が自動的に動作します。

データ移動が開始すると、データ移動の実施状況(dataRebalanceStatus)が、しばらく"Running"となったあと、最終的に"Stopped"に変わることを確認してください。

データ移動の実施状況(dataRebalanceStatus)と進捗率[%](dataRebalanceProgressRate)は、以下のコマンドで確認できます。

すべてのストレージコントローラーについて確認してください。

REST API : GET /v1/objects/storage-controllers

CLI : storage_controller_list

この手順での確認を待たずに、以降の手順を実施することができます。



メモ

- 進捗率[%](dataRebalanceProgressRate)は、ストレージコントローラー管理下の全ボリューム数に対する、データ移動の完了したボリューム数の割合を示します。ボリュームの容量によっては進捗率の更新に時間が掛かる場合があります。
また、データ移動に掛かる時間(目安)は、次の計算式から見積もることができます。
(当該ストレージコントローラーで管理しているストレージプールの使用容量^{*1} × 増設前総論理容量^{*2} ÷ 増設後総論理容量^{*3}) ÷ 42[MiB] × 2[sec]
^{*1}の値は「ストレージコントローラーを管理する」に記載されている次の値になります。
usedCapacity[MiB] : 当該ストレージコントローラーで管理しているストレージプールの使用容量[MiB]
«Bare metal»^{*2}、^{*3}の値は「ドライブ増設時の容量設計(HPEC 4D+1P の場合)«Bare metal»」、「ドライブ増設時の容量設計(HPEC 4D+2P の場合)」、「ドライブ増設時の容量設計(Mirroring の場合)」に記載のドライブ増設時の増設後総論理容量の算出方法を参照し算出してください。
«Cloud»^{*2}、^{*3}の値は「ドライブ増設時の容量設計(HPEC 4D+2P の場合)」、「ドライブ増設時の容量設計(Mirroring の場合)」に記載のドライブ増設時の増設後総論理容量の算出方法を参照し算出してください。
実際には、ストレージプール使用状況によって、必要な時間は増減します。
- データの移動中に、下記のイベントが発生した場合は、データ移動の実施状況(dataRebalanceStatus)が、"Waiting"になることがあります。
 - ストレージプールの拡張が実施された場合
 - ボリュームを削除した場合
 - ストレージコントローラーが管理するストレージプールの容量が枯渇した場合データ移動の実施状況(dataRebalanceStatus)が"Waiting"になった場合、データ移動の待ち要因が解消されるまでデータの移動は抑止され、進捗率[%](dataRebalanceProgressRate)はnullになります。待ち要因が解消されたタイミングで、データ移動は再開されます。また、進捗率[%](dataRebalanceProgressRate)は再計算されて、0 から再表示されます。

9. «Bare metal»構成情報のバックアップを行います。

「構成情報をバックアップする«Bare metal»«Cloud for AWS»」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

10. «Cloud for AWS»構成情報のバックアップを行います。

「構成情報をバックアップする«Bare metal»«Cloud for AWS»」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

ストレージノードを管理する

- 10.1 ストレージノード管理の概要
- 10.2 ストレージノード情報の取得

10.1 ストレージノード管理の概要

ストレージノードの情報取得や構成変更など、以下の操作を行います。

項目	説明
ストレージノード情報の取得	ストレージノードのロール・属性・状態など各種情報を取得できます。ストレージノード情報は一覧取得する方法とストレージノードの ID を指定して取得することができます。
ストレージノードの増設	ストレージプールの容量拡張のためなどに行うストレージノードを増設する操作です。「ストレージノード増設の準備と手順」を参照してください。
ストレージノードの減設	ドライブ容量の縮退や、障害が発生しているストレージノードの切り離しを行う場合には、ストレージノードの減設が必要になります。「ストレージノード減設の条件と手順」を参照してください。
ストレージノードの保守	ストレージノードの保守回復・保守閉塞・交換を行う操作です。「ストレージノードを保守する」を参照してください。
ストレージノードの自動回復機能	ストレージノードの自動回復機能の設定が行えます。「ストレージノードの自動回復機能の設定」を参照してください。

10.2 ストレージノード情報の取得

ストレージノードの情報が一覧または個別に取得できます。

10.2.1 取得できるストレージノード情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- ・ id : ストレージノードの ID(uuid)
- ・ biosUuid : ストレージノードの UUID
- ・ protectionDomainId : 所属するプロテクションドメインの ID(uuid)
- ・ faultDomainId : 所属するフォールトドメインの ID(uuid)
- ・ faultDomainName : 所属するフォールトドメインの名前
- ・ name : ストレージノードの名前
- ・ clusterRole : ストレージクラスターにおけるストレージノードのロール
- ・ storageNodeAttributes : ストレージノードの属性
- ・ statusSummary : ストレージノードの状態のサマリー
- ・ status : ストレージノードの状態
- ・ driveDataRelocationStatus : ドライブデータ再配置の状態
- ・ controlPortIpv4Address : 管理ポートの IP アドレス(IPv4)
- ・ internodePortIpv4Address : ストレージノード間ポートの IP アドレス(IPv4)
- ・ softwareVersion : ストレージソフトウェアのバージョン
- ・ modelName : ストレージノードが動作しているサーバーのモデル名

- serialNumber : ストレージノードが動作しているサーバーのシリアルナンバー
- memory : 物理サーバーに搭載されているメモリー容量[MiB]
- insufficientResourcesForRebuildCapacity : リビルド領域の不足リソース
 - capacityOfDrive : リビルド領域の不足ドライブ容量[GB]
 - numberOfDrives : リビルド領域の不足ドライブ数
- rebuildableResources : リビルド可能リソース
 - numberOfDrives : リビルド可能なドライブ数
- availabilityZoneId : null
- physicalZone : null
- logicalZone : null

10.2.2 取得できるストレージノード情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : ストレージノードの ID(uuid)
- biosUuid : ストレージノードの UUID
- protectionDomainId : 所属するプロテクションドメインの ID(uuid)
- faultDomainId : 所属するフォールトドメインの ID(uuid)
- faultDomainName : 所属するフォールトドメインの名前
- name : ストレージノードの名前
- clusterRole : ストレージクラスターにおけるストレージノードのロール
- storageNodeAttributes : ストレージノードの属性
- statusSummary : ストレージノードの状態のサマリー
- status : ストレージノードの状態
- driveDataRelocationStatus : ドライブデータ再配置の状態
- controlPortIpv4Address : 管理ポートの IP アドレス(IPv4)
- internodePortIpv4Address : ストレージノード間ポートの IP アドレス(IPv4)
- softwareVersion : ストレージソフトウェアのバージョン
- modelName : ストレージノードが動作している VM インスタンスのモデル名
- serialNumber : ストレージノードが動作している VM インスタンスの ID
- memory : VM インスタンスのメモリー容量[MiB]
- insufficientResourcesForRebuildCapacity : リビルド領域の不足リソース
 - capacityOfDrive : リビルド領域の不足ドライブ容量[GB]
 - numberOfDrives : リビルド領域の不足ドライブ数
- rebuildableResources : リビルド可能リソース
 - numberOfDrives : リビルド可能なドライブ数
- availabilityZoneId :

≪Cloud for AWS≫Multi-AZ 構成の場合、フォールトドメインに対応するアベイラビリティゾーンの ID。physicalZone と同じ値のため、基本的には physicalZone を参照してください。
Single-AZ 構成の場合は null
≪Cloud for Google Cloud≫null
≪Cloud for Microsoft Azure≫null

- physicalZone :
≪Cloud for AWS≫Multi-AZ 構成の場合、フォールトドメインに対応するアベイラビリティゾーンの ID。availabilityZoneId と同じ値。Single-AZ 構成の場合は null
≪Cloud for Google Cloud≫Multi-AZ (Multi-Zone)構成の場合、フォールトドメインに対応するゾーンの ID。Single-AZ (Single-Zone)構成の場合は null
≪Cloud for Microsoft Azure≫フォールトドメインに対応する物理ゾーンの ID
- logicalZone :
≪Cloud for AWS≫null
≪Cloud for Google Cloud≫null
≪Cloud for Microsoft Azure≫フォールトドメインに対応する論理ゾーンの ID

10.2.3 ストレージノード情報の一覧を取得する

各ストレージノードの情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. ストレージノード情報の一覧を取得します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list

10.2.4 ストレージノード情報を個別に取得する

指定した ID のストレージノードの情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. ストレージノードの ID を確認します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
2. ストレージノードの情報を取得します。
ストレージノードの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/storage-nodes/<id>
CLI : storage_node_show

ストレージノード増設の準備と手順

- 11.1 ストレージノードの増設<<Bare metal>>
- 11.2 ストレージノードの増設<<Cloud for AWS>>
- 11.3 ストレージノードの増設<<Cloud for Google Cloud>>
- 11.4 ストレージノードの増設<<Cloud for Microsoft Azure>>

11.1 ストレージノードの増設<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ストレージノードの増設は以下の目的のために実施します。

- ストレージプール容量の拡張
- コンピュートポート数の拡張
- システム性能の向上

増設するストレージノードに搭載されたすべてのドライブを対象に、ストレージノードの増設ジョブの延長でストレージプール拡張が実施されます。

増設するストレージノードのドライブ容量は増設前の構成のストレージノードと均一である必要があります。「増設時の容量設計」を参照して必要な容量・ドライブを搭載してください。

増設するストレージノードは「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載してあるハードウェアから選択してください。



注意

- 本マニュアルが対象としているストレージソフトウェアのバージョンでは、以下の条件におけるストレージノード減設をサポートしていません。増設したストレージノードを、その後減設する可能性がある場合は、以下の条件を事前に確認した上でストレージノード増設を実施してください。
 - フォールトドメインが複数で構成されている場合
ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。
 - Universal Replicator 機能を使用している場合
Universal Replicator 機能を使用中にストレージノードを減設する場合は「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」の「Universal Replicator 使用時にストレージノードを減設する<<Bare metal>>」を参照してください。
- ストレージプール拡張の延長で実施される容量バランスやドライブデータ再配置によって、既存ボリュームの I/O 性能に影響が出る場合があります。
加えて、容量バランスおよびドライブデータ再配置の完了後から「増設したストレージノードの設定を行う<<Bare metal>>」に記載の手順を実施するまでの間、既存ボリュームの I/O 性能に影響が出る場合があります。
また、ストレージノード増設時には、ストレージコントローラーの再配置が動作するため、ホスト I/O 性能が 3～4 分ほど低下することがあります。
- VSP One SDS Block の運用管理において、REST API/CLI/VSP One SDS Block Administrator での操作の接続先として、DNS を用意し FQDN を指定する方法で運用している場合、増設するストレージノードの管理ポートの IP アドレスまたは IP アドレスを正引きできる FQDN を割り当て、DNS サーバーに正引きの定義を追加してください。
- 増設するストレージノードと安全な SSL/TLS 通信を行うために、増設するストレージノードの管理ポートの情報を Subject Alternative Name(SAN)に追加したサーバー証明書を作成してください。サーバー証明書の作成手順は「運用管理を SSL/TLS 通信で行う」を参照してください。



メモ

既存のストレージノードに対してストレージプール拡張が実施されておらず、ストレージプールが空の場合は、ストレージノードの増設ジョブの延長でのストレージプール拡張は実施されません。ストレージプール拡張を実施する場合は「空状態にあるストレージプールを拡張する<<Bare metal>>」を参照してください。

ストレージノード増設の操作手順の実施順と参照先を以下に示します。

操作手順の実施順と参照先	備考
1. 「 11.1.1 増設用ストレージノードを準備する<<Bare metal>> 」 2. 「 11.1.2 システム要件ファイルを更新する<<Bare metal>> 」 3. 「 11.1.3 構成ファイルを編集する<<Bare metal>> 」 4. 「 11.1.4 ストレージノードを増設する<<Bare metal>> 」 5. 「 11.1.5 追加した論理容量が使用できることを確認する<<Bare metal>> 」 6. 「 11.1.6 増設したストレージノードの設定を行う<<Bare metal>> 」	1 : 物理サーバー/コントローラーノード操作 2～6 : コントローラーノード操作

ストレージノード増設時の留意事項

■フォールトドメインが 1 つの場合

- 1 つのストレージノードを増設する場合は、上記の表で示した増設手順を一とおり実施してください。
- 複数のストレージノードを増設する場合は、次の手順に従って増設前にドライブデータ再配置の自動開始を抑止しておくことで、増設後のドライブデータ再配置とストレージコントローラーへの容量割り付け処理を一度にまとめることができます。ドライブデータ再配置の自動開始を抑止する方法は「ドライブデータ再配置を中断する<<Bare metal>>」を参照してください。
 - 「[11.1.3 構成ファイルを編集する<<Bare metal>>](#)」を行う前に「[14.5 ドライブデータ再配置を中断する<<Bare metal>>](#)」を実施する。
 - 増設するストレージノードについて、1 つずつ「[11.1.3 構成ファイルを編集する<<Bare metal>>](#)」と「[11.1.4 ストレージノードを増設する<<Bare metal>>](#)」の手順を繰り返し、複数のストレージノードを増設する。
 - 「[14.6 ドライブデータ再配置を再開する<<Bare metal>>](#)」を実施したあと、「[11.1.5 追加した論理容量が使用できることを確認する<<Bare metal>>](#)」から手順を継続する。

■フォールトドメインが複数の場合

フォールトドメインが複数で構成されている場合、ストレージノードを増設するときは、以下に注意してください。

- 各フォールトドメインに同数のストレージノードを割り当て、それらのストレージノードを同時に増設する必要があります。

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	同時に増設するストレージノード数
4D+2P	3	6
Duplication	3	3

- ドライブデータ再配置は実行されません。

11.1.1 増設用ストレージノードを準備する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

増設用ストレージノードのネットワークの物理結線と LAN スイッチの設定を完了させてから、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の以下に記載されている構築準備を行います。

- ・ 「ストレージノードを準備する」



注意

増設するストレージノードのメモリーは、プロテクションドメインに属するストレージノード内で最小のメモリー容量以上であることが必要です。プロテクションドメイン情報から `minimumMemorySize[MiB]` を参照し、増設するストレージノードに必要なメモリー容量の値を確認してください。



メモ 増設するストレージノードの PCI スロット位置が、ストレージクラスター内で動作しているストレージノードの PCI スロットの位置と違っていてもストレージノードの増設はできます。

11.1.2 システム要件ファイルを更新する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

認定済みハードウェア、システム要件が記載された最新のシステム要件ファイルを VSP One SDS Block にインポートします。

サポート対象外のサーバーハードウェアを使用した場合は、ストレージノード増設に失敗します。

前提条件

- ・ 実行に必要なロール : Service

操作手順

1. 最新のシステム要件ファイル(SystemRequirementsFile.yml)をサポートセンターから入手して、コントローラーノードに格納します。



注意

システム要件ファイルの名称は、SystemRequirementsFile.yml から変更しないでください。



メモ

ストレージクラスターに登録されているシステム要件ファイルのバージョンは、以下のコマンドで確認できます。

REST API : GET /v1/objects/storage

CLI : storage_show

最新のシステム要件ファイルのバージョンについては、サポートセンターから情報を入手してください。

2. システム要件ファイルを指定して以下のコマンドを実行します。
クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : POST /v1/objects/system-requirements-file/actions/import/invoke

CLI : system_requirements_file_import

指定したシステム要件ファイルのバージョンが、VSP One SDS Block にインポート済みのバージョンより新しい場合のみインポート処理が行われます。指定したシステム要件ファイルのバージョンが同じか古い場合は、イベントログを出力しインポート処理をスキップします。

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

11.1.3 構成ファイルを編集する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

VSSB 構成ファイル(SystemConfigurationFile.csv)を編集します。

構成ファイルのエクスポートは、コントローラーノード上から操作して行います。



注意

- ・ フォールトドメインが 1 つの場合、複数のストレージノードを増設するには、次の手順に従って増設前にドライブデータ再配置を抑止しておくことで、増設後のドライブデータ再配置とストレージコントローラーへの容量割り付け処理を一度にまとめることができます。
 1. 「構成ファイルを編集する<<Bare metal>>」を行う前に「ドライブデータ再配置を中断する<<Bare metal>>」を実施する。
 2. 増設するストレージノードについて、1 つずつ「構成ファイルを編集する<<Bare metal>>」と「ストレージノードを増設する<<Bare metal>>」の手順を繰り返し、複数のストレージノードを増設する。
 3. 「ドライブデータ再配置を再開する<<Bare metal>>」を実施したあと、「追加した論理容量が使用できることを確認する<<Bare metal>>」から手順を継続する。
- ・ フォールトドメインが複数の場合、複数かつ各フォールトドメインに同数のストレージノードを、同時に増設する必要があります。

構成ファイルに増設する複数のストレージノードについて追記し、増設手順を一とおり実施することで一度に複数のストレージノードが増設できます。

ただし、増設台数は、ユーザーデータの保護種別(redundantType)とフォールトドメイン数によって決まります。「ストレージノードの増設<<Bare metal>>」の「ストレージノード増設時の留意事項」の「フォールトドメインが複数の場合」を参照してください。
- ・ FC 接続から、iSCSI 接続または NVMe/TCP 接続への構成変更はできません。また、iSCSI 接続または NVMe/TCP 接続から、FC 接続への構成変更もできません。

前提条件

- ・ 実行に必要なロール : Service

操作手順

1. 「構成ファイルをエクスポートする<<Bare metal>>」を参照し、VSP One SDS Block から構成ファイルを取得します。

最新状態の構成ファイルを使用するために、必ず取得してください。
2. 取得した VSSB 構成ファイルをテキストエディターで開き、増設するストレージノードの情報を追加します。既存の情報は削除・変更せず、既存の情報の後ろに追加します。

クラスターマスターノードの増設はできません。そのため、増設するストレージノードに対して ClusterMasterRole の指定はできません。ClusterMasterRole に、"clustermaster"を指定した場合は、ストレージノード増設がエラーになるか、増設対象のストレージノードが強制的にクラスターワーカーノードになります。



注意

VSSB 構成ファイルの名称は、SystemConfigurationFile.csv から変更しないでください。

11.1.4 ストレージノードを増設する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージノードの増設は、コントローラーノード上から操作して行います。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - VSP One SDS Block の構成情報の変更・設定
 - 構成ファイルのエクスポート
- 増設対象のストレージノードが追加されるプロテクションドメインの、`storageControllerClusteringPolicy` が `"TwoRedundantStorageNodes"` の場合、ストレージクラスター内に閉塞*しているストレージノードが存在していると、ストレージノードは増設できません。また、`storageControllerClusteringPolicy` が `"TwoRedundantStorageNodes"` ではない場合でも、閉塞*しているストレージノードが存在していると、ストレージノードの増設に失敗することがあります。先に閉塞*しているストレージノードを回復させてからストレージノードを増設してください。
* ストレージノードが閉塞している場合、`status` が以下のいずれかになります。
`"TemporaryBlockage"`、`"MaintenanceBlockage"`、`"PersistentBlockage"`、`"InstallationFailed"`、`"RemovalFailedAndTemporaryBlockage"`、`"RemovalFailedAndMaintenanceBlockage"`、`"RemovalFailedAndPersistentBlockage"`
- 「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の指示に従って、この項に記載されている手順を再度実施する際に、「ストレージソフトウェアのインストール」と「ストレージノード単位のセットアップ」の実施は不要と指示されている場合があります。その場合は、この項に記載されている増設対象のストレージノードに対する「ストレージソフトウェアのインストール」と「ストレージノード単位のセットアップ」の手順を省略してください。
- 増設するストレージノードのメモリーは、プロテクションドメインに属するストレージノード内で最小のメモリー容量以上であることが必要です。プロテクションドメイン情報から `minimumMemorySize[MiB]` を参照し、増設するストレージノードに必要なメモリー容量の値を確認してください。
- ストレージノードの増設中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの増設が完了するのを待ってから再度これらの操作を実施してください。

処理時間の目安

- 手順 4 で実行するストレージノードの増設ジョブの処理時間の目安は以下のとおりです。

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	同時に増設するストレージノード数	各ストレージノードのメモリー容量 [GiB]	処理時間の目安 [min]
4D+1P	1	1	256	35
4D+2P	1	1		50
	3	6		65
Duplication	1	1		35
	3	3		40

- 処理時間の目安について、以下の外部要因によって、手順 4 で実行するストレージノードの増設ジョブの処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。
 - ネットワークの通信状況(ストレージノード間の通信状況)

- 。 サーバーの性能状況(ストレージノードの温度上昇による性能低下など)
- 。 サーバーのハードウェア構成(ストレージノードのプロセッサ、メモリ容量など)
- 。 ストレージノードの起動時間(物理サーバーの起動に時間が掛かる場合など)

前提条件

- ・ 実行に必要なロール : Service

操作手順

1. 「増設用ストレージノードを準備する<<Bare metal>>」の手順で準備した増設対象のストレージノードに対して、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」に記載されている以下の手順を行い、ストレージソフトウェアのインストールを行います。

- ・ 「ストレージソフトウェアをインストールする」



注意

「ストレージソフトウェアをインストールする」の手順で使用するストレージソフトウェアインストーラー(hsds-installer-vssb-<version>-<number>.iso)のバージョンは、ストレージクラスターのバージョンと合わせる必要があります。ストレージクラスターのバージョンは以下で確認できます。

REST API : GET /v1/objects/storage

CLI : storage_show

2. 増設対象のストレージノードに対して、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の以下の手順を行い、ストレージノード単位のセットアップを行います。

- ・ 「ストレージノード単位のセットアップを行う」

3. 増設開始前のストレージプールの論理容量、ストレージプールの空き容量を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

4. ストレージノードを増設します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : POST /v1/objects/storage-nodes

CLI : storage_node_add

上記コマンド実行時に以下の情報をパラメーターとして指定する必要があります。

- ・ 「構成ファイルを編集する<<Bare metal>>」で編集した VSSB 構成ファイル (SystemConfigurationFile.csv)
- ・ 「ストレージノード単位のセットアップを行う」の手順内で設定したセットアップユーザーのパスワード

コマンド実行後に表示されるジョブの ID を確認します。



メモ

- ・ ストレージノードの増設ジョブの実行中は、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノード単位のセットアップを行う」に示す手順は実施できません。
- ・ この操作を実施した際に、以下のイベントログが出力されることがあります。これは、正常な動作のため、そのまま手順を継続してください。

- KARS20067-I
- KARS20068-I
- KARS20069-I
- Universal Replicator 機能使用時には、イベントログ KARS03208-W または KARS03209-W が出力されることがあります。
イベントログ KARS03208-W または KARS03209-W が出力された場合は、イベントログ記載の solution に従って「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」の「Universal Replicator 使用時にストレージノードを増設する」を参照し、対処してください。

5. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

増設が完了するまでは、他の操作が実施できないことがあります。他の操作が失敗した場合は、他の操作のエラーメッセージやイベントログに従って対処してください。



注意

ジョブの処理中に、KARS10914-W または KARS10915-W のイベントログが出力された場合は、チーミング構成が組まれている管理ポートまたはストレージノード間ポートのネットワーク上に一部が接続できないパスが存在している可能性があります。チーミング構成が組まれている場合は、そのままの状態でもストレージクラスターとしての稼働は可能ですが、メッセージに含まれるネットワークパスについて「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「最初にチェックする項目」に記載されているネットワークの接続および設定に関する項目を確認し、問題があれば対処することをお勧めします。
また、問題の対処後に管理ポートまたはストレージノード間ポートの接続を VSP One SDS Block 環境で確認する場合は、以下を実施してください。

(KARS10914-W または KARS10915-W のイベントログが出力されたあとに、KARS08304-I、KARS08305-I、KARS08306-I、KARS08313-I、KARS08314-I、KARS08315-I などのリンク状態の回復を示すイベントログが出力された場合でも、到達性は保証できていないため、リンク状態以外の到達性に懸念がある場合は、以下に示す方法などで接続確認を行うことをお勧めします。)

• 接続確認の再実施(ストレージノード交換)

ストレージノード単位での接続確認を再実施するためには、接続確認でエラーになった接続元ポートが存在するストレージノードに対してストレージノード交換を 1 ノードずつ実施してください。ストレージクラスター全体の停止は発生しません。対象のストレージノードが閉塞していない場合はストレージノード交換の前にストレージノード保守閉塞を実施してください。ストレージノード交換については「ストレージノードを交換する<<Bare metal>>」を、ストレージノード保守閉塞については「ストレージノードを保守閉塞する<<Bare metal>>」を参照してください。

ストレージノード交換が正常終了して、かつ KARS10914-W または KARS10915-W のイベントログが出力されなければ、対象のストレージノードの管理ポートおよびストレージノード間ポートのネットワークの接続状態は問題ありません。



メモ

ストレージクラスターにスペアノードが登録されている場合、ジョブの完了後にイベントログ KARS10733-W が出力されることがあります。これは、以降の手順で実施する「ストレージノードの BMC 情報を登録・編集する<<Bare metal>>」を実施することで解決します。

6. ストレージノードの一覧を取得して、増設したストレージノードの ID が追加されていることを確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

7. ドライブの一覧を取得します。

増設したストレージノードの ID をクエリーパラメーターで指定してコマンドを実行します。
増設したストレージノードが複数存在する場合は、増設したストレージノードの数だけ繰り返し実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

増設したストレージノードに搭載されたドライブがすべてあり、それらのドライブの status がすべて"Normal"であることを確認してください。搭載されたドライブが存在しない場合や status が"Offline"の場合は「ドライブを増設する」を参照し、ドライブの増設とストレージプールの拡張を実施してください。



メモ

既存のストレージノードに対してストレージプール拡張が実施されておらず、ストレージプールが空の場合は、ストレージノードの増設ジョブの延長でのストレージプール拡張は実施されません。ストレージプール拡張を実施する場合は「空状態にあるストレージプールを拡張する<<Bare metal>>」を参照してください。

8. ストレージプールの情報を取得します。

REST API : GET /v1/objects/pools

CLI : pool_list

増設開始前と比べて、ストレージプールの論理容量が拡張され、ストレージプールの空き容量が増加したことを確認してください。ストレージプールの論理容量が拡張されていない場合は、イベントログを取得してください。イベントログ KARS16158-W または KARS16159-W が出力された場合は、増設したストレージノードのドライブの容量が不足しているため、ユーザーが利用可能な容量である論理容量の拡張ができていません。論理容量を拡張するためには「増設時の容量設計」を参照して必要な容量を算出し、「ドライブを増設する」に従ってストレージプールを拡張してください。イベントログ KARS16158-W または KARS16159-W が出力されていない場合は、既存のストレージノードのドライブ容量またはドライブ数が不足しています。「空状態にあるストレージプールを拡張する<<Bare metal>>」に従ってストレージプールを拡張してください。

11.1.5 追加した論理容量が使用できることを確認する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージノードの増設手順が完了しても、追加した論理容量はすぐには使用できません。以下の順で実行される内部処理の完了後、追加した論理容量が使用可能になります。

- ドライブデータ再配置
- ストレージコントローラーへの容量割り付け処理

ドライブデータ再配置の処理時間については「ドライブデータ再配置完了までの時間(目安)<<Bare metal>>」を参照してください。複数のストレージノードを増設した場合、増設したストレージノードの数と同じ回数のドライブデータ再配置が動作します。「ドライブデータ再配置完了までの時間(目安)<<Bare metal>>」で算出できる目安時間は 1 ストレージノード当たりの処理時間になります。



メモ

フォールトドメインが複数の場合、ドライブデータ再配置は実行されません。

ストレージコントローラーへの容量割り付けの処理時間は、このマニュアルの「ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安)」を参照してください。

前提条件

- 実行に必要なロール：Storage

操作手順

1. ドライブデータ再配置の完了を確認します。

「ドライブデータ再配置の状態を確認する<<Bare metal>>」を参照して確認してください。
フォールトドメインが複数で構成されている場合は、ドライブデータ再配置は実行されないため、確認は不要です。

2. ストレージコントローラーへの容量割り付け処理の完了を確認します。

イベントログを取得して、増設したストレージノードのすべてのドライブがストレージプールの容量として使用できるようになったことを確認します。イベントログ KARS16020-I が、増設したストレージノードの数だけ出力されるまでお待ちください。それまでは、他の操作が実施できないことがあります。

REST API：GET /v1/objects/event-logs

CLI：event_log_list

イベントログ KARS16020-I が、増設したストレージノードの数だけ出力されたら、増設したストレージノードのすべてのドライブがストレージプールの容量として追加され、使用できるようになります。

ただし、イベントログ KARS16020-I が、増設したストレージノードの数だけ出力されるまでの間に、ストレージノードに障害が発生していた場合は、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対応してください。

11.1.6 増設したストレージノードの設定を行う<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

増設したストレージノードに対して各種設定を行います。

前提条件

- 実行に必要なロール：Service
- 「追加した論理容量が使用できることを確認する<<Bare metal>>」の手順に従ったストレージプールの容量の確認が済んでいること
ただし、ストレージノードの増設ジョブの延長で、ストレージプール拡張が実施されていない場合は確認不要です。

操作手順

1. 増設したストレージノードの管理ポートの情報を Subject Alternative Name(SAN)に追加したサーバー証明書を、VSP One SDS Block にインポートします。
サーバー証明書のインポート手順は「運用管理を SSL/TLS 通信で行う」を参照してください。
2. ストレージクラスターにスペアノードが登録されている場合は、増設したストレージノードに対して「スペアノードを利用するための BMC アカウントを準備する<<Bare metal>>」と「ストレージノードの BMC 情報を登録・編集する<<Bare metal>>」を実施し、BMC の情報を登録します。

ストレージクラスターに対して「ストレージクラスターに BMC 接続検証用ルート証明書をインポートする<<Bare metal>>」を実施している場合は、増設したストレージノードの BMC に対して BMC の IP アドレスまたは IP アドレスに対応する FQDN を Common Name(CN)または Subject Alternative Name(SAN)に設定したサーバー証明書をインポートしてください。BMC のサーバー証明書の作成および BMC へのサーバー証明書のインポートについては、サーバーベンダーのマニュアルを参照してください。

その後、増設したストレージノードが、スペアノードに切り換えできる状態になっているかを「スペアノード機能の設定を確認する<<Bare metal>>」を参照して確認してください。



メモ

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される次のフィールドがサポートされます。

- 基本制限(Basic Constraints)
- キー使用法(Key Usage)
- サブジェクトキー識別子(Subject Key Identifier)
- 機関キー識別子(Authority Key Identifier)
- 証明書ポリシー(Certificate Policies)
- サブジェクト代替名(Subject Alternative Name)
- 名前の制限(Name Constraints)
- ポリシーの制限(Policy Constraints)
- 拡張キー使用法(Extended Key Usage)
- ポリシー禁止(Inhibit anyPolicy)

3. 増設したストレージノードのコンピュータポートに対して、コンピュータノードのパス情報を登録します。

コンピュータノードのパス情報の登録方法は「コンピュータノードのパス情報を登録する」を参照してください。

マルチテナンシーを構成し、VPS 内にコンピュータノードの登録がある場合、VPS 管理者に依頼してコンピュータノードのパス情報を登録してもらいます。



メモ

増設開始前に既存のストレージノードの全コンピュータポートとの間にパスが設定されていたイニシエーターに関しては、増設したストレージノードのコンピュータポートとの間のパスが自動的に生成されます。その場合、コンピュータノードのパス情報の登録処理は不要です。

4. iSCSI 接続の場合、増設開始前に既存のストレージノードのコンピュータポートに対し、CHAP ユーザーのアクセス許可をしていたとき、増設したストレージノードのコンピュータポートに対しても、認証設定の編集、および CHAP ユーザーのアクセス許可をします。

コンピュータポートに対しての認証設定の編集方法は「ターゲット動作のコンピュータポートの認証設定を編集する」を、CHAP ユーザーのアクセス許可方法は「CHAP ユーザーに対してコンピュータポートへのアクセスを許可する」を参照してください。

5. コンピュータノードから増設したストレージノードに対して接続できることを確認します。

接続できない場合、構成によって I/O 性能の低下やマルチパスの冗長性低下を引き起こすことがあります。

6. 構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



メモ

「追加した論理容量が使用できることを確認する<<Bare metal>>」の手順を完了していない場合、構成バックアップは実行できません。手順が完了したあとに構成バックアップを実行してください。

11.2 ストレージノードの増設<<Cloud for AWS>>

この節での記述内容は Cloud モデル for AWS に適用されます。

ストレージノードの増設は以下の目的のために実施します。

- ストレージプール容量の拡張
- コンピュートポート数の拡張
- システム性能の向上

増設するストレージノードに搭載されたすべてのドライブを対象に、ストレージノードの増設ジョブの延長でストレージプール拡張が実施されます。

増設するストレージノードのドライブ容量は増設前の構成のストレージノードと均一である必要があります。「増設時の容量設計」を参照して必要な容量・ドライブを搭載してください。



注意

- 本マニュアルが対象としているストレージソフトウェアのバージョンでは、増設したストレージノードは減設できません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。
- ストレージプール拡張の延長で実施される容量バランスやドライブデータ再配置によって、既存ボリュームの I/O 性能に影響が出る場合があります。
加えて、容量バランスおよびドライブデータ再配置の完了後から「増設したストレージノードの設定を行う<<Cloud for AWS>>」に記載の手順を実施するまでの間、既存ボリュームの I/O 性能に影響が出る場合があります。
また、ストレージノード増設時には、ストレージコントローラーの再配置が動作するため、ホスト I/O 性能が 3～4 分ほど低下することがあります。
- 増設するストレージノードと安全な SSL/TLS 通信を行うために、増設するストレージノードの管理ポートの情報を Subject Alternative Name(SAN)に追加したサーバー証明書を作成してください。サーバー証明書の作成手順は「運用管理を SSL/TLS 通信で行う」を参照してください。



メモ

既存のストレージノードに対してストレージプール拡張が実施されておらず、ストレージプールが空の場合は、ストレージノードの増設ジョブの延長でのストレージプール拡張は実施されません。ストレージプール拡張を実施する場合は「空状態にあるストレージプールを拡張する<<Cloud>>」を参照してください。

ストレージノード増設の操作手順の実施順と参照先を以下に示します。

操作手順の実施順と参照先	備考
1. 「 11.2.1 ストレージノードを増設する<<Cloud for AWS>> 」 2. 「 11.2.2 追加した論理容量が使用できることを確認する<<Cloud for AWS>> 」 3. 「 11.2.3 増設したストレージノードの設定を行う<<Cloud for AWS>> 」	すべてコントローラーノード操作



注意

ベースライセンスとして Floating を適用している場合、ストレージノードの増設によって AWS License Manager のライセンスの契約容量を超過する場合があります。増設手順を実施する前に「ライセンスの使用量を確認するためにストレージプールの容量を試算する《Cloud for AWS》」を参照して、ストレージノード増設後のストレージプールの容量を計算し、ストレージプールの論理容量が AWS License Manager のライセンスの契約容量に収まるかを確認してください。なお、必要なライセンスの契約容量は、ストレージプールの論理容量を TiB 単位に切り上げて計算してください。

複数のストレージクラスターで AWS License Manager のライセンスを共有している場合は、ストレージクラスターそれぞれのストレージプールの論理容量を先に TiB 単位に切り上げてから、それらを合計した値が、AWS License Manager のライセンスの契約容量に収まるかを確認してください。

(例) 2つのストレージクラスターがあって、それぞれのストレージプールの論理容量が 31.3[TiB]と 47.7[TiB]の場合、それぞれの値を整数値に切り上げて 32[TiB]と 48[TiB]としてから、それらを合計して 80[TiB]と計算します。

契約容量が不足する場合、AWS Marketplace 上でライセンスの契約を更新してください。

■Single-AZ 構成の場合(フォールトドメインの数が 1 つ)

- 各ストレージノードに対して AWS のスプレッドプレイスメントグループの設定を適用しており、ストレージノード増設の際はスプレッドプレイスメントグループ単位にストレージノードを増設する必要があります。ユーザーデータの保護種別ごとの、同一スプレッドプレイスメントグループに所属するストレージノードの数(同時に増設するストレージノード数)は以下のとおりです。

ユーザーデータの保護種別 (redundantType)	同一スプレッドプレイスメント グループに所属するストレージ ノードの数	同時に増設するストレージノード数
4D+2P	6	6
Duplication	3	3

- ドライブデータ再配置は実行されません。

■Multi-AZ 構成の場合(フォールトドメインが複数)

- Multi-AZ 構成の場合、タイブレーカーノードが属するフォールトドメイン以外の各フォールトドメインに同数のストレージノードを割り当て、それらのストレージノードを同時に増設する必要があります。同時に増設するストレージノード数は以下のとおりです。

ユーザーデータの保護種別 (redundantType)	同時に増設するストレージノード数
Duplication	2

- ドライブデータ再配置は実行されません。

11.2.1 ストレージノードを増設する《Cloud for AWS》

この項での記述内容は Cloud モデル for AWS に適用されます。

ストレージノードの増設は、コントローラーノード上から操作して行います。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イ

ベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。

- 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - 構成ファイルのエクスポート
 - ドライブの増設
 - ドライブの交換
- 増設するストレージノードのインスタンスタイプは、既存のストレージノード*のインスタンスタイプと同じにする必要があります。詳細は Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。
* Multi-AZ 構成の場合は、タイプブレーカーノードを除いたストレージノードが対象です。
- 増設対象のストレージノードが追加されるプロテクションドメインの、storageControllerClusteringPolicy が"TwoRedundantStorageNodes"の場合、ストレージクラスター内に閉塞*しているストレージノードが存在していると、ストレージノードは増設できません。また、storageControllerClusteringPolicy が"TwoRedundantStorageNodes"ではない場合でも、閉塞*しているストレージノードが存在していると、ストレージノードの増設に失敗することがあります。先に閉塞*しているストレージノードを回復させてからストレージノードを増設してください。
* ストレージノードが閉塞している場合、status が以下のいずれかになります。
"TemporaryBlockage"、"MaintenanceBlockage"、"PersistentBlockage"、"InstallationFailed"、
"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、
"RemovalFailedAndPersistentBlockage"
- ストレージノードの増設中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの増設が完了するのを待ってから再度これらの操作を実施してください。
- EBS 暗号化を利用している場合は、AWS を操作するアカウントやコントローラーノードに設定する IAM ロールに、AWS Key Management Service へアクセスするための権限を追加する必要があります。詳細は、AWS のユーザーガイドを参照してください。

ストレージノードの増設では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作します。



メモ

- 冗長性確保のため複数台のストレージノードを一度に増設します。複数台のストレージノード増設は、増設手順をひとつとして実施することで可能です。増設台数は、ユーザーデータの保護種別(redundantType)によって決まります。「ストレージノードの増設<<Cloud for AWS>>」の「ストレージノード増設時の留意事項」を参照してください。
- 増設するストレージノードのインスタンスタイプは、既存のストレージノードのインスタンスタイプと同じになります。

処理時間の目安

- 手順 4 で実行するストレージノードの増設ジョブの処理時間の目安は以下のとおりです。

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	同時に増設するストレージノード数	各ストレージノード VM のメモリー容量[GiB]	処理時間の目安 [min]
4D+2P	1	6	128	65
			256	70
Duplication	1	3	128	45

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	同時に増設するストレージノード数	各ストレージノード VM のメモリー容量[GiB]	処理時間の目安 [min]
	3	2	256	45
			128	
			256	

- 処理時間の目安について、以下の外部要因によって、手順 4 の処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。
 - AWS の負荷状況
 - ネットワークの通信状況(コントローラーノード、ストレージノード、AWS との相互間の通信状況)
 - EC2 インスタンスの性能状況

前提条件

- 実行に必要なロール：Service

操作手順

1. 「構成ファイルをエクスポートする《Cloud for AWS》」を参照し、VSP One SDS Block からストレージノード増設用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、`exportFileType` パラメーターに "AddStorageNodes" を指定してください。

最新状態の構成ファイルを使用するために、ストレージノード増設用の構成ファイルは必ず取得してください。



注意 構成ファイルのエクスポートで取得した構成ファイルは編集しないでください。編集するとストレージノード増設に失敗することがあります。設定値を間違えたときは、正しい値を設定して構成ファイルのエクスポートを再度実行してください。

2. 構成ファイルのエクスポートで取得した構成ファイル一式を手順 1 で `templateS3Url` パラメーターで指定した Amazon S3 バケットに格納します。

Amazon S3 にファイルを格納する方法として、例えば AWS CLI を用いて Amazon S3 にファイルをコピーする方法があります。詳細は Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「Amazon S3 の操作例」を参照してください。



注意 VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。

3. 増設開始前のストレージプールの論理容量、ストレージプールの空き容量を確認します。

REST API : GET /v1/objects/pools

CLI : `pool_list`

4. ストレージノードを増設します。

クラスターマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。

REST API : POST /v1/objects/storage-nodes

CLI : `storage_node_add`

コマンド実行後に表示されるジョブの ID を確認します。



注意

AWS 側のリソース不足により EC2 インスタンスなどの各種リソースが作成できず、ストレージノードの増設が失敗することがあります。



メモ

ジョブが完了した際に、イベントログの追加情報が Amazon S3 にアップロードされることがあります。イベントログのアクションで "Error message file" の参照が指示されている場合、メッセージに記載されている Error Message File のパスを基に追加情報を Amazon S3 から取得してください。

5. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

増設が完了するまでは、他の操作が実施できないことがあります。他の操作が失敗した場合は、他の操作のエラーメッセージやイベントログに従って対処してください。

6. ストレージノードの一覧を取得して、増設したストレージノードの ID が追加されていることを確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

7. ドライブの一覧を取得します。

増設したストレージノードの ID をクエリーパラメーターで指定してコマンドを実行します。

増設したストレージノードが複数存在する場合は、増設したストレージノードの数だけ繰り返し実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

増設したストレージノードに搭載されたドライブがすべてあり、それらのドライブの status がすべて "Normal" であることを確認してください。搭載されたドライブが存在しない場合や status が "Offline" の場合は「ドライブを増設する」を参照し、ドライブの増設とストレージプールの拡張を実施してください。



メモ

既存のストレージノードに対してストレージプール拡張が実施されておらず、ストレージプールが空の場合は、ストレージノードの増設ジョブの延長でのストレージプール拡張は実施されません。ストレージプール拡張を実施する場合は「空状態にあるストレージプールを拡張する <<Cloud>>」を参照してください。

8. ストレージプールの情報を取得します。

REST API : GET /v1/objects/pools

CLI : pool_list

増設開始前と比べて、ストレージプールの論理容量が拡張され、ストレージプールの空き容量が増加したことを確認してください。ストレージプールの論理容量が拡張されていない場合は、イベントログを取得してください。イベントログ KARS16158-W または KARS16159-W が出力された場合は、増設したストレージノードのドライブの容量が不足しているため、ユーザーが利用可能な容量である論理容量の拡張ができていません。論理容量を拡張するためには「増設時の容量設計」を参照して必要な容量を算出し、「ドライブを増設する」に従ってストレージプールを拡張してください。イベントログ KARS16158-W または KARS16159-W が出力されていない場合は、既存のストレージノードのドライブ容量またはドライブ数が不足してい

ます。「空状態にあるストレージプールを拡張する<<Cloud>>」に従ってストレージプールを拡張してください。

11.2.2 追加した論理容量が使用できることを確認する<<Cloud for AWS>>

この項での記述内容は Cloud モデル for AWS に適用されます。

ストレージノードの増設手順が完了しても、追加した論理容量はすぐには使用できません。以下の順で実行される内部処理の完了後、追加した論理容量が使用可能になります。

- ストレージコントローラーへの容量割り付け処理

ストレージコントローラーへの容量割り付けの処理時間は、このマニュアルの「ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安)」を参照してください。

前提条件

- 実行に必要なロール : Storage

操作手順

1. ストレージコントローラーへの容量割り付け処理の完了を確認します。

イベントログを取得して、増設したストレージノードのすべてのドライブがストレージプールの容量として使用できるようになったことを確認します。イベントログ KARS16020-I が、増設したストレージノードの数だけ出力されるまでお待ちください。それまでは、他の操作が実施できないことがあります。

REST API : GET /v1/objects/event-logs

CLI : event_log_list

イベントログ KARS16020-I が、増設したストレージノードの数だけ出力されたら、増設したストレージノードのすべてのドライブがストレージプールの容量として追加され、使用できるようになります。

ただし、イベントログ KARS16020-I が、増設したストレージノードの数だけ出力されるまでの間に、ストレージノードに障害が発生していた場合は、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対応してください。

11.2.3 増設したストレージノードの設定を行う<<Cloud for AWS>>

この項での記述内容は Cloud モデル for AWS に適用されます。

増設したストレージノードに対して各種設定を行います。

前提条件

- 実行に必要なロール : Service
- ストレージノードの増設ジョブの延長で、ストレージプール拡張が実施された場合は、「追加した論理容量が使用できることを確認する<<Cloud for AWS>>」の手順に従ったストレージプールの容量の確認が済んでいること
ストレージノードの増設ジョブの延長で、ストレージプール拡張が実施されてない場合は、確認不要です。

操作手順

1. 増設したストレージノードの管理ポートの情報を Subject Alternative Name(SAN)に追加したサーバー証明書を、VSP One SDS Block にインポートします。

サーバー証明書のインポート手順は「運用管理を SSL/TLS 通信で行う」を参照してください。

2. 増設したストレージノードのコンピュータポートに対して、コンピュータノードのパス情報を登録します。
コンピュータノードのパス情報の登録方法は「コンピュータノードのパス情報を登録する」を参照してください。



メモ

増設開始前に既存のストレージノードの全コンピュータポートとの間にパスが設定されていたイニシエーターに関しては、増設したストレージノードのコンピュータポートとの間のパスが自動的に生成されます。その場合、コンピュータノードのパス情報の登録処理は不要です。

3. 増設開始前に既存のストレージノードのコンピュータポートに対し、CHAP ユーザーのアクセス許可をしていたとき、増設したストレージノードのコンピュータポートに対しても、認証設定の編集、および CHAP ユーザーのアクセス許可をします。
コンピュータポートに対しての認証設定の編集方法は「ターゲット動作のコンピュータポートの認証設定を編集する」を、CHAP ユーザーのアクセス許可方法は「CHAP ユーザーに対してコンピュータポートへのアクセスを許可する」を参照してください。
4. コンピュータノードから増設したストレージノードに対して接続できることを確認します。
接続できない場合、構成によって I/O 性能の低下やマルチパスの冗長性低下を引き起こすことがあります。
5. 構成情報のバックアップを行います。
「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



メモ

「追加した論理容量が使用できることを確認する <<Cloud for AWS>>」の手順を完了していない場合、構成バックアップは実行できません。手順が完了したあとに構成バックアップを実行してください。

11.3 ストレージノードの増設 <<Cloud for Google Cloud>>

この節での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージノードの増設は以下の目的のために実施します。

- ストレージプール容量の拡張
- コンピュータポート数の拡張
- システム性能の向上

増設するストレージノードに搭載されたすべてのドライブを対象に、ストレージノードの増設ジョブの延長でストレージプール拡張が実施されます。

増設するストレージノードのドライブ容量は増設前の構成のストレージノードと均一である必要があります。「増設時の容量設計」を参照して必要な容量・ドライブを搭載してください。



注意

- 本マニュアルが対象としているストレージソフトウェアのバージョンでは、増設したストレージノードは減設できません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。

- ・ ストレージプール拡張の延長で実施される容量バランスやドライブデータ再配置によって、既存ボリュームの I/O 性能に影響が出ることがあります。
加えて、容量バランスおよびドライブデータ再配置の完了後から「増設したストレージノードの設定を行う <<Cloud for Google Cloud>>」に記載の手順を実施するまでの間、既存ボリュームの I/O 性能に影響が出ることがあります。
また、ストレージノード増設時には、ストレージコントローラーの再配置が動作するため、ホスト I/O 性能が 3～4 分ほど低下することがあります。
- ・ 増設するストレージノードと安全な SSL/TLS 通信を行うために、増設するストレージノードの管理ポートの情報を Subject Alternative Name(SAN)に追加したサーバー証明書を作成してください。サーバー証明書の作成手順は「運用管理を SSL/TLS 通信で行う」を参照してください。



メモ

既存のストレージノードに対してストレージプール拡張が実施されておらず、ストレージプールが空の場合は、ストレージノードの増設ジョブの延長でのストレージプール拡張は実施されません。ストレージプール拡張を実施する場合は「空状態にあるストレージプールを拡張する <<Cloud>>」を参照してください。

ストレージノード増設の操作手順の実施順と参照先を以下に示します。

操作手順の実施順と参照先	備考
1. 「 11.3.1 ストレージノードを増設する <<Cloud for Google Cloud>> 」 2. 「 11.3.2 追加した論理容量が使用できることを確認する <<Cloud for Google Cloud>> 」 3. 「 11.3.3 増設したストレージノードの設定を行う <<Cloud for Google Cloud>> 」	すべてコントローラーノード操作

ストレージノード増設時の留意事項

■Single-AZ (Single-Zone)構成の場合(フォールトドメインの数が 1 つ)

- ・ 各ストレージノードに対して Google Cloud のスプレッドプレイスメントポリシーの設定を適用しており、ストレージノード増設の際はスプレッドプレイスメントポリシー単位にストレージノードを増設する必要があります。ユーザーデータの保護種別ごとの、同一スプレッドプレイスメントポリシーに所属するストレージノードの数(同時に増設するストレージノード数)は以下のとおりです。

ユーザーデータの保護種別 (redundantType)	同一スプレッドプレイスメント ポリシーに所属するストレージ ノードの数	同時に増設するストレージノード数
4D+2P	6	6
Duplication	3	3

- ・ ドライブデータ再配置は実行されません。

■Multi-AZ (Multi-Zone)構成の場合(フォールトドメインが複数)

- ・ Multi-AZ (Multi-Zone)構成の場合、タイブレーカーノードが属するフォールトドメイン以外の各フォールトドメインに同数のストレージノードを割り当て、それらのストレージノードを同時に増設する必要があります。同時に増設するストレージノード数は以下のとおりです。

ユーザーデータの保護種別 (redundantType)	同時に増設するストレージノード数
Duplication	2

- ・ ドライブデータ再配置は実行されません。

11.3.1 ストレージノードを増設する<<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージノードの増設は、コントローラーノード上から操作して行います。



注意

- ・ 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- ・ 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - 構成ファイルのエクスポート
 - ドライブの減設
 - ドライブの増設
 - ドライブの交換
- ・ 増設対象のストレージノードが追加されるプロテクションドメインの、`storageControllerClusteringPolicy` が `"TwoRedundantStorageNodes"` の場合、ストレージクラスター内に閉塞*しているストレージノードが存在していると、ストレージノードは増設できません。また、`storageControllerClusteringPolicy` が `"TwoRedundantStorageNodes"` ではない場合でも、閉塞*しているストレージノードが存在していると、ストレージノードの増設に失敗することがあります。先に閉塞*しているストレージノードを回復させてからストレージノードを増設してください。
* ストレージノードが閉塞している場合、`status` が以下のいずれかになります。
`"TemporaryBlockage"`、`"MaintenanceBlockage"`、`"PersistentBlockage"`、`"InstallationFailed"`、`"RemovalFailedAndTemporaryBlockage"`、`"RemovalFailedAndMaintenanceBlockage"`、`"RemovalFailedAndPersistentBlockage"`
- ・ ストレージノードの増設中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの増設が完了するのを待ってから再度これらの操作を実施してください。

ストレージノードの増設では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作して行います。



メモ

- ・ 冗長性確保のため複数台のストレージノードを一度に増設します。複数台のストレージノード増設は、増設手順をひととおり実施することで可能です。増設台数は、ユーザーデータの保護種別(`redundantType`)によって決まります。「ストレージノードの増設<<Cloud for Google Cloud>>」の「ストレージノード増設時の留意事項」を参照してください。
- ・ ストレージノードなどの一部のリソースは、固定のリソース名で作成されます。対象となるリソースとリソース名を以下に示します。

リソース	名前
ストレージノード	<code>StorageNode<x>*</code>
* ストレージノード名に付与する<x>はストレージノードの番号で、ストレージノードごとに異なる番号が割り当てられます。番号はすでにストレージクラスターに組み込まれているストレージノードの次の番号から開始します。	

処理時間の目安

- 手順 6 で実行するストレージノードの増設ジョブの処理時間の目安は以下のとおりです。

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	同時に増設するストレージノード数	各ストレージノード VM のメモリー容量[GiB]	処理時間の目安 [min]
4D+2P	1	6	128	55
			256	60
Duplication	1	3	128	35
			256	35
	3	2	128	35
			256	35

- 処理時間の目安について、以下の外部要因によって、手順 6 の処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。
 - Google Cloud の負荷状況
 - ネットワークの通信状況(コントローラーノード、ストレージノード、Google Cloud との相互間の通信状況)
 - Compute Engine インスタンスの性能状況

前提条件

- 実行に必要なロール : Service

操作手順の留意事項

- Terraform は実行可能な環境から実行してください。

操作手順

- 「構成ファイルをエクスポートする<<Cloud for Google Cloud>>」を参照し、VSP One SDS Block からストレージノード増設用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、`exportFileType` パラメーターに "AddStorageNodes" を指定してください。

また、`machineImageId` パラメーターを指定してください。

最新状態の構成ファイルを使用するために、ストレージノード増設用の構成ファイルは必ず取得してください。

- 「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する<<Cloud for Google Cloud>>」を参照し、構成ファイルを解凍して配置します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、ストレージクラスターが閉塞するなどの事態が起こるおそれがあります。

- 増設開始前のストレージプールの論理容量、ストレージプールの空き容量を確認します。

REST API : GET /v1/objects/pools

CLI : `pool_list`

- ストレージノード増設用の構成ファイルをデプロイすることによる影響を確認します。

以下のコマンドを実行します。

```
terraform plan
```

コマンドを実行すると[Terraform will perform the following actions]という表示のあとにリソースに対する変更内容が表示されます。以下のリソースの変更が実施されることを確認してください。

#	リソース種別	リソース操作	リソース名 ¹	確認内容
1	google_compute_disk.user_disks[]	create	<clusterName>-snXX-userdatadiskYY	リソースが「同時に増設するストレージノードの台数 ² × 1 ノード当たりのドライブの台数」の数だけ作成されること
2	google_compute_attached_disk.attached_user_disk[]	create	-	リソースが「同時に増設するストレージノードの台数 ² × 1 ノード当たりのドライブの台数」の数だけ作成されること
3	google_compute_instance.instance[]	create	<clusterName>-snXX	- リソースが「同時に増設するストレージノードの台数²」の数だけ作成されること - リソース名の XX がストレージクラスターに存在するストレージノードの次の番号から始まること
4	google_compute_instance.instance[]	update in-place	<clusterName>-snXX	以下の項目に変更がある場合がありますが、問題ありません。 metadata
5	google_compute_resource_policy.spp[]	create	<clusterName>-resource-policyZZ	Single-AZ (Single-Zone)構成 ³ か Multi-AZ (Multi-Zone)構成 ⁴ かの場合で異なります。
1. リソース名の XX、YY、ZZ はそれぞれ以下を示します。 XX: ストレージノードに割り振られている番号。番号は 2 桁の整数で、構築した順番に 01 から番号が付けられます。 YY: 各ストレージノードのユーザードライブに割り振られている番号。 ZZ: スプレッドプレイスメントポリシーごとに割り振られている番号。 2. 同時に増設するストレージノードの台数は以下です。 - Single-AZ (Single-Zone)構成でデータ保護方式が Duplication の場合: 3 - Single-AZ (Single-Zone)構成でデータ保護方式が 4D+2P の場合: 6 - Multi-AZ (Multi-Zone)構成でデータ保護方式が Duplication の場合: 2 3. Single-AZ (Single-Zone)構成の場合、以下の内容を確認してください。 - リソースが 1 個作成されること - 作成されるストレージノードの番号 XX(#3 における XX)とリソース名の ZZ の組み合わせが、以下のいずれかであること。組み合わせは{XX,YY}で表しています。 - データ保護方式が Duplication の場合: {01-03,01},{04-06,02},{07-09,03},{10-12,04},{13-15,05},{16-18,06} - データ保護方式が 4D+2P の場合: {01-06,01},{07-12,02},{13-18,03}				

#	リソース種別	リソース操作	リソース名 ¹	確認内容
4. Multi-AZ (Multi-Zone)構成の場合、以下の内容を確認してください。 - リソースが以下の個数作成されること - ストレージノードの番号 XX(#3 における XX)が 16 または 17 の場合 : 2 個 - ストレージノードの番号 XX(#3 における XX)が 16 でも 17 でもない場合 : 0 個 - リソースが 2 個作成される場合、リソース名の ZZ が 03 と 04 であること				

5. terraform plan による確認で問題が無ければ、ストレージノードのリソースを作成するため、以下のコマンドを実行します。

```
terraform apply
```

コマンドの実行後、[Enter a value:]と表示されたら[yes]を入力します。

入力すると最後に[Outputs]が出力されます。terraform apply が完了することで、クラウドリソースの作成が完了します。

6. ストレージノードを増設します。

クラスターマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。

REST API : POST /v1/objects/storage-nodes

CLI : storage_node_add

上記コマンドを実行すると、セットアップユーザーのパスワードの入力が要求されます。そのときは、何も入力しないで「Enter」キーを押してください。

コマンド実行後に表示されるジョブの ID を確認します。



メモ

ジョブが完了した際にイベントログの追加情報が Cloud Storage にアップロードされることがあります。イベントログのアクションで"Error message file"の参照が指示されている場合、メッセージに記載されている Error Message File のパスを基に追加情報を Cloud Storage から取得してください。

アップロード先の Cloud Storage のディレクトリーは、ストレージクラスター構築の際に terraform.tfvars ファイルの gsUri で指定したディレクトリーです。

gsUri の情報は terraform output で gsUri のキーを確認してください。

```
terraform output
```

7. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

増設が完了するまでは、他の操作が実施できないことがあります。他の操作が失敗した場合は、他の操作のエラーメッセージやイベントログに従って対処してください。

8. ストレージノードの一覧を取得して、増設したストレージノードの ID が追加されていることを確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

9. ドライブの一覧を取得します。

増設したストレージノードの ID をクエリーパラメーターで指定してコマンドを実行します。

増設したストレージノードが複数存在する場合は、増設したストレージノードの数だけ繰り返し実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

増設したストレージノードに搭載されたドライブがすべてあり、それらのドライブの **status** がすべて **"Normal"**であることを確認してください。搭載されたドライブが存在しない場合や **status** が **"Offline"**の場合は「ドライブを増設する」を参照し、ドライブの増設とストレージプールの拡張を実施してください。



メモ

既存のストレージノードに対してストレージプール拡張が実施されておらず、ストレージプールが空の場合は、ストレージノードの増設ジョブの延長でのストレージプール拡張は実施されません。ストレージプール拡張を実施する場合は「空状態にあるストレージプールを拡張する <<Cloud>>」を参照してください。

10. ストレージプールの情報を取得します。

REST API : GET /v1/objects/pools

CLI : pool_list

増設開始前と比べて、ストレージプールの論理容量が拡張され、ストレージプールの空き容量が増加したことを確認してください。ストレージプールの論理容量が拡張されていない場合は、イベントログ **KARS16158-W** または **KARS16159-W** が出力された場合は、増設したストレージノードのドライブの容量が不足しているため、ユーザーが利用可能な容量である論理容量の拡張ができていません。論理容量を拡張するためには「増設時の容量設計」を参照して必要な容量を算出し、「ドライブを増設する」に従ってストレージプールを拡張してください。イベントログ **KARS16158-W** または **KARS16159-W** が出力されていない場合は、既存のストレージノードのドライブ容量またはドライブ数が不足しています。「空状態にあるストレージプールを拡張する <<Cloud>>」に従ってストレージプールを拡張してください。

11.3.2 追加した論理容量が使用できることを確認する <<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージノードの増設手順が完了しても、追加した論理容量はすぐには使用できません。以下の順で実行される内部処理の完了後、追加した論理容量が使用可能になります。

- ストレージコントローラーへの容量割り付け処理

ストレージコントローラーへの容量割り付けの処理時間は、このマニュアルの「ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安)」を参照してください。

前提条件

- 実行に必要なロール : Storage

操作手順

1. ストレージコントローラーへの容量割り付け処理の完了を確認します。

イベントログを取得して、増設したストレージノードのすべてのドライブがストレージプールの容量として使用できるようになったことを確認します。イベントログ **KARS16020-I** が、増設したストレージノードの数だけ出力されるまでお待ちください。それまでは、他の操作が実施できないことがあります。

REST API : GET /v1/objects/event-logs

CLI : event_log_list

イベントログ KARS16020-I が、増設したストレージノードの数だけ出力されたら、増設したストレージノードのすべてのドライブがストレージプールの容量として追加され、使用できるようになります。

ただし、イベントログ KARS16020-I が、増設したストレージノードの数だけ出力されるまでの間に、ストレージノードに障害が発生していた場合は、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対応してください。

11.3.3 増設したストレージノードの設定を行う <<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

増設したストレージノードに対して各種設定を行います。

前提条件

- 実行に必要なロール : Service
- 「追加した論理容量が使用できることを確認する <<Cloud for Google Cloud>>」の手順に従ったストレージプールの容量の確認が済んでいること
ただし、ストレージノードの増設ジョブの延長で、ストレージプール拡張が実施されてない場合は確認不要です。

操作手順

1. 増設したストレージノードの管理ポートの情報を Subject Alternative Name(SAN)に追加したサーバー証明書を、VSP One SDS Block にインポートします。
サーバー証明書のインポート手順は「運用管理を SSL/TLS 通信で行う」を参照してください。
2. 増設したストレージノードのコンピュータポートに対して、コンピュータノードのパス情報を登録します。
コンピュータノードのパス情報の登録方法は「コンピュータノードのパス情報を登録する」を参照してください。



メモ

増設開始前に既存のストレージノードの全コンピュータポートとの間にパスが設定されていたイニシエーターに関しては、増設したストレージノードのコンピュータポートとの間のパスが自動的に生成されます。その場合、コンピュータノードのパス情報の登録処理は不要です。

3. 増設開始前に既存のストレージノードのコンピュータポートに対し、CHAP ユーザーのアクセス許可をしていたとき、増設したストレージノードのコンピュータポートに対しても、認証設定の編集、および CHAP ユーザーのアクセス許可をします。
コンピュータポートに対しての認証設定の編集方法は「ターゲット動作のコンピュータポートの認証設定を編集する」を、CHAP ユーザーのアクセス許可方法は「CHAP ユーザーに対してコンピュータポートへのアクセスを許可する」を参照してください。
4. コンピュータノードから増設したストレージノードに対して接続できることを確認します。
接続できない場合、構成によって I/O 性能の低下やマルチパスの冗長性低下を引き起こすことがあります。

11.4 ストレージノードの増設 <<Cloud for Microsoft Azure>>

この節での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージノードの増設は以下の目的のために実施します。

- ・ ストレージプール容量の拡張
- ・ コンピュートポート数の拡張
- ・ システム性能の向上

増設するストレージノードに搭載されたすべてのドライブを対象に、ストレージノードの増設ジョブの延長でストレージプール拡張が実施されます。

増設するストレージノードのドライブ容量は増設前の構成のストレージノードと均一である必要があります。「増設時の容量設計」を参照して必要な容量・ドライブを搭載してください。



注意

- ・ 本マニュアルが対象としているストレージソフトウェアのバージョンでは、増設したストレージノードは減設できません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。
- ・ ストレージノード増設失敗後に再度増設を実施しない場合は、不要なリソースを必ず削除してください。不要なリソースが残ったままだと、Microsoft Azure に課金され続けるおそれがあります。再度増設を実施する場合は、増設処理の中で不要なリソースは削除されます。
不要なリソースの削除については、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block の構成情報に存在しないストレージノードの VM(Azure VM インスタンス)を削除する手順<<Cloud for Microsoft Azure>>」を参照してください。
- ・ ストレージプール拡張の延長で実施される容量バランスやドライブデータ再配置によって、既存ボリュームの I/O 性能に影響が出ることがあります。
加えて、容量バランスおよびドライブデータ再配置の完了後から「増設したストレージノードの設定を行う<<Cloud for Microsoft Azure>>」に記載の手順を実施するまでの間、既存ボリュームの I/O 性能に影響が出ることがあります。
また、ストレージノード増設時には、ストレージコントローラーの再配置が動作するため、ホスト I/O 性能が 3~4 分ほど低下することがあります。
- ・ 増設するストレージノードと安全な SSL/TLS 通信を行うために、増設するストレージノードの管理ポートの情報を Subject Alternative Name(SAN)に追加したサーバー証明書を作成してください。サーバー証明書の作成手順は「運用管理を SSL/TLS 通信で行う」を参照してください。



メモ

既存のストレージノードに対してストレージプール拡張が実施されておらず、ストレージプールが空の場合は、ストレージノードの増設ジョブの延長でのストレージプール拡張は実施されません。ストレージプール拡張を実施する場合は「空状態にあるストレージプールを拡張する<<Cloud>>」を参照してください。

ストレージノード増設の操作手順の実施順と参照先を以下に示します。

操作手順の実施順と参照先	備考
1. 「 11.4.1 ストレージノードを増設する<<Cloud for Microsoft Azure>> 」 2. 「 11.4.2 追加した論理容量が使用できることを確認する<<Cloud for Microsoft Azure>> 」 3. 「 11.4.3 増設したストレージノードの設定を行う<<Cloud for Microsoft Azure>> 」	すべてコントローラーノード操作

ストレージノード増設時の留意事項

■Single-AZ 構成の場合(フォールトドメインの数が 1 つ)

- ・ 各ストレージノードに対して Microsoft Azure のスケールセットの設定を適用しており、ストレージノード増設の際はスケールセット単位にストレージノードを増設する必要があります。ユ

ユーザーデータの保護種別ごとの、同一スケールセットに所属するストレージノードの数(同時に増設するストレージノード数)は以下のとおりです。

ユーザーデータの保護種別 (redundantType)	同一スケールセットに所属する ストレージノードの数	同時に増設するストレージノード数
4D+2P	6	6
Duplication	3	3

- ドライブデータ再配置は実行されません。

■Multi-AZ 構成の場合(フォールトドメインが複数)

- Multi-AZ 構成の場合、タイブレーカーノードが属するフォールトドメイン以外の各フォールトドメインに同数のストレージノードを割り当て、それらのストレージノードを同時に増設する必要があります。同時に増設するストレージノード数は以下のとおりです。

ユーザーデータの保護種別 (redundantType)	同時に増設するストレージノード数
Duplication	2

- ドライブデータ再配置は実行されません。

11.4.1 ストレージノードを増設する<<Cloud for Microsoft Azure>>

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージノードの増設は、コントローラーノード上から操作して行います。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - 構成ファイルのエクスポート
 - ドライブの減設
 - ドライブの増設
 - ドライブの交換
- 増設対象のストレージノードが追加されるプロテクションドメインの、storageControllerClusteringPolicy が"TwoRedundantStorageNodes"の場合、ストレージクラスター内に閉塞*しているストレージノードが存在していると、ストレージノードは増設できません。また、storageControllerClusteringPolicy が"TwoRedundantStorageNodes"ではない場合でも、閉塞*しているストレージノードが存在していると、ストレージノードの増設に失敗することがあります。先に閉塞*しているストレージノードを回復させてからストレージノードを増設してください。
* ストレージノードが閉塞している場合、status が以下のいずれかになります。
"TemporaryBlockage"、"MaintenanceBlockage"、"PersistentBlockage"、"InstallationFailed"、
"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、
"RemovalFailedAndPersistentBlockage"

- ・ ストレージノードの増設中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの増設が完了するのを待ってから再度これらの操作を実施してください。

ストレージノードの増設では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作して行います。



メモ

- ・ 冗長性確保のため複数台のストレージノードを一度に増設します。複数台のストレージノード増設は、増設手順をひととおり実施することで可能です。増設台数は、ユーザーデータの保護種別(redundantType)によって決まります。「ストレージノードの増設<<Cloud for Microsoft Azure>>」の「ストレージノード増設時の留意事項」を参照してください。
- ・ 増設するストレージノードの VM のサイズは、既存のストレージノードの VM のサイズと同じになります。
- ・ ストレージノードは以下のリソース名で作成されます。

リソース	リソース名
ストレージノード	<clusterName>-SN<XX>*
* ストレージノード名に付与される<clusterName>はストレージクラスター名です。また、<XX>はストレージノードの番号であり、すでにストレージクラスターに組み込まれているストレージノードの番号の次の番号が割り当てられます。	

処理時間の目安

- ・ 手順 3 で実行するストレージノードの増設ジョブの処理時間の目安は以下のとおりです。

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	同時に増設するストレージノード数	各ストレージノード VM のメモリー容量[GiB]	処理時間の目安 [min]
4D+2P	1	6	128	65
			256	75
Duplication	1	3	128	45
			256	50
	3	2	128	45
			256	50

- ・ 処理時間の目安について、以下の外部要因によって、手順 3 の処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。
 - Microsoft Azure の負荷状況
 - ネットワークの通信状況(コントローラーノード、ストレージノード、Microsoft Azure との相互間の通信状況)
 - Azure VM インスタンスの性能状況

前提条件

- ・ 実行に必要なロール : Service

操作手順

1. 「構成ファイルをエクスポートする<<Cloud for Microsoft Azure>>」を参照し、VSP One SDS Block からストレージノード増設用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、`exportFileType` パラメーターに "AddStorageNodes" を指定してください。

また、`machineImageId` パラメーターを指定してください。

最新状態の構成ファイルを使用するために、ストレージノード増設用の構成ファイルは必ず取得してください。



注意

- `machineImageId` パラメーターは、ストレージクラスターのバージョンと同じ VM イメージを使用してください。
ストレージソフトウェアのバージョンは "aa.bb.cc.dd" の形式になっています。
VM イメージのバージョンは sku 名に記載されています。sku 名は "aa_bb_cc_dd_byol" の形式になっていて、"aa_bb_cc_dd" 部分がバージョンを示します。
"aa.bb.cc.dd" と "aa_bb_cc_dd" の数値が一致していることを確認してください。
- エクスポートした `ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` は解凍しないでください。解凍して使用した場合、ジョブが失敗するおそれがあります。パラメーターで指定する値を間違えた場合は、正しい値を指定して構成ファイルのエクスポートを再度実行し、最新の構成ファイルを取得しなおしてください。

2. 増設開始前のストレージプールの論理容量、ストレージプールの空き容量を確認します。

REST API : GET /v1/objects/pools

CLI : `pool_list`

3. ストレージノードを増設します。

クラスターマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。

コマンド実行時には、手順 1 でエクスポートした

`ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` をパラメーターとして指定する必要があります。

この構成ファイルは解凍せずにパラメーターに指定してください。

REST API : POST /v1/objects/storage-nodes

CLI : `storage_node_add`

上記コマンドを実行すると、セットアップユーザーのパスワードの入力が要求されます。そのときは、何も入力しないで「Enter」キーを押してください。

コマンド実行後に表示されるジョブの ID を確認します。



メモ

イベントログに Error message file が表示されていた場合は、インストール時に作成した Azure Blob Storage のコンテナに追加情報がアップロードされます。

4. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : `job_show`

state が "Succeeded" になっていたらジョブは完了です。

増設が完了するまでは、他の操作が実施できないことがあります。他の操作が失敗した場合は、他の操作のエラーメッセージやイベントログに従って対処してください。



注意

ジョブが完了した際に、イベントログ KARS10965-W が出力されることがあります。その場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「リソースの削除ロックが正しく設定されていない場合の対処<<Cloud for Microsoft Azure>>」を確認し対処してください。

5. ストレージノードの一覧を取得して、増設したストレージノードの ID が追加されていることを確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

6. ドライブの一覧を取得します。

増設したストレージノードの ID をクエリーパラメーターで指定してコマンドを実行します。
増設したストレージノードが複数存在する場合は、増設したストレージノードの数だけ繰り返し実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

増設したストレージノードに搭載されたドライブがすべてあり、それらのドライブの status がすべて"Normal"であることを確認してください。搭載されたドライブが存在しない場合や status が"Offline"の場合は「ドライブを増設する」を参照し、ドライブの増設とストレージプールの拡張を実施してください。



メモ

既存のストレージノードに対してストレージプール拡張が実施されておらず、ストレージプールが空の場合は、ストレージノードの増設ジョブの延長でのストレージプール拡張は実施されません。ストレージプール拡張を実施する場合は「空状態にあるストレージプールを拡張する <<Cloud>>」を参照してください。

7. ストレージプールの情報を取得します。

REST API : GET /v1/objects/pools

CLI : pool_list

増設開始前と比べて、ストレージプールの論理容量が拡張され、ストレージプールの空き容量が増加したことを確認してください。ストレージプールの論理容量が拡張されていない場合は、イベントログを取得してください。イベントログ KARS16158-W または KARS16159-W が出力された場合は、増設したストレージノードのドライブの容量が不足しているため、ユーザーが利用可能な容量である論理容量の拡張ができていません。論理容量を拡張するためには「増設時の容量設計」を参照して必要な容量を算出し、「ドライブを増設する」に従ってストレージプールを拡張してください。イベントログ KARS16158-W または KARS16159-W が出力されていない場合は、既存のストレージノードのドライブ容量またはドライブ数が不足しています。「空状態にあるストレージプールを拡張する <<Cloud>>」に従ってストレージプールを拡張してください。

11.4.2 追加した論理容量が使用できることを確認する <<Cloud for Microsoft Azure>>

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージノードの増設手順が完了しても、追加した論理容量はすぐには使用できません。以下の順で実行される内部処理の完了後、追加した論理容量が使用可能になります。

- ストレージコントローラーへの容量割り付け処理

ストレージコントローラーへの容量割り付けの処理時間は、このマニュアルの「ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安)」を参照してください。

前提条件

- 実行に必要なロール : Storage

操作手順

1. ストレージコントローラーへの容量割り付け処理の完了を確認します。

イベントログを取得して、増設したストレージノードのすべてのドライブがストレージプールの容量として使用できるようになったことを確認します。イベントログ **KARS16020-I** が、増設したストレージノードの数だけ出力されるまでお待ちください。それまでは、他の操作が実施できないことがあります。

REST API : GET /v1/objects/event-logs

CLI : event_log_list

イベントログ **KARS16020-I** が、増設したストレージノードの数だけ出力されたら、増設したストレージノードのすべてのドライブがストレージプールの容量として追加され、使用できるようになります。

ただし、イベントログ **KARS16020-I** が、増設したストレージノードの数だけ出力されるまでの間に、ストレージノードに障害が発生していた場合は、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対応してください。

11.4.3 増設したストレージノードの設定を行う ≪Cloud for Microsoft Azure≫

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

増設したストレージノードに対して各種設定を行います。

前提条件

- 実行に必要なロール : Service
- 「追加した論理容量が使用できることを確認する ≪Cloud for Microsoft Azure≫」の手順に従ったストレージプールの容量の確認が済んでいること
ただし、ストレージノードの増設ジョブの延長で、ストレージプール拡張が実施されてない場合は確認不要です。

操作手順

1. 増設したストレージノードの管理ポートの情報を Subject Alternative Name(SAN)に追加したサーバー証明書を、VSP One SDS Block にインポートします。

サーバー証明書のインポート手順は「運用管理を SSL/TLS 通信で行う」を参照してください。

2. 増設したストレージノードのコンピュータポートに対して、コンピュータノードのパス情報を登録します。

コンピュータノードのパス情報の登録方法は「コンピュータノードのパス情報を登録する」を参照してください。



メモ

増設開始前に既存のストレージノードの全コンピュータポートとの間にパスが設定されていたイニシエーターに関しては、増設したストレージノードのコンピュータポートとの間のパスが自動的に生成されます。その場合、コンピュータノードのパス情報の登録処理は不要です。

3. 増設開始前に既存のストレージノードのコンピュータポートに対し、CHAP ユーザーのアクセス許可をしていたとき、増設したストレージノードのコンピュータポートに対しても、認証設定の編集、および CHAP ユーザーのアクセス許可をします。

コンピュータポートに対しての認証設定の編集方法は「ターゲット動作のコンピュータポートの認証設定を編集する」を、CHAP ユーザーのアクセス許可方法は「CHAP ユーザーに対してコンピュータポートへのアクセスを許可する」を参照してください。

4. コンピュータノードから増設したストレージノードに対して接続できることを確認します。
接続できない場合、構成によって I/O 性能の低下やマルチパスの冗長性低下を引き起こすことがあります。

ストレージノード減設の条件と手順

- 12.1 ストレージノードの減設<<Bare metal>>
- 12.2 ストレージノードの減設<<Cloud for AWS>>
- 12.3 ストレージノードの減設<<Cloud for Google Cloud>>
- 12.4 ストレージノードの減設<<Cloud for Microsoft Azure>>
- 12.5 ストレージノードの減設処理を中止する

12.1 ストレージノードの減設<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ストレージプール容量の縮退を行う場合には、ストレージノードの減設が必要になります。



注意

- ・ フォールトドメインが複数で構成されている場合、ストレージノードの減設はできません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。
- ・ Universal Replicator 機能を使用している場合はストレージノードの減設はできません。Universal Replicator 機能を使用中にストレージノードを減設する場合は「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」の「Universal Replicator 使用時にストレージノードを減設する<<Bare metal>>」を参照してください。

ストレージノードの減設手順は以下のとおりです。

1. 「ストレージノード減設の条件を確認する<<Bare metal>>」
2. 「ストレージノードを減設する<<Bare metal>>」

ストレージノードの減設中のホスト I/O、ユーザーデータの冗長度、処理時間(目安)は以下のとおりです。

項目	説明
ホスト I/O	ストレージノードの減設中もホスト I/O は継続されます。マルチパス構成が組まれていることが前提になります。
ストレージコントローラー	1 つのストレージノードを減設すると、1 つのストレージコントローラーが削除されます。 ストレージノードの減設中、削除されるストレージコントローラーが管理するボリュームは、別のストレージコントローラーへと移動されます。 この処理をボリュームマイグレーションといいます。
ユーザーデータの冗長度	ストレージノードの減設中もユーザーデータの冗長度は維持されます。
処理時間*	ストレージコントローラー間で移動するボリュームの容量とドライブデータ再配置の対象となるドライブデータ容量に依存します。
* 処理時間の目安は、以下の計算式で求められます。 プロテクションドメインに設定された最小メモリーに応じた処理時間(1) + ストレージコントローラー間ボリュームマイグレーションの処理時間(2) + ドライブデータ再配置の処理時間(3) (1) 35[min] (2) 以下から算出します。 ・ 対象となるボリューム : activeStorageNodeId が減設対象のストレージノードの ID となっているストレージコントローラーが持つすべてのボリューム ・ ボリュームマイグレーション性能(ボリューム 1 個当たり、目安) : 14.7[MiB/sec] ・ 並列実行が可能なボリューム数 : 21 個 ・ ボリュームマイグレーション実行オーバーヘッド(ボリューム 1 個当たり、目安) : 1[min] (例 1)対象が 1TiB のボリューム 1 個だった場合 $1[\text{TiB}] / 14.7[\text{MiB/sec}] + 1[\text{min}] \approx 19.8[\text{h}]$ (例 2)対象が 1TiB のボリューム 22 個だった場合 (並列実行が可能なボリューム数の範囲で順次処理されます。) $1[\text{TiB}] / 14.7[\text{MiB/sec}] + 1[\text{TiB}] / 14.7[\text{MiB/sec}] + 22[\text{min}] \approx 40.0[\text{h}]$ (例 3)対象が 1TiB のボリューム 1 個と 500GB のボリューム 1 個だった場合 (並列実行されるため、サイズが大きいほうのボリュームの処理時間になります。) $1[\text{TiB}] / 14.7[\text{MiB/sec}] + 2[\text{min}] \approx 19.8[\text{h}]$	

項目	説明
(3) 「ドライブデータ再配置完了までの時間(目安)≪Bare metal≫」を参照してください。	

処理時間の目安について、以下の外部要因によって 処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。

- ・ ネットワークの通信状況(ストレージノード間の通信状況)
- ・ サーバーの性能状況(ストレージノードの温度上昇による性能低下など)
- ・ サーバーのハードウェア構成(ストレージノードのプロセッサ、メモリー容量など)



注意

- ・ ストレージノードの減設時は、以下の処理の動作中に I/O 性能が不安定になる可能性があります。
 - ボリュームマイグレーション
 - ドライブデータ再配置
- ・ ストレージノードの減設時には、ストレージコントローラーの再配置が動作するため、ホスト I/O 性能が 3 ～4 分程度低下する可能性があります。
- ・ ストレージノードの減設によって削除する管理ポートの情報を Subject Alternative Name(SAN)から削除したサーバー証明書を作成してください。
サーバー証明書の作成手順は「運用管理を SSL/TLS 通信で行う」を参照してください。
- ・ ストレージノードを減設したあと、ハードウェアを廃棄または再利用する場合は、情報漏えい防止の観点からデータ消去することを強くお勧めします。
- ・ ストレージノードを減設したあと、減設したストレージノードをストレージノードとして再利用し、増設する場合でも「ストレージノードの増設≪Bare metal≫」の手順を最初から実施する必要があります。
- ・ VSP One SDS Block の運用管理において、REST API/CLI/VSP One SDS Block Administrator(ブラウザ)での操作の接続先として、DNS を用意し FQDN を指定する方法で運用している場合、ストレージノードを減設したあと、ストレージノードの減設によって削除した管理ポートの IP アドレスについて、DNS サーバーから正引きの定義を削除してください。

12.1.1 ストレージノード減設の条件を確認する≪Bare metal≫

この項での記述内容は Bare metal に適用されます。

ストレージノードが減設できるかどうかを以下の手順で確認してください。



注意

- ・ フォールトドメインが複数で構成されている場合、ストレージノードの減設はできません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。
- ・ Universal Replicator 機能を使用している場合はストレージノードの減設はできません。Universal Replicator 機能を使用中にストレージノードを減設する場合は「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」の「Universal Replicator 使用時にストレージノードを減設する≪Bare metal≫」を参照してください。
- ・ イベントログ KARS06170-C が発行され、未対処だった場合は、ストレージノードの減設はできません。KARS06170-C を対処後にストレージノードの減設を実施してください。
- ・ イベントログ KARS10340-E が発行され、未対処だった場合は、ストレージノードの減設はできません。「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」の「Universal Replicator 使用時にストレージノードを減設する≪Bare metal≫」を参照し、KARS10340-E の対処を実施してから、ストレージノードを減設してください。

前提条件

- ・ 実行に必要なロール : Security、Storage、Monitor、Service、または Resource



メモ

マルチテナンシー機能を使用している場合、手順 8 と 11 でシステムスコープ以外のボリュームも含むすべてのボリュームを参照するために、Monitor ロールが必要です。

操作手順

1. ストレージノードの一覧を取得して、減設対象のストレージノードの ID を記録します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

2. ストレージコントローラーの一覧を取得して、以下を行います。

REST API : GET /v1/objects/storage-controllers

CLI : storage_controller_list

- a. すべてのストレージコントローラーの ID を記録します。
- b. 減設対象のストレージノードの ID が、activeStorageNodeId、standbyStorageNodeId、secondaryStandbyStorageNodeId のいずれかにあるストレージコントローラーの ID を記録します。

ただし、一度ストレージノード減設を実施して、中断または失敗したあとに同じストレージノードに対してストレージノード減設を再実施する場合(ストレージノードの status に "RemovalFailed" が付いている場合)は、減設対象のストレージノードにひもづくストレージコントローラーが存在しない可能性があります。その場合は、該当するストレージコントローラーはなしとして、以降の確認項目のうち、ストレージコントローラーに関連する項目は無視して先に進むようにしてください。

3. ストレージノードの一覧を取得して、減設対象のストレージノードが減設できるかどうかを、以下に従って確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

- ・ 減設対象のストレージノードの clusterRole が "Worker" であること
クラスターマスターノードの減設はできません。そのため、clusterRole が "Master" のストレージノードは減設できません。
- ・ 減設対象のストレージノードの status が "Ready"、"RemovalFailed"、"RemovalFailedAndStopping"、"RemovalFailedAndStopped" のいずれかの値であること
減設対象のストレージノードが、これら以外の status になっている場合、以下に従って対処してください。
 - VSP One SDS Block Administrator でストレージノードの Health Status に "Alerting" が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
ただし、減設対象のストレージノードが、"RemovalFailed"、"RemovalFailedAndStopping"、"RemovalFailedAndStopped" となっている場合も "Alerting" になりますが、その場合は問題ありません。
 - status が "MaintenanceBlockage" となっている場合は「ストレージノードを保守回復する <<Bare metal>>」に従って、ストレージノードを保守回復してください。
 - 上記以外の場合は、ストレージノードに対する処理が実施中のため、status が変わるまで待ってから、再度確認してください。
- ・ ストレージノード減設後のストレージノード数が、次に示すノード数以上であること

ユーザーデータの保護種別 (redundantType)	減設後のストレージノード数
4D+1P	5
4D+2P	6
Duplication	3

すべてが確認できたら、次の手順に進みます。

4. ストレージプールの一覧を取得し、ユーザーデータの冗長度が低下していないことを dataRedundancy で確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

次の表に従って冗長度を確認します。冗長度が低下していなければ手順 7 に進みます。冗長度が低下している場合は次の手順に進みます。

ユーザーデータの保護種別 (redundantType)	dataRedundancy の値	冗長度
4D+1P - Duplication	1	冗長度が低下していません。
	1 未満	冗長度が低下しています。
4D+2P	2	冗長度が低下していません。
	2 未満	冗長度が低下しています。

5. ストレージクラスター内のすべてのストレージノードに関して、以下のいずれかに該当する場合はそれぞれ以下の対処を行います。いずれにも該当しない場合は手順 6 に進みます。
 - VSP One SDS Block Administrator でストレージノードの Health Status に "Alerting" が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
ただし、減設対象のストレージノードが、"RemovalFailed"、
"RemovalFailedAndStopping"、"RemovalFailedAndStopped"となっている場合も
"Alerting"になりますが、その場合は問題ありません。
 - status が "MaintenanceBlockage" のストレージノードがある場合は「ストレージノードを保守回復する <<Bare metal>>」に従って、ストレージノードを保守回復してください。
6. 「リビルドの状態を確認する」を参照して、リビルドが動作中でないこと、およびリビルドでエラーが発生していないことを確認します。
リビルドが動作中でなく、かつエラーが発生していない場合は、次の手順に進みます。
リビルドが動作中、またはリビルドでエラーが発生している場合は「リビルドの状態を確認する」を参照して対処してください。



メモ

フォールトドメインが複数で構成されている場合、手順 7 から 12 までの操作は不要です。

7. 「ドライブデータ再配置の起動契機と動作可能な条件 <<Bare metal>>」を参照して、ストレージノード減設時に実行されるドライブデータ再配置が動作可能であることを確認します。
動作可能な条件に合致しない場合は「ドライブデータ再配置の起動契機と動作可能な条件 <<Bare metal>>」を参照して、ドライブデータ再配置が動作可能になるよう対処してください。
8. 減設処理内のボリュームマイグレーションによって移動されるすべてのボリュームについて、volumeType と status を確認します。

手順 2 で記録したストレージコントローラーのうち、減設対象のストレージノードの ID が `activeStorageNodeId` にあるストレージコントローラーの ID をクエリーパラメーターに指定してコマンドを実行します。

REST API : GET /v1/objects/volumes

CLI : `volume_list`

すべてのボリュームの `volumeType` が "Normal" であり、`status` が "Normal" のとき、次の手順に進みます。

条件を満たさないボリュームがある場合は、以下の対処を実施してください。

- `volumeType` が "Snapshot" の場合「スナップショットを削除する」を参照し、スナップショットボリュームを削除します。
- `status` が "Normal" 以外の場合「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ボリューム障害時の対処」を参照し対処してください。

9. ストレージプール情報の一覧とストレージコントローラー情報の一覧を取得して以下の条件を満たすかどうかを確認します。

(条件)

- ストレージプールの `numberOfVolumes` が 1,024 以下であること
- ストレージプールの `totalVolumeCapacity[MiB]` の値が 100TiB 以下であること
- ストレージプールの `usedCapacity[MiB]` より、ストレージコントローラーの `allocatableCapacity[MiB]` × 0.8 のほうが大きいストレージコントローラーが存在すること

(ストレージプール情報の一覧取得)

• REST API : GET /v1/objects/pools

• CLI : `pool_list`

(ストレージコントローラー情報の一覧取得)

• REST API : GET /v1/objects/storage_controllers

• CLI : `storage_controller_list`

上記の条件をすべて満たす場合は、手順 13 に進みます。

1 つでも条件を満たさない場合は、次の手順に進みます。

10. 減設するストレージノード上で動作するストレージコントローラーを特定します。

手順 2 で記録したストレージコントローラーのうち、減設対象のストレージノードの ID が `activeStorageNodeId` にあるストレージコントローラーを特定します。

11. 減設するストレージノード上で動作するストレージコントローラーのボリュームを、別のストレージコントローラーに移動できるかについて確認します。

移動先ストレージコントローラーとなる条件は以下(a~c)です。条件(a~c)を満たすストレージコントローラーが 1 つでもあれば、ストレージノードは減設できます。

- a. ストレージコントローラーの ID をクエリーパラメーターで指定してコマンドを実行し、以下を満たすかを確認します。またボリュームの ID を記録します。

ストレージコントローラーごとのボリューム数が 1,024 以下であること

• REST API : GET /v1/objects/volumes

• CLI : `volume_list`

- b. 上記で記録した ID のボリューム情報を取得し、以下を満たすかを確認します。

ストレージコントローラーごとのボリューム容量*の総和が 96.96TiB 以下であること

* ボリューム容量は、ボリューム情報の `reservedCapacity[MiB]` です。

- REST API : GET /v1/objects/volumes/<id >
 - CLI : volume_show
- c. ストレージコントローラー情報の一覧を取得し、以下を満たすかを確認します。
- ストレージコントローラーの usedCapacity[MiB]の総和が、ストレージコントローラーの allocatableCapacity[MiB] × 0.8 以下であること
- REST API : GET /v1/objects/storage_controllers
 - CLI : storage_controller_list
12. 手順 11 で行った条件の確認によって、ストレージノードの減設ができない場合は、以下のいずれかの対処を実施します。
- 「ドライブを増設する」を参照し、ドライブの増設とストレージプールの拡張をしてください。
 - 「ストレージノードの増設の準備と手順」を参照し、ストレージノードを増設してください。
 - 「ボリュームを削除する」を参照し、不要なボリュームを削除してください。
13. 以上、すべての手順を実施し、すべての条件を満たすことが確認できたら、ストレージノードの減設ができます。

12.1.2 ストレージノードを減設する《Bare metal》

この項での記述内容は Bare metal に適用されます。

ストレージノードを減設します。減設処理の間は、保守操作や構成変更はできません。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- 減設するストレージノードのコンピュータポート向けの I/O に対して、コンピュータノード側でマルチパス構成が組まれていない場合は、減設前に以下の情報を確認し、必要に応じてパス情報の追加・設定を実施してください。
 - コンピュータノードのパス情報
 - ボリュームとコンピュータノードの接続情報コンピュータノード側でマルチパス構成が組まれていないまま、ストレージノードの減設を実施したときは、ストレージノードの減設中または減設後の障害発生によって、I/O が停止するボリュームが出る可能性があります。
- ストレージノード減設契機のドライブデータ再配置が動作すると、ドライブデータ再配置の中断状態が解除されます。
- ストレージノード減設中はボリュームマイグレーションやドライブデータ再配置などが動き、I/O 性能に影響が出ることがあります。特にオンライントランザクション処理などの I/O サイズが小さい処理が影響を受けるため、これらの処理の実施が少ない時間帯を選んでストレージノード減設を実施することをお勧めします。
- ストレージノードの減設中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの減設が完了するのを待ってから再度これらの操作を実施してください。

前提条件

- 実行に必要なロール : Service
- 「ストレージノード減設の条件を確認する《Bare metal》」の条件を満たしていること

操作手順の留意事項

- script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておく、結果の確認やエラー発生時の対応に有効です。

操作手順

1. iSCSI 接続または NVMe/TCP 接続の場合、コンピュータノードとの接続を切断します。
コンピュータノードと減設対象のストレージノードとの接続状態を確認し、接続されている場合は、減設実施前に、利用している OS の切断手順に従って接続を切断してください。
上記の確認・操作をせずにストレージノードを減設してしまうと、コンピュータノードの OS によっては、接続情報がコンピュータノード側に残ってしまうことがあります。
2. ストレージノードを減設します。
減設するストレージノードの ID を指定してコマンドを実行します。
REST API : DELETE /v1/objects/storage-nodes/<id >
CLI : storage_node_delete
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
減設が完了するまでは、他の操作が実施できないことがあります。
4. ストレージノードの一覧を取得して、減設したストレージノードの ID がなくなったことを確認します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
5. ストレージノードの減設によって削除された管理ポートの情報を Subject Alternative Name(SAN)から削除したサーバー証明書、VSP One SDS Block にインポートしてください。
サーバー証明書のインポート手順は「運用管理を SSL/TLS 通信で行う」を参照してください。
6. 構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



メモ

ドライブデータ再配置の状態(driveDataRelocationStatus)が "Running"、"Error"、"Suspended" のときは構成バックアップは実行できません。
ドライブデータ再配置が正常に完了したことを確認してから構成バックアップを実行してください。ドライブデータ再配置の状態の確認方法は「ドライブデータ再配置の状態を確認する ≪Bare metal≫」を参照してください。



注意

以降の手順 7 でストレージノードの撤去を実施しますが、期待外に OS が起動すると、ストレージノードに残っているネットワーク設定によって、IP アドレス重複などのトラブルを引き起こす可能性があります。また、減設が完了したストレージノードに関連するイベントログや監査ログ

が出力される可能性があります。そのため、撤去するストレージノードに対し、以下を実施してください。

- ・ OS が期待外に起動しないような対処(システムディスクのデータの消去や使用していたシステムディスクをブート対象から外すなど)およびネットワークからの切り離しを行ってください。

7. 物理サーバーを撤去します。

ハードウェアベンダーのマニュアルを参照して実施してください。

8. マルチパスを再構築します。



注意

減設後に、減設されたストレージノード以外のコンピュートポート向けの I/O に対して、コンピュートノード側でマルチパス構成が組まれているかどうかを、以下の情報を取得して確認し、必要に応じてパス情報の追加・設定を実施してください。

- ・ コンピュートノードのパス情報
- ・ ボリュームとコンピュートノードの接続情報

マルチパス構成を組まない場合、ストレージノードの減設後に障害が発生すると、I/O が停止するボリュームが出る可能性があります。

12.2 ストレージノードの減設<<Cloud for AWS>>

この節での記述内容は Cloud モデル for AWS に適用されます。



注意

ストレージクラスターに組み込まれた、正常に動作中のストレージノードの減設はできません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。

ストレージノードの減設手順は以下のとおりです。

1. 「ストレージノード減設の条件を確認する<<Cloud for AWS>>」
2. 「ストレージノードを減設する<<Cloud for AWS>>」

ストレージノードの減設中のホスト I/O、ユーザーデータの冗長度、処理時間は以下のとおりです。

項目	説明
ホスト I/O	ストレージノードの減設中もホスト I/O は継続されます。マルチパス構成が組まれていることが前提になります。
ストレージコントローラー	1 つのストレージノードを減設すると、1 つのストレージコントローラーが削除されます。 ストレージノードの減設中、削除されるストレージコントローラーが管理するボリュームは、別のストレージコントローラーへと移動されます。 この処理をボリュームマイグレーションといいます。
ユーザーデータの冗長度	ストレージノードの減設中もユーザーデータの冗長度は維持されます。
処理時間	ストレージコントローラー間で移動するボリュームの容量に依存します。

処理時間は、以下の外部要因によって 処理時間が増加・減少することがあります。処理時間が増加する場合は、以下の項目に問題がないことを確認してください。

- ・ ネットワークの通信状況(ストレージノード間の通信状況)



注意

- ・ ストレージノードの減設時は、以下の処理の動作中に I/O 性能が不安定になる可能性があります。
 - ボリュームマイグレーション
- ・ ストレージノードの減設時には、ストレージコントローラーの再配置が動作するため、ホスト I/O 性能が 3 ～4 分程度低下する可能性があります。
- ・ ストレージノードの減設によって削除する管理ポートの情報を Subject Alternative Name(SAN)から削除したサーバー証明書を作成してください。
サーバー証明書の作成手順は「運用管理を SSL/TLS 通信で行う」を参照してください。

12.2.1 ストレージノード減設の条件を確認する ≪Cloud for AWS≫

この項での記述内容は Cloud モデル for AWS に適用されます。

ストレージノードが減設できるかどうかを以下の手順で確認してください。



注意

- ・ ストレージクラスターに組み込まれた、正常に動作中のストレージノードの減設はできません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。
- ・ イベントログ KARS06170-C が発行され、未対処だった場合は、ストレージノードの減設はできません。KARS06170-C を対処後にストレージノードの減設を実施してください。

前提条件

- ・ 実行に必要なロール : Security、Storage、Monitor、Service、または Resource

操作手順

1. ストレージノードの一覧を取得して、減設対象のストレージノードの ID を記録します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

2. ストレージコントローラーの一覧を取得して、以下を行います。

REST API : GET /v1/objects/storage-controllers

CLI : storage_controller_list

- a. すべてのストレージコントローラーの ID を記録します。
- b. 減設対象のストレージノードの ID が、activeStorageNodeId、standbyStorageNodeId、secondaryStandbyStorageNodeId のいずれかにあるストレージコントローラーの ID を記録します。

ただし、一度ストレージノード減設を実施して、中断または失敗したあとに同じストレージノードに対してストレージノード減設を再実施する場合(ストレージノードの status に "RemovalFailed" が付いている場合)は、減設対象のストレージノードにひもづくストレージコントローラーが存在しない可能性があります。その場合は、該当するストレージコントローラーはなしとして、以降の確認項目のうち、ストレージコントローラーに関連する項目は無視して先に進むようにしてください。

3. ストレージノードの一覧を取得して、減設対象のストレージノードが減設できるかどうかを、以下に従って確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

- ・ 減設対象のストレージノードの clusterRole が "Worker" であること
クラスターマスターノードの減設はできません。そのため、clusterRole が "Master" のストレージノードは減設できません。

- 減設対象のストレージノードの status が "Ready"、"RemovalFailed"、"RemovalFailedAndStopping"、"RemovalFailedAndStopped" のいずれかの値であること
減設対象のストレージノードが、これら以外の status になっている場合、以下に従って対処してください。
 - VSP One SDS Block Administrator でストレージノードの Health Status に "Alerting" が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
ただし、減設対象のストレージノードが、"RemovalFailed"、"RemovalFailedAndStopping"、"RemovalFailedAndStopped" となっている場合も "Alerting" になりますが、その場合は問題ありません。
 - status が "MaintenanceBlockage" となっている場合は「ストレージノードを保守回復する <<Cloud for AWS>>」に従って、ストレージノードを保守回復してください。
 - 上記以外の場合は、ストレージノードに対する処理が実施中のため、status が変わるまで待ってから、再度確認してください。
- ストレージノード減設後のストレージノード数が、次に示すノード数以上であること

ユーザーデータの保護種別 (redundantType)	減設後のストレージノード数
4D+2P	6
Duplication	3*
* Multi-AZ 構成の場合、タイプレーカーノードを含みます。	

すべてが確認できたら、次の手順に進みます。

- ストレージプールの一覧を取得し、ユーザーデータの冗長度が低下していないことを dataRedundancy で確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

次の表に従って冗長度を確認します。冗長度が低下していなければ手順 7 に進みます。冗長度が低下している場合は次の手順に進みます。

ユーザーデータの保護種別 (redundantType)	dataRedundancy の値	冗長度
Duplication	1	冗長度が低下していません。
	1 未満	冗長度が低下しています。
4D+2P	2	冗長度が低下していません。
	2 未満	冗長度が低下しています。

- ストレージクラスター内のすべてのストレージノードに関して、以下のいずれかに該当する場合はそれぞれ以下の対処を行います。いずれにも該当しない場合は手順 6 に進みます。
 - VSP One SDS Block Administrator でストレージノードの Health Status に "Alerting" が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
ただし、減設対象のストレージノードが、"RemovalFailed"、"RemovalFailedAndStopping"、"RemovalFailedAndStopped" となっている場合も "Alerting" になりますが、その場合は問題ありません。

- status が "MaintenanceBlockage" のストレージノードがある場合は「ストレージノードを保守回復する <<Cloud for AWS>>」に従って、ストレージノードを保守回復してください。
6. 「リビルドの状態を確認する」を参照して、リビルドが動作中でないこと、およびリビルドでエラーが発生していないことを確認します。
- リビルドが動作中でなく、かつエラーが発生していない場合は、次の手順に進みます。
- リビルドが動作中、またはリビルドでエラーが発生している場合は「リビルドの状態を確認する」を参照して対処してください。
7. 以上、すべての手順を実施し、すべての条件を満たすことが確認できたら、ストレージノードの減設ができます。

12.2.2 ストレージノードを減設する <<Cloud for AWS>>

この項での記述内容は Cloud モデル for AWS に適用されます。

ストレージノードを減設します。減設処理の間は、保守操作や構成変更はできません。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- 減設するストレージノードのコンピュータポート向けの I/O に対して、コンピュータノード側でマルチパス構成が組まれていない場合は、減設前に以下の情報を確認し、必要に応じてパス情報の追加・設定を実施してください。
 - コンピュータノードのパス情報
 - ボリュームとコンピュータノードの接続情報コンピュータノード側でマルチパス構成が組まれていないまま、ストレージノードの減設を実施したときは、ストレージノードの減設中または減設後の障害発生によって、I/O が停止するボリュームが出る可能性があります。
- ストレージノード減設中はボリュームマイグレーションなどが動き、I/O 性能に影響が出る場合があります。特にオンライントランザクション処理などの I/O サイズが小さい処理が影響を受けるため、これらの処理の実施が少ない時間帯を選んでストレージノード減設を実施することをお勧めします。
- ストレージノードの減設中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの減設が完了するのを待ってから再度これらの操作を実施してください。
- EBS 暗号化を利用している場合は、AWS を操作するアカウントやコントローラーノードに設定する IAM ロールに、AWS Key Management Service へアクセスするための権限を追加する必要があります。詳細は、AWS のユーザーガイドを参照してください。

前提条件

- 実行に必要なロール : Service
- 「ストレージノード減設の条件を確認する <<Cloud for AWS>>」の条件を満たしていること

操作手順の留意事項

- 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。¥記号を含めてコピーアンドペーストしても正しく動作します。
- 本手順では AWS CLI を使用して実施していますが、CloudFormation のスタックのステータスや動作状況は AWS マネジメントコンソールの AWS CloudFormation コンソールからも確認できます。

- script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておく、結果の確認やエラー発生時の対応に有効です。

操作手順

1. コンピュートノードとの接続を切断します。
コンピュートノードと減設対象のストレージノードとの接続状態を確認し、接続されている場合は、減設実施前に、利用している OS の切断手順に従って接続を切断してください。
上記の確認・操作をせずにストレージノードを減設してしまうと、コンピュートノードの OS によっては、接続情報がコンピュートノード側に残ってしまうことがあります。
2. ストレージノードを減設します。
減設するストレージノードの ID を指定してコマンドを実行します。
REST API : DELETE /v1/objects/storage-nodes/<id >
CLI : storage_node_delete
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
減設が完了するまでは、他の操作が実施できないことがあります。
4. ストレージノードの一覧を取得して、減設したストレージノードの ID がなくなったことを確認します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
5. ストレージノードの減設によって削除された管理ポートの情報を Subject Alternative Name(SAN)から削除したサーバー証明書、VSP One SDS Block にインポートしてください。
サーバー証明書のインポート手順は「運用管理を SSL/TLS 通信で行う」を参照してください。



注意

以降の手順 7 でストレージノードの撤去を実施しますが、期待外に OS が起動すると、ストレージノードに残っているネットワーク設定によって、IP アドレス重複などのトラブルを引き起こす可能性があります。また、減設が完了したストレージノードに関連するイベントログや監査ログが出力される可能性があります。そのため、撤去するストレージノードに対し、以下を実施してください。

- VM の削除を確実に行ってください。

6. 構成情報のバックアップを行います。
「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
7. 以下の後処理を行います。
ただし、増設失敗後に構成に残ってしまったストレージノードに対して減設を実施しており、かつ構成に残ってしまったストレージノードが複数ある場合は、増設に失敗したすべてのストレージノードの減設を実施後に本手順を実施してください。
 - a. 「構成ファイルをエクスポートする <<Cloud for AWS>>」を実施し、VSP One SDS Block から構成に入っていないストレージノードを削除するための構成ファイルを取得します。

構成ファイルをエクスポートする際は、`exportFileType` パラメーターを省略するか、`Normal` を指定してください。

最新状態の構成ファイルを使用するために、必ず取得してください。

- b. 手順 a で準備した VM 構成ファイルを使用して、AWS 上のリソースを削除します。

1. 構成ファイルのエクスポートで取得した構成ファイル一式を手順 a で `templateS3Url` パラメーターで指定した Amazon S3 バケットに格納します。Amazon S3 にファイルを格納する方法として、例えば AWS CLI を用いて Amazon S3 にファイルをコピーする方法があります。詳細は Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「Amazon S3 の操作例」を参照してください。



注意

VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。

2. 次の AWS CLI を実行して、変更セットを作成します。その際、ストレージノードの終了保護を無効にします。

```
aws cloudformation create-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <任意の変更セット名*> ¥
--template-url ¥
<Amazon S3 に格納した VMConfigurationFile.yml の URL(https)> ¥
--include-nested-stacks ¥
--capabilities CAPABILITY_NAMED_IAM ¥
--parameters ParameterKey= ¥
'DisableNodeTerminationProtection',ParameterValue=ALL ¥
ParameterKey='ConfigurationPattern',UsePreviousValue=true
```

* 使用可能文字などは以下の Web サイトを参照してください。

<https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-change-set.html>

3. 次の AWS CLI を実行して、変更セットを表示します(1 階層目)。

```
aws cloudformation describe-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 b-2 で指定した変更セット名>
```

以下の事項を確認します。

- "Status"が"CREATE_COMPLETE"であること
"Status"が"CREATE_IN_PROGRESS"の場合はしばらく待ってから再度実行してください。
- "Changes"の項目数が 1 つであること
- "Changes"内の"ResourceChange"について
"Action"が"Modify"であること
次の手順のため、"ChangeSetId"の値を記録します。

4. 次の AWS CLI を実行して、変更セットを表示します(2 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 b-3 で記録した"ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
"Action"が"Modify"であること
次の手順のため、各項目の"ChangeSetId"の値を記録します。

5. 次の AWS CLI を実行して、変更セットを表示します(3 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 b-4 で記録した"ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
"Action"が"Modify"であること

6. 次の AWS CLI を実行して、作成した変更セットを実行します。

```
aws cloudformation execute-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 b-2 で指定した変更セット名>
```

7. 次の AWS CLI を実行して、変更セットの実行結果を確認します。

`wait stack-update-complete` を実行すると、変更セットの実行が完了するまで待つことができます。

```
aws cloudformation wait stack-update-complete ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

実行が完了したら、`describe-stacks` を実行し、`StackStatus` が"UPDATE_COMPLETE"であることを確認してください。

```
aws cloudformation describe-stacks ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

8. 次の AWS CLI を実行して、変更セットを作成します。

```
aws cloudformation create-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <任意の変更セット名*> ¥
--use-previous-template ¥
--include-nested-stacks ¥
--capabilities CAPABILITY_NAMED_IAM
```

* 使用可能文字などは以下の Web サイトを参照してください。

<https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-change-set.html>

9. 次の AWS CLI を実行して、変更セットを表示します(1 階層目)。

```
aws cloudformation describe-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 b-8 で指定した変更セット名>
```

以下の事項を確認します。

- "Status"が"CREATE_COMPLETE"であること
"Status"が"CREATE_IN_PROGRESS"の場合はしばらく待ってから再度実行してください。
- "Changes"の項目数が 1 つであること
- "Changes"内の"ResourceChange"について

"Action"が"Modify"であること

次の手順のため、"ChangeSetId"の値を記録します。

10. 次の AWS CLI を実行して、変更セットを表示します(2 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 b-9 で記録した"ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
"Action"が"Remove"である項目の"LogicalResourceId"が"StorageNodeXX"または
"SpGYY"であること(XX は削除するストレージノードの番号、YY は削除するストレ
ージノードが属するスプレッドブレイスメントグループの番号)
次の手順のため、各項目の"ChangeSetId"の値を記録します。
- 上記以外の"Changes"内の各項目の"ResourceChange"について
"Action"がすべて"Modify"であること

11. 次の AWS CLI を実行して、変更セットを表示します(3 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 b-10 で記録した"ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
"Action"が"Modify"であること

12. 次の AWS CLI を実行して、作成した変更セットを実行します。

```
aws cloudformation execute-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 b-8 で指定した変更セット名>
```

13. 次の AWS CLI を実行して、変更セットの実行結果を確認します。

wait stack-update-complete を実行すると、変更セットの実行が完了するまで待つことが
できます。

```
aws cloudformation wait stack-update-complete ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

実行が完了したら、describe-stacks を実行し、StackStatus が"UPDATE_COMPLETE"
であることを確認してください。

```
aws cloudformation describe-stacks ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

8. マルチパスを再構築します。



注意

減設後に、減設されたストレージノード以外のコンピュートポート向けの I/O に対して、コンピ
ュートノード側でマルチパス構成が組まれているかどうかを、以下の情報を取得して確認し、必
要に応じてパス情報の追加・設定を実施してください。

- コンピュートノードのパス情報
- ボリュームとコンピュートノードの接続情報

マルチパス構成を組まない場合、ストレージノードの減設後に障害が発生すると、I/O が停止する
ボリュームが出る可能性があります。

12.3 ストレージノードの減設<<Cloud for Google Cloud>>

この節での記述内容は Cloud モデル for Google Cloud に適用されます。



注意

ストレージクラスターに組み込まれた、正常に動作中のストレージノードの減設はできません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。

ストレージノードの減設手順は以下のとおりです。

1. 「ストレージノード減設の条件を確認する<<Cloud for Google Cloud>>」
2. 「ストレージノードを減設する<<Cloud for Google Cloud>>」

ストレージノードの減設中のホスト I/O、ユーザーデータの冗長度、処理時間は以下のとおりです。

項目	説明
ホスト I/O	ストレージノードの減設中もホスト I/O は継続されます。マルチパス構成が組まれていることが前提になります。
ストレージコントローラー	1 つのストレージノードを減設すると、1 つのストレージコントローラーが削除されます。 ストレージノードの減設中、削除されるストレージコントローラーが管理するボリュームは、別のストレージコントローラーへと移動されます。この処理をボリュームマイグレーションといいます。
ユーザーデータの冗長度	ストレージノードの減設中もユーザーデータの冗長度は維持されます。
処理時間	ストレージコントローラー間で移動するボリュームの容量に依存します。

処理時間は、以下の外部要因によって 処理時間が増加・減少することがあります。処理時間が増加する場合は、以下の項目に問題がないことを確認してください。

- ・ ネットワークの通信状況(ストレージノード間の通信状況)



注意

- ・ ストレージノードの減設時は、以下の処理の動作中に I/O 性能が不安定になる可能性があります。
 - ボリュームマイグレーション
- ・ ストレージノードの減設時には、ストレージコントローラーの再配置が動作するため、ホスト I/O 性能が 3 ～4 分程度低下する可能性があります。
- ・ ストレージノードの減設によって削除する管理ポートの情報を Subject Alternative Name(SAN)から削除したサーバー証明書を作成してください。
サーバー証明書の作成手順は「運用管理を SSL/TLS 通信で行う」を参照してください。

12.3.1 ストレージノード減設の条件を確認する<<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージノードが減設できるかどうかを以下の手順で確認してください。



注意

- ・ ストレージクラスターに組み込まれた、正常に動作中のストレージノードの減設はできません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。

- ・ イベントログ KARS06170-C が発行され、未対処だった場合は、ストレージノードの減設はできません。KARS06170-C を対処後にストレージノードの減設を実施してください。
-

前提条件

- ・ 実行に必要なロール : Security、Storage、Monitor、Service、または Resource

操作手順

1. ストレージノードの一覧を取得して、減設対象のストレージノードの ID を記録します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

2. ストレージコントローラーの一覧を取得して、以下を行います。

REST API : GET /v1/objects/storage-controllers

CLI : storage_controller_list

- a. すべてのストレージコントローラーの ID を記録します。
- b. 減設対象のストレージノードの ID が、activeStorageNodeId、standbyStorageNodeId、secondaryStandbyStorageNodeId のいずれかにあるストレージコントローラーの ID を記録します。

ただし、一度ストレージノード減設を実施して、中断または失敗したあとに同じストレージノードに対してストレージノード減設を再実施する場合(ストレージノードの status に "RemovalFailed" が付いている場合)は、減設対象のストレージノードにひもづくストレージコントローラーが存在しない可能性があります。その場合は、該当するストレージコントローラーはなしとして、以降の確認項目のうち、ストレージコントローラーに関連する項目は無視して先に進むようにしてください。

3. ストレージノードの一覧を取得して、減設対象のストレージノードが減設できるかどうかを、以下に従って確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

- ・ 減設対象のストレージノードの clusterRole が "Worker" であること
クラスターマスターノードの減設はできません。そのため、clusterRole が "Master" のストレージノードは減設できません。
- ・ 減設対象のストレージノードの status が "Ready"、"RemovalFailed"、"RemovalFailedAndStopping"、"RemovalFailedAndStopped" のいずれかの値であること
減設対象のストレージノードが、これら以外の status になっている場合、以下に従って対処してください。
 - VSP One SDS Block Administrator でストレージノードの Health Status に "Alerting" が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
ただし、減設対象のストレージノードが、"RemovalFailed"、"RemovalFailedAndStopping"、"RemovalFailedAndStopped" となっている場合も "Alerting" になりますが、その場合は問題ありません。
 - status が "MaintenanceBlockage" となっている場合は「ストレージノードを保守回復する <<Cloud for Google Cloud>>」に従って、ストレージノードを保守回復してください。
 - 上記以外の場合は、ストレージノードに対する処理が実施中のため、status が変わるまで待ってから、再度確認してください。
- ・ ストレージノード減設後のストレージノード数が、次に示すノード数以上であること

ユーザーデータの保護種別 (redundantType)	減設後のストレージノード数
4D+2P	6
Duplication	3*
* Multi-AZ (Multi-Zone)構成の場合、タイブレーカーノードを含みます。	

すべてが確認できたら、次の手順に進みます。

4. ストレージプールの一覧を取得し、ユーザーデータの冗長度が低下していないことを dataRedundancy で確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

次の表に従って冗長度を確認します。冗長度が低下していなければ手順 7 に進みます。冗長度が低下している場合は次の手順に進みます。

ユーザーデータの保護種別 (redundantType)	dataRedundancy の値	冗長度
Duplication	1	冗長度が低下していません。
	1 未満	冗長度が低下しています。
4D+2P	2	冗長度が低下していません。
	2 未満	冗長度が低下しています。

5. ストレージクラスター内のすべてのストレージノードに関して、以下のいずれかに該当する場合はそれぞれ以下の対処を行います。いずれにも該当しない場合は手順 6 に進みます。
 - VSP One SDS Block Administrator でストレージノードの Health Status に"Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
ただし、減設対象のストレージノードが、"RemovalFailed"、
"RemovalFailedAndStopping"、"RemovalFailedAndStopped"となっている場合も
"Alerting"になりますが、その場合は問題ありません。
 - status が"MaintenanceBlockage"のストレージノードがある場合は「ストレージノードを保守回復する<<Cloud for Google Cloud>>」に従って、ストレージノードを保守回復してください。
6. 「リビルドの状態を確認する」を参照して、リビルドが動作中でないこと、およびリビルドでエラーが発生していないことを確認します。
リビルドが動作中でなく、かつエラーが発生していない場合は、次の手順に進みます。
リビルドが動作中、またはリビルドでエラーが発生している場合は「リビルドの状態を確認する」を参照して対処してください。
7. 以上、すべての手順を実施し、すべての条件を満たすことが確認できたら、ストレージノードの減設ができます。

12.3.2 ストレージノードを減設する<<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージノードを減設します。減設処理の間は、保守操作や構成変更はできません。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- 減設するストレージノードのコンピュータポート向けの I/O に対して、コンピュータノード側でマルチパス構成が組まれていない場合は、減設前に以下の情報を確認し、必要に応じてパス情報の追加・設定を実施してください。
 - コンピュータノードのパス情報
 - ボリュームとコンピュータノードの接続情報コンピュータノード側でマルチパス構成が組まれていないまま、ストレージノードの減設を実施したときは、ストレージノードの減設中または減設後の障害発生によって、I/O が停止するボリュームが出る可能性があります。
- ストレージノード減設中はボリュームマイグレーションなどが動き、I/O 性能に影響が出る場合があります。特にオンライントランザクション処理などの I/O サイズが小さい処理が影響を受けるため、これらの処理の実施が少ない時間帯を選んでストレージノード減設を実施することをお勧めします。
- ストレージノードの減設中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの減設が完了するのを待ってから再度これらの操作を実施してください。

前提条件

- 実行に必要なロール : Service
- 「ストレージノード減設の条件を確認する <<Cloud for Google Cloud>>」の条件を満たしていること

操作手順の留意事項

- gcloud CLI と Terraform は実行可能な環境から実行してください。
- 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。
- script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておくと、結果の確認やエラー発生時の対応に有効です。

操作手順

1. コンピュータノードとの接続を切断します。
コンピュータノードと減設対象のストレージノードとの接続状態を確認し、接続されている場合は、減設実施前に、利用している OS の切断手順に従って接続を切断してください。
上記の確認・操作をせずにストレージノードを減設してしまうと、コンピュータノードの OS によっては、接続情報がコンピュータノード側に残ってしまうことがあります。
2. ストレージノードを減設します。
減設するストレージノードの ID を指定してコマンドを実行します。
REST API : DELETE /v1/objects/storage-nodes/<id >
CLI : storage_node_delete
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。

減設が完了するまでは、他の操作が実施できないことがあります。

4. ストレージノードの一覧を取得して、減設したストレージノードの ID がなくなったことを確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

5. ストレージノードの減設によって削除された管理ポートの情報を Subject Alternative Name(SAN)から削除したサーバー証明書を、VSP One SDS Block にインポートしてください。
サーバー証明書のインポート手順は「運用管理を SSL/TLS 通信で行う」を参照してください。

6. ストレージノードのクラウドリソースを削除します。

ただし、ストレージノード増設失敗後に構成に残ってしまったストレージノードに対して減設を実施している場合は、増設に失敗したすべてのストレージノードの減設を実施後に本手順を実施してください。

- a. 「構成ファイルをエクスポートする<<Cloud for Google Cloud>>」を参照し、VSP One SDS Block から構成に入っていないストレージノードを削除するための構成ファイルを取得します。

構成ファイルをエクスポートする際は、exportFileType パラメーターを省略するか、Normal を指定してください。

最新状態の構成ファイルを使用するために必ず取得してください。

- b. 「VM 構成ファイルの Terraform の作業ディレクトリーへ配置する<<Cloud for Google Cloud>>」を参照し、構成ファイルを解凍して配置します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、ストレージクラスターが閉塞するなどの事態が起こるおそれがあります。

- c. 構成に入っていないストレージノードを削除するための構成ファイルをデプロイすることによる影響を確認します。

以下のコマンドを実行します。

```
terraform plan
```

コマンドを実行すると[Terraform will perform the following actions]という表示のあとにリソースに対する変更内容が表示されます。

以下のリソースの変更が実施されることを確認してください。

#	リソース種別	リソース操作	リソース名 ¹	確認内容
1	google_compute_disk.user_disks[]	delete	<clusterName>-snXX-userdatadiskYY	リソースが「同時に削除するストレージノードの台数 ² × 1 ノード当たりのドライブの台数」の数だけ削除されること
2	google_compute_attached_disk.attached_user_disk[]	delete	-	リソースが「同時に削除するストレージノードの台数 ² × 1 ノード当たりのドライブの台数」の数だけ削除されること
3	google_compute_instance.instance[]	delete	<clusterName>-snXX	・ リソースが「同時に削除するストレージノードの台数 ² 」の数だけ削除されること

#	リソース種別	リソース操作	リソース名 ¹	確認内容
				リソース名の XX がストレージクラスターに存在するストレージノードの次の番号から始まること
4	google_compute_instance[]	update in-place	<clusterName>-snXX	以下の項目に変更がある場合がありますが、問題ありません。 - metadata - deletion_protection
5	google_compute_resource_policy.spp[]	delete	<clusterName>-resource-policyZZ	Single-AZ (Single-Zone)構成 ³ か Multi-AZ (Multi-Zone)構成 ⁴ かの場合で異なります。

1. リソース名の XX、YY、ZZ はそれぞれ以下を示します。

XX：ストレージノードに割り振られている番号。番号は 2 桁の整数で、構築した順番に 01 から番号が付けられます。

YY：各ストレージノードのユーザードライブに割り振られている番号。

ZZ：スプレッドプレースメントポリシーごとに割り振られている番号。

2. 同時に削除するストレージノードの台数は以下です。

- Single-AZ (Single-Zone)構成でデータ保護方式が Duplication の場合：3
- Single-AZ (Single-Zone)構成でデータ保護方式が 4D+2P の場合：6
- Multi-AZ (Multi-Zone)構成でデータ保護方式が Duplication の場合：2

3. Single-AZ (Single-Zone)構成の場合、以下の内容を確認してください。

- リソースが 1 個削除されること
- 削除されるストレージノードの番号 XX(#3 における XX)とリソース名の ZZ の組み合わせが、以下のいずれかであること。組み合わせは{XX,YY}で表しています。
 - データ保護方式が Duplication の場合：{01-03,01},{04-06,02},{07-09,03},{10-12,04},{13-15,05},{16-18,06}
 - データ保護方式が 4D+2P の場合：{01-06,01},{07-12,02},{13-18,03}

4. Multi-AZ (Multi-Zone)構成の場合、以下の内容を確認してください。

- リソースが以下の個数削除されること
 - ストレージノードの番号 XX(#3 における XX)が 16 または 17 の場合：2 個
 - ストレージノードの番号 XX(#3 における XX)が 16 でも 17 でもない場合：0 個
- リソースが 2 個削除される場合、リソース名の ZZ が 03 と 04 であること

- d. terraform plan による確認で問題がなければ、手順 c で削除されることを確認したすべてのストレージノード VM(Compute Engine インスタンス)の削除保護を解除します。

削除する Compute Engine インスタンスの数だけ、Compute Engine インスタンスの名前を変えて、以下のコマンドを実行します。

```
gcloud compute instances update <clusterName>-sn<XX> ¥
--zone <Zone> --no-deletion-protection
```

ただし、<clusterName>-sn<XX>は Compute Engine インスタンスの名前で、<clusterName>はクラスター名を、<XX>は手順 c で削除されることを確認したいいずれかの Compute Engine インスタンスの番号を指定します。

- e. ストレージノードのリソースを変更するため、以下のコマンドを実行します。

```
terraform apply
```

コマンドの実行後、[Enter a value:]と表示されたら[yes]を入力します。

入力すると最後に[Outputs]が出力されます。terraform apply が完了することで、クラウドリソースの変更が完了します。

- f. コンピュートポートの通信プロトコルとして IPv6 を併用している(デュアルスタックの)場合、削除したストレージノードで使用していた静的内部 IPv6 アドレスの予約を解除します。

```
gcloud compute addresses delete <clusterName>-sn<XX>-compute-ipv6 ¥  
--region <region>
```

ただし、<clusterName>はクラスター名を、<XX>は手順 e で削除したいいずれかの Compute Engine インスタンスの番号を指定します。

コマンドの実行後、[Do you want to continue (Y/n)?]と表示されたら、[Y]を入力します。入力すると、静的 IPv6 アドレスの予約が解除されます。

この手順を、削除したストレージノードの台数分だけ繰り返し実施します。



メモ

gcloud compute addresses delete コマンドでは、静的内部 IPv6 アドレス名をスペース区切りで指定することで、複数の静的内部 IPv6 アドレスの予約を同時に解除することができます。

7. マルチパスを再構築します。



注意

減設後に、減設されたストレージノード以外のコンピュートポート向けの I/O に対して、コンピュートノード側でマルチパス構成が組まれているかどうかを、以下の情報を取得して確認し、必要に応じてパス情報の追加・設定を実施してください。

- ・ コンピュートノードのパス情報
- ・ ボリュームとコンピュートノードの接続情報

マルチパス構成を組まない場合、ストレージノードの減設後に障害が発生すると、I/O が停止するボリュームが出る可能性があります。

12.4 ストレージノードの減設<<Cloud for Microsoft Azure>>

この節での記述内容は Cloud モデル for Microsoft Azure に適用されます。



注意

- ・ ストレージクラスターに組み込まれた、正常に動作中のストレージノードの減設はできません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。
- ・ ストレージノード減設実施後、不要なリソースを必ず削除してください。不要なリソースが残ったままだと、Microsoft Azure に課金され続けるおそれがあります。

不要なリソースの削除については、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block の構成情報に存在しないストレージノードの VM(Azure VM インスタンス)を削除する手順<<Cloud for Microsoft Azure>>」を参照してください。

ストレージノードの減設手順は以下のとおりです。

1. 「ストレージノード減設の条件を確認する<<Cloud for Microsoft Azure>>」
2. 「ストレージノードを減設する<<Cloud for Microsoft Azure>>」

ストレージノードの減設中のホスト I/O、ユーザーデータの冗長度、処理時間は以下のとおりです。

項目	説明
ホスト I/O	ストレージノードの減設中もホスト I/O は継続されます。マルチパス構成が組まれていることが前提になります。
ストレージコントローラー	1 つのストレージノードを減設すると、1 つのストレージコントローラーが削除されます。 ストレージノードの減設中、削除されるストレージコントローラーが管理するボリュームは、別のストレージコントローラーへと移動されます。この処理をボリュームマイグレーションといいます。
ユーザーデータの冗長度	ストレージノードの減設中もユーザーデータの冗長度は維持されます。
処理時間	ストレージコントローラー間で移動するボリュームの容量に依存します。

処理時間は、以下の外部要因によって 処理時間が増加・減少することがあります。処理時間が増加する場合は、以下の項目に問題がないことを確認してください。

- ・ ネットワークの通信状況(ストレージノード間の通信状況)



注意

- ・ ストレージノードの減設時は、以下の処理の動作中に I/O 性能が不安定になる可能性があります。
 - ボリュームマイグレーション
- ・ ストレージノードの減設時には、ストレージコントローラーの再配置が動作するため、ホスト I/O 性能が 3 ～4 分程度低下する可能性があります。
- ・ ストレージノードの減設によって削除する管理ポートの情報を Subject Alternative Name(SAN)から削除したサーバー証明書を作成してください。
サーバー証明書の作成手順は「運用管理を SSL/TLS 通信で行う」を参照してください。

12.4.1 ストレージノード減設の条件を確認する ≪Cloud for Microsoft Azure≫

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージノードが減設できるかどうかを以下の手順で確認してください。



注意

- ・ ストレージクラスターに組み込まれた、正常に動作中のストレージノードの減設はできません。ただし、増設失敗後に構成に残ってしまったストレージノードは減設できます。
- ・ ストレージノード減設実施後、不要なリソースを必ず削除してください。不要なリソースが残ったままだと、Microsoft Azure に課金され続けるおそれがあります。
不要なリソースの削除については、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block の構成情報に存在しないストレージノードの VM(Azure VM インスタンス)を削除する手順 ≪Cloud for Microsoft Azure≫」を参照してください。
- ・ イベントログ KARS06170-C が発行され、未対処だった場合は、ストレージノードの減設はできません。
KARS06170-C を対処後にストレージノードの減設を実施してください。

前提条件

- ・ 実行に必要なロール : Security、Storage、Monitor、Service、または Resource

操作手順

1. ストレージノードの一覧を取得して、減設対象のストレージノードの ID を記録します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

2. ストレージコントローラーの一覧を取得して、以下を行います。

REST API : GET /v1/objects/storage-controllers

CLI : storage_controller_list

- a. すべてのストレージコントローラーの ID を記録します。
- b. 減設対象のストレージノードの ID が、activeStorageNodeId、standbyStorageNodeId、secondaryStandbyStorageNodeId のいずれかにあるストレージコントローラーの ID を記録します。

ただし、一度ストレージノード減設を実施して、中断または失敗したあとに同じストレージノードに対してストレージノード減設を再実施する場合(ストレージノードの status に "RemovalFailed" が付いている場合は、減設対象のストレージノードにひもづくストレージコントローラーが存在しない可能性があります。その場合は、該当するストレージコントローラーはなしとして、以降の確認項目のうち、ストレージコントローラーに関連する項目は無視して先に進むようにしてください。

3. ストレージノードの一覧を取得して、減設対象のストレージノードが減設できるかどうかを、以下に従って確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

- ・ 減設対象のストレージノードの clusterRole が "Worker" であること
クラスターマスターノードの減設はできません。そのため、clusterRole が "Master" のストレージノードは減設できません。
- ・ 減設対象のストレージノードの status が "Ready"、"RemovalFailed"、"RemovalFailedAndStopping"、"RemovalFailedAndStopped" のいずれかの値であること
減設対象のストレージノードが、これら以外の status になっている場合、以下に従って対処してください。
 - VSP One SDS Block Administrator でストレージノードの Health Status に "Alerting" が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
ただし、減設対象のストレージノードが、"RemovalFailed"、"RemovalFailedAndStopping"、"RemovalFailedAndStopped" となっている場合も "Alerting" になりますが、その場合は問題ありません。
 - status が "MaintenanceBlockage" となっている場合は「ストレージノードを保守回復する <<Cloud for Microsoft Azure>>」に従って、ストレージノードを保守回復してください。
 - 上記以外の場合は、ストレージノードに対する処理が実施中のため、status が変わるまで待つてから、再度確認してください。
- ・ ストレージノード減設後のストレージノード数が、次に示すノード数以上であること

ユーザーデータの保護種別 (redundantType)	減設後のストレージノード数
4D+2P	6
Duplication	3*

ユーザーデータの保護種別 (redundantType)	減設後のストレージノード数
* Multi-AZ 構成の場合、タイプレカーノードを含みます。	

すべてが確認できたら、次の手順に進みます。

4. ストレージプールの一覧を取得し、ユーザーデータの冗長度が低下していないことを dataRedundancy で確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

次の表に従って冗長度を確認します。冗長度が低下していなければ手順 7 に進みます。冗長度が低下している場合は次の手順に進みます。

ユーザーデータの保護種別 (redundantType)	dataRedundancy の値	冗長度
Duplication	1	冗長度が低下していません。
	1 未満	冗長度が低下しています。
4D+2P	2	冗長度が低下していません。
	2 未満	冗長度が低下しています。

5. ストレージクラスター内のすべてのストレージノードに関して、以下のいずれかに該当する場合はそれぞれ以下の対処を行います。いずれにも該当しない場合は手順 6 に進みます。
 - ・ VSP One SDS Block Administrator でストレージノードの Health Status に "Alerting" が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
ただし、減設対象のストレージノードが、"RemovalFailed"、
"RemovalFailedAndStopping"、"RemovalFailedAndStopped" となっている場合も
"Alerting" になりますが、その場合は問題ありません。
 - ・ status が "MaintenanceBlockage" のストレージノードがある場合は「ストレージノードを保守回復する <<Cloud for Microsoft Azure>>」に従って、ストレージノードを保守回復してください。
6. 「リビルドの状態を確認する」を参照して、リビルドが動作中でないこと、およびリビルドでエラーが発生していないことを確認します。
リビルドが動作中でなく、かつエラーが発生していない場合は、次の手順に進みます。
リビルドが動作中、またはリビルドでエラーが発生している場合は「リビルドの状態を確認する」を参照して対処してください。
7. 以上、すべての手順を実施し、すべての条件を満たすことが確認できたら、ストレージノードの減設ができます。

12.4.2 ストレージノードを減設する <<Cloud for Microsoft Azure>>

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージノードを減設します。減設処理の間は、保守操作や構成変更はできません。



注意

- ・ 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イ

ベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。

- 減設するストレージノードのコンピュータポート向けの I/O に対して、コンピュータノード側でマルチパス構成が組まれていない場合は、減設前に以下の情報を確認し、必要に応じてパス情報の追加・設定を実施してください。
 - コンピュータノードのパス情報
 - ボリュームとコンピュータノードの接続情報コンピュータノード側でマルチパス構成が組まれていないまま、ストレージノードの減設を実施したときは、ストレージノードの減設中または減設後の障害発生によって、I/O が停止するボリュームが出る可能性があります。
- ストレージノード減設中はボリュームマイグレーションなどが動き、I/O 性能に影響が出る場合があります。特にオンライントランザクション処理などの I/O サイズが小さい処理が影響を受けるため、これらの処理の実施が少ない時間帯を選んでストレージノード減設を実施することをお勧めします。
- ストレージノードの減設中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの減設が完了するのを待ってから再度これらの操作を実施してください。

前提条件

- 実行に必要なロール：Service
- 「ストレージノード減設の条件を確認する<<Cloud for Microsoft Azure>>」の条件を満たしていること

操作手順の留意事項

- script コマンドや、リダイレクト、tee コマンドなどを利用してコンソールの出力を記録しておくと、結果の確認やエラー発生時の対応に有効です。

操作手順

- コンピュータノードとの接続を切断します。
コンピュータノードと減設対象のストレージノードとの接続状態を確認し、接続されている場合は、減設実施前に、利用している OS の切断手順に従って接続を切断してください。
上記の確認・操作をせずにストレージノードを減設してしまうと、コンピュータノードの OS によっては、接続情報がコンピュータノード側に残ってしまうことがあります。
- ストレージノードを減設します。
減設するストレージノードの ID を指定してコマンドを実行します。
REST API : DELETE /v1/objects/storage-nodes/<id >
CLI : storage_node_delete
コマンド実行後に表示されるジョブの ID を確認します。
- ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
減設が完了するまでは、他の操作が実施できないことがあります。
- ストレージノードの一覧を取得して、減設したストレージノードの ID がなくなったことを確認します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list

5. ストレージノードの減設によって削除された管理ポートの情報を **Subject Alternative Name(SAN)**から削除したサーバー証明書、**VSP One SDS Block** にインポートしてください。
サーバー証明書のインポート手順は「運用管理を **SSL/TLS 通信**で行う」を参照してください。
6. 以下の後処理を行います。
ただし、増設失敗後に構成に残ってしまったストレージノードに対して減設を実施しており、かつ構成に残ってしまったストレージノードが複数ある場合は、増設に失敗したすべてのストレージノードの減設を実施後に、本手順を実施してください。
Azure ポータルのリソースグループにある **VSP One SDS Block** のリソースグループページにアクセスし、減設されたストレージノードの **VM**、**NIC**、**disk**、**VMSS** を選択して削除してください。



メモ

VSP One SDS Block が作成するストレージノードの **VM**、**NIC**、**disk** のリソースには "**<clusterName>-SN<XX>-<suffix>**"形式のリソース名が付与されているため、どのリソースがどのストレージノードに属するリソースか判別できます。
<clusterName>はストレージクラスター名、**<XX>**はストレージノードの番号、**<suffix>**はリソースの種類や番号を示します。
VMSS は **Multi-AZ** 構成の場合、削除する必要はありません。ただし、**Single-AZ** 構成の場合は削除が必要です。**VMSS** のリソースには "**<clusterName>-SS<XX>-scaleSet**"形式のリソース名が付与されています。**<clusterName>**はストレージクラスター名、**<XX>**は **VMSS** の番号を示します。**<XX>**の数字が最大の **VMSS** のページにアクセスして **Azure VM** インスタンスを確認してください。
Azure VM インスタンスに何も記載されていない場合は、その **VMSS** を削除してください。
Azure VM インスタンスに削除予定の **VM** が記載されている場合は、**VM** を削除してから **VMSS** を削除してください。**VM** を削除しないと、**VMSS** は削除できません。
Azure VM インスタンスに削除予定ではない **VM** が記載されている場合は、**VMSS** の削除は不要です。
VSP One SDS Block の構成情報に存在しているリソースにはリソースの削除ロックがかかっているため、誤って削除されることはありません。

7. マルチパスを再構築します。



注意

減設後に、減設されたストレージノード以外のコンピュータポート向けの **I/O** に対して、コンピュータノード側でマルチパス構成が組まれているかどうかを、以下の情報を取得して確認し、必要に応じてパス情報の追加・設定を実施してください。

- ・ コンピュータノードのパス情報
- ・ ボリュームとコンピュータノードの接続情報

マルチパス構成を組まない場合、ストレージノードの減設後に障害が発生すると、**I/O** が停止するボリュームが出る可能性があります。

12.5 ストレージノードの減設処理を中止する

ストレージノードの減設処理を途中で中止します。中止して必要な作業を実施したあとは、再度同一ストレージノードに対してストレージノード減設を実行し、ストレージノードの減設をやり終えてください。

ストレージノード減設の中止要求が完了すると、ストレージノード減設のジョブの **state** は "**Stopping**" となり、ストレージノード減設のジョブが中止できた場合、ストレージノード減設のジョブの **state** は "**Stopped**" になります。

ストレージノード減設の中止を実行したタイミングによっては、ストレージノード減設のジョブの state が "Stopping" になるまでに時間が掛かることがあります。また、ストレージノード減設のジョブが中止されずに最後まで実施されることがあります。



注意

ストレージノード減設の中止要求が完了したあとには、減設対象ストレージノードの status は "RemovalFailed"、statusSummary は "Error" となります。再度同一ストレージノードに対してストレージノード減設を実行し、ストレージノード減設をやり終えることで、この状態は解消されます。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージノードの減設処理を中止します。

REST API : POST /v1/objects/storage/actions/stop-removing-storage-nodes/invoke

CLI : storage_stop_removing_storage_node

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

3. ストレージノード減設のジョブの state を確認します。

ストレージノード減設のジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Stopped" になっていたら減設の中止は完了です。

ストレージノードを保守する

- 13.1 ストレージノード保守の原因と対処
- 13.2 ストレージノードの保守回復
- 13.3 ストレージノードの保守閉塞
- 13.4 ストレージノードの交換
- 13.5 ストレージノードの自動回復機能の設定
- 13.6 ストレージノードの自動回復機能の情報取得
- 13.7 クラウドプラットフォームのメンテナンスについて<<Cloud for Google Cloud>>
- 13.8 クラウドプラットフォームのメンテナンスについて<<Cloud for Microsoft Azure>>

13.1 ストレージノード保守の原因と対処

ストレージノードの保守方法について説明します。

13.1.1 ストレージノード保守の原因と対処<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージノードの保守作業において、ストレージノードを回復・閉塞させるための機能には、以下があります。

項目	機能	参照先
ストレージノードを回復する	ストレージノードの保守回復	・ 「ストレージノードを保守回復する<<Bare metal>>」
	ストレージノードの交換	・ 「ストレージノードを交換する<<Bare metal>>」
	ストレージノードの自動回復	・ 「ストレージノードの自動回復機能を設定する<<Bare metal>>」
ストレージノードを閉塞する	ストレージノードの保守閉塞	・ 「ストレージノードの保守閉塞の条件を確認する<<Bare metal>>」 ・ 「ストレージノードを保守閉塞する<<Bare metal>>」

障害が原因でストレージノードが閉塞した場合、故障や障害箇所によって、回復のために使用する機能が異なります。それぞれ以下の表を参考にして、必要な対処と使用する機能を確認してください。



注意

「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に記載してある回復順序で対処したあと、以下の表に記載してある対処を行ってください。

以下の表には、部品の交換やファームウェアのアップデートなどの際の対処方法についても記載しています。

ハードウェアを交換する場合は「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載してあるハードウェアから選択してください。また、ハードウェアごとに交換条件が異なるため、このマニュアルの「ハードウェア交換の条件<<Bare metal>>」を確認し、条件を満たすハードウェアを使用してください。条件を満たしていないハードウェアを使用し、障害が起きてしまった場合には、サポートセンターの対応が遅れるなどの影響が発生する可能性があります。

また、HPEC 4D+2P または Mirroring Duplication 構成をとっている場合の、以下の表での対処方法における補足説明として次があります。

- ・ ストレージノード障害からの回復以外の目的で、複数のストレージノードの保守閉塞・保守回復を実施する場合は、保守対象のストレージノードに対して、1 台ずつ保守作業を実施してください。ストレージノードの保守回復後のリビルドが動作中の場合は、リビルドが完了するまで、次のストレージノードの保守閉塞の実施はお待ちください。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。

- ・ ストレージノード障害からの回復が目的の場合は、リビルドの完了を待たずに、各ストレージノードの保守作業を実施して問題ありません。



注意

スペアノード機能を使用しているストレージクラスターでは、スペアノード切り換え機能が実施されることで、自動でストレージノードの物理サーバーが切り換わります。ストレージノードの物理サーバーに対して操作・保守を行う際は、下記の内容を確認し、操作・保守する物理サーバーを間違えないように注意してください。

- ・ ストレージノードに対してスペアノードの物理サーバーが適用され、物理サーバーが切り換わった際は、それを示すイベントログが出力されます。
- ・ 「ストレージノードの BMC 情報を個別に取得する<<Bare metal>>」を実施することで、ストレージノードの物理サーバーに搭載されている BMC の接続情報が取得できます。その情報を使用して、対象のストレージノードの BMC に接続することで、対象のストレージノードの物理サーバー情報が確認できます。ただし、設定に誤りがあった場合は、イベントログによってその旨通知されます。BMC の設定が正しいかどうかの確認は「スペアノード機能の設定を確認する<<Bare metal>>」で行います。

目的	原因など	対処方法
ストレージノード障害からの回復 ¹	ストレージノード間ネットワークポート障害など(ネットワーク機器や HBA の故障など)	左記の原因によってストレージノードが閉塞した場合は、必要に応じて故障した部品を交換してから「ストレージノードを保守回復する<<Bare metal>>」を行います。
	CPU やメモリー(DIMM)の故障など	左記の原因によってストレージノードが閉塞した場合は、必要に応じて故障した部品を交換してから「ストレージノードを保守回復する<<Bare metal>>」を行います。
	システムドライブの故障やシステムドライブフルなど	左記の原因によってストレージノードが閉塞した場合は、故障した部品を交換してから、「ストレージノードを交換する<<Bare metal>>」を行います。
	OS やソフトウェアのエラーに起因したリブート	左記の原因によってストレージノードが閉塞した場合は「ストレージノードを保守回復する<<Bare metal>>」を行います。
	OS 障害(OS のバグなど)によってストレージノードが起動不可	左記の原因によって、ストレージノードが閉塞した場合は「ストレージノードを交換する<<Bare metal>>」を行います。
	停電や電源ユニットの故障	左記の原因によってストレージノードが閉塞した場合は、必要に応じて故障した部品を交換してから「ストレージノードを保守回復する<<Bare metal>>」を行います。
	ストレージクラスター起動時の起動し忘れなど	左記の原因によってストレージノードが閉塞した場合は「ストレージノードを保守回復する<<Bare metal>>」を行います。
	ストレージノードのソフトウェアアップデートの失敗	左記の原因によって、ストレージノードが閉塞した場合は「ストレージノードを保守回復する<<Bare metal>>」または「ストレージノード

目的	原因など	対処方法
		ドを交換する<<Bare metal>>」を行います。 失敗の原因によっては「ストレージノードを交換する<<Bare metal>>」の実施が必須になります。
	ディスクコントローラーの故障	左記の原因によってストレージノードが閉塞した場合は、必要に応じて部品を交換してから、「ストレージノードを保守回復する<<Bare metal>>」を行い、ストレージノードを回復します。 ハードウェア交換方法次第では「ストレージノードを交換する<<Bare metal>>」による回復が必要になります。 ストレージノードの保守回復およびストレージノードの交換における、ハードウェア交換の条件については、このマニュアルの「ハードウェア交換の条件<<Bare metal>>」を確認してください。 (注意) ディスクコントローラー交換後、ディスクコントローラーのすべてのケーブルが正しい位置にしっかりと接続されていることを確認してください。ケーブルが正しく接続されていない場合、ストレージノードの回復後にディスクコントローラー配下のドライブが閉塞し、ドライブの交換が必要になることがあります。
	UEFI Shell 画面が表示されており、ストレージノードが起動不可	スベアノード切り換え機能によって OS 起動抑止がされた可能性があります。回復するには「ストレージノードを交換する<<Bare metal>>」を行います。
	BMC ネットワークの障害発生によって、ストレージノードの BMC にアクセスできない(ネットワーク機器や BMC ネットワークポートの故障など)	左記の原因によってスベアノード切り換えが失敗し、ストレージノードが閉塞した場合は、必要に応じて故障した部品を交換してから「ストレージノードを保守回復する<<Bare metal>>」を行います。
ストレージノード障害を伴わない部品の交換		ストレージノードに障害は発生していないが、部品交換が推奨されているような状態から「ストレージノードを保守閉塞する<<Bare metal>>」を行い、部品の交換を行います。その後、「ストレージノードを保守回復する<<Bare metal>>」または「ストレージノードを交換する<<Bare metal>>」を

目的	原因など	対処方法
		行い、ストレージノードを回復します。 ストレージノードの保守回復およびストレージノードの交換における、ハードウェア交換の条件については、このマニュアルの「ハードウェア交換の条件<<Bare metal>>」を確認してください。 ストレージソフトウェアの再インストールが必要になる場合は「ストレージノードを交換する<<Bare metal>>」の実施が必須になります。 (注意) ディスクコントローラー交換後、ディスクコントローラーのすべてのケーブルが正しい位置にしっかりと接続されていることを確認してください。ケーブルが正しく接続されていない場合、ストレージノードの回復後にディスクコントローラー配下のドライブが閉塞し、ドライブの交換が必要になることがあります。
ファームウェアのアップデート		「ストレージノードを保守閉塞する<<Bare metal>>」を行い、ファームウェアアップデートを行ってから「ストレージノードを保守回復する<<Bare metal>>」を行います。²
物理サーバーの移動		ストレージノード単位で「ストレージノードを保守閉塞する<<Bare metal>>」を行い、サーバーの停止やケーブリングを変更してから「ストレージノードを保守回復する<<Bare metal>>」を行います。
物理サーバーの入れ替え		ストレージノード単位で「ストレージノードを保守閉塞する<<Bare metal>>」を行います。さらにそのあと、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の以下に記載されている構築準備を行ってから「ストレージノードを交換する<<Bare metal>>」を実施します。 「ストレージノードを準備する」
ストレージノード単位で管理ポートまたはストレージノード間ポートの接続確認を実施する場合		ストレージノード単位で「ストレージノードを保守閉塞する<<Bare metal>>」を行い、必要に応じてネットワークの問題を是正してから「ストレージノードを交換する<<Bare metal>>」を行います。

目的	原因など	対処方法
1. 対処するストレージノードが、ストレージノードの自動回復機能が対象とする条件に当てはまる場合、ストレージノードの自動回復機能が動作することがあります。詳細は「ストレージノードの自動回復機能を設定する<<Bare metal>>」を参照してください。 2. ストレージクラスタの停止に伴う I/O の停止を許容できる場合は、ストレージノードの保守閉塞とストレージノードの保守回復を実施する代わりに、ストレージクラスタを停止した状態でファームウェアのアップデートをすることでも対処できます。この方法では、複数のストレージノードに対して同時にアップデートを行うことができます。 「ストレージクラスタを停止する<<Bare metal>>」を行い、ストレージノードに対しファームウェアアップデートを行ってから「ストレージクラスタを起動する<<Bare metal>>」を行います。 - 物理サーバーのモデルや設定によって、ファームウェアのアップデート操作後に物理サーバーが自動で起動することがあります。「ストレージクラスタを起動する<<Bare metal>>」を行う前の意図しない契機でストレージノードが自動起動しないよう、使用しているハードウェアのマニュアルを参照して物理サーバーを設定してください。		

ストレージノードのステータスと対処

運用中のストレージノードに何らかの障害が発生したり、手動で保守閉塞を実施したりすると、ストレージノードは閉塞を示す **status** になります。**status** によって必要な対処が変わってきますので、以下の表を参考に対処してください。

また、複数のストレージノードに障害が発生していたり、ヘルスステータスを取得しストレージノード以外にも Alerting が出ている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に沿った回復順序で対処を行ってください。ヘルスステータスの取得方法は、このマニュアルの「ヘルスステータスを取得する」を参照してください。

status	説明と必要な対処
TemporaryBlockage	
	[説明] 何らかの要因で障害が発生し閉塞した状態です。 [必要な対処] - ストレージノードの自動回復機能の設定が有効の場合： ストレージノードの自動回復機能によって回復される可能性がありますので、しばらくお待ちください。詳細は「ストレージノードの自動回復機能を設定する<<Bare metal>>」を参照してください。 - ストレージノードの自動回復機能の設定が無効の場合： 「ストレージノードを保守回復する<<Bare metal>>」または「ストレージノードを交換する<<Bare metal>>」の手順に従って対象のストレージノードの状態を回復してください。
RemovalFailedAndTemporaryBlockage*	
	[説明] 何らかの要因で障害が発生して閉塞し、かつ減設処理が未完了になっている状態です。 [必要な対処] 「ストレージノードを保守回復する<<Bare metal>>」または「ストレージノードを交換する<<Bare metal>>」の手順に従って対象のストレージノードの状態を回復してください。
PersistentBlockage RemovalFailedAndPersistentBlockage*	
	[説明] 以下のいずれかの理由によって閉塞した状態です。 ストレージノードの自動回復機能による自己診断の結果、自動回復不可と判定した場合： PersistentBlockage となったストレージノードは KARS13102-E のイベントログによって示されます。

status	説明と必要な対処
	- ストレージノードの自動回復機能による保守回復またはスペアノード切り換えが失敗した場合： PersistentBlockage となったストレージノードは KARS10526-E または KARS10776-E のイベントログによって示されます。 - ユーザーによる保守操作(ストレージノードの保守回復、ストレージノードの交換、ソフトウェアアップデート)におけるストレージノードの回復処理が失敗した場合： 保守操作の失敗は KARS13011-I のイベントログによって示されます。 PersistentBlockage になったストレージノードはストレージノード情報の一覧を取得して確認してください。
	[必要な対処]「ストレージノードを保守回復する<<Bare metal>>」または「ストレージノードを交換する<<Bare metal>>」の手順に従って対象のストレージノードの状態を回復してください。
MaintenanceBlockage RemovalFailedAndMaintenanceBlockage*	
	[説明] 保守閉塞処理を実施した状態です。また、ストレージノード交換時に一時的に遷移したり、ソフトウェアアップデートに失敗したときに遷移することがあります。ストレージノード交換時のステータスの遷移については「ストレージノードを交換する<<Bare metal>>」を参照してください。
	[必要な対処] 閉塞したストレージノードに対して必要な対処を行ったあと、「ストレージノードを保守回復する<<Bare metal>>」または「ストレージノードを交換する<<Bare metal>>」の手順に従って対象のストレージノードの状態を回復してください。
InstallationFailed	
	[説明] ストレージノード内のインストレーション処理(ソフトウェアアップデートの中で実施されるパッケージ更新やストレージノード交換処理など)が失敗して閉塞した状態です。
	[必要な対処]「ストレージノードを交換する<<Bare metal>>」の手順に従って対象のストレージノードの状態を回復してください。
TemporaryBlockageProcessInProgress MaintenanceBlockageProcessInProgress RemovalFailedAndTemporaryBlockageProcessInProgress* RemovalFailedAndMaintenanceBlockageProcessInProgress*	
	[説明] 閉塞処理が実施中の状態です。
	[必要な対処] 閉塞処理の完了を待ってください。その後、遷移した status によって必要な対処を行ってください。
TemporaryBlockageFailed MaintenanceBlockageFailed RemovalFailedAndMultipleFailures	
	[説明] 閉塞処理が失敗した状態です。
	[必要な対処]「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」を参照して、すべてのストレージノードに対し、ダンプログファイルを採取したあと、サポートセンターに連絡してください。
* RemovalFailed が付いた status になっているストレージノードは、閉塞状態から回復したあとに、ストレージノードの減設を実施する必要があります。詳細は「ストレージノードの減設<<Bare metal>>」の手順に従って対処してください。	

13.1.2 ストレージノード保守の原因と対処<<Cloud for AWS>>

この項での記述内容は Cloud モデル for AWS に適用されます。

ストレージノードの保守作業において、ストレージノードを回復・閉塞させるための機能には、以下があります。

項目	機能	参照先
ストレージノードを回復する	ストレージノードの保守回復	「ストレージノードを保守回復する <<Cloud for AWS>>」
	ストレージノードの交換	「ストレージノードを交換する <<Cloud for AWS>>」
	ストレージノードの自動回復	「ストレージノードの自動回復機能を設定する <<Cloud>>」
ストレージノードを閉塞する	ストレージノードの保守閉塞	「ストレージノードの保守閉塞の条件を確認する <<Cloud>>」 「ストレージノードを保守閉塞する <<Cloud for AWS>>」

障害が原因でストレージノードが閉塞した場合、故障や障害箇所によって、回復のために使用する機能が異なります。それぞれ以下の表を参考にして、必要な対処と使用する機能を確認してください。



注意

- 「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に記載してある回復順序で対処したあと、以下の表に記載してある対処を行ってください。
- 閉塞時と異なるドライブによるストレージノード交換のみサポートされています。

HPEC 4D+2P または Mirroring Duplication 構成をとっている場合の、以下の表での対処方法における補足説明として次があります。

- ストレージノード障害、VM 障害からの回復以外の目的で、複数のストレージノードの保守閉塞・保守回復を実施する場合は、保守対象のストレージノードに対して、1 台ずつ保守作業を実施してください。ストレージノードの保守回復後のリビルドが動作中の場合は、リビルドが完了するまで、次のストレージノードの保守閉塞の実施はお待ちください。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。
- ストレージノード障害、VM 障害からの回復が目的の場合は、リビルドの完了を待たずに、各ストレージノードの保守作業を実施して問題ありません。

目的	原因など	対処方法
ストレージノード障害からの回復*	AWS 環境の障害など	左記の原因によってストレージノードが閉塞した場合は、閉塞したストレージノード VM の EC2 インスタンスの状態を確認してから「ストレージノードを保守回復する <<Cloud for AWS>>」を行います。障害の原因によっては「ストレージノードを交換する <<Cloud for AWS>>」の実施が必須になります。
	ストレージノード間ネットワークポート障害など	左記の原因によってストレージノードが閉塞した場合は、閉塞したストレージノード VM の EC2 インスタンスの状態を確認してから「ス

目的	原因など	対処方法
		ストレージノードを保守回復する 「Cloud for AWS」を行います。
	システムドライブの故障やシステムドライブフルなど	左記の原因によってストレージノードが閉塞した場合は「ストレージノードを交換する「Cloud for AWS」」を行います。
	OS やソフトウェアのエラーに起因したリブート	左記の原因によってストレージノードが閉塞した場合は「ストレージノードを保守回復する「Cloud for AWS」」を行います。
	ストレージクラスター起動時の起動し忘れなど	左記の原因によってストレージノードが閉塞した場合は「ストレージノードを保守回復する「Cloud for AWS」」を行います。
	ストレージノードのソフトウェアアップデートの失敗	左記の原因によって、ストレージノードが閉塞した場合は「ストレージノードを保守回復する「Cloud for AWS」」または「ストレージノードを交換する「Cloud for AWS」」を行います。 失敗の原因によっては「ストレージノードを交換する「Cloud for AWS」」の実施が必須になります。
VM 障害からの回復	VM が削除されている	左記の状態から「ストレージノードを交換する「Cloud for AWS」」を行います。 「ストレージノードを保守回復する「Cloud for AWS」」では状態を回復できません。注意してください。
	AWS マネジメントコンソールからの VM 起動が失敗する、または VM の OS 起動が失敗する	AWS のマニュアルを確認してください。 AWS のマニュアルに従って対処しても VM が起動しない場合は、左記の状態から「ストレージノードを交換する「Cloud for AWS」」を行います。 「ストレージノードを保守回復する「Cloud for AWS」」では状態を回復できません。注意してください。
* 対処するストレージノードがストレージノードの自動回復機能が対象とする条件に当てはまる場合、ストレージノードの自動回復機能が動作する可能性があります。詳細は「ストレージノードの自動回復機能を設定する「Cloud」」を参照してください。		

ストレージノードのステータスと対処

運用中のストレージノードに何らかの障害が発生したり、手動で保守閉塞を実施したりすると、ストレージノードは閉塞を示す **status** になります。**status** によって必要な対処が変わってきますので、以下の表を参考にしてください。

また、複数のストレージノードに障害が発生していたり、ヘルスステータスを取得しストレージノード以外にも Alerting が出ている場合は「Hitachi Virtual Storage Platform One SDS Block トラ

ブルシューティングガイド」に沿った回復順序で対処を行ってください。ヘルスステータスの取得方法は、このマニュアルの「ヘルスステータスを取得する」を参照してください。

status	説明と必要な対処
TemporaryBlockage	
	[説明] 何らかの要因で障害が発生し閉塞した状態です。 [必要な対処] - ストレージノードの自動回復機能の設定が有効の場合： ストレージノードの自動回復機能によって回復される可能性がありますので、しばらくお待ちください。詳細は「ストレージノードの自動回復機能を設定する<<Cloud>>」を参照してください。 - ストレージノードの自動回復機能の設定が無効の場合： 「ストレージノードを保守回復する<<Cloud for AWS>>」または「ストレージノードを交換する<<Cloud for AWS>>」の手順に従って対象のストレージノードの状態を回復してください。
RemovalFailedAndTemporaryBlockage*	
	[説明] 何らかの要因で障害が発生して閉塞し、かつ減設処理が未完了になっている状態です。 [必要な対処] 「ストレージノードを保守回復する<<Cloud for AWS>>」または「ストレージノードを交換する<<Cloud for AWS>>」の手順に従って対象のストレージノードの状態を回復してください。
PersistentBlockage RemovalFailedAndPersistentBlockage*	
	[説明] 以下のいずれかの理由によって閉塞した状態です。 - ストレージノードの自動回復機能による自己診断の結果、自動回復不可と判定した場合： PersistentBlockage となったストレージノードは KARS13102-E のイベントログによって示されます。 - ストレージノードの自動回復機能による保守回復が失敗した場合： PersistentBlockage となったストレージノードは KARS10526-E または KARS10776-E のイベントログによって示されます。 - ユーザーによる保守操作(ストレージノードの保守回復、ストレージノードの交換、ソフトウェアアップデート)におけるストレージノードの回復処理が失敗した場合： 保守操作の失敗は KARS13011-I のイベントログによって示されます。 PersistentBlockage になったストレージノードはストレージノード情報の一覧を取得して確認してください。 [必要な対処] 「ストレージノードを保守回復する<<Cloud for AWS>>」または「ストレージノードを交換する<<Cloud for AWS>>」の手順に従って対象のストレージノードの状態を回復してください。
MaintenanceBlockage RemovalFailedAndMaintenanceBlockage*	
	[説明] 保守閉塞処理を実施した状態です。また、ストレージノード交換時に一時的に遷移したり、ソフトウェアアップデートに失敗したときに遷移することがあります。ストレージノード交換時のステータスの遷移については「ストレージノードを交換する<<Cloud for AWS>>」を参照してください。 [必要な対処] 閉塞したストレージノードに対して必要な対処を行ったあと、「ストレージノードを保守回復する<<Cloud for AWS>>」または「ストレージノードを交換する<<Cloud for AWS>>」の手順に従って対象のストレージノードの状態を回復してください。
InstallationFailed	
	[説明] ストレージノード内のインストレーション処理(ソフトウェアアップデートの中で実施されるパッケージ更新やストレージノード交換処理など)が失敗して閉塞した状態です。

status	説明と必要な対処
	[必要な対処]「ストレージノードを交換する<<Cloud for AWS>>」の手順に従って対象のストレージノードの状態を回復してください。
TemporaryBlockageProcessInProgress MaintenanceBlockageProcessInProgress RemovalFailedAndTemporaryBlockageProcessInProgress* RemovalFailedAndMaintenanceBlockageProcessInProgress*	
	[説明] 閉塞処理が実施中の状態です。
	[必要な対処] 閉塞処理の完了を待ってください。その後、遷移した status によって必要な対処を行ってください。
TemporaryBlockageFailed MaintenanceBlockageFailed RemovalFailedAndMultipleFailures	
	[説明] 閉塞処理が失敗した状態です。
	[必要な対処]「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」を参照して、すべてのストレージノードに対し、ダンプログファイルを採取したあと、サポートセンターに連絡してください。
* RemovalFailed が付いた status になっているストレージノードは、閉塞状態から回復したあとに、ストレージノードの減設を実施する必要があります。詳細は「ストレージノードの減設<<Cloud for AWS>>」の手順に従って対処してください。	

13.1.3 ストレージノード保守の原因と対処<<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージノードの保守作業において、ストレージノードを回復・閉塞させるための機能には、以下があります。

項目	機能	参照先
ストレージノードを回復する	ストレージノードの保守回復	・ 「ストレージノードを保守回復する<<Cloud for Google Cloud>>」
	ストレージノードの交換	・ 「ストレージノードを交換する<<Cloud for Google Cloud>>」
	ストレージノードの自動回復	・ 「ストレージノードの自動回復機能を設定する<<Cloud>>」
ストレージノードを閉塞する	ストレージノードの保守閉塞	・ 「ストレージノードの保守閉塞の条件を確認する<<Cloud>>」 ・ 「ストレージノードを保守閉塞する<<Cloud for Google Cloud>>」

障害が原因でストレージノードが閉塞した場合、故障や障害箇所によって、回復のために使用する機能が異なります。それぞれ以下の表を参考にして、必要な対処と使用する機能を確認してください。



注意

- ・ 「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に記載してある回復順序で対処したあと、以下の表に記載してある対処を行ってください。
- ・ 閉塞時と異なるドライブによるストレージノード交換のみサポートされています。

HPEC 4D+2P または Mirroring Duplication 構成をとっている場合の、以下の表での対処方法における補足説明として次があります。

- ストレージノード障害、VM 障害からの回復以外の目的で、複数のストレージノードの保守閉塞・保守回復を実施する場合は、保守対象のストレージノードに対して、1 台ずつ保守作業を実施してください。ストレージノードの保守回復後のリビルドが動作中の場合は、リビルドが完了するまで、次のストレージノードの保守閉塞の実施はお待ちください。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。
- ストレージノード障害、VM 障害からの回復が目的の場合は、リビルドの完了を待たずに、各ストレージノードの保守作業を実施して問題ありません。

目的	原因など	対処方法
ストレージノード障害からの回復*	Google Cloud 環境の障害など	左記の原因によってストレージノードが閉塞した場合は、閉塞したストレージノード VM の Compute Engine インスタンスの状態を確認してから「ストレージノードを保守回復する<<Cloud for Google Cloud>>」を行います。 障害の原因によっては「ストレージノードを交換する<<Cloud for Google Cloud>>」の実施が必須になります。
	ストレージノード間ネットワークポート障害など	左記の原因によってストレージノードが閉塞した場合は、閉塞したストレージノード VM の Compute Engine インスタンスの状態を確認してから「ストレージノードを保守回復する<<Cloud for Google Cloud>>」を行います。
	システムドライブの故障やシステムドライブフルなど	左記の原因によってストレージノードが閉塞した場合は、「ストレージノードを交換する<<Cloud for Google Cloud>>」を行います。
	OS やソフトウェアのエラーに起因したリブート	左記の原因によってストレージノードが閉塞した場合は「ストレージノードを保守回復する<<Cloud for Google Cloud>>」を行います。
	ストレージクラスター起動時の起動し忘れなど	左記の原因によってストレージノードが閉塞した場合は「ストレージノードを保守回復する<<Cloud for Google Cloud>>」を行います。
	ストレージノードのソフトウェアアップデートの失敗	左記の原因によって、ストレージノードが閉塞した場合は「ストレージノードを保守回復する<<Cloud for Google Cloud>>」または「ストレージノードを交換する<<Cloud for Google Cloud>>」を行います。 失敗の原因によっては「ストレージノードを交換する<<Cloud for Google Cloud>>」の実施が必須になります。

目的	原因など	対処方法
VM 障害からの回復	VM が削除されている	左記の状態から「ストレージノードを交換する<<Cloud for Google Cloud>>」を行います。「ストレージノードを保守回復する<<Cloud for Google Cloud>>」では状態を回復できません。注意してください。
	Google Cloud コンソールからの VM 起動が失敗する、または VM の OS 起動が失敗する	Google Cloud のマニュアルを確認してください。 Google Cloud のマニュアルに従って対処しても VM が起動しない場合は、左記の状態から「ストレージノードを交換する<<Cloud for Google Cloud>>」を行います。「ストレージノードを保守回復する<<Cloud for Google Cloud>>」では状態を回復できません。注意してください。
* 対処するストレージノードがストレージノードの自動回復機能が対象とする条件に当てはまる場合、ストレージノードの自動回復機能が動作する可能性があります。詳細は「ストレージノードの自動回復機能を設定する<<Cloud>>」を参照してください。		

ストレージノードのステータスと対処

運用中のストレージノードに何らかの障害が発生したり、手動で保守閉塞を実施したりすると、ストレージノードは閉塞を示す **status** になります。**status** によって必要な対処が変わってきますので、以下の表を参考に対処してください。

また、複数のストレージノードに障害が発生していたり、ヘルスステータスを取得しストレージノード以外にも Alerting が出ている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に沿った回復順序で対処を行ってください。ヘルスステータスの取得方法は、このマニュアルの「ヘルスステータスを取得する」を参照してください。

status	説明と必要な対処
TemporaryBlockage	
	[説明] 何らかの要因で障害が発生し閉塞した状態です。 [必要な対処] - ストレージノードの自動回復機能の設定が有効の場合： ストレージノードの自動回復機能によって回復される可能性がありますので、しばらくお待ちください。詳細は「ストレージノードの自動回復機能を設定する<<Cloud>>」を参照してください。 - ストレージノードの自動回復機能の設定が無効の場合： 「ストレージノードを保守回復する<<Cloud for Google Cloud>>」または「ストレージノードを交換する<<Cloud for Google Cloud>>」の手順に従って対象のストレージノードの状態を回復してください。
RemovalFailedAndTemporaryBlockage*	
	[説明] 何らかの要因で障害が発生して閉塞し、かつ減設処理が未完了になっている状態です。

status	説明と必要な対処
	[必要な対処]「ストレージノードを保守回復する<<Cloud for Google Cloud>>」または「ストレージノードを交換する<<Cloud for Google Cloud>>」の手順に従って対象のストレージノードの状態を回復してください。
PersistentBlockage RemovalFailedAndPersistentBlockage*	
	[説明] 以下のいずれかの理由によって閉塞した状態です。 ・ ストレージノードの自動回復機能による自己診断の結果、自動回復不可と判定した場合： PersistentBlockage となったストレージノードは KARS13102-E のイベントログによって示されます。 ・ ストレージノードの自動回復機能による保守回復が失敗した場合： PersistentBlockage となったストレージノードは KARS10526-E または KARS10776-E のイベントログによって示されます。 ・ ユーザーによる保守操作(ストレージノードの保守回復、ストレージノードの交換、ソフトウェアアップデート)におけるストレージノードの回復処理が失敗した場合： 保守操作の失敗は KARS13011-I のイベントログによって示されます。 PersistentBlockage になったストレージノードはストレージノード情報の一覧を取得して確認してください。 [必要な対処]「ストレージノードを保守回復する<<Cloud for Google Cloud>>」または「ストレージノードを交換する<<Cloud for Google Cloud>>」の手順に従って対象のストレージノードの状態を回復してください。
MaintenanceBlockage RemovalFailedAndMaintenanceBlockage*	
	[説明] 保守閉塞処理を実施した状態です。また、ストレージノード交換時に一時的に遷移したり、ソフトウェアアップデートに失敗したときに遷移することがあります。ストレージノード交換時のステータスの遷移については「ストレージノードを交換する<<Cloud for Google Cloud>>」を参照してください。 [必要な対処] 閉塞したストレージノードに対して必要な対処を行ったあと、「ストレージノードを保守回復する<<Cloud for Google Cloud>>」または「ストレージノードを交換する<<Cloud for Google Cloud>>」の手順に従って対象のストレージノードの状態を回復してください。
InstallationFailed	
	[説明] ストレージノード内のインストール処理(ソフトウェアアップデートの中で実施されるパッケージ更新やストレージノード交換処理など)が失敗して閉塞した状態です。 [必要な対処]「ストレージノードを交換する<<Cloud for Google Cloud>>」の手順に従って対象のストレージノードの状態を回復してください。
TemporaryBlockageProcessInProgress MaintenanceBlockageProcessInProgress RemovalFailedAndTemporaryBlockageProcessInProgress* RemovalFailedAndMaintenanceBlockageProcessInProgress*	
	[説明] 閉塞処理が実施中の状態です。 [必要な対処] 閉塞処理の完了を待ってください。その後、遷移した status によって必要な対処を行ってください。
TemporaryBlockageFailed MaintenanceBlockageFailed RemovalFailedAndMultipleFailures	
	[説明] 閉塞処理が失敗した状態です。

status	説明と必要な対処
	[必要な対処]「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」を参照して、すべてのストレージノードに対し、ダンプログファイルを採取したあと、サポートセンターに連絡してください。
* RemovalFailed が付いた status になっているストレージノードは、閉塞状態から回復したあとに、ストレージノードの減設を実施する必要があります。詳細は「ストレージノードの減設<<Cloud for Google Cloud>>」の手順に従って対処してください。	

13.1.4 ストレージノード保守の原因と対処<<Cloud for Microsoft Azure>>

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージノードの保守作業において、ストレージノードを回復・閉塞させるための機能には、以下があります。

項目	機能	参照先
ストレージノードを回復する	ストレージノードの保守回復	・ 「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」
	ストレージノードの交換	・ 「ストレージノードを交換する<<Cloud for Microsoft Azure>>」
	ストレージノードの自動回復	・ 「ストレージノードの自動回復機能を設定する<<Cloud>>」
ストレージノードを閉塞する	ストレージノードの保守閉塞	・ 「ストレージノードの保守閉塞の条件を確認する<<Cloud>>」 ・ 「ストレージノードを保守閉塞する<<Cloud for Microsoft Azure>>」

障害が原因でストレージノードが閉塞した場合、故障や障害箇所によって、回復のために使用する機能が異なります。それぞれ以下の表を参考にして、必要な対処と使用する機能を確認してください。



注意

- ・ 「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に記載してある回復順序で対処したあと、以下の表に記載してある対処を行ってください。
- ・ 閉塞時と異なるドライブによるストレージノード交換のみサポートされています。

HPEC 4D+2P または Mirroring Duplication 構成をとっている場合の、以下の表での対処方法における補足説明として次があります。

- ・ ストレージノード障害、VM 障害からの回復以外の目的で、複数のストレージノードの保守閉塞・保守回復を実施する場合は、保守対象のストレージノードに対して、1 台ずつ保守作業を実施してください。ストレージノードの保守回復後のリビルドが動作中の場合は、リビルドが完了するまで、次のストレージノードの保守閉塞の実施はお待ちください。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。
- ・ ストレージノード障害、VM 障害からの回復が目的の場合は、リビルドの完了を待たずに、各ストレージノードの保守作業を実施して問題ありません。

目的	原因など	対処方法
ストレージノード障害からの回復*	Microsoft Azure 環境の障害など	左記の原因によってストレージノードが閉塞した場合は、閉塞したストレージノード VM の Azure VM インスタンスの状態を確認してから「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」を行います。 障害の原因によっては「ストレージノードを交換する<<Cloud for Microsoft Azure>>」の実施が必須になります。
	ストレージノード間ネットワークポート障害など	左記の原因によってストレージノードが閉塞した場合は、閉塞したストレージノード VM の Azure VM インスタンスの状態を確認してから「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」を行います。
	システムドライブの故障やシステムドライブフルなど	左記の原因によってストレージノードが閉塞した場合は、「ストレージノードを交換する<<Cloud for Microsoft Azure>>」を行います。
	OS やソフトウェアのエラーに起因したリブート	左記の原因によってストレージノードが閉塞した場合は「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」を行います。
	ストレージクラスター起動時の起動し忘れなど	左記の原因によってストレージノードが閉塞した場合は「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」を行います。
	ストレージノードのソフトウェアアップデートの失敗	左記の原因によって、ストレージノードが閉塞した場合は「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」または「ストレージノードを交換する<<Cloud for Microsoft Azure>>」を行います。 失敗の原因によっては「ストレージノードを交換する<<Cloud for Microsoft Azure>>」の実施が必須になります。
VM 障害からの回復	VM が削除されている	左記の状態から「ストレージノードを交換する<<Cloud for Microsoft Azure>>」を行います。 「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」では状態を回復できません。注意してください。
	Azure ポータルからの VM 起動が失敗する、または VM の OS 起動が失敗する	Microsoft Azure のマニュアルを確認してください。

目的	原因など	対処方法
		Microsoft Azure のマニュアルに従って対処しても VM が起動しない場合は、左記の状態から「ストレージノードを交換する<<Cloud for Microsoft Azure>>」を行います。「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」では状態を回復できません。注意してください。
* 対処するストレージノードがストレージノードの自動回復機能が対象とする条件に当てはまる場合、ストレージノードの自動回復機能が動作する可能性があります。詳細は「ストレージノードの自動回復機能を設定する<<Cloud>>」を参照してください。		

ストレージノードのステータスと対処

運用中のストレージノードに何らかの障害が発生したり、手動で保守閉塞を実施したりすると、ストレージノードは閉塞を示す **status** になります。**status** によって必要な対処が変わってきますので、以下の表を参考に対処してください。

また、複数のストレージノードに障害が発生していたり、ヘルスステータスを取得しストレージノード以外にも Alerting が出ている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に沿った回復順序で対処を行ってください。ヘルスステータスの取得方法は、このマニュアルの「ヘルスステータスを取得する」を参照してください。

status	説明と必要な対処
TemporaryBlockage	
	[説明] 何らかの要因で障害が発生し閉塞した状態です。 [必要な対処] - ストレージノードの自動回復機能の設定が有効の場合： ストレージノードの自動回復機能によって回復される可能性がありますので、しばらくお待ちください。詳細は「ストレージノードの自動回復機能を設定する<<Cloud>>」を参照してください。 - ストレージノードの自動回復機能の設定が無効の場合： 「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」または「ストレージノードを交換する<<Cloud for Microsoft Azure>>」の手順に従って対象のストレージノードの状態を回復してください。
RemovalFailedAndTemporaryBlockage*	
	[説明] 何らかの要因で障害が発生して閉塞し、かつ減設処理が未完了になっている状態です。 [必要な対処]「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」または「ストレージノードを交換する<<Cloud for Microsoft Azure>>」の手順に従って対象のストレージノードの状態を回復してください。
PersistentBlockage RemovalFailedAndPersistentBlockage*	
	[説明] 以下のいずれかの理由によって閉塞した状態です。 - ストレージノードの自動回復機能による自己診断の結果、自動回復不可と判定した場合： PersistentBlockage となったストレージノードは KARS13102-E のイベントログによって示されます。 - ストレージノードの自動回復機能による保守回復が失敗した場合：

status	説明と必要な対処
	PersistentBlockage となったストレージノードは KARS10526-E または KARS10776-E のイベントログによって示されます。 ユーザーによる保守操作(ストレージノードの保守回復、ストレージノードの交換、ソフトウェアアップデート)におけるストレージノードの回復処理が失敗した場合：保守操作の失敗は KARS13011-I のイベントログによって示されます。 PersistentBlockage になったストレージノードはストレージノード情報の一覧を取得して確認してください。 [必要な対処]「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」または「ストレージノードを交換する<<Cloud for Microsoft Azure>>」の手順に従って対象のストレージノードの状態を回復してください。
MaintenanceBlockage RemovalFailedAndMaintenanceBlockage*	
	[説明] 保守閉塞処理を実施した状態です。また、ストレージノード交換時に一時的に遷移したり、ソフトウェアアップデートに失敗したときに遷移することがあります。ストレージノード交換時のステータスの遷移については「ストレージノードを交換する<<Cloud for Microsoft Azure>>」を参照してください。 [必要な対処] 閉塞したストレージノードに対して必要な対処を行ったあと、「ストレージノードを保守回復する<<Cloud for Microsoft Azure>>」または「ストレージノードを交換する<<Cloud for Microsoft Azure>>」の手順に従って対象のストレージノードの状態を回復してください。
InstallationFailed	
	[説明] ストレージノード内のインストレーション処理(ソフトウェアアップデートの中で実施されるパッケージ更新やストレージノード交換処理など)が失敗して閉塞した状態です。 [必要な対処]「ストレージノードを交換する<<Cloud for Microsoft Azure>>」の手順に従って対象のストレージノードの状態を回復してください。
TemporaryBlockageProcessInProgress MaintenanceBlockageProcessInProgress RemovalFailedAndTemporaryBlockageProcessInProgress* RemovalFailedAndMaintenanceBlockageProcessInProgress*	
	[説明] 閉塞処理が実施中の状態です。 [必要な対処] 閉塞処理の完了を待ってください。その後、遷移した status によって必要な対処を行ってください。
TemporaryBlockageFailed MaintenanceBlockageFailed RemovalFailedAndMultipleFailures	
	[説明] 閉塞処理が失敗した状態です。 [必要な対処]「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」を参照して、すべてのストレージノードに対し、ダンプログファイルを採取したあと、サポートセンターに連絡してください。
* RemovalFailed が付いた status になっているストレージノードは、閉塞状態から回復したあとに、ストレージノードの減設を実施する必要があります。詳細は「ストレージノードの減設<<Cloud for Microsoft Azure>>」の手順に従って対処してください。	

13.2 ストレージノードの保守回復

ストレージノードの保守回復の方法を説明します。

13.2.1 ストレージノードを保守回復する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージノードの保守回復は、手動または障害によって閉塞されたストレージノードに対して実施できる処理です。手動でストレージノードを閉塞する手順は「ストレージノードの保守閉塞の条件を確認する<<Bare metal>>」と「ストレージノードを保守閉塞する<<Bare metal>>」を参照してください。

ストレージノードの保守回復後には、データの冗長度を回復させるためのリビルドが実行されます。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。

フォールトドメイン障害を含む複数ストレージノードの保守回復をする場合は、1 ストレージノードずつ保守回復を実施してください。

ストレージノードの保守回復操作は 1 ストレージノードずつ、シリアルに実施するため、複数のストレージノードの保守回復を行う場合に掛かる時間は、回復対象のストレージノード数×ストレージノードの保守回復時間になります。

ハードウェアを交換する場合は「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載してあるハードウェアから選択してください。また、ハードウェアごとに交換条件が異なるため、このマニュアルの「ハードウェア交換の条件<<Bare metal>>」を確認し、条件を満たすハードウェアを使用してください。



注意

- ここで説明する手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してからここでの手順を実施してください。
ここで説明する手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に、ここでの手順より前に実施する必要がある対処が示されているときは、その対処後に、ここでの手順を実施してください。
- ストレージノード保守回復時、ホスト I/O が 20～25 秒程度停止が生じます。また、ストレージコントローラの冗長度を回復させる際にホスト I/O 性能が 3～4 分程度低下する可能性があります。
- ここで説明する手順でもストレージノードが回復できないことがあります。その場合は「ストレージノード保守の原因と対処<<Bare metal>>」を参照の上、必要に応じて「ストレージノードを交換する<<Bare metal>>」を実施してストレージノードの回復を行ってください。
また、「ストレージノード保守の原因と対処<<Bare metal>>」で、対処方法として、ここでの手順を実施するように示してあるケースであっても、回復処理が失敗することがあります。その場合は「ストレージノードを交換する<<Bare metal>>」を実施してストレージノードの回復を行ってください。
- 保守回復するストレージノードのメモリーは、プロテクションドメインに属するストレージノード内で最小のメモリー容量以上である必要があります。プロテクションドメイン情報から `minimumMemorySize[MiB]` を参照し、回復対象のストレージノードに必要なメモリー容量を確認してください。
ストレージノードに搭載されているメモリー容量が条件を満たしていないときは、条件を満たすようにメモリーを増設してください。
- ストレージノードの保守回復中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの保守回復が完了するのを待ってから再度これらの操作を実施してください。



メモ ストレージノードの保守回復では、管理ポート接続の非冗長化、冗長化を設定することはできません。

ストレージノードの自動回復機能の設定が有効な場合、`status` が "TemporaryBlockage" のストレージノードに対して自動でストレージノードの回復ジョブが発行されます。閉塞しているストレージ

ノードがストレージノードの自動回復機能によるストレージノードの保守回復対象の条件に該当する場合は手動によるストレージノードの保守回復は不要です。詳細は「ストレージノードの自動回復機能を設定する <<Bare metal>>」を参照してください。

以下は、手動でストレージノードの保守回復を実施する手順です。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ストレージノードを保守回復する」

前提条件

- ・ 実行に必要なロール : Service
 - ・ ストレージノードの保守回復のジョブが動作していないこと
 - ・ 以下のどちらかを満たしていること
 - 回復対象のストレージノードの status が "TemporaryBlockage" でないこと
 - ストレージノードの自動回復機能の設定が無効であること
- この条件を満たさない状態で、手動によるストレージノードの保守回復を実施すると、下記の動作となります。
- ・ 手動によるストレージノードの保守回復が失敗します。自動回復機能の設定が有効の場合、ストレージノードの自動回復機能の動作条件を満たすことで、status が "TemporaryBlockage" のストレージノードは、自動回復機能によって自動で回復されるため、手動によるストレージノードの保守回復の実施は不要です。

操作手順

1. ストレージノードの ID と status を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

回復対象のストレージノードの status が "MaintenanceBlockage"、"PersistentBlockage"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、または "RemovalFailedAndPersistentBlockage" であることを確認し、次の手順に進みます。ただし、ストレージノードの自動回復機能の設定が無効の場合は、回復対象のストレージノードの status が "TemporaryBlockage" の場合も次の手順に進みます。

2. ストレージノードの電源をオンにします。

回復対象のストレージノードの電源をオンにします。電源オンの方法は、使用しているハードウェアのマニュアルを参照してください。

回復手順を開始する前から回復対象のストレージノードがパワーオン状態だった場合は、OS のシャットダウン操作によってストレージノードの停止を実施し、ストレージノードの停止を確認したあと、再度ストレージノードの電源をオンしてください。OS のシャットダウンは、ハードウェアのマニュアルを参照してください。

OS のシャットダウン操作後、約 5 分経過しても停止できない場合は、強制停止操作によってストレージノードの停止を行ったあと、再度ストレージノードの電源をオンにしてください。強制停止は、ハードウェアのマニュアルを参照してください。

ストレージノードの電源をオンにしたあと、起動の開始が確認できたら、次の手順に進みます。



注意

- 日立アドバンスサーバ HA8000V シリーズを使用している場合、OS のシャットダウンは、iLO の「電力管理」にて「瞬間的に押す」による停止となります。また、強制停止は、iLO の「電力管理」にて「押し続ける」による停止となります。具体的な操作方法是ハードウェアのマニュアルを参照してください。日立アドバンスサーバ HA8000V シリーズ以外の物理サーバを使用している場合、OS のシャットダウン、強制停止の具体的な操作方法是、各ハードウェアのマニュアルを参照してください。
- ストレージノードが起動しない場合、対象のストレージノードに対し部品交換を実施していたら、交換部品の影響が考えられます。交換部品ごとの対処方法は「ストレージノード保守の原因と対処<<Bare metal>>」またはハードウェアのマニュアルを参照して確認してください。これらに従って対処してもストレージノードが起動しない場合は、「ストレージノードを交換する<<Bare metal>>」を実施してストレージノードの回復を行ってください。

3. ストレージノードの保守回復を実行します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : POST /v1/objects/storage-nodes/<id >/actions/recover/invoke

CLI : storage_node_recover

コマンド実行後に表示されるジョブの ID を確認します。

この処理は、回復対象のストレージノードの起動完了の確認処理(最大 35 分待ち)後に開始され、プロテクションドメインに設定された最小メモリー容量に応じて以下の時間が掛かります。

- プロテクションドメインに設定された最小メモリー容量が 256GiB のとき : 約 25 分

また、リビルド(データ再構築)が実行中のときは、さらに最大で 5 分ほど処理時間が長くなる可能性があります。

その他、以下の外部要因によって処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。

- ネットワークの通信状況(ストレージノード間の通信状況)
- サーバーの性能状況(ストレージノードの温度上昇による性能低下など)
- サーバーのハードウェア構成(ストレージノードのプロセッサ、メモリー容量など)



メモ

- この操作を実施した際に、イベントログ KARS16018-W が出力されることがあります。このタイミングで、このイベントログが出力されることは問題ありませんので、そのまま手順を継続してください。
- この操作を実施した際に、以下のイベントログが出力されることがあります。これは、正常な動作のため、そのまま手順を継続してください。
 - KARS20067-I
 - KARS20068-I
 - KARS20069-I
- ストレージノード保守回復のジョブの動作条件
以下の条件を満たさず、ジョブが失敗した際は、イベントログを参照して対処してください。
 - ストレージクラスターの status が "Ready" であること
 - 対象のストレージノードが閉塞していること
 - クラスターマスターノード(プライマリー)から、対象のストレージノードへストレージノード間ネットワークで接続ができること

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



メモ

ストレージノード回復ジョブが何らかの理由でエラーとなった場合は、エラー処理によってストレージノードの電源オフが実行されます。ただし、ネットワークの障害などによって電源オフの処理が正常に実行できないことがあります。ストレージノード回復ジョブがエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

5. ストレージノードの情報を取得して、ストレージノードの保守回復がされたことを確認します。
- ストレージノードの ID を指定してコマンドを実行します。
- REST API : GET /v1/objects/storage-nodes/<id >
- CLI : storage_node_show
- status が"Ready"または"RemovalFailed"であれば、ストレージノードの保守回復が完了しています。
- ストレージノードの保守回復が完了するまでは、他の操作が実施できないことがあります。
6. ストレージノードが閉塞してから回復が完了するまでの間に、以下に該当するハードウェア部品などを交換した場合は、下記の対処を行います。

交換対象	対処
FCHBA を交換していた場合	「コンピュータポートの情報を個別に取得する」を参照し、FCHBA を交換したコンピュータポートの情報を取得します。 portSpeed が"LinkDown"になっていた場合は、設定しているリンク速度を交換した FCHBA がサポートしていない可能性があります。 configuredPortSpeed から設定しているリンク速度を確認し、交換した FCHBA が設定しているリンク速度をサポートしているかを確認してください。 もし、サポートしていない FCHBA である場合は、「ストレージノード保守の原因と対処<<Bare metal>>」を参照し、適切な FCHBA に交換してください。サポートしている FCHBA を使用していても portSpeed が "LinkDown"となっていた場合は、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ストレージクラスターで障害を検知した場合」を参照して対処してください。
ユーザーデータドライブを交換していた場合 (閉塞時とは異なるユーザーデータドライブに交換していた場合)	「ストレージノードを交換する<<Bare metal>>」の手順 12 以降を実施してください。 「ストレージノードを交換する<<Bare metal>>」の手順を参照する際は、「交換したストレージノード」を「保守回復したストレージノード」と読み替えてください。

7. 構成情報のバックアップを行います。
- 「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
- ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

13.2.2 ストレージノードを保守回復する<<Cloud for AWS>>

この項での記述内容は Cloud モデル for AWS に適用されます。

ストレージノードの保守回復は、手動または障害によって閉塞されたストレージノードに対して実施できる処理です。手動でストレージノードを閉塞する手順は「ストレージノードの保守閉塞の条件を確認する<<Cloud>>」と「ストレージノードを保守閉塞する<<Cloud for AWS>>」を参照してください。

ストレージノードの保守回復後には、データの冗長度を回復させるためのリビルドが実行されます。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。

フォールトドメイン障害を含む複数ストレージノードの保守回復をする場合は、1 ストレージノードずつ保守回復を実施してください。

ストレージノードの保守回復操作は1 ストレージノードずつ、シリアルに実施するため、複数のストレージノードの保守回復を行う場合に掛かる時間は、回復対象のストレージノード数×ストレージノードの保守回復時間になります。



注意

- ここで説明する手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してからここでの手順を実施してください。
ここで説明する手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に、ここでの手順より前に実施する必要がある対処が示されているときは、その対処後に、ここでの手順を実施してください。
- ストレージノード保守回復時、ホスト I/O が 20~25 秒程度停止が生じます。また、ストレージコントローラーの冗長度を回復させる際にホスト I/O 性能が 3~4 分程度低下する可能性があります。
- ここで説明する手順でもストレージノードが回復できないことがあります。その場合は「ストレージノード保守の原因と対処<<Cloud for AWS>>」を参照の上、必要に応じて「ストレージノードを交換する<<Cloud for AWS>>」を実施してストレージノードの回復を行ってください。
また、「ストレージノード保守の原因と対処<<Cloud for AWS>>」で、対処方法として、ここでの手順を実施するように示してあるケースであっても、回復処理が失敗することがあります。その場合は「ストレージノードを交換する<<Cloud for AWS>>」を実施してストレージノードの回復を行ってください。
- ストレージノードの保守回復中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの保守回復が完了するのを待ってから再度これらの操作を実施してください。

ストレージノードの自動回復機能の設定が有効な場合、status が"TemporaryBlockage"のストレージノードに対して自動でストレージノードの回復ジョブが発行されます。閉塞しているストレージノードがストレージノードの自動回復機能によるストレージノードの保守回復対象の条件に該当する場合は手動によるストレージノードの保守回復は不要です。詳細は「ストレージノードの自動回復機能を設定する<<Cloud>>」を参照してください。

以下は、手動でストレージノードの保守回復を実施する手順です。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ストレージノードを保守回復する」

前提条件

- 実行に必要なロール：Service
- ストレージノードの保守回復のジョブが動作していないこと
- 以下のどちらかを満たしていること

- ・ 回復対象のストレージノードの `status` が `"TemporaryBlockage"` でないこと
- ・ ストレージノードの自動回復機能の設定が無効であること

この条件を満たさない状態で、手動によるストレージノードの保守回復を実施すると、下記の動作となります。

- ・ ストレージノードの自動回復機能によるストレージノードの保守回復のジョブと競合する可能性があります。ストレージノードの保守回復のジョブが競合した場合は、先に動作したストレージノードの保守回復のジョブが動作し、後発のストレージノードの保守回復のジョブは失敗します。手動によるストレージノードの回復ジョブが競合によって失敗した場合は、イベントログ `KARS10901-E` が発行され、ストレージノードの自動回復機能によるストレージノードの回復ジョブが競合によって失敗した場合は、イベントログ `KARS10525-W` が発行されます。

操作手順

1. ストレージノードの ID と `status` を確認します。

REST API : `GET /v1/objects/storage-nodes`

CLI : `storage_node_list`

回復対象のストレージノードの `status` が `"MaintenanceBlockage"`、`"PersistentBlockage"`、`"RemovalFailedAndTemporaryBlockage"`、`"RemovalFailedAndMaintenanceBlockage"`、または `"RemovalFailedAndPersistentBlockage"` であることを確認し、次の手順に進みます。ただし、ストレージノードの自動回復機能の設定が無効の場合は、回復対象のストレージノードの `status` が `"TemporaryBlockage"` の場合も次の手順に進みます。

2. ストレージノードの電源をオンにします。

AWS マネジメントコンソールを操作して、回復対象のストレージノード VM(EC2 インスタンス)を開始します。

回復手順を開始する前から回復対象のストレージノード VM(EC2 インスタンス)がパワーオン状態だった場合は、EC2 インスタンスの停止操作によって EC2 インスタンスを停止したあと、再度 EC2 インスタンスを開始してください。

EC2 インスタンスの停止操作後、約 5 分経過しても停止できない場合は、強制停止操作によって EC2 インスタンスの停止を行ったあと、再度 EC2 インスタンスを開始してください。強制停止は、AWS マネジメントコンソールの EC2 インスタンスの停止操作で停止してください。AWS マネジメントコンソールから回復対象のストレージノード VM(EC2 インスタンス)が開始したことを確認してください。

開始が確認できたら次の手順に進みます。



メモ

- ・ EC2 インスタンスの開始方法・停止方法は、AWS のマニュアルを参照してください。
 - ・ EC2 インスタンスの強制停止は、EC2 インスタンスが停止中(`stopping`)の状態のままのときに再度 EC2 インスタンスの停止操作を行うことで実行できます。詳しい操作方法は AWS のマニュアルを参照してください。
-

3. ストレージノードの保守回復を実行します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : `POST /v1/objects/storage-nodes/<id >/actions/recover/invoke`

CLI : `storage_node_recover`

コマンド実行後に表示されるジョブの ID を確認します。

この処理は、回復対象のストレージノード VM の起動完了の確認処理(最大 35 分待ち)後に開始され、プロテクションドメインに設定された最小メモリー容量に応じて以下の時間が掛かります。

- ・プロテクションドメインに設定された最小メモリー容量が 128GiB のとき：約 15 分
- ・プロテクションドメインに設定された最小メモリー容量が 256GiB のとき：約 25 分

また、リビルド(データ再構築)が実行中のときは、さらに最大で 5 分ほど処理時間が長くなる可能性があります。

その他、以下の外部要因によって処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。

- ・ ネットワークの通信状況(ストレージノード間の通信状況)
- ・ EC2 インスタンスの性能状況



メモ

- ・ この操作を実施した際に、イベントログ KARS16018-W が出力されることがあります。このタイミングで、このイベントログが出力されることは問題ありませんので、そのまま手順を継続してください。
 - ・ ストレージノード保守回復のジョブの動作条件
以下の条件を満たさず、ジョブが失敗した際は、イベントログを参照して対処してください。
 - ストレージクラスターの status が"Ready"であること
 - 対象のストレージノードが閉塞していること
 - クラスターマスターノード(プライマリー)から、対象のストレージノードへストレージノード間ネットワークで接続ができること
-

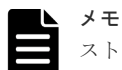
4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



メモ

ストレージノード回復ジョブが何らかの理由でエラーとなった場合は、エラー処理によってストレージノード VM の電源オフが実行されます。ただし、ネットワークの障害などによって電源オフの処理が正常に実行できないことがあります。ストレージノード回復ジョブがエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

5. ストレージノードの情報を取得して、ストレージノードの保守回復がされたことを確認します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/storage-nodes/<id >

CLI : storage_node_show

status が"Ready"または"RemovalFailed"であれば、ストレージノードの保守回復が完了しています。

ストレージノードの保守回復が完了するまでは、他の操作が実施できないことがあります。

6. ストレージノードが閉塞してから回復が完了するまでの間に、以下に該当するコンポーネントなどを交換した場合は、下記の対処を行います。

交換対象	対処
ユーザーデータドライブを交換していた場合 (閉塞時とは異なるユーザーデータドライブに交換していた場合)	「ストレージノードを交換する<<Cloud for AWS>>」の手順 9 以降を実施してください。 「ストレージノードを交換する<<Cloud for AWS>>」の手順を参照する際は、「交換したストレージノード」を「保守回復したストレージノード」と読み替えてください。

7. 構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

13.2.3 ストレージノードを保守回復する<<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージノードの保守回復は、手動または障害によって閉塞されたストレージノードに対して実施できる処理です。手動でストレージノードを閉塞する手順は「ストレージノードの保守閉塞の条件を確認する<<Cloud>>」と「ストレージノードを保守閉塞する<<Cloud for Google Cloud>>」を参照してください。

ストレージノードの保守回復後には、データの冗長度を回復させるためのリビルドが実行されます。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。

フォールトドメイン障害を含む複数ストレージノードの保守回復をする場合は、1 ストレージノードずつ保守回復を実施してください。

ストレージノードの保守回復操作は 1 ストレージノードずつ、シリアルに実施するため、複数のストレージノードの保守回復を行う場合に掛かる時間は、回復対象のストレージノード数×ストレージノードの保守回復時間になります。



注意

- ここで説明する手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してからここでの手順を実施してください。
ここで説明する手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に、ここでの手順より前に実施する必要がある対処が示されているときは、その対処後に、ここでの手順を実施してください。
- ストレージノード保守回復時、ホスト I/O が 20～25 秒程度停止が生じます。また、ストレージコントローラーの冗長度を回復させる際にホスト I/O 性能が 3～4 分程度低下する可能性があります。
- ここで説明する手順でもストレージノードが回復できないことがあります。その場合は「ストレージノード保守の原因と対処<<Cloud for Google Cloud>>」を参照の上、必要に応じて「ストレージノードを交換する<<Cloud for Google Cloud>>」を実施してストレージノードの回復を行ってください。
また、「ストレージノード保守の原因と対処<<Cloud for Google Cloud>>」で、対処方法として、ここでの手順を実施するように示してあるケースであっても、回復処理が失敗することがあります。その場合は「ストレージノードを交換する<<Cloud for Google Cloud>>」を実施してストレージノードの回復を行ってください。
- ストレージノードの保守回復中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの保守回復が完了するのを待ってから再度これらの操作を実施してください。

ストレージノードの自動回復機能の設定が有効な場合、status が"TemporaryBlockage"のストレージノードに対して自動でストレージノードの回復ジョブが発行されます。閉塞しているストレージ

ノードがストレージノードの自動回復機能によるストレージノードの保守回復対象の条件に該当する場合は手動によるストレージノードの保守回復は不要です。詳細は「ストレージノードの自動回復機能を設定する <<Cloud>>」を参照してください。

以下は、手動でストレージノードの保守回復を実施する手順です。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ストレージノードを保守回復する」

前提条件

- ・ 実行に必要なロール : Service
- ・ ストレージノードの保守回復のジョブが動作していないこと
- ・ 以下のどちらかを満たしていること
 - 回復対象のストレージノードの status が "TemporaryBlockage" でないこと
 - ストレージノードの自動回復機能の設定が無効であること

この条件を満たさない状態で、手動によるストレージノードの保守回復を実施すると、下記の動作となります。

- ・ ストレージノードの自動回復機能によるストレージノードの保守回復のジョブと競合する可能性があります。ストレージノードの保守回復のジョブが競合した場合は、先に動作したストレージノードの保守回復のジョブが動作し、後発のストレージノードの保守回復のジョブは失敗します。手動によるストレージノードの回復ジョブが競合によって失敗した場合は、イベントログ KARS10901-E が発行され、ストレージノードの自動回復機能によるストレージノードの回復ジョブが競合によって失敗した場合は、イベントログ KARS10525-W が発行されます。

操作手順

1. ストレージノードの ID と status を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

回復対象のストレージノードの status が "MaintenanceBlockage"、"PersistentBlockage"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、または "RemovalFailedAndPersistentBlockage" であることを確認し、次の手順に進みます。ただし、ストレージノードの自動回復機能の設定が無効の場合は、回復対象のストレージノードの status が "TemporaryBlockage" の場合も次の手順に進みます。

2. ストレージノードの電源をオンにします。

Google Cloud コンソールを操作して、回復対象のストレージノード VM (Compute Engine インスタンス) を開始します。

回復手順を開始する前から回復対象のストレージノード VM (Compute Engine インスタンス) がパワーオン状態だった場合は、Compute Engine インスタンスの停止操作によって Compute Engine インスタンスを停止したあと、再度 Compute Engine インスタンスを開始してください。

Compute Engine インスタンスの停止操作を行っても停止されない場合は、約 90 秒後に Google Cloud によって自動的に強制停止されます。そのあと、再度 Compute Engine インスタンスを開始してください。

Google Cloud コンソールから回復対象のストレージノード VM(Compute Engine インスタンス)が開始したことを確認してください。

開始が確認できたら次の手順に進みます。



メモ

Compute Engine インスタンスの開始方法・停止方法は、Google Cloud のマニュアルを参照してください。

3. ストレージノードの保守回復を実行します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : `POST /v1/objects/storage-nodes/<id >/actions/recover/invoke`

CLI : `storage_node_recover`

コマンド実行後に表示されるジョブの ID を確認します。

この処理は、回復対象のストレージノード VM の起動完了の確認処理(最大 35 分待ち)後に開始され、プロテクションドメインに設定された最小メモリー容量に応じて以下の時間が掛かります。

- ・プロテクションドメインに設定された最小メモリー容量が 128GiB のとき : 約 15 分
- ・プロテクションドメインに設定された最小メモリー容量が 256GiB のとき : 約 25 分

また、リビルド(データ再構築)が実行中のときは、さらに最大で 5 分ほど処理時間が長くなる可能性があります。

その他、以下の外部要因によって処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。

- ・ ネットワークの通信状況(ストレージノード間の通信状況)
- ・ Compute Engine インスタンスの性能状況



メモ

- ・ この操作を実施した際に、イベントログ KARS16018-W が出力されることがあります。このタイミングで、このイベントログが出力されることは問題ありませんので、そのまま手順を継続してください。
- ・ ストレージノード保守回復のジョブの動作条件
以下の条件を満たさず、ジョブが失敗した際は、イベントログを参照して対処してください。
 - ストレージクラスターの status が "Ready" であること
 - 対象のストレージノードが閉塞していること
 - クラスターマスターノード(プライマリー)から、対象のストレージノードへストレージノード間ネットワークで接続ができること

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : `GET /v1/objects/jobs/<jobId >`

CLI : `job_show`

state が "Succeeded" になっていたらジョブは完了です。



メモ

ストレージノード回復ジョブが何らかの理由でエラーとなった場合は、エラー処理によってストレージノード VM の電源オフが実行されます。ただし、ネットワークの障害などによって電源オフの処理が正常に実行できないことがあります。ストレージノード回復ジョブがエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

5. ストレージノードの情報を取得して、ストレージノードの保守回復がされたことを確認します。ストレージノードの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/storage-nodes/<id >

CLI : storage_node_show

status が"Ready"または"RemovalFailed"であれば、ストレージノードの保守回復が完了しています。

ストレージノードの保守回復が完了するまでは、他の操作が実施できないことがあります。

6. ストレージノードが閉塞してから回復が完了するまでの間に、以下に該当するコンポーネントなどを交換した場合は、下記の対処を行います。

交換対象	対処
ユーザーデータドライブを交換していた場合 (閉塞時とは異なるユーザーデータドライブに交換していた場合)	「ストレージノードを交換する<<Cloud for Google Cloud>>」の手順 22 以降を実施してください。 「ストレージノードを交換する<<Cloud for Google Cloud>>」の手順を参照する際は、「交換したストレージノード」を「保守回復したストレージノード」と読み替えてください。

13.2.4 ストレージノードを保守回復する<<Cloud for Microsoft Azure>>

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージノードの保守回復は、手動または障害によって閉塞されたストレージノードに対して実施できる処理です。手動でストレージノードを閉塞する手順は「ストレージノードの保守閉塞の条件を確認する<<Cloud>>」と「ストレージノードを保守閉塞する<<Cloud for Microsoft Azure>>」を参照してください。

ストレージノードの保守回復後には、データの冗長度を回復させるためのリビルドが実行されます。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。

フォールトドメイン障害を含む複数ストレージノードの保守回復をする場合は、1 ストレージノードずつ保守回復を実施してください。

ストレージノードの保守回復操作は 1 ストレージノードずつ、シリアルに実施するため、複数のストレージノードの保守回復を行う場合に掛かる時間は、回復対象のストレージノード数×ストレージノードの保守回復時間になります。



注意

- ここで説明する手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してからここでの手順を実施してください。
ここで説明する手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に、ここでの手順より前に実施する必要がある対処が示されているときは、その対処後に、ここでの手順を実施してください。
- ストレージノード保守回復時、ホスト I/O が 20～25 秒程度停止が生じます。また、ストレージコントローラの冗長度を回復させる際にホスト I/O 性能が 3～4 分程度低下する可能性があります。

- ここで説明する手順でもストレージノードが回復できないことがあります。その場合は「ストレージノード保守の原因と対処<<Cloud for Microsoft Azure>>」を参照の上、必要に応じて「ストレージノードを交換する<<Cloud for Microsoft Azure>>」を実施してストレージノードの回復を行ってください。
また、「ストレージノード保守の原因と対処<<Cloud for Microsoft Azure>>」で、対処方法として、ここでの手順を実施するように示してあるケースであっても、回復処理が失敗することがあります。その場合は「ストレージノードを交換する<<Cloud for Microsoft Azure>>」を実施してストレージノードの回復を行ってください。
- ストレージノードの保守回復中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの保守回復が完了するのを待ってから再度これらの操作を実施してください。

ストレージノードの自動回復機能の設定が有効な場合、status が"TemporaryBlockage"のストレージノードに対して自動でストレージノードの回復ジョブが発行されます。閉塞しているストレージノードがストレージノードの自動回復機能によるストレージノードの保守回復対象の条件に該当する場合は手動によるストレージノードの保守回復は不要です。詳細は「ストレージノードの自動回復機能を設定する<<Cloud>>」を参照してください。

以下は、手動でストレージノードの保守回復を実施する手順です。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ストレージノードを保守回復する」

前提条件

- 実行に必要なロール : Service
- ストレージノードの保守回復のジョブが動作していないこと
- 以下のどちらかを満たしていること
 - 回復対象のストレージノードの status が"TemporaryBlockage"でないこと
 - ストレージノードの自動回復機能の設定が無効であること

この条件を満たさない状態で、手動によるストレージノードの保守回復を実施すると、下記の動作となります。

- ストレージノードの自動回復機能によるストレージノードの保守回復のジョブと競合する可能性があります。ストレージノードの保守回復のジョブが競合した場合は、先に動作したストレージノードの保守回復のジョブが動作し、後発のストレージノードの保守回復のジョブは失敗します。手動によるストレージノードの回復ジョブが競合によって失敗した場合は、イベントログ KARS10901-E が発行され、ストレージノードの自動回復機能によるストレージノードの回復ジョブが競合によって失敗した場合は、イベントログ KARS10525-W が発行されます。

操作手順

1. ストレージノードの ID と status を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

回復対象のストレージノードの status が "MaintenanceBlockage"、"PersistentBlockage"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、または "RemovalFailedAndPersistentBlockage"であることを確認し、次の手順に進みます。ただし、ストレージノードの自動回復機能の設定が無効の場合は、回復対象のストレージノードの status が "TemporaryBlockage"の場合も次の手順に進みます。

2. ストレージノードの電源をオンにします。

Azure ポータルを操作して、回復対象のストレージノード VM(Azure VM インスタンス)を開始します。

回復手順を開始する前から回復対象のストレージノード VM(Azure VM インスタンス)がパワーオン状態だった場合は、Azure VM インスタンスの停止操作によって Azure VM インスタンスを停止したあと、再度 Azure VM インスタンスを開始してください。

Azure VM インスタンスの停止操作を行っても停止されない場合は、約 10 分後に Microsoft Azure によって自動的に強制停止されます。そのあと、再度 Azure VM インスタンスを開始してください。

Azure ポータルから回復対象のストレージノード VM(Azure VM インスタンス)が開始したことを確認してください。

開始が確認できたら次の手順に進みます。



メモ

Azure VM インスタンスの開始方法・停止方法は、Microsoft Azure のマニュアルを参照してください。

3. ストレージノードの保守回復を実行します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : `POST /v1/objects/storage-nodes/<id >/actions/recover/invoke`

CLI : `storage_node_recover`

コマンド実行後に表示されるジョブの ID を確認します。

この処理は、回復対象のストレージノード VM の起動完了の確認処理(最大 35 分待ち)後に開始され、プロテクションドメインに設定された最小メモリー容量に応じて以下の時間が掛かります。

- ・プロテクションドメインに設定された最小メモリー容量が 128GiB のとき : 約 15 分
- ・プロテクションドメインに設定された最小メモリー容量が 256GiB のとき : 約 25 分

また、リビルド(データ再構築)が実行中のときは、さらに最大で 5 分ほど処理時間が長くなる可能性があります。

その他、以下の外部要因によって処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。

- ・ ネットワークの通信状況(ストレージノード間の通信状況)
- ・ Azure VM インスタンスの性能状況



メモ

- ・ この操作を実施した際に、イベントログ KARS16018-W が出力されることがあります。このタイミングで、このイベントログが出力されることは問題ありませんので、そのまま手順を継続してください。
- ・ ストレージノード保守回復のジョブの動作条件
以下の条件を満たさず、ジョブが失敗した際は、イベントログを参照して対処してください。
 - ストレージクラスターの status が "Ready" であること
 - 対象のストレージノードが閉塞していること

- 。 クラスターマスターノード(プライマリー)から、対象のストレージノードへストレージノード間ネットワークで接続ができること

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



メモ

ストレージノード回復ジョブが何らかの理由でエラーとなった場合は、エラー処理によってストレージノード VM の電源オフが実行されます。ただし、ネットワークの障害などによって電源オフの処理が正常に実行できないことがあります。ストレージノード回復ジョブがエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

5. ストレージノードの情報を取得して、ストレージノードの保守回復がされたことを確認します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/storage-nodes/<id >

CLI : storage_node_show

status が"Ready"または"RemovalFailed"であれば、ストレージノードの保守回復が完了しています。

ストレージノードの保守回復が完了するまでは、他の操作が実施できないことがあります。

6. ストレージノードが閉塞してから回復が完了するまでの間に、以下に該当するコンポーネントなどを交換した場合は、下記の対処を行います。

交換対象	対処
ユーザーデータドライブを交換していた場合 (閉塞時とは異なるユーザーデータドライブに交換していた場合)	「ストレージノードを交換する<<Cloud for Microsoft Azure>>」の手順 9 以降を実施してください。 「ストレージノードを交換する<<Cloud for Microsoft Azure>>」の手順を参照する際は、「交換したストレージノード」を「保守回復したストレージノード」と読み替えてください。

13.3 ストレージノードの保守閉塞

ストレージノードの保守閉塞の方法を説明します。

13.3.1 ストレージノードの保守閉塞の条件を確認する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージノードが保守閉塞できるかどうかを以下の手順で確認してください。



注意

- ・ ストレージノードの保守閉塞を実施すると、ユーザーデータ、ストレージコントローラー、クラスターマスターノードなどの冗長化されている要素の冗長度が低下します。保守閉塞したストレージノードを回復させるまでは耐障害性が低下することになるため、一度に保守閉塞を実施する範囲はなるべく必要最低限にとどめるようにしてください。

- 以下に記載した確認手順を行った場合でも、諸条件によって保守閉塞処理が失敗する可能性があります。その場合は、出力されるイベントログを参考に対処してください。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ストレージノードの保守閉塞の条件を確認する」

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ストレージノードの一覧を取得して、保守閉塞対象のストレージノードの ID と status を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

保守閉塞対象のストレージノードの status が "Ready" または "RemovalFailed" のとき、次の手順に進みます。

これら以外の status のストレージノードがある場合、以下に従って対処してください。

- status が "TemporaryBlockage"、"MaintenanceBlockage"、"PersistentBlockage"、"InstallationFailed"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、"RemovalFailedAndPersistentBlockage" の場合は、対象のストレージノードは正常に閉塞されており、ストレージクラスターからの切り離しが完了している状態のため、基本的には保守閉塞の実施は不要です。
このため、再度保守閉塞の実施が必要な場合は、先に対象のストレージノードを回復させる必要があります。
 - VSP One SDS Block Administrator で、ストレージノードの Health Status に "Alerting" が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
ただし、"RemovalFailed" のストレージノードのみが存在する場合も "Alerting" になりますが、その場合は問題ありません。
 - 上記以外の status のストレージノードがあった場合は、それらストレージノードに対する処理が実施中のため、status が変わるのを待ってから、再度確認してください。
2. ストレージクラスターの情報を取得し、キャッシュ保護付きライトバックモードの状態を確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態 (writeBackModeWithCacheProtection) によって以下の対応を行います。

キャッシュ保護付き ライトバックモードの状態	対応方法
Enabled	次の手順に進みます。

キャッシュ保護付き ライトバックモードの状態	対応方法
Disabled	手順 4 に進みます。
Enabling	「キャッシュ保護付きライトバックモードを有効にする<<Bare metal>>」を参照して、キャッシュ保護付きライトバックモードの有効化を実行したあと、次の手順に進みます。 または、キャッシュ保護付きライトバックモードの有効化を中止したあとで、手順 4 に進みます。
Disabling	「キャッシュ保護付きライトバックモードを有効にする<<Bare metal>>」を参照して、キャッシュ保護付きライトバックモードの有効化を実行したあと、次の手順に進みます。

3. 手順 2 で取得したストレージクラスターの情報から、キャッシュ保護付きライトバックモードのキャッシュ保護用メタデータ冗長度のサマリーを確認します。

ストレージプールの一覧を取得し、ユーザーデータの保護種別(redundantType)を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

キャッシュ保護付きライトバックモードのキャッシュ保護用メタデータ冗長度のサマリー (metaDataRedundancyOfCacheProtectionSummary)が以下の表に示す条件を満たしているかを確認します。

ユーザーデータの保護種別 (redundantType)	条件
4D+1P	metaDataRedundancyOfCacheProtectionSummary の値が 1
4D+2P	metaDataRedundancyOfCacheProtectionSummary の値が 1 または 2
Duplication	metaDataRedundancyOfCacheProtectionSummary の値が 1

- ・ 条件を満たしている場合は、次の手順に進みます。
 - ・ 条件を満たしていない場合は、以下に従って対処してください。対処したあと次の手順に進みます。
 - VSP One SDS Block Administrator で、ストレージノードの Health Status に "Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
 - ストレージノードの一覧を取得して、status が"MaintenanceBlockage"のストレージノードがある場合は「ストレージノードを保守回復する<<Bare metal>>」に従って、ストレージノードを保守回復してください。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
 - イベントログ KARS06596-E が出力されている場合は、指示に従って対処を行い、キャッシュ保護用メタデータの冗長度が回復するまで待ってください。
4. 「リビルドの状態を確認する」を参照して、リビルドが実行中でないことを確認します。
リビルドが実行中でない場合は、次の手順に進みます。
リビルドが実行中の場合は、リビルドが完了するのを待ってから次の手順に進みます。

ただし、保守閉塞対象のストレージノードが、直前に回復されたストレージノードである場合は、次の手順に進むことができます。

5. 「ドライブデータ再配置の状態を確認する<<Bare metal>>」を参照して、ドライブデータ再配置が実行中でないことを確認します。

フォールトドメインが複数で構成されている場合は、ドライブデータ再配置は実行されないため、確認は不要です。

ドライブデータ再配置が実行中でない場合は、次の手順に進みます。

ドライブデータ再配置が実行中の場合は、完了するのを待つかドライブデータ再配置の中断を行ってから次の手順に進みます。

6. ストレージプールの情報から、ユーザーデータの冗長度(dataRedundancy)が以下の表に示す条件を満たしているかを確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

ユーザーデータの保護種別 (redundantType)	条件
4D+1P	dataRedundancy の値が 1
4D+2P	dataRedundancy の値が 2
Duplication	dataRedundancy の値が 1

- 条件を満たしている場合は、ストレージノードの保守閉塞ができるため、以上で確認手順は終了です。

ただし、ストレージプール拡張済みドライブを搭載していないストレージノードが存在する場合は、条件を満たしている場合でも次の手順に進んで確認を行う必要があります。

- 条件を満たしていない場合は、次の手順に進みます。

7. ストレージノードの一覧とドライブ一覧を取得し、障害の状態を確認します。

- ストレージノードの一覧取得

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

- ドライブの一覧取得

REST API : GET /v1/objects/drives

CLI : drive_list

ストレージノードとドライブの status を確認し、以下の表に示す条件を満たしているかを確認します。

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	条件
4D+1P	1	閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 0 ^{1,2}
4D+2P	1	以下のいずれかを満たすこと。 - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 1 以下^{1,2} - 保守閉塞対象のストレージノードが所属するスプレッドプレイスメントグループと同じスプレッドプレイスメントグループに所属している閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 1 以下^{1,2}

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	条件
	3	以下のいずれかを満たすこと。 - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 1 以下^{1,2} - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブ、および保守閉塞対象のストレージノードがすべて同じ 1 つのフォールトドメイン内に収まっている¹
Duplication	1	以下のいずれかを満たすこと。 - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 0^{1,2} - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブ、および保守閉塞対象のストレージノードが、冗長化されたストレージコントローラーが属する両方のストレージノードにまたがっていない。かつ、閉塞・閉塞失敗・減設失敗しているストレージノードと保守閉塞対象のストレージノードの中に、クラスターマスターノードが合計 2 ノード以上含まれていない。^{1,3}
	3	以下のいずれかを満たすこと。 - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 0^{1,2} - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブ、および保守閉塞対象のストレージノードがすべて同じ 1 つのフォールトドメイン内に収まっている¹ - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブ、および保守閉塞対象のストレージノードが、冗長化されたストレージコントローラーが属する両方のストレージノードにまたがっていない。かつ、閉塞・閉塞失敗・減設失敗しているストレージノードと保守閉塞対象のストレージノードの中に、クラスターマスターノードが合計 2 ノード以上含まれていない。^{1,3}
1. ストレージノードが閉塞・閉塞失敗している場合、status が以下のいずれかになります。 "TemporaryBlockage"、"MaintenanceBlockage"、"PersistentBlockage"、"InstallationFailed"、"TemporaryBlockageFailed"、"MaintenanceBlockageFailed"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、"RemovalFailedAndPersistentBlockage"、"RemovalFailedAndMultipleFailures" ストレージノードが減設失敗している場合、status が"RemovalFailed"の文字列を含んだものになります。 障害ドライブのステータス："Blockage" 2. 以下の場合は、対象内の障害をまとめて 1 として数えます。 - 閉塞・閉塞失敗・減設失敗しているストレージノード内に障害ドライブが存在している場合 - 同一ストレージノード内で障害ドライブが複数存在している場合 3. ストレージコントローラーの情報は以下で確認できます。 REST API : GET /v1/objects/storage-controllers CLI : storage_controller_list		

上記の表に記載した条件を満たす場合は、ストレージノードの保守閉塞の条件を確認する手順は終了です。

条件を満たさない場合は、以下に従って対処してください。対処することで、ストレージノードの保守閉塞の条件を確認する手順は終了です。

- VSP One SDS Block Administrator で、ストレージノードの Health Status に"Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
- status が"MaintenanceBlockage"のストレージノードがある場合は「ストレージノードを保守回復する<<Bare metal>>」に従って、ストレージノードを保守回復してください。
- 「リビルドの状態を確認する」を参照して、リビルドが動作中でないこと、およびリビルドでエラーが発生していないことを確認します。
リビルドが動作中、またはリビルドでエラーが発生している場合は「リビルドの状態を確認する」を参照して対処してください。

13.3.2 ストレージノードの保守閉塞の条件を確認する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ストレージノードが保守閉塞できるかどうかを以下の手順で確認してください。



注意

- ストレージノードの保守閉塞を実施すると、ユーザーデータ、ストレージコントローラー、クラスターマスターノードなどの冗長化されている要素の冗長度が低下します。保守閉塞したストレージノードを回復させるまでは耐障害性が低下することになるため、一度に保守閉塞を実施する範囲はなるべく必要最低限にとどめるようにしてください。
- 以下に記載した確認手順を行った場合でも、諸条件によって保守閉塞処理が失敗する可能性があります。その場合は、出力されるイベントログを参考に対処をしてください。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ストレージノードの保守閉塞の条件を確認する」

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ストレージノードの一覧を取得して、保守閉塞対象のストレージノードの ID と status を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

保守閉塞対象のストレージノードの status が"Ready"または"RemovalFailed"のとき、次の手順に進みます。

これら以外の status のストレージノードがある場合、以下に従って対処してください。

- status が"TemporaryBlockage"、"MaintenanceBlockage"、"PersistentBlockage"、"InstallationFailed"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、"RemovalFailedAndPersistentBlockage"の

場合は、対象のストレージノードは正常に閉塞されており、ストレージクラスターからの切り離しが完了している状態のため、基本的には保守閉塞の実施は不要です。
このため、再度保守閉塞の実施が必要な場合は、先に対象のストレージノードを回復させる必要があります。

- VSP One SDS Block Administrator で、ストレージノードの Health Status に"Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
ただし、"RemovalFailed"のストレージノードのみが存在する場合も"Alerting"になりますが、その場合は問題ありません。
 - 上記以外の status のストレージノードがあった場合は、それらストレージノードに対する処理が実施中のため、status が変わるのを待ってから、再度確認してください。
2. ストレージクラスターの情報を取得し、キャッシュ保護付きライトバックモードの状態を確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

キャッシュ保護付き ライトバックモードの状態	対応方法
Enabled	次の手順に進みます。
Disabled	手順 4 に進みます。
Enabling	「キャッシュ保護付きライトバックモードを有効にする<<Cloud>>」を参照して、キャッシュ保護付きライトバックモードの有効化を実行したあと、次の手順に進みます。 または、キャッシュ保護付きライトバックモードの有効化を中止したあとで、手順 4 に進みます。
Disabling	「キャッシュ保護付きライトバックモードを有効にする<<Cloud>>」を参照して、キャッシュ保護付きライトバックモードの有効化を実行したあと、次の手順に進みます。

3. 手順 2 で取得したストレージクラスターの情報から、キャッシュ保護付きライトバックモードのキャッシュ保護用メタデータ冗長度のサマリーを確認します。

ストレージプールの一覧を取得し、ユーザーデータの保護種別(redundantType)を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

キャッシュ保護付きライトバックモードのキャッシュ保護用メタデータ冗長度のサマリー(metaDataRedundancyOfCacheProtectionSummary)が以下の表に示す条件を満たしているかを確認します。

ユーザーデータの保護種別 (redundantType)	条件
4D+2P	metaDataRedundancyOfCacheProtectionSummary の値が 1 または 2
Duplication	metaDataRedundancyOfCacheProtectionSummary の値が 1

- 条件を満たしている場合は、次の手順に進みます。

- 条件を満たしていない場合は、以下に従って対処してください。対処したあと次の手順に進みます。
 - VSP One SDS Block Administrator で、ストレージノードの Health Status に "Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
 - ストレージノードの一覧を取得して、status が"MaintenanceBlockage"のストレージノードがある場合は「ストレージノードの保守回復」に従って、ストレージノードを保守回復してください。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
 - イベントログ KARS06596-E が出力されている場合は、指示に従って対処を行い、キャッシュ保護用メタデータの冗長度が回復するまで待ってください。

4. 「リビルドの状態を確認する」を参照して、リビルドが実行中でないことを確認します。

リビルドが実行中でない場合は、次の手順に進みます。

リビルドが実行中の場合は、リビルドが完了するのを待ってから次の手順に進みます。

ただし、保守閉塞対象のストレージノードが、直前に回復されたストレージノードである場合は、次の手順に進むことができます。

5. ストレージプールの情報から、ユーザーデータの冗長度(dataRedundancy)が以下の表に示す条件を満たしているかを確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

ユーザーデータの保護種別 (redundantType)	条件
4D+2P	dataRedundancy の値が 2
Duplication	dataRedundancy の値が 1

- 条件を満たしている場合は、ストレージノードの保守閉塞ができるため、以上で確認手順は終了です。
ただし、ストレージプール拡張済みドライブを搭載していないストレージノードが存在する場合は、条件を満たしている場合でも次の手順に進んで確認を行う必要があります。
- 条件を満たしていない場合は、次の手順に進みます。

6. ストレージノードの一覧とドライブ一覧を取得し、障害の状態を確認します。

- ストレージノードの一覧取得
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
- ドライブの一覧取得
REST API : GET /v1/objects/drives
CLI : drive_list

ストレージノードとドライブの status を確認し、以下の表に示す条件を満たしているかを確認します。

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	条件
4D+2P	1	以下のいずれかを満たすこと。

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	条件
		- 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 1 以下^{1,2} 《Cloud for AWS》保守閉塞対象のストレージノードが所属するスプレッドブレイスメントグループと同じスプレッドブレイスメントグループに所属している閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 1 以下^{1,2,4} 《Cloud for Google Cloud》保守閉塞対象のストレージノードが所属するスプレッドブレイスメントポリシーと同じスプレッドブレイスメントポリシーに所属している閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 1 以下^{1,2,4} 《Cloud for Microsoft Azure》保守閉塞対象のストレージノードが所属するスケールセットと同じスケールセットに所属している閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 1 以下^{1,2,4}
Duplication	1	以下のいずれかを満たすこと。 - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 0^{1,2} - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブ、および保守閉塞対象のストレージノードが、冗長化されたストレージコントローラーが属する両方のストレージノードにまたがっていない。かつ、閉塞・閉塞失敗・減設失敗しているストレージノードと保守閉塞対象のストレージノードの中に、クラスターマスターノードが合計 2 ノード以上含まれていない。^{1,3}
	3	以下のいずれかを満たすこと。 - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブの合計数が 0^{1,2} - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブ、および保守閉塞対象のストレージノードがすべて同じ 1 つのフォールトドメイン内に収まっている¹ - 閉塞・閉塞失敗・減設失敗しているストレージノードと障害ドライブ、および保守閉塞対象のストレージノードが、冗長化されたストレージコントローラーが属する両方のストレージノードにまたがっていない。かつ、閉塞・閉塞失敗・減設失敗しているストレージノードと保守閉塞対象のストレージノードの中に、クラスターマスターノードが合計 2 ノード以上含まれていない。^{1,3}
1. ストレージノードが閉塞・閉塞失敗している場合、status が以下のいずれかになります。 "TemporaryBlockage"、"MaintenanceBlockage"、"PersistentBlockage"、"InstallationFailed"、"TemporaryBlockageFailed"、"MaintenanceBlockageFailed"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、"RemovalFailedAndPersistentBlockage"、"RemovalFailedAndMultipleFailures" ストレージノードが減設失敗している場合、status が"RemovalFailed"の文字列を含んだものになります。 障害ドライブのステータス："Blockage" 2. 以下の場合は、対象内の障害をまとめて 1 として数えます。		

ユーザーデータの保護種別 (redundantType)	フォールトドメイン数	条件
		- 閉塞・閉塞失敗・減設失敗しているストレージノード内に障害ドライブが存在している場合 - 同一ストレージノード内で障害ドライブが複数存在している場合 3. ストレージコントローラーの情報は以下で確認できます。 REST API : GET /v1/objects/storage-controllers CLI : storage_controller_list 4. ≪Cloud for AWS≫各ストレージノード VM が所属しているスプレッドブレイスメントグループは AWS マネジメントコンソールから確認できます。 ≪Cloud for Google Cloud≫各ストレージノード VM が所属しているスプレッドブレイスメントポリシーは Google Cloud コンソールから確認できます。 ≪Cloud for Microsoft Azure≫各ストレージノード VM が所属しているスケールセットは Azure ポータルから確認できます。

上記の表に記載した条件を満たす場合は、ストレージノードの保守閉塞の条件を確認する手順は終了です。

条件を満たさない場合は、以下に従って対処してください。対処することで、ストレージノードの保守閉塞の条件を確認する手順は終了です。

- VSP One SDS Block Administrator で、ストレージノードの Health Status に"Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
- status が"MaintenanceBlockage"のストレージノードがある場合は「ストレージノードの保守回復≪Cloud≫」に従って、ストレージノードを保守回復してください。
- 「リビルドの状態を確認する」を参照して、リビルドが動作中でないこと、およびリビルドでエラーが発生していないことを確認します。
リビルドが動作中、またはリビルドでエラーが発生している場合は「リビルドの状態を確認する」を参照して対処してください。

13.3.3 ストレージノードを保守閉塞する≪Bare metal≫

この項での記述内容は Bare metal モデルに適用されます。

ストレージノードの保守閉塞は、ストレージノードを一時的にストレージクラスターから切り離し、部品交換などの保守が可能な状態にする処理です。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- ストレージノードの保守閉塞中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの保守閉塞が完了するのを待ってから再度これらの操作を実施してください。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ストレージノードを保守閉塞する」

前提条件

- ・ 「ストレージノードの保守閉塞の条件を確認する <<Bare metal>>」に記述した条件を満足していること
- ・ 実行に必要なロール : Service

操作手順

1. 保守閉塞を実行します。
ストレージノードの ID を指定してコマンドを実行します。
REST API : POST /v1/objects/storage-nodes/<id >/actions/block-for-maintenance/invoke
CLI : storage_node_block_for_maintenance
コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
3. ストレージノードの情報を取得して、保守閉塞されたことを確認します。
ストレージノードの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/storage-nodes/<id >
CLI : storage_node_show
コマンド実行後のレスポンスで、status が "MaintenanceBlockage" または "RemovalFailedAndMaintenanceBlockage" であれば、保守閉塞が完了しています。
ストレージノードがパワーオフの状態になります。



注意

- ・ クラスターマスターノードの保守閉塞中に REST API/CLI を発行すると、REST API/CLI が KARS15506-E で失敗する可能性があります。REST API/CLI が KARS15506-E で失敗した場合は、しばらく待ってから(最大約 60 分)、再度 REST API/CLI を実行してください。
- ・ 保守閉塞中のストレージノードに障害が発生した場合、手順 2、3 で確認するジョブの state とストレージノードの status が期待どおりだった場合でも、ストレージノードがパワーオンの状態になることがあります。そのときは、OS のシャットダウン操作によってストレージノードの停止を実施してください。OS のシャットダウン操作後、約 5 分経過しても停止できない場合は、強制停止操作によってストレージノードの停止を行ってください。

メモ



- ・ OS のシャットダウン、強制停止の操作方法は、ハードウェアのマニュアルを参照してください。
- ・ 日立アドバンストサーバ HA8000V シリーズを使用している場合、OS のシャットダウンは、iLO の「電力管理」にて「瞬間的に押す」による停止となります。また、強制停止は、iLO の「電力管理」にて「押し続ける」による停止となります。具体的な操作方法はハードウェアのマニュアルを参照してください。日立アドバンストサーバ HA8000V シリーズ以外の物理サーバーを使用している場合、OS のシャットダウン、強制停止の具体的な操作方法は、各ハードウェアのマニュアルを参照してください。

13.3.4 ストレージノードを保守閉塞する<<Cloud for AWS>>

この項での記述内容は Cloud モデル for AWS に適用されます。

ストレージノードの保守閉塞は、ストレージノードを一時的にストレージクラスターから切り離し、部品交換などの保守が可能な状態にする処理です。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- ストレージノードの保守閉塞中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの保守閉塞が完了するのを待ってから再度これらの操作を実施してください。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ストレージノードを保守閉塞する」

前提条件

- 「ストレージノードの保守閉塞の条件を確認する<<Cloud>>」に記述した条件を満足していること
- 実行に必要なロール：Service

操作手順

1. 保守閉塞を実行します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : POST /v1/objects/storage-nodes/<id >/actions/block-for-maintenance/invoke

CLI : storage_node_block_for_maintenance

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

3. ストレージノードの情報を取得して、保守閉塞されたことを確認します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/storage-nodes/<id >

CLI : storage_node_show

コマンド実行後のレスポンスで、status が"MaintenanceBlockage"または"RemovalFailedAndMaintenanceBlockage"であれば、保守閉塞が完了しています。ストレージノード VM がパワーオフの状態になります。



注意

- ・ クラスターマスターノードの保守閉塞中に REST API/CLI を発行すると、REST API/CLI が KARS15506-E で失敗する可能性があります。REST API/CLI が KARS15506-E で失敗した場合は、しばらく待ってから(最大約 60 分)、再度 REST API/CLI を実行してください。
- ・ 保守閉塞中のストレージノードに障害が発生した場合、手順 2、3 で確認するジョブの state とストレージノードの status が期待どおりだった場合でも、ストレージノード VM(EC2 インスタンス)がパワーオン状態になることがあります。そのときは、EC2 インスタンスの停止操作によって EC2 インスタンスを停止してください。

EC2 インスタンスの停止操作後、約 5 分経過しても停止できない場合は、強制停止操作によって EC2 インスタンスを停止してください。強制停止は、AWS マネジメントコンソールの EC2 インスタンスの停止操作で実施してください。

メモ



- ・ EC2 インスタンスの停止方法は、AWS のマニュアルを参照してください。
- ・ EC2 インスタンスの強制停止は、EC2 インスタンスが停止中(stopping)の状態のままのときに再度 EC2 インスタンスの停止操作を行うことで実行できます。詳しい操作方法は AWS のマニュアルを参照してください。

13.3.5 ストレージノードを保守閉塞する<<Cloud for Google Cloud>>

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージノードの保守閉塞は、ストレージノードを一時的にストレージクラスターから切り離し、部品交換などの保守が可能な状態にする処理です。



注意

- ・ 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- ・ ストレージノードの保守閉塞中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの保守閉塞が完了するのを待ってから再度これらの操作を実施してください。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ストレージノードを保守閉塞する」

前提条件

- ・ 「ストレージノードの保守閉塞の条件を確認する<<Cloud>>」に記述した条件を満足していること
- ・ 実行に必要なロール : Service

操作手順

1. 保守閉塞を実行します。
ストレージノードの ID を指定してコマンドを実行します。

REST API : POST /v1/objects/storage-nodes/<id >/actions/block-for-maintenance/invoke

CLI : storage_node_block_for_maintenance

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

3. ストレージノードの情報を取得して、保守閉塞されたことを確認します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/storage-nodes/<id >

CLI : storage_node_show

コマンド実行後のレスポンスで、status が"MaintenanceBlockage"または

"RemovalFailedAndMaintenanceBlockage"であれば、保守閉塞が完了しています。

ストレージノード VM がパワーオフの状態になります。



注意

- ・ クラスターマスターノードの保守閉塞中に REST API/CLI を発行すると、REST API/CLI が KARS15506-E で失敗する可能性があります。REST API/CLI が KARS15506-E で失敗した場合は、しばらく待ってから(最大約 60 分)、再度 REST API/CLI を実行してください。
- ・ 保守閉塞中のストレージノードに障害が発生した場合、手順 2、3 で確認するジョブの state とストレージノードの status が期待どおりだった場合でも、ストレージノード VM(Compute Engine インスタンス)がパワーオン状態になることがあります。そのときは、Compute Engine インスタンスの停止操作によって Compute Engine インスタンスを停止してください。
Compute Engine インスタンスの停止操作を行っても停止されない場合は、約 90 秒後に Google Cloud によって自動的に強制停止されます。



メモ

Compute Engine インスタンスの停止方法は、Google Cloud のマニュアルを参照してください。

13.3.6 ストレージノードを保守閉塞する<<Cloud for Microsoft Azure>>

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージノードの保守閉塞は、ストレージノードを一時的にストレージクラスターから切り離し、部品交換などの保守が可能な状態にする処理です。



注意

- ・ 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- ・ ストレージノードの保守閉塞中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの保守閉塞が完了するのを待ってから再度これらの操作を実施してください。

VSP One SDS Block Administrator で実施する場合

この操作は VSP One SDS Block Administrator でも実施できます。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ストレージノードを保守閉塞する」

前提条件

- ・ 「ストレージノードの保守閉塞の条件を確認する <<Cloud>>」に記述した条件を満足していること
- ・ 実行に必要なロール：Service

操作手順

1. 保守閉塞を実行します。
ストレージノードの ID を指定してコマンドを実行します。
REST API : POST /v1/objects/storage-nodes/<id >/actions/block-for-maintenance/invoke
CLI : storage_node_block_for_maintenance
コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
3. ストレージノードの情報を取得して、保守閉塞されたことを確認します。
ストレージノードの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/storage-nodes/<id >
CLI : storage_node_show
コマンド実行後のレスポンスで、status が"MaintenanceBlockage"または"RemovalFailedAndMaintenanceBlockage"であれば、保守閉塞が完了しています。
ストレージノード VM がパワーオフの状態になります。
4. Azure ポータルから、保守閉塞されたストレージノード VM(Azure VM インスタンス)の状態が「停止済み(割り当て解除)」となっていることを確認します。



注意

Azure ポータルから、保守閉塞された Azure VM インスタンスの状態が「停止済み(割り当て解除)」となっていることを確認してください。「停止済み(割り当て解除)」になっていない場合は、Azure ポータルから該当の Azure VM インスタンスを停止し、「停止済み(割り当て解除)」にしてください。

Microsoft Azure では、Azure VM インスタンスの状態が「停止済み」の場合、Azure VM インスタンスの課金状態が継続されます。「停止済み(割り当て解除)」の場合は課金状態が継続されません(ディスクの課金状態は継続されます)。停止方法は、Microsoft Azure のマニュアルを確認してください。



注意

- ・ クラスターマスターノードの保守閉塞中に REST API/CLI を発行すると、REST API/CLI が KARS15506-E で失敗する可能性があります。REST API/CLI が KARS15506-E で失敗した場合は、しばらく待ってから(最大約 60 分)、再度 REST API/CLI を実行してください。
- ・ 保守閉塞中のストレージノードに障害が発生した場合、手順 2、3 で確認するジョブの state とストレージノードの status が期待どおりだった場合でも、ストレージノード VM(Azure VM インスタンス)がパワーオンの状態になることがあります。そのときは、Azure VM インスタンスの停止操作によって Azure VM インスタンスを停止してください。
Azure VM インスタンスの停止操作を行っても停止されない場合は、約 10 分後に Microsoft Azure によって自動的に強制停止されます。



メモ

Azure VM インスタンスの停止方法は、Microsoft Azure のマニュアルを参照してください。

13.4 ストレージノードの交換

ストレージノードの交換方法を説明します。

13.4.1 ストレージノードを交換する《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

ストレージノードの交換は、手動または障害によって閉塞されたストレージノードに対して実施できる処理です。手動でストレージノードを閉塞する手順は「ストレージノードの保守閉塞の条件を確認する《Bare metal》」と「ストレージノードを保守閉塞する《Bare metal》」を参照してください。

ストレージノードの交換では、ユーザーデータが格納された閉塞時と同じドライブを使い回して交換する場合と、閉塞時とは異なるドライブを搭載したストレージノードで交換する場合で、手順が異なります。

フォールトドメイン障害を含む複数のストレージノードを交換する場合は、ストレージノードの交換操作は、1 ストレージノードずつ実施してください。

ストレージノード交換後には、データの冗長度を回復させるためのリビルドが実行されます。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。

ストレージノードの交換操作は 1 ストレージノードずつシリアルに実施するため、複数のストレージノード交換を行う場合に掛かる時間は、交換対象のストレージノード数×ストレージノードの交換時間になります。

物理サーバーまたはハードウェア部品を交換する場合は「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載してある物理サーバーまたはハードウェア部品を選択してください。

物理サーバーを継続使用して、ストレージノードを回復させることもできます。

ハードウェアごとに交換条件が異なるため、このマニュアルの「ハードウェア交換の条件《Bare metal》」を確認し、条件を満たすハードウェアを使用してください。

交換前と交換後のストレージノードで、管理ポートのチーミング機能の設定(冗長構成または非冗長構成)に違いがあっても、ストレージノード交換は可能です。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - VSP One SDS Block の構成情報の変更・設定
 - 構成ファイルのエクスポート

ストレージノードの交換は、コンローラーノード上から操作して行います。

ストレージノードの交換では、構成ファイルを使用しなくても実施可能です。

フォールトドメイン障害を含む複数のストレージノードを交換する場合は、ストレージノードの交換操作(手順 1 から 11)は、1 ストレージノードずつ実施してください。



注意

- 交換するストレージノードのメモリーは、プロテクションドメインに属するストレージノード内で最小のメモリー容量以上である必要があります。プロテクションドメイン情報から `minimumMemorySize[MiB]` を参照し、交換するストレージノードのメモリーの値を確認してください。ストレージノードに搭載されているメモリー容量が条件を満たしていないときは、条件を満たすようにメモリーを増設してください。
- 「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の指示に従って、この節に記載されている手順を再度実施する際に、「ストレージソフトウェアのインストール」と「ストレージノード単位のセットアップ」の実施が不要と指示されている場合があります。その場合は、この節に記載されている交換対象のストレージノードに対する「ストレージソフトウェアのインストール」と「ストレージノード単位のセットアップ」の手順を省略してください。
- ストレージクラスターにスペアノードとして登録されている物理サーバーを対象に、手動でストレージノード交換を実施することはできません。手動でストレージノード交換を行う際には、ストレージクラスターにスペアノードとして登録されていない物理サーバーを使用してください。
- ストレージノードの交換中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの交換が完了するのを待ってから再度これらの操作を実施してください。

前提条件

- 実行に必要なロール : Service と Storage
- 以下のどちらかを満たしていること
 - 回復対象のストレージノードの `status` が "TemporaryBlockage" でないこと
 - ストレージノードの自動回復機能の設定が無効であること

この条件を満たさない状態で、手動によるストレージノードの交換を実施すると、手動によるストレージノードの交換が失敗します。自動回復機能の設定が有効の場合、ストレージノードの自動回復機能の動作条件を満たすことで、`status` が "TemporaryBlockage" のストレージノードは、自動回復機能によって自動で回復されるため、手動によるストレージノードの交換の実施は不要です。

操作手順

1. 交換前のストレージノードがネットワーク接続されている場合は、ネットワークから切り離します。

このとき、対象のストレージノードを間違えないように注意してください。



注意

物理サーバーを変更する場合、期待外に交換前のストレージノードの OS が起動すると、ストレージノードに残っているネットワーク設定によって、IP アドレス重複などのトラブルを引き起こす可能性があります。そのため、OS が期待外に起動しないような対処(システムディスクのデータの消去や使用していたシステムディスクをブート対象から外すなど)およびネットワークからの切り離しを行ってください。物理サーバーの操作方法は、ハードウェアベンダーのマニュアルを参照してください。

2. 交換用ストレージノードのネットワークの物理結線と LAN スイッチの設定を完了させてから、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の以下に記載されている構築準備を行います。

- ・ 「ストレージノードを準備する」



メモ

物理サーバーを継続使用している場合は、本手順の再実施は不要です。

3. Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の以下の手順を行い、交換対象のストレージノードに対してストレージソフトウェアのインストールを行います。

- ・ 「ストレージソフトウェアをインストールする」



注意

「ストレージソフトウェアをインストールする」の手順で使用するストレージソフトウェアインストーラー(hsds-installer-vssb-<version>-<number>.iso)のバージョンは、交換対象のストレージノードのバージョンに合わせる必要があります。交換対象のストレージノードのバージョンは以下のコマンドで確認できます。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

4. Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の以下の手順を行い、交換対象のストレージノードに対してストレージノード単位のセットアップを行います。

- ・ 「ストレージノード単位のセットアップを行う」

この手順を実施する際は、新規の設定値ではなく、ストレージクラスター内の構成情報に登録されている交換対象のストレージノードと同じ設定値を入力する必要があります。設定値の確認方法についても上記の手順に記載してありますので、参照してください。

5. 以下の手順によって、システム要件ファイルの更新を実施します。
 - a. 最新のシステム要件ファイル(SystemRequirementsFile.yml)をサポートセンターから入手して、コントローラーノードに格納します。



注意

システム要件ファイルの名称は、SystemRequirementsFile.yml から変更しないでください。

- b. システム要件ファイルを指定して以下のコマンドを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : POST /v1/objects/system-requirements-file/actions/import/invoke

CLI : system_requirements_file_import

指定したシステム要件ファイルのバージョンが、VSP One SDS Block にインポート済みのバージョンより新しい場合のみインポート処理が行われます。指定したシステム要件ファ

イルのバージョンが同じか古い場合は、イベントログを出力しインポート処理をスキップします。

コマンド実行後に表示されるジョブの ID を確認します。

- c. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

6. 交換対象のストレージノードの ID と status を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

交換対象のストレージノードの status が"MaintenanceBlockage"、"PersistentBlockage"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、または"RemovalFailedAndPersistentBlockage"であることを確認し、次の手順に進みます。

ただし、ストレージノードの自動回復機能の設定が無効の場合は、交換対象のストレージノードの status が"TemporaryBlockage"の場合も次の手順に進みます。

7. ストレージノードを交換します。

REST API : POST /v1/objects/storage-nodes/<id >/actions/replace/invoke

CLI : storage_node_replace

上記コマンド実行時に以下の情報をパラメーターとして指定する必要があります。

- ・ 手順 4 の「ストレージノード単位のセットアップを行う」の手順内で設定したセットアップユーザーのパスワード

コマンド実行後に表示されるジョブの ID を確認します。



メモ

ストレージクラスターにスペアノードが登録されている場合、ジョブの完了後にイベントログ KARS10733-W が出力されることがあります。これは、以降の手順で実施する「ストレージノードの BMC 情報を登録・編集する<<Bare metal>>」を実施することで解決します。



メモ

- ・ 本手順によって開始されるストレージノード交換ジョブの実行中は、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノード単位のセットアップを行う」に示される手順は実施できません。
 - ・ この操作を実施した際に、以下のイベントログが出力されることがあります。これは、正常な動作のため、そのまま手順を継続してください。
 - KARS20067-I
 - KARS20068-I
 - KARS20069-I
 - ・ ストレージノード交換のジョブの動作条件
以下の条件を満たさず、ジョブが失敗した際は、イベントログを参照して対処してください。
 - ストレージクラスターの status が"Ready"であること
 - 対象のストレージノードが閉塞していること
 - クラスターマスターノード(プライマリー)から、対象のストレージノードへ管理ネットワークで接続ができること
-

8. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

交換が完了するまでは、他の操作が実施できないことがあります。他の操作が失敗した場合は、他の操作のエラーメッセージやイベントログに従って対処してください。



注意

- ジョブの完了まで約 35 分掛かります。また、リビルド(データ再構築)が実行中のときは、さらに最大で 5 分ほど処理時間が長くなる可能性があります。
- その他、以下の外部要因によって処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。
 - ネットワークの通信状況(ストレージノードの相互間の通信状況)
 - サーバーの性能状況(ストレージノードの温度上昇による性能低下など)
 - ストレージノードの起動時間(物理サーバーの起動に時間が掛かる場合など)
 - サーバーのハードウェア構成(ストレージノードのプロセッサ、メモリー容量など)
- ジョブの処理中に、KARS10914-W または KARS10915-W のイベントログが出力された場合は、チーミング構成が組まれている管理ポートまたはストレージノード間ポートのネットワーク上に一部が接続できないパスが存在している可能性があります。チーミング構成が組まれている場合は、そのままの状態でもストレージクラスターとしての稼働は可能ですが、メッセージに含まれるネットワークパスについて「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「最初にチェックする項目」に記載されているネットワークの接続および設定に関する項目を確認し、問題があれば対処することをお勧めします。

また、問題の対処後に管理ポートまたはストレージノード間ポートの接続を VSP One SDS Block 環境で確認する場合は、以下を実施してください。

(KARS10914-W または KARS10915-W のイベントログが出力されたあとに、KARS08304-I、KARS08305-I、KARS08306-I、KARS08313-I、KARS08314-I、KARS08315-I などのリンク状態の回復を示すイベントログが出力された場合でも、到達性は保証できていないため、リンク状態以外の到達性に懸念がある場合は、以下に示す方法などで接続確認を行うことをお勧めします。)

 - 接続確認の再実施(ストレージノード交換)

ストレージノード単位での接続確認を再実施するためには、接続確認でエラーになった接続元ポートが存在するストレージノードに対してストレージノード交換を 1 ノードずつ実施してください。ストレージクラスター全体の停止は発生しません。対象のストレージノードが閉塞していない場合はストレージノード交換の前にストレージノード保守閉塞を実施してください。ストレージノード保守閉塞については「ストレージノードを保守閉塞する」を参照してください。

ストレージノード交換が正常終了して、かつ KARS10914-W または KARS10915-W のイベントログが出力されなければ、対象のストレージノードの管理ポートおよびストレージノード間ポートのネットワークの接続状態は問題ありません。



メモ

- この手順を実施した際に、イベントログ KARS16018-W、KARS16143-W が出力されることがあります。また、閉塞時と異なるドライブを搭載したストレージノードで交換する場合、交換前のドライブに対してイベントログ KARS05010-E、KARS07005-E、および KARS06596-E が出力されることがあります。このタイミングでこれらのイベントログが発生することは問題ではなく、以降の処理がこれらイベントログへの対処となりますので、そのまま手順を継続してください。

- ・ ストレージノード交換ジョブが何らかの理由でエラーとなった場合は、エラー処理によってストレージノードの電源オフが実行されます。ただし、ネットワークの障害などによって電源オフの処理が正常に実行できないことがあります。ストレージノード交換ジョブがエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Blockトラブルシューティングガイド」に従って対処してください。

9. ストレージノードの一覧を取得して、交換したストレージノードの ID の status を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

status が "Ready" または "RemovalFailed" であれば、ストレージノードの交換が完了しています。

10. ストレージクラスターにスペアノードが登録されている場合は、交換したストレージノードに対して「スペアノードを利用するための BMC アカウントを準備する <<Bare metal>>」と「ストレージノードの BMC 情報を登録・編集する <<Bare metal>>」を実施し、BMC の情報を登録してください。

ストレージクラスターに対して「ストレージクラスターに BMC 接続検証用ルート証明書をインポートする <<Bare metal>>」を実施している場合は、交換したストレージノードの BMC に対して BMC の IP アドレスまたは IP アドレスに対応する FQDN を Common Name(CN) または Subject Alternative Name(SAN) に設定したサーバー証明書をインポートしてください。BMC のサーバー証明書の作成および BMC へのサーバー証明書のインポートについては、サーバーベンダーのマニュアルを参照してください。

その後、交換したストレージノードが、スペアノードに切り換えできる状態になっているかを「スペアノード機能の設定を確認する <<Bare metal>>」を参照して確認してください。



メモ

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される次のフィールドがサポートされます。

- ・ 基本制限(Basic Constraints)
- ・ キー使用法(Key Usage)
- ・ サブジェクトキー識別子(Subject Key Identifier)
- ・ 機関キー識別子(Authority Key Identifier)
- ・ 証明書ポリシー(Certificate Policies)
- ・ サブジェクト代替名(Subject Alternative Name)
- ・ 名前の制限(Name Constraints)
- ・ ポリシーの制限(Policy Constraints)
- ・ 拡張キー使用法(Extended Key Usage)
- ・ ポリシー禁止(Inhibit anyPolicy)

11. 閉塞時と同じユーザーデータが格納されたドライブを使い回してストレージノードを交換する場合は、以上で手順は終了です。

閉塞時とは異なるドライブを搭載したストレージノードで交換する場合は、次の手順に進みます。

12. 拡張前のストレージプールの総物理容量とストレージプールの ID を確認します。

CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

13. ドライブの一覧を取得します。

クエリーパラメーター `storageNodeId` に交換したストレージノードの ID、クエリーパラメーター `status` に "Offline" を指定してコマンドを実行します。

REST API : GET /v1/objects/drives

CLI : `drive_list`

14. ストレージプールを拡張します。

ストレージプールの ID と手順 13 で取得したドライブの ID を指定してコマンドを実行します。

CLI を使う場合はストレージプールの ID の代わりに名前が指定できます。

REST API : POST /v1/objects/pools/<id>/actions/expand/invoke

CLI : `pool_expand`

コマンド実行後に表示されるジョブの ID を確認します。



メモ

コマンドを実行する際に指定したドライブの ID を記録しておいてください。記録した情報は手順 20 で使用します。

15. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : `job_show`

state が "Succeeded" になっていたらジョブは完了です。

16. ストレージプールの情報を取得します。

REST API : GET /v1/objects/pools

CLI : `pool_list`

拡張前に比べて拡張後のストレージプールの総物理容量が拡張されたことを確認します。

17. 「キャッシュ保護用メタデータの冗長度を確認する<<Bare metal>>」を参照して、冗長度が低下していないことを確認します。

冗長度が低下していない場合は、次の手順に進みます。

冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。イベントログ KARS06596-E が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 17 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

18. 「リビルドの状態を確認する」を参照して、リビルドの完了を確認します。

19. ドライブの一覧を取得します。

クエリーパラメーター `storageNodeId` に交換したストレージノードの ID、クエリーパラメーター `status` に "Blockage" を指定してコマンドを実行します。

REST API : GET /v1/objects/drives

CLI : `drive_list`

20. ストレージプールに残されている交換前のドライブの構成情報を削除します。

手順 19 で取得したドライブの ID を指定してコマンドを実行します。



メモ

このとき、指定するドライブの ID に手順 14 で記録したドライブの ID が含まれていないことを確認してください。含まれている場合、そのドライブの ID を除いてコマンドを実行してください。

除いたドライブは、ストレージノード交換手順がすべて完了したあとに「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

REST API : POST /v1/objects/drives/<id >/actions/remove/invoke

CLI : drive_remove

コマンド実行後に表示されるジョブの ID を確認します。

21. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

22. 減設対象のドライブの一覧を取得します。

ストレージノードの ID をクエリーパラメーターで指定してコマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

交換前のドライブの情報が削除されていることを確認します。

23. 構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

13.4.2 ストレージノードを交換する <<Cloud for AWS>>

この項での記述内容は Cloud モデル for AWS に適用されます。

ストレージノードの交換は、手動または障害によって閉塞されたストレージノードに対して実施できる処理です。手動でストレージノードを閉塞する手順は「ストレージノードの保守閉塞の条件を確認する <<Cloud>>」と「ストレージノードを保守閉塞する <<Cloud for AWS>>」を参照してください。

閉塞時と異なるドライブによるストレージノード交換のみサポートされています。

フォールトドメイン障害を含む複数のストレージノードを交換する場合は、ストレージノードの交換操作は、1 ストレージノードずつ実施してください。

ストレージノード交換後には、データの冗長度を回復させるためのリビルドが実行されます。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。

ストレージノードの交換操作は 1 ストレージノードずつシリアルに実施するため、複数のストレージノード交換を行う場合に掛かる時間は、交換対象のストレージノード数×ストレージノードの交換時間になります。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イ

ベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。

- 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - 構成ファイルのエクスポート
 - ドライブの増設
 - ドライブの交換
- ストレージソフトウェアのバージョンが 01.17.0x.30 のストレージノードとストレージソフトウェアのバージョンが 01.18.0x.30 以降のストレージノードが混在している構成で、01.17.0x.30 のストレージノードを交換する場合は、ストレージソフトウェアのバージョン(01.17.0x.30)に対応した「Hitachi Virtual Storage Platform One SDS Block オペレーションガイド」の「ストレージノードを交換する<<Cloud>>」を実施してください。
01.18.0x.30 以降のストレージノードを交換する場合は、このマニュアルの「ストレージソフトウェアのバージョンが混在している場合のストレージノード交換<<Cloud for AWS>>」を実施してください。

ストレージノードの交換は、コントローラーノード上から操作して行います。

ストレージノードの交換では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作します。

複数のストレージノードを交換する場合は、ストレージノードの交換操作(手順 3 から 7)は、1 ストレージノードずつ実施してください。

Multi-AZ 構成でタイブレーカーノードを交換する場合は、手順 9 以降の操作は不要です。



注意

- ストレージノードの交換中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあるため、EC2 インスタンスに対する操作はしないでください。失敗した場合は、ストレージノードの交換が完了するのを待ってから再度これらの操作を実施してください。
- EBS 暗号化を利用している場合は、AWS を操作するアカウントやコントローラーノードに設定する IAM ロールに、AWS Key Management Service へアクセスするための権限を追加する必要があります。詳細は、AWS のユーザーガイドを参照してください。
- 交換前の EC2 インスタンスはストレージノードの交換中に自動的に削除されます。
- AWS コンソール上では、削除した EC2 インスタンスの情報はすぐには削除されず、しばらく残ります。その間、交換対象のストレージノードと同名の EC2 インスタンスが複数表示されます。



メモ

- 交換前と交換後でストレージノード VM の EC2 インスタンスタイプは変わりません。
- status が "TemporaryBlockage"、"PersistentBlockage" のストレージノードに対して、ストレージノードの交換を実施すると、status が一時的に "MaintenanceBlockage" になります。また、status が "RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndPersistentBlockage" のストレージノードに対して、ストレージノードの交換を実施すると、status が一時的に "RemovalFailedAndMaintenanceBlockage" になります。このとき、メッセージ中の Operation が "STORAGE_NODE_BLOCK_FOR_MAINTENANCE" である、ジョブの開始(KARS13009-I)と完了(KARS13010-I または KARS13011-I)を示すイベントログが出力されます。

前提条件

- 実行に必要なロール : Service と Storage

操作手順

1. コントローラーノードにログインします。
2. ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。
REST API : GET /v1/objects/storage
CLI : storage_show
3. コントローラーノードで以下のコマンドを実行してスタックのテンプレートのバージョンを確認します。

```
aws cloudformation describe-stacks ¥  
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥  
--query ¥  
'Stacks[0].Outputs[?OutputKey=='TemplateVersion'].OutputValue' ¥  
--output text
```

スタックのテンプレートのバージョンがストレージソフトウェアのバージョンと同じ場合は、次の手順に進みます。スタックのテンプレートのバージョンが取得できなかった場合やストレージソフトウェアのバージョンと異なる場合は「ソフトウェアアップデート後に必要な操作」の手順に従って、スタックのテンプレートのバージョンをアップデートしてから次の手順に進みます。



注意

- ・ 直前に実施したストレージソフトウェアアップデートが正常に完了していない状態で、ストレージノードを交換する場合は、スタックのテンプレートのバージョンを交換対象のストレージノードのバージョンに合わせる必要があります。交換対象のストレージノードのバージョンは以下のコマンドで確認できます。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

- ・ スタックのテンプレートバージョンが取得できなかった場合や、交換対象のストレージノードのバージョンと異なる場合は「ソフトウェアアップデート後に必要な操作」の手順に従って、スタックのテンプレートのバージョンをアップデートしてからストレージノードの交換を行います。

4. 「構成ファイルをエクスポートする<<Cloud for AWS>>」を参照し、VSP One SDS Block から構成ファイルを取得します。

構成ファイルをエクスポートする際は、exportFileType パラメーターに"ReplaceStorageNode"を指定してください。

また、machineImageId パラメーターに手順 2 で確認したストレージソフトウェアのバージョンに合わせた AMI ID を必ず指定してください。

最新状態の構成ファイルを使用するために、ストレージノード交換用の構成ファイルは必ず取得してください。



メモ

直前に実施したストレージソフトウェアアップデートが正常に完了していない状態で、ストレージノード交換用の構成ファイルをエクスポートする場合は、手順 3 の注意で確認した交換対象のストレージノードのバージョンに合わせた AMI ID を machineImageId パラメーターで指定する必要があります。

5. 構成ファイルのエクスポートで取得した構成ファイル一式を手順 4 で--template_s3_url オプションで指定した Amazon S3 バケットに格納します。

Amazon S3 にファイルを格納する方法として、例えば AWS CLI を用いて Amazon S3 にファイルをコピーする方法があります。詳細は Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「Amazon S3 の操作例」を参照してください。



注意

VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。

6. 交換対象のストレージノードの ID と status を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

交換対象のストレージノードの status が "MaintenanceBlockage"、"TemporaryBlockage"、"PersistentBlockage"、"InstallationFailed"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、または "RemovalFailedAndPersistentBlockage" であることを確認し、次の手順に進みます。

7. ストレージノードを交換します。

クラスターマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。

REST API : POST /v1/objects/storage-nodes/<id>/actions/replace-with-configuration-file/
invoke

CLI : storage_node_replace_with_configuration_file

コマンド実行後に表示されるジョブの ID を確認します。



メモ

ジョブが完了した際に、イベントログの追加情報が Amazon S3 にアップロードされることがあります。イベントログのアクションで "Error message file" の参照が指示されている場合、メッセージに記載されている Error Message File のパスを基に追加情報を Amazon S3 から取得してください。

8. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

交換が完了するまでは、他の操作が実施できないことがあります。他の操作が失敗した場合は、他の操作のエラーメッセージやイベントログに従って対処してください。



注意

- プロテクションドメインに設定された最小メモリー容量が 128GiB の場合は、処理の終了までに約 40 分掛かります。256GiB の場合は、約 50 分掛かります。
また、リビルド(データ再構築)が実行中のときは、さらに最大で 5 分ほど処理時間が長くなる可能性があります。
- その他、以下の外部要因によって処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。
 - AWS の負荷状況
 - ネットワークの通信状況(コントローラーノード、ストレージノード、AWS との相互間の通信状況)
 - EC2 インスタンスの性能状況



メモ

- この手順を実施した際に、イベントログ KARS16018-W、KARS16143-W が出力されることがあります。また、閉塞時と異なるドライブを搭載したストレージノードで交換する場合、交換前のドライブに対してイベントログ KARS05010-E、KARS07005-E、および KARS06596-

E が出力されることがあります。このタイミングでこれらのイベントログが発生することは問題ではなく、以降の処理がこれらイベントログへの対処となりますので、そのまま手順を継続してください。

- ・ ストレージノード交換ジョブが何らかの理由でエラーとなった場合は、エラー処理によってストレージノード VM の電源オフが実行されます。ただし、ネットワークの障害などによって電源オフの処理が正常に実行できないことがあります。ストレージノード交換ジョブがエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

9. 拡張前のストレージプールの総物理容量とストレージプールの ID を確認します。

CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

10. ドライブの一覧を取得します。

クエリーパラメーター `storageNodeId` に交換したストレージノードの ID、クエリーパラメーター `status` に "Offline" を指定してコマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

11. ストレージプールを拡張します。

ストレージプールの ID と手順 10 で取得したドライブの ID を指定してコマンドを実行します。

CLI を使う場合はストレージプールの ID の代わりに名前が指定できます。

REST API : POST /v1/objects/pools/<id >/actions/expand/invoke

CLI : pool_expand

コマンド実行後に表示されるジョブの ID を確認します。



メモ

コマンドを実行する際に指定したドライブの ID を記録しておいてください。記録した情報は手順 17 で使用します。

12. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

13. ストレージプールの情報を取得します。

REST API : GET /v1/objects/pools

CLI : pool_list

拡張前に比べて拡張後のストレージプールの総物理容量が拡張されたことを確認します。

14. 「キャッシュ保護用メタデータの冗長度を確認する <<Cloud>>」を参照して、冗長度が低下していないことを確認します。

冗長度が低下していない場合は、次の手順に進みます。

冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。イベントログ KARS06596-E が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 14 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

15. 「リビルドの状態を確認する」を参照して、リビルドの完了を確認します。
16. ドライブの一覧を取得します。
クエリーパラメーター `storageNodeId` に交換したストレージノードの ID、クエリーパラメーター `status` に "Blockage" を指定してコマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list
17. ストレージプールに残されている交換前のドライブの構成情報を削除します。
手順 16 で取得したドライブの ID を指定してコマンドを実行します。



メモ

このとき、指定するドライブの ID に手順 11 で記録したドライブの ID が含まれていないことを確認してください。含まれている場合、そのドライブの ID を除いてコマンドを実行してください。除いたドライブは、ストレージノード交換手順がすべて完了したあとに「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

REST API : POST /v1/objects/drives/<id>/actions/remove/invoke

CLI : drive_remove

コマンド実行後に表示されるジョブの ID を確認します。

18. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。
19. 減設対象のドライブの一覧を取得します。
ストレージノードの ID をクエリーパラメーターで指定してコマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

交換前のドライブの情報が削除されていることを確認します。
20. 構成情報のバックアップを行います。
「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

13.4.3 ストレージソフトウェアのバージョンが混在している場合のストレージノード交換 <<Cloud for AWS>>

この項での記述内容は Cloud モデル for AWS に適用されます。

ストレージソフトウェアのアップデートを途中で中止したり、エラーによってアップデートが中断されたりした場合に、ストレージクラスター内にバージョンが異なるストレージノードが混在する場合があります。

ストレージソフトウェアのバージョンが 01.17.0x.30 のストレージノードとストレージソフトウェアのバージョンが 01.18.0x.30 以降のストレージノードが混在している構成で、01.18.0x.30 以降のストレージノードを交換する場合は、以下の手順を実施してください。

なお、ストレージソフトウェアのバージョンが 01.17.0x.30 のストレージノードとストレージソフトウェアのバージョンが 01.18.0x.30 以降のストレージノードが混在している構成で、01.17.0x.30 のストレージノードを交換する場合は、ストレージソフトウェアのバージョン(01.17.0x.30)に対応した「Hitachi Virtual Storage Platform One SDS Block オペレーションガイド」の「ストレージノードを交換する <<Cloud>>」を実施してください。

前提条件

- 実行に必要なロール : Service と Storage
- 使用するコントローラーノードに VSP One SDS Block インストーラーがインストールされていること

操作手順

1. ストレージソフトウェアのバージョン(01.17.0x.30)に対応した「Hitachi Virtual Storage Platform One SDS Block オペレーションガイド」の「ストレージノードを交換する <<Cloud>>」の手順 1 から 7 を実施します。
2. 交換対象のストレージノードのバージョン(01.18.0x.30 以降)に合わせた VSP One SDS Block インストーラーをインストールします。
使用するコントローラーノードにインストールされている VSP One SDS Block インストーラーをアンインストールして、交換対象のストレージノードのバージョン(01.18.0x.30 以降)に合わせた VSP One SDS Block インストーラーをインストールしてください。
VSP One SDS Block インストーラーのアンインストール手順とインストール手順については、ストレージソフトウェアのバージョン(01.17.0x.30)に対応した Cloud モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「VSP One SDS Block インストーラーをインストールする」を参照してください。
3. ストレージソフトウェアのバージョン(01.17.0x.30)に対応した「Hitachi Virtual Storage Platform One SDS Block オペレーションガイド」の「ストレージノードを交換する <<Cloud>>」の手順 8 を実施します。
4. ストレージクラスターと同じバージョン(01.17.0x.30)の VSP One SDS Block インストーラーをインストールします。
使用するコントローラーノードにインストールされている VSP One SDS Block インストーラーをアンインストールして、ストレージクラスターと同じバージョン(01.17.0x.30)の VSP One SDS Block インストーラーをインストールしてください。
VSP One SDS Block インストーラーのアンインストール手順とインストール手順については、ストレージソフトウェアのバージョン(01.17.0x.30)に対応した Cloud モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「VSP One SDS Block インストーラーをインストールする」を参照してください。
5. ストレージソフトウェアのバージョン(01.17.0x.30)に対応した「Hitachi Virtual Storage Platform One SDS Block オペレーションガイド」の「ストレージノードを交換する <<Cloud>>」の手順 9 から 19 を実施します。



注意

13.4.4 ストレージノードを交換する《Cloud for Google Cloud》

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージノードの交換は、手動または障害によって閉塞されたストレージノードに対して実施できる処理です。手動でストレージノードを閉塞する手順は「ストレージノードの保守閉塞の条件を確認する《Cloud》」と「ストレージノードを保守閉塞する《Cloud for Google Cloud》」を参照してください。

閉塞時と異なるドライブによるストレージノード交換のみサポートされています。

フォールトドメイン障害を含む複数のストレージノードを交換する場合は、ストレージノードの交換操作は、1 ストレージノードずつ実施してください。

ストレージノード交換後には、データの冗長度を回復させるためのリビルドが実行されます。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。

ストレージノードの交換操作は 1 ストレージノードずつシリアルに実施するため、複数のストレージノード交換を行う場合に掛かる時間は、交換対象のストレージノード数×ストレージノードの交換時間になります。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - 構成ファイルのエクスポート
 - ドライブの減設
 - ドライブの増設
 - ドライブの交換

ストレージノードの交換は、コントローラーノード上から操作して行います。

ストレージノードの交換では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作して行います。

複数のストレージノードを交換する場合は、ストレージノードの交換操作(手順 3 から 21)は、1 ストレージノードずつ実施してください。

Multi-AZ (Multi-Zone)構成でタイブレーカーノードを交換する場合は、手順 22 以降の操作は不要です。



注意

ストレージノードの交換中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの交換が完了するのを待ってから再度これらの操作を実施してください。



メモ

- 交換前と交換後でストレージノード VM の Compute Engine インスタンスタイプは変わりません。
- status が "TemporaryBlockage"、"PersistentBlockage" のストレージノードに対して、ストレージノードの交換を実施すると、status が一時的に "MaintenanceBlockage" になります。また、status が "RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndPersistentBlockage" のストレージノードに対して、ストレージノードの交換を実施すると、status が一時的に "RemovalFailedAndMaintenanceBlockage" になります。このとき、メッセージ中の Operation が "STORAGE_NODE_BLOCK_FOR_MAINTENANCE" である、ジョブの開始(KARS13009-I)と完了(KARS13010-I または KARS13011-I)を示すイベントログが出力されます。

前提条件

- 実行に必要なロール : Service と Storage

操作手順の留意事項

- gcloud CLI と Terraform は実行可能な環境から実行してください。
- 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

操作手順

- コントローラーノードにログインします。
- ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。
REST API : GET /v1/objects/storage
CLI : storage_show
- 「構成ファイルをエクスポートする<<Cloud for Google Cloud>>」を参照し、Compute Engine インスタンスの削除保護を無効にするために VSP One SDS Block から構成ファイルを取得します。
構成ファイルをエクスポートする際は、exportFileType パラメーターを省略するか、Normal を指定してください。
最新状態の構成ファイルを使用するために必ず取得してください。
- 「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する<<Cloud for Google Cloud>>」を参照し、構成ファイルを解凍して配置します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、ストレージクラスターが閉塞するなどの事態が起こるおそれがあります。

- ストレージクラスターのクラウドリソースのバージョンを確認します。
Terraform の作業ディレクトリーで terraform output コマンドを実行します。
"TemplateVersion" キーの値を確認します。

```
terraform output
```

ストレージクラスターのクラウドリソースのバージョンがストレージソフトウェアのバージョンと同じ場合は、次の手順に進みます。異なる場合は「ソフトウェアアップデート後に必要な操作」の手順に従って、ストレージクラスターのクラウドリソースのバージョンをアップデートし、再度手順 3 から実施します。

- 交換対象のストレージノードの ID と status を確認します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list

交換対象のストレージノードの status が "MaintenanceBlockage"、"TemporaryBlockage"、"PersistentBlockage"、"InstallationFailed"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、または "RemovalFailedAndPersistentBlockage" であることを確認し、次の手順に進みます。

7. コンピュートポートの通信プロトコルとして IPv6 を併用している(デュアルスタックの)場合、交換対象のストレージノードの IPv6 アドレスが Google Cloud 上で予約されていることを確認します。

```
gcloud compute addresses list ¥
--filter="name~^<clusterName>-sn<XX>-compute-ipv6"
```

<clusterName>はクラスター名を、<XX>は交換対象であるストレージノードの名前の末尾 2 桁(数字)を指定してください。

クラスター名が "vsponesdsblock"、交換対象であるストレージノードの名前が "StorageNode03" の場合、IPv6 アドレスの名前は "vsponesdsblock-sn03-compute-ipv6" になります。

コマンドを実行した結果から以下を確認してください。

- ADDRESS が交換対象であるストレージノードのコンピュータネットワークの IPv6 アドレスであること
- STATUS が "IN_USE" または "RESERVED" であること

確認できない場合や、コマンド実行時に "Listed 0 items." が表示された場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ストレージノードで使用中の IPv6 アドレスを予約する<<Cloud for Google Cloud>>」を参照して、IPv6 アドレスの予約を実施してください。



注意

もし、予約できていない IPv6 アドレスがある場合は、必ず IPv6 アドレスを予約しなおしてください。予約しなおせずに交換対象のストレージノード VM (Compute Engine インスタンス) を削除した場合、このあとの手順で実施するストレージノードの交換が失敗します。

8. Compute Engine インスタンスの削除保護を無効にすることによる影響を確認します。

以下のコマンドを実行します。

```
terraform plan -out=disable_deletion_protection ¥
-var "deletionProtection=false"
```

コマンドを実行すると [Terraform will perform the following actions] という表示のあとにリソースに対する変更内容が表示されます。

以下のリソースの変更が実施されることを確認してください。

#	リソース種別	リソース操作	リソース名*	確認内容
1	google_compute_instance.ancest[]	update in-place	<clusterName>-snXX	deletion_protection が true から false になること。 以下の項目に変更がある場合がありますが、問題ありません。 ・ metadata
* リソース名の XX は、ストレージノードに割り振られている番号です。番号は 2 桁の整数で、構築した順番に 01 から番号が付けられます。				

9. terraform plan による確認で問題がなければ、Compute Engine インスタンスの削除保護を無効にするため、以下のコマンドを実行します。

```
terraform apply "disable_deletion_protection"
```

terraform apply が完了することで、クラウドリソースの変更が完了します。

10. terraform apply を実施した disable_deletion_protection ファイルを Terraform の作業ディレクトリーから削除します。

```
rm disable_deletion_protection
```

11. 「構成ファイルをエクスポートする<<Cloud for Google Cloud>>」を参照し、VSP One SDS Block からストレージノード交換においてストレージノードを削除するための構成ファイルを取得します。

構成ファイルをエクスポートする際は、exportFileType パラメーターに"ReplaceStorageNode"を指定してください。

また、machineImageId パラメーターと nodeId パラメーターを指定してください。

最新状態の構成ファイルを使用するために、ストレージノード交換用の構成ファイルは必ず取得してください。

12. 「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する<<Cloud for Google Cloud>>」を参照し、構成ファイルを解凍して配置します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、ストレージクラスターが閉塞するなどの事態が起こるおそれがあります。

13. ストレージノード交換用の構成ファイルをデプロイすることによる影響を確認します。

以下のコマンドを実行します。

```
terraform plan
```

コマンドを実行すると[Terraform will perform the following actions]という表示に続いてリソースに対する変更内容が表示されます。

以下のリソースの変更が実施されることを確認してください。

#	リソース種別	リソース操作	リソース名 ¹	確認内容
1	google_compute_disk.user_disks[] ²	delete	<clusterName>-snXX-userdatadiskYY	リソースが「1 ノード当たりのドライブの台数」の数だけ削除されること
2	google_compute_attached_disk.attached_user_disk[] ²	delete	-	リソースが「1 ノード当たりのドライブの台数」の数だけ削除されること
3	google_compute_instance.instance[]	delete	<clusterName>-snXX	リソースが 1 つ削除されること
4	google_compute_instance.instance[]	update in-place	<clusterName>-snXX	以下の項目に変更がある場合がありますが、問題ありません。 ・ metadata ・ deletion_protection
5	google_compute_instance_group.sdsc-instance-group[]	update in-place	<clusterName>-instance-group01	以下の項目に変更がある場合がありますが、問題ありません。 ・ instances

#	リソース種別	リソース操作	リソース名 ¹	確認内容
1. リソース名の XX、YY はそれぞれ以下を示します。 - XX: ストレージノードに割り振られている番号。番号は 2 桁の整数で、構築した順番に 01 から番号が付けられます。 - YY: 各ストレージノードのユーザードライブに割り振られている番号。 2. 交換対象のストレージノードがタイプブレーカーノードの場合、このリソースの変更は実施されません。				

14. terraform plan による確認で問題がなければ、交換対象のストレージノードを削除するため、以下のコマンドを実行します。

```
terraform apply
```

コマンドの実行後、[Enter a value:]と表示されたら[yes]を入力します。

入力すると最後に[Outputs]が出力されます。terraform apply が完了することで、クラウドリソースの変更が完了します。

15. 「構成ファイルをエクスポートする<<Cloud for Google Cloud>>」を参照し、VSP One SDS Block からストレージノード交換において削除したストレージノードを回復するために使用する構成ファイルを取得します。

構成ファイルをエクスポートする際は、exportFileType パラメーターに"ReplaceStorageNode"を指定してください。

また、nodeId パラメーター、machineImageId パラメーター、および recoverSingleNode パラメーターを指定してください。

recoverSingleNode パラメーターには、"true"を指定してください。

最新状態の構成ファイルを使用するために、ストレージノード交換用の構成ファイルは必ず取得してください。

16. 「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する<<Cloud for Google Cloud>>」を参照し、構成ファイルを解凍して配置します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、ストレージクラスターが閉塞するなどの事態が起こるおそれがあります。

17. ストレージノード交換用の構成ファイルをデプロイすることによる影響を確認します。
以下のコマンドを実行します。

```
terraform plan
```

コマンドを実行すると[Terraform will perform the following actions]という表示に続いてリソースに対する変更内容が表示されます。

以下のリソースの変更が実施されることを確認してください。

#	リソース種別	リソース操作	リソース名 ¹	確認内容
1	google_compute_disk.user_data_disks[] ²	create	<clusterName>-snXX-userdatadiskYY	リソースが「1 ノード当たりのドライブの台数」の数だけ作成されること
2	google_compute_attached_disk.attached_user_disk[] ²	create	-	リソースが「1 ノード当たりのドライブの台数」の数だけ作成されること

#	リソース種別	リソース操作	リソース名 ¹	確認内容
3	google_compute_instance.instance[]	create	<clusterName>-snXX	リソースが1つ作成されること
4	google_compute_instance.instance[]	update in-place	<clusterName>-snXX	以下の項目に変更がある場合がありますが、問題ありません。 ・ metadata ・ deletion_protection
5	google_compute_instance_group.up.sdsc-instance-group[]	update in-place	<clusterName>-instance-group01	以下の項目に変更がある場合がありますが、問題ありません。 ・ instances
1. リソース名の XX、YY はそれぞれ以下を示します。 ・ XX : ストレージノードに割り振られている番号。番号は2桁の整数で、構築した順番に01から番号が付けられます。 ・ YY : 各ストレージノードのユーザードライブに割り振られている番号。 2. 交換対象のストレージノードがタイブレーカーノードの場合、このリソースの変更は実施されません。				

18. terraform plan による確認で問題がなければ、交換対象のストレージノードを再作成するため、以下のコマンドを実行します。

```
terraform apply
```

コマンドの実行後、[Enter a value:]と表示されたら[yes]を入力します。

入力すると最後に[Outputs]が出力されます。terraform apply が完了することで、クラウドリソースの変更が完了します。

19. ストレージノードを交換します。

クラスターマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。
REST API : POST /v1/objects/storage-nodes/<id>/actions/replace-with-configuration-file/
invoke

CLI : storage_node_replace_with_configuration_file

コマンド実行後に表示されるジョブの ID を確認します。



メモ

ジョブが完了した際にイベントログの追加情報が Cloud Storage にアップロードされることがあります。イベントログのアクションで"Error message file"の参照が指示されている場合、メッセージに記載されている Error Message File のパスを基に追加情報を Cloud Storage から取得してください。

アップロード先の Cloud Storage のディレクトリーは、ストレージクラスター構築の際に terraform.tfvars ファイルの gsUri で指定したディレクトリーです。

gsUri の情報は terraform output で gsUri のキーを確認してください。

```
terraform output
```

20. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

交換が完了するまでは、他の操作が実施できないことがあります。他の操作が失敗した場合は、他の操作のエラーメッセージやイベントログに従って対処してください。



注意

- ・ プロテクションドメインに設定された最小メモリー容量が 128GiB の場合は、処理の終了までに約 40 分掛かります。256GiB の場合は、約 50 分掛かります。
また、リビルド(データ再構築)が実行中のときは、さらに最大で 5 分ほど処理時間が長くなる可能性があります。
- ・ その他、以下の外部要因によって処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。
 - ・ Google Cloud の負荷状況
 - ・ ネットワークの通信状況(コントローラーノード、ストレージノード、Google Cloud との相互間の通信状況)
 - ・ Compute Engine インスタンスの性能状況



メモ

- ・ この手順を実施した際に、イベントログ KARS16018-W、KARS16143-W が出力されることがあります。また、閉塞時と異なるドライブを搭載したストレージノードで交換する場合、交換前のドライブに対してイベントログ KARS05010-E、KARS07005-E、および KARS06596-E が出力されることがあります。このタイミングでこれらのイベントログが発生することは問題ではなく、以降の処理がこれらイベントログへの対処となりますので、そのまま手順を継続してください。
- ・ ストレージノード交換ジョブが何らかの理由でエラーとなった場合は、エラー処理によってストレージノード VM の電源オフが実行されます。ただし、ネットワークの障害などによって電源オフの処理が正常に実行できないことがあります。ストレージノード交換ジョブがエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

21. ストレージノードの一覧を取得して、交換したストレージノードの ID の status を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

status が"Ready"または"RemovalFailed"であれば、ストレージノードの交換が完了しています。

22. 拡張前のストレージプールの総物理容量とストレージプールの ID を確認します。

CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

23. ドライブの一覧を取得します。

クエリーパラメーター storageNodeId に交換したストレージノードの ID、クエリーパラメーター status に"Offline"を指定してコマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

24. ストレージプールを拡張します。

ストレージプールの ID と手順 23 で取得したドライブの ID を指定してコマンドを実行します。

CLI を使う場合はストレージプールの ID の代わりに名前が指定できます。

REST API : POST /v1/objects/pools/<id >/actions/expand/invoke

CLI : pool_expand

コマンド実行後に表示されるジョブの ID を確認します。



メモ

コマンドを実行する際に指定したドライブの ID を記録しておいてください。記録した情報は手順 30 で使用します。

25. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

26. ストレージプールの情報を取得します。

REST API : GET /v1/objects/pools

CLI : pool_list

拡張前に比べて拡張後のストレージプールの総物理容量が拡張されたことを確認します。

27. 「キャッシュ保護用メタデータの冗長度を確認する<<Cloud>>」を参照して、冗長度が低下していないことを確認します。

冗長度が低下していない場合は、次の手順に進みます。

冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。

イベントログ KARS06596-E が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 27 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

28. 「リビルドの状態を確認する」を参照して、リビルドの完了を確認します。

29. ドライブの一覧を取得します。

クエリーパラメーター storageNodeId に交換したストレージノードの ID、クエリーパラメーター status に"Blockage"を指定してコマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

30. ストレージプールに残されている交換前のドライブの構成情報を削除します。

手順 29 で取得したドライブの ID を指定してコマンドを実行します。



メモ

このとき、指定するドライブの ID に手順 24 で記録したドライブの ID が含まれていないことを確認してください。含まれている場合、そのドライブの ID を除いてコマンドを実行してください。

除いたドライブは、ストレージノード交換手順がすべて完了したあとに「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

REST API : POST /v1/objects/drives/<id >/actions/remove/invoke

CLI : drive_remove

コマンド実行後に表示されるジョブの ID を確認します。

31. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

32. 減設対象のドライブの一覧を取得します。

ストレージノードの ID をクエリーパラメーターで指定してコマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

交換前のドライブの情報が削除されていることを確認します。

13.4.5 ストレージノードを交換する <<Cloud for Microsoft Azure>>

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージノードの交換は、手動または障害によって閉塞されたストレージノードに対して実施できる処理です。手動でストレージノードを閉塞する手順は「ストレージノードの保守閉塞の条件を確認する <<Cloud>>」と「ストレージノードを保守閉塞する <<Cloud for Microsoft Azure>>」を参照してください。

閉塞時と異なるドライブによるストレージノード交換のみサポートされています。

フォールトドメイン障害を含む複数のストレージノードを交換する場合は、ストレージノードの交換操作は、1 ストレージノードずつ実施してください。

ストレージノード交換後には、データの冗長度を回復させるためのリビルドが実行されます。リビルドの動作状態については「リビルドの状態を確認する」を参照してください。

ストレージノードの交換操作は 1 ストレージノードずつシリアルに実施するため、複数のストレージノード交換を行う場合に掛かる時間は、交換対象のストレージノード数×ストレージノードの交換時間になります。



注意

- 本手順の前に実施していた操作がある場合は、その処理が完了またはエラーによって終了したことを確認してから本手順を実施してください。本手順の前に実施していた操作がエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」で本手順より前に実施する必要がある対処が示されているときは、その対処後に本手順を実施してください。
- 次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - 構成ファイルのエクスポート
 - ドライブの減設
 - ドライブの増設
 - ドライブの交換

ストレージノードの交換は、コントローラーノード上から操作して行います。

ストレージノードの交換では、構成ファイルを使用します。構成ファイルのエクスポートは、コントローラーノード上から操作して行います。

複数のストレージノードを交換する場合は、ストレージノードの交換操作(手順 4 から 8)は、1 ストレージノードずつ実施してください。

Multi-AZ 構成でタイブレーカーノードを交換する場合は、手順 9 以降の操作は不要です。



注意

ストレージノードの交換中に、構成の変更を伴う管理操作や他の保守操作を実施すると、これらの操作が失敗することがあります。失敗した場合は、ストレージノードの交換が完了するのを待ってから再度これらの操作を実施してください。



メモ

- 交換前と交換後でストレージノード VM の Azure VM インスタンスタイプは変わりません。
- status が "TemporaryBlockage"、"PersistentBlockage" のストレージノードに対して、ストレージノードの交換を実施すると、status が一時的に "MaintenanceBlockage" になります。また、status が "RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndPersistentBlockage" のストレージノードに対して、ストレージノードの交換を実施すると、status が一時的に "RemovalFailedAndMaintenanceBlockage" になります。このとき、メッセージ中の Operation が "STORAGE_NODE_BLOCK_FOR_MAINTENANCE" である、ジョブの開始(KARS13009-I)と完了(KARS13010-I または KARS13011-I)を示すイベントログが出力されます。

前提条件

- 実行に必要なロール : Service と Storage

操作手順の留意事項

- 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

操作手順

- コントローラーノードにログインします。
- ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。
REST API : GET /v1/objects/storage
CLI : storage_show
- コントローラーノードで以下のコマンドを実行してストレージクラスターを構成するデプロイのバージョンを確認します。

```
az deployment group show --name mainTemplate ¥  
--resource-group <リソースグループ名> ¥  
--query "properties.outputs.templateVersion.value"
```

ストレージクラスターを構成するデプロイのバージョンがストレージソフトウェアのバージョンと同じ場合は、次の手順に進みます。異なる場合は「ソフトウェアアップデート後に必要な操作」の手順に従って、ストレージクラスターのリソースのバージョンをアップデートしてから次の手順に進みます。



注意

mainTemplate の templateVersion が確認できない場合は、Azure ポータル上でクラスター構築時に最初に作成されたデプロイ (InstallationStatus のデプロイより前にあるデプロイ) があるか確認してください。

クラスター構築時に最初に作成されたデプロイがある場合は、そのデプロイを --name に指定して templateVersion を確認してください。

クラスター構築時に最初に作成されたデプロイがない場合は、「ソフトウェアアップデート後に必要な操作」の手順を確認してください。

- 「構成ファイルをエクスポートする <<Cloud for Microsoft Azure>>」を参照し、VSP One SDS Block からストレージノード交換用の構成ファイルを取得します。

構成ファイルをエクスポートする際は、`exportFileType` パラメーターに"ReplaceStorageNode"を指定してください。

また、`machineImageId` パラメーターを指定してください。

最新状態の構成ファイルを使用するために、ストレージノード交換用の構成ファイルは必ず取得してください。



注意

- `machineImageId` パラメーターは、交換対象のストレージノードと同じ VM イメージを使用してください。
ストレージソフトウェアのバージョンは"aa.bb.cc.dd"の形式になっています。VM イメージのバージョンは sku 名に記載されています。sku 名は"aa_bb_cc_dd_byol"の形式になっていて、"aa_bb_cc_dd"部分がバージョンを示します。"aa.bb.cc.dd"と"aa_bb_cc_dd"の数値が一致していることを確認してください。
- エクスポートした `ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` は解凍しないでください。解凍して使用した場合、ジョブが失敗するおそれがあります。パラメーターで指定する値を間違えた場合は、正しい値を指定して構成ファイルのエクスポートを再度実行し、最新の構成ファイルを取得しなおしてください。

5. 交換対象のストレージノードの ID と status を確認します。

REST API : `GET/v1/objects/storage-nodes`

CLI : `storage_node_list`

交換対象のストレージノードの status が"MaintenanceBlockage"、"TemporaryBlockage"、"PersistentBlockage"、"InstallationFailed"、"RemovalFailedAndTemporaryBlockage"、"RemovalFailedAndMaintenanceBlockage"、または"RemovalFailedAndPersistentBlockage"であることを確認し、次の手順に進みます。

6. ストレージノードを交換します。

クラスターマスターノード(プライマリー)またはロードバランサーに対してのみ実行できます。コマンド実行時には、手順 4 でエクスポートした

`ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz` をパラメーターとして指定する必要があります。

この構成ファイルは解凍せずにパラメーターに指定してください。

REST API : `POST /v1/objects/storage-nodes/<id >/actions/replace-with-configuration-file/`
`invoke`

CLI : `storage_node_replace_with_configuration_file`

コマンド実行後に表示されるジョブの ID を確認します。



メモ

イベントログに Error message file が表示されていた場合は、インストール時に作成した Azure Blob Storage のコンテナに追加情報がアップロードされます。

7. ジョブの ID を指定してジョブの state を確認します。

REST API : `GET /v1/objects/jobs/<jobId >`

CLI : `job_show`

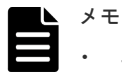
state が"Succeeded"になっていたらジョブは完了です。

交換が完了するまでは、他の操作が実施できないことがあります。他の操作が失敗した場合は、他の操作のエラーメッセージやイベントログに従って対処してください。



注意

- ・ ジョブが完了した際に、イベントログ **KARS10965-W** が出力されることがあります。その場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「リソースの削除ロックが正しく設定されていない場合の対処<<Cloud for Microsoft Azure>>」を確認し対処してください。
- ・ プロテクションドメインに設定された最小メモリー容量が **128GiB** の場合は、処理の終了までに約 40 分掛かります。**256GiB** の場合は、約 50 分掛かります。
また、リビルド(データ再構築)が実行中のときは、さらに最大で 5 分ほど処理時間が長くなる可能性があります。
- ・ その他、以下の外部要因によって処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。
 - ・ Microsoft Azure の負荷状況
 - ・ ネットワークの通信状況(コントローラーノード、ストレージノード、Microsoft Azure との相互間の通信状況)
 - ・ Azure VM インスタンスの性能状況



メモ

- ・ この手順を実施した際に、イベントログ **KARS16018-W**、**KARS16143-W** が出力されることがあります。また、閉塞時と異なるドライブを搭載したストレージノードで交換する場合、交換前のドライブに対してイベントログ **KARS05010-E**、**KARS07005-E**、および **KARS06596-E** が出力されることがあります。このタイミングでこれらのイベントログが発生することは問題ではなく、以降の処理がこれらイベントログへの対処となりますので、そのまま手順を継続してください。
- ・ ストレージノード交換ジョブが何らかの理由でエラーとなった場合は、エラー処理によってストレージノード VM の電源オフが実行されます。ただし、ネットワークの障害などによって電源オフの処理が正常に実行できないことがあります。ストレージノード交換ジョブがエラーによって終了している場合、イベントログや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

8. ストレージノードの一覧を取得して、交換したストレージノードの ID の status を確認します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
status が "Ready" または "RemovalFailed" であれば、ストレージノードの交換が完了しています。
9. 拡張前のストレージプールの総物理容量とストレージプールの ID を確認します。
CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。
REST API : GET /v1/objects/pools
CLI : pool_list
10. ドライブの一覧を取得します。
クエリーパラメーター **storageNodeId** に交換したストレージノードの ID、クエリーパラメーター **status** に "Offline" を指定してコマンドを実行します。
REST API : GET /v1/objects/drives
CLI : drive_list
11. ストレージプールを拡張します。
ストレージプールの ID と手順 10 で取得したドライブの ID を指定してコマンドを実行します。
CLI を使う場合はストレージプールの ID の代わりに名前が指定できます。
REST API : POST /v1/objects/pools/<id>/actions/expand/invoke
CLI : pool_expand

コマンド実行後に表示されるジョブの ID を確認します。



メモ

コマンドを実行する際に指定したドライブの ID を記録しておいてください。記録した情報は手順 17 で使用します。

12. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

13. ストレージプールの情報を取得します。

REST API : GET /v1/objects/pools

CLI : pool_list

拡張前に比べて拡張後のストレージプールの総物理容量が拡張されたことを確認します。

14. 「キャッシュ保護用メタデータの冗長度を確認する<<Cloud>>」を参照して、冗長度が低下していないことを確認します。

冗長度が低下していない場合は、次の手順に進みます。

冗長度が低下していた場合は、キャッシュ保護用メタデータの冗長度が回復するまで待ちます。イベントログ KARS06596-E が出力されていた場合は、メッセージの指示に従って対処してください。対処したあと、再度手順 14 を実施します。



メモ

ストレージノードが閉塞している場合は、保守操作などによるストレージノードの回復を行わなければキャッシュ保護用メタデータの冗長度の回復が行われません。閉塞しているストレージノードに対して先に保守操作で回復を実施してください。

15. 「リビルドの状態を確認する」を参照して、リビルドの完了を確認します。

16. ドライブの一覧を取得します。

クエリーパラメーター **storageNodeId** に交換したストレージノードの ID、クエリーパラメーター **status** に"Blockage"を指定してコマンドを実行します。

REST API : GET /v1/objects/drives

CLI : drive_list

17. ストレージプールに残されている交換前のドライブの構成情報を削除します。

手順 16 で取得したドライブの ID を指定してコマンドを実行します。



メモ

このとき、指定するドライブの ID に手順 11 で記録したドライブの ID が含まれていないことを確認してください。含まれている場合、そのドライブの ID を除いてコマンドを実行してください。除いたドライブは、ストレージノード交換手順がすべて完了したあとに「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。

REST API : POST /v1/objects/drives/<id >/actions/remove/invoke

CLI : drive_remove

コマンド実行後に表示されるジョブの ID を確認します。

18. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

19. 減設対象のドライブの一覧を取得します。

ストレージノードの ID をクエリーパラメーターで指定してコマンドを実行します。
REST API : GET /v1/objects/drives
CLI : drive_list
交換前のドライブの情報が削除されていることを確認します。

13.5 ストレージノードの自動回復機能の設定

ストレージノードの自動回復機能の設定方法を説明します。

13.5.1 ストレージノードの自動回復機能を設定する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージノード自動回復は、ソフトウェア要因(ファームウェア、ドライバなど)によるサーバー障害、またはストレージノード間ネットワークの一時的な障害によるサーバー障害からストレージノードを復旧するために、ストレージノードの自己診断と自動復旧を行う機能です。

ストレージノード自動回復機能は、自己診断の結果、閉塞したストレージノードが自動回復可能と判断した場合に、保守回復を行います。

ストレージノードの自動回復機能による保守回復が以下の要因によって実施できなかった場合、スペアノードが登録してあると、ストレージノードの自動回復機能は、スペアノード切り換えによる回復を行います。ただし、自動回復機能が無効だった場合は、スペアノード切り換えによる回復も無効になります。スペアノード切り換えの詳細については、このマニュアルの「スペアノード切り換えの概要<<Bare metal>>」を参照してください。

- ストレージノードの自動回復機能による自己診断の結果、閉塞したストレージノードが自動保守回復不可だと判断された場合
- ストレージノードの自動回復機能によって発行された保守回復ジョブが失敗した場合

自動回復機能のデフォルトは有効です。



注意

自動回復機能の設定は、マニュアルやイベントログなどで促されない限り、無効にしないでください。(設定の変更は、トラブルシュートによって必要な場合に促されます。)

無効にした場合は、必要な対処の実施後に再度ストレージノードの自動回復機能の設定を有効にしてください。

ストレージノードの自動回復機能による保守回復の対象となるのは、以下の条件に当てはまるストレージノードです。

- status が"TemporaryBlockage"(一時閉塞中)に移行したストレージノード
- ストレージノード間ネットワークがつながるストレージノード

ストレージノードの自動回復機能によるスペアノード切り換えの対象となる条件は「スペアノード切り換えの概要<<Bare metal>>」の「スペアノード切り換えの動作条件」を参照してください。

status が"TemporaryBlockage"以外の閉塞状態のストレージノードは「ストレージノード保守の原因と対処<<Bare metal>>」に従って手動で保守する必要があります。

また、ストレージノードの自動回復機能による自己診断の結果、閉塞したストレージノードが自動回復不可と判断した場合は、ストレージノードの status を"PersistentBlockage"に変更します。変更にあたっては、イベントログ KARS13102-E を発行します。

自己診断によって自動回復不可と判断する主な理由は以下です。また、以下の理由はイベントログ KARS13102-E の Cause に記載されます。障害原因を特定するための参考としてください。

- 障害が発生したストレージノードが永続閉塞判定時間以内に、ストレージノードの保守回復や保守交換によって回復した履歴があった場合(ハードウェア故障などの問題の可能性ありと判断。Cause = Unstable)
 - 障害が発生したストレージノードに対しストレージノード間ネットワークの接続性確認や、回復処理を何度か行っても失敗した場合(保守回復の見込みがなく自動回復不可と判断。Cause = Timeout)
 - 障害が発生したストレージノードに対するスペアノード切り換えの動作条件を満たしていない場合や、スペアノード切り換えによる回復処理を何度か行っても失敗した場合(スペアノード切り換えによる回復の見込みがなく自動回復不可と判断。Cause = UnableToSwitchingSpareNode)
- スペアノード切り換えの動作条件の詳細は「スペアノード切り換えの概要<<Bare metal>>」の「スペアノード切り換えが動作しない例」を参照してください。

永続閉塞判定時間(storageNodePersistentBlockingThresholdTime[h])は、現在からさかのぼって指定の時間以内にストレージノードの回復履歴がある一時閉塞状態のストレージノードを永続閉塞に遷移させるためのパラメーターです。単位は時間でデフォルトは 0(デフォルトは回復履歴があったとしても永続閉塞に遷移させない)になります。このパラメーターは設定変更可能ですが、設定変更は、保守員による指示があった場合に限って実施してください。

ストレージノードの自動回復機能は、障害発生後、ストレージノードの status が "TemporaryBlockage"の間に障害原因を特定し、通常 5 分から 30 分程度でストレージノードの保守回復ジョブを発行しますが、障害の種別や状況に応じてストレージノードの自動回復の可否判定に掛かる時間は変動し、確定するのに最大約 60 分掛かります。

保守回復対象をスペアノード切り換えの対象に変更するまでの時間は 15 分から 60 分までの間で指定することもできます。

REST API : PATCH /v1/objects/storage-auto-recovery-setting

CLI : storage_auto_recovery_setting_set

ただし、以下の条件を両方満たす場合は、スペアノード切り換えが優先して実行されます。

- 切り換え可能なスペアノードが登録されている場合
- 保守回復対象をスペアノード切り換えの対象に変更するまでの時間を変更した場合



メモ

- 変更した保守回復対象をスペアノード切り換えの対象に変更するまでの時間を経過したとしても、障害が発生したストレージノード内でのダンプログファイルの採取(自動で実行されます)が完了していない場合は、設定時間を超えてダンプログファイルの採取が継続されます。保守回復対象をスペアノード切り換えの対象に変更するまでの時間は、障害の発生から最大 40 分まで延長されることがあります。
- 保守回復対象をスペアノード切り換えの対象に変更するまでの時間を変更していても、切り換え可能なスペアノードが登録されていない場合、ストレージノードの自動回復の可否判定を最大約 60 分間継続します。
- 保守回復対象をスペアノード切り換えの対象に変更するまでの時間は、VSP One SDS Block Administrator でも設定できます。
操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の「保守回復対象をスペアノード切り換えの対象に変更するまでの時間を設定する<<Bare metal>>」を参照してください。

保守回復対象をスペアノード切り換えの対象に変更するまでの時間を設定後、ソフトウェアアップデート、またはダウングレードを行った場合の設定時間を以下に示します。

アップデート元またはダウングレード元バージョン	アップデート先またはダウングレード先バージョン	設定時間
01.16.0x.40 以前	01.17.0x.40 以降	60 分(デフォルト値)
01.17.0x.40 以降	01.16.0x.40 以前	60 分(デフォルト値)
01.17.0x.40 以降	01.17.0x.40 以降	アップデート元またはダウングレード元バージョンで設定した時間

ストレージノードの自動回復機能は、閉塞したストレージノードがスペアノード切り換えの対象になってから、通常 5 分程度でストレージノードの交換ジョブを発行しますが、障害の種別や状況に応じてスペアノード切り換えによる回復可否判定に要する時間は変動し、確定するまでに最大 25 分掛かります。

ストレージノードの自動回復機能の動作条件

ストレージノードの自動回復機能による保守回復が動作する条件は以下のとおりです。

- ・ ストレージノードの自動回復機能の設定が有効(true)である
本機能がサポートされているストレージソフトウェアのセットアップ後や本機能をサポートしているバージョンのストレージソフトウェアへのアップデート後は、本機能の設定は有効です。有効/無効の設定と設定確認は、REST API または CLI にて実施できます。
- ・ ストレージノードの保守回復ジョブの動作条件を満たしている

ストレージノードの自動回復機能によるスペアノード切り換えが動作する条件は以下のとおりです。

- ・ ストレージノードの自動回復機能の設定が有効(true)である
本機能がサポートされているストレージソフトウェアのセットアップ後や本機能をサポートしているバージョンのストレージソフトウェアへのアップデート後は、本機能の設定は有効です。有効/無効の設定と設定確認は、REST API または CLI にて実施できます。
- ・ 切り換え可能なスペアノードが登録されている
- ・ ストレージノードに BMC の情報が登録されている
- ・ ストレージノードの交換ジョブの動作条件を満たしている

ストレージノードの自動回復機能が動作しないケース

以下の場合、ストレージノードの自動回復機能の設定が有効に設定されていても、動作しません。ストレージノードの自動回復機能が動作できない場合、必要に応じてイベントログまたはストレージノードの自動回復機能設定の status によってユーザーに通知されます。

ストレージノードの自動回復機能による保守回復が動作しない条件は以下のとおりです。

- ・ ストレージソフトウェアのバージョンアップなど、競合する構成変更が動作している
- ・ 保守回復対象のストレージノードのストレージノード間ネットワークが不通である

スペアノード切り換えの動作条件の詳細は「スペアノード切り換えの概要 <<Bare metal>>」の「スペアノード切り換えが動作しない例」を参照してください。

ストレージノードの自動回復機能の通知

ストレージノードの自動回復機能は、以下の情報通知をします。

- ・ ストレージノードに関する各種情報：イベントログ

- ・ ストレージノードの自動回復機能自体に関する情報：ストレージノードの自動回復機能設定の status

■ストレージノードの自動回復機能が発行するイベントログ

イベントログ	説明
KARS13101-I	ストレージノードの自動回復機能によってストレージノードの保守回復ジョブを投入した際はイベントログ KARS13101-I が発行されます。ストレージノードの保守回復ジョブの成否やエラー原因はジョブ一覧参照で参照するか、イベントログから開始 (KARS13009-I)と完了(KARS13010-I または KARS13011-I)のイベントを確認してください。ストレージノードの保守回復ジョブの成否などは Service ロールのユーザーで参照できます。
KARS13102-E	ストレージノードの自動回復機能による自己診断の結果、閉塞したストレージノードが自動回復不可と判断した場合は、ストレージノードの status を "PersistentBlockage"に変更し、イベントログ KARS13102-E が発行されます。ストレージノードの status を"PersistentBlockage"に変更した理由はイベントログの Cause に記載されます。 ・ Unstable : 障害が発生したストレージノードが永続閉塞判定時間以内にストレージノードの保守回復や保守交換によって回復した履歴があった場合(ハードウェア故障などの問題の可能性ありと判断) ・ Timeout:障害が発生したストレージノードに対しストレージノード間ネットワークの接続性確認や、回復処理を何度か行っても失敗した場合(保守回復の見込みがなく自動回復不可と判断) ・ 障害が発生したストレージノードに対するスペアノード切り換えの動作条件を満たしていない場合や、スペアノード切り換えによる回復処理を何度か行っても失敗した場合(スペアノード切り換えによる回復の見込みがなく自動回復不可と判断。 Cause = UnableToSwitchingSpareNode) スペアノード切り換えの動作条件の詳細は「スペアノード切り換えの概要<<Bare metal>>」の「スペアノード切り換えが動作しない例」を参照してください。
KARS13105-I	ストレージノードの自動回復機能によってストレージノードの交換ジョブを投入した際はイベントログ KARS13105-I が発行されます。ストレージノードの交換ジョブの成否やエラー原因はジョブ一覧参照で参照するか、イベントログから開始 (KARS13009-I)と完了(KARS13010-I または KARS13011-I)のイベントを確認してください。ストレージノードの交換ジョブの成否などは Service ロールのユーザーで参照できます。
KARS13106-I	閉塞したストレージノードを自動回復機能による保守回復対象からスペアノード切り換えの対象へと変更する際は、イベントログ KARS13106-I が発行されます。当該ストレージノードへのスペアノード切り換えを開始する際には、イベントログ KARS13107-I が発行されます。
KARS13107-I	ストレージノードの自動回復機能によってスペアノード切り換えを開始する際には、イベントログ KARS13107-I が発行されます。
KARS13108-E	イベントログ KARS13102-E(Cause=UnableToSwitchingSpareNode)が発行された際、障害が発生したストレージノードの BMC ポートへの接続に失敗していた場合は、イベントログ KARS13108-E が追加で発行されます。 スペアノード切り換えの動作条件の詳細は「スペアノード切り換えの概要<<Bare metal>>」の「スペアノード切り換えが動作しない例」を参照してください。

■ストレージノードの自動回復機能設定の status

ストレージノードの自動回復機能設定の status の確認方法は「ストレージノードの自動回復機能の情報」を取得する<<Bare metal>>」を参照してください。

各 status の意味は以下のとおりです。

status	説明
Disabled	ストレージノードの自動回復機能の設定が無効な状態です。
Normal	ストレージノードの自動回復機能の設定が有効であり、かつストレージノードの自動回復機能が正常に動作している状態です。
Conflict	ストレージソフトウェアのバージョンアップなど、競合する構成変更処理が動作しているため、ストレージノードの自動回復機能が動作できない状態です。競合処理が完了すれば "Normal" に戻ります。
Error	システムに障害が発生しているためにストレージノードの自動回復機能が動作できない状態です。 "Normal" に戻すには保守員による対応が必要です。

ストレージノードの自動回復機能動作時の原因特定

ストレージノードの自動回復機能の設定が有効な状態で運用を続けていると、ユーザーが気付かないうちにストレージノードが閉塞した状態から回復している可能性があります。定期的にイベントログを確認し KARS13101-I または KARS13105-I が存在する場合は、該当時刻におけるネットワークや物理リソースに障害がないかを確認し、システム環境に問題がなく、VSP One SDS Block の問題が疑われる場合はダンプを採取し、サポートセンターに送付してください。

ストレージノードの自動回復機能の設定手順は以下のとおりです。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージノードの自動回復機能の有効/無効を設定します。

REST API : PATCH /v1/objects/storage-auto-recovery-setting

CLI : storage_auto_recovery_setting_set

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

3. 正しく設定できたかを確認します。

REST API : GET /v1/objects/storage-auto-recovery-setting

CLI : storage_auto_recovery_setting_show

isEnabled が "true" であれば、自動回復機能が有効に設定されています。 "false" であれば、無効に設定されています。

4. 構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

13.5.2 ストレージノードの自動回復機能を設定する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ストレージノード自動回復は、ソフトウェア要因(ファームウェア、ドライバーなど)によるサーバー障害、またはストレージノード間ネットワークの一時的な障害によるサーバー障害からストレージノードを復旧するために、ストレージノードの自己診断と自動復旧を行う機能です。

ストレージノード自動回復機能は、自己診断の結果、閉塞したストレージノードが自動回復可能と判断した場合に、保守回復を行います。

自動回復機能のデフォルトは有効です。



注意

自動回復機能の設定は、マニュアルやイベントログなどで促されない限り、無効にしないでください。(設定の変更は、トラブルシュートによって必要な場合に促されます。)

無効にした場合は、必要な対処の実施後に再度ストレージノードの自動回復機能の設定を有効にしてください。

ストレージノードの自動回復機能による保守回復の対象となるのは、以下の条件に当てはまるストレージノードです。

- `status` が `"TemporaryBlockage"`(一時閉塞中)に移行したストレージノード
- ストレージノード間ネットワークがつながるストレージノード

`status` が `"TemporaryBlockage"`以外の閉塞状態のストレージノードは「ストレージノード保守の原因と対処<<Cloud>>」に従って手動で保守する必要があります。

また、ストレージノードの自動回復機能による自己診断の結果、閉塞したストレージノードが自動回復不可と判断した場合は、ストレージノードの `status` を `"PersistentBlockage"`に変更します。変更に応じた場合は、イベントログ `KARS13102-E` を発行します。

自己診断によって自動回復不可と判断する主な理由は以下です。また、以下の理由はイベントログ `KARS13102-E` の `Cause` に記載されます。障害原因を特定するための参考としてください。

- 障害が発生したストレージノードが永続閉塞判定時間以内に、ストレージノードの保守回復や保守交換によって回復した履歴があった場合(ハードウェア故障などの問題の可能性ありと判断。 `Cause = Unstable`)
- 障害が発生したストレージノードに対しストレージノード間ネットワークの接続性確認や、回復処理を何度か行っても失敗した場合(保守回復の見込みがなく自動回復不可と判断。 `Cause = Timeout`)

永続閉塞判定時間(`storageNodePersistentBlockingThresholdTime[h]`)は、現在からさかのぼって指定の時間以内にストレージノードの回復履歴がある一時閉塞状態のストレージノードを永続閉塞に遷移させるためのパラメーターです。単位は時間でデフォルトは 0(デフォルトは回復履歴があったとしても永続閉塞に遷移させない)になります。このパラメーターは設定変更可能ですが、設定変更は、保守員による指示があった場合に限り実施してください。

ストレージノードの自動回復機能は、障害発生後、ストレージノードの `status` が `"TemporaryBlockage"`の間に障害原因を特定し、通常 5 分から 30 分程度でストレージノードの保守回復ジョブを発行しますが、障害の種別や状況に応じてストレージノードの自動回復の可否判定に掛かる時間は変動し、確定するのに最大約 60 分掛かります。

ストレージノードの自動回復の可否判定結果を待たずに、ストレージノードの **status** が "TemporaryBlockage"の間に回復させたい場合は、ストレージノードの手動回復が実施できます。ストレージノードの手動回復を行う場合は、以下に注意してください。

- ストレージノードの自動回復機能の設定が有効な状態でストレージノードの手動回復を実施すると、ストレージノードの自動回復と競合し失敗する場合があります。競合した場合は、先に実行されたストレージノードの保守回復ジョブが動作し、後発のストレージノードの保守回復ジョブは失敗します。競合の結果、ストレージノードの手動回復でのストレージノードの保守回復ジョブが失敗した場合は **KARS10901-E** のイベントログが、ストレージノードの自動回復機能でのストレージノードの保守回復ジョブが失敗した場合は **KARS10525-W** のイベントログが、それぞれ発行されます。競合を避けたい場合は、ストレージノードの自動回復機能の設定を無効にし、5 分ほど待ってからストレージノードの手動回復を実施してください。ストレージノードの自動回復機能の設定を無効にした場合は、ストレージノードの手動回復後に再度、ストレージノードの自動回復機能の設定を有効にしてください。

ストレージノードの自動回復機能の動作条件

ストレージノードの自動回復機能による保守回復が動作する条件は以下のとおりです。

- ストレージノードの自動回復機能の設定が有効(true)である
本機能がサポートされているストレージソフトウェアのセットアップ後や本機能をサポートしているバージョンのストレージソフトウェアへのアップデート後は、本機能の設定は有効です。有効/無効の設定と設定確認は、REST API または CLI にて実施できます。
- ストレージノードの保守回復ジョブの動作条件を満たしている

ストレージノードの自動回復機能が動作しないケース

以下の場合は、ストレージノードの自動回復機能の設定が有効に設定されていても、動作しません。ストレージノードの自動回復機能が動作できない場合、必要に応じてイベントログまたはストレージノードの自動回復機能設定の **status** によってユーザーに通知されます。

ストレージノードの自動回復機能による保守回復が動作しない条件は以下のとおりです。

- ストレージソフトウェアのバージョンアップなど、競合する構成変更が動作している
- 保守回復対象のストレージノードのストレージノード間ネットワークが不通である

ストレージノードの自動回復機能の通知

ストレージノードの自動回復機能は、以下の情報通知をします。

- ストレージノードに関する各種情報：イベントログ
- ストレージノードの自動回復機能自体に関する情報：ストレージノードの自動回復機能設定の **status**

■ストレージノードの自動回復機能が発行するイベントログ

イベントログ	説明
KARS13101-I	ストレージノードの自動回復機能によってストレージノードの保守回復ジョブを投入した際はイベントログ KARS13101-I が発行されます。ストレージノードの保守回復ジョブの成否やエラー原因はジョブ一覧参照で参照するか、イベントログから開始 (KARS13009-I)と完了(KARS13010-I または KARS13011-I)のイベントを確認してください。ストレージノードの保守回復ジョブの成否などは Service ロールのユーザーで参照できます。

イベントログ	説明
KARS13102-E	ストレージノードの自動回復機能による自己診断の結果、閉塞したストレージノードが自動回復不可と判断した場合は、ストレージノードの status を "PersistentBlockage"に変更し、イベントログ KARS13102-E が発行されます。ストレージノードの status を "PersistentBlockage"に変更した理由はイベントログの Cause に記載されます。 • Unstable : 障害が発生したストレージノードが永続閉塞判定時間以内にストレージノードの保守回復や保守交換によって回復した履歴があった場合(ハードウェア故障などの問題の可能性ありと判断) • Timeout : 障害が発生したストレージノードに対しストレージノード間ネットワークの接続性確認や、回復処理を何度か行っても失敗した場合(保守回復の見込みがなく自動回復不可と判断)

■ストレージノードの自動回復機能設定の status

ストレージノードの自動回復機能設定の **status** の確認方法は「ストレージノードの自動回復機能の情報を取得する<<Cloud>>」を参照してください。

各 **status** の意味は以下のとおりです。

status	説明
Disabled	ストレージノードの自動回復機能の設定が無効な状態です。
Normal	ストレージノードの自動回復機能の設定が有効であり、かつストレージノードの自動回復機能が正常に動作している状態です。
Conflict	ストレージソフトウェアのバージョンアップなど、競合する構成変更処理が動作しているため、ストレージノードの自動回復機能が動作できない状態です。競合処理が完了すれば "Normal"に戻ります。
Error	システムに障害が発生しているためにストレージノードの自動回復機能が動作できない状態です。"Normal"に戻すには保守員による対応が必要です。

ストレージノードの自動回復機能動作時の原因特定

ストレージノードの自動回復機能の設定が有効な状態で運用を続けていると、ユーザーが気付かないうちにストレージノードが閉塞した状態から回復している可能性があります。定期的にイベントログを確認し KARS13101-I が存在する場合は、該当時刻におけるネットワークや物理リソースに障害がないかを確認し、システム環境に問題がなく、VSP One SDS Block の問題が疑われる場合はダンプを採取し、サポートセンターに送付してください。

ストレージノードの自動回復機能の設定手順は以下のとおりです。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージノードの自動回復機能の有効/無効を設定します。
REST API : PATCH /v1/objects/storage-auto-recovery-setting
CLI : storage_auto_recovery_setting_set
コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

3. 正しく設定できたかを確認します。

REST API : GET /v1/objects/storage-auto-recovery-setting

CLI : storage_auto_recovery_setting_show

isEnabled が"true"であれば、自動回復機能が有効に設定されています。"false"であれば、無効に設定されています。

4. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

13.6 ストレージノードの自動回復機能の情報取得

ストレージノードの自動回復機能の情報が取得できます。

13.6.1 ストレージノードの自動回復機能の情報を取得する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージノードの自動回復機能の情報を取得します。以下の情報が得られます。

- isEnabled : 自動回復機能の有効/無効
- storageNodePersistentBlockingThresholdTime : 同一ストレージノードにおける複数回の一時閉塞を永続閉塞判定とする際のしきい値[h]
- status : 自動回復機能の状態
- spareNodeSwitchoverWaitingTime : 保守回復対象をスペアノード切り換えの対象に変更するまでの時間[min]



メモ

- status の詳細については、「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」、「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」、またはこのマニュアルの「ストレージノードの自動回復機能を設定する<<Bare metal>>」の「ストレージノードの自動回復機能の通知」を参照してください。
- spareNodeSwitchoverWaitingTime は、VSP One SDS Block Administrator の「Storage Cluster Information」ダイアログで確認できます。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージノードの自動回復機能の情報を取得します。

REST API : GET /v1/objects/storage-auto-recovery-setting

CLI : storage_auto_recovery_setting_show

13.6.2 ストレージノードの自動回復機能の情報を取得する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ストレージノードの自動回復機能の情報を取得します。以下の情報が得られます。

- `isEnabled` : 自動回復機能の有効/無効
- `storageNodePersistentBlockingThresholdTime` : 同一ストレージノードにおける複数回の一時閉塞を永続閉塞判定とする際のしきい値[h]
- `status` : 自動回復機能の状態
- `spareNodeSwitchoverWaitingTime` : 常に null



メモ

`status` の詳細については、「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」、「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」、またはこのマニュアルの「ストレージノードの自動回復機能を設定する<<Cloud>>」の「ストレージノードの自動回復機能の通知」を参照してください。

前提条件

- 実行に必要なロール : `Service`

操作手順

1. ストレージノードの自動回復機能の情報を取得します。

REST API : `GET /v1/objects/storage-auto-recovery-setting`

CLI : `storage_auto_recovery_setting_show`

13.7 クラウドプラットフォームのメンテナンスについて<<Cloud for Google Cloud>>

この節での記述内容は Cloud モデル for Google Cloud に適用されます。

Google Cloud では Compute Engine インスタンスが動作するホストに対してインフラストラクチャのメンテナンスが実行されることがあります。メンテナンス中は対象ホスト上で動作する Compute Engine インスタンスが一時停止することがあります。

この Google Cloud のメンテナンスは、予告などではなく、メンテナンスのために事前に行う作業はありません。

このメンテナンスに伴い発生する一時停止は非常に短時間であり、メンテナンス後もストレージノードは正常に動作を継続します。

ただし、まれに一時停止が長引くことがあり、その際にはストレージノードが閉塞することがあります。ストレージノードが閉塞した際は、他の障害による閉塞時と同様の手順で回復することが可能です。また、ストレージノードが閉塞する場合、他のストレージノードやストレージクラスター外部に影響を与えることを防ぐため、Google Cloud の VPC ファイアウォールに通信を遮断するためのルールが自動的に追加されます。そのため、一時停止から復帰したストレージノードに関する通信は遮断されます。追加されたルールは、閉塞状態のストレージノードが回復した際に自動的に削除されます。追加されるルールの名称は以下のとおりです。

`storage-node-{allow | deny}-{intr | cmpt}<ストレージノードの ID(uuid)>`



注意

マニュアル上での指示がない限り、通信を遮断するためのルールについて、手動でルールを破棄したり編集したりして、ルールの効果を上書きするようなルール追加は行わないでください。

13.8 クラウドプラットフォームのメンテナンスについて《Cloud for Microsoft Azure》

この節での記述内容は Cloud モデル for Microsoft Azure に適用されます。

Microsoft Azure では Azure VM インスタンスが動作するホストに対してインフラストラクチャーのメンテナンスが実行されることがあります。メンテナンス中は対象ホスト上で動作する Azure VM インスタンスが一時停止したり、再起動したりすることがあります。

Microsoft Azure では、VM のメンテナンスの一つに「メモリ保持メンテナンス(Memory preserving maintenance)」があります。

このメンテナンスは、起動している Azure VM インスタンスを一時停止して実行されます。Azure VM インスタンスが一時停止する時間は、10 秒未満です。

また、このメンテナンスは、VSP One SDS Block のストレージクラスターの動作に影響することがあるため、VSP One SDS Block は、Microsoft Azure が発行するメンテナンスの実行予告を監視します。

VSP One SDS Block は、予告を検知すると、以下を実施します。

- ストレージノードの閉塞
メンテナンス対象の Azure VM インスタンスで稼働するストレージノードを閉塞させます。
メンテナンス完了後は、自動的にストレージノードを回復させます。



メモ

- ストレージノードが閉塞される際、閉塞前にイベントログ KARS08331-E が出力されます。イベントログ KARS08331-E が出力された場合は、イベントログに記載の solution に従って対処してください。
イベントログ KARS08331-E は、VSP One SDS Block が予告を検知したときではなく、検知後、ストレージノードを閉塞させる前に出力されます。
- ストレージノードが閉塞している間はストレージクラスターの冗長度が低下します。

- ストレージノードの回復および起動の抑止
以下の動作を抑止します。
 - 対象のストレージノードの保守回復
 - 対象のストレージノードの自動回復
 - ストレージクラスター起動対象のストレージノードの起動



メモ

これらの動作が抑止される際、イベントログ KARS08332-W が出力されます。イベントログ KARS08332-W が出力された場合は、イベントログに記載の solution に従って対処してください。



メモ

ストレージクラスター内のストレージノードが閉塞している状態で、メンテナンスが正常なストレージノードに対して実施された場合、ストレージクラスターに格納されているデータを保護するために VSP One SDS Block はストレージクラスターを閉塞させます。

ただし、冗長構成によってストレージクラスター閉塞の条件が変わります。詳細については Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「VSP One SDS Block がサポートする耐障害性に関する設定と各機能の説明」を参照してください。

ストレージクラスターが閉塞した場合「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って回復を実施してください。

ドライブデータ再配置を管理する<<Bare metal>>

この章での記述内容は Bare metal モデルに適用されます。

- 14.1 ドライブデータ再配置の概要<<Bare metal>>
- 14.2 ドライブデータ再配置の起動契機と動作可能な条件<<Bare metal>>
- 14.3 ドライブデータ再配置完了までの時間(目安)<<Bare metal>>
- 14.4 ドライブデータ再配置の状態を確認する<<Bare metal>>
- 14.5 ドライブデータ再配置を中断する<<Bare metal>>
- 14.6 ドライブデータ再配置を再開する<<Bare metal>>

14.1 ドライブデータ再配置の概要<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ストレージノードの増設や減設によってストレージノード間の容量に偏りが生じた場合、各ストレージノードの容量の使用効率を最適化するため、ストレージノード間のデータ容量を平準化する、ドライブデータ再配置が動作します。

以下のようなケースでは、ドライブデータ再配置を中断してください。中断操作については「ドライブデータ再配置を中断する<<Bare metal>>」を参照してください。また、中断からの再開については「ドライブデータ再配置を再開する<<Bare metal>>」を参照してください。

- ドライブデータ再配置による性能低下を抑止するため(ドライブデータ再配置は、夜間などシステム負荷が軽い場合に再開させる)
- 他の保守操作を優先して実施するため(ドライブデータ再配置は、他の保守操作の完了後に再開させる)

14.2 ドライブデータ再配置の起動契機と動作可能な条件<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ドライブデータの再配置はストレージノードの増設または減設を契機に起動します。

ドライブデータ再配置の起動契機	ドライブデータ再配置先のストレージノード
ストレージノードを増設した場合	増設対象のストレージノードを含む、すべてのストレージノード
ストレージノードを減設した場合	減設対象のストレージノードを除く、すべてのストレージノード



メモ

- 複数フォールトドメイン構成の場合は、ドライブデータの再配置は動作しません。
- ドライブデータ再配置の処理中に、ドライブ障害またはストレージノード障害が発生した場合は、再配置の処理は中断されます。
- 再配置対象となるデータがない場合、ドライブデータ再配置は実行されません。

ドライブデータ再配置が動作する条件は以下のとおりです。

- ストレージクラスターの **status** が"Ready"であること
status が"Ready"でない場合、ドライブデータ再配置を動作させるためには、以下に従って対処してください。
 - status が"Stopping"、"Stopped"の場合「ストレージクラスターを起動する<<Bare metal>>」に従って、ストレージクラスターを起動してください。
 - 上記以外の status の場合、ストレージクラスターに対する処理が実施中のため、status が変わるまで待つてから、再度確認してください。
- すべてのストレージノードの **status** が"Ready"、"Removing"、"RemovalFailed"のいずれかの値であること
これら以外の status のストレージノードがある場合、ドライブデータ再配置を動作させるためには、以下に従って対処してください。

- VSP One SDS Block の VSP One SDS Block Administrator でストレージノードの Health Status に"Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
 ただし、"RemovalFailed"のストレージノードのみが存在する場合も"Alerting"になりますが、その場合は問題ありません。
- status が"MaintenanceBlockage"のストレージノードがある場合は「ストレージノードを保守回復する<<Bare metal>>」に従って、ストレージノードを保守回復してください。
- 上記以外の status のストレージノードがあった場合は、それらストレージノードに対する処理が実施中のため、status が変わるまで待ってから、再度確認してください。
- ・ プロテクションドメインの rebuildStatus が"Stopped"であること。
 rebuildStatus が他の値の場合は「リビルドの状態を確認する」に従って対処してください。
- ・ ドライブデータ再配置先のストレージノードに搭載されているドライブがストレージプールの拡張によってストレージプールに組み込まれていること
- ・ 別契機のドライブデータ再配置が動作中でないこと。
 動作中だった場合は、完了するまでお待ちください。
- ・ 「ドライブデータ再配置を中断する<<Bare metal>>」によって、ドライブデータ再配置が中断されていないこと(プロテクションドメインの driveDataRelocationStatus が"Suspended"になっていないこと)。*
 中断されている場合は「ドライブデータ再配置を再開する<<Bare metal>>」に従ってドライブデータ再配置を再開してください。
 * 次のすべての条件に該当する場合は、ドライブデータ再配置の中断状態であっても、ドライブデータ再配置は動作します。
 - ストレージノード減設契機のドライブデータ再配置である
 - ストレージノード増設契機のドライブデータ再配置が動作していない

14.3 ドライブデータ再配置完了までの時間(目安)<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ドライブデータ再配置の処理時間[min](目安)は以下の式で求められます。

HPEC 4D+1P の場合

処理時間[min] = ((増設または減設対象のストレージノードに搭載されている、ストレージプール拡張済みドライブの総物理容量 - 625[GiB]) / 625[GiB]) × ドライブデータ再配置の単位処理時間 [min]

HPEC 4D+2P の場合

処理時間[min] = ((増設または減設対象のストレージノードに搭載されている、ストレージプール拡張済みドライブの総物理容量 - 900[GiB]) / 900[GiB]) × ドライブデータ再配置の単位処理時間 [min]

Mirroring Duplication の場合

処理時間[min] = ((増設または減設対象のストレージノードに搭載されている、ストレージプール拡張済みドライブの総物理容量 - 200[GiB]) / 200[GiB]) × ドライブデータ再配置の単位処理時間 [min]



注意

ストレージコントローラーへ割り付けられる容量を超えた物理容量を搭載している場合、目安時間の計算値が多めに算出されることがあります。ストレージコントローラーへ割り付けられる最大容量は、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」に記載の以下を参照してください。

- ・ 「ユーザーデータドライブ」の「1 ドライブ当たりの必要容量」の備考欄

ドライブデータ再配置の単位処理時間[min]は、ユーザーデータの保護種別(redundantType)の設定と内部処理 I/O のリソース使用率の設定(asyncProcessingResourceUsageRate)とによって、以下になります。

なお、asyncProcessingResourceUsageRate の設定は、内部処理 I/O(リビルド、ドライブデータ再配置)のリソース使用率を決めるものです。設定値を変更するには「内部処理 I/O のリソース使用率を変更する」を参照してください。

redundantType	asyncProcessingResourceUsageRate	ドライブデータ再配置の単位処理時間[min](目安)
4D+1P	VeryHigh/High/Middle	100
	Low	200
4D+2P	VeryHigh/High/Middle	300
	Low	500
Duplication	VeryHigh/High/Middle	11
	Low	24



メモ

- ・ asyncProcessingResourceUsageRate の VeryHigh/High/Middle において、ドライブデータ再配置の処理時間に違いはありません。
- ・ ドライブデータ再配置の処理時間[min]は、以下の前提条件を満たす構成での測定結果に基づいています。
 - I/O 負荷あり
 - ストレージノード 1 台当たりのユーザーデータドライブの搭載台数：6 台
 - 使用するユーザーデータドライブ：SAS SSD
 - ストレージノード間ネットワークの帯域：10Gbps
 - ネットワークスイッチの MTU サイズ：9000 に設定
 - リビルド領域ポリシー(rebuildCapacityPolicy)の設定が"Fixed"かつ許容されるドライブ障害数(numberOfTolerableDriveFailures)が 1(デフォルト値)、またはリビルド領域ポリシーの設定が"Variable"であること



注意

ドライブデータ再配置の処理時間[min]は、以下の要因によって目安の処理時間よりも増減することがあります。

- ・ I/O 負荷の状況
- ・ ストレージノード 1 台当たりのユーザーデータドライブの搭載台数が 6 台未満の場合、目安時間よりも長くなることがあります。
(ユーザーデータドライブ 1 台当たりの I/O 負荷が高まるため)
- ・ ユーザーデータの保護方式が HPEC、かつストレージノード減設の場合
最小で処理時間(目安)に示した時間、最大で以下の計算式で示す時間が掛かります。
 - 4D+1P：処理時間[min] × (減設前のストレージノード数 / 5)
 - 4D+2P：処理時間[min] × (減設前のストレージノード数 / 6)

- リビルド領域ポリシーの設定が"Fixed"の場合
 - 許容されるドライブ障害数が 0 のとき、目安時間よりも長くなる場合があります。
 - 許容されるドライブ障害数が 2 以上のとき、目安時間よりも短くなる場合があります。
-

14.4 ドライブデータ再配置の状態を確認する <<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ドライブデータ再配置の状態と進捗率は、プロテクションドメインの情報を取得することで確認できます。

ロールによる実行制限はありません。

操作手順

1. プロテクションドメインの情報の一覧を取得して、driveDataRelocationStatus と driveDataRelocationProgressRate[%]を確認します。
REST API : GET /v1/objects/protection-domains
CLI : protection_domain_list
2. driveDataRelocationStatus にはドライブデータ再配置の状態が、driveDataRelocationProgressRate[%]にはドライブデータ再配置の処理の進捗率が表示されます。

- driveDataRelocationStatus
 - Stopped : ドライブデータ再配置の処理を実行していない状態
 - Running : ドライブデータ再配置の処理実行中の状態。ドライブデータ再配置の動作を止める場合は「ドライブデータ再配置を中断する <<Bare metal>>」を参照してください。
 - Error : ドライブデータ再配置の処理がエラー、またはドライブデータ再配置中に「ドライブデータ再配置の起動契機と動作可能な条件 <<Bare metal>>」を満たさなかったため、実行できない状態
 - Suspended : 「ドライブデータ再配置を中断する <<Bare metal>>」によって、ドライブデータ再配置処理が中断している状態
- driveDataRelocationProgressRate[%]
再配置のためのデータ転送が完了するたびに現在の進捗率が表示されます。



メモ

ドライブデータ再配置が中断した場合、再開時の進捗率は 0 から始まります。進捗率は 0 から再開しますが、中断するまでに処理が完了したデータは再度処理せずに、完了していないデータのみ処理します。

なお、ドライブデータ再配置が中断した場合、KARS07012-I または KARS07013-I のイベントログが出力されます。

14.5 ドライブデータ再配置を中断する <<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ドライブデータ再配置処理を中断します。

ドライブデータ再配置が動作中または停止中に、ドライブデータ再配置を中断すると以下の動作になります。

- ドライブデータ再配置処理が動作中だった場合、処理は中断され停止状態になります。
- ドライブデータ再配置処理が停止中だった場合、ストレージノード増設後のドライブデータ再配置は実行されません。



注意

- ストレージノード減設契機のドライブデータ再配置が動作すると、ドライブデータ再配置の中断状態が解除されます。
- ストレージノード減設契機のドライブデータ再配置を中断する場合は、ストレージノード減設の中止を実行してください。
- ストレージノード減設契機のドライブデータ再配置の実行中に、ドライブデータの再配置の中断は実行しないでください。
- ストレージノード減設契機のドライブデータ再配置の実行中に、ドライブデータの再配置の中断を実行した場合は、続けてストレージノード減設の中止を実行してください。

詳細は「ストレージノードの減設処理を中止する」を参照してください。

前提条件

- 実行に必要なロール：Storage または Service

操作手順

1. プロテクションドメインの情報の一覧を取得して、プロテクションドメインの ID と driveDataRelocationStatus を確認します。

REST API : GET /v1/objects/protection-domains

CLI : protection_domain_list

driveDataRelocationStatus が "Stopped" または "Running" のとき、次の手順に進みます。

2. ドライブデータ再配置を中断します。

プロテクションドメインの ID を指定してコマンドを実行します。

REST API : POST /v1/objects/protection-domains/<id>/actions/suspend-drive-data-relocation/invoke

CLI : protection_domain_suspend_drive_data_relocation

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

4. プロテクションドメインの情報の一覧を取得して、driveDataRelocationStatus を確認します。

REST API : GET /v1/objects/protection-domains

CLI : protection_domain_list

driveDataRelocationStatus が "Suspended" となっていることを確認します。



注意

ドライブデータ再配置の中断の要求後に、以下の障害が発生すると、ジョブが成功してもドライブデータ再配置が中断しない場合があります。

- ・ ストレージクラスターの障害
 - ・ クラスターマスターノード(プライマリー)の障害
- この場合は、再度ドライブデータ再配置の中断を実行してください。
-

14.6 ドライブデータ再配置を再開する《Bare metal》

この節での記述内容は Bare metal モデルに適用されます。

中断していたドライブデータ再配置の処理を再開します。

前提条件

- ・ 実行に必要なロール：Storage または Service

操作手順

1. プロテクションドメインの情報の一覧を取得して、プロテクションドメインの ID と driveDataRelocationStatus を確認します。
REST API：GET /v1/objects/protection-domains
CLI：protection_domain_list
driveDataRelocationStatus が"Suspended"のとき、次の手順に進みます。
2. ドライブデータ再配置の再開を実施します。
プロテクションドメインの ID を指定してコマンドを実行します。
REST API：POST /v1/objects/protection-domains/<id >/actions/resume-drive-data-relocation/invoke
CLI：protection_domain_resume_drive_data_relocation
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API：GET /v1/objects/jobs/<jobId >
CLI：job_show
state が"Succeeded"になっていたらジョブは完了です。
4. プロテクションドメインの情報の一覧を取得して、driveDataRelocationStatus を確認します。
REST API：GET /v1/objects/protection-domains
CLI：protection_domain_list
driveDataRelocationStatus が"Stopped"または"Running"となっていることを確認します。

コンピュータノードの接続を管理する

- 15.1 コンピュータノードの情報を登録する
- 15.2 コンピュータノード情報の一覧を取得する
- 15.3 コンピュータノード情報を個別に取得する
- 15.4 コンピュータノードの情報を編集する
- 15.5 コンピュータノードの情報を削除する
- 15.6 コンピュータノードのイニシエーター情報を登録する
- 15.7 コンピュータノードのイニシエーター情報の取得
- 15.8 コンピュータノードのイニシエーター情報を削除する
- 15.9 コンピュータノードのパス情報を登録する
- 15.10 コンピュータノードのパス情報の取得
- 15.11 コンピュータノードのパス情報の削除
- 15.12 ボリュームとコンピュータノードの接続
- 15.13 ボリュームとコンピュータノードの接続情報の取得
- 15.14 ボリュームとコンピュータノードの接続解除
- 15.15 複数のボリュームとコンピュータノードの接続解除

15.1 コンピュートノードの情報を登録する

コンピュートノードの情報を登録します。

登録できるコンピュートノードの最大数は、プロテクションドメイン当たり 1,024 です。ストレージノードの増設や減設によって、最大数が変わることはありません。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「コンピュートノードを登録する」

前提条件

- ・ 実行に必要なロール：Storage
- ・ VPS にコンピュートノードを登録する場合：当該 VPS のスコープ

操作手順

1. VPS にコンピュートノードを登録する場合、登録先の VPS の ID と VPS に設定された条件(コンピュートノード数上限)を確認します。

CLI を使って VPS を名前で指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

2. コンピュートノードの情報を登録します。

コンピュートノードのニックネームとコンピュートノードの OS 種別を指定してコマンドを実行します。

ニックネームを設定する場合は、以下に従ってください。

- ・ 文字数：1～229
- ・ 使用可能文字：1 文字目には、数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(¥.:@_)が使用でき、2 文字目以降には、1 文字目で使用できる文字に加えて記号(-)が使用できます。
- ・ 他のコンピュートノードと同じニックネームは設定できません。

REST API : POST /v1/objects/servers

CLI : server_create

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4. コンピュートノードの一覧を取得して、コンピュートノードの情報が登録されたことを確認します。

REST API : GET /v1/objects/servers

CLI : server_list

5. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

6. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.2 コンピュートノード情報の一覧を取得する

コンピュートノードの情報を一覧で取得します。

- id : コンピュートノードの ID(uuid)
- nickname : コンピュートノードのニックネーム
- osType : コンピュートノードの OS 種別
- totalCapacity : コンピュートノードに割り当てられたストレージプール上のボリュームの総容量[MiB]
- usedCapacity : コンピュートノードに割り当てられたストレージプール上のボリュームの使用量[MiB]
- numberOfPaths : 登録済みのパス数
- vpsId : コンピュートノードが所属する VPS の ID
- vpsName : コンピュートノードが所属する VPS の名前

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. コンピュートノード情報の一覧を取得します。

REST API : GET /v1/objects/servers

CLI : server_list

15.3 コンピュートノード情報を個別に取得する

指定した ID のコンピュートノードについて、以下の情報を取得します。

- numberOfVolumes : 割り当て済みボリューム数
- paths : 登録済みパスの情報の一覧
コンピュートノードのイニシエーターの WWN、iSCSI 名、または host NQN、割り当て先であるターゲット動作のコンピューポート ID の一覧
- id : コンピュートノードの ID(uuid)
- nickname : コンピュートノードのニックネーム

- `osType` : コンピュートノードの OS 種別
- `totalCapacity` : コンピュートノードに割り当てられたストレージプール上のボリュームの総容量[MiB]
- `usedCapacity` : コンピュートノードに割り当てられたストレージプール上のボリュームの使用量[MiB]
- `numberOfPaths` : 登録済みのパス数
- `vpsId` : コンピュートノードが所属する VPS の ID
- `vpsName` : コンピュートノードが所属する VPS の名前

前提条件

- 実行に必要なロール : `Security`、`Storage`、`RemoteCopy`、`Monitor`、`Service`、または `Resource`

操作手順

1. コンピュートノードの ID を確認します。
CLI を使いコンピュートノードをニックネームで指定する場合は、コンピュートノードのニックネームを確認します。
REST API : `GET /v1/objects/servers`
CLI : `server_list`
2. コンピュートノードの情報を取得します。
コンピュートノードの ID を指定してコマンドを実行します。
CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。
REST API : `GET /v1/objects/servers/<id>`
CLI : `server_show`

15.4 コンピュートノードの情報を編集する

コンピュートノードの情報を編集します。コンピュートノードのニックネームと OS 種別が編集できます。

ただし、他のコンピュートノードと同じニックネームは設定できません。



注意

コンピュートノードの情報を編集中は、対象コンピュートノードのボリュームパスに設定しているボリュームに対して、I/O が一時的に停止します。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「コンピュートノードを編集する」

前提条件

- 実行に必要なロール : `Storage`
- VPS に所属するコンピュートノードを編集する場合 : 当該 VPS のスコープ

操作手順

1. VPS に所属するコンピュータノードを編集する場合、VPS の ID を確認します。
CLI を使って VPS を名前で指定する場合は、VPS の名前を確認します。
REST API : GET /v1/objects/virtual-private-storages
CLI : vps_list
2. コンピュータノードの ID を確認します。
CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
3. コンピュータノードの情報を編集します。
コンピュータノードの ID を指定してコマンドを実行します。
CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。
REST API : PATCH /v1/objects/servers/<id >
CLI : server_set
コマンド実行後に表示されるジョブの ID を確認します。
4. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
5. コンピュータノードの一覧を取得して、コンピュータノードの情報が編集されたことを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
6. <<Bare metal>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
7. <<Cloud for AWS>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.5 コンピュータノードの情報を削除する

コンピュータノードの情報を削除します。コンピュータノードの情報を削除すると、コンピュータノードのすべてのイニシエーター情報、すべてのコンピュータノードのパス情報とすべてのポリシーパス情報もあわせて削除されます。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「コンピュートノードを削除する」

前提条件

- ・ 実行に必要なロール : **Storage**
- ・ VPS に所属するコンピュートノードを削除する場合 : 当該 VPS のスコープ

操作手順

1. VPS に所属するコンピュートノードを削除する場合、VPS の ID を確認します。
CLI を使って VPS を名前で指定する場合は、VPS の名前を確認します。
REST API : GET /v1/objects/virtual-private-storages
CLI : vps_list
2. コンピュートノードの ID を確認します。
CLI を使いコンピュートノードをニックネームで指定する場合は、コンピュートノードのニックネームを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
3. コンピュートノードの情報を削除します。
コンピュートノードの ID を指定してコマンドを実行します。
CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。
REST API : DELETE /v1/objects/servers/<id >
CLI : server_delete
コマンド実行後に表示されるジョブの ID を確認します。
4. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
5. コンピュートノードの一覧を取得して、コンピュートノードの情報が削除されたことを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
6. <<Bare metal>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
このマニュアルの「タスクをスケジュールする(コンピュートノードの OS が Windows の場合)」に従って、タスクスケジューラを登録している場合は、手順 8 に進みます。タスクスケジューラを登録していない場合は、以上で手順は終了です。
7. <<Cloud for AWS>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

このマニュアルの「タスクをスケジュールする(コンピュータノードの OS が Windows の場合)」に従って、タスクスケジューラを登録している場合は、次の手順に進みます。タスクスケジューラを登録していない場合は、以上で手順は終了です。

8. スタートメニューから[Windows 管理ツール]>[タスク スケジューラ]を選択します。
「タスク スケジューラ」画面が表示されます。
9. 画面左の[タスク スケジューラ ライブラリ]を選択し「タスクをスケジュールする(コンピュータノードの OS が Windows の場合)」で作成したタスクを選択し、画面右の操作メニューから[削除]をクリックします。
「タスクをスケジュールする(コンピュータノードの OS が Windows の場合)」で作成したタスクはすべて削除してください。
10. 「タスク スケジューラ」画面を閉じます。

15.6 コンピュータノードのイニシエーター情報を登録する

コンピュータノードを操作して、コンピュータノードのイニシエーター名(WWN、iSCSI 名、または host NQN)を調べたあと、コントローラーノードからコンピュータノードのイニシエーター情報を登録します。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「コンピュータノードを登録する」
- ・ 「コンピュータノードを編集する」

登録できるイニシエーターの最大数は、コンピュータノード当たり 4 です。

コンピュータノードとストレージノード間の接続方法によって手順が異なります。

15.6.1 iSCSI 接続している場合



注意

VSP One SDS Block に登録するコンピュータノードのイニシエーター名(iSCSI 名)は、ユニークであることが必要です。ご確認の上、登録してください。イニシエーター名(iSCSI 名)が重複したコンピュータノードからはボリュームが見られなくなります。

また、イニシエーター名(iSCSI 名)の先頭の"iqn"と"eui"は大文字では指定できません。小文字でのみ指定できます。

前提条件

- ・ 実行に必要なロール : Storage
- ・ VPS にイニシエーターを登録する場合 : 当該 VPS のスコープ
- ・ コンピュータノードの情報が登録済みであること

操作手順

1. コンピュートノードを操作して、コンピュートノードのイニシエーター名(iSCSI 名)を確認します。
詳細はコンピュートノードで使用している各種 OS のマニュアルなどを参照してください。
2. 手順 1 で確認したイニシエーター名(iSCSI 名)が、他のコンピュートノードのイニシエーター名(iSCSI 名)と重複していないことを確認します。
重複している場合は、イニシエーター名(iSCSI 名)を変更してください。
3. VPS にイニシエーターを登録する場合、VPS の ID と VPS に設定された条件(イニシエーター数上限)を確認します。
CLI を使って、VPS を名前で指定する場合は、VPS の名前を確認します。
REST API : GET /v1/objects/virtual-private-storages
CLI : vps_list
4. コンピュートノードの ID を確認します。
CLI を使いコンピュートノードをニックネームで指定する場合は、コンピュートノードのニックネームを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
5. イニシエーター情報を登録します。
コンピュートノードの ID、イニシエーターの接続プロトコル、イニシエーターの iSCSI 名を指定してコマンドを実行します。
CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。
REST API : POST /v1/objects/servers/<id>/hbas
CLI : hba_create
コマンド実行後に表示されるジョブの ID を確認します。
6. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId>
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
7. イニシエーター情報の一覧を取得して、イニシエーターの情報が登録されたことを確認します。
コンピュートノードの ID を指定してコマンドを実行します。
CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。
REST API : GET /v1/objects/servers/<id>/hbas
CLI : hba_list
8. ≪Bare metal≫構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
9. ≪Cloud for AWS≫構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.6.2 NVMe/TCP 接続している場合<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。



注意

VSP One SDS Block に登録するコンピュータノードのイニシエーター名(host NQN)は、ユニークであることが必要です。確認してから登録してください。

前提条件

- 実行に必要なロール : Storage
- VPS にイニシエーターを登録する場合 : 当該 VPS のスコープ
- コンピュータノードの情報が登録済みであること

操作手順

1. コンピュータノードを操作して、コンピュータノードのイニシエーター名(host NQN)を確認します。
詳細はコンピュータノードで使用している各種 OS のマニュアルなどを参照してください。
2. 手順 1 で確認したイニシエーター名(host NQN)が、他のコンピュータノードのイニシエーター名(host NQN)と重複していないことを確認します。
重複している場合は、イニシエーター名(host NQN)を変更してください。
3. VPS にイニシエーターを登録する場合、VPS の ID と VPS に設定された条件(イニシエーター数上限)を確認します。
CLI を使って、VPS を名前で指定する場合は、VPS の名前を確認します。
REST API : GET /v1/objects/virtual-private-storages
CLI : vps_list
4. コンピュータノードの ID を確認します。
CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。
REST API : GET /v1/objects/servers
CLI : server_list
5. イニシエーター情報を登録します。
コンピュータノードの ID、イニシエーターの接続プロトコル、イニシエーターの host NQN を指定してコマンドを実行します。
CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。
REST API : POST /v1/objects/servers/<id>/hbas
CLI : hba_create
コマンド実行後に表示されるジョブの ID を確認します。
6. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId>
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
7. イニシエーター情報の一覧を取得して、イニシエーターの情報が登録されたことを確認します。
コンピュータノードの ID を指定してコマンドを実行します。
CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。
REST API : GET /v1/objects/servers/<id>/hbas

CLI : hba_list

8. 構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.6.3 FC 接続している場合<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

前提条件

- ・ 実行に必要なロール : Storage
- ・ VPS にイニシエーターを登録する場合 : 当該 VPS のスコープ
- ・ コンピュートノードの情報が登録済みであること

操作手順

1. HBA ベンダー各社のマニュアルなどを参照して、WWN(WWPN)を確認します。

2. VPS にイニシエーターを登録する場合、VPS の ID と VPS に設定された条件(イニシエーター数上限)を確認します。

CLI を使い、VPS を名前で指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

3. コンピュートノードの ID を確認します。

CLI を使ってコンピュートノードをニックネームで指定する場合は、コンピュートノードのニックネームを確認します。

REST API : GET /v1/objects/servers

CLI : server_list

4. イニシエーター情報を登録します。

コンピュートノードの ID、イニシエーターの接続プロトコル、イニシエーター名(WWN(WWPN))を指定してコマンドを実行します。

CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。

REST API : POST /v1/objects/servers/<id>/hbas

CLI : hba_create

コマンド実行後に表示されるジョブの ID を確認します。

5. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

6. イニシエーター情報の一覧を取得して、イニシエーターの情報が登録されたことを確認します。

コンピュートノードの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。

REST API : GET /v1/objects/servers/<id>/hbas

CLI : hba_list

7. 構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.7 コンピュートノードのイニシエーター情報の取得

コンピュートノードのイニシエーターの情報が一覧または個別に取得できます。

15.7.1 取得できるコンピュートノードのイニシエーター情報

以下の情報が一覧または個別に取得できます。

- id : イニシエーターの ID(uuid)
- serverId : コンピュートノードの ID(uuid)
- name : イニシエーターの WWN、iSCSI 名、または host NQN
- protocol : イニシエーターの接続プロトコル
- portIds : 割り当て先であるターゲット動作のコンピューポートの ID 一覧(uuid)
- vpsId : イニシエーターが所属する VPS の ID
- vpsName : イニシエーターが所属する VPS の名前

15.7.2 コンピュートノードのイニシエーター情報の一覧を取得する

コンピュートノードのイニシエーターの情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. コンピュートノードの ID を確認します。

CLI を使いコンピュートノードをニックネームで指定する場合は、コンピュートノードのニックネームを確認します。

REST API : GET /v1/objects/servers

CLI : server_list

2. イニシエーター情報の一覧を取得します。

コンピュートノードの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。

REST API : GET /v1/objects/servers/<id>/hbas

CLI : hba_list

15.7.3 コンピュートノードのイニシエーター情報を個別に取得する

指定した ID のイニシエーター情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. コンピュートノードの ID を確認します。

CLI を使いコンピュートノードをニックネームで指定する場合は、コンピュートノードのニックネームを確認します。

REST API : GET /v1/objects/servers

CLI : server_list

2. イニシエーターの ID を確認します。

CLI を使いイニシエーターを WWN、iSCSI 名、または host NQN で指定する場合は、イニシエーターの WWN、iSCSI 名、または host NQN を確認します。

コンピュートノードの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。

REST API : GET /v1/objects/servers/<id>/hbas

CLI : hba_list

3. イニシエーター情報を取得します。

コンピュートノードの ID とイニシエーターの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュートノードの ID の代わりにニックネームが、イニシエーターの ID の代わりに WWN、iSCSI 名、または host NQN が指定できます。

REST API : GET /v1/objects/servers/<id>/hbas/<hbaId>

CLI : hba_show

15.8 コンピュートノードのイニシエーター情報を削除する

コンピュートノードのイニシエーター情報を削除します。イニシエーターの情報を削除すると、関連するすべてのコンピュートノードのパス情報もあわせて削除されます。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「コンピュートノードを編集する」

前提条件

- 実行に必要なロール : Storage
- VPS に所属するイニシエーターを削除する場合 : 当該 VPS のスコープ

操作手順

1. VPS に所属するイニシエーターを削除する場合、VPS の ID を確認します。

CLI を使って VPS を名前指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

- CLI : vps_list
2. コンピュートノードの ID を確認します。
- CLI を使いコンピュートノードをニックネームで指定する場合は、コンピュートノードのニックネームを確認します。
- REST API : GET /v1/objects/servers
- CLI : server_list
3. イニシエーターの ID を確認します。
- CLI を使いイニシエーターを WWN、iSCSI 名、または host NQN で指定する場合は、イニシエーターの WWN、iSCSI 名、または host NQN を確認します。
- コンピュートノードの ID を指定してコマンドを実行します。
- CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。
- REST API : GET /v1/objects/servers/<id>/hbas
- CLI : hba_list
4. イニシエーター情報を削除します。
- コンピュートノードの ID とイニシエーターの ID を指定してコマンドを実行します。
- CLI を使う場合はコンピュートノードの ID の代わりにニックネームが、イニシエーターの ID の代わりに WWN、iSCSI 名、または host NQN が指定できます。
- REST API : DELETE /v1/objects/servers/<id>/hbas/<hbaId>
- CLI : hba_delete
- コマンド実行後に表示されるジョブの ID を確認します。
5. ジョブの state を確認します。
- ジョブの ID を指定してコマンドを実行します。
- REST API : GET /v1/objects/jobs/<jobId>
- CLI : job_show
- state が "Succeeded" になっていたらジョブは完了です。
6. イニシエーター情報の一覧を取得して、イニシエーターの情報が削除されたことを確認します。
- コンピュートノードの ID を指定してコマンドを実行します。
- CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。
- REST API : GET /v1/objects/servers/<id>/hbas
- CLI : hba_list
7. <<Bare metal>>構成情報のバックアップを行います。
- 「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。
- ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
8. <<Cloud for AWS>>構成情報のバックアップを行います。
- 「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。
- ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.9 コンピュートノードのパス情報を登録する

コンピュートノードのパス情報を登録します。

登録できるコンピュータノードのパス情報の最大数は、コンピュータノード当たり 4,096、コンピュータポート当たり 255 です。ここで、コンピュータノード当たりのパス情報の最大数は、ストレージノード数、ストレージノードのコンピュータポート数、またはコンピュータノードに登録したイニシエーター数に依存して増減します。

portId パラメーターと hbaId パラメーターの指定によって、以下が行えます。

- portId と hbaId の両方を省略：対象のコンピュータノードが持つすべてのイニシエーターをすべてのコンピュータポートに割り当てる
- hbaId のみを指定：指定したイニシエーターをすべてのコンピュータポートに割り当てる
- portId のみを指定：指定したコンピュータポートを対象のコンピュータノードが持つすべてのイニシエーターに割り当てる
- portId と hbaId の両方を指定：hbaId で指定したイニシエーターを portId で指定したコンピュータポートに割り当てる



注意

- コンピュータノードのパス情報を変更した場合は、I/O を開始する前に対象のコンピュータノード上でストレージの再スキャンを実施してください。
- コンピュータノードとして VMware ESXi を使用している場合は、コンピュータノードとすべてのコンピュータポートの間でパスを設定してください。すべてのパスが設定されていないと、コンピュータノードから一部のボリュームが見えなくなる場合があります。
コンピュータノードとして VMware ESXi を使用していない場合でも、I/O 性能を低下させないよう、コンピュータノードとすべてのコンピュータポートの間でパスを設定することをお勧めします。
- iSCSI 接続で利用する場合、コンピュータノードとストレージ間の最大 TCP コネクション数はストレージノード当たり 128 です。NVMe/TCP 接続で利用する場合、最大 TCP コネクション数はコンピュータポート当たり 255 です。上限を超過した場合、超過した以降のコンピュータノードとストレージ間の接続は失敗します。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「コンピュータノードを登録する」
- 「コンピュータノードを編集する」
ただし、VSP One SDS Block Administrator ではフルメッシュで設定されます。

前提条件

- 実行に必要なロール：Storage
- コンピュータノードとイニシエーターの情報が登録済みであること
- VPS にコンピュータノードのパス情報を登録する場合：当該 VPS のスコープ

操作手順

1. VPS にコンピュータノードのパス情報を登録する場合、登録先の VPS の ID を確認します。
CLI を使って VPS を名前前で指定する場合は、VPS の名前を確認します。
REST API : GET /v1/objects/virtual-private-storages
CLI : vps_list
2. コンピュータノードの ID を確認します。

CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。

REST API : GET /v1/objects/servers

CLI : server_list

3. hbaId パラメーターを指定する場合は、コンピュータノードのイニシエーターの ID を確認します。

コンピュータノードの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。

REST API : GET /v1/objects/servers/<id >/hbas

CLI : hba_list

4. portId パラメーターを指定する場合は、コンピュータノードに割り当てるコンピュータポートの ID を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

5. コンピュータノードのパス情報を登録します。

コンピュータノードの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。また、割り当て先であるターゲット動作のコンピュータポートを ID の代わりに、WWN または iSCSI Name で指定できます。

REST API : POST /v1/objects/servers/<id >/paths

CLI : path_create

コマンド実行後に表示されるジョブの ID を確認します。

6. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

7. パス情報の一覧を取得して、パス情報が追加されたことを確認します。

コンピュータノードの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。

REST API : GET /v1/objects/servers/<id >/paths

CLI : path_list

8. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

9. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.10 コンピュートノードのパス情報の取得

コンピュートノードのパス情報が取得できます。

15.10.1 取得できるコンピュートノードのパス情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- **id** : パスの ID
コンピュートノードのイニシエーターの ID とターゲット動作のコンピューポートの ID をコンマ","でつないだ文字列
- **serverId** : コンピュートノードの ID(uuid)
- **hbaName** : コンピュートノードのイニシエーターの WWN、iSCSI 名、または host NQN
- **hbaId** : コンピュートノードのイニシエーターの ID(uuid)
- **portId** : 割り当て先であるターゲット動作のコンピューポートの ID(uuid)
- **portName** : iSCSI 接続または FC 接続の場合は、割り当て先であるターゲット動作のコンピューポートの iSCSI 名または WWN。NVMe/TCP 接続の場合は、常に null
- **portNickname** : 割り当て先であるターゲット動作のコンピューポートのニックネーム
- **vpsId** : コンピュートノードパスが所属する VPS の ID
- **vpsName** : コンピュートノードパスが所属する VPS の名前

15.10.2 取得できるコンピュートノードのパス情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- **id** : パスの ID
コンピュートノードのイニシエーターの ID とターゲット動作のコンピューポートの ID をコンマ","でつないだ文字列
- **serverId** : コンピュートノードの ID(uuid)
- **hbaName** : コンピュートノードのイニシエーターの iSCSI 名
- **hbaId** : コンピュートノードのイニシエーターの ID(uuid)
- **portId** : 割り当て先であるターゲット動作のコンピューポートの ID(uuid)
- **portName** : 割り当て先であるターゲット動作のコンピューポートの iSCSI 名
- **portNickname** : 割り当て先であるターゲット動作のコンピューポートのニックネーム
- **vpsId** : コンピュートノードパスが所属する VPS の ID
- **vpsName** : コンピュートノードパスが所属する VPS の名前

15.10.3 コンピュートノードのパス情報の一覧を取得する

コンピュートノードのパス情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. コンピュートノードの ID を確認します。
REST API : GET /v1/objects/servers
CLI : server_list
2. コンピュートノードのパス情報の一覧を取得します。
コンピュートノードの ID を指定してコマンドを実行します。
CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。
REST API : GET /v1/objects/servers/<id >/paths
CLI : path_list

15.10.4 コンピュートノードのパス情報を個別に取得する ≪Bare metal≫

この項での記述内容は Bare metal モデルに適用されます。

指定した ID のコンピュートノードのパス情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. コンピュートノードの ID を確認します。
CLI を使いコンピュートノードをニックネームで指定する場合は、コンピュートノードのニックネームを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
2. コンピュートノードのイニシエーターの ID とコンピューポートの ID を確認します。
 - iSCSI 接続の場合 : CLI を使いイニシエーターとコンピューポートを iSCSI 名で指定するときは、イニシエーターとコンピューポートの iSCSI 名を確認します。
 - FC 接続の場合 : CLI を使いイニシエーターとコンピューポートを WWN で指定するときは、イニシエーターとコンピューポートの WWN を確認します。
 - NVMe/TCP 接続の場合 : CLI を使いイニシエーターを host NQN で指定するときは、イニシエーターの host NQN を確認します。コンピュートノードの ID を指定してコマンドを実行します。
CLI を使う場合はコンピュートノードの ID の代わりにニックネームが指定できます。
REST API : GET /v1/objects/servers/<id >/hbas
CLI : hba_list
3. コンピュートノードのパス情報を取得します。
コンピュートノードの ID、イニシエーターの ID、ターゲット動作のコンピューポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが、イニシエーターの ID の代わりに WWN、iSCSI 名、または host NQN が、コンピュータポートの ID の代わりに WWN または iSCSI 名が指定できます。

REST API : GET /v1/objects/servers/<id >/paths/<hbaId >,<portId >

CLI : path_show

15.10.5 コンピュートノードのパス情報を個別に取得する《Cloud》

この項での記述内容は Cloud モデルに適用されます。

指定した ID のコンピュータノードのパス情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. コンピュートノードの ID を確認します。

CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。

REST API : GET /v1/objects/servers

CLI : server_list

2. コンピュートノードのイニシエーターの ID とコンピュータポートの ID を確認します。

CLI を使いイニシエーターとコンピュータポートを iSCSI 名で指定するときは、イニシエーターとコンピュータポートの iSCSI 名を確認します。

コンピュータノードの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。

REST API : GET /v1/objects/servers/<id >/hbas

CLI : hba_list

3. コンピュートノードのパス情報を取得します。

コンピュータノードの ID、イニシエーターの ID、ターゲット動作のコンピュータポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが、イニシエーターの ID の代わりに iSCSI 名が、コンピュータポートの ID の代わりに iSCSI 名が指定できます。

REST API : GET /v1/objects/servers/<id >/paths/<hbaId >,<portId >

CLI : path_show

15.11 コンピュートノードのパス情報の削除

コンピュータノードのパス情報の削除方法について説明します。

15.11.1 コンピュートノードのパス情報を削除する《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

コンピュータノードのパス情報を削除します。



注意

- コンピュートノードがクラスタリング構成かつ認識しているボリュームがオンライン状態の場合、対象のボリュームがオフライン状態であることを確認してから接続の解除を行ってください。
- FC 接続または iSCSI 接続の場合、パス情報を削除するコンピュータノードからアクセスできる状態のボリュームが SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態であるときは、SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態を解除してから、パス情報を削除してください。
- コンピュートノードのパス情報を変更した場合は、対象のコンピュータノード上でストレージの再スキャンを実施してください。削除済みのパス情報がコンピュータノード上に残り続けると誤動作につながります。

前提条件

- 実行に必要なロール : Storage
- VPS に所属するコンピュータノードのパス情報を削除する場合 : 当該 VPS のスコープ

操作手順

1. VPS に所属するコンピュータノードのパス情報を削除する場合、VPS の ID を確認します。

CLI を使って VPS を名前指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

2. コンピュートノードの ID を確認します。

CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。

REST API : GET /v1/objects/servers

CLI : server_list

3. コンピュートノードのパス情報の一覧を取得します。

コンピュータノードの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。

REST API : GET /v1/objects/servers/<id>/paths

CLI : path_list

4. コンピュートノードのパス情報を削除します。

コンピュータノードの ID、イニシエーターの ID、ターゲット動作のコンピュータポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが、イニシエーターの ID の代わりに WWN、iSCSI 名、または host NQN が、コンピュータポートの ID の代わりに WWN または iSCSI 名が指定できます。

REST API : DELETE /v1/objects/servers/<id>/paths/<hbaId>,<portId>

CLI : path_delete

コマンド実行後に表示されるジョブの ID を確認します。

5. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

6. パス情報の一覧を取得して、パス情報が削除されたことを確認します。

コンピュータノードの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。

REST API : GET /v1/objects/servers/<id >/paths

CLI : path_list

7. 構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.11.2 コンピュートノードのパス情報を削除する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

コンピュータノードのパス情報を削除します。



注意

- コンピュートノードがクラスタリング構成かつ認識しているボリュームがオンライン状態の場合、対象のボリュームがオフライン状態であることを確認してから接続の解除を行ってください。
- パス情報を削除するコンピュータノードからアクセスできる状態のボリュームが SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態であるときは、SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態を解除してから、パス情報を削除してください。
- コンピュートノードのパス情報を変更した場合は、対象のコンピュータノード上でストレージの再スキャンを実施してください。削除済みのパス情報がコンピュータノード上に残り続けると誤動作につながります。

前提条件

- 実行に必要なロール : Storage

操作手順

1. コンピュートノードの ID を確認します。

CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。

REST API : GET /v1/objects/servers

CLI : server_list

2. コンピュートノードのパス情報の一覧を取得します。

コンピュータノードの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。

REST API : GET /v1/objects/servers/<id >/paths

CLI : path_list

3. コンピュートノードのパス情報を削除します。

コンピュータノードの ID、イニシエーターの ID、ターゲット動作のコンピュータポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータノードの ID の代わりにニックネームが、イニシエーターの ID の代わりに iSCSI 名が、コンピュータポートの ID の代わりに iSCSI 名が指定できます。

REST API : DELETE /v1/objects/servers/<id >/paths/<hbaId >,<portId >

CLI : path_delete

コマンド実行後に表示されるジョブの ID を確認します。

4. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
5. パス情報の一覧を取得して、パス情報が削除されたことを確認します。
コンピュータノードの ID を指定してコマンドを実行します。
CLI を使う場合はコンピュータノードの ID の代わりにニックネームが指定できます。
REST API : GET /v1/objects/servers/<id >/paths
CLI : path_list
6. <<Cloud for AWS>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.12 ボリュームとコンピュータノードの接続

ボリュームをコンピュータノードに接続する方法について説明します。

15.12.1 ボリュームをコンピュータノードに接続する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ボリュームとコンピュータノード間でパス(ボリュームパス)を設定します。

Universal Replicator を使用している場合は、以下に留意してください。

- universalReplicatorAttribute が"P-VOL"または"S-VOL"のボリュームは、コンピュータノードとの間でボリュームパスが設定できます。
- volumeType が"Journal"または"FormerJournal"のボリュームは、コンピュータノードとの間でボリュームパスは設定できません。

登録できるボリュームパスの最大数は、コンピュータノード当たり 8,192、ストレージコントローラ当たり 2,048、ストレージクラスター当たり 65,536 です。



ヒント

- FC 接続または iSCSI 接続している場合
パラメーターの指定方法として、以下の組み合わせがあります。
 - volumeId、serverId、lun の組み合わせ : volumeId で指定したボリュームを、serverId で指定したコンピュータノードに割り当てる(lun は省略可)
 - volumeIds、serverIds、startLun の組み合わせ : volumeIds で指定したすべてのボリュームを、serverIds で指定したすべてのコンピュータノードに割り当てる(startLun は省略可)
- NVMe/TCP 接続している場合
パラメーターの指定方法として、以下の組み合わせがあります。
 - volumeId、serverId の組み合わせ : volumeId で指定したボリュームを、serverId で指定したコンピュータノードに割り当てる
 - volumeIds、serverIds の組み合わせ : volumeIds で指定したすべてのボリュームを、serverIds で指定したすべてのコンピュータノードに割り当てる



注意 接続プロトコル共通の注意事項

- コンピュートノードとして VMware ESXi を使用している場合は、コンピュートノードのパス情報の登録において、コンピュートノードとすべてのコンピューポートの間でパスを設定してください。すべてのパスが設定されていないと、コンピュートノードから一部のボリュームが見えなくなる場合があります。コンピュートノードとして VMware ESXi を使用していない場合でも、I/O 性能を低下させないよう、コンピュートノードとすべてのコンピューポートの間でパスを設定してください。設定方法は「コンピュートノードのパス情報を登録する」を参照してください。
- ボリュームとコンピュートノードの接続情報を変更した場合は、I/O を開始する前に対象のコンピュートノード上でストレージの再スキャンを実施してください。
- ボリュームパス登録の処理性能
対象のコンピュートノードに登録済みのボリュームパスの数によって以下のように処理時間が増加します。
 - 1 件目のボリュームパスの登録の場合、処理時間は 1～2 秒で処理が完了します。
 - 登録済みボリュームパス 1,000 件当たり、1 ボリュームパス登録の処理時間が 1～2 秒増加します。
 - 8,192 件目(最大)のボリュームパスを登録する場合、処理時間は 15 秒程度掛かります。
- 以下が発生している場合、ホストからボリュームが認識できなくなることがあります。
 - ストレージコントローラーの容量枯渇
ホストからボリュームが認識されない場合、KARS06003-E が出力されているかを確認し、出力されている場合はアクションに従ってストレージコントローラーの問題を解消してください。



注意 FC 接続または iSCSI 接続している場合の注意事項

- lun または startLun を省略してボリュームパスを設定した場合、未使用の LUN 最小値が自動的に割り当てられます。ただし、lun を省略したボリュームパス設定が同時に行われた場合、または複数のボリュームに対してボリュームパスを設定した場合、設定順に昇順で LUN が割り当てられない可能性があります。割り当てる LUN を特定値にしたい場合は、lun を省略せずにボリュームパス設定を実施してください。
- OS によって、一部のボリュームが認識できない場合、次のような挙動になることがあります。ボリューム認識できない状態を解消してから、コンピュートノード上でストレージの再スキャンを再度実施してください。
 - LUN の小さい番号から順番に LUN を認識する際、認識できない LUN が存在した時点で、以降の LUN を認識しない。
 - LUN=0 の LUN を認識できなかった時点で、以降の LUN を認識しない。



注意 NVMe/TCP 接続している場合の注意事項

- ボリュームパスを設定したボリュームは、コンピュートノードからは NVMe デバイスとして認識できるようになります。NVM デバイス制御情報である NVM サブシステムおよび Namespace はストレージ側で自動で割り当てられ、ボリュームパスの設定後に参照可能となります。NVM サブシステムおよび Namespace の割り当てに関する詳細については「NVMe/TCP 接続時のシステム構成<<Bare metal>>」を参照してください。
- 一部またはすべてのボリュームが認識できない場合は、コンピュートノードとストレージノードとの接続を確認し、コンピュートノード上でストレージの再スキャンを実施してください。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ボリュームとコンピュートノードを接続する(Volume)」
- 「ボリュームとコンピュートノードを接続する(Compute Node)」

前提条件

- 実行に必要なロール : Storage
- ボリュームが作成済みでコンピュータノードの情報が登録済みであること
- VPS にボリュームパスを登録する場合 : 当該 VPS のスコープ

操作手順

1. VPS にボリュームパスを登録する場合、登録先の VPS の ID と VPS に設定された条件(ボリュームパス数上限)を確認します。
CLI を使って VPS を名前で指定する場合は、VPS の名前を確認します。
REST API : GET /v1/objects/virtual-private-storages
CLI : vps_list
2. 割り当て対象のボリュームの ID を確認します。
CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。
REST API : GET /v1/objects/volumes
CLI : volume_list
3. 割り当て先のコンピュータノードの ID を確認します。
CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
4. ボリュームをコンピュータノードに接続します。
REST API : POST /v1/objects/volume-server-connections
CLI : volume_server_connection_create
コマンド実行後に表示されるジョブの ID を確認します。
5. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
6. ボリュームとコンピュータノードの接続情報の一覧を取得して、コンピュータノードにボリュームが接続されたことを確認します。
REST API : GET /v1/objects/volume-server-connections
CLI : volume_server_connection_list
7. 構成情報のバックアップを行います。
「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.12.2 ボリュームをコンピュータノードに接続する <<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ボリュームとコンピュータノード間でパス(ボリュームパス)を設定します。

Universal Replicator を使用している場合は、以下に留意してください。

- `universalReplicatorAttribute` が"P-VOL"または"S-VOL"のボリュームは、コンピュータノードとの間でボリュームパスが設定できます。
- `volumeType` が"Journal"または"FormerJournal"のボリュームは、コンピュータノードとの間でボリュームパスは設定できません。

登録できるボリュームパスの最大数は、コンピュータノード当たり 8,192、ストレージコントローラー当たり 2,048、ストレージクラスター当たり 65,536 です。



ヒント

パラメーターの指定方法として、以下の組み合わせがあります。

- `volumeId`、`serverId`、`lun` の組み合わせ：`volumeId` で指定したボリュームを、`serverId` で指定したコンピュータノードに割り当てる(`lun` は省略可)
- `volumeIds`、`serverIds`、`startLun` の組み合わせ：`volumeIds` で指定したすべてのボリュームを、`serverIds` で指定したすべてのコンピュータノードに割り当てる(`startLun` は省略可)



注意

- コンピュータノードとして VMware ESXi を使用している場合は、コンピュータノードのパス情報の登録において、コンピュータノードとすべてのコンピュータポートの間でパスを設定してください。すべてのパスが設定されていないと、コンピュータノードから一部のボリュームが見えなくなる場合があります。コンピュータノードとして VMware ESXi を使用していない場合でも、I/O 性能を低下させないように、コンピュータノードとすべてのコンピュータポートの間でパスを設定してください。設定方法は「コンピュータノードのパス情報を登録する」を参照してください。
- ボリュームとコンピュータノードの接続情報を変更した場合は、I/O を開始する前に対象のコンピュータノード上でストレージの再スキャンを実施してください。
- ボリュームパス登録の処理性能
対象のコンピュータノードに登録済みのボリュームパスの数によって以下のように処理時間が増加します。
 - 1 件目のボリュームパスの登録の場合、処理時間は 1～2 秒で処理が完了します。
 - 登録済みボリュームパス 1,000 件当たり、1 ボリュームパス登録の処理時間が 1～2 秒増加します。
 - 8,192 件目(最大)のボリュームパスを登録する場合、処理時間は 15 秒程度掛かります。
- 以下が発生している場合、ホストからボリュームが認識できなくなることがあります。
 - ストレージコントローラーの容量枯渇
ホストからボリュームが認識されない場合、KARS06003-E が出力されているかを確認し、出力されている場合はアクションに従ってストレージコントローラーの問題を解消してください。
- `lun` または `startLun` を省略してボリュームパスを設定した場合、未使用の LUN 最小値が自動的に割り当てられます。ただし、`lun` を省略したボリュームパス設定が同時に行われた場合、または複数のボリュームに対してボリュームパスを設定した場合、設定順に昇順で LUN が割り当てられない可能性があります。割り当てる LUN を特定値にしたい場合は、`lun` を省略せずにボリュームパス設定を実施してください。
- OS によって、一部のボリュームが認識できない場合、次のような挙動になることがあります。ボリューム認識できない状態を解消してから、コンピュータノード上でストレージの再スキャンを再度実施してください。
 - LUN の小さい番号から順番に LUN を認識する際、認識できない LUN が存在した時点で、以降の LUN を認識しない。
 - LUN=0 の LUN を認識できなかった時点で、以降の LUN を認識しない。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ボリュームとコンピュータノードを接続する(Volume)」
- ・ 「ボリュームとコンピュータノードを接続する(Compute Node)」

前提条件

- ・ 実行に必要なロール : Storage
- ・ ボリュームが作成済みでコンピュータノードの情報が登録済みであること

操作手順

1. 割り当て対象のボリュームの ID を確認します。
CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。
REST API : GET /v1/objects/volumes
CLI : volume_list
2. 割り当て先のコンピュータノードの ID を確認します。
CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
3. ボリュームをコンピュータノードに接続します。
REST API : POST /v1/objects/volume-server-connections
CLI : volume_server_connection_create
コマンド実行後に表示されるジョブの ID を確認します。
4. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId>
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
5. ボリュームとコンピュータノードの接続情報の一覧を取得して、コンピュータノードにボリュームが接続されたことを確認します。
REST API : GET /v1/objects/volume-server-connections
CLI : volume_server_connection_list
6. <<Cloud for AWS>> 構成情報のバックアップを行います。
「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.13 ボリュームとコンピュータノードの接続情報の取得

ボリュームとコンピュータノードの接続情報が取得できます。

15.13.1 取得できるボリュームとコンピュータノードの接続情報 <<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- **id** : ボリュームパスの ID
ボリュームの ID とコンピュータノードの ID をコンマ","でつないだ文字列
- **serverId** : コンピュータノードの ID(uuid)
- **volumeId** : ボリュームの ID(uuid)
- **lun** : FC 接続または iSCSI 接続の場合は LUN。NVMe/TCP 接続の場合は常に null
- **nameSpaceId** : FC 接続または iSCSI 接続の場合は常に null。NVMe/TCP 接続の場合は Namespace
- **nvmSubSystemNqn** : FC 接続または iSCSI 接続の場合は常に null。NVMe/TCP 接続の場合はサブシステムの識別情報
- **vpsId** : ボリュームパスが所属する VPS の ID
- **vpsName** : ボリュームパスが所属する VPS の名前

15.13.2 取得できるボリュームとコンピュータノードの接続情報 《Cloud》

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- **id** : ボリュームパスの ID
ボリュームの ID とコンピュータノードの ID をコンマ","でつないだ文字列
- **serverId** : コンピュータノードの ID(uuid)
- **volumeId** : ボリュームの ID(uuid)
- **lun** : LUN
- **nameSpaceId** : 常に null
- **nvmSubSystemNqn** : 常に null
- **vpsId** : ボリュームパスが所属する VPS の ID
- **vpsName** : ボリュームパスが所属する VPS の名前

15.13.3 ボリュームとコンピュータノードの接続情報の一覧を取得する

ボリュームとコンピュータノードの接続情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ボリュームの ID を確認します。
REST API : GET /v1/objects/volumes
CLI : volume_list
2. コンピュータノードの ID を確認します。
REST API : GET /v1/objects/servers
CLI : server_list
3. ボリュームとコンピュータノードの接続情報の一覧を取得します。

ボリュームの ID またはコンピュータノードの ID をクエリーパラメーターで指定してコマンドを実行します。

REST API : GET /v1/objects/volume-server-connections

CLI : volume_server_connection_list

15.13.4 ボリュームとコンピュータノードの接続情報を個別に取得する

指定した ID のボリュームと指定した ID のコンピュータノードについての接続情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ボリュームの ID を確認します。

CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

2. コンピュータノードの ID を確認します。

CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。

REST API : GET /v1/objects/servers

CLI : server_list

3. ボリュームとコンピュータノードの接続情報を取得します。

ボリュームの ID とコンピュータノードの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が、コンピュータノードの ID の代わりにニックネームが指定できます。

REST API : GET /v1/objects/volume-server-connections/<volumeId>,<serverId>

CLI : volume_server_connection_show

15.14 ボリュームとコンピュータノードの接続解除

ボリュームとコンピュータノードの接続を解除する方法について説明します。

15.14.1 ボリュームとコンピュータノードの接続を解除する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ボリュームとコンピュータノードのパス(ボリュームパス)を削除して接続を解除します。コンピュータノードからボリュームへの I/O がいないことを必ず確認してから、実行してください。

Universal Replicator を使用している場合は、以下に留意してください。

- universalReplicatorAttribute が"P-VOL"または"S-VOL"のボリュームとコンピュータノード間のボリュームパスは、Universal Replicator ペアを削除することで解除できるようになります。



注意

- コンピュートノードがクラスタリング構成かつ認識しているボリュームがオンライン状態の場合、対象のボリュームがオフライン状態であることを確認してから接続の解除を行ってください。
- FC 接続または iSCSI 接続の場合、パス情報を削除するコンピュータノードからアクセスできる状態のボリュームが、SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態である場合は、SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態を解除してから、パス情報を削除してください。
- コンピュートノードのパス情報を変更した場合は、対象のコンピュータノード上でストレージの再スキャンを実施してください。削除済みのパス情報がコンピュータノード上に残り続けると誤動作につながります。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ボリュームとコンピュータノードの接続を解除する」

前提条件

- 実行に必要なロール : Storage
- VPS に所属するボリュームパスを解除する場合 : 当該 VPS のスコープ

操作手順

1. VPS に所属するボリュームパスを解除する場合、VPS の ID を確認します。
CLI を使って VPS を名前で指定する場合は、VPS の名前を確認します。
REST API : GET /v1/objects/virtual-private-storages
CLI : vps_list
2. ボリュームの ID を確認します。
CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。
REST API : GET /v1/objects/volumes
CLI : volume_list
3. コンピュートノードの ID を確認します。
CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
4. ボリュームとコンピュータノードの接続情報の一覧を取得します。
ボリュームの ID またはコンピュータノードの ID をクエリーパラメーターで指定してコマンドを実行します。
CLI を使う場合はボリュームの ID の代わりに名前が、コンピュータノードの ID の代わりにニックネームが指定できます。
REST API : GET /v1/objects/volume-server-connections
CLI : volume_server_connection_list
5. ボリュームとコンピュータノードの接続を解除します。
ボリュームの ID とコンピュータノードの ID を指定してコマンドを実行します。
CLI を使う場合はボリュームの ID の代わりに名前が、コンピュータノードの ID の代わりにニックネームが指定できます。

REST API : DELETE /v1/objects/volume-server-connections/<volumeId >,<serverId >

CLI : volume_server_connection_delete

コマンド実行後に表示されるジョブの ID を確認します。

6. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

7. ボリュームとコンピュータノードの接続情報の一覧を取得して、接続が解除されたことを確認します。

REST API : GET /v1/objects/volume-server-connections

CLI : volume_server_connection_list

8. 構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.14.2 ボリュームとコンピュータノードの接続を解除する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ボリュームとコンピュータノードのパス(ボリュームパス)を削除して接続を解除します。コンピュータノードからボリュームへの I/O がないことを必ず確認してから、実行してください。

Universal Replicator を使用している場合は、以下に留意してください。

- universalReplicatorAttribute が"P-VOL"または"S-VOL"のボリュームとコンピュータノード間のボリュームパスは、Universal Replicator ペアを削除することで解除できるようになります。



注意

- コンピュータノードがクラスタリング構成かつ認識しているボリュームがオンライン状態の場合、対象のボリュームがオフライン状態であることを確認してから接続の解除を行ってください。
- パス情報を削除するコンピュータノードからアクセスできる状態のボリュームが、SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態である場合は、SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態を解除してから、パス情報を削除してください。
- コンピュータノードのパス情報を変更した場合は、対象のコンピュータノード上でストレージの再スキャンを実施してください。削除済みのパス情報がコンピュータノード上に残り続けると誤動作につながります。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ボリュームとコンピュータノードの接続を解除する」

前提条件

- 実行に必要なロール : Storage

操作手順

1. ボリュームの ID を確認します。
CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。
REST API : GET /v1/objects/volumes
CLI : volume_list
2. コンピュートノードの ID を確認します。
CLI を使いコンピュートノードをニックネームで指定する場合は、コンピュートノードのニックネームを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
3. ボリュームとコンピュートノードの接続情報の一覧を取得します。
ボリュームの ID またはコンピュートノードの ID をクエリーパラメーターで指定してコマンドを実行します。
CLI を使う場合はボリュームの ID の代わりに名前が、コンピュートノードの ID の代わりにニックネームが指定できます。
REST API : GET /v1/objects/volume-server-connections
CLI : volume_server_connection_list
4. ボリュームとコンピュートノードの接続を解除します。
ボリュームの ID とコンピュートノードの ID を指定してコマンドを実行します。
CLI を使う場合はボリュームの ID の代わりに名前が、コンピュートノードの ID の代わりにニックネームが指定できます。
REST API : DELETE /v1/objects/volume-server-connections/<volumeId>,<serverId>
CLI : volume_server_connection_delete
コマンド実行後に表示されるジョブの ID を確認します。
5. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId>
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
6. ボリュームとコンピュートノードの接続情報の一覧を取得して、接続が解除されたことを確認します。
REST API : GET /v1/objects/volume-server-connections
CLI : volume_server_connection_list
7. ≪Cloud for AWS≫構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.15 複数のボリュームとコンピュータノードの接続解除

ボリュームとコンピュータノード接続を複数解除する方法について説明します。

15.15.1 複数のボリュームとコンピュータノードの接続を解除する ≪Bare metal≫

この項での記述内容は Bare metal モデルに適用されます。

指定したすべてのボリュームと、指定したすべてのコンピュータノードのパス(ボリュームパス)を削除して接続を解除します。コンピュータノードからボリュームへの I/O がいないことを必ず確認してから、実行してください。



注意

- コンピュータノードがクラスタリング構成かつ認識しているボリュームがオンライン状態の場合、対象のボリュームがオフライン状態であることを確認してから接続の解除を行ってください。
- FC 接続または iSCSI 接続の場合、パス情報を削除するコンピュータノードからアクセスできる状態のボリュームが、SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態である場合は、SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態を解除してから、パス情報を削除してください。
- コンピュータノードのパス情報を変更した場合は、対象のコンピュータノード上でストレージの再スキャンを実施してください。削除済みのパス情報がコンピュータノード上に残り続けると誤動作につながります。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ボリュームとコンピュータノードの接続を解除する」

前提条件

- 実行に必要なロール : Storage
- VPS に所属するボリュームパスを解除する場合 : 当該 VPS のスコープ

操作手順

1. VPS に所属するボリュームパスを解除する場合、VPS の ID を確認します。
CLI を使って VPS を名前で指定する場合は、VPS の名前を確認します。
REST API : GET /v1/objects/virtual-private-storages
CLI : vps_list
2. ボリュームの ID を確認します。
CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。
REST API : GET /v1/objects/volumes
CLI : volume_list
3. コンピュータノードの ID を確認します。
CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。

REST API : GET /v1/objects/servers

CLI : server_list

4. ボリュームとコンピュータノードの接続を解除します。

割り当て解除するボリュームの ID とコンピュータノードの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が、コンピュータノードの ID の代わりにニックネームが指定できます。

REST API : POST /v1/objects/volume-server-connections/actions/release/invoke

CLI : volume_server_connection_release_connections

コマンド実行後に表示されるジョブの ID を確認します。

5. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

6. ボリュームとコンピュータノードの接続情報の一覧を取得して、接続が解除されたことを確認します。

REST API : GET /v1/objects/volume-server-connections

CLI : volume_server_connection_list

7. 構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

15.15.2 複数のボリュームとコンピュータノードの接続を解除する <<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

指定したすべてのボリュームと、指定したすべてのコンピュータノードのパス(ボリュームパス)を削除して接続を解除します。コンピュータノードからボリュームへの I/O がないことを必ず確認してから、実行してください。



注意

- コンピュータノードがクラスタリング構成かつ認識しているボリュームがオンライン状態の場合、対象のボリュームがオフライン状態であることを確認してから接続の解除を行ってください。
- パス情報を削除するコンピュータノードからアクセスできる状態のボリュームが、SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態である場合は、SCSI-2 Reserve または SCSI-3 Persistent Reserve 状態を解除してから、パス情報を削除してください。
- コンピュータノードのパス情報を変更した場合は、対象のコンピュータノード上でストレージの再スキャンを実施してください。削除済みのパス情報がコンピュータノード上に残り続けると誤動作につながります。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ボリュームとコンピュータノードの接続を解除する」

前提条件

- ・ 実行に必要なロール : Storage

操作手順

1. ボリュームの ID を確認します。
CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。
REST API : GET /v1/objects/volumes
CLI : volume_list
2. コンピュータノードの ID を確認します。
CLI を使いコンピュータノードをニックネームで指定する場合は、コンピュータノードのニックネームを確認します。
REST API : GET /v1/objects/servers
CLI : server_list
3. ボリュームとコンピュータノードの接続を解除します。
割り当て解除するボリュームの ID とコンピュータノードの ID を指定してコマンドを実行します。
CLI を使う場合はボリュームの ID の代わりに名前が、コンピュータノードの ID の代わりにニックネームが指定できます。
REST API : POST /v1/objects/volume-server-connections/actions/release/invoke
CLI : volume_server_connection_release_connections
コマンド実行後に表示されるジョブの ID を確認します。
4. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId>
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
5. ボリュームとコンピュータノードの接続情報の一覧を取得して、接続が解除されたことを確認します。
REST API : GET /v1/objects/volume-server-connections
CLI : volume_server_connection_list
6. <<Cloud for AWS>> 構成情報のバックアップを行います。
「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

コンピュータポートを管理する

- 16.1 コンピュータポートの情報の取得
- 16.2 コンピュータポート設定の編集
- 16.3 コンピュータポートのプロトコルを変更する<<Bare metal>>

16.1 コンピュートポートの情報の取得

コンピューポートの情報が取得できます。

16.1.1 取得できるコンピューポートの情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : コンピュートポートの ID(uuid)
- protocol : コンピュートポートの接続プロトコル
- type : コンピュートポートの種別
- nickname : コンピュートポートのニックネーム
- name :
 - iSCSI 接続の場合はコンピューポートの iSCSI 名
 - FC 接続の場合はコンピューポートの WWN
 - NVMe/TCP 接続の場合は常に null
- configuredPortSpeed : リンク速度の設定
- portSpeed : 実際のリンク速度
- portSpeedDuplex : 通信に使用している物理ポートの実際のリンク速度と Duplex。FC 接続構成の場合はリンク速度だけ表示
- protectionDomainId : 所属するプロテクションドメインの ID(uuid)
- storageNodeId : コンピュートポートが存在するストレージノードの ID(uuid)
- interfaceName : インターフェイス名
- statusSummary : コンピュートポートの状態のサマリー
- status : コンピュートポートの状態
- portNumber :
 - リモートパスグループをサポートの場合 : CLx-y 形式で表現されるポート番号
 - リモートパスグループが非サポートの場合 : N/A
- fcInformation :
 - iSCSI 接続の場合は常に null
 - FC 接続の場合は FC ポートの情報
 - NVMe/TCP 接続の場合は常に null
- iscsiInformation :
 - iSCSI 接続の場合は iSCSI ポートの情報
 - FC 接続または NVMe/TCP 接続の場合は常に null
- nvmeTcpInformation :
 - FC 接続または iSCSI 接続の場合は常に null
 - NVMe/TCP 接続の場合は NVMe/TCP ポートの情報

16.1.2 取得できるコンピュートポートの情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : コンピュートポートの ID(uuid)
- protocol : コンピュートポートの接続プロトコル
- type : コンピュートポートの種別
- nickname : コンピュートポートのニックネーム
- name : コンピュートポートの iSCSI 名
- configuredPortSpeed : リンク速度の設定
- portSpeed : 常に"DependsOnHypervisor"
- portSpeedDuplex : 常に"DependsOnHypervisor"
- protectionDomainId : 所属するプロテクションドメインの ID(uuid)
- storageNodeId : コンピュートポートが存在するストレージノードの ID(uuid)
- interfaceName : インターフェイス名
- statusSummary : コンピュートポートの状態のサマリー
- status : コンピュートポートの状態
- portNumber :
 - リモートパスグループをサポートの場合 : CLx-y 形式で表現されるポート番号
 - リモートパスグループが非サポートの場合 : N/A
- fcInformation : 常に null
- iscsiInformation : iSCSI ポートの情報
- nvmeTcpInformation : 常に null

16.1.3 コンピュートポートの情報の一覧を取得する

各コンピュートポートの情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. コンピュートポートの情報の一覧を取得します。

REST API : GET /v1/objects/ports

CLI : port_list

16.1.4 コンピュートポートの情報を個別に取得する

指定した ID のコンピュートポートの情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. コンピュートポートの ID を確認します。

CLI を使いコンピューポートを WWN または iSCSI 名で指定する場合は、コンピューポートの WWN または iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

2. コンピュートポートの情報を取得します。

コンピューポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピューポートの ID の代わりに WWN または iSCSI 名が指定できます。

REST API : GET /v1/objects/ports/<id >

CLI : port_show

16.2 コンピュートポート設定の編集

コンピューポート設定の編集方法について説明します。

16.2.1 コンピュートポートの設定を編集する<<Bare metal>>

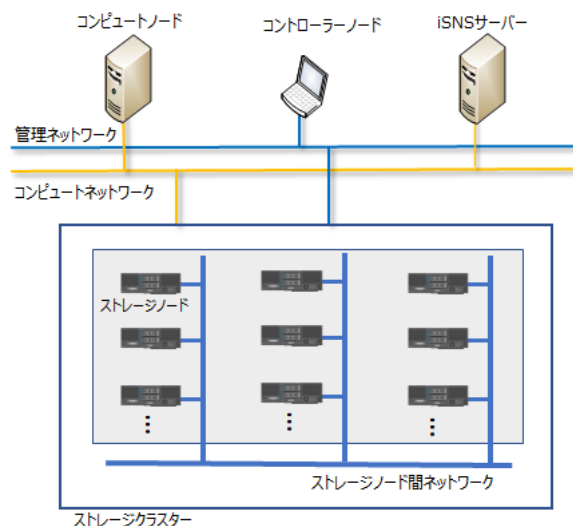
この項での記述内容は Bare metal モデルに適用されます。

コンピューポートの設定を編集します。

iSCSI 接続の場合は、iSNS サーバーを利用できます。FC 接続または NVMe/TCP 接続の場合は、iSNS サーバーは利用できません。

iSNS サーバーの利用について(iSCSI 接続の場合)

iSNS サーバーを利用する際は、iSNS サーバーについての設定を行います。



iSNS(Internet Storage Name Service)は、iSCSI を対象としたネーミングサービスです。iSNS を使用することによって、Initiator/Target の情報(IP アドレス/TCP ポート番号/iSCSI 名など)のディスカバリーが、設定せずに可能になります。



注意

- iSNS サーバー登録時に指定するサーバーアドレスは、コンピュータポートと接続可能な同一セグメント内のネットワークを指定してください。
- 1 台のストレージノードに 2 個のコンピュータポートが存在する場合、ストレージノード内の 2 個のコンピュータポートで iSNS クライアント機能の設定(iSNS クライアント機能の有効無効および接続先の iSNS サーバー情報)を一致させてください。この設定が一致していない場合、iSNS サーバーに情報が正しく反映されないことがあります。
- 一部の iSNS サーバーとの組み合わせにおいて、正しく情報を設定しているにもかかわらず、すべての iSCSI ターゲットが正しく認識されない場合があります。その場合は、手動にて iSCSI ターゲットを個別に追加してください。

VSP One SDS Block で、iSNS を有効に設定すると、iSNS サーバーと接続して以下がサポートされます。

①ネーミングサービス

iSNS は、ネットワーク上の Initiator/Target 情報を iSNS データベースへ登録し、Initiator/Target からの要求に従って iSNS データベースに問い合わせを行います。

②SCN(State Change Notification)

SCN は、iSNS データベースの変更を Initiator/Target へ通知するメッセージです。Initiator/Target が SCN 通知要求の登録を行うと、iSNS は登録した相手に対して SCN を送信するようになります。

③ESI(Entity Status Inquiry)

iSNS は、ESI(Entity Status Inquiry)という Initiator/Target の生存確認機能を備えています。具体的には、iSNS が、定期的に"ESI"を Initiator/Target へ送信し、ネットワーク障害などが原因で ESI に対する応答が一定回数受信できなかったとき、該当する Initiator/Target の登録を iSNS データベースから削除します。

コンピュータポートの種別が Target の場合は、すべてのコンピュータポートが iSNS サーバーに登録されます。

ネーミングサービスで iSNS サーバーに登録する属性を以下に示します。

属性名称	登録要否	属性値種別	属性値レンジ	説明
Delimiter	-	値	0	区切り文字。Delimiter Attribute で使用します。
Entity Identifier(EID)	◎	文字列	256	Entity を一意に指定する ID。MAC アドレスから生成します。物理ポートごとにユニークな値になり、設定変更はできません。 (デフォルト) iqn.1994-04.jp.co.hitachi:rsd.sph.t.XXXXXX.YYY XXXXX : シリアルナンバー(0x0~0xFFFFF) YYY : ポート番号(0x0~0x0FFF)* * 01.14.0x.xx 以前のバージョンのストレージソフトウェアからアップグレードを行っている場合、ポート番号がとる値域は、0x0~0xFFFF です。
Entity Protocol	○	値	4	2 を指定します。

属性名称	登録要否	属性値種別	属性値レンジ	説明
IP address	◎	IP アドレス	IPv4 アドレス : 16 IPv6 アドレス : 40	当該ポートの IP アドレスを設定します。
Portal TCP/UDP Port	◎	値	4	当該ポートのポート番号を設定します。
ESI Interval	○	値	4	ESI 発行間隔(単位 : 秒)。300 秒に設定します。
ESI Port	◎	値	4	ESI 受信ポート番号。ISP4022 へ iSNS サービスを有効としたとき取得した値を設定します。
SCN Port	◎	値	4	SCN 受信ポート番号。ISP4022 へ iSNS サービスを有効としたとき取得した値を設定します。
iSCSI Name	◎	文字列	224	当該 iSCSI Target の iSCSI Name を設定します。
iSCSI Node Type	○	値	4	Target(0x00000001)を設定します。
iSCSI Node Alias	◎	文字列	256	当該 iSCSI Target の iSCSI Alias を設定します。
iSCSI Node SCN Bitmap	◎	値	4	SCN で受ける情報。ターゲット情報のみ受け取るため Bit25 のみ ON とします。
◎ : 登録する KEY 属性 ○ : 登録する属性				

前提条件

- 実行に必要なロール : Storage

操作手順

1. コンピュートポートの ID を確認します。

CLI を使いコンピュートポートを WWN または iSCSI 名で指定する場合は、コンピュートポートの WWN または iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

2. コンピュートポートの設定を編集します。

コンピュートポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュートポートの ID の代わりに WWN または iSCSI 名が指定できません。

iSCSI 接続の場合は、ニックネーム、iSCSI 名、iSNS クライアント機能の有効/無効、iSNS サーバーについて設定します。

FC 接続の場合は、ニックネーム、ネットワークの接続形態を設定します。

ニックネームについて

- 他のコンピュートポートと同じニックネームは設定できません。
- ニックネームを設定する場合は、以下に従ってください。

- 。 文字数：1～32
- 。 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(! # \$ % & ' + - . = @ ^ _ { } ~ () [] :)

iSCSI 名について(iSCSI 接続の場合)

- 。 他のコンピュータポートと同じ iSCSI 名は設定できません。
- 。 ストレージノードの増設によって追加されるコンピュータポートのデフォルト名は設定できません。
例：iqn.1994-04.jp.co.hitachi:rsd.sph.t.<ストレージクラスターの ID>.XXX
ここで、<ストレージクラスターの ID>は「ストレージクラスターの情報を取得する」で得られる internalId を 16 進数に変換したものです。

REST API：PATCH /v1/objects/ports/<id >

CLI：port_set

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API：GET /v1/objects/jobs/<jobId >

CLI：job_show

state が"Succeeded"になっていたらジョブは完了です。

4. コンピュータポートの情報を取得して、コンピュータポートの設定を確認します。

コンピュータポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータポートの ID の代わりに WWN または iSCSI 名が指定できます。

REST API：GET /v1/objects/ports/<id >

CLI：port_show

5. 構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

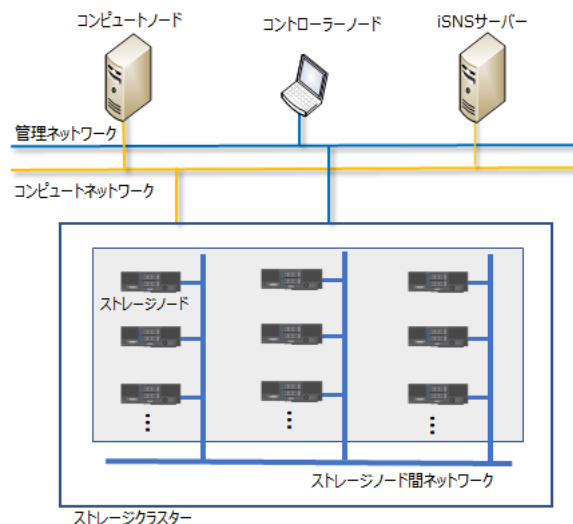
16.2.2 コンピュータポートの設定を編集する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

コンピュータポートの設定を編集します。

iSNS サーバーの利用について

iSNS サーバーを利用する際は、iSNS サーバーについての設定を行います。



iSNS(Internet Storage Name Service)は、iSCSI を対象としたネーミングサービスです。iSNS を使用することによって、Initiator/Target の情報(IP アドレス/TCP ポート番号/iSCSI 名など)のディスカバリーが、設定せずに可能になります。



注意

- iSNS サーバー登録時に指定するサーバーアドレスは、コンピュータポートと接続可能な同一セグメント内のネットワークを指定してください。
- 1 台のストレージノードに 2 個のコンピュータポートが存在する場合、ストレージノード内の 2 個のコンピュータポートで iSNS クライアント機能の設定(iSNS クライアント機能の有効無効および接続先の iSNS サーバー情報)を一致させてください。この設定が一致していない場合、iSNS サーバーに情報が正しく反映されないことがあります。
- 一部の iSNS サーバーとの組み合わせにおいて、正しく情報を設定しているにもかかわらず、すべての iSCSI ターゲットが正しく認識されない場合があります。その場合は、手動にて iSCSI ターゲットを個別に追加してください。

VSP One SDS Block で、iSNS を有効に設定すると、iSNS サーバーと接続して以下がサポートされます。

①ネーミングサービス

iSNS は、ネットワーク上の Initiator/Target 情報を iSNS データベースへ登録し、Initiator/Target からの要求に従って iSNS データベースに問い合わせを行います。

②SCN(State Change Notification)

SCN は、iSNS データベースの変更を Initiator/Target へ通知するメッセージです。Initiator/Target が SCN 通知要求の登録を行うと、iSNS は登録した相手に対して SCN を送信するようになります。

③ESI(Entity Status Inquiry)

iSNS は、ESI(Entity Status Inquiry)という Initiator/Target の生存確認機能を備えています。具体的には、iSNS が、定期的に"ESI"を Initiator/Target へ送信し、ネットワーク障害などが原因で ESI に対する応答が一定回数受信できなかったとき、該当する Initiator/Target の登録を iSNS データベースから削除します。

コンピュータポートの種別が Target の場合は、すべてのコンピュータポートが iSNS サーバーに登録されます。

ネーミングサービスで iSNS サーバーに登録する属性を以下に示します。

属性名称	登録要否	属性値種別	属性値レンジ	説明
Delimiter	-	値	0	区切り文字。Delimiter Attribute で使用します。
Entity Identifier(EID)	◎	文字列	256	Entity を一意に指定する ID。MAC アドレスから生成します。物理ポートごとにユニークな値になり、設定変更はできません。 (デフォルト) iqn.1994-04.jp.co.hitachi:rsd.sph.t.XXXXX.YYY XXXXX : シリアルナンバー(0x0~0xFFFFF) YYY : ポート番号(0x0~0xFF)
Entity Protocol	○	値	4	2 を指定します。
IP address	◎	IP アドレス	IPv4 アドレス : 16 IPv6 アドレス : 40	当該ポートの IP アドレスを設定します。
Portal TCP/UDP Port	◎	値	4	当該ポートのポート番号を設定します。
ESI Interval	○	値	4	ESI 発行間隔(単位 : 秒)。300 秒に設定します。
ESI Port	◎	値	4	ESI 受信ポート番号。ISP4022 へ iSNS サービスを有効としたとき取得した値を設定します。
SCN Port	◎	値	4	SCN 受信ポート番号。ISP4022 へ iSNS サービスを有効としたとき取得した値を設定します。
iSCSI Name	◎	文字列	224	当該 iSCSI Target の iSCSI Name を設定します。
iSCSI Node Type	○	値	4	Target(0x00000001)を設定します。
iSCSI Node Alias	◎	文字列	256	当該 iSCSI Target の iSCSI Alias を設定します。
iSCSI Node SCN Bitmap	◎	値	4	SCN で受ける情報。ターゲット情報のみ受け取るため Bit25 のみ ON とします。
◎ : 登録する KEY 属性 ○ : 登録する属性				

前提条件

- 実行に必要なロール : Storage

操作手順

1. コンピュートポートの ID を確認します。

CLI を使いコンピュートポートを iSCSI 名で指定する場合は、コンピュートポートの iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

2. コンピュートポートの設定を編集します。

コンピューポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピューポートの ID の代わりに iSCSI 名が指定できます。

ニックネーム、iSCSI 名、iSNS クライアント機能の有効/無効、iSNS サーバーについて設定します。

ニックネームについて

- 他のコンピューポートと同じニックネームは設定できません。
- ニックネームを設定する場合は、以下に従ってください。
 - 文字数：1～32
 - 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(! # \$ % & ' + - . = @ ^ _ { } ~ () [] :)

iSCSI 名について

- 他のコンピューポートと同じ iSCSI 名は設定できません。
- ストレージノードの増設によって追加されるコンピューポートのデフォルト名は設定できません。
例：iqn.1994-04.jp.co.hitachi:rsd.sph.t.<ストレージクラスターの ID>.XXX
ここで、<ストレージクラスターの ID>は「ストレージクラスターの情報を取得する」で得られる internalId を 16 進数に変換したものです。

REST API : PATCH /v1/objects/ports/<id >

CLI : port_set

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4. コンピュートポートの情報を取得して、コンピューポートの設定を確認します。

コンピューポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピューポートの ID の代わりに iSCSI 名が指定できます。

REST API : GET /v1/objects/ports/<id >

CLI : port_show

5. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

16.3 コンピュートポートのプロトコルを変更する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ストレージクラスター内のすべてのコンピューポートのプロトコルを一度に変更します。

変更先として指定できるプロトコルは以下のとおりです。

現在のコンピュータポートのプロトコル	変更可能なコンピュータポートのプロトコル
iSCSI	NVMe/TCP*
NVMe/TCP	iSCSI
FC	なし
* Universal Replicator 機能を使用中は、iSCSI から NVMe/TCP へのプロトコル切り替えはできません。プロトコルの変更を行う場合は「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」の「Universal Replicator の構成情報の削除について」を参照して、Universal Replicator の構成情報を削除してください。	

前提条件

- 実行に必要なロール：Storage
- ストレージクラスター内の以下のリソースがすべて削除済みであること
 - コンピュートノードのイニシエーター
 - コンピュートノードパス
 - ボリュームパス
 - コンピュートノード
 - CHAP ユーザー(現在の構成が iSCSI 接続の場合のみ)
- ストレージクラスター内の全コンピュータポートが以下の設定であること
 - iSNS クライアント機能が無効(現在の構成が iSCSI 接続の場合のみ)
 - CHAP 認証が無効(現在の構成が iSCSI 接続の場合のみ)

操作手順

1. コンピュートポートのプロトコルを変更します。
REST API : POST /v1/objects/ports/actions/switch-protocol/invoke
CLI : port_switch_protocol
コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
3. ストレージクラスターを再起動します。
「ストレージクラスターを再起動する<<Bare metal>>」を参照して実施してください。
4. コンピュートポートの一覧を取得して、すべてのコンピュータポートのプロトコルが変更されたことを確認します。
GET /v1/objects/ports
CLI : port_list
protocol が変更先のコンピュータポートのプロトコルであることを確認します。
5. 構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



メモ

コンピュータポートのプロトコル変更完了後、運用を開始する前に「ボリュームをコンピュータノードに接続する《Bare metal》」を参照してボリュームとコンピュータノードを接続してください。

ボリュームを管理する

- 17.1 ボリューム管理の概要
- 17.2 ボリュームの容量削減機能の概要
- 17.3 ボリュームの容量削減機能を有効にする
- 17.4 ボリュームの作成
- 17.5 ボリュームを削除する
- 17.6 ボリュームを拡張する
- 17.7 ボリューム情報の一覧の取得
- 17.8 ボリューム情報の個別取得
- 17.9 ボリュームの設定を編集する
- 17.10 ボリュームが稼働するアベイラビリティゾーンを確認する<<Cloud>>

17.1 ボリューム管理の概要

ボリュームは、コンピュータノードにマウントされてユーザーデータの読み書きが行われる論理デバイスです。ボリュームはストレージコントローラーによって管理され、ユーザーデータはボリュームに関連付けられたストレージプールに書き込まれます。ユーザーデータが書き込まれる領域はユーザーデータが書き込まれた契機にストレージプールから割り当てられます。ユーザーデータはストレージノードやドライブに障害が発生しても保持できるように、複数のストレージノードに書き込まれます。

ボリュームの仕様を以下に示します。

項目	仕様
ボリューム数とスナップショットボリューム数の合計(システム当たり)	1 冗長構成の場合¹ : 0~1,024 × n (ストレージノード数²) 2 冗長構成の場合¹ : 最小値は 0、最大値は次のうち小さいほうが適用されます。 1,024 × n (ストレージノード数) 16,384
ボリューム数とスナップショットボリューム数の合計(1 フォールトドメイン当たり)	1 冗長構成の場合¹: 0~1,024 × n (当該フォールトドメインに所属するストレージノード数²) 2 冗長構成の場合¹ : 最小値は 0、最大値は次のうち小さいほうが適用されます。 1,024 × n (当該フォールトドメインに所属するストレージノード数) 16,384
ボリューム数とスナップショットボリューム数の合計(ストレージノード 1 台当たり)	0~1,024
ボリューム容量(ボリューム 1 個当たり)	«Bare metal» HPEC 4D+1P の場合 : 47[MiB]~96.1[TiB] - HPEC 4D+2P の場合 : 47[MiB]~96.0[TiB] - Mirroring Duplication の場合 : 47[MiB]~96.8[TiB]
ボリューム容量(ストレージノード 1 台当たり) ³	«Bare metal» HPEC 4D+1P の場合 : 0[MiB]~96.1[TiB] - HPEC 4D+2P の場合 : 0[MiB]~96.0[TiB] - Mirroring Duplication の場合 : 0[MiB]~96.8[TiB]
スナップショットを使用した場合のボリューム合計容量の最大値(ストレージコントローラー当たり)	4[PiB](目安) 4[PiB]以上(目安)のスナップショットの取得準備を実施した場合は、KARS06002-E が発生し操作が失敗することがあります。
ボリューム操作とスナップショット操作を同時実行できる最大数	20(目安) 20 以上(目安)の操作を同時に実行した場合は、タイムアウトが発生して操作が失敗することがあります。 ボリューム操作とは、ボリュームの作成、削除、拡張、設定編集を指します。スナップショット操作とは、スナップショットの取得準備、取得、削除、復元を指します。

項目	仕様
	単一操作で複数ボリュームを扱うものについては 1 操作としてカウントします。例えば、1 回のボリューム作成操作で 20 個以上のボリュームを指定した場合は 1 操作としてカウントします。 ジョブの完了は操作の完了を意味しています。ジョブの state が "Succeeded" になっていたら、操作は完了しています。
ボリュームの名前	文字数：1～32 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(.,: @ _)
ボリュームのニックネーム	文字数：1～32 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(.,: @ _)
- 冗長構成については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「VSP One SDS Block がサポートする耐障害性に関する設定と各機能の説明」を参照してください。 ≪Cloud≫Multi-AZ (Multi-Zone)構成の場合、タイプブレーカーノードは容量を持たない(ドライブが存在しない)ため、ストレージノード数の対象には含めません。 - スナップショットボリュームは含まない値です。	

17.1.1 ボリュームとストレージプール

プロビジョニング

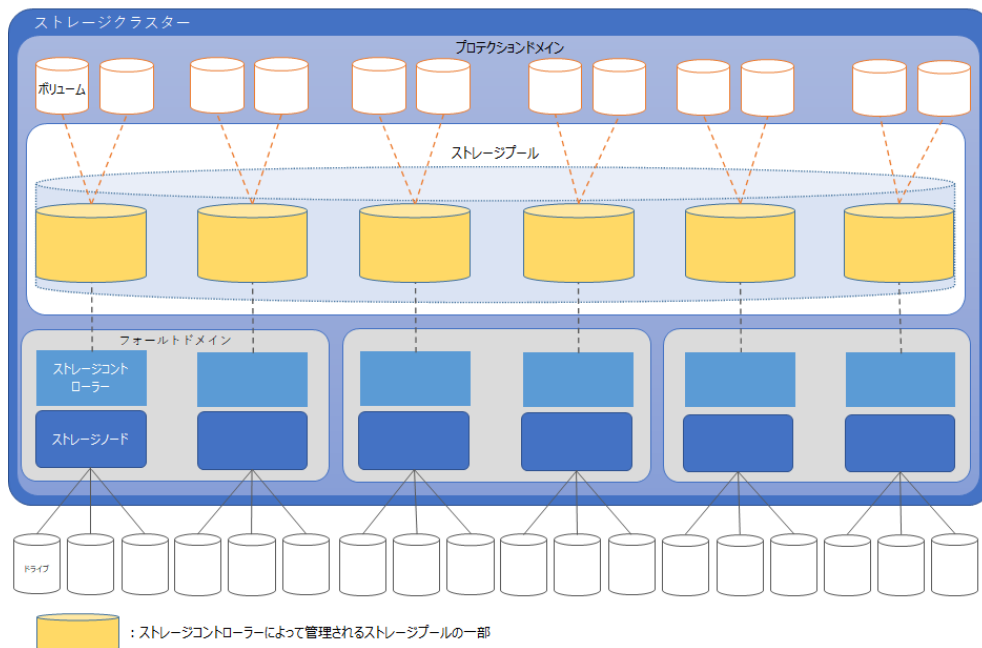
ボリュームに与えられるストレージプールの容量は、ストレージコントローラーによって割り当てられます。デフォルトでは、ストレージプールの容量が効率的に使用できるよう、ボリューム作成時に、空き容量に応じて、最適なストレージコントローラーが容量を割り当てます。また、ボリューム作成時に、容量を割り当てるストレージコントローラーを指定することもできます。

情報量の増加を見越してストレージの容量をあらかじめ設備することは、設備設計やコスト面で難しいといえます。VSP One SDS Block では、実際の物理容量を超えた容量のボリュームが作成できます。これによって、ストレージシステムの構築時は、その時点で必要な物理容量を用意しておき、実際に容量が不足したときに、ドライブやストレージノードを増設してストレージプールの容量を拡張すればよくなります。



注意

- ストレージコントローラーが管理する空き容量が不足すると、ストレージプール全体の論理容量に空きがある場合でもボリュームへの書き込みができなくなります。容量不足が発生しないようにストレージプールの容量状態を監視してください。詳しくは「ストレージプールを管理する」を参照してください。
- オンライントランザクション処理に使用されるボリュームを作成する際には、ストレージプール内のすべてのボリュームの総容量が、ストレージプールの総論理容量を超えないようにしてください。容量バランス処理によって、一時的に I/O 性能に影響が出る場合があります。



オーバープロビジョニング

オーバープロビジョニングとは、ストレージコントローラーが管理するボリュームの予約論理容量 (reservedCapacity[MiB]) を合計した値が、当該ストレージコントローラーで管理できる最大の論理容量 (allocatableCapacity[MiB]) 以上の値になっている状態をいいます。

$\text{allocatableCapacity[MiB]} \leq \text{ストレージコントローラーに属するボリュームの reservedCapacity[MiB] の合計}$

- allocatableCapacity は次のコマンドで確認できます。
REST API : GET /v1/objects/storage-controllers
CLI : storage_controller_list
- reservedCapacity 次のコマンドで確認できます。
REST API : GET /v1/objects/volumes
CLI : volume_list

オーバープロビジョニングの状態にあっても、allocatableCapacity[MiB]以上の容量でのボリューム作成やボリューム拡張はできますが、そのボリューム容量のうち、allocatableCapacity[MiB]以上の容量はライト I/O することができません。

このため、ボリューム作成またはボリューム拡張を行う際にはストレージコントローラーの容量を意識して容量設計を行う必要があります。

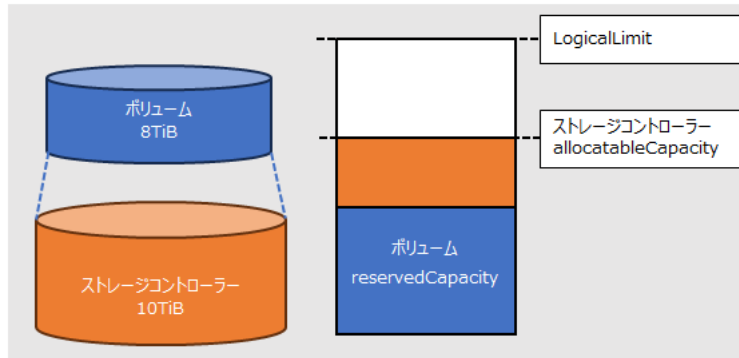
単一ボリュームでオーバープロビジョニングの状態にあったときに容量が枯渇すると、容量バランスで容量の枯渇を解消することはできません。単一ボリュームで容量が枯渇した場合はドライブ増設が必要になります。「ドライブを増設する」を参照してストレージプールの容量を追加してください。



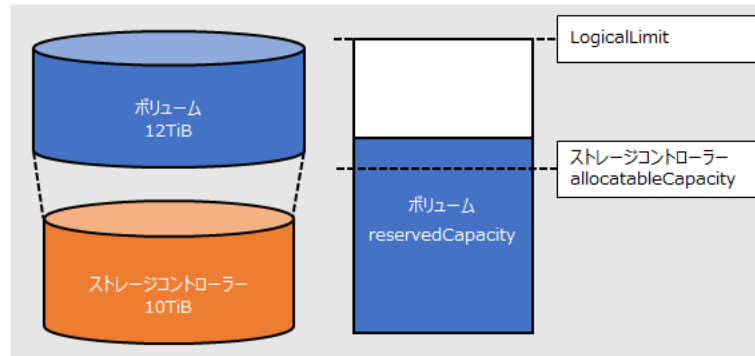
ヒント

ボリューム情報を取得する際、特定のストレージコントローラーに属するボリュームのみの情報を取得するには、クエリーパラメーター storageControllerId (CLI : --storage_controller_id) にストレージコントローラーの ID を指定してコマンドを実行します。

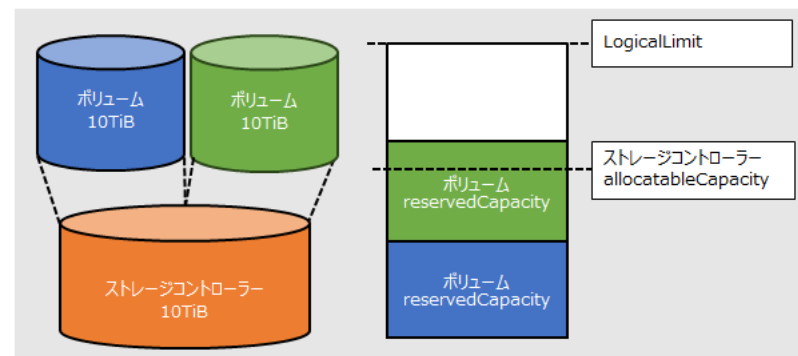
■オーバープロビジョニングの状態ではないケース



■単一ボリュームでオーバープロビジョニングの状態にあるケース



■複数ボリュームでオーバープロビジョニングの状態にあるケース



ボリュームが消費するストレージプールの最大容量

ボリュームは、論理容量のほかに制御情報を必要とします。制御情報は、ボリュームの使用容量には含まれずストレージプール(ボリュームを管理するストレージコントローラー)の使用容量に含まれます。

ボリュームの論理容量がストレージプール(ボリュームを管理するストレージコントローラー)の論理容量の 100%になるようにボリュームを作成すると、ボリュームの使用率が 100%になる前に容量枯渇になります。そのため、ストレージプール(ボリュームを管理するストレージコントローラー)の容量設計を行う際は、論理容量だけではなく、管理領域を含めた容量設計を行ってください。



メモ

- 容量削減機能を使用するボリュームは、メタデータとガベージデータを合わせたシステムデータ量も消費するため、容量設計を行う際は、システムデータ量も含める必要があります。詳細は「ボリュームの容量削減機能の概要」を参照してください。

- ・ スナップショットが使用するストレージプール(ボリュームを管理するストレージコントローラー)の最大容量については「スナップショットで消費するプールの最大容量」を参照してください。
- ・ <<Cloud>>Multi-AZ (Multi-Zone)構成の場合、ボリュームは固定されたフォールトドメイン内で管理されます。そのため、容量設計を行う際は、ストレージプールではなく、所属するフォールトドメインの容量を条件として容量設計を行ってください。

各ボリュームが消費するストレージプールの最大容量は、各ボリューム情報を個別に取得して予約容量(reservedCapacity[MiB])を参照するか、以下の計算式で算出できます。

各ボリュームが消費するストレージプールの最大容量[MiB] = $n \times 42$ [MiB]

- ・ n : (ボリュームの容量[MiB] + ($m \times 168$ [MiB])) $\div 42$ [MiB] (小数点以下切り上げ)
- ・ m : ボリュームの容量[MiB] $\div 3145548$ [MiB] (小数点以下切り上げ)

スナップショットと容量削減機能のシステムデータ量を除外したボリュームが使用するストレージプール(ボリュームを管理するストレージコントローラー)の容量の概算は以下の計算式で算出できます。

ストレージプール(ボリュームを管理するストレージコントローラー)の容量の概算[MiB] = $a + (b \times 210) + (c \times 168)$

- ・ a : ストレージプールまたはストレージコントローラーの totalVolumeCapacity[MiB]
- ・ b : ストレージプールまたはストレージコントローラーが管理しているボリューム数
- ・ c : $a \div 3145548$ (小数点以下切り上げ)

17.1.2 Quality of Service(QoS)機能について

ボリュームには QoS の設定ができます。QoS 機能では、ボリューム単位に異なる性能レベル(I/O 数や転送量)を提供します。ストレージシステムを複数のサービスで共有したり、パブリッククラウドにおいて複数の企業(サービス)を同居させるマルチテナンシーの構成を組む場合、これらの構成ではサービス(アプリケーション)ごとに、ストレージに対して要求する性能レベルが異なります。通常のストレージ設定では過大な I/O を要求するアプリケーションが存在すると、要求された順番に I/O 処理を実行しようと動作するため、他のアプリケーションへの性能レベルが下がる傾向があります。その際、QoS 機能によってボリューム単位に I/O 処理をコントロールすることによって、アプリケーション間の性能干渉を抑え、一定の性能と品質を提供できます。

QoS 機能では以下の詳細機能を提供します。

- ・ 特定ボリュームへのホスト I/O に対する性能上限制御機能(QoS 機能による上限値制御)
- ・ QoS 対象となるボリュームのアラートしきい値監視機能(QoS アラート)

QoS による上限値制御

QoS の上限値制御は、I/O 要求をしたサービスに対して、ストレージシステムが I/O 処理する際の性能上限を定める機能です。

上限値はボリューム単位に設定します。Read と Write は区別せず、Read と Write の上限値を個別に設定することはできません。上限値を設定したボリュームに対して I/O 要求があると、ストレージシステムは、そのボリュームの直近の 1 秒平均の I/O 数と転送量を確認します。I/O が上限値に到達すると、サービスからの I/O 要求は受け付けますが、処理を抑止します。I/O が上限値より下になると I/O 処理が再開されます。上限値制御には、I/O 数による制御(upperLimitForIops[IOPS])、

転送量による制御(upperLimitForTransferRate[MiB/sec])、I/O 数と転送量の両方による制御があります。I/O 数と転送量の両方による上限値制御では、どちらかの上限値に到達した場合に I/O が抑止されます。

QoS の上限値制御は 1 秒平均の I/O 数や転送量を基に制御されますが、参照できるストレージシステムの性能情報は、高解像度の情報でも 5 秒周期での収集です。このため、QoS の上限値制御を観測できないことがあります。具体的には、QoS の I/O 処理が上限値に到達すると QoS アラートが通知されますが、該当ボリュームの高解像度の性能情報で、I/O が上限値に到達していることを観測できないことがあります。

ストレージシステムの性能情報は、容量バランスやストレージノードを減設する際に動作するボリュームマイグレーションによって発生するシステム内部の I/O を含みます。一方で、これらシステム内部で発生する I/O は QoS の対象からは除外されるため、ストレージシステムの性能情報を参照した際に、ボリュームごとに I/O 数で 80[IOPS]程度、転送量で 20[MiB/sec]程度、QoS で設定した上限を超えることがあります。

QoS 上限値制御の設定範囲を次に示します。

項目	I/O 数[IOPS]	転送量[MiB/sec]
上限値設定範囲	-1(上限なし)、100～2,147,483,647	-1(上限なし)、1～2,097,151

QoS アラート

QoS アラートは、QoS を設定したボリュームの状態が、設定値の範囲外にあることを、イベントログ KARS06600-W によってユーザーに通知する機能です。QoS アラート機能を有効にするには、ボリュームごとに QoS アラートしきい値(upperAlertAllowableTime[sec])を設定します。QoS アラートを設定すると、ストレージシステムの内部処理で定期的にアラート条件がチェックされます。

上限値制御の場合、ボリュームへの I/O が、設定した上限値に到達した状態が継続し、その継続時間が QoS アラートしきい値[sec]に達したとき、QoS アラート条件に合致したと判定し、イベントログ KARS06600-W を出力します。

イベントログはストレージシステム単位に出力され、イベントログの頻出を防ぐため、出力後 24 時間は出力が抑止されます。また、ボリュームごとに QoS アラート条件に合致した最新時刻を参照できます。

QoS アラートは-1(アラート無効)、1～600 秒の範囲で設定できます。



メモ

- ・ ストレージクラスターの停止/起動によって、次に示す情報が初期化されます。
 - QoS アラートのイベントログを、24 時間に 1 回出力するための管理情報
 - QoS アラートが発生した最新の時刻
- ・ アラートしきい値時間を変更した場合、変更したタイミングと、しきい値時間を判定したタイミングによって、変更後のしきい値時間に到達しない場合でもアラートが出力されることがあります。
- ・ イベントログ KARS06600-W が出力されたあと、ボリュームの一覧情報を取得する前に以下の保守操作を実施した場合、または容量バランスが動作した場合は、ボリューム情報の一覧において、QoS アラートが発生した最新の時刻の情報が表示されない場合があります。イベントログ KARS06600-W が出力されてから 24 時間以上経過したあとで、イベントログ KARS06600-W が再度出力されていなければ、特に対処は不要です。
 - ストレージノード保守閉塞・回復
 - ストレージソフトウェアアップデート
 - ストレージノード減設

- データマイグレーション
- ストレージクラスターの停止・再起動
- ストレージクラスターの電源障害・再起動
- ストレージノード障害・回復
- ストレージノード保守閉塞・回復、ストレージノード障害・回復、ストレージソフトウェアアップデートを実施したあとは、イベントログ KARS06600-W が出力されてから 24 時間以内であっても、QoS アラート条件に合致したと判定され、イベントログ KARS06600-W が出力されることがあります。

17.2 ボリュームの容量削減機能の概要

ボリューム作成時、以下のいずれかの場合、容量削減機能が有効なボリュームが作られます。容量削減機能が有効なボリュームは、データ圧縮と固定パターンの排除が行われます。

- savingSetting(CLI : --saving_setting)パラメーターで"Compression"を指定してボリュームを作成した場合
- ボリューム作成先の VPS が容量削減機能が有効であった場合(savingSettingOfVolume が "Compression")

データ圧縮では、OSS の圧縮アルゴリズム LZ4 が使われます。

固定パターンの排除では、0x00 データまたは 0xFF データが 8KiB 連続した場合、それらのデータは書き込まずに、制御情報のみを書き込むことで、ストレージプールの使用量を削減します。

容量削減機能が有効なボリュームは、volumeType が通常ボリュームと同じ"Normal"、savingSetting が"Compression"になります。

容量削減機能の処理方式は、新規または更新時の書き込みのデータ圧縮を、書き込みと同期して実行するインライン方式です。

容量削減機能が有効なボリュームは、以下を理解した上で使用してください。

- データ圧縮の効果は書き込まれるデータの圧縮のしやすさによって異なります。
- ユーザーのアプリケーションによって、データが圧縮されている場合は、容量削減機能の削減効果がない場合があります。そのため、実際のデータを用いて、あらかじめ削減効果の検証を実施してください。
- データの圧縮/伸長を実行するため、通常ボリュームと比較し、I/O 性能が低下するおそれがあります。



注意

- <<Cloud for AWS>>容量削減機能を使用する場合は、インスタンスタイプに r7i.8xlarge または r6i.8xlarge を設定して新規インストールする必要があります。インスタンスタイプの設定方法については、Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。
- <<Cloud for Google Cloud>>容量削減機能を使用する場合は、インスタンスタイプに 4-highmem-32 を設定して新規インストールする必要があります。インスタンスタイプの設定方法については、Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。
- <<Cloud for Microsoft Azure>>容量削減機能を使用する場合は、インスタンスタイプに Standard_E32s_v5 を設定して新規インストールする必要があります。インスタンスタイプの設定方法については、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

ボリュームの容量削減機能の有効化要件

ボリュームの容量削減機能を利用することを前提にセットアップを行っている場合は、要件を満たしています。

セットアップ以降に、ボリュームの容量削減機能を利用する場合は「ボリュームの容量削減機能の有効にする」を参照して、要件を満たすようにしてください。

- ・ キャッシュ保護付きライトバックモード機能が有効になっていること
- ・ 各ストレージノード搭載の物理メモリー容量は、256GiB 以上であること
- ・ <<Cloud for AWS>>インスタンスタイプ「r7i.8xlarge」または「r6i.8xlarge」が設定されていること
- ・ <<Cloud for Google Cloud>>インスタンスタイプ「n4-highmem-32」が設定されていること
- ・ <<Cloud for Microsoft Azure>>インスタンスタイプ「Standard_E32s_v5」が設定されていること
- ・ ストレージプールの容量が十分であること



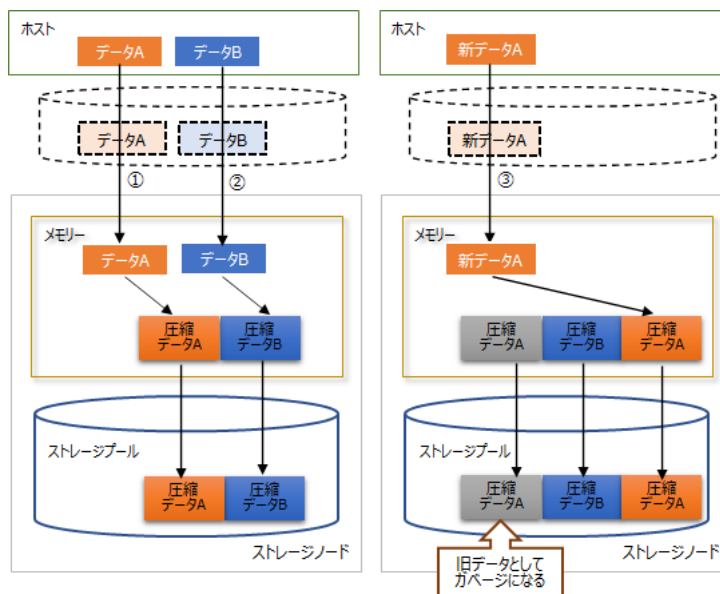
ヒント

ストレージノードに割り当てられているメモリー容量は「ストレージノード情報の一覧を取得する」または「ストレージノード情報を個別に取得する」で参照できます。

容量削減機能が有効なボリュームへのデータ書き込み処理の概要

データの書き込みがあった際、データはメモリー上で圧縮されたあと、ストレージプール(ドライブ)にデータが書き込まれます。

容量削減機能が有効なボリュームの場合、容量削減機能固有のメタデータが作られます。メタデータの量は、圧縮されたデータ量の 3%程度です。



データはメモリー上で圧縮されたあと、ストレージプールに書き込まれる。

- ①データAの書き込み
- ②データBの書き込み
- ③データAの更新

データの更新では、旧データを直接更新せずに、新データを追記したあと、旧データを無効にする。
無効になった旧データはガベージになる。

容量削減機能を使用する場合、使用しない場合とは異なり、データ更新時にストレージプールにデータが追記されるようになります。旧データは無効化され、ガベージとして扱われます。ガベージが一定量たまると、書き込みとは非同期にガベージが占める領域を解放するガベージコレクション処理が動作します。

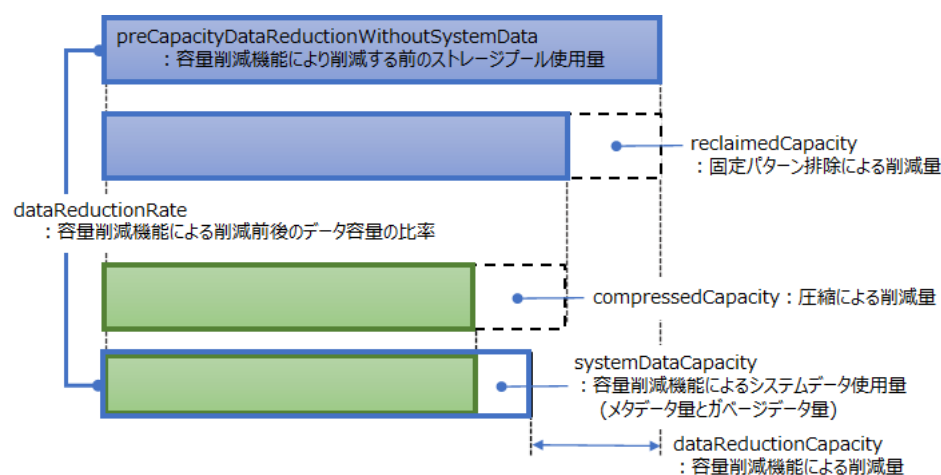
容量削減機能によるデータ削減効果の情報

容量削減機能によるデータ容量の削減効果は、以下の操作で取得できます。

- ボリューム情報の一覧取得
- ボリューム情報の個別取得
- ストレージプール情報の一覧取得
- ストレージプール情報の個別取得
- ストレージクラスターの情報取得

ボリュームの容量削減に関する情報は、ボリューム情報の `dataReductionEffects` で得られます。

ボリュームの容量削減に関する各種情報の関係は、次の図のとおりです。



$$\begin{aligned} \text{dataReductionCapacity} &= \text{reclaimedCapacity} + \text{compressedCapacity} - \text{systemDataCapacity} \\ \text{dataReductionRate} &= \frac{\text{preCapacityDataReductionWithoutSystemData}}{\text{preCapacityDataReductionWithoutSystemData} - \text{dataReductionCapacity}} \times 100 \end{aligned}$$

容量削減情報についての補足

容量削減機能が有効なボリュームの容量表示については以下の点に留意してください。

- ボリューム作成直後であってもメタデータのための領域として、ボリューム容量に応じて、42MiB から最大数百 MiB 使用されます。
- `preCapacityDataReductionWithoutSystemData[MiB]`は、ストレージプールの実使用量がページ単位(42MiB)のため 42 の倍数で表示されます。
- 容量削減情報(`compressedCapacity`、`reclaimedCapacity`、`systemDataCapacity`)はブロック単位(512Byte)で管理されており、ブロック単位の情報を MiB で表示するため、容量削減情報は 1MiB 以下が切り捨てられます。このため実際の値と表示される値に誤差が生じます。

(例) `dataReductionCapacity[MiB] = compressedCapacity[MiB] + reclaimedCapacity[MiB] - systemDataCapacity[MiB]`

(例)実際の値が、compressedCapacity が 2489.5[MiB]、reclaimedCapacity が 6551.5[MiB]、systemDataCapacity が 179.0[MiB]だった場合

- 実際の値から算出される結果：
 $2489.5[\text{MiB}] + 6551.5[\text{MiB}] - 179.0[\text{MiB}] = 8862.0[\text{MiB}]$
 - 1MiB 以下が切り捨てられた値から算出される結果：
 $2489[\text{MiB}] + 6551[\text{MiB}] - 179[\text{MiB}] = 8861.0[\text{MiB}]$
- このように、両者には、1MiB 分の誤差が生じます。



メモ

- 容量削減機能が有効なボリュームの使用開始直後は、メタデータ量がデータの書き込み量よりも大きくなる場合があります。また、データの書き込み中は、ガベージ量がデータの書き込み量よりも大きくなる場合があります。
システムデータ使用量(メタデータ量、ガベージ量)がデータの書き込み量よりも大きくなった場合は、以下のように表示されることがあります。
 - systemDataCapacity[MiB]が preCapacityDataReductionWithoutSystemData[MiB]よりも大きくなる
 - dataReductionCapacity[MiB]が 0 になる
 - postCapacityDataReduction[MiB]が preCapacityDataReductionWithoutSystemData[MiB]よりも大きくなる
 - dataReductionRate[%]が 100 より小さい値になる
- 容量削減機能が有効なボリュームに対してホストから Write Same コマンドまたは Unmap コマンドを実行した場合、当該領域に対して固定パターン排除が行われます。また、そのボリュームが属するストレージプールの使用容量は減少しますが、そのボリュームの使用量は減少しません。

データ量削減状態について

容量削減機能を有効にしたボリュームの状態は以下に示す意味を持ちます。

状態の意味	状態の組み合わせ			必要な対処
	statusSummary	status	dataReductionStatus	
ボリューム作成後の定常状態	Normal	Normal	Enabled	不要
ボリュームの設定の更新中またはボリュームの容量拡張中の状態	Normal	Updating または Expanding	Enabled	不要
ボリュームの削除中の状態	Normal	Deleting	Deleting	不要
ボリュームの作成に失敗した状態	Error	CreationFailed	Enabled	作成に失敗したボリュームを削除したあと、再度ボリュームを作成してください。
ボリューム操作に失敗した状態かつ Failed の状態において回復操作を実行したあとの状態	Error	DeletionFailed、UpdateFailed、または ExpansionFailed	Enabled	再度ボリューム操作を実行してください。

状態の意味	状態の組み合わせ			必要な対処
	statusSummary	status	dataReductionStatus	
メタデータの不整合による要因以外の場合で削除が失敗した状態	Error	DeletionFailed	Deleting	「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」を参照して対処してください。
メタデータの整合性が保証できない状態	Error	MetadataConsistencyError	Failed	
ボリュームの操作中に冗長度を超えた障害などが発生し、その後ストレージクラスターが起動したときの状態	Error	DeletionFailed、 UpdateFailed、 または ExpansionFailed	Failed	
スナップショットのリストアを操作中に冗長度を超えた障害などが発生し、その後起動したときの状態	Error	IOSuppressed	Failed	

容量削減機能の有効化による影響

容量削減機能使用時、ストレージコントローラーの容量が枯渇しかけた場合、書き込み速度を制限する動作をします。条件と書き込み処理への影響を以下に示します。

書き込み性能への影響が発生するケース	書き込み性能への影響	備考
以下のいずれかの状態 - 書き込み要求があったボリュームを管理するストレージコントローラーが管理するストレージプールの使用率が 99% 以上、または空き容量が 40GiB 以下 - 書き込み要求があったボリュームを管理するストレージコントローラーの内部リソースの使用率が一時的に増加した場合	ストレージプールに書き込み可能であることを保証した上でホストに応答を返す処理を行うため、I/O 性能が低下します。 また、ガベージコレクション処理によって回収されるガベージ量に応じた書き込みが受け付けられます。これによって書き込み性能が低下することがあります。	
以下のいずれかの状態 - 書き込み要求があったボリュームを管理するストレージコントローラーが管理するストレージプールの空き容量が 40GiB 以下になったときから、空き容量が 80GiB 以上になるまで動作します。 - ストレージコントローラーが管理するストレージプールの	ガベージコレクション処理によって回収されるガベージ量に応じた書き込みが受け付けられます。これによって書き込み性能が低下することがあります。	左記の状況になった場合は、イベントログ KARS06213-W が通知されます。 書き込み制限が解除されると、イベントログ KARS06212-I が通知されます。

書き込み性能への影響が発生するケース	書き込み性能への影響	備考
空き容量が 80GiB 未満、かつ当該ストレージプールに 1 つ目の容量削減機能が有効なボリュームを作成したときから、空き容量が 80GiB 以上になるまで動作します。		
書き込み要求があったボリュームを管理するストレージコントローラーが管理するストレージプールの使用率が 80%以上だった場合	ガベージコレクション処理に優先的に処理リソースが割り当てられるため、書き込み性能が低下することがあります。	
書き込み要求があったボリュームを管理するストレージコントローラーが管理する内部リソースの使用率が一時的に増加した場合	ボリューム単位で書き込み性能が低下することがあります。また、ガベージコレクション処理によって回収されるガベージ量に応じた書き込みが受け付けられます。これによって書き込み性能が低下することがあります。	左記の状態になった場合は、イベントログ KARS06217-W が通知されます。書き込み制限が解除されると、イベントログ KARS06216-I が通知されます。
書き込み要求があったボリュームを管理するストレージコントローラーの内部リソースの使用率が一時的に増加した場合	ストレージコントローラー単位で影響を受けます。ストレージプールの空き容量の不足が解消されるまで I/O 性能が低下します。	左記の状態になった場合は、イベントログ KARS06218-W が通知されます。

ガベージコレクション処理の発生時の対応、または発生頻度を下げるときの方法として、以下があります。

- メタデータとガベージデータを合わせた量であるシステムデータ使用量 (systemDataCapacity[MiB]) が、ストレージコントローラー情報のボリュームの使用量 (usedVolumeCapacity[MiB]) の 10% 以上の場合は、10% 未満になるようにホストからの I/O を減らす。または、ドライブ増設またはストレージノード増設を行ってストレージプールを拡張する。
- メタデータとガベージデータを合わせた量であるシステムデータ使用量 (systemDataCapacity[MiB]) が、ストレージコントローラー情報のボリュームの使用量 (usedVolumeCapacity[MiB]) の 10% 未満の場合は、ドライブ増設またはストレージノード増設を行ってストレージプールを拡張する。

スナップショットボリュームに対する容量削減機能の適用

容量削減機能が有効なボリュームを P-VOL として S-VOL は作成はできます。ただし、S-VOL は容量削減機能が有効になりません。このことを前提にストレージプールの容量を管理してください。

17.3 ボリュームの容量削減機能を有効にする

セットアップ以降に、ボリュームの容量削減機能を利用することにした場合は、以下の手順を実施してボリュームの容量削減機能を有効にしてください。

以下の場合、ボリュームの容量削減機能を有効にはできません。

- universalReplicatorAttribute が "P-VOL" または "S-VOL" のボリュームは、この節で説明する手順では容量削減機能を有効にはできません。それらのボリュームを容量削減機能を有効なボリ

ュームにするには、Universal Replicator でペア削除をしたあと、この節で説明する手順で容量削減機能が有効なボリュームを作成したのち、Universal Replicator でそのボリュームを使ってペアを作成します。

- volumeType が"Journal"または"FormerJournal"のボリュームは、容量削減機能を有効にはできません。

前提条件

- 実行に必要なロール：Service

操作手順

1. キャッシュ保護付きライトバックモードの状態が有効かどうかを確認します。
「キャッシュ保護付きライトバックモードの有効化」を参照し、状態の確認および有効化を実施してください。
2. 容量削減機能が有効なボリュームを作成します。
「ボリュームの作成」を参照して実施してください。
3. 容量削減機能が無効なボリュームから引き継ぐデータがあるかどうかを確認します。
引き継ぐデータがない場合は、以上で手順は終了です。
引き継ぐデータがある場合は、次の手順に進みます。
4. 作成した容量削減機能が有効なボリュームにホスト経由でデータをコピーします。
5. 必要に応じて、データコピー元のボリュームを削除します。

17.4 ボリュームの作成

ボリュームの作成方法を説明します。

17.4.1 ボリュームを作成する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ボリュームを作成します。

ボリューム作成コマンドで指定する"capacity"にはボリュームの容量を MiB 単位で指定します。作成したボリュームには制御情報が必要になります。そのため、"capacity"に指定できる値の上限としては logicalLimit から制御情報を引いた値になります。

"capacity"に指定できる値の上限値 = $\text{logicalLimit}[\text{MiB}] - ((168[\text{MiB}] \times n) + 42[\text{MiB}])$

- $n = \text{作成するボリュームの論理容量}[\text{MiB}] / 3,145,548[\text{MiB}]$ （小数点以下切り上げ）
- logicalLimit は次のコマンドで確認できます。
REST API : GET /v1/objects/storage-controllers
CLI : storage_controller_list

ボリュームは論理容量のほかに制御情報を必要とします。ボリュームが消費するストレージプールの最大容量は「ボリュームが消費するストレージプールの最大容量」を参照して算出してください。



注意

オーバプロビジョニングになる容量のボリュームを作成した場合、当該ボリュームを管理するストレージコントローラーの allocatableCapacity[MiB]以上の容量はライト I/O することができなくなります。また、単一ボリュームでオーバプロビジョニングの状態にあったときに容量が枯渇すると、ドライブ増設が必要になります。「ドライブを増設する」を参照してストレージプールの容量を追加してください。

Universal Replicator を使用している場合は、以下に留意してください。

- QoS 設定は、直接ホスト I/O を受けるボリューム(主に P-VOL)にのみ適用されます。それ以外のボリュームでは、QoS 設定は無視されます。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ボリュームを作成する」

前提条件

- 実行に必要なロール：Storage
- VPS にボリュームを作成する場合：当該 VPS のスコープ

操作手順

1. マルチテナンシー機能を利用していない場合、またはマルチテナンシー機能を利用してシステムスコープ内のボリュームにボリュームを作成する場合、ボリューム作成先のストレージプールの ID を確認します。

CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

2. VPS 内にボリュームを作成する場合、ストレージプールの ID の代わりに作成先の VPS の ID と VPS に設定された条件(ボリューム数上限、ボリューム容量上限、単一ボリューム容量上限、QoS、ボリューム容量削減機能の各設定)を確認します。

CLI を使い VPS を名前で指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list



メモ

システム管理者は以下の設定について、VPS の設定に制限されず、ボリューム個別に値を設定できます。パラメーターを指定しなかった場合、VPS に設定されたパラメーターでボリュームが作成されます。

- QoS
 - ボリューム容量削減機能
-

3. ボリュームを作成します。

ボリューム作成のパラメーターを指定してコマンドを実行します。

REST API : POST /v1/objects/volumes

CLI : volume_create

コマンド実行後に表示されるジョブの ID を確認します。



ヒント

- savingSetting(CLI : --saving_setting)パラメーターで"Compression"を指定することで、データの圧縮と固定パターンを排除する容量削減機能が有効なボリュームが作成できます。
- ボリュームには名前とニックネームが設定できます。名前はストレージクラスター内でユニークであることが必要であり、ニックネームは重複が許されます。このため、名前は個々のボ

リユームを識別するための名称として、またニックネームはボリュームをグルーピングするための名称として利用できます。

- `storageControllerId`(CLI: `--storage_controller_id`)パラメーターを設定することで、ボリュームを管理するストレージコントローラーを指定してボリュームを作成できます。

4. ジョブの `state` を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : `job_show`

`state` が `"Succeeded"` になっていたらジョブは完了です。

5. ボリュームの一覧を取得して、ボリュームが作成されたことを確認します。

REST API : GET /v1/objects/volumes

CLI : `volume_list`



ヒント

容量削減機能が有効なボリュームの場合は、`savingSetting` が `"Compression"` に設定されます。

6. 構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



注意

容量削減機能が有効なボリュームを作成するに当たっては、ストレージコントローラーが管理するストレージプールの空き容量が 80GiB 以上になるようにしてください。



メモ

ボリュームを管理するストレージコントローラーを指定してボリュームを作成する機能は、以下のようなケースでご利用ください。

- I/O 負荷の高いストレージノードのストレージコントローラーを避けてボリュームを作成する
- 増設したストレージノードで動作するストレージコントローラーに優先的にボリュームを作成する

また、ボリュームを管理するストレージコントローラーを指定してボリュームを作成する場合は以下の点に注意してください。

- ストレージコントローラーの容量使用率が高くなると、容量バランス処理によって、ボリュームが異なるストレージコントローラーに移動する場合があります。
 - 容量バランス処理によるストレージコントローラーの移動を発生させないためには、対象のストレージコントローラーにすでに作成されているボリュームの状況を確認して、ストレージコントローラーの容量使用率が 70%未満となるように容量設計を行うか、ストレージコントローラーの容量使用率が 70%を超える可能性がある場合は、ストレージコントローラーが動作するストレージノードの容量バランス設定を無効にすることを検討してください。
- ただし、容量バランス設定を無効にすると、ストレージコントローラーの容量使用率が高くなっても、容量の平準化が行われず、ストレージコントローラーの容量が枯渇する可能性があります。ストレージコントローラーの容量使用率を監視し、必要な空き容量を確保してください。

- ・ ストレージコントローラーの容量に対して、管理するボリュームの総容量が少ない状態で、ストレージコントローラーの上限までボリュームを作成すると、ストレージプールの容量を使い切ることができません。

17.4.2 ボリュームを作成する《Cloud》

この項での記述内容は Cloud モデルに適用されます。

ボリュームを作成します。

ボリューム作成コマンドで指定する"capacity"にはボリュームの容量を MiB 単位で指定します。作成したボリュームには制御情報が必要になります。そのため、"capacity"に指定できる値の上限としては logicalLimit から制御情報を引いた値になります。

"capacity"に指定できる値の上限値 = logicalLimit[MiB] - ((168[MiB] × n) + 42[MiB])

- ・ n = 作成するボリュームの論理容量[MiB] / 3,145,548[MiB] (小数点以下切り上げ)
- ・ logicalLimit は次のコマンドで確認できます。
REST API : GET /v1/objects/storage-controllers
CLI : storage_controller_list

ボリュームは論理容量のほかに制御情報が必要とします。ボリュームが消費するストレージプールの最大容量は「ボリュームが消費するストレージプールの最大容量」を参照して算出してください。



注意

オーバープロビジョニングになる容量のボリュームを作成した場合、当該ボリュームを管理するストレージコントローラーの allocatableCapacity[MiB]以上の容量はライト I/O することができなくなります。また、単一ボリュームでオーバープロビジョニングの状態にあったときに容量が枯渇すると、ドライブ増設が必要になります。「ドライブを増設する」を参照してストレージプールの容量を追加してください。

Universal Replicator を使用している場合は、以下に留意してください。

- ・ QoS 設定は、直接ホスト I/O を受けるボリューム(主に P-VOL)にのみ適用されます。それ以外のボリュームでは、QoS 設定は無視されます。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ボリュームを作成する」

前提条件

- ・ 実行に必要なロール : Storage

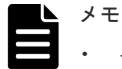
操作手順

1. ボリューム作成先のストレージプールの ID を確認します。
CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。
REST API : GET /v1/objects/pools
CLI : pool_list

2. ボリュームを作成します。

ボリューム作成のパラメーターを指定してコマンドを実行します。

Multi-AZ (Multi-Zone)構成の場合、ボリューム作成先のフォールトドメインの ID を指定する必要があります。



メモ

- <<Cloud for AWS>>ボリューム作成先のフォールトドメインは、I/O を実施するホスト(正/副構成であれば正側)と同じになるフォールトドメインの ID を指定してください。異なるホストからボリュームへ I/O を実施した場合、アベイラビリティゾーン間での通信になるため、通信コストの増加につながります。また、通信レイテンシーも大きくなります。
- <<Cloud for Google Cloud>>ボリューム作成先のフォールトドメインは、I/O を実施するホスト(正/副構成であれば正側)と同じになるフォールトドメインの ID を指定してください。異なるホストからボリュームへ I/O を実施した場合、アベイラビリティゾーン間での通信になるため、通信コストの増加につながります。また、通信レイテンシーも大きくなります。
- <<Cloud for Microsoft Azure>>ボリューム作成先のフォールトドメインは、I/O を実施するホスト(正/副構成であれば正側)と同じになるフォールトドメインの ID を指定してください。異なるホストからボリュームへ I/O を実施した場合、アベイラビリティゾーン間での通信になるため、通信レイテンシーが大きくなります。なお、Microsoft Azure では、アベイラビリティゾーン間の通信料は発生しません。

フォールトドメインの ID の確認

- REST API : GET /v1/objects/fault-domains
- CLI : fault_domain_list

ボリュームの作成

- REST API : POST /v1/objects/volumes
- CLI : volume_create

コマンド実行後に表示されるジョブの ID を確認します。



ヒント

- savingSetting(CLI : --saving_setting)パラメーターで"Compression"を指定することで、データの圧縮と固定パターンを排除する容量削減機能が有効なボリュームが作成できます。
- ボリュームには名前とニックネームが設定できます。名前はストレージクラスター内でユニークであることが必要であり、ニックネームは重複が許されます。このため、名前は個々のボリュームを識別するための名称として、またニックネームはボリュームをグルーピングするための名称として利用できます。
- storageControllerId(CLI : --storage_controller_id)パラメーターを設定することで、ボリュームを管理するストレージコントローラーを指定してボリュームを作成できます。
Multi-AZ (Multi-Zone)構成においてストレージコントローラーを指定した場合、フォールトドメインの ID は指定できません。指定したストレージコントローラーが属するフォールトドメインの ID が指定された場合と同じ扱いになります。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4. ボリュームの一覧を取得して、ボリュームが作成されたことを確認します。

REST API : GET /v1/objects/volumes

**注意**

容量削減機能が有効なボリュームを作成するに当たっては、ストレージコントローラーが管理するストレージプールの空き容量が **80GiB** 以上になるようにしてください。

**メモ**

ボリュームを管理するストレージコントローラーを指定してボリュームを作成する機能は、以下のようなケースでご利用ください。

- I/O 負荷の高いストレージノードのストレージコントローラーを避けてボリュームを作成する
- 増設したストレージノードで動作するストレージコントローラーに優先的にボリュームを作成する

また、ボリュームを管理するストレージコントローラーを指定してボリュームを作成する場合は以下の点に注意してください。

- ストレージコントローラーの容量使用率が高くなると、容量バランス処理によって、ボリュームが異なるストレージコントローラーに移動する場合があります。
- 容量バランス処理によるストレージコントローラーの移動を発生させないためには、対象のストレージコントローラーにすでに作成されているボリュームの状況を確認して、ストレージコントローラーの容量使用率が **70%未満** となるように容量設計を行うか、ストレージコントローラーの容量使用率が **70%を超える** 可能性がある場合は、ストレージコントローラーが動作するストレージノードの容量バランス設定を無効にすることを検討してください。
ただし、容量バランス設定を無効にすると、ストレージコントローラーの容量使用率が高くなっても、容量の平準化が行われず、ストレージコントローラーの容量が枯渇する可能性があります。ストレージコントローラーの容量使用率を監視し、必要な空き容量を確保してください。
- ストレージコントローラーの容量に対して、管理するボリュームの総容量が少ない状態で、ストレージコントローラーの上限までボリュームを作成すると、ストレージプールの容量を使い切ることができません。

**ヒント**

容量削減機能が有効なボリュームの場合は、`savingSetting` が "Compression" に設定されます。

5. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

17.5 ボリュームを削除する

不要になったボリュームを削除します。

以下の場合、ボリュームは削除できません。

- コンピュートノードとボリューム間のパスが設定されている場合は削除できません。
先に、削除するボリュームとコンピュートノード間の接続を解除してください。

- `snapshotAttribute` が"P-VOL"、"P/S-VOL"、または"S-VOL"のボリュームは、この節で説明する手順では削除できません。これらのボリュームの削除方法は「スナップショットを削除する」を参照してください。
- `status` が"ExpansionFailed"のボリュームは削除できません。削除する場合は、`status` が"ExpansionFailed"のボリュームに対して、再度ボリューム拡張を実行し、`status` が"Normal"になったことを確認した上で、ボリュームの削除を実行してください。
- `universalReplicatorAttribute` が"P-VOL"または"S-VOL"のボリュームは、この節で説明する手順では削除できません。Universal Replicator ペアを削除をすることで削除できるようになります。
- `volumeType` が"Journal"のボリュームは、この節で説明する手順では削除できません。Universal Replicator でジャーナルからジャーナルボリュームを取り外すか、ジャーナルを削除するかして、元ジャーナルボリュームにすることで削除できるようになります。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ボリュームを削除する」

前提条件

- 実行に必要なロール：Storage
- VPS 内のボリュームを削除する場合：当該 VPS のスコープ

操作手順

1. VPS 内のボリュームを削除する場合、VPS の ID を確認します。
CLI を使い VPS を名前で指定する場合は、VPS の名前を確認します。
REST API : GET /v1/objects/virtual-private-storages
CLI : `vps_list`
2. ボリュームの ID を確認します。
CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。
REST API : GET /v1/objects/volumes
CLI : `volume_list`
3. ボリュームを削除します。
ボリュームの ID を指定してコマンドを実行します。
CLI を使う場合はボリュームの ID の代わりに名前が指定できます。
REST API : DELETE /v1/objects/volumes/<id >
CLI : `volume_delete`
コマンド実行後に表示されるジョブの ID を確認します。



メモ

- 削除処理に伴う容量削減機能の進捗状況は、ボリューム情報の `dataReductionProgressRate[%]` で確認できます。

- ・ ボリュームの削除に掛かる時間は、このマニュアルの「容量削減機能が有効なボリュームの削除時間(目安)」を参考に見積もってください。

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

5. ボリュームの一覧を取得して、ボリュームが削除されたことを確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

6. ≪Bare metal≫構成情報のバックアップを行います。

「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

7. ≪Cloud for AWS≫構成情報のバックアップを行います。

「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



メモ

- ・ 容量削減機能が有効なボリュームの削除を実行中に、ストレージクラスターが停止した場合、削除のジョブは中断または失敗によって消滅して、ストレージクラスターは停止します。ストレージクラスターを起動すると、削除の処理は自動的に再開されます。
- ・ 削除対象のボリュームが、容量削減機能が有効なボリュームの場合、削除時間はボリュームの容量が大きいほど長くなります。
- ・ 削除処理に伴う容量削減機能の進捗状況は、ボリューム情報の dataReductionProgressRate[%]で確認できます。
- ・ 削除処理が終了するとボリューム情報から対象ボリュームがなくなります。なくなったかどうかはボリューム一覧を取得することで確認できます。
- ・ ボリュームの削除が完了したあと、ストレージプールの使用論理容量(usedCapacity)から削除対象ボリュームのすべての容量が解放されるまで、最大で 24 時間掛かることがあります。

17.6 ボリュームを拡張する

ボリュームの容量を拡張します。

status が"Normal"または"ExpansionFailed"、かつ volumeType が"Normal"の通常ボリュームに対してのみ実行できます。

- ・ status が"Normal"のボリュームに対して実行した場合、パラメーター"additionalCapacity"で指定した容量分のボリュームを拡張します。
- ・ status が"ExpansionFailed"のボリュームに対して実行した場合、ボリューム拡張を再実行します。



メモ

- スナップショットボリュームは、ボリュームの拡張ができません。volumeType が"Snapshot"かつ snapshotAttribute が"P-VOL"であるボリュームを拡張するには、対象のボリュームから作成されたスナップショットボリュームをすべて削除してください。volumeType が"Snapshot"かつ snapshotAttribute が"P/S-VOL"または"S-VOL"であるボリュームの拡張はできません。
- universalReplicatorAttribute が"P-VOL"または"S-VOL"のボリュームは拡張できません。universalReplicatorAttribute が"P-VOL"または"S-VOL"のボリュームを拡張する場合は、Universal Replicator ペアの分割、ボリュームの拡張、Universal Replicator ペアの再同期を順次行ってください。
- volumeType が"Journal"のボリュームの拡張はできません。volumeType が"Journal"のボリュームを拡張する場合は、必要な容量のボリュームをリザーブジャーナルボリュームとして追加し、ジャーナルボリュームをリザーブジャーナルボリュームに置き換えてください。
- volumeType が"FormerJournal"のボリュームは拡張できません。

ボリューム拡張コマンドで指定する"additionalCapacity"には拡張する容量を MiB 単位で指定します。ただし、拡張する領域にも追加で管理領域が必要になります。そのため、"additionalCapacity"に指定できる値の上限としては logicalLimit からこの追加の管理領域を引いた値になります。

"additionalCapacity"に指定できる値の上限値 = $\text{logicalLimit}[\text{MiB}] - ((168[\text{MiB}] \times n) + 42[\text{MiB}])$

- $n = \text{拡張するボリュームに追加する論理容量}[\text{MiB}] / 3,145,548[\text{MiB}]$ （小数点以下切り上げ）
- logicalLimit は次のコマンドで確認できます。
REST API : GET /v1/objects/storage-controllers
CLI : storage_controller_list



注意

- イベントログ KARS06170-C が発行され、未対処だった場合は、KARS06170-C に対処したあとでボリュームの操作を実施してください。
- ボリュームの容量は 42MiB 単位で管理しています。そのため logicalLimit が 0 であっても未使用の容量が存在することがあります。その場合、管理単位の上限(最大で 41MiB の追加)までは、ボリュームの容量が拡張できることがあります。
- オーバープロビジョニングになる容量にボリュームを拡張した場合、当該ボリュームを管理するストレージコントローラーの allocatableCapacity[MiB]以上の容量はライト I/O することができなくなります。また、単一ボリュームでオーバープロビジョニングの状態にあったときに容量が枯渇すると、ドライブ増設が必要になります。「ドライブを増設する」を参照してストレージプールの容量を追加してください。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ボリュームを拡張する」

前提条件

- 実行に必要なロール : Storage
- VPS 内のボリュームを拡張する場合 : 当該 VPS のスコープ

操作手順

1. VPS 内のボリュームを拡張する場合、VPS の ID と VPS に設定された条件(ボリューム容量上限、単一ボリューム容量上限)を確認します。

CLI を使い VPS を名前で指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

2. 拡張するボリュームの ID を確認します。

CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

また、ボリュームの容量を拡張するボリュームの status と volumeType を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

拡張対象のボリュームの status が "Normal" または "ExpansionFailed"、かつ volumeType が "Normal" のとき、次の手順に進みます。

3. ボリュームの容量を拡張します。

ボリュームに追加する容量を additionalCapacity に指定してコマンドを実行します。対象のボリュームの status が "Normal" の場合は必ず値を指定し、"ExpansionFailed" の場合は値を指定せずに実行します。

ボリュームの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : POST /v1/objects/volumes/<id>/actions/expand/invoke

CLI : volume_expand

コマンド実行後に表示されるジョブの ID を確認します。

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

5. ボリュームの情報を取得して、ボリュームの容量が拡張されたことを確認します。

ボリュームの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : GET /v1/objects/volumes/<id>

CLI : volume_show

6. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

7. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

17.7 ボリューム情報の一覧の取得

ボリューム情報の一覧を取得します。

17.7.1 取得できるボリュームの一覧情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が取得できます。

- dataReductionEffects : ボリュームのサマリー情報における容量削減機能の効果
- id : ボリュームの ID(uuid)
- name : ボリュームの名前
- nickname : ボリュームのニックネーム
- volumeNumber : ボリューム番号
- poolId : ストレージプールの ID(uuid)
- poolName : ストレージプールの名前
- totalCapacity : 論理総容量[MiB]
- usedCapacity : 使用論理容量[MiB]
- numberOfConnectingServers : 接続コンピュータノード数
- numberOfSnapshots : スナップショット数
- protectionDomainId : 所属するプロテクションドメインの ID(uuid)
- fullAllocated : ユーザーデータが書き込まれる領域があらかじめすべて割り当てられているかどうか
- volumeType : ボリューム種別(属性)の一覧
- universalReplicatorAttribute : 非同期リモートコピー属性
- isRemoteCopySupported : 非同期リモートコピーで利用可能なボリュームかどうか
- statusSummary : ボリュームの状態のサマリー
- status : ボリュームの状態
- storageControllerId : 当該ボリュームを管理するストレージコントローラーの ID(uuid)
- snapshotAttribute : スナップショットの属性
- snapshotStatus : スナップショットの状態
- savingSetting : 容量削減機能の設定
- savingMode : 容量削減機能の処理モード
- dataReductionStatus : 容量削減機能の状態
- dataReductionProgressRate : 容量削減機能の進捗率[%]
- vpsId : ボリュームが所属する VPS の ID
- vpsName : ボリュームが所属する VPS の名前
- qosParam : QoS に関するパラメーター
 - upperLimitForIops : ボリューム性能上限[IOPS]
 - upperLimitForTransferRate : ボリューム性能上限[MiB/sec]
 - upperAlertAllowableTime : ボリューム性能上限に関するアラートしきい値[sec]
 - upperAlertTime : ボリュームの性能上限を継続して超過した場合に性能上限アラート条件に合致した最終時刻(UTC)
- naaId : ボリュームの NAA ID

- **primaryFaultDomainId** : ボリュームを本来管理するプライマリーのフォールトドメインの ID
- **secondaryFaultDomainId** : プライマリーのフォールトドメインからフェイルオーバーしたときにボリュームを管理するセカンダリーのフォールトドメインの ID(複数フォールトドメイン構成の場合のみ出力。それ以外の構成の場合は null)
- **tertiaryFaultDomainId** : セカンダリーのフォールトドメインからさらにフェイルオーバーしたときにボリュームを管理するフォールトドメインの ID(複数フォールトドメイン構成、かつユーザーデータの保護方式が HPEC 4D+2P の場合のみ出力。それ以外の構成の場合は null)
- **currentFaultDomainId** : ボリュームを現在管理するカレントのフォールトドメインの ID
- **isPrimaryFaultDomain** : プライマリーのフォールトドメインと同じフォールトドメインでボリュームが現在管理されているかどうか(複数フォールトドメイン構成の場合のみ出力。それ以外の構成の場合は null)
- **nguId** :
 - FC 接続または iSCSI 接続の場合は常に null
 - NVMe/TCP 接続の場合はボリュームの NGU ID

17.7.2 取得できるボリュームの一覧情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が取得できます。

- **dataReductionEffects** : ボリュームのサマリー情報における容量削減機能の効果
- **id** : ボリュームの ID(uuid)
- **name** : ボリュームの名前
- **nickname** : ボリュームのニックネーム
- **volumeNumber** : ボリューム番号
- **poolId** : ストレージプールの ID(uuid)
- **poolName** : ストレージプールの名前
- **totalCapacity** : 論理総容量[MiB]
- **usedCapacity** : 使用論理容量[MiB]
- **numberOfConnectingServers** : 接続コンピュータノード数
- **numberOfSnapshots** : スナップショット数
- **protectionDomainId** : 所属するプロテクションドメインの ID(uuid)
- **fullAllocated** : ユーザーデータが書き込まれる領域があらかじめすべて割り当てられているかどうか
- **volumeType** : ボリューム種別(属性)の一覧
- **universalReplicatorAttribute** : 非同期リモートコピー属性
- **isRemoteCopySupported** : 非同期リモートコピーで利用可能なボリュームかどうか
- **statusSummary** : ボリュームの状態のサマリー
- **status** : ボリュームの状態
- **storageControllerId** : 当該ボリュームを管理するストレージコントローラーの ID(uuid)
- **snapshotAttribute** : スナップショットの属性
- **snapshotStatus** : スナップショットの状態

- `savingSetting` : 容量削減機能の設定
- `savingMode` : 容量削減機能の処理モード
- `dataReductionStatus` : 容量削減機能の状態
- `dataReductionProgressRate` : 容量削減機能の進捗率[%]
- `vpsId` : ボリュームが所属する VPS の ID
- `vpsName` : ボリュームが所属する VPS の名前
- `qosParam` : QoS に関するパラメーター
 - `upperLimitForIops` : ボリューム性能上限[IOPS]
 - `upperLimitForTransferRate` : ボリューム性能上限[MiB/sec]
 - `upperAlertAllowableTime` : ボリューム性能上限に関するアラートしきい値[sec]
 - `upperAlertTime` : ボリュームの性能上限を継続して超過した場合に性能上限アラート条件に合致した最終時刻(UTC)
- `naaId` : ボリュームの NAA ID
- `primaryFaultDomainId` : ボリュームを本来管理するプライマリーのフォールトドメインの ID
- `secondaryFaultDomainId` : プライマリーのフォールトドメインからフェイルオーバーしたときにボリュームを管理するセカンダリーのフォールトドメインの ID(複数フォールトドメイン構成の場合のみ出力。それ以外の構成の場合は null)
- `tertiaryFaultDomainId` : セカンダリーのフォールトドメインからさらにフェイルオーバーしたときにボリュームを管理するフォールトドメインの ID(複数フォールトドメイン構成、かつユーザーデータの保護方式が HPEC 4D+2P の場合のみ出力。それ以外の構成の場合は null)
- `currentFaultDomainId` : ボリュームを現在管理するカレントのフォールトドメインの ID
- `isPrimaryFaultDomain` : プライマリーのフォールトドメインと同じフォールトドメインでボリュームが現在管理されているかどうか(複数フォールトドメイン構成の場合のみ出力。それ以外の構成の場合は null)
- `nguid` : 常に null

17.7.3 ボリューム情報の一覧を取得する

各ボリュームの情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ボリューム情報の一覧を取得します。
 REST API : GET /v1/objects/volumes
 CLI : `volume_list`

17.8 ボリューム情報の個別取得

指定した ID のボリュームの情報を取得します。

17.8.1 取得できるボリュームの個別情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

指定した ID のボリュームについて、以下の情報が取得できます。

- reservedCapacity : 予約論理容量[MiB]
- freeCapacity : 空き論理容量[MiB]
- luns :
 - iSCSI 接続の場合はボリュームの LUN 一覧
 - FC 接続の場合はボリュームの LUN 一覧
 - NVMe/TCP 接続の場合は常に null
- nameSpaceId :
 - FC 接続または iSCSI 接続の場合は常に null
 - NVMe/TCP 接続の場合は Namespace
- nvmSubSystemNqn :
 - FC 接続または iSCSI 接続の場合は常に null
 - NVMe/TCP 接続の場合はサブシステムの識別情報
- snapshotProgressRate : スナップショットボリュームの取得準備、削除、リストアの進捗率[%]
- snapshotTimestamp : S-VOL または P/S-VOL の場合、スナップショット作成時点の P-VOL に対して差分データの記録を開始した時刻
- snapshotType : スナップショット種別
S-VOL または P/S-VOL の場合"Snapshot"、その他の場合は null
- dataReductionEffects : 容量削減機能の効果
- snapshotConcordanceRate : 当該ボリュームと 1 つ新しい世代の S-VOL または複製元ボリュームとの一致率[%]
- isWrittenInSvol : コンピュートノードから当該ボリュームへの書き込み有無
- id : ボリュームの ID(uuid)
- name : ボリュームの名前
- nickname : ボリュームのニックネーム
- volumeNumber : ボリューム番号
- poolId : ストレージプールの ID(uuid)
- poolName : ストレージプールの名前
- totalCapacity : 論理総容量[MiB]
- usedCapacity : 使用論理容量[MiB]
- numberOfConnectingServers : 接続コンピュータノード数
- numberOfSnapshots : スナップショット数
- protectionDomainId : 所属するプロテクションドメインの ID(uuid)
- fullAllocated : ユーザーデータが書き込まれる領域があらかじめすべて割り当てられているかどうか
- volumeType : ボリューム種別(属性)の一覧

- `universalReplicatorAttribute` : 非同期リモートコピー属性
- `isRemoteCopySupported` : 非同期リモートコピーで利用可能なボリュームかどうか
- `statusSummary` : ボリュームの状態のサマリー
- `status` : ボリュームの状態
- `storageControllerId` : 当該ボリュームを管理するストレージコントローラーの ID(uuid)
- `snapshotAttribute` : スナップショットの属性
- `snapshotStatus` : スナップショットの状態
- `savingSetting` : 容量削減機能の設定
- `savingMode` : 容量削減機能の処理モード
- `dataReductionStatus` : 容量削減機能の状態
- `dataReductionProgressRate` : 容量削減機能の進捗率[%]
- `vpsId` : ボリュームが所属する VPS の ID
- `vpsName` : ボリュームが所属する VPS の名前
- `qosParam` : QoS に関するパラメーター
 - `upperLimitForIops` : ボリューム性能上限[IOPS]
 - `upperLimitForTransferRate` : ボリューム性能上限[MiB/sec]
 - `upperAlertAllowableTime` : ボリューム性能上限に関するアラートしきい値[sec]
 - `upperAlertTime` : ボリュームの性能上限を継続して超過した場合に性能上限アラート条件に合致した最終時刻(UTC)
- `naaId` : ボリュームの NAA ID
- `primaryFaultDomainId` : ボリュームを本来管理するプライマリーのフォールトドメインの ID
- `secondaryFaultDomainId` : プライマリーのフォールトドメインからフェイルオーバーしたときにボリュームを管理するセカンダリーのフォールトドメインの ID(複数フォールトドメイン構成の場合のみ出力。それ以外の構成の場合は null)
- `tertiaryFaultDomainId` : セカンダリーのフォールトドメインからさらにフェイルオーバーしたときにボリュームを管理するフォールトドメインの ID(複数フォールトドメイン構成、かつユーザーデータの保護方式が HPEC 4D+2P の場合のみ出力。それ以外の構成の場合は null)
- `currentFaultDomainId` : ボリュームを現在管理するカレントのフォールトドメインの ID
- `isPrimaryFaultDomain` : プライマリーのフォールトドメインと同じフォールトドメインでボリュームが現在管理されているかどうか(複数フォールトドメイン構成の場合のみ出力。それ以外の構成の場合は null)
- `nguId` :
 - FC 接続または iSCSI 接続の場合は常に null
 - NVMe/TCP 接続の場合はボリュームの NGU ID

17.8.2 取得できるボリュームの個別情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

指定した ID のボリュームについて、以下の情報が取得できます。

- `reservedCapacity` : 予約論理容量[MiB]
- `freeCapacity` : 空き論理容量[MiB]

- luns : ボリュームの LUN 一覧
- nameSpaceId : 常に null
- nvmsubSystemNqn : 常に null
- snapshotProgressRate : スナップショットボリュームの取得準備、削除、リストアの進捗率[%]
- snapshotTimestamp : S-VOL または P/S-VOL の場合、スナップショット作成時点の P-VOL に対して差分データの記録を開始した時刻
- snapshotType : スナップショット種別
S-VOL または P/S-VOL の場合"Snapshot"、その他の場合は null
- dataReductionEffects : 容量削減機能の効果
- snapshotConcordanceRate : 当該ボリュームと 1 つ新しい世代の S-VOL または複製元ボリュームとの一致率[%]
- isWrittenInSvol : コンピュートノードから当該ボリュームへの書き込み有無
- id : ボリュームの ID(uuid)
- name : ボリュームの名前
- nickname : ボリュームのニックネーム
- volumeNumber : ボリューム番号
- poolId : ストレージプールの ID(uuid)
- poolName : ストレージプールの名前
- totalCapacity : 論理総容量[MiB]
- usedCapacity : 使用論理容量[MiB]
- numberOfConnectingServers : 接続コンピュータノード数
- numberOfSnapshots : スナップショット数
- protectionDomainId : 所属するプロテクションドメインの ID(uuid)
- fullAllocated : ユーザーデータが書き込まれる領域があらかじめすべて割り当てられているかどうか
- volumeType : ボリューム種別(属性)の一覧
- universalReplicatorAttribute : 非同期リモートコピー属性
- isRemoteCopySupported : 非同期リモートコピーで利用可能なボリュームかどうか
- statusSummary : ボリュームの状態のサマリー
- status : ボリュームの状態
- storageControllerId : 当該ボリュームを管理するストレージコントローラーの ID(uuid)
- snapshotAttribute : スナップショットの属性
- snapshotStatus : スナップショットの状態
- savingSetting : 容量削減機能の設定
- savingMode : 容量削減機能の処理モード
- dataReductionStatus : 容量削減機能の状態
- dataReductionProgressRate : 容量削減機能の進捗率[%]
- vpsId : ボリュームが所属する VPS の ID
- vpsName : ボリュームが所属する VPS の名前
- qosParam : QoS に関するパラメーター

- upperLimitForIops : ボリューム性能上限[IOPS]
- upperLimitForTransferRate : ボリューム性能上限[MiB/sec]
- upperAlertAllowableTime : ボリューム性能上限に関するアラートしきい値[sec]
- upperAlertTime : ボリュームの性能上限を継続して超過した場合に性能上限アラート条件に合致した最終時刻(UTC)
- naaId : ボリュームの NAA ID
- primaryFaultDomainId : ボリュームを本来管理するプライマリーのフォールトドメインの ID
- secondaryFaultDomainId : プライマリーのフォールトドメインからフェイルオーバーしたときにボリュームを管理するセカンダリーのフォールトドメインの ID(複数フォールトドメイン構成の場合のみ出力。それ以外の構成の場合は null)
- tertiaryFaultDomainId : セカンダリーのフォールトドメインからさらにフェイルオーバーしたときにボリュームを管理するフォールトドメインの ID(複数フォールトドメイン構成、かつユーザデータの保護方式が HPEC 4D+2P の場合のみ出力。それ以外の構成の場合は null)
- currentFaultDomainId : ボリュームを現在管理するカレントのフォールトドメインの ID
- isPrimaryFaultDomain : プライマリーのフォールトドメインと同じフォールトドメインでボリュームが現在管理されているかどうか(複数フォールトドメイン構成の場合のみ出力。それ以外の構成の場合は null)
- nguId : 常に null

17.8.3 ボリュームの情報を個別に取得する

指定した ID のボリュームの情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ボリュームの ID を確認します。
CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。
REST API : GET /v1/objects/volumes
CLI : volume_list
2. ボリュームの情報を取得します。
ボリュームの ID を指定してコマンドを実行します。
CLI を使う場合はボリュームの ID の代わりに名前が指定できます。
REST API : GET /v1/objects/volumes/<id >
CLI : volume_show

17.9 ボリュームの設定を編集する

通常ボリュームまたはスナップショットボリュームの設定を編集します。ボリュームの名前(name)、ニックネーム(nickname)、QoS に関するパラメーター(upperLimitForIops、upperLimitForTransferRate、upperAlertAllowableTime)が編集できます。

status が "Normal" または "UpdateFailed" のボリュームにのみ実行できます。status が "UpdateFailed" の場合、編集するパラメーターを指定せずにボリューム設定編集を再実行します。

以下に留意して実施してください。

- name には、ストレージクラスター内でユニークな値のみが設定できます。
- nickname には、ボリューム間で重複した値が設定できます。
- 手順 3 で複数パラメーターを指定する場合には、以下の組み合わせでのみ指定できます。組み合わせできない設定変更を行う場合は、再度コマンドを実行してください。
 - name と nickname の組み合わせ
 - upperLimitForIops と upperLimitForTransferRate と upperAlertAllowableTime の組み合わせ



注意

イベントログ KARS06170-C が発行され、未対処だった場合は、KARS06170-C に対処したあとでボリュームの操作を実施してください。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「ボリュームの設定を編集する」
- 「ボリュームの QoS 設定を編集する」

前提条件

- 実行に必要なロール : Storage
- VPS 内のボリュームの設定を編集する場合 : 当該 VPS のスコープ

操作手順

1. VPS 内のボリュームの設定を編集する場合、VPS の ID と VPS に設定された条件(QoS の設定)を確認します。

CLI を使い VPS を名前で指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list



メモ

システム管理者は、VPS の QoS の設定に制限されずボリューム個別に QoS の設定をすることができます。

2. ボリュームの ID を確認します。

CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

3. ボリュームの設定を変更します。

ボリュームの ID とボリューム設定のパラメーターを指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : PATCH /v1/objects/volumes/<id >

CLI : volume_set

コマンド実行後に表示されるジョブの ID を確認します。

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

5. ボリュームの情報を取得して、ボリュームの設定が編集されたことを確認します。

ボリュームの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : GET /v1/objects/volumes/<id >

CLI : volume_show

6. ≪Bare metal≫構成情報のバックアップを行います。

「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

7. ≪Cloud for AWS≫構成情報のバックアップを行います。

「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

17.10 ボリュームが稼働するアベイラビリティーゾーンを確認する ≪Cloud≫

この節での記述内容は Cloud モデルに適用されます。

- ≪Cloud for AWS≫ストレージノードに障害が発生した場合など、ボリュームを管理するアベイラビリティーゾーン(フォールトドメイン)が異なっていることがあります。管理するアベイラビリティーゾーンが異なっていると、アベイラビリティーゾーン間での通信になるため通信コストの増加につながります。また、通信レイテンシーも大きくなります。
- ≪Cloud for Google Cloud≫ストレージノードに障害が発生した場合など、ボリュームを管理するアベイラビリティーゾーン(フォールトドメイン)が異なっていることがあります。管理するアベイラビリティーゾーンが異なっていると、アベイラビリティーゾーン間での通信になるため通信コストの増加につながります。また、通信レイテンシーも大きくなります。
- ≪Cloud for Microsoft Azure≫ストレージノードに障害が発生した場合など、ボリュームを管理するアベイラビリティーゾーン(フォールトドメイン)が異なっていることがあります。管理するアベイラビリティーゾーンが異なっていると、アベイラビリティーゾーン間での通信になるため通信レイテンシーが大きくなります。なお、Microsoft Azure では、アベイラビリティーゾーン間の通信料は発生しません。

このことから、ユーザーは、ボリュームを管理するアベイラビリティーゾーンが異なっていないかを定期的に確認してください。



ヒント

ストレージノード障害の有無はストレージノードの情報を取得して確認してください。

- REST API : GET /v1/objects/storage-nodes
- CLI : storage_node_list

ストレージノードに障害が起きていた場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対応してください。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ボリュームを管理するアベイラビリティーゾーンが異なっていないかを確認します。
クエリーパラメーター isPrimaryFaultDomain(CLI : is_primary_fault_domain)に、"false"を指定してコマンドを実行します。

REST API : GET /v1/objects/volumes

CLI : volume_list

該当するボリュームがなければ、ボリュームを管理するアベイラビリティーゾーンは管理が異なっていません。

該当するボリュームがあった場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対応してください。



ヒント VSP One SDS Block Administrator では、ボリューム一覧参照画面で確認できます。
isPrimaryFaultDomain が"true"であれば、ボリュームを管理するアベイラビリティーゾーンは異なっていません。

スナップショットを使用したボリュームのバックアップと復元

- 18.1 スナップショットの概要
- 18.2 スナップショットの取得準備をする
- 18.3 スナップショットを取得する
- 18.4 スナップショットを削除する
- 18.5 スナップショットからのボリューム復元
- 18.6 ボリュームに対する P-VOL 情報を取得する
- 18.7 ボリュームに対する S-VOL 情報の一覧を取得する

18.1 スナップショットの概要

ボリュームのある時点の複製イメージをスナップショットといいます。複製元のボリュームのデータを誤って更新した場合などに、取得済みのスナップショットからデータを復元できます。複製元のボリュームを P-VOL(Primary Volume)、複製先のボリュームを S-VOL(Secondary Volume)といいます。P-VOL を更新するときに、更新される部分における更新前のデータだけがスナップショットボリュームのデータとしてストレージプールにコピーされます。

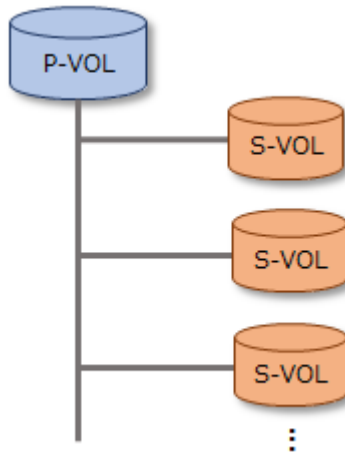
このように、P-VOL と S-VOL の差分データだけを保存することで容量を低減でき、コスト効率のよい複製を作成できます。また、複数の S-VOL 間でもデータを共有して保存するため、複数世代のスナップショットを取得する場合でも消費容量を抑えることができます。ストレージプールを共用するため、スナップショット専用のストレージプールを作成する必要はありません。



注意

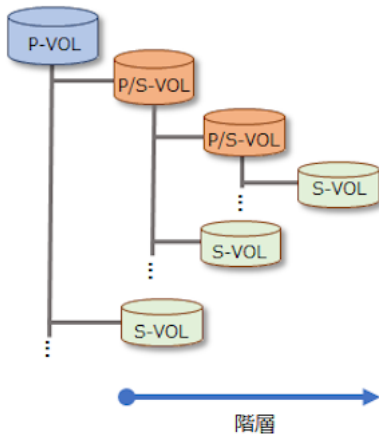
- 以下の点に留意し、ホスト経由などで別装置にも、必要なデータをバックアップしておくことをお勧めします。また、ストレージプールの使用容量を監視し、十分な空き容量を確保するようにしてください。
 - S-VOL は P-VOL のデータを使用しているため、P-VOL に障害が発生してデータが使用できなくなると、S-VOL のデータも使用できなくなります。
 - 差分データはストレージプールに格納しているため、ストレージプールの障害または満杯によってストレージプールが使用できなくなるとスナップショットボリュームのデータが消失します。
 - リストア中(S-VOL のデータから P-VOL のデータを復元する操作を実施中)にスナップショットボリュームのデータを消失した場合、リストア先ボリューム(P-VOL)のデータも使用できなくなります。
 - 容量削減機能が有効なボリュームを P-VOL として S-VOL は作成できますが、S-VOL では容量削減機能が有効になりません。このことを前提にストレージプールの容量を管理してください。
 - イベントログ KARS06170-C が発行された場合には、対象のボリューム(P-VOL)の status と関連するスナップショットボリュームの status は、"IOSuppressed"になり、ボリュームへの I/O は抑止されます。対象のボリューム(P-VOL)から作成されたスナップショットボリュームをすべて削除してください。その後、対象のボリューム(この時点では通常ボリューム)を削除してください。対象のボリュームが通常ボリュームになっても I/O はできません。(ボリュームの status は"IOSuppressed"のままです。)
- 「構成バックアップを行う《Bare metal》《Cloud for AWS》」に従って、ストレージクラスター構成のリストアを実施してもスナップショットを元に戻すことはできません。復元されたスナップショットボリュームとボリュームパスは、システム管理者または利用者によってすべて削除する必要があります。
- スナップショットボリュームは、ボリュームの拡張ができません。volumeType が"Snapshot"かつ snapshotAttribute が"P-VOL"であるボリュームを拡張するには、対象のボリュームから作成されたスナップショットボリュームをすべて削除してください。volumeType が"Snapshot"かつ snapshotAttribute が"P/S-VOL"または"S-VOL"であるボリュームの拡張はできません。

スナップショットの複製元/複製先の関係にある、以下のようなスナップショットの構成をスナップショットツリーといいます。S-VOL は、取得した時刻によって複数の世代が作成されます。



取得済みのスナップショットを複製元として、さらにスナップショットを作成できます。このときのスナップショットの構成をカスケード構成といいます。カスケード構成では、P-VOL であり、かつ S-VOL を持つ属性のボリュームができます。このようなボリュームを P/S-VOL と呼びます。

カスケード構成は、P-VOL より下の階層から数えて、最大 64 階層まで構築できます。例えば、以下の図は、3 階層のカスケード構成を示しています。



スナップショットに関する操作には以下があります。

操作	説明	参照先
スナップショットの取得準備をする	スナップショットを取得するためのボリューム(S-VOL)を作成します。 スナップショットの取得準備を実行すると、必ずボリューム(S-VOL)が作成されます。ボリューム(S-VOL)を作成せずにスナップショットを取得することはできません。	「スナップショットの取得準備をする」
スナップショットを取得する	準備された S-VOL にスナップショットを取得します。	「スナップショットを取得する」
スナップショットを削除する	不要になったスナップショットボリュームを削除します。	「スナップショットを削除する」
スナップショットからボリュームを復元する	S-VOL のデータから P-VOL のデータを復元します。	「スナップショットからのボリューム復元」

操作	説明	参照先
ボリュームに対する P-VOL 情報を取得する	S-VOL の作成元となった P-VOL についての情報を取得します。	「ボリュームに対する P-VOL 情報を取得する」
ボリュームに対する S-VOL 情報の一覧を取得する	P-VOL から作成された S-VOL 情報の一覧を取得します。	「ボリュームに対する S-VOL 情報の一覧を取得する」
スナップショットボリュームの設定を編集する	スナップショットボリュームの設定を編集します。	「ボリュームの設定を編集する」

スナップショットに関する仕様

スナップショットに関する仕様は以下のとおりです。

項目	仕様
S-VOL 数(P-VOL 当たり)	1,023
ボリューム数 (ストレージノード当たり)	P-VOL、P/S-VOL、S-VOL、通常ボリュームを合わせて 1,024
ボリューム数 (システム当たり)	1 冗長構成の場合： P-VOL、P/S-VOL、S-VOL、通常ボリュームを合わせて 1,024 × n (ストレージノード数*) 2 冗長構成の場合： P-VOL、P/S-VOL、S-VOL、通常ボリュームを合わせて、次のうち小さいほうが適用されます。 1,024 × n (ストレージノード数) 16,384
スナップショットを使用した場合のボリューム合計容量の最大値(ストレージコントローラー当たり)	4PiB(目安) 4PiB 以上(目安)のスナップショットの取得準備を実施した場合は、KARS06002-E が発生し操作が失敗することがあります。
ボリューム操作とスナップショット操作を同時実行できる最大数	20(目安) 20 以上(目安)の操作を同時に実行した場合は、タイムアウトが発生して操作が失敗することがあります。 ボリューム操作とは、ボリュームの作成、削除、拡張、設定編集を指します。スナップショット操作とは、スナップショットの取得準備、取得、削除、復元を指します。操作対象には容量削減機能が有効なボリュームも含まれます。 単一操作で複数ボリュームを扱うものについては 1 操作としてカウントします。例えば、1 回のボリューム作成操作で 20 個以上のボリュームを指定した場合は 1 操作としてカウントします。 ジョブの完了は操作の完了を意味しています。ジョブの state が"Succeeded"になっていたら、操作は完了しています。
スナップショットボリュームの名前	文字数：1～32 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(-,.,:@_)
カスケード構成の最大階層	64
* <<Cloud>>Multi-AZ (Multi-Zone)構成の場合、タイブレーカーノードは容量を持たない(ドライブが存在しない)ため、ストレージノード数の対象には含めません。	

ボリューム情報から得られるスナップショットに関する情報

スナップショット情報の一覧を取得することで得られる、スナップショット固有の情報には以下があります。

情報の種類	説明
snapshotStatus	スナップショットの状態表示です。Normal(正常)、Empty(スナップショットのメタデータがない空の状態)*、Deleting(削除中)、Restoring(リストア中)、Preparing(取得準備中)、Prepared(取得準備完了)、Error(異常)のいずれかが表示されます。通常ボリュームの場合は "-" になります。 * S-VOL 作成時または削除時の一時的な状態であり、しばらく待つと S-VOL 作成時は Preparing に遷移し、S-VOL 削除時は当該ボリュームが削除されます。 snapshotStatus は、ボリューム情報の一覧からも取得できます。
snapshotProgressRate[%]	スナップショット操作の進捗率です。snapshotStatus が Preparing、Restoring、Deleting のいずれかである場合に表示されます。それ以外の場合は null 表示になります。 一致率(snapshotConcordanceRate[%])と同時に表示されません。 snapshotProgressRate[%]は、ボリューム情報からも取得できます。
snapshotTimestamp	スナップショット取得時刻です。 snapshotStatus が "Normal" の場合に表示されます。それ以外の場合は null 表示になります。 snapshotTimestamp は、ボリューム情報からも取得できます。
snapshotType	スナップショットボリュームの場合、"Snapshot" と表示されます。 snapshotType は、ボリューム情報からも取得できます。
snapshotConcordanceRate[%]	当該ボリュームと比較対象ボリュームとのデータの一致率[%]を表します。 当該ボリュームが最新世代の S-VOL の場合は、比較対象ボリュームは P-VOL になります。当該ボリュームが最新世代ではない S-VOL の場合は、比較対象ボリュームは 1 つ新しい世代の S-VOL になります。例えば、多世代の構成(P-VOL と S-VOL が 1:N の構成)で P-VOL に書き込みがあった場合は、最新世代の S-VOL だけ一致率が下がります。S-VOL に書き込みがあった場合は、書き込んだ世代の S-VOL だけ一致率が下がります。 一致率は目安であり、大きな誤差が生じることもあります。 一致率の差分の管理単位は 256KiB です。 スナップショットのリストア・削除では、P-VOL と S-VOL のデータ差分量が多いほど、より処理時間が掛かります。 スナップショットのリストア・削除の処理時間を、事前に見積もるための情報として利用できます。 snapshotConcordanceRate[%]は、ボリューム情報からも取得できます。 ≪Bare metal≫スナップショット操作の処理時間の目安は、このマニュアルの「スナップショット操作の処理時間≪Bare metal≫」を参照してください。
isWrittenInSvol	S-VOL へのホストからの書き込みの有無がわかります。 snapshotStatus が "Normal" の場合に表示されます。それ以外の場合は null 表示になります。 isWrittenInSvol は、ボリューム情報からも取得できます。

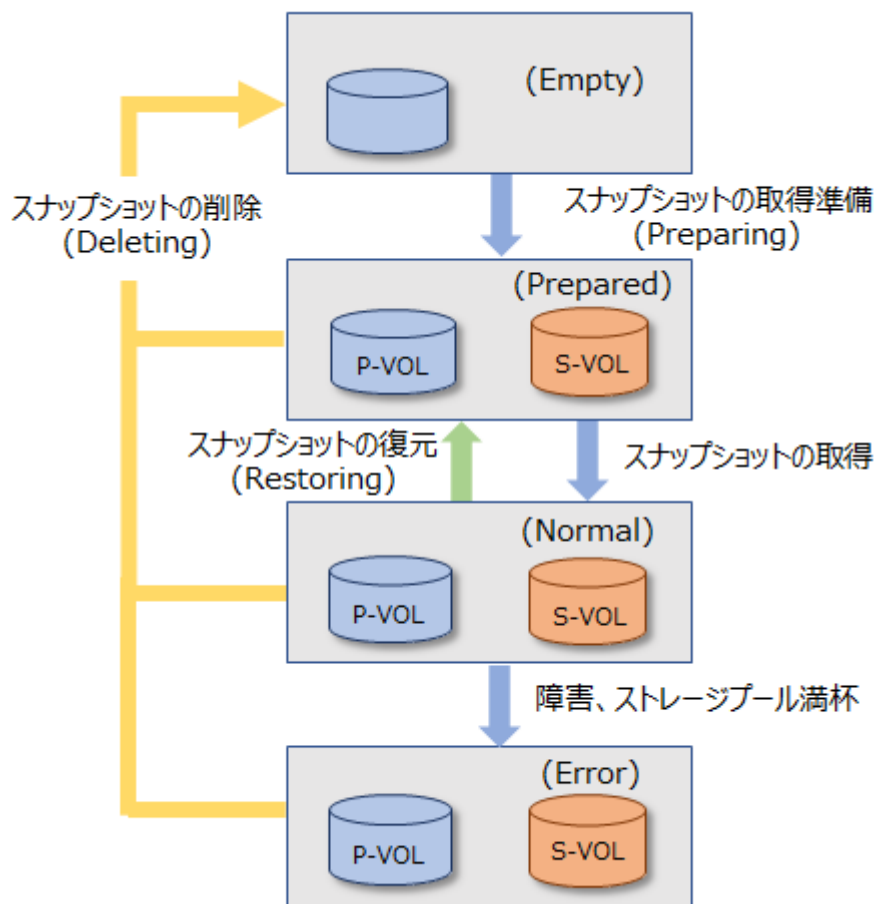
状態遷移(スナップショット操作と snapshotStatus)

スナップショット操作によって snapshotStatus は変わります。



メモ

snapshotStatus が変わるまで 1 分程度掛かることがあります。snapshotStatus の変化を確認する場合は、1 分ほど経過してから再度確認してください。



ヒント

当該ボリュームがスナップショットボリュームであるかどうかは、ボリューム情報の snapshotAttribute でわかります。"P-VOL"、"P/S-VOL"、"S-VOL"のいずれかが表示されます。通常ボリュームの場合は "-" になります。また、P-VOL または P/S-VOL の S-VOL 数は、ボリューム情報の numberOfSnapshots でわかります。

P-VOL、S-VOL への R/W 可否

P-VOL は、複製先の snapshotStatus によらず R/W 可能です。スナップショットからのデータ復元中もホスト I/O を継続することができます。

S-VOL は、snapshotStatus が "Normal" のときだけ R/W 可能です。

スナップショットで消費するプールの最大容量

スナップショットで消費するプールの P-VOL ごとの最大容量は次の式で計算できます。すべての最大容量を算出する場合は、すべての P-VOL 分を計算して合計してください。

P-VOL ごとのストレージプール消費の最大容量[MiB] = ① × 42 + ② × 175,434

- ① : 以下の計算結果から小数点以下を切り上げた値です。
(P-VOL 容量[MiB] × スナップショット数 × 2 ÷ 42)
- ② : 以下の計算結果から小数点以下を切り上げた値です。

$$(P\text{-VOL 容量[MiB]} \times \text{スナップショット数} \times 2 \div 2,921,688)$$

上記の式のスナップショット数は、現在のスナップショット数ではなく、過去からの最大スナップショット数を表します。

ストレージプール容量に関する注意事項

ストレージプール容量から仮想ボリューム管理領域を除いたものが、そのストレージプールでデータを格納できる容量です。仮想ボリューム管理領域は、ストレージプール容量の約 3% です。

仮想ボリューム管理領域の容量は、P-VOL の容量、スナップショット数などによって変化します。P-VOL ごとの容量の目安は、次の計算式で算出します。すべての仮想ボリューム管理領域の容量を算出する場合は、すべての P-VOL 分を計算し合計してください。

$$P\text{-VOL ごと}の仮想ボリューム管理領域の容量[MiB] = (4 + \textcircled{1}) \times 42$$

- ・ ①：以下の計算結果から小数点以下を切り上げた値です。
 $(2 \times \text{更新種別} \times \text{スナップショット数} + 64) \times (\text{ボリューム容量[MiB]} \div 3145728[\text{MiB}])$
- ・ 更新種別：更新するボリュームによって、1 または 2 を設定する
 - P-VOL のみ更新する場合、1 を設定
 - S-VOL のみ更新する場合、1 を設定
 - P-VOL、S-VOL 両方を更新する場合、2 を設定
- ・ スナップショット数：1 つの P-VOL に対する S-VOL 数
- ・ ボリューム容量：P-VOL の容量[MiB]

ストレージプールの容量が不十分だと、ストレージプールが満杯になり、スナップショットボリュームのデータが消失するおそれがあります。そのため、ストレージプールを作成するときは、コピー容量(取得されるスナップショットの差分データの容量)を見積もり、そのコピー容量に対応できるだけのストレージプール容量を設定する必要があります。ストレージプールの容量は必ず 42[MiB]単位で消費されます。したがって、差分データの容量が 42[MiB]よりも少ない場合も、ストレージプールの容量は 42[MiB]必要になります。



メモ

運用中のストレージプールの空き容量には十分注意し、しきい値を超過したり満杯になったりする前にストレージプールの容量を拡張してください。

- ・ スナップショットツリーの一部のスナップショットを削除しても、ストレージプール内のスナップショットボリュームのデータとして割り当てられていた領域は解放されないため、ストレージプールの使用量は減りません。解放されなかった領域は、同一のスナップショットツリーに新たなスナップショットボリュームのデータを格納するときに再度使用されます。
ストレージプールの使用量を削減したい場合は、該当するスナップショットツリーに作成されたスナップショットをすべて削除する必要があります。
- ・ ストレージプールが満杯になって、スナップショットが障害(snapshotStatus が "Error")になると、その後は、ボリュームの削除やドライブの増設などを行って容量不足を解消しても、スナップショットは回復しませんので、注意してください。



注意

ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した場合、キャッシュ保護付きライトバックモード無効時は、スナップショットボリュームのデータが消失することがあります。キャッシュ保護付きライトバックモード有効時は、スナップショットボリュームのデータは保護されます。ただし、キャッシュ保護用メタデータの冗長度を超える障害が発生している状態で、ストレージクラスターの障害が発生した場合は、キャッシュ保護付きライトバックモード有効時でも、スナップショットボリュームのデータは保護されません。

データが消失したスナップショットボリューム(S-VOL または P/S-VOL)のデータは R/W できません。障害の種類によっては、すべてのスナップショットボリュームのデータが消失する可能性があります。R/W できなくなったスナップショットボリュームは削除する以外の対処方法はありません。

必要に応じて、ホスト経由などで別装置にも、データをバックアップしておくことをお勧めします。

ストレージクラスターの障害によって、スナップショットボリュームを削除する方法は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ストレージクラスター起動時に KARS06132-C が発生した場合の対処」を参照してください。

snapshotStatus ごとの操作可否

スナップショットツリーの構成と snapshotStatus によって、実施できる操作の可否を示します。

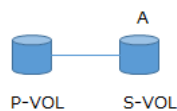


メモ

snapshotStatus が変わるまで 1 分程度掛かることがあります。snapshotStatus の変化を確認する場合は、1 分ほど経過してから再度確認してください。

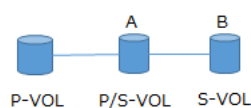
■カスケード構成でない場合

表中の「A に対するスナップショット操作」とは、A 自体の取得準備や取得を行うことを意味しています。A の配下にある別の B に対する取得準備や取得を行う場合は、「■カスケード構成の場合」の「B に対するスナップショット操作」を参照してください。



snapshotType	A の snapshotStatus	A に対するスナップショット操作				
		取得準備&取得 (PrepareAnd Finalize)	取得準備 (Prepare)	取得 (Finalize)	リストア	削除
なし	なし(A が存在しない)	○	○	—	—	—
Snapshot	Empty	—	—	×	×	×*
	Preparing	—	—	×	×	×
	Prepared	—	—	○	△	○
	Normal	—	—	△	○	○
	Restoring	—	—	×	×	×
	Error	—	—	×	×	○
	Deleting	—	—	×	×	×
○：成功する △：成功するが何もされない(ジョブは処理を実行しないで正常終了します) ×：失敗する —：操作自体が不可 * ストレージクラスターの停止によって削除処理が中断された場合は、再度実施することで成功します。						

■カスケード構成の場合



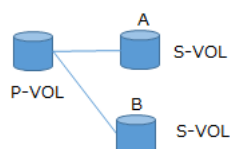
B に対するスナップショット操作を実施する際は、B が操作可能な状態にあることが前提になります。

snapshotType	A の snapshotStatus	B に対するスナップショット操作				
		取得準備&取得 (PrepareAnd Finalize)	取得準備 (Prepare)	取得 (Finalize)	リストア	削除
Snapshot	Empty	×	×	—	—	—
	Preparing	×	×	—	—	—
	Prepared	×	○	×	△	○
	Normal	○	○	○	○	○
	Restoring	×	×	×	△	○
	Error	×	×	×	×	○
	Deleting	×	×	—	—	—
○：成功する △：成功するが何もされない(ジョブは処理を実行しないで正常終了します) ×：失敗する —：操作自体が不可						

A に対するスナップショット操作を実施する際は、A が操作可能な状態にあることが前提になります。

snapshotType	B の snapshotStatus	A に対するスナップショット操作				
		取得準備&取得 (PrepareAnd Finalize)	取得準備 (Prepare)	取得 (Finalize)	リストア	削除
Snapshot	Empty	—	—	○	○	×
	Preparing	—	—	○	○	×
	Prepared	—	—	○	○	×
	Normal	—	—	△	×	×
	Restoring	—	—	△	×	×
	Error	—	—	△	×	×
	Deleting	—	—	△	×	×
○：成功する △：成功するが何もされない(ジョブは処理を実行しないで正常終了します) ×：失敗する —：操作自体が不可						

■複製元 VOL を複数の Snapshot で共有する場合



B に対するスナップショット操作を実施する際は、B が操作可能な状態にあることが前提になります。

snapshotType	A の snapshotStatus	B に対するスナップショット操作				
		取得準備&取得 (PrepareAnd Finalize)	取得準備 (Prepare)	取得 (Finalize)	リストア	削除
Snapshot	Empty	○	○	○	○	○
	Preparing	○	○	○	○	○
	Prepared	○	○	○	○	○
	Normal	○	○	○	○	○
	Restoring	×	○	×	×	○
	Error	×	×	○	○	○
	Deleting	×	×	○	○	○
○：成功する △：成功するが何もされない(ジョブは処理を実行しないで正常終了します) ×：失敗する * イベントログ KARS06132-C が出ている場合は成功します。						

スナップショットの QoS 設定

P-VOL、S-VOL、P/S-VOL には QoS の設定ができます。

QoS 機能については「Quality of Service(QoS)機能について」を参照してください。



メモ

スナップショットには、複製元ボリュームの QoS の設定は引き継がれません。

18.2 スナップショットの取得準備をする

複製元のボリュームを指定してコマンドを実行し、スナップショットを取得するためのボリューム (S-VOL)を作成します。

- スナップショットの取得準備をするには、以下の計算結果が 80 未満であることが必要です。

$$\text{usedCapacity}[\text{MiB}] / \text{allocatableCapacity}[\text{MiB}] \times 100$$

$$\text{usedCapacity}, \text{allocatableCapacity}$$
 は以下のコマンドで確認できます。
REST API : GET /v1/objects/storage-controllers
CLI : storage_controller_list
- 複製元ボリュームの配下に Deleting、Error 状態のスナップショットが存在する場合は取得準備できません。
- 複製元ボリュームがスナップショットの場合、複製元のスナップショットが Normal 状態のときのみ取得準備できます。
- universalReplicatorAttribute が"P-VOL"の場合は、Universal Replicator ペアの状態によらずスナップショットの取得準備はできます。universalReplicatorAttribute が"S-VOL"の場合、Universal Replicator ペアの状態が"PAIR"、"SSUS"、または"PSUE"のときはスナップショットの取得準備はできます。Universal Replicator ペアの状態が"COPY"のときはスナップショットの取得準備はできません。volumeType が"Journal"または"FormerJournal"のボリュームはスナップショットの取得準備はできません。



メモ

スナップショット取得準備とスナップショット取得を一括して実行できます。一括して実行すると操作を簡単化できますが、I/O を停止してからスナップショットを取得する場合には、スナップショット取得準備に掛かる時間も I/O を停止しなければならないため、I/O 停止時間が長くなります。

このため、このマニュアルでは、スナップショットの取得準備と取得を別の操作で実施する手順を説明しています。

スナップショット取得準備とスナップショット取得を一括して実行するには、`operationType` パラメーター (CLI の場合: `--operation_type`) に "PrepareAndFinalize" を指定して手順 4 を実施します。

`operationType` パラメーター (CLI の場合: `--operation_type`) の指定を省略した場合も、スナップショット取得準備とスナップショット取得が一括して実行されますので、注意してください。

前提条件

- 実行に必要なロール: `Storage`
- VPS 内のボリュームについてスナップショットの取得準備をする場合: 当該 VPS のスコープ

操作手順

1. マルチテナンシー機能を利用していない場合、またはマルチテナンシー機能を利用してシステムスコープ内のボリュームについてスナップショットの取得準備をする場合、この手順は実施不要です。次の手順に進んでください。

VPS 内のボリュームについてスナップショットの取得準備をする場合、VPS の ID と VPS に設定された条件 (QoS 設定) を確認します。

CLI を使い、VPS を名前で指定する場合は、VPS の名前を確認します。

REST API: `GET /v1/objects/virtual-private-storages`

CLI: `vps_list`



メモ

システム管理者は、VPS の QoS の設定に制限されずボリューム個別に QoS の設定ができます。

QoS パラメーターを指定しない場合、VPS に設定された QoS パラメーターでスナップショットを取得するためのボリューム (S-VOL) が作成されます。

2. スナップショットの複製元となるボリュームの ID を確認します。

CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

REST API: `GET /v1/objects/volumes`

CLI: `volume_list`

3. 複製元のボリュームの ID を指定して S-VOL 情報の一覧を取得し、`snapshotStatus` が "Deleting"、"Error" いずれかのボリュームが存在しないことを確認します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API: `GET /v1/objects/volumes/<id>/snapshot-volumes`

CLI: `snapshot_volume_list`

`snapshotStatus` が "Deleting" のボリュームがあった場合は、それぞれの処理が完了するのを待ちます。"Error" の場合は、当該 S-VOL を削除します。

4. スナップショットの取得準備をします。

複製元のボリュームの ID と `operationType` パラメーターに "Prepare" を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。また、パラメーターは `--operation_type`、指定値は "Prepare" になります。

REST API: `POST /v1/objects/volumes/actions/create-snapshot/invoke`

CLI : volume_create_snapshot

コマンド実行後に表示されるジョブの ID を確認します。

5. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

6. S-VOL 情報の一覧を取得して、snapshotStatus が"Prepared"である S-VOL が作成されたことを確認します。

複製元のボリュームの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : GET /v1/objects/volumes/<id >/snapshot-volumes

CLI : snapshot_volume_list

手順 5 を実施後、snapshotStatus が変わるまで 1 分程度掛かることがあります。

snapshotStatus の変化を確認する場合は、1 分ほど経過してから再度確認してください。

18.3 スナップショットを取得する

取得準備で作成した複製先ボリュームを指定してスナップショットを取得します。

- 複製元ボリュームの配下に Restoring 状態のスナップショットが存在する場合は取得できません。
- 複製先の当該スナップショットが Prepared 状態のときのみ取得できます。
- 複製元ボリュームがスナップショットの場合、複製元のスナップショットが Normal 状態のときのみ取得できます。
- universalReplicatorAttribute が"P-VOL"の場合は、Universal Replicator ペアの状態によらずスナップショットは取得できます。universalReplicatorAttribute が"S-VOL"の場合、Universal Replicator ペアの状態が"PAIR"、"SSUS"、または"PSUE"のときはスナップショットは取得できます。Universal Replicator ペアの状態が"COPY"のときはスナップショットは取得できません。volumeType が"Journal"または"FormerJournal"のボリュームはスナップショットは取得できません。



メモ

- スナップショットを取得したあと、P-VOL への書き込み要求は、CoW(Copy on Write)方式で処理します。CoW 方式とは、書き込み前のデータをストレージプールへコピーしてから、書き込みを処理する方式です。
- スナップショットボリュームを作成した直後は、P-VOL のデータが更新されると、必ず差分データのコピーが動作します。さらに、ホストからの書き込み I/O が多い状態が続くと、差分データのコピーが大量に動作し、ストレージノード内の負荷が上昇して、書き込み I/O の IOPS 性能だけでなく、読み込み I/O の IOPS 性能も悪化します。IOPS 性能が悪化している場合は、ホストからの書き込み I/O を抑えてください。



注意

データの一貫性を保つため、スナップショットの取得が完了するまでの間、ホスト I/O を停止してください。OS 用システムディスクのボリュームの場合は、OS をシャットダウンしてからスナップショットを取得してください。データ用ディスクのボリュームの場合は、ファイルキャッシュのディスクへの強制書き出しとドライブへの書き込み停止を組み合わせる(例えば sync コマンドと fsfreeze コマンド)、またはアンマウントを実施したあとでスナップショットを取得してください。スナップショットの取得が完了したらホスト I/O を再開してください。OS によってホスト I/O の停止方法は異なるため、使用している OS の手順に従って実施してください。

前提条件

- 実行に必要なロール : Storage
- VPS 内のボリュームについてスナップショットの取得をする場合 : 当該 VPS のスコープ

操作手順

1. マルチテナンシー機能を利用していない場合、またはマルチテナンシー機能を利用してシステムスコープ内のボリュームについてスナップショットの取得をする場合、この手順は実施不要です。次の手順に進んでください。

VPS 内のボリュームについてスナップショットの取得をする場合、VPS の ID を確認します。

CLI を使い、VPS を名前で指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

2. スナップショットの複製元となるボリュームの ID を確認します。

CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

3. 複製元ボリュームの ID を指定して S-VOL 情報の一覧を取得し、snapshotStatus が "Restoring" のボリュームが存在しないことを確認します。

また、複製先ボリュームについて、ID を確認し、snapshotStatus が "Prepared" であることを確認します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : GET /v1/objects/volumes/<id>/snapshot-volumes

CLI : snapshot_volume_list

確認できたら次の手順に進みます。

4. スナップショットを取得します。

複製先のボリュームの ID と operationType パラメーターに "Finalize" を指定してコマンドを実行します。operationType パラメーターに "Finalize" を指定した場合は、QoS パラメーター、および複製元のボリュームの ID や名前を指定することはできません。

CLI を使う場合のボリュームの ID の代わりに名前が指定できます。また、パラメーターは --operation_type、指定値は "Finalize" になります。

REST API : POST /v1/objects/volumes/actions/create-snapshot/invoke

CLI : volume_create_snapshot

コマンド実行後に表示されるジョブの ID を確認します。

5. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

6. 複製先ボリュームの情報を取得して、snapshotStatus が "Normal" になったことを確認します。

REST API : GET /v1/objects/volumes/<id>

CLI : volume_show

手順 5 を実施後、snapshotStatus が変わるまで 1 分程度掛かることがあります。

snapshotStatus の変化を確認する場合は、1 分ほど経過してから再度確認してください。

18.4 スナップショットを削除する

不要になったスナップショットボリュームを削除します。

VSP One SDS Block Administrator からはスナップショットボリュームを削除できません。

以下に留意して実施してください。

- スナップショットボリュームとコンピュータノード間のパス(ボリュームパス)が設定されている場合、スナップショットボリュームは削除できません。削除する前に、スナップショットボリュームとコンピュータノードの接続を解除してください。
- 当該スナップショットが **Prepared**、**Normal**、または **Error** 状態のときのみ削除できます。
- 当該スナップショットを複製元とするスナップショットが存在する場合は削除できません。
- S-VOL を削除する場合は、スナップショット削除のコマンドで削除します。
- P-VOL を削除する場合は、削除対象の P-VOL から作成されたすべてのスナップショットボリューム(S-VOL)を、スナップショットの削除コマンドで削除したあと、削除対象の P-VOL(S-VOL が削除されたため、この時点では通常ボリュームに変化)を、ボリュームの削除コマンドで削除します。
- P/S-VOL を削除する場合は、削除対象の P/S-VOL から作成されたすべてのスナップショットボリューム(S-VOL)を、スナップショットの削除コマンドで削除したあと、削除対象の P/S-VOL(S-VOL が削除されたため、この時点では S-VOL に変化)を、スナップショットの削除コマンドで削除します。



注意

- 「構成バックアップを行う <<Bare metal>> <<Cloud for AWS>>」に従って、ストレージクラスター構成のリストアを実施してもスナップショットを元に戻すことはできません。復元されたスナップショットボリュームとボリュームパスは、システム管理者または利用者によってすべて削除する必要があります。
- スナップショットツリーの一部のスナップショットを削除しても、ストレージプール内のスナップショットボリュームのデータとして割り当てられていた領域は解放されないため、ストレージプールの使用量は減りません。解放されなかった領域は、新たにスナップショットボリュームのデータを格納するときに再度使用されます。ストレージプールの使用量を削減したい場合は、該当するスナップショットツリーに作成されたスナップショットをすべて削除する必要があります。

前提条件

- 実行に必要なロール : **Storage**
- VPS 内のスナップショットボリュームを削除する場合 : 当該 VPS のスコープ

操作手順

- マルチテナンシー機能を利用していない場合、またはマルチテナンシー機能を利用してシステムスコープ内のスナップショットボリュームを削除する場合、この手順は実施不要です。次の手順に進んでください。

VPS 内のスナップショットボリュームを削除する場合、VPS の ID を確認します。

CLI を使い、VPS を名前で指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

- P-VOL または S-VOL のボリュームの ID を確認します。

CLI を使い P-VOL と S-VOL を名前で指定する場合は、P-VOL と S-VOL の名前を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

3. 削除するスナップショットボリュームの情報を取得して、snapshotStatus が "Prepared"、"Normal"、"Error" いずれかであることを確認します。

ボリュームの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : GET /v1/objects/volumes/<id >

CLI : volume_show

確認できたら次の手順に進みます。

4. スナップショットボリュームを削除します。

削除する S-VOL のボリュームの ID を指定してコマンドを実行します。

CLI を使う場合は S-VOL の ID の代わりに名前が指定できます。

REST API : POST /v1/objects/volumes/actions/delete-snapshot/invoke

CLI : volume_delete_snapshot

コマンド実行後に表示されるジョブの ID を確認します。

5. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

6. S-VOL 情報の一覧を取得して、S-VOL が削除されたことを確認します。

P-VOL のボリューム ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : GET /v1/objects/volumes/<id >/snapshot-volumes

CLI : snapshot_volume_list



メモ

S-VOL の snapshotStatus が "Error" になり、当該 S-VOL を指定してもスナップショット削除のコマンドが失敗してしまう場合には、REST API では masterVolumeId と snapshotTree、CLI では --master_volume_id と --snapshot_tree に、それぞれ P-VOL のボリュームの ID と true を指定してスナップショット削除のコマンドを実行することで、P-VOL から作成されたすべての S-VOL を一度に削除します。このとき、当該 P-VOL のツリーに存在するスナップショットボリュームに対して先行操作したコマンドのジョブが失敗する場合があります。また、当該コマンドのジョブも失敗する場合があります。ジョブが失敗した場合は、当該コマンドを再度実行してください。

実行方法については「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」の「POST /v1/objects/volumes/actions/delete-snapshot/invoke」または「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」の「volume_delete_snapshot」を参照してください。

18.5 スナップショットからのボリューム復元

スナップショットからボリュームを復元する方法を説明します。

18.5.1 スナップショットからボリュームを復元する <<Bare metal>>

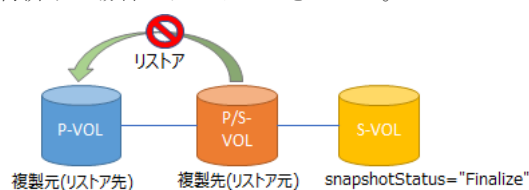
この項での記述内容は Bare metal モデルに適用されます。

複製先ボリュームのデータを用いて、複製元ボリュームのデータを復元する操作をスナップショットのリストアといいます。

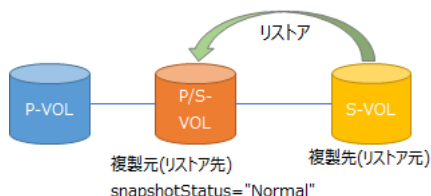
リストアを開始して、**snapshotStatus** が **Restoring** 状態になると、リストアのコピーが未完了であっても、リストア先のボリュームのデータは、仮想的にリストア元のボリュームのデータが反映された状態になり、復元後のデータに即座にアクセスできます。

リストア元のボリュームはリストアの開始によってアクセスが抑止されます。リストアが完了すると、リストア元のボリュームは **Prepared** 状態に遷移します。**Prepared** 状態に遷移したボリュームは、スナップショット取得準備操作を実施することなく、次のスナップショット取得操作を実施できます。

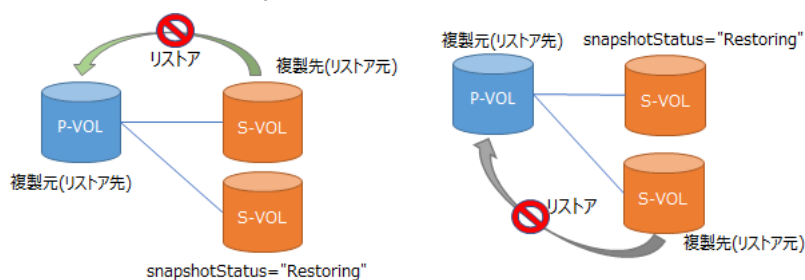
- 複製先(リストア元)の **snapshotStatus** が **"Normal"** のときのみリストアできます。
- カスケード構成における、複製先(リストア元)ボリュームを複製元とするスナップショットが取得済みの場合はリストアできません。



- カスケード構成における、複製元(リストア先)ボリュームがスナップショットの場合、複製元(リストア先)の **snapshotStatus** が **"Normal"** のときのみリストアできます。



- 複製元のボリュームが共有されている構成の場合、複製元(リストア先)ボリュームの配下にすでに **snapshotStatus** が **"Restoring"** のスナップショットが存在する場合は、新たなリストアを開始することはできません。



universalReplicatorAttribute が **"S-VOL"** のボリュームは、スナップショットからはリストアできません。RAID Manager で、Universal Replicator ペアの P-VOL と S-VOL を入れ替えるとリストアできます。



メモ

- リストアの実施によって、リストア元ボリュームのデータがリストア先ボリュームに書き込まれます。このとき、リストア先ボリュームの書き込み前のデータはストレージプールにコピーされるため、ストレージプールの使用量が増えます。リストア中に、ストレージプールの満杯によってスナップショットボリュームのデータが消失すると、リストア先ボリュームのデータも使用できなくなります。リストア実施時には、リストアに必要な容量があるかを、下記の手順 1 から 6 で確認し、不足する場合は必要な空き容量を確保してください。

- ・ リストアは、リストア先ボリュームの IOPS が低い状態のときに実施してください。
リストア先ボリュームのデータがライト I/O によって更新されると、差分データのコピーが動作します。さらに、リストアによるリストア元ボリュームからリストア先ボリュームへのコピーも動作します。これらのコピーが動作することで、ストレージノード内の負荷が上昇して、ライト I/O の IOPS 性能だけでなく、リード I/O の IOPS 性能も悪化するためです。
- ・ 負荷が高まることによって、ストレージノードの内部リソースの使用率が増加した場合、リストアが一時的に停止することがあります。その際は、リストアを一時的に停止したことを示すイベントログ **KARS06160-I** が出力されます。ストレージノードの内部リソースの使用率が低下すると、リストアは自動的に再開します。
- ・ リストア実施中に、冗長構成によって許容される障害数を超える障害が発生した場合は、リストア処理が失敗することがありますが、ノード回復後に失敗したリストアの処理は自動的に再開されます。こうしたケースにおいては、リストアの実施状況を、ボリューム情報の **snapshotStatus** で確認してください。
snapshotStatus が **"Restoring"** の場合はリストアが実行中です。完了するまでお待ちください。
snapshotStatus が **"Prepared"** の場合はリストアが完了しています。



注意

- ・ リストア実施中に、ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した場合、キャッシュ保護付きライトバックモード無効時は、スナップショットボリュームのデータが消失することがあります。キャッシュ保護付きライトバックモード有効時は、スナップショットボリュームのデータは保護されます。ただし、キャッシュ保護用メタデータの冗長度を超える障害が発生している状態で、ストレージクラスターの障害が発生した場合は、キャッシュ保護付きライトバックモード有効時でも、スナップショットボリュームのデータは保護されません。
- ・ リストア実施中に、冗長度を超える障害(ネットワークスイッチまたは電源の障害、ストレージノードの誤ったシャットダウン操作など)によって、ストレージクラスターの障害が発生した場合は、スナップショットボリュームのデータが消失するとともに、リストア先ボリュームのデータも使用できなくなります。リストア実施前には、リストア先ボリュームのデータを、ホスト経由などで別の通常ボリュームにコピーして、バックアップを取っておくこと、およびリストア先ボリュームについて「ボリュームの個別情報を取得する」で得られる情報を記録しておくことをお勧めします。
- ・ データの一貫性を保つため、スナップショットのリストアが完了するまでの間、ホスト I/O を停止してください。OS 用システムディスクのボリュームの場合は、OS をシャットダウンしてから、リストア元ボリューム(S-VOL)からリストアしてください。データ用ディスクのボリュームの場合は、アンマウントしたあとでスナップショットをリストアしてください。ここでは **fsfreeze** コマンドは使用できません。スナップショットのリストアが完了したらファイルシステムをマウントしてホスト I/O を再開してください。OS によってホスト I/O の停止方法は異なります。使用している OS の手順に従って実施してください。

前提条件

- ・ 実行に必要なロール : **Storage**
- ・ VPS 内のボリュームについて、スナップショットからボリュームを復元する場合 : 当該 VPS のスコープ

操作手順

1. マルチテナンシー機能を利用していない場合、またはマルチテナンシー機能を利用してシステムスコープ内のスナップショットからボリュームを復元する場合、この手順は実施不要です。次の手順に進んでください。

VPS 内のボリュームについて、スナップショットからボリュームを復元する場合、VPS の ID を確認します。

CLI を使い、VPS を名前で指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : **vps_list**

2. ボリュームの一覧情報を取得して、リストア元ボリュームの ID と論理総容量[MiB] (**totalCapacity**)を確認します。

以降の手順で、CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

また、リストア元ボリュームの `snapshotStatus` が "Normal" であることを確認します。

REST API : GET /v1/objects/volumes

CLI : `volume_list`

リストア元ボリュームの `snapshotStatus` が "Normal" であることが確認できたら次の手順に進みます。

3. リストア先ボリューム(P-VOL)の ID を取得します。

「ボリュームに対する P-VOL 情報を取得する」を参照して実施します。

4. リストア先ボリュームの情報を取得して、リストア先ボリュームを管理するストレージコントローラーの ID を確認します。

REST API : GET /v1/objects/volumes/<id >

CLI : `volume_show`

5. 手順 4 で確認した ID のストレージコントローラーの情報を取得して、当該ストレージコントローラー上で管理しているストレージプールの使用容量[MiB](`usedCapacity`)と最大論理容量[MiB](`allocatableCapacity`)を確認します。

REST API : GET /v1/objects/storage-controllers/<id >

CLI : `storage_controller_show`

6. 手順 5 で確認した `allocatableCapacity`[MiB]と `usedCapacity`[MiB]の差が、手順 2 で確認した `totalCapacity`[MiB]以上であることを確認します。

確認できたら次の手順に進みます。

7. リストア先のボリュームを指定して S-VOL 情報の一覧を取得し、`snapshotStatus` が "Restoring" のボリュームが存在しないことを確認します。

REST API : GET /v1/objects/volumes/<id >/snapshot-volumes

CLI : `snapshot_volume_list`

確認できたら次の手順に進みます。

8. リストア先のボリュームまたはリストア元のボリュームに対してホスト I/O を実施している場合は、データの一貫性を保つためホスト I/O を停止します。

OS によってホスト I/O の停止方法は異なります。使用している OS の手順に従って実施してください。

9. OS 用システムディスクのボリュームの場合は、OS をシャットダウンします。

データ用ディスクのボリュームの場合は、アンマウントを実施してください。

ここでは `fsfreeze` コマンドは使用できません。

10. スナップショットのリストアを実行します。

リストア元ボリューム(S-VOL)の ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : POST /v1/objects/volumes/actions/restore-snapshot/invoke

CLI : `volume_restore_snapshot`

コマンド実行後に表示されるジョブの ID を確認します。

また、リストアの進捗は、ボリューム情報の `snapshotProgressRate`[%]で確認できます。ボリューム情報の取得方法は、このマニュアルの「ボリューム情報の個別取得」を参照してください。ボリュームの ID には、リストア元ボリュームの ID を指定してください。

11. ジョブの `state` を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

12. リストア元ボリューム(S-VOL)の情報を取得して、snapshotStatus が"Prepared"になったことを確認します。

REST API : GET /v1/objects/volumes/<id >

CLI : volume_show

手順 11 を実施後、snapshotStatus が変わるまで 1 分程度掛かることがあります。

snapshotStatus の変化を確認する場合は、1 分ほど経過してから再度確認してください。

13. OS 用システムディスクのボリュームの場合は、OS を起動します。

データ用ディスクのボリュームの場合は、手順 9 でアンマウントしていたファイルシステムを再度マウントしてください。

必要に応じてホスト I/O を再開してください。

18.5.2 スナップショットからボリュームを復元する<<Cloud>>

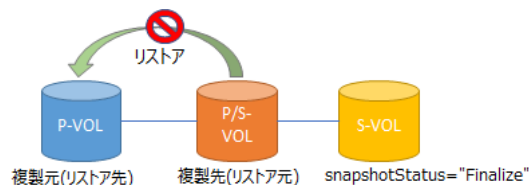
この項での記述内容は Cloud モデルに適用されます。

複製先ボリュームのデータを用いて、複製元ボリュームのデータを復元する操作をスナップショットのリストアといいます。

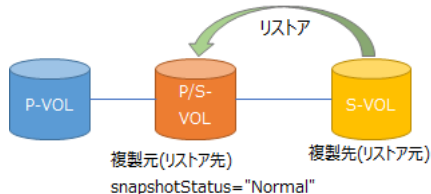
リストアを開始して、snapshotStatus が Restoring 状態になると、リストアのコピーが未完了であっても、リストア先のボリュームのデータは、仮想的にリストア元のボリュームのデータが反映された状態になり、復元後のデータに即座にアクセスできます。

リストア元のボリュームはリストアの開始によってアクセスが抑止されます。リストアが完了すると、リストア元のボリュームは Prepared 状態に遷移します。Prepared 状態に遷移したボリュームは、スナップショット取得準備操作を実施することなく、次のスナップショット取得操作を実施できます。

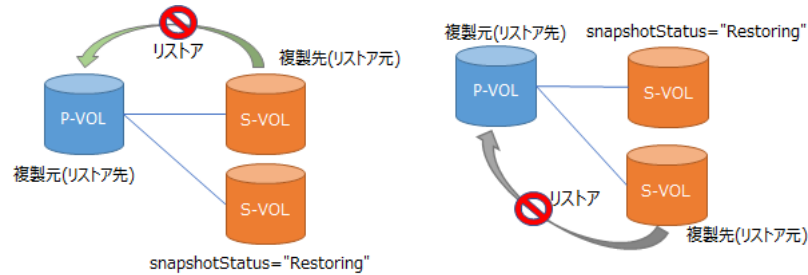
- 複製先(リストア元)の snapshotStatus が"Normal"のときのみリストアできます。
- カスケード構成における、複製先(リストア元)ボリュームを複製元とするスナップショットが取得済みの場合はリストアできません。



- カスケード構成における、複製元(リストア先)ボリュームがスナップショットの場合、複製元(リストア先)の snapshotStatus が"Normal"のときのみリストアできます。



- 複製元のボリュームが共有されている構成の場合、複製元(リストア先)ボリュームの配下にすでに snapshotStatus が"Restoring"のスナップショットが存在する場合は、新たなリストアを開始することはできません。



universalReplicatorAttribute が"S-VOL"のボリュームは、スナップショットからはリストアできません。RAID Manager で、Universal Replicator ペアの P-VOL と S-VOL を入れ替えるとリストアできます。



メモ

- リストアの実施によって、リストア元ボリュームのデータがリストア先ボリュームに書き込まれます。このとき、リストア先ボリュームの書き込み前のデータはストレージプールにコピーされるため、ストレージプールの使用量が増えます。リストア中に、ストレージプールの満杯によってスナップショットボリュームのデータが消失すると、リストア先ボリュームのデータも使用できなくなります。リストア実施時には、リストアに必要な容量があるかを、下記の手順 1 から 5 で確認し、不足する場合は必要な空き容量を確保してください。
- リストアは、リストア先ボリュームの IOPS が低い状態のときに実施してください。リストア先ボリュームのデータがライト I/O によって更新されると、差分データのコピーが動作します。さらに、リストアによるリストア元ボリュームからリストア先ボリュームへのコピーも動作します。これらのコピーが動作することで、ストレージノード内の負荷が上昇して、ライト I/O の IOPS 性能だけでなく、リード I/O の IOPS 性能も悪化するためです。
- 負荷が高まることによって、ストレージノードの内部リソースの使用率が増加した場合、リストアが一時的に停止することがあります。その際は、リストアを一時的に停止したことを示すイベントログ KARS06160-I が出力されます。ストレージノードの内部リソースの使用率が低下すると、リストアは自動的に再開します。
- リストア実施中に、冗長構成によって許容される障害数を超える障害が発生した場合は、リストア処理が失敗することがありますが、ノード回復後に失敗したリストアの処理は自動的に再開されます。こうしたケースにおいては、リストアの実施状況を、ボリューム情報の snapshotStatus で確認してください。snapshotStatus が"Restoring"の場合はリストアが実行中です。完了するまでお待ちください。snapshotStatus が"Prepared"の場合はリストアが完了しています。



注意

- リストア実施中に、ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した場合、キャッシュ保護付きライトバックモード無効時は、スナップショットボリュームのデータが消失することがあります。キャッシュ保護付きライトバックモード有効時は、スナップショットボリュームのデータは保護されます。ただし、キャッシュ保護用メタデータの冗長度を超える障害が発生している状態で、ストレージクラスターの障害が発生した場合は、キャッシュ保護付きライトバックモード有効時でも、スナップショットボリュームのデータは保護されません。
- リストア実施中に、冗長度を超える障害(複数のストレージノード上にある VM インスタンスの障害や誤ったシャットダウン操作など)によって、ストレージクラスターの障害が発生した場合は、スナップショットボリュームのデータが消失するとともに、リストア先ボリュームのデータも使用できなくなります。リストア実施前には、リストア先ボリュームのデータを、ホスト経由などで別の通常ボリュームにコピーして、バックアップを取っておくこと、およびリストア先ボリュームについて「ボリューム情報を個別に取得する」で得られる情報を記録しておくことをお勧めします。
- データの一貫性を保つため、スナップショットのリストアが完了するまでの間、ホスト I/O を停止してください。OS 用システムディスクのボリュームの場合は、OS をシャットダウンしてから、リストア元ボリュ

ーム(S-VOL)からリストアしてください。データ用ディスクのボリュームの場合は、アンマウントしたあとでスナップショットをリストアしてください。ここでは **fsfreeze** コマンドは使用できません。スナップショットのリストアが完了したらファイルシステムをマウントしてホスト I/O を再開してください。OS によってホスト I/O の停止方法は異なります。使用している OS の手順に従って実施してください。

前提条件

- 実行に必要なロール：Storage

操作手順

1. ボリューム情報の一覧を取得して、リストア元ボリュームの ID と論理総容量[MiB] (totalCapacity)を確認します。
以降の手順で、CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。
また、リストア元ボリュームの snapshotStatus が"Normal"であることを確認します。
REST API : GET /v1/objects/volumes
CLI : volume_list
リストア元ボリュームの snapshotStatus が"Normal"であることが確認できたら次の手順に進みます。
2. リストア先ボリューム(P-VOL)の ID を取得します。
「ボリュームに対する P-VOL 情報を取得する」を参照して実施します。
3. リストア先ボリュームの情報を取得して、リストア先ボリュームを管理するストレージコントローラーの ID を確認します。
REST API : GET /v1/objects/volumes/<id >
CLI : volume_show
4. 手順 3 で確認した ID のストレージコントローラーの情報を取得して、当該ストレージコントローラー上で管理しているストレージプールの使用容量[MiB](usedCapacity)と最大論理容量[MiB](allocatableCapacity)を確認します。
REST API : GET /v1/objects/storage-controllers/<id >
CLI : storage_controller_show
5. 手順 4 で確認した allocatableCapacity[MiB]と usedCapacity[MiB]の差が、手順 1 で確認した totalCapacity[MiB]以上であることを確認します。
確認できたら次の手順に進みます。
6. リストア先のボリュームを指定して S-VOL 情報の一覧を取得し、snapshotStatus が "Restoring"のボリュームが存在しないことを確認します。
REST API : GET /v1/objects/volumes/<id >/snapshot-volumes
CLI : snapshot_volume_list
確認できたら次の手順に進みます。
7. リストア先のボリュームまたはリストア元のボリュームに対してホスト I/O を実施している場合は、データの一貫性を保つためホスト I/O を停止します。
OS によってホスト I/O の停止方法は異なります。使用している OS の手順に従って実施してください。
8. OS 用システムディスクのボリュームの場合は、OS をシャットダウンします。
データ用ディスクのボリュームの場合は、アンマウントを実施してください。
ここでは **fsfreeze** コマンドは使用できません。
9. スナップショットのリストアを実行します。
リストア元ボリューム(S-VOL)の ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : POST /v1/objects/volumes/actions/restore-snapshot/invoke

CLI : volume_restore_snapshot

コマンド実行後に表示されるジョブの ID を確認します。

また、リストアの進捗は、ボリューム情報の `snapshotProgressRate[%]` で確認できます。ボリューム情報の取得方法は、このマニュアルの「ボリューム情報の個別取得」を参照してください。ボリュームの ID には、リストア元ボリュームの ID を指定してください。

10. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

11. リストア元ボリューム(S-VOL)の情報を取得して、`snapshotStatus` が "Prepared" になったことを確認します。

REST API : GET /v1/objects/volumes/<id>

CLI : volume_show

手順 10 を実施後、`snapshotStatus` が変わるまで 1 分程度掛かることがあります。

`snapshotStatus` の変化を確認する場合は、1 分ほど経過してから再度確認してください。

12. OS 用システムディスクのボリュームの場合は、OS を起動します。

データ用ディスクのボリュームの場合は、手順 8 でアンマウントしていたファイルシステムを再度マウントしてください。

必要に応じてホスト I/O を再開してください。

18.6 ボリュームに対する P-VOL 情報を取得する

S-VOL の作成元となった P-VOL について、以下の情報を取得します。

- `masterVolumeId` : P-VOL のボリュームの ID(uuid)
- `vpsId` : ボリュームが所属する VPS の ID
- `vpsName` : ボリュームが所属する VPS の名前
- `qosParam` : QoS に関するパラメーター
 - `upperLimitForIops` : ボリューム性能上限[IOPS]
 - `upperLimitForTransferRate` : ボリューム性能上限[MiB/sec]
 - `upperAlertAllowableTime` : ボリューム性能上限に関するアラートしきい値[sec]
 - `upperAlertTime` : ボリュームの性能上限を継続して超過した場合に性能上限アラート条件に合致した最終時刻(UTC)

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. S-VOL のボリュームの ID を確認します。

CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

2. P-VOL 情報を取得します。

S-VOL のボリュームの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : GET /v1/objects/volumes/<id >/master-volume

CLI : master_volume_show

18.7 ボリュームに対する S-VOL 情報の一覧を取得する

P-VOL から作成された S-VOL 情報の一覧を取得します。以下の情報が得られます。

- snapshotVolumeId : S-VOL であるボリュームの ID(uuid)
- snapshotVolumeName : S-VOL であるボリュームの名前
- snapshotVolumeNickname : S-VOL であるボリュームのニックネーム
- statusSummary : 当該 S-VOL の状態のサマリー
- status : ボリュームの状態
- snapshotStatus : スナップショットの状態
snapshotStatus が変わるまで 1 分程度掛かることがあります。snapshotStatus の変化を確認する場合は、1 分ほど経過してから再度確認してください。
- snapshotProgressRate : 当該 S-VOL の取得準備、削除、リストアの進捗率(%)
- snapshotTimestamp : スナップショット作成時点の P-VOL に対して差分データの記録を開始した時刻
- snapshotType : スナップショット種別
- snapshotConcordanceRate : 当該ボリュームと 1 つ新しい世代の S-VOL または複製元ボリューム(P-VOL)との一致率[%]
- isWrittenInSvol : コンピュートノード(ホスト)から当該ボリュームへの書き込み有無
- vpsId : ボリュームが所属する VPS の ID
- vpsName : ボリュームが所属する VPS の名前
- qosParam : QoS に関するパラメーター
 - upperLimitForIops : ボリューム性能上限[IOPS]
 - upperLimitForTransferRate : ボリューム性能上限[MiB/sec]
 - upperAlertAllowableTime : ボリューム性能上限に関するアラートしきい値[sec]
 - upperAlertTime : ボリュームの性能上限を継続して超過した場合に性能上限アラート条件に合致した最終時刻(UTC)

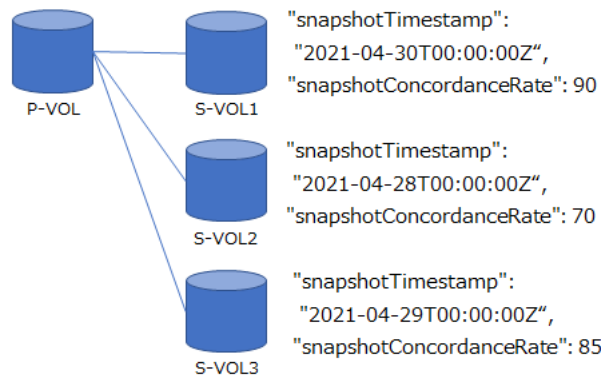


メモ

S-VOL の一致率は、以下ようになります。世代の新旧は snapshotTimestamp で確認できます。

- 最新世代(S-VOL1)の snapshotConcordanceRate[%]は、P-VOL との一致率
- S-VOL2 の snapshotConcordanceRate[%]は、1 つ新しい世代の S-VOL3 との一致率
- S-VOL3 の snapshotConcordanceRate[%]は、1 つ新しい世代の S-VOL1 との一致率

P-VOL に書き込みがあった場合、最新世代の S-VOL1 の一致率は、P-VOL への書き込み量が差分データ量として反映されるため下がって見えます。S-VOL に書き込みがあった場合、書き込んだ S-VOL の一致率だけが下がります。



前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. マルチテナンシー機能を利用していない場合、またはマルチテナンシー機能を利用してシステムスコープ内のボリュームに対する S-VOL 情報の一覧を取得する場合、この手順は実施不要です。次の手順に進んでください。

VPS 内のボリュームに対する S-VOL 情報の一覧を取得する場合、VPS の ID を確認します。

CLI を使い、VPS を名前で指定する場合は、VPS の名前を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

2. P-VOL のボリュームの ID を確認します。

CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

3. S-VOL 情報の一覧を取得します。

P-VOL のボリュームの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : GET /v1/objects/volumes/<id>/snapshot-volumes

CLI : snapshot_volume_list



メモ

スナップショットボリュームの削除またはリストアの実施中に、ストレージクラスターが停止した場合、削除またはリストアのジョブは中断または失敗によって消滅して、ストレージクラスターは停止します。ストレージクラスターを起動すると、削除またはリストアの処理は、自動的に再開されます。

スナップショットボリュームの削除またはリストアの実施状況は、ボリューム情報を取得し snapshotStatus を確認してください。削除処理が終了すると snapshotStatus は "Empty" に、リストア処理が終了すると

"Prepared" になります。

再開した削除処理によって、スナップショットボリュームが削除され、snapshotStatus が "Empty" になっていても S-VOL は残っています(ストレージクラスターが停止した場合には自動では削除されません)。S-VOL を削除するために、スナップショットボリュームの削除を再度実施してください。

ユーザーを管理する

- 19.1 ユーザー管理の概要
- 19.2 ユーザー情報の一覧を取得する
- 19.3 ユーザーの詳細情報を取得する
- 19.4 ユーザーを作成する
- 19.5 ユーザー情報を編集する
- 19.6 ユーザーを削除する
- 19.7 自身のパスワードを変更する
- 19.8 ユーザーをユーザーグループに追加する
- 19.9 ユーザーをユーザーグループから削除する
- 19.10 ユーザーグループの一覧を取得する
- 19.11 ユーザーグループの詳細情報を取得する
- 19.12 ユーザーグループを作成する
- 19.13 ユーザーグループ情報を編集する
- 19.14 ユーザーグループを削除する
- 19.15 外部認証サーバーを利用する
- 19.16 外部認証サーバーの設定を取得する
- 19.17 外部認証サーバーのルート証明書を取得する

19.1 ユーザー管理の概要

VSP One SDS Block のストレージクラスターの操作や設定を行うユーザーは、VSP One SDS Block に登録が必要です。例えば、REST API の場合は、リクエストヘッダーの Authorization に、"<ユーザー ID>:<パスワード>"を Base64 でエンコードした値を指定します。CLI の場合は、--user オプションにユーザー ID を指定して実行し、対話形式でパスワードを入力します。

コンソールインターフェイスでは、対話形式でユーザー ID とパスワードを入力します。

ビルトインユーザーグループとビルトインユーザー

VSP One SDS Block には、SecurityAdministrators や ServiceAdministrators など、6 つのユーザーグループ(ビルトインユーザーグループ)があらかじめ登録されています。また、ビルトインユーザーとして、admin が登録されています。

項目	説明
ユーザー ID	admin
ユーザーのオブジェクト ID	admin
パスワード	hsds-admin 初回操作時にパスワード変更が求められます。
所属するユーザーグループ ID	SystemAdministrators
所属するユーザーグループのオブジェクト ID	SystemAdministrators

ユーザーとグループユーザーの初期状態を図示すると以下のようになります。ユーザーグループには、操作権限を規定するロール(Storage、Service、Security など)が設定されています。

ビルトインユーザーグループは削除できません。設定されているロールの変更はできません。また、ビルトインユーザーは削除できません。

AuditAdministrators □-ル: Audit, Monitor	StorageAdministrators □-ル: Storage, RemoteCopy, Resource	ServiceAdministrators □-ル: Storage, RemoteCopy, Service
SecurityAdministrators □-ル: Security, Monitor	MonitorUsers □-ル: Monitor	SystemAdministrators  admin □-ル: Audit, Security, Storage, RemoteCopy, Monitor, Service, Resource

ビルトインユーザーはコンソールインターフェイスを使用できます。

セットアップ完了後の状態

ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」に従って、セットアップが完了したあとは、システムの運用に必須であるユーザーが、SecurityAdministrators と ServiceAdministrators にそれぞれ作られています。作成されたユーザーの、ユーザー ID、ユーザーオブジェクト ID、パスワードについては、これらユーザーを作成した管理者の方にお問い合わせください。その後、必要に応じて、自身のパスワードを変更してください。

また、セットアップ完了後、admin ユーザーは無効になっています。必要であれば、有効に設定できます。

AuditAdministrators ロール: Audit, Monitor	StorageAdministrators ロール: Storage, RemoteCopy, Resource	ServiceAdministrators ロール: Storage, RemoteCopy, Service
SecurityAdministrators ロール: Security, Monitor	MonitorUsers ロール: Monitor	SystemAdministrators admin ロール: Audit, Security, Storage, RemoteCopy, Monitor, Service, Resource

ユーザーの作成とユーザーグループ

ユーザーの操作権限は、所属するユーザーグループに設定されているロールによって決まります。例えば、ユーザーの作成は、Security ロールを持つユーザーグループに所属するユーザーにのみ可能です。

また、マルチテナンシー機能を利用する場合、ユーザーが操作できる対象は、所属するユーザーグループに設定されているスコープにより制限できます。スコープについては、このマニュアルの「マルチテナンシーを構成する<<Bare metal>>」を参照してください。

新規に作成されたユーザーが最初に行うことができる操作はパスワード変更だけです。パスワードの変更後には、与えられたロールに許された操作が実行できます。なお、セットアップ中に作成されたユーザーは、パスワード変更が行われています。

ユーザーは、複数のユーザーグループに登録できます。

ユーザーグループは新規に作成できます。

ロールと実行できる操作

ロールによって、実行できる操作は以下のように異なります。システムの運用方針に従ってユーザーを作成してください。

マルチテナンシー構成をとっている場合は、下表に記載のロール以外に、VPS 管理者のロール (VpsSecurity、VpsStorage、VpsMonitor)があります。マルチテナンシー構成については、このマニュアルの「マルチテナンシーを構成する<<Bare metal>>」を参照してください。



注意

Security ロールを持つ有効なユーザーのパスワードは絶対に紛失しないようにしてください。Security ロールを持つ有効なすべてのユーザーのパスワードを紛失した場合、システムの運用に必須であるアカウント管理などの操作が実行できなくなります。

ロール	実行できる主な操作
Security	監査ログファイルの作成・ダウンロード、CHAP 認証、ユーザー管理、セッション情報の取得、イベントログ設定、監査ログ設定、外部認証サーバー連携、許可リスト設定、サーバー証明書のインポート、VSP One SDS Block Administrator のログイン画面と CLI Basic 認証時に表示するメッセージの設定、ターゲット動作のコンピュートポートの認証設定、暗号化管理など
Storage	ライセンス管理、ボリューム管理、スナップショット管理、コンピュートノード管理、コンピュートノードのイニシエーター情報・パス情報の登録・削除、ボリュームとコンピュートノードの接続・解除、コンピュートポートの設定、ストレ

ロール	実行できる主な操作
	ージブールの容量拡張、容量バランス、ドライブ管理、性能情報・容量情報の取得、ドライブデータ再配置の中断と再開など
RemoteCopy	リモートパスグループ操作、ジャーナルグループ操作、RAID Manager によるペア操作
Monitor	性能情報・容量情報の取得、容量バランスの設定の取得、ライセンス情報の取得など
Audit	監査ログファイルの作成・ダウンロード (VSP One SDS Block Administrator にログインするには、Audit ロール以外のロールが必要です。)
Service	ストレージノード管理(保守、増設、減設など)、ストレージクラスターの停止、ストレージソフトウェアのアップデート、ドライブデータ再配置の中断と再開など
Resource	VPS の作成・編集・削除 Resource ロールを持つユーザーが、VSP One SDS Block Administrator を使う場合は、Monitor ロールを割り当てることをお勧めします。これによって、Resource ロールの参照可能範囲まで参照できるようになります。



メモ

- 以下の操作は、ロールによる実行制限はありません。
 - 自身のセッション参照/生成/削除
 - VSP One SDS Block Administrator のログイン画面および CLI Basic 認証時の警告バナーに表示するメッセージの取得
 - API バージョンの取得
 - ジョブ情報の取得
 - ストレージクラスターマスター(プライマリー)であるかを示す情報の取得
 - ストレージクラスターのネットワーク設定
 - 自身のユーザー情報の取得
 - 自身のパスワード変更
- 以下の操作は、Security、Storage、RemoteCopy、Monitor、Service、または Resource のロールを持つユーザーが実行できます。
 - ストレージプールの情報取得
 - ドライブ情報の取得
 - ストレージノードのネットワーク設定の取得
 - リモート iSCSI ポートの情報取得
 - リモートパスグループの情報取得
- 以下の操作は、Storage、RemoteCopy、Monitor、または Resource のロールを持つユーザーが実行できます。
 - ライセンス情報の取得
- 以下の操作は、Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource のロールを持つユーザーが実行できます。
 - ヘルスステータスの取得
 - プロテクションドメイン情報の取得
 - ストレージクラスター情報の取得
 - ストレージノード情報の取得
 - フォールトドメイン情報の取得

- 管理ポート、ストレージノード間ポートの情報取得
- ストレージクラスターの時刻設定の取得
- 以下の操作は、Security、Storage、RemoteCopy、Monitor、Service、Resource、VpsSecurity、VpsStorage、または VpsMonitor のロールを持つユーザーが実行できます。
 - ボリューム情報の取得
 - S-VOL 情報、P-VOL 情報の取得
 - コンピュートノードの情報取得
 - コンピュートノードのイニシエーター情報の取得
 - コンピュートノードのパス情報の取得
 - ボリュームとコンピュートノードの接続情報の取得
 - ジャーナルの情報取得
- 以下の操作は、Security、Storage、RemoteCopy、Monitor、Service、Resource、VpsStorage、または VpsMonitor のロールを持つユーザーが実行できます。
 - コンピュートポートの情報の取得

Basic 認証・セッション認証・チケット認証

ストレージクラスターの操作を、例えば、REST API で行う場合、リクエストヘッダーの Authorization に認証情報を指定して、VSP One SDS Block に認証リクエストを送信します。

VSP One SDS Block では、Basic 認証とセッション認証およびチケット認証という、3 種類の認証方式がサポートされます。

Basic 認証は、ユーザー ID とパスワードを認証情報とする方式です。Basic 認証ではリクエストのたびに認証が行われます。

セッション認証は、トークンを認証情報とする方式であり、一定期間、認証を省略できます。このため、アプリケーションによる自動操作などに利用するときには有用です。トークンはセッションを生成する REST API や CLI を実行することで得られます。トークンの生成方法は「セッションを生成する」を参照してください。セッションはストレージシステムによって削除される場合があります。詳細は「セッション管理の概要」を参照してください。特に、アプリケーションによる自動操作などに利用する場合は、セッションが削除されると、再度セッションを生成する必要があることに注意してください。

チケット認証は、ストレージノードの停止時や障害発生によって、Basic 認証やセッション認証が使用できない場合の代替手段です。チケット認証を実施する際は、認証チケットを発行した際のユーザー名とパスワードを同時に指定してください。認証チケット、ユーザー名、パスワードの指定の方法は「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」の「認証方式」と「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」の「マスターコマンドオプション」を参照してください。

認証チケットの発行と破棄の方法は「認証チケットを管理する」を参照してください。



メモ

認証チケットを利用して、認証が失敗したときは以下を確認してください。

- ユーザー名、パスワードが認証チケット発行時のものと異なっていないか
- 認証チケットの有効期限が切れていないか
- 認証チケット発行時に、ユーザーが認証チケットを使って行うそれぞれの操作に必要なロールを持っていたか
- 別のストレージクラスターで発行されたチケットではないか
- 認証チケット発行後に認証チケットが破棄されていないか

認証チケットが破棄されていた場合は、再度、認証チケットを発行してください。ストレージクラスターの停止中などで認証チケットが再発行できない場合は、サポートセンターに連絡してください。

- VSP One SDS Block で Universal Replicator を使用する場合は、RAID Manager の認証が必要になります。詳細は、「RAID Manager ユーザガイド」の「ユーザ認証機能」または「ユーザ認証」を参照してください。

生成できるセッションの上限数と削除

セッション生成数には上限があり、上限を超えるとコマンドが実行できなくなります。セッション生成数の上限は、マルチテナンシー機能を利用しない場合 64 です。マルチテナンシー機能を利用する場合、VPS に所属しないユーザーのセッションの上限数は 64、VPS に所属するユーザーのセッションの上限数は 436 です。

認証をリクエストした際に、すでにセッションが上限数に達していた場合は 503 Service Unavailable が返却されます。

セッションはユーザー操作によるセッション削除のほか、トークンの有効期限が過ぎた場合、セッションを使用しないままタイムアウト期間を超過した場合などに自動で削除されます。また、当該ユーザーの編集や削除、パスワード変更、ユーザーグループからユーザーの削除、ユーザーの所属グループの編集によっても当該ユーザーのセッションは削除されます。

セッションが削除された場合は、ユーザーによるセッションの生成が必要になります。

ユーザー認証設定とシステム要件

ユーザー認証に適用される設定をユーザー認証設定といいます。ユーザー認証設定にはパスワードの複雑さ、パスワードの有効期限、ロックアウト、セッションに関するパラメーターがあり、設定値は変えられます。「ユーザー認証設定を編集する」を参照してください。

また、以下のシステム要件があります。

項目	要件	備考
ユーザーの最大数	32	ビルトインユーザーや外部認証サーバー上のユーザーを含みます。
ユーザーグループの最大数	32	ビルトイングループや外部認証サーバー上のグループを含みます。
1 ユーザーが所属できるユーザーグループの最大数	8	
ユーザー ID で使用できる文字数と文字種	• 文字数：6～255¹ • 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(! # \$ % ' . @ ^ _ ` { } ~) コンソールインターフェイスの使用を許可するユーザーの場合は以下の制限となります。 • 文字数：6～28 • 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(. _) • 先頭使用可能文字：英大文字(A-Z)、英小文字(a-z)、記号(_)	

項目	要件	備考
パスワードで使用できる文字数と文字種	文字数：1～256 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(!"#\$%&'()*+,-./:;<=>@[¥]^_`{ }~)	パスワードの最小文字数は、ユーザー認証設定で設定できます。ユーザー認証設定でのデフォルトは8です。
ユーザーグループ ID で使用できる文字数と文字種	文字数：1～64 ² 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、記号(!"#\$%&'-.@^_`{ }~)	
1. VSP One SDS Block が連携できる外部認証サーバー上のユーザー名の最大長は 64 文字です。 2. VSP One SDS Block が連携できる外部認証サーバー上のユーザーグループ名の最大長は 64 文字です。		

コンソールインターフェイスのユーザーについて

REST API または CLI によって、コンソールインターフェイスの使用を許可されたユーザーに関する以下の操作を実施すると、その情報は、1 分周期で実施される内部処理によって反映され、イベントログ KARS20067-I が出力されます。このため、反映が終わるまで一定の時間を要します。

- ・ ユーザーの作成
- ・ ユーザー情報の編集
- ・ ユーザーの削除
- ・ 自身のパスワードの変更
- ・ ユーザーグループへのユーザーの追加
- ・ ユーザーグループからのユーザーの削除
- ・ ユーザーグループ情報の編集



メモ

コンソールインターフェイスの使用を許可されたユーザーに関する以下の操作を実施した場合、イベントログは出力されません。

- ・ ユーザー情報を編集したが該当ユーザーが無効(isEnabled が"false")のままの場合
- ・ ユーザー情報を編集しユーザーを無効から有効に変更したが、認証設定での requiresInitialPasswordReset が"true"の場合
- ・ ユーザーをユーザーグループに追加または削除したが、ユーザーのロールに変更がない場合
- ・ ユーザーグループ情報を編集したが、そのグループに属するユーザーのロールに変更がない場合

外部認証サーバーの利用

外部認証サーバーとの連携を設定すると、外部認証サーバーに登録されたユーザー情報を利用して認証できるようになります。連携可能な外部認証サーバーについては、「外部認証サーバーを利用する」を参照してください。

19.2 ユーザー情報の一覧を取得する

登録されているユーザーの情報を一覧で取得します。以下の情報が得られます。

- ・ userId：ユーザー ID
- ・ userObjectId：ユーザーのオブジェクト ID

- passwordExpirationTime : パスワードの有効期限
- isEnabled : ユーザーの有効/無効
- userGroups : ユーザーが所属するユーザーグループ ID の一覧(ユーザーグループ ID、ユーザーグループのオブジェクト ID)
- isBuiltIn : ビルトインユーザーかどうか
- authentication : 認証の種別
- roleNames : ユーザーグループのロール
- isEnabledConsoleLogin : コンソールインターフェイスの使用可否
- vpsId : ユーザーが所属する VPS の ID
- privileges : ユーザーがアクセス可能な VPS 情報の一覧



メモ

外部認証が有効であり、かつ mappingMode を"Group"に設定している場合は、外部認証サーバー上のユーザーの情報は取得されず、authentication が"local"のユーザーの情報のみが取得されます。

前提条件

- 実行に必要なロール : Security

操作手順

1. ユーザー情報の一覧を取得します。
REST API : GET /v1/objects/users
CLI : user_list

19.3 ユーザーの詳細情報を取得する

登録されているユーザーについて、以下の情報を取得します。

外部認証が有効であり、かつ mappingMode を"Group"に設定している場合は、外部認証サーバー上のユーザー ID の情報は取得されません。

- userId : ユーザー ID
- userObjectId : ユーザーのオブジェクト ID
- passwordExpirationTime : パスワードの有効期限
- isEnabled : ユーザーの有効/無効
- userGroups : ユーザーが所属するユーザーグループ ID の一覧(ユーザーグループ ID、ユーザーグループのオブジェクト ID)
- isBuiltIn : ビルトインユーザーかどうか
- authentication : 認証の種別
- roleNames : ユーザーグループのロール
- isEnabledConsoleLogin : コンソールインターフェイスの使用可否
- vpsId : ユーザーが所属する VPS の ID
- privileges : ユーザーがアクセス可能な VPS 情報の一覧

前提条件

- 任意のユーザーの詳細情報を取得するときに必要なロール：Security
自身のユーザー情報を取得するときは、ロールによる実行制限はありません。

操作手順

1. ユーザー ID を確認します。
REST API : GET /v1/objects/users
CLI : user_list
2. ユーザーの詳細情報を取得します。
ユーザー ID を指定してコマンドを実行します。
REST API : GET /v1/objects/users/<userId>
CLI : user_show

19.4 ユーザーを作成する

ユーザーを作成します。マルチテナンシー機能を利用しない場合、登録できるユーザー数はビルトインユーザーを含めて最大で 32 です。マルチテナンシー機能を利用する場合、VPS に所属しないユーザー数はビルトインユーザーを含めて最大 32 で、VPS に所属するユーザー数は最大 256 です。

外部認証するユーザーの場合は、外部認証サーバー上のユーザーと同じ名前でユーザーを作成します。

作成されたユーザーが最初に行える操作は、パスワードの変更だけです。パスワード変更後は、与えられたロールに許されるコマンドが実行できます。

前提条件

- 実行に必要なロール：Security
- VPS 内にユーザーを作成する場合：当該 VPS のスコープ

操作手順

1. ユーザーを所属させるユーザーグループ ID を確認します。
REST API : GET /v1/objects/user-groups
CLI : user_group_list
2. ユーザーを作成します。
ユーザー ID、パスワード、所属させるユーザーグループ ID(複数指定可：最大 8)、認証の種別を指定してコマンドを実行します。
ユーザーにコンソールインターフェイスの使用を許可する場合は、isEnabledConsoleLogin に "true"を指定してください。



メモ

- ユーザー認証設定の requiresInitialPasswordReset が "true"に設定されている場合、本機能で作成したユーザーにコンソールインターフェイスを使用する権限を与えても、コンソールインターフェイスでは使用できない状態になっています。「自身のパスワードを変更する」を用いることでコンソールインターフェイスで使用できるようになります。
- コンソールインターフェイスの使用を許可する場合は、次の設定が必要です。

- Security ロールまたは Service ロールが割り当てられたユーザーグループに所属すること
- 認証の種別(authentication)が"local"であること

外部認証サーバーで認証する場合は、認証の種別を"external"と指定し、パスワードの指定は不要です。

REST API : POST /v1/objects/users

CLI : user_create

コマンド実行後のレスポンスにユーザー情報が表示されます。

3. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

4. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

19.5 ユーザー情報を編集する

登録されているユーザー情報について、以下が編集できます。ビルトインユーザーのユーザー情報も編集できます。

- パスワード
- ユーザーの有効/無効

Security または Service ロールが割り当てられたユーザーグループのユーザーがすべて無効になるような編集はできません。

コンソールインターフェイスを使用できるユーザーがゼロになる操作はできません。

ユーザー認証設定の `requiresInitialPasswordReset` が"true"に設定されている場合、本機能でパスワード変更してもコンソールインターフェイスでは使用できない状態になっています。「自身のパスワードを変更する」を用いることでコンソールインターフェイスで使えるようになります。

ユーザー情報を編集すると、そのユーザーのセッションは削除されます。



メモ

ユーザー認証設定の `requiresInitialPasswordReset` が"true"に設定されている場合、本機能でパスワードを変更すると、そのユーザーのパスワードの有効期限が切れた状態になっています。「自身のパスワードを変更する」を用いることで有効期限切れの状態が解除されます。

前提条件

- 実行に必要なロール : Security
- VPS 内のユーザー情報を編集する場合 : 当該 VPS のスコープ

操作手順

1. ユーザー ID を確認します。
REST API : GET /v1/objects/users
CLI : user_list
2. ユーザー情報を編集します。
ユーザー ID、新しいパスワード、ユーザーの有効/無効を指定してコマンドを実行します。
REST API : PATCH /v1/objects/users/<userId >
CLI : user_set
コマンド実行後のレスポンスにユーザー情報が表示されます。
3. <<Bare metal>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
4. <<Cloud for AWS>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

19.6 ユーザーを削除する

ユーザーを削除します。ただし、**Security** または **Service** ロールが割り当てられたユーザーグループのユーザーがゼロになる操作はできません。また、ビルトインユーザーは削除できません。

コンソールインターフェイスを使用できるユーザーがゼロになる操作はできません。

ユーザーを削除すると、そのユーザーのセッションは削除されます。

前提条件

- 実行に必要なロール : **Security**
- VPS 内のユーザーを削除する場合 : 当該 VPS のスコープ

操作手順

1. ユーザー ID を確認します。
REST API : GET /v1/objects/users
CLI : user_list
2. ユーザーを削除します。
ユーザー ID を指定してコマンドを実行します。
REST API : DELETE /v1/objects/users/<userId >
CLI : user_delete
3. ユーザー情報の一覧を取得して、ユーザーが削除されたことを確認します。
REST API : GET /v1/objects/users
CLI : user_list
4. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

5. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

19.7 自身のパスワードを変更する

自身のパスワードを変更できます。ただし、ローカルで認証するユーザー(authentication が "local")のみが実行できます。

パスワードを変更すると、自身のセッションは削除されます。

ロールによる実行制限はありません。

VSP One SDS Block Administrator で実施する場合

VSP One SDS Block Administrator では、初めてログインする場合、またはパスワードの有効期限が切れている場合に実施できます。

ログインボタンをクリックしたあと表示される、パスワード変更画面から操作します。操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・「VSP One SDS Block Administrator のログインとログアウト」

操作手順

1. 自身のパスワードを変更します。

ユーザー ID、現在のパスワード、新しいパスワードを指定してコマンドを実行します。

REST API : PATCH /v1/objects/users/<userId >/password

CLI : user_password_set

コマンド実行後のレスポンスにユーザー情報が表示されます。

変更したパスワードには有効期限があります。有効期限は、レスポンスとして表示されるユーザー情報で確認できます。有効期限のデフォルトは 42 日間です。

2. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



注意

認証チケットを発行しているユーザーのパスワードを変更する際は、変更後に、再度チケットを発行してください。



メモ

- ・ ユーザー認証設定の `requiresInitialPasswordReset` が `"true"` に設定されている場合、「ユーザーを作成する」および「ユーザー情報を編集する」でパスワードを設定したユーザーはコンソールインターフェイスを使用できない状態になっています。本機能を用いることでコンソールインターフェイスでできるようになります。
- ・ パスワードの変更は、1 分周期で実施される内部処理によってコンソールインターフェイスに反映され、イベントログ KARS20067-I が出力されます。このため、反映が終わるまで一定の時間を要します。

3. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



注意

認証チケットを発行しているユーザーのパスワードを変更する際は、変更後に、再度チケットを発行してください。



メモ

- ・ ユーザー認証設定の `requiresInitialPasswordReset` が `"true"` に設定されている場合、「ユーザーを作成する」および「ユーザー情報を編集する」でパスワードを設定したユーザーはコンソールインターフェイスを使用できない状態になっています。本機能を用いることでコンソールインターフェイスでできるようになります。
- ・ パスワードの変更は、1 分周期で実施される内部処理によってコンソールインターフェイスに反映され、イベントログ KARS20067-I が出力されます。このため、反映が終わるまで一定の時間を要します。

19.8 ユーザーをユーザーグループに追加する

ユーザーを別のユーザーグループに追加します。

ユーザーをユーザーグループに追加すると、そのユーザーのセッションは削除されます。

前提条件

- ・ 実行に必要なロール：Security
- ・ VPS 内のユーザーをユーザーグループに追加する場合：当該 VPS のスコープ

操作手順

1. 追加して所属させるユーザーグループ ID を確認します。

REST API : GET /v1/objects/user-groups

CLI : `user_group_list`

2. ユーザー ID とユーザーグループ ID(複数可)を指定してコマンドを実行します。

REST API : POST /v1/objects/users/<userId>/actions/add-user-group/invoke

CLI : `user_add_user_group`

コマンド実行後のレスポンスにユーザー情報が表示されます。

3. <<Bare metal>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
4. <<Cloud for AWS>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

19.9 ユーザーをユーザーグループから削除する

指定したユーザーグループからユーザーを削除します。

ユーザーグループからユーザーを削除すると、そのユーザーのセッションは削除されます。

コンソールインターフェイスを使用できるユーザーの場合、本操作によって Security ロールまたは Service ロールのどちらも持たなくなる操作はできません。

前提条件

- ・ 実行に必要なロール : Security
- ・ VPS 内のユーザーをユーザーグループから削除する場合 : 当該 VPS のスコープ

操作手順

1. ユーザーを削除するユーザーグループ ID を確認します。
REST API : GET /v1/objects/user-groups
CLI : user_group_list
2. ユーザー ID とユーザーグループ ID(複数可)を指定してコマンドを実行します。
REST API : POST /v1/objects/users/<userId >/actions/delete-user-group/invoke
CLI : user_delete_user_group
コマンド実行後のレスポンスにユーザー情報が表示されます。
3. <<Bare metal>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
4. <<Cloud for AWS>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

19.10 ユーザーグループの一覧を取得する

登録されているユーザーグループの一覧を取得します。以下の情報が得られます。

- `userGroupId` : ユーザーグループの ID
- `userGroupObjectId` : ユーザーグループのオブジェクト ID
- `roleNames` : ユーザーグループのロール
- `isBuiltIn` : ビルトインユーザーグループかどうか
- `externalGroupName` : 外部認証サーバー連携時、外部認証サーバーに登録されたユーザーグループの名称
- `vpsId` : ユーザーグループが所属する VPS の ID
- `scope` : ユーザーグループがアクセス可能な VPS の ID

前提条件

- 実行に必要なロール : Security

操作手順

1. ユーザーグループ一覧を取得します。
REST API : GET /v1/objects/user-groups
CLI : `user_group_list`

19.11 ユーザーグループの詳細情報を取得する

登録されているユーザーグループについて、以下の情報を取得します。

- `memberUsers` : 所属するユーザー情報(ユーザー ID とユーザーのオブジェクト ID)の一覧
- `userGroupId` : ユーザーグループの ID
- `userGroupObjectId` : ユーザーグループのオブジェクト ID
- `roleNames` : ユーザーグループのロール
- `isBuiltIn` : ビルトインユーザーグループかどうか
- `externalGroupName` : 外部認証サーバー連携時、外部認証サーバーに登録されたユーザーグループの名称
- `vpsId` : ユーザーグループが所属する VPS の ID
- `scope` : ユーザーグループがアクセス可能な VPS の ID

前提条件

- 実行に必要なロール : Security

操作手順

1. ユーザーグループ ID を確認します。
REST API : GET /v1/objects/user-groups
CLI : `user_group_list`
2. ユーザーグループの詳細情報を取得します。
ユーザーグループ ID を指定してコマンドを実行します。
REST API : GET /v1/objects/user-groups/<userGroupId>
CLI : `user_group_show`

19.12 ユーザーグループを作成する

ユーザーグループを作成します。

マルチテナンシー機能を利用しない場合、登録できるユーザーグループの数はビルトインユーザーグループを含めて最大 32 です。マルチテナンシー機能を利用する場合、VPS に所属しないユーザーグループの数はビルトインユーザーを含めて最大 32 で、VPS に所属するユーザーグループの数は最大 256 です。

外部認証サーバーと連携する場合、外部認証サーバーに登録されているグループ名を登録します。外部認証サーバーに登録されているグループ名の文字種や文字数は外部認証サーバーの要件に基づきます。

前提条件

- 実行に必要なロール：Security
- VPS 内にユーザーグループを作成する場合：当該 VPS のスコープ

操作手順

1. ユーザーグループを作成します。

ユーザーグループ ID、ロール(複数指定可)、外部認証サーバーに登録されたグループの名称(外部認証サーバー連携時)を指定してコマンドを実行します。

マルチテナンシー機能を利用する場合は、所属する VPS(システム管理者の場合は"system")とスコープも指定します。

REST API : POST /v1/objects/user-groups

CLI : user_group_create

コマンド実行後のレスポンスにユーザーグループ情報が表示されます。

2. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

3. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

19.13 ユーザーグループ情報を編集する

ユーザーグループの情報を編集します。ロールが編集できます。ただし、ビルトインユーザーグループのロールは変更できません。

Security ロールまたは Service ロールを持つユーザーがゼロになる操作は行えません。

コンソールインターフェイスを使用できるユーザーが所属する場合、本操作によってそのユーザーが Security ロールまたは Service ロールのどちらも持たなくなる操作はできません。

ユーザーグループ情報を編集すると、そのユーザーグループに所属するユーザーのセッションは削除されます。また、外部認証を有効に設定し、外部認証サーバー上でユーザーをグループ単位で管理している場合、外部グループに対応するローカルのユーザーグループを編集するとすべてのセッションが削除されます。

前提条件

- 実行に必要なロール : Security
- VPS 内のユーザーグループ情報を編集する場合 : 当該 VPS のスコープ

操作手順

1. ユーザーグループ ID を確認します。

REST API : GET /v1/objects/user-groups

CLI : user_group_list

2. ユーザーグループの情報を編集します。

ユーザーグループ ID とロール(複数可)を指定してコマンドを実行します。

マルチテナンシー機能を利用する場合は、スコープも指定します。スコープを指定する場合は、"system"も含めて指定してください。

REST API : PATCH /v1/objects/user-groups/<userGroupId >

CLI : user_group_set

コマンド実行後のレスポンスにユーザーグループ情報が表示されます。

3. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

4. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

19.14 ユーザーグループを削除する

ユーザーグループを削除します。ユーザーが 1 人も所属しないユーザーグループが削除できます。ただし、ビルトインユーザーグループは削除できません。

外部認証を有効に設定し、外部認証サーバー上でユーザーをグループ単位で管理している場合、外部グループに対応するローカルのユーザーグループを削除するとすべてのセッションが削除されます。

前提条件

- 実行に必要なロール : Security
- VPS 内のユーザーグループを削除する場合 : 当該 VPS のスコープ

操作手順

1. 削除するユーザーグループのユーザーグループ ID を確認します。
REST API : GET /v1/objects/user-groups
CLI : user_group_list
2. ユーザーグループの詳細情報を取得します。
ユーザーグループ ID を指定してコマンドを実行します。
REST API : GET /v1/objects/user-groups/<userGroupId >
CLI : user_group_show
所属するユーザーがないことが確認できたら、次の手順に進みます。
3. ユーザーグループを削除します。
ユーザーグループ ID を指定してコマンドを実行します。
REST API : DELETE /v1/objects/user-groups/<userGroupId >
CLI : user_group_delete
4. ユーザーグループの一覧を取得して、ユーザーグループが削除されたことを確認します。
REST API : GET /v1/objects/user-groups
CLI : user_group_list
5. ≪Bare metal≫構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
6. ≪Cloud for AWS≫構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

19.15 外部認証サーバーを利用する

外部認証サーバーの利用法について説明します。

19.15.1 外部認証サーバー利用の概要

外部認証サーバーとの連携を設定すると、外部認証サーバーに登録されたユーザー情報を利用して認証できるようになります。連携可能な外部認証サーバーは以下のとおりです。

外部認証サーバーのサポートバージョン

名称	バージョン
Active Directory	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Server 2025
389 Directory Server	2.x
OpenLDAP*	2.5.x

名称	バージョン
* OpenLDAP は今後の VSP One SDS Block のアップデートでサポート対象外とする予定です。他の外部認証サーバーへ移行することを検討してください。	

使用できる TLS プロトコル

- LDAPS
- StartTLS

TLS プロトコルを使用する際は、外部認証サーバー設定の `isStartTlsEnabled`、`primaryLdapServerUrl`、`secondaryLdapServerUrl` を以下に従って設定してください。

使用する TLS プロトコル	外部認証サーバーの設定値	
	<code>isStartTlsEnabled</code>	<code>primaryLdapServerUrl</code> <code>secondaryLdapServerUrl</code>
LDAPS	false	ldaps://example1.com
StartTLS	true	ldap://example2.com



ヒント

外部認証サーバー設定は、以下の REST API または CLI を参照してください。

REST API : `PATCH /v1/objects/external-auth-server-setting`

CLI : `external_auth_server_setting_set`



注意

- 外部認証サーバーとして Windows Server を利用する際は、TLS プロトコルを必ず有効にし、外部認証サーバーのルート証明書をインポートしてください。Windows Server では 2020 年 1 月以降デフォルトで LDAP サーバー署名必須の設定が有効になっているため、TLS プロトコルが無効の場合は接続に失敗することがあります。
- StartTLS 時は、複数 LDAP サーバーを指定していても、Primary 側に設定したサーバーのダウンまたは接続不可能によって外部認証が不可となります(StartTLS 時は LDAP サーバーの冗長構成はサポートされません)。また、Secondary 側だけに LDAP サーバーを指定した場合も、外部認証は不可となります。StartTLS 時に外部 LDAP サーバーがダウンしたケースでは、ローカルユーザーでログインし、外部認証サーバー設定の編集で、外部 LDAP サーバーの指定を変更するようにしてください。
- 外部認証サーバーの冗長構成を組んでいる状態で Primary の外部認証サーバーに障害が発生すると、最大で 10 分程度応答が遅延することがあります。



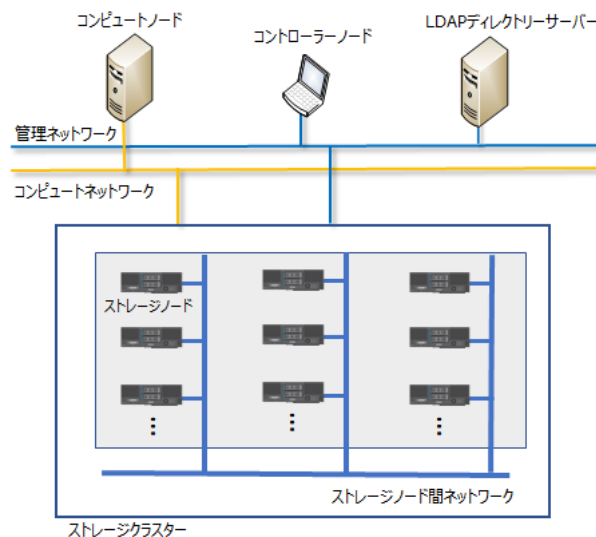
注意

ストレージシステムと外部認証サーバーの接続のセキュリティを確保するため、外部認証サーバーを下記のよう構成してください。

- ストレージシステムが外部認証サーバーとの接続に使用している LDAP クライアントは、下位互換性のために安全でない再ネゴシエーションを許可しています。外部認証サーバーとの TLS 接続に当たっては、RFC5746 に対応した外部認証サーバーの使用をお勧めします。
- 外部認証サーバーが TLS1.2 に対応していること
ストレージシステムが外部認証サーバーとの接続に使用している LDAP クライアントは TLS1.2 のみを使用しますが、外部認証サーバー側の設定においても、脆弱なプロトコルバージョン(SSL2.0、SSL3.0、TLS1.0、TLS1.1)を無効化することをお勧めします。
- 外部認証サーバーが TLS の暗号スイートとして、次の(1)～(6)のうち 1 つ以上をサポートしていること
(1) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
(2) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
(3) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- (4) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- (5) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- (6) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

- 暗号スイートの要件を満たさない場合、外部認証サーバーとの TLS 接続に失敗します。
- 外部認証サーバーが上記の暗号スイートをサポートしているかどうかは、使用する外部認証サーバーのマニュアルを参照してください。
- 使用する暗号スイートの鍵交換方式(DHE、ECDHE)に応じて、外部認証サーバー側に鍵交換(DHE、ECDHE)の設定が必要な場合があります。具体的な設定方法については、使用する外部認証サーバーのマニュアルを参照してください。なお、OpenLDAP では、ECDHE 鍵交換方式をサポートするのは 2.4.48 以降です。
- 外部認証サーバー側に設定するサーバー証明書が、RSA 証明書か ECC 証明書かによって、使用可能な暗号スイートが異なります。RSA 証明書の場合は上記の(1)～(4)が、ECC 証明書の場合は上記の(5)、(6)が使用できます。外部認証サーバーへのサーバー証明書の設定方法については、使用する外部認証サーバーのマニュアルを参照してください。
- ストレージシステムが外部認証サーバーとの接続に使用している LDAP クライアントは、上記の暗号スイートのみを使用しますが、上記以外で脆弱な暗号スイートについては、外部認証サーバー側の設定において無効化することをお勧めします。脆弱な暗号スイートとは、RFC7540 Appendix A. TLS 1.2 Cipher Suite Black List に示される暗号スイート(Cipher Suite)を指します。
- 外部認証サーバーに複数のサーバー証明書を設定する場合は、ストレージシステムにインポートする 1 つのルート証明書ですべてのサーバー証明書の信頼性を証明できるよう、サーバー証明書を発行していること



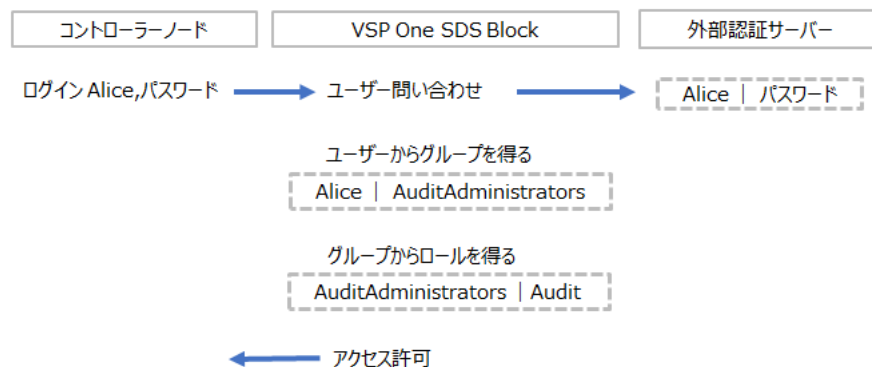
利用ケースには、以下の 2 つがあります。

外部認証サーバー上でユーザーをグループで管理していない場合

VSP One SDS Block に登録されたユーザーグループの情報をを使用して認可します。VSP One SDS Block での利用手順は、外部認証サーバーとの連携を設定したあと、外部認証サーバーに登録してあるユーザー名と同じ名前(ユーザー ID)でユーザーを VSP One SDS Block ローカルに作成します。以降、これらのユーザーを外部ユーザーと表記することがあります。

(例)外部ユーザーである Alice が、Audit ロールを持つビルトインユーザーグループ AuditAdministrators に所属している場合

ユーザー名に Alice、パスワードに Alice のパスワードを指定して、Audit ロールが必要な GET /v1/objects/audit-logs/download を発行して、監査ログファイルがダウンロードできます。



この場合、Alice が正しいパスワードを指定したことは、外部認証サーバーが確認します。VSP One SDS Block は、外部認証サーバーが応答したユーザーからグループを得て、またグループからロールを得て、URL /v1/objects/audit-logs/download のアクセスに必要なロールと比較した上でアクセスを許可します。

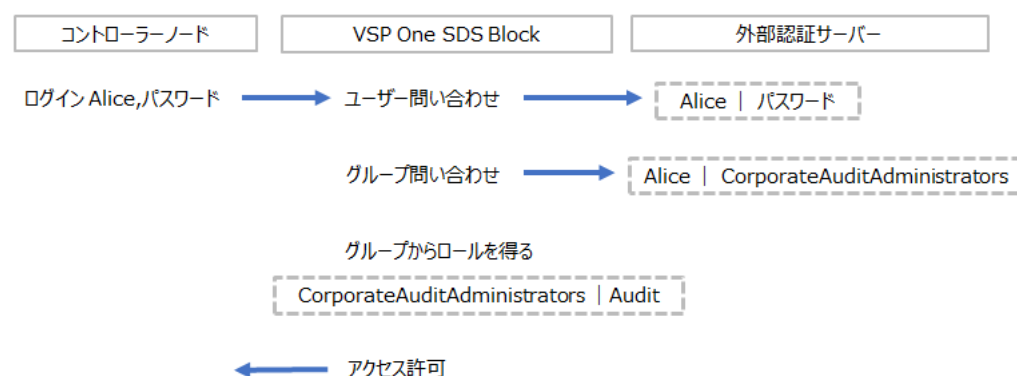
VSP One SDS Block には、ユーザー Alice と、グループ AuditAdministrators が登録されている必要があります。パスワードは登録されている必要はありません。

外部認証サーバー上でユーザーをグループで管理していない場合のことを、外部認証、ローカル認可する利用ケースと呼びます。PATCH /v1/objects/external-auth-server-setting(CLI : external_auth_server_setting_set)での、mappingMode(CLI : --mapping_mode)パラメーターに "User"を指定した場合に該当します。

外部認証サーバー上でユーザーをグループ単位で管理している場合

この利用ケースは外部認証サーバーが Active Directory の場合にサポートされます。外部認証サーバーに登録されたユーザーグループ情報を使用して認可します。外部ユーザーは外部認証サーバーのグループに属していることが前提になります。VSP One SDS Block での利用手順は、外部認証サーバーとの連携を設定したあと、ユーザーグループを VSP One SDS Block ローカルに作成し、パラメーターに外部グループの名称を設定します。この場合、ユーザーを個別に作成する必要はありません。以降、これらのユーザーグループを外部グループと表記することがあります。

(例)ユーザー Alice が、外部認証サーバーに定義された CorporateAuditAdministrators グループに属していた場合



この場合、Alice が正しいパスワードを指定したことと、Alice が CorporateAuditAdministrators に所属することは、外部認証サーバーが確認します。VSP One SDS Block は、外部認証サーバーが応答したグループからロールを得て、URL /v1/objects/audit-logs/download のアクセスに必要なロールと比較してアクセスを許可します。

VSP One SDS Block には、ユーザー Alice が登録されている必要はありませんが、グループ CorporateAuditAdministrators は登録されている必要があります。具体的には、CorporateAuditAdministrators に対応するユーザーグループを externalGroupName(CLI : --external_group_name) パラメーターに指定した POST /v1/objects/user-groups(CLI : user_group_create) を実行します。

外部認証サーバー上でユーザーをグループ単位で管理している場合のことを、外部認証、外部認可する利用ケースと呼びます。PATCH /v1/objects/external-auth-server-setting(CLI : external_auth_server_setting_set) での、mappingMode(CLI : --mapping_mode) パラメーターに "Group" を指定した場合に該当します。

外部認証サーバーを利用する場合、Basic 認証の場合は、外部認証サーバーに毎回問い合わせが行われて最新情報が確認されます。セッション認証の場合は、外部認証サーバーへの問い合わせは行われず、トークンの有効/無効のみで認証が判断されます。



メモ

外部認証サーバー利用時の注意事項

- 外部認証サーバーとの接続が切れると外部認証サーバー上のユーザーでの認証ができなくなります。外部認証サーバーとの接続の復旧作業を実施するためには、Security ロールを持つユーザーが必要になります。そのため、ローカル認証の Security ロールを持つユーザーを最低 1 人有効にしてください。外部認証サーバーとの接続が切れている状態で実施したい操作がほかにある場合、操作に必要なロールを持つローカル認証のユーザーを作成しておくことを検討してください。
- VSP One SDS Block が連携できる外部認証サーバー上のユーザー名とユーザーグループ名の最大長は 64 文字です。
- 外部認証サーバー上でのパスワード変更が VSP One SDS Block に反映されるまで、5 分ほど掛かることがあります。ただし、外部認証サーバーの設定によっては、それ以上掛かることもあります。
- 外部認証サーバー上でユーザーをグループで管理している場合、またはユーザーをグループで管理してなくても外部認証サーバーを利用している場合には、ユーザーグループ関連の以下のパラメーターおよび属性は必ず設定してください。

- userIdAttribute
- userTreeDn
- userObjectClass
- externalGroupNameAttribute
- userGroupTreeDn
- userGroupObjectClass

ユーザーをグループで管理していない場合、グループ関連のパラメーター externalGroupNameAttribute、userGroupTreeDn、userGroupObjectClass は、ユーザー関連のパラメーター userIdAttribute、userTreeDn、userObjectClass と同じ値を指定してください。POST /v1/objects/external-auth-server-setting/actions/verify-connectivity/invoke(CLI : external_auth_server_setting_verify_connectivity) などによる接続確認のときは、結果の numberOfExternalUserGroups の値は無視してください。

設定値の詳細は「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」または「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」を参照してください。

- 外部認証サーバーとして Windows Server を利用し、外部認証サーバー上でユーザーをグループ単位で管理している場合は、「Domain Users」にしか属していない(つまりデフォルトのユーザーグループにしか属していない)ユーザーの認証はできません。

上記「外部認証サーバー上でユーザーをグループ単位で管理している場合」の記述に従って、ユーザーを「Domain Users」以外の外部グループにも所属するように設定してください。

VSP One SDS Block における mappingMode の使い方

外部認証サーバーが 389 Directory Server または OpenLDAP の場合は、mappingMode(CLI : --mapping_mode)で"Group"は使えません。389 Directory Server および OpenLDAP ではユーザーが所属するグループを検索する操作がサポートされないためです。

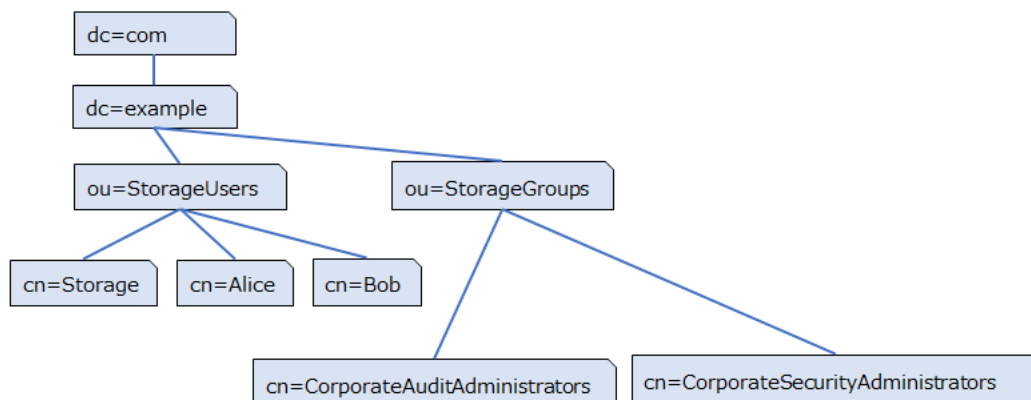
外部認証サーバーが Active Directory の場合は、mappingMode(CLI : --mapping_mode)に、"User" または"Group"のどちらも指定できます。Active Directory のグループが、VSP One SDS Block のロールに対応する場合、mappingMode(CLI : --mapping_mode)で"Group"を使ってください。そうでない場合、mappingMode(CLI : --mapping_mode)で"User"を使ってください。

- mappingMode(CLI : --mapping_mode)で"Group"を使うことが適切な例
ユーザー Alice は、Active Directory の CorporateAuditAdministrators グループに所属しています。そのグループのメンバーは、VSP One SDS Block の Audit ロールを持ちます。この場合、mappingMode(CLI : --mapping_mode)で"Group"を使えば、VSP One SDS Block でユーザーのパスワードや、ユーザーとグループの所属関係を管理する必要はなく、Active Directory による一元的な管理ができます。
- mappingMode(CLI : --mapping_mode)で"User"を使うことが適切な例
ユーザー Alice は Active Directory のセールス部門グループに所属しています。別のユーザー Bob は経理部門グループに所属しています。2 人に、VSP One SDS Block の Audit ロールを持たせたい場合、Active Directory のグループと VSP One SDS Block のロールは無関係なので、mappingMode(CLI : --mapping_mode)で"User"を使うことが適切です。そこで、2 人を VSP One SDS Block の AuditAdministrators ビルトインユーザーグループに所属させます。こうすることで、VSP One SDS Block でユーザーのパスワードを管理する必要はなく、Active Directory による一元的な管理ができます。

外部認証サーバーの設定例

外部認証サーバーとして Windows Server を利用し、外部認証サーバー上でユーザーをグループ単位で管理する場合の例です。

Active Directory は、以下のディレクトリー構造を持っているとします。



これに対応する PATCH /v1/objects/external-auth-server-setting(CLI : external_auth_server_setting_set)のパラメーター設定の例を次に示します。

パラメーター		設定値
REST API	CLI	
isEnabled	is_enabled	true

パラメーター		設定値
REST API	CLI	
authProtocol	auth_protocol	LDAP
mappingMode	mapping_mode	Group
primaryLdapServerUrl	primary_ldap_server_url	ldaps://ad.example.com
secondaryLdapServerUrl	secondary_ldap_server_url	""
isStartTlsEnabled	is_start_tls_enabled	false
baseDn	base_dn	dc=example,dc=com
bindDn	bind_dn	cn=Storage,ou=StorageUsers,dc=example,dc=com
bindDnPassword	bind_dn_password	Secret
userIdAttribute	user_id_attribute	sAMAccountName
userTreeDn	user_tree_dn	ou=StorageUsers,dc=example,dc=com
userObjectClass	user_object_class	User
externalGroupNameAttribute	external_group_name_attribute	sAMAccountName
userGroupTreeDn	user_group_tree_dn	ou=StorageGroups,dc=example,dc=com
userGroupObjectClass	user_group_object_class	Group

VSP One SDS Block は、外部認証サーバーにおいて、ユーザーおよびグループを探す場合、再帰的な検索はしません。このため、VSP One SDS Block が参照するユーザーは `userTreeDn`(CLI : `user_tree_dn`)の直下に、グループは `userGroupTreeDn`(CLI : `user_group_tree_dn`)の直下にある必要があります。

`bindDn`(CLI : `bind_dn`)に指定するユーザーアカウントは、`userTreeDn`(CLI : `user_tree_dn`)と `userGroupTreeDn`(CLI : `user_group_tree_dn`)以下のすべてのエントリーを参照する権限が必要です。そのアカウントは、`userTreeDn`(CLI : `user_tree_dn`)の下にある必要はありません。

`userObjectClass`(CLI : `user_object_class`)、`userGroupObjectClass`(CLI : `user_group_object_class`)の適切な値は、お使いの外部認証サーバーによって異なります。外部認証サーバーのスキーマの設定を見るには、Linux の `ldapsearch` コマンド、または Windows の `ldp.exe` を使って、`baseDn`(CLI : `base_dn`)以下の既存のユーザーとグループを参照してください。

(例) コマンドラインが長いので、¥記号を使用して改行しています。¥記号を含めてコピーアンドペーストしても正しく動作します。

```
$ ldapsearch -D <bind_dn> ¥
-w <bind_dn_password> ¥
-H <primary_ldap_server_url> ¥
-b <base_dn> ¥
"(objectClass=*)" "
```

`POST /v1/objects/external-auth-server-setting/actions/verify-connectivity/invoke`(CLI : `external_auth_server_setting_verify_connectivity`)は、`ldapsearch` コマンドを使って外部認証サーバーに接続できるかを確認します。以下は、そのときに発行されるコマンドの例です。`POST /v1/objects/external-auth-server-setting/actions/verify-connectivity/invoke` が失敗する場合、以下のコマンドを、Linux サーバーで実行すると、原因がわかることがあります。`-d 1` オプションを追加すると、デバッグ用のトレースが表示され、問題解決に役立つことがあります。

(例) コマンドラインが長いので、¥記号を使用して改行しています。¥記号を含めてコピーアンドペーストしても正しく動作します。

```
$ ldapsearch -D <bind_dn> ¥
-w <bind_dn_password> ¥
-H <primary_ldap_server_url> ¥
-b <user_tree_dn> ¥
"(&(objectClass=<user_object_class>)(<user_id_attribute>=*))" ¥
<user_id_attribute>
```

19.15.2 外部認証サーバー利用の操作

外部認証サーバーとの連携を設定します。

前提条件

- 実行に必要な外部サービス(TLS プロトコル使用時) : DNS サーバー
TLS プロトコル使用時は、LDAP サーバーは FQDN で指定する必要があります。A レコードに LDAP サーバーが登録された DNS サーバーを VSP One SDS Block に登録してください。



注意

DNS サーバーを利用している場合、ストレージノードは、DNS サーバーにおいて設定された時間 (DNS TTL[sec]) だけ、DNS への問い合わせ結果をキャッシュしています。このため、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL の間、ストレージノードが古い IP アドレスにアクセスする場合があります。DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL で設定された時間が経過したあとに外部認証サーバー設定を実行してください。

- 実行に必要なロール : Security

操作手順

1. 外部認証サーバーの設定を編集します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

外部認証サーバーとの接続する際の通信パラメーター timeoutSeconds(CLI : --timeout_seconds)、retryIntervalMilliseconds(CLI : --retry_interval_milliseconds)、maxRetries(CLI : --max_retries)はデフォルト値をそのまま使用してください。設定変更は、指示があった場合にのみ実施してください。

システムの初期値は、timeoutSeconds(CLI : --timeout_seconds)が 7、retryIntervalMilliseconds(CLI : --retry_interval_milliseconds)が 100、maxRetries(CLI : --max_retries)が 1 です。

REST API : PATCH /v1/objects/external-auth-server-setting

CLI : external_auth_server_setting_set

コマンド実行後のレスポンスに外部認証サーバーの設定情報が表示されます。

2. TLS プロトコルを使用する場合は、外部認証サーバーのサーバー証明書の信頼性を証明するルート証明書を VSP One SDS Block にインポートします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

外部認証サーバーとルート証明書ファイルを指定してコマンドを実行します。

REST API : POST /v1/objects/external-auth-server-root-certificates/<targetServer >/actions/import/invoke

CLI : external_auth_server_root_certificate_import

コマンド実行後に表示されるジョブの ID を確認します。



メモ

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される次のフィールドがサポートされます。

- 基本制限(Basic Constraints)
- キー使用法(Key Usage)
- サブジェクトキー識別子(Subject Key Identifier)
- 機関キー識別子(Authority Key Identifier)
- 証明書ポリシー(Certificate Policies)
- サブジェクト代替名(Subject Alternative Name)
- 名前の制限(Name Constraints)
- ポリシーの制限(Policy Constraints)
- 拡張キー使用法(Extended Key Usage)
- ポリシー禁止(Inhibit anyPolicy)

3. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4. 外部認証サーバーとの接続を確認します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : POST /v1/objects/external-auth-server-setting/actions/verify-connectivity/invoke

CLI : external_auth_server_setting_verify_connectivity

コマンド実行後のレスポンスに、LDAP サーバー上で検索できた外部認証可能なユーザー数とユーザーグループ数が表示されます。

外部認証サーバーとの接続に失敗した場合は、コマンドのレスポンスに、手順 1 で設定した外部認証サーバーごとに、接続に失敗した要因を示すメッセージやエラーコードが表示されます。それらを基に失敗の原因を取り除いたあと、再度接続を確認してください。

また、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に稼働中の接続障害の一般的な原因と対処が記載されていますのでそちらも参照してください。

5. 外部ユーザーまたは外部グループを登録します。

外部ユーザーを登録する場合は、ユーザーを作成します。

REST API : POST /v1/objects/users

CLI : user_create

このとき、パラメーターは以下のように指定します。

- userId : 外部認証サーバー上のユーザー ID
- userGroupIds : 所属させるユーザーグループの ID(複数指定可)
- authentication : "external"

外部グループを登録する場合は、ユーザーグループを作成します。

REST API : POST /v1/objects/user-groups

CLI : user_group_create

このとき、パラメーターは以下のように指定します。

- `userGroupId` : ユーザーグループの ID
 - `roleNames` : ユーザーグループに割り当てるロール(複数指定可)
 - `externalGroupName` : 外部認証サーバーに登録されたグループの名称
6. ユーザー一覧かユーザーグループ一覧を取得して、手順 5 の操作が正しくできたかを確認します。
 7. 外部ユーザーで **Basic** 認証を実行し、外部認証サーバーの設定と、外部ユーザーまたは外部グループの登録が正しくできたかを確認します。
 8. **«Bare metal»** 構成情報のバックアップを行います。
「構成情報をバックアップする **«Bare metal» «Cloud for AWS»**」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
 9. **«Cloud for AWS»** 構成情報のバックアップを行います。
「構成情報をバックアップする **«Bare metal» «Cloud for AWS»**」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

19.16 外部認証サーバーの設定を取得する

外部認証サーバーの設定を取得します。以下の情報が得られます。

- `isEnabled` : 外部認証の有効/無効
- `authProtocol` : 外部認証時に使用する認証プロトコル
- `ldapSetting` : LDAP 認証の設定情報

前提条件

- 実行に必要なロール : **Security**

操作手順

1. 外部認証サーバーの設定を取得します。
クラスターマスターノード(プライマリー)に対してのみ実行できます。
REST API : `GET /v1/objects/external-auth-server-setting`
CLI : `external_auth_server_setting_show`

19.17 外部認証サーバーのルート証明書を取得する

「外部認証サーバーを利用する」でインポートした、ストレージシステムが外部認証サーバーのサーバー証明書の信頼性を検証するために使用するルート証明書は、DER 形式のファイルとして出力されます。

前提条件

- 実行に必要なロール : **Security**

操作手順

1. 外部認証サーバーのサーバー証明書の信頼性を検証するためのルート証明書を取得します。
クラスターマスターノード(プライマリー)に対してのみ実行できます。

外部認証サーバーを指定してコマンドを実行します。

REST API: GET /v1/objects/external-auth-server-root-certificates/<targetServer >/download

CLI : external_auth_server_root_certificate_download

セッションを管理する

- 20.1 セッション管理の概要
- 20.2 セッション情報の取得
- 20.3 セッションを生成する
- 20.4 セッションを削除する

20.1 セッション管理の概要

セッションは、ユーザーとストレージシステム間の接続情報です。

セッションを生成する REST API や CLI を実行することで、セッションを生成できます。セッションを生成すると、トークンが取得できます。

ユーザーインターフェイスに RAID Manager を使用している場合もセッションを生成します。その場合のセッションのタイムアウト時間は 60 分固定です。

セッション生成数にはストレージシステム全体で上限があり、上限を超えると新たなセッションが生成できなくなります。

セッション生成数の上限は、マルチテナンシー機能を利用しない場合 64 です。マルチテナンシー機能を利用する場合、VPS に所属しないセッションの上限数は 64、VPS に所属するセッションの上限数は 436 です。ユーザーが複数の異なる VPS に所属する場合は、所属するそれぞれの VPS にセッションが生成されたものとして計算されます。

セッション生成数の上限に達しても、Basic 認証やチケット認証は利用できます。セッション生成数の上限に達した場合は、不要なセッションを削除するか、Basic 認証やチケット認証の利用を検討してください。

生成されたセッションは、以下の場合に削除されます。

- セッション(トークン)の有効期限が過ぎた場合
- セッションを使用しないままタイムアウト時間を超過した場合
- クラスタマスターノード(プライマリー)がフェイルオーバーした場合
- セッション削除、ユーザーの編集や削除、パスワード変更、ユーザーグループからのユーザーの削除、またはユーザーが所属するユーザーグループの編集を実行された場合

トークンの有効期限(デフォルト：24 時間)はストレージシステム全体で共通です。トークンの有効期限の変更方法については「ユーザー認証設定を編集する」を参照してください。

セッションのタイムアウト時間(デフォルト：30 分)はセッションごとに指定することもストレージシステム全体で共通とすることもできます。セッションごとに指定する場合は、セッション作成時にタイムアウト時間を指定します。セッション作成時にタイムアウト時間を指定しなかった場合は、ストレージシステム全体での設定が適用されます。セッションのタイムアウト時間の、ストレージシステム全体での設定の変更方法については「ユーザー認証設定を編集する」を参照してください。



注意

セッション作成で取得したトークンが漏えいした場合、意図しない第三者に VSP One SDS Block を操作されるおそれがあります。取得したトークンは漏えいしないよう適切に管理してください。

20.2 セッション情報の取得

セッション情報が一覧または個別に取得できます。

20.2.1 取得できるセッション情報

以下の情報が一覧または個別に取得できます。

- sessionId : セッション ID(uuid)
- userId : ユーザー ID
- userObjectId : ユーザーのオブジェクト ID
- expirationTime : セッションの有効期限
- createTime : セッションが生成された日時
- lastAccessTime : セッションが最後に使用された日時
- roleNames : 当該セッションを保持するユーザーに割り当てられているロールの一覧
- vpsId : セッションを生成したユーザーが所属する VPS の ID
- privileges : セッションを生成したユーザーがアクセス可能な VPS 情報の一覧

20.2.2 セッションの一覧を取得する

セッション情報の一覧を取得します。

前提条件

- 実行に必要なロール : Security
ただし、自身のセッション情報の一覧を取得するときは、ロールによる実行制限はありません。

操作手順

1. ユーザーが生成したセッション情報の一覧を取得します。

REST API : GET /v1/objects/sessions

CLI : session_list

20.2.3 セッション情報を取得する

指定した ID のセッション情報を取得します。

前提条件

- 自身が所属する VPS 内の任意のセッション ID を指定するのに必要なロール : Security
Security ロールを持たないユーザーは、自身のセッション ID のみ指定できます。

操作手順

1. セッションの ID を確認します。

REST API : GET /v1/objects/sessions

CLI : session_list

2. セッションの ID を指定してセッション情報を取得します。

REST API : GET /v1/objects/sessions/<sessionId >

CLI : session_show

20.3 セッションを生成する

セッションを生成します。セッション認証用のトークンが生成され、以下のセッション情報が表示されます。生成されたトークンを使ったセッション認証ができるようになります。

ロールによる実行制限はありません。

- token : トークン
- sessionId : セッション ID(uuid)
- userId : ユーザー ID
- userObjectId : ユーザーのオブジェクト ID
- expirationTime : セッションの有効期限
- createTime : セッションが生成された日時
- lastAccessTime : セッションが最後に使用された日時
- roleNames : 当該セッションを保持するユーザーに割り当てられているロールの一覧
- vpsId : セッションを生成したユーザーが所属する VPS の ID
- privileges : セッションを生成したユーザーがアクセス可能な VPS 情報の一覧

前提条件

- VPS 内でセッションを追加する場合 : 当該 VPS のスコープ

操作手順

1. セッションを生成します。
セッションタイムアウトまでの時間[sec]が指定できます。
REST API : POST /v1/objects/sessions
CLI : session_create
コマンド実行後のレスポンスにセッション情報が表示されます。

20.4 セッションを削除する

生成済みのセッションを削除します。

前提条件

- 自身が所属する VPS 内の任意のセッション ID を指定するのに必要なロール : Security
Security ロールを持たないユーザーは、自身のセッション ID のみ指定できます。
- VPS 内のセッションを削除する場合 : 当該 VPS のスコープ

操作手順

1. セッションの ID を確認します。
REST API : GET /v1/objects/sessions
CLI : session_list
2. セッションの ID を指定してセッションを削除します。
REST API : DELETE /v1/objects/sessions/<sessionId >
CLI : session_delete
3. セッションの一覧を取得して、セッションが削除できたかを確認します。
REST API : GET /v1/objects/sessions
CLI : session_list

ユーザー認証設定を編集する

- 21.1 ユーザー認証設定を編集する
- 21.2 ユーザー認証設定を取得する

21.1 ユーザー認証設定を編集する

以下のユーザー認証設定が設定できます。ユーザー認証設定にはパスワードポリシーが含まれています。

項目	説明	システムの初期値	設定できる値域
minLength	パスワードの最小文字数。	8	1～256
minNumberOfUpperCaseChars	パスワードに含まれるアルファベット大文字の最小文字数。	0	0～16
minNumberOfLowerCaseChars	パスワードに含まれるアルファベット小文字の最小文字数。	1	0～16
minNumberOfNumerals	パスワードに含まれる数字(0-9)の最小文字数。	1	0～16
minNumberOfSymbols	パスワードに含まれる記号(アルファベットや数字以外の文字)の最小文字数。	0	0～16
numberOfPasswordHistory	過去と同じパスワードを禁止する世代数。例えば、2の場合は、1つ前のパスワードは設定できない。 1の場合は禁止しない。	1	1～10
requiresInitialPasswordReset	新規ユーザーが、初めてREST API や CLI を実行するときや、VSP One SDS Block Administrator でログインしたときに、パスワードの変更を必要とするかの設定。 "true"の場合、初回の操作時にパスワードの変更が強制される。	true	Boolean
minAgeDays	パスワードを変更してから、次に変更できるまでの日数。 0の場合は即時再変更ができる。 maxAgeDays より短くなければならない。	0	0～10
maxAgeDays	パスワードを変更してから、そのパスワードが使用できる日数。 指定日数を過ぎるとそのパスワードは無効になる。 0の場合は期限なし。	42	0～365
maxAttempts	アカウントを一時的に無効にする(アカウントロック)までの連続ログイン失敗回数。 0の場合はアカウントロックは無効。	3	0～10

項目	説明	システムの初期値	設定できる値域
	コンソールインターフェイスのログイン時にも適用される。		
lockoutSeconds[sec]	アカウントロックから解除されるまでの時間[sec]。 コンソールインターフェイスのログイン時にも適用される。	600	60～600
maxLifetimeSeconds[sec]	トークンの有効期間[sec]。	86400	1800～604800
maxIdleSeconds[sec]	セッションがタイムアウトするまでの時間[sec]。 タイムアウトする前に当該セッションでアクセスすれば、そこからタイムアウトがカウントされる。 セッション生成時にセッションタイムアウトするまでの時間(aliveTime[sec])を指定した場合は、その指定がmaxIdleSeconds[sec]よりも優先される。	1800	300～86400

前提条件

- 実行に必要なロール：Security

操作手順

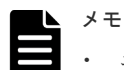
1. ユーザー認証設定を編集します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API：PATCH /v1/objects/user-auth-setting

CLI：user_auth_setting_set

コマンド実行後のレスポンスにユーザー認証設定の情報が表示されます。



メモ

- ユーザー認証設定の編集は、1分周期で実施される内部処理によってコンソールインターフェイスに反映され、イベントログ KARS20068-I が出力されます。このため、反映が終わるまで一定の時間を要します。
- 以下の操作を実施した場合、イベントログは出力されません。
 - ユーザー認証設定を編集したが、lockoutSetting に変更がない場合
 - ユーザー認証設定での requiresInitialPasswordReset が"true"の場合で、まだパスワードを変更していないユーザーを有効から無効に変更した場合
 - ユーザー認証設定での requiresInitialPasswordReset が"true"の場合で、まだパスワードを変更していないユーザーのパスワードを変更した場合
- maxAgeDays を変更した時点で、すでに設定されていたパスワードの有効期限は変更されません。maxAgeDays 更新後に設定されたパスワードの有効期限は、更新後の maxAgeDays の値に従います。

2. ≪Bare metal≫構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

3. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

21.2 ユーザー認証設定を取得する

ユーザー認証設定について、以下の情報を取得します。ユーザー認証設定にはパスワードポリシーが含まれています。

ロールによる実行制限はありません。

- `passwordComplexitySetting` : パスワードの複雑さの設定
- `passwordAgeSetting` : パスワードの有効期限の設定
- `lockoutSetting` : ロックアウトの設定
- `sessionSetting` : セッションの設定

操作手順

1. ユーザー認証設定を取得します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : `GET /v1/objects/user-auth-setting`

CLI : `user_auth_setting_show`

運用管理を SSL/TLS 通信で行う

- 22.1 TLS とは
- 22.2 SSL/TLS 通信の設定の流れ
- 22.3 サーバー証明書を更新するときの注意事項
- 22.4 OpenSSL のインストール
- 22.5 秘密鍵を作成する
- 22.6 秘密鍵を暗号化する
- 22.7 証明書署名要求を作成する
- 22.8 署名付き証明書を取得する
- 22.9 秘密鍵のパスフレーズの確認と解除
- 22.10 ルート証明書をインポートする
- 22.11 SSL/TLS 通信の署名付き証明書をインポートする
- 22.12 SSL/TLS 通信のクライアント要件
- 22.13 サーバー証明書に関する警告メッセージが表示されたときの対処

22.1 TLS とは

TLS(Transport Layer Security)は、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す。TLS 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。

以降、TLS に関する説明では、以下の用語を使います。

鍵ペア

秘密鍵と公開鍵の組み合わせです。この 2 つの暗号鍵は、数学的關係に基づいて決められます。

サーバー証明書

デジタル証明書と呼ばれることもあります。サーバー(VSP One SDS Block)と鍵ペアを結び付けるものです。サーバー証明書によって、VSP One SDS Block は自身がサーバーであることをクライアントに証明します。これによって VSP One SDS Block とクライアントは TLS を利用して通信できるようになります。サーバー証明書には次の 2 つの種類があります。

- 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、信頼できる認証局に送付して署名してもらいます。認証局には VeriSign、Symantec、自社内で運用している認証局などがあります。署名付きの証明書を利用する場合は、コストと要件が増えますが、信頼性は向上します。また、認証局の Web サイトには証明書の発行手続きなどが紹介されています。
このマニュアルで説明する署名付き証明書の取得についての手順はあくまでも例です。詳細な手順は、証明書の署名を要求する認証局の Web サイトや自社内で認証局を運用している担当部署に確認してください。
- 自己署名付きの証明書
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 上でコントローラーノードと VSP One SDS Block の間で通信を行う場合は、この証明書でも十分なセキュリティを確保できる場合がありますが、暗号化通信のテストなどの目的でだけ使用することをお勧めします。
このマニュアルで説明する自己署名付きの証明書の取得についての手順はあくまでも例です。



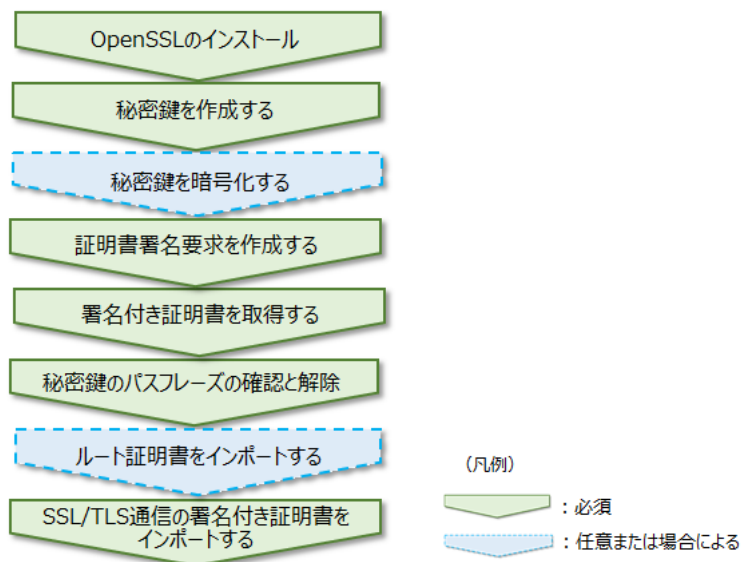
メモ

REST API または VSP One SDS Block Administrator は、https で通信することによって SSL/TLS 通信になります。

22.2 SSL/TLS 通信の設定の流れ

SSL/TLS 通信に必要な設定の流れを以下に示します。

SSL/TLS 通信に必要な設定に関する操作はコントローラーノードで実施してください。



注意

SSL/TLS 通信を有効にするには、サーバー証明書の有効期間が切れていないことが条件です。サーバー証明書の有効期間が切れている場合、SSL/TLS 通信を行うと警告メッセージが表示されます。また、通信のセキュリティも保証されません。サーバー証明書の有効期間が切れていた場合は、上記のフローのうち「秘密鍵を作成する」から「SSL/TLS 通信の署名付き証明書をインポートする」までを再度実施してください。

22.3 サーバー証明書を更新するときの注意事項

サーバー証明書を更新するときは以下に注意してください。

この節では、Subject Alternative Name を SAN と表記しています。

- VSP One SDS Block はインストール直後、自己署名証明書がインポートされています。サーバー証明書の初回更新はセキュアな通信が保障されないため注意してください。
また、自己署名証明書の場合、SSL/TLS 通信時に警告が表示されます。「サーバー証明書に関する警告メッセージが表示されたときの対処」を参考に対処してください。
- サーバー証明書を更新している間は、REST API、CLI によるストレージシステムの構成変更ができません。(構成変更とは、作成、更新、削除を行う管理操作を指します。例えば、ボリュームの作成などが該当します。)
- ストレージシステムの構成変更をしている間は、サーバー証明書の更新はできません。他の管理操作をしていないことを確認してから、サーバー証明書を更新してください。
- サーバー証明書の更新は非同期に行われます。また、サーバー証明書の更新に伴うサーバーの再起動によって、REST API、CLI、および VSP One SDS Block Administrator による操作が一時的に失敗することがあります。
- サーバー証明書の更新はシステムに大きな影響を与えます。ストレージシステムの故障の原因となることがあるため、設定するサーバー証明書と秘密鍵の内容は十分にご確認ください。
- サーバー証明書の SAN に IP アドレスを設定した状態で、構成情報の変更・設定によって管理ネットワークを変更する場合、サーバー証明書の更新が複数回必要になり、管理が複雑になります。
サーバー証明書を作成する際は、以下のように SAN に FQDN を指定する方法をお勧めします。
詳細は「証明書署名要求を作成する」を参照してください。



メモ VSP One SDS Block で、Universal Replicator 利用時に RAID Manager を使用する場合は、SAN に FQDN は指定できません。

≪Bare metal≫

- 推奨 1

クラスター代表 IP アドレスに対応する FQDN とストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN の、サブドメインをワイルドカード形式で指定したもの
(例: *.example.com)

- 推奨 2

クラスター代表 IP アドレスに対応する FQDN

(例: storage.example.com)

ストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN(ノード数分)

(例: storage-node1.example.com,storage-node2.example.com,...)

≪Cloud≫

- 推奨 1

ロードバランサーの FQDN とストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN の、サブドメインをワイルドカード形式で指定したもの
(例: *.example.com)

- 推奨 2

ロードバランサーの FQDN

(例: storage.example.com)

ストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN(ノード数分)

(例: storage-node1.example.com,storage-node2.example.com,...)

22.4 OpenSSL のインストール

SSL/TLS 通信設定に必要な秘密鍵、公開鍵の作成には OpenSSL を利用します。

- Linux OpenSSL の場合はデフォルトでインストールされるため、別途、OpenSSL のインストールは不要です。端末から"openssl version"と入力してみて、バージョン情報が表示されれば、OpenSSL はインストールされています。
- Windows の場合は、OpenSSL の公式 Web サイト(<http://www.openssl.org/>)からソースコードを入手してコンパイルするか、サードパーティー製のバイナリーを利用してください。

22.5 秘密鍵を作成する

OpenSSL のコマンドを使って秘密鍵を作成します。

OpenSSL のコマンドは、Windows と Linux で共通です。Windows であればコマンドプロンプト、Linux であればターミナル端末など、コマンド実行が可能なコンソールから実行します。

操作手順

1. 次のコマンドを実行します。

```
openssl genrsa -out server.key 2048
```

秘密鍵として、server.key ファイルが、コマンドを実行したフォルダーに作成されます。

オプション	説明
-out <秘密鍵ファイル名>	指定した名前で秘密鍵ファイルを出力します。秘密鍵ファイル名は任意です。
2048	鍵長の指定です。セキュリティを高めるために、2048 以上で設定してください。

22.6 秘密鍵を暗号化する

秘密鍵は第三者に漏えいすると、サーバーのセキュリティに悪影響を及ぼすおそれがあります。そのため、第三者から解読できないよう、暗号化できます。OpenSSL のコマンドを使って秘密鍵を暗号化します。

OpenSSL のコマンドは、Windows と Linux で共通です。Windows であればコマンドプロンプト、Linux であればターミナル端末など、コマンド実行が可能なコンソールから実行します。

操作手順

1. 次のコマンドを実行します。

```
openssl genrsa -aes256 -out server.key 2048
```

コマンドを実行すると、パスフレーズの入力を求められます。パスフレーズは暗号化のためのパスワードです。パスフレーズは忘れないようにしてください。また、第三者に知られないようにしてください。

オプション	説明
-aes256	暗号化アルゴリズムです。AES-256 のほかにも種類があります。利用可能な暗号化アルゴリズムについては、次のコマンドを実行し確認してください。 openssl genrsa -h
-out <秘密鍵ファイル名>	指定した名前で、秘密鍵ファイルを出力します。
2048	鍵長の指定です。

22.7 証明書署名要求を作成する

OpenSSL のコマンドを使って証明書署名要求を作成します。

OpenSSL のコマンドは、Windows と Linux で共通です。Windows であればコマンドプロンプト、Linux であればターミナル端末など、コマンド実行が可能なコンソールから実行します。

この節では、Subject Alternative Name を SAN と表記しています。

操作手順

1. OpenSSL の設定ファイルを作業用のディレクトリーにコピーします。



メモ

設定ファイルの配置場所は環境によって異なります。

Linux : 多くの場合、/etc/pki/tls/openssl.cnf に格納されています。

Windows : openssl のインストール時の設定によって異なります。

2. 手順 1 でコピーしたファイルを開き、下記に従って追記・修正します。

セクション名	パラメーター名	値	説明
req	req_extensions	v3_req	証明書署名要求の設定に v3_req セクションを加えます。
v3_req	subjectAltName	@alt_names	SAN の値として、alt_names セクションを読み込みます。
alt_names	DNS.<数値> = FQDN	ストレージノードの管理ポートの IP アドレスおよびストレージクラスターの代表 IP アドレスに対応する FQDN	ストレージノードの管理ポートの IP アドレスおよびストレージクラスターの代表 IP アドレスに対応する FQDN に対する証明書を発行します。 パラメーター名の数値には、1 から昇順にユニークな値を記載します。 alt_names セクションがなければ設定ファイルに作成します。
	IP.<数値> = IP アドレス	ストレージノードの管理ポートの IP アドレスおよびストレージクラスターの代表 IP アドレス	ストレージノードの管理ポートの IP アドレスおよびストレージクラスターの代表 IP アドレスに対する証明書を発行します。

(設定例) : 上記以外の項目は省略

```
[ req ]
req_extensions = v3_req

[ v3_req ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = storage.example.com
DNS.2 = storage-node1.example.com
DNS.3 = storage-node2.example.com
```

すべてのストレージノードと安全な SSL/TLS 通信をするために、下記 2 点が Subject Alternative Name(SAN)にすべて記載されているか、下記 2 点の FQDN のサブドメインをワイルドカード形式で(Common Name(CN)ではなく)SAN に指定(例:*.example.com)されているものを推奨します。

- ・ 代表 IP アドレスを使用する場合は、代表 IP アドレスに対応する FQDN
- ・ ストレージノードの管理ポートの IP アドレスに対応する FQDN

Google Chrome version 58 から CN が非推奨になっているため、VSP One SDS Block Administrator を利用する場合は SAN を推奨します。

管理ポートの IP アドレスの構成変更をする際に、DNS の対象のレコードを変更するだけであるため、SAN は FQDN での登録を推奨します。FQDN を使用する場合は、Bare metal モ

デルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「DNS サーバーを設定する」を参照し、DNS サーバーの設定もあわせて実施してください。

ストレージノードの増設・減設を行う際に、サーバー証明書の再作成を不要とするには、FQDN のサブドメインをワイルドカード形式にしてください。

3. 次のコマンドを実行します。

```
openssl req -sha256 -new -key server.key -out server.csr -config <手順 2 で作成したファイル>
```

オプション	説明
req	証明書署名要求(csr)の作成要求です。
-sha256	署名ハッシュアルゴリズムです。 SHA-2 に該当するアルゴリズムをご利用ください。
-key <秘密鍵ファイル名>	証明書署名要求を作成するための秘密鍵ファイル名を指定します。
-out <公開鍵ファイル名>	指定した名前で証明書署名要求ファイルを出力します。証明書署名要求ファイル名は任意です。拡張子は通常.csr を使います。
-config <手順 2 で作成したファイル>	手順 2 で作成した、証明書に SAN として登録する情報を記載した設定ファイル名を指定します。



注意

ハッシュアルゴリズムには、SHA-256 を使用してください。セキュリティ上の問題が起きるため、MD5 や SHA-1 を使用しないでください。

4. サーバー証明書に書かれる情報を、対話形式で入力します。

- Country Name(2 letter code)[AU] : 国名を 2 文字で入力します。(入力例 : JP)
- State or Province Name (full name)[Some-State] : 都道府県名を指定します。(入力例 : Kanagawa)
- Locality Name(eg, city)[] : 市区町村名または地域名を指定します。(入力例 : Odawara)
- Organization Name(eg, company)[Internet Widgits Pty Ltd] : 組織名を入力します。(入力例 : Hitachi)
- Organization Unit Name(eg, section)[] : 部署名を入力します。(入力例 : ITPD)
- Common Name(eg, server FQDN or YOUR name)[] : 任意の値を入力します。(入力例 : 未入力)
- Email Address [] : メールアドレスを入力します。(入力例 : 未入力)
- A challenge password [] : 入力不要です。
- An optional company name [] : 入力不要です。

```
$ openssl req -sha256 -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Kanagawa
```

```
Locality Name (eg, city) []:Odawara
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Hitachi
Organizational Unit Name (eg, section) []:ITPD
Common Name (eg, server FQDN or YOUR name) []:
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

22.8 署名付き証明書を取得する

秘密鍵と証明書署名要求を作成したら、公開鍵の署名付き証明書ファイルを取得します。署名付き証明書ファイルの取得には、次の 3 つの方法があります。

- ・ 自社内で運用している認証局の証明書を取得する(推奨)
- ・ VeriSign などの認証局に依頼して公式の証明書を取得する(推奨)
- ・ 自己署名をして証明書を作成する

自社内で運用している認証局の証明書を取得する

サーバー証明書の取得方法は、自社内の担当部署に問い合わせてください。自社内で運用しているサーバー証明書(以降、社内サーバー証明書)には、その妥当性を証明するためのルート証明書が対になって存在します。VSP One SDS Block とのセキュアな通信を実現するためには、ルート証明書を VSP One SDS Block と通信するクライアントマシンにインポートする必要があります。社内サーバー証明書とともに、ルート証明書も入手してください。ルート証明書のインポート方法は「ルート証明書をインポートする」を参照してください。

認証局に依頼して公式の証明書を取得する

署名付きの信頼できる証明書を取得する場合は、VeriSign などの認証局に証明書署名要求用ファイル(csr ファイル)を送付し、署名付きの公開鍵証明書(cert ファイル)を取得します。認証局へ依頼する手続きについては、依頼する認証局の Web サイトなどを参照してください。

この証明書を利用する場合は、コストと要件が増えますが、信頼性は向上します。

認証局に依頼する場合は、VSP One SDS Block をホスト名(Common Name)で指定してください。

自己署名付きの証明書を取得する

認証局に署名を依頼せずに、自己署名をして、署名付きの公開鍵証明書を作成できます。自己署名証明書の利用は、暗号化通信のテストなどの目的でだけ使用することをお勧めします。

自己署名付きの証明書に SAN を付与する場合は、SAN の情報を記載したファイルを用意し、次のコマンドを実行します。

(例)有効期間を 30 日に設定します。また、ハッシュアルゴリズムに SHA-256 を使用します。

```
openssl x509 -req -sha256 -days 30 -in server.csr -signkey server.key -
out server.crt -extfile <SAN の情報を記載したファイル>
```

(SAN の情報を記載したファイルの設定例)

subjectAltName = IP:<ストレージノードの管理ポートの IP アドレス>, IP:<ストレージノードの管理ポートの IP アドレス>, IP:<ストレージノードの管理ポートの IP アドレス>

コマンドを実行したディレクトリーに `server.crt` ファイルが作成されます。この `server.crt` ファイルが署名付きの公開鍵証明書になります。



注意

- ハッシュアルゴリズムには、**SHA-256** を使用してください。セキュリティ上の問題が起きるため、MD5 や SHA-1 を使用しないでください。
- 自己署名証明書を利用する場合、SSL/TLS 通信時に警告メッセージが表示されます。SSL/TLS 通信を行う場合は、警告を無視するオプションを付与してください。



メモ

X.509 v3 の拡張属性を付与した自己署名証明書を、信頼するルート証明書としてブラウザー、CLI にインポートする場合は、認証局として有効な証明書とするため、以下の属性値を設定する必要があります。

- X509v3 Basic Constraints が CA:TRUE となっていること
- X509v3 Key Usage を設定する場合、次の値が設定されていること
 - Digital Signature
 - Certificate Sign

22.9 秘密鍵のパスフレーズの確認と解除

パスフレーズが設定された秘密鍵は、VSP One SDS Block には適用できません。パスフレーズが設定されていたら、パスフレーズを解除します。

OpenSSL のコマンドは、Windows と Linux で共通です。Windows であればコマンドプロンプト、Linux であればターミナル端末など、コマンド実行が可能なコンソールから実行します。

前提条件

- 秘密鍵が作成済みであること

操作手順

- 秘密鍵ファイルが作成されているディレクトリーに移動します。
- 次のコマンドを実行します。

コマンドを実行したとき、パスフレーズが設定されていると、パスフレーズの入力促されます。次の手順に進みます。何も表示されなかった場合にはパスフレーズは設定されていません。次の手順は不要です。秘密鍵は VSP One SDS Block に適用できます。

```
openssl rsa -in <入力用の秘密鍵ファイル名> -out <出力用の秘密鍵ファイル名>
```



メモ

入力用と出力用の秘密鍵ファイル名を同じにすると、秘密鍵ファイルが上書きされます。上書きしたくない場合は別の名前を指定するか、バックアップを取ってから実行してください。

- パスフレーズの入力が促されたら、パスフレーズを入力します。
正しいパスフレーズを入力すると、パスフレーズが解除され、秘密鍵は VSP One SDS Block に適用できるようになります。

(例)

```
openssl rsa -in server.key -out server.key  
Enter pass phrase for server.key:
```

22.10 ルート証明書をインポートする

VSP One SDS Block Administrator で使うブラウザー、CLI には、デフォルトで信頼された認証局が発行した証明書の妥当性を証明するルート証明書がインポートされています。しかし、自組織の認証局で発行されたルート証明書などは、個別にインポートする必要があります。ルート証明書の取り扱い方法は、REST API、CLI、ブラウザーで異なります。



メモ

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される次のフィールドがサポートされます。

- 基本制限(Basic Constraints)
- キー使用法(Key Usage)
- サブジェクトキー識別子(Subject Key Identifier)
- 機関キー識別子(Authority Key Identifier)
- 証明書ポリシー(Certificate Policies)
- サブジェクト代替名(Subject Alternative Name)
- 名前の制限(Name Constraints)
- ポリシーの制限(Policy Constraints)
- 拡張キー使用法(Extended Key Usage)
- ポリシー禁止(Inhibit anyPolicy)

以降、コントローラーノードにルート証明書をインポートする手順を説明します。

22.10.1 REST API でルート証明書を扱う方法

REST API のリクエストを発行するプログラムによってルート証明書の利用方法は異なります。

ご使用のプログラムに合わせてルート証明書をインポートしてください。

22.10.2 CLI プログラムにルート証明書をインストールする方法

CLI プログラムではルート証明書を `certifi` という Python ライブラリーで管理しています。`certifi` はルート証明書のリスト情報を持っており、そこへルート証明書の情報を追加します。以下の手順に従って、実施してください。

操作手順

1. python3 インタプリターを起動します。

```
$ python3
```



メモ

Python3 のインストールのしかたによっては、"python"でよい場合や、"python3.4"と詳細バージョンまで必要な場合があります。

2. 以下に従って入力することで、`certifi` の証明書リストファイル(`cacert.pem`)のパスが表示されます。

```
>>>import certifi
>>>print(certifi.where())
```

(例)Linux で実行した場合

```
$ python3
>>>import certifi
>>>print(certifi.where())
/usr/lib/python3.4/site-package/certifi/cacert.pem
```

3. ルート証明書をテキストエディターなどで開き、内容をコピーします。
以下の範囲をコピーします。

```
-----BEGIN CERTIFICATE----- //ここから
:
:
:
-----END CERTIFICATE----- //ここまで
```

4. コピーした内容を、`certifi` の証明書リストファイル(`cacert.pem`)に追加します。
手順 2 で調べたパスにあるファイルをテキストエディターなどで開き、手順 3 でコピーした内容を、ファイルの末尾に追加します。



注意

- `certifi` ライブラリーのアップデートを行うと、再度ルート証明書のインストールを行う必要があります。
- インストールしたルート証明書を削除するには、手順 4 で `certifi` の証明書リストファイル(`cacert.pem`)に追記した内容を削除します。
- Python の `certifi` ライブラリーを `whl` ファイルを使用してインストールした場合の、ルート証明書のインストール方法を記載しています。OS のライブラリーパッケージを使用して `certifi` ライブラリーをインストールした場合は、各 OS の方法によるルート証明書のインストールが必要になる場合があります。



メモ

証明書リストファイル(`cacert.pem`)には、`#`で始まる行をコメントとして記載することができます。

22.10.3 ブラウザーにルート証明書をインポートする方法

インポート方法はブラウザーによって異なります。各ブラウザーの公式ページなどを参照して、ルート証明書をインポートしてください。



注意

信頼された証明機関以外から発行されたルート証明書をブラウザーにインポートする場合、セキュリティの観点で重大な問題を引き起こすおそれがあります。自組織のガイドラインなどをよく理解した上で、十分注意して扱ってください。

22.11 SSL/TLS 通信の署名付き証明書をインポートする

VSP One SDS Block との SSL/TLS 通信に任意の証明書を利用するには、秘密鍵と署名付き公開鍵証明書を VSP One SDS Block にインポートし、証明書を更新します。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「サーバー証明書をインポートする」

前提条件

- ・ 実行に必要なロール : Security
- ・ 秘密鍵が作成済みであること
- ・ 署名付き公開鍵証明書が取得済みであること
- ・ 秘密鍵の形式が PEM 形式または DER 形式であること
- ・ 署名付き公開鍵証明書の形式が X509 形式であること
- ・ 秘密鍵のパスフレーズが解除されていること
- ・ インポートできるサーバー証明書は、証明書と秘密鍵の一对です。
- ・ インポートするサーバー証明書は、RSA 形式は鍵長が 1024 ビット以上 8192 ビット以下のものをサポートしており、2048 ビット以上のものの利用を推奨します。ECC 形式は prime256v1、secp384r1、secp521r1 のうち、いずれかの楕円曲線のサーバー証明書の利用ができます。



メモ

- ・ X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される次のフィールドがサポートされます。
 - 基本制限(Basic Constraints)
 - キー使用法(Key Usage)
 - サブジェクトキー識別子(Subject Key Identifier)
 - 機関キー識別子(Authority Key Identifier)
 - 証明書ポリシー(Certificate Policies)
 - サブジェクト代替名(Subject Alternative Name)
 - 名前の制限(Name Constraints)
 - ポリシーの制限(Policy Constraints)
 - 拡張キー使用法(Extended Key Usage)
 - ポリシー禁止(Inhibit anyPolicy)
- ・ 証明書チェーンの階層数は、ルート CA 証明書を含めて 10 階層以下としてください。

操作手順

1. サーバー証明書をインポートします。
クラスターマスターノード(プライマリー)に対してのみ実行できます。
ストレージクラスターに転送するサーバー証明書ファイル(公開鍵)とサーバー証明書ファイル(秘密鍵)を指定してコマンドを実行します。
REST API : POST /v1/objects/server-certificate/actions/import/invoke
CLI : server_certificate_import
コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

3. サーバー証明書を検証します。

「SSL/TLS 通信のクライアント要件」を確認の上、任意の REST API や CLI を実行、またはブラウザを用いて VSP One SDS Block Administrator を表示し、セキュリティ警告*が表示されないことを確認してください。セキュリティ警告が表示された場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「SSL/TLS 証明書エラー発生時の対処」に従って対処してください。

* セキュリティ警告は以下のいずれかの単語、または文章を含んだエラーメッセージです。

"SSL"、"TLS"、"セキュリティ証明書"、"保護されません"、"安全ではありません"、"server certificate"

VSP One SDS Block Administrator を使用している場合は、ブラウザのエラー画面で、詳細なエラー情報を含めてメッセージを確認してください。

4. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



注意

誤ったサーバー証明書をインポートしたなどの操作ミスによって、再度インポートを実行する場合は、処理の競合を避けるために、実行間隔を 60 秒以上空けてください。

5. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。



注意

誤ったサーバー証明書をインポートしたなどの操作ミスによって、再度インポートを実行する場合は、処理の競合を避けるために、実行間隔を 60 秒以上空けてください。

22.12 SSL/TLS 通信のクライアント要件

SSL/TLS 通信のクライアント要件について説明します。

22.12.1 SSL/TLS 通信のクライアント要件<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

サーバー証明書検証を有効にして接続する場合の要件

サーバー証明書検証を有効にして接続する場合は、REST API、CLI、または VSP One SDS Block Administrator での操作で指定する接続先が、サーバー証明書の Subject Alternative Name(SAN) または CN の情報に含まれていることが要件になります。

この項では、Subject Alternative Name を SAN と表記しています。



メモ

- SSL/TLS 通信のサーバー証明書の検証では、接続元は「接続元が指定した接続先(IP アドレス,FQDN)」が「接続先のサーバー証明書の SAN または CN」に含まれていることを検証します。
- VSP One SDS Block で、Universal Replicator 利用時に RAID Manager を使用する場合は、SAN に FQDN は指定できません。

サーバー証明書の SAN または CN の情報ごとの、サーバー証明書検証する際に指定すべき接続先の例を以下に示します。

「証明書署名要求を作成する」に従ってサーバー証明書を作成すると、次表 No.1 または No.2 に該当するサーバー証明書になっています。

No.	SAN	CN	サーバー証明書検証する際に指定すべき接続先
1	• クラスター代表 IP アドレスに対応する FQDN (例: storage.example.com) • ストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN(ノード数分) (例: storage-node1.example.com, storage-node2.example.com,...)	-	以下のうちのどちらかを指定します。 • クラスター代表 IP アドレスに対応する FQDN • ストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN IP アドレスでの指定ではサーバー証明書検証エラーになります。
2	クラスター代表 IP アドレスに対応する FQDN とストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN の、サブドメインをワイルドカード形式で指定したもの (例: *.example.com)	-	
3	-	クラスター代表 IP アドレスに対応する FQDN とストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN の、サブドメインをワイルドカード形式で指定したもの (例: *.example.com)	
4	• クラスター代表 IP アドレス (例: 192.0.2.100) • ストレージノードの管理ポートの IP アドレス(ノード数分) (例: 192.0.2.101, 192.0.2.102,...)	-	以下のうちのどちらかを指定します。 • クラスター代表 IP アドレス • ストレージノードの管理ポートの IP アドレス FQDN での指定ではサーバー証明書検証エラーになります。

暗号スイートの要件

REST API を利用するクライアントソフトウェア、VSP One SDS Block Administrator を利用するブラウザーは、以下の SSL/TLS の暗号スイートの要件を満たすことが必要です。

VSP One SDS Block にインポートしているサーバー証明書の種類	暗号スイートの要件
RSA 証明書	以下のうち 1 つ以上をサポートしていること • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECC 証明書	以下のうち 1 つ以上をサポートしていること • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256



メモ

- VSP One SDS Block にインポートするサーバー証明書が RSA 証明書か ECC 証明書かによって、暗号スイートの要件が異なります。デフォルトでインポートされているサーバー証明書は RSA 証明書です。また、このマニュアルに従って、サーバー証明書を作成・インポートした場合は、RSA 証明書がインポートされます。
 - 暗号スイートの要件を満たさない場合、SSL/TLS 通信が失敗します。
 - Linux*のコントローラーノードで動作する CLI は、上記の暗号スイートをサポートしています。
 - Windows*のコントローラーノードで動作する CLI は、上記の暗号スイートをサポートしていますが、暗号スイートが有効化されている必要があります。OS のデフォルトでは有効化されています。詳細は Microsoft 社のマニュアルを参照してください。
 - CLI 以外について、コントローラーノードで、上記の暗号スイートをサポートしているかどうかは、REST API を使用するクライアントソフトウェア/VSP One SDS Block Administrator を利用するブラウザーのドキュメントを参照してください。
- * コントローラーノードでサポートする OS は、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

22.12.2 SSL/TLS 通信のクライアント要件<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

サーバー証明書検証を有効にして接続する場合の要件

サーバー証明書検証を有効にして接続する場合は、REST API、CLI、または VSP One SDS Block Administrator での操作で指定する接続先が、サーバー証明書の Subject Alternative Name(SAN) または CN の情報に含まれていることが要件になります。

この項では、Subject Alternative Name を SAN と表記しています。



メモ

- SSL/TLS 通信のサーバー証明書の検証では、接続元は「接続元が指定した接続先(IP アドレス,FQDN)」が「接続先のサーバー証明書の SAN または CN」に含まれていることを検証します。
- VSP One SDS Block で、Universal Replicator 利用時に RAID Manager を使用する場合は、SAN に FQDN は指定できません。

サーバー証明書の SAN または CN の情報ごとの、サーバー証明書検証する際に指定すべき接続先の例を以下に示します。

「証明書署名要求を作成する」に従ってサーバー証明書を作成すると、次表 No.1 または No.2 に該当するサーバー証明書になっています。

No.	SAN	CN	サーバー証明書検証する際に指定すべき接続先
1	- ロードバランサーの FQDN (例: storage.example.com) - ストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN(ノード数分) (例: storage-node1.example.com, storage-node2.example.com,...)	-	以下のうちのどちらかを指定します。 - ロードバランサーの FQDN - ストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN IP アドレスでの指定ではサーバー証明書検証エラーになります。
2	ロードバランサーの FQDN とストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN の、サブドメインをワイルドカード形式で指定したもの (例: *.example.com)	-	
3	-	ロードバランサーの FQDN とストレージノードの管理ポートの IP アドレスそれぞれに対応する FQDN の、サブドメインをワイルドカード形式で指定したもの (例: *.example.com)	
4	- ロードバランサーの IP アドレス (例: 192.0.2.100) - ストレージノードの管理ポートの IP アドレス(ノード数分) (例: 192.0.2.101, 192.0.2.102,...)	-	以下のうちのどちらかを指定します。 - ロードバランサーの IP アドレス - ストレージノードの管理ポートの IP アドレス FQDN での指定ではサーバー証明書検証エラーになります。

暗号スイートの要件

REST API を利用するクライアントソフトウェア、VSP One SDS Block Administrator を利用するブラウザーは、以下の SSL/TLS の暗号スイートの要件を満たすことが必要です。

VSP One SDS Block にインポートしているサーバー証明書の種類	暗号スイートの要件
RSA 証明書	以下のうち 1 つ以上をサポートしていること - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECC 証明書	以下のうち 1 つ以上をサポートしていること - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256



メモ

- VSP One SDS Block にインポートするサーバー証明書が RSA 証明書か ECC 証明書かによって、暗号スイートの要件が異なります。デフォルトでインポートされているサーバー証明書は RSA 証明書です。また、このマニュアルに従って、サーバー証明書を作成・インポートした場合は、RSA 証明書がインポートされます。
 - 暗号スイートの要件を満たさない場合、SSL/TLS 通信が失敗します。
 - Linux*のコントローラーノードで動作する CLI は、上記の暗号スイートをサポートしています。
 - Windows*のコントローラーノードで動作する CLI は、上記の暗号スイートをサポートしていますが、暗号スイートが有効化されている必要があります。OS のデフォルトでは有効化されています。詳細は Microsoft 社のマニュアルを参照してください。
 - CLI 以外について、コントローラーノードで、上記の暗号スイートをサポートしているかどうかは、REST API を使用するクライアントソフトウェア/VSP One SDS Block Administrator を利用するブラウザのドキュメントを参照してください。
- * コントローラーノードでサポートする OS は、ご使用のクラウドプラットフォームに対応する「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

22.13 サーバー証明書に関する警告メッセージが表示されたときの対処

REST API、CLI、または VSP One SDS Block Administrator(ブラウザ)での操作で、VSP One SDS Block と SSL/TLS 通信した場合、サーバー証明書が信頼された証明機関から発行されたものではないときは、サーバー証明書に関する警告メッセージが表示されます。この表示をなくすためには、信頼された証明機関から発行されたサーバー証明書を VSP One SDS Block にインポートしてください。

また「SSL/TLS 通信のクライアント要件」を満たしているかを確認してください。

警告を無視した場合でも、安全な通信ではありませんが SSL/TLS 通信を行うことはできます。(通信の暗号化は行われますが、通信相手の認証は行われません。)

- REST API で警告が表示された場合は、REST API を発行するプログラムやコマンドに合わせて、証明書に関する警告を無視する処理追加やオプション指定を実施してください。
- ブラウザーで警告が表示された場合は「サイトの閲覧を続行する」を実行してください。ご利用のブラウザによって操作が若干異なります。
- CLI での操作で警告が表示された場合は、`--ignore_certificate_errors` オプションを追加して警告を無視してください。

CHAP 認証を利用する

- 23.1 CHAP ユーザーを作成して CHAP 認証を設定する
- 23.2 CHAP ユーザー情報の一覧を取得する
- 23.3 CHAP ユーザー情報を個別に取得する
- 23.4 CHAP ユーザー情報を編集する
- 23.5 CHAP ユーザーを削除する
- 23.6 ターゲット動作のコンピュートポートの認証設定を取得する
- 23.7 ターゲット動作のコンピュートポートの認証設定を編集する
- 23.8 CHAP ユーザーに対してコンピュートポートへのアクセスを許可する
- 23.9 コンピュートポートへのアクセスを許可した CHAP ユーザー情報の取得
- 23.10 CHAP ユーザーに対してコンピュートポートへのアクセス許可を解除する

23.1 CHAP ユーザーを作成して CHAP 認証を設定する

ストレージシステムへの接続要求が、正当なコンピュータノードからのものであることを確認するための、CHAP(Challenge-Handshake Authentication Protocol)による認証が利用できます。

コンピュータノードが iSCSI 接続のときのみ利用できます。

CHAP 認証を利用するかどうかは、コンピュータポートごとに設定できます。

以下では CHAP ユーザーを作成し、CHAP 認証を設定する手順を説明します。

CHAP 認証に関するシステムの要件は以下のとおりです。

項目	要件	備考
CHAP ユーザーの最大数	プロテクションドメイン当たり 1,024	最大コンピュータノード数と同じ です。
CHAP ユーザー名と CHAP シークレットの組み合わせ	CHAP ユーザー名と CHAP シークレットの組み合わせは、システム内でユニークであることが必須です。	
CHAP ユーザー名	文字数：1～223 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、Space、記号(. - + @ _ = : [] ~)	以下のパラメーター設定に適用されます。 - targetChapUserName(CLI : --target_chap_user_name) - initiatorChapUserName(CLI : --initiator_chap_user_name)
CHAP シークレット	文字数：12～32 使用可能文字：数字(0-9)、英大文字(A-Z)、英小文字(a-z)、Space、記号(. - + @ _ = : [] ~)	以下のパラメーター設定に適用されます。 - targetChapSecret - initiatorChapSecret



注意

- CHAP 認証設定の変更時、VSP One SDS Block は、安全のために設定変更前の状態での接続を破棄することを目的とし、コンピュータノードとコンピュータポート間の iSCSI 接続を強制的に切断します。事前に各種 OS の切断手順に従ってコンピュータノードとコンピュータポート間の iSCSI 接続を切断することをお勧めします。CHAP 認証設定の変更後、変更した内容に合わせて改めて iSCSI 接続を確立してください。
- VPS を作成している場合、CHAP 認証設定を実施することで VPS に所属するコンピュータノードからストレージシステムへの接続要求時にも CHAP 認証が必要になります。そのため、CHAP 認証設定を行った場合は、必ず VPS 管理者に連絡してください。

前提条件

- 実行に必要なロール：Security

操作手順

- CHAP ユーザーを作成します。

CHAP ユーザー名と CHAP シークレットを指定してコマンドを実行します。

必要に応じて、双方向認証用の CHAP ユーザー名と CHAP シークレットを指定してください。

REST API : POST /v1/objects/chap-users

CLI : chap_user_create

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

3. コンピュートポートの一覧を取得して指定するコンピュータポートの ID を確認します。

CLI を使いコンピュータポートを iSCSI 名で指定する場合は、コンピュータポートの iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

4. コンピュートポートの認証設定を編集します。

コンピュータポートの ID、コンピュータポート側の認証方式、iSCSI 接続におけるディスクバリー時の CHAP 認証有効/無効、CHAP の双方向認証有効/無効を指定してコマンドを実行します。

CLI を使う場合はコンピュータポートの ID の代わりに iSCSI 名が指定できます。

同じコンピュータポートにおいて、CHAP ユーザー名の重複はできません。

REST API : PATCH /v1/objects/port-auth-settings/<id >

CLI : port_auth_setting_set

コマンド実行後に表示されるジョブの ID を確認します。

5. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

6. CHAP ユーザーに対してコンピュータポートへのアクセスを許可します。

コンピュータポートの ID と CHAP 認証でアクセスを許可する CHAP ユーザーの ID を指定してコマンドを実行します。

CLI を使う場合は CHAP ユーザーの ID の代わりに CHAP ユーザー名が指定できます。

REST API : POST /v1/objects/port-auth-settings/<id >/chap-users

CLI : port_auth_setting_chap_user_create

コマンド実行後に表示されるジョブの ID を確認します。

7. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

8. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

9. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

23.2 CHAP ユーザー情報の一覧を取得する

CHAP ユーザーの情報を一覧で取得します。以下の情報が得られます。

- `id` : CHAP ユーザー ID(uuid)
- `targetChapUserName` : コンピュートポートすなわちターゲット側で CHAP 認証する際に利用する CHAP ユーザー名
- `initiatorChapUserName` : コンピュートノードのイニシエーター側で CHAP 認証する際に利用する CHAP ユーザー名

前提条件

- 実行に必要なロール : Security

操作手順

1. CHAP ユーザーの一覧を取得します。
REST API : GET /v1/objects/chap-users
CLI : chap_user_list

23.3 CHAP ユーザー情報を個別に取得する

指定した ID の CHAP ユーザーについて、以下の情報を取得します。

- `portIds` : CHAP 認証で当該 CHAP ユーザーがアクセス許可されている、コンピューポート ID(uuid)の一覧
- `id` : CHAP ユーザー ID(uuid)
- `targetChapUserName` : コンピュートポートすなわちターゲット側で CHAP 認証する際に利用する CHAP ユーザー名
- `initiatorChapUserName` : コンピュートノードのイニシエーター側で CHAP 認証する際に利用する CHAP ユーザー名

前提条件

- 実行に必要なロール : Security

操作手順

1. CHAP ユーザーの ID を確認します。
CLI を使い CHAP ユーザーを CHAP ユーザー名で指定する場合は、CHAP ユーザー名を確認します。
REST API : GET /v1/objects/chap-users
CLI : chap_user_list
2. CHAP ユーザーの ID を指定して CHAP ユーザーの情報を取得します。
CLI を使う場合は CHAP ユーザーの ID の代わりに CHAP ユーザー名が指定できます。

REST API : GET /v1/objects/chap-users/<chapUserId >

CLI : chap_user_show

23.4 CHAP ユーザー情報を編集する

CHAP ユーザー情報を編集します。

前提条件

- 実行に必要なロール : Security

操作手順

1. CHAP ユーザーの ID を確認します。

CLI を使い CHAP ユーザーを CHAP ユーザー名で指定する場合は、CHAP ユーザー名を確認します。

REST API : GET /v1/objects/chap-users

CLI : chap_user_list

2. CHAP ユーザーの情報を編集します。

CHAP ユーザーの ID、CHAP ユーザー名、CHAP シークレットを指定してコマンドを実行します。必要に応じて、双方向認証用の CHAP ユーザー名と CHAP シークレットを指定してください。

CLI を使う場合は CHAP ユーザーの ID の代わりに CHAP ユーザー名が指定できます。

REST API : PATCH /v1/objects/chap-users/<chapUserId >

CLI : chap_user_set

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

4. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

5. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

23.5 CHAP ユーザーを削除する

CHAP ユーザーを削除します。

前提条件

- 実行に必要なロール : Security

操作手順

1. 削除する CHAP ユーザーの ID を確認します。
CLI を使い CHAP ユーザーを CHAP ユーザー名で指定する場合は、CHAP ユーザー名を確認します。
REST API : GET /v1/objects/chap-users
CLI : chap_user_list
2. CHAP ユーザーを削除します。
CHAP ユーザーの ID を指定してコマンドを実行します。
CLI を使う場合は CHAP ユーザーの ID の代わりに CHAP ユーザー名が指定できます。
REST API : DELETE /v1/objects/chap-users/<chapUserId >
CLI : chap_user_delete
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの ID を指定してジョブの state を確認します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
4. ≪Bare metal≫構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
5. ≪Cloud for AWS≫構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

23.6 ターゲット動作のコンピュータポートの認証設定を取得する

指定した ID のターゲット動作のコンピュータポートの認証設定について、以下の情報を取得します。

- id : コンピュータポートの ID(uuid)
- authMode : コンピュータポート側の認証方式
- isDiscoveryChapAuth : iSCSI 接続におけるディスカバリー時の CHAP 認証有効/無効
- isMutualChapAuth : CHAP の双方向認証有効/無効

前提条件

- 実行に必要なロール : Security

操作手順

1. コンピュートポートの ID を確認します。

CLI を使いコンピュートポートを iSCSI 名で指定する場合は、コンピュートポートの iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

2. コンピュートポートの認証設定を取得します。

コンピュートポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュートポートの ID の代わりに iSCSI 名が指定できます。

REST API : GET /v1/objects/port-auth-settings/<id >

CLI : port_auth_setting_show

23.7 ターゲット動作のコンピュートポートの認証設定を編集する

ターゲット動作のコンピュートポートの認証設定を編集します。



注意

- CHAP 認証設定の変更時、VSP One SDS Block は、安全のために設定変更前の状態での接続を破棄することを目的とし、コンピュートノードとコンピュートポート間の iSCSI 接続を強制的に切断します。事前に各種 OS の切断手順に従ってコンピュートノードとコンピュートポート間の iSCSI 接続を切断することをお勧めします。CHAP 認証設定の変更後、変更した内容に合わせて改めて iSCSI 接続を確立してください。
- VPS を作成している場合、本設定を実施することで VPS に所属するコンピュートノードからストレージシステムへの接続状態に影響が及びます。そのため、本設定を行った場合は、必ず VPS 管理者に連絡してください。

前提条件

- 実行に必要なロール : Security

操作手順

1. コンピュートポートの ID を確認します。

CLI を使いコンピュートポートを iSCSI 名で指定する場合は、コンピュートポートの iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

2. コンピュートポートの認証設定を編集します。

コンピュートポートの ID とコンピュートポートの認証設定のパラメーターを指定してコマンドを実行します。

CLI を使う場合はコンピュートポートの ID の代わりに iSCSI 名が指定できます。

REST API : PATCH /v1/objects/port-auth-settings/<id >

CLI : port_auth_setting_set

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

5. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

23.8 CHAP ユーザーに対してコンピュータポートへのアクセスを許可する

CHAP ユーザーに対してコンピュータポートへ CHAP 認証でのアクセスを許可します。



メモ

コンピュータポートへ CHAP 認証でのアクセスを許可後にストレージノードを増設した場合、増設したストレージノードのコンピュータポートに対しても CHAP ユーザーのアクセス許可をしてください。

前提条件

- 実行に必要なロール : Security

操作手順

1. コンピュータポートの ID を確認します。

CLI を使いコンピュータポートを iSCSI 名で指定する場合は、コンピュータポートの iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

2. アクセスする CHAP ユーザーの ID を確認します。

CLI を使い CHAP ユーザーを CHAP ユーザー名で指定する場合は、CHAP ユーザー名を確認します。

REST API : GET /v1/objects/chap-users

CLI : chap_user_list

3. CHAP ユーザーからのアクセスを許可します。

コンピュータポートの ID と CHAP ユーザーの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータポートの ID の代わりに iSCSI 名が、CHAP ユーザーの ID の代わりに CHAP ユーザー名が指定できます。

REST API : POST /v1/objects/port-auth-settings/<id >/chap-users

CLI : port_auth_setting_chap_user_create

コマンド実行後に表示されるジョブの ID を確認します。

4. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

5. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

6. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

23.9 コンピュートポートへのアクセスを許可した CHAP ユーザー情報の取得

コンピューポートへのアクセスを許可した CHAP ユーザー情報を一覧または個別に取得できます。

23.9.1 取得できるコンピューポートへのアクセスを許可した CHAP ユーザー情報

以下の情報が一覧または個別に取得できます。

- id : コンピューポートへのアクセスを許可した CHAP ユーザー ID(uuid)
- targetChapUserName : コンピューポートすなわちターゲット側で CHAP 認証する際に利用する CHAP ユーザー名
- initiatorChapUserName : コンピューポートのイニシエーター側で CHAP 認証する際に利用する CHAP ユーザー名

23.9.2 コンピューポートへのアクセスを許可した CHAP ユーザー情報の一覧を取得する

コンピューポートへのアクセスを許可した CHAP ユーザー情報の一覧を取得します。

前提条件

- 実行に必要なロール : Security

操作手順

1. コンピューポートの ID を確認します。

CLI を使いコンピューポートを iSCSI 名で指定する場合は、コンピューポートの iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

2. コンピューポートへのアクセスを許可した CHAP ユーザーの一覧を取得します。

コンピューポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピューポートの ID の代わりに iSCSI 名が指定できます。

REST API : GET /v1/objects/port-auth-settings/<id>/chap-users

CLI : port_auth_setting_chap_user_list

23.9.3 コンピュートポートへのアクセスを許可した CHAP ユーザー情報を個別に取得する

指定した ID のコンピュートポートへのアクセスを許可した CHAP ユーザー情報を取得します。

前提条件

- 実行に必要なロール : Security

操作手順

1. コンピュートポートの ID を確認します。

CLI を使いコンピュートポートを iSCSI 名で指定する場合は、コンピュートポートの iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

2. CHAP ユーザーの ID を確認します。

CLI を使い CHAP ユーザーを CHAP ユーザー名で指定する場合は、CHAP ユーザー名を確認します。

REST API : GET /v1/objects/chap-users

CLI : chap_user_list

3. アクセスを許可した CHAP ユーザーの情報を取得します。

コンピュートポートの ID と CHAP ユーザーの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュートポートの ID の代わりに iSCSI 名が、CHAP ユーザーの ID の代わりに CHAP ユーザー名が指定できます。

REST API : GET /v1/objects/port-auth-settings/<id>/chap-users/<chapUserId>

CLI : port_auth_setting_chap_user_show

23.10 CHAP ユーザーに対してコンピュートポートへのアクセス許可を解除する

CHAP ユーザーに対して、ターゲット動作のコンピュートポートへの CHAP 認証でのアクセス許可を解除します。



注意

- VPS を作成している場合、本設定を実施することで VPS に所属するコンピュートノードからストレージシステムへの接続状態に影響が及びます。そのため、本設定を行った場合は、必ず VPS 管理者に連絡してください。

前提条件

- 実行に必要なロール : Security

操作手順

1. コンピュートポートの ID を確認します。

CLI を使いコンピュートポートを iSCSI 名で指定する場合は、コンピュートポートの iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

2. アクセス許可を解除する CHAP ユーザーの ID を確認します。

CLI を使い CHAP ユーザーを CHAP ユーザー名で指定する場合は、CHAP ユーザー名を確認します。

REST API : GET /v1/objects/chap-users

CLI : chap_user_list

3. CHAP ユーザーに対して、コンピュートポートへのアクセス許可を解除します。

コンピュートポートの ID と CHAP ユーザーの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュートポートの ID の代わりに iSCSI 名が、CHAP ユーザーの ID の代わりに CHAP ユーザー名が指定できます。

REST API : DELETE /v1/objects/port-auth-settings/<id>/chap-users/<chapUserId>

CLI : port_auth_setting_chap_user_delete

コマンド実行後に表示されるジョブの ID を確認します。

4. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

5. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

6. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

システムの性能情報・容量情報を取得する

- 24.1 ストレージシステムの性能情報と容量情報
- 24.2 管理ポートの性能情報の取得
- 24.3 ドライブの性能情報の取得
- 24.4 ストレージノード間ポートの性能情報の取得
- 24.5 ストレージプールの容量情報の取得
- 24.6 ストレージプールの性能情報の取得
- 24.7 コンピュートポートの性能情報の取得
- 24.8 ストレージクラスターの性能情報(低解像度)を取得する
- 24.9 ストレージノードの性能情報の取得
- 24.10 ボリュームの容量情報の取得
- 24.11 ボリュームの性能情報の取得
- 24.12 ジャーナルの性能情報の取得

24.1 ストレージシステムの性能情報と容量情報

VSP One SDS Block が収集している各リソースについての性能情報と容量情報を取得できます。

ユーザーが取得できる性能情報には、1 分周期で収集する時間的低解像度(以降、低解像度)の情報と、5 秒周期で収集する時間的高解像度(以降、高解像度)の情報があります。低解像度の情報とは履歴からの情報であり、高解像度の情報とは最新の情報です。(一部の情報は、低解像度でのみ取得されます。)

低解像度の情報は最大で 2 日分保持されます。最大保持日数を超えた低解像度の情報は古い順に削除されます。

高解像度の情報はストレージシステムに問題が発生したときには、問題が発生した特定のリソースに関する高解像度の情報を取得して、問題解決に役立ててください。

低解像度の情報は定期的に取得することで、正常稼働しているか、異常発生はないかなどについての確認にご使用ください。

24.2 管理ポートの性能情報の取得

管理ポートの性能情報が一覧または個別に取得できます。

24.2.1 取得できる管理ポートの性能情報

以下の情報が一覧または個別に取得できます。

- id : 管理ポートの ID(uuid)
- receiveTransferRate : 1 秒当たりのデータ受信量[MiB/sec]
- sendTransferRate : 1 秒当たりのデータ送信量[MiB/sec]

24.2.2 管理ポートの性能情報(低解像度)の一覧を取得する

各管理ポートの性能情報(低解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 管理ポートの性能情報の一覧を取得します。
REST API : GET /v1/objects/performances/control-ports
CLI : control_port_performance_list

24.2.3 管理ポートの性能情報(高解像度)の一覧を取得する

各管理ポートの性能情報(高解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得する管理ポートの ID を確認します。
REST API : GET /v1/objects/control-ports
CLI : control_port_list
2. 管理ポートの性能情報の一覧を取得します。
管理ポートの ID をクエリパラメーターで指定してコマンドを実行します。管理ポートの ID は最大で 32 個まで指定できます。
REST API : GET /v1/objects/detail-performances/control-ports
CLI : control_port_detail_performance_list

24.2.4 管理ポートの性能情報を個別に取得する

指定した ID の管理ポートの性能情報を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得する管理ポートの ID を確認します。
REST API : GET /v1/objects/control-ports
CLI : control_port_list
2. 性能情報を取得します。
管理ポートの ID を指定してコマンドを実行します。
REST API(低解像度) : GET /v1/objects/performances/control-ports/<id >
REST API(高解像度) : GET /v1/objects/detail-performances/control-ports/<id >
CLI(低解像度) : control_port_performance_show
CLI(高解像度) : control_port_detail_performance_show

24.3 ドライブの性能情報の取得

ドライブの性能情報が一覧または個別に取得できます。

24.3.1 取得できるドライブの性能情報

以下の情報が一覧または個別に取得できます。

- id : ドライブの ID(uuid)
- readIOPS : 1 秒当たりのリード I/O 数[IOPS]
- writeIOPS : 1 秒当たりのライト I/O 数[IOPS]
- readTransferRate : 1 秒当たりのリード転送量[MiB/sec]
- writeTransferRate : 1 秒当たりのライト転送量[MiB/sec]
- responseTime : 平均応答時間[msec]
- usage : 当該ドライブの I/O 実行時間 / 経過時間の割合[%]

24.3.2 ドライブの性能情報(低解像度)の一覧を取得する

各ドライブの性能情報(低解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報の一覧を取得します。

REST API : GET /v1/objects/performances/drives

CLI : drive_performance_list



メモ

以下に示すような操作、または障害が発生した場合には、コンピュータノードからの I/O とは非同期にドライブへのアクセスが発生することがあります。システムの負荷が高い場合には一時的に性能に影響を及ぼすことがあります。

- ストレージプール拡張
- ボリューム操作
- ストレージノード保守
- ストレージノード増設・減設
- ドライブ増設・減設
- ストレージノード障害
- ドライブ障害

24.3.3 ドライブの性能情報(高解像度)の一覧を取得する

各ドライブの性能情報(高解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得するドライブの ID を確認します。

REST API : GET /v1/objects/drives

CLI : drive_list

2. 性能情報の一覧を取得します。

ドライブの ID をクエリーパラメーターで指定してコマンドを実行します。ドライブの ID は最大で 32 個まで指定できます。

REST API : GET /v1/objects/detail-performances/drives

CLI : drive_detail_performance_list



メモ

以下に示すような操作、または障害が発生した場合には、コンピュータノードからの I/O とは非同期にドライブへのアクセスが発生することがあります。システムの負荷が高い場合には一時的に性能に影響を及ぼすことがあります。

- ストレージプール拡張

- ボリューム操作
- ストレージノード保守
- ストレージノード増設・減設
- ドライブ増設・減設
- ストレージノード障害
- ドライブ障害

24.3.4 ドライブの性能情報を個別に取得する

指定した ID のドライブについて、以下の性能情報を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得するドライブの ID を確認します。

REST API : GET /v1/objects/drives

CLI : drive_list

2. 性能情報を取得します。

ドライブの ID を指定してコマンドを実行します。

REST API(低解像度) : GET /v1/objects/performances/drives/<id >

REST API(高解像度) : GET /v1/objects/detail-performances/drives/<id >

CLI(低解像度) : drive_performance_show

CLI(高解像度) : drive_detail_performance_show



メモ

以下に示すような操作、または障害が発生した場合には、コンピュータノードからの I/O とは非同期にドライブへのアクセスが発生することがあります。システムの負荷が高い場合には一時的に性能に影響を及ぼすことがあります。

- ストレージプール拡張
- ボリューム操作
- ストレージノード保守
- ストレージノード増設・減設
- ドライブ増設・減設
- ストレージノード障害
- ドライブ障害

24.4 ストレージノード間ポートの性能情報の取得

ストレージノード間ポートの性能情報が一覧または個別に取得できます。

24.4.1 取得できるストレージノード間ポートの性能情報

以下の情報が一覧または個別に取得できます。

- id : ストレージノード間ポートの ID(uuid)

- receiveTransferRate : 1 秒当たりのデータ受信量[MiB/sec]
- sendTransferRate : 1 秒当たりのデータ送信量[MiB/sec]

24.4.2 ストレージノード間ポートの性能情報(低解像度)の一覧を取得する

各ストレージノード間ポートの性能情報(低解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. ストレージノード間ポートの性能情報の一覧を取得します。
REST API : GET /v1/objects/performances/internode-ports
CLI : internode_port_performance_list

24.4.3 ストレージノード間ポートの性能情報(高解像度)の一覧を取得する

各ストレージノード間ポートの性能情報(高解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得するストレージノード間ポートの ID を確認します。
REST API : GET /v1/objects/internode-ports
CLI : internode_port_list
2. ストレージノード間ポートの性能情報の一覧を取得します。
ストレージノード間ポートの ID をクエリーパラメーターで指定してコマンドを実行します。
ストレージノード間ポートの ID は最大で 32 個まで指定できます。
REST API : GET /v1/objects/detail-performances/internode-ports
CLI : internode_port_detail_performance_list

24.4.4 ストレージノード間ポートの性能情報を個別に取得する

指定した ID のストレージノード間ポートの性能情報を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得するストレージノード間ポートの ID を確認します。
REST API : GET /v1/objects/internode-ports
CLI : internode_port_list
2. 性能情報を取得します。
ストレージノード間ポートの ID を指定してコマンドを実行します。

REST API(低解像度) : GET /v1/objects/performances/internode-ports/<id >
REST API(高解像度) : GET /v1/objects/detail-performances/internode-ports/<id >
CLI(低解像度) : internode_port_performance_show
CLI(高解像度) : internode_port_detail_performance_show

24.5 ストレージプールの容量情報の取得

ストレージプールの容量情報が一覧または個別に取得できます。

24.5.1 取得できるストレージプールの容量情報

以下の情報が一覧または個別に取得できます。

- id : ストレージプールの ID(uuid)
- usedCapacity : 総使用量[MiB]

24.5.2 ストレージプールの容量情報(低解像度)の一覧を取得する

各ストレージプールの容量情報(低解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. ストレージプールの容量情報の一覧を取得します。
REST API : GET /v1/objects/performances/pool-capacities
CLI : pool_capacity_performance_list

24.5.3 ストレージプールの容量情報(低解像度)を個別に取得する

指定した ID のストレージプールの容量情報(低解像度)を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 容量情報を取得するストレージプールの ID を確認します。
CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。
REST API : GET /v1/objects/pools
CLI : pool_list
2. 容量情報を取得します。
ストレージプールの ID を指定してコマンドを実行します。
CLI を使う場合はストレージプールの ID の代わりに名前が指定できます。
REST API : GET /v1/objects/performances/pool-capacities/<id >
CLI : pool_capacity_performance_show

24.6 ストレージプールの性能情報の取得

ストレージプールの性能情報が一覧または個別に取得できます。

24.6.1 取得できるストレージプールの性能情報

以下の情報が一覧または個別に取得できます。

- **id** : ストレージプールの ID(uuid)
- **volumeReadIOPS** : ホストおよびボリュームマイグレーションによる当該ストレージプールに属するボリュームの 1 秒当たりのリード I/O 数[IOPS]
- **volumeWriteIOPS** : ホストおよびボリュームマイグレーションによる当該ストレージプールに属するボリュームの 1 秒当たりのライト I/O 数[IOPS]
- **volumeReadTransferRate** : ホストおよびボリュームマイグレーションによる当該ストレージプールに属するボリュームの 1 秒当たりのリード転送量[MiB/sec]
- **volumeWriteTransferRate** : ホストおよびボリュームマイグレーションによる当該ストレージプールに属するボリュームの 1 秒当たりのライト転送量[MiB/sec]
- **readResponseTime** : ホストおよびボリュームマイグレーションによる当該ストレージプールに属するボリュームのリード平均応答時間[msec]
- **writeResponseTime** : ホストおよびボリュームマイグレーションによる当該ストレージプールに属するボリュームのライト平均応答時間[msec]
- **readHitRate** : ホストおよびボリュームマイグレーションによる当該ストレージプールに属するボリュームの読み込みリクエストに対するキャッシュヒット率[%]
- **writeHitRate** : ホストおよびボリュームマイグレーションによる当該ストレージプールに属するボリュームの書き込みリクエストに対するキャッシュヒット率[%]
- **urWriteIOPS** : ホストから Universal Replicator の当該ストレージプールに属する P-VOL への 1 秒当たりのライト I/O 数[IOPS]
- **urWriteTransferRate** : ホストから Universal Replicator の当該ストレージプールに属する P-VOL への 1 秒当たりのライト転送量[MiB/sec]
- **urInitialCopyHitRate** : Universal Replicator の形成コピーによる当該ストレージプールに属する P-VOL の読み込みリクエストに対するキャッシュヒット率[%]
- **urInitialCopyTransferRate** : Universal Replicator の形成コピーによる当該ストレージプールに属する P-VOL の 1 秒当たりのデータ送信量[MiB/sec]
- **masterJournalRIOPS** : 当該ストレージプールにおける応答した 1 秒当たりのリードジャーナルコマンド数[IOPS]
- **masterJournalCount** : 当該ストレージプールにおけるジャーナルデータの 1 秒当たりの送信数
- **masterJournalTransferRate** : 当該ストレージプールにおけるジャーナルデータの 1 秒当たりの送信量[MiB/sec]
- **masterJournalRIOResponseTime** : 当該ストレージプールにおけるリードジャーナルコマンドを受信してから応答を送信するまでの平均時間[msec]
- **remoteJournalRIOPS** : 当該ストレージプールにおける発行した 1 秒当たりのリードジャーナルコマンド数[IOPS]
- **remoteJournalCount** : 当該ストレージプールにおけるジャーナルデータの 1 秒当たりの受信数

- `remoteJournalTransferRate` : 当該ストレージプールにおけるジャーナルデータの 1 秒当たりの受信量[MiB/sec]
- `remoteJournalRIOResponseTime` : 当該ストレージプールにおけるリードジャーナルコマンドを送信してから応答を受信するまでの平均時間[msec]

24.6.2 ストレージプールの性能情報(低解像度)の一覧を取得する

各ストレージプールの性能情報(低解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : `Storage`、`RemoteCopy`、`Monitor`、または `Resource`

操作手順

1. ストレージプールの性能情報の一覧を取得します。

REST API : `GET /v1/objects/performances/pools`

CLI : `pool_performance_list`

24.6.3 ストレージプールの性能情報(低解像度)を個別に取得する

指定した ID のストレージプールの性能情報(低解像度)を取得します。

前提条件

- 実行に必要なロール : `Storage`、`RemoteCopy`、`Monitor`、または `Resource`

操作手順

1. 性能情報を取得するストレージプールの ID を確認します。

CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。

REST API : `GET /v1/objects/pools`

CLI : `pool_list`

2. 性能情報を取得します。

ストレージプールの ID を指定してコマンドを実行します。

CLI を使う場合はストレージプールの ID の代わりに名前が指定できます。

REST API : `GET /v1/objects/performances/pools/<id>`

CLI : `pool_performance_show`

24.7 コンピュートポートの性能情報の取得

コンピューポートの性能情報が一覧または個別に取得できます。

24.7.1 取得できるコンピューポートの性能情報<<Bare metal>>

この項での記述内容は `Bare metal` モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- `id` : コンピューポートの ID(uuid)

- `fc` : FC 接続の場合は FC ポートの性能情報。iSCSI 接続または NVMe/TCP 接続の場合は常に `null`
- `iscsi` : iSCSI 接続の場合は iSCSI ポートの性能情報。FC 接続または NVMe/TCP 接続の場合は常に `null`
- `nvmeTcp` : NVMe/TCP 接続の場合は NVMe/TCP ポートの性能情報。FC 接続または iSCSI 接続の場合は常に `null`

24.7.2 取得できるコンピュートポートの性能情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- `id` : コンピュートポートの ID(uuid)
- `fc` : `null`
- `iscsi` : iSCSI ポートの性能情報
- `nvmeTcp` : `null`

24.7.3 コンピュートポートの性能情報(低解像度)の一覧を取得する

各コンピュートポートの性能情報(低解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : `Storage`、`RemoteCopy`、`Monitor`、または `Resource`

操作手順

1. コンピュートポートの性能情報の一覧を取得します。

REST API : `GET /v1/objects/performances/ports`

CLI : `port_performance_list`

24.7.4 コンピュートポートの性能情報(高解像度)の一覧を取得する

各コンピュートポートの性能情報(高解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : `Storage`、`RemoteCopy`、`Monitor`、または `Resource`

操作手順

1. 性能情報を取得するコンピュートポートの ID を確認します。

CLI を使いコンピュートポートを WWN または iSCSI 名で指定する場合は、コンピュートポートの WWN または iSCSI 名を確認します。

REST API : `GET /v1/objects/ports`

CLI : `port_list`

2. コンピュートポートの性能情報の一覧を取得します。

コンピュートポートの ID をクエリーパラメーターで指定してコマンドを実行します。コンピュートポートの ID は最大で 32 個まで指定できます。

CLI を使う場合はコンピュータポートの ID の代わりに WWN または iSCSI 名が指定できます。

REST API : GET /v1/objects/detail-performances/ports

CLI : port_detail_performance_list

24.7.5 コンピュートポートの性能情報を個別に取得する

指定した ID のコンピュータポートの性能情報を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得するコンピュータポートの ID を確認します。

CLI を使いコンピュータポートを WWN または iSCSI 名で指定する場合は、コンピュータポートの WWN または iSCSI 名を確認します。

REST API : GET /v1/objects/ports

CLI : port_list

2. 性能情報を取得します。

コンピュータポートの ID を指定してコマンドを実行します。

CLI を使う場合はコンピュータポートの ID の代わりに WWN または iSCSI 名が指定できます。

REST API(低解像度) : GET /v1/objects/performances/ports/<id >

REST API(高解像度) : GET /v1/objects/detail-performances/ports/<id >

CLI(低解像度) : port_performance_show

CLI(高解像度) : port_detail_performance_show

24.8 ストレージクラスターの性能情報(低解像度)を取得する

ストレージクラスターの性能情報(低解像度)を取得します。

- id : ストレージクラスターの UUID
- averageCpuUsage : 全ストレージノードに対する平均 CPU 使用率[%]
- averageMemoryUsage : 全ストレージノードに対する平均メモリー使用率[%]

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. ストレージクラスターの性能情報を取得します。

REST API : GET /v1/objects/performances/storage

CLI : storage_performance_show

24.9 ストレージノードの性能情報の取得

ストレージノードの性能情報が一覧または個別に取得できます。

24.9.1 取得できるストレージノードの性能情報

以下の情報が一覧または個別に取得できます。

- **id** : ストレージノードの ID(uuid)
- **volumeReadIOPS** : ホストおよびボリュームマイグレーションによる当該ストレージノードに属するボリュームの 1 秒当たりのリード I/O 数[IOPS]
- **volumeWriteIOPS** : ホストおよびボリュームマイグレーションによるストレージノードに属するボリュームの 1 秒当たりのライト I/O 数[IOPS]
- **volumeReadTransferRate** : ホストおよびボリュームマイグレーションによるストレージノードに属するボリュームの 1 秒当たりのリード転送量[MiB/sec]
- **volumeWriteTransferRate** : ホストおよびボリュームマイグレーションによるストレージノードに属するボリュームの 1 秒当たりのライト転送量[MiB/sec]
- **driveReadIOPS** : ドライブの 1 秒当たりのリード I/O 数[IOPS]
- **driveWriteIOPS** : ドライブの 1 秒当たりのライト I/O 数[IOPS]
- **driveReadTransferRate** : ドライブの 1 秒当たりのリード転送量[MiB/sec]
- **driveWriteTransferRate** : ドライブの 1 秒当たりのライト転送量[MiB/sec]
- **readResponseTime** : ホストおよびボリュームマイグレーションによる当該ストレージノードに属するボリュームのリード平均応答時間[msec]
- **writeResponseTime** : ホストおよびボリュームマイグレーションによる当該ストレージノードに属するボリュームのライト平均応答時間[msec]
- **readHitRate** : ホストおよびボリュームマイグレーションによる当該ストレージノードに属するボリュームの読み込みリクエストに対するキャッシュヒット率[%]
- **writeHitRate** : ホストおよびボリュームマイグレーションによる当該ストレージノードに属するボリュームの書き込みリクエストに対するキャッシュヒット率[%]
- **urWriteIOPS** : ホストから Universal Replicator の当該ストレージノードに属する P-VOL の 1 秒当たりのライト I/O 数[IOPS]
- **urWriteTransferRate** : ホストから Universal Replicator の当該ストレージノードに属する P-VOL への 1 秒当たりのライト転送量[MiB/sec]
- **urInitialCopyHitRate** : Universal Replicator の形成コピーによる当該ストレージノードに属する P-VOL の読み込みリクエストに対するキャッシュヒット率[%]
- **urInitialCopyTransferRate** : Universal Replicator の形成コピーによる当該ストレージノードに属する P-VOL の 1 秒当たりのデータ送信量[MiB/sec]
- **masterJournalRIOPS** : 当該ストレージノードにおける応答した 1 秒当たりのリードジャーナルコマンド数[IOPS]
- **masterJournalCount** : 当該ストレージノードにおけるジャーナルデータの 1 秒当たりの送信数
- **masterJournalTransferRate** : 当該ストレージノードにおけるジャーナルデータの 1 秒当たりの送信量[MiB/sec]

- `masterJournalRIOResponseTime` : 当該ストレージノードにおけるリードジャーナルコマンドを受信してから応答を送信するまでの平均時間[msec]
- `remoteJournalRIOPS` : 当該ストレージノードにおける発行した 1 秒当たりのリードジャーナルコマンド数[IOPS]
- `remoteJournalCount` : 当該ストレージノードにおけるジャーナルデータの 1 秒当たりの受信数
- `remoteJournalTransferRate` : 当該ストレージノードにおけるジャーナルデータの 1 秒当たりの受信量[MiB/sec]
- `remoteJournalRIOResponseTime` : 当該ストレージノードにおけるリードジャーナルコマンドを送信してから応答を受信するまでの平均時間[msec]
- `cpu` : 当該ストレージノードの CPU 性能情報の一覧
- `cpuSummary` : 当該ストレージノードの CPU 性能のサマリー情報
- `memory` : メモリーの性能情報

24.9.2 ストレージノードの性能情報の一覧を取得する

各ストレージノードの性能情報を一覧で取得します。

前提条件

- 実行に必要なロール : `Storage`、`RemoteCopy`、`Monitor`、または `Resource`

操作手順

1. ストレージノードの性能情報の一覧を取得します。
REST API(低解像度) : `GET /v1/objects/performances/storage-nodes`
REST API(高解像度) : `GET /v1/objects/detail-performances/storage-nodes`
CLI(低解像度) : `storage_node_performance_list`
CLI(高解像度) : `storage_node_detail_performance_list`

24.9.3 ストレージノードの性能情報を個別に取得する

指定した ID のストレージノードの性能情報を取得します。

前提条件

- 実行に必要なロール : `Storage`、`RemoteCopy`、`Monitor`、または `Resource`

操作手順

1. 性能情報を取得するストレージノードの ID を確認します。
REST API : `GET /v1/objects/storage-nodes`
CLI : `storage_node_list`
2. 性能情報を取得します。
ストレージノードの ID を指定してコマンドを実行します。
REST API(低解像度) : `GET /v1/objects/performances/storage-nodes/<id>`
REST API(高解像度) : `GET /v1/objects/detail-performances/storage-nodes/<id>`
CLI(低解像度) : `storage_node_performance_show`
CLI(高解像度) : `storage_node_detail_performance_show`

24.10 ボリュームの容量情報の取得

ボリュームの容量情報が一覧または個別に取得できます。

24.10.1 取得できるボリュームの容量情報

以下の情報が一覧または個別に取得できます。

- id : ボリュームの ID(uuid)
- vpsId : ボリュームが所属する VPS の ID
- capacityUsage : 使用量[MiB]

24.10.2 ボリュームの容量情報(低解像度)の一覧を取得する

各ボリュームの容量情報(低解像度)を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. ボリュームの容量情報の一覧を取得します。

REST API : GET /v1/objects/performances/volume-capacities

CLI : volume_capacity_performance_list

24.10.3 ボリュームの容量情報(低解像度)を個別に取得する

指定した ID のボリューム容量情報(低解像度)を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 容量情報を取得するボリュームの ID を確認します。

CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

2. 容量情報を取得します。

ボリュームの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API : GET /v1/objects/performances/volume-capacities/<id >

CLI : volume_capacity_performance_show

24.11 ボリュームの性能情報の取得

ボリュームの性能情報が一覧または個別に取得できます。

24.11.1 取得できるボリュームの性能情報

以下の情報が一覧または個別に取得できます。

- id : ボリュームの ID(uuid)
- vpsId : ボリュームが所属する VPS の ID
- readIOPS : ホストおよびボリュームマイグレーションによる 1 秒当たりのリード I/O 数[IOPS]
- writeIOPS : ホストおよびボリュームマイグレーションによる 1 秒当たりのライト I/O 数[IOPS]
- readTransferRate : ホストおよびボリュームマイグレーションによる 1 秒当たりのリード転送量[MiB/sec]
- writeTransferRate : ホストおよびボリュームマイグレーションによる 1 秒当たりのライト転送量[MiB/sec]
- readResponseTime : ホストおよびボリュームマイグレーションによるリード平均応答時間[msec]
- writeResponseTime : ホストおよびボリュームマイグレーションによるライト平均応答時間[msec]
- readHitRate : ホストおよびボリュームマイグレーションによる読み込みリクエストに対するキャッシュヒット率[%]
- writeHitRate : ホストおよびボリュームマイグレーションによる書き込みリクエストに対するキャッシュヒット率[%]
- urWriteIOPS : ホストから Universal Replicator の P-VOL への 1 秒当たりのライト I/O 数[IOPS]
- urWriteTransferRate : ホストから Universal Replicator の P-VOL への 1 秒当たりのライト転送量[MiB/sec]
- urInitialCopyHitRate : Universal Replicator の形成コピーによる P-VOL の読み込みリクエストに対するキャッシュヒット率[%]
- urInitialCopyTransferRate : Universal Replicator の形成コピーによる P-VOL の 1 秒当たりのデータ送信量[MiB/sec]

24.11.2 ボリュームの性能情報の一覧を取得する

各ボリュームの性能情報を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得するボリュームの ID を確認します。
CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

2. 性能情報の一覧を取得します。

高解像度の性能情報を取得する場合は、ボリュームの ID をクエリーパラメーターで指定してコマンドを実行します。ボリュームの ID は最大で 32 個まで指定できます。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API(低解像度) : GET /v1/objects/performances/volumes

REST API(高解像度) : GET /v1/objects/detail-performances/volumes

CLI(低解像度) : volume_performance_list

CLI(高解像度) : volume_detail_performance_list

24.11.3 ボリュームの性能情報を個別に取得する

指定した ID のボリュームの性能情報を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得するボリュームの ID を確認します。

CLI を使いボリュームを名前で指定する場合は、ボリュームの名前を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

2. 性能情報を取得します。

ボリュームの ID を指定してコマンドを実行します。

CLI を使う場合はボリュームの ID の代わりに名前が指定できます。

REST API(低解像度) : GET /v1/objects/performances/volumes/<id >

REST API(高解像度) : GET /v1/objects/detail-performances/volumes/<id >

CLI(低解像度) : volume_performance_show

CLI(高解像度) : volume_detail_performance_show

24.12 ジャーナルの性能情報の取得

ジャーナルの性能情報が一覧または個別に取得できます。

24.12.1 取得できるジャーナルの性能情報

以下の情報が一覧または個別に取得できます。

- id : ジャーナルの ID(uuid)
- vpsId : ジャーナルが所属する VPS の ID
- writeIOPS : ホストからマスタージャーナルに属する P-VOL への 1 秒当たりのライト I/O 数 [IOPS]
- writeTransferRate : ホストからマスタージャーナルに属する P-VOL への 1 秒当たりのライト転送量 [MiB/sec]

- initialCopyHitRate : 形成コピーによるマスタージャーナルに属する P-VOL の読み込みリクエストに対するキャッシュヒット率[%]
- initialCopyTransferRate : 形成コピーによるジャーナルデータの 1 秒当たりの送信量[MiB/sec]
- masterJournalRIOPS : 応答した 1 秒当たりのリードジャーナルコマンド数[IOPS]
- masterJournalCount : ジャーナルデータの 1 秒当たりの送信数
- masterJournalTransferRate : ジャーナルデータの 1 秒当たりの送信量[MiB/sec]
- masterJournalRIOResponseTime : リードジャーナルコマンドを受信してから応答を送信するまでの平均時間[msec]
- masterJournalDataUsageRate : マスタージャーナルボリュームのジャーナルデータの利用率[%]
- masterJournalMetaDataUsageRate : マスタージャーナルボリュームのメタデータの利用率[%]
- remoteJournalRIOPS : 発行した 1 秒当たりのリードジャーナルコマンド数[IOPS]
- remoteJournalCount : ジャーナルデータの 1 秒当たりの受信数
- remoteJournalTransferRate : ジャーナルデータの 1 秒当たりの受信量[MiB/sec]
- remoteJournalRIOResponseTime : リードジャーナルコマンドを送信してから応答を受信するまでの平均時間[msec]
- remoteJournalDataUsageRate : リストアジャーナルボリュームのジャーナルデータの利用率[%]
- remoteJournalMetaDataUsageRate : リストアジャーナルボリュームのメタデータ使用率[%]

24.12.2 ジャーナルの性能情報の一覧を取得する

各ジャーナルの性能情報を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得するジャーナルの ID を確認します。

REST API : GET /v1/objects/journals

CLI : journal_list

2. 性能情報の一覧を取得します。

高解像度の性能情報を取得する場合は、ジャーナルの ID をクエリーパラメーターで指定してコマンドを実行します。ジャーナルの ID は最大で 32 個まで指定できます。

REST API(低解像度) : GET /v1/objects/performances/journals

REST API(高解像度) : GET /v1/objects/detail-performances/journals

CLI(低解像度) : journal_performance_list

CLI(高解像度) : journal_detail_performance_list

24.12.3 ジャーナルの性能情報を個別に取得する

指定した ID のジャーナルの性能情報を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. 性能情報を取得するジャーナルの ID を確認します。
CLI を使いジャーナル番号で指定する場合は、ジャーナル番号を確認します。
REST API : GET /v1/objects/journals
CLI : journal_list
2. 性能情報を取得します。
ジャーナルの ID を指定してコマンドを実行します。
CLI を使う場合はジャーナルの ID の代わりにジャーナル番号が指定できます。
REST API(低解像度) : GET /v1/objects/performances/journals/<id >
REST API(高解像度) : GET /v1/objects/detail-performances/journals/<id >
CLI(低解像度) : journal_performance_show
CLI(高解像度) : journal_detail_performance_show

ネットワーク設定の情報を取得する

- 25.1 ストレージクラスターのネットワーク情報の取得
- 25.2 管理ポートの情報の取得
- 25.3 ストレージノード間ポートの情報の取得
- 25.4 ストレージノードのネットワーク設定の取得

25.1 ストレージクラスターのネットワーク情報の取得

ストレージクラスターのネットワーク情報を取得できます。

25.1.1 取得できるストレージクラスターのネットワーク情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が取得できます。

- primaryDnsServerIpAddress : 1 つ目の名前解決リクエスト先 DNS サーバーの IP アドレス
- secondaryDnsServerIpAddress : 2 つ目の名前解決リクエスト先 DNS サーバーの IP アドレス
- virtualIpv4Address : ストレージクラスターの代表 IP アドレス(IPv4)
ストレージクラスターの代表 IP アドレスが付与されているストレージノードに障害が発生した場合、その IP アドレスは別の正常なストレージノードに引き継がれます。

25.1.2 取得できるストレージクラスターのネットワーク情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が取得できます。

- primaryDnsServerIpAddress : 1 つ目の名前解決リクエスト先 DNS サーバーの IP アドレス
- secondaryDnsServerIpAddress : 常に空白文字列("")
- virtualIpv4Address : 常に空白文字列("")

25.1.3 ストレージクラスターのネットワーク情報を取得する

ストレージクラスターのネットワーク情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. ストレージクラスターのネットワーク設定を取得します。
REST API : GET /v1/objects/storage-network-setting
CLI : storage_network_setting_show

25.2 管理ポートの情報の取得

管理ポートの情報が一覧または個別に取得できます。

25.2.1 取得できる管理ポート情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : 管理ポートの ID(uuid)
- storageNodeId : 管理ポートが存在するストレージノードの ID(uuid)
- macAddress : MAC アドレス
- mtuSize : MTU サイズ[byte]
- interfaceName : インターフェイス名
- deviceName : NIC のデバイス名
- configuredPortSpeed : 通信に使用している物理ポートのリンク速度の設定
- portSpeedDuplex : 通信に使用している物理ポートの実際のリンク速度と Duplex
- isTeamingEnabled : チーミング構成時は"true"。そうでない場合は"false"
- ipv4Information : 管理ポートの IPv4 設定情報
- teaming : チーミング構成時はチーミング情報、そうでない場合は null
- redundancy : 物理ポートの冗長度。チーミング構成時は"1"、そうでない場合は"0"
- status : 管理ポートの状態
チーミング構成時は"Normal"、"Warning"、または"Error"。チーミング構成をとっていない場合は、"Normal"または"Error"
- statusSummary : 管理ポートの状態のサマリー
チーミング構成時は"Normal"、"Warning"、または"Error"。チーミング構成をとっていない場合は、"Normal"または"Error"

25.2.2 取得できる管理ポート情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : 管理ポートの ID(uuid)
- storageNodeId : 管理ポートが存在するストレージノードの ID(uuid)
- macAddress : MAC アドレス
- mtuSize : MTU サイズ[byte]
- interfaceName : インターフェイス名
- deviceName : NIC のデバイス名
- configuredPortSpeed : 通信に使用している物理ポートのリンク速度の設定
- portSpeedDuplex : 常に"DependsOnHypervisor"
- isTeamingEnabled : 常に"DependsOnHypervisor"
- ipv4Information : 管理ポートの IPv4 設定情報
- teaming : 常に null
- redundancy : 物理ポートの冗長度。チーミング構成時は"1"、そうでない場合は"0"
- status : 常に"Normal"
- statusSummary : 常に"Normal"

25.2.3 管理ポートの情報の一覧を取得する

各管理ポートの情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. 管理ポートの情報の一覧を取得します。
REST API : GET /v1/objects/control-ports
CLI : control_port_list

25.2.4 管理ポートの情報を個別に取得する

指定した ID の管理ポートの情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. 管理ポートの ID を確認します。
REST API : GET /v1/objects/control-ports
CLI : control_port_list
2. 管理ポートの情報を取得します。
管理ポートの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/control-ports/<id >
CLI : control_port_show

25.3 ストレージノード間ポートの情報の取得

ストレージノード間ポートの情報が一覧または個別に取得できます。

25.3.1 取得できるストレージノード間ポート情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : ストレージノード間ポートの ID(uuid)
- storageNodeId : ストレージノード間ポートが存在するストレージノードの ID(uuid)
- macAddress : MAC アドレス
- mtuSize : MTU サイズ[byte]
- interfaceName : インターフェイス名

- `deviceName` : NIC のデバイス名
- `configuredPortSpeed` : 通信に使用している物理ポートのリンク速度の設定[bps]
- `portSpeedDuplex` : 通信に使用している物理ポートの実際のリンク速度と Duplex
- `isTeamingEnabled` : チーミングの有効/無効
- `ipv4Information` : ストレージノード間ポートの IPv4 設定情報
- `teaming` : ストレージノード間ポートのチーミング情報
- `redundancy` : 物理ポートの冗長度
- `status` : ストレージノード間ポートの状態。"Normal"、"Warning"、または"Error"
- `statusSummary` : ストレージノード間ポートの状態のサマリー。"Normal"、"Warning"、または"Error"

25.3.2 取得できるストレージノード間ポート情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- `id` : ストレージノード間ポートの ID(uuid)
- `storageNodeId` : ストレージノード間ポートが存在するストレージノードの ID(uuid)
- `macAddress` : MAC アドレス
- `mtuSize` : MTU サイズ[byte]
- `interfaceName` : インターフェイス名
- `deviceName` : NIC のデバイス名
- `configuredPortSpeed` : 通信に使用している物理ポートのリンク速度の設定[bps]
- `portSpeedDuplex` : 常に"DependsOnHypervisor"
- `isTeamingEnabled` : 常に"DependsOnHypervisor"
- `ipv4Information` : ストレージノード間ポートの IPv4 設定情報
- `teaming` : 常に null
- `redundancy` : 物理ポートの冗長度
- `status` : 常に"Normal"
- `statusSummary` : 常に"Normal"

25.3.3 ストレージノード間ポートの情報の一覧を取得する

各ストレージノード間ポートの情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. ストレージノード間ポートの情報の一覧を取得します。

REST API : GET /v1/objects/internode-ports

CLI : `internode_port_list`

25.3.4 ストレージノード間ポートの情報を個別に取得する

指定した ID のストレージノード間ポートの情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. ストレージノード間ポートの ID を確認します。
REST API : GET /v1/objects/internode-ports
CLI : internode_port_list
2. ストレージノード間ポートの情報を取得します。
ストレージノード間ポートの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/internode-ports/<id >
CLI : internode_port_show

25.4 ストレージノードのネットワーク設定の取得

ストレージノードのネットワーク設定が一覧または個別に取得できます。

25.4.1 取得できるストレージノードのネットワーク設定

以下の設定が一覧または個別に取得できます。

- id : ストレージノードの ID(uuid)
- ipv4Route : ルーティングテーブル(IPv4)

25.4.2 ストレージノードのネットワーク設定の一覧を取得する

各ストレージノードのネットワーク設定(ルーティングテーブル)を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ストレージノードのネットワーク設定の一覧を取得します。
REST API : GET /v1/objects/storage-node-network-settings
CLI : storage_node_network_setting_list

25.4.3 ストレージノードのネットワーク設定を個別に取得する

指定した ID のストレージノードについてのネットワーク設定(ルーティングテーブル)を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ストレージノードの ID を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

2. ネットワーク設定を取得します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/storage-node-network-settings/<id >

CLI : storage_node_network_setting_show

ストレージプールを管理する

- 26.1 ストレージプール管理の概要
- 26.2 ストレージプールの容量情報
- 26.3 ストレージプールの容量状態
- 26.4 ストレージプールのリビルド領域について
- 26.5 ストレージプールの情報の取得
- 26.6 ストレージプールの設定を編集する
- 26.7 リビルド領域の不足に対処する
- 26.8 ライセンスの使用量を確認するためにストレージプールの容量を試算する《Cloud for AWS》

26.1 ストレージプール管理の概要

ストレージプール管理は、複数のストレージノードにあるドライブからなる容量情報をまとめて管理します。ユーザーは、ストレージノードやドライブの物理的な境界をほとんど意識することなく、ストレージプールの容量や状態を管理できます。

ストレージプールの使用率は 80%以下になるように余裕をもって運用してください。ストレージプールの使用率が 80%を超えると、容量バランスによるストレージコントローラー間の偏り解消が行えなくなります。

この章では、ストレージプールの情報を取得する方法、取得できるストレージプールの情報、ストレージプールの設定の編集方法、リビルド領域の管理方法について説明します。ストレージプールへの容量追加方法については「ドライブを増設する」、「ストレージノード増設の準備と手順」を参照してください。

26.2 ストレージプールの容量情報

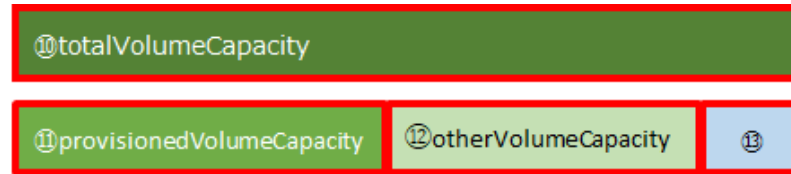
ストレージプール情報の一覧の取得、またはストレージプール情報の取得で得られる情報のうち、ストレージプールの容量情報には以下の①～⑩があります。これらの情報は、VSP One SDS Block Administrator でも確認できます。



- ① totalPhysicalCapacity : ストレージプールに割り当てたドライブの総容量[MiB]
- ② totalRawCapacity : ドライブをストレージプールに追加して利用可能になった容量[MiB]
- ③ metaDataPhysicalCapacity : totalPhysicalCapacity における、制御情報用容量[MiB]
- ④ usablePhysicalCapacity : totalRawCapacity のうち、論理容量に利用可能な容量[MiB]
- ⑤ reservedPhysicalCapacity : totalRawCapacity のうち、論理容量に利用しない容量[MiB]
- ⑥ blockedPhysicalCapacity : totalRawCapacity のうち、閉塞している容量[MiB]
- ⑦ totalCapacity : ストレージプールのユーザーが利用可能な容量[MiB]
- ⑧ usedCapacity : ユーザーデータやユーザーデータに関するメタデータを実際に格納した容量[MiB]

⑨ freeCapacity : ストレージプールで使用していない容量[MiB]

ストレージプールの容量情報では、作成済みの合計ボリューム容量なども確認できます。



名称	説明	含まれるボリュームの種別とスナップショットの属性
⑩totalVolumeCapacity[MiB]	作成済み合計ボリューム容量。 (プロビジョンドボリューム、アザーボリューム、一時ボリュームの合計容量。)	• volumeType : Normal • volumeType : Snapshot • volumeType : MigrationDestination
⑪provisionedVolumeCapacity[MiB]	作成済みプロビジョンドボリューム容量。 (通常ボリューム、スナップショットボリューム(P-VOL)、ジャーナルボリューム、元ジャーナルボリュームの総容量。)	• volumeType : Normal • volumeType : Snapshot かつ snapshotAttribute : P-VOL • volumeType : Journal • volumeType : FormerJournal
⑫otherVolumeCapacity[MiB]	作成済みアザーボリューム容量。 (スナップショットボリューム(S-VOL、P/S-VOL)の総容量。)	• volumeType : Snapshot かつ snapshotAttribute : P/S-VOL • volumeType : Snapshot かつ snapshotAttribute : S-VOL
⑬temporaryVolumeCapacity[MiB]	作成済み一時ボリューム容量。 <<Cloud>>データマイグレーション、容量バランスで一時的に作成されるボリュームの総容量。 <<Bare metal>>容量バランスで一時的に作成されるボリュームの総容量。	• volumeType : MigrationDestination



メモ

- スナップショットボリュームは、作成済み容量より使用容量が多くなることがあります。
- 上記の表の各容量にはボリュームの制御情報は含まれていません。制御情報を含めた容量を求める場合は「ボリュームが消費するストレージプールの最大容量」を参照して算出してください。
- totalCapacity[MiB](ストレージプールの論理容量)はリビルド領域ポリシー(rebuildCapacityPolicy)の設定値によって変化する場合があります。詳細は「ストレージプールのリビルド領域について」を参照してください。



注意

totalCapacity[MiB](ストレージプールの論理容量)より、totalVolumeCapacity[MiB]が小さい場合でも、ストレージコントローラーごとの使用容量に偏りがあるときは、ストレージコントローラーの容量が満杯になることがあります。ストレージコントローラーの容量が満杯時には、以下の障害が発生することがあります。

- 通常ボリューム、スナップショットボリューム、または容量削減機能が有効なボリュームの削除を除く操作が失敗する

- ・ 通常ボリューム、スナップショットボリューム、または容量削減機能が有効なボリュームへの I/O がエラーになる
- ・ スナップショットボリュームのデータが消失する

26.3 ストレージプールの容量状態

ストレージプール情報の一覧の取得、またはストレージプール情報の取得から得られる情報のうち、ストレージプールの容量状態について以下に示します。これらの情報は、VSP One SDS Block Administrator でも確認できます。

ストレージプールの状態(status)

状態	説明
正常(Normal)	ストレージプール使用率が警告しきい値未満の状態です。
警告しきい値超過 (ExceededThreshold)	ストレージプール使用率が警告しきい値以上、枯渇しきい値未満の状態です。ストレージプール容量の枯渇リスクが高まっているため、対処が必要です。
枯渇しきい値超過 (Error)	ストレージプール使用率が 100%である。または、枯渇しきい値以上の状態です。ストレージプール容量の枯渇リスクが極めて高まっており、早急な対処が必要です。

当該ストレージプールを管理しているすべてのストレージコントローラーの容量状態の集約情報 (storageControllerCapacitiesGeneralStatus)

状態	説明
正常(Normal)	当該ストレージプールを管理しているすべてのストレージコントローラーの capacityStatus が "Normal" の状態です。
警告(Warning)	当該ストレージプールを管理しているストレージコントローラーのうち、capacityStatus が "Warning" のものが 1 つ以上あり、"Error" のものがない状態です。
異常(Error)	当該ストレージプールを管理しているストレージコントローラーのうち、capacityStatus が "Error" のものが 1 つ以上ある状態です。

26.4 ストレージプールのリビルド領域について

リビルド領域とは、ドライブに障害が発生したときに動作するリビルドで使用する領域です。リビルド領域が確保できている場合、ユーザーデータの保護方式でユーザーデータが冗長化されている間は、ドライブ障害が発生した場合でも、リビルドによって自動でユーザーデータの冗長度を回復できます。リビルドはユーザーデータの冗長度を回復する機能であるため、リビルド領域が確保できていても、リビルド開始前またはリビルド中は冗長度が低下しています。

ハードウェアまたはクラウドプラットフォームの複数同時障害に対する耐性は、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」にある「VSP One SDS Block がサポートする耐障害性に関する設定と各機能の説明」に記載の機能によって設定されます。

リビルド領域に関する設定項目

「ストレージプールの設定を編集する」で設定可能なリビルド領域に関する設定項目には以下があります。

項目	説明	備考
リビルド領域ポリシー (rebuildCapacityPolicy)	ストレージプールのドライブ障害時にリビルドするための空き容量の確保方法について決める設定です。インストール後のデフォルト値は"Fixed"です。 Fixed : 指定したリビルド領域のリソース種別・リソース数分の障害でリビルドできるようにストレージプール内に論理容量とは独立したリビルド領域を確保します。リビルド領域を論理容量と独立して管理する場合に設定してください。 Variable : リビルド領域を確保できる構成では、各ストレージノードでドライブ 1 台の障害でリビルドができるようにリビルド領域を確保します。リビルド領域は論理容量と共有しており、いずれかのストレージコントローラーの使用容量が大きくなったときにリビルド領域を論理容量に割り当てます。また、ストレージノードやドライブに障害が発生して論理容量が確保できなくなると、論理容量が減少することがあります。その場合は、障害の復旧を行うことで論理容量が回復します。リビルド領域について細かい管理をせず運用する場合に設定してください。	
リビルド領域のリソース種別・リソース数 (rebuildCapacityResourceSetting)	許容されるドライブ障害数 (numberOfTolerableDriveFailures) は、リビルド領域ポリシー (rebuildCapacityPolicy) が "Fixed" のときにのみ設定してください。各設定項目に対応するリソースで指定した回数のリビルドができるようにリビルド領域を確保します。 numberOfTolerableDriveFailures : 各ストレージノードで指定回数のドライブ障害が発生してもリビルド可能になるようにリビルド領域を確保します。ストレージノードに搭載されているドライブ数未満の値を設定してください。インストール後のデフォルト値は 1 です。	• numberOfTolerableDriveFailures に 0 を指定するとすべてのドライブ容量を使って論理容量を構成しますが、構成によって論理容量化できない物理容量が残っているとリビルドが実行可能な場合があります。 • rebuildCapacityPolicy が "Fixed" のときに numberOfTolerableDriveFailures を参照すると設定した値が設定値として表示されます。 • rebuildCapacityPolicy が "Variable" のときに numberOfTolerableDriveFailures を参照すると、当該設定値は無効のため "null" (または表示形式の指定によ

項目	説明	備考
		で"None")が表示されます。

リビルド領域を管理するために参照する項目

ストレージプール情報の一覧を取得して、リビルド領域の管理ができます。下記の情報を確認することでリビルド領域の状態を確認します。

項目	説明
リビルド領域の確保状態 (rebuildCapacityStatus)	Sufficient : リビルド領域のリソース種別・リソース数の許容されるドライブ障害数で指定したリビルド領域を確保できている状態です。ストレージプールのリビルド可能リソースのリビルド可能なドライブ数が、許容されるドライブ障害数と同値である場合に、この状態になります。 ただし、許容されるドライブ障害数が 0 の場合は、"Sufficient"にはならず、"None"になります。 また、リビルド領域ポリシーが"Variable"の場合は、リビルド可能なドライブ数が 1 のときに"Sufficient"になります。 Partial Shortage : リビルド領域のリソース種別・リソース数の許容されるドライブ障害数で指定したリビルド領域を一部確保できている状態です。ストレージプールのリビルド可能リソースのリビルド可能なドライブ数が 1 以上かつ許容されるドライブ障害数未満である場合にこの状態になります。 None : リビルド領域を確保していないストレージノードが存在する状態です。ストレージプールのリビルド可能リソースのリビルド可能なドライブ数が 0 の場合に、この状態になります。リビルド領域ポリシーを"Fixed"、リビルド領域のリソース種別・リソース数の許容されるドライブ障害数を 0 に指定した場合もこの状態になります。ストレージプールのリビルド可能なドライブ数は、ストレージノードのリビルド可能なドライブ数の最小値となるので、リビルド領域の確保状態が"None"の場合でも、障害が発生するドライブによってはリビルドが可能な場合があります。
リビルド可能リソース (rebuildableResources)	リビルド可能なドライブ数(numberOfDrives) : ストレージプールが確保しているリビルド領域で現在リビルド可能なドライブ数を示します。この情報はストレージノード単位でも参照可能であり、ストレージプールが示す数は、ストレージノードのリビルド可能回数の最小値です。

リビルド領域管理の注意事項

- リビルド領域を確保している状態では、ストレージノードに搭載しているすべてのドライブに I/O が分散せず、搭載しているドライブ数分の性能向上がされないことがあります。リビルド領域ポリシーが"Variable"の場合は各ストレージノードでドライブ 1 台、リビルド領域ポリシー"Fixed"の場合は各ストレージノードで許容されるドライブ障害数を除いた性能スケールとなる場合があります。
- ストレージノードに搭載しているドライブ容量が均一でない場合、任意のドライブに障害が発生してもリビルドが可能なように、ドライブの容量が大きい順に容量をリビルド領域として確保します。

例えば、ストレージノード 1 台当たり、ドライブ A(6.4TB)、ドライブ B(3.2TB)、ドライブ C(1.6TB)の 3 台を搭載している構成で、リビルド領域ポリシーが"Fixed"、許容されるドライブ障害数が 2 の場合、ドライブ容量が 1 番目に大きなドライブ A と 2 番目に大きなドライブ B の容量分の合計 9.6TB がリビルド領域として確保されます。

- ・ ストレージプールにすでに容量がある状態で、リビルド領域ポリシーとリビルド領域のリソース種別・リソース数を変更すると、ストレージプールの論理容量が変化することがあります。ストレージプールの論理容量が増加すると、ストレージプールの設定の編集後、内部処理であるストレージコントローラーへの容量割り付け処理が実行されることがあります。これら処理の終了によって、追加された容量が使用できるようになります。



注意

拡張済みのストレージプールに対してストレージプールの設定を編集する際に、リビルド領域のリソース種別・リソース数の許容されるドライブ障害数を減らしたり、リビルド領域ポリシーを"Variable"に変更したりする場合は十分に注意してください。一度ストレージコントローラーへ容量割り付けされた領域は、再度リビルド領域ポリシーを変更してもリビルド領域に戻せません。

≪Cloud≫リビルド領域が確保されなくなること、ドライブ障害発生時にドライブの自動復旧が動作できなくなることがあります。ドライブの自動復旧の動作条件については「ドライブを交換する≪Cloud≫」を参照してください。

26.5 ストレージプールの情報の取得

ストレージプールの情報が一覧または個別に取得できます。

26.5.1 取得できるストレージプールの情報≪Bare metal≫

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- ・ id : ストレージプールの ID(uuid)
- ・ name : ストレージプールの名前
- ・ protectionDomainId : 所属するプロテクションドメインの ID(uuid)
- ・ statusSummary : ストレージプールの状態のサマリー
- ・ status : ストレージプールの状態
- ・ totalCapacity : ストレージプールの論理容量[MiB]
- ・ totalRawCapacity : ストレージプールの総物理容量における、有効物理容量[MiB]
- ・ usedCapacity : ストレージプールの使用容量[MiB]
- ・ freeCapacity : ストレージプールの空き容量[MiB]
- ・ totalPhysicalCapacity : ストレージプールの総物理容量[MiB]
- ・ metaDataPhysicalCapacity : ストレージプールの総物理容量における、制御情報用容量[MiB]
- ・ reservedPhysicalCapacity : ストレージプールの有効物理容量における、制御情報以外で内部的に予約された、冗長構成をとれない領域[MiB]
- ・ usablePhysicalCapacity : ストレージプールの有効物理容量における、論理容量に利用可能な容量[MiB]
- ・ blockedPhysicalCapacity : ストレージプールの有効物理容量において、閉塞している容量[MiB]
- ・ capacityManage : 容量管理
 - usedCapacityRate : 使用率[%]

- maximumReserveRate : 最大予約率[%]
- thresholdWarning : 警告しきい値[%]
- thresholdDepletion : 枯渇しきい値[%]
- thresholdStorageControllerDepletion : 当該ストレージプールを管理しているストレージコントローラーの枯渇しきい値[%]
- savingEffects : 当該ストレージプールでの容量削減機能の効果
 - efficiencyDataReduction : 容量削減機能による削減前後のデータ容量の比率[%]
 - preCapacityDataReduction : 容量削減機能によって削減される前のデータの容量[MiB]
 - postCapacityDataReduction : 容量削減機能によって削減されたあとのデータの容量[MiB]
 - totalEfficiencyStatus : 合計効果の状態
 - dataReductionWithoutSystemDataStatus : 容量削減機能の削減効果の状態
 - totalEfficiency : 合計効果の比率[%]
 - dataReductionWithoutSystemData : 容量削減機能によって削減されたストレージプール全体の削減効果の比率[%]
 - preCapacityDataReductionWithoutSystemData : 容量削減機能によって削減される前のストレージプール全体の容量[MiB]
 - postCapacityDataReductionWithoutSystemData : 容量削減機能によって削減されたあとのストレージプール全体の容量[MiB]
 - calculationStartTime : 計算を開始した日時
 - calculationEndTime : 計算を終了した日時
- numberOfVolumes : ストレージプールに属するボリューム数
- redundantPolicy : ユーザーデータの保護方式
- redundantType : ユーザーデータの保護種別
- dataRedundancy : ユーザーデータの冗長度
- storageControllerCapacitiesGeneralStatus : 当該ストレージプールを管理しているすべてのストレージコントローラーの容量状態(capacityStatus)の集約情報
- totalVolumeCapacity : 当該ストレージコントローラー上で作成済みの合計ボリューム容量[MiB]
- provisionedVolumeCapacity : 当該ストレージコントローラー上で作成済みのプロビジョンドボリューム容量[MiB]
- otherVolumeCapacity : 当該ストレージコントローラー上で作成済みのアザーボリューム容量[MiB]
- temporaryVolumeCapacity : 当該ストレージコントローラー上で作成済みの一時ボリューム容量[MiB]
- rebuildCapacityPolicy : リビルド領域ポリシー
- rebuildCapacityResourceSetting : リビルド領域のリソース種別・リソース数
 - numberOfTolerableDriveFailures : 許容されるドライブ障害数
- rebuildCapacityStatus : リビルド領域の確保状態
- rebuildableResources : リビルド可能リソース
 - numberOfDrives : リビルド可能なドライブ数

- encryptionStatus : ストレージプールのデータ暗号化の状態



メモ

totalEfficiency[%]は、ボリューム作成機能とスナップショット機能、および容量削減機能による、容量消費の節減効果を示します。

ストレージプールの使用容量(usedCapacity[MiB])に対する作成済みの合計ボリューム容量

(totalVolumeCapacity[MiB])の比率をストレージコントローラーごとに算出して、各ストレージコントローラーの作成済みの合計ボリューム容量の大きさに応じて重みを付けた平均の比率[%]です。作成済みの合計ボリューム容量の大きいストレージコントローラーの容量消費の節減効果ほど、より totalEfficiency の値に反映されます。例えば、各ストレージコントローラーにおいて、いずれも作成済みの合計ボリューム容量が 1,000 で、ストレージプールの使用容量が 50 の場合は、REST API と CLI では、totalEfficiency として、2,000[%]が出力されます。

VSP One SDS Block Administrator では、totalEfficiency に相当する値が、ダッシュボード画面(Total Efficiency)と Storage Pool 画面(TOTAL EFFICIENCY)に"20.00:1"と表示されます。また、VSP One SDS Block Administrator のダッシュボード画面では、比率が 9,999,999:100 より大きい場合は、">999999.99:1"と表示されます。

スナップショットボリュームを使用している場合、P-VOL と S-VOL の差分データだけを保持することで使用済みのストレージプールの容量を低減できます。そのため、作成済みの合計ボリューム容量が同じでも、スナップショットボリュームを含まない場合と比べて、totalEfficiency の値は大きくなります。

ストレージプールの拡張処理が動作して、KARS16017-I、KARS16020-I、KARS16022-I、KARS16081-I のいずれかが出力されている場合は、スナップショット操作を実施していなくても、totalEfficiency の値が大きくなる場合があります。なお、スナップショット操作とは、スナップショットの取得準備、取得、削除、復元を指します。

26.5.2 取得できるストレージプールの情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : ストレージプールの ID(uuid)
- name : ストレージプールの名前
- protectionDomainId : 所属するプロテクションドメインの ID(uuid)
- statusSummary : ストレージプールの状態のサマリー
- status : ストレージプールの状態
- totalCapacity : ストレージプールの論理容量[MiB]
- totalRawCapacity : ストレージプールの総物理容量における、有効物理容量[MiB]
- usedCapacity : ストレージプールの使用容量[MiB]
- freeCapacity : ストレージプールの空き容量[MiB]
- totalPhysicalCapacity : ストレージプールの総物理容量[MiB]
- metaDataPhysicalCapacity : ストレージプールの総物理容量における、制御情報用容量[MiB]
- reservedPhysicalCapacity : ストレージプールの有効物理容量における、制御情報以外で内部的に予約された、冗長構成をとれない領域[MiB]
- usablePhysicalCapacity : ストレージプールの有効物理容量における、論理容量に利用可能な容量[MiB]
- blockedPhysicalCapacity : ストレージプールの有効物理容量において、閉塞している容量[MiB]
- capacityManage : 容量管理
 - usedCapacityRate : 使用率[%]

- maximumReserveRate : 最大予約率[%]
- thresholdWarning : 警告しきい値[%]
- thresholdDepletion : 枯渇しきい値[%]
- thresholdStorageControllerDepletion : 当該ストレージプールを管理しているストレージコントローラーの枯渇しきい値[%]
- savingEffects : 当該ストレージプールでの容量削減機能の効果
 - efficiencyDataReduction : 容量削減機能による削減前後のデータ容量の比率[%]
 - preCapacityDataReduction : 容量削減機能によって削減される前のデータの容量[MiB]
 - postCapacityDataReduction : 容量削減機能によって削減されたあとのデータの容量[MiB]
 - totalEfficiencyStatus : 合計効果の状態
 - dataReductionWithoutSystemDataStatus : 容量削減機能の削減効果の状態
 - totalEfficiency : 合計効果の比率[%]
 - dataReductionWithoutSystemData : 容量削減機能によって削減されたストレージプール全体の削減効果の比率[%]
 - preCapacityDataReductionWithoutSystemData : 容量削減機能によって削減される前のストレージプール全体の容量[MiB]
 - postCapacityDataReductionWithoutSystemData : 容量削減機能によって削減されたあとのストレージプール全体の容量[MiB]
 - calculationStartTime : 計算を開始した日時
 - calculationEndTime : 計算を終了した日時
- numberOfVolumes : ストレージプールに属するボリューム数
- redundantPolicy : ユーザーデータの保護方式
- redundantType : ユーザーデータの保護種別
- dataRedundancy : ユーザーデータの冗長度
- storageControllerCapacitiesGeneralStatus : 当該ストレージプールを管理しているすべてのストレージコントローラーの容量状態(capacityStatus)の集約情報
- totalVolumeCapacity : 当該ストレージコントローラー上で作成済みの合計ボリューム容量[MiB]
- provisionedVolumeCapacity : 当該ストレージコントローラー上で作成済みのプロビジョンドボリューム容量[MiB]
- otherVolumeCapacity : 当該ストレージコントローラー上で作成済みのアザーボリューム容量[MiB]
- temporaryVolumeCapacity : 当該ストレージコントローラー上で作成済みの一時ボリューム容量[MiB]
- rebuildCapacityPolicy : リビルド領域ポリシー
- rebuildCapacityResourceSetting : リビルド領域のリソース種別・リソース数
 - numberOfTolerableDriveFailures : 許容されるドライブ障害数
- rebuildCapacityStatus : リビルド領域の確保状態
- rebuildableResources : リビルド可能リソース
 - numberOfDrives : リビルド可能なドライブ数

- `encryptionStatus` : ストレージプールのデータ暗号化の状態。ストレージプールの暗号化の設定が無効の場合は"`DependsOnCloudService`"



メモ

`totalEfficiency[%]`は、ボリューム作成機能とスナップショット機能、および容量削減機能による、容量消費の節減効果を示します。

ストレージプールの使用容量(`usedCapacity[MiB]`)に対する作成済みの合計ボリューム容量

(`totalVolumeCapacity[MiB]`)の比率をストレージコントローラーごとに算出して、各ストレージコントローラーの作成済みの合計ボリューム容量の大きさに応じて重みを付けた平均の比率[%]です。作成済みの合計ボリューム容量の大きいストレージコントローラーの容量消費の節減効果ほど、より `totalEfficiency` の値に反映されます。例えば、各ストレージコントローラーにおいて、いずれも作成済みの合計ボリューム容量が 1,000 で、ストレージプールの使用容量が 50 の場合は、REST API と CLI では、`totalEfficiency` として、2,000[%]が出力されます。

VSP One SDS Block Administrator では、`totalEfficiency` に相当する値が、ダッシュボード画面(Total Efficiency)と Storage Pool 画面(TOTAL EFFICIENCY)に"20.00:1"と表示されます。また、VSP One SDS Block Administrator のダッシュボード画面では、比率が 9,999,999:100 より大きい場合は、">99999.99:1"と表示されます。

スナップショットボリュームを使用している場合、P-VOL と S-VOL の差分データだけを保持することで使用済みのストレージプールの容量を低減できます。そのため、作成済みの合計ボリューム容量が同じでも、スナップショットボリュームを含まない場合と比べて、`totalEfficiency` の値は大きくなります。

ストレージプールの拡張処理が動作して、KARS16017-I、KARS16020-I、KARS16022-I、KARS16081-I のいずれかが出力されている場合は、スナップショット操作を実施していなくても、`totalEfficiency` の値が大きくなることがあります。なお、スナップショット操作とは、スナップショットの取得準備、取得、削除、復元を指します。

26.5.3 ストレージプールの情報の一覧を取得する

各ストレージプールの情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ストレージプールの情報の一覧を取得します。

REST API : GET /v1/objects/pools

CLI : `pool_list`

26.5.4 ストレージプールの情報を個別に取得する

指定した ID のストレージプールの情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ストレージプールの ID を確認します。

CLI を使いストレージプールを名前で指定する場合は、ストレージプールの名前を確認します。

REST API : GET /v1/objects/pools

CLI : `pool_list`

2. ストレージプール情報を取得します。

ストレージプールの ID を指定してコマンドを実行します。

CLI を使う場合はストレージプールの ID の代わりに名前が指定できます。

REST API : GET /v1/objects/pools/<id >

CLI : pool_show

26.6 ストレージプールの設定を編集する

ストレージプールの設定を編集します。リビルド領域ポリシー(rebuildCapacityPolicy)、リビルド領域のリソース種別・リソース数(rebuildCapacityResourceSetting)の許容されるドライブ障害数(numberOfTolerableDriveFailures)が編集できます。各設定項目の詳細については、「ストレージプールのリビルド領域について」を参照してください。

インストール後のデフォルト値は、リビルド領域ポリシーが"Fixed"、許容されるドライブ障害数が 1 です。この設定では、各ストレージノードの最も容量が大きなドライブ分の容量がリビルド用の領域として確保されます。

VSP One SDS Block Administrator からはストレージプールの設定は編集できません。



注意

- ・ ストレージプールの設定を編集するとストレージプール容量が変化したり、内部処理であるストレージコントローラーへの容量割り付け処理が動作したりすることがあるため、実行前に「ストレージプールのリビルド領域について」に記載のリビルド領域管理の注意事項を確認してください。
- ・ <<Cloud for AWS>>ベースライセンスとして Floating を適用している場合、以下に注意してください。
 - 許容されるドライブ障害数(numberOfTolerableDriveFailures)の変更によって AWS License Manager のライセンスの契約容量を超過する場合があります。許容されるドライブ障害数(numberOfTolerableDriveFailures)を変更できるかどうか「ライセンスの使用量を確認するためにストレージプールの容量を試算する<<Cloud>>」を参照して、許容されるドライブ障害数(numberOfTolerableDriveFailures)を変更してもストレージプールの論理容量が AWS License Manager のライセンスの契約容量に収まるかを確認してください。なお、必要なライセンスの契約容量は、ストレージプールの論理容量を TiB 単位に切り上げて計算してください。複数のストレージクラスターで AWS License Manager のライセンスを共有している場合は、ストレージクラスターそれぞれのストレージプールの論理容量を先に TiB 単位に切り上げてから、それらを合計した値が、AWS License Manager のライセンスの契約容量に収まるかを確認してください。
(例) 2 つのストレージクラスターがあって、それぞれのストレージプールの論理容量が 31.3[TiB]と 47.7[TiB]の場合、それぞれの値を整数値に切り上げて 32[TiB]と 48[TiB]としてから、それらを合計して 80[TiB]と計算します。
契約容量が不足する場合、AWS Marketplace 上でライセンスの契約を更新してください。
 - リビルド領域ポリシーは"Fixed"から変更できません。

前提条件

- ・ 実行に必要なロール : Storage
- ・ ストレージプールのユーザーデータの冗長度が低下していないこと

操作手順

1. ストレージプールの ID と論理容量を確認します。
REST API : GET /v1/objects/pools
CLI : pool_list
2. リビルド領域ポリシーを"Variable"から"Fixed"、許容されるドライブ障害数を 0 に変更する場合は、任意のストレージコントローラーの当該ストレージコントローラー上で管理できる最大

の論理容量[MiB](allocatableCapacity)と当該ストレージコントローラー上で管理している論理容量[MiB](currentlyAllocatableCapacity)を確認します。

REST API : GET /v1/objects/storage-controllers

CLI : storage_controller_list

3. ストレージプールの設定を編集します。

ストレージプールの ID を指定してコマンドを実行します。

REST API : PATCH /v1/objects/pools/<id >

CLI : pool_set

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



注意

リビルド領域ポリシーの変更後に、指定したリビルド領域を確保できていなかった場合、ジョブの state は"Succeeded"になりますが、イベントログ KARS16147-W が出力されます。この場合は、ストレージプールの設定は変更できていますが、リビルド領域を確保するためには「リビルド領域の不足に対処する」に従ってドライブの増設が必要になります。

5. ストレージプールの情報を取得して、リビルド領域ポリシー、リビルド領域のリソース種別・リソース数、論理容量を確認します。

ストレージプールの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/pools/<id >

CLI : pool_show

論理容量が編集前と比べて増加している場合や、リビルド領域ポリシーを"Variable"から

"Fixed"、許容されるドライブ障害数を 0 に編集した場合は、内部処理であるストレージコントローラーへの容量割り付け処理が実行されることがあります。

イベントログを確認し、ストレージコントローラーへの容量割り付け処理開始を示すイベントログ KARS16021-I が出力されていない場合は、次の手順に進んでください。

ストレージコントローラーへの容量割り付け処理開始を示すイベントログ KARS16021-I が出力されている場合、イベントログ KARS16022-I または KARS16081-I が、既存のストレージノードの数だけ出力されるまでお待ちください。それまでは、他の操作が実施できないことがあります。ただし、イベントログ KARS16022-I または KARS16081-I が、既存のストレージノードの数だけ出力されるまでの間に、ストレージノードに障害が発生していた場合、ストレージプールの拡張ができていないことがあります。この場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」を参照して対処してください。

ストレージコントローラーへの容量割り付けの処理時間は、このマニュアルの「ストレージコントローラーへの容量割り付けの処理時間(論理容量)(目安)」を参照してください。

6. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

7. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

26.7 リビルド領域の不足に対処する

リビルド領域を確保するストレージプール設定で、リビルド領域の確保状態(rebuildCapacityStatus)が"Sufficient"でなく、対処をしたい場合、ドライブの増設が必要です。VSP One SDS Block の VSP One SDS Block Administrator でドライブの Health Status に "Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って対処してください。対処後に、まだリビルド領域が不足している場合は下記の手順を実施してください。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource
- VSP One SDS Block の VSP One SDS Block Administrator でドライブの Health Status に "Alerting"が表示されていないこと

操作手順

1. ストレージプールのリビルド領域の確保状態、リビルド領域ポリシー、リビルド領域のリソース種別・リソース数の許容されるドライブ障害数を確認します。
リビルド領域の確保状態が"Sufficient"の場合やリビルド領域を確保しない設定にしている場合は対処は不要です。
REST API : GET /v1/objects/pools
CLI : pool_list
2. ストレージノードの一覧を取得します。操作に必要な情報は VSP One SDS Block Administrator でも確認可能です。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
3. ストレージノードのリビルド可能なドライブ数を確認し、リビルド領域が不足しているストレージノードを特定します。
リビルド領域が不足しているストレージノードは下記のように判定します。
 - リビルド領域ポリシーが"Fixed"の場合
リビルド可能なドライブ数がストレージプールに設定した許容されるドライブ障害数未満のストレージノード
 - リビルド領域ポリシーが"Variable"の場合
リビルド可能なドライブ数が 0 のストレージノード
4. 手順 3 で特定したストレージノードのリビルド領域の不足リソース(InsufficientResourcesForRebuildCapacity)を確認し、リビルド領域の不足リソースで表示しているリビルド領域の不足ドライブ容量(capacityOfDrive)以上の容量のドライブをリビルド領域の不足ドライブ数(numberOfDrives)以上増設してください。
ドライブの増設については「ドライブを増設する」を参照してください。
5. すべてのストレージノードに対して対処が完了したら、ストレージプールの情報を取得し、リビルド領域の確保状態が"Sufficient"になっていることを確認してください。リビルド領域の確保状態は VSP One SDS Block Administrator でも確認可能です。
REST API : GET /v1/objects/pools

26.8 ライセンスの使用量を確認するためにストレージプールの容量を試算する《Cloud for AWS》

この節での記述内容は Cloud モデル for AWS に適用されます。

ベースライセンスとして Floating を適用している場合、ドライブやストレージノードの増設、許容されるドライブ障害数の変更によって AWS License Manager のライセンスの契約容量を超過する場合があります。

増設や変更手順を実施する前に、REST API または CLI を使用して、AWS License Manager のライセンスの契約容量に収まるかを取得情報から確認します。

ストレージノード数、ドライブ数、および許容されるドライブ障害数を指定してストレージプールの容量を試算する場合は「ストレージノード数、ドライブ数、およびドライブ障害数を指定して論理容量を試算する《Cloud for AWS》」を参照してください。

追加するストレージノード数、ドライブ数、または変更予定の許容されるドライブ障害数を指定してストレージプールの容量を試算する場合は「追加するストレージノード数、ドライブ数、またはドライブ障害数を指定して論理容量を試算する《Cloud for AWS》」を参照してください。



注意 構成変更を実施中のときは、以降に記載してある操作は実施しないでください。また、これらの操作では、指定されたストレージノード数または指定されたストレージノードの増加数について、ユーザーデータ保護方式、アベイラビリティゾーン構成における最小ストレージノード数、同時増設するストレージノード数といった要件を満たすかどうかの確認は行われません。



メモ

ベースライセンスとして Trial、Subscription、または Utility を適用している場合は、ここで説明するストレージプールの容量の試算はできません。

26.8.1 ストレージノード数、ドライブ数、およびドライブ障害数を指定して論理容量を試算する《Cloud for AWS》

この節での記述内容は Cloud モデル for AWS に適用されます。

ストレージプール容量の試算情報を取得します。ストレージクラスターを構成するストレージノード数、ドライブの数、および許容されるドライブ障害数を指定したときの試算情報が取得できます。

- `estimatedPoolCapacityInTiB` : 容量試算結果[TiB]。論理容量が構成できない場合は `null`
- `differenceCapacityInTiB` : 現在の論理容量と `estimatedPoolCapacityInTiB` の差分[TiB]。論理容量が構成できない場合は `null`
- `numberOfStorageNodes` : 指定されたストレージノードの数。
- `numberOfDrives` : 指定された各ストレージノードのドライブの数。
- `numberOfTolerableDriveFailures` : 指定された構成で許容されるドライブ障害数。



ヒント

ストレージクラスターが Multi-AZ 構成の場合、ストレージノード数はタイブレーカーノードを除いて指定してください。

前提条件

- 実行に必要なロール : Storage または Monitor

操作手順

1. 容量試算の対象となるストレージプールの ID を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

2. 以下のコマンドを実行します。

ストレージプールの ID と、容量試算のためのパラメーター(numberOfStorageNodes、numberOfDrives、および numberOfTolerableDriveFailures)を指定してコマンドを実行します。

REST API : GET /v1/objects/pools/<id >/estimated-capacity-for-specified-configuration

CLI : estimated_capacity_for_specified_configuration_show



メモ

ベースライセンスとして Floating が適用されていない環境でコマンドを実行した場合、ジョブは失敗します。

26.8.2 追加するストレージノード数、ドライブ数、またはドライブ障害数を指定して論理容量を試算する《Cloud for AWS》

この節での記述内容は Cloud モデル for AWS に適用されます。

ストレージプール容量の試算情報を取得します。現状に加えて増設するストレージノード数、ドライブの数、または変更予定の許容されるドライブ障害数を指定したときの試算情報が取得できます。

- estimatedPoolCapacityInTiB : 容量試算結果[TiB]。論理容量が構成できない場合は null
- differenceCapacityInTiB : 現在の論理容量と estimatedPoolCapacityInTiB の差分[TiB]。論理容量が構成できない場合は null
- numberOfStorageNodes : 指定されたストレージノードの増加数。指定がなかった場合は null
- numberOfDrives : 指定された各ストレージノードに増設するドライブの増加数。指定がなかった場合は null
- numberOfTolerableDriveFailures : 指定された構成で許容されるドライブ障害数。指定がなかった場合は null

前提条件

- 実行に必要なロール : Storage または Monitor

操作手順

1. 容量増加の対象となるストレージプールの ID を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

2. 以下のコマンドを実行します。

ストレージプールの ID と、容量試算のためのパラメーター(numberOfStorageNodes、numberOfDrives、または numberOfTolerableDriveFailures)を指定してコマンドを実行します。

REST API : GET /v1/objects/pools/<id >/estimated-capacity-for-updated-configuration

CLI : estimated_capacity_for_updated_configuration_show



メモ

ベースライセンスとして Floating が適用されていない環境でコマンドを実行した場合、ジョブは失敗します。

ストレージクラスターの情報を取得する

- 27.1 ストレージクラスター情報の取得
- 27.2 フォールトドメイン情報の一覧の取得
- 27.3 フォールトドメイン情報の個別取得
- 27.4 ヘルスステータスを取得する
- 27.5 クラスターマスターノード(プライマリー)かを確認する

27.1 ストレージクラスターの情報の取得

ストレージクラスターの情報が取得できます。

27.1.1 取得できるストレージクラスターの情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が取得できます。

- `storageDeviceId` : ストレージ装置の種別を識別するための ID
- `id` : ストレージクラスターの UUID
- `modelName` : 製品モデル名
- `internalId` : ストレージクラスターの内部で利用する ID
- `nickname` : ストレージクラスターのニックネーム
- `numberOfTotalVolumes` : 作成済みボリューム数
- `numberOfTotalServers` : 登録済みコンピュータノード数
- `numberOfTotalStorageNodes` : ストレージクラスターを構成するストレージノードの総数
- `numberOfReadyStorageNodes` : ストレージクラスターにおける通常動作中のストレージノード数
- `numberOfFaultDomains` : ストレージクラスターを構成するフォールトドメインの総数
- `totalPoolRawCapacity` : ストレージクラスターを構成する全ストレージプールの有効物理容量の総和[MiB]
- `totalPoolPhysicalCapacity` : ストレージクラスターを構成する全ストレージプールの総物理容量[MiB]
- `totalPoolCapacity` : ストレージクラスターを構成する全ストレージプールの総論理容量[MiB]
- `usedPoolCapacity` : ストレージクラスターを構成する全ストレージプールの総使用容量[MiB]
- `freePoolCapacity` : ストレージクラスターを構成する全ストレージプールの総空き容量[MiB]
- `savingEffects` : ストレージクラスター全体での容量削減機能の効果
- `softwareVersion` : ストレージソフトウェアのバージョン
- `statusSummary` : ストレージクラスターの状態のサマリー
- `status` : ストレージクラスターの管理状態
- `writeBackModeWithCacheProtection` : 当該ストレージクラスターのキャッシュ保護付きライトバックモードの状態
- `metaDataRedundancyOfCacheProtectionSummary` : キャッシュ保護付きライトバックモードのキャッシュ保護用メタデータ冗長度のサマリー
- `installationMethod` : ストレージクラスターの構築方法
- `systemRequirementsFileVersion` : ストレージクラスターに登録されているシステム要件ファイルのバージョン
- `serviceId` : ストレージクラスターのサービス ID。当該属性には常に `null` が出力されます。
- `deploymentType` : ストレージノードの配置種別。常に"Normal"

- `metadataDriveWriteReductionMode`: ストレージクラスターのメタデータのドライブ書き込み削減モードの状態



メモ

`totalEfficiency[%]`は、ボリューム作成機能とスナップショット機能、および容量削減機能による、容量消費の節減効果を示します。

ストレージプールの使用容量(`usedCapacity[MiB]`)に対する作成済みの合計ボリューム容量

(`totalVolumeCapacity[MiB]`)の比率をストレージコントローラーごとに算出して、各ストレージコントローラーの作成済みの合計ボリューム容量の大きさに応じて重みを付けた平均の比率です。作成済みの合計ボリューム容量の大きいストレージコントローラーの容量消費の節減効果ほど、より `totalEfficiency` の値に反映されます。例えば、各ストレージコントローラーにおいて、いずれも作成済みの合計ボリューム容量が 1,000 で、ストレージプールの使用容量が 50 の場合は、REST API と CLI では、`totalEfficiency` として、2,000 が出力されます。

VSP One SDS Block Administrator では、`totalEfficiency` に相当する値が、ダッシュボード画面(Total Efficiency)と Storage Pool 画面(TOTAL EFFICIENCY)に"20.00:1"と表示されます。また、VSP One SDS Block Administrator のダッシュボード画面では、比率が 9,999,999:100 より大きい場合は、">99999.99:1"と表示されます。

スナップショットボリュームを使用している場合、P-VOL と S-VOL の差分データだけを保持することで使用済みのストレージプールの容量を低減できます。そのため、作成済みの合計ボリューム容量が同じでも、スナップショットボリュームを含まない場合と比べて、`totalEfficiency` の値は大きくなります。

ストレージプールの拡張処理が動作して、KARS16017-I、KARS16020-I、KARS16022-I、KARS16081-I のいずれかが出力されている場合は、スナップショット操作を実施していなくても、`totalEfficiency` の値が大きくなることがあります。なお、スナップショット操作とは、スナップショットの取得準備、取得、削除、復元を指します。

27.1.2 取得できるストレージクラスターの情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が取得できます。

- `storageDeviceId`: ストレージ装置の種別を識別するための ID
- `id`: ストレージクラスターの UUID
- `modelName`: 製品モデル名
- `internalId`: ストレージクラスターの内部で利用する ID
- `nickname`: ストレージクラスターのニックネーム
- `numberOfTotalVolumes`: 作成済みボリューム数
- `numberOfTotalServers`: 登録済みコンピュータノード数
- `numberOfTotalStorageNodes`: ストレージクラスターを構成するストレージノードの総数
- `numberOfReadyStorageNodes`: ストレージクラスターにおける通常動作中のストレージノード数
- `numberOfFaultDomains`: ストレージクラスターを構成するフォールトドメインの総数
- `totalPoolRawCapacity`: ストレージクラスターを構成する全ストレージプールの有効物理容量の総和[MiB]
- `totalPoolPhysicalCapacity`: ストレージクラスターを構成する全ストレージプールの総物理容量[MiB]
- `totalPoolCapacity`: ストレージクラスターを構成する全ストレージプールの総論理容量[MiB]
- `usedPoolCapacity`: ストレージクラスターを構成する全ストレージプールの総使用容量[MiB]
- `freePoolCapacity`: ストレージクラスターを構成する全ストレージプールの総空き容量[MiB]
- `savingEffects`: ストレージクラスター全体での容量削減機能の効果

- `softwareVersion` : ストレージソフトウェアのバージョン
- `statusSummary` : ストレージクラスターの状態のサマリー
- `status` : ストレージクラスターの管理状態
- `writeBackModeWithCacheProtection` : 当該ストレージクラスターのキャッシュ保護付きライトバックモードの状態
- `metaDataRedundancyOfCacheProtectionSummary` : キャッシュ保護付きライトバックモードのキャッシュ保護用メタデータ冗長度のサマリー
- `installationMethod` : ストレージクラスターの構築方法
- `systemRequirementsFileVersion` : ストレージクラスターに登録されているシステム要件ファイルのバージョン
- `serviceId` : ストレージクラスターのサービス ID。当該属性には常に `null` が出力されます。
- `deploymentType` : ストレージノードの配置種別。Single-AZ (Single-Zone)構成の場合は常に "Normal"、Multi-AZ (Multi-Zone)構成の場合は"Multi-AZ"
- `metadataDriveWriteReductionMode` : ストレージクラスターのメタデータのドライブ書き込み削減モードの状態



メモ

- `totalEfficiency[%]`は、ボリューム作成機能とスナップショット機能、および容量削減機能による、容量消費の節減効果を示します。
ストレージプールの使用容量(`usedCapacity[MiB]`)に対する作成済みの合計ボリューム容量(`totalVolumeCapacity[MiB]`)の比率をストレージコントローラーごとに算出して、各ストレージコントローラーの作成済みの合計ボリューム容量の大きさに応じて重みを付けた平均の比率です。作成済みの合計ボリューム容量の大きいストレージコントローラーの容量消費の節減効果ほど、より `totalEfficiency` の値に反映されます。例えば、各ストレージコントローラーにおいて、いずれも作成済みの合計ボリューム容量が 1,000 で、ストレージプールの使用容量が 50 の場合は、REST API と CLI では、`totalEfficiency` として、2,000 が出力されます。
VSP One SDS Block Administrator では、`totalEfficiency` に相当する値が、ダッシュボード画面(Total Efficiency)と Storage Pool 画面(TOTAL EFFICIENCY)に"20.00:1"と表示されます。また、VSP One SDS Block Administrator のダッシュボード画面では、比率が 9,999,999:100 より大きい場合は、">999999.99:1"と表示されます。
スナップショットボリュームを使用している場合、P-VOL と S-VOL の差分データだけを保持することで使用済みのストレージプールの容量を低減できます。そのため、作成済みの合計ボリューム容量が同じでも、スナップショットボリュームを含まない場合と比べて、`totalEfficiency` の値は大きくなります。
ストレージプールの拡張処理が動作して、KARS16017-I、KARS16020-I、KARS16022-I、KARS16081-I のいずれかが出力されている場合は、スナップショット操作を実施していなくても、`totalEfficiency` の値が大きくなる場合があります。なお、スナップショット操作とは、スナップショットの取得準備、取得、削除、復元を指します。
- `numberOfTotalVolumes` で取得できる作成済みボリューム数には、`volumeType` が "ExternalMigrationOrigin"のボリュームは含まれません。

27.1.3 ストレージクラスターの情報を取得する

ストレージクラスターについての情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. ストレージクラスターの情報を取得します。

REST API : GET /v1/objects/storage

CLI : storage_show

27.2 フォールトドメイン情報の一覧の取得

フォールトドメイン情報の一覧を取得します。

27.2.1 取得できるフォールトドメインの一覧情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が取得できます。

- id : フォールトドメインの ID(uuid)
- name : フォールトドメインの名前
- statusSummary : フォールトドメインの状態のサマリー
- status : フォールトドメインの状態
- numberOfStorageNodes : フォールトドメインに属するストレージノード数
- availabilityZoneId : null
- physicalZone : null
- logicalZone : null
- totalCapacity : フォールトドメイン上で管理できる最大の論理容量[MiB]
- usedCapacity : フォールトドメインの使用容量[MiB]
- freeCapacity : フォールトドメインの空き容量[MiB]
- usedCapacityRate : フォールトドメインの論理容量の使用率[%]
- totalVolumeCapacity : 当該フォールトドメイン上で作成済みのボリュームの総容量[MiB]
- provisionedVolumeCapacity : 当該フォールトドメインで作成済みのプロビジョンドボリュームの総容量[MiB]
- otherVolumeCapacity : 当該フォールトドメインで作成済みのアザーボリュームの総容量[MiB]
- temporaryVolumeCapacity : 当該フォールトドメインで作成済みの一時的なボリュームの総容量[MiB]

27.2.2 取得できるフォールトドメインの一覧情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が取得できます。

- id : フォールトドメインの ID(uuid)
- name : フォールトドメインの名前
- statusSummary : フォールトドメインの状態のサマリー
- status : フォールトドメインの状態
- numberOfStorageNodes : フォールトドメインに属するストレージノード数

- **availabilityZoneId** :
 <<Cloud for AWS>>Multi-AZ 構成の場合、フォールトドメインに対応するアベイラビリティゾーンの ID。physicalZone と同じ値のため、基本的には **physicalZone** を参照してください。
 Single-AZ 構成の場合 null
 <<Cloud for Google Cloud>>null
 <<Cloud for Microsoft Azure>>null
- **physicalZone** :
 <<Cloud for AWS>>Multi-AZ 構成の場合、フォールトドメインに対応するアベイラビリティゾーン
 の ID。availabilityZoneId と同じ値。Single-AZ 構成の場合は null
 <<Cloud for Google Cloud>>Multi-AZ (Multi-Zone)構成の場合、フォールトドメインに対応する
 ゾーンの ID。Single-AZ (Single-Zone)構成の場合は null
 <<Cloud for Microsoft Azure>>フォールトドメインに対応する物理ゾーンの ID
- **logicalZone** :
 <<Cloud for AWS>>null
 <<Cloud for Google Cloud>>null
 <<Cloud for Microsoft Azure>>フォールトドメインに対応する論理ゾーンの ID
- **totalCapacity** : フォールトドメイン上で管理できる最大の論理容量[MiB]
- **usedCapacity** : フォールトドメインの使用容量[MiB]
- **freeCapacity** : フォールトドメインの空き容量[MiB]
- **usedCapacityRate** : フォールトドメインの論理容量の使用率[%]
- **totalVolumeCapacity** : 当該フォールトドメイン上で作成済みのボリュームの総容量[MiB]
- **provisionedVolumeCapacity**: 当該フォールトドメインで作成済みのプロビジョンドボリューム
 の総容量[MiB]
- **otherVolumeCapacity** : 当該フォールトドメインで作成済みのアザーボリュームの総容量[MiB]
- **temporaryVolumeCapacity** : 当該フォールトドメインで作成済みの一時的なボリュームの総容
 量[MiB]

27.2.3 フォールトドメイン情報の一覧を取得する

各フォールトドメインの情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. フォールトドメイン情報の一覧を取得します。
 REST API : GET /v1/objects/fault-domains
 CLI : fault_domain_list

27.3 フォールトドメイン情報の個別取得

指定した ID のフォールトドメインの情報を取得します。

27.3.1 取得できるフォールトドメインの個別情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

指定した ID のフォールトドメインについて、以下の情報が取得できます。

- storageNodeIds : フォールトドメインに属するストレージノードの ID(uuid)の一覧
- id : フォールトドメインの ID(uuid)
- name : フォールトドメインの名前
- statusSummary : フォールトドメインの状態のサマリー
- status : フォールトドメインの状態
- numberOfStorageNodes : フォールトドメインに属するストレージノード数
- availabilityZoneId : null
- physicalZone : null
- logicalZone : null
- totalCapacity : フォールトドメイン上で管理できる最大の論理容量[MiB]
- usedCapacity : フォールトドメインの使用容量[MiB]
- freeCapacity : フォールトドメインの空き容量[MiB]
- usedCapacityRate : フォールトドメインの論理容量の使用率[%]
- totalVolumeCapacity : 当該フォールトドメイン上で作成済みのボリュームの総容量[MiB]
- provisionedVolumeCapacity : 当該フォールトドメインで作成済みのプロビジョンドボリュームの総容量[MiB]
- otherVolumeCapacity : 当該フォールトドメインで作成済みのアザーボリュームの総容量[MiB]
- temporaryVolumeCapacity : 当該フォールトドメインで作成済みの一時的なボリュームの総容量[MiB]

27.3.2 取得できるフォールトドメインの個別情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

指定した ID のフォールトドメインについて、以下の情報が取得できます。

- storageNodeIds : フォールトドメインに属するストレージノードの ID(uuid)の一覧
- id : フォールトドメインの ID(uuid)
- name : フォールトドメインの名前
- statusSummary : フォールトドメインの状態のサマリー
- status : フォールトドメインの状態
- numberOfStorageNodes : フォールトドメインに属するストレージノード数
- availabilityZoneId :
 <<Cloud for AWS>>Multi-AZ 構成の場合、フォールトドメインに対応するアベイラビリティゾーン
 の ID。physicalZone と同じ値のため、基本的には physicalZone を参照してください。
 Single-AZ 構成の場合は null
 <<Cloud for Google Cloud>>null
 <<Cloud for Microsoft Azure>>null
- physicalZone :

≪Cloud for AWS≫Multi-AZ 構成の場合、フォールトドメインに対応するアベイラビリティゾーンの ID。availabilityZoneId と同じ値。Single-AZ 構成の場合は null
≪Cloud for Google Cloud≫Multi-AZ (Multi-Zone)構成の場合、フォールトドメインに対応するゾーンの ID。Single-AZ (Single-Zone)構成の場合は null
≪Cloud for Microsoft Azure≫フォールトドメインに対応する物理ゾーンの ID

- logicalZone :
≪Cloud for AWS≫null
≪Cloud for Google Cloud≫null
≪Cloud for Microsoft Azure≫フォールトドメインに対応する論理ゾーンの ID
- totalCapacity : フォールトドメイン上で管理できる最大の論理容量[MiB]
- usedCapacity : フォールトドメインの使用容量[MiB]
- freeCapacity : フォールトドメインの空き容量[MiB]
- usedCapacityRate : フォールトドメインの論理容量の使用率[%]
- totalVolumeCapacity : 当該フォールトドメイン上で作成済みのボリュームの総容量[MiB]
- provisionedVolumeCapacity : 当該フォールトドメインで作成済みのプロビジョンドボリュームの総容量[MiB]
- otherVolumeCapacity : 当該フォールトドメインで作成済みのアザーボリュームの総容量[MiB]
- temporaryVolumeCapacity : 当該フォールトドメインで作成済みの一時的なボリュームの総容量[MiB]

27.3.3 フォールトドメイン情報を個別に取得する

指定した ID のフォールトドメインの情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. フォールトドメインの ID を確認します。
REST API : GET /v1/objects/fault-domains
CLI : fault_domain_list
2. フォールトドメインの情報を取得します。
フォールトドメインの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/fault-domains/<id >
CLI : fault_domain_show

27.4 ヘルスステータスを取得する

各リソースのヘルスステータスを取得します。

- type : リソース種別
- status : ヘルスステータス
status は、"Normal"または"Alerting"で表示されます。ストレージノード、ストレージプール、コンピュートポート、ドライブ、ボリューム、管理ポート、ストレージノード間ポートについて

ては、対象のプロテクションドメインに属しているリソース種別のうち、1 つ以上のリソースで `statusSummary` が "Warning" または "Error" だった場合、ヘルスステータスは "Alerting" になります。

- `protectionDomainId` : プロテクションドメインの ID(uuid)
ストレージクラスター全体で管理するリソース(ストレージクラスター、ライセンス、フォールトドメイン)の場合、プロテクションドメインの ID は null になります。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. 各リソースのヘルスステータスを取得します。

REST API : GET /v1/objects/health-status

CLI : `health_status_show`

27.5 クラスターマスターノード(プライマリー)かを確認する

リクエスト先のストレージノードが、クラスターマスターノード(プライマリー)であるか否かを示す以下の情報を取得します。

ロールによる実行制限はありません。

- `isStorageMasterNodePrimary` : リクエスト先のストレージノードが、クラスターマスターノード(プライマリー)であるか否かを示す情報

操作手順

1. クラスターマスターノード(プライマリー)であることを確認します。

REST API : GET /configuration/storage-master-node-primary-flag

CLI : `storage_master_node_primary_flag_show`

`isStorageMasterNodePrimary` として true が返されたときは、リクエスト先のストレージノードが、クラスターマスターノード(プライマリー)です。この場合、REST API のときは HTTP ステータスコードとして 200(OK)が返ります。一方、KARS15590-E のエラーが返されたときは、クラスターマスターノード(プライマリー)ではありません。この場合、REST API のときは HTTP ステータスコードとして 404(Not Found)が返ります。

プロテクションドメインを管理する

- 28.1 プロテクションドメイン情報の一覧を取得する
- 28.2 プロテクションドメイン情報を個別に取得する
- 28.3 内部処理 I/O のリソース使用率を変更する

28.1 プロテクションドメイン情報の一覧を取得する

各プロテクションドメインの情報を一覧で取得します。以下の情報が取得できます。

- `id` : プロテクションドメインの ID(uuid)
- `name` : プロテクションドメインの名前
- `redundantPolicy` : ユーザーデータの保護方式
- `redundantType` : ユーザーデータの保護種別
- `driveDataRelocationStatus` : ドライブデータ再配置の状態
- `driveDataRelocationProgressRate` : ドライブデータ再配置の処理の進捗率[%]
- `rebuildStatus` : リビルドの状態
- `rebuildProgressRate` : リビルドの処理の進捗率[%]
- `memoryMode` : 使用しているメモリーの設定
- `asyncProcessingResourceUsageRate` : 内部処理 I/O リソース使用率
- `numberOfFaultDomains` : プロテクションドメイン内のフォールトドメインの総数
- `storageControllerClusteringPolicy` : ストレージコントローラーのクラスターポリシー
- `minimumMemorySize` : プロテクションドメインに属する各ストレージノードの中で最小となるメモリーの値[MiB]

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. プロテクションドメイン情報の一覧を取得します。

REST API : GET /v1/objects/protection-domains

CLI : `protection_domain_list`

28.2 プロテクションドメイン情報を個別に取得する

指定した ID のプロテクションドメインについて、以下の情報を取得します。

- `totalPhysicalCapacity` : プロテクションドメイン内のドライブの総容量[MiB]
- `isFastRebuildEnabled` : 高速リビルドの有効/無効
- `id` : プロテクションドメインの ID(uuid)
- `name` : プロテクションドメインの名前
- `redundantPolicy` : ユーザーデータの保護方式
- `redundantType` : ユーザーデータの保護種別
- `driveDataRelocationStatus` : ドライブデータ再配置の状態
- `driveDataRelocationProgressRate` : ドライブデータ再配置の処理の進捗率[%]
- `rebuildStatus` : リビルドの状態

- rebuildProgressRate : リビルドの処理の進捗率[%]
- memoryMode : 使用しているメモリーの設定
- asyncProcessingResourceUsageRate : 内部処理 I/O リソース使用率
- numberOfFaultDomains : プロテクションドメイン内のフォールトドメインの総数
- storageControllerClusteringPolicy : ストレージコントローラーのクラスターポリシー
- minimumMemorySize : プロテクションドメインに属する各ストレージノードの中で最小となるメモリーの値[MiB]

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. プロテクションドメインの ID を確認します。
REST API : GET /v1/objects/protection-domains
CLI : protection_domain_list
2. プロテクションドメインの情報を取得します。
プロテクションドメインの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/protection-domains/<id >
CLI : protection_domain_show

28.3 内部処理 I/O のリソース使用率を変更する

ホスト I/O と、内部処理 I/O(リビルド、ドライブデータ再配置)が同時に動作中の場合、内部処理 I/O に対するストレージノード間ネットワークの帯域の割り当て比率を設定します。

内部処理 I/O が動作していない場合は、ストレージノード間ネットワークの帯域は、設定によらず、すべてホスト I/O に割り当てられます。

設定値	説明	備考
VeryHigh	内部処理 I/O を最優先します。 内部処理 I/O に対しストレージノード間ネットワークの帯域を最大で 80%程度割り当てます。 "VeryHigh"が有効に機能する条件は、ストレージノード間ネットワークで 25Gbps 以上の帯域が使用できることです。	左記の割り当て比率は、ストレージノード間ネットワークで 10Gbps 以上(VeryHigh の場合は 25Gbps 以上)の帯域が使用できることを前提としています。
High	内部処理 I/O を優先します。 内部処理 I/O に対しストレージノード間ネットワークの帯域を最大で 80%程度割り当てます。	
Middle (デフォルト)	内部処理 I/O に対しストレージノード間ネットワークの帯域を最大で 60%程度割り当てます。	
Low	ホスト I/O を優先します。 内部処理 I/O に対しストレージノード間ネットワークの帯域を最大で 20%程度割り当てます。	



注意

VeryHigh の設定で内部処理 I/O を動作させるには、ストレージノード間ネットワークで 25Gbps 以上の帯域が使用できることが条件です。設定する前に、ストレージノード間ネットワークの設定を見直し、条件を満たしていることを確認してください。条件を満たしていない場合、利用可能なストレージノード間ネットワーク帯域がすべて消費される影響で、ホスト I/O、内部処理 I/O ともに性能が著しく低下することがあります。

前提条件

- 実行に必要なロール：Storage または Service

操作手順

1. プロテクションドメインの ID を確認します。

REST API : GET /v1/objects/protection-domains

CLI : protection_domain_list

2. プロテクションドメインの設定を編集します。

プロテクションドメインの ID を指定してコマンドを実行します。

REST API : PATCH /v1/objects/protection-domains/<id >

CLI : protection_domain_set

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

内部処理 I/O が動作中に設定変更した場合は、設定された値は、1 時間以内(目安)に機能します。

4. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

5. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

ストレージコントローラーを管理する

- 29.1 機能の概要
- 29.2 ストレージコントローラーの容量状態
- 29.3 ストレージコントローラーの情報の取得
- 29.4 ストレージコントローラーの設定を編集する

29.1 機能の概要

ストレージコントローラーは、ストレージノードの容量やボリュームを管理する VSP One SDS Block の一部のプロセスです。

各ストレージノードの容量は、ストレージコントローラーによって管理されます。ストレージコントローラーは、システムの構成や使用状況を監視しており、自動で容量の拡張を実施します。

ストレージコントローラーはストレージノードと同数あり、それらが複数動作して、それぞれが管理する容量をまとめたものが、ストレージプールの全体容量になります。

容量拡張の契機

ストレージプールの拡張の際に追加した容量や、リビルド(データ再構築)の処理の際に予約されていた容量を、ユーザーデータ容量として利用可能にします。

主に以下に該当する場合に容量の拡張が実施されます。

- ・ ストレージプールの拡張を実行したとき
- ・ ストレージプールの容量の使用率が上がったとき

処理時間(目安)

ストレージコントローラーへの容量割り付けの処理時間は、このマニュアルの「ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安)」を参照してください。

29.2 ストレージコントローラーの容量状態

ストレージコントローラー情報の一覧の取得、またはストレージコントローラー情報の取得で得られる情報のうち、ストレージコントローラーの容量状態について以下に示します。

ストレージコントローラーの容量状態(capacityStatus)

状態	説明
正常(Normal)	ストレージコントローラーが管理している容量の使用率が高くなく、正常な状態です。 具体的には以下の状態です。 ・ 当該ストレージコントローラー上で管理できる最大の論理容量に対する使用率が、max 未満(ストレージプールの枯渇しきい値が 80%未満)である ・ 当該ストレージコントローラー上で管理している論理容量に対する使用率が 80%未満である
警告(Warning)	ストレージコントローラーが管理している容量の使用率が高くなっている状態です。または、容量の使用率が高くなったときに動作するストレージコントローラーの容量の最大拡張が実行できていない状態です。 具体的には以下の状態です。 ・ 当該ストレージコントローラー上で管理できる最大の論理容量に対する使用率が、max 以上(ストレージプールの枯渇しきい値が 80%)であり、かつストレージコントローラー枯渇しきい値未満である ・ 当該ストレージコントローラー上で管理している論理容量に対する使用率が 80%以上、かつストレージコントローラー枯渇しきい値未満、かつリビルド

状態	説明
	用の容量を使用したストレージコントローラーの容量の最大拡張が 5 分以上実行されていない
異常(Error)	ストレージコントローラーが管理している容量の使用率が高く、枯渇の可能性がある状態です。 具体的には以下の状態です。 - 当該ストレージコントローラー上で管理できる最大の論理容量に対する使用率がストレージコントローラー枯渇しきい値以上である - 当該ストレージコントローラー上で管理している論理容量に対する使用率がストレージコントローラー枯渇しきい値以上である

29.3 ストレージコントローラーの情報の取得

ストレージコントローラーの情報が一覧または個別に取得できます。

29.3.1 取得できるストレージコントローラーの情報

以下の情報が一覧または個別に取得できます。

- id : ストレージコントローラーの ID(uuid)
- allocatableCapacity : 当該ストレージコントローラー上で管理できる最大の論理容量[MiB]
- currentlyAllocatableCapacity : 当該ストレージコントローラー上で管理している論理容量[MiB]
- usedCapacity : 当該ストレージコントローラーで管理しているストレージプールの使用容量[MiB]
- logicalLimit : 当該ストレージコントローラー上で作成可能なボリュームの最大論理容量[MiB]
- volumeMaximumCapacity : 当該ストレージコントローラー上で作成可能な単一ボリュームの最大容量[MiB]
- freeCapacity : 当該ストレージコントローラーで管理しているストレージプールの空き容量[MiB]
- status : ストレージコントローラーの状態
- metaDataRedundancyOfCacheProtection : ストレージコントローラーにおけるキャッシュ保護付きライトバックモードのキャッシュ保護用メタデータ冗長度
- activeStorageNodeId : アクティブ側のストレージコントローラーが動作しているストレージノードの ID(uuid)
- standbyStorageNodeId : スタンバイ側のストレージコントローラーが動作しているストレージノードの ID(uuid)
- secondaryStandbyStorageNodeId : 2 台目のスタンバイ側のストレージコントローラーが動作しているストレージノードの ID(uuid)
- isDetailedLoggingMode : ログ詳細化モードの有効/無効
- allocatableCapacityUsageRate : 当該ストレージコントローラー上で管理できる最大の論理容量に対する使用率[%]
- currentlyAllocatableCapacityUsageRate : 当該ストレージコントローラー上で管理している論理容量に対する使用率[%]
- capacityStatus : 当該ストレージコントローラーが管理している容量の状態

- **dataRebalanceStatus**: ストレージコントローラー単位に管理するユーザーデータ容量に対する平準化処理の状態
- **dataRebalanceProgressRate**: ストレージコントローラー単位に管理するユーザーデータ容量に対する平準化処理の進捗率[%]
- **totalVolumeCapacity**: 当該ストレージコントローラー上で作成済みの合計ボリューム容量 [MiB]
- **provisionedVolumeCapacity**: 当該ストレージコントローラー上で作成済みのプロビジョンドボリューム容量 [MiB]
- **otherVolumeCapacity**: 当該ストレージコントローラー上で作成済みのアザーボリューム容量 [MiB]
- **temporaryVolumeCapacity**: 当該ストレージコントローラー上で作成済みの一時ボリューム容量 [MiB]
- **capacitiesExcludingSystemData**: ストレージコントローラーの容量削減機能によって削減された容量に関する情報
 - **usedVolumeCapacity**: ボリュームの使用量 [MiB]
 - **compressedCapacity**: 圧縮による削減量 [MiB]。容量削減機能によるシステムデータ使用量は含まない。
 - **reclaimedCapacity**: 固定パターン排除による削減量 [MiB]。容量削減機能によるシステムデータ使用量は含まない。
 - **systemDataCapacity**: 容量削減機能によるシステムデータ使用量(メタデータ量およびガベージデータ量) [MiB]
 - **preUsedCapacity**: 容量削減対象データの削減前の容量 [MiB]
 - **preCompressedCapacity**: 圧縮対象データの圧縮前の容量 [MiB]
- **udpPort**: 仮想コマンドデバイスの UDP 通信ポート番号
- **pinInformation**: PIN の情報
- **primaryFaultDomainId**: ストレージコントローラーの本来アクティブなストレージノードが属するプライマリーのフォールトドメインの ID

29.3.2 ストレージコントローラー情報の一覧を取得する

各ストレージコントローラーの情報を一覧で取得します。

前提条件

- 実行に必要なロール: Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ストレージコントローラーの情報の一覧を取得します。

REST API: GET /v1/objects/storage-controllers

CLI: storage_controller_list

29.3.3 ストレージコントローラー情報を個別に取得する

指定した ID のストレージコントローラーの情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. ストレージコントローラーの ID を確認します。
REST API : GET /v1/objects/storage-controllers
CLI : storage_controller_list
2. ストレージコントローラーの情報を取得します。
ストレージコントローラーの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/storage-controllers/<id >
CLI : storage_controller_show

29.4 ストレージコントローラーの設定を編集する

ストレージコントローラーの設定を編集します。ログ詳細化モードの有効/無効の設定ができます。ただし、サポートセンターから依頼があった場合のみ、設定を true にしてください。

前提条件

- 実行に必要なロール : Service

操作手順

1. 特定のストレージコントローラーについての設定を編集する場合は、ストレージコントローラーの ID を指定してコマンドを実行します。
すべてのストレージコントローラーについての設定を編集する場合は、ストレージコントローラーの ID を指定せずにコマンドを実行します。
ログ詳細化モードの設定パラメーターは必須です。
REST API : POST /v1/objects/storage-controllers/actions/configure/invoke
CLI : storage_controller_configure
コマンド実行後に表示されるジョブの ID を確認します。



ヒント

ストレージコントローラーの ID は以下のコマンドで確認できます。

REST API : GET /v1/objects/storage-controllers
CLI : storage_controller_list

2. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
3. ≪Bare metal≫構成情報のバックアップを行います。
「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

4. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

リビルド(データ再構築)の状態を確認する

- 30.1 リビルドの概要
- 30.2 リビルドが動作可能な条件
- 30.3 リビルド完了までの時間(目安)
- 30.4 リビルドの状態を確認する

30.1 リビルドの概要

リビルド(データ再構築)は、ドライブやストレージノードの障害の際に、低下したデータの冗長度を自動的に回復させる機能です。

リビルドには次の 2 種類があります。

- 通常リビルド(Normal Rebuild) : リビルド対象のストレージノード、ドライブのデータをすべて再構築するリビルドです。単にリビルドと書いている場合は、通常リビルドの意味です。
- 高速リビルド(Fast Rebuild) : リビルド対象のストレージノード、ドライブのうち、必要なデータのみを再構築するリビルドです。高速リビルドは、通常リビルドに比べて、リビルド時間が短くなります。

リビルドの起動契機ごとの、リビルドの種類を以下に示します。

リビルドの起動契機		リビルドの種類
ドライブ障害の発生 ¹		通常リビルド
ソフトウェアアップデートの実施 ²		高速リビルド
ストレージノードの保守回復	ストレージノード障害発生後の手動での保守回復	通常リビルド
	保守閉塞後の手動での保守回復	高速リビルド
	ストレージノードの自動回復	
ストレージノードの交換		通常リビルド
1. ドライブの障害が発生した場合、同一のストレージノードに十分な空き領域がないときは、ドライブ容量不足によるリビルドの失敗になりますので、注意してください。 2. ソフトウェアアップデートが中断された場合、ソフトウェアアップデート実施中だったストレージノードのみ、ソフトウェアアップデート中断後に通常リビルドが動作する場合があります。		



メモ

- リビルド処理中に、ストレージノードの保守回復などの操作を実行することによって、リビルドが追加で動作する場合、リビルド処理はいったん中断したあとに、自動的に再開します。リビルド中断のイベントログ **KARS07002-I** が出力されたあと、リビルド開始のイベントログ **KARS07000-I** が出力されていれば、リビルドは正常に再開しており問題ありません。
- 高速リビルドが動作するケースでも、以下の条件に当てはまる場合は、通常リビルドが動作します。また、高速リビルドの動作後に、以下の条件を検知した場合も通常リビルドに切り替わります。その場合は、**KARS07102-I** のイベントログが出力されます。
 - リビルドが中断した場合¹
 - 保守回復するストレージノードのドライブを交換した場合
 - リビルドの内部処理でエラーが発生した場合
 - **HPEC 4D+2P** において、ユーザーデータの冗長度(**dataRedundancy**)が 0(冗長度なし)の場合²
 - ストレージノードの保守閉塞または障害発生後に、ストレージクラスターの停止または電断があった場合
- 1. リビルド中のストレージノードやドライブの閉塞、ストレージクラスターの電断、停止、ソフトウェアアップデートの中断など。中断したあとに動作するリビルドは通常リビルドになります。
- 2. 冗長度が 2 に回復するまでは通常リビルド動作となります。
- ドライブ障害と、そのドライブが搭載されているストレージノードの障害が併発した場合、以下の現象が発生する場合があります。
 - リビルドが複数回動作する

- リビルドのための空き領域の不足を示すイベントログ(KARS07005-E)が出力される
リビルドが複数回動作する場合はリビルドの中断を示すイベントログ(KARS07002-D)が出力されますが、その後しばらくして再開します。最終的にリビルドの完了を示すイベントログ(KARS07001-D)が出力されれば問題ありません。
- また、空き容量の不足を示すイベントログ(KARS07005-E)の出力は一時的なものである可能性があり、最終的にリビルドの完了を示すイベントログ(KARS07001-D)が出力されれば容量不足は解消されています。

30.2 リビルドが動作可能な条件

- リビルドに必要な空き領域が確保できること
ドライブの空き容量が不足していた場合は、リビルドできる領域のみ、リビルドが行われます。
- ストレージクラスターの status が"Ready"または"NondisruptiveUpdating"であること
status が"Ready"または"NondisruptiveUpdating"以外の場合、リビルドを動作させるためには、以下に従って対処してください。
 - 《Bare metal》status が"Stopping"または"Stopped"の場合「ストレージクラスターを起動する《Bare metal》」に従って、ストレージクラスターを起動してください。
 - 《Cloud》status が"Stopping"または"Stopped"の場合「ストレージクラスターを起動する《Cloud》」に従って、ストレージクラスターを起動してください。
 - 上記以外の status の場合、ストレージクラスターに対する処理が実施中のため、status が変わるまで待つてから、再度確認してください。
- 他のリビルドが動作していないこと
先行して他のリビルドが動作している場合は、先行のリビルドが完了するまで待たされる可能性があります。

30.3 リビルド完了までの時間(目安)

リビルドの処理時間[min](目安)は、以下の計算式から算出できます。

リビルド対象のデータ容量[TiB]×リビルドの単位処理時間[min]

リビルド対象のデータ容量は次のとおりです。

区分		リビルド対象のデータ容量
通常リビルド	ドライブ障害の場合	障害が発生したドライブの物理容量
	ストレージノードの保守回復の場合	- リビルド領域ポリシーが"Variable"の場合 回復対象ストレージノードに搭載されている物理容量 - リビルド領域ポリシーが"Fixed"の場合 回復対象ストレージノードに搭載されている物理容量から、確保しているリビルド領域の容量を引き算した容量 ここで、リビルド領域の容量は以下のように導き出します。 - 回復対象ストレージノードのリビルド可能リソース(rebuildableResources)のリビルド可能なドライブ数(numberOfDrives)を確認します。 - 回復対象ストレージノードのドライブを、容量の大きな順に numberOfDrives の数だけ選択します。 - 選択したドライブの物理容量の合計がリビルド領域の容量になります。

区分		リビルド対象のデータ容量
		リビルド領域の詳細は、このマニュアルの「ストレージプールのリビルド領域について」を参照してください。 また、回復対象ストレージノードのリビルド可能リソース(rebuildableResources)のリビルド可能なドライブ数(numberOfDrives)は、参照できないことがあるため(例えば、ストレージノードの status が"PersistentBlockage"の場合など)、その時点で見積もりが必要な場合はストレージプール情報のリビルド可能回数(numberOfDrives)を参照してください。
高速リビルド		ストレージノードの閉塞期間中に、ドライブへのライト I/O によって更新されたデータ容量。ライト I/O の負荷状況によって変化します。ドライブへのライト I/O は、コンピュータノードからの I/O とは非同期に動作することがあります。 ただし、ライト I/O がない領域でも、100GiB 当たり 3 秒程度の処理時間が掛かります。



ヒント

ドライブへのライト I/O の有無の確認方法については「ドライブの性能情報(低解像度)の一覧を取得する」または「ドライブの性能情報(高解像度)の一覧を取得する」を参照してください。

リビルドの単位処理時間[min]は、ドライブ上にユーザーデータがある(使用領域)場合とユーザーデータがない(未使用領域)場合で異なるため、ストレージプールの使用率(usedCapacityRate(%))から以下のように算出します。

リビルド種別	リビルド単位処理時間[min]
通常リビルド	$\text{ストレージプールの使用率}[\%] / 100 \times \text{使用領域のリビルド単位処理時間}[\text{min}] + (100[\%] - \text{ストレージプールの使用率}[\%]) / 100 \times \text{未使用領域のリビルド単位処理時間}[\text{min}]$
高速リビルド	使用領域のリビルド単位処理時間[min]

使用領域/未使用領域のリビルドの単位処理時間は、ユーザーデータの保護種別(redundantType)の設定と内部処理 I/O のリソース使用率の設定(asyncProcessingResourceUsageRate)によって、以下のように数値が変わります。

なお、asyncProcessingResourceUsageRate の設定は、内部処理 I/O(リビルド、ドライブデータ再配置)のリソース使用率を決めるものです。設定値を変更するには「内部処理 I/O のリソース使用率を変更する」を参照してください。

redundantType	asyncProcessingResourceUsageRate	使用領域のリビルド単位処理時間 [min]	未使用領域のリビルド単位処理時間 [min]
4D+1P	VeryHigh	30	8
	High	60	12
	Middle	80	15
	Low	200	30
4D+2P	VeryHigh	45	10
	High	90	15
	Middle	120	20
	Low	210	30

redundantType	asyncProcessingResourceUsageRate	使用領域のリビルド単位処理時間 [min]	未使用領域のリビルド単位処理時間 [min]
Duplication	VeryHigh	15	8
	High	25	12
	Middle	35	15
	Low	160	80

リビルドの処理時間[min]は、以下の前提条件を満たす構成での測定結果に基づいています。

- Bare metal モデル
- I/O 負荷あり
- ストレージノード数：6 台
- ストレージノード 1 台当たりのユーザーデータドライブの搭載台数：8 台
- 使用するユーザーデータドライブ：SAS SSD
- asyncProcessingResourceUsageRate が High/Middle/Low の場合：ストレージノード間ネットワークの帯域が 10Gbps
asyncProcessingResourceUsageRate が VeryHigh の場合：ストレージノード間ネットワークの帯域が 25Gbps
- ネットワークスイッチの MTU サイズ：9000 に設定
- allocatableCapacityUsageRate[%](ストレージコントローラー上で管理できる最大の論理容量に対する使用率)がストレージコントローラー間で均一

リビルドの処理時間[min]は、以下の条件によって上記の目安より増減することがあります。

- I/O 負荷の状況
- ストレージノード 1 台当たりのユーザーデータドライブの搭載台数
ユーザーデータドライブの搭載台数が 8 台未満の場合、ユーザーデータドライブ 1 台当たりの I/O 負荷が高まることによって、目安よりも長くなることがあります。
ユーザーデータドライブの搭載台数が 9 台以上の場合、ユーザーデータドライブ 1 台当たりの I/O 負荷が減ることによって、目安よりも短くなることがあります。
- HPEC の場合のストレージノード数
ストレージノード数が 6 台未満の場合、ストレージノード 1 台当たりの I/O 負荷が高まることによって、目安よりも長くなることがあります。
ストレージノード数が 7 台以上の場合、ストレージノード 1 台当たりの I/O 負荷が減ることによって、目安よりも短くなることがあります。
- allocatableCapacityUsageRate[%]のストレージコントローラー間での状況
allocatableCapacityUsageRate[%](ストレージコントローラー上で管理できる最大の論理容量に対する使用率)がストレージコントローラー間で均一でない場合、目安よりも増減することがあります。
- ストレージプールの使用率が減少する操作の実施直後、または内部処理が動作した直後*
ストレージプールの使用率が減少する操作の実施直後、または内部処理が動作した直後は、ドライブ上の使用領域が残っているため、目安よりも長くなることがあります。
* 以下のような操作の実施または内部処理が動作した場合には、ストレージプールの使用率が減少します。
 - ボリューム削除

- スナップショット削除
- ストレージノード増設
- 容量バランス
- 容量削減機能によるガベージコレクション
- UNMAP コマンドによる I/O
- WRITE SAME コマンドによる I/O



メモ

- 複数のストレージノードについて、ストレージノードの保守回復または交換を実施する場合、リビルドの処理時間[min]は、ストレージノード 1 台当たりのリビルドの処理時間[min]×保守回復または交換対象のストレージノードの数だけ掛かります。
- ドライブ障害契機のリビルドが動作した場合、ドライブ間のデータ配置が変更される影響でリビルドの処理時間[min]が目安時間よりも増加することがあります。リビルド完了までの時間はイベントログ KARS07003-I で確認できます。



注意

ストレージコントローラーへ割り付けられる容量を超えた物理容量を搭載している場合、目安時間の計算値が多めに算出されることがあります。ストレージコントローラーへ割り付けられる最大容量は、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」に記載の以下を参照してください。

- 「ユーザーデータドライブ」の「1 ドライブ当たりの必要容量」の備考欄

リビルドが動作中の場合、リビルド完了までの残り時間[min]の目安はイベントログ KARS07003-I で確認できます。ただし、リビルド完了までの時間は、以下の条件によって増減することがあります。

- ネットワークスイッチの性能や I/O 負荷の状況
- 障害や保守操作などによってリビルドが中断したあと、再度実行された場合
- リビルド中にストレージクラスターが停止した場合
- 高速リビルドが通常リビルドに切り替わった場合

イベントログ一覧の取得方法は「イベントログの一覧を取得する」を参照してください。



メモ

- KARS07003-I で表示する進捗率と残り時間は、以下の情報を示しています。
 - 進捗率[%]：リビルド対象データ全体に対するリビルド処理の進捗率です。すべてのリビルド対象データの処理に成功すると 100[%]になります。リビルドに失敗したデータがある場合 100[%]になりません。
 - 残り時間[min]：リビルド処理が終了(完了または中断)するまでの目安時間です。リビルドに失敗したデータがある場合でも 0[min]になります。
- リビルド処理で失敗したデータがある場合、リビルド処理は一度終了します。その後、リビルドが再実行され、失敗したデータのリビルドを試みます。
- KARS07003-I のイベントログは進捗率が 10 ポイント以上増減した場合*、または進捗率が 100%になった場合に出力されます。
 - * 進捗率は内部処理やストレージシステムの状態によって後退することがあります。また、後退時に表示される残り時間は、実際の残り時間よりも長い時間が表示される可能性があります。
- KARS07003-I で表示されるリビルドの残り時間は、進捗率が低い期間では精度が悪くなる傾向があります。進捗率が進むにつれ、徐々に実態に合った時間に補正されます。

30.4 リビルドの状態を確認する

リビルドの状態と進捗率は、プロテクションドメインの情報を取得することで確認できます。

ロールによる実行制限はありません。

操作手順

1. プロテクションドメインの情報の一覧を取得して、`rebuildStatus` と `rebuildProgressRate[%]`を確認します。

REST API : GET /v1/objects/protection-domains

CLI : `protection_domain_list`

2. `rebuildStatus` にはリビルドの状態が、`rebuildProgressRate[%]`にはリビルドの処理の進捗率が表示されます。

- `rebuildStatus`

- **Stopped** : リビルドの処理を実行していない状態
- **Running** : リビルドの処理実行中の状態。リビルドの実行は止められません。リビルドの完了を待ってから、再度、手順 1 と手順 2 を実施して、リビルドの状態を確認してください。
- **Error** : リビルドの処理がエラーで実行できない状態。イベントログを確認し対処してください。

- `rebuildProgressRate[%]`

リビルドの進捗率[%]が表示されます。リビルドの進捗率は 1 ポイント以上の増減があれば更新されます。(高速リビルドなど短時間で進捗が進む場合は、1 ポイント単位ではなく数ポイント単位で更新される場合があります。)



メモ

以下の場合にはリビルドの進捗が 0 から再開します。

- 高速リビルドが、通常リビルドに切り替わった場合
- リビルドが中断して再開した場合
- リビルド中にストレージクラスター障害またはクラスターマスターノード(プライマリー)障害が発生した場合
進捗率は 0 から開始しますが、それまでに処理が完了したデータは再度処理せずに、完了していないデータのみ処理します。
- 進捗率は内部処理やストレージシステムの状態によって後退することがありますが、異常ではありません。
リビルド中に障害が発生した場合などに、処理途中の領域に対してロールバック処理が動作するため、ロールバックした分だけ進捗が後退します。

共通情報を取得する

- 31.1 API のバージョン・名称を取得する
- 31.2 ジョブの情報の取得
- 31.3 モデルを確認する

31.1 API のバージョン・名称を取得する

API について、以下の情報を取得します。

ロールによる実行制限はありません。

- apiVersion : API バージョン
- productName : API 名称

操作手順

1. API のバージョン情報などを取得します。

REST API : GET /configuration/version

CLI : version_show

31.2 ジョブの情報の取得

ジョブの情報が一覧または個別に取得できます。

31.2.1 取得できるジョブの情報

以下の情報が一覧または個別に取得できます。

- jobId : ジョブの ID(uuid)
- self : 当該ジョブ情報にアクセスするための URL
- userId : 当該ジョブの作成契機となる API を発行したユーザーの ID
- status : ジョブの進捗状況
- state : ジョブの状態
- createTime : ジョブが作成された時刻
- updateTime : ジョブの状態が更新された時刻
- completedTime : ジョブの実行が完了した時刻
- request : リクエスト情報
- affectedResources : ジョブの操作対象リソースにアクセスするための URL
- error : ジョブのエラー情報

31.2.2 ジョブの情報の一覧を取得する

各ジョブの情報を一覧で取得します。

ロールによる実行制限はありません。

操作手順

1. ジョブの情報の一覧を取得します。

REST API : GET /v1/objects/jobs

CLI : job_list



メモ

- ジョブの情報が見つからない場合は、ジョブ情報の一覧を取得する際にクエリーパラメーターによるフィルター機能で絞り込む、またはジョブ ID を指定して「ジョブの情報を個別に取得する」を実行してください。クエリーパラメーターについては「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」を参照してください。
- ストレージシステム内に保持できるジョブの情報は最大で 10 万件です。最大保持件数を超えたジョブの情報は古い順に削除されます。ただし、ストレージシステム内部で自動的に実行されるジョブも含まれるため、取得できるジョブの情報の総数はこの数よりも小さくなります。

31.2.3 ジョブの情報を個別に取得する

指定した ID のジョブの情報を取得します。

ロールによる実行制限はありません。

操作手順

1. ジョブの ID を取得します。
REST API : GET /v1/objects/jobs
CLI : job_list
2. ジョブの情報を取得します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId>
CLI : job_show



メモ

ストレージシステム内に保持できるジョブの情報は最大で 10 万件です。最大保持件数を超えたジョブの情報は古い順に削除されます。ただし、ストレージシステム内部で自動的に実行されるジョブも含まれるため、取得できるジョブの情報の総数はこの数よりも小さくなります。

31.3 モデルを確認する

利用しているストレージソフトウェアのモデルは、ストレージクラスターの情報から確認できます。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、Audit、または Resource

操作手順

1. ストレージクラスターの情報を取得します。
REST API : GET /v1/objects/storage
CLI : storage_show
2. modelName の値によってモデルを確認します。

modelName の値	モデル
VSSBB1	Bare metal モデル
VSSBA1	Cloud モデル for AWS
VSSBG1	Cloud モデル for Google Cloud

modelName の値	モデル
VSSBM1	Cloud モデル for Microsoft Azure

ストレージソフトウェアアップデートの要件と手順

- 32.1 ストレージソフトウェアアップデートの概要
- 32.2 参考事項・制限事項
- 32.3 ストレージソフトウェアをアップグレードする<<Bare metal>>
- 32.4 ストレージソフトウェアをアップグレードする<<Cloud for AWS>>
- 32.5 ストレージソフトウェアをアップグレードする<<Cloud for Google Cloud>>
- 32.6 ストレージソフトウェアをアップグレードする<<Cloud for Microsoft Azure>>
- 32.7 ストレージソフトウェアをダウングレードする<<Bare metal>>
- 32.8 ストレージソフトウェアをダウングレードする<<Cloud for AWS>>
- 32.9 ストレージソフトウェアをダウングレードする<<Cloud for Google Cloud>>
- 32.10 ストレージソフトウェアをダウングレードする<<Cloud for Microsoft Azure>>
- 32.11 ソフトウェアアップデートを中止する
- 32.12 転送済みのソフトウェアアップデートファイルの情報を取得する

32.1 ストレージソフトウェアアップデートの概要

この章で説明するアップデート方法について

この章では、ストレージソフトウェアのアップデート方法のうち、次のアップデート方法について説明します。

- このマニュアルが対象とするバージョンへのアップグレード方法
- このマニュアルが対象とするバージョンからのダウングレード方法
ただし、ダウングレード対象のバージョンがない場合は、ダウングレード手順の記載はありません。



注意

- ソフトウェアアップデート中は、各ストレージノードのソフトウェア更新処理の中で、断続的にユーザーデータの冗長度が低下します。
- ソフトウェアアップデート中には、ストレージクラスター内のストレージノードの数だけ以下が発生します。
 - ストレージノードのソフトウェア更新処理中、20～25 秒程度ホスト I/O が停止します。
 - ストレージコントローラーの冗長度を回復させる際に、ホスト I/O 性能が 3～4 分程度低下する可能性があります。



メモ

このマニュアルが対象とするストレージソフトウェアのバージョンから、新しいバージョンにアップグレードする方法は、アップグレード先のバージョンに対応したマニュアルを参照してください。
また、このマニュアルが対象とするストレージソフトウェアのバージョンへ、新しいバージョンからダウングレードする方法は、新しいバージョンに対応したマニュアルを参照してください。

アップグレードとダウングレード

ストレージソフトウェアのアップデートは、それぞれ以下の場合に行います。アップデートは、ホストからの I/O を継続したまま実施できます。

区分	使用事例	操作手順の参照先
ソフトウェアアップグレード	ストレージソフトウェアを新しいバージョンに更新します。 • 機能追加・機能拡張 • 性能向上・信頼性向上 • 新しい規格への対応 • バグ修正 • セキュリティ対応	• ≪Bare metal≫「ストレージソフトウェアをアップグレードする≪Bare metal≫」 • ≪Cloud for AWS≫「ストレージソフトウェアをアップグレードする≪Cloud for AWS≫」 • ≪Cloud for Google Cloud≫「ストレージソフトウェアをアップグレードする≪Cloud for Google Cloudl≫」 • ≪Cloud for Microsoft Azure≫「ストレージソフトウェアをアップグレードする≪Cloud for Microsoft Azure≫」
ソフトウェアダウングレード	ストレージソフトウェアを旧バージョンに更新します。 • アップデート後の動作が不安定なときに、対策バージョン受領までの期	• ≪Bare metal≫「ストレージソフトウェアをダウングレードする≪Bare metal≫」 • ≪Cloud for AWS≫「ストレージソフトウェアをダウングレードする≪Cloud for AWS≫」

区分	使用事例	操作手順の参照先
	間、旧バージョンで運用する場合	・ <<Cloud for Google Cloud>> 「ストレージソフトウェアをダウングレードする<<Cloud for Google Cloud>>」 ・ <<Cloud for Microsoft Azure>> 「ストレージソフトウェアをダウングレードする<<Cloud for Microsoft Azure>>」



ヒント

ストレージソフトウェアのバージョンは、ストレージクラスターの情報を取得することで確認できます。

ソフトウェアの互換性について

このマニュアルが対象とするバージョンとアップデート対象のバージョンとの互換性は、次表のとおりです(○：アップデート可)。



メモ アップデート元バージョンとアップデート先バージョンがアップデート可ではない場合でも、アップデート可のバージョンへ段階的にアップデートすることで、目的のアップデート先バージョンにアップデートすることがあります。例えば、Bare metal モデルの 01.12.0x.40 から 01.15.0x.40 にアップグレードする場合、01.12.0x.40 から 01.14.0x.40 へアップグレードしてから、01.14.0x.40 から 01.15.0x.40 にアップグレードします。

<<Bare metal>>

アップデート元バージョン	アップデート先バージョン							
	01.11.0x.40	01.12.0x.40	01.13.0x.40	01.14.0x.40	01.15.0x.40	01.16.0x.40	01.17.0x.40	01.18.0x.40
01.11.0x.40	○	○	○	○	×	×	×	×
01.12.0x.40	○	○	○	○	×	×	×	×
01.13.0x.40	○	○	○	○	○	○	×	×
01.14.0x.40	○	○	○	○	○	○	×	×
01.15.0x.40	×	×	○	○	○	○	○	×
01.16.0x.40	×	×	○	○	○	○	○	×
01.17.0x.40	×	×	×	×	○	○	○	○
01.18.0x.40	×	×	×	×	×	×	○	○

<<Cloud for AWS>>

アップデート元バージョン	アップデート先バージョン			
	01.15.0x.30	01.16.0x.30	01.17.0x.30	01.18.0x.30
01.15.0x.30	○	○	○	×
01.16.0x.30	○	○	○	×
01.17.0x.30	○*	○*	○	○
01.18.0x.30	×	×	○	○

* ストレージノードとして使用している EC2 インスタンスのインスタンスタイプが、m6i.8xlarge または r6i.8xlarge の場合のみ実施できます。それ以外のインスタンスタイプの場合は実施しないでください。

≪Cloud for Google Cloud≫

アップデート元バージョン	アップデート先バージョン
	01.18.0x.60
01.18.0x.60	○

≪Cloud for Microsoft Azure≫

アップデート元バージョン	アップデート先バージョン
	01.18.0x.50
01.18.0x.50	○

ソフトウェアアップデートの処理時間

処理時間は、以下の計算式から算出できます。

ストレージノード 1 台当たりの処理時間[min] = プロテクションドメインに設定された最小メモリー容量に応じた処理時間(1) + リビルド処理時間(2)

≪Bare metal≫

- ・ (1) 35[min]
物理ノードの起動に時間が掛かるストレージノードが含まれている場合、処理時間が長くなる可能性があります。
- ・ (2) リビルド処理時間については「リビルド完了までの時間(目安)」を参照してください。

≪Cloud≫

- ・ (1) 最小メモリー容量が 128GiB の場合 : 30[min]、256GiB の場合 : 35[min]
- ・ (2) リビルド処理時間については「リビルド完了までの時間(目安)」を参照してください。

処理時間について、以下の外部要因によって処理時間が増加・減少することがあります。処理時間が増加する場合は、これらの項目に問題がないことを確認してください。

- ・ ネットワークの通信状況(ストレージノード間の通信状況)
- ・ ≪Bare metal≫サーバーの性能状況(ストレージノードの温度上昇による性能低下など)
- ・ ≪Bare metal≫サーバーのハードウェア構成(ストレージノードのプロセッサ、メモリー容量など)
- ・ ≪Cloud≫VM インスタンスの性能状況

32.2 参考事項・制限事項

ソフトウェアアップデートは、以下の記載事項を理解した上で実施してください。

- ・ ソフトウェアアップデートの対象
- ・ ソフトウェアアップデートが制限されるケース
- ・ ソフトウェアアップデート中に制限される操作
- ・ ソフトウェアアップデート中の動作
- ・ ソフトウェアアップデート後に必要な操作

32.2.1 ソフトウェアアップデートの対象

ソフトウェアアップデートの対象は、ストレージノード内のソフトウェアです。

- <<Bare metal>>
コンピュータノード、コントローラーノード、サーバーベンダーのファームウェアは対象外です。
サーバーベンダーのファームウェアの更新は、別途ベンダーからの提示に従って実施してください。
- <<Cloud>>
コンピュータノード、コントローラーノードのファームウェアは対象外です。

32.2.2 ソフトウェアアップデートが制限されるケース

ストレージノードが閉塞中の場合やデータの冗長度が低下している場合

ストレージノードが閉塞中の場合やデータの冗長度が低下している場合、ソフトウェアアップデートは実行できません。閉塞中のストレージノードまたはデータの冗長度を回復させてからソフトウェアアップデートを実施してください。

- 閉塞中のストレージノードがある場合は「ストレージノード保守の原因と対処」を参照し、ストレージノードの回復を実施してください。
- データの冗長度が低下している場合は、リビルド完了後にソフトウェアアップデートを実施してください。リビルドの状態は「リビルド(データ再構築)の状態を確認する」を参照してください。



注意

- ソフトウェアアップデートはリビルド中でも実施できますが、ソフトウェアアップデートによってユーザーデータへのアクセスができなくなる場合は、ソフトウェアアップデートが失敗します。リビルドによるソフトウェアアップデートの失敗を確実に回避するには、リビルドが動作していないときにソフトウェアアップデートを実施してください。リビルドが動作中かどうかを確認するには「リビルドの状態を確認する」を参照してください。
- ストレージプールの容量バランス処理中に、ソフトウェアアップデートを実行すると、ソフトウェアアップデートが優先され、ストレージプールの容量バランス処理は、イベントログ KARS06336-I を出力し中断します。ソフトウェアアップデートを実行してからストレージプールの容量バランス処理が中断されるまでには、30 分程度掛かる場合があります。中断されるまでの間に、容量バランス処理が進行していることを示すイベントログ KARS06300-I、KARS06301-I が出力されることがあります。ソフトウェアアップデートが完了したあと、改めて容量バランスの動作条件を満たしているかが判断されて、動作条件を満たしている場合は容量バランスの処理が再実行されます。
- ダウングレード前のバージョンにおいて、ダウングレード先のバージョンでは非サポートの機能を使用しているかどうかを確認し、使用している場合は、それらの機能を無効にしてからダウングレードを実施してください。機能の無効化を実施せずにダウングレードを実施した場合は、ダウングレードが中断されます。無効化すべき機能と機能を無効化する方法は、ご使用のモデルによって以下を参照してください。
 - <<Bare metal>> 「ストレージソフトウェアをダウングレードする<<Bare metal>>」の注意事項
 - <<Cloud for AWS>> 「ストレージソフトウェアをダウングレードする<<Cloud for AWS>>」の注意事項
 - <<Cloud for Google Cloud>> 「ストレージソフトウェアをダウングレードする<<Cloud for Google Cloud>>」の注意事項
 - <<Cloud for Microsoft Azure>> 「ストレージソフトウェアをダウングレードする<<Cloud for Microsoft Azure>>」の注意事項

32.2.3 ソフトウェアアップデート中に制限される操作

ソフトウェアアップデート中は以下の操作が制限されます。

- ソフトウェアアップデート(二重実行)
- ストレージクラスターの停止
- ストレージクラスターに関する設定の変更
- 構成の変更を伴う管理操作や他の保守操作(例えば、ストレージノードの増設、ストレージノードの減設、ストレージノードの保守閉塞)



メモ

上記に加えて、ソフトウェアアップデート中に REST API/CLI を発行すると、REST API/CLI が KARS15506-E で失敗する可能性があります。

REST API/CLI が KARS15506-E で失敗した場合は、しばらく待ってから(最大約 60 分)、再度 REST API/CLI を実行してください。

32.2.4 ソフトウェアアップデート中の動作

ソフトウェアアップデート中の動作と、ソフトウェアアップデートを中断した場合の留意事項は以下のとおりです。

ソフトウェアアップデート中のバージョンの混在について

ソフトウェアアップデート中に発生するストレージノード間でのストレージソフトウェアのバージョン混在は許容されます。

ソフトウェアアップデートを中断した場合の留意事項

「ソフトウェアアップデートを中止する」の手順に従ってソフトウェアアップデートを中断した状態、またはソフトウェアアップデートが何らかの障害によって中断した状態から、再度ソフトウェアアップデートを実行する場合は以下の手順から実施してください。

- <<Bare metal>>
「ストレージソフトウェアをアップグレードする<<Bare metal>>」の手順 4、または「ストレージソフトウェアをダウングレードする<<Bare metal>>」の手順 5 から実施してください。
- <<Cloud for AWS>>
「ストレージソフトウェアをアップグレードする<<Cloud for AWS>>」の手順 3、または「ストレージソフトウェアをダウングレードする<<Cloud for AWS>>」の手順 3 から実施してください。
- <<Cloud for Google Cloud>>
「ストレージソフトウェアをアップグレードする<<Cloud for Google Cloud>>」の手順 3、または「ストレージソフトウェアをダウングレードする<<Cloud for Google Cloud>>」の手順 3 から実施してください。
- <<Cloud for Microsoft Azure>>
「ストレージソフトウェアをアップグレードする<<Cloud for Microsoft Azure>>」の手順 3、または「ストレージソフトウェアをダウングレードする<<Cloud for Microsoft Azure>>」の手順 3 から実施してください。

ソフトウェアアップデートを中止してリトライする場合、アップデート済みのストレージノードの処理はスキップされます。



注意

ストレージソフトウェアのバージョン混在の禁止について

ストレージノード間でのストレージソフトウェアのバージョン混在は禁止です。作業を途中で中止したような場合は、再度アップデートを行い、すべてのストレージノードのバージョンが一致するよう、ソフトウェアアップデートを行ってください。

バージョンが混在したまま利用すると、以下のような状態になることがあります。

- ストレージクラスターが起動しない
- 管理操作ができない
- I/O ができない
- データが消失する(例えば、バージョンの異なるノード間でデータを二重書きできるが、バージョンの異なるストレージノード間でリビルドできないケース)

また、ソフトウェアアップデートの作業中に、一時的に 01.17.0x.xx と 01.18.0x.xx のバージョンが混在する場合、Web サーバーの更新のため、以下の状態になることがあります。

- REST API および CLI 実行時に KARS15000-E、KARS19504-E が発生する
- ストレージクラスターのバージョンと REST API のバージョンが一致しない
- ストレージクラスターのバージョンと一致するバージョンの CLI を使用しているにもかかわらず、CLI 実行時にバージョン不一致の警告が発生する

ソフトウェアアップデートの処理順序

ソフトウェアアップデートはストレージノードの役割を基準に処理順序が決まります(役割内は順不同です)。処理順序は以下のとおりです。

1. クラスターマスターノード(セカンダリー)
2. クラスターマスターノード(プライマリー)
3. クラスターワーカーノード



メモ

《Bare metal》サーバー本体の保守(ファームウェア更新)を行う際に、この順番で行う必要はありません。

32.2.5 ソフトウェアアップデート後に必要な操作

ソフトウェアアップデート後には、以下の操作が必要になります。

《Bare metal》

- ストレージソフトウェアを 01.13.0x.40 より前のバージョンから 01.13.0x.40 以降のバージョンにアップグレードした場合は、キャッシュ保護付きライトバックモードは無効になっています。キャッシュ保護付きライトバックモードが無効の場合、ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した際に、スナップショットボリュームのデータが消失するリスクがあります。このマニュアルの「キャッシュ保護付きライトバックモードを有効にする《Bare metal》」を参照してキャッシュ保護付きライトバックモードを有効にしてください。
- Universal Replicator を使用している場合は、アップグレード前にペア分割したペアをすべて再同期してください。
- ストレージソフトウェアのバージョン 01.17.0x.40 からは、外部認証サーバー設定の timeoutSeconds(CLI : --timeout_seconds)と maxRetries(CLI : --max_retries)がデフォルト値に設定されます。設定値は変更しないでください。

《Cloud for AWS》

- ソフトウェアアップデートの完了後には、VSP One SDS Block で使用する AWS スタックの CloudFormation テンプレートファイルのアップデートが必要です。詳しい手順は「ストレージソフトウェアをアップグレードする<<Cloud for AWS>>」の手順 14 または「ストレージソフトウェアをダウングレードする<<Cloud for AWS>>」の手順 12 を参照してください。
- Universal Replicator を使用している場合は、アップグレード前にペア分割したペアをすべて再同期してください。
- ストレージソフトウェアのバージョン 01.17.0x.30 からは、外部認証サーバー設定の timeoutSeconds(CLI : --timeout_seconds)と maxRetries(CLI : --max_retries)がデフォルト値に設定されます。設定値は変更しないでください。

<<Cloud for Google Cloud>>

- ソフトウェアアップデートの完了後には、VSP One SDS Block で使用するクラウドリソースのアップデートが必要です。詳しい手順は「ストレージソフトウェアをアップグレードする<<Cloud for Google Cloud>>」の手順 12 または「ストレージソフトウェアをダウングレードする<<Cloud for Google Cloud>>」の手順 11 を参照してください。
- Universal Replicator を使用している場合は、アップグレード前にペア分割したペアをすべて再同期してください。

<<Cloud for Microsoft Azure>>

- ソフトウェアアップデートの完了後には、VSP One SDS Block で使用するストレージクラスターを構成するデプロイのアップデートが必要です。詳しい手順は「ストレージソフトウェアをアップグレードする<<Cloud for Microsoft Azure>>」の手順 12 または「ストレージソフトウェアをダウングレードする<<Cloud for Microsoft Azure>>」の手順 11 を参照してください。
- Universal Replicator を使用している場合は、アップグレード前にペア分割したペアをすべて再同期してください。

32.3 ストレージソフトウェアをアップグレードする<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ストレージソフトウェアを新しいバージョンに更新します。

ソフトウェアアップデート中に発生するストレージノード間でのストレージソフトウェアのバージョン混在は許容されます。バージョン混在中は、アップグレード前のバージョンでの動作が保障されます。

ストレージソフトウェアのバージョンが切り替わるのは、手順 9 を実行中に、各ストレージノードのアップグレードがすべて完了したときです。

このため、手順 1 から 10 までの REST API または CLI は、アップグレード前のストレージソフトウェアのバージョンに対応する「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」または「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」に従ってください。

なお、アップグレードを途中で中止したり、エラーによってアップグレードが中断されたりした場合に、アップグレード以外の操作を実施する場合は、アップグレード前のバージョンに対応したマニュアルを参照して操作してください。



注意

バージョン 01.15.0x.40 未満から 01.15.0x.40 以降へのアップグレード中に、01.15.0x.40 以降にアップグレード済みだったストレージノードにストレージノード交換が必要な障害が発生すると、アップグレードは失敗します。この結果、ストレージクラスターのバージョンは 01.15.0x.40 未満のままですが、障害が発生したストレージノードは 01.15.0x.40 以降にアップグレードされています。ストレージクラスターのバージョンが 01.15.0x.40 未満であることから管理ポート非冗長化と PCI スロット柔軟化は非サポートになります。このため、交換用のストレージノードは 01.15.0x.40 未満(ストレージクラスターのバージョン)でサポートされている構成かつ管理ポートのチーミングを有効な状態にしてください。サーバー構成については「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。

前提条件

- 実行に必要なロール : Service
- Universal Replicator のペアはすべて分割されていること

作業フロー



操作手順の留意事項

手順 1 から 11 までは、コントローラーノードで実行する操作です。

操作手順

1. 日立アドバンスドサーバ HA8000V シリーズを使用している場合、アップデート後のストレージソフトウェアのバージョンに対応したバージョンの SPH(Service Pack for HA8000V)への更新が必要になることがあります。

「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照し、ストレージソフトウェアのバージョンと SPH のバージョンの組み合わせを確認の上、必要な場合は SPH を更新してください。



メモ 手順 1 は最後の手順としても実施できます。

2. ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

アップグレードが必要な場合は、次の手順に進みます。

3. サポートセンターから以下のファイルを入手して、コントローラーノードに格納します。

(入手するファイル)

次のファイルは、アップグレード先のバージョンに合ったものを入手してください。

- hsd-update-**<version>**-**<number>**.tar

ストレージソフトウェアのアップデートファイルです。手順 2 で取得したストレージノードのバージョン aa.bb.cc.dd の dd 部分の数字と、ストレージソフトウェアのアップデートファイルの<version>の下 2 桁の数字が一致することを確認してください。一致しないストレージソフトウェアのアップデートファイルは使用しないでください。

(例)hsd-update-01000000-7070.tar

- EULA_for_SLE_for_StorageNode.txt

ストレージノードで使用している SUSE Linux Enterprise に関する EULA 文書です。

- EULA_for_SPDK.txt

ストレージノードで使用している Cavium SPDK FC Target Driver に関する EULA 文書です。

次のファイルは、最新のものを入手してください。

- SystemRequirementsFile.yml

システム要件ファイルです。

4. 格納した 2 つの EULA 文書の記載内容を確認します。

同意いただける場合は、次の手順に進みます。同意できない場合は、ソフトウェアアップデートを中止してください。

5. ジョブの情報を取得して、実行中のソフトウェアアップデートのジョブがないことを確認します。

REST API : GET /v1/objects/jobs

CLI : job_list

実行中のソフトウェアアップデートのジョブがない場合は、次の手順に進みます。



注意

ソフトウェアアップデートのジョブが実行中だったとき、以降の操作を行うと、実行中だったソフトウェアアップデートのジョブは失敗しますので注意してください。

6. ストレージソフトウェアのアップデートファイルをストレージクラスターにアップロードします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

ストレージクラスターに転送するストレージソフトウェアのアップデートファイルを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/upload-software-update-file/invoke

CLI : storage_upload_software_update_file

実行結果は、コンソール上に出力されます。REST API では、HTTP ステータスコードとして 204 が、CLI ではメッセージとして"Completed."が、それぞれ返ったらアップロードは成功です。その際、イベントログは出力されません。



メモ

アップデートファイルのアップロード完了以降、ソフトウェアアップグレードの実行前までは、転送済みのソフトウェアアップデートファイルの情報を取得できます。操作方法は「転送済みのソフトウェアアップデートファイルの情報を取得する」を参照してください。

7. 手順 3 で格納したシステム要件ファイルを指定して以下のコマンドを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : POST /v1/objects/system-requirements-file/actions/import/invoke

CLI : system_requirements_file_import

指定したシステム要件ファイルのバージョンが、VSP One SDS Block にインポート済みのバージョンより新しい場合のみインポート処理が行われます。指定したシステム要件ファイルのバージョンが同じか古い場合は、イベントログを出力しインポート処理をスキップします。

コマンド実行後に表示されるジョブの ID を確認します。

8. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

9. ソフトウェアアップデートを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

mode パラメーターを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/update-software/invoke

CLI : storage_update_software

コマンド実行後に表示されるジョブの ID を確認します。

10. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



注意

- ソフトウェアアップデートが KARS10109-E で失敗した場合は、他の競合するジョブが動作しているためソフトウェアアップデートを実行できなかったことを意味しています。競合したジョブを中断するか、ジョブが完了するのをしばらく待ってから再実施してください。なお、当該メッセージで表示される競合ジョブの ID に、ストレージクラスターが内部で実行し

ているジョブの ID が表示されることがあります。ストレージクラスターが内部で実行しているジョブの state は参照できません。

- ソフトウェアアップデートが KARS10110-E で失敗した場合は、ストレージソフトウェアのアップデートファイルがストレージクラスターに存在していなかったことを意味します。手順 6 でストレージソフトウェアのアップデートファイルのアップロードに成功している場合でも、以下のケースなどで KARS10110-E が出力される場合があります。その場合は手順 6 から再度実施してください。
 - ソフトウェアアップデート実施中にクラスターマスターノード(プライマリー)が障害を原因に閉塞した場合
 - ソフトウェアアップデート実施中にストレージクラスターの停止または電断があった場合
 - ソフトウェアアップデートのオプション指定に誤りがあったため、KARS10115-E が出力された場合
- VSP One SDS Block Administrator を利用している場合は、手順 10 を実施後に、数秒待ってから以下を実施してください。
 1. Web ブラウザーまたはタブをいったん閉じます。
 2. Web ブラウザーのキャッシュをクリアします。
 3. VSP One SDS Block Administrator を開き直して使用します。

11. ストレージクラスターの情報を取得して、ストレージソフトウェアが更新されたことを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

12. CLI を使用している場合は、ストレージソフトウェアのアップグレードに合わせてコントローラーノードに CLI プログラムの最新版をインストールします。

CLI プログラムのインストール手順は、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。



メモ

ストレージソフトウェアより CLI プログラムのバージョンが古い状態で CLI を実行した場合、一致するバージョンまたは新しいバージョンへの更新を促す警告文が標準エラー出力に出力されます。

13. Universal Replicator を使用している場合は、必要に応じて管理サーバーに最新版の RAID Manager をインストールします。



メモ

RAID Manager のバージョンが古い場合、正しい情報を参照または取得できないことがあります。

14. SNMP を利用している場合は、ストレージソフトウェアのアップグレードにあわせてアップグレード先のバージョンに合った拡張 MIB を SNMP マネージャーに取り込みます。

拡張 MIB の取り込み手順は「拡張 MIB の取り込み」を参照してください。

15. スペアノードを使用している場合は、ストレージソフトウェアのアップグレードに合わせてスペアノードのソフトウェアのアップグレードを行います。

ただし、ストレージソフトウェアとスペアノードのソフトウェアのバージョンが一致している場合は、スペアノードのソフトウェアのアップグレードは不要です。

ストレージソフトウェアのアップグレード後にスペアノードを使用しない場合は、以下の手順 a のみを実施し、手順 b~d は実施しないでください。

- a. ストレージクラスターからスペアノードの情報を削除します。

- 「スペアノードの情報を削除する<<Bare metal>>」に記載してある作業を実施します。
- b. スペアノードにストレージソフトウェアをインストールします。
- Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージソフトウェアをインストールする」に記載してある作業を実施します。
- c. スペアノードに対して、ストレージノード単位のセットアップを行います。
- Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノード単位のセットアップを行う」に記載してある作業を実施します。
- d. スペアノードの情報を登録します。
- 「スペアノードの情報を登録する<<Bare metal>>」に記載してある作業を実施します。
16. ストレージソフトウェアを 01.13.0x.xx より前のバージョンから 01.13.0x.xx 以降のバージョンにアップグレードした場合は、このマニュアルの「キャッシュ保護付きライトバックモードを有効にする<<Bare metal>>」を参照してキャッシュ保護付きライトバックモードを有効にしてください。
- ストレージソフトウェアを 01.13.0x.xx より前のバージョンから 01.13.0x.xx 以降のバージョンにアップグレードした場合は、キャッシュ保護付きライトバックモードは無効になっています。キャッシュ保護付きライトバックモードが無効の場合、ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した際に、スナップショットボリュームのデータが消失するリスクがあります。
17. 構成情報のバックアップを行います。
- 「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
- ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

32.4 ストレージソフトウェアをアップグレードする<<Cloud for AWS>>

この節での記述内容は Cloud モデル for AWS に適用されます。

ストレージソフトウェアを新しいバージョンに更新します。

ソフトウェアアップデート中に発生するストレージノード間でのストレージソフトウェアのバージョン混在は許容されます。バージョン混在中は、アップグレード前のバージョンでの動作が保障されます。

ストレージソフトウェアのバージョンが切り替わるのは、手順 6 を実行中に、各ストレージノードのアップグレードがすべて完了したときです。

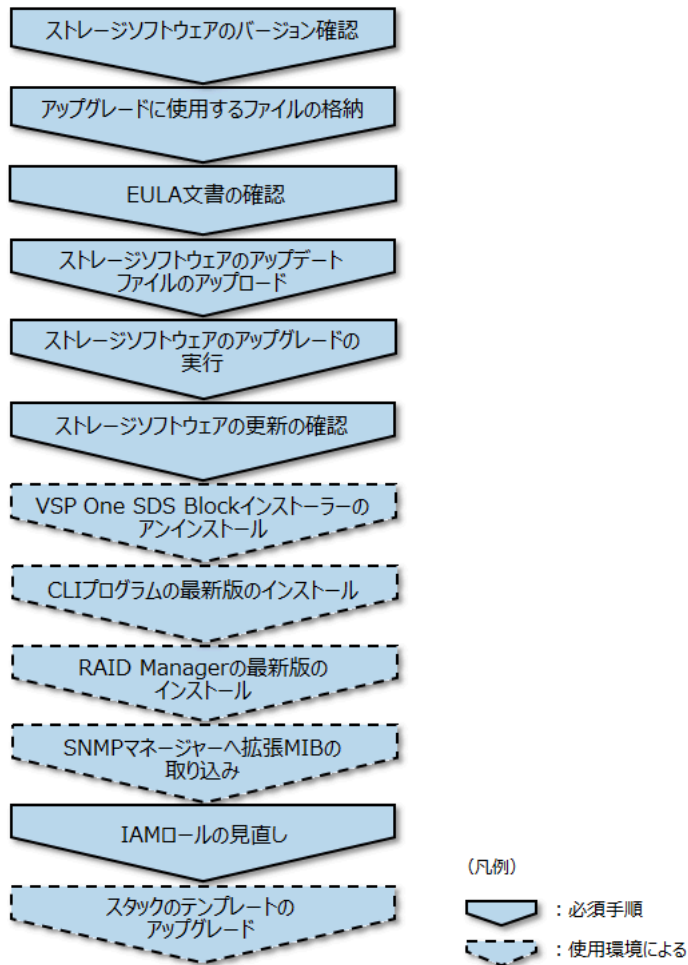
このため、手順 1 から 7 までの REST API または CLI は、アップグレード前のストレージソフトウェアのバージョンに対応する「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」または「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」に従ってください。

なお、アップグレードを途中で中止したり、エラーによってアップグレードが中断されたりした場合に、アップグレード以外の操作を実施する場合は、アップグレード前のバージョンに対応したマニュアルを参照して操作してください。ただし、ストレージソフトウェアのバージョンが 01.17.0x.30 のストレージノードとストレージソフトウェアのバージョンが 01.18.0x.30 以降のストレージノードが混在している構成で、01.18.0x.30 以降のストレージノードを交換する場合は、このマニュアルの「ストレージソフトウェアのバージョンが混在している場合のストレージノード交換<<Cloud for AWS>>」を参照してください。

前提条件

- ・ 実行に必要なロール : Service
- ・ Universal Replicator のペアはすべて分割されていること

作業フロー



操作手順の留意事項

- ・ 手順 1 から 10 までは、コントローラーノードで実行する操作です。
- ・ 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

操作手順

1. ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。
REST API : GET /v1/objects/storage
CLI : storage_show
アップグレードが必要な場合は、次の手順に進みます。
2. ダウンロードサーバーから以下のファイルを入手して、コントローラーノードに格納します。
(入手するファイル)
次のファイルは、アップグレード先のバージョンに合ったものを入手してください。
 - ・ hsd-update-<version>-<number>.tar

ストレージソフトウェアのアップデートファイルです。手順 1 で取得したストレージノードのバージョン aa.bb.cc.dd の dd 部分の数字と、ストレージソフトウェアのアップデートファイルの<version>の下 2 桁の数字が一致することを確認してください。一致しないストレージソフトウェアのアップデートファイルは使用しないでください。

(例)hsds-update-01000000-7070.tar

- EULA_for_SLE_for_StorageNode.txt

ストレージノードで使用している SUSE Linux Enterprise に関する EULA 文書です。

- EULA_for_SPDK.txt

ストレージノードで使用している Cavium SPDK FC Target Driver に関する EULA 文書です。

3. 格納した 2 つの EULA 文書の記載内容を確認します。

同意いただける場合は、次の手順に進みます。同意できない場合は、ソフトウェアアップデートを中止してください。

4. ジョブの情報を取得して、実行中のソフトウェアアップデートのジョブがないことを確認します。

REST API : GET /v1/objects/jobs

CLI : job_list

実行中のソフトウェアアップデートのジョブがない場合は、次の手順に進みます。



注意

ソフトウェアアップデートのジョブが実行中だったとき、以降の操作を行うと、実行中だったソフトウェアアップデートのジョブは失敗しますので注意してください。

5. ストレージソフトウェアのアップデートファイルをストレージクラスターにアップロードします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

ストレージクラスターに転送するストレージソフトウェアのアップデートファイルを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/upload-software-update-file/invoke

CLI : storage_upload_software_update_file

実行結果は、コンソール上に出力されます。REST API では、HTTP ステータスコードとして 204 が、CLI ではメッセージとして"Completed."が、それぞれ返ったらアップロードは成功です。その際、イベントログは出力されません。



メモ

アップデートファイルのアップロード完了以降、ソフトウェアアップグレードの実行前までは、転送済みのソフトウェアアップデートファイルの情報を取得できます。操作方法は「転送済みのソフトウェアアップデートファイルの情報を取得する」を参照してください。

6. ソフトウェアアップデートを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

mode パラメーターを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/update-software/invoke

CLI : storage_update_software

コマンド実行後に表示されるジョブの ID を確認します。

7. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



注意

- ・ ソフトウェアアップデートが KARS10109-E で失敗した場合は、他の競合するジョブが動作しているためソフトウェアアップデートを実行できなかったことを意味しています。競合したジョブを中断するか、ジョブが完了するのをしばらく待ってから再実施してください。なお、当該メッセージで表示される競合ジョブの ID に、ストレージクラスターが内部で実行しているジョブの ID が表示されることがあります。ストレージクラスターが内部で実行しているジョブの state は参照できません。
- ・ ソフトウェアアップデートが KARS10110-E で失敗した場合は、ストレージソフトウェアのアップデートファイルがストレージクラスターに存在していなかったことを意味します。手順 5 でストレージソフトウェアのアップデートファイルのアップロードに成功している場合でも、以下のケースなどで KARS10110-E が出力される場合があります。その場合は手順 5 から再度実施してください。
 - ・ ソフトウェアアップデート実施中にクラスターマスターノード(プライマリー)が障害を原因に閉塞した場合
 - ・ ソフトウェアアップデート実施中にストレージクラスターの停止または電断があった場合
 - ・ ソフトウェアアップデートのオプション指定に誤りがあったため、KARS10115-E が出力された場合
- ・ VSP One SDS Block Administrator を利用している場合は、手順 7 を実施後に、数秒待ってから以下を実施してください。
 1. Web ブラウザーまたはタブをいったん閉じます。
 2. Web ブラウザーのキャッシュをクリアします。
 3. VSP One SDS Block Administrator を開き直して使用します。

8. ストレージクラスターの情報を取得して、ストレージソフトウェアが更新されたことを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

9. ストレージソフトウェアを 01.17.0x.30 から 01.18.0x.30 以降にアップグレードした場合は、インストーラーのアンインストールを行います。

アンインストールは、Linux の場合は root ユーザー、Windows の場合は管理者権限があるユーザーで実施してください。

コントローラーノード用の EC2 インスタンスにログインし、以下のコマンドでアンインストールを実施してください。

<Windows の場合>

```
> py -m pip uninstall hsds_installer
```

<Linux の場合>

```
# python3 -m pip uninstall hsds_installer
```

10. CLI を使用している場合は、ストレージソフトウェアのアップグレードに合わせてコントローラーノードに CLI プログラムの最新版をインストールします。

CLI プログラムのインストール手順は、Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。



メモ

ストレージソフトウェアより CLI プログラムのバージョンが古い状態で CLI を実行した場合、一致するバージョンまたは新しいバージョンへの更新を促す警告文が標準エラー出力に出力されます。

11. Universal Replicator を使用している場合は、必要に応じて管理サーバーに最新版の RAID Manager をインストールします。



メモ

RAID Manager のバージョンが古い場合、正しい情報を参照または取得できないことがあります。

12. SNMP を利用している場合は、ストレージソフトウェアのアップグレードに合わせてアップグレード先のバージョンに合った拡張 MIB を SNMP マネージャーに取り込みます。
拡張 MIB の取り込み手順は「拡張 MIB の取り込み」を参照してください。
13. Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「コントローラーノードを EC2 コンソールから構築する」を参照し、コントローラーノードに付与している IAM ロールの権限に過不足があれば修正します。
14. Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「セットアップの前提条件を確認する」を参照し、ストレージノードに付与している IAM ロールの権限に過不足があれば修正します。
15. ストレージソフトウェアのアップグレードに合わせてスタックのテンプレートのアップグレードを行います。

ただし、アップグレード先のストレージソフトウェアのバージョンと、スタックのテンプレートのバージョンが一致している場合は、スタックのテンプレートのアップグレードは不要です。



メモ

スタックのテンプレートのバージョンは以下のコマンドで確認できます。

```
aws cloudformation describe-stacks ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--query ¥
'Stacks[0].Outputs[?OutputKey==`TemplateVersion`].OutputValue' ¥
--output text
```

- a. ストレージソフトウェアを 01.17.0x.30 から 01.18.0x.30 以降にアップグレードした場合は、手順 14 で見直したストレージノードに付与している IAM ロールと同じ IAM ポリシーを、以下の名称の IAM ロールにも付与します。

```
<ClusterName>-MasterNode-IAMRole
```

- b. 「構成ファイルをエクスポートする《Cloud for AWS》」を参照し、VSP One SDS Block からアップグレード後のバージョンに対応した構成ファイルを取得します。

構成ファイルをエクスポートする際は、exportFileType パラメーターを省略するか、Normal を指定してください。

最新状態の構成ファイルを使用するために、必ず取得してください。

- c. 手順 a で IAM ロールに IAM ポリシーを付与した場合は、IAM ポリシーの設定を IAM ロールから削除します。

```
<ClusterName>-MasterNode-IAMRole
```

- d. 構成ファイルのエクスポートで取得した構成ファイル一式を手順 b で templateS3Url パラメーターで指定した Amazon S3 バケットに格納します。

Amazon S3 にファイルを格納する方法として、例えば AWS CLI を用いて Amazon S3 にファイルをコピーする方法があります。詳細は Cloud モデル for AWS の「Hitachi Virtual

Storage Platform One SDS Block セットアップガイド」にある「Amazon S3 の操作例」を参照してください。



注意

VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。

- e. 次の AWS CLI を実行して、変更セットを作成します。

```
aws cloudformation create-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <任意の変更セット名*> ¥
--template-url ¥
<Amazon S3 に格納した VMConfigurationFile.yml の URL (https)> ¥
--include-nested-stacks ¥
--capabilities CAPABILITY_NAMED_IAM
```

* 使用可能文字などは以下の Web サイトを参照してください。

<https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-change-set.html>

- f. 次の AWS CLI を実行して、変更セットを表示します(1 階層目)。

```
aws cloudformation describe-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 e で指定した変更セット名>
```

以下の事項を確認します。

- "Status"が"CREATE_COMPLETE"であること
"Status"が"CREATE_IN_PROGRESS"の場合はしばらく待ってから再度実行してください。
- "Changes"の項目数が 1 つであること
- "Changes"内の"ResourceChange"について
"Action"が"Modify"であること
次の手順のため、"ChangeSetId"の値を記録します。

- g. 次の AWS CLI を実行して、変更セットを表示します(2 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 f で記録した "ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
"Action"が"Modify"であること
次の手順のため、各項目の"ChangeSetId"の値を記録します。

- h. 次の AWS CLI を実行して、変更セットを表示します(3 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 g で記録した "ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
"Action"が"Modify"であること



メモ

ストレージソフトウェアを 01.15.00.30 より前のバージョンから 01.15.00.30 以降のバージョンにアップグレードした場合は、"LogicalResourceId"が"MasterNodeIAMPolicy"の項目について、"Action"が"Remove"になります。

- i. 次の AWS CLI を実行して、作成した変更セットを実行します。

```
aws cloudformation execute-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 e で指定した変更セット名>
```

- j. 次の AWS CLI を実行して、変更セットの実行結果を確認します。

wait stack-update-complete を実行すると、変更セットの実行が完了するまで待つことができます。

```
aws cloudformation wait stack-update-complete ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

実行が完了したら、**describe-stacks** を実行し、StackStatus が"UPDATE_COMPLETE"であることを確認してください。

```
aws cloudformation describe-stacks ¥
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

16. 構成情報のバックアップを行います。

「構成情報をバックアップする《Bare metal》《Cloud for AWS》」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

32.5 ストレージソフトウェアをアップグレードする《Cloud for Google Cloud》

この節での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージソフトウェアを新しいバージョンに更新します。

ソフトウェアアップデート中に発生するストレージノード間でのストレージソフトウェアのバージョン混在は許容されます。バージョン混在中は、アップグレード前のバージョンでの動作が保障されます。

ストレージソフトウェアのバージョンが切り替わるのは、手順 6 を実行中に、各ストレージノードのアップグレードがすべて完了したときです。

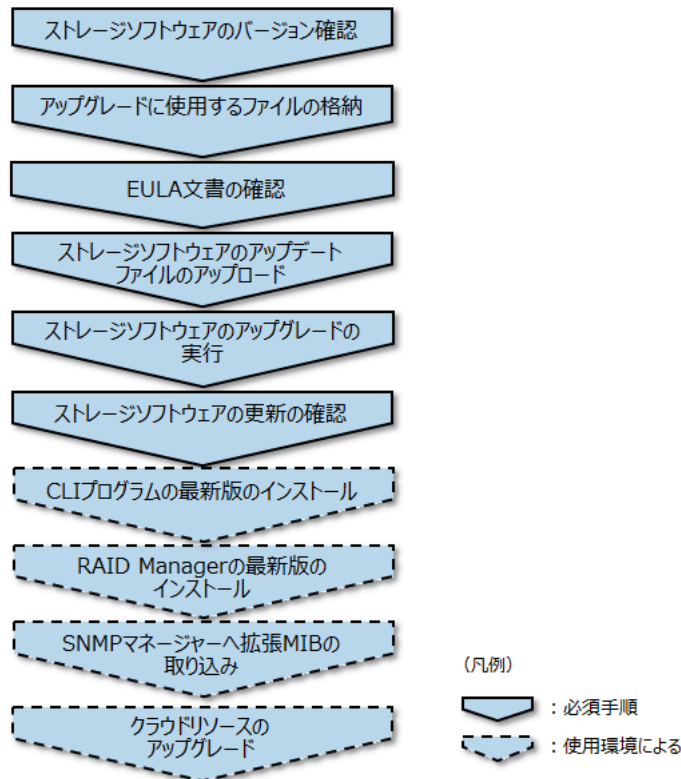
このため、手順 1 から 7 までの REST API または CLI は、アップグレード前のストレージソフトウェアのバージョンに対応する「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」または「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」に従ってください。

なお、アップグレードを途中で中止したり、エラーによってアップグレードが中断されたりした場合に、アップグレード以外の操作を実施する場合は、アップグレード前のバージョンに対応したマニュアルを参照して操作してください。

前提条件

- ・ 実行に必要なロール : Service
- ・ Universal Replicator のペアはすべて分割されていること

作業フロー



操作手順の留意事項

- ・ 手順 1 から 8 までは、コントローラーノードで実行する操作です。
- ・ Terraform は実行可能な環境から実行してください。
- ・ 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

操作手順

1. ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。
REST API : GET /v1/objects/storage
CLI : storage_show
アップグレードが必要な場合は、次の手順に進みます。
2. ダウンロードサーバーから以下のファイルを入手して、コントローラーノードに格納します。
(入手するファイル)
次のファイルは、アップグレード先のバージョンに合ったものを入手してください。
 - ・ hsds-update-<version>-<number>.tar
ストレージソフトウェアのアップデートファイルです。手順 1 で取得したストレージノードのバージョン aa.bb.cc.dd の dd 部分の数字と、ストレージソフトウェアのアップデートフ

ファイルの<version>の下 2 桁の数字が一致することを確認してください。一致しないストレージソフトウェアのアップデートファイルは使用しないでください。

(例)hsds-update-01000000-7070.tar

- EULA_for_SLE_for_StorageNode.txt
ストレージノードで使用している SUSE Linux Enterprise に関する EULA 文書です。
- EULA_for_SPDK.txt
ストレージノードで使用している Cavium SPDK FC Target Driver に関する EULA 文書です。

3. 格納した 2 つの EULA 文書の記載内容を確認します。

同意いただける場合は、次の手順に進みます。同意できない場合は、ソフトウェアアップデートを中止してください。

4. ジョブの情報を取得して、実行中のソフトウェアアップデートのジョブがないことを確認します。

REST API : GET /v1/objects/jobs

CLI : job_list

実行中のソフトウェアアップデートのジョブがない場合は、次の手順に進みます。



注意

ソフトウェアアップデートのジョブが実行中だったとき、以降の操作を行うと、実行中だったソフトウェアアップデートのジョブは失敗しますので注意してください。

5. ストレージソフトウェアのアップデートファイルをストレージクラスターにアップロードします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

ストレージクラスターに転送するストレージソフトウェアのアップデートファイルを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/upload-software-update-file/invoke

CLI : storage_upload_software_update_file

実行結果は、コンソール上に出力されます。REST API では、HTTP ステータスコードとして 204 が、CLI ではメッセージとして"Completed."が、それぞれ返ったらアップロードは成功です。その際、イベントログは出力されません。



メモ

アップデートファイルのアップロード完了以降、ソフトウェアアップグレードの実行前までは、転送済みのソフトウェアアップデートファイルの情報を取得できます。操作方法は「転送済みのソフトウェアアップデートファイルの情報を取得する」を参照してください。

6. ソフトウェアアップデートを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

mode パラメーターを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/update-software/invoke

CLI : storage_update_software

コマンド実行後に表示されるジョブの ID を確認します。

7. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



注意

- ソフトウェアアップデートが KARS10109-E で失敗した場合は、他の競合するジョブが動作しているためソフトウェアアップデートを実行できなかったことを意味しています。競合したジョブを中断するか、ジョブが完了するのをしばらく待ってから再実施してください。なお、当該メッセージで表示される競合ジョブの ID に、ストレージクラスターが内部で実行しているジョブの ID が表示されることがあります。ストレージクラスターが内部で実行しているジョブの state は参照できません。
- ソフトウェアアップデートが KARS10110-E で失敗した場合は、ストレージソフトウェアのアップデートファイルがストレージクラスターに存在していなかったことを意味します。手順 5 でストレージソフトウェアのアップデートファイルのアップロードに成功している場合でも、以下のケースなどで KARS10110-E が出力される場合があります。その場合は手順 5 から再度実施してください。
 - ソフトウェアアップデート実施中にクラスターマスターノード(プライマリー)が障害を原因に閉塞した場合
 - ソフトウェアアップデート実施中にストレージクラスターの停止または電断があった場合
 - ソフトウェアアップデートのオプション指定に誤りがあったため、KARS10115-E が出力された場合
- VSP One SDS Block Administrator を利用している場合は、手順 7 を実施後に、数秒待ってから以下を実施してください。
 - Web ブラウザーまたはタブをいったん閉じます。
 - Web ブラウザーのキャッシュをクリアします。
 - VSP One SDS Block Administrator を開き直して使用します。

8. ストレージクラスターの情報を取得して、ストレージソフトウェアが更新されたことを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

9. CLI を使用している場合は、ストレージソフトウェアのアップグレードに合わせてコントローラーノードに CLI プログラムの最新版をインストールします。

CLI プログラムのインストール手順は、Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。



メモ

ストレージソフトウェアより CLI プログラムのバージョンが古い状態で CLI を実行した場合、一致するバージョンまたは新しいバージョンへの更新を促す警告文が標準エラー出力に出力されます。

10. Universal Replicator を使用している場合は、必要に応じて管理サーバーに最新版の RAID Manager をインストールします。



メモ

RAID Manager のバージョンが古い場合、正しい情報を参照または取得できないことがあります。

11. SNMP を利用している場合は、ストレージソフトウェアのアップグレードに合わせてアップグレード先のバージョンに合った拡張 MIB を SNMP マネージャーに取り込みます。

拡張 MIB の取り込み手順は「拡張 MIB の取り込み」を参照してください。

12. ストレージソフトウェアのアップグレードに合わせてストレージクラスターを構成するクラウドリソースのアップグレードを行います。
- a. 「構成ファイルをエクスポートする<<Cloud for Google Cloud>>」を参照し、VSP One SDS Block からアップグレード後のバージョンに対応した構成ファイルを取得します。
- 構成ファイルをエクスポートする際は、exportFileType パラメーターを省略するか、Normal を指定してください。
- 最新状態の構成ファイルを使用するために必ず取得してください。
- b. 「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する <<Cloud for Google Cloud>>」を参照し、構成ファイルを解凍して配置します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、ストレージクラスターが閉塞するなどの事態が起こるおそれがあります。

- c. クラウドリソースのバージョンを確認します。

Terraform の作業ディレクトリーで terraform output コマンドを実行します。

"TemplateVersion"キーの値を確認します。

```
terraform output
```

手順 8 で確認したストレージソフトウェアのバージョンとクラウドリソースのバージョンが一致している場合は、以上で手順は終了です。

- d. 構成ファイルをデプロイすることによる影響を確認します。

以下のコマンドを実行します。

```
terraform plan
```

コマンドを実行すると[Terraform will perform the following actions]という表示に続いてリソースに対する変更内容が表示されます。

以下のリソースの変更が実施されることを確認してください。

#	リソース種別	リソース操作	リソース名*	確認内容
1	google_compute_instance.instance[]	update in-place	<clusterName>-snXX	以下の項目に変更がある場合がありますが、問題ありません。 • metadata • deletion_protection
2	Changes to Output	update in-place	なし	TemplateVersion がアップグレード後のバージョンに変更。 Changes to Output は最後に出力されます。

*リソース名の XX は、ストレージノードに割り振られている番号

- e. terraform plan による確認で問題がなければ、以下のコマンドを実行します。

```
terraform apply
```

コマンドの実行後、[Enter a value:]と表示されたら[yes]を入力します。

入力すると最後に[Outputs]が出力されます。terraform apply が完了することで、クラウドリソースの変更が完了します。

32.6 ストレージソフトウェアをアップグレードする ≪Cloud for Microsoft Azure≫

この節での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージソフトウェアを新しいバージョンに更新します。

ソフトウェアアップデート中に発生するストレージノード間でのストレージソフトウェアのバージョン混在は許容されます。バージョン混在中は、アップグレード前のバージョンでの動作が保障されます。

ストレージソフトウェアのバージョンが切り替わるのは、手順 6 を実行中に、各ストレージノードのアップグレードがすべて完了したときです。

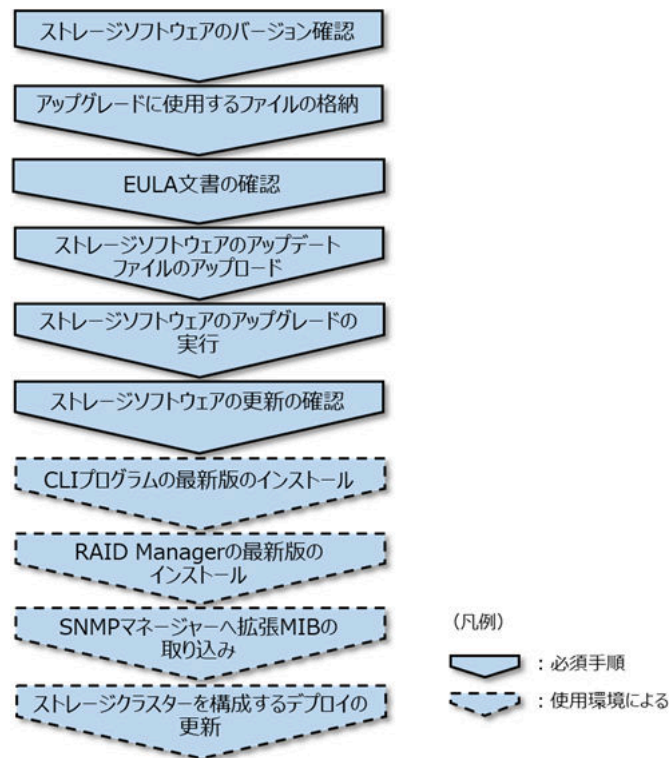
このため、手順 1 から 7 までの REST API または CLI は、アップグレード前のストレージソフトウェアのバージョンに対応する「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」または「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」に従ってください。

なお、アップグレードを途中で中止したり、エラーによってアップグレードが中断されたりした場合に、アップグレード以外の操作を実施する場合は、アップグレード前のバージョンに対応したマニュアルを参照して操作してください。

前提条件

- 実行に必要なロール : Service
- Universal Replicator のペアはすべて分割されていること
- コントローラーノードで Azure CLI が実行できること

作業フロー



操作手順の留意事項

- 手順 1 から 8 までは、コントローラーノードで実行する操作です。
- 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

操作手順

- ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。
REST API : GET /v1/objects/storage
CLI : storage_show
アップグレードが必要な場合は、次の手順に進みます。
- ダウンロードサーバーから以下のファイルを入手して、コントローラーノードに格納します。
(入手するファイル)
次のファイルは、アップグレード先のバージョンに合ったものを入手してください。
 - hsds-update-<version>-<number>.tar
ストレージソフトウェアのアップデートファイルです。手順 1 で取得したストレージノードのバージョン aa.bb.cc.dd の dd 部分の数字と、ストレージソフトウェアのアップデートファイルの<version>の下 2 桁の数字が一致することを確認してください。一致しないストレージソフトウェアのアップデートファイルは使用しないでください。
(例)hsds-update-01000000-7070.tar
 - EULA_for_SLE_for_StorageNode.txt
ストレージノードで使用している SUSE Linux Enterprise に関する EULA 文書です。
 - EULA_for_SPDK.txt
ストレージノードで使用している Cavium SPDK FC Target Driver に関する EULA 文書です。

3. 格納した 2 つの EULA 文書の記載内容を確認します。

同意いただける場合は、次の手順に進みます。同意できない場合は、ソフトウェアアップデートを中止してください。

4. ジョブの情報を取得して、実行中のソフトウェアアップデートのジョブがないことを確認します。

REST API : GET /v1/objects/jobs

CLI : job_list

実行中のソフトウェアアップデートのジョブがない場合は、次の手順に進みます。



注意

ソフトウェアアップデートのジョブが実行中だったとき、以降の操作を行うと、実行中だったソフトウェアアップデートのジョブは失敗しますので注意してください。

5. ストレージソフトウェアのアップデートファイルをストレージクラスターにアップロードします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

ストレージクラスターに転送するストレージソフトウェアのアップデートファイルを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/upload-software-update-file/invoke

CLI : storage_upload_software_update_file

実行結果は、コンソール上に出力されます。REST API では、HTTP ステータスコードとして 204 が、CLI ではメッセージとして "Completed." が、それぞれ返ったらアップロードは成功です。その際、イベントログは出力されません。



メモ

アップデートファイルのアップロード完了以降、ソフトウェアアップグレードの実行前までは、転送済みのソフトウェアアップデートファイルの情報を取得できます。操作方法は「転送済みのソフトウェアアップデートファイルの情報を取得する」を参照してください。

6. ソフトウェアアップデートを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

mode パラメーターを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/update-software/invoke

CLI : storage_update_software

コマンド実行後に表示されるジョブの ID を確認します。

7. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。



注意

- ソフトウェアアップデートが KARS10109-E で失敗した場合は、他の競合するジョブが動作しているためソフトウェアアップデートを実行できなかったことを意味しています。競合したジョブを中断するか、ジョブが完了するのをしばらく待ってから再実施してください。なお、当該メッセージで表示される競合ジョブの ID に、ストレージクラスターが内部で実行しているジョブの ID が表示されることがあります。ストレージクラスターが内部で実行しているジョブの state は参照できません。
- ソフトウェアアップデートが KARS10110-E で失敗した場合は、ストレージソフトウェアのアップデートファイルがストレージクラスターに存在していなかったことを意味します。手

順 5 でストレージソフトウェアのアップデートファイルのアップロードに成功している場合でも、以下のケースなどで KARS10110-E が出力される場合があります。その場合は手順 5 から再度実施してください。

- ソフトウェアアップデート実施中にクラスターマスターノード(プライマリー)が障害を原因に閉塞した場合
- ソフトウェアアップデート実施中にストレージクラスターの停止または電断があった場合
- ソフトウェアアップデートのオプション指定に誤りがあったため、KARS10115-E が出力された場合
- VSP One SDS Block Administrator を利用している場合は、手順 7 を実施後に、数秒待ってから以下を実施してください。
 1. Web ブラウザーまたはタブをいったん閉じます。
 2. Web ブラウザーのキャッシュをクリアします。
 3. VSP One SDS Block Administrator を開き直して使用します。

8. ストレージクラスターの情報を取得して、ストレージソフトウェアが更新されたことを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

9. CLI を使用している場合は、ストレージソフトウェアのアップグレードに合わせてコントローラーノードに CLI プログラムの最新版をインストールします。

CLI プログラムのインストール手順は、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。



メモ

ストレージソフトウェアより CLI プログラムのバージョンが古い状態で CLI を実行した場合、一致するバージョンまたは新しいバージョンへの更新を促す警告文が標準エラー出力に出力されません。

10. Universal Replicator を使用している場合は、必要に応じて管理サーバーに最新版の RAID Manager をインストールします。



メモ

RAID Manager のバージョンが古い場合、正しい情報を参照または取得できないことがあります。

11. SNMP を利用している場合は、ストレージソフトウェアのアップグレードに合わせてアップグレード先のバージョンに合った拡張 MIB を SNMP マネージャーに取り込みます。

拡張 MIB の取り込み手順は「拡張 MIB の取り込み」を参照してください。

12. ストレージソフトウェアのアップグレードに合わせて、ストレージクラスターを構成するデプロイの更新を行います。

ただし、手順 8 で確認したストレージソフトウェアのバージョンとデプロイのバージョンが一致している場合は、本手順の実施は不要です。



メモ

デプロイのバージョンは以下のコマンドで確認できます。

```
az deployment group show ¥
--name mainTemplate ¥
--resource-group <リソースグループ名> ¥
--query "properties.outputs.templateVersion.value"
```



注意

mainTemplate の templateVersion が確認できない場合は、Azure ポータル上でクラスター構築時に最初に作成されたデプロイ (InstallationStatus のデプロイより前にあるデプロイ) があるか確認してください。

クラスター構築時に最初に作成されたデプロイがある場合は、そのデプロイを --name に指定して templateVersion を確認してください。

クラスター構築時に最初に作成されたデプロイがない場合は、本手順を実施してください。

- a. 「構成ファイルをエクスポートする<<Cloud for Microsoft Azure>>」を参照し、VSP One SDS Block からアップグレード後のバージョンに対応した構成ファイルを取得します。
構成ファイルをエクスポートする際は、exportFileType パラメーターを省略するか、Normal を指定してください。
最新状態の構成ファイルを使用するために必ず取得してください。
- b. エクスポートした ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz を解凍します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、その後の操作が失敗するおそれがあります。

- c. 次の Azure CLI を実行して、デプロイの更新を行います。

```
az deployment group create ¥
--name mainTemplate ¥
--resource-group <作成したリソースグループ名> ¥
--template-file VMConfigurationFile.json ¥
--parameters @VMConfigurationFile.parameters.json
```



メモ

name は mainTemplate を指定してください。

- d. 次の Azure CLI を実行して、デプロイ結果が "Succeeded" であることを確認します。
"Running" の場合は、しばらくしてから再度次の Azure CLI を実行してください。

```
az deployment group show ¥
--name mainTemplate ¥
--resource-group <リソースグループ名> ¥
--query "properties.provisioningState"
```

- e. 次の Azure CLI を実行して、デプロイのバージョンを確認し、ストレージソフトウェアのバージョンと同じであることを確認します。

```
az deployment group show ¥
--name mainTemplate ¥
--resource-group <リソースグループ名> ¥
--query "properties.outputs.templateVersion.value"
```

32.7 ストレージソフトウェアをダウングレードする<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ストレージソフトウェアを旧バージョンに更新できます。

ソフトウェアアップデート中に発生するストレージノード間でのストレージソフトウェアのバージョン混在は許容されます。バージョン混在中は、ダウングレード後のバージョンでの動作が保障されます。

ダウングレードの留意事項

以下の表のダウングレード先バージョンへのダウングレードを実施する場合、表の機能を使用しているときは、ダウングレード先バージョンでは当該機能がサポートされていないため、ダウングレードは失敗します。ダウングレードが失敗した場合には、イベントログ **KARS10107-E** が出力されます。イベントログ **KARS10107-E** のメッセージには、ダウングレード失敗の要因となった機能名が出力されます。

以下の表に該当しない機能名がイベントログ **KARS10107-E** のメッセージに表示された場合、ダウングレード元バージョンとダウングレード先バージョンの間に互換性がない可能性があるため、「ソフトウェアの互換性について」を参照し、「アップデート元バージョン」と互換性がある「アップデート先バージョン」へのダウングレードを実施してください。

ダウングレードを行う場合は、表に記載されている無効化方法に従って各機能を無効化してからダウングレードを実施してください。無効化方法が記載されていない場合はダウングレードできません。

ダウングレード先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
01.11.0x.40	マルチテナンシー	Multi-Tenancy	「マルチテナンシーを構成する<<Bare metal>>」を参照し、ストレージクラスターに作成している VPS をすべて削除してください。
		Multi-Tenancy with data compression settings	容量削減機能が設定されている VPS の容量削減機能の設定を無効にする、または、その VPS が不要な場合には削除してください。「マルチテナンシーを構成する<<Bare metal>>」を参照して実施してください。
	QoS	QoS	QoS が設定されているボリューム、スナップショット、VPS があれば、それらを削除するか、それらの QoS の設定を無効にしてください。 「ボリュームを管理する」、「スナップショットを使用したボリュームのバックアップと復元」、「マルチテナンシーを構成する<<Bare metal>>」を参照して実施してください。
	Resource ロール	Resource role	「ユーザーを管理する」を参照し、ビルトインユーザーグループを除く、下記のロールを持つユーザーグループを削除してください。または、対象のユーザーグループから下記のロールを削除してください。 - Resource - VpsSecurity - VpsStorage - VpsMonitor
	スペアノード	Spare node	「スペアノードの情報を削除する<<Bare metal>>」に従って、ストレージクラスター

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
			に登録されているスベアノードをすべて削除してください。
	パスワードポリシー設定の制限解除	Restrictions lifting of password policy settings	「ユーザー認証設定を編集する」を参照し、以下のように設定してください。 • minLength : 11 以下 • minNumberOfUpperCaseChars : 1 以下 • minNumberOfLowerCaseChars : 8 以下 • minNumberOfNumerals : 1 以下 • minNumberOfSymbols : 1 以下 • numberOfPasswordHistory : 任意(制限なし)
	容量削減機能	Data Compression with memory data protection	容量削減機能が有効になっているボリュームをすべて削除してください。
	キャッシュ保護付きライトバックモード	Write back mode with cache protection	一度キャッシュ保護付きライトバックモードを有効にしたストレージクラスターに対しては、キャッシュ保護付きライトバックモードを無効にすることはできません。
	格納データ暗号化	Data at rest encryption	「暗号化環境の設定を編集する」を参照して、暗号化環境の設定を無効にしてください。ただし、ストレージプールを拡張したあとに暗号化環境の設定を無効にすることはできません。
	NVMe/TCP 接続	NVMe_TCP Target	「コンピュータポートのプロトコルを変更する<<Bare metal>>」を参照して、コンピュータポートのプロトコルを iSCSI に変更してください。
	管理ポート非冗長化	Non-redundant control port	「ストレージノードを交換する<<Bare metal>>」を参照して、管理ポートのチーミングが無効なストレージノードをすべて、管理ポートをチーミングしたストレージノードに交換してください。 または「ストレージノードを減設する<<Bare metal>>」を参照して、管理ポートのチーミングが無効なストレージノードを減設してください。
	PCI スロット柔軟化	Configuration flexibility	「ストレージノードを交換する<<Bare metal>>」を参照して、NIC アダプター(イーサネット)またはディスクアレイコントローラーの搭載 PCI スロット位置がバージョン 1.11.0x.40 でサポートされていないストレージノードをバージョン 1.11.0x.40 でサポートされている構成のストレージノードに交換してください。 または「ストレージノードを減設する<<Bare metal>>」を参照して、NIC アダプター(イーサネット)またはディスクアレイコントローラーの搭載 PCI スロット位置がバージョン

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
			1.11.0x.40 でサポートされていないストレージノードを減設してください。
	ボリューム作成	Volumes available for remote copy	バージョン 01.15.0x.40 以降で作成したボリュームをすべて削除してください。具体的には「ボリュームの一覧情報を取得する」を参照して、各ボリュームの isRemoteCopySupported を確認し、非同期リモートコピーで利用可能なボリューム (true)があれば、それらをすべて削除してください。
	マルチテナンシー外部認証・外部認可	Multi-Tenancy with external authentication and authorization	以下の両方に当てはまるユーザーグループを削除してください。 • VPS 管理グループ • 外部認証、外部認可のマッピンググループ
	FC Target	FC Target Applicable Platforms Enhancement	無効化方法はありません。
	Universal Replicator	Remote copy support Extended	VSP One B20 のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy Applicable Platforms Enhancement	以下をすべて削除してください。 • リモートパスグループ • リモート iSCSI ポート • ジャーナルグループ • volumeType が "FormerJournal" のボリューム
		Remote copy support Extended 2	VSP E1090、VSP E1090H のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy support Extended 3	接続先が VSP One SDS Block となっているリモートパスグループとリモート iSCSI ポートを削除してください。
		Multiple iSCSI Login For Remote Copy	異なるリモートパスグループで、同じ iSCSI ポート間のリモートパスが存在しない状態にしてください。
	容量バランス設定の対象追加	Capacity balance settings for storage controller	容量バランスの無効化設定の方法をダウングレード先でサポートしている方法にて代替する必要があります。具体的には下記の手順を実施してください。 ストレージクラスターの容量バランスを無効にしている場合、「ストレージノードの容量バランスの設定を編集する」を参照し、すべてのストレージノードの容量バランスを無効に設定してください。 ストレージコントローラーの容量バランスを無効にしている場合、「ストレージコントローラー情報の一覧を取得する」を参照して、activeStorageNodeId に表示されているスト

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
			レージノードに対して、容量バランスを無効に設定してください。 上記の手順を実施後、「ストレージクラスターの容量バランスの設定を編集する」と「ストレージコントローラーの容量バランスの設定を編集する」を参照し、ストレージクラスターとストレージコントローラーの容量バランスの設定をそれぞれ有効に設定してください。
	メタデータのドライブ書き込み削減	Reduction of drive writes for metadata	「メタデータのドライブ書き込み削減モードを無効にする」を参照して、メタデータのドライブ書き込み削減モードを無効に変更してください。
	NVMe Drive Direct Attach	NVMe Direct Attach	ユーザーデータドライブが NVMe Drive Direct Attach で構成されているストレージノードがある場合は、そのストレージノードをすべて、NVMe Drive Direct Attach で構成されていないストレージノードに交換するか、ストレージノードを減設してください。
	許可リストで IP アドレスの範囲指定を許可	Allowlist support network address	許可リストに設定されている CIDR 表記の IP アドレスをすべて削除してください。
01.12.0x.40	マルチテナンシー	Multi-Tenancy with data compression settings	容量削減機能が設定されている VPS の容量削減機能の設定を無効にする、または、その VPS が不要な場合には削除してください。 「マルチテナンシーを構成する ≪Bare metal≫」を参照して実施してください。
	パスワードポリシー設定の制限解除	Restrictions lifting of password policy settings	「ユーザー認証設定を編集する」を参照し、以下のように設定してください。 • minLength : 11 以下 • minNumberOfUpperCaseChars : 1 以下 • minNumberOfLowerCaseChars : 8 以下 • minNumberOfNumerals : 1 以下 • minNumberOfSymbols : 1 以下 • numberOfPasswordHistory : 任意(制限なし)
	容量削減機能	Data Compression with memory data protection	容量削減機能が有効になっているボリュームをすべて削除してください。
	キャッシュ保護付きライトバックモード	Write back mode with cache protection	一度キャッシュ保護付きライトバックモードを有効にしたストレージクラスターに対しては、キャッシュ保護付きライトバックモードを無効にすることはできません。
	格納データ暗号化	Data at rest encryption	「暗号化環境の設定を編集する」を参照して、暗号化環境の設定を無効にしてください。ただし、ストレージプールを拡張したあとに暗号化環境の設定を無効にすることはできません。

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
	NVMe/TCP 接 続	NVMe_TCP Target	「コンピュータポートのプロトコルを変更す る<<Bare metal>>」を参照して、コンピュ ータポートのプロトコルを iSCSI に変更して ください。
	管理ポート非冗 長化	Non-redundant control port	「ストレージノードを交換する<<Bare metal>>」を参照して、管理ポートのチー ミングが無効なストレージノードをすべて、管 理ポートをチーミングしたストレージノード に交換してください。 または「ストレージノードを減設する<<Bare metal>>」を参照して、管理ポートのチー ミングが無効なストレージノードを減設して ください。
	PCI スロット柔 軟化	Configuration flexibility	「ストレージノードを交換する<<Bare metal>>」を参照して、NIC アダプター(イー サネット)またはディスクアレイコントロー ラーの搭載 PCI スロット位置がバージョン 1.12.0x.40 でサポートされていないストレ ージノードをバージョン 1.12.0x.40 でサポー トされている構成のストレージノードに交換 してください。 または「ストレージノードを減設する<<Bare metal>>」を参照して、NIC アダプター(イー サネット)またはディスクアレイコントロー ラーの搭載 PCI スロット位置がバージョン 1.12.0x.40 でサポートされていないストレ ージノードを減設してください。
	ボリューム作成	Volumes available for remote copy	バージョン 01.15.0x.40 以降で作成したボリ ュームをすべて削除してください。具体的 には「ボリュームの一覧情報を取得する」を参 照して、各ボリュームの isRemoteCopySupported を確認し、非同期 リモートコピーで利用可能なボリューム (true)があれば、それらをすべて削除して ください。
	マルチテナンシ ー外部認証・外 部認可	Multi-Tenancy with external authentication and authorization	以下の両方に当てはまるユーザーグループを 削除してください。 • VPS 管理グループ • 外部認証、外部認可のマッピンググルー プ
	FC Target	FC Target Applicable Platforms Enhancement	無効化方法はありません。
	Universal Replicator	Remote copy support Extended	VSP One B20 のリモートパスグループとリ モート iSCSI ポートを削除してください。
		Remote copy Applicable Platforms Enhancement	以下をすべて削除してください。 • リモートパスグループ • リモート iSCSI ポート • ジャーナルグループ

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
			volumeType が"FormerJournal"のボリューム
		Remote copy support Extended 2	VSP E1090、VSP E1090H のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy support Extended 3	接続先が VSP One SDS Block となっているリモートパスグループとリモート iSCSI ポートを削除してください。
		Multiple iSCSI Login For Remote Copy	異なるリモートパスグループで、同じ iSCSI ポート間のリモートパスが存在しない状態にしてください。
	容量バランス設定の 対象追加	Capacity balance settings for storage controller	容量バランスの無効化設定の方法をダウングレード先でサポートしている方法にて代替する必要があります。具体的には下記の手順を実施してください。 ストレージクラスターの容量バランスを無効にしている場合、「ストレージノードの容量バランスの設定を編集する」を参照し、すべてのストレージノードの容量バランスを無効に設定してください。 ストレージコントローラーの容量バランスを無効にしている場合、「ストレージコントローラー情報の一覧を取得する」を参照して、activeStorageNodeId に表示されているストレージノードに対して、容量バランスを無効に設定してください。 上記の手順を実施後、「ストレージクラスターの容量バランスの設定を編集する」と「ストレージコントローラーの容量バランスの設定を編集する」を参照し、ストレージクラスターとストレージコントローラーの容量バランスの設定をそれぞれ有効に設定してください。
	メタデータのドライブ書き込み削減	Reduction of drive writes for metadata	「メタデータのドライブ書き込み削減モードを無効にする」を参照して、メタデータのドライブ書き込み削減モードを無効に変更してください。
	NVMe Drive Direct Attach	NVMe Direct Attach	ユーザーデータドライブが NVMe Drive Direct Attach で構成されているストレージノードがある場合は、そのストレージノードをすべて、NVMe Drive Direct Attach で構成されていないストレージノードに交換するか、ストレージノードを減設してください。
01.13.0x.40	許可リストで IP アドレスの範囲 指定を許可	Allowlist support network address	許可リストに設定されている CIDR 表記の IP アドレスをすべて削除してください。
	格納データ暗号化	Data at rest encryption	「暗号化環境の設定を編集する」を参照して、暗号化環境の設定を無効にしてください。ただし、ストレージプールを拡張したあとに暗号化環境の設定を無効にすることはできません。

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
	NVMe/TCP 接 続	NVMe_TCP Target	「コンピュータポートのプロトコルを変更する<<Bare metal>>」を参照して、コンピュータポートのプロトコルを iSCSI に変更してください。
	管理ポート非冗 長化	Non-redundant control port	「ストレージノードを交換する<<Bare metal>>」を参照して、管理ポートのチーミングが無効なストレージノードをすべて、管理ポートをチーミングしたストレージノードに交換してください。 または「ストレージノードを減設する<<Bare metal>>」を参照して、管理ポートのチーミングが無効なストレージノードを減設してください。
	PCI スロット柔 軟化	Configuration flexibility	「ストレージノードを交換する<<Bare metal>>」を参照して、NIC アダプター(イーサネット)またはディスクアレイコントローラーの搭載 PCI スロット位置がバージョン 1.13.0x.40 でサポートされていないストレージノードをバージョン 1.13.0x.40 でサポートされている構成のストレージノードに交換してください。 または「ストレージノードを減設する<<Bare metal>>」を参照して、NIC アダプター(イーサネット)またはディスクアレイコントローラーの搭載 PCI スロット位置がバージョン 1.13.0x.40 でサポートされていないストレージノードを減設してください。
	ボリューム作成	Volumes available for remote copy	バージョン 01.15.0x.40 以降で作成したボリュームをすべて削除してください。具体的には「ボリュームの一覧情報を取得する」を参照して、各ボリュームの isRemoteCopySupported を確認し、非同期リモートコピーで利用可能なボリューム(true)があれば、それらをすべて削除してください。
	マルチテナンシ ー外部認証・外 部認可	Multi-Tenancy with external authentication and authorization	以下の両方に当てはまるユーザーグループを削除してください。 • VPS 管理グループ • 外部認証、外部認可のマッピンググループ
	FC Target	FC Target Applicable Platforms Enhancement	無効化方法はありません。
	Universal Replicator	Remote copy support Extended	VSP One B20 のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy Applicable Platforms Enhancement	以下をすべて削除してください。 • リモートパスグループ • リモート iSCSI ポート • ジャーナルグループ

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
			volumeType が"FormerJournal"のボリューム
		Remote copy support Extended 2	VSP E1090、VSP E1090H のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy support Extended 3	接続先が VSP One SDS Block となっているリモートパスグループとリモート iSCSI ポートを削除してください。
		Multiple iSCSI Login For Remote Copy	異なるリモートパスグループで、同じ iSCSI ポート間のリモートパスが存在しない状態にしてください。
	容量バランス設定の 対象追加	Capacity balance settings for storage controller	容量バランスの無効化設定の方法をダウングレード先でサポートしている方法にて代替する必要があります。具体的には下記の手順を実施してください。 ストレージクラスターの容量バランスを無効にしている場合、「ストレージノードの容量バランスの設定を編集する」を参照し、すべてのストレージノードの容量バランスを無効に設定してください。 ストレージコントローラーの容量バランスを無効にしている場合、「ストレージコントローラー情報の一覧を取得する」を参照して、activeStorageNodeId に表示されているストレージノードに対して、容量バランスを無効に設定してください。 上記の手順を実施後、「ストレージクラスターの容量バランスの設定を編集する」と「ストレージコントローラーの容量バランスの設定を編集する」を参照し、ストレージクラスターとストレージコントローラーの容量バランスの設定をそれぞれ有効に設定してください。
	メタデータのドライブ書き込み削減	Reduction of drive writes for metadata	「メタデータのドライブ書き込み削減モードを無効にする」を参照して、メタデータのドライブ書き込み削減モードを無効に変更してください。
	NVMe Drive Direct Attach	NVMe Direct Attach	ユーザーデータドライブが NVMe Drive Direct Attach で構成されているストレージノードがある場合は、そのストレージノードをすべて、NVMe Drive Direct Attach で構成されていないストレージノードに交換するか、ストレージノードを減設してください。
01.14.0x.40	許可リストで IP アドレスの範囲 指定を許可	Allowlist support network address	許可リストに設定されている CIDR 表記の IP アドレスをすべて削除してください。
	管理ポート非冗 長化	Non-redundant control port	「ストレージノードを交換する <<Bare metal>>」を参照して、管理ポートのチャミングが無効なストレージノードをすべて、管理ポートをチャミングしたストレージノードに交換してください。

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
			または「ストレージノードを減設する<<Bare metal>>」を参照して、管理ポートのチーミングが無効なストレージノードを減設してください。
	PCI スロット柔軟化	Configuration flexibility	「ストレージノードを交換する<<Bare metal>>」を参照して、NIC アダプター(イーサネット)またはディスクアレイコントローラーの搭載 PCI スロット位置がバージョン 1.14.0x.40 でサポートされていないストレージノードをバージョン 1.14.0x.40 でサポートされている構成のストレージノードに交換してください。 または「ストレージノードを減設する<<Bare metal>>」を参照して、NIC アダプター(イーサネット)またはディスクアレイコントローラーの搭載 PCI スロット位置がバージョン 1.14.0x.40 でサポートされていないストレージノードを減設してください。
	ボリューム作成	Volumes available for remote copy	バージョン 01.15.0x.40 以降で作成したボリュームをすべて削除してください。具体的には「ボリュームの一覧情報を取得する」を参照して、各ボリュームの isRemoteCopySupported を確認し、非同期リモートコピーで利用可能なボリューム(true)があれば、それらをすべて削除してください。
	マルチテナンシー外部認証・外部認可	Multi-Tenancy with external authentication and authorization	以下の両方に当てはまるユーザーグループを削除してください。 • VPS 管理グループ • 外部認証、外部認可のマッピンググループ
	FC Target	FC Target Applicable Platforms Enhancement	無効化方法はありません。
	Universal Replicator	Remote copy support Extended	VSP One B20 のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy Applicable Platforms Enhancement	以下をすべて削除してください。 • リモートパスグループ • リモート iSCSI ポート • ジャーナルグループ • volumeType が"FormerJournal"のボリューム
		Remote copy support Extended 2	VSP E1090、VSP E1090H のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy support Extended 3	接続先が VSP One SDS Block となっているリモートパスグループとリモート iSCSI ポートを削除してください。

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
		Multiple iSCSI Login For Remote Copy	異なるリモートパスグループで、同じ iSCSI ポート間のリモートパスが存在しない状態に してください。
	容量バランス設 定の対象追加	Capacity balance settings for storage controller	容量バランスの無効化設定の方法をダウング レード先でサポートしている方法にて代替す る必要があります。具体的には下記の手順を 実施してください。 ストレージクラスターの容量バランスを無効 にしている場合、「ストレージノードの容量バ ランスの設定を編集する」を参照し、すべて のストレージノードの容量バランスを無効に 設定してください。 ストレージコントローラーの容量バランスを 無効にしている場合、「ストレージコントロー ラー情報の一覧を取得する」を参照して、 activeStorageNodeId に表示されているスト レージノードに対して、容量バランスを無効 に設定してください。 上記の手順を実施後、「ストレージクラスター の容量バランスの設定を編集する」と「スト レージコントローラーの容量バランスの設定 を編集する」を参照し、ストレージクラス ターとストレージコントローラーの容量バラン スの設定をそれぞれ有効に設定してくださ い。
	メタデータのド ライブ書き込み 削減	Reduction of drive writes for metadata	「メタデータのドライブ書き込み削減モード を無効にする」を参照して、メタデータのド ライブ書き込み削減モードを無効に変更して ください。
	NVMe Drive Direct Attach	NVMe Direct Attach	ユーザーデータドライブが NVMe Drive Direct Attach で構成されているストレージ ノードがある場合は、そのストレージノード をすべて、NVMe Drive Direct Attach で構 成されていないストレージノードに交換する か、ストレージノードを減設してください。
	許可リストで IP アドレスの範囲 指定を許可	Allowlist support network address	許可リストに設定されている CIDR 表記の IP アドレスをすべて削除してください。
01.15.0x.40	マルチテナンシ ー外部認証・外 部認可	Multi-Tenancy with external authentication and authorization	以下の両方に当てはまるユーザーグループを 削除してください。 • VPS 管理グループ • 外部認証、外部認可のマッピンググルー プ
	FC Target	FC Target Applicable Platforms Enhancement	無効化方法はありません。
	Universal Replicator	Remote copy support Extended	VSP One B20 のリモートパスグループとリ モート iSCSI ポートを削除してください。

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
		Remote copy Applicable Platforms Enhancement	以下をすべて削除してください。 - リモートパスグループ - リモート iSCSI ポート - ジャーナルグループ - volumeType が"FormerJournal"のボリューム
		Remote copy support Extended 2	VSP E1090、VSP E1090H のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy support Extended 3	接続先が VSP One SDS Block となっているリモートパスグループとリモート iSCSI ポートを削除してください。
		Multiple iSCSI Login For Remote Copy	異なるリモートパスグループで、同じ iSCSI ポート間のリモートパスが存在しない状態にしてください。
	容量バランス設定の対象追加	Capacity balance settings for storage controller	容量バランスの無効化設定の方法をダウングレード先でサポートしている方法にて代替する必要があります。具体的には下記の手順を実施してください。 ストレージクラスターの容量バランスを無効にしている場合、「ストレージノードの容量バランスの設定を編集する」を参照し、すべてのストレージノードの容量バランスを無効に設定してください。 ストレージコントローラーの容量バランスを無効にしている場合、「ストレージコントローラー情報の一覧を取得する」を参照して、activeStorageNodeId に表示されているストレージノードに対して、容量バランスを無効に設定してください。 上記の手順を実施後、「ストレージクラスターの容量バランスの設定を編集する」と「ストレージコントローラーの容量バランスの設定を編集する」を参照し、ストレージクラスターとストレージコントローラーの容量バランスの設定をそれぞれ有効に設定してください。
	メタデータのドライブ書き込み削減	Reduction of drive writes for metadata	「メタデータのドライブ書き込み削減モードを無効にする」を参照して、メタデータのドライブ書き込み削減モードを無効に変更してください。
	NVMe Drive Direct Attach	NVMe Direct Attach	ユーザーデータドライブが NVMe Drive Direct Attach で構成されているストレージノードがある場合は、そのストレージノードをすべて、NVMe Drive Direct Attach で構成されていないストレージノードに交換するか、ストレージノードを減設してください。
	許可リストで IP アドレスの範囲 指定を許可	Allowlist support network address	許可リストに設定されている CIDR 表記の IP アドレスをすべて削除してください。

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
01.16.0x.40	マルチテナンシー外部認証・外部認可	Multi-Tenancy with external authentication and authorization	以下の両方に当てはまるユーザーグループを削除してください。 - VPS 管理グループ - 外部認証、外部認可のマッピンググループ
	FC Target	FC Target Applicable Platforms Enhancement	無効化方法はありません。
	Universal Replicator	Remote copy support Extended	VSP One B20 のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy Applicable Platforms Enhancement	以下をすべて削除してください。 - リモートパスグループ - リモート iSCSI ポート - ジャーナルグループ - volumeType が"FormerJournal"のボリューム
		Remote copy support Extended 2	VSP E1090、VSP E1090H のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy support Extended 3	接続先が VSP One SDS Block となっているリモートパスグループとリモート iSCSI ポートを削除してください。
		Multiple iSCSI Login For Remote Copy	異なるリモートパスグループで、同じ iSCSI ポート間のリモートパスが存在しない状態にしてください。
	容量バランス設定の対象追加	Capacity balance settings for storage controller	容量バランスの無効化設定の方法をダウングレード先でサポートしている方法にて代替する必要があります。具体的には下記の手順を実施してください。 ストレージクラスターの容量バランスを無効にしている場合、「ストレージノードの容量バランスの設定を編集する」を参照し、すべてのストレージノードの容量バランスを無効に設定してください。 ストレージコントローラーの容量バランスを無効にしている場合、「ストレージコントローラー情報の一覧を取得する」を参照して、activeStorageNodeId に表示されているストレージノードに対して、容量バランスを無効に設定してください。 上記の手順を実施後、「ストレージクラスターの容量バランスの設定を編集する」と「ストレージコントローラーの容量バランスの設定を編集する」を参照し、ストレージクラスターとストレージコントローラーの容量バランスの設定をそれぞれ有効に設定してください。

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
	メタデータのドライブ書き込み削減	Reduction of drive writes for metadata	「メタデータのドライブ書き込み削減モードを無効にする」を参照して、メタデータのドライブ書き込み削減モードを無効に変更してください。
	NVMe Drive Direct Attach	NVMe Direct Attach	ユーザーデータドライブが NVMe Drive Direct Attach で構成されているストレージノードがある場合は、そのストレージノードをすべて、NVMe Drive Direct Attach で構成されていないストレージノードに交換するか、ストレージノードを減設してください。
	許可リストで IP アドレスの範囲指定を許可	Allowlist support network address	許可リストに設定されている CIDR 表記の IP アドレスをすべて削除してください。
01.17.0x.40	Universal Replicator	Remote copy support Extended 2	VSP E1090、VSP E1090H のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy support Extended 3	接続先が VSP One SDS Block となっているリモートパスグループとリモート iSCSI ポートを削除してください。
		Multiple iSCSI Login For Remote Copy	異なるリモートパスグループで、同じ iSCSI ポート間のリモートパスが存在しない状態にしてください。
	メタデータのドライブ書き込み削減	Reduction of drive writes for metadata	「メタデータのドライブ書き込み削減モードを無効にする」を参照して、メタデータのドライブ書き込み削減モードを無効に変更してください。
	NVMe Drive Direct Attach	NVMe Direct Attach	ユーザーデータドライブが NVMe Drive Direct Attach で構成されているストレージノードがある場合は、そのストレージノードをすべて、NVMe Drive Direct Attach で構成されていないストレージノードに交換するか、ストレージノードを減設してください。
	許可リストで IP アドレスの範囲指定を許可	Allowlist support network address	許可リストに設定されている CIDR 表記の IP アドレスをすべて削除してください。



メモ

ダウングレード時のバージョン切り替えについて

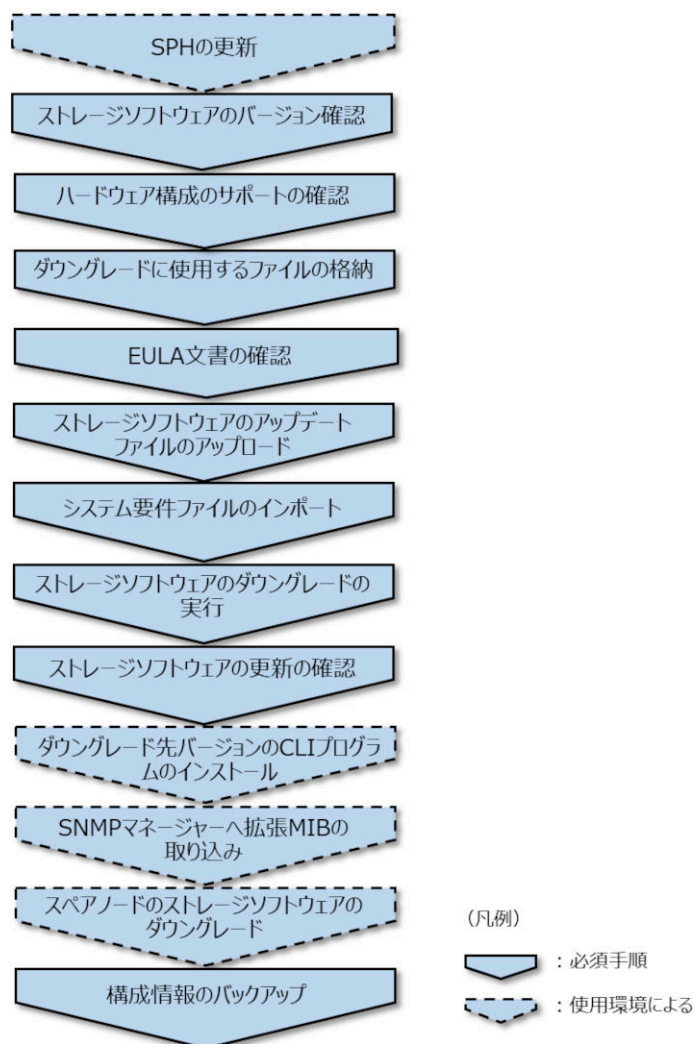
- ストレージソフトウェアのバージョンが切り替わるのは、ソフトウェアアップデートの実行コマンドを投入した直後です。
このため、バージョンが切り替わるまでの、手順 1 から 10 までの REST API または CLI は、このマニュアルが対象とするバージョンに対応する「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」または「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」に従ってください。
- バージョンの切り替えと連動し、ストレージクラスターの動作が切り替わります。そのため、ダウングレード前の一部の機能(アップグレードによってこれまで使えていた新機能)が使用できなくなります。ダウングレードを実施する場合は、これら新機能を事前に無効化する必要があります。無効化を実施せずにダウングレードすると、イベントログ KARS10107-E が出力されソフトウェアアップデートは中止されます。

- ・ ダウングレードを途中で中止したり、エラーによってダウングレードが中断されたりした場合に、アップデート以外の操作を実施する場合は、ストレージソフトウェアのバージョンに対応したマニュアルを参照して各操作を実施してください。

前提条件

- ・ 実行に必要なロール：Service

作業フロー



操作手順の留意事項

手順 1 から 10 までは、コントローラーノードで実行する操作です。

操作手順

1. 日立アドバンストサーバ HA8000V シリーズを使用している場合、アップデート後のストレージソフトウェアのバージョンに対応したバージョンの SPH(Service Pack for HA8000V)への更新が必要になることがあります。

「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照し、ストレージソフトウェアのバージョンと SPH のバージョンの組み合わせを確認の上、必要な場合は SPH を更新してください。



メモ 手順 1 は最後の手順としても実施できます。

2. ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

ソフトウェアダウングレードが必要な場合は、次の手順に進みます。

3. ダウングレード先のバージョンが、現在のハードウェア構成をサポートしているか確認します。
サポートされるハードウェアは、ダウングレード先のバージョンに対応する「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。サポートされている場合は、次の手順に進みます。

4. サポートセンターから以下のファイルを入手して、コントローラーノードに格納します。
(入手するファイル)

次のファイルは、ダウングレード先のバージョンに合ったものを入手してください。

- hsds-update-<version>-<number>.tar

ストレージソフトウェアのアップデートファイルです。手順 2 で取得したストレージノードのバージョン aa.bb.cc.dd の dd 部分の数字と、ストレージソフトウェアのアップデートファイルの<version>の下 2 桁の数字が一致することを確認してください。一致しないストレージソフトウェアのアップデートファイルは使用しないでください。

(例)hsds-update-01000000-7070.tar

- EULA_for_SLE_for_StorageNode.txt

ストレージノードで使用している SUSE Linux Enterprise に関する EULA 文書です。

- EULA_for_SPDK.txt

ストレージノードで使用している Cavium SPDK FC Target Driver に関する EULA 文書です。

次のファイルは、最新のものをサポートセンターから入手してください。

- SystemRequirementsFile.yml

システム要件ファイルです。

5. 格納した 2 つの EULA 文書の記載内容を確認します。

同意いただける場合は、次の手順に進みます。同意できない場合は、ソフトウェアのダウングレードを中止してください。

6. ジョブの情報を取得して、実行中のソフトウェアアップデートのジョブがないことを確認します。

REST API : GET /v1/objects/jobs

CLI : job_list

実行中のソフトウェアアップデートのジョブがない場合は、次の手順に進みます。



注意

ソフトウェアアップデートのジョブが実行中だったとき、以降の操作を行うと、実行中だったソフトウェアアップデートのジョブは失敗しますので注意してください。

7. ストレージソフトウェアのアップデートファイルをストレージクラスターにアップロードします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

ストレージクラスターに転送するストレージソフトウェアのアップデートファイルを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/upload-software-update-file/invoke

CLI : storage_upload_software_update_file

実行結果は、コンソール上に出力されます。REST API では、HTTP ステータスコードとして 204 が、CLI ではメッセージとして"Completed."が、それぞれ返ったらアップロードは成功です。その際、イベントログは出力されません。



メモ

アップデートファイルのアップロード完了以降、ソフトウェアダウングレードの実行前までは、転送済みのソフトウェアアップデートファイルの情報を取得できます。操作方法は「転送済みのソフトウェアアップデートファイルの情報を取得する」を参照してください。

8. 手順 4 で格納したシステム要件ファイルを指定して以下のコマンドを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : POST /v1/objects/system-requirements-file/actions/import/invoke

CLI : system_requirements_file_import

指定したシステム要件ファイルのバージョンが、VSP One SDS Block にインポート済みのバージョンより新しい場合のみインポート処理が行われます。指定したシステム要件ファイルのバージョンが同じか古い場合は、イベントログを出力しインポート処理をスキップします。

コマンド実行後に表示されるジョブの ID を確認します。

9. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

10. ストレージソフトウェアのダウングレードを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

mode パラメーターと downgrade パラメーターを指定してコマンドを実行します。downgrade パラメーターには"true"を指定してください。downgrade パラメーターに"true"が指定されていない場合、ソフトウェアダウングレードは実行できません。

REST API : POST /v1/objects/storage/actions/update-software/invoke

CLI : storage_update_software

コマンド実行後に表示される、ジョブの ID を確認します。



注意

VSP One SDS Block Administrator を利用している場合は、手順 10 を実施後に、数秒待ってから以下を実施してください。

1. Web ブラウザーまたはタブをいったん閉じます。
2. Web ブラウザーのキャッシュをクリアします。
3. VSP One SDS Block Administrator を開き直して使用します。

また、VSP One SDS Block Administrator の Storage Cluster Information 画面の STORAGE SOFTWARE VERSION にエラーメッセージが表示されていないことを確認してください。表示されていた場合は、エラーメッセージに従って対処してください。

11. ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



注意

- ソフトウェアダウングレードが KARS10109-E で失敗した場合は、他の競合するジョブが動作しているためソフトウェアダウングレードを実行できなかったことを意味しています。競合したジョブを中断するか、ジョブが完了するのをしばらく待ってから再実施してください。なお、当該メッセージで表示される競合ジョブの ID に、ストレージクラスターが内部で実行しているジョブの ID が表示されることがあります。ストレージクラスターが内部で実行しているジョブの state は参照できません。
- ソフトウェアアップデートが KARS10110-E で失敗した場合は、ストレージソフトウェアのアップデートファイルがストレージクラスターに存在していなかったことを意味しています。手順 7 でストレージソフトウェアのアップデートファイルのアップロードに成功している場合でも、以下のケースなどで KARS10110-E が出力される場合があります。その場合は手順 7 から再度実施してください。
 - ソフトウェアアップデート実施中にクラスターマスターノード(プライマリー)が障害を原因に閉塞した場合
 - ソフトウェアアップデート実施中にストレージクラスターの停止または電断があった場合

12. ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、ストレージクラスターの情報を取得して、ストレージソフトウェアが更新されたことを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

13. CLI を使用している場合は、ストレージソフトウェアのダウングレード先のバージョンに対応した CLI プログラムをコントローラーノードにインストールします。

CLI プログラムのインストール手順は、ダウングレード先のバージョンに対応した Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」に記載してある「VSP One SDS Block の CLI プログラムをインストールする」を参照してください。



メモ

ストレージソフトウェアより CLI プログラムのバージョンが古い状態で CLI を実行した場合、一致するバージョンまたは新しいバージョンへの更新を促す警告文が標準エラー出力に出力されます。

14. SNMP を利用している場合は、ストレージソフトウェアのダウングレードにあわせてダウングレード先のバージョンに合った拡張 MIB を SNMP マネージャーに取り込みます。

ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、「拡張 MIB の取り込み」に記載してある作業を実施します。

15. スペアノードを使用している場合は、ストレージソフトウェアのダウングレードに合わせてスペアノードのソフトウェアのダウングレードを行います。

ただし、ストレージソフトウェアとスペアノードのソフトウェアのバージョンが一致している場合は、スペアノードのソフトウェアのダウングレードは不要です。

ストレージソフトウェアのダウングレード後にスペアノードを使用しない場合は、以下の手順 a のみを実施し、手順 b～d は実施しないでください。

以下の手順は、ダウングレード先のバージョンに対応したマニュアルを参照してください。

- a. ストレージクラスターからスペアノードの情報を削除します。

「スペアノードの情報を削除する <<Bare metal>>」に記載してある作業を実施します。

- b. スペアノードに、ダウングレード先のバージョンのストレージソフトウェアをインストールします。
Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージソフトウェアをインストールする」に記載してある作業を実施します。
 - c. スペアノードに対して、ストレージノード単位のセットアップを行います。
Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノード単位のセットアップを行う」に記載してある作業を実施します。
 - d. スペアノードの情報を登録します。
「オペレーションガイド」の「スペアノードの情報を登録する<<Bare metal>>」に記載してある作業を実施します。
16. ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、構成情報のバックアップを実施します。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

32.8 ストレージソフトウェアをダウングレードする<<Cloud for AWS>>

この節での記述内容は Cloud モデル for AWS に適用されます。

ストレージソフトウェアを旧バージョンに更新できます。

ソフトウェアアップデート中に発生するストレージノード間でのストレージソフトウェアのバージョン混在は許容されます。バージョン混在中は、ダウングレード後のバージョンでの動作が保障されます。

ダウングレードの留意事項

以下の表のダウングレード先バージョンへのダウングレードを実施する場合、表の機能を使用してときは、ダウングレード先バージョンでは当該機能がサポートされていないため、ダウングレードは失敗します。ダウングレードが失敗した場合には、イベントログ KARS10107-E が出力されます。イベントログ KARS10107-E のメッセージには、ダウングレード失敗の要因となった機能名が出力されます。

以下の表に該当しない機能名がイベントログ KARS10107-E のメッセージに表示された場合、ダウングレード元バージョンとダウングレード先バージョンの間に互換性がない可能性があるため、「ソフトウェアの互換性について」を参照し、「アップデート元バージョン」と互換性がある「アップデート先バージョン」へのダウングレードを実施してください。

ダウングレードを行う場合は、表に記載されている無効化方法に従って各機能を無効化してからダウングレードを実施してください。無効化方法が記載されていない場合はダウングレードできません。

ダウングレード先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
01.15.0x.30	Universal Replicator	Remote copy support Extended	VSP One B20 のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy support Extended 2	VSP E1090、VSP E1090H のリモートパスグループとリモート iSCSI ポートを削除してください。

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
		Remote copy support Extended 3	接続先が VSP One SDS Block となっている リモートパスグループとリモート iSCSI ポ ートを削除してください。
		Multiple iSCSI Login For Remote Copy	異なるリモートパスグループで、同じ iSCSI ポート間のリモートパスが存在しない状態 にしてください。
		Remote path group capacity expansion	以下の状態にしてください。 - リモートパスグループ当たりのリモート パス数が 8 以下 - ストレージクラスター当たりのリモート iSCSI ポート数が 512 以下
	格納データ暗号 化 (料金モデル BYOL を選択し ている場合のみ)	Data at rest encryption Applicable Platforms Enhancement	「暗号化環境の設定を編集する」を参照して、 暗号化環境の設定を無効にしてください。 ただし、ストレージプールを拡張したあとに 暗号化環境の設定を無効にすることはでき ません。
	ComputePort IPv6	Compute Port IPv6 Applicable Platforms Enhancement	無効化方法はありません。
	容量バランス設 定の対象追加	Capacity balance settings for storage controller	容量バランスの無効化設定の方法をダウン グレード先でサポートしている方法にて代 替する必要があります。具体的には下記の 手順を実施してください。 ストレージクラスターの容量バランスを無 効にしている場合、「ストレージノードの容 量バランスの設定を編集する」を参照し、す べてのストレージノードの容量バランスを 無効に設定してください。 ストレージコントローラーの容量バランス を無効にしている場合、「ストレージコント ローラー情報の一覧を取得する」を参照し て、activeStorageNodeId に表示されている ストレージノードに対して、容量バランスを 無効に設定してください。 上記の手順を実施後、「ストレージクラス ターの容量バランスの設定を編集する」と「ス トレージコントローラーの容量バランスの 設定を編集する」を参照し、ストレージクラ スターとストレージコントローラーの容量 バランスの設定をそれぞれ有効に設定して ください。
	メタデータのド ライブ書き込み 削減	Reduction of drive writes for metadata	「メタデータのドライブ書き込み削減モード を無効にする」を参照して、メタデータのド ライブ書き込み削減モードを無効に変更し てください。
	許可リストで IP アドレスの範囲 指定を許可	Allowlist support network address	許可リストに設定されている CIDR 表記の IP アドレスをすべて削除してください。

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
	格納データ暗号化 (料金モデル Usage Pricing または Contract を選択している 場合のみ)	Data at rest encryption Applicable Pricing Model Enhancement	「暗号化環境の設定を編集する」を参照して、暗号化環境の設定を無効にしてください。 ただし、ストレージプールを拡張したあとに暗号化環境の設定を無効にすることはできません。
01.16.0x.30	Universal Replicator	Remote copy support Extended 2	VSP E1090、VSP E1090H のリモートパスグループとリモート iSCSI ポートを削除してください。
		Remote copy support Extended 3	接続先が VSP One SDS Block となっているリモートパスグループとリモート iSCSI ポートを削除してください。
		Multiple iSCSI Login For Remote Copy	異なるリモートパスグループで、同じ iSCSI ポート間のリモートパスが存在しない状態にしてください。
		Remote path group capacity expansion	以下の状態にしてください。 - リモートパスグループ当たりのリモートパス数が 8 以下 - ストレージクラスター当たりのリモート iSCSI ポート数が 512 以下
	ComputePort IPv6	Compute Port IPv6 Applicable Platforms Enhancement	無効化方法はありません。
	容量バランス設定の対象追加	Capacity balance settings for storage controller	容量バランスの無効化設定の方法をダウングレード先でサポートしている方法にて代替する必要があります。具体的には下記の手順を実施してください。 ストレージクラスターの容量バランスを無効にしている場合、「ストレージノードの容量バランスの設定を編集する」を参照し、すべてのストレージノードの容量バランスを無効に設定してください。 ストレージコントローラーの容量バランスを無効にしている場合、「ストレージコントローラー情報の一覧を取得する」を参照して、activeStorageNodeId に表示されているストレージノードに対して、容量バランスを無効に設定してください。 上記の手順を実施後、「ストレージクラスターの容量バランスの設定を編集する」と「ストレージコントローラーの容量バランスの設定を編集する」を参照し、ストレージクラスターとストレージコントローラーの容量バランスの設定をそれぞれ有効に設定してください。
	メタデータのドライブ書き込み削減	Reduction of drive writes for metadata	「メタデータのドライブ書き込み削減モードを無効にする」を参照して、メタデータのド

ダウングレード 先バージョン	機能名	KARS10107-E に出力される機能名	無効化方法
			ライブ書き込み削減モードを無効に変更してください。
	許可リストで IP アドレスの範囲 指定を許可	Allowlist support network address	許可リストに設定されている CIDR 表記の IP アドレスをすべて削除してください。
	格納データ暗号 化 (料金モデル Usage Pricing または Contract を選択している 場合のみ)	Data at rest encryption Applicable Pricing Model Enhancement	「暗号化環境の設定を編集する」を参照して、 暗号化環境の設定を無効にしてください。 ただし、ストレージプールを拡張したあとに 暗号化環境の設定を無効にすることはでき ません。
01.17.0x.30	Universal Replicator	Remote copy support Extended 2	VSP E1090、VSP E1090H のリモートパス グループとリモート iSCSI ポートを削除し てください。
		Remote copy support Extended 3	接続先が VSP One SDS Block となっている リモートパスグループとリモート iSCSI ポ ートを削除してください。
		Multiple iSCSI Login For Remote Copy	異なるリモートパスグループで、同じ iSCSI ポート間のリモートパスが存在しない状態 にしてください。
		Remote path group capacity expansion	以下の状態にしてください。 - リモートパスグループ当たりのリモート パス数が 8 以下 - ストレージクラスター当たりのリモート iSCSI ポート数が 512 以下
	メタデータのド ライブ書き込み 削減	Reduction of drive writes for metadata	「メタデータのドライブ書き込み削減モード を無効にする」を参照して、メタデータのド ライブ書き込み削減モードを無効に変更し てください。
	許可リストで IP アドレスの範囲 指定を許可	Allowlist support network address	許可リストに設定されている CIDR 表記の IP アドレスをすべて削除してください。
	格納データ暗号 化 (料金モデル Usage Pricing または Contract を選択している 場合のみ)	Data at rest encryption Applicable Pricing Model Enhancement	「暗号化環境の設定を編集する」を参照して、 暗号化環境の設定を無効にしてください。 ただし、ストレージプールを拡張したあとに 暗号化環境の設定を無効にすることはでき ません。



メモ

ダウングレード時のバージョン切り替えについて

- ストレージソフトウェアのバージョンが切り替わるのは、ソフトウェアアップデートの実行コマンドを投入した直後です。
このため、バージョンが切り替わるまでの、手順 1 から 6 までの REST API または CLI は、このマニュアルが対象とするバージョンに対応する「Hitachi Virtual Storage Platform One SDS Block REST API リフ

アレンス」または「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」に従ってください。

- バージョンの切り替えと連動し、ストレージクラスターの動作が切り替わります。そのため、ダウングレード前の一部の機能(アップグレードによってこれまで使えていた新機能)が使用できなくなります。ダウングレードを実施する場合は、これら新機能を事前に無効化する必要があります。無効化を実施せずにダウングレードすると、イベントログ KARS10107-E が出力されソフトウェアアップデートは中止されます。
- ダウングレードを途中で中止したり、エラーによってダウングレードが中断されたりした場合に、アップデート以外の操作を実施する場合は、ストレージソフトウェアのバージョンに対応したマニュアルを参照して各操作を実施してください。ただし、ストレージソフトウェアのバージョンが 01.17.0x.30 のストレージノードとストレージソフトウェアのバージョンが 01.18.0x.30 以降のストレージノードが混在している構成で、01.18.0x.30 以降のストレージノードを交換する場合は、このマニュアルの「ストレージソフトウェアのバージョンが混在している場合のストレージノード交換<<Cloud for AWS>>」を参照してください。

前提条件

- 実行に必要なロール : Service

作業フロー



操作手順の留意事項

- 手順 1 から 10 までは、コントローラーノードで実行する操作です。
- 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

操作手順

1. ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

ソフトウェアダウングレードが必要な場合は、次の手順に進みます。

2. サポートセンターから以下のファイル入手して、コントローラーノードに格納します。

(入手するファイル)

次のファイルは、ダウングレード先のバージョンに合ったものを入手してください。

- hsd-update-<version>-<number>.tar

ストレージソフトウェアのアップデートファイルです。手順 1 で取得したストレージノードのバージョン aa.bb.cc.dd の dd 部分の数字と、ストレージソフトウェアのアップデートファイルの<version>の下 2 桁の数字が一致することを確認してください。一致しないストレージソフトウェアのアップデートファイルは使用しないでください。

(例)hsd-update-01000000-7070.tar

- EULA_for_SLE_for_StorageNode.txt

ストレージノードで使用している SUSE Linux Enterprise に関する EULA 文書です。

- EULA_for_SPDK.txt

ストレージノードで使用している Cavium SPDK FC Target Driver に関する EULA 文書です。

- hsd-cf-template-files-<model>-<version>-<number>.zip

VSP One SDS Block の構成を管理するためのファイルです。<model>は AWS Marketplace で選択した料金モデルです。料金モデルに合わせて次のファイルを使用してください。

- BYOL(Bring Your Own License)を選択した場合 : <model>が BYOL のファイル
- Usage Pricing を選択した場合 : <model>が Utility のファイル
- Contract を選択した場合 : <model>が Floating のファイル

3. 格納した 2 つの EULA 文書の記載内容を確認します。

同意いただける場合は、次の手順に進みます。同意できない場合は、ソフトウェアのダウングレードを中止してください。

4. ジョブの情報を取得して、実行中のソフトウェアアップデートのジョブがないことを確認します。

REST API : GET /v1/objects/jobs

CLI : job_list

実行中のソフトウェアアップデートのジョブがない場合は、次の手順に進みます。



注意

ソフトウェアアップデートのジョブが実行中だったとき、以降の操作を行うと、実行中だったソフトウェアアップデートのジョブは失敗しますので注意してください。

5. ストレージソフトウェアのアップデートファイルをストレージクラスターにアップロードします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

ストレージクラスターに転送するストレージソフトウェアのアップデートファイルを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/upload-software-update-file/invoke

CLI : storage_upload_software_update_file

実行結果は、コンソール上に出力されます。REST API では、HTTP ステータスコードとして 204 が、CLI ではメッセージとして"Completed."が、それぞれ返ったらアップロードは成功です。その際、イベントログは出力されません。



メモ

アップデートファイルのアップロード完了以降、ソフトウェアダウングレードの実行前までは、転送済みのソフトウェアアップデートファイルの情報を取得できます。操作方法は「転送済みのソフトウェアアップデートファイルの情報を取得する」を参照してください。

6. ストレージソフトウェアのダウングレードを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

mode パラメーターと downgrade パラメーターを指定してコマンドを実行します。downgrade パラメーターには"true"を指定してください。downgrade パラメーターに"true"が指定されていない場合、ソフトウェアダウングレードは実行できません。

REST API : POST /v1/objects/storage/actions/update-software/invoke

CLI : storage_update_software

コマンド実行後に表示される、ジョブの ID を確認します。



注意

VSP One SDS Block Administrator を利用している場合は、手順 6 を実施後に、数秒待ってから以下を実施してください。

1. Web ブラウザーまたはタブをいったん閉じます。
2. Web ブラウザーのキャッシュをクリアします。
3. VSP One SDS Block Administrator を開き直して使用します。

また、VSP One SDS Block Administrator の Storage Cluster Information 画面の STORAGE SOFTWARE VERSION にエラーメッセージが表示されていないことを確認してください。表示されていた場合は、エラーメッセージに従って対処してください。

7. ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



注意

- ・ ソフトウェアダウングレードが KARS10109-E で失敗した場合は、他の競合するジョブが動作しているためソフトウェアダウングレードを実行できなかったことを意味しています。競合したジョブを中断するか、ジョブが完了するのをしばらく待ってから再実施してください。なお、当該メッセージで表示される競合ジョブの ID に、ストレージクラスターが内部で実行しているジョブの ID が表示されることがあります。ストレージクラスターが内部で実行しているジョブの state は参照できません。
- ・ ソフトウェアアップデートが KARS10110-E で失敗した場合は、ストレージソフトウェアのアップデートファイルがストレージクラスターに存在していなかったことを意味しています。手順 5 でストレージソフトウェアのアップデートファイルのアップロードに成功している場合でも、以下のケースなどで KARS10110-E が出力される場合があります。その場合は手順 5 から再度実施してください。

- ・ ソフトウェアアップデート実施中にクラスターマスターノード(プライマリ)が障害を原因に閉塞した場合
- ・ ソフトウェアアップデート実施中にストレージクラスターの停止または電断があった場合
- ・ ジョブの state が"Failed"や"Stopped"になった場合でも、一部のストレージノードのダウングレードが完了している場合、ストレージソフトウェアのバージョンが更新されます。手順 8 に進んでください。

8. ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、ストレージクラスターの情報を取得して、ストレージソフトウェアが更新されたことを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show



注意

ストレージソフトウェアのバージョンが更新されていない場合は、手順 9 以降の手順を実施する必要はありません。ストレージソフトウェアのバージョンがダウングレード先のバージョンに更新されている場合、手順 9 に進んでください。

9. ストレージソフトウェアを 01.17.0x.30 にダウングレードする場合は、ダウングレード先のバージョンに対応した VSP One SDS Block インストーラーをインストールします。

VSP One SDS Block インストーラーのインストール手順は、ダウングレード先のバージョンに対応した Cloud モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」にある「VSP One SDS Block インストーラーをインストールする」を参照してください。

10. CLI を使用している場合は、ストレージソフトウェアのダウングレード先のバージョンに対応した CLI プログラムをコントローラーノードにインストールします。

CLI プログラムのインストール手順は、ダウングレード先のバージョンに対応した Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」に記載してある「VSP One SDS Block の CLI プログラムをインストールする」を参照してください。



メモ

ストレージソフトウェアより CLI プログラムのバージョンが古い状態で CLI を実行した場合、一致するバージョンまたは新しいバージョンへの更新を促す警告文が標準エラー出力に出力されます。

11. SNMP を利用している場合は、ストレージソフトウェアのダウングレードにあわせてダウングレード先のバージョンに合った拡張 MIB を SNMP マネージャーに取り込みます。

ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、「拡張 MIB の取り込み」に記載してある作業を実施します。

12. ストレージソフトウェアのダウングレードに合わせてスタックのテンプレートのダウングレードを行います。

ただし、ダウングレード先のストレージソフトウェアのバージョンと、スタックのテンプレートのバージョンが一致している場合は、スタックのテンプレートのダウングレードは不要です。



メモ

スタックのテンプレートのバージョンは以下のコマンドで確認できます。

```
aws cloudformation describe-stacks ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
```



```
--query ¥  
'Stacks[0].Outputs[?OutputKey==`TemplateVersion`].OutputValue' ¥  
--output text
```

- a. ダウングレード先のバージョンに対応した以下のファイルをコントローラーノードにコピーします。

- 構成ファイル(.zip)

VSP One SDS Block のダウングレードで使用するファイルです。

ファイル名は、hsds-system-configuration-files-**<model>**-**<version>**-**<number>**.zip です。

(例) hsds-system-configuration-files-Utility-01150030-0000.zip

コントローラーノードへファイルをコピーする方法として、例えばサポートセンターから入手したファイルを Amazon S3 へ格納したあと、AWS CLI を用いて Amazon S3 からファイルをコピーする方法があります。操作例は Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」にある「Amazon S3 の操作例」を参照してください。



注意

VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。

- b. コピーしたファイルを解凍し、取得した以下の各ファイルをエディターで開き、各項目に値を設定します。各項目に設定する値については、このマニュアルの「ダウングレード時の VM 構成ファイルを作成する<<Cloud for AWS>>」を参照してください。

Single-AZ の場合：

- VM 構成ファイル
 - VMConfigurationFile_<model>.yaml
 - VMConfigurationFile_4D2P.yaml*
 - VMConfigurationFile_Duplication.yaml*

* 構成によってどちらかのファイルを使用します。ユーザーデータの保護方式が HPEC 4D+2P の場合は、VMConfigurationFile_4D2P.yaml の各項目を設定します。ユーザーデータの保護方式が Mirroring Duplication の場合は、VMConfigurationFile_Duplication.yaml の各項目を設定します。

Multi-AZ の場合：

- VM 構成ファイル
 - VMConfigurationFile_<model>_3AZ.yaml
 - VMConfigurationFile_Duplication_3AZ.yaml*

* Multi-AZ 構成の場合はファイル名から「_3AZ」を削除してから使用してください。



注意

- VMConfigurationFile_4D2P.yaml、VMConfigurationFile_Duplication.yaml、VMConfigurationFile_node01.yaml、VMConfigurationFile_nodeNN.yaml、VMConfigurationFile_nodeTB.yaml のファイル名は変更せずに使用してください。
- VMConfigurationFile.yaml(ダウンロードサーバーから提供された時点のファイル名は、VMConfigurationFile_<model>.yaml または VMConfigurationFile_<model>_3AZ.yaml)

はファイル名を変更できます。変更した場合は、以降の手順に記載されているファイル名を変更後のファイル名に読み替えてください。

- c. 手順 b で取り出した VM 構成ファイルを「ダウングレード時の VM 構成ファイルを作成する <<Cloud for AWS>>」の手順 6 で指定した Amazon S3 バケットに格納します。

Amazon S3 にファイルを格納する方法として、例えば AWS CLI を用いて Amazon S3 にファイルをコピーする方法があります。詳細は Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」にある「Amazon S3 の操作例」を参照してください。



注意

VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。

- d. 次の AWS CLI を実行して、変更セットを作成します。

```
aws cloudformation create-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <任意の変更セット名*> ¥
--template-url ¥
<Amazon S3 に格納した VMConfigurationFile.yml の URL (https)> ¥
--include-nested-stacks ¥
--capabilities CAPABILITY_NAMED_IAM
```

* 使用可能文字などは以下の Web サイトを参照してください。

<https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-change-set.html>

- e. 次の AWS CLI を実行して、変更セットを表示します(1 階層目)。

```
aws cloudformation describe-change-set ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--change-set-name <手順 d で指定した変更セット名>
```

以下の事項を確認します。

- "Status"が"CREATE_COMPLETE"であること
"Status"が"CREATE_IN_PROGRESS"の場合はしばらく待ってから再度実行してください。
- "Changes"の項目数が 1 つであること
- "Changes"内の"ResourceChange"について
"Action"が"Modify"であること
次の手順のため、"ChangeSetId"の値を記録します。

- f. 次の AWS CLI を実行して、変更セットを表示します(2 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 e で記録した "ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
"Action"が"Modify"であること
次の手順のため、各項目の"ChangeSetId"の値を記録します。

- g. 次の AWS CLI を実行して、変更セットを表示します(3 階層目)。

```
aws cloudformation describe-change-set ¥
--change-set-name <手順 f で記録した "ChangeSetId">
```

以下の事項を確認します。

- "Changes"内の各項目の"ResourceChange"について
"Action"が"Modify"であること

h. 次の AWS CLI を実行して、変更セットを実行します。

```
aws cloudformation execute-change-set ¥  
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥  
--change-set-name <手順 d で指定した変更セット名>
```

i. 次の AWS CLI を実行して、変更セットの実行結果を確認します。

```
aws cloudformation wait stack-update-complete ¥  
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

`wait stack-update-complete` を実行すると、変更セットの実行が完了するまで待つことができます。実行が完了したら、`describe-stacks` を実行し、`StackStatus` が `"UPDATE_COMPLETE"`であることを確認してください。

```
aws cloudformation describe-stacks ¥  
--stack-name <Marketplace からのインストール時に設定したスタック名>
```

13. ダウングレード先のバージョンに対応した Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」にある「コントローラーノードを配置する」を参照し、コントローラーノードに付与している IAM ロールを見直してください。
14. ダウングレード先のバージョンに対応した Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」にある「セットアップの前提条件を確認する」を参照し、コントローラーノードに付与している IAM ロールを見直してください。
15. ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、構成情報のバックアップを実施します。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

32.8.1 ダウングレード時の VM 構成ファイルを作成する ≪Cloud for AWS≫

この節での記述内容は Cloud モデル for AWS に適用されます。

VM 構成ファイルの作成は、ダウングレードを目的に行います。本バージョンからダウングレードする際に、ダウングレード先のバージョンの VM 構成ファイルを作成するときの手順について記載します。



注意 本節の操作手順で修正している項目以外は、設定値を変更しないでください。本節の操作手順で修正している項目以外を変更した場合、予期しないエラーが発生するおそれがあります。



メモ

- 各項目のコロン(:)のうしろには、1 文字以上の半角スペースが必要です。
- 改行コードは LF、CR LF のどちらでも問題ありません。

前提条件

サポートセンターからダウングレード先の以下のファイルを取得していること

Single-AZ の場合 :

- VMConfigurationFile.yml*
- VMConfigurationFile_4D2P.yml(ユーザーデータの保護方式が HPEC 4D+2P の場合)

- VMConfigurationFile_Duplication.yml(ユーザーデータの保護方式が Mirroring Duplication の場合)

* VMConfigurationFile_BYOL.yml と VMConfigurationFile_Utility.yml のことを指します。

Multi-AZ の場合 :

- VMConfigurationFile.yml*
- VMConfigurationFile_Duplication_3AZ.yml

* VMConfigurationFile_BYOL_3AZ.yml と VMConfigurationFile_Utility_3AZ.yml のことを指します。

操作手順の留意事項

以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

操作手順

1. VM 構成ファイルに記載するパラメーターの値を取得します。

```
aws cloudformation describe-stacks ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--query 'Stacks[0].Parameters'
```

コマンドを実行した結果は、ParameterKey と ParameterValue の組が配列になって表示されます。describe-stacks の実行結果を以下に例示します。手順 2 で転記する箇所はイタリック体(斜体)で示しています。

```
[
  {
    "ParameterKey": "StorageNodeInstanceType",
    "ParameterValue": "m6i.8xlarge"
  },
  {
    "ParameterKey": "ConfigurationPattern",
    "ParameterValue": "Mirroring Duplication ( 6 Nodes )"
  },
  ===== 一部省略 =====
  {
    "ParameterKey": "AvailabilityZone",
    "ParameterValue": "ap-northeast-1a"
  }
]
```

2. VMConfigurationFile.yml の「Parameters:」セクションの各パラメーターの「Default」項目に、手順 1 の describe-stacks で取得した"ParameterValue"を転記します。

このとき、転記先の VMConfigurationFile.yml のパラメーターが、手順 1 で取得した describe-stacks の"ParameterKey"と一致することを確認してください。手順 1 で取得した"ParameterKey"と一致する「Parameters:」セクションのパラメーターがない場合の転記は不要です。

このとき、以下のパラメーターは転記せず、以下に示す値を記入してください。

- RemoveNodeNumber : "-"
- RecoverNodeNumber : "-"
- RemoveDriveNodeNumber : "-"
- RemoveDriveNumber : "-"
- DisableNodeTerminationProtection : "-"

- AmiId : "ami-xxxxxxxxxxxxxxxxxx"

また、転記先の VMConfigurationFile.yml のパラメーターに「AllowedValues」項目が存在する場合、「Default」と同じ値をリスト内に転記してください。



注意

転記する際は、設定値をダブルクォーテーション(")で囲みます。ダブルクォーテーションで囲んでいなかった場合、予期しないエラーが発生することがあります。

「VMConfigurationFile.yml」への転記例を以下に示します。修正箇所はイタリック体(斜体)で示しています。

■ 転記前

```
===== 一部省略 =====
Parameters:
===== 一部省略 =====
  AvailabilityZone:
    Description: Select the availability zone where you want to
    deploy VSSB.
    Type: AWS::EC2::AvailabilityZone::Name

===== 一部省略 =====
  StorageNodeInstanceType:
    Description: Select the instance type for each storage node.
    Type: String
    AllowedValues:
["m7i.8xlarge","m6i.8xlarge","r7i.8xlarge","r6i.8xlarge"]
    Default: "r6i.8xlarge"

  ConfigurationPattern:
    Description: Select the data protection method and the number of
    storage nodes
    Type: String
    AllowedValues: [
      "Mirroring Duplication ( 3 Nodes )",
      "Mirroring Duplication ( 6 Nodes )",
      "Mirroring Duplication ( 9 Nodes )",
      "Mirroring Duplication ( 12 Nodes )",
      "Mirroring Duplication ( 15 Nodes )",
      "Mirroring Duplication ( 18 Nodes )"
    ]
    Default: "Mirroring Duplication ( 3 Nodes )"
===== 一部省略 =====
```

■ 転記後

```
===== 一部省略 =====
Parameters:
===== 一部省略 =====
  AvailabilityZone:
    Description: Select the availability zone where you want to
    deploy VSSB.
    Type: AWS::EC2::AvailabilityZone::Name
    Default: "<手順1で確認した AvailabilityZone の\"ParameterValue\">"

===== 一部省略 =====
  StorageNodeInstanceType:
    Description: Select the instance type for each storage node.
    Type: String
    AllowedValues: ["m7i.8xlarge","m6i.8xlarge",
"r7i.8xlarge","r6i.8xlarge"]
    Default: "<手順1で確認した StorageNodeInstanceType の
\"ParameterValue\">"

  ConfigurationPattern:
    Description: Select the data protection method and the number of
    storage nodes
    Type: String
    AllowedValues: [
===== 一部省略 =====
```

```
"Mirroring Duplication ( 3 Nodes )",
"Mirroring Duplication ( 6 Nodes )",
"Mirroring Duplication ( 9 Nodes )",
"Mirroring Duplication ( 12 Nodes )",
"Mirroring Duplication ( 15 Nodes )",
"Mirroring Duplication ( 18 Nodes )"]
Default: "<手順 1 で確認した ConfigurationPattern の"ParameterValue">"
```

3. ネストされたスタック(2 階層目)の ID を確認します。

```
aws cloudformation describe-stack-resources ¥
--stack-name <Marketplace からのインストール時に設定したスタック名> ¥
--query 'StackResources[0].PhysicalResourceId' ¥
--output text
```

4. VM 構成ファイルに記載する AMI ID の情報を取得します。

```
aws cloudformation describe-stacks ¥
--stack-name <手順 3 で確認したネストされたスタックの ID> ¥
--query ¥
'Stacks[0].Parameters[?contains(ParameterKey,`StorageNodeAMIId`)]
| sort_by(@, &ParameterKey)'
```

describe-stacks の実行結果を以下に例示します。手順 5 で転記する箇所はイタリック体(斜体)で示しています。

```
[
  {
    "ParameterKey": "StorageNodeAMIId01",
    "ParameterValue": "ami-xxxxxxxxxxxxxxxxxx"
  },
  {
    "ParameterKey": "StorageNodeAMIId02",
    "ParameterValue": "ami-xxxxxxxxxxxxxxxxxx"
  },
  ===== 一部省略 =====
  {
    "ParameterKey": "StorageNodeAMIId17",
    "ParameterValue": "ami-xxxxxxxxxxxxxxxxxx"
  },
  {
    "ParameterKey": "StorageNodeAMIId18",
    "ParameterValue": "ami-xxxxxxxxxxxxxxxxxx"
  }
]
```

5. VMConfigurationFile.yml の「StorageNodeAMIIdXX」(XX は 01, 02, 03...)の値を手順 4 の describe-stacks で確認した「StorageNodeAMIIdXX」の"ParameterValue"に書き換えます。以下の階層の「StorageNodeAMIIdXX」の値を書き換えてください。

- Resources: StorageCluster4D2P: Properties: Parameters: StorageNodeAMIIdXX
- Resources: StorageClusterDuplication: Properties: Parameters: StorageNodeAMIIdXX

■書き換え前

```
StorageNodeAMIIdXX: ##StorageNodeAMIIdXX##
```

■書き換え後

```
StorageNodeAMIIdXX: <手順 5 で確認した StorageNodeAMIIdXX の
"ParameterValue">
```

VMConfigurationFile.yml への転記例を以下に示します。修正箇所はイタリック体(斜体)で示しています。

■書き換え前

```
Resources:

# ----- Cluster stack definitions start here. -----

StorageClusterDuplication:
  Type: AWS::CloudFormation::Stack
  Condition: StorageClusterDuplicationCreate
  Properties:
    TemplateURL: https://bucketname/
VMConfigurationFile_Duplication.yml
  Parameters:
    LicenseType: BYOL
===== 一部省略 =====
    RemoveDriveNumber: {"Ref": RemoveDriveNumber}
    StorageNodeAMIId01: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId02: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId03: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId04: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId05: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId06: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId07: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId08: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId09: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId10: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId11: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId12: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId13: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId14: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId15: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId16: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId17: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
    StorageNodeAMIId18: {"Fn::FindInMap": [VssbApAmi, "Ref":
'AWS::Region', Value]}
```

■書き換え後

```
Resources:

# ----- Cluster stack definitions start here. -----

StorageClusterDuplication:
  Type: AWS::CloudFormation::Stack
  Condition: StorageClusterDuplicationCreate
  Properties:
    TemplateURL: https://bucketname/
VMConfigurationFile_Duplication.yml
  Parameters:
    LicenseType: BYOL
===== 一部省略 =====
    RemoveDriveNumber: {"Ref": RemoveDriveNumber}
    StorageNodeAMIId01: <手順 5 で確認した StorageNodeAMIId01 の AMI ID>
    StorageNodeAMIId02: <手順 5 で確認した StorageNodeAMIId02 の AMI ID>
```

```
StorageNodeAMIId03: <手順 5 で確認した StorageNodeAMIId03 の AMI ID>
StorageNodeAMIId04: <手順 5 で確認した StorageNodeAMIId04 の AMI ID>
StorageNodeAMIId05: <手順 5 で確認した StorageNodeAMIId05 の AMI ID>
StorageNodeAMIId06: <手順 5 で確認した StorageNodeAMIId06 の AMI ID>
StorageNodeAMIId07: <手順 5 で確認した StorageNodeAMIId07 の AMI ID>
StorageNodeAMIId08: <手順 5 で確認した StorageNodeAMIId08 の AMI ID>
StorageNodeAMIId09: <手順 5 で確認した StorageNodeAMIId09 の AMI ID>
StorageNodeAMIId10: <手順 5 で確認した StorageNodeAMIId10 の AMI ID>
StorageNodeAMIId11: <手順 5 で確認した StorageNodeAMIId11 の AMI ID>
StorageNodeAMIId12: <手順 5 で確認した StorageNodeAMIId12 の AMI ID>
StorageNodeAMIId13: <手順 5 で確認した StorageNodeAMIId13 の AMI ID>
StorageNodeAMIId14: <手順 5 で確認した StorageNodeAMIId14 の AMI ID>
StorageNodeAMIId15: <手順 5 で確認した StorageNodeAMIId15 の AMI ID>
StorageNodeAMIId16: <手順 5 で確認した StorageNodeAMIId16 の AMI ID>
StorageNodeAMIId17: <手順 5 で確認した StorageNodeAMIId17 の AMI ID>
StorageNodeAMIId18: <手順 5 で確認した StorageNodeAMIId18 の AMI ID>
```

6. アップロードする予定のフォルダーの S3 URL を指定します。以下のファイルについて修正します。

- VMConfigurationFile.yml

VMConfigurationFile.yml の「Parameters:」セクションの「TemplateS3URL」の「Default」項目の値を「https://<バケット名>.s3.<リージョン ID>.amazonaws.com/<アップロード予定のフォルダー名>」に書き換えます。



注意

VM 構成ファイルを格納する先の Amazon S3 バケット名にはドット(".")を含めないでください。



メモ 作成した構成ファイルの構文エラーをチェックすることができます。チェックするには、以下のコマンドを順番に実行します。

- python3
- from awscli.customizations.cloudformation.yamlhelper import yaml_parse
- f = open("<VM 構成ファイルのパス>", "r")
- yaml_parse(f.read())

構文エラーがある場合は、コマンド実行後のコンソール出力に VM 構成ファイルの問題箇所が表示されるため、当該箇所を是正してください。

32.9 ストレージソフトウェアをダウングレードする ≪Cloud for Google Cloud≫

この節での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージソフトウェアを旧バージョンに更新できます。

ソフトウェアアップデート中に発生するストレージノード間でのストレージソフトウェアのバージョン混在は許容されます。バージョン混在中は、ダウングレード後のバージョンでの動作が保障されます。



メモ

ダウングレード時のバージョン切り替えについて

- ストレージソフトウェアのバージョンが切り替わるのは、ソフトウェアアップデートの実行コマンドを投入した直後です。

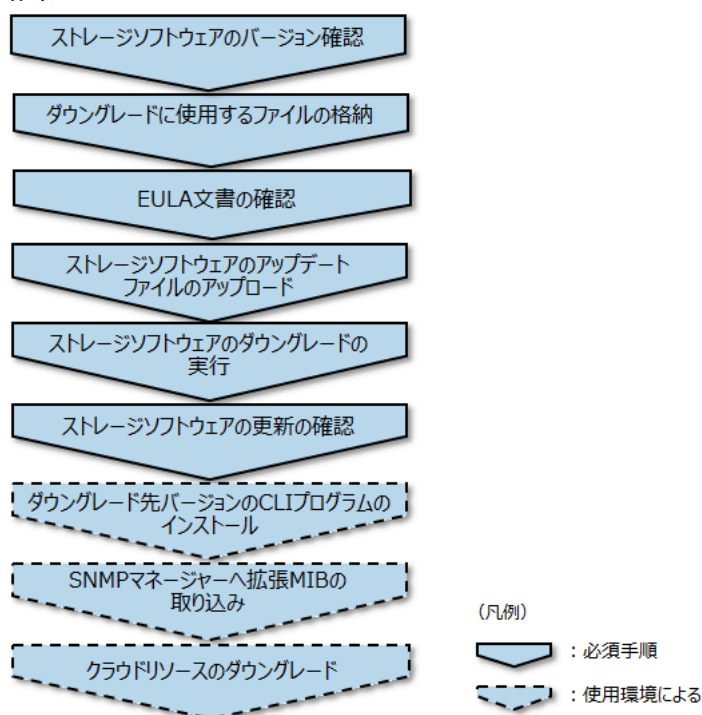
このため、バージョンが切り替わるまでの、手順 1 から 6 までの REST API または CLI は、このマニュアルが対象とするバージョンに対応する「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」または「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」に従ってください。

- バージョンの切り替えと連動し、ストレージクラスターの動作が切り替わります。そのため、ダウングレード前の一部の機能(アップグレードによってこれまで使えていた新機能)が使用できなくなります。ダウングレードを実施する場合は、これら新機能を事前に無効化する必要があります。無効化を実施せずにダウングレードすると、イベントログ KARS10107-E が出力されソフトウェアアップデートは中止されます。
- ダウングレードを途中で中止したり、エラーによってダウングレードが中断されたりした場合に、アップデート以外の操作を実施する場合は、ストレージソフトウェアのバージョンに対応したマニュアルを参照して各操作を実施してください。

前提条件

- 実行に必要なロール : Service

作業フロー



操作手順の留意事項

- 手順 1 から 6 までは、コントローラーノードで実行する操作です。
- Terraform は実行可能な環境から実行してください。
- 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

操作手順

1. ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。
REST API : GET /v1/objects/storage
CLI : storage_show
ソフトウェアダウングレードが必要な場合は、次の手順に進みます。

- サポートセンターから以下のファイル入手して、コントローラーノードに格納します。

(入手するファイル)

次のファイルは、ダウングレード先のバージョンに合ったものを入手してください。

- `hsds-update-<version>-<number>.tar`

ストレージソフトウェアのアップデートファイルです。手順 1 で取得したストレージノードのバージョン `aa.bb.cc.dd` の `dd` 部分の数字と、ストレージソフトウェアのアップデートファイルの `<version>` の下 2 桁の数字が一致することを確認してください。一致しないストレージソフトウェアのアップデートファイルは使用しないでください。

(例)`hsds-update-01000000-7070.tar`

- `EULA_for_SLE_for_StorageNode.txt`

ストレージノードで使用している SUSE Linux Enterprise に関する EULA 文書です。

- `EULA_for_SPDK.txt`

ストレージノードで使用している Cavium SPDK FC Target Driver に関する EULA 文書です。

- 格納した 2 つの EULA 文書の記載内容を確認します。

同意いただける場合は、次の手順に進みます。同意できない場合は、ソフトウェアのダウングレードを中止してください。

- ジョブの情報を取得して、実行中のソフトウェアアップデートのジョブがないことを確認します。

REST API : `GET /v1/objects/jobs`

CLI : `job_list`

実行中のソフトウェアアップデートのジョブがない場合は、次の手順に進みます。



注意

ソフトウェアアップデートのジョブが実行中だったとき、以降の操作を行うと、実行中だったソフトウェアアップデートのジョブは失敗しますので注意してください。

- ストレージソフトウェアのアップデートファイルをストレージクラスターにアップロードします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

ストレージクラスターに転送するストレージソフトウェアのアップデートファイルを指定してコマンドを実行します。

REST API : `POST /v1/objects/storage/actions/upload-software-update-file/invoke`

CLI : `storage_upload_software_update_file`

実行結果は、コンソール上に出力されます。REST API では、HTTP ステータスコードとして 204 が、CLI ではメッセージとして "Completed." が、それぞれ返ったらアップロードは成功です。その際、イベントログは出力されません。



メモ

アップデートファイルのアップロード完了以降、ソフトウェアダウングレードの実行前までは、転送済みのソフトウェアアップデートファイルの情報を取得できます。操作方法は「転送済みのソフトウェアアップデートファイルの情報を取得する」を参照してください。

- ストレージソフトウェアのダウングレードを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

mode パラメーターと downgrade パラメーターを指定してコマンドを実行します。downgrade パラメーターには"true"を指定してください。downgrade パラメーターに"true"が指定されていない場合、ソフトウェアダウングレードは実行できません。

REST API : POST /v1/objects/storage/actions/update-software/invoke

CLI : storage_update_software

コマンド実行後に表示される、ジョブの ID を確認します。



注意

VSP One SDS Block Administrator を利用している場合は、手順 6 を実施後に、数秒待ってから以下を実施してください。

1. Web ブラウザーまたはタブをいったん閉じます。
2. Web ブラウザーのキャッシュをクリアします。
3. VSP One SDS Block Administrator を開き直して使用します。

また、VSP One SDS Block Administrator の Storage Cluster Information 画面の STORAGE SOFTWARE VERSION にエラーメッセージが表示されていないことを確認してください。表示されていた場合は、エラーメッセージに従って対処してください。

7. ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



注意

- ・ ソフトウェアダウングレードが KARS10109-E で失敗した場合は、他の競合するジョブが動作しているためソフトウェアダウングレードを実行できなかったことを意味しています。競合したジョブを中断するか、ジョブが完了するのをしばらく待ってから再実施してください。なお、当該メッセージで表示される競合ジョブの ID に、ストレージクラスターが内部で実行しているジョブの ID が表示されることがあります。ストレージクラスターが内部で実行しているジョブの state は参照できません。
 - ・ ソフトウェアアップデートが KARS10110-E で失敗した場合は、ストレージソフトウェアのアップデートファイルがストレージクラスターに存在していなかったことを意味しています。手順 5 でストレージソフトウェアのアップデートファイルのアップロードに成功している場合でも、以下のケースなどで KARS10110-E が出力される場合があります。その場合は手順 5 から再度実施してください。
 - ・ ソフトウェアアップデート実施中にクラスターマスターノード(プライマリ)が障害を原因に閉塞した場合
 - ・ ソフトウェアアップデート実施中にストレージクラスターの停止または電断があった場合
-

8. ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、ストレージクラスターの情報を取得して、ストレージソフトウェアが更新されたことを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

9. CLI を使用している場合は、ストレージソフトウェアのダウングレード先のバージョンに対応した CLI プログラムをコントローラーノードにインストールします。

CLI プログラムのインストール手順は、ダウングレード先のバージョンに対応した Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド

ド」に記載してある「VSP One SDS Block の CLI プログラムをインストールする」を参照してください。



メモ

ストレージソフトウェアより CLI プログラムのバージョンが古い状態で CLI を実行した場合、一致するバージョンまたは新しいバージョンへの更新を促す警告文が標準エラー出力に出力されません。

10. SNMP を利用している場合は、ストレージソフトウェアのダウングレードにあわせてダウングレード先のバージョンに合った拡張 MIB を SNMP マネージャーに取り込みます。

ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、「拡張 MIB の取り込み」に記載してある作業を実施します。

11. ストレージソフトウェアのダウングレードに合わせて、ストレージクラスターを構成するクラウドリソースのダウングレードを行います。
 - a. 「構成ファイルをエクスポートする <<Cloud for Google Cloud>>」を参照し、VSP One SDS Block からダウングレード後のバージョンに対応した構成ファイルを取得します。

構成ファイルをエクスポートする際は、exportFileType パラメーターを省略するか、Normal を指定してください。

最新状態の構成ファイルを使用するために必ず取得してください。

- b. 「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する <<Cloud for Google Cloud>>」を参照し、構成ファイルを解凍して配置します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、ストレージクラスターが閉塞するなどの事態が起こるおそれがあります。

- c. クラウドリソースのバージョンを確認します。

Terraform の作業ディレクトリーで terraform output コマンドを実行します。

"TemplateVersion"キーの値を確認します。

```
terraform output
```

手順 8 で確認したストレージソフトウェアのバージョンとクラウドリソースのバージョンが一致している場合は、以上で手順は終了です。

- d. 構成ファイルをデプロイすることによる影響を確認します。

以下のコマンドを実行します。

```
terraform plan
```

コマンドを実行すると[Terraform will perform the following actions]という表示に続いてリソースに対する変更内容が表示されます。

以下のリソースの変更が実施されることを確認してください。

#	リソース種別	リソース操作	リソース名*	確認内容
1	google_compute_instance.instance[]	update in-place	<clusterName>-snXX	以下の項目に変更がある場合がありますが、問題ありません。 • metadata • deletion_protection

#	リソース種別	リソース操作	リソース名*	確認内容
2	Changes to Output	update in-place	なし	TemplateVersion がダウングレード後のバージョンに変更。 Changes to Output は最後に出力されます。
*リソース名の XX は、ストレージノードに割り振られている番号				

- e. terraform plan による確認で問題がなければ、以下のコマンドを実行します。

```
terraform apply
```

コマンドの実行後、[Enter a value:]と表示されたら[yes]を入力します。

入力すると最後に[Outputs]が出力されます。terraform apply が完了することで、クラウドリソースの変更が完了します。

32.10 ストレージソフトウェアをダウングレードする《Cloud for Microsoft Azure》

この節での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージソフトウェアを旧バージョンに更新できます。

ソフトウェアアップデート中に発生するストレージノード間でのストレージソフトウェアのバージョン混在は許容されます。バージョン混在中は、ダウングレード後のバージョンでの動作が保障されます。



メモ

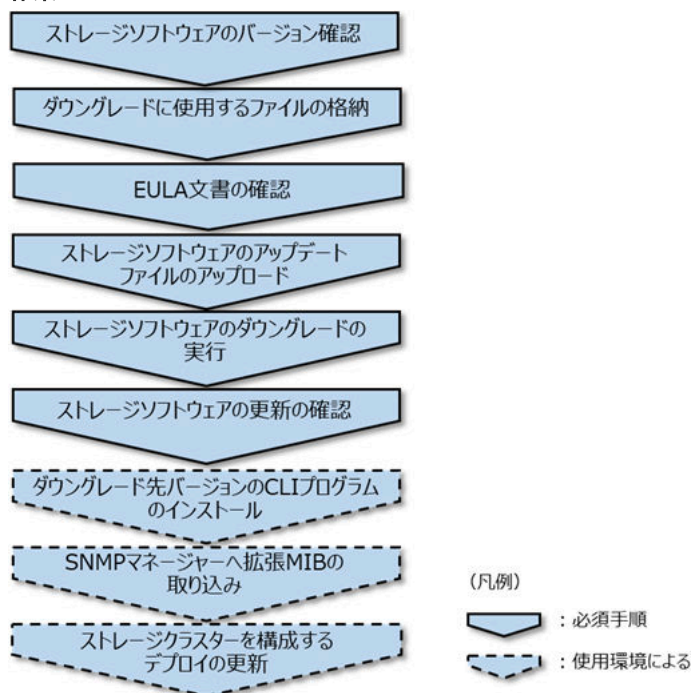
ダウングレード時のバージョン切り替えについて

- ストレージソフトウェアのバージョンが切り替わるのは、ソフトウェアアップデートの実行コマンドを投入した直後です。
このため、バージョンが切り替わるまでの、手順 1 から 6 までの REST API または CLI は、このマニュアルが対象とするバージョンに対応する「Hitachi Virtual Storage Platform One SDS Block REST API リファレンス」または「Hitachi Virtual Storage Platform One SDS Block CLI リファレンス」に従ってください。
- バージョンの切り替えと連動し、ストレージクラスターの動作が切り替わります。そのため、ダウングレード前の一部の機能(アップグレードによってこれまで使っていた新機能)が使用できなくなります。ダウングレードを実施する場合は、これら新機能を事前に無効化する必要があります。無効化を実施せずにダウングレードすると、イベントログ KARS10107-E が出力されソフトウェアアップデートは中止されます。
- ダウングレードを途中で中止したり、エラーによってダウングレードが中断されたりした場合に、アップデート以外の操作を実施する場合は、ストレージソフトウェアのバージョンに対応したマニュアルを参照して各操作を実施してください。

前提条件

- 実行に必要なロール : Service
- コントローラーノードで Azure CLI が実行できること

作業フロー



操作手順の留意事項

- ・ 手順 1 から 6 までは、コントローラーノードで実行する操作です。
- ・ 以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

操作手順

1. ストレージクラスターの情報を取得して、ストレージソフトウェアのバージョンを確認します。
REST API : GET /v1/objects/storage
CLI : storage_show
ソフトウェアダウングレードが必要な場合は、次の手順に進みます。
2. サポートセンターから以下のファイル入手して、コントローラーノードに格納します。
(入手するファイル)
次のファイルは、ダウングレード先のバージョンに合ったものを入手してください。
 - ・ hsd-update-**<version>**-**<number>**.tar
ストレージソフトウェアのアップデートファイルです。手順 1 で取得したストレージノードのバージョン aa.bb.cc.dd の dd 部分の数字と、ストレージソフトウェアのアップデートファイルの<version>の下 2 桁の数字が一致することを確認してください。一致しないストレージソフトウェアのアップデートファイルは使用しないでください。
(例)hsd-update-01000000-7070.tar
 - ・ EULA_for_SLE_for_StorageNode.txt
ストレージノードで使用している SUSE Linux Enterprise に関する EULA 文書です。
 - ・ EULA_for_SPDK.txt
ストレージノードで使用している Cavium SPDK FC Target Driver に関する EULA 文書です。
3. 格納した 2 つの EULA 文書の記載内容を確認します。

同意いただける場合は、次の手順に進みます。同意できない場合は、ソフトウェアのダウングレードを中止してください。

4. ジョブの情報を取得して、実行中のソフトウェアアップデートのジョブがないことを確認します。

REST API : GET /v1/objects/jobs

CLI : job_list

実行中のソフトウェアアップデートのジョブがない場合は、次の手順に進みます。



注意

ソフトウェアアップデートのジョブが実行中だったとき、以降の操作を行うと、実行中だったソフトウェアアップデートのジョブは失敗しますので注意してください。

5. ストレージソフトウェアのアップデートファイルをストレージクラスターにアップロードします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

ストレージクラスターに転送するストレージソフトウェアのアップデートファイルを指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/upload-software-update-file/invoke

CLI : storage_upload_software_update_file

実行結果は、コンソール上に出力されます。REST API では、HTTP ステータスコードとして 204 が、CLI ではメッセージとして"Completed."が、それぞれ返ったらアップロードは成功です。その際、イベントログは出力されません。



メモ

アップデートファイルのアップロード完了以降、ソフトウェアダウングレードの実行前までは、転送済みのソフトウェアアップデートファイルの情報を取得できます。操作方法は「転送済みのソフトウェアアップデートファイルの情報を取得する」を参照してください。

6. ストレージソフトウェアのダウングレードを実行します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

mode パラメーターと downgrade パラメーターを指定してコマンドを実行します。downgrade パラメーターには"true"を指定してください。downgrade パラメーターに"true"が指定されていない場合、ソフトウェアダウングレードは実行できません。

REST API : POST /v1/objects/storage/actions/update-software/invoke

CLI : storage_update_software

コマンド実行後に表示される、ジョブの ID を確認します。



注意

VSP One SDS Block Administrator を利用している場合は、手順 6 を実施後に、数秒待ってから以下を実施してください。

1. Web ブラウザーまたはタブをいったん閉じます。

2. Web ブラウザーのキャッシュをクリアします。

3. VSP One SDS Block Administrator を開き直して使用します。

また、VSP One SDS Block Administrator の Storage Cluster Information 画面の STORAGE SOFTWARE VERSION にエラーメッセージが表示されていないことを確認してください。表示されていた場合は、エラーメッセージに従って対処してください。

7. ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。



注意

- ソフトウェアダウングレードが KARS10109-E で失敗した場合は、他の競合するジョブが動作しているためソフトウェアダウングレードを実行できなかったことを意味しています。競合したジョブを中断するか、ジョブが完了するのをしばらく待ってから再実施してください。なお、当該メッセージで表示される競合ジョブの ID に、ストレージクラスターが内部で実行しているジョブの ID が表示されることがあります。ストレージクラスターが内部で実行しているジョブの state は参照できません。
- ソフトウェアアップデートが KARS10110-E で失敗した場合は、ストレージソフトウェアのアップデートファイルがストレージクラスターに存在していなかったことを意味しています。手順 5 でストレージソフトウェアのアップデートファイルのアップロードに成功している場合でも、以下のケースなどで KARS10110-E が出力される場合があります。その場合は手順 5 から再度実施してください。
 - ソフトウェアアップデート実施中にクラスターマスターノード(プライマリー)が障害を原因に閉塞した場合
 - ソフトウェアアップデート実施中にストレージクラスターの停止または電断があった場合

8. ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、ストレージクラスターの情報を取得して、ストレージソフトウェアが更新されたことを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

9. CLI を使用している場合は、ストレージソフトウェアのダウングレード先のバージョンに対応した CLI プログラムをコントローラーノードにインストールします。

CLI プログラムのインストール手順は、ダウングレード先のバージョンに対応した Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」に記載してある「VSP One SDS Block の CLI プログラムをインストールする」を参照してください。



メモ

ストレージソフトウェアより CLI プログラムのバージョンが古い状態で CLI を実行した場合、一致するバージョンまたは新しいバージョンへの更新を促す警告文が標準エラー出力に出力されます。

10. SNMP を利用している場合は、ストレージソフトウェアのダウングレードにあわせてダウングレード先のバージョンに合った拡張 MIB を SNMP マネージャーに取り込みます。

ダウングレード先のバージョンに対応した「オペレーションガイド」を参照し、「拡張 MIB の取り込み」に記載してある作業を実施します。

11. ストレージソフトウェアのダウングレードに合わせて、ストレージクラスターを構成するデプロイの更新を行います。

ただし、手順 8 で確認したストレージソフトウェアのバージョンとデプロイのバージョンが一致している場合は、本手順の実施は不要です。



メモ

デプロイのバージョンは以下のコマンドで確認できます。

```
az deployment group show ¥
--name mainTemplate ¥
```



```
--resource-group <リソースグループ名> ¥  
--query "properties.outputs.templateVersion.value"
```



注意

mainTemplate の templateVersion が確認できない場合は、Azure ポータル上でクラスター構築時に最初に作成されたデプロイ(InstallationStatus のデプロイより前にあるデプロイ)があるか確認してください。

クラスター構築時に最初に作成されたデプロイがある場合は、そのデプロイを--name に指定して templateVersion を確認してください。

クラスター構築時に最初に作成されたデプロイがない場合は、本手順を実施してください。

- a. 「構成ファイルをエクスポートする<<Cloud for Microsoft Azure>>」を参照し、VSP One SDS Block からダウングレード後のバージョンに対応した構成ファイルを取得します。
構成ファイルをエクスポートする際は、exportFileType パラメーターを省略するか、Normal を指定してください。
最新状態の構成ファイルを使用するために必ず取得してください。
- b. エクスポートした ConfigurationFiles_<YYYYMMDD>_<hhmmss>.tar.gz を解凍します。



注意

解凍した構成ファイルは、マニュアルによる指示がない限り絶対に編集しないでください。編集した場合、その後の操作が失敗するおそれがあります。

- c. 次の Azure CLI を実行して、デプロイの更新を行います。

```
az deployment group create ¥  
--name mainTemplate ¥  
--resource-group <作成したリソースグループ名> ¥  
--template-file VMConfigurationFile.json ¥  
--parameters @VMConfigurationFile.parameters.json
```



メモ

name は mainTemplate を指定してください。

- d. 次の Azure CLI を実行して、デプロイ結果が"Succeeded"であることを確認します。
"Running"の場合は、しばらくしてから再度次の Azure CLI を実行してください。

```
az deployment group show ¥  
--name mainTemplate ¥  
--resource-group <リソースグループ名> ¥  
--query "properties.provisioningState"
```

- e. 次の Azure CLI を実行して、デプロイのバージョンを確認し、ストレージソフトウェアのバージョンと同じであることを確認します。

```
az deployment group show ¥  
--name mainTemplate ¥  
--resource-group <リソースグループ名> ¥  
--query "properties.outputs.templateVersion.value"
```


32.11 ソフトウェアアップデートを中止する

実行中のストレージソフトウェアのアップデートを中止します。中止要求は即座に受け付けられますが、実際の処理は、中止要求のコマンドが実行された時点でアップデート中であったストレージノードのアップデート処理が完了したあとに中止されます。このため、中止要求を実行した場合、最後のストレージノードがアップデート処理中だったときは、アップデートは中止できません。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージノードの一覧を取得して、アップデート中のストレージノードの ID を記録します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
status が "NondisruptiveUpdating" であるストレージノードが、アップデート中のストレージノードです。
status が "NondisruptiveUpdating" となるストレージノードがない場合は、手順 3 に進みます。
2. アップデート中のストレージノードがクラスターマスターノード(プライマリー)でないことを確認します。
手順 1 で取得したストレージノードの ID を指定して「クラスターマスターノード(プライマリー)かを確認する」の手順を実施します。アップデート中のストレージノードがクラスターマスターノード(プライマリー)であった場合、手順 1 と手順 2 を再度実施して、アップデート中のストレージノードがクラスターマスターノード(プライマリー)でなくなるまで待ってください。
3. ストレージソフトウェアのアップデートの中止を要求します。
REST API : POST /v1/objects/storage/actions/stop-software-update/invoke
CLI : storage_stop_software_update
コマンド実行後に表示されるジョブの ID を確認します。
もし、手順 1 から 3 まで実施する間に、イベントログ KARS10100-I が出力された場合は、手順 1 からやり直してください。



注意

アップデートの中止を要求したあとに、ストレージクラスターを停止した場合(ストレージクラスターの電断障害からの再起動を含む)は、ストレージクラスターの再起動後に、もう一度、手順 3 を実施してください。

4. ジョブの state を確認します。
アップデートの中止を要求するジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId>
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
また、中止要求が完了した場合は affectedResources に中止対象のアップデート実行のジョブが返されます。
5. アップデート実行のジョブの state を確認します。

手順 4 で返された `affectedResources` を基に、アップデート実行のジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : `job_show`

`state` が `"Stopped"` になったらアップデート実行のジョブの中止は完了です。

6. ストレージクラスターの情報を取得して、ソフトウェアアップデートが中止されたことを確認します。

REST API : GET /v1/objects/storage

CLI : `storage_show`

`status` が `"NondisruptiveUpdating"` 以外になっていれば、ソフトウェアアップデートが中止されています。



注意

- ソフトウェアアップデートを中止後、再度ソフトウェアアップデートを実行する場合は「ストレージソフトウェアをアップグレードする<<Bare metal>>」または「ストレージソフトウェアをアップグレードする<<Cloud>>」、あるいは「ストレージソフトウェアをダウングレードする<<Bare metal>>」または「ストレージソフトウェアをダウングレードする<<Cloud>>」の EULA 文書の記載内容確認からそれぞれ実施してください。
- ソフトウェアアップデートを中止した場合、ソフトウェアアップデート中のストレージノードに対するリビルドが完了しないため、冗長度が低下した状態になる可能性があります。その場合、ソフトウェアアップデートを中止後、冗長度を回復するためにリビルドが動作します。この契機では通常リビルドが動作します。リビルドに掛かる時間は「リビルド完了までの時間(目安)」の通常リビルドの項目を参照してください。

32.12 転送済みのソフトウェアアップデートファイルの情報を取得する

ストレージクラスターに転送(アップロード)したストレージソフトウェアのアップデートファイルについて、以下の情報を取得します。

- `version` : ストレージソフトウェアのアップデートファイルのバージョン



メモ

この操作は、以下の手順の間に実施できる操作です。

- アップグレード時の、アップデートファイルのアップロード完了後からソフトウェアアップグレードの実行前までです。ソフトウェアアップグレードを実行すると情報は取得できません。
- ダウングレード時の、アップデートファイルのアップロード完了後からソフトウェアダウングレードの実行前までです。ソフトウェアダウングレードを実行すると情報は取得できません。

前提条件

- 実行に必要なロール : `Service`

操作手順

1. アップデートファイルの情報(バージョン)を取得します。
クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : GET /v1/objects/storage/software-update-file

CLI : `storage_software_update_file_show`

ストレージクラスターを起動/停止する

- 33.1 ストレージクラスターの起動/停止の概要
- 33.2 ストレージクラスターの起動
- 33.3 ストレージクラスターを強制起動する
- 33.4 ストレージクラスターの停止
- 33.5 ストレージクラスターの強制停止
- 33.6 ストレージクラスターの再起動

33.1 ストレージクラスターの起動/停止の概要

≪Bare metal≫ストレージクラスターの起動は、ストレージノードの電源オンで行います。

≪Cloud for AWS≫ストレージクラスターの起動は、EC2 インスタンスの開始で行います。

≪Cloud for Google Cloud≫ストレージクラスターの起動は、Compute Engine インスタンスの開始で行います。

≪Cloud for Microsoft Azure≫ストレージクラスターの起動は、Azure VM インスタンスの開始で行います。

ストレージクラスターの停止は、REST API または CLI で行います。

ストレージクラスターの停止時のパラメーター指定で、自動で再起動させることもできます。



メモ

VSP One SDS Block ではストレージノードの suspend/resume はサポートしていません。



注意

このマニュアルや「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」などのマニュアル、メッセージによる指示がない限りは、運用中にストレージノードに対する電源操作*を実施しないでください。指示がない契機での電源操作は、ストレージノードの障害やデータ消失につながる可能性があります。

* ≪Cloud for AWS≫AWS マネジメントコンソールを用いた電源操作を含みます。

* ≪Cloud for Google Cloud≫Google Cloud コンソールを用いた電源操作を含みます。

* ≪Cloud for Microsoft Azure≫Azure ポータルを用いた電源操作を含みます。

33.2 ストレージクラスターの起動

ストレージクラスターの起動方法について説明します。

33.2.1 ストレージクラスターを起動する≪Bare metal≫

この項での記述内容は Bare metal モデルに適用されます。

停止中のストレージクラスターを起動します。



ヒント

ストレージノードとして使用しているサーバーの BMC にて、複数のサーバーの電源操作をまとめて行うための機能が提供されている場合、その機能を使用することでストレージクラスターの起動を簡易化できます。複数のサーバーの電源操作をまとめて行うための機能については、使用しているハードウェアのマニュアルを参照してください。

前提条件

- 実行に必要なロール : Security、Storage、Monitor、Service、または Resource
-



注意

イベントログ KARS08124-C の対処としてストレージクラスターを起動する場合、イベントログ KARS08124-C で表示されたストレージノードに接続されている、ネットワークケーブルやネットワークスイッチの接続性に問題がないか確認してください。問題がある場合は、問題を解消したあとに以降の手順に進んでください。

KARS08124-C は、ストレージノードの障害発生によってストレージクラスターの動作継続が不可能となったことを示すイベントログです。接続されているネットワークケーブルやネットワークスイッチの異常が、当該ストレージノードの障害の原因となっているおそれがあります。

操作手順

1. スペアノードを登録している場合は、スペアノードの電源をオンにします。
電源オンの方法は、使用しているハードウェアのマニュアルを参照してください。
2. ストレージクラスターを構成するすべてのストレージノードの電源をオンにします。
電源オンの方法は、使用しているハードウェアのマニュアルを参照してください。
すべてのストレージノードの電源を遅滞なく(最初のストレージノードの電源オンと最後のストレージノードの電源オンが 7 分以内になるよう)オンにします。起動が遅滞したストレージノードがあった場合、イベントログ KARS08108-E が出力されます。この場合は、手順 4 に従って対処してください。
3. ストレージノードの起動時には、ストレージソフトウェアの診断機能が自動実行されます。診断の結果、ストレージソフトウェア起動に適さないと判定された場合は、障害内容と対処方法が提示されますので対処してください。
ストレージノードに異常がなければ、各ストレージノードのストレージソフトウェアが自動的に起動し、ストレージクラスターが構成されます。
全ストレージノードの電源オンからストレージクラスターの起動完了までに掛かる時間は以下のとおりです。
 - ・ 通常：約 20 分+UEFI ブート時間(目安：5～10 分)
 - ・ 最大：約 175 分+UEFI ブート時間(目安：5～10 分)UEFI ブート時間は、使用しているハードウェアや UEFI 設定(メモリーテストなどのブート時間最適化に関する設定)によって異なるため、使用しているハードウェアのマニュアルを参照してください。
4. 起動し忘れたストレージノードや起動が遅滞したストレージノードがあった場合、イベントログ KARS08108-E が出力され、ストレージクラスターの起動が抑止されることがあります。この場合は、メッセージの内容に従って対処します。
対処したことによって、KARS08108-E で示されたすべてのストレージノードの起動が確認された場合は、KARS08111-I が出力され、ストレージクラスターの起動が自動的に再開されます。



注意

- ・ 対処してから 30 分+UEFI ブート時間(目安：5～10 分)が経過しても、KARS08111-I が出力されない場合は、このマニュアルの「ストレージクラスターを強制起動する」に従って、ストレージクラスターを強制的に起動させることができます。
- ・ スペアノード使用時の注意
ストレージノード起動後、UEFI Shell 画面が表示されているストレージノードがあるかどうかを確認してください。UEFI Shell 画面が表示されている場合、該当のノードはスペアノード切り換えが行われたストレージノードです。その場合、以下の手順に従ってストレージクラスターを起動してください。
 1. 該当ストレージノードの物理サーバーを撤去します。ハードウェアベンダーのマニュアルを参照して実施してください。
撤去作業中に、期待外に OS が起動すると、ストレージノードに残っているネットワーク設定によって、IP アドレス重複などのトラブルを引き起こす可能性があります。そのため、撤去するストレージノードに対し、ネットワークからの切り離しを行ってください。
 2. 物理サーバーの撤去後、このマニュアルの「ストレージクラスターを強制起動する」に従ってストレージクラスターを強制起動させてください。

3. ストレージクラスター起動後に閉塞しているストレージノードが存在する場合は、
「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従ってストレージノードの回復を行ってください。
-

5. イベントログの一覧を取得して、ストレージクラスターの起動の完了を確認します。
イベントログ KARS08100-I の出力が確認できたら、ストレージクラスターの起動は完了です。
イベントログの一覧の取得方法は「イベントログの一覧を取得する」を参照してください。
6. ストレージクラスターの status が"Ready"であることを確認します。
REST API : GET /v1/objects/storage
CLI : storage_show
7. 容量削減機能を利用している場合は、イベントログの一覧を参照してストレージクラスターの起動後に容量削減機能が有効なボリュームのデータが保証されていない状態となっていないかを確認します。
イベントログ KARS06201-E、KARS06220-C、KARS06221-C、または KARS06222-C が出ている場合は、容量削減機能が有効なボリュームのデータが消失している可能性があります。すべてのストレージノードに対しダンプログファイルを採取し、サポートセンターに連絡してください。
8. スナップショットを利用している場合は、イベントログの一覧を参照して、ストレージクラスターの起動後にスナップショットボリュームのデータが消失していないかを確認します。
ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した場合、キャッシュ保護付きライトバックモード無効時は、スナップショットボリュームのデータが消失することがあります。キャッシュ保護付きライトバックモード有効時は、スナップショットボリュームのデータは保護されます。ただし、キャッシュ保護用メタデータの冗長度を超える障害が発生している状態で、ストレージクラスターの障害が発生した場合は、キャッシュ保護付きライトバックモード有効時でも、スナップショットボリュームのデータは保護されません。
イベントログ KARS06132-C が出ている場合は、スナップショットボリュームのデータが消失しています。「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ストレージクラスター起動時に KARS06132-C が発生した場合の対処」に従って対処してください。
-



メモ

ストレージクラスター起動後の VSP One SDS Block Administrator において、以下の情報がダッシュボード画面に表示されますが、この情報からストレージクラスターの起動状態を判断することはできません。

- ・ リソースのヘルスステータス
- ・ ナビゲーションバーのヘルスステータスサマリー

ストレージクラスターの起動状態は、手順 6 に記載のとおり、ストレージクラスターの情報 (status) から判断してください。

33.2.2 ストレージクラスターを起動する《Cloud for AWS》

この項での記述内容は Cloud モデル for AWS に適用されます。

停止中のストレージクラスターを起動します。

前提条件

- ・ 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource



注意

- ・ イベントログ KARS08124-C の対処としてストレージクラスターを起動する場合、イベントログ KARS08124-C で表示されたストレージノードとのノード間通信の接続性が失われているような異常が発生していないか「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」を参照して確認してください。問題があった場合は、問題を解消したあとに以降の手順に進んでください。KARS08124-C は、ストレージノードの障害発生によってストレージクラスターの動作継続が不可能になったことを示すイベントログです。当該ストレージノードとのノード間通信の接続性異常が、当該ストレージノードの障害の原因になっているおそれがあります。
- ・ EBS 暗号化を利用している場合は、AWS を操作するアカウントやコントローラーノードに設定する IAM ロールに、AWS Key Management Service へアクセスするための権限を追加する必要があります。詳細は、AWS のユーザーガイドを参照してください。

操作手順

1. AWS マネジメントコンソールを操作して、ストレージクラスターを構成するすべての EC2 インスタンスを遅滞なく(最初の EC2 インスタンスの開始と最後の EC2 インスタンスの開始が 7 分以内になるよう)開始します。

開始が遅滞した EC2 インスタンスがあった場合、イベントログ KARS08108-E が出力されます。この場合は、手順 3 に従って対処してください。

EC2 インスタンスの開始方法は、AWS のマニュアルを参照してください。

2. EC2 インスタンスの起動時には、ストレージソフトウェアの診断機能が自動実行されます。診断の結果、ストレージソフトウェア起動に適さないと判定された場合は、障害内容と対処方法が提示されますので対処してください。

ストレージノードに異常がなければ、各ストレージノードのストレージソフトウェアが自動的に起動し、ストレージクラスターが構成されます。

全 EC2 インスタンスの開始からストレージクラスターの起動完了までに掛かる時間は以下のとおりです。

- ・ 通常 : 約 20 分
- ・ 最大 : 約 175 分

3. 起動し忘れた EC2 インスタンスや起動が遅滞した EC2 インスタンスがあった場合、イベントログ KARS08108-E が出力され、ストレージクラスターの起動が抑止されることがあります。この場合は、メッセージの内容に従って対処します。

対処したことによって、KARS08108-E で示されたすべての EC2 インスタンスの起動が確認された場合は、KARS08111-I が出力され、ストレージクラスターの起動が自動的に再開されます。



注意

対処してから約 30 分が経過しても、KARS08111-I が出力されない場合は、このマニュアルの「ストレージクラスターを強制起動する」に従って、ストレージクラスターを強制的に起動させることができます。

4. イベントログの一覧を取得して、ストレージクラスターの起動の完了を確認します。
イベントログ KARS08100-I の出力が確認できたら、ストレージクラスターの起動は完了です。
イベントログの一覧の取得方法は「イベントログの一覧を取得する」を参照してください。

5. ストレージクラスターの status が "Ready"であることを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

6. 容量削減機能を利用している場合は、イベントログの一覧を参照してストレージクラスターの起動後に容量削減機能が有効なボリュームのデータが保証されていない状態となっていないかを確認します。

イベントログ KARS06201-E、KARS06220-C、KARS06221-C、または KARS06222-C が出ている場合は、容量削減機能が有効なボリュームのデータが消失している可能性があります。すべてのストレージノードに対しダンプログファイルを採取し、サポートセンターに連絡してください。

7. スナップショットを利用している場合は、イベントログの一覧を参照して、ストレージクラスターの起動後にスナップショットボリュームのデータが消失していないかを確認します。

ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した場合、キャッシュ保護付きライトバックモード無効時は、スナップショットボリュームのデータが消失することがあります。キャッシュ保護付きライトバックモード有効時は、スナップショットボリュームのデータは保護されます。ただし、キャッシュ保護用メタデータの冗長度を超える障害が発生している状態で、ストレージクラスターの障害が発生した場合は、キャッシュ保護付きライトバックモード有効時でも、スナップショットボリュームのデータは保護されません。

イベントログ KARS06132-C が出ている場合は、スナップショットボリュームのデータが消失しています。「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ストレージクラスター起動時に KARS06132-C が発生した場合の対処」に従って対処してください。



メモ

ストレージクラスター起動後の VSP One SDS Block Administrator において、以下の情報がダッシュボード画面に表示されますが、この情報からストレージクラスターの起動状態を判断することはできません。

- ・ リソースのヘルスステータス
- ・ ナビゲーションバーのヘルスステータスサマリー

ストレージクラスターの起動状態は、手順 5 に記載のとおり、ストレージクラスターの情報 (status) から判断してください。

33.2.3 ストレージクラスターを起動する《Cloud for Google Cloud》

この項での記述内容は Cloud モデル for Google Cloud に適用されます。

停止中のストレージクラスターを起動します。

前提条件

- ・ 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource



注意

イベントログ KARS08124-C の対処としてストレージクラスターを起動する場合、イベントログ KARS08124-C で表示されたストレージノードとのノード間通信の接続性が失われているような異常が発生していないか「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」を参照して確認してください。問題があった場合は、問題を解消したあと以降の手順に進んでください。KARS08124-C は、ストレージノードの障害発生によってストレージクラスターの動作継続が不可能になったことを示すイベントログです。当該ストレージノードとのノード間通信の接続性異常が、当該ストレージノードの障害の原因になっているおそれがあります。

操作手順

1. Google Cloud コンソールを操作して、ストレージクラスターを構成するすべての Compute Engine インスタンスを遅滞なく(最初の Compute Engine インスタンスの開始と最後の Compute Engine インスタンスの開始が 7 分以内になるよう)開始します。

開始が遅滞した Compute Engine インスタンスがあった場合、イベントログ KARS08108-E が出力されます。この場合は、手順 3 に従って対処してください。

Compute Engine インスタンスの開始方法は、Google Cloud のマニュアルを参照してください。

2. Compute Engine インスタンスの起動時には、ストレージソフトウェアの診断機能が自動実行されます。診断の結果、ストレージソフトウェア起動に適さないと判定された場合は、障害内容と対処方法が提示されますので対処してください。

ストレージノードに異常がなければ、各ストレージノードのストレージソフトウェアが自動的に起動し、ストレージクラスターが構成されます。

全 Compute Engine インスタンスの開始からストレージクラスターの起動完了までに掛かる時間は以下のとおりです。

- ・ 通常：約 20 分
- ・ 最大：約 175 分

3. 起動し忘れた Compute Engine インスタンスや起動が遅滞した Compute Engine インスタンスがあった場合、イベントログ KARS08108-E が出力され、ストレージクラスターの起動が抑止されることがあります。この場合は、メッセージの内容に従って対処します。

対処したことによって、KARS08108-E で示されたすべての Compute Engine インスタンスの起動が確認された場合は、KARS08111-I が出力され、ストレージクラスターの起動が自動的に再開されます。



注意

対処してから約 30 分が経過しても、KARS08111-I が出力されない場合は、このマニュアルの「ストレージクラスターを強制起動する」に従って、ストレージクラスターを強制的に起動させることができます。

4. イベントログの一覧を取得して、ストレージクラスターの起動の完了を確認します。
イベントログ KARS08100-I の出力が確認できたら、ストレージクラスターの起動は完了です。
イベントログの一覧の取得方法は「イベントログの一覧を取得する」を参照してください。

5. ストレージクラスターの status が"Ready"であることを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

6. 容量削減機能を利用している場合は、イベントログの一覧を参照してストレージクラスターの起動後に容量削減機能が有効なボリュームのデータが保証されていない状態となっていないかを確認します。

イベントログ KARS06201-E、KARS06220-C、KARS06221-C、または KARS06222-C が出ている場合は、容量削減機能が有効なボリュームのデータが消失している可能性があります。すべてのストレージノードに対しダンプログファイルを採取し、サポートセンターに連絡してください。

7. スナップショットを利用している場合は、イベントログの一覧を参照して、ストレージクラスターの起動後にスナップショットボリュームのデータが消失していないかを確認します。

ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した場合、キャッシュ保護付きライトバックモード無効時は、スナップショットボリュームのデータが消失することがあります。キャッシュ保護付きライトバックモード有効時は、スナップショットボリュームのデータは保護されます。ただし、キャッシュ保護用メタデータの冗長度を超える障害が発生している状態で、ストレージクラスターの障害が発生した場合は、キャッシュ保護付きライトバックモード有効時でも、スナップショットボリュームのデータは保護されません。

イベントログ KARS06132-C が出ている場合は、スナップショットボリュームのデータが消失しています。「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド

ド」の「ストレージクラスター起動時に KARS06132-C が発生した場合の対処」に従って対処してください。



メモ

ストレージクラスター起動後の VSP One SDS Block Administrator において、以下の情報がダッシュボード画面に表示されますが、この情報からストレージクラスターの起動状態を判断することはできません。

- ・ リソースのヘルスステータス
 - ・ ナビゲーションバーのヘルスステータスサマリー
- ストレージクラスターの起動状態は、手順 5 に記載のとおり、ストレージクラスターの情報 (status) から判断してください。

33.2.4 ストレージクラスターを起動する《Cloud for Microsoft Azure》

この項での記述内容は Cloud モデル for Microsoft Azure に適用されます。

停止中のストレージクラスターを起動します。

前提条件

- ・ 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource



注意

イベントログ KARS08124-C の対処としてストレージクラスターを起動する場合、イベントログ KARS08124-C で表示されたストレージノードとのノード間通信の接続性が失われているような異常が発生していないか「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」を参照して確認してください。問題があった場合は、問題を解消したあとに以降の手順に進んでください。KARS08124-C は、ストレージノードの障害発生によってストレージクラスターの動作継続が不可能になったことを示すイベントログです。当該ストレージノードとのノード間通信の接続性異常が、当該ストレージノードの障害の原因になっているおそれがあります。

操作手順

1. Azure ポータルを操作して、ストレージクラスターを構成するすべての Azure VM インスタンスを遅滞なく(最初の Azure VM インスタンスの開始と最後の Azure VM インスタンスの開始が 7 分以内になるよう)開始します。

開始が遅滞した Azure VM インスタンスがあった場合、イベントログ KARS08108-E が出力されます。この場合は、手順 3 に従って対処してください。

Azure VM インスタンスの開始方法は、Microsoft Azure のマニュアルを参照してください。

2. Azure VM インスタンスの起動時には、ストレージソフトウェアの診断機能が自動実行されます。診断の結果、ストレージソフトウェア起動に適さないと判定された場合は、障害内容と対処方法が提示されますので対処してください。

ストレージノードに異常がなければ、各ストレージノードのストレージソフトウェアが自動的に起動し、ストレージクラスターが構成されます。

全 Azure VM インスタンスの開始からストレージクラスターの起動完了までに掛かる時間は以下のとおりです。

- ・ 通常 : 約 20 分
- ・ 最大 : 約 175 分

3. 起動し忘れた Azure VM インスタンスや起動が遅滞した Azure VM インスタンスがあった場合、イベントログ KARS08108-E が出力され、ストレージクラスターの起動が抑止されることがあります。この場合は、メッセージの内容に従って対処します。

対処したことによって、KARS08108-E で示されたすべての Azure VM インスタンスの起動が確認された場合は、KARS08111-I が出力され、ストレージクラスターの起動が自動的に再開されます。



注意

対処してから約 30 分が経過しても、KARS08111-I が出力されない場合は、このマニュアルの「ストレージクラスターを強制起動する」に従って、ストレージクラスターを強制的に起動させることができます。

4. イベントログの一覧を取得して、ストレージクラスターの起動の完了を確認します。
イベントログ KARS08100-I の出力が確認できたら、ストレージクラスターの起動は完了です。
イベントログの一覧の取得方法は「イベントログの一覧を取得する」を参照してください。

5. ストレージクラスターの status が "Ready" であることを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

6. 容量削減機能を利用している場合は、イベントログの一覧を参照してストレージクラスターの起動後に容量削減機能が有効なボリュームのデータが保証されていない状態となっていないかを確認します。

イベントログ KARS06201-E、KARS06220-C、KARS06221-C、または KARS06222-C が出ている場合は、容量削減機能が有効なボリュームのデータが消失している可能性があります。すべてのストレージノードに対しダンプログファイルを採取し、サポートセンターに連絡してください。

7. スナップショットを利用している場合は、イベントログの一覧を参照して、ストレージクラスターの起動後にスナップショットボリュームのデータが消失していないかを確認します。

ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した場合、キャッシュ保護付きライトバックモード無効時は、スナップショットボリュームのデータが消失することがあります。キャッシュ保護付きライトバックモード有効時は、スナップショットボリュームのデータは保護されます。ただし、キャッシュ保護用メタデータの冗長度を超える障害が発生している状態で、ストレージクラスターの障害が発生した場合は、キャッシュ保護付きライトバックモード有効時でも、スナップショットボリュームのデータは保護されません。

イベントログ KARS06132-C が出ている場合は、スナップショットボリュームのデータが消失しています。「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ストレージクラスター起動時に KARS06132-C が発生した場合の対処」に従って対処してください。



メモ

ストレージクラスター起動後の VSP One SDS Block Administrator において、以下の情報がダッシュボード画面に表示されますが、この情報からストレージクラスターの起動状態を判断することはできません。

- ・ リソースのヘルスステータス
- ・ ナビゲーションバーのヘルスステータスサマリー

ストレージクラスターの起動状態は、手順 5 に記載のとおり、ストレージクラスターの情報 (status) から判断してください。

33.3 ストレージクラスターを強制起動する

ストレージクラスターの起動が抑止された状態から、ストレージクラスターを強制的に起動させます。ストレージクラスターの強制起動操作を実施した場合、起動していないストレージノードは自動的に閉塞されて、ストレージクラスターの起動が行われます。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージクラスターの情報を取得します。

REST API : GET /v1/objects/storage

CLI : storage_show

ストレージクラスターの status が "StartFailed" のとき、次の手順に進みます。

2. ストレージクラスターを強制起動します。

パラメーターを指定せずにコマンドを実行します。

コマンドは、ストレージクラスターの代表 IP アドレス(またはそれに対応したホスト名)に対して、またはコマンド実行後にイベントログ KARS08108-E で指定されることがないストレージノードに対して実行してください。

REST API : POST /v1/objects/storage/actions/resume-suppressed-start-processing/invoke

CLI : storage_resume_suppressed_start_processing

ストレージクラスターの強制起動操作によって、ストレージクラスターの起動が再開された場合は、イベントログ KARS08111-I が出力されます。ストレージクラスターの強制起動操作から約 12 分、最大 65 分でストレージクラスターの起動は完了します。

3. イベントログの一覧を取得して、ストレージクラスターの起動の完了を確認します。

イベントログ KARS08100-I の出力が確認できたら、ストレージクラスターの起動は完了です。

イベントログの一覧の取得方法は「イベントログの一覧を取得する」を参照してください。

4. ストレージクラスターの status が "Ready" であることを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

5. 容量削減機能を利用している場合は、イベントログの一覧を参照してストレージクラスターの起動後に容量削減機能が有効なボリュームのデータが保証されていない状態となっていないかを確認します。

イベントログ KARS06201-E、KARS06220-C、KARS06221-C、または KARS06222-C が出ている場合は、容量削減機能が有効なボリュームのデータが消失している可能性があります。すべてのストレージノードに対しダンプログファイルを採取し、サポートセンターに連絡してください。

6. スナップショットを利用している場合は、イベントログの一覧を参照して、ストレージクラスターの起動後にスナップショットボリュームのデータが消失していないかを確認します。

ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した場合、キャッシュ保護付きライトバックモード無効時は、スナップショットボリュームのデータが消失することがあります。キャッシュ保護付きライトバックモード有効時は、スナップショットボリュームのデータは保護されます。ただし、キャッシュ保護用メタデータの冗長度を超える障害が発生している状態で、ストレージクラスターの障害が発生した場合は、キャッ

シュ保護付きライトバックモード有効時でも、スナップショットボリュームのデータは保護されません。

イベントログ KARS06132-C が出ている場合は、スナップショットボリュームのデータが消失しています。

「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「ストレージクラスター起動時に KARS06132-C が発生した場合の対処」に従って対処してください。



メモ

ストレージクラスター起動後の VSP One SDS Block Administrator において、以下の情報がダッシュボード画面に表示されますが、この情報からストレージクラスターの起動状態を判断することはできません。

- リソースのヘルスステータス
 - ナビゲーションバーのヘルスステータスサマリー
- ストレージクラスターの起動状態は、手順 4 に記載のとおり、ストレージクラスターの情報 (status) から判断してください。

33.4 ストレージクラスターの停止

ストレージクラスターの停止方法について説明します。

33.4.1 ストレージクラスターを停止する《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

ストレージクラスターを停止します。



注意

- ユーザー操作を実施中のときは、ストレージクラスターは停止できません(停止操作はキャンセルされます)。ユーザー操作の完了を確認してから、ストレージクラスターの停止を実行してください。ただし、以下のユーザー操作については、実施中の場合でもストレージクラスターは停止できます。ストレージクラスターを停止した場合、実施中のユーザー操作は中断されることがあります。中断されたユーザー操作は、ストレージクラスターを再起動したあと「ジョブの情報を個別に取得する」を参照しジョブの情報を取得して、対処してください。
 - ストレージプールの拡張
 - ボリュームの作成
 - ボリュームの削除
 - ボリュームの設定編集
 - ボリュームとコンピュータノードの接続
 - ボリュームとコンピュータノードの接続を解除
- ストレージクラスターを停止した場合、以下が処理中だったとき、それらの処理は中断されることがあります。中断された処理は、ストレージクラスターの再起動後に再開されます。
 - リビルド
 - ドライブデータ再配置
 - 容量バランス
 - ストレージコントローラーの容量追加
 - ストレージコントローラー単位に管理するユーザーデータ容量に対する平準化処理
 - スナップショットのリストア
 - スナップショットボリュームの削除

- ストレージノードの自動回復による保守回復ジョブまたは交換ジョブが動作している場合、ストレージクラスターは停止できません(停止操作はキャンセルされます)。
「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「競合する処理による操作失敗への対処」に記載されている内容を参照し、実行中の保守回復ジョブまたは交換ジョブが完了するのを待ってから、ストレージクラスターの停止を実行してください。
- Universal Replicator 機能を使用中にストレージクラスターを停止する場合は、「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」の「計画的にストレージシステムを停止、再開する」を参照してください。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージクラスターの情報を取得します。
REST API : GET /v1/objects/storage
CLI : storage_show
ストレージクラスターの status が "Ready" のとき、次の手順に進みます。
2. ストレージクラスターを停止します。
パラメーターを指定せずにコマンドを実行します。
REST API : POST /v1/objects/storage/actions/shutdown/invoke
CLI : storage_shutdown
ストレージクラスターの停止が完了するまでの時間は約 20 分、最大約 90 分です。
3. ストレージノードの電源がオフになったことを確認します。
電源状態の確認方法は、ハードウェアのマニュアルを参照してください。



注意

この手順によってストレージノードが停止した状態で、FCHBA またはディスクコントローラーの交換または構成変更を行わないでください。FCHBA またはディスクコントローラーの交換または構成変更する場合には、ストレージノードの保守閉塞によってストレージノードを停止させてから実施してください。

4. スペアノードを登録している場合は、OS のシャットダウン操作によってスペアノードの停止を行ってください。
OS のシャットダウンは、ハードウェアのマニュアルを参照してください。
OS のシャットダウン操作後、約 5 分経過しても停止できない場合は、強制停止操作によってスペアノードの停止を行ってください。強制停止の操作方法は、ハードウェアのマニュアルを参照してください。
日立アドバンスサーバ HA8000V シリーズを使用している場合、OS のシャットダウンは、iLO の「電力管理」にて「瞬間的に押す」による停止になります。また、強制停止は、iLO の「電力管理」にて「押し続ける」による停止になります。具体的な操作方法はハードウェアのマニュアルを参照してください。日立アドバンスサーバ HA8000V シリーズ以外の物理サーバーを使用している場合、OS のシャットダウン、強制停止の具体的な操作方法は、各ハードウェアのマニュアルを参照してください。

33.4.2 ストレージクラスターを停止する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ストレージクラスターを停止します。



注意

- ユーザー操作を実施中のときは、ストレージクラスターは停止できません(停止操作はキャンセルされます)。ユーザー操作の完了を確認してから、ストレージクラスターの停止を実行してください。
ただし、以下のユーザー操作については、実施中の場合でもストレージクラスターは停止できます。ストレージクラスターを停止した場合、実施中のユーザー操作は中断されることがあります。中断されたユーザー操作は、ストレージクラスターを再起動したあと「ジョブの情報を個別に取得する」を参照しジョブの情報を取得して、対処してください。
 - ストレージプールの拡張
 - ボリュームの作成
 - ボリュームの削除
 - ボリュームの設定編集
 - ボリュームとコンピュータノードの接続
 - ボリュームとコンピュータノードの接続を解除
- ストレージクラスターを停止した場合、以下が処理中だったとき、それらの処理は中断されることがあります。中断された処理は、ストレージクラスターの再起動後に再開されます。
 - リビルド
 - 容量バランス
 - ストレージコントローラーの容量追加
 - ストレージコントローラー単位に管理するユーザーデータ容量に対する平準化処理
 - スナップショットのリストア
 - スナップショットボリュームの削除
- ストレージノードの自動回復による保守回復ジョブまたは交換ジョブが動作している場合、ストレージクラスターは停止できません(停止操作はキャンセルされます)。
「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「競合する処理による操作失敗への対処」に記載されている内容を参照し、実行中の保守回復ジョブまたは交換ジョブが完了するのを待ってから、ストレージクラスターの停止を実行してください。
- Universal Replicator 機能を使用中にストレージクラスターを停止する場合は、「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」の「計画的にストレージシステムを停止、再開する」を参照してください。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージクラスターの情報を取得します。
REST API : GET /v1/objects/storage
CLI : storage_show
ストレージクラスターの status が"Ready"のとき、次の手順に進みます。
2. ストレージクラスターを停止します。
パラメーターを指定せずにコマンドを実行します。
REST API : POST /v1/objects/storage/actions/shutdown/invoke
CLI : storage_shutdown
ストレージクラスターの停止が完了するまでの時間は約 20 分、最大約 90 分です。
3. 以下を確認します。
 - <<Cloud for AWS>>

AWS マネジメントコンソールから、EC2 インスタンスが停止されたことを確認してください。



注意

ストレージクラスターの停止が完了する前にロードバランサーからストレージノードの EC2 インスタンスには通信ができなくなるため、ロードバランサー経由で停止処理の完了を確認することはできません。また、停止しているストレージノードに対してコントローラーノードからロードバランサー経由でアクセスしようとしても、ロードバランサーからストレージノードへの通信ができないためエラーとなります。

- <<Cloud for Google Cloud>>

Google Cloud コンソールから、Compute Engine インスタンスが停止されたことを確認してください。



注意

ストレージクラスターの停止が完了する前にロードバランサーからストレージノードの Compute Engine インスタンスには通信ができなくなるため、ロードバランサー経由で停止処理の完了を確認することはできません。また、停止しているストレージノードに対してコントローラーノードからロードバランサー経由でアクセスしようとしても、ロードバランサーからストレージノードへの通信ができないためエラーとなります。

- <<Cloud for Microsoft Azure>>

Azure ポータルから、Azure VM インスタンスが停止されたことを確認してください。



注意

- ストレージクラスターの停止が完了する前にロードバランサーからストレージノードの Azure VM インスタンスには通信ができなくなるため、ロードバランサー経由で停止処理の完了を確認することはできません。また、停止しているストレージノードに対してコントローラーノードからロードバランサー経由でアクセスしようとしても、ロードバランサーからストレージノードへの通信ができないためエラーとなります。
- Azure VM インスタンスが停止されたことを確認する際、Azure ポータルで、Azure VM インスタンスの状態が「停止済み(割り当て解除)」となっていることを確認してください。「停止済み(割り当て解除)」になっていない場合は、Azure ポータルから該当の Azure VM インスタンスを停止し、「停止済み(割り当て解除)」にしてください。Microsoft Azure では、Azure VM インスタンスの状態が「停止済み」の場合、Azure VM インスタンスの課金状態が継続されます。「停止済み(割り当て解除)」の場合は課金状態が継続されません(ディスクの課金状態は継続されます)。停止方法は、Microsoft Azure のマニュアルを確認してください。

33.5 ストレージクラスターの強制停止

ストレージクラスターを強制停止する方法について説明します。

33.5.1 ストレージクラスターを強制停止する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージクラスターを強制的に停止させます。



注意

- この操作は、マニュアルやメッセージ、または保守員から、実施するよう誘導された場合に限って実施してください。
- 構成情報の変更・設定時のトラブルシューティングで強制停止を実施する場合、手順内で実施するストレージクラスター情報取得の REST API または CLI と、ストレージクラスターの強制停止の REST API または CLI がエラーになることがあります。その場合は、すべてのストレージノードの管理ネットワークが正常かを確認してください。管理ネットワークに問題がない場合は、OS のシャットダウン操作によってストレージノードを停止してください。OS のシャットダウン操作後、約 5 分経過しても停止できない場合は、強制停止操作によってストレージノードを停止してください。
ストレージノードとして使用しているサーバーの BMC にて、複数のサーバーの電源操作をまとめて行うための機能が提供されている場合、その機能を使用することで OS のシャットダウンまたは強制停止によるストレージノードの停止操作を簡易化できます。



メモ

OS のシャットダウン操作、強制停止の操作、複数のサーバーの電源操作をまとめて行うための機能については、使用しているハードウェアのマニュアルを参照してください。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージクラスターの情報を取得します。

REST API : GET /v1/objects/storage

CLI : storage_show

正常にストレージクラスターの情報が表示されることを確認してください。



注意

- すべてのクラスターマスターノードに対して実行しても、ストレージクラスターの情報が取得できない場合、異常が発生している可能性があります。



メモ

ストレージクラスターの代表 IP アドレスを設定している場合、ストレージクラスターの代表 IP アドレスは使用せずに各クラスターマスターノードに割り当てている IP アドレス、またはそれらの FQDN に対して実行してください。

- エラーメッセージが出力された場合は、エラーメッセージに従って対処してください。
- 次に示す時間が経過してもストレージクラスターの情報が取得できない、または HTTP ステータスコード 500 が返る場合は対処が必要です。
30 分+UEFI ブート時間(目安 : 5~10 分)
「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「最初にチェックする項目」の「VSP One SDS Block を構成する管理ネットワーク、コンピュータネットワーク、ストレージノード間ネットワーク、BMC ネットワークはすべて正常に動作していますか。」に従ってネットワークの状態を確認し、異常がある場合は解決してください。解決後、再度手順 1 から実施してください。
- ネットワークに問題がなく、30 分+UEFI ブート時間(目安 : 5~10 分)以上経過してもストレージクラスターの情報が取得できない場合は、OS のシャットダウン操作によってストレージノードを停止してください。
OS のシャットダウン操作後、約 5 分経過しても停止できない場合は、強制停止操作によってストレージノードの停止を行ってください。

ストレージノードとして使用しているサーバーの BMC にて、複数のサーバーの電源操作をまとめて行うための機能が提供されている場合、その機能を使用することで OS のシャットダウンまたは強制停止によるストレージノードの停止操作を簡易化できます。

メモ

- OS のシャットダウン操作、強制停止の操作、複数のサーバーの電源操作をまとめて行うための機能については、使用しているハードウェアのマニュアルを参照してください。
- 
- 日立アドバンストサーバ HA8000V シリーズを使用している場合、OS のシャットダウンは、iLO の「電力管理」にて「瞬間的に押す」による停止となります。また、強制停止は、iLO の「電力管理」にて「押し続ける」による停止となります。具体的な操作方法是ハードウェアのマニュアルを参照してください。日立アドバンストサーバ HA8000V シリーズ以外の物理サーバーを使用している場合、OS のシャットダウン、強制停止の具体的な操作方法是、各ハードウェアのマニュアルを参照してください。
-

2. ストレージクラスターの強制停止を実施します。

"force"パラメーターを"true"に指定して、ストレージクラスターの代表 IP アドレスまたはクラスターマスターノード(プライマリー)の IP アドレス、あるいはそれらの FQDN に対してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/shutdown/invoke

CLI : storage_shutdown

3. ストレージノードの電源がオフになったことを確認します。電源状態の確認方法は、ハードウェアのマニュアルを参照してください。



注意

- 約 20 分経過してもストレージノードが停止していない場合、OS のシャットダウン操作によってストレージノードの停止を行ってください。その際すべてのストレージノードを、できるだけ同時にシャットダウンするようにしてください。

OS のシャットダウン操作後、約 5 分経過しても停止できない場合は、強制停止操作によってストレージノードの停止を行ってください。

ストレージノードとして使用しているサーバーの BMC にて、複数のサーバーの電源操作をまとめて行うための機能が提供されている場合、その機能を使用することで OS のシャットダウンまたは強制停止によるストレージノードの停止操作を簡易化できます。

メモ

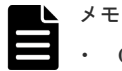


OS のシャットダウン操作、強制停止の操作、複数のサーバーの電源操作をまとめて行うための機能については、使用しているハードウェアのマニュアルを参照してください。

- ストレージノードが停止した状態で、FCHBA またはディスクコントローラーの交換または構成変更を行わないでください。
-

4. スペアノードを登録している場合は、OS のシャットダウン操作によってスペアノードの停止を行ってください。

OS のシャットダウン操作後、約 5 分経過しても停止できない場合は、強制停止操作によってスペアノードの停止を行ってください。



メモ

- OS のシャットダウン、強制停止の操作は、ハードウェアのマニュアルを参照してください。
- 日立アドバンストサーバ HA8000V シリーズを使用している場合、OS のシャットダウンは、iLO の「電力管理」にて「瞬間的に押す」による停止になります。また、強制停止は、iLO の「電力管理」にて「押し続ける」による停止になります。具体的な操作方法はハードウェアのマニュアルを参照してください。日立アドバンストサーバ HA8000V シリーズ以外の物理サーバーを使用している場合、OS のシャットダウン、強制停止の具体的な操作方法は、各ハードウェアのマニュアルを参照してください。

33.5.2 ストレージクラスターを強制停止する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ストレージクラスターを強制的に停止させます。



注意

この操作は、マニュアルやメッセージ、または保守員から、実施するよう誘導された場合に限り実施してください。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージクラスターの情報を取得します。

REST API : GET /v1/objects/storage

CLI : storage_show

正常にストレージクラスターの情報が表示されることを確認してください。



注意

- すべてのクラスターマスターノードに対して実行しても、ストレージクラスターの情報が取得できない場合、異常が発生している可能性があります。
- エラーメッセージが出力された場合は、エラーメッセージに従って対処してください。
- 30 分以上経過してもストレージクラスターの情報が取得できない、または HTTP ステータスコード 500 が返る場合は対処が必要です。
- <<Cloud for AWS>> ネットワークに問題がなく、30 分以上経過してもストレージクラスターの情報が取得できない場合は、EC2 インスタンスの停止操作によって EC2 インスタンスを停止してください。
EC2 インスタンスの停止操作後、約 5 分経過しても停止できない場合は、強制停止操作によって EC2 インスタンスの停止を行ってください。強制停止は、AWS マネジメントコンソールの EC2 インスタンスの停止操作で停止してください。



メモ

EC2 インスタンスの強制停止は、EC2 インスタンスが停止中(stopping)の状態のまのときに再度 EC2 インスタンスの停止操作を行うことで実行できます。詳しい操作方法は AWS のマニュアルを参照してください。

- <<Cloud for Google Cloud>>ネットワークに問題がなく、30 分以上経過してもストレージクラスターの情報が取得できない場合は、Compute Engine インスタンスの停止操作によって Compute Engine インスタンスを停止してください。
Compute Engine インスタンスの停止操作を行っても停止されない場合は、約 90 秒後に Google Cloud によって自動的に強制停止されます。
- <<Cloud for Microsoft Azure>>ネットワークに問題がなく、30 分以上経過してもストレージクラスターの情報が取得できない場合は、Azure VM インスタンスの停止操作によって Azure VM インスタンスを停止してください。
Azure VM インスタンスの停止操作を行っても停止されない場合は、約 10 分後に Microsoft Azure によって自動的に強制停止されます。

2. ストレージクラスターの強制停止を実施します。

"force"パラメーターを"true"に指定して、ストレージクラスターのクラスターマスターノード(プライマリー)の IP アドレス、または FQDN に対してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/shutdown/invoke

CLI : storage_shutdown

3. 以下を確認します。

- <<Cloud for AWS>>

AWS マネジメントコンソールから、EC2 インスタンスが停止されたことを確認してください。



注意

約 20 分経過しても EC2 インスタンスが停止していない場合、EC2 インスタンスの停止操作によって EC2 インスタンスを停止してください。EC2 インスタンスの停止は、AWS マネジメントコンソールから行ってください。

EC2 インスタンスの停止操作後、約 5 分経過しても停止できない場合は、強制停止操作によって EC2 インスタンスの停止を行ったあと、再度 EC2 インスタンスを起動してください。強制停止は、AWS マネジメントコンソールの EC2 インスタンスの停止操作で停止してください。

メモ



- EC2 インスタンスの停止操作は、AWS のマニュアルを参照してください。
- EC2 インスタンスの強制停止は、EC2 インスタンスが停止中(stopping)の状態のままのときに再度 EC2 インスタンスの停止操作を行うことで実行できます。
詳しい操作方法は AWS のマニュアルを参照してください。

- <<Cloud for Google Cloud>>

Google Cloud コンソールから、Compute Engine インスタンスが停止されたことを確認してください。



注意

約 20 分経過しても Compute Engine インスタンスが停止していない場合、Compute Engine インスタンスの停止操作によって Compute Engine インスタンスを停止してください。

Compute Engine インスタンスの停止は、Google Cloud コンソールから行ってください。

Compute Engine インスタンスの停止操作を行っても停止されない場合は、約 90 秒後に Google Cloud によって自動的に強制停止されます。



メモ

Compute Engine インスタンスの停止操作は、Google Cloud のマニュアルを参照してください。

- <<Cloud for Microsoft Azure>>
Azure ポータルから、Azure VM インスタンスが停止されたことを確認してください。



注意

- 約 20 分経過しても Azure VM インスタンスが停止していない場合、Azure VM インスタンスの停止操作によって Azure VM インスタンスを停止してください。Azure VM インスタンスの停止は、Azure ポータルから行ってください。
Azure VM インスタンスの停止操作を行っても停止されない場合は、約 10 分後に Microsoft Azure によって自動的に強制停止されます。
- 手順 2 のストレージクラスターの強制停止を実施すると、Azure ポータルでの Azure VM インスタンスの状態は「停止済み」になります。Azure ポータルから、ストレージクラスターを構成するすべての Azure VM インスタンスを停止して、すべての Azure VM インスタンスの状態が「停止済み(割り当て解除)」になることを確認してください。Microsoft Azure では、Azure VM インスタンスの状態が「停止済み」の場合、Azure VM インスタンスの課金状態が継続されます。「停止済み(割り当て解除)」の場合は課金状態が継続されません(ディスクの課金状態は継続されます)。



メモ

Azure VM インスタンスの停止操作は、Microsoft Azure のマニュアルを参照してください。

33.6 ストレージクラスターの再起動

ストレージクラスターを再起動する方法について説明します。

33.6.1 ストレージクラスターを再起動する <<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージクラスターを停止したあと、自動的に再起動します。



注意

- ユーザー操作を実施中のときは、ストレージクラスターは停止できません(停止操作はキャンセルされます)。ユーザー操作の完了を確認してから、ストレージクラスターの停止を実行してください。
ただし、以下のユーザー操作については、実施中の場合でもストレージクラスターは停止できます。ストレージクラスターを停止した場合、実施中のユーザー操作は中断されることがあります。中断されたユーザー操作は、ストレージクラスターを再起動したあと「ジョブの情報を個別に取得する」を参照しジョブの情報を取得して、対処してください。
 - ストレージプールの拡張
 - ボリュームの作成
 - ボリュームの削除
 - ボリュームの設定編集

- ボリュームとコンピュートノードの接続
- ボリュームとコンピュートノードの接続を解除
- ストレージクラスターを停止した場合、以下が処理中だったとき、それらの処理は中断されることがあります。中断された処理は、ストレージクラスターの再起動後に再開されます。
 - リビルド
 - ドライブデータ再配置
 - 容量バランス
 - ストレージコントローラーの容量追加
 - ストレージコントローラー単位に管理するユーザーデータ容量に対する平準化処理
 - スナップショットのリストア¹
 - スナップショットボリュームの削除^{1,2}

1 スナップショットのリストアまたは削除の実施状況は、ボリューム情報を取得し `snapshotStatus` を確認してください。

2 スナップショットボリュームの削除が再開し、`snapshotStatus` が "Empty" になっていても S-VOL は残っています(ストレージクラスターが停止した場合には自動では削除されません)。S-VOL を削除するために、スナップショットボリュームの削除を再度実施してください。
- ストレージノードの自動回復による保守回復ジョブまたは交換ジョブが動作している場合、ストレージクラスターは停止できません(停止操作はキャンセルされます)。

「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「競合する処理による操作失敗への対処」に記載されている内容を参照し、実行中の保守回復ジョブまたは交換ジョブが完了するのを待ってから、ストレージクラスターの停止を実行してください。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージクラスターの情報を取得します。

REST API : GET /v1/objects/storage

CLI : `storage_show`

ストレージクラスターの `status` が "Ready" のとき、次の手順に進みます。
2. ストレージクラスターを停止します。

`reboot` パラメーターに "true" を指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/shutdown/invoke

CLI : `storage_shutdown`

停止が完了するまでの時間は約 20 分、最大約 90 分です。
3. 停止に続いてストレージクラスターの起動が開始します。

ストレージノードに異常がなければ、各ストレージノードのストレージソフトウェアが自動的に起動し、ストレージクラスターが構成されます。

全ストレージノードの立ち上げからストレージクラスターの起動完了までに掛かる時間は以下のとおりです。

 - 通常 : 約 20 分+UEFI ブート時間(目安 : 5~10 分)
 - 最大 : 約 175 分+UEFI ブート時間(目安 : 5~10 分)

UEFI ブート時間は使用しているハードウェアや UEFI 設定(メモリーテストなどのブート時間最適化に関する設定)によって異なるため、使用しているハードウェアのマニュアルを参照してください。
4. イベントログの一覧を取得して、ストレージクラスターの起動の完了を確認します。

イベントログ KARS08100-I の出力が確認できたら、ストレージクラスターの起動は完了です。

イベントログの一覧の取得方法は「イベントログの一覧を取得する」を参照してください。

5. ストレージクラスターの status が "Ready"であることを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

33.6.2 ストレージクラスターを再起動する <<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

ストレージクラスターを停止したあと、自動的に再起動します。



注意

- ユーザー操作を実施中のときは、ストレージクラスターは停止できません(停止操作はキャンセルされます)。ユーザー操作の完了を確認してから、ストレージクラスターの停止を実行してください。ただし、以下のユーザー操作については、実施中の場合でもストレージクラスターは停止できます。ストレージクラスターを停止した場合、実施中のユーザー操作は中断されることがあります。中断されたユーザー操作は、ストレージクラスターを再起動したあと「ジョブの情報を個別に取得する」を参照しジョブの情報を取得して、対処してください。

- ストレージプールの拡張
- ボリュームの作成
- ボリュームの削除
- ボリュームの設定編集
- ボリュームとコンピュータノードの接続
- ボリュームとコンピュータノードの接続を解除

- ストレージクラスターを停止した場合、以下が処理中だったとき、それらの処理は中断されることがあります。中断された処理は、ストレージクラスターの再起動後に再開されます。

- リビルド
- 容量バランス
- ストレージコントローラーの容量追加
- ストレージコントローラー単位に管理するユーザーデータ容量に対する平準化処理
- スナップショットのリストア¹
- スナップショットボリュームの削除^{1,2}

1 スナップショットのリストアまたは削除の実施状況は、ボリューム情報を取得し snapshotStatus を確認してください。

2 スナップショットボリュームの削除が再開し、snapshotStatus が "Empty" になっていても S-VOL は残っています(ストレージクラスターが停止した場合には自動では削除されません)。S-VOL を削除するために、スナップショットボリュームの削除を再度実施してください。

- ストレージノードの自動回復による保守回復ジョブまたは交換ジョブが動作している場合、ストレージクラスターは停止できません(停止操作はキャンセルされます)。

「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「競合する処理による操作失敗への対処」に記載されている内容を参照し、実行中の保守回復ジョブまたは交換ジョブが完了するのを待ってから、ストレージクラスターの停止を実行してください。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージクラスターの情報を取得します。

REST API : GET /v1/objects/storage

CLI : storage_show

ストレージクラスターの status が"Ready"のとき、次の手順に進みます。

2. ストレージクラスターを停止します。

reboot パラメーターに"true"を指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/shutdown/invoke

CLI : storage_shutdown

停止が完了するまでの時間は約 20 分、最大約 90 分です。

3. 停止に続いてストレージクラスターの起動が開始します。

ストレージノードに異常がなければ、各ストレージノードのストレージソフトウェアが自動的に起動し、ストレージクラスターが構成されます。

≪Cloud for AWS≫全 EC2 インスタンスの立ち上げからストレージクラスターの起動完了までに掛かる時間は以下のとおりです。

- ・ 通常 : 約 20 分
- ・ 最大 : 約 175 分

≪Cloud for Google Cloud≫全 Compute Engine インスタンスの立ち上げからストレージクラスターの起動完了までに掛かる時間は以下のとおりです。

- ・ 通常 : 約 20 分
- ・ 最大 : 約 175 分

≪Cloud for Microsoft Azure≫全 Azure VM インスタンスの立ち上げからストレージクラスターの起動完了までに掛かる時間は以下のとおりです。

- ・ 通常 : 約 20 分
- ・ 最大 : 約 175 分

4. イベントログの一覧を取得して、ストレージクラスターの起動の完了を確認します。

イベントログ KARS08100-I の出力が確認できたら、ストレージクラスターの起動は完了です。

イベントログの一覧の取得方法は「イベントログの一覧を取得する」を参照してください。

5. ストレージクラスターの status が"Ready"であることを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

ストレージクラスターの構成情報を変更・設定する<<Bare metal>>

この章での記述内容は Bare metal モデルに適用されます。

- 34.1 構成情報の変更・設定の概要<<Bare metal>>
- 34.2 管理ネットワーク変更時の運用の注意<<Bare metal>>
- 34.3 構成情報の変更・設定のために VSSB 構成ファイルを編集する<<Bare metal>>
- 34.4 構成情報を変更・設定する<<Bare metal>>

34.1 構成情報の変更・設定の概要<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

セットアップの際に使用した VSSB 構成ファイル(SystemConfigurationFile.csv)の、一部の設定を変更して、ストレージクラスターの構成情報を再設定できます。

変更できる設定は以下のとおりです。各項目の意味は、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。

区分	項目名	備考
[Cluster]	NtpServer1	NTP サーバーは最低 1 つ必須です。 ストレージクラスターの代表 IP アドレスと DNS サーバーの設定は任意です。ただし、外部認証サーバーで LDAPS または StartTLS を使用している場合、DNS サーバーは最低 1 つ必須です。DNS サーバーにアクセス不可能な値を指定した場合、処理は失敗します。
	NtpServer2	
	Timezone	
	DnsServer1	
	DnsServer2	
	ClusterIpv4Address	
[Nodes]	ControlNWIPv4	—
	ControlNWIPv4Subnet	
	ControlNWMtUSize	
	InterNodeNWIPv4	
	InterNodeNWIPv4Subnet	
	InterNodeNWMtUSize	
	ControlInterNodeNWIPv4RouteDestination<x>	
	ControlInterNodeNWIPv4RouteGateway<x>	
	ControlInterNodeNWIPv4RouteInterface<x>	
	ComputeNWIPv4Address<y>	左記に示す項目の削除・追加はできません (コンピュータポートの追加・削除は不可です)。
	ComputeNWIPv4Subnet<y>	
	ComputeNWIPv4Gateway<y>	
	ComputeNWIPv6Mode<y>	
	ComputeNWIPv6Global1_<y>	
	ComputeNWIPv6SubnetPrefix<y>	
	ComputeNWIPv6Gateway<y>	
	ComputeNWMtUSize<y>	



注意

- HostName は変更できません。また、ClusterMasterRole の対応を変えることはできません。VSSB 構成ファイル(SystemConfigurationFile.csv)の修正時には注意してください。
- FC 接続から、iSCSI 接続または NVMe/TCP 接続への構成変更はできません。また、iSCSI 接続または NVMe/TCP 接続から、FC 接続への構成変更もできません。
- HostName、ClusterMasterRole 以外の変更できない設定項目を変更した場合は、該当する構成情報の変更は無視されます。無視される構成情報の変更を含んでいる場合でも、変更操作そのものは、成功で完了します。

- 外部認証サーバーで LDAPS または StartTLS を使用している場合に DNS を 1 つも設定しないと、起動後外部ユーザー認証が失敗します。ローカルの Service ロールを持つユーザーでストレージクラスターを停止し、再度本機能を用いて DNS を設定し直してください。
- VSSB 構成ファイルを編集する際、[FaultDomains]や[Nodes]など複数行定義する区分内での行の入れ替えは行わないでください。
- VSSB 構成ファイルを編集する際、「構成情報の変更・設定のために VSSB 構成ファイルを編集する <<Bare metal>>」に記載の構成ファイルをエクスポートする手順は必ず実施してください。ストレージソフトウェアのインストール時に使用した VSSB 構成ファイルと、エクスポートして取得した VSSB 構成ファイルでは、[FaultDomains]や[Nodes]など複数行定義する区分内の行が入れ替わっている場合があります。その場合でもエクスポートした VSSB 構成ファイルの行の並びは変更せずに編集してください。
- 構成情報の変更・設定の前に、変更する管理ネットワーク、ストレージノード間ネットワーク、コンピュータネットワークの依存関係や影響範囲を調査し、構成情報の変更・設定後に外部サーバーやストレージソフトウェアの設定変更の必要があればそれぞれ対処してください。例えば、コンピュータネットワークの変更は iSNS サーバーに影響があります。
- Universal Replicator 機能を使用中にコンピュータポートの IP アドレスを変更すると、接続先のストレージシステムとのリモートパスが切れてしまいます。このため、コンピュータポートの IP アドレスを変更した場合は、現状のリモートパスを削除してから、新しいコンピュータポートの IP アドレスでリモートパスを追加してください。

34.2 管理ネットワーク変更時の運用の注意 <<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

構成情報の変更・設定によって、管理ネットワークの設定(ControlNWMTUSize、ControlNWIPv4、または ControlNWIPv4Subnet)を変更すると、外部サービスとつながらなくなる可能性があります。

この節では、Subject Alternative Name を SAN と表記しています。



注意

外部サーバーとの接続が切れると、構成情報の変更・設定完了後、外部認証が使用できなくなります。外部認証サーバーとの接続性が切れた状態で各種ストレージ操作をするために、必ずローカルの Security ロールを持つユーザーを最低 1 人有効にしておき、必要に応じて任意のロールを持つローカルユーザーを追加してください。

管理ネットワーク変更時は、コントローラーノード、または利用している外部サーバーに関して、構成情報の変更・設定前、構成情報の変更・設定後の各段階で、以下を実施してください。

区分	構成情報の変更・設定前		構成情報の変更・設定後
	ストレージクラスター再起動前	ストレージクラスター再起動後～構成情報の変更・設定前	
コントローラーノード	「許可リストの設定」に従って、新しいコントローラーノードの IP アドレスまたは IP アドレスの範囲(CIDR 表記)を登録します。	コントローラーノードの IP アドレスを変更します。	-
ストレージノード	「運用管理を SSL/TLS 通信で行う」に従ってサーバー証明書を VSP One SDS Block に適用してください。ただし、サーバー証明書の SAN に IP アドレスを指定する場合は、変更前後の管理ネットワーク用の IP	サーバー証明書に FQDN を指定している場合は、--host に任意のストレージノードの FQDN を指定し本機能を実行してください。 サーバー証明書に IP アドレスを指定している場合は、--host	サーバー証明書に IP アドレスを指定している場合は、全ストレージノードの変更前の管理ネットワーク用の IP アドレスは不要なため、SAN に変更後の全ストレージノードの管理ネットワーク用の IP アドレス

区分	構成情報の変更・設定前		構成情報の変更・設定後
	ストレージクラスター再起動前	ストレージクラスター再起動後～構成情報の変更・設定前	
	アドレスが SAN に指定されている必要があります。 (操作が複雑になるためサーバー証明書は FQDN を指定して作成されることを推奨します。)	に任意のストレージノードの管理ネットワーク用の IP アドレスを指定し本機能を実行してください。	が記載されたサーバー証明書を発行し、VSP One SDS Block に適用してください。
NTP サーバー	-	NTP サーバーの IP アドレスを構成情報の変更・設定によって指定するものに変更します。 BMC の設定にて、BMC 時刻同期先の NTP サーバーの IP アドレスを構成情報の変更・設定によって指定するものへの変更も実施してください。	-
DNS サーバー*	-	DNS サーバーの IP アドレスを構成情報の変更・設定によって指定するものに変更します。 サーバー証明書検証を実施する場合は、FQDN から変更後の管理ネットワーク用の IP アドレスを正引き可能な DNS サーバーを用意し、コントローラーノードからアクセス可能な状態にしてください。	-
Syslog サーバー	イベントログの Syslog 転送を有効に設定している場合は、無効に設定可能であれば無効に設定します。 転送を無効に設定しないと、構成情報変更・設定後に記載した対処の前に、転送失敗のイベントが発生することがあります。	サーバー側の IP アドレスを、VSP One SDS Block と接続可能な管理ネットワーク上のアドレスに変更します。	「イベントログの Syslog 転送設定の編集」と「監査ログの Syslog 転送設定の編集」に従って、新しい Syslog サーバーを設定します。
SMTP サーバー	イベントログの SMTP 転送を有効に設定している場合、無効に設定可能であれば無効に設定します。 転送を無効に設定しないと、構成情報変更・設定後に記載した対処の前に、転送失敗のイベントが発生することがあります。		「イベントログの SMTP 転送設定の編集」に従って、新しい SMTP サーバーを設定します。
SNMP サーバー	SNMP を有効に設定している場合、無効に設定可能であれば無効に設定します。 無効に設定しないと、構成情報変更・設定後に記載した対処の前に、トラップ発報失敗のイベントが発生することがあります。		「SNMP アクセスコントロールの設定」に従って、新しい SNMP サーバーを設定します。

区分	構成情報の変更・設定前		構成情報の変更・設定後
	ストレージクラスター再起動前	ストレージクラスター再起動後～構成情報の変更・設定前	
外部認証サーバー	ローカルの Security ロールを持つユーザーを最低 1 人有効にしておきます。	外部認証サーバーで LDAPS または StartTLS を使用している場合は、VSSB 構成ファイル (SystemConfigurationFile.csv) に最低 1 つ有効な DNS サーバーが指定されていることを確認してください。	「外部認証サーバーを利用する」に従って、新しい外部認証サーバーを設定します。
スぺアノード	「スぺアノードの情報を削除する<<Bare metal>>」に従ってスぺアノードの情報を削除します。 情報を削除しない場合、構成情報変更・設定後に記載した対処の前に、スぺアノードの接続に関するイベントログが発生することがあります。	スぺアノードの IP アドレスを、VSP One SDS Block と接続可能な管理ネットワーク上のアドレスに変更します。 変更方法は「スぺアノードを管理する<<Bare metal>>」を参照してください。	「スぺアノードの情報を登録する<<Bare metal>>」に従って、新しいスぺアノードを登録します。
* DNS サーバーを利用している場合、コントローラーノードおよびストレージノードは、DNS サーバーにおいて設定された時間(DNS TTL[sec])だけ、DNS への問い合わせ結果をキャッシュしています。このため、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは、DNS TTL の間、コントローラーノードおよびストレージノードが古い IP アドレスにアクセスする場合があります。したがって、DNS サーバー側の登録内容(ホスト名と IP アドレスの対応)を変更したときは DNS TTL で設定された時間が経過したあとに操作を実行してください。			

34.3 構成情報の変更・設定のために VSSB 構成ファイルを編集する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

VSSB 構成ファイル(SystemConfigurationFile.csv)を編集します。



注意

- ・トラブルシュートの際に必要なため、実行操作の画面のログを、構成情報の変更・設定を実施したときからすべて採取してください。
- ・変更前後の VSSB 構成ファイルは、トラブルシュートの際に使用しますので、構成情報の変更・設定前に、必ずコントローラーノードの外部にバックアップを作成し、構成情報の変更・設定中は保管してください。構成情報の変更・設定が正常終了したあとはバックアップは不要になります。
- ・FC 接続から、iSCSI 接続または NVMe/TCP 接続への構成変更はできません。また、iSCSI 接続または NVMe/TCP 接続から、FC 接続への構成変更もできません。
- ・Universal Replicator 機能を使用中にコンピュータポートの IP アドレスを変更すると、接続先のストレージシステムとのリモートパスが切れてしまいます。このため、コンピュータポートの IP アドレスを変更した場合は、現状のリモートパスを削除してから、新しいコンピュータポートの IP アドレスでリモートパスを追加してください。

認証チケットの発行および構成ファイルのエクスポートは、コントローラーノードにログインして操作します。

前提条件

- 構成情報を変更・設定するための認証チケット発行に必要なロール：Security
- 実行に必要なロール：Service

操作手順

- Security ロールのユーザーで認証チケットファイルを作成します。

作成した認証チケットは、構成情報の変更・設定が完了するまでコントローラーノードに保存してください。

チケットの有効期間を指定してコマンドを実行します。

REST API：POST /v1/objects/tickets

CLI：ticket_create

コマンド実行後のレスポンスに、有効期間と認証チケットが以下のように表示されます。＜認証チケット＞の部分の文字列をファイルに保存してください。その際、改行コードを含めないように注意してください。

REST API での出力例：

```
{
  "ticket":"<認証チケット>",
  "expirationTime":"<有効期間>"
}
```

(format オプション未指定時の)CLI での出力例：

Ticket:<認証チケット>

Expiration Time:<有効期間>

詳しくは「認証チケットを発行する」を参照してください。

- 「構成ファイルをエクスポートする＜＜Bare metal＞＞」を参照し、VSP One SDS Block から構成ファイルを取得します。

最新状態の構成ファイルを使用するために、必ず取得してください。

- 構成変更のパラメーターを事前確認するために、VSSB 構成ファイル (SystemConfigurationFile.csv) を別名でコピーします。

- VSSB 構成ファイルを、テキストエディターで開き編集します。

- 手順 3 でコピーした編集前の VSSB 構成ファイルと、手順 4 の編集後の VSSB 構成ファイルを用いて、変更不可のパラメーターが更新されていないかを確認します。

- CLI：configuration_modify

構文と必須のパラメーターは以下のとおりです。

```
hsds [マスターコマンドオプション] configuration_modify --dry_check
<boolean> --new_system_configuration_file <file> --
current_system_configuration_file <file>
```

区分	オプション	説明
マスターコマンド オプション	--host	任意のストレージノードの管理ネットワーク用の IP アドレス、またはホスト名(FQDN)
	--user	チケット認証用のユーザー名
	--auth_ticket `less`<手順 1 で取得した チケットファイルのパス>	認証チケットファイルのパスを指定します。

区分	オプション	説明
		コントローラーノードの OS によって、less コマンドがない場合があります。その場合は<認証チケットファイル>内の文字列を指定します。
サブコマンドオプション	--dry_check	"true"を指定します。
	--new_system_configuration_file	手順 4 で編集した VSSB 構成ファイルのパス
	--current_system_configuration_file	手順 3 でコピーした編集前の VSSB 構成ファイルのパス

VSSB 構成ファイルの変更不可パラメーターの確認が成功した場合は、変更対象のリソース一覧と「[OK] Specified parameters are changeable.」のメッセージが表示されます。変更対象のリソースが意図どおりの場合は次の手順に進みます。

変更差分がない場合は「[WARN] There is no difference.」と表示されます。

また、外部認証サーバーで LDAPS、StartTLS を使用している場合は、DNS サーバーが登録されている必要があります。編集後の VSSB 構成ファイルに、DNS サーバーが 1 つも設定されていない場合は「[WARN] There is no DNS server.」と表示されます。その場合は、DNS サーバーの記載を追加するか、外部認証サーバーで LDAPS、StartTLS を使用していないことを確認してください。

変更不可パラメーターが変更されていたり、編集前後の VSSB 構成ファイルのフォーマットが間違っていた場合はエラーが出力されます。エラーに従ってファイル修正し、再度この手順を実施してください。

- 手順 3 でコピーした編集前の VSSB 構成ファイルと、手順 5 で変更不可パラメーターの確認まで実施した編集後の VSSB 構成ファイルを外部にバックアップを作成してください。

34.4 構成情報を変更・設定する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ストレージクラスターを停止してから、構成情報を変更・設定するコマンドを入力します。

構成情報を変更・設定するには、コントローラーノードにログインして操作します。



注意

- 構成ファイルを使用する次の保守操作は、同一ストレージクラスターに対して同時に複数実施しないでください。
 - ストレージノードの増設
 - ストレージノードの交換
 - VSP One SDS Block の構成情報の変更・設定
 - 構成ファイルのエクスポート
 - 構成バックアップ
- 構成情報の変更・設定を実施する際は、事前に構成情報のバックアップが採取していることを確認してください。バックアップの採取手順は、このマニュアルの「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照してください。
- 構成情報の変更・設定を実施する際は、この節に記載している操作手順、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」、およびメッセージによる指示がない限りはストレージノードに対する電源操作を実施しないでください。

- ・トラブルシュートの際に必要なため、実行操作の画面のログを、構成情報の変更・設定を実施したときからすべて採取してください。
- ・構成情報の変更・設定のためのストレージクラスター再起動後、この節に記載している操作手順にある REST API、CLI 以外で実行できる操作は、以下の CLI のみです。ほかの操作は実行できません。また、以下の CLI も構成情報の変更・設定 CLI 実行中は実行しないでください。

configuration_parameter_setting_mode
configuration_modify (--dry_check オプションが"true"の場合のみ)

- ・構成情報の変更・設定のためのストレージクラスター再起動後、構成情報変更・設定操作を取りやめたい場合は、構成パラメーター設定モードを解除します。
--mode オプションに"disable"、--system_configuration_file オプションに現在のストレージノードの管理ポートの IP アドレスが記載された構成ファイルを指定して、以下の CLI を実行してください。

configuration_parameter_setting_mode
エラーが発生した場合は、エラーメッセージに従って対処し、再度実行してください。すべてのストレージノードの構成パラメーター設定モードを解除したあと、すべてのストレージノードをパワーオフしてください。その後、再度すべてのストレージノードを起動してください。電源操作については、各ベンダーのマニュアルを参照してください。

全ストレージノードの電源オンからストレージクラスターの起動完了までに掛かる時間は以下のとおりです。

- ・ 通常：約 20 分+UEFI ブート時間(目安：5～10 分)
- ・ 最大：約 175 分+UEFI ブート時間(目安：5～10 分)

UEFI ブート時間は、使用しているハードウェアや UEFI 設定(メモリーテストなどのブート時間最適化に関する設定)によって異なるため、使用しているハードウェアのマニュアルを参照してください。

- ・スเปアノードの情報は構成情報の変更・設定では変更できません。スเปアノードの情報を変更したい場合は、「スเปアノードを管理する<<Bare metal>>」を参照してください。
- ・FC 接続から、iSCSI 接続または NVMe/TCP 接続への構成変更はできません。また、iSCSI 接続または NVMe/TCP 接続から、FC 接続への構成変更もできません。
- ・Universal Replicator 機能を使用中にコンピュートポートの IP アドレスを変更すると、接続先のストレージシステムとのリモートパスが切れてしまいます。このため、コンピュートポートの IP アドレスを変更した場合は、現状のリモートパスを削除してから、新しいコンピュートポートの IP アドレスでリモートパスを追加してください。

前提条件

- ・構成情報を変更・設定するための認証チケット発行に必要なロール：Security
- ・「管理ネットワーク変更時の運用の注意<<Bare metal>>」に記載された各段階の内容をすべて満たすこと
操作手順の実施前には、「管理ネットワーク変更時の運用の注意<<Bare metal>>」の「ストレージクラスター再起動前」の内容をすべて満たしてください。
操作手順における、ストレージクラスターの再起動後～構成情報の変更・設定前、構成情報の変更・設定後のそれぞれの段階においては、「管理ネットワーク変更時の運用の注意<<Bare metal>>」に記載された各段階の内容をすべて満たしてください。
- ・「構成情報の変更・設定のために VSSB 構成ファイルを編集する<<Bare metal>>」を実施し、編集前・編集後の SystemConfigurationFile.csv と認証チケットがあること

操作手順

1. コントローラーノードにログインします。
2. ストレージノードの一覧を取得して、すべてのストレージノードの status が"Ready"であることを確認します。

REST API：GET /v1/objects/storage-nodes

CLI：storage_node_list

"Ready"以外の status のストレージノードが存在する場合は、以下に従って対処してください。

- VSP One SDS Block の VSP One SDS Block Administrator でストレージノードの Health Status に"Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
 - status が"MaintenanceBlockage"のストレージノードがある場合は「ストレージノードを保守回復する<<Bare metal>>」に従って、ストレージノードを保守回復してください。
 - 上記以外の status のストレージノードがあった場合は、それらのストレージノードに対する処理が実施中のため、status が変わるまで待ってから、再度確認してください。
3. 次の手順で行うストレージクラスターの再起動操作の前に、ストレージクラスターの再起動操作によって中断される処理がすべて終了していることを確認します。確認できたら次の手順に進みます。
- 中断される処理については「ストレージクラスターを停止する<<Bare metal>>」を参照してください。
4. ストレージクラスターを再起動します。
- reboot パラメーターに"true"、configParameterSettingMode パラメーターに"true"を指定してコマンドを実行します。
- REST API : POST /v1/objects/storage/actions/shutdown/invoke
- CLI : storage_shutdown
- 停止が完了するまでの時間は約 20 分、最大約 90 分です。
5. 停止に続いて、すべてのストレージノードの起動が開始します。ストレージノードに異常がなければ、5~10 分程度ですべてのストレージノードが起動します。
- すべてのストレージノードが再起動したかどうかを以下の方法で確認してください。
- 手順 4 の再起動操作のあとに、BMC のログに再起動を示すメッセージ(Server reset.など)があること
BMC のログの確認方法は、ベンダーのマニュアルを参照してください。
 - コンソールインターフェイスの「Keyboard layout configuration」画面が表示されていること
コンソールインターフェイスの操作については「コンソールインターフェイスの操作」を参照してください。
6. 構成情報を変更・設定する以下のコマンドを実行します。
- 実施時間は、ストレージノード数と UEFI ブート時間によって異なります。
ストレージノード数が多いと実施時間が長くなります。
 - ストレージノード数 3 の場合は 20 分(目安)+ UEFI ブート時間(目安 5~10 分)程度
 - ストレージノード数 32 の場合は 40 分(目安)+ UEFI ブート時間(目安 5~10 分)程度
 上記に加えて、構成情報を変更・設定の中で、各ストレージノードの再起動完了の確認処理(最大 60 分)が行われます。
起動に時間が掛かるストレージノードが含まれている場合、実施時間がさらに長くなる場合があります。
 - 実行前に認証チケットファイル、編集した VSSB 構成ファイル (SystemConfigurationFile.csv)、編集前の VSSB 構成ファイル (SystemConfigurationFile.csv)がコントローラーノードにあることを確認してください。
- CLI : configuration_modify

構文と必須のパラメーターは以下のとおりです。

```
hsds [マスターコマンドオプション] configuration_modify --  
new_system_configuration_file <file> --  
current_system_configuration_file <file>
```

区分	オプション	説明
マスターコマンド オプション	--host	構成情報を変更・設定する前の任意の ストレージノードの管理ネットワー ク用の IP アドレス、またはホスト名 (FQDN)
	--user	チケット認証用のユーザー名
	--auth_ticket 'less <認証チケットファイ ルのパス>'	認証チケットファイルのパスを指定し ます。 コントローラーノードの OS によって、 less コマンドがない場合があります。 その場合は<認証チケットファイル>内 の文字列を指定します。
サブコマンドオプ ション	--new_system_configuration_file	編集した VSSB 構成ファイルのパスを 指定します。
	--current_system_configuration_file	編集前の VSSB 構成ファイルのパスを 指定します。



ヒント

IP アドレスを指定する場合は、変更前の IP アドレスを指定してください。また、サーバー証明書に IP アドレスを指定して作成すると、構成情報の変更・設定操作が複雑になるため、サーバー証明書は FQDN を指定して作成することをお勧めします。

ストレージノードの証明書の検証に失敗する場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「SSL/TLS 証明書エラー発生時の対処」を参照してください。コマンドを実行の際にサーバー証明書検証を実施しない場合は--ignore_certificate_errors を付与して実行してください。

また、--host に指定する値は「SSL/TLS 通信のクライアント要件」を参照してください。ただし、以下の点に注意してください。

- --host にはストレージクラスターの代表 IP アドレス、またはそれに対応する FQDN の指定は不可であること
 - --host に管理ネットワーク用の IP アドレスを指定する場合は、変更前の IP アドレスであること
7. 以下のメッセージが表示されたら、構成情報の変更・設定は行われました。続いて、ストレージクラスターが自動で起動します。

```
The configuration modify was successful.
```



注意

構成情報の変更・設定処理中に誤操作や通信障害などでコンソールが終了してしまった場合は、「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「構成情報の変更・設定時の障害の対処<<Bare metal>>」を参照してください。

8. イベントログの一覧を取得して、ストレージクラスターの起動の完了を確認します。

構成情報の変更・設定後にイベントログ **KARS08100-I** の出力が確認できたら、ストレージクラスターの起動は完了です。イベントログの一覧の取得方法は「イベントログの一覧を取得する」を参照してください。ストレージノードに異常がなければ、各ストレージノードのストレージソフトウェアが自動的に起動し、ストレージクラスターが構成されます。全ストレージノードの電源オンからストレージクラスターの起動完了までに掛かる時間は以下のとおりです。

- ・ 通常：約 20 分+UEFI ブート時間(目安：5～10 分)
- ・ 最大：約 135 分+UEFI ブート時間(目安：5～10 分)

ストレージクラスター起動中は、一時的に **REST API** または **CLI** のアクセスができなくなることがあります。アクセスに失敗した際は再度実行してください。

9. ストレージクラスターの **status** が **"Ready"**であることを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show



メモ

管理ポートの IP アドレスまたはストレージクラスターの代表 IP アドレスを変更する場合は、サーバー証明書に関する警告メッセージが表示される場合があります。警告メッセージが表示された場合は、リクエスト送信先の IP アドレスまたはホスト名を確認してから「サーバー証明書に関する警告メッセージが表示されたときの対処」を参照し、箇条書きで記載されている実行環境ごとの警告無視方法に従ってください。手順 10 でサーバー証明書をインポートすることで、警告メッセージは表示されなくなります。

10. 管理ポートの IP アドレスまたはストレージクラスターの代表 IP アドレスを変更する場合は、このマニュアルの「運用管理を SSL/TLS 通信で行う」に従ってサーバー証明書を更新してください。
11. 正しく設定できたかを確認します。

確認手順は、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージクラスターの構成を確認する」を参照してください。



注意

構成情報の変更・設定が完了し、ストレージクラスターの立ち上げが完了したら、構成情報が意図した内容になっているかを必ず確認してください。確認を行わず、意図と異なる設定でシステムが動作すると、システムの可用性や性能に悪影響を及ぼす可能性があります。

12. 以下のコマンドで、コントローラーノード上に存在する認証チケットのファイルを削除します。

```
$ rm <認証チケットファイル名>
```



注意

削除する認証チケットファイルを間違えないよう注意してください。Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」に作成方法を記載した、障害時のダンプ採取用の認証チケットファイルなどを、間違えて削除しないよう注意してください。間違えて削除した結果、最悪の場合、ストレージクラスターに 1 つも認証チケットファイルがない状態に陥る危険があります。誤って認証チケットファイルを削除した場合は、再度、認証チケットを発行するか、外部サーバーに保管してあるバックアップから復旧させてください。

13. 構成情報のバックアップを行います。

「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

認証チケットを管理する

- 35.1 認証チケットを発行する
- 35.2 認証チケットを破棄する

35.1 認証チケットを発行する

認証チケットを発行します。認証チケットは構成情報の変更・設定とダンプファイルの作成の際に必要です。

前提条件

- ・ 構成情報を変更・設定するための認証チケット発行に必要なロール：Security
- ・ ダンプファイルを生成するための認証チケット発行に必要なロール：Service

操作手順

1. 認証チケットを発行します。

チケットの有効期間を指定してコマンドを実行します。

REST API：POST /v1/objects/tickets

CLI：ticket_create

コマンド実行後のレスポンスに認証チケットと有効期間が表示されます。

2. 発行した認証チケットから、認証チケットファイルを作成します。

手順 1 のコマンド実行後のレスポンスに、有効期間と認証チケットが以下のように表示されます。<認証チケット>の部分の文字列をファイルに保存してください。

- ・ REST API での出力例：

```
{
  "ticket":"<認証チケット>",
  "expirationTime":"<有効期間>"
}
```
- ・ (format オプション未指定時の)CLI での出力例：

```
Ticket:<認証チケット>
Expiration Time:<有効期間>
```



メモ

<認証チケット>には改行は含まれないことに注意してください。

35.2 認証チケットを破棄する

認証チケットを破棄するよりも前に発行された、すべての認証チケットを破棄します。

認証チケットの破棄は以下のようなケースで実施してください。

- ・ 認証チケットを紛失した
- ・ 盗難などのセキュリティインシデントが発生した
- ・ サポートセンターが認証チケットを発行した
- ・ 構成情報をリストアした

障害などによって認証チケットの破棄が一部のストレージノードで反映できなかった場合は、該当するストレージノードがイベントログで通知されます。

前提条件

- 実行に必要なロール : Security

操作手順

1. 認証チケットを破棄します。

REST API : POST /v1/objects/tickets/actions/revoke-all/invoke

CLI : ticket_revoke_all

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。手順 5 に進みます。

ジョブが失敗している場合は、手順 3、4 に進みます。

3. 認証チケットの破棄に失敗したストレージノードが存在した場合、イベントログで通知されます。イベントログを確認して、失敗したストレージノードを特定します。
4. 特定したストレージノードの status を調べ、閉塞していたらストレージノードの保守回復、または保守交換を行います。ストレージノードが閉塞していなかったら、一度保守閉塞してからストレージノードの保守回復または保守交換を行います。
5. 認証チケットの破棄が完了したら、Service および Security ロールを持つすべてのユーザーに、認証チケットを破棄したことを連絡し、認証チケットを再作成するようお願いしてください。

構成情報をバックアップする<<Bare metal>> <<Cloud for AWS>>

この章での記述内容は Bare metal モデルおよび Cloud モデル for AWS に適用されます。

- 36.1 構成バックアップ・構成リストアの概要<<Bare metal>> <<Cloud for AWS>>
- 36.2 構成バックアップを行う<<Bare metal>> <<Cloud for AWS>>

36.1 構成バックアップ・構成リストアの概要<<Bare metal>> <<Cloud for AWS>>

この節での記述内容は Bare metal モデルおよび Cloud モデル for AWS に適用されます。

VSP One SDS Block が提供している保守操作では回復ができず、VSP One SDS Block の再インストールが必要な障害に備えるため、ストレージクラスターの構成などの情報をバックアップしておきます。バックアップした情報をリストアすることで、復旧を行います。

<<Bare metal>>構成リストア時に、障害が発生したハードウェアを交換する際、構成変更は行えません。同一の形名、搭載数、搭載箇所に限ってのハードウェア交換が行えます。形名については「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」、ハードウェアごとの詳細な交換条件は、このマニュアルの「ハードウェア交換の条件<<Bare metal>>」を確認してください。

<<Bare metal>>構成リストア時にスペアノードの登録情報が削除されるため、構成リストア作業内でスペアノードの再インストールとストレージクラスターへの再登録、ストレージノードの BMC 情報の再登録を実施します。また、構成リストア時のストレージノードの再インストール対象には、構成バックアップ時にスペアノードとして用意した物理ノードを使用することができます。

ユーザーデータの暗号化鍵の情報はバックアップした情報には含まれません。構成バックアップ時点で格納データ暗号化を利用している場合、構成リストアの際に暗号化鍵が再作成されます。このとき、構成バックアップ時点での暗号化鍵の数にかかわらず、システムの最大数だけ暗号化鍵が作成され、その後作成した暗号化鍵の割り当てと削除が行われることがあります。結果として、構成バックアップ時点で暗号化鍵が割り当てられていたドライブは、構成リストア後、新しく作成された暗号化鍵が割り当てられた状態になります。

Universal Replicator 機能使用時に、ペアを作成した状態でバックアップした情報を用いて構成リストアを行った場合、ペアに関係する情報は正しくリストアされません。その場合の対処は「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」の「VSP One SDS Block 構成リストア後のペア復旧(イベントログ KARS13300-W が発生した場合の対処)<<Bare metal>>」を参照して実施してください。



注意

- 複数の障害が同時に発生すると、通常の保守操作では回復ができなくなることがあるため、「ヘルスステータスを取得する」を参照して、定期的にストレージクラスターの状態確認を行い、障害が発生していた場合は対処するようにしてください。
- ユーザーデータは、構成バックアップ・構成リストアの対象外です。ユーザーデータのバックアップは、ユーザーにて実施してください。
- <<Cloud for AWS>>構成リストアを実行することでストレージノードの MAC アドレス、ストレージノードの UUID、ドライブの ID が変更されることがあります。MAC アドレスを用いたネットワーク接続性の管理を行っている場合は、ネットワーク接続可否の管理をいったん解除し、構成リストア完了後に新しい MAC アドレスでネットワーク接続可否の管理を再開してください。ストレージノードの UUID でストレージノードを管理している場合、またはドライブの ID でドライブを管理している場合は、管理をいったん解除してください。
- 構成バックアップ時点で格納データ暗号化を利用している場合、構成リストアを実行することで、ユーザーデータの暗号化鍵の UUID が変更されます。そのため、暗号化鍵の UUID を VSP One SDS Block の外部で管理している場合は、構成リストア完了後に暗号化鍵の情報を参照し、外部で管理している暗号化鍵の情報を見直してください。
- 構成リストア作業後、暗号化鍵の数("dek"の値 + "free"の値)が 4096 ではないことがあります。構成リストア作業によって暗号化鍵の割り当てと削除が行われた結果であるため問題ありません。

バックアップ操作は、各構成変更操作を行ったあとの手順の中で実施します。複数の構成変更操作を実施したあとに、一括でバックアップ操作を行うこともできます。

バックアップ操作が必要になる主な操作は以下のとおりです。バックアップ操作が必要となる各操作の手順中には、バックアップ操作を行う手順を記載しています。

- ストレージノードの増設・減設・交換
- ドライブの増設・減設・交換
- ボリュームの作成・削除
- <<Bare metal>>VSP One SDS Block の構成情報の変更・設定
- ストレージソフトウェアのアップデート

障害発生の際は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」を参照して対処してください。対処の結果、リストア操作が必要であるとサポートセンターによって判断された場合は、事前に取得していたバックアップファイルを使用して、日立の保守員がリストア作業を実施します。



注意

リストア作業については、以下の要因によって処理時間が増加することがあります。

- <<Bare metal>>
 - 交換が必要なドライブ数
 - ネットワークの通信状況(コントローラーノード、ストレージノードとの相互間の通信状況)
 - サーバーの性能状況(ストレージノードの温度上昇による性能低下など)
- <<Cloud for AWS>>
 - 交換が必要なドライブ数
 - クラウドプラットフォームの負荷状況
 - ネットワークの通信状況(コントローラーノード、ストレージノード、クラウドプラットフォームとの相互間の通信状況)
 - VM インスタンスの性能状況

36.2 構成バックアップを行う <<Bare metal>> <<Cloud for AWS>>

この節での記述内容は Bare metal モデルおよび Cloud モデル for AWS に適用されます。

バックアップは、VSP One SDS Block の CLI プログラムがインストールされているコントローラーノードにログインして操作します。この操作によって構成バックアップファイルが作成されます。

構成バックアップファイルの最大ファイルサイズは 765[MiB]です。保管中の構成バックアップファイルが破損してしまった場合に備えて、4 世代を目安にバックアップファイルを複数保有してください。



注意

- バックアップ操作の実施中は、構成変更操作を実施できないため、バックアップ操作の完了を待ってから、他の構成変更操作を実施してください。バックアップ操作中に他の構成変更操作を実施した場合は、バックアップ操作または構成変更操作が失敗することがあるため注意してください。
- この節での説明に従って構成バックアップファイルを生成した際に、スナップショットボリュームが存在していた場合、ストレージクラスター構成のリストアを実施したことによって構成が復元されたスナップショット

ットボリュームとボリュームパスは、システム管理者または利用者によってすべて削除する必要があります。

- ソフトウェアアップデート完了後に VSP One SDS Block の CLI のバージョンがストレージクラスターのバージョンと異なる場合、構成情報のバックアップコマンドが失敗する可能性があります。ストレージクラスターのバージョンと一致するバージョンの CLI プログラムを使用してください。

前提条件

前提条件を満たしていない場合、違反した条件に対応するエラーメッセージが表示されます。メッセージが表示された場合は、以下の前提条件を満たしていることを上から順番に確認してください。

- 実行に必要なロール : Service
- 構成変更操作が実行中でないこと
 - <<Bare metal>>
 - REST API、CLI、VSP One SDS Block Administrator によるストレージシステム全般*に関する作成、更新、削除を行う管理操作が実行中でないこと
 - ストレージノード増設、ストレージノード交換、構成ファイルのエクスポート、構成情報の変更・設定が実行中でないこと条件を満たしていない場合、KARS13110-E、KARS13116-E、KARS19207-E、KARS19213-E のいずれかのエラーメッセージが表示されます。
* 監査ログ、コンピュートノード、ドライブ、イベントログ、ダンプログ、認証チケット、VSP One SDS Block Administrator ログインメッセージ、ライセンス、セキュア通信、セッション、スナップショット、ソフトウェアバージョン、ストレージクラスター、ストレージコントローラー、ストレージノード、ストレージプール、ユーザーロール、ボリューム、管理ポート、ストレージノード間ポート、コンピュートポート、VPS、スペアノード、リモートパス、リモートパスグループ、ジャーナル、リモート iSCSI ポート
 - <<Cloud for AWS>>
 - REST API、CLI、VSP One SDS Block Administrator によるストレージシステム全般*に関する作成、更新、削除を行う管理操作が実行中でないこと
 - ストレージノード増設、ストレージノード交換、構成ファイルのエクスポートが実行中でないこと
 - クラウドプラットフォーム上での操作を伴う保守操作が実行中でないこと条件を満たしていない場合、KARS13110-E、KARS13116-E、KARS19207-E、KARS19208-E、KARS19209-E、KARS19213-E のいずれかのエラーメッセージが表示されます。
* 監査ログ、コンピュートノード、ドライブ、イベントログ、ダンプログ、認証チケット、VSP One SDS Block Administrator ログインメッセージ、ライセンス、セキュア通信、セッション、スナップショット、ソフトウェアバージョン、ストレージクラスター、ストレージコントローラー、ストレージノード、ストレージプール、ユーザーロール、ボリューム、管理ポート、ストレージノード間ポート、コンピュートポート、VPS、リモートパス、リモートパスグループ、ジャーナル、リモート iSCSI ポート
- 自動で動作する次の処理が動作していないこと
条件を満たしていない場合、KARS13110-E または KARS13115-E のエラーメッセージが表示されます。
 - リビルド
rebuildStatus が"Stopped"であることを確認してください。確認方法は「リビルドの状態を確認する」を参照してください。
 - ドライブデータ再配置

driveDataRelocationStatus が"Stopped"であることを確認してください。確認方法は「ドライブデータ再配置の状態を確認する<<Bare metal>>」を参照してください。

- 容量バランス
動作開始時にはイベントログ KARS16028-I が発行され、動作終了後にはイベントログ KARS16029-I が発行されます。
- ストレージプールの拡張
動作開始時にはイベントログ KARS16021-I が発行され、動作終了後にはイベントログ KARS16017-I、KARS16020-I、KARS16022-I、KARS16081-I のいずれかが発行されます。
- ドライブ減設
動作開始時には Operation が"DRIVE_REMOVE"であるイベントログ KARS13009-I が発行され、動作終了後にはイベントログ KARS05022-I が発行されます。
- 「ストレージノード増設の準備と手順」を実施中の場合、ご使用のモデルに対応した以下の手順が完了していること
 - <<Bare metal>> 「追加した論理容量が使用できることを確認する<<Bare metal>>」
 - <<Cloud for AWS>> 「追加した論理容量が使用できることを確認する<<Cloud for AWS>>」
完了していない場合は KARS13110-E のエラーメッセージが表示されます。
- ストレージノード間でストレージソフトウェアのバージョンが混在していないこと
条件を満たしていない場合、KARS13111-E のエラーメッセージが表示されます。
- ストレージクラスター内の各リソースで障害が発生していないこと
条件を満たしていない場合、KARS13112-E のエラーメッセージが表示されます。
- ヘルスステータスを確認し、各リソースが以下の条件を満たしていること

リソース	条件
ストレージクラスター	status が"Normal"であること
ストレージノード	
コンピュータポート	
ボリューム	
ドライブ	
フォールトドメイン	
管理ポート	条件はありません。*
ストレージノード間ポート	条件はありません。
ストレージプール	status が"Normal"または"Alerting"であること
ライセンス	
* CLI を実行するに当たっては、実行対象ストレージノードの管理ポートとの接続性が必要です。	

- 各リソースの状態を個別に参照し、以下の条件を満たしていること

リソース	条件
ストレージクラスター	• status が"Ready"であること • statusSummary が"Normal"であること • キャッシュ保護付きライトバックモードが有効の場合は、metaDataRedundancyOfCacheProtectionSummary が以下の条件を満たしていること ユーザーデータの保護種別(redundantType)はストレージプールのリソースから確認してください。

リソース	条件
	・ <<Bare metal>>ユーザーデータの保護種別(redundantType)が 4D+1P のとき : metaDataRedundancyOfCacheProtectionSummary の値が 1 であること ・ ユーザーデータの保護種別(redundantType)が 4D+2P のとき : metaDataRedundancyOfCacheProtectionSummary の値が 2 であること ・ ユーザーデータの保護種別(redundantType)が Duplication のとき : metaDataRedundancyOfCacheProtectionSummary の値が 1 であること
ストレージノード	・ status が "Ready" であること ・ statusSummary が "Normal" であること
コンピュータポート	・ status が "Normal" であること ・ statusSummary が "Normal" であること
スナップショット	
ボリューム	
ドライブ	・ status が "Normal" または "Offline" であること ・ statusSummary が "Normal" であること
管理ポート	条件はありません。*
ストレージノード間ポート	条件はありません。
ストレージプール	dataRedundancy が以下の条件を満たしていること ・ <<Bare metal>>ユーザーデータの保護種別(redundantType)が 4D+1P のとき : dataRedundancy の値が 1 であること ・ ユーザーデータの保護種別(redundantType)が 4D+2P のとき : dataRedundancy の値が 2 であること ・ ユーザーデータの保護種別(redundantType)が Duplication のとき : dataRedundancy の値が 1 であること
ライセンス	・ status が "Active"、"Warning"、"OverWritten" のいずれかであること ・ statusSummary が "Normal" または "Warning" であること
リモートバスグループ、リモートバス	・ cuStatus が "Normal" であること ・ remotePaths における pathStatus が "Normal" であること
ジャーナル	status が "Normal" であること
* CLI を実行するに当たっては、実行対象ストレージノードの管理ポートとの接続性が必要です。	

- ・ <<Cloud for AWS>>データマイグレーションが実施中でないこと
条件を満たしていない場合、KARS13114-E のエラーメッセージが表示されます。



注意

データマイグレーション実施中は、構成バックアップが失敗します。そのため、データマイグレーション実施中に VSP One SDS Block の再インストールが必要な障害が発生した場合、データマイグレーションと並行して実施した構成変更操作の結果は、構成リストアによって復元できません。構成変更操作は可能な限りデータマイグレーションを実施する前または完了後に実施してください。

- ・ キャッシュ保護付きライトバックモードが有効な状態で構成バックアップを行う場合、事前に各ストレージノードの 3 台以上のドライブに対してストレージプール拡張が完了していること
キャッシュ保護付きライトバックモードの状態の確認については「キャッシュ保護付きライトバックモードの概要」を参照してください。また、ストレージプール拡張の手順については「ストレージプールを拡張する」を参照してください。
条件を満たしていない場合、KARS13117-E のエラーメッセージが表示されます。

操作手順の留意事項

手順 1 から 6 までは、コントローラーノードにログインして実行する操作です。

操作手順

1. 構成変更操作が実行中でないことを、ジョブの一覧を取得して確認します。
クエリーパラメーター `status` に "Running" を指定してコマンドを実行し、取得結果を絞り込みます。
REST API : GET /v1/objects/jobs
CLI : `job_list`
確認できたら次の手順に進みます。
動作中の操作が存在する場合は、処理が完了してからバックアップを開始してください。



メモ

一部の構成変更操作は本手順によって確認することができません。実行中の構成変更操作があった場合はバックアップ実行時に KARS13110-E、KARS13115-E、または KARS13116-E のエラーメッセージが表示されるため、処理が完了してからバックアップを行ってください。

2. 各ストレージノードのバージョンが同一であることを確認します。
REST API : GET /v1/objects/storage-nodes
CLI : `storage_node_list`
確認できたら次の手順に進みます。
各ストレージノードのバージョンが一致しない場合は、ソフトウェアアップデートを完了させてからバックアップを開始してください。
3. ストレージクラスター内の各リソースで障害が発生していないことを確認します。
各リソースの `status` を確認します。
REST API : GET /v1/objects/health-status
CLI : `health_status_show`
確認できたら次の手順に進みます。
障害が発生している場合は、各障害を回復させてからバックアップを開始してください。
4. バックアップを実行するノード上に 2GiB 以上の空き容量があることを、ユーティリティコマンドを実行して確認します。
<Linux の場合>

```
$ df
```


<Windows の場合>

```
$ dir
```


空き容量が不足している場合は不要なファイルを削除してください。
確認できたら次の手順に進みます。

5. 構成情報のバックアップコマンドを実行します。実施には最大 50 分程度掛かります。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

CLI : configuration_backup_file_create

バックアップコマンドが正常に終了すると、バックアップを実行するノードに、以下のファイル名で構成バックアップファイルが作成されます。

- ディレクトリー：
バックアップコマンドを実行したディレクトリー
- ファイル名：
hsds_config_backup_<internalID>_<VERSION>_<YYYYMMDD>_<hhmmss>.tar
 - internalID : ストレージクラスター固有の ID 情報
 - VERSION : ストレージクラスターのバージョン
 - YYYYMMDD : 構成バックアップファイルの作成年月日
 - hhmmss : 構成バックアップファイルの作成時分秒



メモ バックアップコマンドは通常 30 分以内に完了しますが、CPU 使用率の上昇、システムディスクの応答速度低下、ユーザーデータドライブの応答速度低下などの要因によって最大 50 分程度掛かることがあります。



注意

- バックアップコマンドの失敗時にはコンソールに表示されるエラーメッセージに従って対処してください。
- バックアップコマンドでは内部で構成ファイルのエクスポートを行うため、イベントログに構成ファイルのエクスポートに関するログが出力されることがあります。また一度のバックアップコマンドの実行で構成ファイルのエクスポートのログが 2 回出力されることがありますが異常ではありません。
- 実行中に、「Ctrl」+「C」などを入力して中断したあとや、エラーによって終了したあと、構成バックアップファイルのダウンロード開始を示すイベントログ **KARS13121-I** が出力されることがあります。この場合、構成バックアップファイルがダウンロードされることはありません。バックアップコマンドを再度実行してください。
- 実行中に、「Ctrl」+「C」などを入力して中断した際や VSP One SDS Block とのネットワークが切断された際に、構成バックアップファイル作成を再度実行すると、**KARS13110-E**、**KARS19207-E**、**KARS19208-E**、**KARS19213-E**、**KARS19216-E** が表示されて失敗することがあります。この場合は、30 分ほど待ってから構成バックアップファイル作成を再度実行してください。
- バックアップコマンドを実行すると、進捗が表示されます。この進捗表示は、処理状況によっては均等に増えないことがあり、最大で 10 分更新されないことがあります。
- vcenter_user および --vcenter_password のオプションは使用しないため指定しないでください。

6. 構成バックアップファイルをファイル保管用サーバーに移動します。

- 《Bare metal》
 - バックアップコマンドを実行したディレクトリーに構成バックアップファイルが作成されているため、必要に応じてコントローラーノード上の保管用ディレクトリーや保管用外部サーバーにファイルを移動してください。
- 《Cloud for AWS》

- 。 バックアップコマンドを実行したディレクトリーに構成バックアップファイルが作成されているため、必要に応じてコントローラーノード上の保管用ディレクトリーや保管用外部サーバー、またはオブジェクトストレージなどにファイルを移動してください。

7. 構成バックアップファイルの破損チェックを実施します。

以降の操作は、コントローラーノードなどの構成バックアップファイルを保管したサーバーで実施してください。

コマンド内の構成バックアップファイル名で「<xxxxxxxxxx>」とある箇所は
<internalID>_<VERSION>_<YYYYMMDD>_<hhmmss>の情報が入ります。

Windows であれば PowerShell、Linux であればターミナル端末など、コマンド実行が可能なコンソールから実行します。

a. 構成バックアップファイルを展開します。

```
$ tar xvf ¥  
hsds_config_backup_<xxxxxxxxxx>.tar
```

b. 構成バックアップファイルのハッシュ値を計算します。

<Linux の場合>

```
$ sha256sum ¥  
hsds_config_backup_<xxxxxxxxxx>/data.tar
```

<Windows の場合>

```
$ Get-FileHash `.  
hsds_config_backup_<xxxxxxxxxx>/data.tar
```

c. 構成バックアップファイル内に格納されているハッシュ値を参照して、確認したハッシュ値と一致することを確認します。

```
$ cat ¥  
hsds_config_backup_<xxxxxxxxxx>/checksum
```

値が一致しない場合は、手順 6 からやり直してください。

d. 展開したファイルを削除します。

```
$ rm -r hsds_config_backup_<xxxxxxxxxx>
```



注意

バックアップファイルが破損してしまった場合、リストア操作が実施できなくなる可能性があるため、本手順を定期的に行ってファイルが破損していないことを確認することをお勧めします。

ストレージソフトウェアをアンインストールする

- 37.1 ストレージソフトウェアのアンインストールの概要
- 37.2 スタックを削除する<<Cloud for AWS>>
- 37.3 VPC ファイアウォール上のルールを削除する<<Cloud for Google Cloud>>
- 37.4 ストレージクラスターを削除する<<Cloud for Google Cloud>>
- 37.5 ストレージクラスターを削除する<<Cloud for Microsoft Azure>>
- 37.6 構成バックアップファイルを削除する<<Bare metal>> <<Cloud for AWS>>

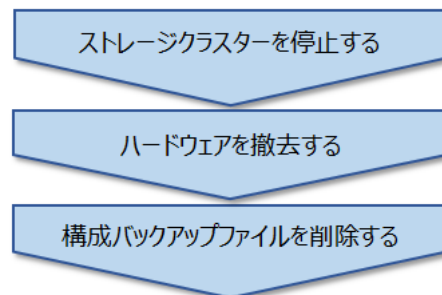
37.1 ストレージソフトウェアのアンインストールの概要

《Bare metal》

ストレージソフトウェアをアンインストールするには、以下を順次実施します。

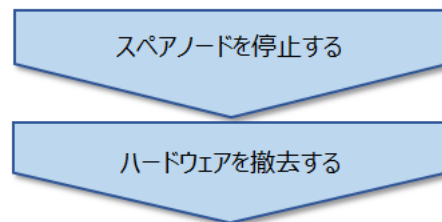
■ストレージクラスターの停止

ストレージクラスターの停止方法は、このマニュアルの「ストレージクラスターを停止する《Bare metal》」を参照してください。



■スペアノードの停止

スペアノードの停止方法は、このマニュアルの「ストレージクラスターを停止する《Bare metal》」の手順 4 を参照してください。



注意

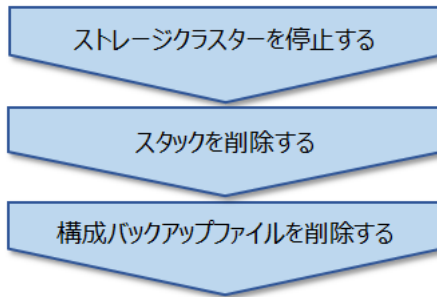
ハードウェアを撤去後、再利用する場合は以下の点に留意してください。

- ハードウェアの撤去や再利用の際のデータ消去自体は必須作業ではありませんが、情報漏えい防止の観点からデータ消去することを強くお勧めします。
- システムディスクのデータを消去することをお勧めします。
- 期待外に、ストレージノードとして使用していた物理サーバーの OS が起動すると、ストレージノードに残っているネットワーク設定によって、IP アドレス重複などのトラブルを引き起こす可能性があります。そのため、撤去するストレージノードに対し、以下を実施してください。
 - ネットワークからの切り離しを行ってください。物理サーバーの操作方法は、ハードウェアベンダーのマニュアルを参照してください。

《Cloud for AWS》

ストレージソフトウェアをアンインストールするには、以下を順次実施します。

ストレージクラスターの停止方法は、このマニュアルの「ストレージクラスターを停止する《Cloud for AWS》」を参照してください。



注意

EC2 インスタンスや EBS ボリュームを撤去後、再利用する場合は以下の点に留意してください。

- システムディスクのデータを消去することをお勧めします。
- ストレージノードとして使用していた EC2 インスタンスやドライブとして使用していた EBS ボリュームが残っていると、ストレージクラスターを使用していなくても、期待外に費用が掛かる可能性があります。

≪Cloud for Google Cloud≫

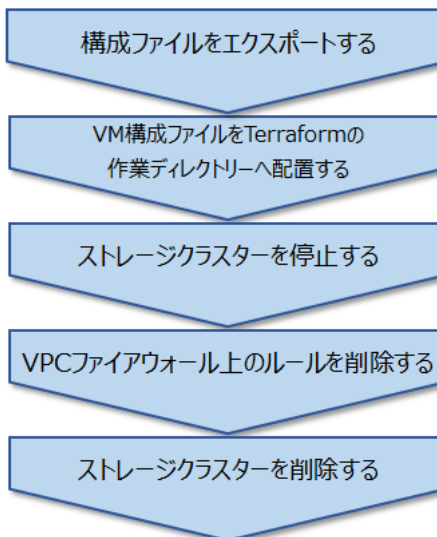
ストレージソフトウェアをアンインストールするには、以下を順次実施します。

「構成ファイルをエクスポートする」および「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する」は、最後に terraform apply を実行した作業ディレクトリーが不明な場合のみ実施します。

構成ファイルのエクスポート方法は、このマニュアルの「構成ファイルをエクスポートする ≪Cloud for Google Cloud≫」を参照してください。

VM 構成ファイルを Terraform の作業ディレクトリーへ配置する方法は、このマニュアルの「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する ≪Cloud for Google Cloud≫」を参照してください。

ストレージクラスターの停止方法は、このマニュアルの「ストレージクラスターを停止する ≪Cloud for Google Cloud≫」を参照してください。



注意

Compute Engine インスタンスや Google Cloud Hyperdisk ボリュームを撤去後、再利用する場合は以下の点に留意してください。

- システムディスクのデータを消去することをお勧めします。

- ・ ストレージノードとして使用していた **Compute Engine** インスタンスやドライブとして使用していた **Google Cloud Hyperdisk** ボリュームが残っていると、ストレージクラスターを使用していなくても、期待外に費用が掛かる可能性があります。ストレージノードで使用していた静的内部 IP アドレスは、残っていても費用が掛かることはありません。

≪Cloud for Microsoft Azure≫

ストレージソフトウェアをアンインストールするには、以下を順次実施します。

ストレージクラスターの停止方法は、このマニュアルの「ストレージクラスターを停止する ≪Cloud for Microsoft Azure≫」を参照してください。

ストレージクラスターを停止する

ストレージクラスターを削除する



注意

Azure VM インスタンスや Azure マネージドディスクボリュームを撤去後、再利用する場合は以下の点に留意してください。

- ・ システムディスクのデータを消去することをお勧めします。
- ・ ストレージノードとして使用していた **Azure VM** インスタンスやドライブとして使用していた **Azure** マネージドディスクボリュームが残っていると、ストレージクラスターを使用していなくても、期待外に費用が掛かる可能性があります。

37.2 スタックを削除する ≪Cloud for AWS≫

この節での記述内容は Cloud モデル for AWS に適用されます。

ストレージソフトウェアをアンインストールするために、スタックを削除します。

Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」に従って作成したスタックのうち不要となるスタックを、「セットアップ手順」で作成した順番とは逆の順番で削除してください。

ストレージノードの EC2 インスタンスは、誤操作などによる削除を防ぐために終了保護を有効に設定しています。スタックを削除するときは終了保護を無効に変更してから実施する必要があります。

EC2 インスタンスの終了保護は、AWS マネジメントコンソールの EC2 の画面などで設定が変更できます。



注意

スタックの削除が実施されない場合、AWS に課金され続けるおそれがあるため、ストレージクラスター構築時に作成したスタックはすべて削除してください。

37.3 VPC ファイアウォール上のルールを削除する ≪Cloud for Google Cloud≫

この節での記述内容は Cloud モデル for Google Cloud に適用されます。

Google Cloud の VPC ファイアウォールに通信を遮断するために追加されたルールが残っている場合、当該ルールを削除してください。

削除対象のルールは以下のネットワークに使用している VPC ネットワークに登録されています。

- ストレージノード間ネットワーク
- コンピュートネットワーク

ルールの追加と削除に関する概要および削除対象のルールの名称については、このマニュアルの「クラウドプラットフォームのメンテナンスについて<<Cloud for Google Cloud>>」を参照してください。ルールを削除する方法については、Google Cloud のユーザーガイドを参照してください。



メモ

ルールを削除する際、ストレージクラスターのストレージノードの ID(uuid)が確認できない場合は、Google Cloud の[VPC ファイアウォール ルール]画面でルールをクリックし、表示される IP アドレスを参考にしてください。

確認した IP アドレスが破棄する Compute Engine インスタンスで使用されていた場合は、当該ルールを削除してください。

37.4 ストレージクラスターを削除する<<Cloud for Google Cloud>>

この節での記述内容は Cloud モデル for Google Cloud に適用されます。

ストレージクラスターを削除(アンインストール)する必要がある場合は、以下の手順に従ってください。

操作手順の留意事項

以下の操作手順において、コマンドラインが長いコマンドの場合、¥記号を使用して改行しています。

操作手順

1. Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」にある「Google アカウントの権限について」に記載の条件を満たす Google アカウントでログインします。
2. gcloud CLI と Terraform の実行が可能な VM(例：Cloud Shell)にログインします。
3. 最後に terraform apply を実行した Terraform の作業ディレクトリーに移動します。



メモ

Terraform の作業ディレクトリーとは terraform のコマンドを実行するディレクトリーを指します。作業ディレクトリーには terraform の構成ファイル(VM 構成ファイル)やパッケージなどが格納されています。

最後に terraform apply を実行した作業ディレクトリーが不明な場合は、「構成ファイルをエクスポートする<<Cloud for Google Cloud>>」を参照して構成ファイルを取得したあとに、「VM 構成ファイルを Terraform の作業ディレクトリーへ配置する<<Cloud for Google Cloud>>」を参照して、作業ディレクトリーを作成します。

4. コンピュートポートの通信プロトコルとして IPv6 を併用している(デュアルスタックの場合、ストレージクラスターで使用していた静的内部 IPv6 アドレスを確認します。

```
gcloud compute addresses list ¥
--filter="name~^<clusterName>-sn[0-9]{2}-compute-ipv6$"
```

実行した結果から、静的内部 IPv6 アドレスの **name** と **region** を確認してください。

コマンド実行時に "Listed 0 items." と表示された場合は、手順 6 に進みます。

5. コンピュートポートの通信プロトコルとして IPv6 を併用している(デュアルスタックの場合)、ストレージクラスターで使用していた静的内部 IPv6 アドレスの予約を解除します。

```
gcloud compute addresses delete <静的内部 IPv6 アドレス名> ¥
--region <リージョン>
```

手順 4 で確認した静的内部 IPv6 アドレスの **name** を<静的内部 IPv6 アドレス名>に、**region** を<リージョン>に指定します。

コマンドの実行後、[Do you want to continue (Y/n)?]と表示されたら、[Y]を入力します。

入力すると、静的 IPv6 アドレスの予約が解除されます。



メモ

gcloud compute addresses delete コマンドは、静的内部 IPv6 アドレス名をスペース区切りで指定することで、複数の静的内部 IPv6 アドレスの予約を同時に解除することが可能です。

また、手順 4 で確認した静的内部 IPv6 アドレスのスペース区切りの文字列は以下のコマンドで取得できます。

```
gcloud compute addresses list ¥
--filter="name~^<clusterName>-sn[0-9]{2}-compute-ipv6$" ¥
--format="value(name)" | tr "\n" " "
```

手順 4 で確認した静的内部 IPv6 アドレスの予約をすべて解除してよい場合、この結果を gcloud compute addresses delete コマンドの入力(<静的内部 IPv6 アドレス名>)とすることで、一括で予約を解除することが可能です。

6. Compute Engine インスタンスの削除保護を無効にするため、以下のコマンドを実行します。

```
terraform plan -out=disable_deletion_protection ¥
-var "deletionProtection=false"
```

```
terraform apply "disable_deletion_protection"
```



メモ

terraform plan の実行時、「No changes.」と表示されても問題ありません。

7. terraform.tfvars ファイルの情報を基に、削除する構成に誤りがないかを確認するため以下のコマンドを実行します。

```
terraform plan -destroy
```

コマンド実行後、最後に[Outputs]が出力されます。削除する構成に誤りがないことを確認してください。

8. terraform plan -destroy での確認で問題がなければ、ストレージクラスターを削除するため以下のコマンドを実行します。

```
terraform destroy
```

コマンドの実行後、[Enter a value:]と表示されたら[yes]を入力します。

アンインストールが始まり、最後に[Destroy complete!]が出力されたらストレージクラスターの削除は完了です。

9. Compute Engine の[VM インスタンス]と[ディスク]を確認し、構成が削除されていることを確認します。

37.5 ストレージクラスターを削除する<<Cloud for Microsoft Azure>>

この節での記述内容は Cloud モデル for Microsoft Azure に適用されます。

ストレージクラスターを削除(アンインストール)する必要がある場合は、以下の手順に従ってください。



注意

この手順を実行すると、ストレージクラスター構築時に作成されたストレージアカウントが削除され、ストレージアカウントに保存されていたデータもすべて削除されます。



メモ

ストレージクラスターを削除する際は、デプロイ時に作成されたカスタムロールを必ず削除してください。カスタムロールを残したままにすると、次回同じ名前でデプロイを実行した際、処理が失敗する原因となります。また、リソースの削除ロックの解除も必ず実施してください。リソースの削除ロックが付与されたままだと、ストレージクラスター用リソースグループの削除は失敗します。

操作手順

1. Azure ポータルにサインインします。
2. カスタムロールの割り当て解除およびカスタムロールの削除を実施します。
 - a. ストレージクラスター用リソースグループの画面へ移動し、ストレージクラスター構築時に自動で作成されたマネージド ID のリソースを選択します。
 - b. メニューから[Azure ロールの割り当て]を選択し、表示された「役割」と「リソース名」を記録します。
 - c. 表示された役割の項目を選択します。
 - d. [割り当て]を選択して、該当するマネージド ID の割り当てを削除します。
 - e. 手順 b で記録したリソース名のリソースグループの画面に移動します。
 - f. メニューの[アクセス制御(IAM)]から[役割]を選択します。
 - g. 手順 b で記録した[役割]で検索し、該当するロールを削除します。
3. Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」にある「ストレージクラスターを構築する」で作成されたリソースの削除ロックを解除します。
 - a. ストレージクラスター用リソースグループの画面へ移動し、メニューの[設定]から[ロック]を選択します。
 - b. 表示されたすべてのリソースのロックを削除します。
4. ストレージクラスター用リソースグループの画面へ移動し、リソースグループを削除します。
[概要]から[リソースグループの削除]を選択し、表示された画面の説明に従ってリソースグループを削除してください。
リソースグループが削除されていることが確認できたら完了です。

37.6 構成バックアップファイルを削除する<<Bare metal>> <<Cloud for AWS>>

この節での記述内容は Bare metal モデルおよび Cloud モデル for AWS に適用されます。

コントローラーノードなどに保管している、不要になった構成バックアップファイルを削除してください。



注意

構成リストア操作の中で、ストレージソフトウェアをアンインストールする場合は、構成バックアップファイルの削除は実施しないでください。

コンソールインターフェイスの操作

- 38.1 コンソールインターフェイスの概要
- 38.2 ログインとログアウト
- 38.3 コンソールトップメニュー画面について
- 38.4 「Show storage cluster information」画面について
- 38.5 コンソールインターフェイスの留意事項

38.1 コンソールインターフェ이스の概要

ここで説明するコンソール画面は、ストレージノードに対する「ストレージクラスターの構築」、「ストレージノード増設」および「ストレージノード交換」における、それぞれの操作完了後の画面です。

コンソールインターフェ이스は、VSP One SDS Block において、セットアップ後に発生したストレージノードの障害などによって、VSP One SDS Block Administrator や REST API などが使用できない状況にあるとき、トラブルシュー트에必要な機能を提供します。

《Bare metal》コンソールインターフェ이스は、BMC の Web インターフェイス画面と BMC のリモートコンソールを使用して操作します。BMC の Web コンソールインターフェイス画面と BMC のリモートコンソールへの接続方法は、ストレージノードとして使用する物理サーバーのベンダーが提供する BMC のユーザーガイドを参照してください。

《Cloud》コンソールインターフェ이스は、VM インスタンスのシリアルコンソールを使用して操作します。シリアルコンソールへの接続方法は、クラウドプラットフォームのマニュアルを参照してください。



注意

- 《Bare metal》

コンソールインターフェイスでの操作は、BMC が提供するリモートコンソールのみをサポートします。リモートコンソール以外の接続での操作では正常に動作しない可能性があります。

38.2 ログインとログアウト

コンソールインターフェイスのログイン操作とログアウト操作について説明します。

38.2.1 ログイン操作とログアウト操作《Bare metal》

この項での記述内容は Bare metal モデルに適用されます。

コンソールインターフェイスのログイン操作とログアウト操作について説明します。

前提条件

- 実行に必要なロール：Security または Service
- コンソールインターフェイスでの使用(isEnabledConsoleLogin)が有効化されているユーザーであること

操作手順

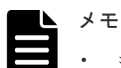
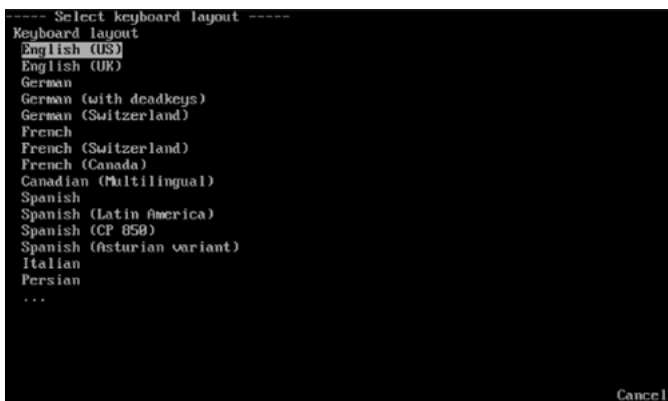
1. ストレージノードの BMC の Web インターフェイス画面にログインし、リモートコンソールに接続します。
2. 「Keyboard layout configuration」画面が表示され、現在のキーボードレイアウトが、Current keyboard layout に表示されます。



設定を変更しない場合は本手順を実施する必要はありません。次の手順に進みます。

設定を変更する場合は、[Select keyboard layout]を選択し「Enter」キーを押します。

「Select keyboard layout」画面に、サポートしているキーボードレイアウトのリストが表示されます。キーボードレイアウトのリストの末尾に[...]が表示されている場合は、末尾の[...]を選択し「Enter」キーを押すことで、リストの続きを表示できます。キーボードレイアウトのリストの先頭に[...]が表示されている場合は、先頭の[...]を選択し「Enter」キーを押すことで、前のリストを表示できます。ご使用のキーボードのレイアウトに合うキーボードレイアウトを選択して「Enter」キーを押します。



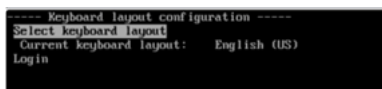
メモ

- ・ キーボードレイアウトを選択して「Enter」キーを押した際に一瞬画面が青くなりますが、この現象は問題ありません。
- ・ キーボードレイアウトを変更しない場合は、[Cancel]を選択して「Enter」キーを押すことで、キーボードレイアウトを変更せずに「Keyboard layout configuration」画面に戻ることができます。

「Select keyboard layout (Keyboard test)」画面が表示されます。Keyboard test 欄を利用して、選択したキーボードレイアウトの動作確認を実施できます。動作確認が終わったら[OK]を選択して「Enter」キーを押します。

「Keyboard layout configuration」画面が表示されたら、選択したキーボードレイアウトが Current keyboard layout に表示されていることを確認してください。

3. 「Keyboard layout configuration」画面で「↓」キーを押して[Login]を選択して「Enter」キーを押します。



4. ログインプロンプトが表示されたら、ユーザー ID とパスワードを入力してログインします。

```
Login:
Password: _
```

ログインが成功すると「Storage node console top menu」画面が表示されます。

5. ログアウトする場合は、「Storage node console top menu」画面で「↓」キーを押して「Logout」を選択し「Enter」キーを押します。

ログアウトが成功すると「Keyboard layout configuration」メニューが表示されます。



注意

- コンソールインターフェイスでの作業が完了したら、必ずログアウトしてください。
ログアウトせずに BMC のリモートコンソールを終了させた場合、ログイン状態が維持されます。この状態で再度 BMC のリモートコンソールにアクセスした場合はログイン済みの画面が表示されることがあります。
- コンソールインターフェイス操作中に画面から離れる場合は、ログアウトしてください。
複数のユーザーが BMC のリモートコンソールに接続を行うと、BMC は同時接続を通知するダイアログを表示します。ダイアログを操作することで、あとから接続したユーザーの接続を拒否することができますが、何も操作を行わなかった場合、あとから接続したユーザーに接続を許可するため、ログイン状態の画面が操作可能になる場合があります。
- 30 分間キー操作を行わなかった場合、自動でログアウトされます。

38.2.2 ログイン操作とログアウト操作<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

コンソールインターフェイスのログイン操作とログアウト操作について説明します。

前提条件

- 実行に必要なロール：Security または Service
- コンソールインターフェイスでの使用(isEnabledConsoleLogin)が有効化されているユーザーであること

操作手順

1. VM インスタンスのシリアルコンソールに接続します。
2. ログインプロンプトが表示されたら、ユーザー ID とパスワードを入力してログインします。

```
Login:
Password: _
```

ログインが成功すると「Storage node VM console top menu」画面が表示されます。



メモ

シリアルコンソールに接続後に約 10 秒経過してもログインプロンプトが表示されない場合、コンソール上で「Ctrl」+「U」を入力してから「Enter」キーを押してください。

3. ログアウトする場合は、「Storage node VM console top menu」画面で「↓」キーを押して「Logout」を選択し「Enter」キーを押します。

ログアウトが成功するとログインプロンプトが表示されます。



注意

- コンソールインターフェイスでの作業が完了したら、必ずログアウトしてください。

ログアウトせずにシリアルコンソールを終了させた場合、ログイン状態が維持される可能性があります。この状態で再度シリアルコンソールに接続した場合はログイン済みの画面が表示されることがあります。

- コンソールインターフェイス操作中に画面から離れる場合は、ログアウトしてください。
- 30 分間キー操作を行わなかった場合、自動でログアウトされます。

38.3 コンソールトップメニュー画面について

「Storage node console top menu」画面(Bare metal モデルの場合)または「Storage node VM console top menu」画面(Cloud モデルの場合)には、以下の情報が表示されます。

- ストレージノードの時刻(ローカル時刻表示)
- Storage node name : ストレージノードの名称
- IP address : ストレージノードの管理ネットワーク用の IP アドレス

「Storage node console top menu」画面(Bare metal モデルの場合)または「Storage node VM console top menu」画面(Cloud モデルの場合)では、以下のメニューが選択できます。「↑」「↓」と「Enter」キーを使用してメニューを選択してください。

表示されるメニュー	説明	遷移先画面
Show storage cluster information	ストレージクラスター情報を表示します。	「Show storage cluster information」画面
Logout	ログアウトします。	• <<Bare metal>> 「Keyboard layout configuration」画面 • <<Cloud>> ログインプロンプト

コンソールインターフェイスでの操作が完了したら、ログアウトしてください。

38.4 「Show storage cluster information」画面について

「Show storage cluster information」画面は、サポートセンターから依頼があった場合に参照する画面です。

「Show storage cluster information」画面では、以下の情報が表示されます。

- ストレージノードの時刻(ローカル時刻表示)
- Storage node name : ストレージノードの名称
- Storage cluster Id : ストレージクラスターの ID
- System random Id : 装置固有のランダムな ID

「Show storage cluster information」画面では、以下のメニューが選択できます。「↑」「↓」と「Enter」キーを使用してメニューを選択してください。

表示されるメニュー	説明	遷移先画面
Back to top	コンソールトップメニュー画面に戻ります。	• <<Bare metal>> 「Storage node console top menu」画面 • <<Cloud>> 「Storage node VM console top menu」画面

本画面での確認が完了したら、「Back to top」を選択しコンソールトップメニュー画面に戻ってください。

38.5 コンソールインターフェイスの留意事項

コンソールインターフェイス使用時に、操作が行えなくなったような場合は、それぞれ以下の対処をしてください。

- <<Bare metal>> 「Alt」キーと他のキーを同時に押した場合、BMC のリモートコンソールに真っ黒な画面が表示され、操作が行えなくなることがあります。その場合は「Alt」+「F1」キーを押してください。
- <<Bare metal>> 「ScrollLock」キーを押した場合、画面がロックされ、その後のキー入力ができなくなることがあります。その場合は「ScrollLock」キーを押して画面のロックを解除してください。
- <<Bare metal>> コンソールインターフェイスの画面の表示が乱れる場合があります。その場合は、BMC のリモートコンソールを一度閉じてから、再度開いてください。
- ログインプロンプトの表示が乱れる場合があります。その場合は「Enter」キーを押して一度ログインを失敗させ、ログインプロンプトを再表示させてください。

また、入力モードの状態、入力欄には以下の文字以外は入力しないでください。

- 数字(0-9)
- 英大文字(A-Z)、英小文字(a-z)
- 記号(! " # \$ % & ' () * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~)

上記以外の文字やキーを入力すると、画面が正常に表示されないことがあります。その場合は、一度別の画面を表示したあと、再度元の画面を表示してください。

マルチテナンシーを構成する<<Bare metal>>

この章での記述内容は Bare metal モデルに適用されます。

- 39.1 マルチテナンシーの概要<<Bare metal>>
- 39.2 VPS に関する設定について<<Bare metal>>
- 39.3 テナント共通の設定<<Bare metal>>
- 39.4 システム管理者向けの設定<<Bare metal>>
- 39.5 VPS を作成する<<Bare metal>>
- 39.6 VPS の利用状況を確認する<<Bare metal>>
- 39.7 VPS の情報の取得<<Bare metal>>
- 39.8 VPS の設定を編集する<<Bare metal>>
- 39.9 VPS を削除する<<Bare metal>>
- 39.10 性能低下・操作不可の監視と対処<<Bare metal>>
- 39.11 リソース不足・性能問題発生時の対処<<Bare metal>>

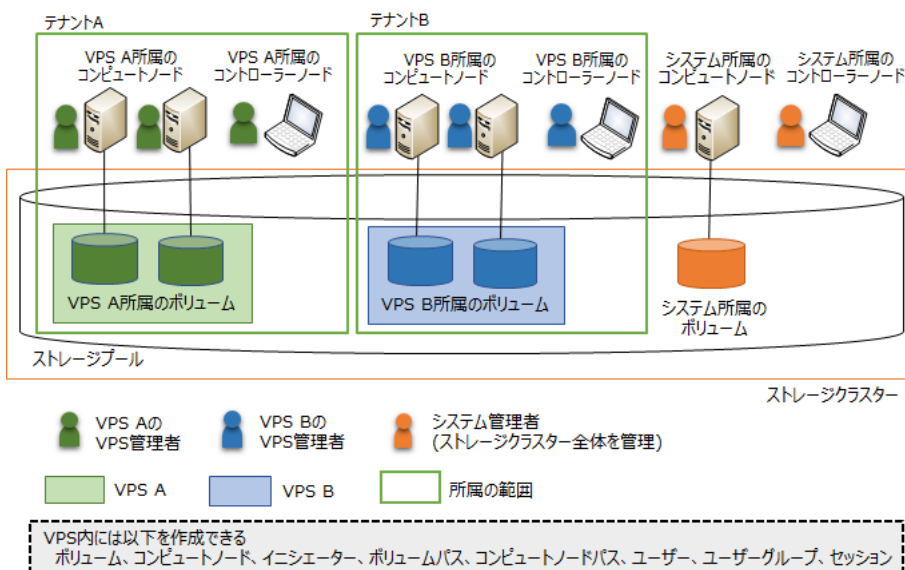
39.1 マルチテナンシーの概要<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

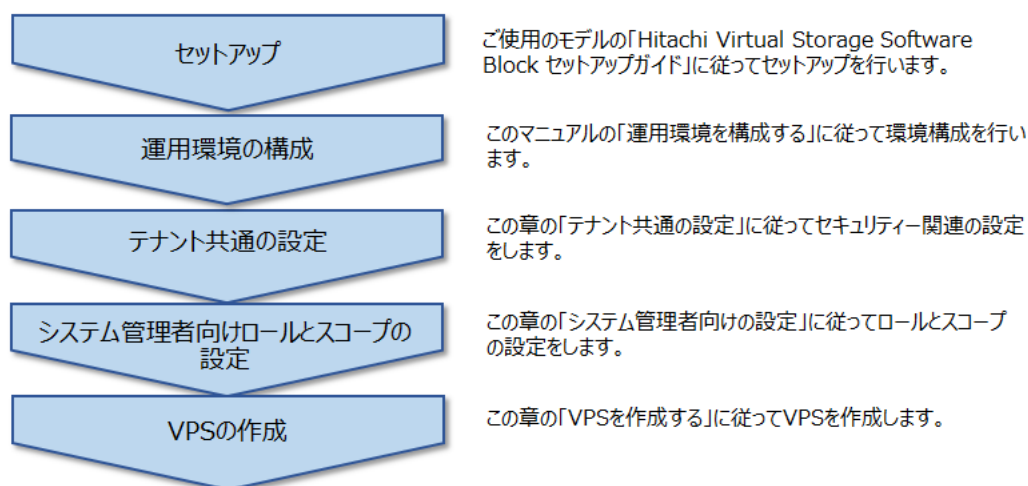
大規模ストレージシステムにおいて、1つのストレージのリソースを複数のテナント(会社や部署)で分配または共有利用できるようにする機能をマルチテナンシーと呼びます。

VSP One SDS Block のマルチテナンシー機能は、会社資産のストレージシステムを複数部署など同一社内でも共有する場合を想定しています。マルチテナンシー機能によって分配された個々のテナントごとのストレージを、仮想プライベートストレージ(VPS : Virtual Private Storage)と呼びます。

コンピュータノードとコントローラーノードはテナントごとに用意します。



マルチテナンシーの構築までの流れと参照先は以下のとおりです。



VPS 管理者

マルチテナンシー構成において、個々の VPS を管理する管理者を VPS 管理者と呼びます。

各 VPS は、システム管理者によって作成されます。VPS 作成時には、その VPS に作成可能なリソースの上限などの条件を設定でき、VPS 管理者はこの条件の範囲内でストレージソフトウェアの機能を利用できます。VPS 管理者による VPS の運用方法については「Hitachi Virtual Storage Platform One SDS Block 仮想プライベートストレージ管理者向けオペレーションガイド」を参照してください。

作成できるリソースと所属

VPS には以下のリソースを作成できます。作成したリソースは、作成したユーザーと同じ VPS に所属するリソースになり、所属する VPS の ID を属性に持つことになります。

- ボリューム(スナップショットボリュームを含む)
- コンピュートノード
- ボリュームとコンピュートノードの接続(ボリュームパス)
- コンピュートノードのアクセス経路(コンピュートノードパス)
- イニシエーター
- ユーザー
- ユーザーグループ
- セッション

リソースは、1 つの VPS に所属するか、どの VPS にも所属しないシステム所属かのいずれかです。どの VPS にも属さないシステム所属リソースの VPS の ID と名前は"(system)"になります。

VPS 作成以前に存在したリソースはすべて、どの VPS にも属さないシステム所属のリソースになります。

外部認証サーバー上で VPS 管理者をグループ単位で管理しているケースでは同一のユーザーが複数の VPS に所属できます。その場合、VPS の ID は"(multiVpsMembership)"になります。VPS の ID が"(multiVpsMembership)"のユーザーが管理操作を行う場合、アクセスする VPS を特定するため操作対象のリソースが所属する VPS の ID 指定が必要です。

スコープ

スコープは、ユーザーが操作できるリソースの範囲を指定するものです。スコープはユーザーグループに設定され、どのユーザーグループに所属するかによって、ユーザーのスコープが決定します。

ビルトインユーザーグループのスコープには、"(system)"だけが設定されています。"(system)"だけが設定されているユーザーグループに所属しているユーザーは、VPS 外にあるシステム所属のリソースにのみアクセスできます。

システム管理者向けのユーザーグループのスコープは、デフォルトで"(system)"になります。複数の VPS をスコープに追加することもできます。

VPS 管理者向けのユーザーグループのスコープには、作成したユーザーが所属する VPS がデフォルトで設定されます。



メモ

- システム管理者向けのロールのうち Monitor、Audit、Service、Resource には、スコープによる操作範囲の制限は適用されません。
- 所属する VPS の数が増えると、REST API または CLI の操作の性能に影響があります。そのため、外部認証サーバー上でユーザーをグループ単位で管理しているケースで、ユーザーグループのスコープに割り当てる VPS は、必要最低限になるよう運用してください。

マルチテナンシー構成におけるロールと操作

ロールはユーザーグループに設定され、どのユーザーグループに所属するかによって、ユーザーのロールが決定します。ロールによって、ユーザーが実行できる操作(REST API または CLI)が決まります。

システム管理者のうち、VPS の管理操作(VPS の作成・編集・削除)を行うのに必要なロールは Resource です。Resource ロールを持つビルトインユーザーグループとして、StorageAdministrators と SystemAdministrators が用意されています。

VPS 管理者として用意されているロールには VpsSecurity、VpsStorage、VpsMonitor があります。

システム管理者と VPS 管理者が行うロールごとの操作は以下のようになります。

区分	ロール	マルチテナンシー構成における操作
システム管理者	Security	セキュリティー全般の管理者ですが、マルチテナンシー構成においては、原則として VPS 内のユーザーの変更は VPS 管理者 (VpsSecurity)に任すようにします。 VPS 作成/削除時には、VPS 管理者を作成/削除します。 システム所属(VPS 外)のリソースとスコープを持つ VPS のリソースを操作できます。
	Storage	ストレージ全般の管理者ですが、マルチテナンシー構成においては、原則として VPS 内のボリュームやコンピュートノードの変更は VPS 管理者(VpsStorage)に任すようにします。 障害対応で異常ボリュームの削除などを代行する場合があります。 システム所属(VPS 外)のリソースとスコープを持つ VPS のリソースを操作できます。
	RemoteCopy	リモートコピー全般の管理者です。Universal Replicator の操作を行う場合は、VSP One SDS Block 全体の Universal Replicator の管理者(全スコープ)に依頼してください。
	Monitor	ストレージ全般の管理者(参照のみ)として、ボリュームの障害を検知するために、VPS 内のボリュームも参照できます。
	Audit	監査ログ全般の管理者としてすべての VPS を監査できます。
	Service	ストレージ全般の保守管理者です。
	Resource	VPS にリソースを割り当てる管理者です。具体的には、VPS の参照・作成・編集・削除が行えます。
VPS 管理者	VpsSecurity	VPS のセキュリティー管理者です。自身が担当する VPS 内のユーザー管理を担います。セキュリティー管理者として必要な、ユーザー、ユーザーグループ、セッションの管理用の操作が許可されます。また、VPS 内のユーザー、ユーザーグループ設定の際に必要な外部認証サーバー設定の参照が許可されます。
	VpsStorage	VPS のストレージ管理者です。ストレージ管理者として必要な、以下のリソースの管理用操作が許可されます。 ・ ボリューム(スナップショットボリュームを含む) ・ コンピュートノード ・ ボリュームとコンピュートノードの接続(ボリュームパス) ・ コンピュートノードのアクセス経路(コンピュートノードパス) ・ イニシエーター

区分	ロール	マルチテナンシー構成における操作
	VpsMonitor	自身が担当する VPS 内の以下のリソースについて参照のみが許可されます。 ・ ボリューム(スナップショットボリュームを含む) ・ コンピュートノード ・ ボリュームとコンピュートノードの接続(ボリュームパス) ・ コンピュートノードのアクセス経路(コンピュートノードパス) ・ イニシエーター



メモ

VPS 管理者に許可される具体的な操作については「Hitachi Virtual Storage Platform One SDS Block 仮想プライベートストレージ管理者向けオペレーションガイド」を参照してください。

システム管理者と VPS 管理者の役割分担

システム管理者と VPS 管理者は以下のように役割を分担して実施してください。

リソースの所属	区分	管理者
システム所属(VPS 外)		システム管理者
VPS 内	通常時	VPS 管理者
	異常時	システム管理者と VPS 管理者が協調して対応

構成情報のバックアップ

システム管理者は構成変更操作を行ったあとの一連の手順の中で構成情報のバックアップを実施しますが、マルチテナンシー構成においては、VPS 管理者は構成情報のバックアップができないため、システム管理者の構成変更操作時のバックアップに加えて、1 日に 1 回など定期的に、システム管理者が構成情報のバックアップを実施してください。最終バックアップ時刻以降の操作で変更した構成を復元するためには、監査ログの Syslog サーバー転送設定をして、監査ログがストレージクラスター以外にも保存されるようにしておく必要があります。構成リストア実施後に、最終バックアップ時刻以降の操作履歴を監査ログ管理権限をもつシステム管理者に取得してもらってください。取得した監査ログを用いて操作を特定し、同じ操作を同じ順序で実施することで、最終バックアップ時刻以降の構成変更を復元してください。



注意

- ・ 構成リストア実施後に、監査ログから操作を特定し再現することで復元した構成情報の UUID は、新しい UUID に変化しています。UUID で管理している構成情報がある場合、新しい UUID で操作し直してください。
- ・ 構成情報のバックアップは、「構成バックアップを行う<<Bare metal>><<Cloud for AWS>>」の前提条件を満たさない場合に失敗します。構成情報の定期的なバックアップをスクリプトなどで自動化する場合は、バックアップが失敗したときにリトライするようにしてください。繰り返し失敗する場合は、構成情報のバックアップのリトライをやめ、失敗時のメッセージに従って対処するとともに、前提条件を満たしているか確認してください。

39.2 VPS に関する設定について<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

VPS 構成のストレージクラスターに作成できるリソースの数や性能の設定値には上限があります。収容するテナントの要件を基に、上限に納まるかどうかを事前に検討する必要があります。必要に応じて、ストレージノードやドライブの増設などの検討が必要になります。

これらの値は、VPS 作成時に指定でき、VPS 作成後に編集できます。

項目	決め方と上限値
VPS 名	VPS の名前です。 以下の規則に従ってください。 - 各 VPS は異なる名称であること "system"は予約語のため使用不可 32 文字(32[byte])まで - 使用可能な文字 - 英数字(英字の場合、大文字・小文字を区別する) "-"(ハイフン) ","(コンマ) "."(ドット) ":"(コロン) "@"(アットマーク) "_"(アンダースコア)
ユーザーグループ数の上限	VPS に作成できるユーザーグループ数の上限です。 以下の上限値を超えない範囲で、VPS に割り当てる数を設定します。 VPS 管理者用のユーザーグループ数の上限：256
ユーザー数の上限	VPS に作成できるユーザー数の上限です。 以下の上限値を超えない範囲で、VPS に割り当てる数を設定します。 VPS 管理者用のユーザー数の上限：256 (外部認証・外部認可はサポートされません。)
セッション数の上限	VPS に作成できるセッション数の上限です。 以下の上限値を超えない範囲で、VPS に割り当てる数を設定します。 VPS 管理者用のセッション数の上限：436
コンピュータノード数の上限	VPS に作成できるコンピュータノード数の上限です。 以下の上限値を超えない範囲で、VPS に割り当てる数を設定します。 システム全体での上限値：1,024
ボリューム数の上限	VPS に作成できるボリューム数の上限です。 以下の上限値を超えない範囲で、VPS に割り当てる数を設定します。 システム全体での上限値は以下のとおりです。 - HPEC 4D+1P または Mirroring Duplication の場合 - フォールトドメイン数 1 の場合：32,768 - フォールトドメイン数 3 の場合：30,720 - HPEC 4D+2P の場合：16,384
ボリューム総容量の上限	VPS に作成できるボリューム総容量の上限です。ボリュームの管理領域は含みません。 VPS にはその時点のストレージプールの容量以上のボリューム総容量の上限を設定できます。この場合、ストレージプール容量が不足したときにドライブやストレージノードを増設してストレージプールの容量の拡張が必要になります。 システム全体での上限値を超えるボリューム総容量の上限は設定できません。 システム全体での上限値は、(増設可能な最大ストレージノード数) × (ストレージノード当たりの上限値)となり、以下のとおりです。 - HPEC 4D+1P の場合：32 × 96.1 = 3,075.2[TiB] - HPEC 4D+2P の場合 - フォールトドメイン数 1 の場合：32 × 96.0 = 3,072[TiB]

項目	決め方と上限値
	・ フォールトドメイン数 3 の場合 : $30 \times 96.0 = 2,880$[TiB] ・ Mirroring Duplication の場合 ・ フォールトドメイン数 1 の場合 : $32 \times 96.8 = 3,097.6$[TiB] ・ フォールトドメイン数 3 の場合 : $30 \times 96.8 = 2,904$[TiB]
単一ボリューム容量の上限	単一ボリューム容量の上限です。単一ボリューム容量に上限を設けない場合は、-1 を指定するか、指定を省略します。 システムの上限値を超える値は設定できません。システムの上限値は以下のとおりです。 ・ HPEC 4D+1P の場合 : 96.1[TiB] ・ HPEC 4D+2P の場合 : 96.0[TiB] ・ Mirroring Duplication の場合 : 96.8[TiB]
ボリューム性能上限[IOPS]	VPS 内に作成されるボリュームの性能上限[IOPS]の値です。 値域は 100～2,147,483,647 です。設定しない場合は、-1 を指定するか、指定を省略します。
ボリューム性能上限[MiB/sec]	VPS 内に作成されるボリュームの性能上限[MiB/sec]の値です。 値域は 1～2,097,151 です。設定しない場合は、-1 を指定するか、指定を省略します。
性能上限に関するアラートしきい値 [sec]	ボリューム性能上限[IOPS]またはボリューム性能上限[MiB/sec]を設定している場合にのみ設定できます。VPS 内に作成されるボリュームの性能上限アラートしきい値の設定値です。いずれかのボリューム性能上限に到達してから、その状態が継続し、継続時間がアラートしきい値に設定した時間に達した場合に、イベントログを出力して通知します。 値域は 1～600 です。-1 を指定するとイベントログは出力されません。
ボリュームの容量削減設定	VPS 内に作成されるボリュームの容量削減の設定です。Disabled、Compression のどちらかを選択できます。設定しない場合は Disabled を指定するか、指定を省略します。

その他、以下の上限値があります。

- ・ イニシエーター数 : (コンピュートノード数の上限 $\times$ 4)の計算結果が自動で設定されます。
- ・ ボリュームパス数 : (ボリューム数の上限 $\times$ 2)の計算結果が自動で設定されます。

容量削減機能の設定について

容量削減機能の設定についての詳細は「ボリュームの容量削減機能の概要」を参照してください。

VPS に容量削減機能を設定すると、VPS 内にボリュームを作成した際に、VPS の容量削減機能の設定がボリュームに自動で設定されます。

VPS 管理者は VPS の容量削減機能の設定で指定されたボリュームのみ作成ができます。

システム管理者は VPS の容量削減機能の設定によらず、個別に容量削減機能を指定してボリュームを作成できます。

VPS に設定するリソース上限値とシステム上限値に関する注意事項

各 VPS に割り当て可能なリソースの上限はシステム全体での上限値ですが、複数の VPS に割り当てたリソースの合計がシステム上限を超えるような設定はできません。そのように設定した場合には、イベントログ KARS16155-W が出力されます。

各 VPS に定めた上限までリソースを確実に作成できるようにするためには、VPS に割り当てるリソースの合計がシステム上限を超えないように設定してください。作成済みの VPS に割り当て済みのリソース数の合計値は「VPS の情報の一覧を取得する <<Bare metal>>」の手順で取得できます。

QoS に関する設定について

VPS に設定できる項目のうち、ボリューム性能上限[IOPS]、ボリューム性能上限[MiB/sec]、性能上限アラートしきい値[sec]は、QoS に関する項目です。QoS についての詳細は「Quality of Service(QoS)機能について」を参照してください。

VPS にこれらを設定すると、VPS 内にボリュームを作成した際に、VPS の QoS 設定がボリュームに自動で設定されます。

VPS 内のボリュームには個別にも QoS の設定ができます。システム管理者の場合、VPS の QoS 設定にかかわらずボリューム単位で QoS の設定ができますが、VPS 管理者の場合は、VPS に設定された QoS の設定よりも小さな値しか設定できません。また、VPS 管理者は性能上限アラートしきい値をボリューム個別には設定できません。

VPS 単位で性能上限を設定する場合は、以下の計算式の結果を基に設定します。

- ボリューム性能上限 × ボリューム数

性能上限アラートしきい値を設定すると、性能上限を設定した任意のボリュームで、性能上限到達時間[IOPS]がしきい値の時間[sec]継続した際にイベントログ KARS06600-W が出力されます。

VPS に性能上限アラートしきい値を設定する場合には、VPS 管理者にボリューム個別で性能上限を設定しないよう依頼してください。

VPS 内リソースの名称について

VPS に作成するユーザー、ユーザーグループ、ボリューム、コンピュートノードの名前はストレージクラスター内でユニークである必要があります。そのため、これらのリソースを作成する際には VPS 名を接頭語にするなど名前の重複を回避するための命名規則を定めて運用するよう VPS 管理者に依頼してください。

39.3 テナント共通の設定 <<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

下表に記載の項目は、全 VPS に共通となるため、システム管理者の責任で設定します。外部認証の設定は、外部認証サーバーに VPS 管理者のアカウント情報を含む点を除いて、マルチテナンシー構成ではない運用の場合と同等です。

以下を参考に、必要に応じて設定してください。

設定項目	設定内容
外部認証サーバー	システム管理者と各 VPS 管理者のアカウント情報を保持する外部認証サーバーの情報を設定します。 外部認証サーバーは、ストレージクラスターで 1 つしか指定できません。正確には、primary と secondary の 2 つが指定できますが、2 つ指定した場合、両者は同じツリー構造を持つ必要があります。テナントはそれぞれが異なるユーザーを持ちますから、テ

設定項目	設定内容
	ナントごとに Active Directory サーバーを持つ構成にはできませんので、注意してください。
監査ログ	監査ログすべて(VPS の操作含む)を集約するログサーバーの情報を設定します。
ユーザー認証	すべてのユーザーが守るべきパスワード規則を指定します。
イベントログ	イベントログの syslog 転送、SMTP 転送を設定します。
コンピュータポート	iSNS サーバー、iSCSI 名、FC 接続のネットワークポロジータを設定します。
CHAP 認証	CHAP 認証を設定します。
ログイン時・CLI Basic 認証時に表示するメッセージ	ログイン時・CLI Basic 認証時に表示するメッセージを設定します。
許可リスト	コントローラーノードの IP アドレスまたは IP アドレスの範囲 (CIDR 表記)を許可リストに設定します。

39.4 システム管理者向けの設定《Bare metal》

この節での記述内容は Bare metal モデルに適用されます。

VPS 内のリソースの変更は、VPS 管理者に任せておき、システム管理者は障害の対処や VPS を削除する際の残リソースの削除作業など、システム管理者が VPS 内リソースを変更する必要があるときのみスコープの追加をしてください。また、リソース操作が完了次第、該当のユーザーグループのスコープに割り当てられている VPS の記述を、ユーザーグループから削除するようにしてください。具体的には、システム管理者には、次表のようにロールとスコープを割り当てることをお勧めします。

システム管理者の 責任範囲	割り当てロール	割り当てスコープ	備考
セキュリティ管理	Security、Monitor	system	必要に応じて個別 VPS をスコープに追加します。外部認証・外部認可ユーザーの場合は、必要に応じて個別 VPS の管理権限を持つユーザーグループを付与します。
ストレージ管理	Storage、RemoteCopy、Monitor、Resource	system	必要に応じて個別 VPS をスコープに追加します。外部認証・外部認可ユーザーの場合は、必要に応じて個別 VPS の管理権限を持つユーザーグループを付与します。
ストレージ管理(参照のみ)	Monitor	指定は不要です。	-
監査ログ管理	Audit、Monitor	指定は不要です。	-
ストレージ保守管理	Storage、RemoteCopy、Service	system	必要に応じて個別 VPS をスコープに追加します。外部認証・外部認可ユーザーの場合は、必要に応じて個別 VPS の管理権限を持つユーザーグループを付与します。

システム管理者の 責任範囲	割り当てロール	割り当てスコー プ	備考
全権を付与する管理 者	Security、Storage、 RemoteCopy、Monitor、 Audit、Service、Resource	system	必要に応じて個別 VPS をスコープに追 加します。外部認証・外部認可ユーザ ーの場合は、必要に応じて個別 VPS の管 理権限を持つユーザーグループを付与 します。

また、VPS の数が増えると、REST API または CLI の操作の性能に影響があります。そのため、システム管理者のユーザーグループのスコープに割り当てる VPS は、必要最低限になるよう運用してください。



メモ

参考として、VPS を 64 個作成したシステムで、以下の管理操作を実行する場合、最大 10 秒ほど掛かる場合があります。

- ・ ユーザーグループの一覧を取得する
- ・ ユーザーグループを作成する
- ・ ユーザーグループ情報を編集する

VPS を 64 個作成したシステムで、以下の管理操作を実行する場合、最大 20 秒ほど掛かる場合があります。

- ・ ユーザー情報の一覧を取得する
- ・ VPS の情報の一覧を取得する

また、ユーザーグループのスコープに複数の VPS を割り当てると、すべての REST API または CLI の性能に影響があり、応答まで 10～30 秒ほど掛かる場合があります。

39.5 VPS を作成する ≪Bare metal≫

この節での記述内容は Bare metal モデルに適用されます。

VPS は、最大 64 個作成できます。

VPS の作成に必要なすべての手順を以下の表に示します。この節の「操作手順」では、表中の No.3 で行う操作方法を説明しています。その他の項目の操作方法は、該当する説明箇所を参照してください。

No.	必要なロール	作業
1	Security Storage	「テナント共通の設定 ≪Bare metal≫」を参照して、テナント間で共通の設定をします。
2	Security	「システム管理者向けの設定 ≪Bare metal≫」を参照して、システム管理者用のユーザー、ユーザーグループを作成します。
3	Resource	本節「VPS を作成する ≪Bare metal≫」の操作手順を実施して、VPS を作成します。
4	Security	Security 管理者自身が所属するユーザーグループのスコープに、作成した VPS を追加します。 Security 管理者に作成した VPS のスコープを付与するには、Security 管理者が所属するユーザーグループを編集して当該 VPS のスコープを指定するか、当該 VPS のスコープを持つユーザーグループに Security 管理者を追加します。 ユーザーグループを編集する場合は、スコープの指定に "system" も含めてください。「ユーザーグループ情報を編集する」または「ユーザーをユーザーグループに追加する」を参照してください。
5	Security	VPS 内に VpsSecurity ロールを持つユーザーグループを作成します。

No.	必要なロール	作業
		「ユーザーグループを作成する」を参照してください。
6	Security	VPS 内にユーザー(VPS 内のセキュリティ管理者)を作成します。上記(No.5)で作成したユーザーグループの所属にします。 「ユーザーを作成する」を参照してください。
7	Security	Security 管理者自身が所属するユーザーグループを編集し、作成した VPS をスコープから外します。 「ユーザーグループ情報を編集する」を参照してください。
8	Security	上記(No.6)で作成したユーザー名とパスワードを VPS 管理者に連絡し、「Hitachi Virtual Storage Platform One SDS Block 仮想プライベートストレージ管理者向けオペレーションガイド」を参照して、必要なユーザーやユーザーグループなどのリソースを作成するよう依頼します。

前提条件

- 実行に必要なロール：Resource

操作手順

1. ストレージプールの ID を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

2. VPS を作成します。

ストレージプールの ID と VPS 作成のパラメーターを指定してコマンドを実行します。

各パラメーターに設定可能な最大値は「VPS に関する設定について<<Bare metal>>」を参照してください。

REST API : POST /v1/objects/virtual-private-storages

CLI : vps_create

VPS のイニシエーター数とボリュームパス数の上限値は、以下の計算式に基づき設定されます。

- イニシエーター数の上限値：コンピュータノード数の上限 × 4
- ボリュームパス数の上限値：ボリューム数の上限 × 2

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

39.6 VPS の利用状況を確認する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

各 VPS に割り当てたリソース/性能の数量、または実際の使用状況は下記の方法で確認できます。日々の監視、またはトラブル発生時に割り当て量/使用量の妥当性の判断に利用してください。

区分	使用状況	コマンド	説明
リソース	上限値	REST API : GET /v1/objects/virtual-private-storages	VPS 内に作成が許される上限値を確認できます。実際に作成できるか

区分	使用状況	コマンド	説明
		CLI : vps_list	どうかはストレージクラスターの空きリソースによります。
	使用量	REST API : GET /v1/objects/virtual-private-storages CLI : vps_list	VPS 内で実際に使っている量を確認できます。
ボリューム性能	上限値	REST API : GET /v1/objects/virtual-private-storages CLI : vps_list	VPS 内の全ボリュームに適用される IOPS や transferRate[MiB/sec] の上限を確認できます。
	使用量	REST API : GET /v1/objects/performances/volumes/<id > CLI : volume_performance_show REST API : GET /v1/objects/detail-performances/volumes/<id > CLI : volume_detail_performance_show	個々のボリュームに対して、IOPS や transferRate[MiB/sec]を確認できます。性能問題の起きているボリュームが上限値に達していたら、上限値の見直しを検討する必要があります。

39.7 VPS の情報の取得<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

VPS の情報が一覧または個別に取得できます。

39.7.1 取得できる VPS の情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。また、Security、Storage、Monitor、Service ロールで一覧取得する場合、作成済みの VPS 数やユーザー数などの合計数、およびそれらについて設定された上限の合計数が得られます。

- id : VPS の ID
- name : VPS の名前
- upperLimitForNumberOfUserGroups : VPS のユーザーグループ数の上限
- numberOfUserGroupsCreated : VPS の作成済みユーザーグループ数
- upperLimitForNumberOfUsers : VPS のユーザー数の上限
- numberOfUsersCreated : VPS の作成済みユーザー数
- upperLimitForNumberOfSessions : VPS のセッション数の上限
- numberOfSessionsCreated : VPS の作成済みセッション数
- upperLimitForNumberOfServers : VPS のコンピュータノード数の上限
- numberOfServersCreated : VPS の作成済みコンピュータノード数
- upperLimitForNumberOfHbas : VPS のイニシエーター数の上限
- numberOfHbasCreated : VPS の作成済みイニシエーター数
- upperLimitForNumberOfVolumeServerConnections : VPS のボリュームとコンピュータノードの接続情報数の上限
- numberOfVolumeServerConnectionsCreated : VPS の作成済みボリュームとコンピュータノードの接続情報数

- volumeSettings : VPS のボリュームに関する情報
 - poolId : 使用するストレージプールの ID
 - upperLimitForNumberOfVolumes : VPS のボリューム数の上限
 - numberOfVolumesCreated : VPS の作成済みボリューム数
 - upperLimitForCapacityOfVolumes : VPS のボリューム総容量の上限[MiB]
 - capacityOfVolumesCreated : VPS の作成済みボリューム総容量[MiB]
 - upperLimitForCapacityOfSingleVolume : VPS の単一ボリューム容量の上限[MiB]
 - savingSettingOfVolume : VPS のボリュームの容量削減機能の設定
 - savingModeOfVolume : VPS の容量削減機能の処理モード
 - qosParam
 - upperLimitForIops : VPS のボリューム性能上限[IOPS]
 - upperLimitForThroughput : VPS のボリューム性能上限[MiB/sec]
 - upperLimitForAlertThreshold : VPS のボリューム性能上限に関するアラートしきい値 [sec]

39.7.2 VPS の情報の一覧を取得する <<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

各 VPS の情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. VPS の情報の一覧を取得します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

39.7.3 VPS の情報を個別に取得する <<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

指定した ID の VPS の情報を取得します。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

1. VPS の ID を確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

2. VPS の情報を取得します。

VPS の ID を指定してコマンドを実行します。

REST API : GET /v1/objects/virtual-private-storages/<id >

CLI : vps_show

39.8 VPS の設定を編集する《Bare metal》

この節での記述内容は Bare metal モデルに適用されます。

VPS の設定を編集します。

前提条件

- 実行に必要なロール : Resource

操作手順

1. 設定を編集する VPS の ID と VPS に作成済みのリソースを確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

2. upperLimitForCapacityOfSingleVolume を変更する場合、VPS 内のボリューム一覧を参照し、VPS に作成済みのボリュームで最大の容量を確認します。

REST API : GET /v1/objects/volumes

CLI : volume_list

3. VPS の設定を編集します。

VPS の ID と編集内容を指定してコマンドを実行します。

各パラメーターに設定可能な最大値は「VPS に関する設定について《Bare metal》」を参照してください。

編集のパラメーターを 1 つも指定しないでコマンドを実行した場合、ジョブは失敗します。

QoS 以外の上限値を編集する場合、VPS 内に作成済みのリソース数や容量を下回る値を設定してコマンドを実行した場合、ジョブは失敗します。

REST API : PATCH /v1/objects/virtual-private-storages/<id >

CLI : vps_set

コマンド実行後に表示されるジョブの ID を確認します。

4. QoS、ボリューム容量削減機能の設定を編集した場合、VPS 内に作成済みボリュームについての QoS 設定、ボリューム容量削減機能の設定は変更されません。

QoS の場合は「ボリュームの設定を編集する」を参照して、個別にボリュームの設定を編集します。



メモ

作成済みボリュームの容量削減機能の設定は変更できません。

5. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

39.9 VPS を削除する《Bare metal》

この節での記述内容は Bare metal モデルに適用されます。

VPS を削除します。

VPS の削除に必要なすべての手順を以下の表に示します。この節の「操作手順」では、表中の No.6 で行う操作方法を説明しています。その他の項目の操作方法是、該当する説明箇所またはマニュアルを参照してください。

No.	必要なロール	作業
1	VpsStorage	VpsStorage ロールを持つ VPS 管理者に依頼して、削除対象の VPS 所属のボリュームやコンピュータノードを削除してもらいます。 「Hitachi Virtual Storage Platform One SDS Block 仮想プライベートストレージ 管理者向けオペレーションガイド」を参照してください。
2	VpsSecurity	VpsSecurity ロールを持つ VPS 管理者に依頼して、削除対象の VPS 所属のユーザーとユーザーグループを削除してもらいます。 ただし、自身のログインに使用しているユーザーとユーザーグループは残します。 「Hitachi Virtual Storage Platform One SDS Block 仮想プライベートストレージ 管理者向けオペレーションガイド」を参照してください。
3	Security	Security 管理者自身が所属するユーザーグループの範囲に、削除対象の VPS を追加します。 Security 管理者に削除対象の VPS の範囲を付与するには、Security 管理者が所属するユーザーグループを編集して当該 VPS の範囲を指定するか、当該 VPS の範囲を持つユーザーグループに Security 管理者を追加します。 「ユーザーグループ情報を編集する」または「ユーザーをユーザーグループに追加する」を参照してください。
4	Security	削除対象の VPS 所属のユーザー、ユーザーグループ、セッションをすべて削除します。削除対象の VPS への個別のアクセス権を与えていた(システム所属の)ユーザーグループがあれば、その VPS を範囲から削除します。 「ユーザーを削除する」「ユーザーグループを削除する」または「セッションを削除する」を参照してください。
5	Security	Security 管理者自身が所属するユーザーグループの範囲から、削除対象の VPS を削除します。 「ユーザーグループ情報を編集する」を参照してください。
6	Resource	本節「VPS を削除する <<Bare metal>>」の操作手順を実施して、VPS を削除します。

前提条件

- 実行に必要なロール : Resource

操作手順

- 削除する VPS の ID と VPS に作成済みのリソースを確認します。

REST API : GET /v1/objects/virtual-private-storages

CLI : vps_list

- VPS を削除します。

VPS の ID を指定してコマンドを実行します。

VPS 内にリソースが残っていたり、VPS を範囲に含むユーザーグループが残っていたりした場合、ジョブは失敗します。

REST API : DELETE /v1/objects/virtual-private-storages/<id >

CLI : vps_delete

コマンド実行後に表示されるジョブの ID を確認します。



ヒント

すべてのユーザーグループの scope に削除したい VPS が 1 つでも含まれている場合、その VPS は削除できません。ユーザーグループには、VPS 管理者用のユーザーグループとシステム管理者用のユーザーグループがあります。そのため、あらかじめ、以下の操作手順に従って削除する VPS の ID を検索し、ユーザーグループから取り除いてから VPS を削除してください。

1. クエリーパラメーター `vpsId` に "system" を指定してユーザーグループの一覧を取得し、各ユーザーグループの `scope` に削除する VPS の ID が残っているかを確認します。
2. クエリーパラメーター `vpsId` に削除する VPS の ID を指定してユーザーグループの一覧を取得し、各ユーザーグループの `scope` に削除する VPS の ID が残っているかを確認します。
ここで、ユーザーグループの一覧を取得するユーザーは、削除する VPS の `scope` を持つユーザーグループに所属している必要があります。
3. 上記手順の 1、2 の実行結果から見つかった削除しようとしている VPS の ID を `scope` に持つユーザーグループを確認し、ユーザーグループを編集して、`scope` に含まれる VPS の ID をユーザーグループから削除するか、不要なユーザーグループだった場合はそのユーザーグループを削除してください。

3. ジョブの ID を指定してジョブの state を確認します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

39.10 性能低下・操作不可の監視と対処 <<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

I/O 性能の低下や管理操作の失敗などの発生に備え、システム管理者は以下に従って監視と発生時の対処を実施してください。

監視対象	問題が発生したときの各 VPS への影響	監視方法	問題の回避または対処方法
I/O リソース	I/O 性能の低下	システムの性能情報を監視します。	- ボリュームまたは VPS に QoS を設定します。 - I/O 流入の大きなボリュームの QoS を変更します(制約を強くします)。 - ドライブまたはストレージノードの増設によってストレージクラスターの性能を增強します。
ストレージプール容量	- スナップショット作成不可¹ - 通常ボリュームの作成不可² - スナップショット障害² - I/O 不可²	ストレージプール容量またはヘルスステータスを監視します。	- VPS 管理者は VPS 内の不要なボリュームを削除するか、システム管理者にシステム所属の不要なボリュームを削除するよう要請します。 - ドライブまたはストレージノードを増設します。
容量バランス	I/O 性能の低下	通常は、定常監視は不要です。	このマニュアルの「容量バランスの概要」を参照して、

監視対象	問題が発生したときの 各 VPS への影響	監視方法	問題の回避または対処方法
		必要に応じてイベントログを監視します。	容量バランスの設定を判断します。
VPS 内リソースの名前の重複	管理操作の失敗	通常は、定常監視は不要です。 必要に応じてリソース一覧を取得して確認します。	VPS 名を接頭語にするなど、VPS 間でリソース名が重複しないようにルールを取り決めます。
各リソースのストレージクラスターでの上限	リソースの新規作成不可	ストレージクラスターでの上限のため、基本的には通常の運用で定常監視は不要です。 - VPS を参照して、各 VPS の作成済みリソース数を確認します。 - 各リソースを一覧参照して作成済みリソース数を確認します。	- VPS に割り当てるリソース数の合計がシステム全体の上限値を超えないようにします。VPS に割り当てたリソース数の合計がシステム上限値を超えた場合は、イベントログ KARS16155-W が出力されます。 - 不要なリソースを削除します。
操作排他による操作の競合	管理操作の失敗	通常は、定常監視は不要です。 必要に応じてイベントログを監視します。	しばらく待ってから再実行をするよう VPS 管理者に依頼します。
1 ストレージコントローラーの使用率が 80%以上のとき 2 ストレージコントローラーの使用率が 100%のとき			

39.11 リソース不足・性能問題発生時の対処<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

リソースや性能が不足すると VPS でエラーや性能問題が起きます。そのような場合は、以下を参考に対処を検討してください。

区分	超過時に起きる現象	VPS 管理者の対処例	システム管理者の対処例
ボリューム容量	ボリューム作成に失敗	VPS 内の不要ボリュームを削除します。	-
		システム管理者にボリューム容量の上限拡大を依頼します。	以下を検討して実施します。 ストレージクラスター全体で VPS に割り当て可能なリソースが余っている場合： - 剰余分のリソースから割り当て ストレージクラスター全体で VPS に割り当て可能なリソースが余っていない場合： - ストレージノード増設でシステムの剰余分のリソースを増やして割り当て

区分	超過時に起きる現象	VPS 管理者の対処例	システム管理者の対処例
			他 VPS で未使用の割り当て済みリソースを回収して再割り当て
ボリューム数	ボリューム作成に失敗	VPS 内の不要ボリュームを削除します。	-
		システム管理者にボリューム数の上限拡大を依頼します。	以下を検討して実施します。 - システム未使用領域からの割り当て - ストレージノード増設によってシステム未使用領域を増やして割り当て - 他 VPS の未使用領域を回収して再割り当て
ボリューム性能 [IOPS]およびボリューム性能[MiB/sec]	性能問題	システム管理者にボリューム数×ボリューム性能の内訳変更を依頼します。	ボリューム数×ボリューム性能の内訳変更を行います。
		システム管理者にボリューム数×ボリューム性能の上限拡大を依頼します。	以下を検討して実施します。 - システム未使用領域からの割り当て - ストレージノード増設によってシステム未使用領域を増やして割り当て - ドライブ増設によってシステム未使用領域を増やして割り当て - 他 VPS の未使用領域を回収して再割り当て
ユーザーグループ数	ユーザーグループ作成に失敗	VPS 内の不要ユーザーグループを削除します。	-
		システム管理者にユーザーグループ数の上限拡大を依頼します。	以下を検討して実施します。 - システム未使用領域からの割り当て - 他 VPS の未使用領域を回収して再割り当て
ユーザー数	ユーザー作成に失敗	VPS 内の不要ユーザーを削除します。	-
		システム管理者にユーザー数の上限拡大を依頼します。	以下を検討して実施します。 - システム未使用領域からの割り当て - 他 VPS の未使用領域を回収して再割り当て
セッション数	セッション作成に失敗 (認証チケット取得や VSP One SDS Block Administrator ログインに失敗)	REST API/CLI の BASIC 認証で操作します。	-
		VPS 内の不要セッションを削除します。	-
		システム管理者にセッション数の上限拡大を依頼します。	以下を検討して実施します。

区分	超過時に起きる現象	VPS 管理者の対処例	システム管理者の対処例
			- システム未使用領域からの割り当て - 他 VPS の未使用領域を回収して再割り当て
コンピュータノード数	コンピュータノード作成に失敗	VPS 内の不要コンピュータノードを削除します。	-
		システム管理者にコンピュータノード数の上限拡大を依頼します。	以下を検討して実施します。 - システム未使用領域からの割り当て - 他 VPS の未使用領域を回収して再割り当て
イニシエーター数	イニシエーター作成に失敗	VPS 内の不要イニシエーターを削除します。	-
		システム管理者にコンピュータノード数の上限拡大を依頼します。	コンピュータノード数の上限を拡大します。
ボリュームパス数	ボリュームパス作成に失敗	VPS 内の不要ボリュームパスを削除します。	-
		システム管理者にボリューム数の上限拡大を依頼します。	ボリューム数の上限を拡大します。

スペアノードを管理する<<Bare metal>>

この章での記述内容は Bare metal モデルに適用されます。

- 40.1 スペアノードの概要<<Bare metal>>
- 40.2 スペアノード切り換えの概要<<Bare metal>>
- 40.3 スペアノードを準備する<<Bare metal>>
- 40.4 スペアノードを利用するための BMC アカウントを準備する<<Bare metal>>
- 40.5 ストレージクラスターに BMC 接続検証用ルート証明書をインポートする<<Bare metal>>
- 40.6 ストレージクラスターから BMC 接続検証用ルート証明書を取得する<<Bare metal>>
- 40.7 ストレージクラスターから BMC 接続検証用ルート証明書を削除する<<Bare metal>>
- 40.8 ストレージノードの BMC 情報を登録・編集する<<Bare metal>>
- 40.9 ストレージノードの BMC 情報の取得<<Bare metal>>
- 40.10 スペアノードの情報を登録する<<Bare metal>>
- 40.11 スペアノードの情報を編集する<<Bare metal>>
- 40.12 スペアノードの情報の取得<<Bare metal>>
- 40.13 スペアノードの情報を削除する<<Bare metal>>
- 40.14 スペアノード機能の設定を確認する<<Bare metal>>

40.1 スペアノードの概要<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

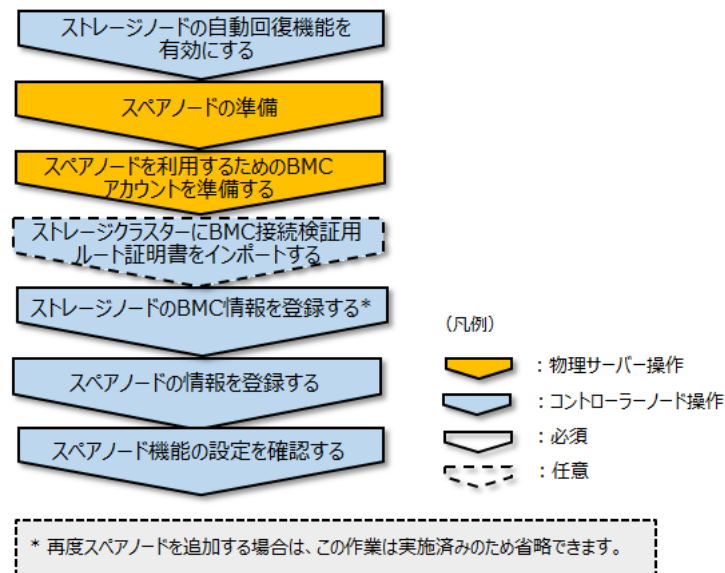
スペアノード機能は、ストレージクラスターに待機用のノードを登録し、障害発生ストレージノードが自動回復による保守回復で復旧できない場合に、障害発生ストレージノードから待機用のノードへ切り換えることで冗長性の回復を行う機能です。

以降、待機用のノードをスペアノードと呼びます。スペアノードは1つのフォールトドメインにつき、1つ登録できます。

スペアノード機能を利用するまでの流れ

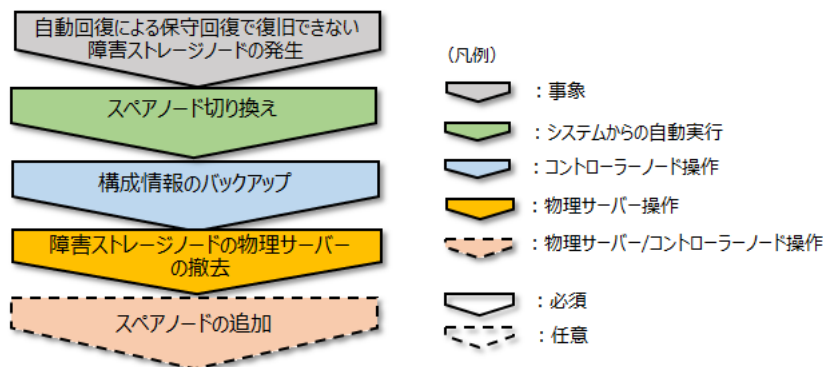
スペアノード機能は、ストレージノードの自動回復機能が有効のときのみ利用可能です。自動回復機能はデフォルト設定で有効です。自動回復機能の設定を確認する、または有効にする場合は、このマニュアルの「ストレージノードの自動回復機能を設定する<<Bare metal>>」を参照してください。

スペアノード機能を利用できるようにするまでの流れを以下に示します。



スペアノードを用いた回復の流れ

スペアノードを用いた障害からの回復は、以下の流れで行われます。



自動回復による保守回復で復旧できない障害ストレージノードが発生した際には、自動回復機能によるスペアノード切り換えによって回復が行われます。スペアノード切り換えの詳細は、このマニュアルの「スペアノード切り換えの概要<<Bare metal>>」を参照してください。

スペアノード切り換えは、自動回復設定が有効のときにのみ行われます。自動回復設定の詳細は、このマニュアルの「ストレージノードの自動回復機能を設定する<<Bare metal>>」を参照してください。

スペアノード切り換えの各処理が完了し、ストレージノードの回復・データの冗長度の回復・障害発生ストレージノードの物理サーバーに搭載されていたドライブの減設が完了したあとに、「構成情報をバックアップする<<Bare metal>> <<Cloud for AWS>>」を参照して構成情報のバックアップを行ってください。

また、スペアノード切り換え後、スペアノードと切り換わったストレージノードの物理サーバーをイベントログ KARS10780-I、KARS10781-I、KARS10782-W から特定し、該当する物理サーバーを撤去してください。物理サーバーの撤去は、ハードウェアベンダーのマニュアルを参照して実施してください。

その後、引き続きスペアノード機能を利用する場合は、再度スペアノードを追加してください。スペアノードの追加は「スペアノード機能を利用するまでの流れ」に従って実施してください。



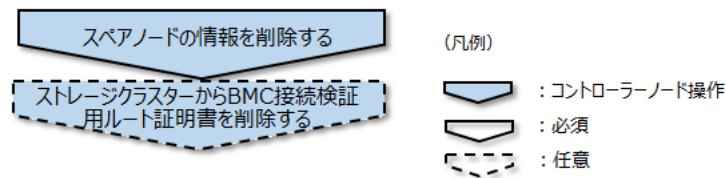
注意

- ・ 「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載されているサーバーモデル以外はスペアノード機能が非サポートのため、スペアノード切り換えができない可能性があります。スペアノード切り換えをサポートしているサーバーモデルについては「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。
- ・ スペアノード機能を使用しているストレージクラスターでは、スペアノード切り換え機能が実施されることで、自動でストレージノードの物理サーバーが切り換わります。ストレージノードの物理サーバーに対して操作・保守を行う際は、下記の内容を確認し、操作・保守する物理サーバーを間違えないように注意してください。
 - ストレージノードに対してスペアノードの物理サーバーが適用され、物理サーバーが切り換わった際は、それを示すイベントログが出力されます。
 - 「ストレージノードの BMC 情報を個別に取得する<<Bare metal>>」を実施することで、ストレージノードの物理サーバーに搭載されている BMC の接続情報が取得できます。その情報を使用して対象のストレージノードの BMC に接続することで、対象のストレージノードの物理サーバーの情報が確認できます。ただし、設定に誤りがある場合は、イベントログにて通知されます。BMC の設定が正しいかどうかの確認は「スペアノード機能の設定を確認する<<Bare metal>>」で行います。
 - 「スペアノードの情報を個別に取得する<<Bare metal>>」を実施することで、スペアノードの物理サーバーに搭載されている BMC の接続情報が取得できます。その情報を使用して対象のスペアノードの BMC に接続することで、対象のスペアノードの物理サーバーの情報が確認できます。ただし、設定に誤りがある場合は、イベントログにて通知されます。BMC の設定が正しいかどうかの確認は「スペアノード機能の設定を確認する<<Bare metal>>」で行います。

- ・ 期待外に OS が起動すると、ストレージノードに残っているネットワーク設定によって、IP アドレス重複などのトラブルを引き起こすことがあります。そのため、撤去するストレージノードに対し、以下を実施してください。
 - ネットワークからの切り離しを行ってください。

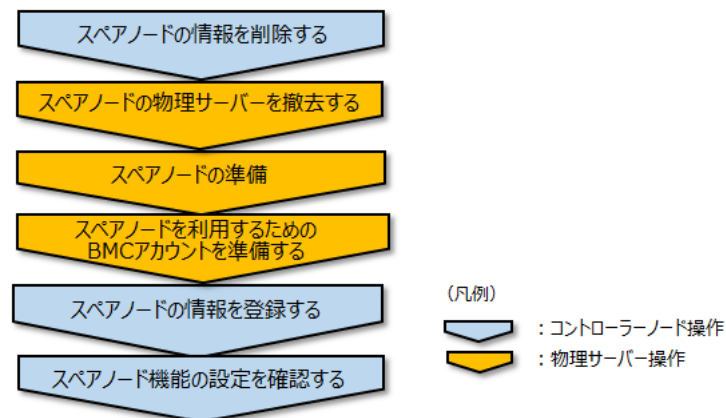
スペアノード機能の利用を停止するまでの流れ

スペアノード機能の利用を停止するための流れは以下のとおりです。



スペアノードの物理サーバーを交換するまでの流れ

予防保守などでスペアノードの物理サーバーを交換する場合の流れは以下のとおりです。



- ・ スペアノード情報の削除は「スペアノードの情報を削除する<<Bare metal>>」に従って実施してください。
- ・ スペアノードの物理サーバーの撤去においては、BMC の Web コンソールからスペアノードの OS シャットダウンを実施後に、ハードウェアベンダーのマニュアルを参照して物理サーバーの撤去を実施してください。
- ・ スペアノードの物理サーバーの撤去後は、上記のフローに従って、再度スペアノードを登録してください。

40.2 スペアノード切り換えの概要<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

スペアノード切り換え機能は、ストレージノードの自動回復機能による保守回復で回復ができなかった障害ストレージノードに対し、障害ストレージノードとスペアノードを切り換えることで回復を行う機能です。保守回復対象をスペアノード切り換えの対象に変更するまでの時間は 15 分から 60 分までの間で指定することができます。

スペアノード切り換え機能では、status が"TemporaryBlockage"(一時閉塞中)のストレージノードに対して以下の機能が自動で順次実施され、ストレージノードの回復・データの冗長度の回復・障害発生ストレージノードの物理サーバーに搭載されていたドライブの減設が行われます。

- ・ 障害ストレージノードの OS シャットダウン
- ・ 障害ストレージノードの OS 起動抑止
- ・ 障害ストレージノードにスペアノードの物理サーバーを適用
- ・ ストレージノード交換(自動回復)
- ・ ストレージプール拡張
- ・ リビルド(データ再構築)
- ・ ドライブ減設

スペアノード切り換えでは、対象のスペアノードに搭載されているすべてのドライブを対象にストレージプール拡張が実施されます。ストレージプール拡張の対象となるドライブが搭載されていない場合は、ストレージプール拡張は実施されません。



注意

- ・ 「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載されているサーバーモデル以外はスペアノード機能が非サポートのため、スペアノード切り換えができない可能性があります。スペアノード切り換えをサポートしているサーバーモデルについては「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。
- ・ 障害発生ストレージノードに搭載されているドライブは、ドライブ減設が完了するまで同じストレージクラスター内での再利用はできません。
- ・ スペアノード切り換えの各処理が行われている間は、対象のスペアノードでの下記の操作を行わないでください。スペアノード切り換えの各処理が失敗することがあります。
 - コンソールインターフェイスへのセットアップユーザーでのログインおよび操作
 - SFTP を使用したスペアノードへの接続
- ・ スペアノード切り換えでは、BMC の提供するサーバー管理 API を使用して障害ストレージノードの電源オフが実行されます。スペアノード切り換えの動作中は障害ストレージノードの電源オンを行わないでください。また、停止した障害ストレージノードの物理サーバーの撤去の際は、ストレージノードの電源オンを行わずネットワークから切り離してください。ネットワークから切り離さず電源オンを実施すると、ストレージクラスターのストレージノードと IP アドレスの重複が発生する可能性があります。
- ・ 停止した障害ストレージノードを、誤って電源オンしたことによる IP アドレス重複を引き起こさないように、障害ストレージノードは OS 起動抑止によって UEFI Shell が起動するようにブート設定が変更されます。
- ・ 「スペアノードを準備する<<Bare metal>>」での前提条件を満たしていない場合、リビルド(データ再構築)とドライブ減設の間でストレージコントローラーへの容量割り付け処理が自動で動作することがあり、その場合はドライブ減設が失敗します。ドライブ減設が失敗した場合、しばらく待てばドライブ減設が自動で動作するため対処不要です。また「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」に従って、保守操作でドライブ減設を行うことでも対処できます。
- ・ 切り離した障害ストレージノードの調査が必要になった場合、ダンプログファイルの採取をサポートセンターから依頼することがあります。



メモ

ストレージノード交換が実施された際に、イベントログ KARS16018-W、KARS16143-W が出力されることがあります。また、ストレージクラスターから切り離された障害ストレージノードの物理サーバーに搭載されたドライブに対して、イベントログ KARS05010-E、KARS07005-E、および KARS06596-E が出力されることがあります。このタイミングでこれらのイベントログが発生することは問題ではなく、スペアノード切り換えによってデータの冗長度の回復・ドライブの減設が完了していれば、これらのイベントログへの対処は不要です。

障害ストレージノードにスペアノードの物理サーバーを適用

スペアノード切り換えの際には、スペアノードとして登録されていた物理サーバーを障害ストレージノードの新たな物理サーバーとして使用できるように設定が行われます。

その際、自動回復による保守回復では復旧できないと判断された障害ストレージノードの物理サーバーに対しては、BMC の提供するサーバー管理 API を使用し OS のシャットダウンと起動抑止が行われたあと、ストレージクラスターから切り離されます。

これによって、スペアノードとして登録されていた物理サーバーが対象のストレージノードに適用され、対象のストレージノードの物理サーバーが切り換わります。

スペアノードがストレージノードに適用され、対象のストレージノードの物理サーバーが切り換わった際には、イベントログ KARS10780-I、KARS10781-I、KARS10782-W が出力されます。



メモ

障害ストレージノードとスペアノードで管理ポートのチーミング機能の設定(冗長構成または非冗長構成)に違いがあっても、スペアノード切り換えは可能です。

障害ストレージノードから引き継がれる情報

以下のような各種設定情報は障害ストレージノードから引き継がれ、障害ストレージノードにスペアノードの物理サーバーを適用する際に物理サーバーに設定されます。

情報の種類	引き継がれる主な情報
ストレージノード情報	・ ストレージノード名
管理ネットワーク情報	・ IP アドレス ・ サブネットマスク ・ ルーティングテーブル ・ MTU サイズ
ストレージノード間ネットワーク情報	・ IP アドレス ・ サブネットマスク ・ ルーティングテーブル ・ MTU サイズ
コンピュータネットワーク情報	・ IP アドレス ・ サブネットマスク ・ ルーティングテーブル ・ MTU サイズ ・ コンピュータポートの接続プロトコル情報 ・ コンピュータポートの種別 ・ コンピュータポートのニックネーム ・ FC ポートのネットワークの接続形態 ・ FC ポートの転送速度



メモ

スペアノード機能を使用しているストレージクラスターでは、スペアノード切り換え機能が実施されることで、自動でストレージノードの物理サーバーが切り換わります。ストレージノードの物理サーバーに対して操作・保守を行う際は、下記の内容を確認し、操作・保守する物理サーバーを間違えないように注意してください。

- BMC 情報や MAC アドレス、チーミング機能など物理サーバーに依存する情報は、障害ストレージノードから引き継がれません。スペアノードの物理サーバーの情報が適用されます。
- ストレージノードに対してスペアノードの物理サーバーが適用され、物理サーバーが切り換わった際は、それを示すイベントログが出力されます。
- 「ストレージノードの BMC 情報を個別に取得する<<Bare metal>>」を実施することで、ストレージノードの物理サーバーに搭載されている BMC の接続情報が取得できます。その情報を使用して対象のストレージノードの BMC に接続することで、対象のストレージノードの物理サーバーの情報が確認できます。ただし、設定に誤りがあった場合は、イベントログにて通知されます。BMC の設定が正しいかどうかの確認は「スペアノード機能の設定を確認する<<Bare metal>>」で行います。
- 「スペアノードの情報を個別に取得する<<Bare metal>>」を実施することで、スペアノードの物理サーバーに搭載されている BMC の接続情報が取得できます。その情報を使用して対象のスペアノードの BMC に接続することで、対象のスペアノードの物理サーバーの情報が確認できます。ただし、設定に誤りがあった場合は、イベントログにて通知されます。BMC の設定が正しいかどうかの確認は「スペアノード機能の設定を確認する<<Bare metal>>」で行います。

スペアノード切り換えの動作条件

スペアノード切り換え機能は、自動回復機能から実施されます。ストレージノードの自動回復機能によるスペアノード切り換えの対象となるのは、以下の条件に当てはまるストレージノードです。

- status が"TemporaryBlockage"(一時閉塞中)に移行したストレージノード
- 切り換えに使用可能なスペアノードが登録されているストレージノード

ストレージノードの自動回復機能によるスペアノード切り換えが動作する条件は以下のとおりです。

- ストレージノードの自動回復機能の設定が有効(true)
ストレージノードの自動回復機能の設定はデフォルトで有効(true)です。有効/無効の設定と設定確認は、REST API または CLI にて実施できます。
- 切り換え可能なスペアノードが登録されている
- ストレージノードに BMC の情報が登録されている
- ストレージノードの交換ジョブの動作条件を満たしている

ストレージノードの自動回復機能の詳細は「ストレージノードの自動回復機能を設定する<<Bare metal>>」を参照してください。

スペアノード切り換えが動作しない例

ストレージノードの自動回復機能の設定を有効にしても、スペアノード切り換えが動作しない場合があります。以下に例を示します。

- ストレージソフトウェアのバージョンアップなど、競合する構成変更が動作している
- 電源障害によって、切り換え対象のストレージノードの BMC へ電源が供給されていない
- 電源障害によって、スペアノードまたはスペアノードの BMC へ電源が供給されていない
- ネットワーク障害によって、切り換え対象のストレージノードの BMC にアクセスできない
- ネットワーク障害によって、スペアノードの管理ネットワークポートまたはスペアノードの BMC にアクセスできない
- ネットワーク障害によって、スペアノードのストレージノード間ネットワークポートにアクセスできない
- ストレージノード、スペアノードの BMC アカウントに付与した権限が適切でない

- ・ ストレージノードに登録している BMC 情報が誤っている
- ・ ストレージクラスターに登録している BMC 接続検証用ルート証明書で、BMC に登録している証明書を検証できない
- ・ スペアノードに登録しているスペアノード情報が誤っている
- ・ コンピュートポートの種別がストレージノードとスペアノードで不一致となっている



メモ

イベントログ KARS13102-E(Cause=UnableToSwitchingSpareNode)の発行前後に、"The spare node is not in a state in which spare node switchover is possible."の文字列を含むイベントログがほかにも発行されていないければ、スペアノードは引き続き利用できます。

40.3 スペアノードを準備する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

スペアノードを準備します。



注意

「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載されているサーバーモデル以外はスペアノード機能が非サポートのため、スペアノード切り換えができない可能性があります。スペアノード切り換えをサポートしているサーバーモデルについては「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。



メモ

スペアノードでの PCI スロット位置が、ストレージクラスター内で動作しているストレージノードでの PCI スロット位置と違いがあった場合でもスペアノード切り換えは可能です。スペアノードでの管理ポートの数は、ストレージクラスター内で動作しているストレージノードでの数と同一である必要はありません。ただし、コンピュータポートの数は、スペアノードとストレージクラスター内で動作しているストレージノードで同一である必要があります。

前提条件

- ・ スペアノードの有効物理容量が稼働しているストレージノードの構成と均一であること
- ・ 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。
- ・ ストレージノードとスペアノードでコンピュータポートの種別が一致していること

操作手順

1. スペアノードのネットワークの物理結線と LAN スイッチの設定を完了させてから、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の以下に記載されている構築準備を行います。
 - ・ 「ストレージノードを準備する」



注意

- ・ スペアノードのメモリー容量は、プロテクションドメインに所属するストレージノード内で最小のメモリー容量以上である必要があります。プロテクションドメイン情報から `minimumMemorySize[MiB]` を参照し、スペアノードに必要なメモリー容量を確認してください。スペアノードに搭載されているメモリー容量が条件を満たしていないときは、条件を満たすようにメモリーを増設してください。

- スペアノードのネットワーク構成または要件については、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「スペアノードに関する設定」、「管理ネットワークの要件」、「コンピュートネットワークの要件(iSCSI)」、「コンピュートネットワークの要件(NVMe/TCP)」、「コンピュートネットワークの要件(FC)」を参照してください。

2. Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の以下の手順を行い、スペアノードに対してストレージソフトウェアのインストールを行います。

- 「ストレージソフトウェアをインストールする」



メモ

「ストレージソフトウェアをインストールする」の手順で使用するストレージソフトウェアインストーラー(hsds-installer-vssb-<version>-<number>.iso)のバージョンは、ストレージクラスターのバージョンに合わせる必要があります。ストレージクラスターのバージョンは以下のコマンドで確認できます。

REST API : GET /v1/objects/storage

CLI : storage_show

3. スペアノードに対して、Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の以下の手順を行い、ストレージノード単位のセットアップを行います。

- 「ストレージノード単位のセットアップを行う」

4. スペアノードを利用するための BMC アカウントを準備してください。

「スペアノードを利用するための BMC アカウントを準備する<<Bare metal>>」を参照してください。

40.4 スペアノードを利用するための BMC アカウントを準備する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

スペアノード機能は、BMC の提供するサーバー管理 API を利用して実現しています。BMC の提供するサーバー管理 API を利用するために必要な権限を BMC のアカウントに付与する必要があります。この節では日立アドバンストサーバ HA8000V シリーズの BMC である iLO のアカウント設定例を記載します。



注意

「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載されているサーバーモデル以外はスペアノード機能が非サポートのため、スペアノード切り換えができない可能性があります。スペアノード切り換えをサポートしているサーバーモデルについては「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。

以下の説明は iLO 上の操作となります。

初めてスペアノード機能を利用する場合は、ストレージクラスター内のすべてのストレージノードと「スペアノードを準備する<<Bare metal>>」で準備したスペアノードに対して以下の手順を実施してください。

スペアノード機能を利用中に、任意のストレージノードもしくはスペアノードを追加または再設定する場合は、当該ストレージノードもしくはスペアノードに対して以下の手順を実施してください。

具体的な操作方法はサーバーベンダーのマニュアルを参照してください。

操作手順

1. ストレージノードの iLO の Web コンソールにログインします。
2. iLO ユーザーアカウントまたはディレクトリーグループを追加し、以下の権限を付与します。

- ・ ログイン
- ・ 仮想電源およびリセット
- ・ iLO の設定を構成

既存ユーザーアカウントまたは既存ディレクトリーグループを使用する場合は、前述の権限が付与されていることを確認します。付与されていない場合は、ユーザーアカウントの編集またはディレクトリーグループの編集より付与してください。具体的な操作方法はサーバーベンダーのマニュアルを参照してください。



注意

- ・ 権限が正しく付与されていないとスベアノード切り換えに失敗します。スベアノード機能を利用する際は、権限の付与を必ず行ってください。

40.5 ストレージクラスターに BMC 接続検証用ルート証明書をインポートする《Bare metal》

この節での記述内容は Bare metal モデルに適用されます。

ストレージクラスターに BMC 接続検証用ルート証明書をインポートします。

ストレージクラスターに BMC 接続検証用ルート証明書がインポートされていると、スベアノード機能で利用する BMC の提供するサーバー管理 API にアクセスするときに、接続先 BMC のサーバー証明書を検証します。インポートされていない場合は、接続先 BMC のサーバー証明書の検証はせずに BMC の提供するサーバー管理 API へアクセスします。

前提条件

- ・ 実行に必要なロール： Security
- ・ インポートするルート証明書の形式は PEM 形式または DER 形式であること

操作手順

1. BMC の IP アドレスまたは IP アドレスに対応する FQDN を Common Name(CN)または Subject Alternative Name(SAN)に設定したサーバー証明書を BMC にインポートします。

ストレージクラスター内のすべての BMC に対して実施してください。

BMC のサーバー証明書の作成および BMC へのサーバー証明書のインポートについては、サーバーベンダーのマニュアルを参照してください。

2. コントローラーノードから BMC にインポートしたサーバー証明書の信頼性を証明するルート証明書をストレージクラスターにインポートします。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

ルート証明書を指定してコマンドを実行します。

REST API : POST /v1/objects/bmc-root-certificate/actions/import/invoke

CLI : bmc_root_certificate_import

コマンド実行後に表示されるジョブの ID を確認します。



メモ

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される次のフィールドがサポートされます。

- 基本制限(Basic Constraints)
- キー使用法(Key Usage)
- サブジェクトキー識別子(Subject Key Identifier)
- 機関キー識別子(Authority Key Identifier)
- 証明書ポリシー(Certificate Policies)
- サブジェクト代替名(Subject Alternative Name)
- 名前の制限(Name Constraints)
- ポリシーの制限(Policy Constraints)
- 拡張キー使用法(Extended Key Usage)
- ポリシー禁止(Inhibit anyPolicy)



注意

すでにルート証明書が登録されている状態で、新しいルート証明書をインポートしたときは、新しいルート証明書で上書き更新されます。
インポートしたルート証明書で BMC にインポートしたサーバー証明書が検証可能かの確認は、このマニュアルの「スペアノードの情報を登録する<<Bare metal>>」のあとに、「スペアノード機能の設定を確認する<<Bare metal>>」で行います。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

40.6 ストレージクラスターから BMC 接続検証用ルート証明書を取得する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

「ストレージクラスターに BMC 接続検証用ルート証明書をインポートする<<Bare metal>>」でインポートした、BMC がスペアノード機能で利用する BMC の提供するサーバー管理 API にアクセスするときに、接続先 BMC のサーバー証明書の信頼性を検証するために使用するルート証明書を取得します。DER 形式のファイルとして出力されます。

前提条件

- 実行に必要なロール : Security

操作手順

1. BMC のサーバー証明書の信頼性を検証するためのルート証明書を取得します。
クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : GET /v1/objects/bmc-root-certificate/download

CLI : bmc_root_certificate_download

40.7 ストレージクラスターから BMC 接続検証用ルート証明書を削除する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ストレージクラスターから BMC 接続検証用ルート証明書を削除します。

ストレージクラスターに BMC 接続検証用ルート証明書がインポートされていると、スペアノード機能で利用する BMC の提供するサーバー管理 API にアクセスするときに、接続先 BMC のサーバー証明書を検証します。インポートされていない場合は、接続先 BMC のサーバー証明書の検証はせずに BMC の提供するサーバー管理 API へアクセスします。

前提条件

- 実行に必要なロール : Security

操作手順

1. コントローラーノードからストレージクラスターにインポートしたルート証明書を削除します。

クラスターマスターノード(プライマリー)に対してのみ実行できます。

REST API : POST /v1/objects/bmc-root-certificate/actions/delete/invoke

CLI : bmc_root_certificate_delete

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。



メモ

ルート証明書がインポートされていない状態で本コマンドを実行した場合は、"Succeeded"になります。

40.8 ストレージノードの BMC 情報を登録・編集する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ストレージノードの BMC 情報を登録・編集します。

スペアノード機能が BMC の提供するサーバー管理 API を利用するために、ここでの操作手順の実施が必要です。ここでの操作手順を、ストレージクラスターを構成する全ストレージノードに適用してください。



注意

「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載されているサーバーモデル以外はスベアノード機能が非サポートのため、スベアノード切り換えができない可能性があります。スベアノード切り換えをサポートしているサーバーモデルについては「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「ストレージノードの BMC 情報を登録・編集する <<Bare metal>>」

前提条件

- ・ 実行に必要なロール： Service

操作手順

1. コントローラーノードから、登録・編集する BMC 情報とストレージノードの ID を指定して以下のコマンドを実行します。

REST API : PATCH /v1/objects/storage-node-bmc-access-settings/<id >

CLI : storage_node_bmc_access_setting_set

コマンド実行時に以下の情報をパラメーターとして指定する必要があります。

- ・ ストレージノードの BMC の接続先アドレス(IPv4 アドレスまたは FQDN)
- ・ スベアノードを利用するために準備した BMC アカウントのユーザー名とパスワード



注意

BMC への認証はセッション認証を利用しています。BMC 側で BMC アカウントのユーザー名およびパスワード変更を実施した場合は、必ず本手順を実施し、変更した BMC アカウントのユーザー名およびパスワードを VSP One SDS Block へ再登録してください。再登録しない場合は、VSP One SDS Block から BMC へ変更前の BMC 認証情報を用いて作成したセッション情報でアクセスします。変更前の BMC 認証情報を用いて作成されたセッション情報が削除されたタイミングで、新たにセッション情報の作成を試みます。本手順を実施していない場合、変更前の BMC アカウントのユーザー名およびパスワードで BMC への認証を試みるため、セッション作成に失敗し VSP One SDS Block から BMC へのアクセスができなくなります。結果、スベアノード切り換えが動作しなくなります。

コマンド実行後に表示されるジョブの ID を確認します。

2. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。



注意

登録・編集した BMC 情報とストレージノードの組み合わせが正しいことの確認は、このマニュアルの「スベアノードの情報を登録する <<Bare metal>>」のあとに、「スベアノード機能の設定を確認する <<Bare metal>>」で行います。

40.9 ストレージノードの BMC 情報の取得<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

ストレージノードの BMC 情報が一覧または個別に取得できます。

40.9.1 取得できるストレージノードの BMC 情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : ストレージノードの ID(uuid)
- bmcName : BMC のホスト名または IP アドレス(IPv4)
- bmcUser : BMC 接続用のユーザー名

40.9.2 ストレージノードの BMC 情報の一覧を取得する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

各ストレージノードの BMC 情報を一覧で取得します。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージノードの BMC 情報の一覧を取得します。
REST API : GET /v1/objects/storage-node-bmc-access-settings
CLI : storage_node_bmc_access_setting_list

40.9.3 ストレージノードの BMC 情報を個別に取得する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

指定した ID のストレージノードの BMC 情報を取得します。

前提条件

- 実行に必要なロール : Service

操作手順

1. ストレージノードの ID を確認します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
2. ストレージノードの BMC 情報を取得します。
ストレージノードの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/storage-node-bmc-access-settings/<id >
CLI : storage_node_bmc_access_setting_show

40.10 スペアノードの情報を登録する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

スペアノードの情報を登録します。



注意

- 「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載されているサーバーモデル以外はスペアノード機能が非サポートのため、スペアノード切り換えができない可能性があります。スペアノード切り換えをサポートしているサーバーモデルについては「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。
- 特定のストレージクラスターで使用中のスペアノードを、他のストレージクラスターのスペアノードとして登録することはできません。
- 特定のストレージクラスターで使用していたストレージノードまたはスペアノードを、別のストレージクラスターでスペアノードとして使用する場合は、「スペアノードを準備する<<Bare metal>>」の記載に従って、ストレージソフトウェアのインストールなどの手順を再度実施する必要があります。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「スペアノードの情報を登録する<<Bare metal>>」

前提条件

- 実行に必要なロール：Service
- 「スペアノードを準備する<<Bare metal>>」に従って、登録するスペアノードの準備を行っていること
- すべてのストレージノードの status が"Ready"であること
- ストレージノードの自動回復機能の設定が有効であること
自動回復設定の詳細は、このマニュアルの「ストレージノードの自動回復機能を設定する<<Bare metal>>」を参照してください。

操作手順

1. ストレージノードの一覧を取得して、すべてのストレージノードの status が"Ready"であることを確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

"Ready"以外の status のストレージノードが存在する場合は、以下に従って対処してください。

- VSP One SDS Block の VSP One SDS Block Administrator でストレージノードの Health Status に"Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
- status が"MaintenanceBlockage"のストレージノードがある場合は「ストレージノードを保守回復する<<Bare metal>>」に従って、ストレージノードを保守回復してください。

- ・ 上記以外の **status** のストレージノードがあった場合は、それらのストレージノードに対する処理が実施中のため、**status** が変わるまで待ってから、再度確認してください。
2. スペアノードを登録するフォールトドメインの ID を確認します。

REST API : GET /v1/objects/fault-domains

CLI : fault_domain_list

3. スペアノードの情報を登録します。

REST API : POST /v1/objects/spare-nodes

CLI : spare_node_create

上記コマンドの実行時には、フォールトドメインの ID と、以下の情報をパラメーターとして指定する必要があります。

このマニュアルと Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」に記載されている手順に沿って指定したパラメーターの値を指定してください。

- ・ Bare metal モデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノード単位のセットアップを行う」の手順内で設定した以下
 - 管理ポートのネットワークの IP アドレス
 - セットアップユーザーのパスワード
- ・ このマニュアルの「スペアノードを利用するための BMC アカウントを準備する<<Bare metal>>」の手順内で設定した以下
 - BMC のホスト名または IP アドレス
 - BMC のユーザー名
 - BMC のパスワード

コマンド実行後に表示されるジョブの ID を確認します。

4. ジョブの **state** を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

5. スペアノード情報一覧を取得して、スペアノードの情報が登録されたことを確認します。

REST API : GET /v1/objects/spare-nodes

CLI : spare_node_list



メモ

登録した BMC 情報とスペアノードの組み合わせが正しいかどうかの確認は「スペアノード機能の設定を確認する<<Bare metal>>」で行います。

40.11 スペアノードの情報を編集する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

スペアノードの情報を編集します。



注意

「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載されているサーバーモデル以外はスペアノード機能が非サポートのため、スペアノード切り換えができない可能性があります。スペアノード切り換えをサポートしているサーバーモデルについては「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- ・ 「スペアノードの情報を編集する<<Bare metal>>」

前提条件

- ・ 実行に必要なロール：Service
- ・ すべてのストレージノードの status が"Ready"であること

操作手順

1. ストレージノードの一覧を取得して、すべてのストレージノードの status が"Ready"であることを確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

"Ready"以外の status のストレージノードが存在する場合は、以下に従って対処してください。

- ・ VSP One SDS Block の VSP One SDS Block Administrator でストレージノードの Health Status に"Alerting"が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
 - ・ status が"MaintenanceBlockage"のストレージノードがある場合は「ストレージノードを保守回復する<<Bare metal>>」に従って、ストレージノードを保守回復してください。
 - ・ 上記以外の status のストレージノードがあった場合は、それらのストレージノードに対する処理が実施中のため、status が変わるまで待つてから、再度確認してください。
2. スペアノードの ID を確認します。

REST API : GET /v1/objects/spare-nodes

CLI : spare_node_list

3. スペアノードの情報を編集します。

スペアノードの ID を指定してコマンドを実行します。

「スペアノードの情報を登録する<<Bare metal>>」の手順 3 にあるパラメーターが編集でき、編集したパラメーターのみ更新されます。

REST API : PATCH /v1/objects/spare-nodes/<id >

CLI : spare_node_set

コマンド実行後に表示されるジョブの ID を確認します。



注意

BMC への認証はセッション認証を利用しています。BMC 側で BMC アカウントのユーザー名およびパスワード変更を実施した場合は、必ず本手順を実施し、変更した BMC アカウントのユーザー名およびパスワードを VSP One SDS Block へ再登録してください。再登録しない場合は、VSP

One SDS Block から BMC へ変更前の BMC 認証情報を用いて作成したセッション情報でアクセスします。変更前の BMC 認証情報を用いて作成されたセッション情報が削除されたタイミングで、新たにセッション情報の作成を試みます。本手順を実施していない場合、変更前の BMC アカウントのユーザー名およびパスワードで BMC への認証を試みるため、セッション作成に失敗し VSP One SDS Block から BMC へのアクセスができなくなります。結果、スペアノード切り換えが動作しなくなります。

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

5. スペアノード情報一覧を取得して、スペアノードの情報が編集されたことを確認します。

REST API : GET /v1/objects/spare-nodes

CLI : spare_node_list



メモ

編集したスペアノードの BMC 情報が正しいかどうかの確認は「スペアノード機能の設定を確認する<<Bare metal>>」で行います。

40.12 スペアノードの情報の取得<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージクラスターに登録されたスペアノードの情報が一覧または個別に取得できます。

40.12.1 取得できるスペアノードの情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : スペアノードの ID(uuid)
- name : スペアノードの名前
- faultDomainId : スペアノードが所属するフォールトドメインの ID(uuid)
- faultDomainName : スペアノードが所属するフォールトドメインの名前
- controlPortIpv4Address : 管理ポートの IP アドレス(IPv4)
- softwareVersion : ストレージソフトウェアのバージョン
- biosUuid : BIOS の ID(uuid)
- modelName : スペアノードが動作しているサーバーのモデル名
- serialNumber : スペアノードが動作しているサーバーのシリアルナンバー
- bmcName : BMC のホスト名または IP アドレス(IPv4)
- bmcUser : BMC 接続用のユーザー名

40.12.2 スペアノードの情報を一覧で取得する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

ストレージクラスターに登録されたスペアノードの情報を一覧で取得します。

前提条件

- 実行に必要なロール： Service

操作手順

1. スペアノード情報の一覧を取得します。
REST API : GET /v1/objects/spare-nodes
CLI : spare_node_list

40.12.3 スペアノードの情報を個別に取得する<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

指定した ID のスペアノードの情報を取得します。

前提条件

- 実行に必要なロール： Service

操作手順

1. スペアノードの ID を確認します。
REST API : GET /v1/objects/spare-nodes
CLI : spare_node_list
2. スペアノード情報を取得します。
スペアノードの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/spare-nodes/<id >
CLI : spare_node_show

40.13 スペアノードの情報を削除する<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

スペアノードの情報を削除します。

VSP One SDS Block Administrator で実施する場合

ここで説明する操作は VSP One SDS Block Administrator でも実施できます。

操作手順などについては「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」の以下を参照してください。

- 「スペアノードの情報を削除する<<Bare metal>>」

前提条件

- 実行に必要なロール : Service
- すべてのストレージノードの status が "Ready" であること

操作手順

1. ストレージノードの一覧を取得して、すべてのストレージノードの status が "Ready" であることを確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

"Ready" 以外の status のストレージノードが存在する場合は、以下に従って対処してください。

- VSP One SDS Block の VSP One SDS Block Administrator でストレージノードの Health Status に "Alerting" が表示されている場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
- status が "MaintenanceBlockage" のストレージノードがある場合は「ストレージノードを保守回復する <<Bare metal>>」に従って、ストレージノードを保守回復してください。
- 上記以外の status のストレージノードがあった場合は、それらのストレージノードに対する処理が実施中のため、status が変わるまで待つから、再度確認してください。

2. スペアノードの ID を確認します。

REST API : GET /v1/objects/spare-nodes

CLI : spare_node_list

3. スペアノードの情報を削除します。

スペアノードの ID を指定してコマンドを実行します。

REST API : DELETE /v1/objects/spare-nodes/<id >

CLI : spare_node_delete

コマンド実行後に表示されるジョブの ID を確認します。

4. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が "Succeeded" になっていたらジョブは完了です。

5. スペアノード情報一覧を取得して、スペアノード情報が削除されたことを確認します。

REST API : GET /v1/objects/spare-nodes

CLI : spare_node_list

40.14 スペアノード機能の設定を確認する <<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

スペアノードの切り換えが実行可能な状態であるかどうかを確認します。

前提条件

- 実行に必要なロール : Service

- ・ 「ストレージノードの BMC 情報を登録・編集する<<Bare metal>>」および「スぺアノードの情報を登録する<<Bare metal>>」の手順が完了し、ストレージクラスターにスぺアノードが登録されていること

操作手順

1. イベントログの一覧を取得します。イベントログの一覧の取得方法は「イベントログの一覧を取得する」を参照してください。
2. 「スぺアノードの情報を登録する<<Bare metal>>」や「スぺアノードの情報を編集する<<Bare metal>>」で対象としたスぺアノードを確認する場合は、対象とするスぺアノードごとにイベントログ KARS10722-I が出力されていることを確認します。

スぺアノードの情報についての登録や編集を行っていない場合は、確認不要です。



メモ

「スぺアノードの情報を登録する<<Bare metal>>」や「スぺアノードの情報を編集する<<Bare metal>>」での手順の実行直後にフェイルオーバーが発生した場合など、ストレージクラスターの動作状況によっては、イベントログ KARS10722-I が出力されない場合があります。その場合は、イベントログ KARS10720-I または KARS10721-I が出力されていれば確認に問題はありません。

3. 「ストレージノードの BMC 情報を登録・編集する<<Bare metal>>」で登録の対象としたストレージノードを確認する場合は、対象としたストレージノードごとにイベントログ KARS10732-I が出力されていることを確認します。

ストレージノードの BMC 情報の登録を行っていない場合は、確認不要です。



メモ

「ストレージノードの BMC 情報を登録・編集する<<Bare metal>>」の手順の実行直後にフェイルオーバーが発生した場合など、ストレージクラスターの動作状況によっては、イベントログ KARS10732-I が出力されない場合があります。その場合は、イベントログ KARS10720-I または KARS10721-I が出力されていれば確認に問題はありません。

4. 以下に該当する未対処のイベントログが出力されていないことを確認します。

- ・ KARS107xx-W(x は任意の数字)
- ・ KARS107xx-E(x は任意の数字)

上記に該当する未対処のイベントログが出力されていた場合は、それぞれ対処してください。対処が終わったら、手順 1 からやり直してください。

上記に該当する未対処のイベントログがなかった場合は、以上で手順は終了です。



注意

- ・ イベントログ KARS10777-W が出力されている場合、対象とするストレージノードは、スぺアノード機能が非サポートのサーバーモデルのため、スぺアノード切り換えができない可能性があります。スぺアノード切り換えをサポートしているサーバーモデルについては「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。
- ・ イベントログ KARS10778-W が出力されている場合、対象とするスぺアノードは、スぺアノード機能が非サポートのサーバーモデルのため、スぺアノード切り換えができない可能性があります。スぺアノード切り換えをサポートしているサーバーモデルについては「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。
- ・ スぺアノード切り換え非サポートのサーバーモデルを使用時、スぺアノード機能が BMC の提供するサーバー管理 API を利用できないため、BMC に関連する他の KARS107xx-W や KARS107xx-E(x は任意の数字)のイベントログが出力されている場合があります。その場合、

BMC に関連する他の KARS107xx-W や KARS107xx-E(x は任意の数字)のイベントログに対処しても回復せずスペアノード切り換えを利用できません。スペアノード切り換えを利用する場合は、スペアノード切り換えをサポートしているサーバーモデルへストレージノード交換を実施してください。スペアノード切り換えをサポートしているサーバーモデルについては「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」を参照してください。



メモ

ストレージノードまたはスペアノードの BMC を再起動した場合、BMC の再起動が完了するまで KARS10726-W または KARS10734-W が出力されることがあります。BMC 再起動後、KARS10722-I または KARS10732-I が出力されれば問題はありません。

キャッシュ保護付きライトバックモードを 管理する

- 41.1 キャッシュ保護付きライトバックモードの概要
- 41.2 キャッシュ保護付きライトバックモードの有効化
- 41.3 キャッシュ保護用メタデータの冗長度の確認

41.1 キャッシュ保護付きライトバックモードの概要

キャッシュ保護付きライトバックモードは、装置給電停止障害からストレージシステム上のデータを保護するための機能です。キャッシュ保護付きライトバックモードが有効に設定されている場合、揮発メモリー上で管理するデータの更新を、ストレージコントローラーがすべてログ(キャッシュ保護用メタデータ)としてディスクに書き込みます。これによって、ストレージシステムが稼働中に装置への給電が意図せず断たれたとしても、給電回復後の再立ち上げ時に、キャッシュ保護用メタデータをディスクから読み出し、メモリー上のデータを給電停止前の状態に復元します。

- この機能を有効にするには、ストレージシステムの稼働を一度停止する必要があります。手順の詳細については「キャッシュ保護付きライトバックモードの有効化」を参照してください。
- 《Bare metal》この機能は、ストレージソフトウェアの 01.13.0x.40 のバージョンからサポートされます。ストレージソフトウェアの 01.13.0x.40 のバージョン以降で新規インストールをした場合、この機能はデフォルトで有効になります。ソフトウェアアップデート時は、アップデート前の設定を引き継ぎます。
- 《Cloud》新規インストール時は、この機能はデフォルトで有効になります。ソフトウェアアップデート時は、アップデート前の設定を引き継ぎます。
- 《Bare metal》ストレージソフトウェアを 01.13.0x.40 より前のバージョンにダウングレードする場合は、この機能を無効にする必要があります。詳細は、「ストレージソフトウェアをダウングレードする《Bare metal》」を参照してください。
- キャッシュ保護付きライトバックモードのキャッシュ保護用メタデータは、システム内で冗長性を持って管理されます。ユーザーデータディスクやストレージノードの障害発生時には、一時的に冗長度が落ちた状態になりますが、保守操作などによる障害回復後にキャッシュ保護用メタデータの冗長度も回復されます。キャッシュ保護用メタデータの冗長度の確認方法は、このマニュアルの「キャッシュ保護用メタデータの冗長度の確認」を参照してください。
- 一度この機能を有効にしたストレージクラスターに対して、再度無効にすることはできません。



注意

《Bare metal》ストレージソフトウェアを 01.13.0x.40 より前のバージョンから 01.13.0x.40 以降のバージョンにアップグレードした場合は、キャッシュ保護付きライトバックモードは無効になっています。キャッシュ保護付きライトバックモードが無効の場合、ストレージクラスターへの電源供給の停止などによってストレージクラスターの障害が発生した際に、スナップショットボリュームのデータが消失するリスクがあります。このマニュアルの「キャッシュ保護付きライトバックモードを有効にする《Bare metal》」を参照してキャッシュ保護付きライトバックモードを有効にしてください。

キャッシュ保護付きライトバックモードの状態について

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)はストレージクラスターの情報から取得できます。ストレージクラスター情報の取得方法は、このマニュアルの「ストレージクラスターの情報を取得する」を参照してください。

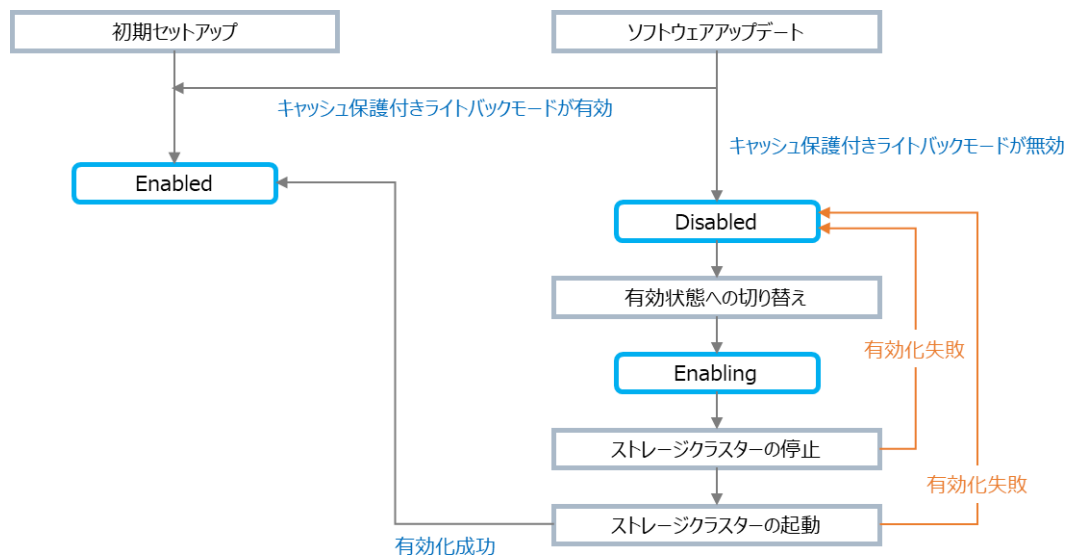
キャッシュ保護付きライトバックモードの状態表示とその説明を以下に示します。

状態表示	説明
Enabled	キャッシュ保護付きライトバックモードが有効な状態です。 初期セットアップ、キャッシュ保護付きライトバックモードが無効な状態から有効な状態への切り替えができたとき、この状態になります。
Disabled	キャッシュ保護付きライトバックモードが無効な状態です。 キャッシュ保護付きライトバックモードが非サポートのバージョンからソフトウェアをアップグレードしたとき、この状態になります。

状態表示	説明
	また、以下の場合にもこの状態になります。 無効な状態から有効な状態への切り替え手順において、ストレージクラスターの再起動前に、無効な状態への切り替えを実施したとき、またはストレージクラスターの再起動の段階でキャッシュ保護付きライトバックモードの構成情報を作成する前に、障害などによってストレージクラスターの再起動が失敗したとき
Enabling	キャッシュ保護付きライトバックモードの設定が切り替えの途中段階であることを示します。 "Disabled"状態から有効な状態への切り替えを実施することで、"Enabling"状態になります。その後、ストレージクラスターを停止してから必要に応じてメモリーを増設し、ストレージクラスターを再起動することで、"Enabled"状態へ切り替わります。
Disabling	キャッシュ保護付きライトバックモードの設定が切り替えの途中段階であることを示します。 一度キャッシュ保護付きライトバックモードが有効な状態になったあとは、"Disabling"状態になることはありません。

キャッシュ保護付きライトバックモードの状態の遷移

初期セットアップ、またはキャッシュ保護付きライトバックモードが非サポートのバージョンからのソフトウェアアップデート後のキャッシュ保護付きライトバックモードについての状態遷移を以下に示します。



メモ

メモリーを増設が必要になる条件については「キャッシュ保護付きライトバックモードの有効化」を参照してください。

41.2 キャッシュ保護付きライトバックモードの有効化

キャッシュ保護付きライトバックモードを有効にします。

41.2.1 キャッシュ保護付きライトバックモードを有効にする<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

キャッシュ保護付きライトバックモードを有効にする場合は、以下の手順を実施してください。



注意

キャッシュ保護付きライトバックモードを有効にするには、手順 8 でのストレージクラスターの停止を実行する前に、ホストからの I/O をすべて停止させる必要があります。



メモ

手順 7 まで実施していても、手順 8 をまだ実施していなければ、キャッシュ保護付きライトバックモードを無効にするコマンドを実行することで、有効化を取り消すことができます。

前提条件

- 実行に必要なロール : Service
- すべてのストレージノードの **status** が "Ready" であること
ストレージノード情報の一覧取得、および VSP One SDS Block Administrator の Health Status にて確認してください。
 - VSP One SDS Block Administrator で、ストレージノードの Health Status に "Alerting" が表示されていた場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
 - ストレージノード情報の一覧を取得し、**status** が "MaintenanceBlockage" のストレージノードがあった場合は「ストレージノードを保守回復する <<Bare metal>>」に従って、ストレージノードを保守回復してください。
 - ストレージノードに対する処理が実施中の場合は **status** が "Ready" になるのを待ってください。
- リビルドが動作中でないこと
「リビルドの状態を確認する」を参照して確認してください。
- ストレージコントローラーへの容量割り付け処理が完了していること
「ストレージプールを拡張する」を参照してください。
- **status** が "Normal" であるドライブが各ストレージノードに 3 台以上搭載されていること
ドライブの情報の一覧を取得して確認してください。**status** が "Normal" のドライブが 3 台に満たないストレージノードが存在した場合は「ドライブを増設する」を参照して対象のストレージノードに不足分のドライブを増設した上で、ストレージプールの拡張を実施してください。

操作手順

1. ストレージクラスターの情報を取得して、使用しているストレージソフトウェアのバージョンが、キャッシュ保護付きライトバックモードをサポートしているバージョンかどうかを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

01.13.0x.xx 未満のバージョンを使用している場合は、手順 2 に進みます。

01.13.0x.xx 以上のバージョンを使用している場合は、手順 3 に進みます。

2. ストレージソフトウェアのアップグレードを行います。

キャッシュ保護付きライトバックモードがサポートされているバージョン(01.13.0x.xx 以上)までアップグレードを順次実施してください。

各バージョンの「オペレーションガイド」に記載されている「ストレージソフトウェアアップデートの要件と手順」を参照して実施してください。

3. 物理サーバーのメモリーの増設が必要であるかを確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

すべての物理サーバーのメモリー量が 256GiB 以上である場合は、メモリーの増設は不要です。次の手順に進みます。

メモリー量が 256GiB 未満の物理サーバーがあり、かつ容量削減機能を使用する場合は、手順 9 のメモリーの増設が必要になります。次の手順に進みます。

メモリー量が 256GiB 未満の物理サーバーがあり、かつ容量削減機能を使用しない場合は、メモリーの増設は不要です。次の手順に進みます。

4. キャッシュ保護付きライトバックモードの状態を確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

キャッシュ保護付き ライトバックモードの状態	対応方法
Enabled	手順 3 でメモリーの増設が必要であることを確認した場合は、手順 7 に進みます。メモリーの増設作業が必要でなかった場合は、以上で手順は終了です。
Disabled	手順 5 に進みます。
Enabling	手順 7 に進みます。
Disabling	手順 5、6、11 を順次実施してください。 手順 7 から 10 は実施不要です。

5. キャッシュ保護付きライトバックモードを有効にします。

isEnabled パラメーターに"true"を指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/set-write-back-mode-with-cache-protection/
invoke

CLI : storage_write_back_mode_with_cache_protection_set

コマンド実行後に表示されるジョブの ID を確認します。

6. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

7. ホストからの I/O をすべて停止します。

8. ストレージクラスターを停止します。

「ストレージクラスターを停止する<<Bare metal>>」を参照して実施してください。

9. 手順 3 でメモリーの増設が必要であることを確認した場合は、ハードウェアのマニュアルを参照してメモリーを増設します。

10. ストレージクラスターを起動します。

「ストレージクラスターを起動する<<Bare metal>>」を参照して実施してください。

11. キャッシュ保護付きライトバックモードの状態が"Enabled"であることを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

41.2.2 キャッシュ保護付きライトバックモードを有効にする<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

キャッシュ保護付きライトバックモードを有効にする場合は、以下の手順を実施してください。



注意

キャッシュ保護付きライトバックモードを有効にするには、手順 5 でのストレージクラスターの停止を実行する前に、ホストからの I/O をすべて停止させる必要があります。



メモ

手順 4 まで実施していても、手順 5 をまだ実施していなければ、キャッシュ保護付きライトバックモードを無効にするコマンドを実行することで、有効化を取り消すことができます。

前提条件

- 実行に必要なロール : Service
- すべてのストレージノードの status が "Ready" であること
ストレージノード情報の一覧取得、および VSP One SDS Block Administrator の Health Status にて確認してください。
 - VSP One SDS Block Administrator で、ストレージノードの Health Status に "Alerting" が表示されていた場合は「Hitachi Virtual Storage Platform One SDS Block トラブルシューティングガイド」の「VSP One SDS Block Administrator でヘルスステータス異常を検知した場合」に従って対処してください。
 - ストレージノード情報の一覧を取得し、status が "MaintenanceBlockage" のストレージノードがあった場合は「ストレージノードの保守回復」に従って、ストレージノードを保守回復してください。
 - ストレージノードに対する処理が実施中の場合は status が "Ready" になるのを待ってください。
- リビルドが動作中でないこと
「リビルドの状態を確認する」を参照してください。
- ストレージコントローラーへの容量割り付け処理が完了していること
「ストレージプールを拡張する」を参照してください。
- status が "Normal" であるドライブを各ストレージノードに 6 台以上搭載していること
ドライブの情報の一覧を取得して確認してください。status が "Normal" のドライブが 6 台に満たないストレージノードが存在した場合は「ドライブを増設する」を参照して対象のストレージノードに不足分のドライブを増設した上で、ストレージプールの拡張を実施してください。



メモ

- <<Cloud for AWS>>容量削減機能を合わせて使用する場合は、インスタンスタイプに r7i.8xlarge または r6i.8xlarge を設定して初期インストールする必要があります。インスタンスタイプの設定方法については、Cloud モデル for AWS の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。
インスタンスタイプに r7i.8xlarge または r6i.8xlarge を設定して初期インストールした場合は、キャッシュ保護付きライトバックモードは有効になるため、有効化の実施手順は不要です。
- <<Cloud for Google Cloud>>容量削減機能を合わせて使用する場合は、インスタンスタイプに 4-highmem-32 を設定して新規インストールする必要があります。インスタンスタイプの設定方法については、Cloud モデル for Google Cloud の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。
インスタンスタイプに 4-highmem-32 を設定して初期インストールした場合は、キャッシュ保護付きライトバックモードは有効になるため、有効化の実施手順は不要です。
- <<Cloud for Microsoft Azure>>容量削減機能を合わせて使用する場合は、インスタンスタイプに Standard_E32s_v5 を設定して新規インストールする必要があります。インスタンスタイプの設定方法に

については、Cloud モデル for Microsoft Azure の「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」を参照してください。
インスタンスタイプに **Standard_E32s_v5** を設定して初期インストールした場合は、キャッシュ保護付きライトバックモードは有効になるため、有効化の実施手順は不要です。

操作手順

1. キャッシュ保護付きライトバックモードの状態を確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

キャッシュ保護付き ライトバックモードの状態	対応方法
Enabled	以上で手順は終了です。
Disabled	手順 2 に進みます。
Enabling	手順 4 に進みます。
Disabling	手順 2、3、7 を順次実施してください。 手順 4 から 6 は実施不要です。

2. キャッシュ保護付きライトバックモードを有効にします。

isEnabled パラメーターに"true"を指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/set-write-back-mode-with-cache-protection/
invoke

CLI : storage_write_back_mode_with_cache_protection_set

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId>

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4. ホストからの I/O をすべて停止します。

5. ストレージクラスターを停止します。

「ストレージクラスターを停止する<<Cloud>>」を参照して実施してください。

6. ストレージクラスターを起動します。

<<Cloud for AWS>> 「ストレージクラスターを起動する<<Cloud for AWS>>」を参照して実施してください。

<<Cloud for Google Cloud>> 「ストレージクラスターを起動する<<Cloud for Google Cloud>>」を参照して実施してください。

<<Cloud for Microsoft Azure>> 「ストレージクラスターを起動する<<Cloud for Microsoft Azure>>」を参照して実施してください。

7. キャッシュ保護付きライトバックモードの状態が"Enabled"であることを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

41.3 キャッシュ保護用メタデータの冗長性の確認

キャッシュ保護用メタデータの冗長性を確認します。

41.3.1 キャッシュ保護用メタデータの冗長性を確認する <<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

キャッシュ保護付きライトバックモードのキャッシュ保護用メタデータの冗長性は以下の手順で確認できます。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

- ストレージプールの一覧を取得し、ユーザーデータの保護種別を確認します。
REST API : GET /v1/objects/pools
CLI : pool_list
- ストレージクラスターの情報を取得し、キャッシュ保護付きライトバックモードの状態とキャッシュ保護用メタデータ冗長性のサマリーを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

キャッシュ保護付き ライトバックモードの状態	対応方法
Enabled	次の手順に進みます。
Disabled	キャッシュ保護付きライトバックモードは無効です。確認手順は終了です。
Enabling	「キャッシュ保護付きライトバックモードを有効にする<<Bare metal>>」を参照して、有効化を実行したあと、次の手順に進みます。
Disabling	「キャッシュ保護付きライトバックモードを有効にする<<Bare metal>>」を参照して、有効化を実行したあと、次の手順に進みます。

- ユーザーデータの保護種別とキャッシュ保護付きライトバックモードのキャッシュ保護用メタデータ冗長性のサマリー(metaDataRedundancyOfCacheProtectionSummary)から、以下の表に従ってキャッシュ保護用メタデータの冗長性を判断します。

ユーザーデータの保護種別 (redundantType)	キャッシュ保護用メタデータ冗長性のサマリー (metaDataRedundancyOfCacheProtectionSummary)
4D+1P	1 : 冗長度低下なし 0 : 冗長度低下あり -1 : メタデータ損失状態
4D+2P	2 : 冗長度低下なし 1 または 0 : 冗長度低下あり

ユーザーデータの保護種別 (redundantType)	キャッシュ保護用メタデータ冗長度のサマリー (metaDataRedundancyOfCacheProtectionSummary)
	-1 : メタデータ損失状態
Duplication	1 : 冗長度低下なし 0 : 冗長度低下あり -1 : メタデータ損失状態

41.3.2 キャッシュ保護用メタデータの冗長度を確認する<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

キャッシュ保護付きライトバックモードのキャッシュ保護用メタデータの冗長度は以下の手順で確認できます。

前提条件

- 実行に必要なロール : Security、Storage、RemoteCopy、Monitor、Service、または Resource

操作手順

- ストレージプールの一覧を取得し、ユーザーデータの保護種別を確認します。

REST API : GET /v1/objects/pools

CLI : pool_list

- ストレージクラスターの情報を取得し、キャッシュ保護付きライトバックモードの状態とキャッシュ保護用メタデータ冗長度のサマリーを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

キャッシュ保護付きライトバックモードの状態(writeBackModeWithCacheProtection)によって以下の対応を行います。

キャッシュ保護付き ライトバックモードの状態	対応方法
Enabled	次の手順に進みます。
Disabled	キャッシュ保護付きライトバックモードは無効です。確認手順は終了です。
Enabling	「キャッシュ保護付きライトバックモードを有効にする<<Cloud>>」を参照して、有効化を実行したあと、次の手順に進みます。
Disabling	「キャッシュ保護付きライトバックモードを有効にする<<Cloud>>」を参照して、有効化を実行したあと、次の手順に進みます。

- ユーザーデータの保護種別とキャッシュ保護付きライトバックモードのキャッシュ保護用メタデータ冗長度のサマリー(metaDataRedundancyOfCacheProtectionSummary)から、以下の表に従ってキャッシュ保護用メタデータの冗長度を判断します。

ユーザーデータの保護種別 (redundantType)	キャッシュ保護用メタデータ冗長度のサマリー (metaDataRedundancyOfCacheProtectionSummary)
4D+2P	2 : 冗長度低下なし 1 または 0 : 冗長度低下あり -1 : メタデータ損失状態
Duplication	1 : 冗長度低下なし 0 : 冗長度低下あり

ユーザーデータの保護種別 (redundantType)	キャッシュ保護用メタデータ冗長度のサマリー (metaDataRedundancyOfCacheProtectionSummary)
	-1 : メタデータ損失状態

格納データ暗号化を利用する

- 42.1 格納データ暗号化の概要
- 42.2 暗号化環境の設定を編集する
- 42.3 暗号化環境の設定の情報を取得する
- 42.4 ストレージプールの暗号化の設定を編集する
- 42.5 暗号化鍵を作成する
- 42.6 暗号化鍵を削除する
- 42.7 暗号化鍵の情報の取得
- 42.8 暗号化鍵の個数を取得する

42.1 格納データ暗号化の概要

格納データ暗号化は、ユーザーデータをストレージシステム内のソフトウェアによって暗号化する機能です。ユーザーデータを暗号化すると、ストレージシステム内のドライブ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。



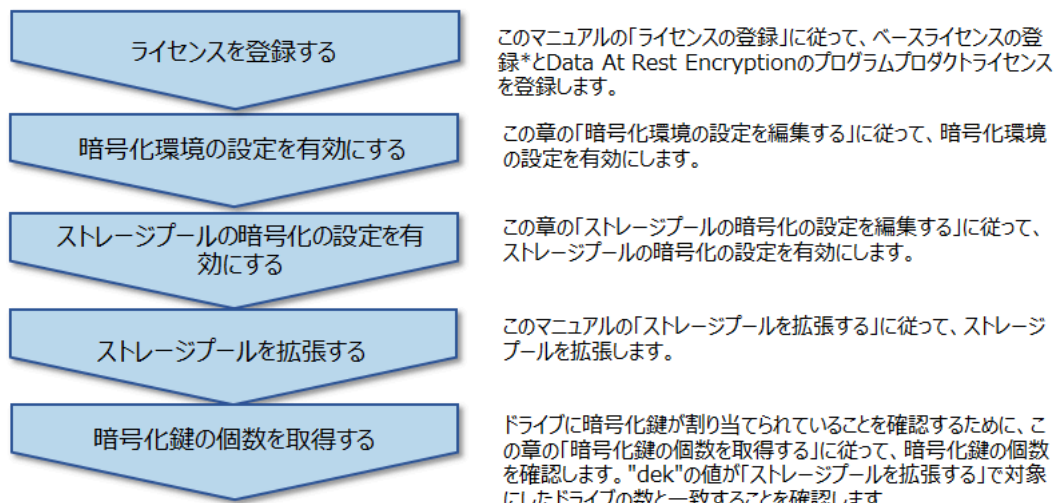
メモ

ユーザーデータドライブのデータのみが暗号化の対象です。システムドライブのデータは暗号化の対象ではありません。

格納データ暗号化を有効化する場合、ユーザーデータを暗号化/復号化するため、格納データ暗号化を無効化している場合と比較し、I/O 性能が低下する可能性があります。また、保守操作の処理時間が長くなる可能性があります。

格納データ暗号化を利用するには、Data At Rest Encryption のプログラムプロダクトライセンスを登録する必要があります。プログラムプロダクトライセンスは、ベースライセンスが Trial 以外の場合のみ登録できます。プログラムプロダクトライセンスを登録する前に、Trial 以外のベースライセンスが登録されていることを確認してください。ライセンスの種類の詳細についてはこのマニュアルの「ライセンス管理の概要」を参照してください。

格納データ暗号化を利用するまでの流れとマニュアルの参照先は以下のとおりです。格納データ暗号化を有効化する場合、暗号化環境の設定を有効にする手順およびストレージプールの暗号化の設定を有効化する場合、必ずストレージプールを拡張する前に実施してください。ストレージプールを拡張したあとでは、暗号化環境の設定およびストレージプールの暗号化の設定は変更できません。



* ベースライセンスの登録については、Bare metalモデルまたは料金モデルにBYOLを選択しているCloudモデルのみ実施してください。

暗号方式の仕様

ユーザーデータの暗号方式の仕様を以下に示します。

項目	仕様
暗号アルゴリズム	Advanced Encryption Standard (AES) 256 bit

項目	仕様
暗号モード	XTS モード

暗号化鍵の管理

格納データ暗号化には、ストレージクラスター内で暗号化鍵を管理する機能が備わっています。ドライブがストレージプールの容量に追加されるとき、それぞれのドライブに異なる 1 つの暗号化鍵が自動で割り当てられます。ドライブごとに割り当てられた暗号化鍵を使用してユーザーデータは暗号化されます。暗号化されたドライブの減設時、または暗号化されたドライブを搭載したストレージノードの減設時には、対象のドライブに割り当てられた暗号化鍵は自動で削除されます。ストレージクラスターごとに保持できる暗号化鍵の最大数は、ドライブに未割り当ての暗号化鍵とドライブに割り当て済みの暗号化鍵を合わせて 4,096 個です。ストレージクラスターの構築後、初めて暗号化環境の設定を有効にしたとき、未割り当ての暗号化鍵が最大数の 4,096 個作成されます。

ストレージプールの暗号化の設定を有効にしている場合、特定の保守操作または処理が実行されたとき、未割り当ての暗号化鍵がドライブに割り当てられること、また、ドライブに割り当て済みの暗号化鍵が削除されることがあります。未割り当ての暗号化鍵は自動的に補充されないため、Security ロールを持ったシステム管理者が未割り当ての暗号化鍵の個数を監視して、必要に応じて暗号化鍵を追加で作成してください。なお、未割り当ての暗号化鍵の個数がしきい値(256 個)以下になった場合、イベントログ KARS13280-W が出力されます。

未割り当ての暗号化鍵がドライブに割り当てられるケース、およびドライブに割り当て済みの暗号化鍵が削除されるケースは次のとおりです。

■未割り当ての暗号化鍵がドライブに割り当てられる保守操作または処理

保守操作または処理	割り当てられる暗号化鍵の個数
ストレージプールの拡張	ストレージプールに追加する対象のドライブの数
ドライブの増設	増設するドライブの数
ドライブの交換	交換するドライブの数
ストレージノードの増設	増設するストレージノードに搭載されているドライブの数*
ストレージノードの交換	交換後のストレージノードに搭載されているドライブの数。ただし、ストレージノードの交換前後で同じドライブを搭載する場合、それらのドライブの数は除きます。
«Bare metal» スペアノードへの切り換え	切り換え後のストレージノードに搭載されるドライブの数
«Bare metal» 構成リストアの実施	構成バックアップ時点で暗号化鍵が割り当てられていたドライブの数。構成リストアを実施する場合の暗号化鍵の情報の状態の詳細については、このマニュアルの「構成バックアップ・構成リストアの概要«Bare metal»«Cloud for AWS»」を参照してください。
«Cloud for AWS» 構成リストアの実施	構成バックアップ時点で暗号化鍵が割り当てられていたドライブの数。構成リストアを実施する場合の暗号化鍵の情報の状態の詳細については、このマニュアルの「構成バックアップ・構成リストアの概要«Bare metal»«Cloud for AWS»」を参照してください。
* ストレージノードを増設する処理の途中で障害が発生した場合、増設するストレージノードに搭載しているドライブへの割り当て済みの暗号化鍵が削除されることがあります。その場合、障害に対処したあと再度ストレージノードを増設するときに、前回割り当て済みの暗号化鍵は再び使用されず、別の未割り当ての暗号化鍵が割り当てられます。	

■ ドライブに割り当て済みの暗号化鍵が削除される保守操作または処理

保守操作または処理	割り当てられる暗号化鍵の個数
ドライブの減設*	減設するドライブの数
ドライブの交換	交換するドライブの数
ストレージノードの減設	減設するストレージノードに搭載されているドライブの数
ストレージノードの交換	交換後のストレージノードに搭載されているドライブの数。ただし、ストレージノードの交換前後で同じドライブを搭載する場合、それらのドライブの数は除きます。
≪Bare metal≫ スペアノードへの切り換え	切り換え前のストレージノードに搭載されているドライブの数
*≪Bare metal≫ このマニュアルの手順に従わずに、予期せずストレージノードからドライブが物理的に抜き取られた場合も、抜き取られたドライブに対応する暗号化鍵が削除されます。 *≪Cloud for AWS≫ このマニュアルの手順に従わずに、予期せずストレージノードから EBS ボリュームがデタッチされた場合も、抜き取られたドライブに対応する暗号化鍵が削除されます。 *≪Cloud for Google Cloud≫ このマニュアルの手順に従わずに、予期せずストレージノードから Google Cloud Hyperdisk ボリュームがデタッチされた場合も、抜き取られたドライブに対応する暗号化鍵が削除されます。 *≪Cloud for Microsoft Azure≫ このマニュアルの手順に従わずに、予期せずストレージノードから Azure マネージドディスクボリュームがデタッチされた場合も、抜き取られたドライブに対応する暗号化鍵が削除されます。	

監査ログ

監査ログ機能を使用して、ストレージクラスター内の暗号化鍵に関する事象の記録を取得できます。監査ログを取得する方法は「監査ログを管理する」を参照してください。

REST API/CLI の操作の記録に加えて、格納データ暗号化では以下の契機で監査ログが記録されます。監査ログの内容の詳細については「Hitachi Virtual Storage Platform One SDS Block 監査ログリファレンス」を参照してください。

記録される契機	Audit event
未割り当ての暗号化鍵がドライブに割り当てられる保守操作または処理が実行されたとき*	ENCRYPTION KEY ALLOCATED
ドライブに割り当て済みの暗号化鍵が削除される保守操作または処理が実行されたとき*	ENCRYPTION KEY DELETED
* 記録される契機に対応する保守操作または処理は「暗号化鍵の管理」を参照してください。	

≪Bare metal≫

これらの監査ログは暗号化鍵ごとに記録され、それぞれの監査ログには暗号化鍵が割り当てられたドライブの WWID(WWN)の情報が含まれます。

予期せずストレージノードからドライブが物理的に抜き取られた場合、ENCRYPTION KEY DELETED の監査ログが記録されます。これによって、抜き取られたドライブに対応する暗号化鍵がストレージクラスター内から削除されたことを監査ログに含まれるドライブの WWID(WWN)の情報から確認することができます。

≪Cloud for AWS≫

これらの監査ログは暗号化鍵ごとに記録され、それぞれの監査ログには EBS のボリューム ID からハイフンを除いた値が出力されます。

予期せずストレージノードから EBS ボリュームがデタッチされた場合、ENCRYPTION KEY DELETED の監査ログが記録されます。これによって、抜き取られたドライブに対応する暗号化鍵がストレージクラスター内から削除されたことを監査ログに含まれるドライブの EBS のボリューム ID からハイフンを除いた値の情報から確認することができます。

≪Cloud for Google Cloud≫

これらの監査ログは暗号化鍵ごとに記録され、それぞれの監査ログには Google Cloud Hyperdisk ボリュームのディスク名が出力されます。

予期せずストレージノードから Google Cloud Hyperdisk ボリュームがデタッチされた場合、ENCRYPTION KEY DELETED の監査ログが記録されます。これによって、抜き取られたドライブに対応する暗号化鍵がストレージクラスター内から削除されたことを監査ログに含まれるドライブの Google Cloud Hyperdisk ボリュームのディスク名から確認することができます。

≪Cloud for Microsoft Azure≫

これらの監査ログは暗号化鍵ごとに記録され、それぞれの監査ログには Azure マネージドディスク ボリュームのディスク名が出力されます。

予期せずストレージノードから Azure マネージドディスクボリュームがデタッチされた場合、ENCRYPTION KEY DELETED の監査ログが記録されます。これによって、抜き取られたドライブに対応する暗号化鍵がストレージクラスター内から削除されたことを監査ログに含まれるドライブの Azure マネージドディスクボリュームのディスク名から確認することができます。

42.2 暗号化環境の設定を編集する

暗号化環境の設定を編集します。

暗号化環境の設定を有効にすると、ストレージクラスター内で保持する暗号化鍵の数が 4,096 個になるよう、未割り当ての暗号化鍵が作成されます。

前提条件

- 実行に必要なロール : Security
- Data At Rest Encryption のプログラムプロダクトライセンスを登録していること
- 暗号化環境の設定を無効から有効または有効から無効に変更する場合「空状態にあるストレージプールの拡張」を実施していないこと
「空状態にあるストレージプールの拡張」を実施していないことは、ストレージプールの情報の totalPhysicalCapacity[MiB]の値が 0 であることによって確認できます。
- 暗号化環境の設定を有効から無効にする場合、ストレージプールの暗号化の設定が無効であること

操作手順

1. 暗号化環境の設定を編集します。
暗号化環境の設定の有効/無効を指定して、コマンドを実行します。
REST API : PATCH /v1/objects/encryption-settings
CLI : encryption_setting_set
コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

3. 暗号化環境の設定の情報を取得して、暗号化環境の設定が編集されたことを確認します。

REST API : GET /v1/objects/encryption-settings

CLI : encryption_setting_show

4. 手順 1 で暗号化環境の設定を有効にした場合、暗号化鍵の個数を取得して、暗号化鍵が作成されたことを確認します。

REST API : GET /v1/objects/encryption-key-counts

CLI : encryption_key_count_show

"dek"の値と"free"の値の合計が 4096 であることを確認します。システムで初めて暗号化環境の設定を無効から有効にした場合は、"dek"の値が 0、"free"の値が 4096 になります。

5. <<Bare metal>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

6. <<Cloud for AWS>>構成情報のバックアップを行います。

「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

42.3 暗号化環境の設定の情報を取得する

暗号化環境の設定の情報について、以下の情報を取得します。

- isEnabled : 暗号化環境を有効にするかどうか
- kms : 暗号化鍵管理サーバーを使用するかどうか
- warningThresholdOfFreeKey : 暗号化対象に未割り当ての暗号化鍵の個数の警告しきい値

前提条件

- 実行に必要なロール : Security

操作手順

1. 暗号化環境の設定の情報を取得します。

REST API : GET /v1/objects/encryption-settings

CLI : encryption_setting_show

42.4 ストレージプールの暗号化の設定を編集する

ストレージプールの暗号化の設定を編集します。

前提条件

- 実行に必要なロール : Security

- Data At Rest Encryption のプログラムプロダクトライセンスを登録していること
- ストレージプールの暗号化の設定を無効から有効にする場合、暗号化環境の設定が有効であること
- ストレージプールの暗号化の設定を無効から有効、または有効から無効に変更する場合「空状態にあるストレージプールの拡張」を実施していないこと
「空状態にあるストレージプールの拡張」を実施していないことは、ストレージプールの情報の totalPhysicalCapacity[MiB]の値が 0 であることによって確認できます。

操作手順

1. ストレージプールの ID を確認します。
REST API : GET /v1/objects/pools
CLI : pool_list
2. ストレージプールの暗号化の設定を編集します。
ストレージプールの ID とストレージプールの暗号化の設定の有効/無効を指定して、コマンドを実行します。
REST API : PATCH /v1/objects/encryption-units/pools/<id >
CLI : encryption_unit_pool_set
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
4. ストレージプールの情報を取得して、ストレージプールの暗号化の設定が編集されたことを確認します。
ストレージプールの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/pools/<id >
CLI : pool_show
5. <<Bare metal>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
6. <<Cloud for AWS>>構成情報のバックアップを行います。
「構成情報をバックアップする<<Bare metal>><<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

42.5 暗号化鍵を作成する

暗号化鍵を作成します。

この手順で作成する暗号化鍵はドライブに未割り当ての暗号化鍵です。ストレージクラスターごとに保持できる暗号化鍵の最大数は、ドライブに未割り当ての暗号化鍵とドライブに割り当て済みの暗号化鍵を合わせて 4,096 個です。ストレージクラスターごとに保持できる暗号化鍵の最大数を超えないように暗号化鍵を作成してください。



メモ

未割り当ての暗号化鍵は、この章の「暗号化環境の設定を編集する」に従って、暗号化環境の設定を有効にした場合にも作成されます。暗号化環境の設定を有効にすると、ストレージクラスター内で保持する暗号化鍵の数が 4,096 個になるよう、未割り当ての暗号化鍵が作成されます。ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「格納データ暗号化を設定する」に従って、セットアップの作業をしている場合には本操作は不要です。

前提条件

- 実行に必要なロール：Security
- Data At Rest Encryption のプログラムプロダクトライセンスを登録していること
- 暗号化環境の設定が有効であること

操作手順

1. 暗号化鍵の個数を取得して、作成可能な暗号化鍵の数を確認します。
REST API : GET /v1/objects/encryption-key-counts
CLI : encryption_key_count_show
作成可能な暗号化鍵の数は以下の計算で求められます。
作成可能な暗号化鍵の数 = 4096 - ("dek"の値 + "free"の値)
2. 暗号化鍵を作成します。
作成する暗号化鍵の数を指定してコマンドを実行します。手順 1 で求めた作成可能な暗号化鍵の数以下の値を指定します。
REST API : POST /v1/objects/encryption-keys
CLI : encryption_key_create
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId>
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
4. 暗号化鍵の個数を取得して、暗号化鍵が作成されたことを確認します。
REST API : GET /v1/objects/encryption-key-counts
CLI : encryption_key_count_show

42.6 暗号化鍵を削除する

暗号化鍵を削除します。

この手順で削除できる暗号化鍵はドライブに未割り当ての暗号化鍵のみです。割り当て済みの暗号化鍵は自動的に削除されるため、基本的には本手順を実施する必要はありません。割り当て済みの暗号化鍵が削除される契機は、この章の「格納データ暗号化の概要」を参照してください。何らかの事情によって特定の未割り当ての暗号化鍵を削除する場合は本手順で削除することができます。

前提条件

- 実行に必要なロール：Security
- Data At Rest Encryption のプログラムプロダクトライセンスを登録していること
- 暗号化環境の設定が有効であること

操作手順

1. 削除する暗号化鍵の ID を確認します。
REST API : GET /v1/objects/encryption-keys
CLI : encryption_key_list
2. 暗号化鍵を削除します。
暗号化鍵の ID を指定してコマンドを実行します。
REST API : DELETE /v1/objects/encryption-keys/<id >
CLI : encryption_key_delete
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
4. 暗号化鍵の一覧を取得して、暗号化鍵が削除されたことを確認します。
REST API : GET /v1/objects/encryption-keys
CLI : encryption_key_list

42.7 暗号化鍵の情報の取得

暗号化鍵の情報が一覧または個別に取得できます。

42.7.1 取得できる暗号化鍵の情報<<Bare metal>>

この項での記述内容は Bare metal モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : 暗号化鍵の ID(uuid)
- createTime : 暗号化鍵の作成日時
- keyType : 暗号化鍵の種別
 - DEK : 暗号化対象に割り当て済みの暗号化鍵
 - Free : 暗号化対象に未割り当ての暗号化鍵
- targetInformation : 暗号化鍵の割り当て先となるリソースの ID(uuid)。対象のリソースはドライブ
暗号化鍵が使用されていない場合は、00000000-0000-0000-0000-000000000000 が出力される
- keyGeneratedLocation : 暗号化鍵の生成場所。内部生成暗号化鍵の場合 "Internal"
- numberOfBackups : 暗号化鍵のバックアップ回数。常に 0
- targetName : 暗号化鍵の割り当て先となるリソースの名前
ドライブの場合は WWID(WWN)

42.7.2 取得できる暗号化鍵の情報<<Cloud>>

この項での記述内容は Cloud モデルに適用されます。

以下の情報が一覧または個別に取得できます。

- id : 暗号化鍵の ID(uuid)
- createTime : 暗号化鍵の作成日時
- keyType : 暗号化鍵の種別
 - DEK : 暗号化対象に割り当て済みの暗号化鍵
 - Free : 暗号化対象に未割り当ての暗号化鍵
- targetInformation : 暗号化鍵の割り当て先となるリソースの ID(uuid)。対象のリソースはドライブ
暗号化鍵が使用されていない場合は、00000000-0000-0000-0000-000000000000 が出力される
- keyGeneratedLocation : 暗号化鍵の生成場所。内部生成暗号化鍵の場合"Internal"
- numberOfBackups : 暗号化鍵のバックアップ回数。常に 0
- targetName : 暗号化鍵の割り当て先となるリソースの名前
 <<Cloud for AWS>> ドライブの場合は EBS のボリューム ID からハイフンを除いた値
 <<Cloud for Google Cloud>> ドライブの場合はディスク名
 <<Cloud for Microsoft Azure>> ドライブの場合はディスク名

42.7.3 暗号化鍵の情報の一覧を取得する

暗号化鍵の情報を一覧で取得します。

前提条件

- 実行に必要なロール : Security

操作手順

1. 暗号化鍵の情報を一覧で取得します。
 REST API : GET /v1/objects/encryption-keys
 CLI : encryption_key_list

42.7.4 暗号化鍵の情報を個別に取得する

指定した ID の暗号化鍵の情報を取得します。

前提条件

- 実行に必要なロール : Security

操作手順

1. 暗号化鍵の情報を一覧で取得し、暗号化鍵の ID を確認します。
 REST API : GET /v1/objects/encryption-keys
 CLI : encryption_key_list
2. 暗号化鍵の情報を取得します。
 暗号化鍵の ID を指定してコマンドを実行します。
 REST API : GET /v1/objects/encryption-keys/<id >
 encryption_key_show

42.8 暗号化鍵の個数を取得する

暗号化鍵の個数について、以下の情報を取得します。

- dek : 暗号化対象に割り当て済みの暗号化鍵の個数
- free : 暗号化対象に未割り当ての暗号化鍵の個数

前提条件

- 実行に必要なロール : Security

操作手順

1. 暗号化鍵の個数を取得します。

REST API : GET /v1/objects/encryption-key-counts

CLI : encryption_key_count_show

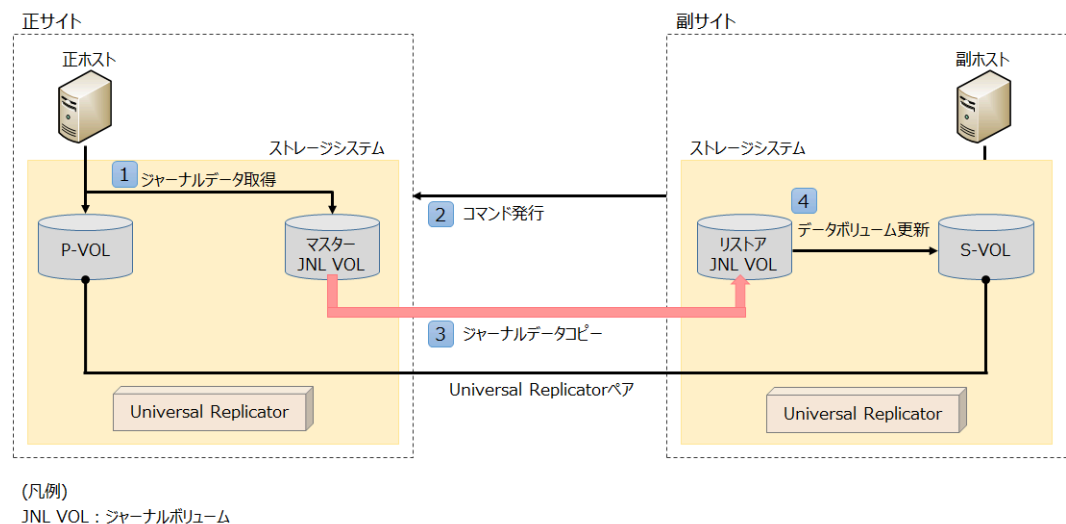
Universal Replicator を利用する

- 43.1 Universal Replicator の概要
- 43.2 Universal Replicator 利用時の留意事項

43.1 Universal Replicator の概要

Universal Replicator は、ストレージシステムに格納されているデータを遠隔地に設置された別のストレージシステムにコピーする機能です。地震などの自然災害によってストレージシステム(正サイトのストレージシステム)が被災した場合でも、遠隔地に設置されたストレージシステム(副サイトのストレージシステム)でデータを保護できます。

Universal Replicator を利用したシステム構築方法については「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」を参照してください。



43.2 Universal Replicator 利用時の留意事項

Universal Replicator を利用してシステムを構築する際に利用する VSP One SDS Block の機能と、各機能における留意事項には以下があります。

Universal Replicator を利用したシステム構築の全容は「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」に記載してあります。その他の参照マニュアルは下表の備考欄に記載してあります。備考欄に参照マニュアルの記載がない説明の詳細は、このマニュアルに記載されています。

機能	留意事項	備考
RAID Manager	以下のペア操作を行うときに使用します。 - ペア作成 - ペア分割 - ペア再同期 - ペア削除 - ペア正副入れ替え	- 操作方法は「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」を参照してください。 - RAID Manager からのアクセス(セッション)のタイムアウト時間は 3,600 秒です。
ネットワーク	Universal Replicator を使用する場合、以下のネットワークを使用できるように設定する必要があります。	詳しくは「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」を参照してください。

機能	留意事項	備考
	- VSP One SDS Block のコンピュータネットワーク(ストレージシステム間の通信のため) - VSP One SDS Block の管理ネットワーク(RAID Manager と VSP One SDS Block 間の通信のため)	なお、各ストレージシステムの RAID Manager 間の通信も設定する必要があります。
ボリューム	通常ボリュームとして作成し、ジャーナルを定義することで、ジャーナルボリュームになります。	- ペアを組んでいるボリュームやジャーナルボリュームの削除・圧縮・拡張はできません。ジャーナルから外されたジャーナルボリュームは削除できます。 - ジャーナルグループ作成・変更については「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」を参照してください。
容量バランス	ジャーナルが 1 つ以上存在するストレージコントローラーのボリュームは容量バランスによる移動の対象外になります。Universal Replicator を利用する場合、容量バランスは無効に設定してください。	
ロール	Universal Replicator、RAID Manager を利用する際に必要なロールとして以下があります。これらのロールはビルトインユーザーグループにも含まれています。 RemoteCopy	
VSP One SDS Block Administrator	Universal Replicator に関する操作として以下が行えます。 - リモートパスグループ管理 - ボリューム管理	- 左記以外にも、ボリューム情報、ストレージコントローラー情報などに、Universal Replicator のサポートによって追加された情報があり、それらの情報が表示されます。 - 詳しくは「Hitachi Virtual Storage Platform One SDS Block Administrator GUI ガイド」を参照してください。
REST API/CLI	Universal Replicator に関する操作として以下が行えます。 - リモートパスグループ - ボリューム管理 - ジャーナル管理	詳しくは「Hitachi Virtual Storage Platform One SDS Block Universal Replicator ガイド」を参照してください。
サーバー証明書	Universal Replicator を利用する場合は、サーバー証明書の Subject Alternative Name に IP アドレスを設定してください。	
キャッシュ保護付きライトバックモード	Universal Replicator を利用する場合は、キャッシュ保護付きライトバックモードを有効に設定してください。	

容量バランスを管理する

- 44.1 容量バランスの概要
- 44.2 容量バランスの発動条件
- 44.3 ストレージクラスターの容量バランスの設定を編集する
- 44.4 ストレージクラスターの容量バランスの設定を取得する
- 44.5 ストレージコントローラーの容量バランスの設定を編集する
- 44.6 ストレージコントローラーの容量バランスの設定を取得する
- 44.7 ストレージノードの容量バランスの設定を編集する
- 44.8 ストレージノードの容量バランスの情報の取得

44.1 容量バランスの概要

ストレージコントローラー間の容量使用率が偏ると、VSP One SDS Block は、容量使用率の高いストレージコントローラーから、容量使用率の低いストレージコントローラーに自動的にボリュームを移動します。この処理を容量バランスといいます。容量バランスは、ストレージプール全体でストレージコントローラーごとの容量使用率を平準化する目的で動作します。容量バランスの有効/無効は設定で変更することができます。容量バランスのデフォルトは有効です。容量バランスの設定は、ストレージクラスター・ストレージノード・ストレージコントローラーの粒度で有効/無効が設定可能です。

容量バランスの設定を無効にすると、下記の動作になります。

いずれか1つでも無効に設定すると、各説明に記載してあるストレージコントローラーの容量バランスが無効となります。

- ストレージクラスター：
ストレージクラスター上で動作しているストレージコントローラーを移動先/移動元とするボリューム移動は行われません。
システム全体の容量バランスを止めたい場合はこちらを無効に設定してください。
- ストレージノード：
指定したストレージノード上でアクティブまたはスタンバイとして動作するストレージコントローラーを移動先/移動元とするボリューム移動は行われません。
ストレージノードの設定は旧バージョンとの互換性を保つために用意してあります。新たに設定を変更する場合は、ストレージクラスターかストレージコントローラーでの指定を検討してください。
- ストレージコントローラー：
指定したストレージコントローラーを移動先/移動元とするボリューム移動は行われません。
特定のストレージコントローラーのみの容量バランスを止めたい場合はこちらを無効に設定してください。

各設定値は独立して設定でき、例えば、ストレージクラスターの設定を変更しても、ストレージノード・ストレージコントローラーそれぞれの設定値は維持されます。

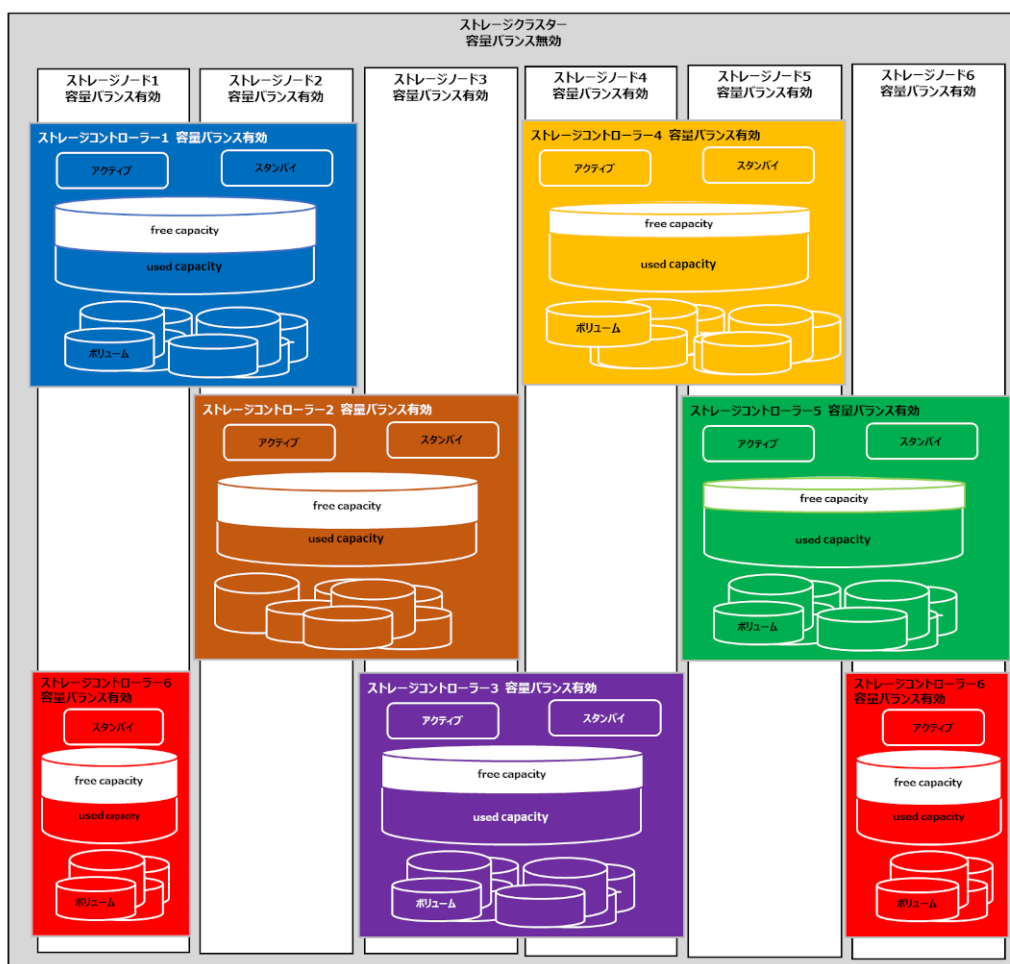


メモ

- ストレージノードを指定して無効設定を行っている場合、ストレージノードの増設/減設に伴って、ストレージノード上で動作するストレージコントローラーが変わる場合があります。
ストレージノードの増設/減設に影響を受けないようにするためには、ストレージノードの設定は使用せず、ストレージクラスターやストレージコントローラーの設定を使用してください。
- ストレージノードの無効設定から、ストレージクラスターの無効設定に移行する際は、先にストレージクラスターの設定を無効に設定し、そのあとで、すべてのストレージノードの設定を有効に設定してください。
- ストレージノードの無効設定から、ストレージコントローラーの無効設定に移行する際は「ストレージコントローラー情報の一覧を取得する」を参照して、`activeStorageNodeId`、`standbyStorageNodeId`、`secondaryStandbyStorageNodeId` のいずれかのフィールドに対象のストレージノードが表示されているストレージコントローラーすべてに対して、設定を変更してください。その後、対象のストレージノードの設定を有効に設定してください。

(1)下図は、ストレージクラスターの容量バランスを無効に設定した際の状態を示しています。

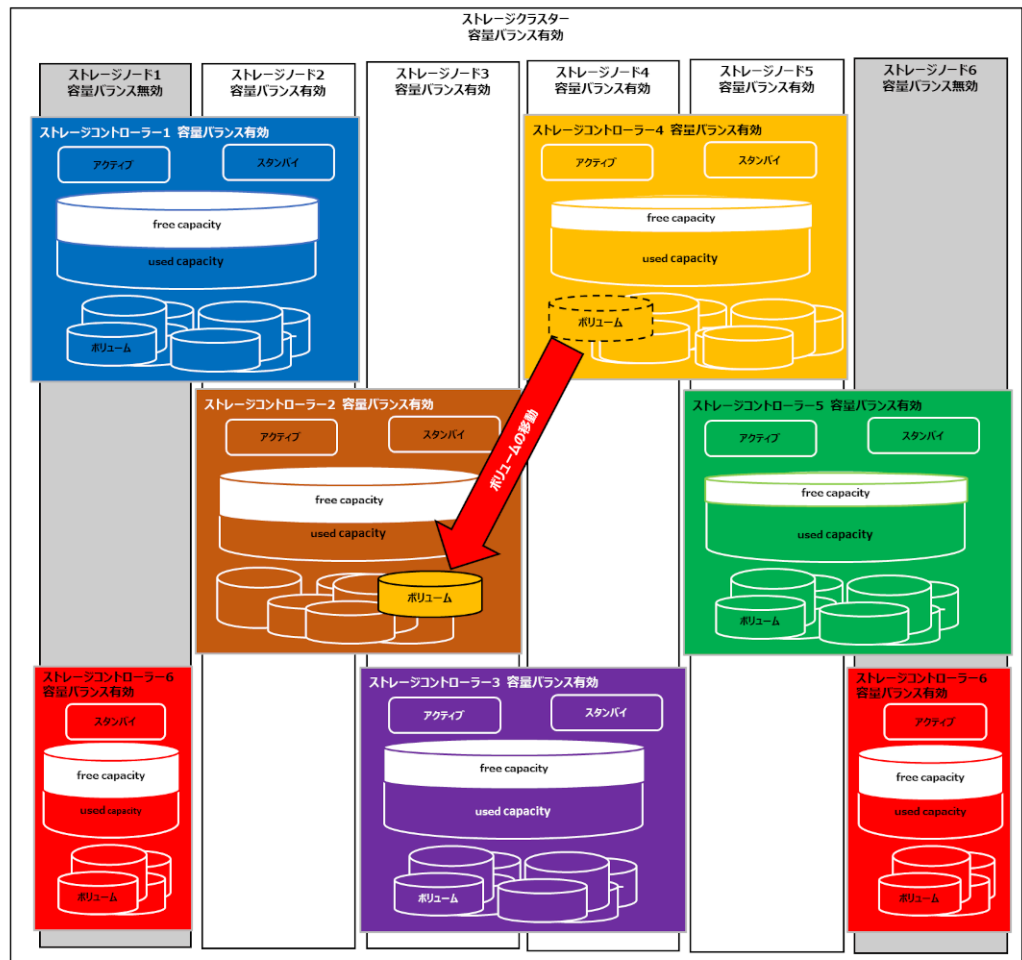
この場合、すべてのストレージコントローラーの管理するボリュームは容量バランスで移動する対象とならず、移動先のストレージコントローラーとしても選定されません。



(2)下図は、ストレージノード1とストレージノード6の容量バランスを無効に設定した際の状態を示しています。

この場合、ストレージコントローラー1、ストレージコントローラー5、およびストレージコントローラー6の管理するボリュームは容量バランスで移動する対象とならず、移動先のストレージコントローラーとしても選定されません。

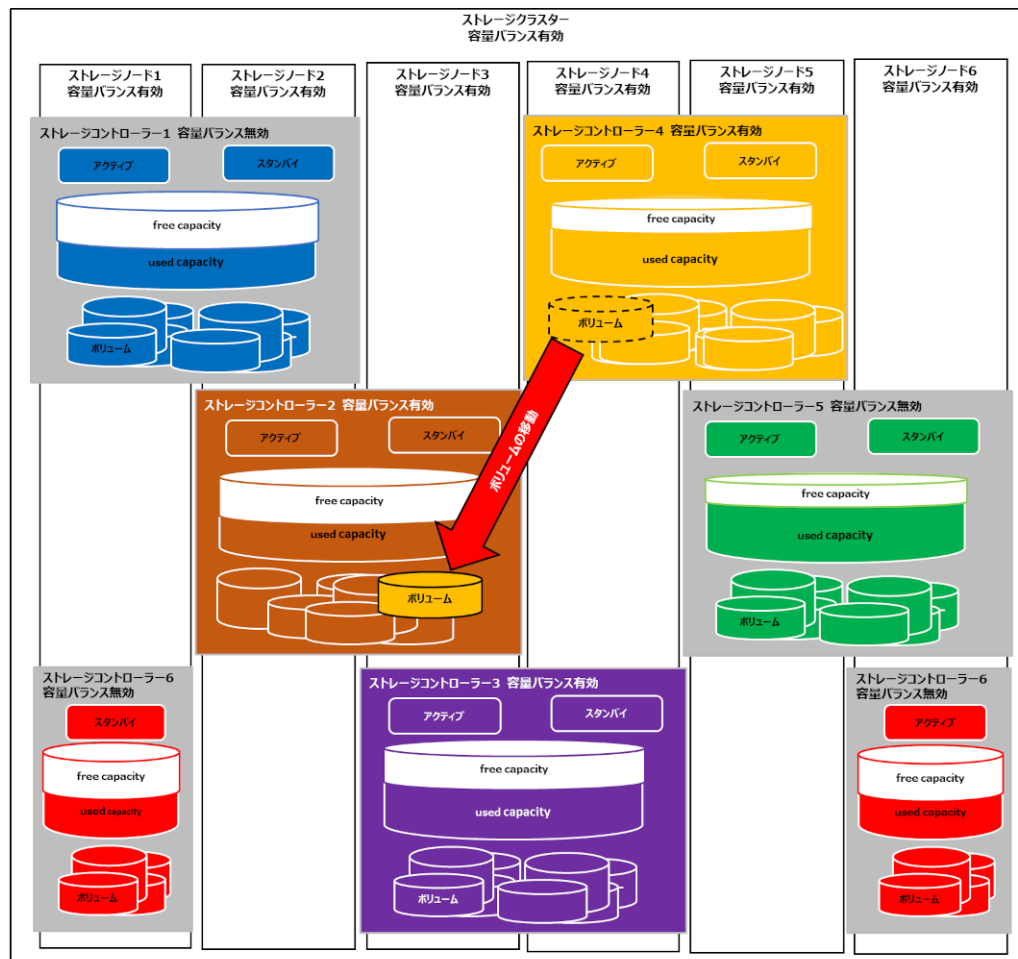
また、ストレージコントローラー4とストレージコントローラー5の使用容量が高く、ストレージコントローラー1とストレージコントローラー2、およびストレージコントローラー6の容量使用率が低いです。このとき、容量バランスが有効となっているストレージノードにのみ関連するストレージコントローラーで容量バランスが実行されます。そのため、ストレージコントローラー4からストレージコントローラー2へ、容量バランスによるボリュームの移動が実行されます。



(3)下図は、ストレージコントローラー 1 とストレージコントローラー 5 とストレージコントローラー 6 の容量バランスを無効に設定した際の状態を示しています。

この場合、ストレージコントローラー 1 とストレージコントローラー 5、およびストレージコントローラー 6 が管理するボリュームは容量バランスで移動する対象とならず、移動先のストレージコントローラーとしても選定されません。

また、ストレージコントローラー 4 とストレージコントローラー 5 の使用容量が高く、ストレージコントローラー 1 とストレージコントローラー 2、およびストレージコントローラー 6 の容量使用率が低いです。このとき、容量バランスが有効となっているストレージノードにのみ関連するストレージコントローラーで容量バランスが実行されます。そのため、ストレージコントローラー 4 からストレージコントローラー 2 へ、容量バランスによるボリュームの移動が実行されます。



44.2 容量バランスの発動条件

容量バランスは、以下の条件をすべて満たすときに発動します。容量バランスの発動後は「動作中の容量バランスの中断について」に示す操作が実行されたとき、または事象が発生したときに中断されます。



メモ

≪Cloud≫Multi-AZ (Multi-Zone)構成の場合、容量バランスは同一のフォールトドメイン内のストレージコントローラー間で行われます。したがって、容量バランスによってボリューム移動が行われる範囲は、同一のフォールトドメイン内に限定されます。

このため、以下に記載されている条件を参照する際は、「ストレージプール」を「フォールトドメイン」と読み替えてください。

容量バランスの範囲となるフォールトドメインは、対象となるストレージコントローラーのプライマリフォールトドメインになります。

(1) ストレージプールの容量使用率(usedCapacityRate[%])が 80 以下であること

(2) 以下の 4 つの条件をすべて満たすストレージコントローラーが存在すること

- ・ ストレージコントローラーの容量使用率(allocatableCapacityUsageRate[%])が 70 以上である
- ・ ストレージコントローラーの容量が枯渇しないよう、以下のいずれかの条件を満たしている

- ・ 当該ストレージコントローラーの全ボリュームの管理領域を含めた容量が `allocatableCapacity[MiB]` 以上である(オーバープロビジョニングしている)
- ・ 当該ストレージコントローラーにスナップショットボリュームが存在する
- ・ 当該ストレージコントローラーに容量削減機能が有効なボリュームが存在する
- ・ ストレージコントローラーの容量使用率(`allocatableCapacityUsageRate[%]`)がストレージプールの容量使用率(`usedCapacityRate[%]`)以上である
- ・ 容量バランスが動作中のストレージコントローラーではない

(3)以下の3つの条件すべてを満たすストレージコントローラーであること

- ・ ストレージクラスターの容量バランス設定が有効である
- ・ 当該ストレージコントローラーの容量バランス設定が有効である
- ・ 当該ストレージコントローラーがアクティブまたはスタンバイとして動作するストレージノードの容量バランス設定が有効である

動作中の容量バランスの中断について

以下の操作が実行された、または事象が発生した場合、容量バランスは中断されることがあります。

- ・ 移動中のボリュームを対象とするボリューム操作、またはスナップショット操作が開始された
- ・ 移動元ストレージノードを対象とするストレージノード減設が開始された
- ・ 移動先ストレージノードを対象とするストレージノード減設が開始された
- ・ 移動先ストレージコントローラーの容量使用率(`allocatableCapacityUsageRate[%]`)が 95 に到達した
- ・ 移動元ストレージノードが閉塞した
- ・ ストレージクラスターの停止
- ・ ソフトウェアアップデート
- ・ リビルド

容量バランスが中断された場合、対象ボリュームごとに移動が中断されたことを示すイベントログ `KARS06332-I` が出力されます。上記の操作または事象の完了後、改めて容量バランスの発動条件を満たしているか定期的に判断されて、発動条件を満たしている場合は容量バランスの処理が再発動されます。

容量バランス設定(有効/無効)の判断

以下のような場合は容量バランスを有効にしてください。

- ・ ストレージプールやストレージコントローラーの容量使用率に合わせて、容量バランスを自動で動作させたい
- ・ 容量使用率が高くなったときに、ストレージノードの増設で容量追加をして、既存のストレージコントローラーのボリュームが移動可能なら自動で移動させたい

以下のような場合は容量バランスを無効にしてください。

容量バランスを無効にした場合は、容量が枯渇しないようにストレージコントローラーごとの容量使用率を監視してください。

- ・ 容量よりも I/O 性能を優先しており、容量バランスによるボリュームの移動で I/O 性能を低下させたくない

- 容量を使い切れるようにボリュームを作成しているので、ボリュームを移動したくない
- ストレージコントローラーを指定してボリュームを作成しており、ボリュームを移動したくない
- ストレージノード増設をして、その増設したストレージノードにボリュームを移動したくない



メモ

- 以下のボリュームは、容量バランスによるストレージノード間での移動は行われません。
 - スナップショットボリューム(P-VOL、P/S-VOL、または S-VOL)
 - 容量削減機能の状態(dataReductionStatus)が"Failed"のボリューム
 - 容量削減機能が有効になったボリュームで当該ボリュームの圧縮前容量に対し、当該ボリュームが消費するシステムデータ量が占める割合が 10%を超えているボリューム
- 以下のボリュームが存在する場合は、容量バランスによる容量の平準化の効果が十分ではないことがあります。
 - ボリュームの容量が、ストレージコントローラーの allocatableCapacity[MiB]の 20%を超えるボリュームが存在する
- 容量バランスは、ストレージプール全体の容量使用率を平準化することが目的のため、ストレージプールの容量使用率を上回っているストレージコントローラーにはボリュームを移動しません。

≪Bare metal≫容量バランスの処理性能と並列移動が可能なボリューム数は以下のとおりです。

- 容量バランスの処理性能(ボリューム 1 個当たり、目安) : 14.7[MiB/sec]
- 並列移動が可能なボリューム数(ストレージノード 1 台当たり) : 42 個



注意

ストレージノードの容量バランスの処理中は、既存ボリュームの I/O 性能に影響が出ることがあります。特に、容量削減機能が有効なボリュームを対象とした容量バランスによるボリューム移動の際には、既存ボリュームの I/O 性能への影響がより大きく出ることがあります。

44.3 ストレージクラスターの容量バランスの設定を編集する

ストレージクラスターの容量バランスの有効/無効を設定します。容量バランスのデフォルトは有効です。

前提条件

- 実行に必要なロール : Storage

操作手順

1. ストレージクラスターの容量バランスの設定を編集します。
type に StorageCluster を指定し、容量バランスの有効/無効を指定してコマンドを実行します。
REST API : PATCH /v1/objects/capacity-settings
CLI : capacity_setting_set
コマンド実行後に表示されるジョブの ID を確認します。
2. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId>
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。

3. ストレージクラスターの容量バランスの設定を取得して、容量バランスの設定が編集されたことを確認します。

REST API : GET /v1/objects/capacity-settings

CLI : capacity_setting_list

4. ≪Bare metal≫構成情報のバックアップを行います。

「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

5. ≪Cloud for AWS≫構成情報のバックアップを行います。

「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

44.4 ストレージクラスターの容量バランスの設定を取得する

ストレージクラスターの容量バランスの設定を一覧で取得します。以下の情報が得られます。

- storageCluster : ストレージクラスターの容量バランスの設定
- storageControllers : ストレージコントローラーの容量バランスの設定

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. ストレージクラスターの容量バランスの設定を取得します。

REST API : GET /v1/objects/capacity-settings

CLI : capacity_setting_list

44.5 ストレージコントローラーの容量バランスの設定を編集する

ストレージコントローラーの容量バランスの有効/無効を設定します。容量バランスのデフォルトは有効です。

前提条件

- 実行に必要なロール : Storage

操作手順

1. ストレージコントローラーの ID を確認します。

REST API : GET /v1/objects/storage-controllers

CLI : storage_controller_list

2. ストレージコントローラーの容量バランスの設定を編集します。

type に StorageController を指定し、ストレージコントローラーの ID と容量バランスの有効/無効を指定してコマンドを実行します。

REST API : PATCH /v1/objects/capacity-settings

CLI : capacity_setting_set

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4. ストレージコントローラーの容量バランスの設定を取得して、容量バランスの設定が編集されたことを確認します。

REST API : GET /v1/objects/capacity-settings

CLI : capacity_setting_list

5. ≪Bare metal≫構成情報のバックアップを行います。

「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

6. ≪Cloud for AWS≫構成情報のバックアップを行います。

「構成情報をバックアップする ≪Bare metal≫ ≪Cloud for AWS≫」を参照して実施してください。

ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

44.6 ストレージコントローラーの容量バランスの設定を取得する

ストレージコントローラーの容量バランスの設定を一覧で取得します。以下の情報が得られます。

- storageCluster : ストレージクラスターの容量バランスの設定
- storageControllers : ストレージコントローラーの容量バランスの設定

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. ストレージコントローラーの容量バランスの設定を取得します。

REST API : GET /v1/objects/capacity-settings

CLI : capacity_setting_list

44.7 ストレージノードの容量バランスの設定を編集する

ストレージノードの容量バランスの有効/無効を設定します。容量バランスのデフォルトは有効です。



メモ

本コマンドは、旧バージョンとの互換性を保つために用意してあります。新たに設定を変更する場合は、ストレージクラスターかストレージコントローラーでの設定を検討してください。

前提条件

- 実行に必要なロール : Storage

操作手順

1. ストレージノードの ID を確認します。
REST API : GET /v1/objects/storage-nodes
CLI : storage_node_list
2. ストレージノードの容量バランスの設定を編集します。
ストレージノードの ID と容量バランスの有効/無効を指定してコマンドを実行します。
REST API : PATCH /v1/objects/storage-node-capacity-settings/<id >
CLI : storage_node_capacity_setting_set
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が "Succeeded" になっていたらジョブは完了です。
4. ストレージノードの容量バランスの設定を取得して、容量バランスの設定が編集されたことを確認します。
ストレージノードの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/storage-node-capacity-settings/<id >
CLI : storage_node_capacity_setting_show
5. <<Bare metal>>構成情報のバックアップを行います。
「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。
6. <<Cloud for AWS>>構成情報のバックアップを行います。
「構成情報をバックアップする <<Bare metal>> <<Cloud for AWS>>」を参照して実施してください。
ただし、継続して他手順の操作を実施する場合は、すべての操作が完了したあとに構成情報のバックアップを行ってください。

44.8 ストレージノードの容量バランスの情報の取得

ストレージノードの容量バランスの情報が一覧または個別に取得できます。

44.8.1 取得できるストレージノードの容量バランスの情報

以下の情報が一覧または個別に取得できます。

- id : ストレージノードの ID(uuid)
- capacityBalancingSetting : 容量バランスの設定

44.8.2 ストレージノードの容量バランスの情報を一覧で取得する

各ストレージノードの容量バランスの情報を一覧で取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. ストレージノードの容量バランスの設定を一覧で取得します。

REST API : GET /v1/objects/storage-node-capacity-settings

CLI : storage_node_capacity_setting_list

44.8.3 ストレージノードの容量バランスの情報を個別に取得する

指定したストレージノードの容量バランスの情報を取得します。

前提条件

- 実行に必要なロール : Storage、RemoteCopy、Monitor、または Resource

操作手順

1. ストレージノードの ID を確認します。

REST API : GET /v1/objects/storage-nodes

CLI : storage_node_list

2. ストレージノードの容量バランスの設定を取得します。

ストレージノードの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/storage-node-capacity-settings/<id >

CLI : storage_node_capacity_setting_show

メタデータのドライブ書き込み削減モードを管理する

- 45.1 メタデータのドライブ書き込み削減モードの概要
- 45.2 メタデータのドライブ書き込み削減モードを有効にする
- 45.3 メタデータのドライブ書き込み削減モードを無効にする

45.1 メタデータのドライブ書き込み削減モードの概要

メタデータのドライブ書き込み削減モードは、メタデータのドライブ書き込み削減機能の有効/無効状態を示すモードです。メタデータのドライブ書き込み削減モードが有効に設定されている場合、メタデータのドライブ書き込み削減機能が有効であることを示します。

- メタデータのドライブ書き込み削減機能は、ストレージソフトウェアの 01.18.0x.xx のバージョンからサポートされます。ストレージソフトウェアの 01.18.0x.xx のバージョン以降で新規インストールをした場合、この機能はデフォルトで有効になります。
- ストレージソフトウェアを 01.18.0x.xx 以降のバージョンにアップグレードした場合は、キャッシュ保護付きライトバックモードの状態に従って、メタデータのドライブ書き込み削減モードが設定されます。
キャッシュ保護付きライトバックモードが有効の場合は、メタデータのドライブ書き込み削減モードは有効になります。
キャッシュ保護付きライトバックモードが無効の場合は、メタデータのドライブ書き込み削減モードは無効になります。
- ストレージソフトウェアを 01.18.0x.xx より前のバージョンにダウングレードする場合は、メタデータのドライブ書き込み削減モードを無効にする必要があります。手順の詳細は、「メタデータのドライブ書き込み削減モードを無効にする」を参照してください。

メタデータのドライブ書き込み削減モードの状態について

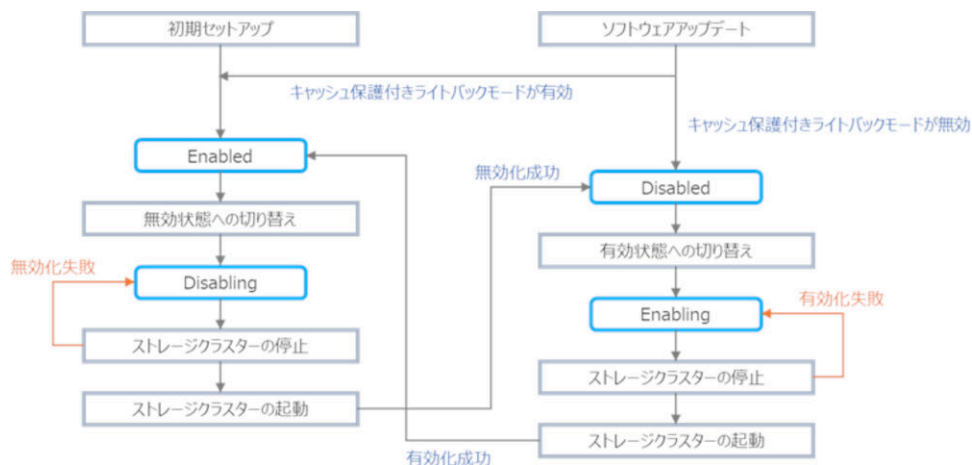
メタデータのドライブ書き込み削減モードの状態(metadataDriveWriteReductionMode)はストレージクラスターの情報から取得できます。ストレージクラスター情報の取得方法は、このマニュアルの「ストレージクラスターの情報を取得する」を参照してください。

メタデータのドライブ書き込み削減モードの状態表示とその説明を以下に示します。

状態表示	説明
Enabled	メタデータのドライブ書き込み削減機能が有効な状態です。
Disabled	メタデータのドライブ書き込み削減機能が無効な状態です。
Enabling	メタデータのドライブ書き込み削減機能を無効から有効に切替中であることを示します。 Disabled 状態から有効な状態への切り替えを実施することで、"Enabling"状態になります。そのあと、ストレージクラスターを停止してからストレージクラスターを起動することで、"Enabled"状態へ切り替わります。
Disabling	メタデータのドライブ書き込み削減機能を有効から無効に切替中であることを示します。 Enabled 状態から無効な状態への切り替えを実施することで、"Disabling"状態になります。そのあと、ストレージクラスターを停止してからストレージクラスターを起動することで、"Disabled"状態へ切り替わります。

メタデータのドライブ書き込み削減モードの状態の遷移

初期セットアップ、またはメタデータのドライブ書き込み削減モードが非サポートのバージョンからのソフトウェアアップデート後のメタデータのドライブ書き込み削減モードについての状態遷移を以下に示します。



45.2 メタデータのドライブ書き込み削減モードを有効にする

メタデータのドライブ書き込み削減モードを有効にする場合は、以下の手順を実施してください。



注意

メタデータのドライブ書き込み削減モードを有効にするには、手順 5 でのストレージクラスターの停止を実行する前に、ホストからの I/O をすべて停止させる必要があります。

前提条件

- 実行に必要なロール：Service
- ストレージクラスターの status が"Ready"であること
ストレージノード情報の一覧取得、および VSP One SDS Block Administrator の Health Status にて確認してください。
- キャッシュ保護付きライトバックモードが有効であること
「キャッシュ保護付きライトバックモードの有効化」を参照し、キャッシュ保護付きライトバックモードの状態の確認および有効化を実施してください。

操作手順

1. メタデータのドライブ書き込み削減モードの状態を確認します。

REST API：GET /v1/objects/storage

CLI：storage_show

メタデータのドライブ書き込み削減モードの状態(metadataDriveWriteReductionMode)によって以下の対応を行います。

メタデータのディスク書き込み削減モードの状態	対応方法
Enabled	以上で手順は終了です。
Disabled	次の手順に進みます。
Enabling	手順 4 に進みます。
Disabling	「メタデータのドライブ書き込み削減モードを無効にする」の手順 4 以降を実施し、再度手順 1 から実行してください。

2. メタデータのドライブ書き込み削減モードを有効にします。

isEnabled パラメーターに"true"を指定してコマンドを実行します。

REST API : POST /v1/objects/storage/actions/set-metadata-drive-write-reduction-mode/
invoke

CLI : storage_metadata_drive_write_reduction_mode_set

コマンド実行後に表示されるジョブの ID を確認します。

3. ジョブの state を確認します。

ジョブの ID を指定してコマンドを実行します。

REST API : GET /v1/objects/jobs/<jobId >

CLI : job_show

state が"Succeeded"になっていたらジョブは完了です。

4. ホストからの I/O をすべて停止します。

5. ストレージクラスターを停止します。

「ストレージクラスターの停止」を参照して実施してください。

6. ストレージクラスターを起動します。

「ストレージクラスターの起動」を参照して実施してください。

7. メタデータのドライブ書き込み削減モード(metadataDriveWriteReductionMode)の状態が "Enabled"であることを確認します。

REST API : GET /v1/objects/storage

CLI : storage_show

45.3 メタデータのドライブ書き込み削減モードを無効にする

メタデータのドライブ書き込み削減モードを無効にする場合は、以下の手順を実施してください。



注意
メタデータのドライブ書き込み削減モードを無効にするには、手順 5 でのストレージクラスターの停止を実行する前に、ホストからの I/O をすべて停止させる必要があります。

前提条件

- 実行に必要なロール : Service
- ストレージクラスターの status が"Ready"であること
ストレージノード情報の一覧取得、および VSP One SDS Block Administrator の Health Status にて確認してください。

操作手順

1. メタデータのドライブ書き込み削減モードの状態を確認します。
- REST API : GET /v1/objects/storage
- CLI : storage_show
- メタデータのドライブ書き込み削減モードの状態(metadataDriveWriteReductionMode)によって以下の対応を行います。

メタデータのディスク書き込み削減モードの状態	対応方法
Enabled	次の手順に進みます。
Disabled	以上で手順は終了です。

メタデータのディスク書き込み削減モードの状態	対応方法
Enabling	「メタデータのドライブ書き込み削減モードを有効にする」の手順 4 以降を実施し、再度手順 1 から実行してください。
Disabling	手順 4 に進みます。

2. メタデータのドライブ書き込み削減モードを無効にします。
isEnabled パラメーターに"false"を、force パラメーターに"true"を指定してコマンドを実行します。
REST API : POST /v1/objects/storage/actions/set-metadata-drive-write-reduction-mode/
invoke
CLI : storage_metadata_drive_write_reduction_mode_set
コマンド実行後に表示されるジョブの ID を確認します。
3. ジョブの state を確認します。
ジョブの ID を指定してコマンドを実行します。
REST API : GET /v1/objects/jobs/<jobId >
CLI : job_show
state が"Succeeded"になっていたらジョブは完了です。
4. ホストからの I/O をすべて停止します。
5. ストレージクラスターを停止します。
「ストレージクラスターの停止」を参照して実施してください。
6. ストレージクラスターを起動します。
「ストレージクラスターの起動」を参照して実施してください。
7. メタデータのドライブ書き込み削減モード(metadataDriveWriteReductionMode)の状態が
"Disabled"であることを確認します。
REST API : GET /v1/objects/storage
CLI : storage_show

容量設計(HPEC 4D+1P の場合)≪Bare metal≫

この章での記述内容は Bare metal モデルに適用されます。

- A.1 容量設計の考え方(1):物理容量(HPEC 4D+1P の場合)≪Bare metal≫
- A.2 容量設計の考え方(2):論理容量(HPEC 4D+1P の場合)≪Bare metal≫
- A.3 容量設計方法(1)-1 物理容量から論理容量(HPEC 4D+1P の場合)≪Bare metal≫
- A.4 容量設計方法(2) 論理容量から物理容量(HPEC 4D+1P の場合)≪Bare metal≫

A.1 容量設計の考え方(1):物理容量(HPEC 4D+1P の場合)≪Bare metal≫

この節での記述内容は Bare metal モデルに適用されます。

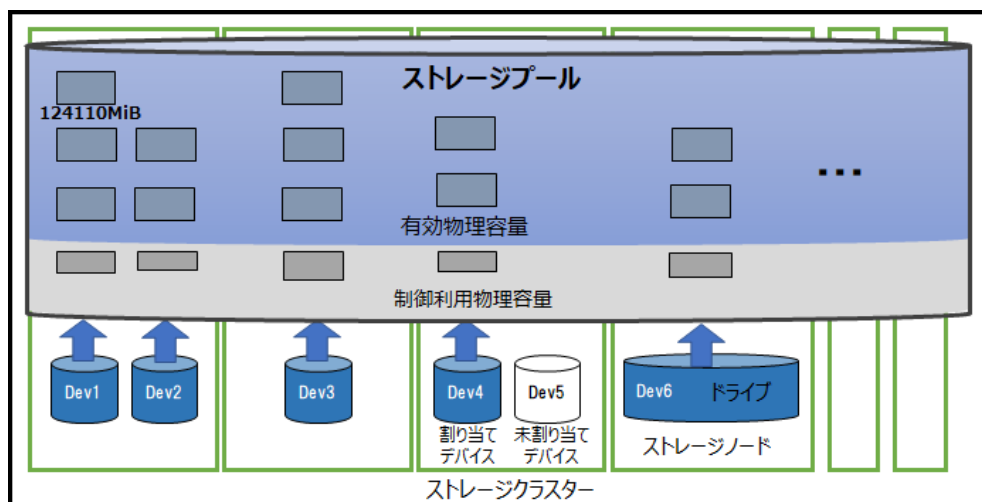
ドライブの物理容量は、有効物理容量と制御利用物理容量に分けられます。

- 有効物理容量[MiB](totalRawCapacity)：ドライブをストレージプールに追加して利用可能になった容量のことです。
- 制御利用物理容量[MiB](metaDataPhysicalCapacity)：ストレージプールに割り当てたドライブの総容量(総物理容量)における、制御情報用容量のことです。

HPEC 4D+1P の場合の、有効物理容量($C_{\text{rawDevice}}$)[MiB]は、以下の計算式から求められます。

なお、計算式は近似式であり、最大で 1GiB 程度の誤差が生じることがあります。

```
(CrawDevice)=floor((Cdevice×512/  
(512+8))-2048[MiB]-124110[MiB],124110[MiB])  
floor(数値,基準値)：基準値の倍数のうち、最も数値に近く数値を超えない値  
Cdevice：ドライブの物理容量[MiB]
```



A.2 容量設計の考え方(2):論理容量(HPEC 4D+1P の場合)≪Bare metal≫

この節での記述内容は Bare metal モデルに適用されます。

以下を前提として説明します。

- ストレージクラスター内のストレージノードおよびドライブの有効物理容量が均一であること
- 不良ストレージノードや不良ドライブがないこと
- 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

論理容量

論理容量[MiB](totalCapacity)は、ストレージプールのうち、ユーザーが利用可能な容量のことです。容量バランスによるストレージコントローラー間の偏り解消を行うために、論理容量[MiB](totalCapacity)は、使用予定の容量が 80%以下になるように余裕をもって構築してください。

論理容量[MiB](totalCapacity)は、以下の計算で求められます。

まず、論理化利用物理容量[MiB](usablePhysicalCapacity)を求めます。

ストレージノードの有効物理容量[MiB]から、構成変更用の予約容量(620550MiB)と、リビルド領域として確保される容量($C_{\text{rawDevice}} \times N_{\text{rebuild}}$)を除いたあとの容量のうち、620550MiB の倍数分の容量が論理化利用物理容量[MiB](usablePhysicalCapacity)になります。

論理化利用物理容量 [MiB/Node]=RoundDown (($C_{\text{rawNode}} - 620550 - C_{\text{rawDevice}} \times N_{\text{rebuild}}$) $\div$ 620550) $\times$ 620550

C_{rawNode} : 有効物理容量 [MiB/Node]

$C_{\text{rawDevice}}$: 有効物理容量 [MiB/Device]

N_{rebuild} : ストレージプールに設定された許容されるドライブ障害数
(リビルド領域ポリシー"Variable"の場合は 0 で計算する)

RoundDown (数値) : 数値を整数に切り捨て

論理化利用物理容量[MiB]の 620550MiB ごとの、496440MiB が論理容量になります。

また、ストレージコントローラーはそれぞれ 4200MiB の管理容量を必要とし、この管理容量は論理容量から除かれます。

論理容量 [MiB]= (($C_{\text{usableNode}} \div 620550$) $\times$ 496440) - 4200) $\times$ N_{node}

$C_{\text{usableNode}}$: 論理化利用物理容量 [MiB/Node]

N_{node} : ストレージノード数 [台/Cluster]

計算の結果、論理容量が 0 以下になった場合は、論理容量が構成されません。ただし、計算した論理容量が 0 以下かつ N_{rebuild} が 1(デフォルト値)のとき、 N_{rebuild} を 0 にして再計算することで論理容量が構築できる場合は、リビルド領域を残さずに論理容量を構築します。

ストレージコントローラーが管理できる容量には上限があり、以下を超える容量は論理容量として使用されません。

- ・ 論理化利用物理容量 : 125971650[MiB/Node]
- ・ 論理容量 : 100773120[MiB/Node]

物理予約容量

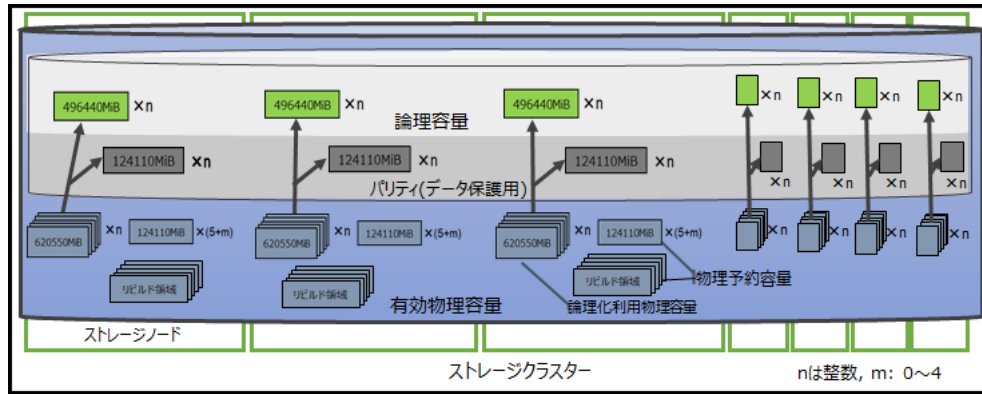
物理予約容量[MiB](reservedPhysicalCapacity)は、ストレージプールの有効物理容量のうち論理容量に利用しない容量のことです。物理予約容量は、以下の計算式から求められます。

物理予約容量 [MiB]= ($C_{\text{rawNode}} - C_{\text{usableNode}}$) $\times$ N_{node}

C_{rawNode} : 有効物理容量 [MiB/Node]

$C_{\text{usableNode}}$: 論理化利用物理容量 [MiB/Node]

N_{node} : ストレージノード数 [台/Cluster]



メモ

上図に記載の論理利用物理容量[MiB](usablePhysicalCapacity)とは、ストレージプールの有効物理容量のうち、論理容量に利用可能な容量のことです。

また、物理予約容量[MiB](reservedPhysicalCapacity)とは、ストレージプールの有効物理容量のうち、論理容量に利用しない容量のことです。

A.3 容量設計方法(1)-1 物理容量から論理容量(HPEC 4D+1P の場合)《Bare metal》

この節での記述内容は Bare metal モデルに適用されます。

以下を前提としています。

- ・ ストレージクラスター内のストレージノードおよびドライブの有効物理容量が均一であること
- ・ 不良ストレージノードや不良ドライブがないこと
- ・ 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

(例)ストレージノード 5 台構成、各ストレージノード 16TB(1.6TB のドライブ×10)、リビルド領域ポリシー"Fixed"・許容されるドライブ障害数 1

なお、計算式は近似式であり、最大で 1GiB 程度の誤差が生じることがあります。

操作手順

1. ドライブの単位を TiB に変換します。

$$1.6 \times (1000^4 \div 1024^4) = 1.4552 [\text{TiB}]$$

2. 「容量設計の考え方(1):物理容量(HPEC 4D+1P の場合)《Bare metal》」記載の式で、ドライブ(1.6TB)1 台当たりの有効物理容量を算出します。

$$\text{floor}((1.4552 \times 1024^2 \times 512 / (512 + 8)) - 2048 [\text{MiB}] - 124110 [\text{MiB}], 124110 [\text{MiB}]) = 1365210 [\text{MiB/Device}]$$

floor(数値, 基準値) : 数値を基準値に近い倍数に切り下げ

3. ストレージノード 1 台当たりの有効物理容量を算出します。

$$1365210 \times 10 = 13652100 [\text{MiB/Node}]$$

4. 「容量設計の考え方(2):論理容量(HPEC 4D+1P の場合)≪Bare metal≫」記載の式で、ストレージクラスターの論理化利用物理容量を算出します。

$\text{RoundDown}((13652100 - 620550 - 1365210) \div 620550) \times 620550 = 11169900 \text{ [MiB]}$
RoundDown(数値) : 数値を整数に切り捨て

5. 「容量設計の考え方(2):論理容量(HPEC 4D+1P の場合)≪Bare metal≫」記載の式で、ストレージクラスターの論理容量を算出します。

$(11169900 \div 620550 \times 496440 - 4200) \times 5 = 44658600 \text{ [MiB/Cluster]}$

A.4 容量設計方法(2) 論理容量から物理容量(HPEC 4D+1P の場合)≪Bare metal≫

この節での記述内容は Bare metal モデルに適用されます。

以下を前提としています。

- ・ ストレージクラスター内のストレージノードおよびドライブの有効物理容量が均一であること
- ・ 不良ストレージノードや不良ドライブがないこと
- ・ 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

(例)50TiB の論理容量をストレージノード 5 台(ドライブスロット 20 個)で確保するときのストレージノード 1 台当たりの必要物理容量を算出する、リビルド領域ポリシー"Fixed"・許容されるドライブ障害数 1

操作手順

1. 論理容量の増加単位は 496440MiB(「容量設計の考え方(2):論理容量(HPEC 4D+1P の場合)≪Bare metal≫」)のため、各ストレージノードに必要な有効物理容量は以下の式で算出します。

$\text{RoundUp}(((50 \times 1024^2) \div 5 + 4200) \times (620550 \div 496440)) + 620550 = 13733000 \text{ [MiB/Node]}$
RoundUp(数値) : 数値を整数に切り上げ

2. 使用するドライブの有効物理容量を算出します。

例えば、ドライブ(1.6TB)の有効物理容量は 1365210[MiB/Device]です。

ドライブ 1 台分の容量はリビルド領域として確保されるので、必要なドライブ数は次の式で算出します。

$\text{RoundUp}(13733000 \div 1365210) + 1 = 12 \text{ [台/Node]}$
RoundUp(数値) : 数値を整数に切り上げ

以上の計算から、1.6TB のドライブ 12 台を搭載したストレージノード 5 台のストレージクラスター構築によって、50TiB の論理容量を使用できることがわかります。

容量設計(HPEC 4D+2P の場合)

- B.1 容量設計の考え方(1):物理容量(HPEC 4D+2P の場合)
- B.2 容量設計の考え方(2):論理容量(HPEC 4D+2P の場合)
- B.3 容量設計方法(1)-1 物理容量から論理容量(HPEC 4D+2P の場合)
- B.4 容量設計方法(2) 論理容量から物理容量(HPEC 4D+2P の場合)

B.1 容量設計の考え方(1):物理容量(HPEC 4D+2P の場合)

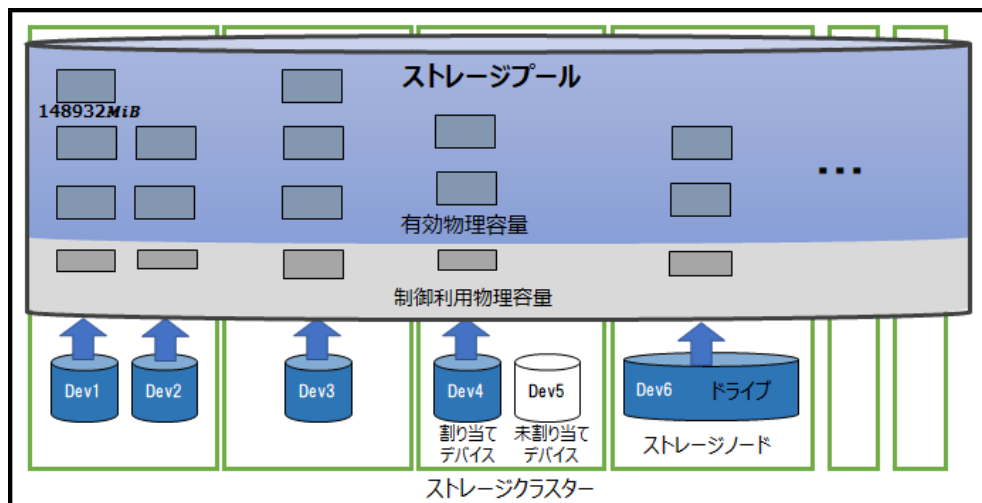
ドライブの物理容量は、有効物理容量と制御利用物理容量に分けられます。

- 有効物理容量[MiB](totalRawCapacity)：ドライブをストレージプールに追加して利用可能になった容量のことです。
- 制御利用物理容量[MiB](metaDataPhysicalCapacity)：ストレージプールに割り当てたドライブの総容量(総物理容量)における、制御情報用容量のことです。

HPEC 4D+2P の場合の、有効物理容量($C_{\text{rawDevice}}$ [MiB])は、以下の計算式から求められます。

なお、計算式は近似式であり、最大で 1GiB 程度の誤差が生じることがあります。

```
(CrawDevice)=floor((Cdevice×512/  
(512+8))-2048[MiB]-148932[MiB],148932[MiB])  
floor(数値,基準値)：基準値の倍数のうち、最も数値に近く数値を超えない値  
Cdevice：ドライブの物理容量[MiB]
```



B.2 容量設計の考え方(2):論理容量(HPEC 4D+2P の場合)

以下を前提として説明します。

- ストレージクラスター内のストレージノードおよびドライブの有効物理容量が均一であること
- 不良ストレージノードや不良ドライブがないこと
- 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

論理容量

論理容量[MiB](totalCapacity)は、ストレージプールのうちユーザーが利用可能な容量のことです。容量バランスによるストレージコントローラー間の偏り解消を行うために、論理容量[MiB](totalCapacity)は、使用予定の容量が 80%以下になるように余裕をもって構築してください。

論理容量[MiB](totalCapacity)は、以下の計算で求められます。

まず、論理化利用物理容量[MiB](usablePhysicalCapacity)を求めます。

各ストレージノードの有効物理容量[MiB]から、構成変更用の予約容量(893592MiB)と、リビルド領域として確保される容量($C_{\text{rawDevice}} \times N_{\text{rebuild}}$)を除き、残った容量から 893592MiB ごとの合計が、論理化利用物理容量[MiB](usablePhysicalCapacity)になります。

論理化利用物理容量 [MiB/Node] = $\text{RoundDown}((C_{\text{rawNode}} - 893592 - C_{\text{rawDevice}} \times N_{\text{rebuild}}) \div 893592) \times 893592$

C_{rawNode} : 有効物理容量 [MiB/Node]

$C_{\text{rawDevice}}$: 有効物理容量 [MiB/Device]

N_{rebuild} : ストレージプールに設定された許容されるドライブ障害数
(リビルド領域ポリシー "Variable" の場合は 0 で計算する)

RoundDown(数値) : 数値を整数に切り捨て

論理化利用物理容量[MiB]の 893592MiB ごとの、595728MiB が論理容量になります。

また、ストレージコントローラーはそれぞれ 4200MiB の管理容量を必要とし、この管理容量は論理容量から除かれます。

論理容量 [MiB] = $((C_{\text{usableNode}} \div 893592) \times 595728) - 4200) \times N_{\text{node}}$

$C_{\text{usableNode}}$: 論理化利用物理容量 [MiB/Node]

N_{node} : ストレージノード数 [台/Cluster]

計算の結果、論理容量が 0 以下になった場合は、論理容量が構成されません。ただし、計算した論理容量が 0 以下かつ N_{rebuild} が 1(デフォルト値)のとき、 N_{rebuild} を 0 にして再計算することで論理容量が構築できる場合は、リビルド領域を残さずに論理容量を構築します。

ストレージコントローラーが管理できる容量には上限があり、以下を超える容量は論理容量として使用されません。

- ・ 論理化利用物理容量 : 151017048[MiB/Node]
- ・ 論理容量 : 100673832[MiB/Node]

物理予約容量

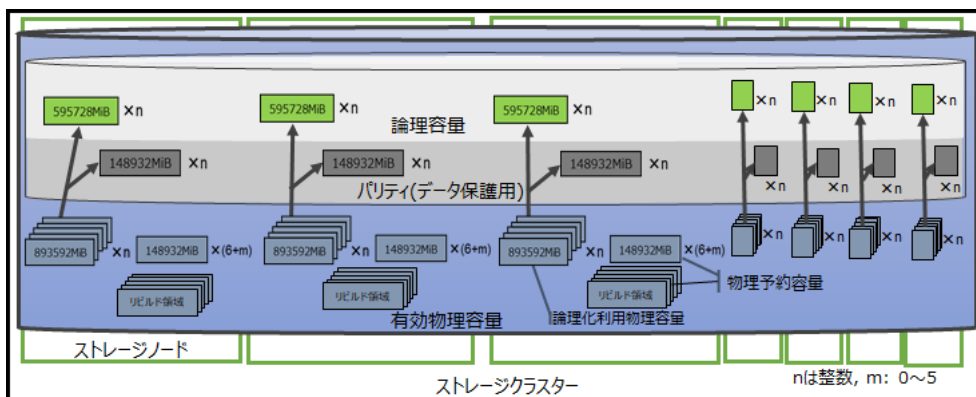
物理予約容量[MiB](reservedPhysicalCapacity)は、ストレージプールの有効物理容量のうち論理容量に利用しない容量のことです。物理予約容量は、以下の計算式から求められます。

物理予約容量 [MiB] = $(C_{\text{rawNode}} - C_{\text{usableNode}}) \times N_{\text{node}}$

C_{rawNode} : 有効物理容量 [MiB/Node]

$C_{\text{usableNode}}$: 論理化利用物理容量 [MiB/Node]

N_{node} : ストレージノード数 [台/Cluster]





ヒント

上図に記載の論理化利用物理容量[MiB](usablePhysicalCapacity)とは、ストレージプールの有効物理容量のうち、論理容量に利用可能な容量のことです。

また、物理予約容量[MiB](reservedPhysicalCapacity)とは、ストレージプールの有効物理容量のうち、論理容量に利用しない容量のことです。

B.3 容量設計方法(1)-1 物理容量から論理容量(HPEC 4D+2P の場合)

以下を前提としています。

- ・ ストレージクラスター内のストレージノードおよびドライブの有効物理容量が均一であること
- ・ 不良ストレージノードや不良ドライブがないこと
- ・ 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

(例)ストレージノード 6 台構成、各ストレージノード 16TB(1.6TB のドライブ×10)、リビルド領域ポリシー"Fixed"・許容されるドライブ障害数 1

なお、計算式は近似式であり、最大で 1GiB 程度の誤差が生じることがあります。

操作手順

1. ドライブの単位を TiB に変換します。

$$1.6 \times (1000^4 \div 1024^4) = 1.4552 [\text{TiB}]$$

2. 「容量設計の考え方(1):物理容量(HPEC 4D+2P の場合)」記載の式で、ドライブ(1.6TB)1 台当たりの有効物理容量を算出します。

$$\text{floor}((1.4552 \times 1024^2 \times 512 / (512 + 8)) - 2048 [\text{MiB}] - 148932 [\text{MiB}], 148932 [\text{MiB}]) = 1340388 [\text{MiB/Device}]$$

floor(数値, 基準値) : 数値を基準値に近い倍数に切り下げ

3. ストレージノード 1 台当たりの有効物理容量を算出します。

$$1340388 \times 10 = 13403880 [\text{MiB/Node}]$$

4. 「容量設計の考え方(2):論理容量(HPEC 4D+2P の場合)」記載の式で、ストレージクラスターの論理化利用容量を算出します。

$$\text{RoundDown}((13403880 - 893592 - 1340388) \div 893592) \times 893592 = 10723104 [\text{MiB}]$$

RoundDown(数値) : 数値を整数に切り捨て

5. 「容量設計の考え方(2):論理容量(HPEC 4D+2P の場合)」記載の式で、ストレージクラスターの論理容量を算出します。

$$(10723104 \div 893592 \times 595728 - 4200) \times 6 = 42867216 [\text{MiB/Cluster}]$$

B.4 容量設計方法(2) 論理容量から物理容量(HPEC 4D+2P の場合)

以下を前提としています。

- ・ ストレージクラスター内のストレージノードおよびドライブの有効物理容量が均一であること
- ・ 不良ストレージノードや不良ドライブがないこと
- ・ 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

(例)50TiB の論理容量をストレージノード 6 台(ドライブスロット 20 個)で確保するときのストレージノード 1 台当たりの必要物理容量を算出する、リビルド領域ポリシー"Fixed"・許容されるドライブ障害数 1

操作手順

1. 論理容量の増加単位は 595728MiB(「容量設計の考え方(2):論理容量(HPEC 4D+2P の場合)」)のため、各ストレージノードで必要な有効物理容量は以下の式で算出します。

$$\text{RoundUp}((50 \times 1024^2) \div 6 + 4200) \times (893592 \div 595728) + 893592 = 14007092 \text{ [MiB/Node]}$$

RoundUp(数値) : 数値を整数に切り上げ

2. 使用するドライブの有効物理容量を算出します。

例えば、ドライブ(1.6TB)の有効物理容量は 1340388[MiB/Device]です。

ドライブ 1 台分の容量はリビルド領域として確保されるので、必要なドライブ数は次の式で算出します。

$$\text{RoundUp}(14007092 \div 1340388) + 1 = 12 \text{ [台/Node]}$$

RoundUp(数値) : 数値を整数に切り上げ

以上の計算から、1.6TB のドライブ 12 台を搭載したストレージノード 6 台のストレージクラスター構築によって、50TiB の論理容量を使用できることがわかります。



容量設計(Mirroring の場合)

- C.1 容量設計の考え方(1):物理容量(Mirroring の場合)
- C.2 容量設計の考え方(2):論理容量(Mirroring の場合)
- C.3 容量設計方法(1)-1 物理容量から論理容量(Mirroring の場合)
- C.4 容量設計方法(2) 論理容量から物理容量(Mirroring の場合)

C.1 容量設計の考え方(1):物理容量(Mirroring の場合)

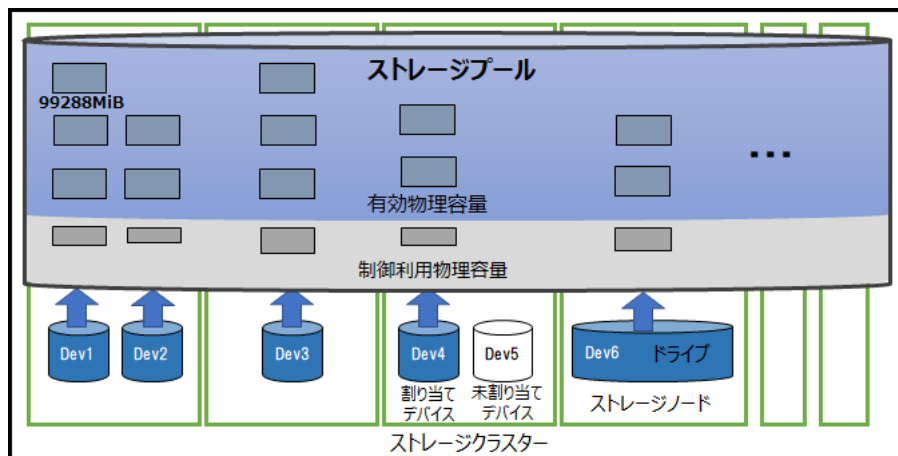
ドライブの物理容量は、有効物理容量と制御利用物理容量に分けられます。

- 有効物理容量[MiB](totalRawCapacity)：ドライブをストレージプールに追加して利用可能になった容量のことです。
- 制御利用物理容量[MiB](metaDataPhysicalCapacity)：ストレージプールに割り当てたドライブの総容量(総物理容量)における、制御情報用容量のことです。

Mirroring の場合の、有効物理容量($C_{\text{rawDevice}}$ [MiB])は、以下の計算式から求められます。

なお、計算式は近似式であり、最大で 1GiB 程度の誤差が生じることがあります。

```
( $C_{\text{rawDevice}}$  [MiB]) = floor ( ( $C_{\text{device}} \times 512 /$   
( $512 + 8$ ) ) -  $3072$  [MiB] -  $99288$  [MiB],  $99288$  [MiB] )  
floor (数値, 基準値) : 基準値の倍数のうち、最も数値に近く数値を超えない値  
 $C_{\text{device}}$  : ドライブの物理容量 [MiB]
```



C.2 容量設計の考え方(2):論理容量(Mirroring の場合)

以下を前提として説明します。

- ストレージクラスター内のストレージノードおよびドライブの有効物理容量が均一であること
- 不良ストレージノードや不良ドライブがないこと
- 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

論理容量

論理容量[MiB](totalCapacity)は、ストレージプールのうちユーザーが利用可能な容量のことです。容量バランスによるストレージコントローラー間の偏り解消を行うために、論理容量[MiB](totalCapacity)は、使用予定の容量が 80%以下になるように余裕をもって構築してください。

論理容量[MiB](totalCapacity)は、以下の計算で求められます。

まず、論理化利用物理容量[MiB](usablePhysicalCapacity)を求めます。

各ストレージノードの有効物理容量[MiB]から、構成変更用の予約容量(198576MiB)と、リビルド領域として確保される容量($C_{\text{rawDevice}} \times N_{\text{rebuild}}$)を除き、残った容量から 198576MiB ごとの合計が、論理化利用物理容量[MiB](usablePhysicalCapacity)になります。

論理化利用物理容量[MiB] = $\text{RoundDown}((C_{\text{rawNode}} - 198576 - C_{\text{rawDevice}} \times N_{\text{rebuild}}) \div 198576) \times 198576$
 C_{rawNode} : 有効物理容量[MiB/Node]
 $C_{\text{rawDevice}}$: 有効物理容量[MiB/Device]
 N_{rebuild} : ストレージプールに設定された許容されるドライブ障害数
 (リビルド領域ポリシー"Variable"の場合は 0 で計算する)
 RoundDown(数値) : 数値を整数に切り捨て

論理化利用物理容量[MiB]の 198576MiB ごとの、99288MiB が論理容量になります。

また、ストレージコントローラーはそれぞれ 4200MiB の管理容量を必要とし、この管理容量は論理容量から除かれます。

論理容量[MiB] = $((C_{\text{usableNode}} \div 198576) \times 99288) - 4200) \times N_{\text{node}}$
 $C_{\text{usableNode}}$: 論理化利用物理容量[MiB/Node]
 N_{node} : ストレージノード数[台/Cluster]

計算の結果、論理容量が 0 以下になった場合は、論理容量が構成されません。ただし、計算した論理容量が 0 以下かつ N_{rebuild} が 1(デフォルト値)のとき、 N_{rebuild} を 0 にして再計算することで論理容量が構築できる場合は、リビルド領域を残さずに論理容量を構築します。

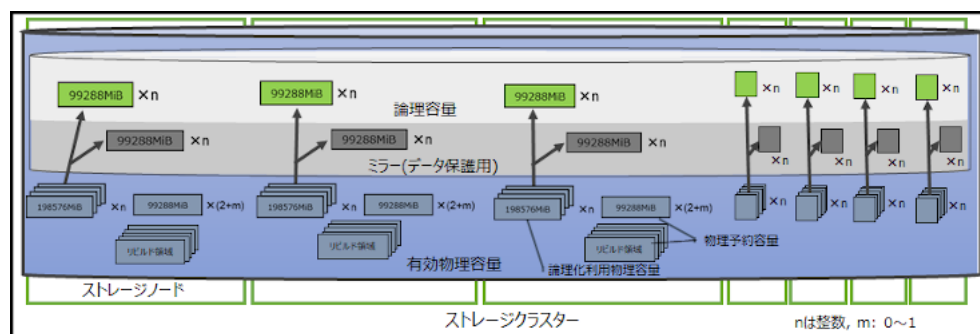
ストレージコントローラーが管理できる容量には上限があり、以下を超える容量は論理容量として使用されません。

- ・ 論理化利用物理容量 : 203143248[MiB/Node]
- ・ 論理容量 : 101567424[MiB/Node]

物理予約容量

物理予約容量[MiB](reservedPhysicalCapacity)は、ストレージプールの有効物理容量のうち論理容量に利用しない容量のことです。物理予約容量は、以下の計算式から求められます。

物理予約容量[MiB] = $(C_{\text{rawNode}} - C_{\text{usableNode}}) \times N_{\text{node}}$
 C_{rawNode} : 有効物理容量[MiB/Node]
 $C_{\text{usableNode}}$: 論理化利用物理容量[MiB/Node]
 N_{node} : ストレージノード数[台/Cluster]



ヒント

上図に記載の論理化利用物理容量[MiB](usablePhysicalCapacity)とは、ストレージプールの有効物理容量のうち、論理容量に利用可能な容量のことです。

C.3 容量設計方法(1)-1 物理容量から論理容量(Mirroring の場合)

以下を前提としています。

- ・ ストレージクラスター内のストレージノードおよびドライブの有効物理容量が均一であること
- ・ 不良ストレージノードや不良ドライブがないこと
- ・ 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

(例)ストレージノード 6 台構成、各ストレージノード 16TB(1.6TB のドライブ×10)、リビルド領域ポリシー"Fixed"・許容されるドライブ障害数 1

なお、計算式は近似式であり、最大で 1GiB 程度の誤差が生じることがあります。

操作手順

1. ドライブの単位を TiB に変換します。

$$1.6 \times (1000^4 \div 1024^4) = 1.4552 \text{ [TiB]}$$

2. 「容量設計の考え方(1):物理容量(Mirroring の場合)」記載の式で、ドライブ(1.6TB)1 台当たりの有効物理容量を算出します。

$$\text{floor}((1.4552 \times 1024^2 \times 512 / (512 + 8)) - 3072 \text{ [MiB]} - 99288 \text{ [MiB]}, 99288 \text{ [MiB]}) = 1390032 \text{ [MiB/Device]}$$

floor(数値, 基準値) : 数値を基準値に近い倍数に切り下げ

3. ストレージノード 1 台当たりの有効物理容量を算出します。

$$1390032 \times 10 = 13900320 \text{ [MiB/Node]}$$

4. 「容量設計の考え方(2):論理容量(Mirroring の場合)」記載の式で、ストレージクラスターの論理化利用物理容量を算出します。

$$\text{RoundDown}((13900320 - 198576 - 1390032) \div 198576) \times 198576 = 12311712 \text{ [MiB]}$$

RoundDown(数値) : 数値を整数に切り捨て

5. 「容量設計の考え方(2):論理容量(Mirroring の場合)」記載の式で、ストレージクラスターの論理容量を算出します。

$$(12311712 \div 198576 \times 99288 - 4200) \times 6 = 36909936 \text{ [MiB/Cluster]}$$

C.4 容量設計方法(2) 論理容量から物理容量(Mirroring の場合)

以下を前提としています。

- ・ ストレージクラスター内のストレージノードおよびドライブの有効物理容量が均一であること
- ・ 不良ストレージノードや不良ドライブがないこと
- ・ 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

(例)50TiB の論理容量をストレージノード 6 台(ドライブスロット 20 個)で確保するときのストレージノード 1 台当たりの必要物理容量を算出する、リビルド領域ポリシー"Fixed"・許容されるドライブ障害数 1

操作手順

1. 論理容量の増加単位は 99288MiB(「容量設計の考え方(2):論理容量(Mirroring の場合)」)のため、各ストレージノードに必要な有効物理容量は以下の式で算出します。

```
RoundUp(((50×10242)÷6 + 4200) × (198576÷99288)) + 198576=17683243 [MiB/Node]
```

RoundUp(数値) : 数値を整数に切り上げ

2. 使用するドライブの有効物理容量を算出します。

例えば、ドライブ(1.6TB)の有効物理容量は 1340388[MiB/Device]です。

ドライブ 1 台分の容量はリビルド領域として確保されるので、必要なドライブ数は次の式で算出します。

```
RoundUp(17683243÷1340388) + 1=15 [台/Node]
```

RoundUp(数値) : 数値を整数に切り上げ

以上の計算から、1.6TB のドライブ 15 台を搭載したストレージノード 6 台のストレージクラスター構築によって、50TiB の論理容量を使用できることがわかります。



増設時の容量設計

- D.1 容量増設の方法
- D.2 ストレージノード増設時の容量設計(HPEC 4D+1P の場合)≪Bare metal≫
- D.3 ドライブ増設時の容量設計(HPEC 4D+1P の場合)≪Bare metal≫
- D.4 ストレージノード増設時の容量設計(HPEC 4D+2P の場合)
- D.5 ドライブ増設時の容量設計(HPEC 4D+2P の場合)
- D.6 ストレージノード増設時の容量設計(Mirroring の場合)
- D.7 ドライブ増設時の容量設計(Mirroring の場合)

D.1 容量増設の方法

VSP One SDS Block に容量を追加するには以下の 2 つの方法があります。

ストレージノード増設

ストレージノードを増設して、その増設したストレージノードの容量を追加します。

- ・ メリット：増設したストレージノード分の処理性能の向上が見込める(ただし、I/O 特性による)
- ・ デメリット：新規ストレージノード分のコストが掛かる(価格、設置場所、導入費など)
- ・ デメリット：≪Bare metal≫フォールトドメインが 1 つの場合、ドライブデータ再配置が動作するため、増設した容量が使えるようになるまで時間が掛かる

ドライブ増設

各ストレージノードにドライブを増設して、その分だけ容量を追加します。

- ・ メリット：ドライブ増設に掛かるコストだけが必要なので、ストレージノード増設に比べてコストが抑えられる
- ・ デメリット：各ストレージノードのドライブ搭載数の上限までしか増設できない

D.2 ストレージノード増設時の容量設計(HPEC 4D+1P の場合) ≪Bare metal≫

この節での記述内容は Bare metal モデルに適用されます。

HPEC 4D+1P の場合の、ストレージノード増設時の容量設計について説明します。

以下を前提としています。

- ・ 増設ストレージノードの有効物理容量が増設前の構成のストレージノードと均一であること
- ・ 不良ストレージノードや不良ドライブがないこと
- ・ 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

操作手順

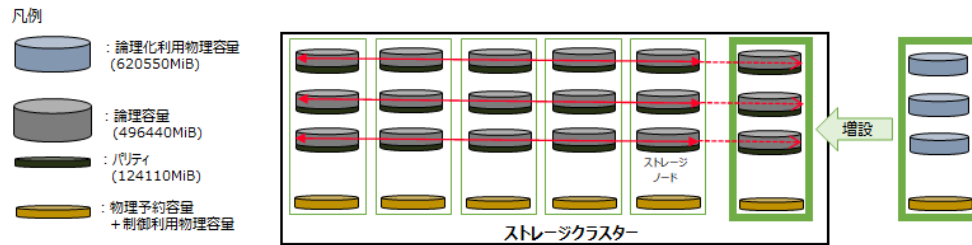
1. 前提の条件下では、増設ストレージノードによる増加論理容量は、増設前の構成のストレージノードの論理容量と同じになるので、総論理容量は下記の式で算出できます。

増設後総論理容量 = $C \times (N + A) \div N$

C：増設前総論理容量

N：増設前ストレージノード数

A：増設ストレージノード数 (1 台から増設可能)



D.3 ドライブ増設時の容量設計(HPEC 4D+1P の場合)≪Bare metal≫

この節での記述内容は Bare metal モデルに適用されます。

HPEC 4D+1P の場合の、ドライブ増設時の容量設計について説明します。

以下を前提としています。

- 増設ドライブの有効物理容量が均一であり、全ストレージノードへの増設であること
- 不良ストレージノードや不良ドライブがないこと
- 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

操作手順

- 「容量設計の考え方(1):物理容量(HPEC 4D+1P の場合)≪Bare metal≫」記載の式で、増設ドライブの有効物理容量を算出します。
- 増設ドライブによる増加論理容量は、次の式で算出できます。

増設後総論理容量 [MiB] = $C + \text{RoundDown}((R + A - 620550 - C_{\text{rawDevice}} \times N_{\text{rebuild}}) \div 620550) \times N \times 496440$

C : 増設前総論理容量

RoundDown (数値) : 数値を整数に切り捨て

R : 増設前各ノードの物理予約容量

A : 増設ドライブの有効物理容量

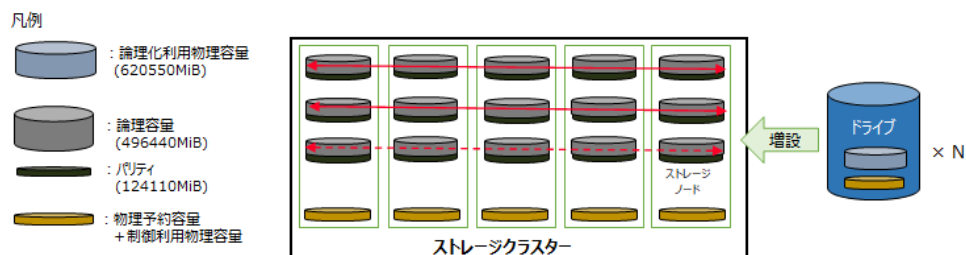
N : ストレージノード数

$C_{\text{rawDevice}}$: 有効物理容量 [MiB/Device]

N_{rebuild} : ストレージプールに設定された許容されるドライブ障害数
(リビルド領域ポリシー "Variable" の場合は 0 で計算する)

なお、ストレージコントローラーが管理できる容量には上限があり、以下を超える容量は論理容量として使用されません。

100773120 × ストレージノード数 [MiB]



D.4 ストレージノード増設時の容量設計(HPEC 4D+2P の場合)

HPEC 4D+2P の場合の、ストレージノード増設時の容量設計について説明します。

以下を前提としています。

- ・ 増設ストレージノードの有効物理容量が増設前の構成のストレージノードと均一であること
- ・ 不良ストレージノードや不良ドライブがないこと
- ・ 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

操作手順

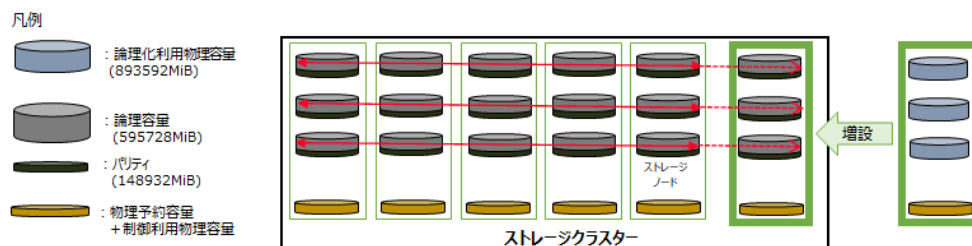
1. 前提の条件下では、増設ストレージノードによる増加論理容量は、増設前の構成のストレージノードの論理容量と同じになるので、総論理容量は下記の式で算出できます。

増設後総論理容量 = $C \times (N + A) \div N$

C : 増設前総論理容量

N : 増設前ストレージノード数

A : 増設ストレージノード数 (1 台から増設可能)



D.5 ドライブ増設時の容量設計(HPEC 4D+2P の場合)

HPEC 4D+2P の場合の、ドライブ増設時の容量設計について説明します。

以下を前提としています。

- ・ 増設ドライブの有効物理容量が均一であり、全ストレージノードへの増設であること
- ・ 不良ストレージノードや不良ドライブがないこと
- ・ 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

操作手順

1. 「容量設計の考え方(1):物理容量(HPEC 4D+2P の場合)」記載の式で、増設ドライブの有効物理容量を算出します。
2. 前提の条件下では、増設ドライブによる増加論理容量は、次の式で算出できます。

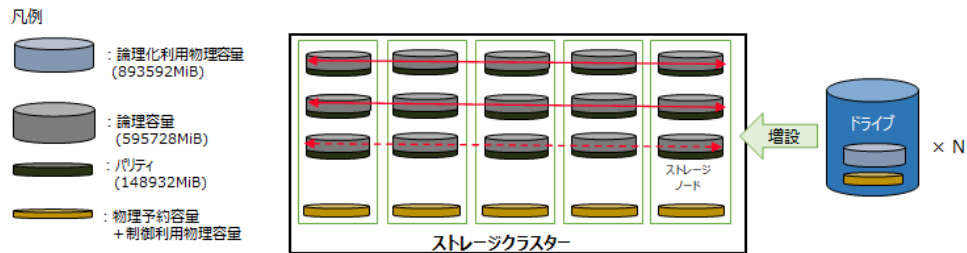
増設後総論理容量 [MiB] = $C + \text{RoundDown}((R + A - 893592 - C_{\text{rawDevice}} \times N_{\text{rebuild}}) \div 893592) \times N \times 595728$

C : 増設前総論理容量

RoundDown (数値) : 数値を整数に切り捨て
R : 増設前各ノードの物理予約容量
A : 増設ドライブの有効物理容量
N : ストレージノード数
C_{rawDevice} : 有効物理容量 [MiB/Device]
N_{rebuild} : ストレージプールに設定された許容されるドライブ障害数
(リビルド領域ポリシー "Variable" の場合は 0 で計算する)

なお、ストレージコントローラーが管理できる容量には上限があり、以下を超える容量は論理容量として使用されません。

100673832 × ストレージノード数 [MiB]



D.6 ストレージノード増設時の容量設計(Mirroring の場合)

Mirroring の場合の、ストレージノード増設時の容量設計について説明します。

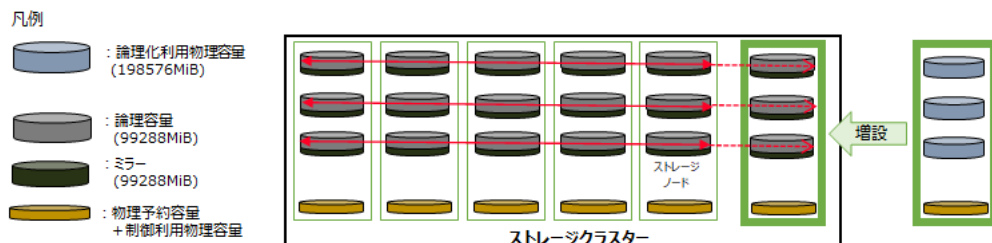
以下を前提としています。

- 増設ストレージノードの有効物理容量が増設前の構成のストレージノードと均一であること
- 不良ストレージノードや不良ドライブがないこと
- 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

操作手順

- 前提の条件下では、増設ストレージノードによる増加論理容量は、増設前の構成のストレージノードの論理容量と同じになるので、総論理容量は下記の式で算出できます。

増設後総論理容量 = $C \times ((N+A) \div N)$
C : 増設前総論理容量
N : 増設前ストレージノード数
A : 増設ストレージノード数 (1 台から増設可能)



D.7 ドライブ増設時の容量設計(Mirroring の場合)

Mirroring の場合の、ドライブ増設時の容量設計について説明します。

以下を前提としています。

- 増設ドライブの有効物理容量が均一であり、全ストレージノードへの増設であること
- 不良ストレージノードや不良ドライブがないこと
- 構成や各ストレージノードの容量およびドライブ数がシステム要件を満たしていること
ストレージノードの要件については、ご使用のモデルの「Hitachi Virtual Storage Platform One SDS Block セットアップガイド」の「ストレージノードの要件」を参照してください。

操作手順

- 「容量設計の考え方(1):物理容量(Mirroring の場合)」記載の式で、増設ドライブの有効物理容量を算出します。
- 前提の条件下では、増設ドライブによる増加論理容量は、次の式で算出できます。

増設後総論理容量 [MiB] = $C + \text{RoundDown}((R + A - 198576 - C_{\text{rawDevice}} \times N_{\text{rebuild}}) \div 198576) \times N \times 99288$

C : 増設前総論理容量

RoundDown(数値) : 数値を整数に切り捨て

R : 増設前各ノードの物理予約容量

A : 増設ドライブの有効物理容量

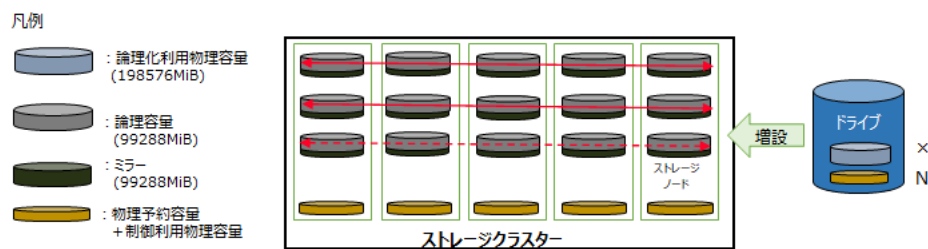
N : ストレージノード数

$C_{\text{rawDevice}}$: 有効物理容量 [MiB/Device]

N_{rebuild} : ストレージプールに設定された許容されるドライブ障害数
(リビルド領域ポリシー "Variable" の場合は 0 で計算する)

なお、ストレージコントローラーが管理できる容量には上限があり、以下を超える容量は論理容量として使用されません。

$1001567424 \times \text{ストレージノード数}$ [MiB]





ALUA 構築ガイドライン

- E.1 必要な事前設定
- E.2 ALUA の設定手順

E.1 必要な事前設定

E.1.1 VMware ESXi

共通設定

VMware ESXi6.X(5.X も含む)の場合、下記の Update と KB を適用してください。

- VMware ESXi5.5 Update3 and KB2146717
- VMware ESXi6.0 Update2 and KB2145663

なお、SCSI Timeout 設定値は、デフォルト 140 秒であり、コンピュータノードの要件の 120 秒以上であるため変更は不要です。

交替パスソフトの設定

追加設定は必要ありません。

ゲスト間クラスターの場合の設定

ゲスト間クラスター(MSCS など)でリザーブ(SCSI-2,SCSI-3)を使用しているデバイスは、以下の KB を参考にして各 VMware ESXi から `perennially-reserved` を `TRUE` にしてください。ストレージの構成によらず設定してください。

- ESXi host takes a long time to start during rescan of RDM LUNs
<https://knowledge.broadcom.com/external/article/318851>

E.1.2 Microsoft Windows

共通設定

このマニュアルの「コンピュータノードの設置」を参照し、SCSI Timeout 設定値を変更してください。

交替パスソフトの設定(MPIO の場合)

レジストリーの設定を変更する必要があります。以下の Web サイトを参照し、レジストリーの値を設定してください。

[http://technet.microsoft.com/en-us/library/ee619749\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee619749(v=ws.10).aspx)

- PathVerifyEnabled を 1 に設定する
- UseCustomPathRecoveryInterval を 1 に設定する
- PathRecoveryInterval(デフォルト 40)を PDORemovePeriod(デフォルト 20)よりも小さい値に設定する

レジストリーを編集する際は、以下の Web サイトを参照し、慎重に編集してください。

<http://support.microsoft.com/kb/136393>

クラスターの場合の設定

追加設定は必要ありません。

E.1.3 Linux

このマニュアルの「コンピュータノードの設置」を参照し、SCSI Timeout 設定値およびマルチパス設定を変更してください。

E.2 ALUA の設定手順

E.2.1 VMware ESXi(NMP の場合)

ストレージ側で指定される ALUA 有効/無効の設定を、コンピュータノード側に認識させる手順です。

ストレージ側で設定した ALUA 優先度の変更を、コンピュータノード側に認識させる手順は特にありません。自動で認識されます。

操作手順

1. 専用の SATP が未作成であることを確認します。

次のコマンドで何も出力されない場合、SATP が未作成であると判断できます。作成済みの場合、以降の手順は実施不要です。

```
# esxcli storage nmp satp rule list | grep Hi-SDS
```

2. 専用の SATP を作成します。

```
# esxcli storage nmp satp rule add -V HITACHI -M "^Hi-SDS*" -s VMW_SATP_ALUA -c tpgs_on --psp="VMW_PSP_RR"
```

3. 設定を認識させるためにコンピュータノードをリブートします。

E.2.2 Microsoft Windows(MPIO の場合)

ストレージ側で指定される ALUA 有効/無効の設定を、コンピュータノード側に認識させるための特別な手順はありません。

ストレージ側で設定した ALUA 優先度の変更を、コンピュータノード側に認識させるには、デバイスマネージャーからハードウェアの変更のスキャンを実行します。以下のコマンドで確認されます。

```
# mpclaim -s -d XXX
```

このとき、優先パスと非優先パスは以下の形式で表示されます。

優先パスの表示 : Active/Optimized

非優先パスの表示 : Active/Unoptimized

E.2.3 Linux 系(Device Mapper の場合)

ストレージ側で指定される ALUA 有効/無効の設定を、コンピュータノード側に認識させるには、以下の手順を実行します。

操作手順

1. /etc/multipath.conf の以下の項目について、設定値を変更します。

項目	設定値
vendor	"HITACHI"
product	"Hi-SDS*"
path_grouping_policy	group_by_prio
prio	alua
detect_path_checker/ detect_checker ¹	no
path_checker ²	readsector0
dev_loss_tmo	お使いのディストリビューションのマニュアルを参照し、最大値を設定してください。

1. お使いのディストリビューションによってパラメーター名が異なります。お使いのディストリビューションのマニュアルを参照し、適切なパラメーター名を設定してください。

2. VSP One SDS Block でストレージノード障害が発生した場合、readsector0 以外の値が設定されているとパスが誤閉塞する可能性があります。そのため、必ず readsector0 を設定してください。

2. 交替パスデーモンのリロードを行います。

```
# service multipathd reload
```

ストレージ側で設定した ALUA 優先度の変更を、コンピュータノード側に認識させる手順はありません。自動で認識されます。

ストレージ側で設定した ALUA の優先度は、以下のコマンドで確認できます。

```
# multipath -ll
```

このとき、優先パスと非優先パスは以下の形式で表示されます。

優先パスの表示 : prio=50 status=active

非優先パスの表示 : prio=10 status=enable

VSP One SDS Block では、ALUA と非 ALUA のデバイスが混在する構成はサポートしていません。



ANA 構築ガイドライン

- F.1 必要な事前設定
- F.2 ANA の設定手順

F.1 必要な事前設定

F.1.1 VMware ESXi

共通設定

VMware ESXi7.0 Update 3c 以降のバージョンである必要があります。

NVMe Timeout 設定値は、デフォルト 140 秒であり、コンピュータノードの要件の 120 秒以上であるため変更は不要です。

交替パスソフトの設定

追加設定は必要ありません。

ゲスト間クラスターの場合の設定

追加設定は必要ありません。

F.1.2 Linux

このマニュアルの「コンピュータノードを設置する<<Bare metal>>」を参照し、NVMe Timeout 設定値およびマルチパス設定を変更してください。

F.2 ANA の設定手順

F.2.1 VMware ESXi(HPP の場合)

ストレージ側で指定される ANA 有効/無効の設定を、コンピュータノード側に認識させる手順です。

ストレージ側で設定した ANA 優先度の変更を、コンピュータノード側に認識させる手順は特にありません。自動で認識されます。

操作手順

1. 専用の claimrule が未作成であることを確認します。

次のコマンドで何も出力されない場合、claimrule が未作成であると判断できます。作成済みの場合、以降の手順は実施不要です。

```
# esxcli storage core claimrule list | grep "HITACHI SDS-System"
```

2. 専用の claimrule を作成します。

```
# esxcli storage core claimrule add -u -t vendor --nvme-controller-model "HITACHI SDS-System" -P HPP -g "pss=LB-RR"
```

3. 設定を認識させるためにコンピュータノードをリブートします。

F.2.2 Linux 系(Native NVMe Multipath の場合)

ストレージ側で指定される ANA 有効/無効の設定を、コンピュータノード側に認識させる手順です。

ストレージ側で設定した ANA 優先度の変更を、コンピュータノード側に認識させる手順は特にありません。自動で認識されます。

操作手順

1. Native NVMe Multipath を有効にします。
お使いのディストリビューションのマニュアルを参照し、有効にしてください。
2. Native NVMe Multipath の以下の項目について、設定値を変更します。
お使いのディストリビューションのマニュアルを参照し、変更してください。

項目	設定値
iopolicy	round-robin
ctrl_loss_tmo	-1

3. ストレージ側で設定した ANA の優先度は、以下のコマンドで確認できます。

```
# nvme list-subsys /dev/<デバイス名>
```

このとき、優先パスと非優先パスは以下の形式で表示されます。

- 優先パスの表示：optimized
- 非優先パスの表示：non-optimized

VSP One SDS Block では、ANA と非 ANA のデバイスが混在する構成はサポートしていません。



スナップショット操作の処理時間<<Bare metal>>

この章での記述内容は Bare metal モデルに適用されます。

□ G.1 スナップショット操作の処理時間(目安)<<Bare metal>>

G.1 スナップショット操作の処理時間(目安)≪Bare metal≫

この節での記述内容は Bare metal モデルに適用されます。

I/O なし、他の操作を実施していない条件下で、スナップショットの 1 回の操作をした場合の目安 (単位：秒)になります。下表を参考に処理時間を見積もってください。

- リストアと削除の処理時間は、ボリュームの totalCapacity[MiB]と snapshotConcordanceRate[%]に依存して変わります。
- PrepareAndFinalize と Prepare の処理時間は、S-VOL の作成時間を含みます。
- リストア対象世代と、リストアの複写元と複写先の差分状況によっては、下表に記載したリストア時間の約 2 倍掛かることがあります。最新世代以外からのリストア、または S-VOL 書き込みありの世代からのリストアでは、処理時間を 2 倍で見積もってください。
- リストアにおけるコピー処理の負荷によって I/O に与える影響が高い場合、ストレージコントローラーによってコピー処理が停止されることがあります。過負荷状態でないにもかかわらず、コピー処理が停滞する場合は、該当ストレージノードに対してダンプログファイルを採取し、サポートセンターに連絡してください。
- リストアにおいて、一致率やコピー処理の抑止によってリストア時間が長時間化することを考慮し、同時に実行を指示できる数を 500 までとする上限をシステムに設けています。500 を超えてリストア操作を指示した場合は、KARS06143-E によって通知するとともにリストア操作は失敗します。

totalCapacity[GiB]	snapshotConcordanceRate[%]	取得準備 &取得 (Prepare AndFinalize)[sec]	取得準備 (Prepare) [sec]	取得 (Finalize) [sec]	リストア[sec]		削除[sec]
					容量削減 機能無効	容量削減 機能有効	
51200	100	36	38	0	9727	10778	1350
16384	100	14	13	0	3723	3572	573
4096	100	8	8	0	961	903	162
1024	100	7	6	0	241	229	54
256	100	6	6	0	61	64	29
128	100	8	6	0	60	34	22
128	75	-	-	-	2583	1431	44
128	50	-	-	-	5045	2911	74
128	0	-	-	-	9729	6214	101
-：発生しない組み合わせ							

REST API では masterVolumeId と snapshotTree、CLI では --master_volume_id と --snapshot_tree に、それぞれ P-VOL のボリュームの ID と true を指定してスナップショットの削除コマンドを実行した場合は、P-VOL から作成されたすべてのスナップショットボリューム(S-VOL または P/S-VOL)を一度に削除します。

削除時間の目安は、以下の計算式で算出できます。

スナップショットボリューム数¹ × 単位ボリューム削除時間[sec] + スナップショット構成削除時間[sec] + 600[sec]²

1. 指定した P-VOL から作成されたすべての S-VOL または P/S-VOL の数
2. システム内部のスナップショットのコピー処理と競合した場合のみ発生するコピー停止処理の待ち時間

単位ボリューム削除時間とスナップショット構成削除時間は、P-VOL のサイズによって以下のように目安時間が変わります。

P-VOL のサイズ[GiB]	単位ボリューム削除時間[sec]	スナップショット構成削除時間[sec]
128	10	4
256	10	4
1024	10	4
4096	11	10
8192	11	15
16384	15	32
32768	19	64
51200	24	92
65536	29	107
98304	41	161



ハードウェア交換の条件<<Bare metal>>

この章での記述内容は Bare metal モデルに適用されます。

□ H.1 ハードウェア交換の条件<<Bare metal>>

H.1 ハードウェア交換の条件<<Bare metal>>

この節での記述内容は Bare metal モデルに適用されます。

交換する部品は「Hitachi Virtual Storage Platform One SDS Block ハードウェア互換性リファレンス」に記載してあるハードウェアから選択してください。ハードウェア交換の際に特別な条件があるものは以下のとおりです。



注意

交換前と型名の異なる部品を使用してハードウェア交換を行った場合は、交換前と交換後でシステムの性能に影響が出る可能性があります。

コンポーネント	ハードウェア交換の条件		
	ストレージノードの交換	ストレージノードの保守回復	構成リストア
プロセッサ	特になし	特になし	形名が交換前と同一であること
メモリー	メモリー容量が交換前と同等以上であること	メモリー容量が交換前と同等以上であること	- 交換前後で同一のスロットに搭載していること - 搭載枚数が交換前と同一であること - メモリー容量が交換前と同等以上であること
イーサネット(コンピュータポート、ストレージノード間ポート、管理ポート)	各コンポーネントの PCI スロット位置は任意です。管理ポートの数は同一である必要はありませんが、交換前後でコンピュータポート数は同一である必要があります。	交換前後で同一のスロットに搭載している必要があります。また、交換前後で管理ポート数もコンピュータポート数も同一である必要があります。	- 形名が交換前と同一であること - 交換前後で同一のスロットに搭載している必要があります。また、交換前後でコンピュータポート数は同一である必要がありますが、管理ポートの数は同一である必要はありません。
ファイバーチャネル(コンピュータポート)	- 交換前の FCHBA とポート数が同一であること - 交換前の FCHBA と SFP データ転送速度が同一であること	- 交換前の FCHBA とポート数が同一であること - 交換前の FCHBA と SFP データ転送速度が同一であること - 交換前後で同一の PCI スロットに搭載していること - FCHBA が 2 枚以上搭載されていないこと	- 形名が交換前と同一であること - 交換前の FCHBA と SFP データ転送速度が同一であること - 交換前後で同一の PCI スロットに搭載していること

コンポーネント	ハードウェア交換の条件		
	ストレージノードの交換	ストレージノードの保守回復	構成リストア
ディスクコントローラー (システムドライブ用)	各コンポーネントの PCI スロット位置は任意です。	不可	- 形名が交換前と同一であること - 交換前後で同一の PCI スロットに搭載していること
ディスクコントローラー (ユーザーデータドライブ用)	各コンポーネントの PCI スロット位置は任意です。	- 形名が交換前と同一であること - 交換前後で同一の PCI スロットに搭載していること	- 形名が交換前と同一であること - 交換前後で同一の PCI スロットに搭載していること
システムドライブ	特になし	RAID1 構成を組んでいて、かつその一部のシステムドライブの交換であること (RAID1 構成を組んでいない、または RAID1 構成を構成するすべてのシステムドライブを交換する場合は、ストレージノードの交換による回復が必要になります。)	- 形名が交換前と同一であること - 交換前後で同一のスロットに搭載していること
ユーザーデータドライブ	ドライブの物理容量が交換前と同等以上であること	ドライブの物理容量が交換前と同等以上であること	- 形名が交換前と同一であること - 交換前後で同一のスロットに搭載していること



容量削減機能が有効なボリュームの削除時間

- I.1 容量削減機能が有効なボリュームの削除時間(目安)

I.1 容量削減機能が有効なボリュームの削除時間(目安)

容量削減機能が有効なボリュームの削除時間の目安(単位：秒)を求める計算式は以下のとおりです。

ボリュームの削除時間[sec] = (ボリュームの totalCapacity[MiB] ÷ 1024) ÷ ボリューム削除速度

- ・ ボリュームの削除速度：0.28[GiB/sec]

容量削減機能が有効なボリュームの削除は、以下の要素によって削除までに掛かる時間が変わります。

- ・ ストレージノードの CPU 数
- ・ 同時に削除したボリューム数
- ・ 削除するボリュームの容量
- ・ 削除するボリュームに書き込まれているデータ量

ボリュームの削除速度の測定条件は以下のとおりです。



メモ

- ・ 測定結果は、他の処理が動作していないケースでの一例です。また、実際の性能を保証するものではありません。
- ・ I/O 処理などによってストレージノードが他の処理を実行している場合は目安より削除速度が遅くなる場合があります。
- ・ 削除完了の監視は 60 秒周期で行われるため、削除時間(目安)よりも 60 秒ほど追加で時間が掛かることがあります。

項目	条件
CPU 数	16
メモリー	234GiB
同時に削除したボリューム数	20 個
容量削減機能による削減前後のデータ容量の比率 *	2:1
* 削減前と削減後のデータ容量の比率を N:1 で表しています。パーセント[%]で表す場合は、 $(1 - 1/N) \times 100$ で計算します。	



ストレージコントローラーへの容量割り付けの処理時間

- J.1 ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安)
- J.2 ストレージコントローラーへの容量割り付けの処理時間(論理容量)(目安)

J.1 ストレージコントローラーへの容量割り付けの処理時間(物理容量)(目安)

ストレージコントローラーへの容量割り付けの処理時間(目安)は以下の計算式で求められます。

この処理は、ストレージコントローラーごとに順次実行される処理と各ストレージコントローラーで並列に実行される処理からなります。

順次実行される処理は、ストレージノード 1 台当たりのストレージプールに拡張するドライブ(以降、拡張対象のドライブ)の総物理容量と、ストレージコントローラー数(ストレージノード数)に依存します。

並列に実行される処理は、ストレージノード 1 台当たりの拡張対象のドライブの総物理容量に依存します。

順次処理の単位処理時間[sec] × (ストレージノード 1 台当たりの拡張対象のドライブの総物理容量[GiB]^{*1} ÷ 割り付け単位容量[GiB])^{*2} × ストレージノード数^{*3} + 並列処理の単位処理時間[sec] × (ストレージノード 1 台当たりの拡張対象のドライブの総物理容量[GiB]^{*1} ÷ 割り付け単位容量[GiB])^{*2}

*1: ストレージノードを増設するときは、「ストレージノード 1 台当たりの拡張対象のドライブ」は「追加するストレージノード 1 台当たりの拡張対象のドライブ」と読み替えてください。

*2: ストレージノード 1 台当たりの拡張対象のドライブの総物理容量[GiB] ÷ 割り付け単位容量[GiB]は、小数点以下を切り捨ててください。

*3: ストレージノードを増設するときは、「ストレージノード数」は「追加するストレージノード数」と読み替えてください。

順次処理の単位処理時間、並列処理の単位処理時間、割り付け単位容量は、ユーザーデータの保護種別によって以下の値となります。

ユーザーデータの保護種別 (redundantType)	順次処理の単位処理時間[sec]	並列処理の単位処理時間[sec]	割り付け単位容量 [GiB]
<<Bare metal>> 4D+1P	1.8	23.0	121
4D+2P	2.0		145
Duplication	3.2		194

(例)ストレージコントローラーへの容量割り付け処理時間の計算式の例を以下に示します。

条件:

- ユーザーデータの保護種別(redundantType)が Duplication
- ストレージノード数が 3 台
- ストレージノード 1 台当たりの拡張対象のドライブ容量が 1.6[TiB]
- ストレージノード 1 台当たりの拡張対象のドライブ数が 6 台

計算式の例：

$$3.2 \times (1.6 \times 1024 \times 6 \div 194) \times 3 + 23 \times (1.6 \times 1024 \times 6 \div 194) = 3.2 \times 50 \times 3 + 23 \times 50 = 1630[\text{sec}]$$

なお、上記の処理時間はストレージノードの CPU 数が 14 の場合です。それ以外の場合は以下のとおりです。

- CPU 数が 14 未満の場合：上記より処理時間が増加することがあります。
- CPU 数が 15 以上の場合：上記より処理時間が減少することがあります。

J.2 ストレージコントローラーへの容量割り付けの処理時間(論理容量)(目安)

ストレージコントローラーへの容量割り付けの処理時間(目安)は以下の計算式で求められます。

この処理は、ストレージコントローラーごとに順次実行される処理と各ストレージコントローラーで並列に実行される処理からなります。

順次実行される処理は、ストレージコントローラー 1 つ当たりの増加した論理容量と、ストレージコントローラー数(ストレージノード数)に依存します。

並列に実行される処理は、ストレージコントローラー 1 つ当たりの増加した論理容量に依存します。

- 論理容量が編集前と比べて増加している場合

$$\text{順次処理の単位処理時間}[\text{sec}] \times (\text{ストレージコントローラー 1 つ当たりの増加した論理容量}[\text{GiB}] \div \text{割り付け単位容量}[\text{GiB}])^{*1} \times \text{ストレージノード数} + \text{並列処理の単位処理時間}[\text{sec}] \times (\text{ストレージコントローラー 1 つ当たりの増加した論理容量}[\text{GiB}] \div \text{割り付け単位容量}[\text{GiB}])^{*1}$$

- リビルド領域ポリシーを"Variable"から"Fixed"、許容されるドライブ障害数を 0 に編集した場合

$$\text{順次処理の単位処理時間}[\text{sec}] \times (((\text{任意のストレージコントローラーの allocatableCapacity}[\text{MiB}] - \text{任意のストレージコントローラーの currentlyAllocatableCapacity}[\text{MiB}]) \div 1024) [\text{GiB}] \div \text{割り付け単位容量}[\text{GiB}])^{*2} \times \text{ストレージノード数} + \text{並列処理の単位処理時間}[\text{sec}] \times (((\text{任意のストレージコントローラーの allocatableCapacity}[\text{MiB}] - \text{任意のストレージコントローラーの currentlyAllocatableCapacity}[\text{MiB}]) \div 1024) [\text{GiB}] \div \text{割り付け単位容量}[\text{GiB}])^{*2}$$

*1：ストレージコントローラー 1 つ当たりの増加した論理容量[GiB] ÷ 割り付け単位容量[GiB]は、小数点以下を切り捨ててください。

*2：(((任意のストレージコントローラーの allocatableCapacity[MiB] - 任意のストレージコントローラーの currentlyAllocatableCapacity[MiB]) ÷ 1024)[GiB] ÷ 割り付け単位容量[GiB])は、小数点以下を切り捨ててください。

順次処理の単位処理時間、並列処理の単位処理時間、割り付け単位容量は、ユーザーデータの保護種別によって以下の値となります。

ユーザーデータの保護種別 (redundantType)	順次処理の単位処理時間[sec]	並列処理の単位処理時間[sec]	割り付け単位容量 [GiB]
≪Bare metal≫ 4D+1P	1.8	23.0	97
4D+2P	2.0		
Duplication	3.2		

(例)ストレージコントローラーへの容量割り付け処理時間の計算式の例を以下に示します。

条件：

- ・ ユーザーデータの保護種別(redundantType)が Duplication
- ・ ストレージノード数が 3 台
- ・ ストレージコントローラー 1 つ当たりの増加した論理容量が 198[GiB]

計算式の例：

$$3.2 \times (198 \div 97) \times 3 + 23 \times (198 \div 97) = 3.2 \times 2 \times 3 + 23 \times 2 = 65[\text{sec}]$$

なお、上記の処理時間はストレージノードの CPU 数が 14 の場合です。それ以外の場合は以下のとおりです。

- ・ CPU 数が 14 未満の場合：上記より処理時間が増加することがあります。
- ・ CPU 数が 15 以上の場合：上記より処理時間が減少することがあります。



用語解説

(英字)

BMC ネットワーク

ストレージノードの BMC とコントローラーノードを接続するネットワーク。BMC をコントローラーノードから操作するために使用される。

BMC ポート

BMC ネットワークに接続するためのストレージノードのポート。

Data At Rest Encryption

用語解説の「格納データ暗号化」を参照してください。

host NQN(NVMe Qualified Name)

NVMe/TCP の通信プロトコルで、NVMe ホストを特定するための識別子。

Multi-AZ 構成

リソースを複数のアベイラビリティゾーン(Google Cloud においてはゾーン)に配置し、データセンター障害が発生してもシステム停止とされない構成。Cloud モデル for Google Cloud では Multi-Zone 構成とも表記する。

Namespace

NVM サブシステム上に作られるボリューム情報。

NVM サブシステム

Namespace を共有する NVM デバイス制御システム。

PIN

ストレージコントローラーのキャッシュ上に障害が発生した状態。

P/S-VOL

カスケード構成のスナップショットツリーにおいて、P-VOL であり、かつ S-VOL を持つ属性のボリューム。

P-VOL

スナップショットでの、コピー元のボリューム。
Universal Replicator では、リモートコピー元のボリューム。

Single-AZ 構成

リソースを単一のアベイラビリティゾーン(Google Cloud においてはゾーン)に配置する構成。Cloud モデル for Google Cloud では Single-Zone 構成とも表記する。

S-VOL

スナップショットでの、コピー先のボリューム。
Universal Replicator では、リモートコピー先のボリューム。

Universal Replicator

本来のデータセンター(正サイトのストレージシステム)とは別のデータセンター(副サイトのストレージシステム)を遠隔地に設置して、正サイトの P-VOL へのデータ書き込みとは非同期に、副サイトにある S-VOL にデータをコピーする機能。

UR データボリューム

P-VOL、S-VOL、または P/S-VOL のうち、Universal Replicator のコピー対象になっているボリューム。

VM

仮想マシン。

VPS

Virtual Private Storage の略。用語解説の「仮想プライベートストレージ」を参照してください。

VPS 管理者

マルチテナンシー構成において、仮想プライベートストレージ(VPS)を管理する管理者。

(ア行)

アザーボリューム容量

スナップショットボリューム(S-VOL、P/S-VOL)の総容量。

一時ボリューム容量

データマイグレーション、容量バランスで一時的に作成されるボリュームの総容量。

イニシエーター

コンピュータノードからボリュームへアクセスするときのコンピュータノード側のエンドポイント。

イベントログ

システムの動作を記録するファイル。VSP One SDS Block では、障害通知目的のログを指す。

(カ行)

格納データ暗号化

ユーザーデータをストレージシステム内のソフトウェアによって暗号化する機能。

仮想コマンドデバイス

RAID Manager のコマンドを Out-of-band 方式で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。

仮想プライベートストレージ

マルチテナンシー構成において、ストレージクラスターから論理的に分割された仮想ストレージ。

カレントフォールトドメイン

ボリュームを管理するストレージコントローラーが現在属するフォールトドメイン。

管理ネットワーク

≪Bare metal≫コントローラーノードと、ストレージノード間のネットワーク。VSP One SDS Block の管理操作や SNMP、NTP などの外部サービスとの通信に使用する。

≪Cloud≫コントローラーノードと、ストレージノード間のネットワーク。VSP One SDS Block の管理操作や SNMP などの外部サービスとの通信に使用する。

管理ポート

≪Cloud≫管理ネットワークに接続するストレージノードの仮想ポート。

≪Bare metal≫管理ネットワークに接続するストレージノードのポート。

クラスターマスターノード(セカンダリー)

クラスターマスターノード(プライマリー)に障害が発生した場合に、クラスターマスターノード(プライマリー)に代わって、ストレージクラスター全体を管理する役割を持つストレージクラスター内にあるストレージノード。

クラスターマスターノード(プライマリー)

ストレージクラスター全体を管理する役割を持つストレージクラスター内にあるストレージノード。

クラスターワーカーノード

ストレージクラスター全体を管理する役割を持たないストレージクラスター内にあるストレージノード。

形成コピー

ペア作成またはペア再同期の契機で実行されるコピー。

更新コピー

ジャーナルボリュームに格納された更新データを S-VOL に反映させるコピー。

構成バックアップファイル≪Bare metal≫ ≪Cloud for AWS≫

ストレージクラスターの構成情報をバックアップしたファイル。

構成ファイル

≪Cloud≫VSSB 構成ファイルと VM 構成ファイルの総称。

≪Bare metal≫VSSB 構成ファイルのこと。

コンシステンシーグループ

データの一貫性を保ってコピーされるボリュームの集合。同一ジャーナルに属する UR データボリュームは、すべて同じコンシステンシーグループに属する。

コンソールインターフェイス

ストレージノードのコンソール(BMC 経由の仮想コンソールなど)のインターフェイス。

コントローラーノード

VSP One SDS Block の管理機能(ボリューム作成など)の指示に使われる管理用のノード。

コンピュータネットワーク

コンピュータノードとストレージノードとの間のネットワーク。ユーザーデータの入出力に使用する。

コンピュータノード

ユーザーのアプリケーションが動作し、ユーザーデータの入出力をストレージノードに指示するノード。コンピュータポートに接続しているホスト。

コンピュータポート

≪Cloud≫ コンピュータネットワークに接続するストレージノードの仮想ポート。

≪Bare metal≫ コンピュータネットワークに接続するストレージノードのポート。

(サ行)

システム管理者

ストレージクラスター全体を管理する管理者。

システムコントローラー

ストレージノード自体の稼働やストレージノード間の連携、ストレージクラスターの運用や保守に必要な VSP One SDS Block の一部のプロセス。

自動回復

用語解説の「ストレージノード自動回復」を参照してください。

ジャーナル

ジャーナルボリュームと UR データボリュームを関連付ける仕組み。

ジャーナルボリューム

Universal Replicator で、P-VOL から S-VOL にコピーするデータと、制御用のメタデータを格納するボリューム。

障害ドライブ

障害が発生して、保守交換が必要なドライブ。

シンプロビジョニング

最小容量の領域のみを最初に確保し、必要に応じて拡張していく仮想ストレージの作成方式。

スケールアウト

ストレージノードの追加によって、CPU 数、メモリー容量、ドライブ数などを増加させ、システムの性能や容量を向上させる方式。

スコープ

ユーザーが操作できるリソースの範囲。ユーザーグループに設定され、どのユーザーグループに属するかによって、ユーザーのスコープが決定する。

ストレージクラスター

複数のストレージノードから構築される、仮想的なストレージシステム。

ストレージコントローラー

ストレージノードの容量やボリュームを管理する VSP One SDS Block の一部のプロセス。

ストレージコントローラー再配置

ストレージノードの増設や減設によってストレージノード間のストレージコントローラー数に偏りが生じるため、各ストレージノードのストレージコントローラー数を最適化する機能。

ストレージソフトウェア

ストレージクラスターを実現する VSP One SDS Block のソフトウェア。

ストレージノード

≪Bare metal≫VSP One SDS Block を構成する CPU、メモリー、ドライブが割り当てられた物理サーバー。または、ストレージノード上で動作する VSP One SDS Block ソフトウェアのプロセスグループを指す。

≪Cloud≫VSP One SDS Block を構成する CPU、メモリー、ドライブが割り当てられた仮想サーバー。または、ストレージノード上で動作する VSP One SDS Block ソフトウェアのプロセスグループを指す。

ストレージノード間ネットワーク

ストレージノード間のネットワーク。ストレージノード間のユーザーデータのやりとりや、ストレージノード間の管理情報の通信に使用する。

ストレージノード間ポート

≪Cloud≫ストレージノード間のネットワークに接続するストレージノードの仮想ポート。

≪Bare metal≫ストレージノード間のネットワークに接続するストレージノードのポート。

ストレージノード減設

ストレージノードをストレージクラスターから取り除く処理。

ストレージノード交換

閉塞しているストレージノードを手動で回復させる機能または処理。

以下を交換して、閉塞しているストレージノードを回復する。

≪Cloud≫ストレージノード VM

≪Bare metal≫物理ノード

ストレージノード自動回復

ソフトウェア要因(ファームウェア、ドライバなど)によるサーバー障害、またはストレージノード間ネットワークの一時的な障害によるサーバー障害からストレージノードを復旧するために、ストレージノードの自己診断と自動復旧を行う機能。

ストレージノード増設

ストレージノードをストレージクラスターに追加する処理。

ストレージノード保守回復

閉塞しているストレージノードを手動で回復させる機能または処理。以下を使用して、閉塞しているストレージノードを回復する。

≪Bare metal≫閉塞前からストレージノードとして使用していた物理ノード

≪Cloud≫既存のストレージノード VM

ストレージノード保守閉塞

ストレージノードを一時的にストレージクラスターから切り離し、部品交換などの保守が可能な状態にする処理。

ストレージプール

複数のドライブをまとめた論理的なユーザーデータ格納域。

スナップショットボリューム

P-VOL、S-VOL、P/S-VOL のどれかであるボリューム。

スペアノード

スペアノード機能で使用する待機用のノード。

スペアノード機能

ストレージクラスターに、待機用のノードを登録し、障害発生ストレージノードが自動回復による保守回復で復旧できない場合に、障害発生ストレージノードから待機用のノードへ切り換えることで冗長性の回復を行う機能。

セカンダリーフォールトドメイン

プライマリーフォールトドメインに切り替えが必要な障害が発生したときの、切り替え先のフォールトドメイン。ボリュームの管理は、切り替え先であるセカンダリーフォールトドメインに所属するストレージコントローラーに切り替わる。

(タ行)

代表ストレージノード

Bare metal モデルのセットアップ手順において、ストレージクラスターの構築に使用する任意のストレージノード。クラスターマスターノード(プライマリー)とは異なる。

タイブレーカーノード

Multi-AZ(Multi-Zone)構成において、分散合意でのスプリットブレイン問題を回避するために監視機能を動作させるストレージノード。ストレージコントローラー、ドライブ、コンピュータポートは持たない。

ターゲット

コンピュータノードからボリュームへアクセスするときのストレージクラスター側のエンドポイント。

ターシャリーフォールトドメイン

セカンダリーフォールトドメインに切り替えが必要な障害が発生したときの、切り替え先のフォールトドメイン。

通常ボリューム

ローカルコピー(スナップショット/データマイグレーション)の P-VOL、S-VOL、P/S-VOL のどれでもないボリューム。

ディスクコントローラー

ドライブを利用するために必要なハードウェア。

データマイグレーション

外部ストレージシステムから VSP One SDS Block 内にボリューム単位でデータを移行する機能。

ドライブ

≪Bare metal≫ユーザーデータや OS を格納する物理デバイス。SSD や HDD の一般名称。
≪Cloud for AWS≫ユーザーデータや OS を格納する EBS。

≪Cloud for Google Cloud≫ユーザーデータや OS を格納する Google Cloud Hyperdisk。
≪Cloud for Microsoft Azure≫ユーザーデータや OS を格納する Azure マネージドディスク。

ドライブ再組み入れ

閉塞しているドライブを再利用して回復させる機能または処理。

ドライブ自動回復

障害が起きたドライブを自動で回復させる機能。

ドライブデータ再配置

ストレージノードの増設や減設によってストレージノード間の容量に偏りが生じた場合、各ストレージノードの容量の使用効率を最適化するため、ストレージノード間のデータ容量を平準化する機能。

(ハ行)

フェイルオーバー

クラスターマスターノード(プライマリー)の障害時に、クラスターマスターノード(セカンダリー)をクラスターマスターノード(プライマリー)に切り替える機能。

フォールトドメイン

電源系統やネットワークスイッチを共有しているストレージノードのグループ。グループ内のストレージノードがまとまって異常になってもストレージの運用を継続できるようにするための構成。

物理ノード

ストレージを利用する環境において、その環境に属する物理サーバー。

プライマリーフォールトドメイン

ボリュームを管理するストレージコントローラーが本来属するフォールトドメイン。

プログラムプロダクトライセンス

機能単位のライセンス。

プロテクションドメイン

ストレージノードやストレージノード間ネットワークで障害が発生したときに、障害範囲を限定するための設定。

プロビジョンドボリューム容量

通常ボリューム、スナップショットボリューム(P-VOL)、ジャーナルボリューム、元ジャーナルボリュームの総容量。

閉塞

ストレージやストレージを構成するリソースにおける状態の一種で、I/O ができない状態のこと。

閉塞ドライブ

閉塞状態にあるドライブ。保守交換が必要かどうかは未確定の状態。

ベースライセンス

基本的な機能を提供するライセンス。

保守回復

用語解説の「ストレージノード保守回復」を参照してください。

保守閉塞

用語解説の「ストレージノード保守閉塞」を参照してください。

ボリューム

コンピュータノードにマウントしてユーザーデータの読み書きを行う論理デバイス。

ボリューム種別

通常ボリューム、スナップショットボリューム、マイグレーション先ボリューム、またはマイグレーション元ボリューム(仮想ボリューム)のどれに該当するかを示す情報。

Universal Replicator では、通常ボリューム、スナップショットボリューム、マイグレーション先ボリューム、マイグレーション元ボリューム(仮想ボリューム)、ジャーナルボリューム、または元ジャーナルボリュームのどれに該当するかを示す情報。

ボリュームパス

コンピュータノードとボリュームの接続情報。コンピュータノードからボリュームを利用するために必要な設定情報の1つ。

ボリュームマイグレーション

ストレージノードの減設時に、減設するストレージノードにあるボリュームを別のストレージノードに移動すること。

(マ行)

マスタージャーナルボリューム

P-VOL と関連付けられているジャーナルボリューム。

マルチテナンシー機能

大規模ストレージシステムにおいて、1つのストレージのリソースを複数のテナント(会社や部署)で分配または共有利用できるようにする機能。分配された個々のストレージシステムが仮想プライベートストレージ(VPS)となる。

ミラー

マスタージャーナルとリストアジャーナルのペア関係。

ミラーユニット

ジャーナルを所属ミラーごとに細分化して管理する際の管理単位。1つのジャーナルが複数ミラーに属する場合は、属するミラーごとに状態や適用すべきオプションが異なる。これらの状態やオプションは(ジャーナルではなく)各ミラーユニットが保持する。

(ヤ行)

容量バランス

ストレージコントローラー間の容量使用率が偏ると、自動的に使用率の高いストレージコントローラーから使用率の低いストレージコントローラーにボリュームを移動する機能。

(ラ行)

ライセンスキー

対応するライセンスを VSP One SDS Block で有効化するためのキー。

リザーブジャーナルボリューム

予備のジャーナルボリューム。

リストアジャーナルボリューム

S-VOL と関連付けられているジャーナルボリューム。

リビルド

ドライブやストレージノードの障害の際に、低下したデータの冗長度を自動的に回復させる機能。

リビルド領域

ストレージプールのうち、ドライブ障害時のデータリビルド用に確保されている領域。

リモートストレージシステム

リモートパスグループおよびリモートパスを形成する 2 つのストレージシステムのうち、操作対象(ローカルストレージシステム)ではないストレージシステムのこと。

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。

リモートパスグループ

リモートパスを束ねたもの。

ローカルストレージシステム

リモートパスグループおよびリモートパスに関する操作の対象となるストレージシステムのこと。

© 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
