

Hitachi Command Suite Software

システム構成ガイド (Web Version)

3020-3-W22-C0

対象製品

Hitachi Device Manager 7.6.1

Hitachi Tiered Storage Manager 7.6.1

Hitachi Tiered Storage Manager は、経済産業省が 2003 年度から 3 年間実施した「ビジネスグリッドコンピューティングプロジェクト」の技術開発の成果を含みます。

輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。

なお、不明な場合は、弊社担当営業にお問い合わせください。

商標類

Active Directory は、米国 Microsoft Corporation の、米国およびその他の国における登録商標または商標です。

Adobe、および Flash は、Adobe Systems Incorporated (アドビシステムズ社) の米国ならびに他の国における商標または登録商標です。

AIX は、米国およびその他の国における International Business Machines Corporation の商標です。

AIX 5L は、米国およびその他の国における International Business Machines Corporation の商標です。

Ethernet は、富士ゼロックス株式会社の登録商標です。

Firefox は Mozilla Foundation の登録商標です。

HP-UX は、Hewlett-Packard Development Company, L.P. のオペレーティングシステムの名称です。

Internet Explorer は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Itanium は、アメリカ合衆国およびその他の国における Intel Corporation の商標です。

Kerberos は、マサチューセッツ工科大学 (MIT : Massachusetts Institute of Technology) で開発されたネットワーク認証のプロトコルの名称です。

Linux は、Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。

Microsoft および Hyper-V は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Novell、および NetWare は、Novell, Inc. の米国およびその他の国における登録商標または商標です。

Oracle と Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes software developed by IAIK of Graz University of Technology.

RC4 は、EMC Corporation の米国およびその他の国における登録商標または商標です。

Red Hat は、米国およびその他の国で Red Hat, Inc. の登録商標もしくは商標です。

RSA および BSAFE は、米国 EMC コーポレーションの米国およびその他の国における商標または登録商標です。

すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標がついた製品は、米国 Sun Microsystems, Inc. が開発したアーキテクチャに基づくものです。

SUSE は日本における Novell, Inc. の商標です。

UNIX は、The Open Group の米国ならびに他の国における登録商標です。

VERITAS および VERITAS ロゴは、Symantec Corporation の米国およびその他の国における商標または登録商標です。

Veritas および Veritas Storage Foundation は、Symantec Corporation の米国およびその他の国における商標または登録商標です。

VMware、vCenter Server は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。

VMware、VMware vSphere は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。

VMware、VMware vSphere ESX は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。

VMware、VMware vSphere ESXi は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。

Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows Server は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows Vista は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

Hitachi Device Manager および Hitachi Tiered Storage Manager には、Oracle Corporation またはその子会社、関連会社が著作権を有している部分が含まれています。

Hitachi Device Manager および Hitachi Tiered Storage Manager には、UNIX System Laboratories, Inc.が著作権を有している部分が含まれています。

Hitachi Device Manager および Hitachi Tiered Storage Manager は、米国 EMC コーポレーションの RSA BSAFE® ソフトウェアを搭載しています。

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from <ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/>.

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (<http://relaxngcc.sf.net/>).

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (<http://java.apache.org/>).

This product includes software developed by Andy Clark.

This product includes software developed by the OpenSSL project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).



発行

2014年1月 3020-3-W22-C0

著作権

All Rights Reserved. Copyright © 2010, 2014, Hitachi, Ltd.

目次

はじめに.....	25
対象読者.....	26
マニュアルの構成.....	26
マイクロソフト製品の表記について.....	27
このマニュアルで使用している記号.....	28
1. 概要.....	29
1.1 システム構成.....	30
1.1.1 ハードウェア構成.....	30
1.1.2 ソフトウェア構成.....	31
1.2 ネットワーク構成.....	32
1.2.1 セキュリティについての一般的なリスク.....	33
1.2.2 最もセキュアな構成：管理用の LAN を分離し、ファイアウォールを設置した場合.....	33
1.2.3 番目にセキュアな構成：管理用の LAN を分離し、管理下のデバイスとの間にファイアウォールを設置した場合.....	34
1.2.4 3番目にセキュアな構成：管理用の LAN を分離し、管理サーバをデュアルホームにした場合.....	35
1.2.5 最もセキュアでない構成：フラットなネットワーク.....	36
1.3 管理サーバのシステム要件.....	37
1.3.1 管理リソース数の上限.....	37
1.3.2 メモリーヒープサイズの変更（Hitachi Command Suite 共通コンポーネント）.....	38
1.3.3 メモリーヒープサイズの変更（Device Manager サーバ）.....	39
1.3.4 JDK の変更.....	40
1.4 ホストのシステム要件.....	41
1.4.1 Device Manager で管理できるホスト.....	41
1.4.2 Device Manager のホスト管理ソフトウェア.....	42
1.4.3 通常ホストのシステム要件.....	43
(1) 通常ホストの前提環境（Host Data Collector で管理する場合）.....	43
(2) 通常ホストの前提環境（Device Manager エージェントで管理する場合）.....	45
1.4.4 仮想マシンのシステム要件.....	45
(1) 仮想マシンの前提環境（Host Data Collector で管理する場合）.....	45
(2) 仮想マシンの前提環境（Device Manager エージェントで管理する場合）.....	48
(3) 仮想マシンにボリュームを割り当てるための操作フロー.....	49
(4) 仮想 WWN を Device Manager に登録する（createnpivinfo コマンド）.....	52
(5) 仮想マシンの構成変更時に必要な作業.....	53
1.4.5 仮想化サーバのシステム要件.....	53
(1) 仮想化サーバの前提環境（Host Data Collector で管理する場合）.....	53
(2) 仮想化サーバの前提環境（vMA で管理する場合）.....	54
(3) vMA での仮想化サーバの監視構成.....	55
(4) 仮想化サーバを管理対象にするための操作フロー.....	57
(5) 仮想化サーバの運用に関する注意事項.....	58

1.4.6	メインフレームホストのシステム要件	58
	(1) メインフレームホストを管理対象にするための操作フロー	59
1.4.7	ファイルサーバのシステム要件	59
	(1) Hitachi NAS Platform の前提環境	59
	(2) Hitachi Virtual File Platform の前提環境	61
	(3) ファイルサーバを管理対象にするための操作フロー	61
	(4) ファイルサーバの運用に関する注意事項	62
1.5	関連製品	63
1.6	Device Manager でのコピーペア管理	64
1.6.1	Device Manager でコピーペアを管理できるストレージシステム	64
1.6.2	コピーペアを管理する場合のシステム構成	65
	(1) 通常構成でコピーペアを管理する場合のシステム構成	66
	(2) 一括管理構成でコピーペアを管理する場合のシステム構成	68
	(3) 仮想コマンドデバイスサーバ構成でコピーペアを管理する場合のシステム構成	71
	(4) SVP 構成でコピーペアを管理する場合のシステム構成 (構成定義ファイルでコピーペアを定義した場合)	73
	(5) SVP 構成でコピーペアを管理する場合のシステム構成 (デバイスグループとしてコピーペアを定義した場合)	75
1.6.3	コピーペアを管理する場合のストレージシステムの要件	78
1.6.4	コピーペアを管理する場合の Device Manager エージェントの前提バージョン	81
1.6.5	コピーペアを管理する場合の注意事項	83
1.7	コマンドを実行する場合の注意事項	84
2.	ネットワーク構成に応じた設定	85
2.1	ポートの設定	86
2.1.1	Hitachi Command Suite 製品で 사용되는ポート	86
	(1) Hitachi Command Suite 共通コンポーネントで 사용되는ポート	86
	(2) Device Manager サーバで 사용되는ポート	87
	(3) Tiered Storage Manager サーバで 사용되는ポート	88
	(4) Host Data Collector で 사용되는ポート	89
	(5) Device Manager エージェントで 사용되는ポート	90
	(6) ストレージシステムで 사용되는ポート	90
2.1.2	Hitachi Command Suite 共通コンポーネントで 사용되는ポートの変更	92
2.1.3	ファイアウォールの例外登録	96
	(1) ファイアウォールへの例外登録が必要なポート	96
	(2) ファイアウォールの例外登録 (Windows)	104
	(3) ファイアウォールの例外登録 (Red Hat Enterprise Linux)	106
	(4) ファイアウォールの例外登録 (SUSE Linux Enterprise Server)	106
2.2	ブリッジ機能を使用する場合のネットワークの設定	107
2.3	IPv6 環境で運用する場合の Device Manager の設定	108
2.3.1	Device Manager を IPv6 環境に移行するときの設定	108
2.3.2	IPv6 に対応したストレージシステムと連携するための設定	109
2.4	管理サーバの IP アドレスまたはホスト名の変更	110
2.4.1	管理サーバのホスト名の変更	110
2.4.2	管理サーバの IP アドレスの変更	111
2.4.3	管理サーバの IP アドレスまたはホスト名の変更後に必要な作業	112
2.5	Hitachi Command Suite 製品の URL の変更 (hcmdschgurl コマンド)	114
3.	ユーザーアカウントを管理するために必要な設定	117
3.1	パスワードポリシーとは	118
3.1.1	パスワードポリシーの設定	118
3.2	アカウントロックとは	119
3.2.1	アカウントロックポリシーとは	120

3.2.2 アカунロックポリシーの設定.....	120
3.2.3 System アカウンのロックに関する設定.....	120
3.2.4 アカウンロックの解除.....	121
3.3 外部認証サーバでのユーザー管理.....	122
4. セキュリティ設定.....	123
4.1 警告バナーとは.....	124
4.1.1 警告バナーに表示するメッセージの条件.....	124
4.1.2 警告バナーに表示するメッセージの作成と登録.....	124
4.1.3 警告バナーからのメッセージの削除.....	125
4.2 通信に関するセキュリティ設定.....	126
4.3 管理サーバに接続できる管理クライアントを制限するための設定.....	126
4.4 Device Manager CLI または Tiered Storage Manager CLI でパスワードをコード化するときの強度の変更.....	128
5. 関連製品と連携するために必要な設定.....	129
5.1 Element Manager を使用するために必要な設定.....	130
5.1.1 Storage Navigator Modular 2 と連携するための前提条件.....	130
(1) Storage Navigator Modular 2 利用時の前提条件.....	130
(2) Storage Navigator Modular 2 と連携する場合の注意事項.....	131
5.1.2 Element Manager を使用するための設定.....	131
5.1.3 Element Manager を使用するための設定の解除.....	133
5.2 ストレージシステムの性能情報を収集するために必要な設定.....	134
5.2.1 ストレージシステムの性能情報を収集するためのシステム構成.....	134
5.2.2 Device Manager サーバ、 Tuning Manager サーバおよび Tuning Manager - Agent for RAID 間で通信するための設定.....	136
5.2.3 ストレージシステムの性能情報を収集するための設定.....	137
(1) エンタープライズクラスストレージおよび HUS VM の性能情報を収集するための設定.....	137
(2) ミッドレンジストレージの性能情報を収集するための設定.....	138
5.2.4 Device Manager サーバを設定するための操作フロー（ストレージシステムの性能情報の収集）.....	139
(1) Tuning Manager サーバとのリモート接続（非クラスタ環境）.....	141
(2) Tuning Manager サーバとのリモート接続（Microsoft Cluster Service または Windows Server Failover Clustering）.....	142
(3) Tuning Manager サーバとのリモート接続（Veritas Cluster Server）.....	144
(4) Tuning Manager サーバとのリモート接続（Sun Cluster）.....	145
(5) Tuning Manager サーバとのリモート接続およびポート番号の設定（htmsetup コマンド）.....	147
(6) config.xml ファイルおよび configforclient.xml ファイルの設定.....	148
5.2.5 管理クライアントの設定（ストレージシステムの性能情報の収集）.....	148
5.3 Universal Replicator の性能を分析するために必要な設定.....	149
5.3.1 Universal Replicator の性能を分析するためのシステム構成.....	149
5.3.2 Universal Replicator の性能を分析するための Device Manager の設定.....	151
5.3.3 Universal Replicator の性能を分析するための Replication Manager の設定.....	151
5.3.4 Universal Replicator の性能を分析するための Tuning Manager の設定.....	152
5.4 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするために必要な設定.....	152
5.4.1 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするための前提環境.....	152
5.4.2 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするための設定.....	153
6. ログおよびアラートの設定.....	155
6.1 統合ログの設定.....	156
6.1.1 トレースログファイルの設定（Windows）.....	156
6.1.2 トレースログファイルの設定（Solaris または Linux）.....	156
6.1.3 Tiered Storage Manager CLI のログファイル採取の設定.....	157
6.2 監査ログを採取するために必要な設定.....	157

6.2.1	監査ログに出力される監査事象	159
6.2.2	監査ログの環境設定ファイルの編集	167
6.3	アラートの設定	169
6.3.1	Device Manager での障害検知	169
6.3.2	SNMP トラップをアラートに表示するための設定	170
6.3.3	アラートを E メール通知するための操作フロー	170
(1)	SMTP サーバの設定	171
(2)	受信ユーザーの登録	171
(3)	アラート通知のプロパティ設定	172
(4)	SMTP 認証ユーザーアカウントの Device Manager への登録	172
(5)	アラート通知テンプレートのカスタマイズ	173
6.4	SNMP トラップをログファイルに出力するための設定	175
6.4.1	SNMP トラップをログファイルに出力するための設定	175
6.5	イベント通知を使用するために必要な設定	176
6.5.1	イベント通知のためのプロパティの設定	177
6.5.2	イベント通知テンプレートの編集	177
6.5.3	SMTP 認証ユーザーの設定	181
(1)	hdvmmmodmailuser コマンド	181
(2)	htsmmodmailuser コマンド	182
6.6	JP1/IM でログを参照するために必要な設定	183
6.6.1	管理サーバが Windows の場合	183
6.6.2	管理サーバが Solaris または Red Hat Enterprise Linux の場合	184
7.	CIM/WBEM のセットアップ	187
7.1	CIM/WBEM とは	188
7.2	Device Manager の CIM/WBEM 機能	188
7.3	ネームスペースの指定方法	189
7.4	CIM/WBEM 機能を使用するためのユーザーアカウント	190
7.5	CIM/WBEM 機能を利用するための設定	190
7.5.1	CIM/WBEM 機能で使用するポートの変更	192
7.6	CIM/WBEM 機能でストレージシステムの性能情報を取得するための設定	192
7.6.1	CIM/WBEM 機能で性能情報を取得する場合のシステム構成	193
7.6.2	エンタープライズクラスストレージの性能情報を取得するための設定	194
(1)	ストレージシステムに必要な設定	194
(2)	性能情報を収集するホストに必要な設定	194
(3)	Device Manager サーバに必要な設定	195
(4)	コマンドデバイスを登録する (perf_findcmddev コマンド)	195
(5)	perf_cmddev.properties ファイルの形式	196
7.6.3	ミッドレンジストレージの性能情報を取得するための設定	198
(1)	ストレージシステムに必要な設定	198
(2)	性能情報を取得するユーザーアカウントの登録 (hdvmmmodpolluser コマンド)	198
7.7	SLP サービスの制御	199
7.7.1	サービスディスカバリー機能を使用する場合の前提ソフトウェア	199
7.7.2	SLP サービスの起動と停止	199
(1)	SLP サービスの起動と停止 (Windows)	199
(2)	SLP デーモンの起動と停止 (Solaris)	200
(3)	SLP デーモンの起動と停止 (Red Hat Enterprise Linux)	200
(4)	SLP デーモンの起動と停止 (SUSE Linux Enterprise Server)	201
7.7.3	SLP サービスの解除	201
(1)	SLP サービスの解除 (Windows)	201
(2)	SLP デーモンの解除 (Solaris)	201
(3)	SLP デーモンの解除 (Linux)	202
7.7.4	OpenSLP のログに関する注意事項	202

8. クラスタ環境でのセットアップ	203
8.1 管理サーバの環境の確認	204
8.2 Windows でのセットアップ	204
8.2.1 新規インストール (Windows)	205
(1) 実行系ノードでの手順	205
(2) 待機系ノードでの手順	207
(3) Microsoft Cluster Service の設定	209
(4) Microsoft Cluster Service に登録するリソースの値	210
(5) Windows Server Failover Clustering の設定	211
(6) Windows Server Failover Clustering に登録するリソースのプロパティ	212
8.2.2 アップグレードまたは上書きインストール (Windows)	214
(1) 準備作業	214
(2) 実行系ノードでの手順	215
(3) 待機系ノードでの手順	216
8.2.3 クラスタ環境への変更 (Windows)	217
8.2.4 アンインストール (Windows)	220
8.3 Solaris でのセットアップ	222
8.3.1 新規インストール (Solaris)	222
(1) 実行系ノードでの手順	222
(2) 待機系ノードでの手順	225
(3) スクリプトの作成 (Veritas Cluster Server の場合)	227
(4) スクリプトの作成 (Sun Cluster の場合)	228
(5) クラスタリソースの登録 (Veritas Cluster Server の場合)	231
(6) クラスタリソースの登録 (Sun Cluster の場合)	234
8.3.2 アップグレードまたは上書きインストール (Solaris)	238
(1) Veritas Cluster Server での準備作業	238
(2) Sun Cluster での準備作業	239
(3) 実行系ノードでの手順	239
(4) 待機系ノードでの手順	241
(5) クラスタリソースの設定 (Veritas Cluster Server の場合)	241
(6) クラスタリソースの設定 (Sun Cluster の場合)	242
8.3.3 クラスタ環境への変更 (Solaris)	242
8.3.4 アンインストール (Solaris)	245
(1) アンインストール (Veritas Cluster Server の場合)	245
(2) アンインストール (Sun Cluster の場合)	247
9. サービスの起動と停止	249
9.1 Hitachi Command Suite の常駐プロセス	250
9.2 サービスの起動	251
9.3 サービスの停止	253
9.4 サービスの稼働状態の確認	254
10. データベースの管理	255
10.1 データベースを管理する前に	256
10.2 データベースのバックアップ	256
10.2.1 データベースのバックアップ (非クラスタ構成の場合)	257
10.2.2 データベースのバックアップ (Microsoft Cluster Service または Windows Server Failover Clustering の場合)	257
10.2.3 データベースのバックアップ (Veritas Cluster Server の場合)	259
10.2.4 データベースのバックアップ (Sun Cluster の場合)	261
10.3 データベースの復元	262
10.3.1 データベース不整合時のデータベースの復元	263
(1) データベース不整合時のデータベースの復元 (非クラスタ構成の場合)	263

(2) データベース不整合時のデータベースの復元 (Microsoft Cluster Service または Windows Server Failover Clustering の場合)	265
(3) データベース不整合時のデータベースの復元 (Veritas Cluster Server の場合)	267
(4) データベース不整合時のデータベースの復元 (Sun Cluster の場合)	269
10.3.2 データベース破損時のデータベースの復元.....	272
(1) データベース破損時のデータベースの復元 (非クラスタ構成の場合)	272
(2) データベース破損時のデータベースの復元 (Microsoft Cluster Service または Windows Server Failover Clustering の場合)	273
(3) データベース破損時のデータベースの復元 (Veritas Cluster Server の場合)	276
(4) データベース破損時のデータベースの復元 (Sun Cluster の場合)	277
10.4 データベースの移行.....	280
10.4.1 データベースを移行する場合の注意事項.....	280
10.4.2 データベースを移行する流れ.....	281
10.4.3 移行先サーバへの Hitachi Command Suite 製品のインストール.....	281
10.4.4 移行元サーバでのデータベースのエクスポート.....	281
(1) データベースのエクスポート (非クラスタ構成の場合)	282
(2) データベースのエクスポート (Microsoft Cluster Service または Windows Server Failover Clustering の場合)	282
(3) データベースのエクスポート (Veritas Cluster Server の場合)	284
(4) データベースのエクスポート (Sun Cluster の場合)	286
10.4.5 移行先サーバでのデータベースのインポート.....	287
(1) データベースのインポート (非クラスタ構成の場合)	288
(2) データベースのインポート (Microsoft Cluster Service または Windows Server Failover Clustering の場合)	290
(3) データベースのインポート (Veritas Cluster Server の場合)	293
(4) データベースのインポート (Sun Cluster の場合)	296
11. Device Manager エージェントの運用.....	301
11.1 Device Manager エージェントを運用するための前提条件.....	302
11.1.1 複数の NIC が搭載されたホストを使用する場合の前提条件.....	302
11.1.2 Device Manager エージェントを運用する場合の注意事項.....	302
11.2 Device Manager エージェントの環境設定.....	303
11.2.1 Device Manager エージェントで使用する Java の実行環境の変更 (javapath_setup コマンド)	304
11.2.2 Device Manager エージェントの Windows ファイアウォールへの例外登録 (firewall_setup コマンド)	305
11.2.3 java プロセスの SED への例外登録 (AIX)	306
11.2.4 コピーペアを管理するために必要な設定.....	306
11.2.5 ホストで 100 個以上の LU を管理する場合に必要な設定.....	309
(1) ホストで 100 個以上の LU を管理する場合のプロパティの目安値 (ボリュームマネージャーを使用していないとき)	309
(2) ホストで 100 個以上の LU を管理する場合のプロパティの目安値 (ボリュームマネージャーを使用しているとき)	310
11.2.6 Device Manager エージェントの常駐プロセス.....	312
(1) Device Manager エージェントのサービスの起動, 停止, 稼働状態の確認 (hbsasrv コマンド) 313	
(2) サービスの実行ユーザーの変更 (Windows)	314
11.3 Device Manager エージェントの操作.....	314
11.3.1 エージェント機能の確認 (hbsa_modinfo コマンド)	314
11.3.2 Device Manager エージェントのレジストリーとファイルの削除 (hbsa_util コマンド)	315
11.3.3 Device Manager エージェントのバージョンの表示 (hdvm_info コマンド)	316
11.3.4 Device Manager サーバの情報, HiScan コマンドの実行周期および RAID Manager または P9000 RAID Manager の情報の設定 (hdvmagt_setting コマンド)	316
11.3.5 Device Manager サーバへのホスト情報の手動通知 (HiScan コマンド)	318
11.3.6 デバイス情報の取得 (hldutil コマンド)	320
(1) hldutil コマンドで表示される情報.....	322
(2) hldutil コマンドで表示される RaidID が表すストレージシステムの機種.....	323

(3) hidutil コマンドで指定できるソートキー.....	323
11.4 構成定義ファイルの利用	324
11.4.1 構成定義ファイルを利用するための前提環境.....	324
11.4.2 構成定義ファイルの編集.....	324
(1) Device Manager がサポートしている構成定義ファイルのパラメーター.....	325
(2) 構成定義ファイルの記述規則.....	326
(3) HORCM_MON パラメーターの記述形式.....	327
(4) HORCM_CMD パラメーターの記述形式.....	328
(5) HORCM_DEV パラメーターの記述形式.....	330
(6) HORCM_LDEV パラメーターの記述形式.....	331
(7) HORCM_INST パラメーターの記述形式.....	333
(8) HORCM_INSTP パラメーターの記述形式.....	334
11.4.3 構成定義ファイルの格納場所の変更.....	336
11.4.4 構成定義ファイルを利用する上での注意事項.....	337
11.5 Device Manager エージェントのリモートインストール.....	338
11.5.1 Device Manager エージェントをリモートインストールするための操作フロー.....	338
11.5.2 Device Manager エージェントをリモートインストールする場合のシステム構成.....	338
11.5.3 Device Manager エージェントのパッケージング (Windows)	339
11.5.4 Device Manager エージェントのパッケージング (UNIX)	340
11.5.5 Device Manager エージェントの配布指令の作成, 登録および実行 (Windows)	341
11.5.6 Device Manager エージェントの配布指令の作成, 登録および実行 (Solaris)	341
11.5.7 リモートインストールの実行結果の戻り値.....	342
12. Host Data Collector のセットアップ.....	345
12.1 Host Data Collector のインストール	346
12.1.1 Host Data Collector のインストール条件.....	346
12.1.2 Host Data Collector のインストール (Windows)	346
12.1.3 Host Data Collector のインストール (Solaris または Linux)	347
12.1.4 Host Data Collector を運用する場合の注意事項.....	348
12.1.5 管理サーバへの Host Data Collector マシンの登録.....	349
12.2 Host Data Collector の環境設定.....	350
12.2.1 Host Data Collector の常駐プロセス.....	350
(1) サービスの起動 (Host Data Collector)	351
(2) サービスの停止 (Host Data Collector)	351
(3) サービスの稼働状態の確認 (Host Data Collector)	352
12.2.2 Host Data Collector のファイアウォールへの例外登録 (Windows)	352
(1) Host Data Collector のサービスの例外登録 (非 SSL 通信用)	352
(2) Host Data Collector のサービスの例外登録 (SSL 通信用)	353
12.2.3 Host Data Collector で使用する Java の実行環境の変更.....	354
12.2.4 Host Data Collector マシンに複数の IP アドレスがある場合の設定.....	355
12.2.5 Host Data Collector のバージョンの確認.....	355
12.3 Host Data Collector のアンインストール.....	355
12.3.1 Host Data Collector のアンインストール (Windows)	355
12.3.2 Host Data Collector のアンインストール (Solaris または Linux)	356
13. トラブルシューティング.....	357
13.1 一般的な問題と解決策.....	358
13.1.1 管理サーバで発生したトラブルへの対処方法 (Device Manager)	358
(1) Device Manager の GUI にログインできない.....	358
(2) Hitachi Command Suite 共通コンポーネントまたは Device Manager サーバのサービスを起動で きない.....	358
(3) 管理サーバの起動後や Hitachi Command Suite 製品のサービスの起動後に Device Manager サー バにアクセスできない.....	359
(4) Hitachi Virtual File Platform の SNMP トラップを受信できない.....	359

(5) ストレージシステムの構成変更やリフレッシュがエラー終了した.....	360
13.1.2 管理サーバで発生したトラブルへの対処方法 (Tiered Storage Manager)	360
(1) Tiered Storage Manager サーバの起動に失敗した.....	360
(2) Tiered Storage Manager サーバが停止しない.....	361
(3) Tiered Storage Manager サーバで異常終了したりクラスタ環境でフェールオーバーが発生した りする.....	361
(4) データベースに障害が発生し Tiered Storage Manager の操作ができない.....	362
13.1.3 ホストで発生したトラブルへの対処方法.....	363
(1) HiScan コマンドを実行しても、Device Manager サーバにホスト情報を登録できない.....	363
(2) 通信エラーが発生して、ほかの Hitachi Command Suite 製品の処理が停止した.....	363
(3) [プログラムと機能] 画面に [HBase Agent] が2つ表示されている.....	364
(4) [プログラムと機能] 画面に [HBase Agent] が残っている.....	364
(5) JavaVM が異常終了する.....	364
(6) ホストで OutOfMemory エラーが発生し、しばらく時間が経過しても応答がない.....	364
(7) Device Manager の GUI にファイルシステム名が表示されない.....	365
(8) ストレージシステムの構成変更が Device Manager サーバに反映されない.....	366
(9) Device Manager エージェントの機能が使用できない.....	366
(10) 対処不要なエラー.....	366
13.2 トラブル発生時に採取が必要な保守情報.....	367
13.2.1 管理サーバの保守情報の取得 (hcmdsgetlogs コマンド)	368
13.2.2 Host Data Collector マシンの保守情報の取得 (hdc_gettras コマンド)	370
13.2.3 Host Data Collector 管理対象ホストの保守情報の取得 (hdc_target_gettras コマンド)	370
13.2.4 Device Manager エージェントの保守情報の取得 (TIC コマンド)	371
13.2.5 HBase Storage Mgmt Common Service のスレッドダンプ取得 (Windows)	372
13.2.6 HCS Device Manager Web Service のスレッドダンプ取得 (Windows)	373
13.2.7 HBase Storage Mgmt Common Service のスレッドダンプ取得 (Solaris または Linux)	373
13.2.8 HCS Device Manager Web Service のスレッドダンプ取得 (Solaris または Linux)	374
13.3 監査ログの確認.....	374
13.3.1 監査ログのメッセージテキスト.....	376
(1) Hitachi Command Suite 共通コンポーネントの処理として出力される場合.....	376
(2) Device Manager サーバの処理として出力される場合.....	377
(3) 関連製品の起動情報として出力される場合.....	377
(4) Device Manager サーバ (CIM 経由) の処理として出力される場合.....	379
(5) Tiered Storage Manager の処理として出力される場合.....	380
13.3.2 Device Manager サーバリクエスト受理詳細メッセージ.....	385
(1) 詳細メッセージに出力されるコマンド.....	386
(2) 詳細メッセージに出力されるターゲット.....	386
(3) 詳細メッセージに出力されるオプション.....	387
(4) 詳細メッセージに出力されるパラメーター.....	389
13.3.3 Tiered Storage Manager のユーザー操作と監査ログの対応.....	403
(1) GUI 操作と監査ログの対応.....	403
(2) CLI 操作と監査ログの対応.....	405
付録 A Device Manager サーバのプロパティ.....	409
A.1 Device Manager サーバのプロパティファイル.....	411
A.1.1 Device Manager サーバのプロパティの変更.....	412
A.1.2 Device Manager サーバのプロパティファイルの記述規則.....	412
A.2 Device Manager サーバの構成情報に関するプロパティ (server.properties ファイル)	412
A.2.1 server.http.host.....	413
A.2.2 server.http.port.....	413
A.2.3 server.https.port.....	414
A.2.4 server.rmi.port.....	414
A.2.5 server.http.entity.maxLength.....	415
A.2.6 server.base.home.....	415
A.2.7 server.horcmconfigfile.hostname.....	415

A.2.8	server.base.initialsynchro	415
A.2.9	server.cim.agent	416
A.2.10	server.cim.support	416
A.2.11	server.cim.support.job	416
A.2.12	server.cim.support.protocol	416
A.2.13	server.cim.http.port	416
A.2.14	server.cim.https.port	417
A.2.15	server.configchange.enabled	417
A.2.16	server.logicalview.initialsynchro	417
A.2.17	server.mail.enabled	418
A.2.18	server.mail.from	418
A.2.19	server.mail.smtp.host	418
A.2.20	server.mail.smtp.port	418
A.2.21	server.mail.smtp.auth	419
A.2.22	server.mail.errorsTo	419
A.2.23	server.eventNotification.mail.to	419
A.2.24	server.mail.alert.type	419
A.2.25	server.mail.alert.status	420
A.2.26	server.subsystem.ssid.availableValues	420
A.2.27	server.smisclient.indication.port	420
A.2.28	server.agent.differentialrefresh.manual.enabled	420
A.2.29	server.agent.differentialrefresh.periodical.enabled	421
A.2.30	server.logicalGroupMapping.updateInterval	421
A.3	Device Manager のデータベースに関するプロパティ (database.properties ファイル)	421
A.3.1	dbm.traceSQL	421
A.3.2	dbm.startingCheck.retryCount	422
A.3.3	dbm.startingCheck.retryPeriod	422
A.4	Device Manager のログ出力に関するプロパティ (logger.properties ファイル)	422
A.4.1	logger.loglevel	422
A.4.2	logger.MaxBackupIndex	422
A.4.3	logger.MaxFileSize	423
A.4.4	logger.hicommandbase.loglevel	423
A.4.5	logger.hicommandbase.sysloglevel	423
A.4.6	logger.hicommandbase.MaxBackupIndex	424
A.4.7	logger.hicommandbase.MaxFileSize	424
A.5	Device Manager のスレッドに関するプロパティ (dispatcher.properties ファイル)	424
A.5.1	server.dispatcher.message.timeout	424
A.5.2	server.dispatcher.message.timeout.in.processing	425
A.5.3	server.dispatcher.daemon.pollingPeriod	425
A.5.4	server.dispatcher.traps.purgePeriod	425
A.5.5	server.dispatcher.daemon.receiveTrap	425
A.5.6	server.dispatcher.snm2.configchange.pollingPeriod	425
A.5.7	server.dispatcher.configchange.pollingPeriod	426
A.5.8	server.dispatcher.daemon.configUpdate.detection.interval	426
A.5.9	server.dispatcher.daemon.autoSynchro.doRefresh	427
A.5.10	server.dispatcher.daemon.autoSynchro.type	427
A.5.11	server.dispatcher.daemon.autoSynchro.dayOfWeek	428
A.5.12	server.dispatcher.daemon.autoSynchro.startTime	428
A.5.13	server.dispatcher.daemon.autoSynchro.interval	428
A.5.14	server.dispatcher.daemon.configUpdate.detection.variable.enabled	429
A.5.15	server.dispatcher.daemon.autoSynchro.performance.doRefresh	430
A.5.16	server.dispatcher.daemon.autoSynchro.performance.startTime	430
A.5.17	server.dispatcher.daemon.autoSynchro.logicalGroup.doRefresh	430
A.6	Device Manager の MIME に関するプロパティ (mime.properties ファイル)	431
A.7	Device Manager の GUI に関するプロパティ (client.properties ファイル)	431
A.7.1	client.rmi.port	431

A.7.2 client.migration.use.legacymode.....	432
A.8 Device Manager のセキュリティに関するプロパティ.....	432
A.9 Device Manager の SNMP トラップのログ出力に関するプロパティ (customizedsnmptrap.properties ファイル)	432
A.9.1 customizedsnmptrap.customizedSNMPTrapEnable.....	433
A.9.2 customizedsnmptrap.customizelist.....	433
A.10 Device Manager からラUNCHするアプリケーションに関するプロパティ (launchapp.properties ファイル)	434
A.10.1 launchapp.snm2.url.....	435
A.10.2 launchapp.snm2.rmi.port.....	435
A.10.3 launchapp.elementmanager.role.mode.....	435
A.10.4 launchapp.elementmanager.usehostname.....	436
A.11 ホストとの通信に関するプロパティ (host.properties ファイル)	436
A.11.1 host.mf.agent.connection.timeout.....	436
A.11.2 host.agent.access.timeoutForRpm.....	436
A.12 Host Data Collector との連携に関するプロパティ (hostdatacollectors.properties ファイル)	436
A.12.1 hdc.request.timeout.....	437
A.12.2 hdc.rmiregistry.....	437
A.12.3 hdc.rmserver.....	438
A.12.4 hdc.classloader.....	438
A.12.5 hdc.usessl.....	439
A.13 マイグレーションに関するプロパティ (migration.properties ファイル)	439
A.13.1 migration.dataErase.defaultValue.....	439
A.13.2 migration.plan.candidateVolumeCountLimit.....	440
A.13.3 migration.plan.candidateCapacityGroupDisplayMaxCount.....	440
A.13.4 migration.multiExecution.....	440
A.14 Tuning Manager との連携に関するプロパティ (tuningmanager.properties ファイル)	440
A.14.1 htnm.infoAcquirePeriod.....	441
A.14.2 htnm.servers.....	441
A.14.3 htnm.server <i>n</i> .host.....	441
A.14.4 htnm.server <i>n</i> .protocol.....	442
A.14.5 htnm.server <i>n</i> .port.....	442
A.14.6 htnm.flashMode.....	442
A.14.7 hdvm.analytics.disabled.....	442
A.14.8 hdvm.analytics.healthcheck.excludeMainframe.....	442
A.14.9 hdvm.analytics.healthcheck.notification.exportreport.locale.....	443
A.15 Universal Replicator の性能分析に関するプロパティ (replication.properties ファイル)	443
A.15.1 server.dispatcher.daemon.replication.config.doUpdate.....	443
A.15.2 server.dispatcher.daemon.replication.config.updateInterval.....	444
A.15.3 server.dispatcher.daemon.replication.config.offset.....	444
A.15.4 server.dispatcher.daemon.replication.config.minute.....	445
A.15.5 server.dispatcher.daemon.replication.performance.rpm.updateInterval.....	445
A.15.6 server.dispatcher.daemon.replication.performance.tnm.updateInterval.....	445
A.15.7 server.dispatcher.daemon.replication.performance.tnm.offset.....	445
A.15.8 server.dispatcher.daemon.replication.performance.tnm.minute.....	446
A.15.9 hdvm.replication.disabled.....	446
A.16 Replication Manager との連携に関するプロパティ (rpmlib.properties ファイル)	447
A.16.1 rpmlib.rpm.port.....	447
A.17 CIM/WBEM 機能に関するプロパティ (jserver.properties ファイル, cimxmlcpa.properties ファイル, cimxmlscpa.properties ファイル)	447
A.17.1 com.wbemsolutions.jserver.bindto.....	448
A.17.2 HTTPPort.....	448
A.17.3 HTTPSPort.....	448

付録 B Tiered Storage Manager サーバのプロパティ	449
B.1 Tiered Storage Manager サーバのプロパティファイル	450
B.1.1 Tiered Storage Manager サーバのプロパティの変更	450
B.1.2 Tiered Storage Manager サーバのプロパティファイルの記述規則	451
B.2 Tiered Storage Manager サーバの動作に関するプロパティ (server.properties ファイル)	451
B.2.1 server.rmi.secure	451
B.2.2 server.rmi.port	452
B.2.3 server.rmi.security.port	452
B.2.4 server.base.initialsynchro	453
B.2.5 server.mail.smtp.host	453
B.2.6 server.mail.from	453
B.2.7 server.mail.errorsTo	453
B.2.8 server.mail.smtp.port	453
B.2.9 server.mail.smtp.auth	454
B.2.10 server.eventNotification.mail.to	454
B.2.11 server.eventMonitoringIntervallnMinute	454
B.2.12 server.migration.multiExecution	454
B.2.13 server.checkOutVolumeRange	454
B.2.14 server.migration.dataErase.defaultValue	454
B.2.15 server.migrationPlan.candidateVolumeCountLimit	455
B.2.16 server.migrationPlan.candidateCapacityGroupDisplayMaxCount	455
B.2.17 server.migration.maxRetryCount	455
B.3 Tiered Storage Manager の GUI に関するプロパティ (client.properties ファイル)	456
B.3.1 client.ldev.rowsperpage.retain.enabled	456
B.4 Tiered Storage Manager のデータベースに関するプロパティ (database.properties ファイル)	456
B.4.1 dbm.traceSQL	456
B.5 Tiered Storage Manager から Device Manager サーバへのアクセスに関するプロパティ (devicemanager.properties ファイル)	457
B.5.1 hdvm.protocol	457
B.5.2 hdvm.port	457
B.5.3 hdvm.timeout	457
B.5.4 hdvm.rmi.port	457
B.6 Tiered Storage Manager のログ出力に関するプロパティ (logger.properties ファイル)	458
B.6.1 logger.messageLogLevel	458
B.6.2 logger.traceLogLevel	459
B.6.3 logger.syslogLevel	459
B.6.4 logger.serverMessageFileCount	459
B.6.5 logger.serverTraceFileCount	460
B.6.6 logger.guiMessageFileCount	460
B.6.7 logger.guiTraceFileCount	460
B.6.8 logger.serverMessageMaxFileSize	461
B.6.9 logger.serverTraceMaxFileSize	461
B.6.10 logger.guiMessageMaxFileSize	461
B.6.11 logger.guiTraceMaxFileSize	461
B.7 Tiered Storage Manager のセキュリティに関するプロパティ	462
付録 C Host Data Collector のプロパティ	463
C.1 Host Data Collector のプロパティファイル	464
C.1.1 Host Data Collector のプロパティの変更	464
C.2 Host Data Collector の動作に関するプロパティ (hdcbase.properties ファイル)	464
C.2.1 hdc.service.localport	465
C.2.2 hdc.adapter.adapterProcessNum	465
C.2.3 hdc.adapter.localport	465
C.2.4 hdc.common.rmi.registryPort	465

C.2.5	hdc.common.rmi.serverPort.....	466
C.2.6	hdc.common.http.serverPort.....	466
C.2.7	hdc.common.rmi.ssl.registryPort.....	466
C.2.8	hdc.common.rmi.ssl.serverPort.....	467
C.2.9	hdc.common.https.serverPort.....	467
C.2.10	hdc.service.rmi.registryIPAddress.....	467
C.2.11	hdc.service.fileCleanup.startTime.....	468
C.2.12	hdc.adapter.esx.timeout.....	468
C.2.13	hdc.ssl.secure.....	468
C.3	Host Data Collector のログ出力に関するプロパティ (logger.properties ファイル)	469
C.3.1	logger.trace.level.....	469
C.3.2	logger.trace.maxFileSize.....	470
C.3.3	logger.trace.numOfFiles.....	470
C.3.4	logger.iotrace.maxFileSize.....	470
C.3.5	logger.iotrace.numOfFiles.....	470
C.4	Host Data Collector の Java 環境に関するプロパティ (javaconfig.properties ファイル)	471
C.4.1	javapathlocation.....	471
付録 D	Device Manager エージェントのプロパティ	473
D.1	Device Manager エージェントのプロパティファイル.....	474
D.1.1	Device Manager エージェントのプロパティの変更.....	474
D.2	Device Manager エージェントと Replication Manager サーバとの連携に関するプロパティ (agent.properties ファイル)	474
D.2.1	agent.rm.TimeOut.....	475
D.2.2	agent.rm.everytimeShutdown.....	475
D.2.3	agent.rm.shutdownWait.....	475
D.2.4	agent.rm.horcmInstance.....	475
D.2.5	agent.rm.horcmService.....	476
D.2.6	agent.logger.loglevel.....	476
D.2.7	agent.logger.MaxBackupIndex.....	476
D.2.8	agent.logger.MaxFileSize.....	477
D.3	Device Manager エージェントの hldutil コマンドの動作に関するプロパティ (hldutil.properties ファイル)	477
D.3.1	agent.util.hpux.displayDsf.....	477
D.4	Device Manager エージェントのログ出力に関するプロパティ (logger.properties ファイル)	478
D.4.1	logger.loglevel.....	478
D.4.2	logger.MaxBackupIndex.....	478
D.4.3	logger.MaxFileSize.....	479
D.5	Device Manager エージェントのプログラム情報に関するプロパティ (programproductinfo.properties ファイ ル)	479
D.5.1	veritas.volume.manager.version.....	480
D.6	Device Manager エージェントの動作に関するプロパティ (server.properties ファイル)	480
D.6.1	server.agent.port.....	480
D.6.2	server.http.localPort.....	480
D.6.3	server.http.port.....	481
D.6.4	server.http.host.....	481
D.6.5	server.http.socket.agentAddress.....	481
D.6.6	server.http.socket.bindAddress.....	481
D.6.7	server.agent.maxMemorySize.....	482
D.6.8	server.agent.shutDownTime.....	482
D.6.9	server.agent.JRE.location.....	482
D.6.10	server.http.entity.maxLength.....	483
D.6.11	server.http.security.clientIP.....	483
D.6.12	server.server.authorization.....	483
D.6.13	server.server.serverIPAddress.....	483

D.6.14 server.server.serverPort.....	484
D.6.15 server.agent.rm.centralizePairConfiguration.....	484
D.6.16 server.agent.rm.cuLdevForm.....	484
D.6.17 server.agent.rm.exclusion.instance.....	485
D.6.18 server.agent.rm.location.....	485
D.6.19 server.agent.rm.optimization.userHorcmFile.....	485
D.6.20 server.agent.rm.horcm.poll.....	486
D.6.21 server.agent.rm.temporaryInstance.....	486
D.6.22 server.agent.rm.temporaryPort.....	486
D.6.23 server.agent.rm.pairDefinitionForm.....	487
D.6.24 server.agent.rm.userAuthentication.....	488
D.6.25 server.agent.rm.ignorePairStatus.....	488
D.6.26 server.agent.rm.horcmSource.....	488
D.6.27 server.agent.rm.moduleTimeOut.....	489
D.6.28 server.http.server.timeOut.....	489
D.6.29 server.util.processTimeOut.....	489
D.6.30 server.agent.evtwait.timeout.....	490
D.6.31 server.agent.rmxp.location.....	490
付録 E このマニュアルの参考情報.....	491
E.1 関連マニュアル.....	492
E.2 このマニュアルでの表記.....	492
E.3 このマニュアルで使用している略語.....	498
E.4 KB（キロバイト）などの単位表記について.....	501
索引.....	503

目次

図 1-1 基本的なシステム構成.....	30
図 1-2 最もセキュアな構成：管理用の LAN を分離し、ファイアウォールを設置した場合.....	34
図 1-3 2 番目にセキュアな構成：管理用の LAN を分離し、管理下のデバイスとの間にファイアウォールを設置した場合.....	35
図 1-4 3 番目にセキュアな構成：管理用の LAN を分離し、管理サーバをデュアルホームにした場合の構成.....	36
図 1-5 最もセキュアでない構成：フラットネットワーク.....	37
図 1-6 仮想マシンの前提環境（Host Data Collector で管理する場合）.....	46
図 1-7 仮想マシンの前提環境（Device Manager エージェントで管理する場合）.....	48
図 1-8 仮想マシンにボリュームを割り当てるための操作フロー（仮想マシンごとに HBA が割り当てられている構成）.....	49
図 1-9 仮想マシンにボリュームを割り当てるための操作フロー（複数の仮想マシンで HBA を共有している構成）.....	50
図 1-10 仮想マシンにボリュームを割り当てるための操作フロー（仮想マシンごとに仮想 HBA が割り当てられている構成）.....	51
図 1-11 仮想化サーバの前提環境（Host Data Collector で管理する場合）.....	54
図 1-12 仮想化サーバの前提環境（vMA を使用する場合）.....	55
図 1-13 vMA で同じ物理環境の VMware ESX を監視する場合のシステム構成.....	56
図 1-14 vMA で別の物理環境の VMware ESX を監視する場合のシステム構成.....	56
図 1-15 vMA で VMware vCenter Server を監視する場合のシステム構成.....	57
図 1-16 仮想化サーバを管理対象にするための操作フロー.....	58
図 1-17 メインフレームホストを管理対象にするための操作フロー.....	59
図 1-18 Hitachi NAS Platform の前提環境.....	60
図 1-19 ファイルサーバを管理対象にするための操作フロー.....	62
図 1-20 コピーペア管理のシステム構成例（通常構成）.....	66
図 1-21 コピーペア管理のシステム構成例（一括管理構成）.....	69
図 1-22 コピーペア管理のシステム構成例（仮想コマンドデバイスサーバ構成）.....	71
図 1-23 コピーペア管理のシステム構成例（構成定義ファイルでコピーペアを定義した場合）.....	74
図 1-24 コピーペア管理のシステム構成例（デバイスグループとしてコピーペアを定義した場合）.....	76
図 2-1 管理サーバのブリッジ機能を使用したネットワークの構成例.....	107
図 5-1 ストレージシステムの性能情報を収集するためのシステム構成例.....	135
図 5-2 Device Manager サーバを設定するための操作フロー（ストレージシステムの性能情報の収集）.....	140
図 5-3 プライマリーサイトの Device Manager サーバに接続して性能分析する場合のシステム構成例.....	150
図 7-1 Device Manager の CIM コンポーネント.....	188
図 7-2 ストレージシステムの性能情報を収集する場合のシステム構成例.....	193
図 11-1 リモートインストールの流れ.....	338
図 11-2 JP1/NETM/DM を使用するためのシステム構成.....	339
図 B-1 出力レベルのしきい値に指定した値と出力されるメッセージの関係.....	458

表目次

表 1-1 管理リソース数の上限値.....	37
表 1-2 Hitachi Command Suite 共通コンポーネントのメモリーヒープサイズの目安.....	38
表 1-3 Device Manager サーバのメモリーヒープサイズの目安.....	39
表 1-4 Device Manager で管理できるホスト.....	42
表 1-5 Device Manager のホスト管理ソフトウェア.....	42
表 1-6 Hitachi File Services Manager のインストール条件.....	61
表 1-7 Device Manager でコピーペアを管理できるストレージシステム.....	64
表 1-8 コピーペアを管理するためのストレージシステムの要件.....	78
表 1-9 GUI でコピーペアを管理する場合の Device Manager エージェントの要件.....	81
表 1-10 CLI でコピーペアを管理するための Device Manager エージェントの要件.....	81
表 1-11 CLI でコピーペアを管理する場合のストレージシステムごとの Device Manager エージェントの要件.....	82
表 2-1 Hitachi Command Suite 共通コンポーネントで使用されるポート.....	86
表 2-2 Device Manager サーバで使用されるポート.....	87
表 2-3 Tiered Storage Manager サーバで使用されるポート.....	88
表 2-4 Host Data Collector で使用されるポート.....	89
表 2-5 Device Manager エージェントで使用されるポート.....	90
表 2-6 ストレージシステムで使用されるポート.....	90
表 2-7 Hitachi Command Suite 共通コンポーネントのポート番号設定ファイル.....	93
表 2-8 管理サーバと管理クライアントとの間のファイアウォールで例外登録が必要なポート番号.....	97
表 2-9 管理サーバとストレージシステムとの間のファイアウォールで例外登録が必要なポート番号.....	97
表 2-10 管理クライアントとストレージシステムとの間のファイアウォールで例外登録が必要なポート番号.....	98
表 2-11 管理サーバと通常ホストとの間のファイアウォールで例外登録が必要なポート番号.....	99
表 2-12 管理サーバと仮想化サーバとの間のファイアウォールで例外登録が必要なポート番号.....	100
表 2-13 管理サーバとメインフレームホストとの間のファイアウォールで例外登録が必要なポート番号.....	100
表 2-14 管理サーバとファイルサーバとの間のファイアウォールで例外登録が必要なポート番号.....	100
表 2-15 Device Manager の管理サーバと Tuning Manager の管理サーバとの間のファイアウォールで例外登録が必要なポート番号.....	101
表 2-16 管理サーバと Host Data Collector をインストールしたマシンとの間のファイアウォールで例外登録が必要なポート番号.....	101
表 2-17 Host Data Collector をインストールしたマシンとホストとの間のファイアウォールで例外登録が必要なポート番号.....	102
表 2-18 管理サーバと SMI-S プロバイダーとの間のファイアウォールで例外登録が必要なポート番号.....	102
表 2-19 管理サーバと CIM クライアントとの間のファイアウォールで例外登録が必要なポート番号.....	103
表 2-20 管理サーバとメールサーバとの間のファイアウォールで例外登録が必要なポート番号.....	103
表 2-21 管理サーバと外部認証サーバとの間のファイアウォールで例外登録が必要なポート番号.....	104
表 2-22 netsh コマンドで指定する例外登録名とパス.....	105
表 3-1 security.conf ファイルで指定できるパスワードポリシー.....	118

表 3-2 security.conf ファイルで指定できるアカウントロックポリシー.....	120
表 5-1 ヘルスチェックを実行するためのレコードの保存期間（エンタープライズクラスストレージおよび HUS VM の場合）.....	138
表 5-2 ヘルスチェックを実行するためのレコードの保存期間（ミッドレンジストレージの場合）.....	139
表 6-1 HtsmgetTL.properties ファイルで設定するプロパティ.....	157
表 6-2 監査ログの種別と説明.....	158
表 6-3 監査ログに出力される監査事象（種別が StartStop の場合）.....	159
表 6-4 監査ログに出力される監査事象（種別が Authentication の場合）.....	159
表 6-5 監査ログに出力される監査事象（種別が ConfigurationAccess の場合）.....	159
表 6-6 監査ログに出力される監査事象（種別が AccessControl の場合）.....	165
表 6-7 監査ログに出力される監査事象（種別が ExternalService の場合）.....	166
表 6-8 auditlog.conf ファイルに設定する項目.....	167
表 6-9 Log.Facility に指定できる値と syslog.conf での指定値の対応.....	168
表 6-10 監査事象の重要度、syslog.conf の重要度、およびイベントログの種類の対応.....	168
表 6-11 Device Manager で表示できるアラート.....	169
表 6-12 mail-alert-detection.txt ファイルに指定できるパラメーター.....	174
表 6-13 メールで通知できる Tiered Storage Manager のイベント.....	176
表 6-14 イベント通知メールのテンプレート.....	177
表 6-15 タスク終了イベントのパラメーター（[データマイグレーション] ウィザードで作成するマイグレーションタスク）.....	180
表 6-16 タスク終了イベントのパラメーター（Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI で作成するタスク）.....	180
表 6-17 時間経過イベントのパラメーター.....	181
表 7-1 ネームスペースおよび SMI-S のバージョンの対応.....	190
表 7-2 Device Manager でのロールと実行できる CIM メソッドの対応.....	190
表 7-3 性能情報を収集する場合の RAID Manager LIB の前提バージョン.....	194
表 7-4 perf_cmddev.properties ファイルの設定項目.....	197
表 8-1 管理サーバの環境ごとのセットアップ方法.....	204
表 8-2 HiRDB をリソースとして登録するための設定（Microsoft Cluster Service の場合）.....	210
表 8-3 HBase Storage Mgmt Common Service をリソースとして登録するための設定（Microsoft Cluster Service の場合）.....	210
表 8-4 HBase Storage Mgmt Web Service をリソースとして登録するための設定（Microsoft Cluster Service の場合）.....	210
表 8-5 HCS Device Manager Web Service をリソースとして登録するための設定（Microsoft Cluster Service の場合）.....	211
表 8-6 HiCommandServer をリソースとして登録するための設定（Microsoft Cluster Service の場合）.....	211
表 8-7 Tiered Storage Manager サーバをリソースとして登録するための設定（Microsoft Cluster Service の場合）.....	211
表 8-8 HiRDB/ClusterService_HD0 のプロパティの設定（Windows Server Failover Clustering の場合）.....	212
表 8-9 HBase Storage Mgmt Common Service のプロパティの設定（Windows Server Failover Clustering の場合）.....	212
表 8-10 HBase Storage Mgmt Web Service のプロパティの設定（Windows Server Failover Clustering の場合）.....	213
表 8-11 HCS Device Manager Web Service のプロパティの設定（Windows Server Failover Clustering の場合）.....	213
表 8-12 HiCommandServer のプロパティの設定（Windows Server Failover Clustering の場合）.....	213
表 8-13 HiCommand Tiered Storage Manager のプロパティの設定（Windows Server Failover Clustering の場合）.....	213
表 8-14 HiRDB をリソースとして登録するための設定.....	232
表 8-15 HBase Storage Mgmt Common Service をリソースとして登録するための設定.....	232
表 8-16 HBase Storage Mgmt Web Service をリソースとして登録するための設定.....	233
表 8-17 HCS Device Manager Web Service をリソースとして登録するための設定.....	233
表 8-18 HiCommandServer をリソースとして登録するための設定.....	233
表 8-19 Tiered Storage Manager サーバをリソースとして登録するための設定.....	233
表 8-20 HiRDB をリソースとして登録するためのパラメーターと設定値.....	235
表 8-21 HBase Storage Mgmt Common Service をリソースとして登録するためのパラメーターと設定値.....	235

表 8-22 HBase Storage Mgmt Web Service をリソースとして登録するためのパラメーターと設定値.....	236
表 8-23 HCS Device Manager Web Service をリソースとして登録するためのパラメーターと設定値.....	236
表 8-24 HiCommandServer をリソースとして登録するためのパラメーターと設定値.....	237
表 8-25 HiCommand Tiered Storage Manager をリソースとして登録するためのパラメーターと設定値.....	237
表 9-1 常駐プロセス (Windows の場合)	250
表 9-2 常駐プロセス (Solaris または Linux の場合)	250
表 10-1 バックアップ・復元とエクスポート・インポートの違い.....	256
表 10-2 データベースを復元する場合の type オプションの指定値 (非クラスタ構成の場合)	264
表 10-3 データベースを復元する場合の type オプションの指定値 (Microsoft Cluster Service または Windows Server Failover Clustering の場合)	266
表 10-4 データベースを復元する場合の type オプションの指定値 (Veritas Cluster Server の場合)	268
表 10-5 データベースを復元する場合の type オプションの指定値 (Sun Cluster の場合)	270
表 10-6 データベースを移行する場合の type オプションの指定値 (非クラスタ構成の場合)	289
表 10-7 データベースを移行する場合の type オプションの指定値 (Microsoft Cluster Service または Windows Server Failover Clustering の場合)	291
表 10-8 データベースを移行する場合の type オプションの指定値 (Veritas Cluster Server の場合)	295
表 10-9 データベースを移行する場合の type オプションの指定値 (Sun Cluster の場合)	297
表 11-1 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (ボリュームマネージャーを使用していないと き)	309
表 11-2 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (Windows 環境でボリュームマネージャーを使 用しているとき)	310
表 11-3 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (Solaris 環境でボリュームマネージャーを使 用しているとき)	310
表 11-4 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (AIX 環境でボリュームマネージャーを使 用しているとき)	311
表 11-5 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (Linux 環境でボリュームマネージャーを使 用しているとき)	311
表 11-6 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (HP-UX 環境でボリュームマネージャーを使 用しているとき)	311
表 11-7 Device Manager エージェントの常駐プロセス (Windows)	312
表 11-8 Device Manager エージェントの常駐プロセス (UNIX)	312
表 11-9 hdvmagt_setting コマンドで設定する情報.....	316
表 11-10 hldutil コマンドで表示される情報.....	322
表 11-11 hldutil コマンドで表示される RaidID とストレージシステムの機種種の対応.....	323
表 11-12 hldutil コマンドで指定できるソートキー.....	324
表 11-13 HORCM_MON パラメーターの ip_address に指定できる値.....	327
表 11-14 HORCM_MON パラメーターの記述形式のサポート状況.....	328
表 11-15 HORCM_CMD パラメーターの記述形式のサポート状況.....	329
表 11-16 HORCM_DEV パラメーターの記述形式のサポート状況.....	331
表 11-17 HORCM_LDEV パラメーターの記述形式のサポート状況.....	333
表 11-18 HORCM_INST パラメーターの ip_address に指定できる値.....	334
表 11-19 HORCM_INST パラメーターの記述形式のサポート状況.....	334
表 11-20 HORCM_INSTP パラメーターの ip_address に指定できる値.....	335
表 11-21 HORCM_INSTP パラメーターの記述形式のサポート状況.....	336
表 11-22 リモートインストールの実行結果の戻り値.....	343
表 12-1 Host Data Collector のインストール中に入力する情報.....	346
表 12-2 Host Data Collector の常駐プロセス (Windows)	350
表 12-3 Host Data Collector の常駐プロセス (Solaris または Linux)	350
表 13-1 保守情報を取得する場合の type オプションの指定値.....	369
表 13-2 メッセージ部に出力される情報.....	375
表 13-3 Device Manager サーバリクエスト受理時またはレスポンス送信時に出力される情報.....	377

表 13-4 ラウンチリクエスト受理時またはレスポンス送信時に出力される情報.....	378
表 13-5 ラウンチセッション ID の有無とラウンチ識別子の内容.....	378
表 13-6 Device Manager サーバ (CIM 経由) リクエスト受理時またはレスポンス送信時に出力される情報.....	379
表 13-7 監査ログのメッセージテキストに出力される項目 (メッセージ本文, 操作種別および操作対象)	380
表 13-8 監査ログのメッセージテキストに出力される項目 (追加情報)	381
表 13-9 監査ログに出力されるメッセージ.....	383
表 13-10 監査ログに出力される操作種別 (OP) の意味.....	384
表 13-11 監査ログに出力される操作対象 (Res) の意味.....	384
表 13-12 詳細メッセージに出力される情報.....	385
表 13-13 詳細メッセージに出力されるコマンド.....	386
表 13-14 詳細メッセージに出力されるターゲット.....	386
表 13-15 詳細メッセージに出力されるオプション.....	387
表 13-16 詳細メッセージに出力されるパラメーターの情報.....	390
表 13-17 エレメントの内容と対応する属性値の出力順.....	390
表 13-18 ストレージシステム種別 共通出力名称一覧.....	403
表 13-19 レプリケーション操作種別属性 共通出力名称一覧.....	403
表 13-20 GUI 操作と, 監査ログに出力される主要情報の対応.....	404
表 13-21 CLI コマンドと, 監査ログに出力される情報の対応.....	406
表 A-1 Device Manager サーバのプロパティファイル.....	411
表 A-2 customizedsnmptrap.customizelist プロパティで指定する項目.....	433
表 B-1 Tiered Storage Manager サーバのプロパティファイル.....	450
表 B-2 メッセージログの出力レベル.....	458
表 B-3 トレースログの出力レベル.....	459
表 C-1 Host Data Collector のプロパティファイル.....	464
表 C-2 hdc.ssl.secure プロパティの値とオープンするポート番号の対応.....	468
表 C-3 トレースログの出力レベル.....	469
表 D-1 Device Manager エージェントのプロパティファイル.....	474
表 D-2 Device Manager エージェントが構成定義ファイルに記述する形式を決める条件.....	487



はじめに

このマニュアルは、Hitachi Device Manager、Hitachi Tiered Storage Manager および Hitachi Command Suite 共通コンポーネントのシステム構成、環境設定およびトラブルシューティングについて説明したものです。

以降、このマニュアルでは、Hitachi Device Manager を Device Manager、Hitachi Tiered Storage Manager を Tiered Storage Manager と略します。

- 対象読者
- マニュアルの構成
- マイクロソフト製品の表記について
- このマニュアルで使用している記号

対象読者

このマニュアルは、Device Manager または Tiered Storage Manager を使用してシステムを運用管理される方を対象としています。また、対象読者には次のような知識があることを前提としています。

- ストレージシステム固有の管理ツールに関する基本的な知識
- SAN (Storage Area Network) に関する基本的な知識
- 前提 OS に関する基本的な知識
- 前提クラスタソフトウェアに関する基本的な知識

マニュアルの構成

このマニュアルは、次に示す章と付録から構成されています。

第 1 章 概要

Device Manager および Tiered Storage Manager を使用する場合のシステム構成とシステム要件について説明しています。

第 2 章 ネットワーク構成に応じた設定

ネットワーク構成に応じて必要な Hitachi Command Suite 製品での設定について説明しています。

第 3 章 ユーザーアカウントを管理するために必要な設定

Hitachi Command Suite 製品のユーザーアカウントを管理するために必要な設定について説明しています。

第 4 章 セキュリティ設定

Hitachi Command Suite 製品を運用する際に必要なセキュリティ設定について説明しています。

第 5 章 関連製品と連携するために必要な設定

関連製品と連携するために必要な設定について説明しています。

第 6 章 ログおよびアラートの設定

Hitachi Command Suite 製品でシステムの状態や障害を監視するために必要な設定について説明しています。

第 7 章 CIM/WBEM のセットアップ

CIM/WBEM のセットアップ方法について説明しています。

第 8 章 クラスタ環境でのセットアップ

クラスタ環境で運用する場合のセットアップ方法について説明しています。

第 9 章 サービスの起動と停止

管理サーバ上の Hitachi Command Suite 製品のサービスを起動したり停止したりする方法について説明しています。

第 10 章 データベースの管理

Hitachi Command Suite 製品のデータベースをバックアップしたり、復元したりする方法について説明しています。

第 11 章 Device Manager エージェントの運用

Device Manager エージェントを運用するために必要な設定や、Device Manager エージェントの操作について説明しています。

第 12 章 Host Data Collector のセットアップ

Host Data Collector のセットアップ方法について説明しています。

第 13 章 トラブルシューティング

Device Manager および Tiered Storage Manager の運用中に発生した問題の解決策やログファイルの参照方法について説明しています。

付録 A Device Manager サーバのプロパティ

Device Manager サーバのプロパティファイルについて説明しています。

付録 B Tiered Storage Manager サーバのプロパティ

Tiered Storage Manager サーバのプロパティファイルについて説明しています。

付録 C Host Data Collector のプロパティ

Host Data Collector のプロパティファイルについて説明しています。

付録 D Device Manager エージェントのプロパティ

Device Manager エージェントのプロパティファイルについて説明しています。

付録 E このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報について説明しています。

マイクロソフト製品の表記について

このマニュアルでは、マイクロソフト製品の名称を次のように表記しています。

表記	製品名
Active Directory	Microsoft® Active Directory
Hyper-V	Microsoft® Hyper-V®
Internet Explorer	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none">• Microsoft® Internet Explorer®• Windows® Internet Explorer®
Microsoft Cluster Service	Microsoft® Cluster Service
Windows	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none">• Microsoft® Windows® 7• Microsoft® Windows Server® 2003• Microsoft® Windows Server® 2003 R2• Microsoft® Windows Server® 2008• Microsoft® Windows Server® 2008 R2• Microsoft® Windows Server® 2012• Microsoft® Windows Server® 2012 R2• Microsoft® Windows Vista®• Microsoft® Windows® XP
Windows 7	Microsoft® Windows® 7
Windows Server 2003	Microsoft® Windows Server® 2003
Windows Server 2003 R2	Microsoft® Windows Server® 2003 R2

表記	製品名
Windows Server 2008	Microsoft® Windows Server® 2008
Windows Server 2008 R2	Microsoft® Windows Server® 2008 R2
Windows Server 2012	Microsoft® Windows Server® 2012
Windows Server 2012 R2	Microsoft® Windows Server® 2012 R2
Windows Server Failover Clustering	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> • Windows Server® Failover Clustering • Microsoft® Failover Cluster
Windows Vista	Microsoft® Windows Vista®
Windows XP	Microsoft® Windows® XP

このマニュアルで使用している記号

このマニュアルでは、次に示す記号を使用しています。

記号	意味と例
[] (角括弧)	画面、メニュー、ボタン、キーボードのキーなどを示します。 また、表示項目を連続して選択する場合には、[] を一でつないで説明しています。
< > (山括弧)	可変値であることを示します。

また、このマニュアルでは、次に示す記号を使用してコマンドの文法を説明しています。

記号	意味と例
 (ストローク)	複数の項目に対して項目間の区切りを示し、「または」の意味を示します。 (例) 「A B C」は、「A, B, または C」を示します。
{ } (波括弧)	この記号で囲まれている複数の項目の中から、必ず一組の項目を選択します。項目と項目の区切りは「 」で示します。 (例) 「{A B C}」は、「A, B, または C のどれかを必ず指定する」ことを示します。
[] (角括弧)	この記号で囲まれている項目は、任意に指定できます (省略できます)。 (例) 「[A]」は、「必要に応じて A を指定する」ことを示します (必要でない場合は、A を省略できます)。 「[B C]」は、「必要に応じて B, または C を指定する」ことを示します (必要でない場合は、B および C を省略できます)。
...点線 (リーダー)	記述が省略されていることを示します。この記号の直前に示された項目を繰り返し複数個指定できます。 (例) 「A,B,C...」は、「A と B の後ろに C を複数個指定できる」ことを示します。

概要

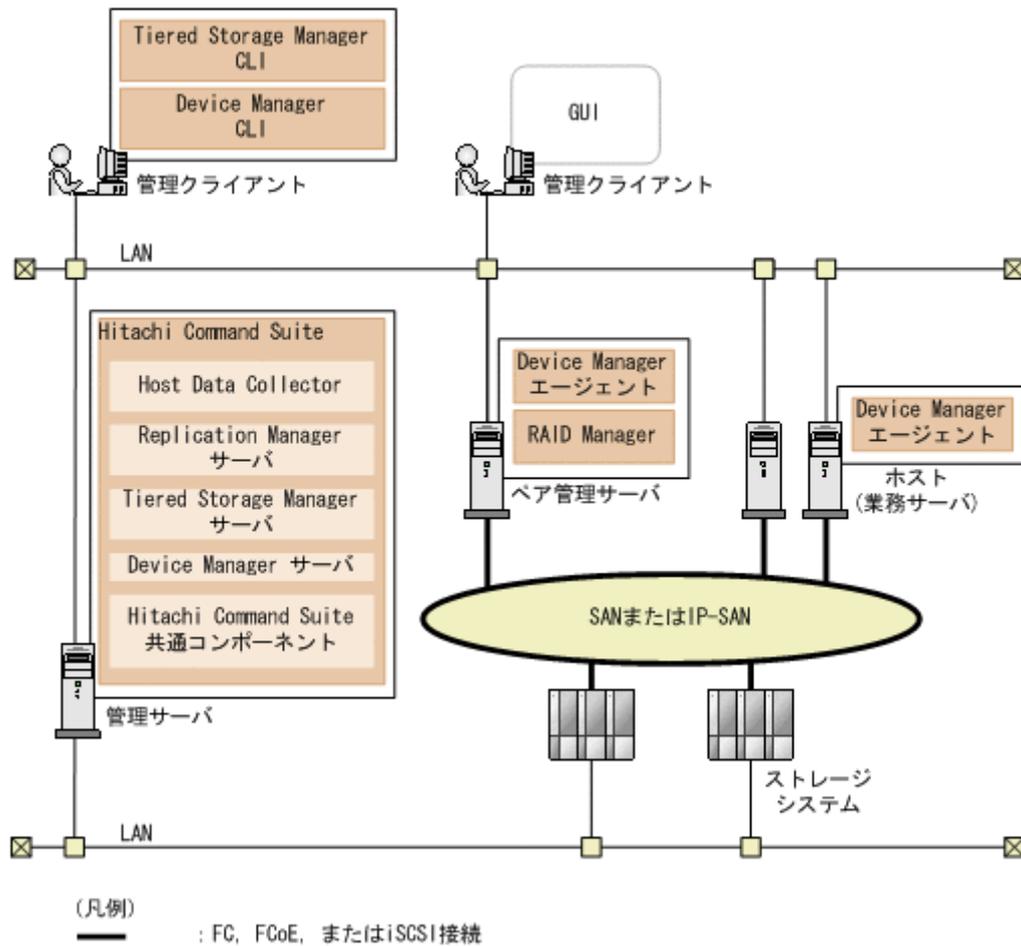
この章では, Device Manager および Tiered Storage Manager のシステム構成とシステム要件について説明します。

- 1.1 システム構成
- 1.2 ネットワーク構成
- 1.3 管理サーバのシステム要件
- 1.4 ホストのシステム要件
- 1.5 関連製品
- 1.6 Device Manager でのコピーペア管理
- 1.7 コマンドを実行する場合の注意事項

1.1 システム構成

Device Manager および Tiered Storage Manager を使用する場合の基本的なシステム構成を次の図に示します。

図 1-1 基本的なシステム構成



管理サーバと管理クライアント間、管理サーバとストレージシステム間は TCP/IP ネットワークで接続する必要があります。

また、ホストとストレージシステム間は FC または FCoE で SAN を構成します。HUS100, Hitachi AMS2000, Hitachi SMS および Hitachi AMS/WMS では、FC または FCoE の代わりに iSCSI で IP-SAN を構成することもできます。

Device Manager および Tiered Storage Manager の主なシステム構成要素を以降で説明します。

1.1.1 ハードウェア構成

Device Manager および Tiered Storage Manager を使用する場合のハードウェア構成を次に示します。

管理サーバ

ストレージシステムやホストなどを統合管理するマシンです。Hitachi Command Suite をインストールします。2 台のマシンを使用した Active-Standby 型のクラスタリングにも対応しています。

管理クライアント

Device Manager および Tiered Storage Manager を操作する際に使用するマシンです。

ホスト（業務サーバ）

ストレージシステム内のボリュームを利用するマシンです。

ペア管理サーバ

コピーペアの構成や状態を 1 台のホストで一括管理する場合に必要なマシンです。

ストレージシステム

Hitachi Command Suite 製品で管理するストレージシステムです。



注意 1 台のストレージシステムは、1 台の管理サーバで管理してください。1 台のストレージシステムを複数の管理サーバで管理するシステムは構成しないでください。

1.1.2 ソフトウェア構成

Device Manager および Tiered Storage Manager を使用する場合のソフトウェア構成を次に示します。

Hitachi Command Suite

次のコンポーネントから構成されています。

Hitachi Command Suite 共通コンポーネント

ユーザーアカウントの管理やセキュリティ監視など Hitachi Command Suite 製品で共通の機能を提供するコンポーネントです。

Device Manager サーバ

ストレージシステムのボリュームを管理するためのコンポーネントです。



注意 1 つの Device Manager サーバで、分割ストレージごとに複数のストレージ管理者のアカウントを使い分けることはできません。個々の分割ストレージを管理したい場合は、分割ストレージごとに Device Manager サーバを用意する必要があります。

Tiered Storage Manager サーバ

ストレージシステムのボリュームをマイグレーションするためのコンポーネントです。

Replication Manager サーバ

ストレージシステムのボリュームを複製するためのコンポーネントです。

Host Data Collector

ホスト（通常ホスト、仮想マシンおよび仮想化サーバ）の情報、および各ホストで利用されているボリュームの情報を収集するためのコンポーネントです。



重要 別マシンに Host Data Collector だけをインストールすることもできます。

Device Manager エージェント

ホストやストレージシステムの情報を収集して Device Manager サーバに通知するコンポーネントです。次の運用を行う場合に必要です。

コピーペアの管理

RAID Manager または P9000 RAID Manager と連携して、Device Manager または Replication Manager でコピーペアの作成や構成変更、状態変更を行う場合に必要です。

性能情報の取得

Device Manager の CIM/WBEM 機能を使用して、Virtual Storage Platform, Universal Storage Platform V/VM および Hitachi USP の性能情報を取得する場合に必要です。



重要 次の OS では、Global Link Manager エージェントが自動的にインストールされます。

- Windows
- Solaris 9 (SPARC)
- Solaris 10 (SPARC)
- Solaris 11 (SPARC)
- HP-UX

Global Link Manager エージェントは、ホストとストレージシステムとの間の LUN パス管理に DMP (VxVM の Dynamic Multipathing 機能) や HP-UX マルチパスを使用している場合に、Global Link Manager サーバと通信して、LUN パスに関する情報を通知したり、ホストに必要な設定をしたりするために必要です。

RAID Manager または P9000 RAID Manager

ストレージシステム上のコピーペアを制御するためのプログラムです。
コピーペアの構成や状態を Device Manager で管理する場合に必要です。

GUI

Web ベースのグラフィカルインターフェースです。

CLI

キャラクターベースのインターフェースです。システムの初期導入時や、同じ設定変更を大量に実施する際などには、CLI を使用することで、作業を効率化できます。

1.2 ネットワーク構成

Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, SANRISE9900V および HUS VM には、SVP と呼ばれるサービスプロセッサが搭載されています。SVP には 2 つの Ethernet アダプターがあります。1 つ目の Ethernet アダプターは、プライベート (内部) Ethernet LAN 用で、ストレージシステム内での通信だけに使用されます。ユーザーが利用でき、内部 LAN にアクセスできるデバイスは、SVP だけです。2 つ目の Ethernet アダプターは、ほかのアプリケーションが SVP と対話するために使用されます。この LAN は、パブリック LAN と呼ばれ、ストレージシステムの外部にあるほかのコンピュータからも参照できます。Device Manager は、ストレージシステムおよび構成変更に関する SVP との通信にこのパブリック LAN を使用します。

Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, SANRISE9900V および HUS VM は、SVP インターフェースを介して管理されますが、それ以外のストレージシステム (例えば、HUS100, Hitachi AMS2000, Hitachi SMS, Hitachi AMS/WMS および SANRISE9500V) には、プライベート LAN がありません。その代わりに、HUS100, Hitachi AMS2000, Hitachi SMS, Hitachi AMS/WMS および SANRISE9500V は、パブリック LAN に直接接続するための Ethernet ワークインターフェースを持ちます。これらのストレージシステムは、リモート管理用の API を持っているため、LAN に接続すれば、さまざまな管理アプリケーションからアクセスできるようになります。



警告 Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, SANRISE9900V および HUS VM は、パブリック LAN とプライベート LAN の両方を持ちます。Device Manager は、ストレージシステムおよび構成変更に関する SVP との通信にパブリック LAN を使用します。どのような状況下でも、外部ネットワークにプライベート LAN を接続してはいけません。ストレージシステムで深刻な問題が発生するおそれがあります。

1.2.1 セキュリティについての一般的なリスク

HUS100, Hitachi AMS2000, Hitachi SMS, Hitachi AMS/WMS および SANRISE9500V は、パブリック LAN に接続するよう設計されているため、これらのストレージシステムをパブリックネットワークに接続する場合には特に注意が必要です。

システム管理者は、多くの場合、管理用の LAN と業務用の LAN を切り離します。そうすることで、管理用の LAN を独立させ、業務用のネットワークから管理用のトラフィックを切り離し、セキュリティ上の危険性を減らしています。もし、業務に使用する LAN に SVP のような管理端末が共存していたら、IP ネットワーク上のどのエンティティからでもストレージシステムにアクセスできてしまいます。アクセスが意図的なものであるかどうかに関わらず、結果として生じるリスクから、ストレージサービス拒否という現実の障害が発生するおそれがあります。DoS 攻撃によって、I/O 操作中のポートからストレージの領域がアンバインドされるなど、悪意のある目的で管理用のセッションが乗っ取られる危険性があります。

管理用の LAN の構成に関するガイドラインを以下に示します。

- ・ 業務に使用する LAN からのトラフィックが管理用の LAN を流れたり、経由したりしてはいけません。
- ・ 管理用の LAN 上にある管理インターフェースまたはコントローラーを搭載したすべてのホストを最大限に強化して危険性を減らし、ステーションまたはデバイス全体が管理インターフェース以外のソフトウェアによって使用されないようにします（この場合の強化とは、不要なソフトウェアの削除、不要なサービスのシャットダウン、および最新のパッチへの更新を含みます）。
- ・ 管理用の LAN は、例えば Device Manager サーバのように、管理用の LAN と業務用の LAN の間で仲立ちとして動作しているマシンでだけ、業務用の LAN とつながるようにします。
- ・ プライベート LAN と管理用の LAN の両方につながるマシンを、ファイアウォールの後ろに置くと、意図しないアクセスをさらに防げます。

1.2.2 最もセキュアな構成：管理用の LAN を分離し、ファイアウォールを設置した場合

この構成では、Device Manager サーバがインストールされているマシンをデュアルホームにするか、NIC を 2 つ持たせる必要があります。Device Manager 以外の管理アプリケーションでも同様に構成する必要があります。各マシンの第 1 の NIC は、管理用のマシンと管理対象のストレージシステムとの間の管理用トラフィック専用の LAN に接続します。第 2 の NIC は、ファイアウォールによってアクセスが管理されている LAN に接続します。「[図 1-2 最もセキュアな構成：管理用の LAN を分離し、ファイアウォールを設置した場合](#)」に示すように、各業務サーバは、個別のファイアウォールを持つ異なる LAN に接続することもできます。ファイアウォールには、Device Manager のクライアントまたは特定の管理アプリケーションのクライアントにだけ管理サーバへのアクセスを許可する、厳しいアクセス規則を設定します。

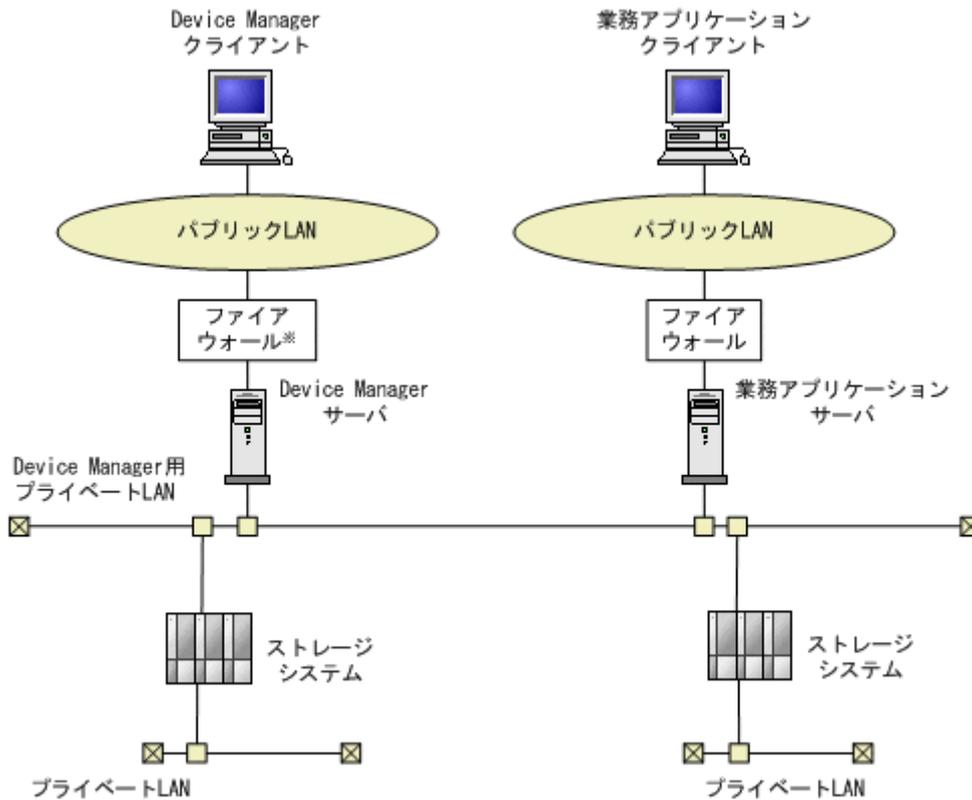
この構成は、最もセキュアな構成ですが、さまざまなネットワークコンポーネント、サーバ、管理下のデバイスのすべてを管理するオーバーヘッドを必要とするため、最も柔軟性のない構成です。この構成をよりセキュアにするには、基礎となる管理アプリケーション OS を最大限に強化する必要があります。このためには、例えば、Telnet, FTP, SMTP などのサービスを使用不可にします。さらに、できれば、不要なパッケージをすべて除去してください。



注意 Virtual Storage Platform, Universal Storage Platform VVM, Hitachi USP, SANRISE9900V および HUS VM を Element Manager で操作する場合、管理クライアントの Java Web Start およびブラウザとストレージシステムの間で直接通信を行います。そのため、管理クライアントとストレージシステムが異なるネットワークに接続されている場合、互いに直接通信できるようにネットワークを設定する必要があります。

管理用の LAN を分離し、ファイアウォールを設置した場合の構成を次の図に示します。

図 1-2 最もセキュアな構成：管理用の LAN を分離し、ファイアウォールを設置した場合



注※ Device Managerは、NATには対応していません。

1.2.3 2 番目にセキュアな構成：管理用の LAN を分離し、管理下のデバイスとの間にファイアウォールを設置した場合

この構成では、Device Manager サーバがインストールされているマシンとそのほかのすべての業務サーバをシングルホームにし、ファイアウォールによって、Device Manager 管理下から実デバイスを分離します。ファイアウォールのルールで、ストレージシステムへのアクセスは、Device Manager サーバとそのほかの必要な管理アプリケーションに制限されます。Device Manager にアクセスする管理用のクライアントからのトラフィックは、ファイアウォールを超えられないため、管理下のストレージシステムと直接対話はできませんが、Device Manager や管理アプリケーションを使用して、管理操作に直接関与できます。

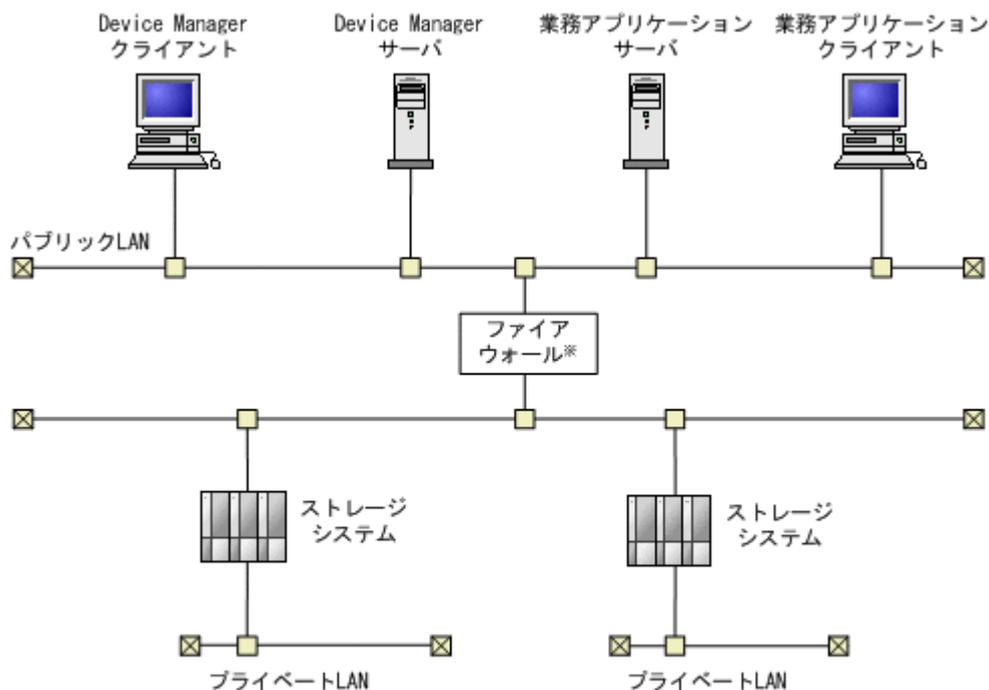
この構成は 2 番目にセキュアな構成で、最もセキュアな構成に比べて柔軟性があります。この構成では、管理下のデバイスは保護されますが、管理アプリケーションサーバ自体は保護されません。したがって、すべての管理アプリケーションサーバを最大限に強化する必要があります。



注意 Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, SANRISE9900V および HUS VM を Element Manager で操作する場合、管理クライアントに使用しているマシンの Java Web Start およびブラウザとストレージシステムの間で直接通信を行います。そのため、管理クライアントとストレージシステムが異なるネットワークに接続されている場合、互いに直接通信できるようにネットワークを設定する必要があります。

管理用の LAN を分離し、管理下のデバイスとの間にファイアウォールを設置した場合の構成を次の図に示します。

図 1-3 2 番目にセキュアな構成：管理用の LAN を分離し、管理下のデバイスとの間にファイアウォールを設置した場合



注※ Device Managerは、NATには対応していません。

1.2.4 3 番目にセキュアな構成：管理用の LAN を分離し、管理サーバをデュアルホームにした場合

この構成では、管理サーバ自体が、管理用の LAN と業務用の LAN との接続点として動作します。Device Manager やそのほかの管理アプリケーションが稼働しているサーバをデュアルホームにします。第 1 の NIC は、管理下のデバイスとつながっている管理用の LAN に接続し、第 2 の NIC を、管理クライアント（例えば、Device Manager の GUI）とつながっている業務用の LAN に接続します。管理アプリケーションサーバが業務用の LAN と管理用の LAN とのゲートウェイとして動作し、ファイアウォールを追加しないため、サーバ自体が 2 つのネットワークの間でトラフィックを行き来させないように、十分注意する必要があります。

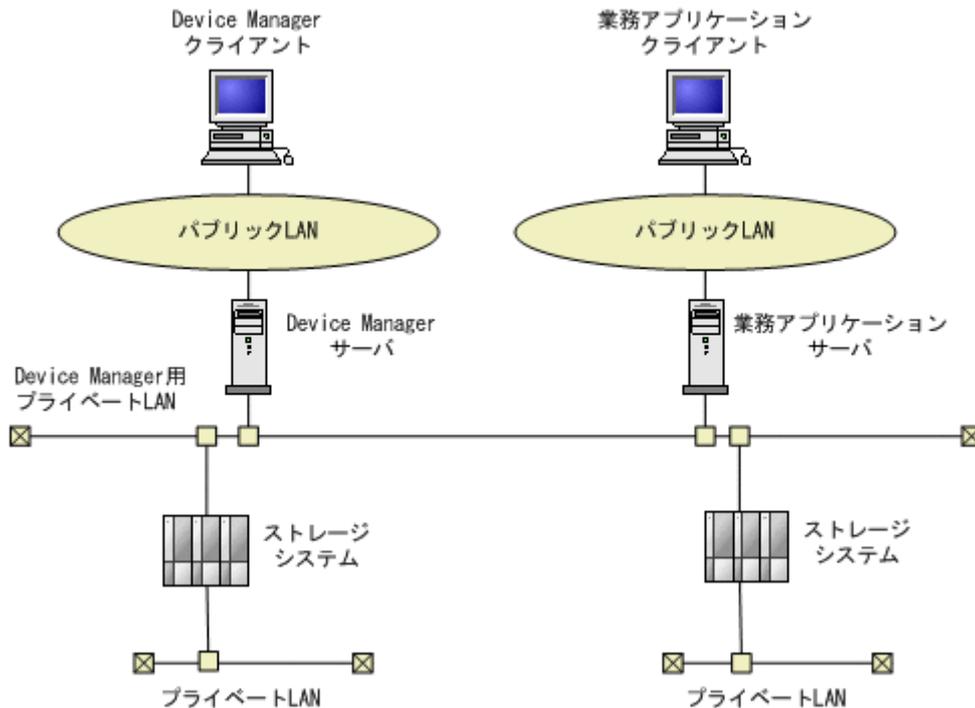
この構成は、3 番目にセキュアな構成で、最もセキュアな構成および 2 番目に安全な構成よりも柔軟性があります。この構成では、管理下のデバイスは保護されますが、管理アプリケーションサーバ自体は保護されません。したがって、管理アプリケーションサーバを最大限に強化する必要があります。さらに、管理アプリケーションが 2 つの LAN の間でゲートウェイとして動作することから、OS の強化がより重要になります。



注意 Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, SANRISE9900V および HUS VM を Element Manager で操作する場合、管理クライアントの Java Web Start およびブラウザとストレージシステムの間で直接通信を行います。そのため、管理クライアントとストレージシステムが異なるネットワークに接続されている場合、互いに直接通信できるようにネットワークを設定する必要があります。

管理用の LAN を分離し、管理サーバをデュアルホームにした場合の構成を次の図に示します。

図 1-4 3 番目にセキュアな構成：管理用の LAN を分離し、管理サーバをデュアルホームにした場合の構成



1.2.5 最もセキュアでない構成：フラットなネットワーク

この構成では、管理アプリケーションサーバ、管理下のデバイス、管理クライアントのすべてが同じネットワーク上に共存しています。

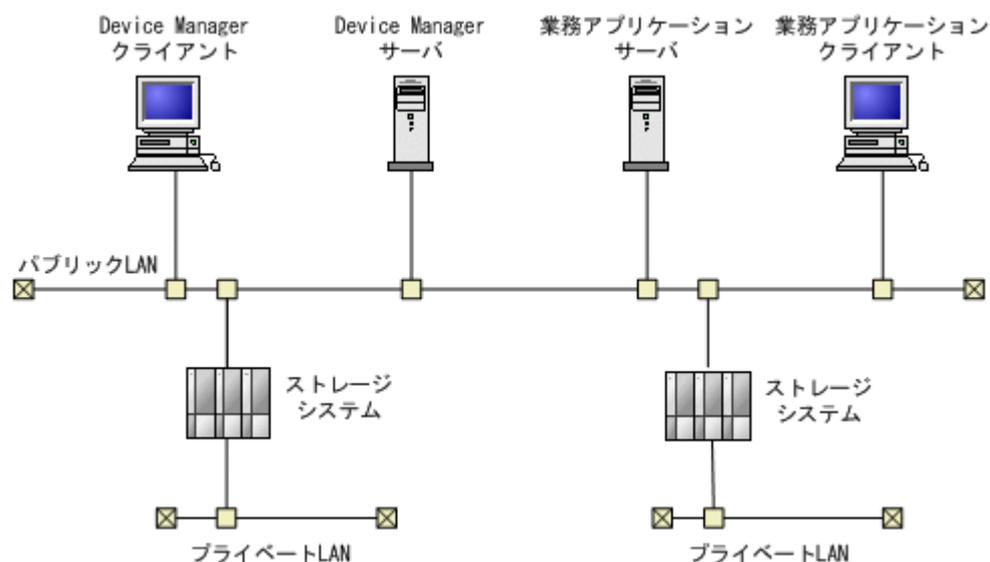
この構成は、最も柔軟性が高いものの、最もセキュアでない構成です。この構成では、ストレージ管理の操作に必要なコンポーネントがまったく保護されないため、管理アプリケーションサーバの強化が最重要になります。加えて、管理下の各デバイスに対するマイクロコードの更新（特に、デバイス管理用端末自体のセキュリティと何らかの関係がある場合）について考慮する必要があります。



重要 構成が管理用の LAN に合わない場合に、この構成が必要となることもあります。

次の図は、フラットネットワークを示しています。

図 1-5 最もセキュアでない構成：フラットネットワーク



1.3 管理サーバのシステム要件

ここでは管理サーバのシステム要件について説明します。

1.3.1 管理リソース数の上限

Device Manager, Tiered Storage Manager および Replication Manager で管理できるリソース数には上限があります。

次の表に示す値を超えない構成で各製品を運用することを推奨します。

表 1-1 管理リソース数の上限値

リソース	Device Manager サーバの上限
LDEV 数※1	1,000,000
LDEV 数とバス数※2 の合計	5,000,000

注

CIM/WBEM 機能を利用する場合の管理リソース数の上限値は次のとおりです。Device Manager で管理するストレージシステムのリソース数が、この上限値を超える場合は、`server.cim.support` プロパティの値を `false` に変更してください (デフォルト: `true`)。

- LUN 数
128,000
- Security 数 (Device Manager, Tiered Storage Manager および Replication Manager で管理しているストレージシステムの LUN にセキュリティを設定するために割り当てられた WWN と iSCSI ネームの総数)
192,000
- LDEV 数
128,000 (オープン用 LDEV 数だけの上限値は 64,000)

注※1

メインフレーム用の LDEV 数とオープンシステム用の LDEV 数の合計値です。

注※2

パス数 = <LDEV 数> × <1LDEV 当たりの平均パス数>

関連項目

- A.1.1 Device Manager サーバのプロパティの変更
- A.2.11 server.cim.support.job

1.3.2 メモリーヒープサイズの変更 (Hitachi Command Suite 共通コンポーネント)

Hitachi Command Suite 共通コンポーネントのメモリーヒープサイズを変更するには、`hcmdschgheap` コマンドを実行します。

事前に確認しておく情報

- 管理対象となる LDEV 数とコピーペア数

Device Manager, Tiered Storage Manager および Replication Manager の運用で想定される LDEV 数およびコピーペア数から、必要なメモリーヒープサイズを算出してください。LDEV 数から算出したメモリーヒープサイズとコピーペア数から算出したメモリーヒープサイズのうち、値が大きい方を設定してください。

表 1-2 Hitachi Command Suite 共通コンポーネントのメモリーヒープサイズの目安

利用環境		設定するメモリーヒープサイズ			
OS	管理リソース	Small (下限：128MB, 上限：256MB)	Medium (下限：256MB, 上限：512MB)	Large (下限：512MB, 上限：1024MB)	
Windows (x86)	1 台のストレージシステム 当たりの LDEV 数	8,000 以下	8,001 以上	--	
	管理対象 の全コ ピーペア 数	オープンボ リュームだけ	5,000 以下	5,001 以上	--
		メインフレーム ボリュームだけ	5,000 以下	5,001 以上	--
		混在環境※	40,000 以下	40,001 以上	--
Windows (x64), Solaris または Linux	1 台のストレージシステム 当たりの LDEV 数	8,000 以下	8,001~14,000	14,001 以上	
	管理対象 の全コ ピーペア 数	オープンボ リュームだけ	5,000 以下	5,001~12,000	12,001 以上
		メインフレーム ボリュームだけ	5,000 以下	5,001~60,000	60,001 以上
		混在環境※	40,000 以下	40,001~60,000	60,001 以上

(凡例)

-- : 指定できません。

注※

オープンボリュームとメインフレームボリュームの両方を管理する場合は、次の計算式を使ってコピーペア数を算出してください。

(<オープン系システムのコピーペア数>×6) + <メインフレーム系システムのコピーペア数>

メモリーヒープサイズを変更するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. 現在のメモリーヒープサイズの設定を確認します。

Windows の場合：

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmdschgheap /print
```

Solaris または Linux の場合：

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdschgheap -print
```

3. メモリーヒープサイズを変更します。

Windows の場合：

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmdschgheap /set [Small|Medium|Large]
```

Solaris または Linux の場合：

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdschgheap -set [Small|Medium|Large]
```

4. Hitachi Command Suite 製品のサービスを起動します。



注意 hcmdsweb または hcmdsweb2 コマンドを使ってヒープサイズを設定していた場合、すでに設定されている値よりも小さい値に変更することはできません。小さい値に変更したい場合は、一度 Hitachi Command Suite をアンインストールしたあと、再度インストールしてから、設定したいヒープサイズの値で変更してください。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

1.3.3 メモリーヒープサイズの変更（Device Manager サーバ）

Device Manager サーバのメモリーヒープサイズを変更するには、Server.ini ファイル（Windows の場合）または hicommand.sh ファイル（Solaris または Linux の場合）を編集します。

事前に確認しておく情報

- 管理対象となる LDEV 数

表 1-3 Device Manager サーバのメモリーヒープサイズの目安

管理リソース	メモリーヒープサイズ		
	256MB (下限：128MB)	512MB (下限：128MB)	1024MB (下限：128MB)
1 台のストレージシステム当たりの LDEV 数	2,000 以下	6,000 以下	6,001 以上

- 管理対象となるファイルサーバの構成（ファイルサーバを管理対象にする場合）
ファイルサーバのクラスタ数や台数に応じて、次のとおりメモリーヒープサイズを設定してください。

- クラスタ数が 1 つ、または非クラスタ構成のファイルサーバを 1 台管理する場合
メモリーヒープサイズは 512MB を設定してください。
 - クラスタ数が 2 つ以上、または非クラスタ構成のファイルサーバを 2 台以上管理する場合
メモリーヒープサイズは 1024MB を設定してください。
- LDEV 数から算出したメモリーヒープサイズと値が異なる場合、どちらか大きい方を設定してください。

メモリーヒープサイズを変更するには：

1. 次のファイルをテキストエディターで開きます。

Windows の場合：

< *Device Manager* サーバのインストールフォルダ > %HiCommandServer%Server.ini

Solaris または Linux の場合：

< *Device Manager* サーバのインストールディレクトリ > /hicommand.sh

2. メモリーヒープサイズを変更します。

Windows の場合：

次に示す形式で JVM_XOPT_HEAP_MAX に適切な値を指定してください。

JVM_XOPT_HEAP_MAX=-Xmx <設定値> m

Solaris または Linux の場合：

start オプションのスクリプトに記載されている java コマンドの -Xmx オプションに値を設定してください。

変更例：値を 256MB から 512MB に変更する場合

変更前：java -Xmx256m -classpath ...

変更後：java -Xmx512m -classpath ...

3. Hitachi Command Suite 製品のサービスを再起動します。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

1.3.4 JDK の変更

運用開始後に、Hitachi Command Suite 製品で使用する JDK を変更するには、hcmdschgjdk コマンドを実行します。

事前に完了しておく操作

- Hitachi Command Suite 製品が前提とする JDK の確認
詳細は、「ソフトウェア添付資料」を参照してください。

JDK を変更するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. 使用する JDK を変更します。
次のコマンドを実行して、表示された画面で使用する JDK を選択します。

Windows の場合：

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmdschgjdk
```

Solaris (SPARC) または Linux の場合 :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdschgjdk
```

3. Hitachi Command Suite 製品のサービスを起動します。
4. 次の通信路で SSL/TLS を使用している場合は、サーバ証明書をトラストストア (jssecacerts) に再度インポートします。
インポートし直すことで、サーバ証明書の格納場所が使用する JDK の配下に切り替わります。
 - Device Manager サーバと Replication Manager サーバ間
hcmdskeytool ユーティリティ (Windows の場合) または keytool ユーティリティ (Solaris または Linux の場合) で、Device Manager サーバのサーバ証明書 (認証局のサーバ証明書, または自己署名証明書) をインポートし直します。
 - Tuning Manager サーバと Device Manager サーバ間
hcmdskeytool ユーティリティ (Windows の場合) または keytool ユーティリティ (Solaris または Linux の場合) で、Hitachi Command Suite 共通コンポーネントのサーバ証明書 (認証局のサーバ証明書, または自己署名証明書) をインポートし直します。
5. Windows ファイアウォールが有効になっている環境で、Oracle JDK に切り替えた場合は、Oracle JDK の java.exe ファイルを手動で例外登録します。



重要

- 管理サーバの OS が Solaris (SPARC) の場合、Device Manager GUI から Hitachi NAS Platform を管理するためには、Oracle JDK 6 または Oracle JDK 7 への切り替えが必要です。
- 管理サーバの OS が Solaris (x64) の場合、JDK の変更はできません。
- Hitachi Command Suite 製品の運用中に Oracle JDK を上書きまたはアップグレードインストールした場合は、使用する JDK を登録し直してください。
- Hitachi Command Suite 製品の運用中に Oracle JDK をアンインストールする場合は、使用する JDK を Hitachi Command Suite に同梱された JDK に切り替えてください。
- バージョン 7.0 以前の Hitachi Command Suite 製品が管理サーバにインストールされている場合は、Oracle JDK には変更できません。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

1.4 ホストのシステム要件

Device Manager では、管理対象のストレージシステムのボリュームを使用するマシンをホストとして管理できます。各ホストのディスクリソースを Device Manager で一元管理することで、利用状況に応じて最適なボリュームを割り当てることができます。

1.4.1 Device Manager で管理できるホスト

ホスト (業務サーバ) にストレージシステムのボリュームを割り当てたり、各ホストでのボリュームの使用状況を確認したりするためには、Device Manager のリソースとして登録する必要があります。

Device Manager では、次の表に示すホストでのボリュームの利用状況を管理できます。

表 1-4 Device Manager で管理できるホスト

ホスト		説明
オープンホスト	通常ホスト	仮想化ソフトウェアがインストールされていない環境
	仮想マシン※	仮想化ソフトウェア上に作成された仮想環境
	仮想化サーバ	仮想化ソフトウェアがインストールされた物理環境※
メインフレームホスト		メインフレームボリュームを利用するマシン
ファイルサーバ	Hitachi Virtual File Platform	NAS 機能を使用して、ストレージシステム内のファイルをネットワーク上の複数のクライアントと共有するためのマシン
	Hitachi NAS Platform	

注※

仮想マシン、および Windows Server 2008 Hyper-V または Windows Server 2012 Hyper-V がインストールされた物理環境は、Device Manager への登録後は通常ホストとして扱われます。



重要 Device Manager で管理するホストのホスト名は、50 バイト以内であることが前提です。

1.4.2 Device Manager のホスト管理ソフトウェア

Device Manager では、ホスト管理ソフトウェアを経由して各ホストの情報を収集することで、ホストを統合管理できます。

表 1-5 Device Manager のホスト管理ソフトウェア

ホスト管理ソフトウェア	オープンホスト			メインフレームホスト	ファイルサーバ
	通常ホスト	仮想マシン	仮想化サーバ		
Host Data Collector※	○	○	○	×	×
Device Manager エージェント※	○	○	×	×	×
vMA	×	×	○	×	×
Mainframe Agent	×	×	×	○	×
ファイルサーバ管理ソフトウェア	×	×	×	×	○

(凡例)

- : サポートしている
- × : サポートしていない

注※

通常ホストまたは仮想マシンが Host Data Collector と Device Manager エージェントの両方の管理対象になっている場合、GUI および CLI には Device Manager エージェントが取得した情報が優先されて表示されます。

- Host Data Collector で管理する
Host Data Collector では、通常ホスト、仮想マシンおよび仮想化サーバを管理できます。

Device Manager GUI/CLI でネットワーク上に存在するホストを探索すると、見つかったホストが Device Manager に登録されます。

- Device Manager エージェントで管理する
Device Manager エージェントでは、通常ホストおよび仮想マシンを管理できます。
それぞれのホストに Device Manager エージェントをインストールすると、ホストが Device Manager に登録されます。
- vMA で管理する
vMA では、仮想化サーバを管理できます。
Device Manager GUI/CLI で vMA 管理下の仮想化サーバを探索すると、見つかった仮想化サーバが Device Manager に登録されます。
なお、vMA で管理できる仮想化サーバは VMware ESX 4.x または VMware ESXi 4.x だけです。
- Mainframe Agent で管理する
Mainframe Agent では、メインフレームホストを管理できます。
Device Manager CLI で、メインフレームホストと、それを管理する Mainframe Agent を Device Manager に登録します。
- ファイルサーバ管理ソフトウェアで管理する
ファイルサーバ管理ソフトウェアでは、ファイルサーバを管理できます。
ファイルサーバ管理ソフトウェアで、管理対象のファイルサーバを Device Manager に登録します。



重要

- Plug-in for Virtualization Server Provisioning を使用する環境では、vMA で仮想化サーバを管理してください。
 - Compute Systems Manager を導入している環境では、Compute Systems Manager で登録した通常ホストおよび仮想マシンは、Device Manager にも自動的に登録されます。
-

関連項目

- [1.1.2 ソフトウェア構成](#)
- [ホスト管理ソフトウェアの管理対象ホストの詳細：ソフトウェア添付資料](#)

1.4.3 通常ホストのシステム要件

Host Data Collector または Device Manager エージェントで管理する場合、Device Manager への登録前に各通常ホストでの環境設定が必要です。

(1) 通常ホストの前提環境（Host Data Collector で管理する場合）

Host Data Collector で管理するためには、Host Data Collector のインストール後、それぞれの通常ホストで環境設定が必要です。

Host Data Collector は、管理サーバにインストールする Hitachi Command Suite に同梱されているほか、管理サーバ以外のマシンにインストールすることもできます。

また、通常ホストでは、Device Manager に登録する前に、次の環境設定を済ませておく必要があります。UNIX ホストを管理する場合、ホストを Device Manager に登録する時に使用する UNIX アカウントによって、それぞれの UNIX ホストで必要になる環境設定が異なります。

Windows ホストを管理する場合

- Host Data Collector のサービス (Host Data Collector Base Service) の実行ユーザーに Administrator 権限を持つユーザーが割り当てられている。
- admin\$ がネットワーク共有されている。

Windows の net share コマンドで確認できます。ただし、セキュリティ監視プログラムが通常ホストにインストールされていると、Host Data Collector ではホスト情報を収集できないことがあります。

- Windows のファイアウォールの設定で、[ファイルとプリンタの共有] が例外として登録されている。

UNIX ホストを管理する場合 (root アカウントでホストの情報を収集するとき)

- SSH が有効になっている。
- リモートから root でパスワード認証による SSH ログインができるように設定されている。
- 管理対象の通常ホストの OS が AIX の場合、環境変数 ODMDIR が設定されている。



重要 root アカウントで Device Manager に登録したホストを、一般ユーザーアカウントを使って二重に登録しないでください。

UNIX ホストを管理する場合 (一般ユーザーアカウントでホストの情報を収集するとき)

- SSH が有効になっている。
- ホスト登録時に使用するユーザーアカウントが Host Data Collector 専用で作成されている (推奨)。
- 管理対象の通常ホストの OS が AIX の場合、環境変数 ODMDIR が設定されている。
- /tmp ディレクトリに更新権限 (rwx) が設定されている。
- sudo コマンドが実行できるように環境変数 PATH に設定されている。
- sudo コマンドを実行できるように、/etc/sudoers ファイルに設定されている。
sudo コマンドを実行できるようにするには、次の定義を追加してください。

```
<ホスト登録時に使用するユーザー名> <登録対象のホスト>=(<実行ユーザー名のエイリアス>)NOPASSWD:/tmp/FsDataGatherLauncher.Unix.sh
```

<登録対象のホスト>には、IP アドレス、ホスト名または ALL を指定します。

<実行ユーザー名のエイリアス>には、ALL または root を指定します。



重要 一般ユーザーアカウントで Device Manager に登録したホストを、root アカウントを使って二重に登録しないでください。



重要 次に示すホストの項目では、セミコロン (;) を含む名称を使用しないでください。

- Windows ホストを管理する場合
 - ネットワーク接続名
 - 共有ディスクのコメント欄
- UNIX ホストを管理する場合
 - マウント先のディレクトリ名
 - ディスクグループ名 (ボリュームグループ名、ディスクセット名)
 - 論理ボリューム名
 - ネットワーク名
 - 共有ディスクのディレクトリ名
 - ネットワークドライブのデバイス名 (参照先ホスト上で設置済みの共有ディスクのディレクトリ名)

関連項目

- ・ 12. Host Data Collector のセットアップ

(2) 通常ホストの前提環境（Device Manager エージェントで管理する場合）

Device Manager エージェントで管理するためには、通常ホストごとに Device Manager エージェントをインストールします。

インストール後は、管理サーバの情報や HiScan コマンドの実行周期などを設定する必要があります。

また、通常ホストの OS が AIX の場合は、環境変数 ODMDIR の設定も必要です。



重要 次に示すホストの項目では、セミコロン (;) を含む名称を使用しないでください。

- ・ Windows ホストを管理する場合
 - ・ ネットワーク接続名
 - ・ 共有ディスクのコメント欄
 - ・ UNIX ホストを管理する場合
 - ・ マウント先のディレクトリ名
 - ・ ディスクグループ名（ボリュームグループ名、ディスクセット名）
 - ・ 論理ボリューム名
 - ・ ネットワーク名
 - ・ 共有ディスクのディレクトリ名
 - ・ ネットワークドライブのデバイス名（参照先ホスト上で設置済みの共有ディスクのディレクトリ名）
-

関連項目

- ・ Device Manager エージェントのセットアップ方法：マニュアル「*Hitachi Command Suite Software インストールガイド*」

1.4.4 仮想マシンのシステム要件

Device Manager では、次の構成の仮想マシンを管理できます。

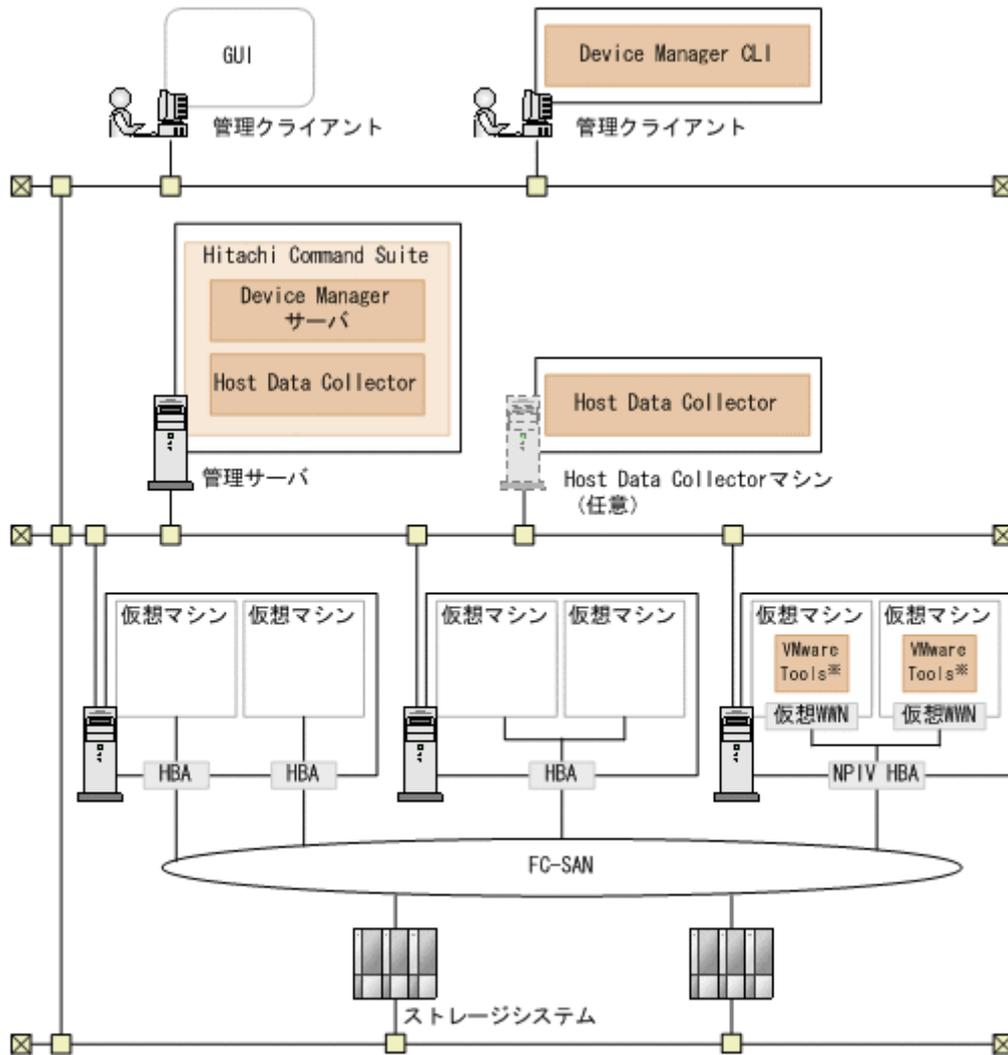
- ・ 仮想マシンごとに HBA が割り当てられている構成
- ・ 複数の仮想マシンで HBA を共有している構成
- ・ 仮想マシンごとに仮想 HBA が割り当てられている構成（NPIV HBA を使用している場合）

Host Data Collector または Device Manager エージェントで管理する場合、Device Manager への登録前に各仮想マシンでの環境設定が必要です。

(1) 仮想マシンの前提環境（Host Data Collector で管理する場合）

Host Data Collector で管理するためには、Host Data Collector のインストール後、それぞれの仮想マシンで環境設定が必要です。

図 1-6 仮想マシンの前提環境 (Host Data Collector で管理する場合)



注※ 仮想化ソフトウェアにVMware ESXを使用している場合に必要です。

Host Data Collector は、管理サーバにインストールする Hitachi Command Suite に同梱されているほか、管理サーバ以外のマシンにインストールすることもできます。

また、仮想マシンでは、Device Manager に登録する前に、次の環境設定を済ませておく必要があります。UNIX ホストを管理する場合、ホストを Device Manager に登録する時に使用する UNIX アカウントによって、それぞれの UNIX ホストで必要になる環境設定が異なります。

Windows ホストを管理する場合

- Host Data Collector のサービス (Host Data Collector Base Service) の実行ユーザーに Administrator 権限を持つユーザーが割り当てられている。
- admin\$ がネットワーク共有されている。

Windows の net share コマンドで確認できます。ただし、セキュリティ監視プログラムが仮想マシンにインストールされていると、Host Data Collector ではホスト情報を収集できないことがあります。

- Windows のファイアウォールの設定で、[ファイルとプリンタの共有] が例外として登録されている。

- ・ 仮想マシンごとに仮想 HBA が割り当てられている構成の場合 (NPIV HBA を使用している場合)、次の環境設定が完了している。
 - 同一の物理環境で稼働する仮想化サーバの Device Manager への登録
 - 管理対象の各仮想マシンへの VMware Tools のインストール (仮想化ソフトウェアに VMware ESX を使用している場合)
 - Device Manager への仮想 WWN の登録 (仮想化サーバを vMA で管理する場合)

UNIX ホストを管理する場合 (root アカウントでホストの情報を収集するとき)

- ・ SSH が有効になっている。
- ・ リモートから root でパスワード認証による SSH ログインができるように設定されている。
- ・ 仮想マシンごとに仮想 HBA が割り当てられている構成の場合 (NPIV HBA を使用している場合)、次の環境設定が完了している。
 - 同一の物理環境で稼働する仮想化サーバの Device Manager への登録
 - 管理対象の各仮想マシンへの VMware Tools のインストール
 - Device Manager への仮想 WWN の登録 (仮想化サーバを vMA で管理する場合)



重要 root アカウントで Device Manager に登録したホストを、一般ユーザーアカウントを使って二重に登録しないでください。

UNIX ホストを管理する場合 (一般ユーザーアカウントでホストの情報を収集するとき)

- ・ SSH が有効になっている。
- ・ ホスト登録時に使用するユーザーアカウントが Host Data Collector 専用に作成されている (推奨)。
- ・ /tmp ディレクトリに更新権限 (rwx) が設定されている。
- ・ sudo コマンドが実行できるように環境変数 PATH に設定されている。
- ・ sudo コマンドを実行できるように、/etc/sudoers ファイルに設定されている。
sudo コマンドを実行できるようにするには、次の定義を追加してください。

```
<ホスト登録時に使用するユーザー名> <登録対象のホスト>=(<実行ユーザー名のエイリアス>)NOPASSWD:/tmp/FsDataGatherLauncher.Unix.sh
```

<登録対象のホスト>には、IP アドレス、ホスト名または ALL を指定します。

<実行ユーザー名のエイリアス>には、ALL または root を指定します。

- ・ 仮想マシンごとに仮想 HBA が割り当てられている構成の場合 (NPIV HBA を使用している場合)、次の環境設定が完了している。
 - 同一の物理環境で稼働する仮想化サーバの Device Manager への登録
 - 管理対象の各仮想マシンへの VMware Tools のインストール
 - Device Manager への仮想 WWN の登録 (仮想化サーバを vMA で管理する場合)



重要 一般ユーザーアカウントで Device Manager に登録したホストを、root アカウントを使って二重に登録しないでください。

関連項目

- ・ [12. Host Data Collector のセットアップ](#)

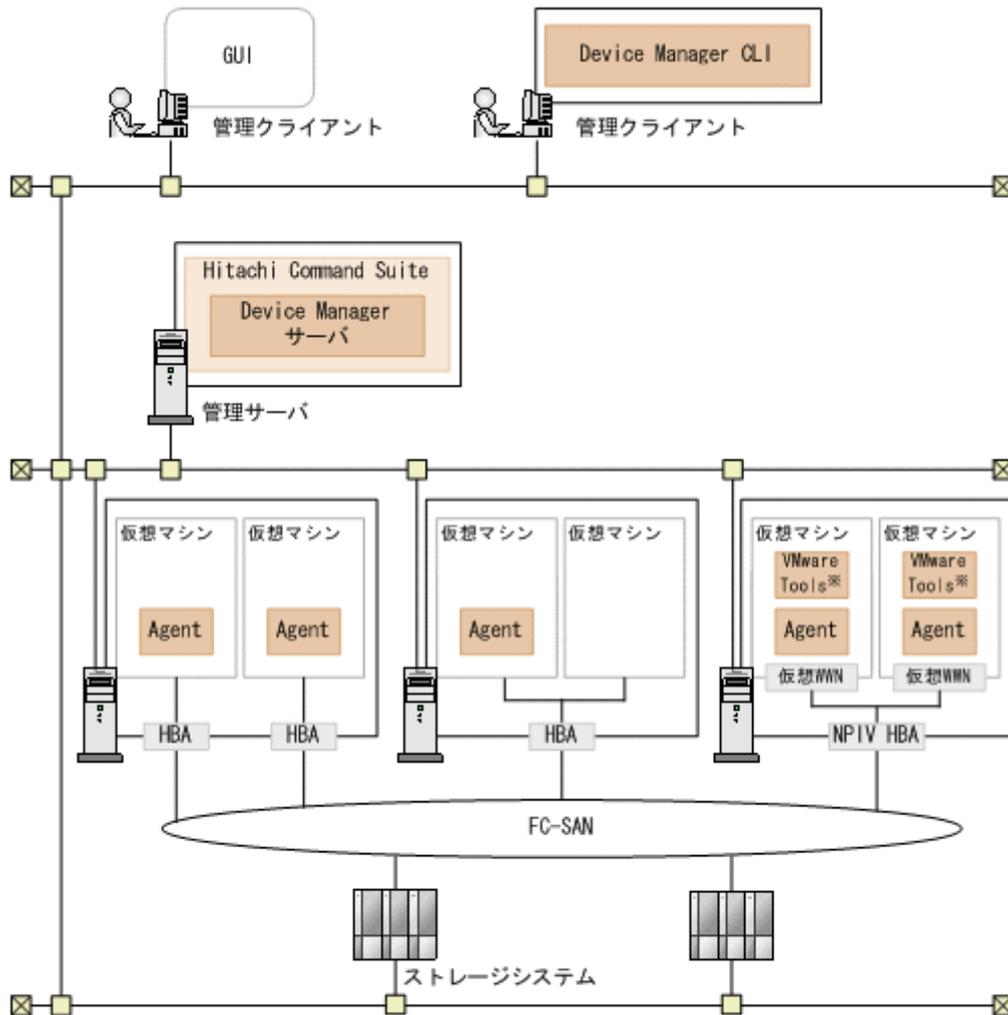
- ・ 仮想化サーバの登録方法：マニュアル「*Hitachi Command Suite Software ユーザーズガイド*」またはマニュアル「*Hitachi Command Suite Software CLI リファレンスガイド*」

(2) 仮想マシンの前提環境（Device Manager エージェントで管理する場合）

Device Manager エージェントで管理するためには、仮想マシンに Device Manager エージェントをインストールし、管理サーバの情報や HiScan コマンドの実行周期などを設定する必要があります。

HBA の構成によって、前提環境が異なります。

図 1-7 仮想マシンの前提環境（Device Manager エージェントで管理する場合）



(凡例)

Agent : Device Manager エージェント

注※ 仮想化ソフトウェアにVMware ESXを使用している場合に必要です。

- ・ 仮想マシンごとに HBA が割り当てられている構成
 - 仮想マシンごとに Device Manager エージェントをインストールしてください。
 - 仮想マシンの OS が AIX の場合、環境変数 ODMDIR を設定してください。
- ・ 複数の仮想マシンで HBA を共有している構成
 - 仮想マシンのうち、どれか 1 台にだけ Device Manager エージェントをインストールしてください。

- 仮想マシンの OS が AIX の場合、環境変数 ODMDIR を設定してください。
- 仮想マシンごとに仮想 HBA が割り当てられている構成（NPIV HBA を使用している場合）
 - 仮想マシンごとに Device Manager エージェントをインストールしてください。
 - 仮想化ソフトウェアに VMware ESX を使用している場合は、仮想マシンごとに VMware Tools をインストールしてください。
 - 同一の物理環境で稼働する仮想化サーバも Device Manager に登録してください。
Device Manager への仮想化サーバの登録は、vMA 経由でも Host Data Collector 経由でもかまいません。ただし、仮想化サーバを vMA で管理する場合は、Device Manager への仮想 WWN の登録が必要になります。
- 仮想マシンの OS が AIX の場合、環境変数 ODMDIR を設定してください。

関連項目

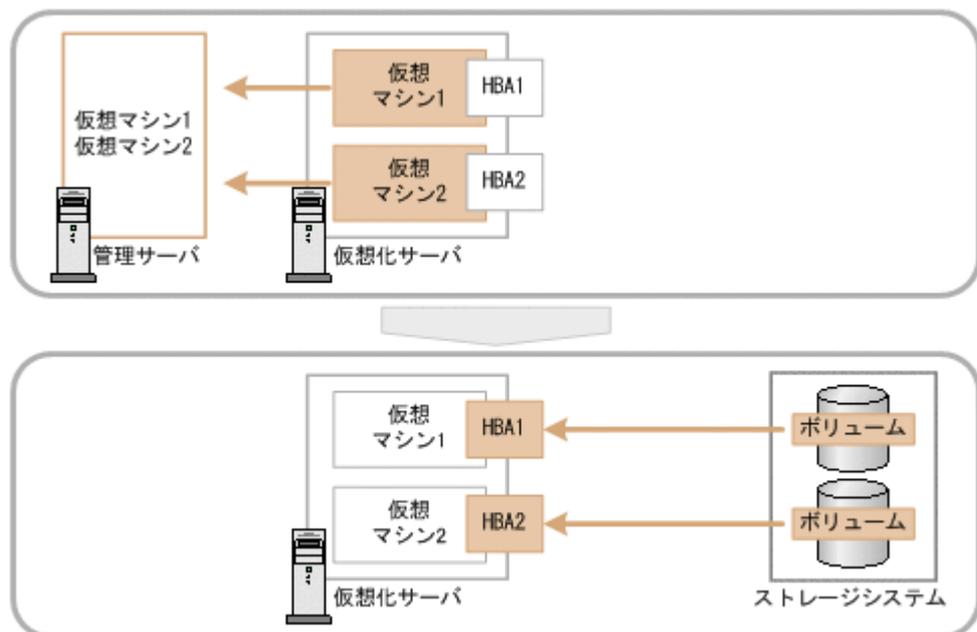
- Device Manager エージェントのセットアップ方法：マニュアル「*Hitachi Command Suite Software インストールガイド*」

(3) 仮想マシンにボリュームを割り当てるための操作フロー

HBA の構成によって、ホストの登録方法やボリュームの割り当て方法などが異なります。

仮想マシンごとに HBA が割り当てられている構成

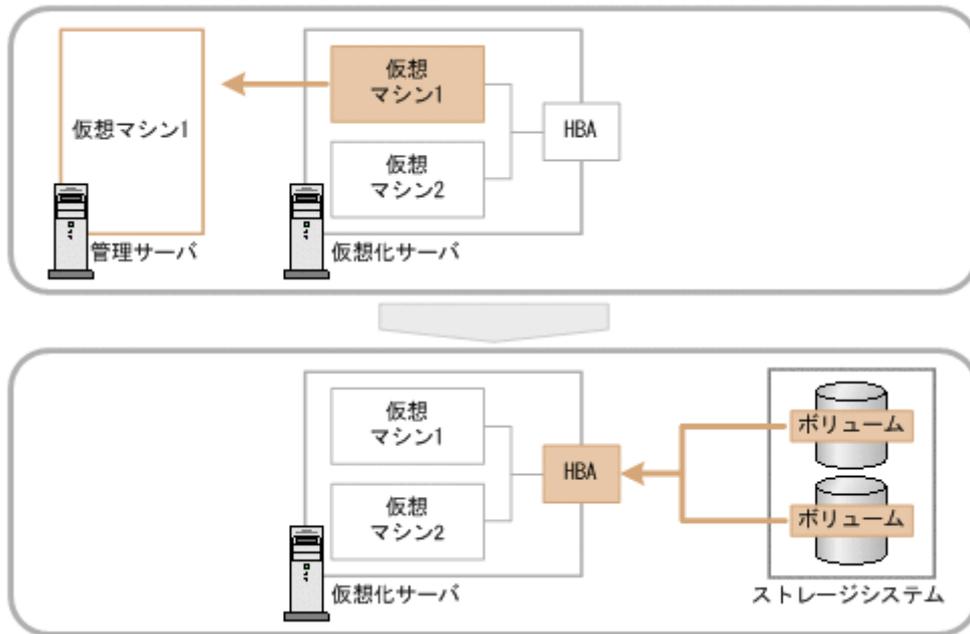
図 1-8 仮想マシンにボリュームを割り当てるための操作フロー（仮想マシンごとに HBA が割り当てられている構成）



1. ボリュームの使用状況を管理したい各仮想マシンを通常ホストとして Device Manager に登録します。
同一の物理環境で稼働する仮想化サーバは、Device Manager に登録しないでください。
2. 仮想マシン（WWN）ごとにボリュームの LUN パスを割り当て、割り当てたボリュームを仮想マシンに RAW デバイスとして認識させます。
データストアを構成しているボリュームは、Device Manager では認識されません。

複数の仮想マシンで HBA を共有している構成

図 1-9 仮想マシンにボリュームを割り当てるための操作フロー(複数の仮想マシンで HBA を共有している構成)



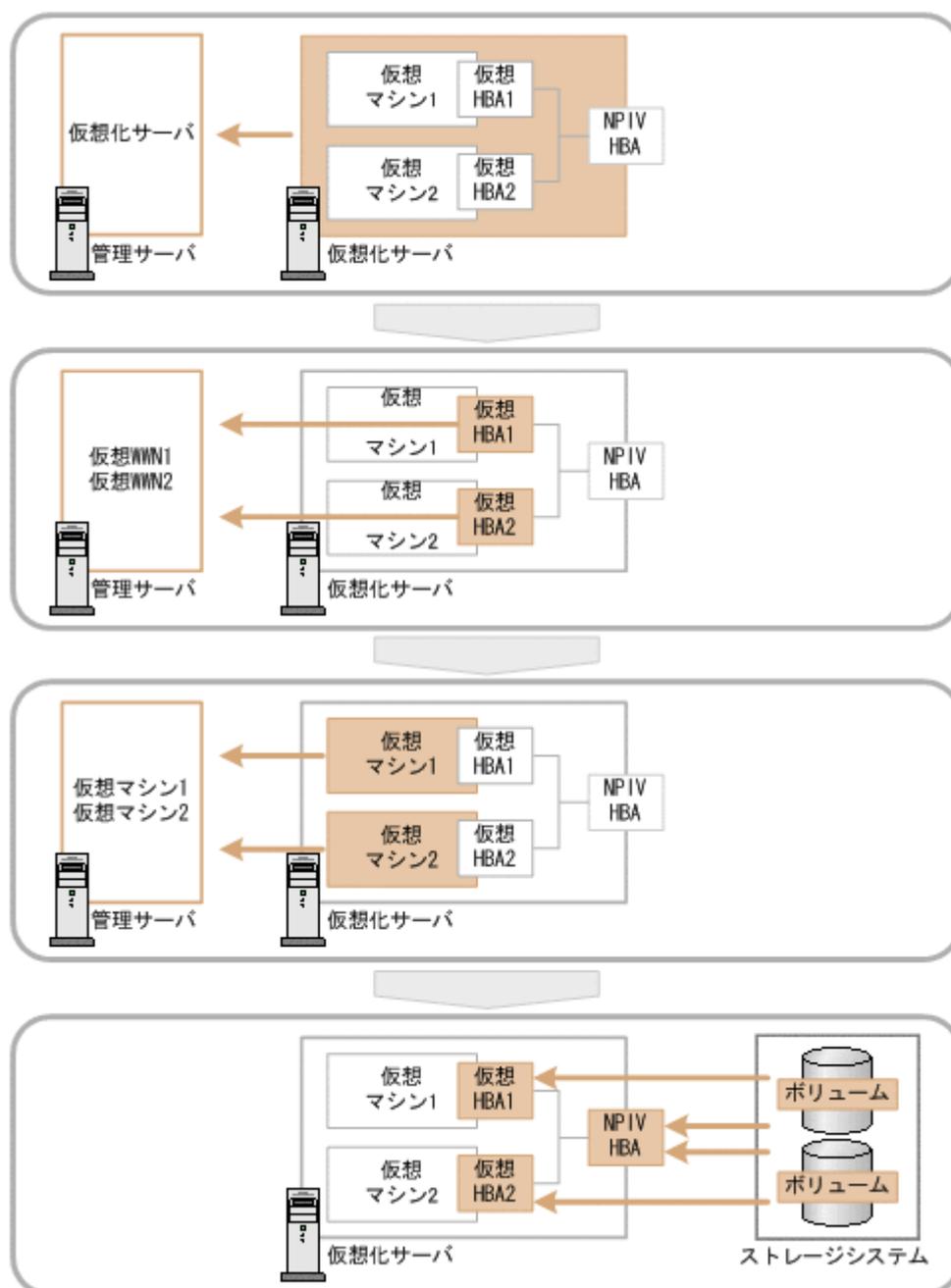
1. 仮想マシンが HBA を共有している仮想マシンのうち 1 台だけを通常ホストとして Device Manager に登録します。
同一の物理環境で稼働する仮想化サーバは、Device Manager に登録しないでください。
2. Device Manager に登録された仮想マシン (WWN) にボリュームの LUN パスを割り当て、割り当てたボリュームを仮想マシンに RAW デバイスとして認識させます。
データストアを構成しているボリュームは、Device Manager では認識されません。



重要 HBA を共有している別の仮想マシンにボリュームを割り当てたい場合も、Device Manager では、Device Manager の管理対象になっている仮想マシンに LUN パスを割り当てる必要があります。ボリュームが実際にはどの仮想マシンに割り当てられているかを、LUN パスの割り当て後に Device Manager で識別できるように、各ボリュームにラベルを設定しておくことをお勧めします。

仮想マシンごとに仮想 HBA が割り当てられている構成（NP IV HBA を使用している場合）

図 1-10 仮想マシンにボリュームを割り当てるための操作フロー（仮想マシンごとに仮想 HBA が割り当てられている構成）



1. ボリュームの使用状況を管理したい仮想マシンが稼働する仮想化サーバを Device Manager に登録します。
2. vMA で仮想化サーバを管理する場合は、createnpivinfo コマンドを実行し、各仮想 HBA に割り当てられた仮想 WWN を Device Manager に登録します。
3. ボリュームの使用状況を管理したい各仮想マシンを Device Manager に通常ホストとして登録します。
4. 仮想化サーバ（物理 WWN）と仮想マシン（仮想 WWN）の両方にボリュームの LUN パスを割り当て、RAW デバイスとしてボリュームを認識させます。
データストアを構成しているボリュームは、Device Manager では認識されません。

関連項目

- ・ 仮想化サーバの登録方法：マニュアル「*Hitachi Command Suite Software ユーザーズガイド*」またはマニュアル「*Hitachi Command Suite Software CLI リファレンスガイド*」

(4) 仮想 WWN を Device Manager に登録する (createnpivinfo コマンド)

NPIV HBA が使用されている仮想化サーバを vMA で管理している場合、createnpivinfo コマンドを実行して、各仮想マシンに割り当てられた仮想 WWN を Device Manager に登録しておく必要があります。

事前に完了しておく操作

- ・ 管理対象にする仮想マシンの起動
- ・ VMware Tools の起動
- ・ Device Manager への仮想化サーバの登録
詳細は、マニュアル「*Hitachi Command Suite Software ユーザーズガイド*」またはマニュアル「*Hitachi Command Suite Software CLI リファレンスガイド*」を参照してください。
- ・ Administrator 権限 (Windows の場合) または root 権限 (Solaris または Linux の場合) でのログイン

事前に確認しておく情報

- ・ 仮想化サーバ、または仮想化サーバを管理している VMware vCenter Server のホスト名または IP アドレス
- ・ 仮想化サーバ、または仮想化サーバを管理している VMware vCenter Server のユーザー ID
- ・ 仮想化サーバ、または仮想化サーバを管理している VMware vCenter Server のパスワード

仮想 WWN を Device Manager に登録するには：

1. 管理サーバで次のコマンドを実行して、仮想 WWN の情報を Device Manager に登録します。

Windows の場合：

```
< Device Manager サーバのインストールフォルダ > %HiCommandServer%\tools  
%createnpivinfo [-v] [<ホスト名または IP アドレス> <ユーザー ID> <パスワード>]
```

Solaris または Linux の場合：

```
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/tools/  
createnpivinfo [-v] [<ホスト名または IP アドレス> <ユーザー ID> <パスワード>]
```

○ -v

コマンドの実行結果の詳細を標準出力に表示する場合に指定します。

仮想マシンのホスト名と仮想 WWN が npivmapping.properties ファイルに出力されます。

Windows の場合：

```
< Device Manager サーバのインストールフォルダ > %HiCommandServer%\config  
%npivmapping.properties
```

Solaris または Linux の場合：

```
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/  
config/npivmapping.properties
```

(5) 仮想マシンの構成変更時に必要な作業

仮想マシンごとに仮想 HBA が割り当てられている (NPIV HBA を使用している) 構成の場合、仮想マシンの構成が変更になったら、Device Manager に仮想マシンの情報を反映する必要があります。

仮想マシンを別の仮想化サーバに移動した場合

移動元と移動先の仮想化サーバの情報を Device Manager で更新 (リフレッシュ) する必要があります。移動元の仮想化サーバにボリュームが割り当てられていない状態になるときには、Device Manager から移動元の仮想化サーバの情報を手動で削除してください。

仮想 WWN を追加または変更した場合

- a. createnpivinfo コマンドを実行し、仮想 WWN を Device Manager に登録する。
仮想化サーバが vMA で管理されている場合に必要な作業です。
- b. Device Manager GUI/CLI で、Device Manager に登録された仮想マシンおよび仮想化サーバの情報をリフレッシュする。

コマンドデバイスを設定または解除した場合

仮想化サーバを再起動してください。

ホスト名を変更した場合、または仮想マシンを撤去した場合

npivmapping.properties ファイルを手動で更新してください。

Windows の場合 :

```
< Device Manager サーバのインストールフォルダ > %HiCommandServer%\config  
%npivmapping.properties
```

Solaris または Linux の場合 :

```
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/  
config/npivmapping.properties
```

関連項目

- ・ 仮想マシンおよび仮想化サーバのリフレッシュ方法 : マニュアル「Hitachi Command Suite Software ユーザーズガイド」またはマニュアル「Hitachi Command Suite Software CLI リファレンスガイド」

1.4.5 仮想化サーバのシステム要件

仮想化サーバを Device Manager で管理するためには、Host Data Collector または vMA が必要です。

Device Manager は、Host Data Collector または vMA を使用して、仮想化サーバのマシン情報および仮想化サーバに割り当てられているボリュームの情報を収集します。

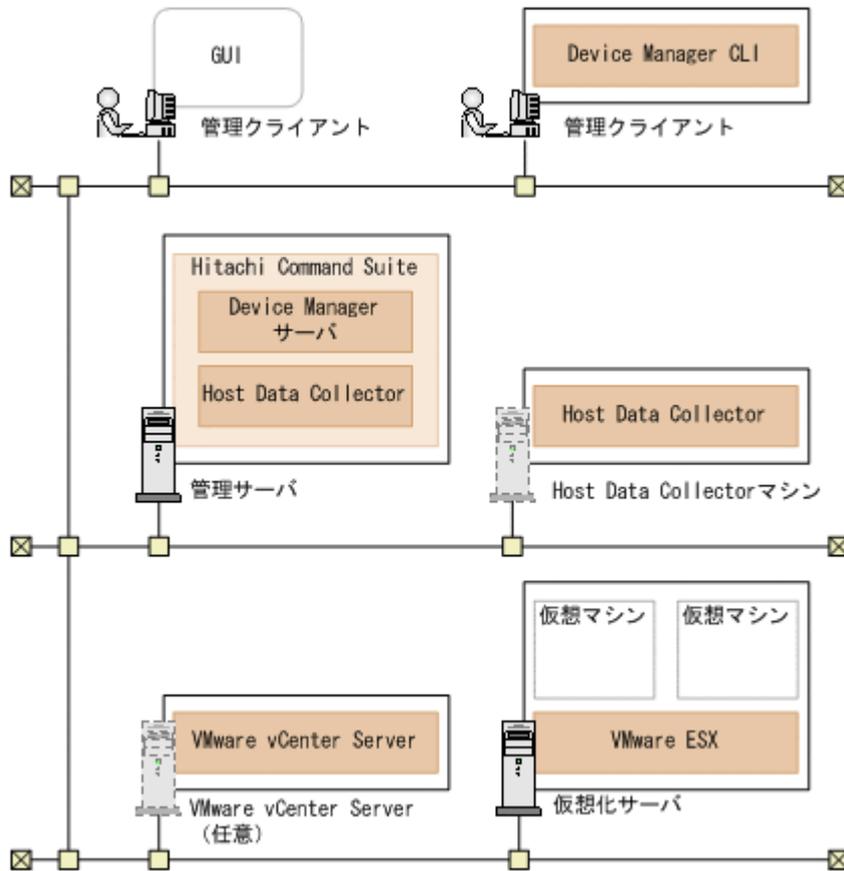
Host Data Collector と vMA のどちらで仮想化サーバを管理するかによって、前提となるシステム構成や環境設定が異なります。

(1) 仮想化サーバの前提環境 (Host Data Collector で管理する場合)

Host Data Collector で仮想化サーバを管理するためには、Host Data Collector のインストールが必要です。

Host Data Collector で管理できる仮想化サーバは、VMware ESX 4.x、VMware ESXi 4.x または VMware ESXi 5.x です。

図 1-11 仮想化サーバの前提環境（Host Data Collector で管理する場合）



- Host Data Collector は、管理サーバにインストールする Hitachi Command Suite に同梱されているほか、管理サーバ以外のマシンにインストールすることもできます。
 なお、Host Data Collector マシンを複数台設置する場合は、各マシンにインストールされた Host Data Collector のバージョンおよびリビジョンを同じにしてください。
- 仮想化サーバ上の仮想マシンに仮想 HBA が割り当てられている場合は、その仮想マシンに VMware Tools をインストールする必要があります。
- Host Data Collector マシンと仮想化サーバ、Host Data Collector マシンと VMware vCenter Server の通信には、IPv6 も使用できます。

関連項目

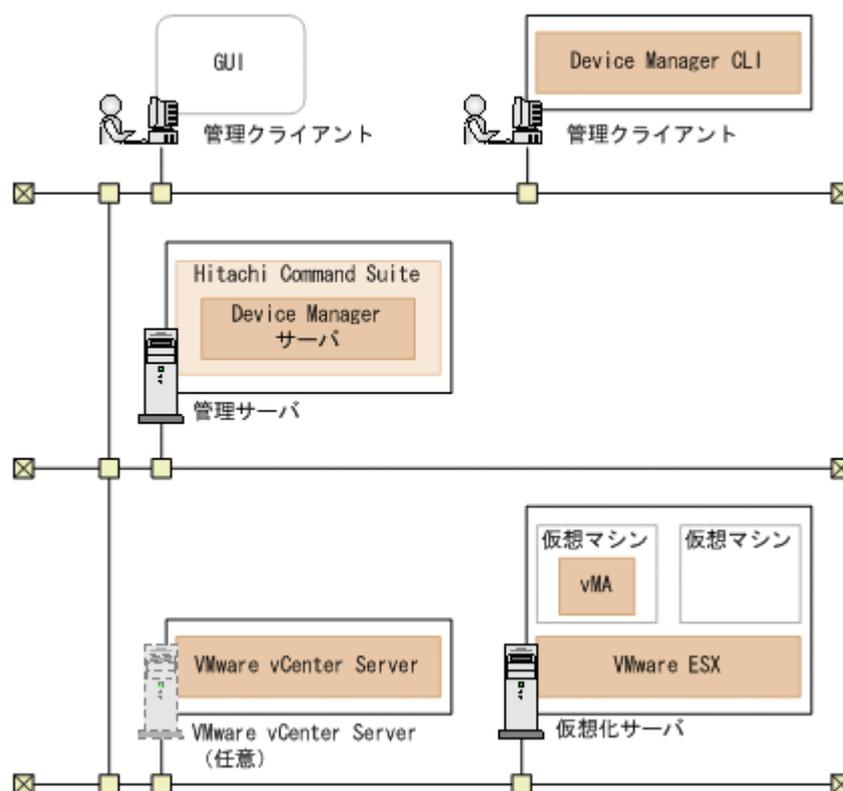
- 12. Host Data Collector のセットアップ

(2) 仮想化サーバの前提環境（vMA で管理する場合）

vMA で仮想化サーバを管理するためには、vMA のデプロイが必要です。

vMA で管理できる仮想化サーバは、VMware ESX 4.x または VMware ESXi 4.x です。

図 1-12 仮想化サーバの前提環境 (vMA を使用する場合)



- 仮想化サーバに vMA をデプロイし、仮想化サーバまたは VMware vCenter Server を vMA の監視対象に設定する必要があります。
- Device Manager サーバと vMA との通信には、IPv6 も使用できます。ただし、Device Manager サーバと vMA との通信に IPv6 を使用する場合であっても、次の通信は IPv4 で行われるように環境構築する必要があります。
 - vMA と VMware ESX との通信
 - vMA と VMware vCenter Server との通信
 - VMware vCenter Server と VMware ESX との通信

Device Manager では、vMA が仮想化サーバを直接監視する構成と、VMware vCenter Server 経由で仮想化サーバを監視する構成をサポートしています。

(3) vMA での仮想化サーバの監視構成

Device Manager でサポートしている構成には、vMA が仮想化サーバを直接監視する構成と、VMware vCenter Server 経由で仮想化サーバを監視する構成があります。

vMA で VMware ESX を監視する構成

仮想化サーバに vMA をデプロイし、仮想化サーバを vMA の監視対象にした構成です。

図 1-13 vMA で同じ物理環境の VMware ESX を監視する場合のシステム構成

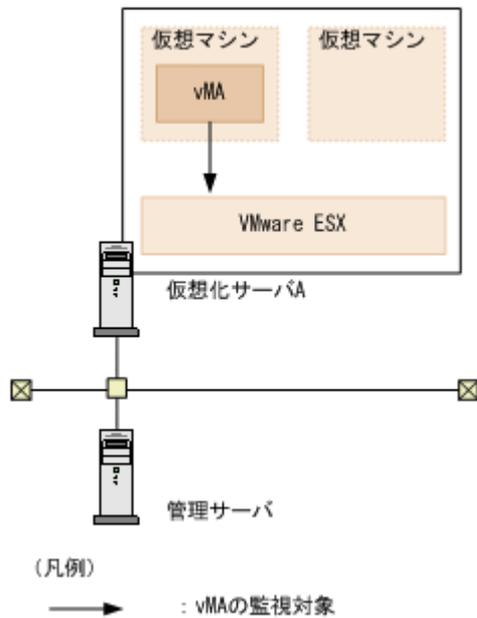
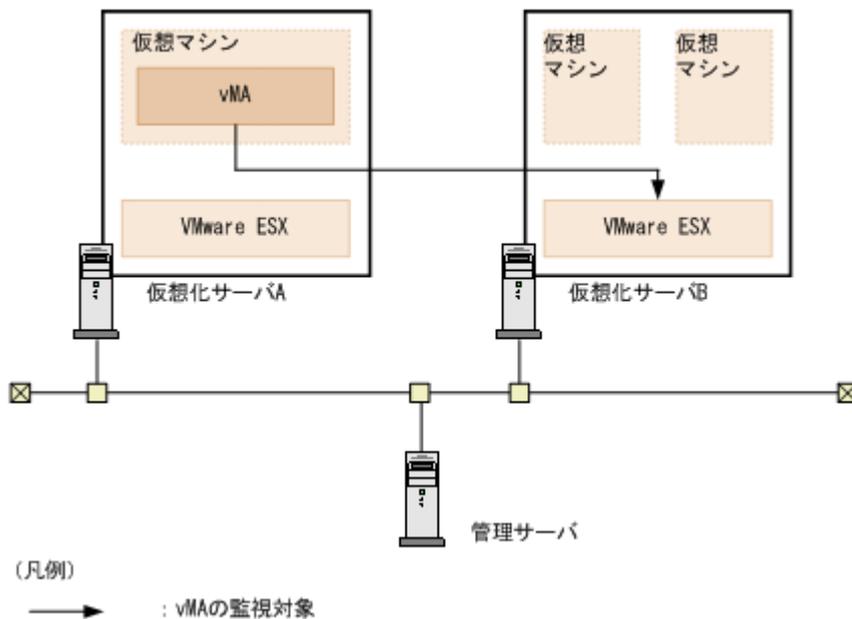


図 1-14 vMA で別の物理環境の VMware ESX を監視する場合のシステム構成



仮想化サーバを Device Manager に登録するためには、vMA の IP アドレスやユーザーアカウント情報を指定する必要があります。vMA の情報を指定すると、vMA の管理対象の物理環境が仮想化サーバとして登録されます。

また、vMA の管理対象の VMware ESX が、vMA が稼働する物理環境とは別の物理環境で稼働している場合も、vMA の情報を Device Manager に登録してください。



重要

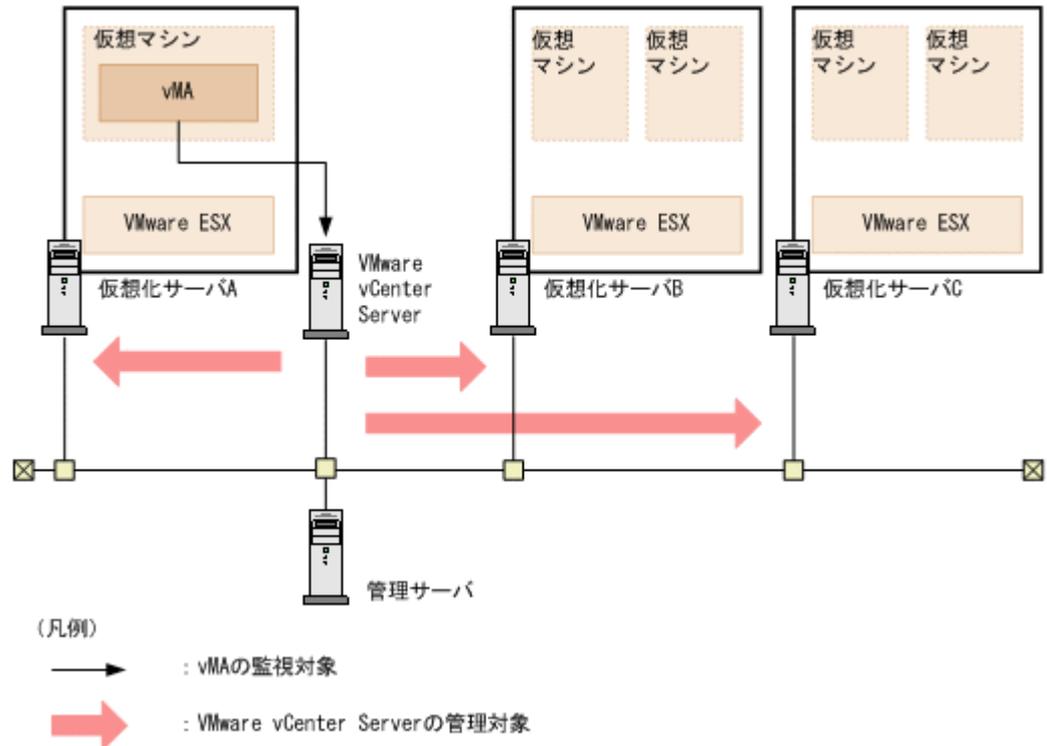
- NPIV HBA を使用した構成を除いて、仮想化サーバ上で稼働する仮想マシンは Device Manager の管理対象にはしないでください。
- vMA の IP アドレスやユーザーアカウント情報を変更した際には、Device Manager に vMA を再登録する必要があります (削除する必要はありません)。

- ・ 仮想化サーバを別の vMA の管理下に移動した場合は、移動元の vMA を再登録したあと、移動先の vMA を再登録する必要があります（削除する必要はありません）。

vMA で VMware vCenter Server を監視する構成

仮想化サーバに vMA をデプロイし、VMware vCenter Server を vMA の監視対象にした構成です。

図 1-15 vMA で VMware vCenter Server を監視する場合のシステム構成



仮想化サーバを Device Manager に登録するためには、vMA の IP アドレスやユーザーアカウント情報を指定する必要があります。vMA の情報を指定すると、VMware vCenter Server の管理対象の物理環境が仮想化サーバとして登録されます。



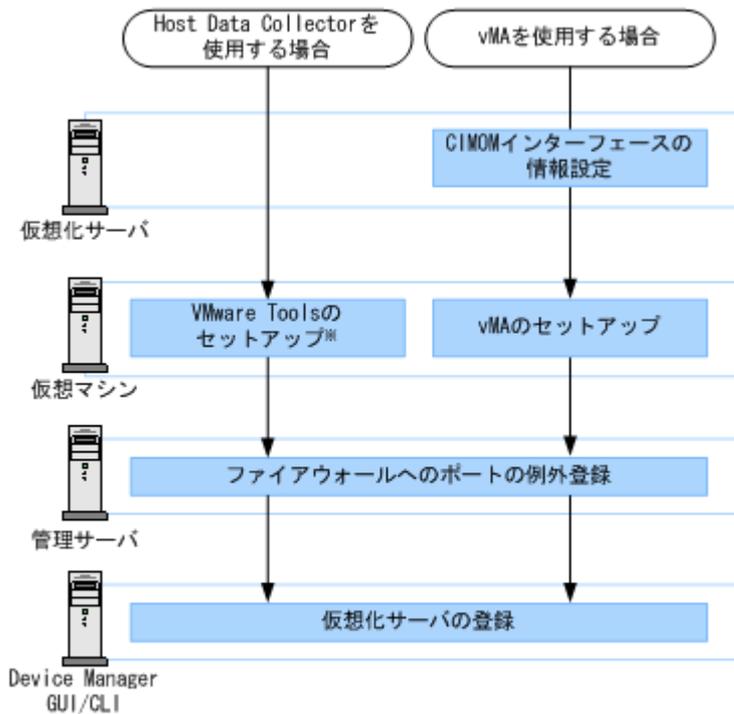
重要

- ・ NPIV HBA を使用した構成を除いて、仮想化サーバ上で稼働する仮想マシンは Device Manager の管理対象にはしないでください。
- ・ 次の場合には、Device Manager に vMA を再登録する必要があります（削除する必要はありません）。
vMA の IP アドレスやユーザーアカウント情報の変更
VMware vCenter Server の管理下にある仮想化サーバの増減設
- ・ 仮想化サーバを別の VMware vCenter Server の管理下に移動した場合は、次の操作を Device Manager で実行する必要があります。
 1. 仮想化サーバの通信パラメーターを移動先の VMware vCenter Server を監視する vMA の情報に変更する。
 2. 仮想化サーバの情報を更新（リフレッシュ）する。

(4) 仮想化サーバを管理対象にするための操作フロー

Device Manager で仮想化サーバを管理するためには、事前に環境設定が必要です。

図 1-16 仮想化サーバを管理対象にするための操作フロー



注※ 仮想マシンに仮想HBAが割り当てられている場合に必要な作業です。

(5) 仮想化サーバの運用に関する注意事項

仮想化サーバの運用に関する注意事項は次のとおりです。

- 最新の仮想化サーバのボリューム情報を確認したい場合は、Device Manager で次のどちらかの操作が必要です。
 - 仮想化サーバごとに手動リフレッシュを実行する
 - 管理元の vMA を Device Manager に再登録する（削除する必要はありません）

なお、仮想化サーバのハードウェア構成を変更した場合は、vMA および VMware vCenter Server に監視対象の仮想化サーバの構成情報が反映されたあとに、Device Manager の情報を更新（リフレッシュ）する必要があります。仮想化サーバの構成情報が vMA および VMware vCenter Server に自動的に反映されるよう設定されている場合は、構成を変更してから vMA および VMware vCenter Server に情報が反映されるまでの間にタイムラグが発生することがあります。

vMA および VMware vCenter Server に仮想化サーバの構成情報を反映する方法や、反映間隔を調整する方法については、VMware 社のドキュメントを参照してください。

- Logical Domains を使用する場合、サービスドメインの物理ディスクをゲストドメインの仮想ディスクとしてエクスポートするときは、フルディスクを指定してください。スライスディスクを指定すると、仮想ディスクの情報を正常に取得できなくなります。

1.4.6 メインフレームホストのシステム要件

Device Manager および Tiered Storage Manager では、Mainframe Agent と連携することで、メインフレームボリュームに対して次のことができます。

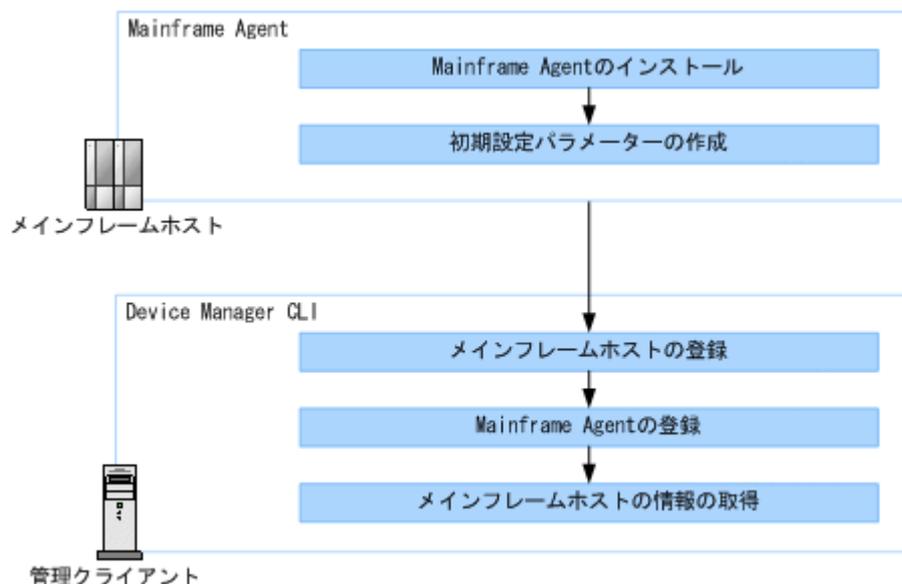
- メインフレームボリュームの使用状況やストレージシステムの論理 DKC シリアル番号の参照 (Device Manager)

- ・ メインフレームボリュームのマイグレーションやシュレディング (Tiered Storage Manager)

(1) メインフレームホストを管理対象にするための操作フロー

Mainframe Agent と連携してメインフレームホストのボリュームを管理するためには、Mainframe Agent と Device Manager でそれぞれ環境設定が必要です。

図 1-17 メインフレームホストを管理対象にするための操作フロー



関連項目

- ・ Device Manager CLI での環境設定：マニュアル「*Hitachi Command Suite Software CLI リファレンスガイド*」
- ・ Mainframe Agent での環境設定：マニュアル「*Hitachi Command Suite Software Mainframe Agent ユーザーズガイド*」

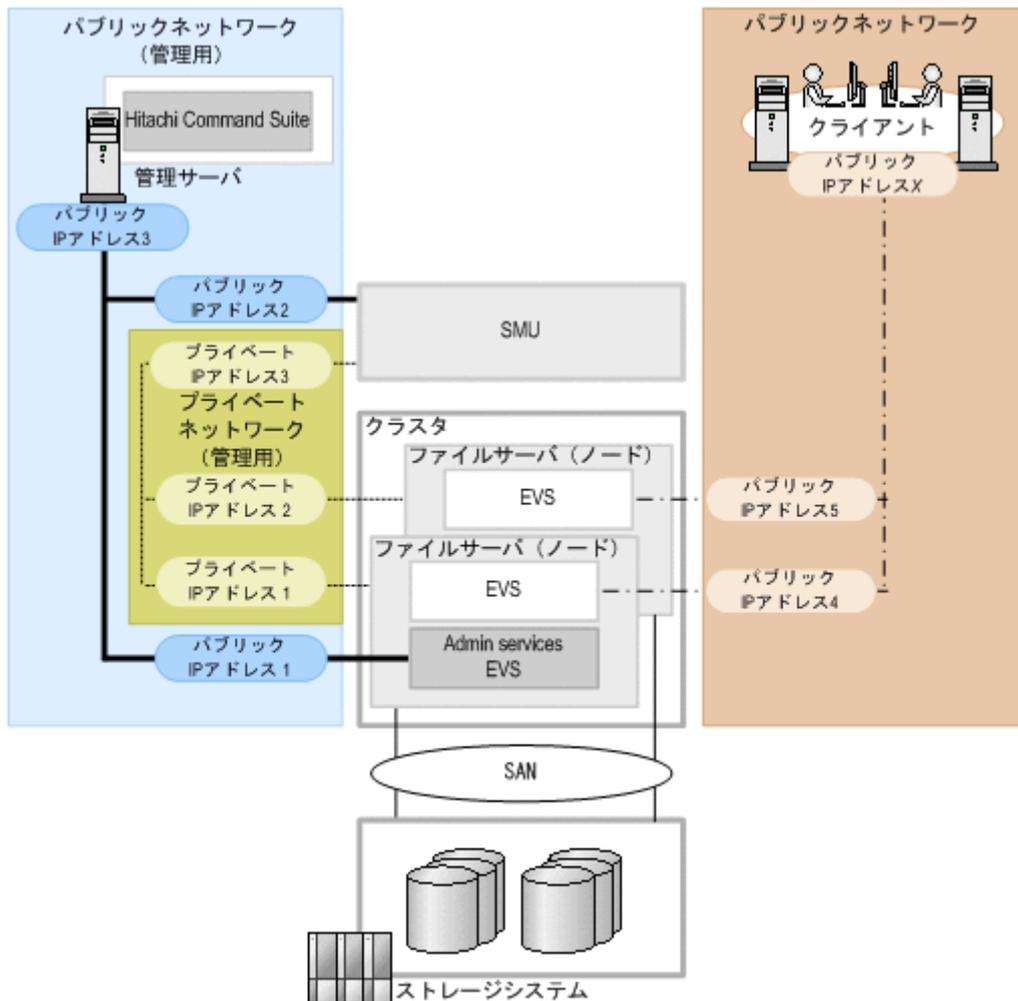
1.4.7 ファイルサーバのシステム要件

Device Manager では、ストレージシステムのボリュームをファイルサーバに割り当てたり、ファイルサーバの情報を確認したりできます。

(1) Hitachi NAS Platform の前提環境

Device Manager で Hitachi NAS Platform を管理するためには、管理サーバが System Management Unit (SMU) および Admin services EVS と通信できるシステム構成にする必要があります。

図 1-18 Hitachi NAS Platform の前提環境



- 管理サーバは、SMU および Admin services EVS と通信できるネットワーク上に設置してください。
- SMU のバージョンは、ファイルサーバ (ノード) のファームウェアのバージョン以上にしてください。
- クラスタ内のファイルサーバ (ノード) のファームウェアのバージョンは一致させてください。
- Hitachi NAS Platform を Device Manager で管理する場合は、Device Manager GUI でクラスタごとに次の情報を登録してください。
 - Admin services EVS の IP アドレス (図中のパブリック IP アドレス 1)
IP アドレスは、SMU の [EVS Management] ページで確認できます。
 - Server Control (SSC) 用のユーザーアカウント
デフォルトユーザーとして supervisor アカウントが用意されています。



重要 Device Manager GUI で、ファイルサーバのシステムドライブやストレージプール、ファイルシステム、ファイル共有などの情報を確認したい場合は、ストレージシステムのボリュームからファイルサーバに対して LUN セキュリティを設定しておく必要があります。

関連項目

- SMU での設定方法 : Hitachi NAS Platform のマニュアル

(2) Hitachi Virtual File Platform の前提環境

Device Manager で Hitachi Virtual File Platform を管理するためには、Hitachi File Services Manager がインストールされた管理サーバと、Device Manager がインストールされた管理サーバが通信できるシステム構成にする必要があります。

Device Manager で行う運用によって、Hitachi File Services Manager のインストール条件が異なります。

表 1-6 Hitachi File Services Manager のインストール条件

Device Manager からの操作	Device Manager と同じ管理サーバにインストールした場合	Device Manager と異なる管理サーバにインストールした場合
Hitachi File Services Manager (ログイン画面) のラウンチ	○	○
ファイルサーバの登録, 管理	○	○
ファイルサーバへのボリュームの割り当て	○	○
ファイルシステムの作成, 拡張および削除	○	×
ファイル共有の追加, 編集および解除	○	×
ダッシュボードでのファイルシステムおよびスナップショットの容量情報の確認	○	×
ファイルサーバのアラート監視	○	○

(凡例)

- : 実行できる
- × : 実行できない

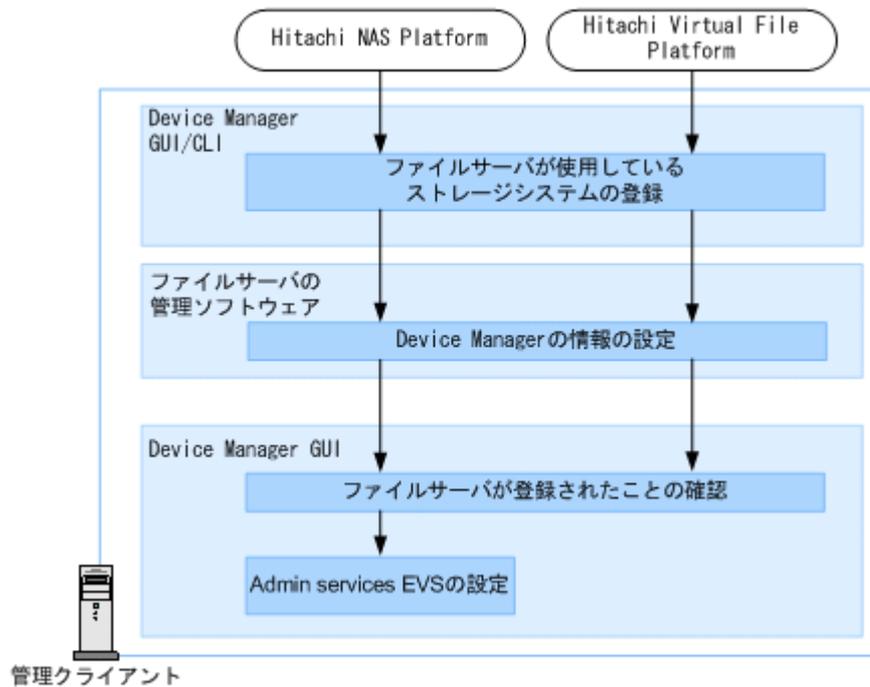
関連項目

- ・ [6.3 アラートの設定](#)
- ・ Hitachi File Services Manager のインストール方法および環境設定 : Hitachi Virtual File Platform のマニュアル
- ・ Hitachi File Services Manager の前提バージョン : ソフトウェア添付資料

(3) ファイルサーバを管理対象にするための操作フロー

Device Manager でファイルサーバにボリュームを割り当てたり、ボリューム情報を参照したりするためには、ファイルサーバの管理ソフトウェアと Device Manager でそれぞれ環境設定が必要です。

図 1-19 ファイルサーバを管理対象にするための操作フロー



重要 ファイルサーバで使用できるストレージシステムについては、ファイルサーバのマニュアルを参照してください。

関連項目

- Device Manager GUI/CLI での設定方法：マニュアル「*Hitachi Command Suite Software ユーザーズガイド*」またはマニュアル「*Hitachi Command Suite Software CLI リファレンスガイド*」
- ファイルサーバ管理ソフトウェアでの設定方法：ファイルサーバのマニュアル

(4) ファイルサーバの運用に関する注意事項

ファイルサーバの運用に関する注意事項は次のとおりです。

- Device Manager をバージョン 6.3 以前からアップグレードインストールした場合、ファイルサーバを管理するためには、`server.properties` ファイルの `server.http.entity.maxLength` プロパティの値を 1310720 以上に変更しておくことをお勧めします。
- Hitachi NAS Platform の場合、ファイルサーバの情報は毎日 AM 3:00 に Device Manager のデータベースに反映されます。
SMU の [Hitachi Device Managers] 画面で同期操作を実行すると、ユーザーの任意のタイミングで Hitachi NAS Platform の最新の情報を Device Manager のデータベースに反映できます。
- Hitachi Virtual File Platform の場合、ファイルサーバの情報は毎日 1 回 Device Manager のデータベースに反映されます。反映時刻は Hitachi File Services Manager で設定します。また、ファイルサーバの情報を Hitachi File Services Manager のデータベースに反映する際に、自動的に Device Manager のデータベースにも反映されるように設定できます。

関連項目

- [A.1.1 Device Manager サーバのプロパティの変更](#)

- [A.2.5 server.http.entity.maxLength](#)
- SMU での設定方法 : Hitachi NAS Platform のマニュアル
- Hitachi File Services Manager での設定方法 : Hitachi Virtual File Platform のマニュアル

1.5 関連製品

Device Manager および Tiered Storage Manager の関連製品について説明します。

Replication Manager

Replication Manager は、ストレージネットワークに分散するレプリケーションボリュームの構成や稼働状況を一元的に管理するための製品です。Replication Manager の GUI は、Device Manager の GUI から表示できます。

Tuning Manager

Tuning Manager は、ストレージネットワーク全体の性能や容量を一元的に監視し、ストレージシステムの安定稼働を支援する製品です。Tuning Manager の GUI は、Device Manager の GUI から表示できます。

Dynamic Link Manager

Dynamic Link Manager は、ストレージシステムとホスト間の LUN パスをホストごとに管理するための製品です。

Global Link Manager

Global Link Manager は、複数のホストに対する LUN パスを一元管理するための製品です。Global Link Manager の GUI は、Device Manager の GUI から表示できます。

Compute Systems Manager

Compute Systems Manager は、大規模なシステム環境でホスト（業務サーバ）の運用と管理を支援する製品です。ホストの資産情報の収集、障害情報の確認、電源の制御などができます。Compute Systems Manager の GUI は、Device Manager の GUI から表示できます。

Hitachi File Services Manager

Hitachi File Services Manager は、Hitachi Virtual File Platform を運用および管理するための製品です。Hitachi File Services Manager の GUI は、Device Manager の GUI から表示できます。

JP1/IM

JP1/IM は、ジョブ管理やストレージ管理などのミドルウェア製品である JP1 シリーズと連携して、システム全体を統合管理するための製品です。

Device Manager および Tiered Storage Manager では、JP1/IM と連携することで次のことができます。

- JP1/IM の統合機能メニュー画面から、Hitachi Command Suite 製品の GUI を起動する
- JP1/IM の統合コンソールで、Device Manager および Tiered Storage Manager のログ（Windows : イベントログ, Solaris または Linux : syslog）を参照する

なお、JP1/IM と連携するためには、JP1/Base および JP1/IM での環境設定が必要です。

JP1/NETM/DM

JP1/NETM/DM は、ネットワークを利用して、ソフトウェアの配布やクライアントの資産管理を実現するための製品です。JP1/NETM/DM を利用することで、クライアント管理の自動化・省力化を図れます。

Device Manager では、JP1/NETM/DM と連携することで、Device Manager エージェントをリモートインストールできます。

関連項目

- 5.4 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするために必要な設定
- 6.6 JP1/IM でログを参照するために必要な設定

1.6 Device Manager でのコピーペア管理

Device Manager では、ストレージシステムのボリュームを複製し、大切な業務データを冗長化することで、システムの信頼性の向上を図れます。

Device Manager では、複製する正ボリューム (P-VOL) と副ボリューム (S-VOL) の組を「コピーペア」と呼びます。

Device Manager では、次の方法でコピーペアを管理できます。

- GUI
Device Manager GUI から Replication Manager GUI をラUNCHすることで、コピーペアを定義したりペア状態を変更したりできます。Replication Manager のライセンスを登録していない場合にも、Device Manager のライセンスだけで Replication Manager の一部の機能を使用できます。
- CLI
Device Manager CLI でコピーペアを定義したりペア状態を変更したりできます。

1.6.1 Device Manager でコピーペアを管理できるストレージシステム

Device Manager でコピーペアを管理できるストレージシステムは、GUI を使う場合と CLI を使う場合で異なります。

表 1-7 Device Manager でコピーペアを管理できるストレージシステム

ストレージシステム	GUI	CLI
Virtual Storage Platform	○	○
Universal Storage Platform V/VM	○	○
Hitachi USP	○	○
SANRISE9900V	×	×
HUS VM	○	○
HUS100	○	○
Hitachi AMS2000	○	○
Hitachi AMS/WMS	○	○
SANRISE9500V	×	○

(凡例) ○ : サポート, × : 非サポート

関連項目

- 1.6.2 コピーペアを管理する場合のシステム構成
- 1.6.3 コピーペアを管理する場合のストレージシステムの要件

1.6.2 コピーペアを管理する場合のシステム構成

Device Manager では、コピーペアを管理する場合、4つのシステム構成をサポートしています。

- 通常構成
各業務サーバにコマンドデバイスをファイバーチャネル接続して、ホストごとにコピーペアを管理する構成です。
- ペア管理サーバを使用した構成（一括管理構成）
業務サーバとは別に、1台のマシン（ペア管理サーバ）にコマンドデバイスをファイバーチャネル接続して、コピーペアを一括管理する構成です。
一括管理構成では、Device Manager エージェントをインストールできない OS のホストのコピーペアも管理できます。
- 仮想コマンドデバイスサーバを使用した構成
1台のマシン（仮想コマンドデバイスサーバ）にコマンドデバイスをファイバーチャネル接続し、LAN 上のマシンから仮想コマンドデバイスサーバを経由してコピーペアを管理する構成です。
- 仮想コマンドデバイスに SVP を使用した構成
ストレージシステムの物理コマンドデバイスの代わりに、SVP を仮想コマンドデバイスとして使用して、コピーペアを直接管理する構成です。ストレージシステムにコマンドデバイスを用意する必要がありません。この構成は P-VOL と S-VOL の両方が Virtual Storage Platform または HUS VM に存在する場合にだけサポートされています。
構成定義ファイルを使用してコピーペアを定義・管理する構成と、デバイスグループとしてコピーペアを定義・管理する構成があります。



重要

- SVP を使用した構成（Out-of-band 方式）でコピーペアを管理する場合、物理コマンドデバイスを使用した構成（In-band 方式）でコピーペアを管理する場合に比べて、RAID Manager のコマンドの応答時間が増加する傾向があるため、Replication Manager の処理時間も増加することがあります。
- SVP を使用した構成の場合、GUI では、デバイスグループとして定義されたコピーペアの構成の確認とペア状態の変更もできます。



注意 Device Manager 以外の管理ツールで作成したコピーペアを、Device Manager で管理する場合は、次の点に注意してください。

- Storage Navigator, SVP, または RAID Manager LIB で作成したコピーペアの場合
次のどちらかの対応が必要です。
 - 構成定義ファイルを手動で作成し、コピーペアを定義する。
 - 作成時に使用した管理ツールでコピーペアを解除したあと、Device Manager でコピーペアを作成する。
- コピーグループに定義された Thin Image コピーペアの場合
Device Manager GUI で 65 世代以上のコピーペアを管理する場合は、既存のコピーグループを削除したあと、スナップショットグループでコピーペアを作成してください。
Device Manager CLI で管理する場合は、コピーペア作成時に使用した管理ツールでコピーペアを解除したあと、Device Manager CLI でコピーペアを作成してください。



注意 仮想 ID を用いたデータ移行に使用しているリソースグループに属するボリュームを指定してコピーペアを定義または管理する場合の要件を次に示します。

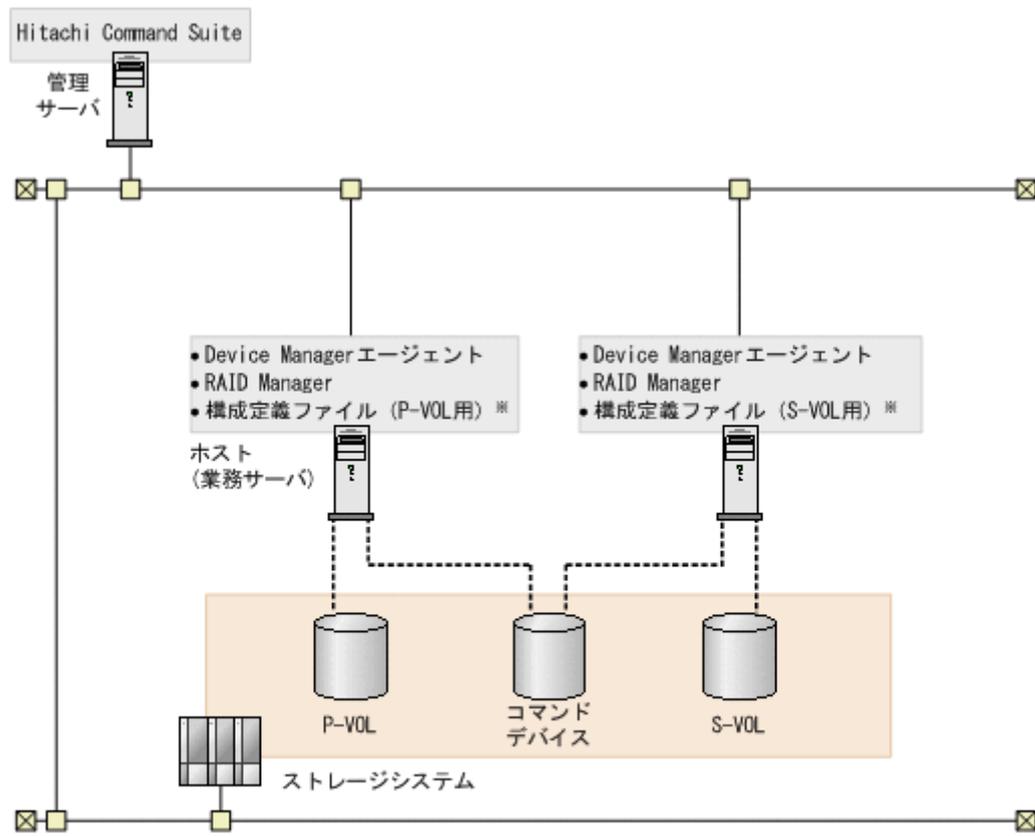
- コピーペアの管理方法は、一括管理構成である必要があります。
- 構成定義ファイルを移行後の環境に合わせて再作成する必要があります。
 - HORCM_LDEV パラメーターの Serial# に物理 ID を指定する。
 - HORCM_CMD パラメーターに、ストレージシステムリソースグループ ID が 0 (meta_resource) のコマンドデバイスを指定する。

- ・ コマンドデバイスの認証モードを有効にし、ストレージシステムリソースグループ ID が 0 (meta_resource) のすべてのコマンドデバイスに対して、raidcom -login コマンドを実行して、ユーザー認証を行ってください。ペア管理サーバの OS が Windows の場合は、Device Manager エージェントのサービス (HBsA Service) の実行ユーザーでユーザー認証を行ってください。

(1) 通常構成でコピーペアを管理する場合のシステム構成

前提条件を満たすように管理サーバやホスト（業務サーバ）、ストレージシステムを構築してください。

図 1-20 コピーペア管理のシステム構成例（通常構成）



(凡例)

----- : LUNセキュリティが設定されていることを示します。

注※ スナップショットグループに定義されたThin Imageコピーペアは、構成定義ファイルは不要です。

管理サーバの条件

次のマシンが Device Manager の管理リソースとして登録されていること。

- P-VOL を認識しているホスト
- S-VOL を認識しているホスト

ホスト（業務サーバ）の条件

- Device Manager エージェントがインストールされていること。
 - ・ P-VOL を認識しているホストと S-VOL を認識しているホストが 1 台ずつある場合、それぞれのホストに Device Manager エージェントをインストールしてください。
 - ・ P-VOL を認識しているホストと S-VOL を認識しているホストが複数台ある場合、P-VOL を認識しているホストのうちの 1 台と、S-VOL を認識しているホストのうちの 1 台に Device Manager エージェントをインストールしてください。

ただし、スナップショットグループに定義されたコピーペアの場合、P-VOL を認識しているホストに Device Manager エージェントをインストールしてください (S-VOL を認識しているホストへのインストールは不要です)。

- RAID Manager がインストールされていること。

P-VOL を認識しているホストと S-VOL を認識しているホストが複数台ある場合、P-VOL を認識しているホストのうちの 1 台と、S-VOL を認識しているホストのうちの 1 台に RAID Manager をインストールしてください。

ホストが認識しているコマンドデバイスが認証機能に対応している場合は、バージョン 01-25-03/01 以降の RAID Manager をインストールしてください。

また、1 台のホストで H シリーズとそれ以外の日立ストレージシステムのコピーペアを管理する場合には、RAID Manager と P9000 RAID Manager の両方をインストールする必要があります。

- NIC が複数ある場合、Device Manager エージェントおよび RAID Manager が利用する IP アドレスが同じであること。

コピーペア (P-VOL および S-VOL) の条件

- P-VOL および S-VOL が 1 台の管理サーバ (Device Manager サーバ) で管理されていること。
- P-VOL および S-VOL がホスト (業務サーバ) に認識されていること (ただし、スナップショットグループに定義されたコピーペアを管理する場合は、S-VOL を認識している必要はありません)。

P-VOL と S-VOL は別のホストに割り当てることを推奨します。

- P-VOL および S-VOL から、ホスト (業務サーバ) に対して、LUN セキュリティが設定されていること。

P-VOL および S-VOL から、それぞれ異なるホストに LUN セキュリティが割り当てられていてもかまいません。

コマンドデバイスの条件

- コマンドデバイスが、P-VOL を認識しているホストと S-VOL を認識しているホストの両方に認識されていること (ただし、スナップショットグループに定義されたコピーペアを管理する場合は、S-VOL を認識しているホストがコマンドデバイスを認識している必要はありません)。

- コマンドデバイスから、P-VOL または S-VOL を認識しているホストに対して、LUN セキュリティが設定されていること。

P-VOL を認識しているホストに対しては P-VOL 側のコマンドデバイスから、S-VOL を認識しているホストに対しては S-VOL 側のコマンドデバイスから、LUN セキュリティが設定されている必要があります。



注意 認証モードが有効なコマンドデバイスがホスト (業務サーバ) に接続されている場合、Device Manager の GUI または CLI からコピーペアに対する操作を実行する前には、ホストで `raidcom - login` コマンドを実行して、ユーザー認証を行ってください。

- ・ ホストの OS が Windows の場合は、Device Manager エージェントのサービス (HBsA Service) の実行ユーザーでユーザー認証を行ってください。
- ・ ホストに同一ストレージシステム内のコマンドデバイスが複数接続されている場合は、すべてのコマンドデバイスの認証モードを有効にしてください。
ストレージシステムに対してユーザー認証を一度実行すれば、同一ストレージシステム内のすべてのコマンドデバイスにアクセスできるようになります。
- ・ 認証モードを無効から有効に変更した場合、コマンドデバイスを認識しているほかのホストがあれば、そのホストでもユーザー認証を行ってください。

リソースグループの条件 (Virtual Storage Platform または HUS VM 内のリソースを分割管理している場合)

- ユーザーの管理対象のリソースグループに、次のボリューム、または次のボリュームを含むストレージシステムが登録されていること。
 - ・ P-VOL
 - ・ S-VOL
 - ・ プールを構成する全プールボリューム (Copy-on-Write Snapshot または Thin Image ペアを管理する場合)
 - ・ ジャーナルを構成する全ジャーナルボリューム (Universal Replicator ペアを管理する場合)
 - コマンドデバイスが登録された共用のリソースグループが作成され、各ユーザーに割り当てられていること。
- なお、各ユーザーが別のコマンドデバイスを使用する場合は、共用リソースグループの代わりに、各ユーザーの管理対象のリソースグループにコマンドデバイスを登録してください。



注意 Device Manager エージェントの起動中に、RAID Manager のコマンドを直接実行して、ストレージシステムに対するユーザー認証のログアウト処理をしないでください。Device Manager の GUI または CLI からの処理が正常に終了しなくなるおそれがあります。ログアウトする必要がある場合は、Device Manager エージェントのサービスを事前に停止してください。

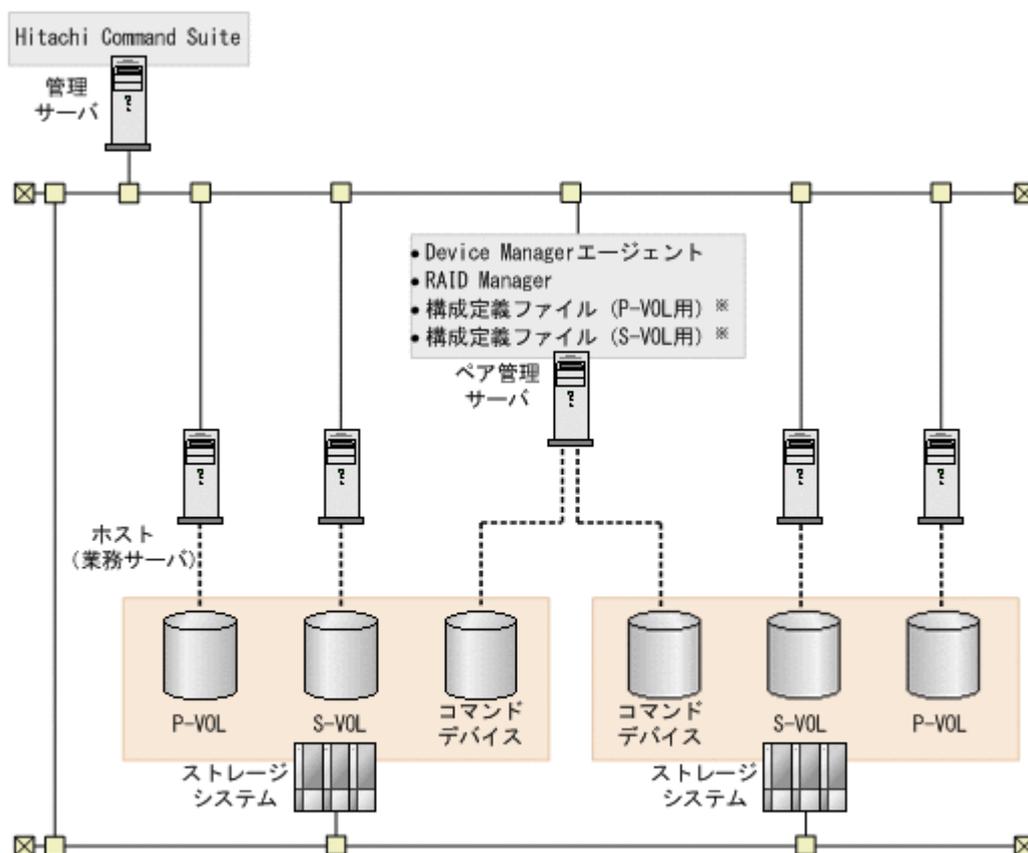
関連項目

- ・ 1.6.3 コピーペアを管理する場合のストレージシステムの要件
- ・ 1.6.4 コピーペアを管理する場合の Device Manager エージェントの前提バージョン
- ・ RAID Manager のインストール手順 : RAID Manager のマニュアル

(2) 一括管理構成でコピーペアを管理する場合のシステム構成

前提条件を満たすように管理サーバやペア管理サーバ、ストレージシステムを構築してください。

図 1-21 コピーペア管理のシステム構成例（一括管理構成）



(凡例)

----- : LUNセキュリティが設定されていることを示します。

注※ スナップショットグループに定義されたThin Imageコピーペアは、構成定義ファイルは不要です。

管理サーバの条件

- 次のマシンが Device Manager の管理リソースとして登録されていること。
P-VOL を認識しているホスト
S-VOL を認識しているホスト
ペア管理サーバ

ペア管理サーバの条件

- Device Manager エージェントがインストールされていること。
- Device Manager エージェントの `server.agent.rm.centralizePairConfiguration` プロパティに `enable` が設定されていること (デフォルト: `disable`)。
- RAID Manager がインストールされていること。
ペア管理サーバが認識しているコマンドデバイスが認証機能に対応している場合は、バージョン 01-25-03/01 以降の RAID Manager をインストールしてください。
また、H シリーズとそれ以外の日立ストレージシステムのコピーペアを管理する場合には、RAID Manager と P9000 RAID Manager の両方をインストールする必要があります。
- NIC が複数ある場合、Device Manager エージェントおよび RAID Manager が利用する IP アドレスが同じであること。

コピーペア (P-VOL および S-VOL) の条件

- P-VOL および S-VOL が 1 台の管理サーバ (Device Manager サーバ) で管理されていること。
- P-VOL および S-VOL がホスト (業務サーバ) に認識されていること。
P-VOL と S-VOL は別の業務サーバに割り当ててを推奨します。
- P-VOL および S-VOL からホスト (業務サーバ) に対して、LUN セキュリティが設定されていること。
ペア管理サーバが P-VOL または S-VOL を認識している必要はありません。

コマンドデバイスの条件

- コマンドデバイスがペア管理サーバに認識されていること。
コマンドデバイスセキュリティが使用されていない必要があります。
- コマンドデバイスからペア管理サーバに対して、LUN セキュリティが設定されていること。
TrueCopy または Universal Replicator のペアを管理する場合、P-VOL および S-VOL 両方のストレージシステムのコマンドデバイスから、LUN セキュリティが設定されている必要があります。



注意 認証モードが有効なコマンドデバイスがペア管理サーバに接続されている場合、Device Manager の GUI または CLI からコピーペアに対する操作を実行する前には、ホストで `raidcom -login` コマンドを実行して、ユーザー認証を行ってください。

- ペア管理サーバの OS が Windows の場合は、Device Manager エージェントのサービス (HBsA Service) の実行ユーザーでユーザー認証を行ってください。
- ペア管理サーバに同一ストレージシステム内のコマンドデバイスが複数接続されている場合は、すべてのコマンドデバイスの認証モードを有効にしてください。
ストレージシステムに対してユーザー認証を一度実行すれば、同一ストレージシステム内のすべてのコマンドデバイスにアクセスできるようになります。
- 認証モードを無効から有効に変更した場合、コマンドデバイスを認識しているほかのホストがあれば、そのホストでもユーザー認証を行ってください。

リソースグループの条件 (Virtual Storage Platform または HUS VM 内のリソースを分割管理している場合)

- ユーザーの管理対象のリソースグループに、次のボリューム、または次のボリュームを含むストレージシステムが登録されていること。
 - P-VOL
 - S-VOL
 - プールを構成する全プールボリューム (Copy-on-Write Snapshot または Thin Image ペアを管理する場合)
 - ジャーナルを構成する全ジャーナルボリューム (Universal Replicator ペアを管理する場合)
- コマンドデバイスが登録された共用のリソースグループが作成され、各ユーザーに割り当てられていること。
なお、各ユーザーが別のコマンドデバイスを使用する場合は、共用リソースグループの代わりに、各ユーザーの管理対象のリソースグループにコマンドデバイスを登録してください。



注意 Device Manager エージェントの起動中に、RAID Manager のコマンドを直接実行して、ストレージシステムに対するユーザー認証のログアウト処理をしないでください。Device Manager の GUI または CLI からの処理が正常に終了しなくなるおそれがあります。ログアウトする必要がある場合は、Device Manager エージェントのサービスを事前に停止してください。

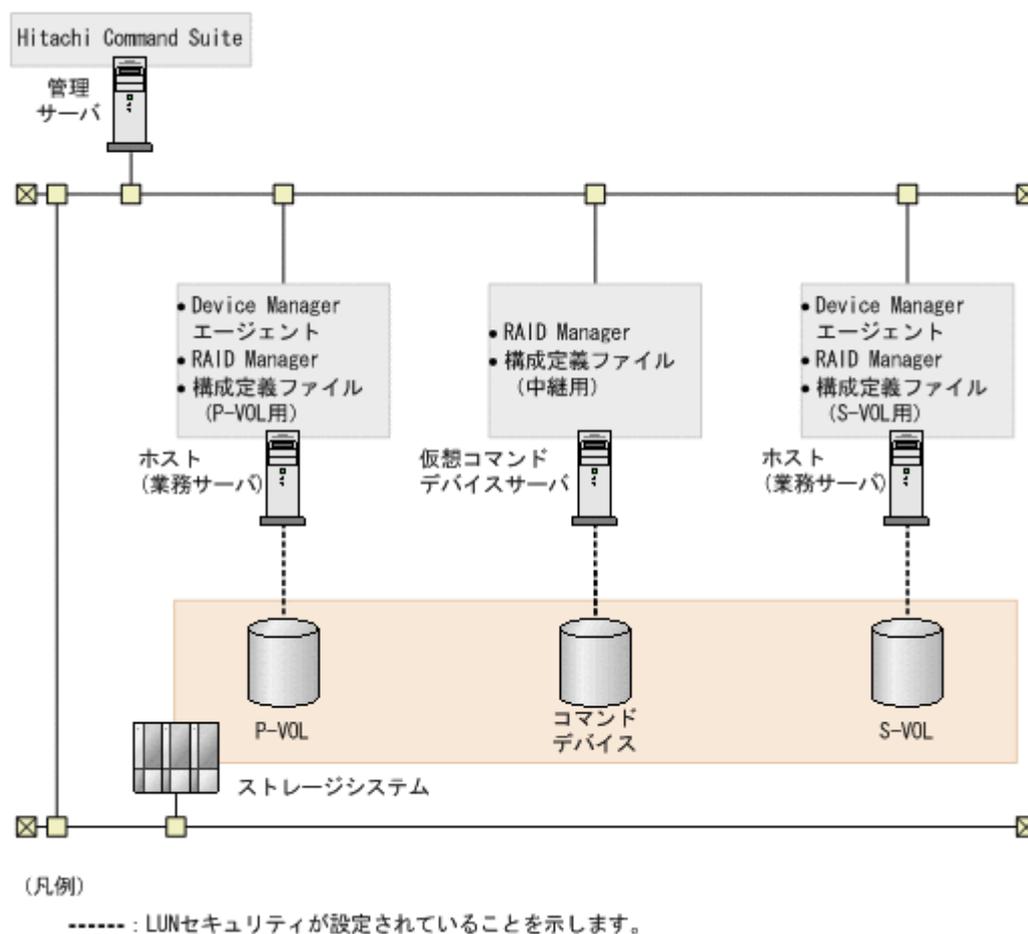
関連項目

- 1.6.3 コピーペアを管理する場合のストレージシステムの要件
- 1.6.4 コピーペアを管理する場合の Device Manager エージェントの前提バージョン
- D.1.1 Device Manager エージェントのプロパティの変更
- D.6.15 server.agent.rm.centralizePairConfiguration
- RAID Manager のインストール手順 : RAID Manager のマニュアル

(3) 仮想コマンドデバイスサーバ構成でコピーペアを管理する場合のシステム構成

前提条件を満たすように管理サーバやホスト（業務サーバ）、仮想コマンドデバイスサーバ、ストレージシステムを構築してください。

図 1-22 コピーペア管理のシステム構成例（仮想コマンドデバイスサーバ構成）



管理サーバの条件

次のマシンが Device Manager の管理リソースとして登録されていること。

- P-VOL を認識しているホスト
- S-VOL を認識しているホスト

ホスト（業務サーバ）の条件

- バージョン 7.1 以降の Device Manager エージェントがインストールされていること。
- バージョン 01-25-03/01 以降の RAID Manager がインストールされていること。

H シリーズとそれ以外の日立ストレージシステムのコピーペアを管理する場合には、RAID Manager と P9000 RAID Manager の両方をインストールする必要があります。

- ホスト（業務サーバ）に NIC が複数ある場合、Device Manager エージェントおよび RAID Manager が利用する IP アドレスが同じであること。

仮想コマンドデバイスサーバの条件

- バージョン 01-25-03/01 以降の RAID Manager がインストールされていること。
H シリーズとそれ以外の日立ストレージシステムのコピーペアを管理する場合には、RAID Manager と P9000 RAID Manager の両方をインストールする必要があります。
- 中継用の horcm インスタンスが起動していること。



注意

- 仮想コマンドデバイスサーバ上の構成定義ファイルに HORCM_ALLOW_INST パラメーターを設定する場合、業務サーバの RAID Manager イニシエーターポートにはデフォルトのポート番号（34000+<インスタンス番号>+1）を使用してください。
- 認証モードが有効なコマンドデバイスがホスト（仮想コマンドデバイスサーバ）に接続されている場合、Device Manager の GUI または CLI からコピーペアに対する操作を実行する前には、ホストで raidcom -login コマンドを実行して、ユーザー認証を行ってください。
 - ホストの OS が Windows の場合は、Device Manager エージェントのサービス（HBsA Service）の実行ユーザーでユーザー認証を行ってください。
 - 仮想コマンドデバイスサーバに同一ストレージシステム内のコマンドデバイスが複数接続されている場合は、すべてのコマンドデバイスの認証モードを有効にしてください。
ストレージシステムに対してユーザー認証を一度実行すれば、同一ストレージシステム内のすべてのコマンドデバイスにアクセスできるようになります。
 - 認証モードを無効から有効に変更した場合、コマンドデバイスを認識しているほかのホストがあれば、そのホストでもユーザー認証を行ってください。

コピーペア（P-VOL および S-VOL）の条件

- P-VOL および S-VOL が 1 台の管理サーバ（Device Manager サーバ）で管理されていること。
- P-VOL または S-VOL がホスト（業務サーバ）に認識されていること。
P-VOL と S-VOL は別の業務サーバに割り当てることを推奨します。
- P-VOL および S-VOL からホスト（業務サーバ）に対して、LUN セキュリティが設定されていること。
仮想コマンドデバイスサーバが P-VOL または S-VOL を認識している必要はありません。

コマンドデバイスの条件

- コマンドデバイスが仮想コマンドデバイスサーバに認識されていること。
コマンドデバイスセキュリティが使用されていない必要があります。
- コマンドデバイスから仮想コマンドデバイスサーバに対して、LUN セキュリティが設定されていること。
TrueCopy または Universal Replicator のペアを管理する場合、P-VOL および S-VOL 両方のストレージシステムのコマンドデバイスから、LUN セキュリティが設定されている必要があります。

リソースグループの条件 (Virtual Storage Platform または HUS VM 内のリソースを分割管理している場合)

- ユーザーの管理対象のリソースグループに、次のボリューム、または次のボリュームを含むストレージシステムが登録されていること。

- P-VOL
- S-VOL
- プールを構成する全プールボリューム（Copy-on-Write Snapshot または Thin Image ペアを管理する場合）
- ジャーナルを構成する全ジャーナルボリューム（Universal Replicator ペアを管理する場合）

ただし、リソースを分割管理すると、一部の Replication Manager GUI の表示が遅くなる場合があります。仮想コマンドデバイスを使用する場合は、ストレージシステム単位のリソースグループ（デフォルトリソースグループ）をユーザーに割り当てることをお勧めします。



注意 Device Manager エージェントの起動中に、RAID Manager のコマンドを直接実行して、ストレージシステムに対するユーザー認証のログアウト処理をしないでください。Device Manager の GUI または CLI からの処理が正常に終了しなくなるおそれがあります。ログアウトする必要がある場合は、Device Manager エージェントのサービスを事前に停止してください。

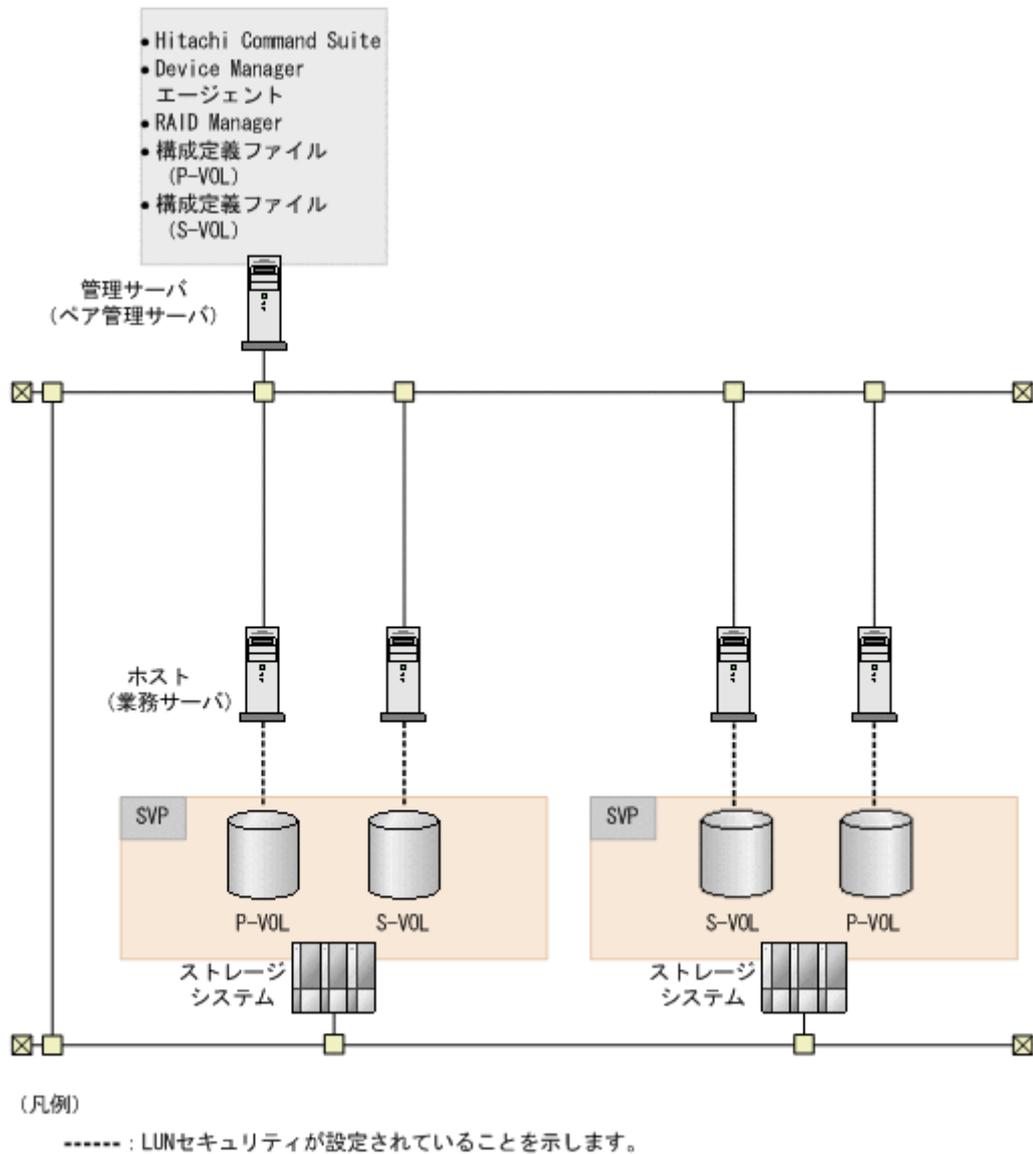
関連項目

- [1.6.3 コピーペアを管理する場合のストレージシステムの要件](#)
- [1.6.4 コピーペアを管理する場合の Device Manager エージェントの前提バージョン](#)
- RAID Manager のインストール手順：RAID Manager のマニュアル

(4) SVP 構成でコピーペアを管理する場合のシステム構成（構成定義ファイルでコピーペアを定義した場合）

前提条件を満たすように管理サーバやペア管理サーバ、ストレージシステムを構築してください。

図 1-23 コピーペア管理のシステム構成例（構成定義ファイルでコピーペアを定義した場合）



管理サーバの条件

- 次のマシンが Device Manager の管理リソースとして登録されていること。
 P-VOL を認識しているホスト
 S-VOL を認識しているホスト

ペア管理サーバの条件

- バージョン 7.1 以降の Device Manager エージェントがインストールされていること。
- バージョン 01-25-03/01 以降の RAID Manager がインストールされていること。
 H シリーズとそれ以外の日立ストレージシステムのコピーペアを管理する場合には、RAID Manager と P9000 RAID Manager の両方をインストールする必要があります。

コピーペア (P-VOL および S-VOL) の条件

- P-VOL および S-VOL が 1 台の管理サーバ (Device Manager サーバ) で管理されていること。
- P-VOL および S-VOL からホスト (業務サーバ) に対して、LUN セキュリティが設定されていること。

管理サーバが P-VOL または S-VOL を認識している必要はありません。

- P-VOL または S-VOL がホスト（業務サーバ）に認識されていること。
P-VOL と S-VOL は別の業務サーバに割り当てることを推奨します。

リソースグループの条件 (Virtual Storage Platform または HUS VM 内のリソースを分割管理している場合)

- ユーザーの管理対象のリソースグループに、次のボリュームが登録されていること。
 - ・ P-VOL
 - ・ S-VOL
 - ・ プールを構成する全プールボリューム (Copy-on-Write Snapshot または Thin Image ペアを管理する場合)
 - ・ ジャーナルを構成する全ジャーナルボリューム (Universal Replicator ペアを管理する場合)

ただし、リソースを分割管理すると、一部の Replication Manager GUI の表示が遅くなることがあります。仮想コマンドデバイスを使用する場合は、ストレージシステム単位のリソースグループ (デフォルトリソースグループ) をユーザーに割り当てることをお勧めします。



注意

- ・ Device Manager の GUI または CLI からコピーペアに対する操作を実行する前に、管理サーバで `raidcom -login` コマンドを実行して、ユーザー認証を行ってください。管理サーバの OS が Windows の場合は、Device Manager エージェントのサービス (HBsA Service) の実行ユーザーでユーザー認証を行ってください。
- ・ Device Manager エージェントの起動中に、RAID Manager のコマンドを直接実行して、ストレージシステムに対するユーザー認証のログアウト処理をしないでください。Device Manager の GUI または CLI からの処理が正常に終了しなくなるおそれがあります。ログアウトする必要がある場合は、Device Manager エージェントのサービスを事前に停止してください。
- ・ SVP のユーザー ID またはパスワードが変更になった場合は、GUI で次の設定変更が必要です。
 1. Device Manager の [ストレージシステム編集] 画面で、変更後の SVP のユーザー ID またはパスワードを設定する。
 2. Replication Manager の [構成設定] 画面で、設定を変更したストレージシステムの構成情報を更新する。

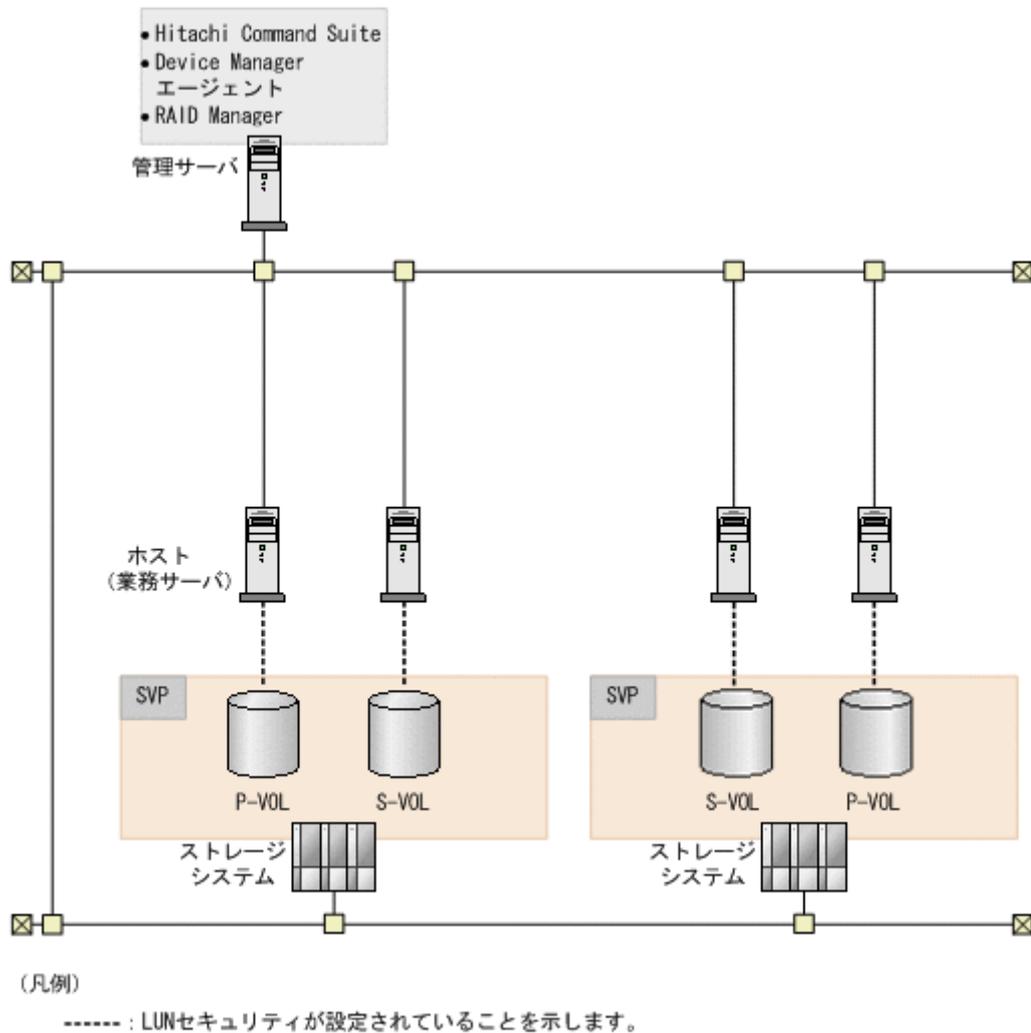
関連項目

- ・ 1.6.3 コピーペアを管理する場合のストレージシステムの要件
- ・ 1.6.4 コピーペアを管理する場合の Device Manager エージェントの前提バージョン
- ・ RAID Manager のインストール手順 : RAID Manager のマニュアル

(5) SVP 構成でコピーペアを管理する場合のシステム構成 (デバイスグループとしてコピーペアを定義した場合)

前提条件を満たすように管理サーバやホスト (業務サーバ)、ストレージシステムを構築してください。

図 1-24 コピーペア管理のシステム構成例（デバイスグループとしてコピーペアを定義した場合）



管理サーバの条件

- 次のマシンが Device Manager の管理リソースとして登録されていること。
P-VOL を認識しているホスト
S-VOL を認識しているホスト
- バージョン 7.1 以降の Device Manager エージェントがインストールされていること。
- バージョン 01-25-03/01 以降の RAID Manager がインストールされていること。
H シリーズとそれ以外の日立ストレージシステムのコピーペアを管理する場合には、RAID Manager と P9000 RAID Manager の両方をインストールする必要があります。
- Replication Manager サーバと Device Manager サーバ間を SSL で通信できること。
- 次のどちらかの条件を満たすこと。
 - ・ P-VOL および S-VOL が割り当てられていないこと。

管理サーバからコピーペアを作成したい場合は、管理サーバ上の Device Manager エージェントの `server.agent.rm.centralizePairConfiguration` プロパティに `enable` を設定してください（デフォルト：`disable`）。

・管理サーバ上の Device Manager エージェントの `server.agent.rm.ignorePairStatus` プロパティに `true` が設定されていること。

Device Manager の GUI または CLI で最新のコピーペア情報を確認したい場合は、次の方法でストレージシステムをリフレッシュしてください。

GUI: ストレージシステムビューで該当するストレージシステムを選択し、[ストレージシステム情報更新] ボタンをクリックします。

CLI: 該当するストレージシステムに対して AddStorageArray コマンドを実行します。

コピーペア (P-VOL および S-VOL) の条件

- P-VOL および S-VOL が 1 台の管理サーバ (Device Manager サーバ) で管理されていること。
- P-VOL および S-VOL からホスト (業務サーバ) に対して、LUN セキュリティが設定されていること。
管理サーバが P-VOL または S-VOL を認識している必要はありません。
- P-VOL または S-VOL がホスト (業務サーバ) に認識されていること。
P-VOL と S-VOL は別の業務サーバに割り当ててを推奨します。

リソースグループの条件 (Virtual Storage Platform または HUS VM 内のリソースを分割管理している場合)

- ユーザーの管理対象のリソースグループに、次のボリュームが登録されていること。
 - ・ P-VOL
 - ・ S-VOL
 - ・ プールを構成する全プールボリューム (Copy-on-Write Snapshot または Thin Image ペアを管理する場合)
 - ・ ジャーナルを構成する全ジャーナルボリューム (Universal Replicator ペアを管理する場合)
- ただし、リソースを分割管理すると、一部の Replication Manager GUI の表示が遅くなることがあります。仮想コマンドデバイスを使用する場合は、ストレージシステム単位のリソースグループ (デフォルトリソースグループ) をユーザーに割り当ててをお勧めします。



注意

- ・ 管理サーバに Replication Manager Application エージェントをインストールしないでください。
- ・ Device Manager エージェントの起動中に、RAID Manager のコマンドを直接実行して、ストレージシステムに対するユーザー認証のログアウト処理をしないでください。Device Manager の GUI または CLI からの処理が正常に終了しなくなるおそれがあります。ログアウトする必要がある場合は、Device Manager エージェントのサービスを事前に停止してください。
- ・ SVP のユーザー ID またはパスワードが変更になった場合は、GUI で次の設定変更が必要です。
 1. Device Manager の [ストレージシステム編集] 画面で、変更後の SVP のユーザー ID またはパスワードを設定する。
 2. Replication Manager の [構成設定] 画面で、設定を変更したストレージシステムの構成情報を更新する。

関連項目

- ・ [1.6.3 コピーペアを管理する場合のストレージシステムの要件](#)
- ・ [1.6.4 コピーペアを管理する場合の Device Manager エージェントの前提バージョン](#)
- ・ [D.1.1 Device Manager エージェントのプロパティの変更](#)
- ・ [D.6.15 server.agent.rm.centralizePairConfiguration](#)
- ・ [D.6.25 server.agent.rm.ignorePairStatus](#)
- ・ RAID Manager のインストール手順: RAID Manager のマニュアル

1.6.3 コピーペアを管理する場合のストレージシステムの要件

Element Manager を使用して、ストレージシステムの要件に沿って環境構築してください。

表 1-8 コピーペアを管理するためのストレージシステムの要件

ストレージシステム	機能	要件
Virtual Storage Platform Universal Storage Platform V/VM Hitachi USP HUS VM	Universal Replicator ※1	<ul style="list-style-type: none"> • Universal Replicator の前提ソフトウェアをインストールし、ライセンスを有効にする必要があります。 • M-R バスに使用される 2 ポート間にファイバーチャネル接続が必要です。※2 • M-R バスの MCU ポートが Initiator ポートであり、RCU ポートが RCU Target ポートである必要があります。※2 • RCU と M-R バスが、MCU に登録されている必要があります。※2 • ストレージシステムキャッシュまたは不揮発性メモリーが十分にある必要があります。 • ジャーナルグループにジャーナルボリュームが登録されている必要があります。 <p>参考： ポートの構成後、Device Manager でストレージシステムをリフレッシュする必要があります。また、キャッシュの追加が必要な場合は、保守員に連絡してください。</p>
	TrueCopy ※1	<ul style="list-style-type: none"> • TrueCopy の前提ソフトウェアをインストールし、ライセンスを有効にする必要があります。 • M-R バスに使用される 2 ポート間にファイバーチャネル接続が必要です。 • M-R バスの MCU ポートが Initiator ポートであり、RCU ポートが RCU Target ポートである必要があります。 • RCU と M-R バスが、MCU に登録されている必要があります。 • ストレージシステムキャッシュまたは不揮発性メモリーが十分にある必要があります。 <p>参考： ポートの構成後、Device Manager でストレージシステムをリフレッシュする必要があります。また、キャッシュの追加が必要な場合は、保守員に連絡してください。</p>
	ShadowImage ※1	ShadowImage の前提ソフトウェアをインストールし、ライセンスを有効にする必要があります。
	Copy-on-Write Snapshot	<ul style="list-style-type: none"> • Copy-on-Write Snapshot の前提ソフトウェアをインストールし、ライセンスを有効にする必要があります。 • S-VOL 用に、特殊な LU である V-VOL をあらかじめ作成する必要があります。次の順序で準備してください。 <ol style="list-style-type: none"> a. プールの作成 b. V-VOL の作成

ストレージシステム	機能	要件
	Thin Image	<ul style="list-style-type: none"> Thin Image の前提ソフトウェアをインストールし、ライセンスを有効にする必要があります。 スナップショットグループに定義された Thin Image コピーペアの場合、ストレージシステム内のコマンドデバイスの認証モードを有効にし、ホストで <code>raidcom -login</code> コマンドを実行して、ユーザー認証を行ってください。 S-VOL 用に、特殊な LU である V-VOL をあらかじめ作成する必要があります。次の順序で準備してください。 <ul style="list-style-type: none"> a プールの作成 b V-VOL の作成
HUS100 Hitachi AMS2000 Hitachi AMS/WMS SANRISE9500V	TrueCopy	<ul style="list-style-type: none"> TrueCopy の前提ソフトウェアをインストールし、ライセンスを有効にする必要があります。 パス経路に使用される 2 ポート間にファイバーチャネル接続が必要です。 TrueCopy のパスが構成されている必要があります。HUS100 および Hitachi AMS2000 の場合、1 台のストレージシステムから複数のストレージシステムにパスを設定できます。 システムスタート属性がデュアルアクティブモードである必要があります。 SANRISE9500V の場合は、データシェアモードが有効である必要があります。 SANRISE9500V の場合は、SCSI ID/Port ID 引き継ぎモードが使用しないに設定されている必要があります。 Hitachi AMS2000 および Hitachi AMS/WMS で TrueCopy remote replication または TrueCopy Extended Distance を使用する場合は、または HUS100 で TrueCopy remote replication を使用する場合は、DM-LU を設定する必要があります。 Hitachi AMS2000 および Hitachi AMS/WMS で、TrueCopy Extended Distance を使用する場合はデータプールを設定する必要があります。このデータプールは Copy-on-Write Snapshot のデータプールと共有できます。 HUS100 で TrueCopy Extended Distance を使用する場合は、DP プールを作成する必要があります。管理データと差分データが同じ DP プールに格納されるように設定してください。この DP プールは Copy-on-Write Snapshot の DP プールと共有できます。
	ShadowImage	<ul style="list-style-type: none"> ShadowImage の前提ソフトウェアをインストールし、ライセンスを有効にする必要があります。

ストレージシステム	機能	要件
		<ul style="list-style-type: none"> システムスタート属性がデュアルアクティブモードである必要があります。 SANRISE9500V の場合は、データシェアモードが有効である必要があります。 SANRISE9500V の場合は、SCSI ID/Port ID 引き継ぎモードが使用しないに設定されている必要があります。 HUS100, Hitachi AMS2000 および Hitachi AMS/WMS の場合は、DM-LU を設定する必要があります。
	Copy-on-Write Snapshot QuickShadow	<ul style="list-style-type: none"> Copy-on-Write Snapshot または QuickShadow の前提ソフトウェアをインストールし、ライセンスを有効にする必要があります。 S-VOL 用に、特殊な LU である V-VOL をあらかじめ作成する必要があります。次の順序で準備してください。 HUS100 の場合 <ul style="list-style-type: none"> a. DP プールの作成 管理データと差分データが同じ DP プールに格納されるように設定してください。 この DP プールは TrueCopy Extended Distance の DP プールと共有できます。 b. V-VOL の作成 Hitachi AMS2000, Hitachi AMS/WMS, および SANRISE9500V の場合 <ul style="list-style-type: none"> a. データプールの作成 このデータプールは TrueCopy Extended Distance のデータプールと共有できます。 b. V-VOL の作成 Hitachi AMS2000 および Hitachi AMS/WMS の場合は、DM-LU を設定する必要があります。

注※1

メインフレームボリュームのコピーペアについては、構成の確認だけを CLI でできます。コピーペアの構成を Device Manager CLI で確認するために必要なストレージシステムの要件はありません。

注※2

TrueCopy での設定を共用できます。ただし、Universal Replicator の場合は、P-VOL 側と S-VOL 側の両方のストレージシステムに対して設定が必要です。



注意

- 要件に応じてストレージシステムを構成したあと、ストレージシステムをリフレッシュする必要があります。コピーペアに対する操作を実行する前には、最新の情報が反映されているか確認してください。
- Device Manager によって管理されるストレージシステムのシリアル番号は、すべて一意である必要があります。TrueCopy または Universal Replicator の場合は、Device Manager によって管理されないリモートストレージシステムのシリアル番号も一意である必要があります。
- Virtual Storage Platform または HUS VM の LU でペアを作成する場合、デバイスグループに関連づけられている LU は使用しないでください。

関連項目

- 1.6.1 Device Manager でコピーペアを管理できるストレージシステム
- (1) 通常構成でコピーペアを管理する場合のシステム構成
- (2) 一括管理構成でコピーペアを管理する場合のシステム構成
- (3) 仮想コマンドデバイスサーバ構成でコピーペアを管理する場合のシステム構成
- (4) SVP 構成でコピーペアを管理する場合のシステム構成 (構成定義ファイルでコピーペアを定義した場合)
- (5) SVP 構成でコピーペアを管理する場合のシステム構成 (デバイスグループとしてコピーペアを定義した場合)

1.6.4 コピーペアを管理する場合の Device Manager エージェントの前提バージョン

管理対象のストレージシステムや使用するプログラムによって、Device Manager エージェントの前提バージョンが異なります。

GUI でコピーペアを管理する場合

操作対象のストレージシステムによって、Device Manager エージェントの前提バージョンが異なります。

表 1-9 GUI でコピーペアを管理する場合の Device Manager エージェントの要件

ストレージシステム	Device Manager エージェントのバージョン
Virtual Storage Platform	7.0 以降
Universal Storage Platform V/VM	6.0 以降
Hitachi USP	6.0 以降
HUS VM	7.3.1 以降
HUS100	7.2.0 以降
Hitachi AMS2000	6.0 以降
Hitachi AMS/WMS	6.0 以降

CLI で管理する場合

プログラムや操作内容、操作対象のストレージシステムのモデルによって、必要な Device Manager エージェントのバージョンが異なります。

表 1-10 CLI でコピーペアを管理するための Device Manager エージェントの要件

プログラム	Device Manager からの操作	Device Manager エージェントのバージョン※
Universal Replicator	状態表示	04-00 以降
	状態表示 (3DR)	05-50 以降
	状態変更	05-60 以降
TrueCopy	状態表示	02-30 以降
	状態表示 (TrueCopy Extended Distance)	05-10 以降
	状態変更	02-40 以降
	状態変更 (TrueCopy Extended Distance)	05-10 以降
ShadowImage	状態表示	02-30 以降

プログラム	Device Manager からの操作	Device Manager エージェントのバージョン※
	状態表示 (最大 1 : 3)	05-50 以降
	状態変更	02-40 以降
	状態変更 (最大 1 : 3)	05-50 以降
Copy-on-Write Snapshot	状態表示	04-10 以降
	状態変更	04-10 以降
Thin Image	状態表示	7.4.0 以降
	状態変更	7.6.1 以降
QuickShadow	状態表示	03-00 以降
	状態表示 (最大 1 : 15)	05-50 以降
	状態変更	03-00 以降
	状態変更 (最大 1 : 15)	05-50 以降

注

構成定義ファイルを作成するためには、各ホストに、03-01 以降の Device Manager エージェントをインストールする必要があります。

注※

ストレージシステムごとの Device Manager エージェントの要件を次の表に示します。

表 1-11 CLI でコピーペアを管理する場合のストレージシステムごとの Device Manager エージェントの要件

ストレージシステムのモデル名	Device Manager エージェントのバージョン
Hitachi Virtual Storage Platform Hitachi Virtual Storage Platform VP9500	7.0 以降
Hitachi Universal Storage Platform V Hitachi Universal Storage Platform H24000	05-70 以降
Hitachi Universal Storage Platform VM Hitachi Universal Storage Platform H20000	05-80 以降
Hitachi Universal Storage Platform Hitachi Universal Storage Platform H12000	03-50 以降
Hitachi Network Storage Controller Hitachi Universal Storage Platform H10000	04-00 以降
SANRISE9900V SANRISE H1024 SANRISE H128	02-20 以降
Hitachi Unified Storage VM	7.3.1 以降
Hitachi Unified Storage 150	7.2.0 以降
Hitachi Unified Storage 130	
Hitachi Unified Storage 110	
Hitachi Adaptable Modular Storage AMS2500 (H/W Rev. 0100)	6.0 以降
Hitachi Adaptable Modular Storage AMS2300 (H/W Rev. 0100)	
Hitachi Adaptable Modular Storage AMS2100 (H/W Rev. 0100)	
Hitachi Adaptable Modular Storage AMS2500 (H/W Rev. 0200)	6.4 以降
Hitachi Adaptable Modular Storage AMS2300 (H/W Rev. 0200)	

ストレージシステムのモデル名	Device Manager エージェント のバージョン
Hitachi Adaptable Modular Storage AMS2100 (H/W Rev. 0200)	
Hitachi Adaptable Modular Storage AMS2010	
Hitachi Adaptable Modular Storage 1000	05-00 以降
Hitachi Adaptable Modular Storage 500	04-20 以降
Hitachi Adaptable Modular Storage 200	
Hitachi Workgroup Modular Storage 100	04-10 以降
SANRISE 9580V	03-00 以降
SANRISE 9585V	02-20 以降

関連項目

- (1) 通常構成でコピーペアを管理する場合のシステム構成
- (2) 一括管理構成でコピーペアを管理する場合のシステム構成
- (3) 仮想コマンドデバイスサーバ構成でコピーペアを管理する場合のシステム構成
- (4) SVP 構成でコピーペアを管理する場合のシステム構成 (構成定義ファイルでコピーペアを定義した場合)
- (5) SVP 構成でコピーペアを管理する場合のシステム構成 (デバイスグループとしてコピーペアを定義した場合)

1.6.5 コピーペアを管理する場合の注意事項

コピーペアを管理する場合の注意事項は次のとおりです。

- 次の場合は、Device Manager でコピーペアの管理ができなくなるため、構成定義ファイルを修正する必要があります。
 - Device Manager サーバの `server.properties` ファイルにある `server.horcmconfigfile.hostname` プロパティに `ipaddress` を設定している場合にホストの IP アドレスを変更したとき
 - Device Manager サーバの `server.properties` ファイルにある `server.horcmconfigfile.hostname` プロパティに `hostname` を設定している場合にホスト名を変更したとき
- 次の手順で構成定義ファイルを修正してください。
- 自ホストの構成定義ファイルを修正する。
 - 自ホスト上の Device Manager エージェントを再起動する。
 - 相手ホストの構成定義ファイルを修正する。
 - ストレージシステムのリフレッシュを実行する。
- RAID Manager や Protection Manager で管理しているコピーペアを Device Manager で制御するためには、コピーペアの P-VOL を認識しているホスト上の構成定義ファイルと S-VOL を認識しているホスト上の構成定義ファイルに記述されているグループ名およびペア名が一致している必要があります。一致していない場合は、Device Manager からそのコピーペアを制御できません。また、複数のコピーペアを同じホストで管理する場合、次に示す条件を満たす必要があります。条件を満たしていないコピーペアがある場合は、構成定義ファイルを修正してください。
 - ホストの Device Manager エージェントのバージョンが 05-60 以前の場合：

同一ホスト内で次の組み合わせが一意であること。

グループ名

ペア名

- ホストの **Device Manager** エージェントのバージョンが **05-70** 以降の場合：

同一ホスト内で次の組み合わせが一意であること。

ポート番号

グループ名

ペア名

- **RAID Manager** を使用してコピーペアを作成したい場合や **RAID Manager** を使用してコピーペアをすでに管理している場合には、**Device Manager CLI** で構成定義ファイルを作成できません。
 - **Device Manager CLI** で作成した構成定義ファイルを使用して、**Device Manager** でコピーペアを作成することはできません。
 - **Device Manager CLI** で作成した構成定義ファイルを使用して **RAID Manager** でコピーペアを作成するためには、**MU** 番号を適切な値に変更する必要があります。
 - **Device Manager** で不正な構成定義ファイルを作成してしまった場合、**Device Manager** では構成定義ファイルを削除できないため、ペアを管理しているホストで構成定義ファイルを削除または編集する必要があります。ペア操作に使用しない構成定義ファイル、および誤った構成定義ファイルは、ストレージシステムの追加やリフレッシュなどのパフォーマンスに影響を及ぼすことがあります。このような構成定義ファイルは、ペアを管理しているホストで削除してください。

関連項目

- [11.2.4 コピーペアを管理するために必要な設定](#)
- [A.2.7 server.horcconfigfile.hostname](#)

1.7 コマンドを実行する場合の注意事項

Windows で UAC (User Account Control) 機能が有効になっている場合、コマンドを実行するには、管理者権限でコマンドプロンプトを起動してください。

ネットワーク構成に応じた設定

この章では、ネットワーク構成に応じて必要な Hitachi Command Suite 製品での設定について説明します。

- 2.1 ポートの設定
- 2.2 ブリッジ機能を使用する場合のネットワークの設定
- 2.3 IPv6 環境で運用する場合の Device Manager の設定
- 2.4 管理サーバの IP アドレスまたはホスト名の変更
- 2.5 Hitachi Command Suite 製品の URL の変更 (hcmdschgurl コマンド)

2.1 ポートの設定

ここでは、Hitachi Command Suite 製品で使用されるポート番号と、ファイアウォールの設定について説明します。

2.1.1 Hitachi Command Suite 製品で使用されるポート

Hitachi Command Suite 製品で使用されるポート番号が、同一マシンに共存するほかのプログラムと重複しないように調整してください。

重複する場合は、そのプログラムの設定を変更するか、Hitachi Command Suite 製品の設定を変更してください。



参考 ポート番号によっては、OS の一時割り当てポートと重複しているものもあります。Hitachi Command Suite 製品で使用するポート番号を OS の `services` ファイルに設定することで、一時割り当て対象から外すこともできます。

(1) Hitachi Command Suite 共通コンポーネントで使用されるポート

管理サーバでは、Hitachi Command Suite 共通コンポーネントで使用されるポート番号が同一マシンに共存するほかのプログラムと重複しないようにしてください。

表 2-1 Hitachi Command Suite 共通コンポーネントで使用されるポート

ポート番号	説明
23015/tcp※	管理クライアント（GUI）と通信する際に、HBase Storage Mgmt Web Service へのアクセスで使用されます。 このポート番号は変更できます。
23016/tcp	管理クライアント（GUI）と SSL で通信する際に、HBase Storage Mgmt Web Service へのアクセスで使用されます。 このポート番号は変更できます。
23017/tcp	Hitachi Command Suite 共通コンポーネントの内部通信（Web サーバとの通信）で使用されます。 このポート番号は変更できます。
23018/tcp	Hitachi Command Suite 共通コンポーネントの内部通信（Web サーバからの終了メッセージを受信）で使用されます。 このポート番号は変更できます。
23019/tcp～23024/tcp	Tuning Manager がインストールされている場合に、使用されるポートです。 このポート番号は変更できます。
23025/tcp	Hitachi Command Suite 共通コンポーネントの内部通信（Web サーバとの通信）で使用されます。 このポート番号は変更できます。
23026/tcp	Hitachi Command Suite 共通コンポーネントの内部通信（Web サーバからの終了メッセージを受信）で使用されます。 このポート番号は変更できます。
23027/tcp 23028/tcp	Compute Systems Manager がインストールされている場合に、使用されるポートです。 このポート番号は変更できます。
23029/tcp 23030/tcp	Hitachi Command Suite 共通コンポーネントで予約済みのポートです。
23031/tcp	管理サーバの OS が Windows の場合に、Hitachi Command Suite 共通コンポーネントの内部通信（シングルサインオン）で使用されます。 このポート番号は変更できます。
23032/tcp	Hitachi Command Suite 共通コンポーネントの内部通信（HiRDB）で使用されます。

ポート番号	説明
	このポート番号は変更できます。
23033/tcp 23034/tcp	Hitachi Command Suite 共通コンポーネントで予約済みのポートです。
45001/tcp～49000/tcp	管理サーバの OS が Windows XP, Windows Server 2003 R2, Solaris または Linux の場合に、Hitachi Command Suite 共通コンポーネントの内部通信 (HiRDB) で一時割り当てポートとして使用されます。 Hitachi Command Suite 製品では設定を変更できません。これらのポートを使用する製品が同一マシンにインストールされている場合は、その製品の設定を変更してください。それ以外の OS では、OS 標準の一時割り当てポートが使用されます。

注※

SSL を設定している場合でも使用されます。SSL 通信だけを許可したい場合は、ファイアウォールを設定してください。

関連項目

- 2.1.2 Hitachi Command Suite 共通コンポーネントで使用されるポートの変更
- 2.1.3 ファイアウォールの例外登録
- Tuning Manager および Compute Systems Manager がインストールされている場合に使用されるポートの変更方法：各製品のマニュアル

(2) Device Manager サーバで使用されるポート

管理サーバでは、Device Manager サーバで使用されるポート番号が同一マシンに共存するほかのプログラムと重複しないようにしてください。

表 2-2 Device Manager サーバで使用されるポート

ポート番号	説明
162/udp	ストレージシステム (Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, SANRISE 9900V および HUS VM) やファイルサーバ (Hitachi Virtual File Platform) から SNMP トラップを受信する際に使用されます。 Device Manager では設定を変更できません。このポートを使用する製品が同一マシンにインストールされている場合は、その製品の設定を変更してください。
427/tcp	CIM クライアント (サービスディスカバリー) と通信する際に使用されます。 Device Manager では設定を変更できません。このポートを使用する製品が同一マシンにインストールされている場合は、その製品の設定を変更してください。
2001/tcp※	Device Manager サーバの内部通信、管理クライアント (GUI および CLI)、ストレージシステムおよびホスト (Device Manager エージェントおよびファイルサーバ) と通信する際に使用されます。 ほかの製品でこのポートが使用されていると、Device Manager サーバが起動しません。 このポートは、Device Manager サーバの server.properties ファイルにある server.http.port プロパティで変更できます。
2443/tcp	Device Manager サーバの内部通信および SSL で管理クライアント (GUI および CLI) と通信する際に使用されます。 このポートは、Device Manager サーバの server.properties ファイルにある server.https.port プロパティで変更できます。
5983/tcp	SMI-S プロバイダーからインディケーション通知を受信する際に使用されます。 このポートは、Device Manager サーバの server.properties ファイルにある server.smisclient.indication.port プロパティで変更できます。

ポート番号	説明
5988/tcp	CIM クライアント（オブジェクト操作）と非 SSL で通信する際に使用されます。 このポート番号は変更できます。
5989/tcp	CIM クライアント（オブジェクト操作）と SSL で通信する際に使用されます。 このポート番号は変更できます。
23055/tcp	Device Manager サーバの内部通信で使用されます。 このポートは、Device Manager サーバの server.properties ファイルにある server.rmi.port プロパティで変更できます。
24220/tcp	HiRDB によって使用されます。 このポートは、htmsetup コマンドで変更できます。
Any/tcp	Tuning Manager の View Server との通信で使用されます。 デフォルトでは、任意の空きポート番号が使用される設定になっています。 Tuning Manager の管理サーバと Device Manager の管理サーバの間にファイアウォールが設置されている場合など、特定のポート番号が使用される設定に変更したい場合は、config.xml ファイルおよび configforclient.xml ファイルの ownPort パラメーターにポート番号を登録してください。

注※

SSL を設定している場合でも使用されます。SSL 通信だけを許可したい場合は、ファイアウォールを設定してください。

関連項目

- 2.1.3 ファイアウォールの例外登録
- (5) Tuning Manager サーバとのリモート接続およびポート番号の設定（htmsetup コマンド）
- (6) config.xml ファイルおよび configforclient.xml ファイルの設定
- 7.5.1 CIM/WBEM 機能で使用するポートの変更
- A.1.1 Device Manager サーバのプロパティの変更
- A.2.2 server.http.port
- A.2.3 server.https.port
- A.2.4 server.rmi.port
- A.2.27 server.smisclient.indication.port

(3) Tiered Storage Manager サーバで使用されるポート

管理サーバでは、Tiered Storage Manager サーバで使用されるポート番号が同一マシンに共存するほかのプログラムと重複しないようにしてください。

表 2-3 Tiered Storage Manager サーバで使用されるポート

ポート番号	説明
20352/tcp	管理クライアント（Tiered Storage Manager CLI および Legacy モードの Tiered Storage Manager GUI）と通信する際に使用されます。 このポートは、Tiered Storage Manager サーバの server.properties ファイルにある server.rmi.port プロパティで変更できます。
24500/tcp	管理クライアント（Tiered Storage Manager CLI および Legacy モードの Tiered Storage Manager GUI）と SSL で通信する際に使用されます。 このポートは、Tiered Storage Manager サーバの server.properties ファイルにある server.rmi.security.port プロパティで変更できます。

関連項目

- B.1.1 Tiered Storage Manager サーバのプロパティの変更
- B.2.2 server.rmi.port
- B.2.3 server.rmi.security.port

(4) Host Data Collector で使用されるポート

Host Data Collector のインストール先マシンでは、Host Data Collector で使用されるポート番号が同一マシンに共存するほかのプログラムと重複しないようにしてください。

表 2-4 Host Data Collector で使用されるポート

ポート番号	説明
22098/tcp	Host Data Collector の内部通信および Device Manager サーバと RMI レジストリー間の非 SSL 通信で使用されます。 このポートは、Host Data Collector の <code>hdcbase.properties</code> ファイルにある <code>hdc.common.rmi.registryPort</code> プロパティで変更できます。
22099/tcp	Device Manager サーバと RMI サーバ間の非 SSL 通信で使用されます。 このポートは、Host Data Collector の <code>hdcbase.properties</code> ファイルにある <code>hdc.common.rmi.serverPort</code> プロパティで変更できます。
22100/tcp	Device Manager サーバとクラスローダー間の非 SSL 通信で使用されます。 このポートは、Host Data Collector の <code>hdcbase.properties</code> ファイルにある <code>hdc.common.http.serverPort</code> プロパティで変更できます。
22104/tcp	Device Manager サーバと RMI レジストリー間の SSL 通信で使用されます。 このポートは、Host Data Collector の <code>hdcbase.properties</code> ファイルにある <code>hdc.common.rmi.ssl.registryPort</code> プロパティで変更できます。
22105/tcp	Device Manager サーバと RMI サーバ間の SSL 通信で使用されます。 このポートは、Host Data Collector の <code>hdcbase.properties</code> ファイルにある <code>hdc.common.rmi.ssl.serverPort</code> プロパティで変更できます。
22106/tcp	Device Manager サーバとクラスローダー間の SSL 通信で使用されます。 このポートは、Host Data Collector の <code>hdcbase.properties</code> ファイルにある <code>hdc.common.https.serverPort</code> プロパティで変更できます。
22110/tcp	Service プロセスと Adapter プロセス間の通信で使用されます。 このポートは、Host Data Collector の <code>hdcbase.properties</code> ファイルにある <code>hdc.service.localport</code> プロパティで変更できます。
22111/tcp~22120/tcp	Service プロセスと Adapter プロセス間の通信で使用されます。 これらのポートは、Host Data Collector の <code>hdcbase.properties</code> ファイルにある <code>hdc.adapter.localport</code> プロパティで変更できます。

関連項目

- C.1.1 Host Data Collector のプロパティの変更
- C.2.1 `hdc.service.localport`
- C.2.3 `hdc.adapter.localport`
- C.2.4 `hdc.common.rmi.registryPort`
- C.2.5 `hdc.common.rmi.serverPort`
- C.2.6 `hdc.common.http.serverPort`
- C.2.7 `hdc.common.rmi.ssl.registryPort`
- C.2.8 `hdc.common.rmi.ssl.serverPort`
- C.2.9 `hdc.common.https.serverPort`

(5) Device Manager エージェントで使用されるポート

Device Manager エージェントのインストール先マシンでは、Device Manager エージェントで使用されるポート番号が同一マシンに共存するほかのプログラムと重複しないようにしてください。

表 2-5 Device Manager エージェントで使用されるポート

ポート番号	説明
24041/tcp	Device Manager サーバと通信する際に使用されます。 このポートは、Device Manager エージェントの server.properties ファイルにある server.agent.port プロパティで変更できます。
24042/tcp	Device Manager サーバと通信する際に使用されます。 このポートは、Device Manager エージェントの server.properties ファイルにある server.http.port プロパティで変更できます。
24043/tcp	Device Manager エージェントの内部通信で使用されます。 このポートは、Device Manager エージェントの server.properties ファイルにある server.http.localPort プロパティで変更できます。

関連項目

- [D.1.1 Device Manager エージェントのプロパティの変更](#)
- [D.6.1 server.agent.port](#)
- [D.6.2 server.http.localPort](#)
- [D.6.3 server.http.port](#)

(6) ストレージシステムで使用されるポート

Device Manager および Tiered Storage Manager でストレージシステムを管理するためには、管理サーバや管理クライアント（GUI）との通信用ポートを用意する必要があります。

表 2-6 ストレージシステムで使用されるポート

対象ストレージシステム	ポート番号	説明
Virtual Storage Platform	80/tcp	管理クライアント（GUI）と通信する際に使用されます。 このポート番号は変更できません。
	443/tcp	管理クライアント（GUI）から SSL で Element Manager を起動する際に使用されます。 このポート番号は変更できません。
	1099/tcp	管理サーバまたは管理クライアント（GUI）と通信する際に使用されます。 このポート番号は変更できません。
	51099/tcp	管理サーバまたは管理クライアント（GUI）と通信する際に使用されます。 このポート番号は変更できません。
	51100/tcp	管理サーバまたは管理クライアント（GUI）と通信する際に使用されます。 このポート番号は変更できません。
Universal Storage Platform V/VM	80/tcp	管理クライアント（GUI）と通信する際に使用されます。 このポート番号は変更できません。
	443/tcp	管理クライアント（GUI）から SSL で Element Manager を起動する際に使用されます。 このポート番号は変更できません。

対象ストレージシステム	ポート番号	説明
	1099/tcp	管理サーバまたは管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
	51099/tcp	管理サーバまたは管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
	51100/tcp	管理サーバまたは管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
Hitachi USP	80/tcp	管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
	443/tcp	管理クライアント (GUI) から SSL で Element Manager を起動する際に使用されます。 このポート番号は変更できません。
	1099/tcp	管理サーバまたは管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
	51099/tcp	管理サーバまたは管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
SANRISE9900V	80/tcp	管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
	1099/tcp	管理サーバまたは管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
	51099/tcp	管理サーバまたは管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
HUS VM	80/tcp	管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
	443/tcp	SSL で Element Manager を起動する際に使用されます。 このポート番号は変更できません。
	1099/tcp	管理クライアント (GUI) と通信する際に使用されます。 このポート番号は変更できません。
	51099/tcp	管理サーバと通信する際に使用されます。 このポート番号は変更できません。
	51100/tcp	管理サーバと通信する際に使用されます。 このポート番号は変更できません。
SANRISE9500V	2000/tcp	管理サーバと通信する際に使用されます。 このポート番号は変更できません。
Hitachi AMS/WMS	2000/tcp	管理サーバと通信する際に使用されます。 このポート番号は変更できません。
	28355/tcp	管理サーバと通信する際に使用されます。 このポート番号は変更できません。
Hitachi AMS2000	2000/tcp	管理サーバと非 SSL で通信する際に使用されます。 このポート番号は変更できません。

対象ストレージシステム	ポート番号	説明
	28355/tcp	管理サーバと SSL で通信する際に使用されます。 このポート番号は変更できます。
Hitachi SMS	2000/tcp	管理サーバと非 SSL で通信する際に使用されます。 このポート番号は変更できます。
	28355/tcp	管理サーバと SSL で通信する際に使用されます。 このポート番号は変更できます。
HUS100	2000/tcp	管理サーバと非 SSL で通信する際に使用されます。 このポート番号は変更できます。
	28355/tcp	管理サーバと SSL で通信する際に使用されます。 このポート番号は変更できます。

ミッドレンジストレージ（HUS100、Hitachi SMS、Hitachi AMS2000、Hitachi AMS/WMS、SANRISE9500V）で 사용되는ポート番号（2000/tcp または 28355/tcp）を変更した場合には、管理サーバの OS の `services` ファイルに、変更後のポート番号を設定する必要があります。`services` ファイルに設定しないでミッドレンジストレージを操作すると、エラー（コード：DMEA000006）が発生し、操作が失敗することがあります。

また、ミッドレンジストレージと管理サーバ（Device Manager サーバ）間の通信は、通信するプロトコル（SSL または非 SSL）ごとに使用するポート番号を統一してください。ミッドレンジストレージ間で通信に使用するポート番号が異なる場合、管理サーバの `services` ファイルに設定されているポート番号と異なるポート番号を使用するミッドレンジストレージに対する操作がエラーとなることがあります。また、`services` ファイルに設定されているポート番号と同じ番号を使用しているミッドレンジストレージでも、操作はエラーにはなりませんが、時間が掛かることがあります。

関連項目

- ・ ポート番号の変更方法および `services` ファイルの設定方法：各ストレージシステムのマニュアル

2.1.2 Hitachi Command Suite 共通コンポーネントで使用されるポートの変更

Hitachi Command Suite 製品のインストール後に、Hitachi Command Suite 共通コンポーネントで使用されるポートを変更する場合は、Hitachi Command Suite 共通コンポーネントの設定ファイルを編集する必要があります。

Hitachi Command Suite 共通コンポーネントで使用されるポートを変更するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. Hitachi Command Suite 共通コンポーネントの設定ファイルを編集して、ポート番号の設定を変更します。
3. Hitachi Command Suite 製品のサービスを起動します。
4. 次のポート番号を変更した場合には、管理サーバにインストールされている全 Hitachi Command Suite 製品の URL を変更する必要があります。
 - 23015/tcp（HBase Storage Mgmt Web Service へのアクセスに使用）
非 SSL で管理サーバと管理クライアント間の通信を行うときには、URL を変更する必要があります。
 - 23016/tcp（SSL 対応の HBase Storage Mgmt Web Service へのアクセスに使用）

SSL で管理サーバと管理クライアント間の通信を行うときには、URL を変更する必要があります。

なお、ファイアウォールが設置されている場合など、管理サーバと管理クライアントとの間のネットワーク環境によっては、URL の変更が不要なこともあります。

表 2-7 Hitachi Command Suite 共通コンポーネントのポート番号設定ファイル

デフォルトのポート番号	設定ファイル	変更場所
23015/tcp	Windows の場合： <Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%httpsd%conf %httpsd.conf Solaris または Linux の場合： <Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/httpsd/ conf/httpsd.conf	Listen
	Windows の場合： <Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%conf %hssso.conf Solaris または Linux の場合： <Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/conf/ hssso.conf	hssso.hostport
23016/tcp	Windows の場合： <Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%httpsd%conf %httpsd.conf Solaris または Linux の場合： <Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/httpsd/ conf/httpsd.conf	<ul style="list-style-type: none"> VirtualHost <ホスト名>:<ポート> Listen*1
23017/tcp	Windows の場合： <Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%CC%web %redirector%workers.properties Solaris または Linux の場合： <Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/CC/web/ redirector/workers.properties	worker.worker1.port
	Windows の場合： <Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%CC%web %containers%HiCommand%usrconf %usrconf.properties Solaris または Linux の場合： <Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/CC/web/ containers/HiCommand/usrconf/ usrconf.properties	webserver.connector.ajp13.port
23018/tcp	Windows の場合： <Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%CC%web %containers%HiCommand%usrconf %usrconf.properties Solaris または Linux の場合：	webserver.shutdown.port

デフォルトのポート番号	設定ファイル	変更場所
	< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /CC/web/containers/HiCommand/usrconf/usrconf.properties	
23025/tcp	Windows の場合 : < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %CC%\web\%redirector%\workers.properties Solaris または Linux の場合 : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /CC/web/redirector/workers.properties	worker.worker5.port
	Windows の場合 : < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %CC%\web\%containers%\DeviceManagerWebService\usrconf\usrconf.properties Solaris または Linux の場合 : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /CC/web/containers/DeviceManagerWebService/usrconf/usrconf.properties	webserver.connector.ajp13.port
23026/tcp	Windows の場合 : < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %CC%\web\%containers%\DeviceManagerWebService\usrconf\usrconf.properties Solaris または Linux の場合 : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /CC/web/containers/DeviceManagerWebService/usrconf/usrconf.properties	webserver.shutdown.port
23031/tcp ^{※2}	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %httpsd%\conf\%hssso_httpsd.conf	Listen 127.0.0.1: <ポート番号>
23032/tcp	Windows の場合 : < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %HDB%\CONF\%emb\%HiRDB.ini Solaris または Linux の場合 : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /HDB/conf/emb/HiRDB.ini	PDNAMEPORT
	Windows の場合 : < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %HDB%\CONF\%pdsys Solaris または Linux の場合 : < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /HDB/conf/pdsys	pd_name_port
	Windows の場合 : < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %database%\work\%def_pdsys	pd_name_port

デフォルトのポート番号	設定ファイル	変更場所
	Solaris または Linux の場合： < Hitachi Command Suite 共通コンポーネン トのインストールディレクトリ > /database/ work/def_pdsys	

注※1

HBase Storage Mgmt Web Service へのアクセスで SSL を有効にする場合でも、Listen 23015 行を削除したり、コメント行にしたりしないでください。

注※2

このポートは、管理サーバの OS が Windows の場合にだけ使用されます。



重要 Hitachi Command Suite 共通コンポーネントのポート番号を変更した場合、運用環境によっては次の設定も見直す必要があります。

- 管理クライアント (GUI) で Internet Explorer 6 を使用している場合 (23015/tcp および 23016/tcp) ポップアップブロックの設定を変更する必要があります。
- Element Manager を使用して、Hitachi AMS/WMS または SANRISE9500V を操作する場合 (23015/tcp および 23016/tcp) launchapptool を使用して、Storage Navigator Modular 2 の URL を変更する必要があります。
- Tuning Manager から性能情報を取得している場合 (23015/tcp および 23016/tcp) 同一マシンに Tuning Manager サーバがインストールされているときは、htnm.server.n.port プロパティの設定を見直してください。
- Plug-in for Virtualization Server Provisioning を使用している場合 (23015/tcp および 23016/tcp) Plug-in for Virtualization Server Provisioning の設定を変更する必要があります。
- JP1/IM と連携している場合 (23015/tcp および 23016/tcp) JP1/IM の統合機能メニュー画面から、シングルサインオン機能を使用して Hitachi Command Suite 製品の GUI を呼び出せるように設定している場合は、JP1/IM - View の構成定義ファイルを変更する必要があります。
- Hitachi Virtual File Platform を管理対象ホストとして Device Manager に登録している場合 Device Manager サーバにファイルサーバの構成情報を通知する必要があります。Hitachi File Services Manager の [HDvM 設定編集] ダイアログの [リフレッシュ時に通知する] チェックボックスで [はい] を選択して [OK] ボタンをクリックし、[Processing Node] ウィンドウの [Processing Node 更新] ボタンをクリックしてください。
- Sun Cluster を使用して管理サーバをクラスタ構成にしている場合 (23015/tcp~23017/tcp, 23025/tcp, 23032/tcp) クラスタリソースの登録情報を更新する必要があります。

関連項目

- (1) Hitachi Command Suite 共通コンポーネントで使用されるポート
- 2.5 Hitachi Command Suite 製品の URL の変更 (hcmdschgurl コマンド)
- 5.1.2 Element Manager を使用するための設定
- 5.4 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするために必要な設定
- (6) クラスタリソースの登録 (Sun Cluster の場合)
- 9.2 サービスの起動
- 9.3 サービスの停止
- A.1.1 Device Manager サーバのプロパティの変更
- A.14.5 htnm.server.n.port

- Plug-in for Virtualization Server Provisioning の設定方法：マニュアル「*Hitachi Command Suite Software Plug-in for Virtualization Server Provisioning ユーザーズガイド*」
- Hitachi File Services Manager での設定方法：Hitachi Virtual File Platform のマニュアル

2.1.3 ファイアウォールの例外登録

Hitachi Command Suite 製品で使用されるポートやプロセスをファイアウォールに例外登録すると、登録されたポートやプロセスへの外部からの接続が許可されます。



重要 運用開始後に Windows ファイアウォールを有効にした場合や管理サーバの OS に Linux を使用する場合は、管理サーバに接続されているネットワーク上にファイアウォールが設置されているときは、管理サーバで使用されるポートについては、Hitachi Command Suite のインストール後にユーザーが手動で例外登録を行う必要があります。

- Windows の場合
Hitachi Command Suite を構成する各コンポーネントをファイアウォールの例外リストに登録します。
- Linux の場合
Hitachi Command Suite で使用されるポート番号をファイアウォールの例外リストに登録します。

(1) ファイアウォールへの例外登録が必要なポート

管理サーバや管理クライアント、ストレージシステムなどをつなぐネットワーク上にファイアウォールが設置されている環境では、Hitachi Command Suite 製品で使用されるポートをファイアウォールの例外として登録する必要があります。

- 表 2-8 管理サーバと管理クライアントとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-9 管理サーバとストレージシステムとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-10 管理クライアントとストレージシステムとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-11 管理サーバと通常ホストとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-12 管理サーバと仮想化サーバとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-13 管理サーバとメインフレームホストとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-14 管理サーバとファイルサーバとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-15 Device Manager の管理サーバと Tuning Manager の管理サーバとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-16 管理サーバと Host Data Collector をインストールしたマシンとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-17 Host Data Collector をインストールしたマシンとホストとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-18 管理サーバと SMI-S プロバイダーとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-19 管理サーバと CIM クライアントとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-20 管理サーバとメールサーバとの間のファイアウォールで例外登録が必要なポート番号
- 表 2-21 管理サーバと外部認証サーバとの間のファイアウォールで例外登録が必要なポート番号

表 2-8 管理サーバと管理クライアントとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理クライアント (GUI, Device Manager CLI)	2001/tcp※	管理サーバ	非 SSL 通信の場合に設定が必要 です。
any/tcp	管理クライアント (GUI, Device Manager CLI)	2443/tcp※	管理サーバ	SSL 通信の場合に設定が必要 です。
any/tcp	管理クライアント (Tiered Storage Manager CLI)	20352/tcp※	管理サーバ	非 SSL 通信の場合に設定が必要 です。
any/tcp	管理クライアント (GUI)	23015/tcp※	管理サーバ	非 SSL 通信の場合に設定が必要 です。
any/tcp	管理クライアント (GUI)	23016/tcp※	管理サーバ	SSL 通信の場合に設定が必要 です。
any/tcp	管理クライアント (Tiered Storage Manager CLI)	24500/tcp※	管理サーバ	SSL 通信の場合に設定が必要 です。

注※

ポート番号は変更できます。

表 2-9 管理サーバとストレージシステムとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/udp	<ul style="list-style-type: none"> • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • SANRISE9900 V • HUS VM 	162/udp	管理サーバ	-
any/tcp	管理サーバ	443/tcp	<ul style="list-style-type: none"> • Virtual Storage Platform • HUS VM 	-
any/tcp	管理サーバ	1099/tcp	<ul style="list-style-type: none"> • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • SANRISE9900 V • HUS VM 	-
any/tcp	管理サーバ	2000/tcp※	<ul style="list-style-type: none"> • Hitachi AMS/WMS 	-

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
			<ul style="list-style-type: none"> SANRISE9500 V 	
any/tcp	管理サーバ	2000/tcp※	<ul style="list-style-type: none"> HUS100 Hitachi SMS Hitachi AMS2000 	非 SSL で通信する場合に設定が必要です。
any/tcp	<ul style="list-style-type: none"> Universal Storage Platform V/VM Hitachi USP 	2001/tcp※	管理サーバ	ストレージシステムの任意のポートから管理サーバの 2001/tcp ポートに通信できるように、ファイアウォールを設定してください。
any/tcp	管理サーバ	28355/tcp※	<ul style="list-style-type: none"> HUS100 Hitachi SMS Hitachi AMS2000 	SSL で通信する場合に設定が必要です。
any/tcp	管理サーバ	51099/tcp	<ul style="list-style-type: none"> Virtual Storage Platform Universal Storage Platform V/VM Hitachi USP SANRISE9900 V HUS VM 	-
any/tcp	管理サーバ	51100/tcp	<ul style="list-style-type: none"> Universal Storage Platform V/VM 	バージョン 6.0.0-00 以降の Device Manager サーバにアップグレードインストールした際に設定が必要です。
any/tcp	管理サーバ	51100/tcp	<ul style="list-style-type: none"> Virtual Storage Platform 	-

(凡例)

- : 該当なし

注※

ポート番号は変更できます。

表 2-10 管理クライアントとストレージシステムとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理クライアント (GUI)	80/tcp	<ul style="list-style-type: none"> Virtual Storage Platform Universal Storage Platform V/VM Hitachi USP SANRISE9900 V 	-

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
			<ul style="list-style-type: none"> • HUS VM 	
any/tcp	管理クライアント (GUI)	443/tcp	<ul style="list-style-type: none"> • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • HUS VM 	SSL で Element Manager を使用する場合に設定が必要です。
any/tcp	管理クライアント (GUI)	1099/tcp	<ul style="list-style-type: none"> • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • SANRISE9900 V • HUS VM 	-
any/tcp	管理クライアント (GUI)	51099/tcp	<ul style="list-style-type: none"> • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • SANRISE9900 V • HUS VM 	-
any/tcp	管理クライアント (GUI)	51100/tcp	<ul style="list-style-type: none"> • Virtual Storage Platform • Universal Storage Platform V/VM • HUS VM 	-

(凡例)

- : 該当なし

表 2-11 管理サーバと通常ホストとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	<ul style="list-style-type: none"> • 通常ホスト • 仮想マシン 	2001/tcp※	管理サーバ	-
any/tcp	管理サーバ	24041/tcp※	<ul style="list-style-type: none"> • 通常ホスト • 仮想マシン 	-
any/tcp	管理サーバ	24042/tcp※	<ul style="list-style-type: none"> • 通常ホスト • 仮想マシン 	-

(凡例)

- : 該当なし

注※

ポート番号は変更できます。

表 2-12 管理サーバと仮想化サーバとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理サーバ	443/tcp	<ul style="list-style-type: none"> VMware ESX VMware ESX を管理している VMware vCenter Server 	NPIV を使用して仮想 WWN を仮想マシンに割り当てている場合に設定が必要です。
any/tcp	管理サーバ	5988/tcp	vMA	vMA を使用する構成で、かつ非 SSL 通信の場合に設定が必要です。
any/tcp	管理サーバ	5988/tcp	VMware ESX	vMA を使用しない構成で、かつ非 SSL 通信の場合に設定が必要です。
any/tcp	管理サーバ	5989/tcp	vMA	vMA を使用する構成で、かつ SSL 通信の場合に設定が必要です。
any/tcp	管理サーバ	5989/tcp	VMware ESX	vMA を使用しない構成で、かつ SSL 通信の場合に設定が必要です。

表 2-13 管理サーバとメインフレームホストとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理サーバ	24042/tcp※	メインフレームホスト	-

(凡例)

-: 該当なし

注※

ポート番号は変更できます。

表 2-14 管理サーバとファイルサーバとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	<ul style="list-style-type: none"> Hitachi Virtual File Platform Hitachi NAS Platform 	2001/tcp※	管理サーバ	-
any/tcp	管理サーバ	8443/tcp	Hitachi NAS Platform	-

(凡例)

-: 該当なし

注※

ポート番号は変更できます。

表 2-15 Device Manager の管理サーバと Tuning Manager の管理サーバとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	Device Manager の管理サーバ	22286/tcp ^{※1}	Tuning Manager の管理サーバ	リモート接続された Tuning Manager から、パリティグループの利用率やボリュームの IOPS などの性能情報を取得する場合に設定が必要です。
any/tcp	Device Manager の管理サーバ	22900/tcp～22999/tcp	Tuning Manager の管理サーバ	Tuning Manager とリモート接続する場合に設定が必要です。
any/tcp	Device Manager の管理サーバ	45001/tcp～49000/tcp	Tuning Manager の管理サーバ	-
any/tcp	Tuning Manager の管理サーバ	23015/tcp ^{※1}	Device Manager の管理サーバ	Tuning Manager とリモート接続する場合に設定が必要です。
any/tcp	Tuning Manager の管理サーバ	23032/tcp ^{※2}	Device Manager の管理サーバ	-
any/tcp	Tuning Manager の管理サーバ	24220/tcp ^{※2}	Device Manager の管理サーバ	Tuning Manager とリモート接続する場合に設定が必要です。
any/tcp	Tuning Manager の管理サーバ	1024/tcp～65535/tcp ^{※3}	Device Manager の管理サーバ	リモート接続された Tuning Manager から、パリティグループの利用率やボリュームの IOPS などの性能情報を取得する場合に設定が必要です。

(凡例)

- : 該当なし

注※1

ポート番号は変更できます。

注※2

ポート番号は 5001～65535 の範囲で変更できます。

注※3

Device Manager と Tuning Manager の View Server との通信で使用されるポート番号です。config.xml ファイルおよび configforclient.xml ファイルの ownPort パラメータに設定したポート番号を登録してください。config.xml ファイルおよび configforclient.xml ファイルについては、「(6) config.xml ファイルおよび configforclient.xml ファイルの設定」を参照してください。

表 2-16 管理サーバと Host Data Collector をインストールしたマシンとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理サーバ	22098/tcp [※]	Host Data Collector をインストールしたマシン	次の条件をすべて満たすときに設定が必要です。 ・ Host Data Collector を管理サーバとは別のマシンにインストールしたとき

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理サーバ	22099/tcp [※]	Host Data Collector をインストールしたマシン	・ 非 SSL 通信のとき
any/tcp	管理サーバ	22100/tcp [※]	Host Data Collector をインストールしたマシン	
any/tcp	管理サーバ	22104/tcp [※]	Host Data Collector をインストールしたマシン	次の条件をすべて満たすときに設定が必要です。 <ul style="list-style-type: none"> Host Data Collector を管理サーバとは別のマシンにインストールしたとき SSL 通信のとき
any/tcp	管理サーバ	22105/tcp [※]	Host Data Collector をインストールしたマシン	
any/tcp	管理サーバ	22106/tcp [※]	Host Data Collector をインストールしたマシン	

注※

ポート番号は変更できます。

表 2-17 Host Data Collector をインストールしたマシンとホストとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	Host Data Collector をインストールしたマシン	22/tcp [※]	通常ホスト	管理対象の通常ホストの OS が UNIX の場合に設定が必要です。
any/tcp	Host Data Collector をインストールしたマシン	80/tcp	<ul style="list-style-type: none"> VMware ESX VMware ESX を管理している VMware vCenter Server 	管理対象の仮想化サーバと非 SSL で通信する場合に設定が必要です。
any/tcp	Host Data Collector をインストールしたマシン	139/tcp	通常ホスト	管理対象の通常ホストの OS が Windows の場合に設定が必要です。
any/tcp	Host Data Collector をインストールしたマシン	443/tcp	<ul style="list-style-type: none"> VMware ESX VMware ESX を管理している VMware vCenter Server 	管理対象の仮想化サーバと SSL で通信する場合に設定が必要です。

注※

ポート番号は変更できます。

表 2-18 管理サーバと SMI-S プロバイダーとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	SMI-S プロバイダー	5983/tcp [※]	管理サーバ	-

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理サーバ	5988/tcp※	SMI-S プロバイダー	非 SSL 通信の場合に設定が必要です。
any/tcp	管理サーバ	5989/tcp※	SMI-S プロバイダー	SSL 通信の場合に設定が必要です。

(凡例)

- : 該当なし

注※

ポート番号は変更できます。

表 2-19 管理サーバと CIM クライアントとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	CIM クライアント	427/tcp	管理サーバ	-
any/tcp	CIM クライアント	5988/tcp※	管理サーバ	非 SSL 通信の場合に設定が必要です。
any/tcp	CIM クライアント	5989/tcp※	管理サーバ	SSL 通信の場合に設定が必要です。

(凡例)

- : 該当なし

注※

ポート番号は変更できます。

表 2-20 管理サーバとメールサーバとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理サーバ (Device Manager サーバ)	25/tcp※ ¹	メールサーバ※ ²	次の事象を E メールでユーザーに通知する場合に設定が必要です。 <ul style="list-style-type: none"> ストレージシステムでのアラートの発生 [データマイグレーション] ウィザードから実行したタスクの完了
any/tcp	管理サーバ (Tiered Storage Manager サーバ)	25/tcp※ ¹	メールサーバ※ ³	次の事象を E メールでユーザーに通知する場合に設定が必要です。 <ul style="list-style-type: none"> Tiered Storage Manager CLI で実行したタスクの終了 Legacy モードの Tiered Storage Manager GUI ([マイグレーション] ウィザード) で実行したタスクの終了 ボリュームロック期限の満了

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
				・ マイグレーショングループの指定期間の経過
any/tcp	管理サーバ (Storage Navigator Modular 2)	25/tcp	メールサーバ※4	操作対象のストレージシステムが Hitachi AMS/WMS または SANRISE9500V で、かつ Storage Navigator Modular 2 の E メール障害報告機能を利用する場合に設定が必要です。

注※1

ポート番号は変更できます。

注※2

Device Manager サーバの `server.mail.smtp.host` プロパティに指定したメールサーバです。

注※3

Tiered Storage Manager サーバの `server.mail.smtp.host` プロパティに指定したメールサーバです。

注※4

Storage Navigator Modular 2 で、ストレージシステムの障害報告を発信できるように設定したメールサーバです。

表 2-21 管理サーバと外部認証サーバとの間のファイアウォールで例外登録が必要なポート番号

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
any/tcp	管理サーバ	88/tcp※	Kerberos サーバ	-
any/udp	管理サーバ	88/udp※	Kerberos サーバ	-
any/tcp	管理サーバ	359/tcp※	LDAP ディレクトリサーバ	-
any/udp	管理サーバ	1812/udp※	RADIUS サーバ	-

(凡例)

- : 該当なし

注※

一般的に使用されるポート番号です。外部認証サーバで変更されていることがあります。

関連項目

- ・ (2) ファイアウォールの例外登録 (Windows)
- ・ (3) ファイアウォールの例外登録 (Red Hat Enterprise Linux)
- ・ (4) ファイアウォールの例外登録 (SUSE Linux Enterprise Server)

(2) ファイアウォールの例外登録 (Windows)

`hcmdsfwcancel` コマンドおよび `netsh` コマンドを実行して、Hitachi Command Suite を構成する各コンポーネントをファイアウォールの例外リストに登録します。

ファイアウォールの例外リストに登録するには：

1. 次のコマンドを実行して、Hitachi Command Suite 共通 Web サービスを例外リストに登録します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin
%hcmdsfcancel.bat
```

2. 次のコマンドを実行して、Hitachi Command Suite で使用するそのほかのコンポーネントを例外リストに登録します。

Windows XP, Windows Server 2003 R2, Windows Vista または Windows Server 2008 の場合

```
netsh firewall add allowedprogram program="<パス>" name="<例外登録名>" mode=ENABLE
```

Windows 7, Windows Server 2008 R2 または Windows Server 2012 の場合

```
netsh advfirewall firewall add rule name="<例外登録名>" dir=in
action=allow program=" <パス>" description="<パス>" enable=yes
```

3. 設定を有効にするために、Hitachi Command Suite 製品のサービスを再起動します。

表 2-22 netsh コマンドで指定する例外登録名とパス

コンポーネント	例外登録名	パス
Device Manager サーバ	Device Manager	< Device Manager サーバのインストールフォルダ > %HiCommandServer%HiCommandServer.exe
Tiered Storage Manager サーバ	Tiered Storage Manager(htsmService)	< Tiered Storage Manager サーバのインストールフォルダ > %bin%htsmService.exe
	Tiered Storage Manager(htsmHDvMUser)	< Tiered Storage Manager サーバのインストールフォルダ > %inst%htsmHDvMUser.exe
	Tiered Storage Manager(htsmVersion)	< Tiered Storage Manager サーバのインストールフォルダ > %inst%htsmVersion.exe
	Tiered Storage Manager(schemaDrop)	< Tiered Storage Manager サーバのインストールフォルダ > %inst%schemaDrop.exe
	Tiered Storage Manager(schemaCreate)	< Tiered Storage Manager サーバのインストールフォルダ > %inst%schemaCreate.exe
JDK	HBase(cmd)	Windows XP または Windows Server 2003 R2 の場合 < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %jdk%jre%bin%java.exe Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2 または Windows Server 2012 の場合 < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %jdk5_0%jre%bin%java.exe※
	HBase(cmd)	Windows XP または Windows Server 2003 R2 の場合 < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %jdk%bin%java.exe Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2 または Windows Server 2012 の場合 < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %jdk5_0%bin%java.exe※

注※

Hitachi Command Suite に同梱されている JDK 以外の JDK を使用する場合は、使用する JDK のインストールフォルダにある `java.exe` を絶対パスで指定してください。

関連項目

- (1) ファイアウォールへの例外登録が必要なポート
- 9.2 サービスの起動
- 9.3 サービスの停止

(3) ファイアウォールの例外登録 (Red Hat Enterprise Linux)

テキストモードセットアップユーティリティを使用して、Hitachi Command Suite で使用されるポート番号をファイアウォールの例外リストに登録します。

ファイアウォールの例外リストに登録するには：

1. ターミナルウィンドウから `setup` コマンドを実行します。
テキストモードセットアップユーティリティの [ツール選択] 画面が表示されます。
2. [ファイアウォールの設定] を選択し、[Tab] キーで [実行ツール] ボタンへ移動し、[Enter] キーを押します。
[ファイアウォール設定] 画面が表示されます。
3. [セキュリティレベル] を [有効] に合わせ、スペースキーを押してチェックを入れ、[Tab] キーで [カスタマイズ] ボタンへ移動し、[Enter] キーを押します。
[ファイアウォール設定—カスタマイズ] 画面が表示されます。
4. [その他のポート] に例外登録するポートを指定し、[Tab] キーで [OK] ボタンへ移動し、[Enter] キーを押します。

(例)

その他のポート 162:udp 2001:tcp 23015:tcp



重要 すでにポートが指定されていた場合は、空白区切りで追加入力してください。

5. [ファイアウォール設定] 画面に戻ったら、[セキュリティレベル] が [有効] になっていることを確認し、[Tab] キーで [OK] ボタンへ移動し、[Enter] キーを押します。

関連項目

- (1) ファイアウォールへの例外登録が必要なポート

(4) ファイアウォールの例外登録 (SUSE Linux Enterprise Server)

SUSEfirewall2 ファイルを編集して、Hitachi Command Suite で使用されるポート番号をファイアウォールの例外リストに登録します。

ファイアウォールの例外リストに登録するには：

1. `/etc/sysconfig/SUSEfirewall2` ファイルを編集して、例外登録するポートを指定します。
例外登録するポート番号を次の形式で指定します。
 - `FW_SERVICES_EXT_TCP="<TCP ポート番号>"`
 - `FW_SERVICES_EXT_UDP="<UDP ポート番号>"`

次に示す例では、2001, 23015, 23016, 23017, 23018, 161 および 162 だけが例外登録されます。

```
FW_SERVICES_EXT_TCP="2001 23015:23018"  
FW_SERVICES_EXT_UDP="161 162"
```

2. /sbin/SuSEfirewall12 を実行します。

関連項目

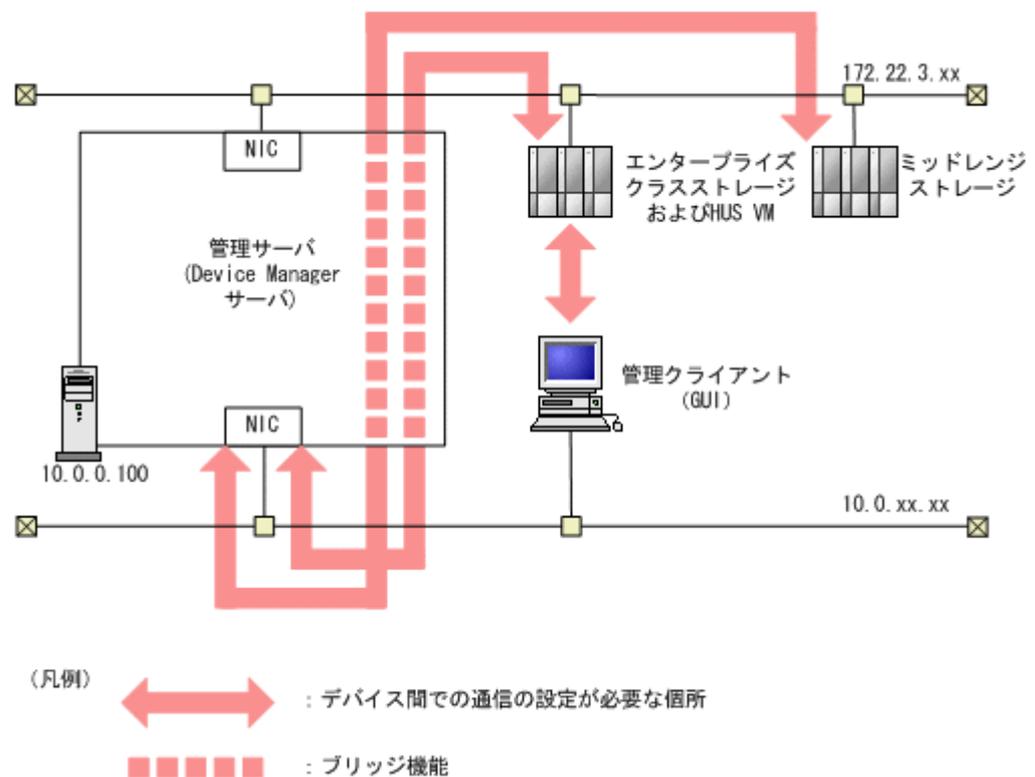
- ・ (1) ファイアウォールへの例外登録が必要なポート

2.2 ブリッジ機能を使用する場合のネットワークの設定

管理サーバに NIC を複数搭載してブリッジ機能を使用する場合、管理サーバ、管理クライアント、およびストレージシステム間でお互いに通信できるようにネットワークを設定してください。

次の図に示す構成を例に、設定が必要な個所を説明します。

図 2-1 管理サーバのブリッジ機能を使用したネットワークの構成例



図中の矢印に示すデバイス間でお互いに通信できるように、ルーター、管理クライアント、および管理サーバを設定してください。

- ・ エンタープライズクラスストレージおよび HUS VM と、管理クライアントの間
- ・ エンタープライズクラスストレージおよび HUS VM と、管理サーバの間
- ・ ミッドレンジストレージと管理サーバの間

管理クライアントとミッドレンジストレージの間の通信は、Storage Navigator Modular 2 または Storage Navigator Modular が管理するため、設定する必要はありません。



注意 Hitachi Command Suite 製品の次の設定で IP アドレスを指定するときは、管理クライアントに接続されているネットワーク側の IP アドレス（「図 2-1 管理サーバのブリッジ機能を使用したネットワークの構成例」中の 10.0.0.100）を指定してください。ホスト名は指定しないでください。

- Device Manager の Web サーバ機能が動作するマシンの設定（server.http.host プロパティ）
- Device Manager からラUNCHする Storage Navigator Modular 2 の URL の設定（launchapp.snm2.url プロパティ）

関連項目

- A.1.1 Device Manager サーバのプロパティの変更
- A.2.1 server.http.host
- A.10.1 launchapp.snm2.url

2.3 IPv6 環境で運用する場合の Device Manager の設定

Device Manager は、IPv6 による通信をサポートしています。IPv6 環境で運用する場合、環境に応じて Device Manager の設定を変更する必要があります。

IPv6 環境で運用する際は、次に示す前提条件を満たすようにしてください。

- IPv6 を使用する場合も、製品内部で IPv4 の処理をする必要があるため、IPv6 と IPv4 の両方を使用できるように OS を設定してください。
- 使用できる IPv6 アドレスはグローバルアドレスだけです。グローバルユニークローカルアドレス（サイトローカルアドレス）やリンクローカルアドレスは使用できません。
- Device Manager サーバの IP アドレスまたはホスト名を指定する場合は、ホスト名で指定することを推奨します。IPv6 アドレスを指定した場合、Internet Explorer 6 では Device Manager サーバに接続できなかつたり、画面遷移ができなかつたりすることがあります。
- Element Manager を使用して、Hitachi AMS/WMS または SANRISE9500V を操作する場合、Storage Navigator Modular 2 の URL を設定する際には、ホスト名を指定してください。

関連項目

- 5.1 Element Manager を使用するために必要な設定

2.3.1 Device Manager を IPv6 環境に移行するときの設定

IPv4 環境で運用していた Device Manager を IPv6 環境で運用する場合は、httpsd.conf ファイルを編集します。



重要 IPv6 環境に Device Manager を新規インストールした場合、インストーラーが自動的に設定を変更するため、この作業は不要です。

Device Manager を IPv6 環境に移行するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. httpsd.conf ファイルを開きます。
httpsd.conf ファイルの格納先を次に示します。
 - Windows の場合：
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%httpsd%conf
%httpsd.conf
 - Solaris または Linux の場合：

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /httpsd/
conf/httpsd.conf

- 「#Listen [::]:<ポート番号>」の先頭にある番号記号 (#) を削除して、IPv6 での通信を有効にします。

SSL 通信の場合の httpsd.conf ファイルを例に、番号記号 (#) を削除する個所を次に示します。

```
ServerName example.com
:
Listen 23015
#Listen [::]:23015
SSLDisable
:
SSLSessionCacheSize 0
Listen 23016
#Listen [::]:23016
<VirtualHost *:23016>
    ServerName example.com
    SSLEnable
:
```

先頭にある番号記号 (#) を削除

先頭にある番号記号 (#) を削除
(SSL通信の場合だけ)



注意

- 非 SSL 通信の場合、SSLSessionCacheSize の下にある Listen 行の番号記号 (#) を削除する必要はありません。
- デフォルトでは、すべての IPv6 アドレスと通信できるように設定されています。
- ポート番号は IPv4 の Listen 行と同じ番号を指定してください。
- IPv4 の Listen 行を削除したり編集したりしないでください。誤って削除、編集した場合、IPv4 での通信ができなくなります。

- Hitachi Command Suite 製品のサービスを起動します。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

2.3.2 IPv6 に対応したストレージシステムと連携するための設定

IPv6 アドレスで管理している Universal Storage Platform V/VMM を Element Manager で操作する場合は、Device Manager サーバの server.properties ファイルを編集します。

IPv6 に対応したストレージシステムと連携するには：

- Device Manager サーバの server.properties ファイルにある server.http.host プロパティに、次のどちらかを設定します。
 - Device Manager サーバがインストールされているマシンの IPv6 アドレス
 - Device Manager サーバがインストールされているマシンのホスト名
ホスト名から IPv6 アドレスの名前解決ができる必要があります。



注意 IPv4 アドレスで管理している Universal Storage Platform V/VMM または Hitachi USP も Device Manager の管理対象にする場合は、server.http.host プロパティに指定した IPv6 アドレスが設定されている NIC に、IPv4 アドレスも設定する必要があります。

関連項目

- A.1.1 Device Manager サーバのプロパティの変更
- A.2.1 server.http.host

2.4 管理サーバの IP アドレスまたはホスト名の変更

ネットワーク構成の変更などに伴い、管理サーバの IP アドレスまたはホスト名が変更になった場合は、Hitachi Command Suite 製品の設定も変更する必要があります。

2.4.1 管理サーバのホスト名の変更

変更後のホスト名を Hitachi Command Suite 製品に反映するには、`/etc/hosts` ファイル (Solaris または Linux の場合)、`httpsd.conf` ファイル、および `cluster.conf` ファイル (クラスタ構成の場合) を編集したあと、マシンを再起動します。

事前に確認しておく情報

- 変更後の管理サーバのホスト名
ホスト名は 32 バイト以内である必要があります。Hitachi Command Suite 製品では、大文字と小文字は区別されます。



参考 事前に管理サーバのホスト名を変更した場合、`hostname` コマンドで表示させた変更後のホスト名を控えておいてください。Windows の場合は `ipconfig /ALL` コマンドでも表示できます。

管理サーバのホスト名を変更するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. 管理クライアントや SMI-S プロバイダーと、管理サーバとの通信に TLS/SSL を使用している場合は、変更後のホスト名を使用して、管理サーバのサーバ証明書を作成し直します。
次のコンポーネント間の通信に SSL/TLS を使用している場合に必要な作業です。
 - 管理サーバと管理クライアント (GUI) 間
 - 管理サーバと管理クライアント (Device Manager CLI) 間
 - Device Manager サーバと Replication Manager サーバ間
 - Tuning Manager サーバと Device Manager サーバ間
 - SMI-S プロバイダーと管理サーバ間
 - 管理サーバと CIM クライアント間
3. Solaris または Linux の場合、`/etc/hosts` ファイルを編集します。
管理サーバのホスト名を変更後のホスト名に変更します。Linux の場合は、`localhost` が記述されている行よりも、上の行に変更後のホスト名を記述してください。
4. `httpsd.conf` ファイルを編集します。
`ServerName` パラメーターの値を変更後のホスト名に変更します。
 - Windows の場合：
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%httpsd%conf
¥httpsd.conf
 - Solaris または Linux の場合：
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/httpsd/
conf/httpsd.conf管理サーバと管理クライアントとの通信に TLS/SSL を使用している場合は、さらに次の設定も変更してください。
 - <VirtualHost>タグにホスト名が指定されている場合は、アスタリスク (*) に変更します。

- <VirtualHost>タグ内の ServerName パラメーターの値を変更後のホスト名に変更します。
5. cluster.conf ファイルを編集します (クラスタ構成の場合だけ)。

論理ホスト名, 実行系ノードのホスト名, 待機系ノードのホスト名のうち, 該当するホスト名を変更後のホスト名に変更します。

 - Windows の場合 :


```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %conf
          %cluster.conf
```
 - Solaris の場合 :


```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /conf/
          cluster.conf
```
 6. 管理サーバのホスト名を変更し, マシンを再起動します。

Hitachi Command Suite 共通コンポーネントの設定ファイルを変更する前に, 管理サーバのホスト名を変更していた場合は, ここではマシンの再起動だけを実行してください。
 7. Hitachi Command Suite 製品のサービスが起動していることを確認します。
 8. Hitachi Command Suite 製品の URL にホスト名を使用している場合は, 管理サーバにインストールされている全 Hitachi Command Suite 製品の設定を変更します。
 9. 運用環境によって, 各 Hitachi Command Suite 製品の設定を見直します。
 10. データベースをバックアップします。

ホスト名を変更するとバックアップしたデータベースは使用できなくなります。

関連項目

- [2.4.3 管理サーバの IP アドレスまたはホスト名の変更後に必要な作業](#)
- [2.5 Hitachi Command Suite 製品の URL の変更 \(hcmdschgurl コマンド\)](#)
- [9.3 サービスの停止](#)
- [9.4 サービスの稼働状態の確認](#)
- [10.2.1 データベースのバックアップ \(非クラスタ構成の場合\)](#)
- [10.2.2 データベースのバックアップ \(Microsoft Cluster Service または Windows Server Failover Clustering の場合\)](#)
- [10.2.3 データベースのバックアップ \(Veritas Cluster Server の場合\)](#)
- [10.2.4 データベースのバックアップ \(Sun Cluster の場合\)](#)

2.4.2 管理サーバの IP アドレスの変更

変更後の IP アドレスを Hitachi Command Suite 製品に反映するには, httpsd.conf ファイルを編集したあと, マシンを再起動します。

事前に確認しておく情報

- 変更後の管理サーバの IP アドレス



注意 クラスタ構成ファイル (cluster.conf ファイル) の設定は変更しないでください。

管理サーバの IP アドレスを変更するには :

1. Hitachi Command Suite 製品のサービスを停止します。

2. httpsd.conf ファイルを編集します。

ServerName パラメーターに変更前の IP アドレスが指定されている場合は、ホスト名または変更後の IP アドレスに変更します。

- Windows の場合 :

< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > \httpsd\conf
¥httpsd.conf

- Solaris または Linux の場合 :

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /httpsd/
conf/httpsd.conf



重要 httpsd.conf ファイルの設定ではホスト名を指定することをお勧めします。

3. 管理サーバの IP アドレスを変更し、マシンを再起動します。
Hitachi Command Suite 共通コンポーネントの設定ファイルを変更する前に、管理サーバの IP アドレスを変更していた場合は、ここではマシンの再起動だけを実行してください。
4. Hitachi Command Suite 製品のサービスが起動していることを確認します。
5. Hitachi Command Suite 製品の URL に IP アドレスを使用している場合は、管理サーバにインストールされている全 Hitachi Command Suite 製品の設定を変更します。
6. 運用環境によって、各 Hitachi Command Suite 製品の設定を見直します。
7. データベースをバックアップします。
IP アドレスを変更するとバックアップしたデータベースは使用できなくなります。

関連項目

- 2.4.3 管理サーバの IP アドレスまたはホスト名の変更後に必要な作業
- 2.5 Hitachi Command Suite 製品の URL の変更 (hcmdschgurl コマンド)
- 9.3 サービスの停止
- 9.4 サービスの稼働状態の確認
- 10.2.1 データベースのバックアップ (非クラスタ構成の場合)
- 10.2.2 データベースのバックアップ (Microsoft Cluster Service または Windows Server Failover Clustering の場合)
- 10.2.3 データベースのバックアップ (Veritas Cluster Server の場合)
- 10.2.4 データベースのバックアップ (Sun Cluster の場合)

2.4.3 管理サーバの IP アドレスまたはホスト名の変更後に必要な作業

管理サーバの IP アドレスまたはホスト名を変更した場合に、運用環境によっては Device Manager, Tiered Storage Manager および Replication Manager の設定を見直す必要があります。

- server.http.host プロパティに変更前のホスト名または IP アドレスを設定している場合
変更後のホスト名または IP アドレスに設定し直したあと、Hitachi Command Suite 製品のサービスを再起動する必要があります。
- Device Manager エージェントを使用している場合
hdvmagt_setting コマンドを実行して、Device Manager サーバの情報の設定を変更する必要があります。
- Replication Manager を使用している場合

情報取得元として登録していた IP アドレスまたはホスト名を変更した場合は、情報取得元を登録し直してください。

- Element Manager を使用して、Hitachi AMS/WMS または SANRISE9500V を操作する場合 launchapptool を使用して、Storage Navigator Modular 2 の URL を変更する必要があります。
- RADIUS サーバを利用してアカウントを認証している場合
exauth.properties ファイルの設定を見直してください。
- Device Manager サーバと Tuning Manager サーバがリモート接続している場合
次の条件をすべて満たすときには、リポジトリの所在登録を変更してください。
 - Device Manager サーバがインストールされているマシンの IP アドレスを変更した
 - Device Manager サーバがインストールされているマシンの IP アドレスを Tuning Manager サーバがインストールされているマシンの hssso.conf ファイルに設定している
- Tuning Manager から性能情報を取得している場合
config.xml ファイルおよび configforclient.xml ファイルの ownHost パラメーターの設定を見直してください。
- ファイルサーバの SNMP トラップを受信している場合
SNMP トラップの通知先 (SNMP マネージャー) のホスト名または IP アドレスを Hitachi File Services Manager で変更してください。
- Plug-in for Virtualization Server Provisioning を使用している場合
Plug-in for Virtualization Server Provisioning の設定を変更する必要があります。
- JP1/IM と連携している場合
JP1/IM の統合機能メニュー画面から、シングルサインオン機能を使用して Hitachi Command Suite 製品の GUI を呼び出せるように設定している場合は、JP1/IM - View の構成定義ファイルを変更する必要があります。

そのほかに IP アドレスやホスト名が設定されているスクリプトファイルやバッチファイルなどがあれば設定を見直してください。

関連項目

- [5.1.2 Element Manager を使用するための設定](#)
- [\(6\) config.xml ファイルおよび configforclient.xml ファイルの設定](#)
- [5.4 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするために必要な設定](#)
- [9.2 サービスの起動](#)
- [9.3 サービスの停止](#)
- [11.3.4 Device Manager サーバの情報, HiScan コマンドの実行周期および RAID Manager または P9000 RAID Manager の情報の設定 \(hdvmagt_setting コマンド\)](#)
- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.2.1 server.http.host](#)
- Replication Manager 情報取得元の登録方法：マニュアル「*Hitachi Command Suite Replication Manager Software ユーザーズガイド*」
- リポジトリの所在登録を変更する方法：マニュアル「*Hitachi Command Suite Tuning Manager Software 運用管理ガイド*」
- ファイルサーバの SNMP トラップ通知先の変更方法：ファイルサーバのマニュアル
- Plug-in for Virtualization Server Provisioning の設定方法：マニュアル「*Hitachi Command Suite Software Plug-in for Virtualization Server Provisioning ユーザーズガイド*」

- Device Manager, Tiered Storage Manager および Replication Manager 以外で必要になる設定 : 各 Hitachi Command Suite 製品のマニュアル

2.5 Hitachi Command Suite 製品の URL の変更 (hcmdschgurl コマンド)

次の構成変更に伴い、運用開始後に Hitachi Command Suite 製品の URL が変更になった場合には、GUI に登録されている各 Hitachi Command Suite 製品の URL も hcmdschgurl コマンドで変更する必要があります。

- HBase Storage Mgmt Web Service が使用するポートの変更
- 管理サーバのホスト名または IP アドレスの変更
- SSL を使用するため、または SSL の使用を中止するための設定変更
- クラスタ環境への移行

Hitachi Command Suite 製品の URL を変更するには :

1. hcmdschgurl コマンドを実行します。

Windows の場合 :

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin
%hcmdschgurl {/print | /list | /change <変更前の URL > <変更後の URL
> | /change <変更後の URL > /type < Hitachi Command Suite 製品の名称 > }
```

Solaris または Linux の場合 :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/
hcmdschgurl {-print | -list | -change <変更前の URL > <変更後の URL
> | -change <変更後の URL > -type < Hitachi Command Suite 製品の名称 > }
```

- print

現在登録されている URL とプログラムのリストを表示する場合に指定します。

- list

print オプションと同じ内容を異なるフォーマットで表示する場合に指定します。

- change

URL を変更する場合に指定します。

- type

特定の Hitachi Command Suite 製品の URL だけを変更する場合に、対象の製品の名称を指定します。Device Manager の URL だけを変更する場合には、DeviceManager と指定します。Tiered Storage Manager の URL だけを変更する場合には、TieredStorageManager と指定します。Replication Manager の URL だけを変更する場合には、ReplicationManager と指定します。そのほかの Hitachi Command Suite 製品の名称については、それぞれのマニュアルを参照してください。

2. Windows の場合は、ショートカットファイルの URL を変更します。

Windows XP, Windows Server 2003 R2, Windows Vista, Windows 7, Windows Server 2008 または Windows Server 2008 R2 の場合 :

```
[スタート] - [すべてのプログラム] - [Hitachi Command Suite] - [Login - HCS]
を右クリックして、[プロパティ] - [Web ドキュメント] タブの URL を変更します。
```

Windows Server 2012 の場合 :

スタート画面からアプリケーションの一覧画面を表示し、[Hitachi Command Suite] の [Login - HCS] を右クリックして、[プロパティ] - [Web ドキュメント] タブの URL を変更します。

URL の形式は次のとおりです。

<プロトコル>://<管理サーバの IP アドレス>:<ポート番号>/DeviceManager/

◦ <プロトコル>

非 SSL 通信の場合は http、SSL 通信の場合は https を指定します。

◦ <管理サーバの IP アドレス>

管理サーバの IP アドレスまたはホスト名を指定します。

◦ <ポート番号>

httpsd.conf ファイルの Listen 行に指定したポート番号を指定します。非 SSL 通信の場合は非 SSL 通信用のポート番号（デフォルト：23015）、SSL 通信の場合は、SSL 通信用のポート番号（デフォルト：23016）を指定してください。

httpsd.conf ファイルの格納先は次のとおりです。

<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%httpsd%conf
%httpsd.conf



注意

- 指定する URL は、プロトコルとポートを含む完全な URL である必要があります。IPv6 アドレスは使用できません。IPv6 環境ではホスト名で指定してください。以下にその例を示します。

http://127.0.0.1:23015

http://hostname:23015

- クラスタ環境への移行に伴い URL を変更する場合は、<変更後の URL >は次の形式で指定してください。

http://<論理ホスト名>:<ポート番号>

関連項目

- 2.1.2 Hitachi Command Suite 共通コンポーネントで使用されるポートの変更
- 2.4.1 管理サーバのホスト名の変更
- 2.4.2 管理サーバの IP アドレスの変更
- 8.2.3 クラスタ環境への変更 (Windows)
- 8.3.3 クラスタ環境への変更 (Solaris)

ユーザーアカウントを管理するために必要な設定

この章では、Hitachi Command Suite 製品のユーザーアカウントを管理するために必要な設定について説明します。

- 3.1 パスワードポリシーとは
- 3.2 アカウントロックとは
- 3.3 外部認証サーバでのユーザー管理

3.1 パスワードポリシーとは

パスワードポリシーとは、ユーザーアカウントのパスワードに使用できる文字数や、文字種の組み合わせなどに関する条件のことです。

パスワードポリシーを設定することで、推測されやすいパスワードをユーザーが設定することを防ぎ、第三者から不正にアクセスされるリスクを軽減できます。

パスワードポリシーには、次の条件を指定できます。

- パスワードの最小文字数
- パスワードに含める大文字の最小数
- パスワードに含める小文字の最小数
- パスワードに含める数字の最小数
- パスワードに含める記号の最小数
- ユーザー ID と同じパスワードの設定可否

ユーザーアカウントを管理サーバで管理する場合は、これらの条件を設定してパスワードを複雑にすることをお勧めします。

3.1.1 パスワードポリシーの設定

Hitachi Command Suite 製品のパスワードポリシーは、`security.conf` ファイルで設定します。

パスワードポリシーを設定するには：

1. `security.conf` ファイルを編集します。
`security.conf` ファイルの格納先を次に示します。

- Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>\%conf%\sec  
%security.conf
```

- Solaris または Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/  
conf/sec/security.conf
```

`security.conf` ファイルで指定できるパスワードポリシーを次の表に示します。

表 3-1 `security.conf` ファイルで指定できるパスワードポリシー

項目	説明
<code>password.min.length</code>	パスワードの最小文字数を指定します。指定できる値の範囲は、1～256 です。 デフォルト：4
<code>password.min.uppercase</code>	パスワードに含める大文字の最小数を指定します。指定できる値の範囲は、0～256 です。0 を指定した場合、大文字の数に制限はなくなります。 デフォルト：0
<code>password.min.lowercase</code>	パスワードに含める小文字の最小数を指定します。指定できる値の範囲は、0～256 です。0 を指定した場合、小文字の数に制限はなくなります。 デフォルト：0
<code>password.min.numeric</code>	パスワードに含める数字の最小数を指定します。指定できる値の範囲は、0～256 です。0 を指定した場合、数字の数に制限はなくなります。

項目	説明
	デフォルト：0
password.min.symbol	パスワードに含める記号の最小数を指定します。指定できる値の範囲は、0～256 です。0 を指定した場合、記号の数に制限はなくなります。 デフォルト：0
password.check.userID	ユーザー ID と同じパスワードを設定できるようにするかを指定します。true を指定した場合、ユーザー ID と同じパスワードは設定できなくなります。false を指定した場合、ユーザー ID と同じパスワードを設定できます。 デフォルト：false

security.conf ファイルの設定値を変更すると、直ちに変更後のパスワードポリシーが有効になります。



注意

- 設定したパスワードポリシーは、すべての Hitachi Command Suite 製品で、ユーザーアカウントを追加するとき、またはパスワードを変更するときに適用されます。既存のユーザーアカウントのパスワードには適用されないため、設定した条件をパスワードが満たしていない場合でも、システムにログインできます。
- パスワードポリシーは GUI から設定できます。ただし、クラスタ構成の環境の場合には、GUI から設定すると実行系ノードだけに反映されます。待機系ノードに反映するときは、ノードを切り替えてから同一の設定を実施してください。
- 外部認証サーバと連携してユーザー認証を行う場合、パスワードの文字種の組み合わせは外部認証サーバでの設定が適用されます。ただし、Hitachi Command Suite 製品にユーザーのパスワードを登録する場合は、Hitachi Command Suite 製品で規定された文字種を使用する必要があります。

3.2 アカウントロックとは

アカウントロックとは、ユーザーアカウントをロックする（一時的に無効にする）ことです。

アカウントロックを有効にすることで、第三者による不正アクセスのリスクを軽減できます。ユーザーアカウントを管理サーバで管理する場合は、アカウントロックを有効にすることをお勧めします。

Hitachi Command Suite 製品では、ユーザーが複数回連続して GUI へのログインに失敗した場合に、ユーザーアカウントを自動的にロックできます。

アカウントロックを有効にするには、アカウントロックポリシー（アカウントをロックするログイン連続失敗回数）を設定する必要があります。



参考 GUI では、アカウントロックの方法として、任意のユーザーアカウントのロック状態を変更することもできます。

なお、ロック状態の変更は、User Management の Admin 権限を持つユーザーだけが操作できます。



注意

- System アカウントは、Hitachi Command Suite 製品の初期導入時にはアカウントロックの対象になっていません。System アカウントにはすべての Hitachi Command Suite 製品の Admin 権限が設定されています。セキュリティを強化するために System アカウントもロックの対象にする場合は、設定を変更する必要があります。
- 外部認証サーバと連携してユーザー認証を行う場合、自動ロックの制御は、外部認証サーバでの設定が適用されます。

3.2.1 アカウントロックポリシーとは

アカウントロックポリシーとは、ユーザーが複数回連続して GUI へのログインに失敗した場合に、そのユーザーアカウントを自動的にロックするログイン連続失敗回数のことです。

アカウントロックポリシーを設定すると、シングルサインオン機能を利用しているすべての Hitachi Command Suite 製品に直ちに適用されます。例えば、ログイン連続失敗回数が 3 回に設定されている場合、ユーザーが、Device Manager で 1 回、Tiered Storage Manager で 1 回、Replication Manager で 1 回、連続してログインに失敗すると、ユーザーアカウントが自動的にロックされます。

3.2.2 アカウントロックポリシーの設定

Hitachi Command Suite 製品のアカウントロックポリシーは、security.conf ファイルで設定します。

アカウントロックポリシーを設定するには：

1. security.conf ファイルを編集します。
security.conf ファイルの格納先を次に示します。

- Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%conf%sec  
%security.conf
```

- Solaris または Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/  
conf/sec/security.conf
```

security.conf ファイルで指定できるアカウントロックポリシーを次の表に示します。

表 3-2 security.conf ファイルで指定できるアカウントロックポリシー

項目	説明
account.lock.num	自動的にアカウントをロックするまでのログイン連続失敗回数を指定します。指定できる値の範囲は、0～10 です。 ユーザーがログインに連続して失敗した回数が指定値に達すると、ユーザーアカウントが自動的にロックされます。 0 を指定した場合、ユーザーがログインに何度失敗しても、ユーザーアカウントはロックされません。 デフォルト：0

security.conf ファイルの設定値を変更すると、直ちに変更後のアカウントロックポリシーが有効になります。



注意

- ログイン連続失敗回数を変更した場合、その値は、変更後にログインに失敗したときから適用されます。ログイン中のユーザーがいるときに、再度そのユーザーでログインを試行し、失敗回数が指定値に達すると、そのユーザーアカウントはロックされます。ただし、すでにログインしているユーザーは操作を継続できます。
- アカウントロックポリシーは GUI からでも設定できます。ただし、クラスタ構成の環境の場合には、GUI から設定すると実行系ノードだけに反映されます。待機系ノードに反映するときは、ノードを切り替えてから同一の設定を実施してください。

3.2.3 System アカウントのロックに関する設定

System アカウントもアカウントロックの対象にする場合は、user.conf ファイルで設定します。

System アカウントをアカウントロックの対象にするには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. user.conf ファイルを開きます。
user.conf ファイルの格納先を次に示します。
 - Windows の場合：
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%conf
%user.conf
 - Solaris または Linux の場合：
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/conf/
user.confuser.conf ファイルが存在しない場合は、新規に作成してください。
3. 次の形式で account.lock.system プロパティを指定します。

```
account.lock.system=true
```

4. Hitachi Command Suite 製品のサービスを起動します。

すべての Hitachi Command Suite 製品で、System アカウントがアカウントロックの対象になります。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

3.2.4 アカウントロックの解除

ロックされたユーザーアカウントは、hcmdsunlockaccount コマンドで解除できます。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

事前に確認しておく情報

- ロックされたユーザーアカウントに User Management の Admin 権限があることの確認
User Management の Admin 権限がないユーザーアカウントの場合は、User Management の Admin 権限を持つほかのユーザーにアカウントロックの解除を依頼してください。
- ロックされたユーザーアカウントのユーザー ID とパスワード

アカウントロックを解除するには：

1. hcmdsunlockaccount コマンドを実行して、ロックを解除します。

Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin  
%hcmdsunlockaccount [/user <ユーザー ID > /pass <パスワード>]
```

Solaris または Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdsunlockaccount [-user <ユーザー ID > -pass <パスワード>]
```

user オプションおよび pass オプションを省略してコマンドを実行すると、対話形式でユーザー ID およびパスワードを入力できます（対話形式では入力した文字列が伏せ字で表示されません）。



注意 ユーザー ID またはパスワードに記号が含まれる場合は、コマンドライン上でエスケープする必要があります。

- Windows の場合：
円記号 (¥) が末尾にある場合は、末尾の円記号 (¥) を円記号 (¥) でエスケープしてください。
また、アンバサンド (&), 縦線 (|) またはアクサンシルコンフлекс (^) が含まれる場合は、記号 1 文字ごとに引用符 (") で囲むか、アクサンシルコンフлекс (^) でエスケープしてください。
 - Solaris または Linux の場合：
記号 1 文字ごとに円記号 (¥) でエスケープしてください。
-

3.3 外部認証サーバでのユーザー管理

このマニュアルでは、以下の内容は、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制により非公開となっています。以下の内容については、製品に付属するマニュアルをご覧ください。

セキュリティ設定

この章では、Hitachi Command Suite 製品を運用する際に必要なセキュリティ設定について説明します。

- 4.1 警告バナーとは
- 4.2 通信に関するセキュリティ設定
- 4.3 管理サーバに接続できる管理クライアントを制限するための設定
- 4.4 Device Manager CLI または Tiered Storage Manager CLI でパスワードをコード化するときの強度の変更

4.1 警告バナーとは

警告バナーとは、Hitachi Command Suite 製品のログイン画面に表示されるセキュリティメッセージ欄のことです。

Hitachi Command Suite 製品では、ログイン時のセキュリティリスク対策として、任意のメッセージを警告バナーに表示できます。不正なアクセスを試みようとする第三者に対し、事前に警告を発することで、データの破壊や情報の漏洩などのリスクを軽減できます。

4.1.1 警告バナーに表示するメッセージの条件

hcmdsbanner コマンドで警告バナーに表示するメッセージを登録する場合、文字数や文字コードに制限があります。

- HTML タグを使って記載してください。フォント属性の変更や任意の位置での改行などの操作もできます。

HTML タグの条件を次に示します。

- 任意の位置で改行する場合は、
タグを使用してください。
- HTML の構文で使用する文字 (< > " ' &) を表示する場合は、HTML のエスケープシーケンスを使用してください。例えば、ログイン画面にアンパサンド (&) を表示する場合は、HTML ファイルでは「&」と記述します。
- 使用できる最大文字数は 1,000 文字です (HTML タグも文字数としてカウントされます)。
- 使用できる文字コードは Unicode (UTF-8) です。

4.1.2 警告バナーに表示するメッセージの作成と登録

Hitachi Command Suite 製品の警告バナーに表示するメッセージは、テキストエディターなどを使って作成し、hcmdsbanner コマンドを実行して登録します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

警告バナーに表示するメッセージを作成および登録するには：

1. テキストエディターなどを使い、メッセージを作成します。

英語 (bannermsg.txt) と日本語 (bannermsg_ja.txt) のメッセージのサンプルファイルが次の場所にあります。

- Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>\¥sample  
¥resource
```

- Solaris または Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/sample/  
resource
```

このサンプルファイルはインストールの際に上書きされてしまうので、利用する場合はコピーしたものを編集してください。

メッセージのひな形を次に示します。

```
<center><b>警告</b></center>  
これは{会社名}のコンピュータシステムです。このコンピュータシステムは、承認を受けた人だけがその業務のためにのみ使用できます。承認を受けない人からのアクセスや使用があった場合、侵入者として刑
```

事、民事、および行政上の訴訟を提起する場合があります。
犯罪捜査を含む公の目的のために、このコンピュータシステムに対するすべてのアクセスの履歴は、責任者によって傍受、記録、読み取り、複写、および開示される場合があります。アクセスした人に関する私的な機密情報についても機密性とプライバシーの要件に従って暗号化され、アクセス履歴として記録されます。このシステムを使用する人は、承認を受けているかどうかに関係なく、上記の条件に同意したものとみなします。このシステムにおいてプライバシーの権利はありません。

2. hcmsgbanner コマンドを実行して、メッセージを登録します。

◦ Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin  
%hcmsgbanner /add /file <ファイル名> [/locale <ロケール名>]
```

◦ Solaris または Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmsgbanner -add -file <ファイル名> [-locale <ロケール名>]
```

<ファイル名>

メッセージを格納したファイルを絶対パスで指定します。Solaris または Linux の場合、空白を含むパスは指定しないでください。

<ロケール名>

メッセージに使用した言語のロケールを指定します（英語は en、日本語は ja です）。省略すると、ロケールに関係なく、登録したメッセージが常に警告バナーに表示されます（デフォルトのロケールのメッセージとして登録されます）。

GUI を複数のロケールで使用する場合、同じ内容のメッセージをロケールごとに別の言語で登録しておく、Web ブラウザーのロケールに合わせて、メッセージを自動的に切り替えられます。

1 つの Web ブラウザーに複数の言語が設定されている場合、警告バナーのロケールは Web ブラウザーの言語の優先順位に従います。



重要 指定したロケールのメッセージがすでに登録されていた場合に、hcmsgbanner コマンドを実行すると、上書き更新されます。



参考 次の場合は GUI からでも操作できます。

- ロケールを指定せずにメッセージを登録する場合
- hcmsgbanner コマンドで locale オプションを省略して登録したメッセージを編集する場合
ただし、GUI から操作する場合は、次の制限があります。
- 使用できる HTML タグに制限があります。
- クラスタ構成の環境の場合は、実行系ノードだけに反映されます。待機系ノードに反映するときは、ノードを切り替えてから同一の操作を実施してください。

メッセージが管理サーバに登録され、Hitachi Command Suite 製品のログイン画面に表示されます。

4.1.3 警告バナーからのメッセージの削除

Hitachi Command Suite 製品の警告バナーに表示されたメッセージを削除するには hcmsgbanner コマンドを実行します。

事前に完了しておく操作

- Administrator 権限（Windows の場合）または root（Solaris または Linux の場合）でのログイン

事前に確認しておく情報

- 削除するメッセージのロケール（英語は en、日本語は ja です）

メッセージを削除するには：

1. hcmdsbanner コマンドを実行します。

- Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>\%bin  
%hcmdsbanner /delete [/locale <ロケール名>]
```

- Solaris または Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdsbanner -delete [-locale <ロケール名>]
```

<ロケール名>

削除するメッセージのロケールを指定します（英語は en、日本語は ja です）。省略するとデフォルトのロケールが指定されます。



参考 次のメッセージは GUI から削除できます。

- GUI から登録したメッセージ
 - hcmdsbanner コマンドで locale オプションを省略して登録したメッセージ
- ただし、クラスタ構成の環境の場合、GUI から操作すると実行系ノードだけに反映されます。待機系ノードに反映するときは、ノードを切り替えてから同一の操作を実施してください。

4.2 通信に関するセキュリティ設定

このマニュアルでは、以下の内容は、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制により非公開となっています。以下の内容については、製品に付属するマニュアルをご覧ください。

4.3 管理サーバに接続できる管理クライアントを制限するための設定

Hitachi Command Suite 製品では、GUI/CLI 経由で管理サーバにアクセスする管理クライアントを制限できます。管理サーバに接続できる管理クライアントを制限するには、httpsd.conf ファイルと Device Manager サーバのプロパティファイルを編集します。

事前に確認しておく情報

- 管理サーバへの接続を許可する管理クライアントのマシン情報
接続を許可する管理クライアントの情報は、次のどれかの形式で指定します。
 - ドメイン名（例 hitachi.datasystem.com）
 - ドメイン名の一部（例 hitachi）
 - IPv4 または IPv6 アドレス（例 10.1.2.3, 127.0.0.1, 2001::123:4567:89ab:cdef）
 - IPv4 アドレスの一部（例 10.1 この場合、10.1.0.0/16 と同じ意味になります）
 - IPv4 のネットワーク/ネットマスクの形式（例 10.1.0.0/255.255.0.0）
 - IPv4 または IPv6 のネットワーク/c の CIDR 形式（c は、ネットワークアドレスのビット数を表す 10 進の整数）（例 10.1.0.0/16, 2001:0:0:1230::/64）

管理サーバに接続できる管理クライアントを制限するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. 管理サーバへの接続を許可する管理クライアントの情報を、httpsd.conf ファイルの最終行に登録します。

httpsd.conf ファイルの格納先

- Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%httpsd%conf%httpsd.conf
```

- Solaris または Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/httpsd/conf/httpsd.conf
```

httpsd.conf ファイルへの指定形式

```
<Location /DeviceManagerWebService>
    order allow,deny
    allow from <管理クライアントの情報> [<管理クライアントの情報>...]
</Location>
```

- order は、必ず形式どおりに指定してください。余分な空白やタブなどを挿入すると動作しません。
- allow from 行は、複数記述できます。
- 1 行の allow from 内で管理クライアントを複数指定する場合は、空白で区切ってください。
- 管理サーバで Hitachi Command Suite 製品の GUI または CLI を使用する場合は、ローカルループバックアドレス (127.0.0.1 または localhost) も指定する必要があります。

httpsd.conf ファイルの登録例

```
<Location /DeviceManagerWebService>
    order allow,deny
    allow from 127.0.0.1 10.0.0.1 2001::123:4567:89ab:cdef
    allow from 10.1.0.0/16 2001:0:0:1230::/64
</Location>
```

3. Device Manager サーバの server.properties ファイルにある server.http.security.clientIP プロパティまたは server.http.security.clientIPv6 プロパティに、管理クライアントの情報を登録します。
4. Hitachi Command Suite 製品のサービスを起動します。



注意 httpsd.conf ファイルに登録していない管理クライアントからほかの Hitachi Command Suite 製品にログインしている場合は、その Hitachi Command Suite 製品では GUI を起動できません。

関連項目

- [9.2 サービスの起動](#)
- [9.3 サービスの停止](#)

4.4 Device Manager CLI または Tiered Storage Manager CLI でパスワードをコード化するときの強度の変更

このマニュアルでは、以下の内容は、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制により非公開となっています。以下の内容については、製品に付属するマニュアルをご覧ください。

関連製品と連携するために必要な設定

この章では、関連製品と連携するために必要な設定について説明します。

- 5.1 Element Manager を使用するために必要な設定
- 5.2 ストレージシステムの性能情報を収集するために必要な設定
- 5.3 Universal Replicator の性能を分析するために必要な設定
- 5.4 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするために必要な設定

5.1 Element Manager を使用するために必要な設定

Device Manager では Storage Navigator Modular 2 と連携することで、Element Manager を使って、次のストレージシステムの詳細情報を参照したり、構成を変更したりできます。

- HUS100, Hitachi AMS2000 または Hitachi SMS の場合
HUS100, Hitachi AMS2000 および Hitachi SMS の場合は、ストレージシステムを Device Manager に登録すると Element Manager を使用できるように自動的に設定されます。このため、環境設定は不要です。
- Hitachi AMS/WMS または SANRISE 9500V の場合
launchapptool を使用して、環境設定を実施する必要があります。

ここでは、Storage Navigator Modular 2 と連携する場合の前提条件と環境設定について説明します。

5.1.1 Storage Navigator Modular 2 と連携するための前提条件

Storage Navigator Modular 2 利用時の前提条件および注意事項を次に示します。

(1) Storage Navigator Modular 2 利用時の前提条件

- HUS100, Hitachi AMS2000 または Hitachi SMS を Device Manager の GUI から管理する場合、Device Manager サーバと Storage Navigator Modular 2 を同じサーバにインストールしてください。
- Storage Navigator Modular 2 の Web サーバは、マシンに複数の NIC が搭載されていても、1つの NIC を通してしかアクセスできません。複数の NIC を搭載したマシン環境で Storage Navigator Modular 2 と連携する場合、Storage Navigator Modular 2 の Web サーバへのアクセスに使用する NIC を設定する必要があります。この設定で指定する IP アドレスは、Device Manager サーバのインストール時に指定したものと同じにしてください。設定方法については、Storage Navigator Modular 2 のマニュアルを参照してください。
- Storage Navigator Modular 2 が単体で正常に動作することを確認してください。Storage Navigator Modular 2 で Java Plug-in の設定が必要です。環境設定および起動方法については、Storage Navigator Modular 2 のマニュアルを参照してください。
- Storage Navigator Modular 2 には、Device Manager がサポートしているストレージシステムだけを登録してください。
- HUS100, Hitachi AMS2000 および Hitachi SMS を管理する場合は、次の条件を満たすようにユーザーを設定してください。
 - Storage Navigator Modular 2 の Modify 権限が設定されている
 - 対象のストレージシステムに対応するリソースグループが割り当てられている
 - 割り当てたリソースグループに対する Device Manager のロールとして Modify が設定されている

Storage Navigator Modular 2 でユーザーアカウントを登録する方法については、Storage Navigator Modular 2 のマニュアルを参照してください。リソースグループを割り当てる方法については、マニュアル「*Hitachi Command Suite Software ユーザーズガイド*」を参照してください。

- 操作対象のストレージシステムで Password Protection または Account Authentication が有効なときは、「HDvM」から始まるユーザー ID を使用しないでください。

ストレージシステムで、Password Protection または Account Authentication が有効なとき、Storage Navigator Modular 2 をラUNCHすると、Storage Navigator Modular 2 がストレージシステムにアクセスするための一時的なユーザーアカウントが作成されます。このユーザーア

アカウントは、「HDvM」から始まるユーザー ID でストレージシステムに自動的に登録され、Storage Navigator Modular 2 を終了すると自動的に削除されます。このため、ユーザー ID が「HDvM」から始まるユーザーアカウントを手動で登録したり、登録内容を変更したりすると、ラウンチが失敗するおそれがあります。

- HUS100, Hitachi AMS2000 または Hitachi SMS でアドバンスドセキュリティモードを有効または無効に切り替えると、ストレージシステムに登録されたユーザーアカウントは削除されます。Storage Navigator Modular 2 を使用して、ユーザーアカウントを登録し直してください。
- HUS100, Hitachi AMS2000 および Hitachi SMS を管理する場合、Storage Navigator Modular 2 での通信プロトコルの設定を、Device Manager の GUI または CLI での設定と一致させてください。

Device Manager サーバに登録済みのストレージシステムの通信プロトコルを変更する場合には、必ず Device Manager から実施してください。Storage Navigator Modular 2 から変更すると、Device Manager サーバとストレージシステム間で通信できなくなるおそれがあります。

(2) Storage Navigator Modular 2 と連携する場合の注意事項

- Element Manager を使用してファームウェアの更新またはマイクロプログラムの交換をしないでください。また、ファームウェアの更新中またはマイクロプログラムの交換中は Element Manager を使用できません (DMES059510 エラーになります)。

5.1.2 Element Manager を使用するための設定

Element Manager で Hitachi AMS/WMS または SANRISE 9500V を操作するためには、launchapptool を使用して環境設定を実施する必要があります。

1. Storage Navigator Modular 2 をインストールします。
2. コマンドプロンプトまたはターミナルウィンドウから、次のコマンドを実行します。
 - Windows の場合：
< Device Manager サーバのインストールフォルダ > %HiCommandServer%\tools
%launchapptool.bat
 - Solaris または Linux の場合：
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/tools/
launchapptool.sh
3. メインメニューが表示されたら、「1」を選択します。

```
=====
launchapptool
=====
1) Storage Navigator Modular 2 launch setup
2) Delete launch settings
3) Exit

>1
Launch Settings for Storage Navigator Modular 2 will now Start.
```

すでに Element Manager を使用できるように環境設定が済んでいる場合は、現在の設定を変更するかどうかを確認するメッセージが表示されます。

設定を変更する場合は、「y」を選択します。設定を変更しない場合は、「n」を選択します。

4. Web サーバの URL に使用するプロトコルを指定します。
http プロトコルを使用する場合は、「1」を選択します。https プロトコルを使用する場合は、「2」を選択します。

```
Specify the URL protocol.
1) http
2) https
  Caution: To use https, settings to enable SSL communication
            with the web server must be specified in advance.

Enter Value [default=1]
>1
```



注意 「2」を選択する場合は、Web サーバ（Hitachi Command Suite 共通コンポーネント）と GUI の間を SSL で通信できるように設定しておく必要があります。

5. Web サーバの URL に指定する IP アドレスまたはホスト名を入力します。
管理クライアント（GUI）からアクセスできる IPv4 アドレスまたはホスト名を指定します。

```
Specify the IP address or hostname of the web server.
Enter Value [default=10.208.64.140]
>10.208.64.140
```



重要

- ・ ローカルホストを使用する場合は、ホスト名ではなくローカルホストの IP アドレスを指定してください。
- ・ 管理サーバに NIC が複数搭載されている場合、IP アドレスには管理クライアント（GUI）が接続されているネットワーク側の IP アドレスを指定してください。ホスト名は指定しないでください。

6. Web サーバの URL に指定するポート番号を入力します。

```
Specify the port number of the web server.
Enter Value [default=23015]
>23015
```

7. Storage Navigator Modular 2 で、RMI の通信に使用するポート番号を変更した場合、変更後のポート番号を入力します。

```
Specify the port number for RMI communications.
Enter Value [default=1099]
>1099
```



注意 通信用ポート番号を変更していない場合は、入力しないでください。

8. Hitachi Command Suite 製品のサービスを再起動します。
ラUNCH環境の設定が有効になります。

```
Launch setup has successfully completed.

You must restart the Device Manager Server and Common Component Services
for this these changes to take effect.

Exit - Default is n?(y, n):
```

9. Device Manager の GUI または CLI で、Element Manager で操作するストレージシステムをリフレッシュします。

関連項目

- ・ [9.2 サービスの起動](#)
- ・ [9.3 サービスの停止](#)
- ・ Storage Navigator Modular 2 のインストール方法 : Storage Navigator Modular 2 のマニュアル

5.1.3 Element Manager を使用するための設定の解除

Element Manager で Hitachi AMS/WMS または SANRISE 9500V を操作する必要がなくなった場合には、必要に応じて設定を解除してください。

1. コマンドプロンプトまたはターミナルウィンドウから、次のコマンドを実行します。

- Windows の場合：

```
< Device Manager サーバのインストールフォルダ > %HiCommandServer%\tools  
%launchapptool.bat
```

- Solaris または Linux の場合：

```
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/tools/  
launchapptool.sh
```

2. メインメニューが表示されたら、2 を選択します。

ラUNCH環境のリストが表示されます。

3. 1 を選択します。

設定を削除するかどうかを確認するメッセージが表示されます。

```
=====
launchapptool
=====

1) Storage Navigator Modular 2 launch setup
2) Delete launch settings
3) Exit

>2

Specify the launch setting to be deleted.
1) Storage Navigator Modular 2
2) Cancel
Enter Value
>1

Launch settings will now be deleted.

Would you like to delete launch settings?(y, n):y
```

4. 設定を解除する場合は、y を指定します。設定の解除を中止する場合は、「n」を指定します。

5. Hitachi Command Suite 製品のサービスを再起動します。

設定が解除されます。

```
Launch settings have successfully been deleted.

You must restart the Device Manager Server and Common Component Services
for this these changes to take effect.

Exit - Default is n?(y, n):
```

関連項目

- [9.2 サービスの起動](#)
- [9.3 サービスの停止](#)

5.2 ストレージシステムの性能情報を収集するために必要な設定

Device Manager および Tiered Storage Manager では、Tuning Manager と連携することで、パリティグループ利用率やボリュームの IOPS などの性能情報を収集し、[モビリティ] タブや [分析] タブで確認できます。

Tiered Storage Manager と Tuning Manager が連携すると、[モビリティ] タブでハードウェア階層の利用状況やボリュームの I/O 性能を確認し、必要に応じて階層ポリシーを設定したり、ボリュームをマイグレーションしたりして、ストレージリソースの利用効率を最適化できます。

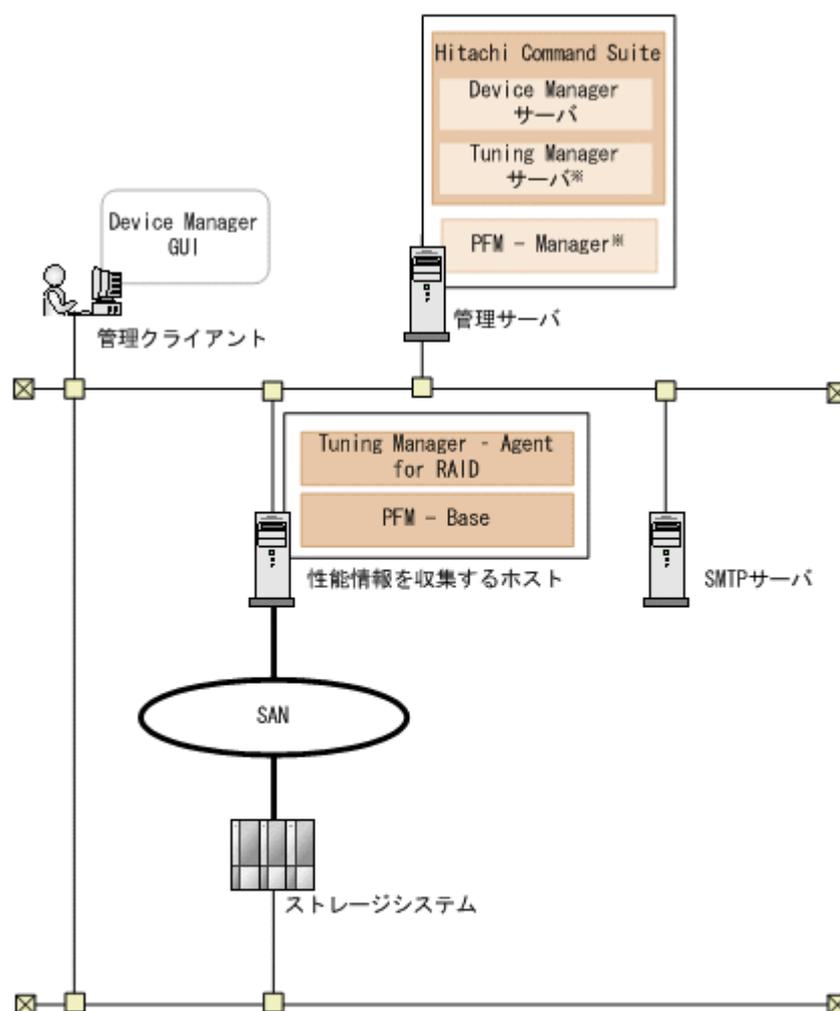
また、Device Manager と Tuning Manager が連携すると、[分析] タブで次のことができます。

- 業務サーバ上のアプリケーションで性能問題が発生した場合に、要因がストレージシステムにあるのかどうかを分析できます。
- ストレージシステム全体の性能を定期的に分析し、問題の兆候を検出できます（ヘルスチェック）。
ヘルスチェック結果は E メールでユーザーに通知できます。

5.2.1 ストレージシステムの性能情報を収集するためのシステム構成

ストレージシステムの性能情報を収集するには、Tuning Manager サーバや Tuning Manager - Agent for RAID を設置する必要があります。

図 5-1 ストレージシステムの性能情報を収集するためのシステム構成例



(凡例)

— : ファイバーチャネル

注※ Device Managerとは異なるマシンにインストールされている場合もあります。

ストレージシステムや各マシンに必要な設定を次に示します。

ストレージシステム

Tuning Manager - Agent for RAID がストレージシステムの性能情報を収集できるように、ストレージシステムでの設定が必要です。

性能情報を収集するホスト

次の設定が必要です。

- Tuning Manager - Agent for RAID および前提プログラムのインストール
- 監視対象ストレージシステムごとのインスタンス環境の設定
- Tuning Manager サーバのインストールマシン (接続先 PFM - Manager) の設定 (Tuning Manager サーバと Tuning Manager - Agent for RAID が異なるマシンにインストールされている場合)

設定が完了したら、`jpcspm start` コマンドを実行して、Tuning Manager - Agent for RAID のインスタンスを起動します。Tuning Manager - Agent for RAID は、インスタンスの起動後

から性能情報の収集を開始します。なお、初回のデータ取得には最大 1 時間掛かることがあります。

管理サーバ

Device Manager サーバ

Tuning Manager との連携に関するプロパティの設定が必要です。設定が完了したら、Device Manager GUI/CLI で監視対象のストレージシステムをリフレッシュします。必要に応じて、Tuning Manager サーバとのリモート接続や、ヘルスチェック結果を E メール通知するための設定などを実施します。

Tuning Manager サーバ

Tuning Manager サーバおよび前提プログラムのインストールが必要です。Device Manager サーバと Tuning Manager サーバが異なるマシンにインストールされている場合は、Tuning Manager サーバが Device Manager サーバに接続できるように設定します。

管理クライアント

[分析] タブから Tuning Manager の Performance Reporter をラUNCHする場合、レポート定義ファイルをインポートします。

SMTP サーバ

ヘルスチェック結果を E メール通知する場合は、Device Manager サーバが SMTP サーバに接続できるように、SMTP 認証の設定が必要です。

関連項目

- [A.1.1 Device Manager サーバのプロパティの変更](#)
- Tuning Manager サーバの設定方法：マニュアル「*Hitachi Command Suite Tuning Manager Software インストールガイド*」
- Tuning Manager - Agent for RAID の設定方法：マニュアル「*Hitachi Command Suite Tuning Manager - Agent for RAID*」

5.2.2 Device Manager サーバ、Tuning Manager サーバおよび Tuning Manager - Agent for RAID 間で通信するための設定

Device Manager サーバ、Tuning Manager サーバ、および Tuning Manager - Agent for RAID 間で正しく通信できるように、各マシンの設定内容を確認します。

- 各マシンの GMT が一致していること。
GMT が 5 分以上異なるときは、エラーになることがあります。
- 各マシンでほかのプログラムを共存させる場合、ポート番号が重複していないこと。また、マシン間にファイアウォールが設置されている場合は、使用するポート番号を例外登録していること。
- Tuning Manager サーバおよび Tuning Manager - Agent for RAID のインストール先マシンが、ホスト名から IP アドレスに名前解決できること。
 - ホスト名が 33 バイト以上の場合、エイリアス名を設定し、エイリアス名から IP アドレスへの名前解決ができるようにしてください。
 - IPv6 環境で運用する場合、IPv4 と IPv6 の両方を使用できるように設定してください。また、ホスト名から IPv6 アドレスを解決できるように設定してください。

- Tuning Manager サーバまたは Tuning Manager - Agent for RAID のインストール先マシンが複数 NIC を搭載している場合、jpcchosts ファイルに IP アドレスを設定し、jpcchosts ファイルをシステム内で統一するようにしてください。
- Tuning Manager サーバと Device Manager サーバを同一マシンにインストールし、通信に TLS/SSL を使用する場合、Tuning Manager サーバと Device Manager サーバで設定が完了していること。



参考 Device Manager サーバのインストール先マシンと Tuning Manager - Agent for RAID のインストール先マシンでタイムゾーンが異なり、かつ Device Manager サーバのインストール先マシンの時刻が Tuning Manager - Agent for RAID のインストール先マシンの時刻よりも早い環境で運用する場合、[モビリティ] タブを参照した時刻によっては性能情報が正しく表示されないことがあります。時差を考慮し、次のどちらかの方法で運用してください。

- Device Manager サーバの dispatcher.properties ファイルにある `server.dispatcher.daemon.autoSynchro.performance.startTime` プロパティの値を変更する。両マシンのローカルタイムが同じ日付になる時刻以降を設定してください。
- 両マシンのローカルタイムが同じ日付になる時刻以降に性能情報をリフレッシュする。
[ストレージシステム更新] 画面で [性能情報を更新する] チェックボックスをチェックしてストレージシステムをリフレッシュするか、`RefreshPerformanceData` コマンドを実行してください。

関連項目

- [2.1 ポートの設定](#)
- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.5.16 server.dispatcher.daemon.autoSynchro.performance.startTime](#)
- Tuning Manager サーバの設定方法および使用するポート番号について：マニュアル「*Hitachi Command Suite Tuning Manager Software インストールガイド*」
- Tuning Manager - Agent for RAID が使用するポート番号および Tuning Manager - Agent for RAID の設定方法について：マニュアル「*Hitachi Command Suite Tuning Manager - Agent for RAID*」

5.2.3 ストレージシステムの性能情報を収集するための設定

エンタープライズクラスストレージ (Virtual Storage Platform, Universal Storage Platform V/VM および Hitachi USP) および HUS VM と、ミッドレンジストレージ (HUS100, Hitachi AMS2000, Hitachi SMS, Hitachi AMS/WMS および SANRISE9500V) の性能情報を収集するための設定について説明します。

(1) エンタープライズクラスストレージおよび HUS VM の性能情報を収集するための設定

Tuning Manager - Agent for RAID がエンタープライズクラスストレージ (Virtual Storage Platform, Universal Storage Platform V/VM および Hitachi USP) および HUS VM の性能情報を収集できるように、エンタープライズクラスストレージおよび HUS VM での設定が完了していることを確認します。

- 監視対象ストレージシステムのマイクロコードバージョンが、Tuning Manager - Agent for RAID のサポート範囲内であること。
- Tuning Manager - Agent for RAID のインストール先マシンから、監視対象ストレージシステムに作成した Tuning Manager - Agent for RAID 専用のコマンドデバイスにアクセスできること。
- 監視対象ストレージシステムが Hitachi USP の場合、PI_RGS レコードについて、Performance Monitor で性能情報を収集するための設定が完了していること。

- ヘルスチェックを実行する場合、下記のレコードについて、レコードの保存期間の設定が完了していること。設定するレコードの保存期間を「表 5-1 ヘルスチェックを実行するためのレコードの保存期間（エンタープライズクラスストレージおよび HUS VM の場合）」に示します。
 - PI_CLPS レコード
 - PI_LDA レコード
 - PI_PLS レコード（Hitachi USP の場合は設定不要）
 - PI_PRCs レコード
 - PI_PTS レコード
 - PI_RGS レコード

表 5-1 ヘルスチェックを実行するためのレコードの保存期間(エンタープライズクラスストレージおよび HUS VM の場合)

Store データベースバージョン	プロパティ名	設定値
1.0	Product Interval - Hour Drawer	Month
	Product Interval - Day Drawer	Year
2.0	Period - Hour Drawer (Day)	9 以上
	Period - Day Drawer (Week)	5 以上

関連項目

- Tuning Manager - Agent for RAID の監視対象ストレージシステムの前提マイクロコードバージョン、コマンドデバイスの設定方法、および性能情報を収集するためのレコードの設定方法について：マニュアル「*Hitachi Command Suite Tuning Manager - Agent for RAID*」
- レコードの保存期間の設定方法：マニュアル「*Hitachi Command Suite Tuning Manager Software 運用管理ガイド*」

(2) ミッドレンジストレージの性能情報を収集するための設定

Tuning Manager - Agent for RAID がミッドレンジストレージ（HUS100, Hitachi AMS2000, Hitachi SMS, Hitachi AMS/WMS および SANRISE9500V）の性能情報を収集できるように、ミッドレンジストレージでの設定が完了していることを確認します。

- 監視対象ストレージシステムのマイクロコードバージョンが、Tuning Manager - Agent for RAID のサポート範囲内であること。
- 監視対象ストレージシステムが HUS100, Hitachi AMS2000, Hitachi SMS または Hitachi AMS/WMS で、Account Authentication を有効にしている場合、Tuning Manager - Agent for RAID 専用のアカウントを作成していること。
- 下記のレコードについて、Storage Navigator Modular または Storage Navigator Modular 2 で性能情報を収集するための設定が完了していること。
 - PD_CLPC レコード（SANRISE9500V の場合は設定不要）
 - PI_CLCS レコード
 - PI_CLPS レコード（SANRISE9500V の場合は設定不要）
 - PI_LDA レコード
 - PI_LDS レコード
 - PI_PDOS レコード
 - PI_PRCs レコード
 - PI_PTS レコード

- PI_RGS レコード
- 監視対象ストレージシステムが SANRISE9500V の場合、重複しないシリアル番号（装置 ID）が設定されていること。
- ヘルスチェックを実行する場合、下記のレコードについて、レコードの保存期間の設定が完了していること。設定するレコードの保存期間を「表 5-2 ヘルスチェックを実行するためのレコードの保存期間（ミッドレンジストレージの場合）」に示します。
 - PI_CLCS レコード
 - PI_LDA レコード
 - PI_PRCs レコード
 - PI_PTS レコード
 - PI_RGS レコード

表 5-2 ヘルスチェックを実行するためのレコードの保存期間（ミッドレンジストレージの場合）

Store データベースバージョン	プロパティ名	設定値
1.0	Product Interval - Hour Drawer	Month
	Product Interval - Day Drawer	Year
2.0	Period - Hour Drawer (Day)	9 以上
	Period - Day Drawer (Week)	5 以上

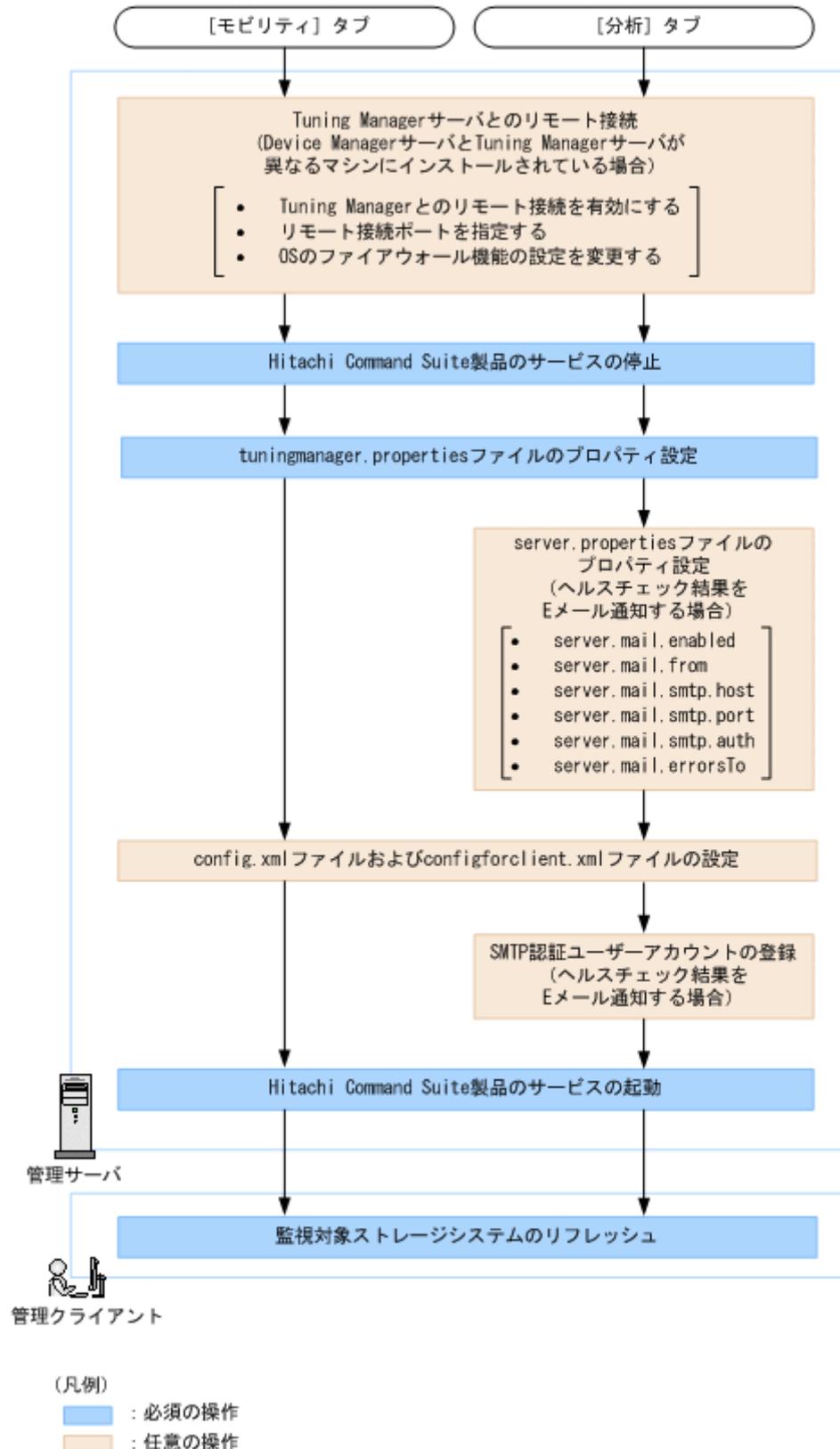
関連項目

- Tuning Manager - Agent for RAID の監視対象ストレージシステムの前提マイクロコードバージョン、Tuning Manager - Agent for RAID 専用のアカウントの作成方法、性能情報を収集するためのレコードの設定方法、およびシリアル番号（装置 ID）の重複確認について：マニュアル「*Hitachi Command Suite Tuning Manager - Agent for RAID*」
- レコードの保存期間の設定方法：マニュアル「*Hitachi Command Suite Tuning Manager Software 運用管理ガイド*」

5.2.4 Device Manager サーバを設定するための操作フロー（ストレージシステムの性能情報の収集）

ストレージシステムの性能情報を収集するには、Device Manager サーバの Tuning Manager との連携に関するプロパティを設定して、Device Manager GUI/CLI で監視対象のストレージシステムをリフレッシュする必要があります。必要に応じて、Tuning Manager サーバとのリモート接続や、ヘルスチェック結果を E メール通知するための設定などを実施します。

図 5-2 Device Manager サーバを設定するための操作フロー（ストレージシステムの性能情報の収集）



注意

- Tuning Manager サーバとのリモート接続には、次の制限があります。
 - IPv6 での通信をサポートしていません。
 - SSL または TLS で暗号化した通信をサポートしていません。

- 次のコマンドを実行した場合は、Tuning Manager サーバとのリモート接続の設定が初期化されるため、再度設定してください。

hcmsdbclustersetup (クラスタの設定)

hcmsdbremake (データベースの再作成)

- 次のコマンドでデータベースを復元または移行した場合は、復元または移行先のマシンでリモート接続の設定が再度必要です。

hcmsdbtrans

hcmsdbbackups および hcmsdb -restore の組み合わせ

hcmsdbtrans および hcmsdbrepair の組み合わせ



重要 監視対象のストレージシステムをリフレッシュしたあと、正常に完了していることを確認してください。

Device Manager GUI の場合

[データ収集タスク] タブの「ストレージシステム更新」タスクの [状態] が完了になっていることを確認してください。

Device Manager CLI の場合

AddStorageArray コマンドの実行が正常に終了していることを確認してください。



参考 Device Manager サーバと Tuning Manager サーバが同じマシンにインストールされている場合、tuningmanager.properties ファイルを編集しなくても監視対象のストレージシステムをリフレッシュすれば、[分析] タブを利用できます。この場合、システムは下記の設定で動作します。

- htnm.servers=1 (接続する Tuning Manager サーバの数)
- htnm.server.0.host=127.0.0.1 (接続する Tuning Manager サーバの IP アドレス)
- htnm.server.0.protocol=http (Tuning Manager サーバと Hitachi Command Suite 共通コンポーネント間の通信方式)
- htnm.server.0.port=23015 (接続する Tuning Manager サーバの HBase Storage Mgmt Web Service のポート番号)

[モビリティ] タブを使用する場合や運用環境が上記と異なる場合は、上記の4つのプロパティに適切な値を指定してください。

関連項目

- (4) SMTP 認証ユーザーアカウントの Device Manager への登録
- 9.2 サービスの起動
- 9.3 サービスの停止
- A.2.17 server.mail.enabled
- A.2.18 server.mail.from
- A.2.19 server.mail.smtp.host
- A.2.20 server.mail.smtp.port
- A.2.21 server.mail.smtp.auth
- A.2.22 server.mail.errorsTo
- A.14 Tuning Manager との連携に関するプロパティ (tuningmanager.properties ファイル)

(1) Tuning Manager サーバとのリモート接続 (非クラスタ環境)

非クラスタ環境で Tuning Manager サーバとのリモート接続の有効/無効を切り替えるには、htmsetup コマンドを実行します。

事前に完了しておく操作

- Device Manager サーバの hosts ファイルの編集

Tuning Manager サーバのホスト名と IP アドレスを登録します。

hosts ファイルの格納先

Windows の場合： < Windows のシステムフォルダ > ¥system32¥drivers¥etc¥hosts

Solaris または Linux の場合： /etc/hosts

- リモート接続用のポートの設定（Linux でファイアウォール機能を有効にしている場合）
- Administrator 権限（Windows の場合）または root（Solaris または Linux の場合）でのログイン

Tuning Manager サーバとリモート接続するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. htmsetup コマンドを実行します。
3. メニューが表示されたら、1 (Configure the settings for remote connection) を指定します。
4. ポート番号（有効値：5001～65535，デフォルト値：24220）を指定します。
設定が完了すると、HiRDB が起動されます。Windows の場合、Windows ファイアウォールの例外登録も設定されます。
5. Hitachi Command Suite 製品のサービスを起動します。

関連項目

- (1) ファイアウォールへの例外登録が必要なポート
- 9.3 サービスの停止

(2) Tuning Manager サーバとのリモート接続（Microsoft Cluster Service または Windows Server Failover Clustering）

クラスタ管理アプリケーションが Microsoft Cluster Service または Windows Server Failover Clustering の場合は、Hitachi Command Suite 製品のサービスやリソースグループをクラスタの管理対象から外したあと、htmsetup コマンドを実行します。

事前に完了しておく操作

- Device Manager サーバの hosts ファイル（< Windows のシステムフォルダ > ¥system32¥drivers¥etc¥hosts）の編集
Tuning Manager サーバの物理ホスト名と物理 IP アドレスを登録します。
- Administrator 権限でのログイン

Tuning Manager サーバとリモート接続するには：

1. クラスタ管理アプリケーションで次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
2. Hitachi Command Suite 製品のサービスを停止します。
3. クラスタ管理アプリケーションで次のサービスをオフラインにします。

HiRDB/ClusterService_HD0

4. クラスタ管理アプリケーションで、次のリソースグループのフェールオーバーを抑止します。
 - HiCommand Tiered Storage Manager
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service
 - HiCommandServer
 - HiRDB/ClusterService_HD0
 - 上記以外に手順 1 でオフラインにしたサービス

Microsoft Cluster Service の場合

リソース名を右クリックし、[プロパティ] – [詳細設定] タブで、[再開しない] を選択します。

Windows Server Failover Clustering の場合

リソース名を右クリックし、[プロパティ] – [ポリシー] タブで、[リソースが失敗状態になった場合は、再起動しない] を選択します。

5. htmsetup コマンドを実行します。
6. メニューが表示されたら、1 (Configure the settings for remote connection) を指定します。
7. ポート番号 (有効値 : 5001~65535, デフォルト値 : 24220) を指定します。
設定が完了すると、HiRDB が起動されます。Windows ファイアウォールの例外登録も設定されます。
8. Hitachi Command Suite 製品のサービスを停止します。
9. Hitachi Command Suite 製品のサービスを登録しているグループを待機系に移動します。
10. 待機系ノードで htmsetup コマンドを実行します。
実行系ノードと同じ設定にしてください。
11. Hitachi Command Suite 製品のサービスを停止します。
12. [サービス] ウィンドウで次のプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HCS Device Manager Web Service
- HiCommandServer
- HiCommand Tiered Storage Manager

13. クラスタ管理アプリケーションで、次のリソースグループのフェールオーバーを有効にします。
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service
 - HiCommandServer
 - HiCommand Tiered Storage Manager
 - HiRDB/ClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service の場合

リソース名を右クリックし、[プロパティ] – [詳細設定] タブで、[再開する] を選択します。

Windows Server Failover Clustering の場合

リソース名を右クリックし、[プロパティ] – [ポリシー] タブで [リソースが失敗状態になった場合は、現在のノードで再起動を試みる] と [再起動に失敗した場合は、この役割のすべてのリソースをフェールオーバーする] (または [再起動に失敗した場合は、このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする]) を選択します。

14. クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスを登録しているグループをオンラインにします。

関連項目

- 9.3 サービスの停止
- Device Manager および Tiered Storage Manager 以外にクラスタの管理対象から外す必要のあるサービスおよびリソースグループについて：各 Hitachi Command Suite 製品のマニュアル

(3) Tuning Manager サーバとのリモート接続 (Veritas Cluster Server)

クラスタ管理アプリケーションが Veritas Cluster Server の場合は、Hitachi Command Suite 製品のサービスやリソースグループをクラスタの管理対象から外したあと、htmsetup コマンドを実行します。

事前に完了しておく操作

- Device Manager サーバの hosts ファイル (/etc/hosts) の編集
Tuning Manager サーバの物理ホスト名と物理 IP アドレスを登録します。
- root でのログイン

Tuning Manager サーバとリモート接続するには：

1. 実行系ノードの Java Console で Cluster Manager を起動します。
2. 次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
3. 手順 2 の各サービスを右クリックして、コンテキストメニューにある [Enabled] のチェックを外します。
4. Hitachi Command Suite 製品のサービスを停止します。
5. HiRDB のサービスをオフラインにします。
6. HiRDB のサービスを右クリックして、コンテキストメニューにある [Enabled] のチェックを外します。
7. Cluster Explorer ウィンドウの [Service Groups] タブを選択します。

8. Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Freeze] - [Temporary] を選択します。
9. htmsetup コマンドを実行します。
10. メニューが表示されたら、1 (Configure the settings for remote connection) を指定します。
11. ポート番号 (有効値 : 5001~65535, デフォルト値 : 24220) を指定します。
設定が完了すると、HiRDB が起動されます。
12. Hitachi Command Suite 製品のサービスを停止します。
13. Cluster Explorer ウィンドウで [Service Groups] タブを選択します。
14. Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから次の操作を順に実行します。
 - [Unfreeze] を選択します。
 - [Switch To] - [<ホスト名>] を選択します。
 - [Freeze] - [Temporary] を選択します。
15. 待機系ノードで htmsetup コマンドを実行します。
実行系ノードと同じ設定にしてください。
16. Hitachi Command Suite 製品のサービスを停止します。
17. Java Console で Cluster Manager を起動します。
18. Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Unfreeze] を選択します。
19. Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Enable Resources] を選択します。
20. Veritas Cluster Server の設定ファイルに変更内容を保存します。[File] メニューから [Save Configuration] を選択します。
21. Veritas Cluster Server の設定ファイルを閉じます。[File] メニューから [Close Configuration] を選択します。
22. 実行系ノードで Hitachi Command Suite 製品のサービスを登録しているグループをオンラインにします。

関連項目

- 9.3 サービスの停止
- Device Manager および Tiered Storage Manager 以外にクラスタの管理対象から外す必要のあるサービスおよびリソースグループについて : 各 Hitachi Command Suite 製品のマニュアル

(4) Tuning Manager サーバとのリモート接続 (Sun Cluster)

クラスタ管理アプリケーションが Sun Cluster の場合は、Hitachi Command Suite 製品のサービスやリソースグループをクラスタの管理対象から外したあと、htmsetup コマンドを実行します。

事前に完了しておく操作

- Device Manager サーバの hosts ファイル (/etc/hosts) の編集
Tuning Manager サーバの物理ホスト名と物理 IP アドレスを登録します。
- root でのログイン

Tuning Manager サーバとリモート接続するには：

1. 実行系ノードで次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント (HiRDB を除く)、Device Manager および Tiered Storage Manager のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j BaseWebService
# /usr/cluster/bin/scswitch -n -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j BaseCommonService
# /usr/cluster/bin/scswitch -n -M -j TieredStorageManager
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースの監視を無効にしてください。

2. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント (HiRDB を除く)、Device Manager および Tiered Storage Manager のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -j BaseWebService
# /usr/cluster/bin/scswitch -n -j BaseCommonService
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースを無効にしてください。

3. Hitachi Command Suite 製品のサービスを停止します。
4. 次のコマンドを実行して、HiRDB のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```
5. 次のコマンドを実行して、HiRDB のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```
6. htmsetup コマンドを実行します。
7. メニューが表示されたら、1 (Configure the settings for remote connection) を指定します。
8. ポート番号 (有効値 : 5001~65535, デフォルト値 : 24220) を指定します。
設定が完了すると、HiRDB が起動されます。
9. Hitachi Command Suite 製品のサービスを停止します。

10. 次のコマンドを実行して Hitachi Command Suite 製品のサービスを登録しているグループを待機系ノードに移動します。

```
# /usr/cluster/bin/scswitch -z -g <グループ名> -h <ホスト名>
```

11. 待機系ノードで htmsetup コマンドを実行します。実行系ノードと同じ設定にしてください。
12. Hitachi Command Suite 製品のサービスを停止します。

13. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager のサービスおよび Tiered Storage Manager のサービスを有効にします。

```
# /usr/cluster/bin/scswitch -e -j HiRDB
# /usr/cluster/bin/scswitch -e -j BaseCommonService
# /usr/cluster/bin/scswitch -e -j BaseWebService
# /usr/cluster/bin/scswitch -e -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -j HiCommandServer
# /usr/cluster/bin/scswitch -e -j TieredStorageManager
```

上記以外の Hitachi Command Suite 製品のリソースを無効にしていた場合は、同様にリソースを有効にしてください。

14. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager のサービスおよび Tiered Storage Manager のサービスの監視を有効にします。

```
# /usr/cluster/bin/scswitch -e -M -j HiRDB
# /usr/cluster/bin/scswitch -e -M -j BaseCommonService
# /usr/cluster/bin/scswitch -e -M -j BaseWebService
# /usr/cluster/bin/scswitch -e -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer
# /usr/cluster/bin/scswitch -e -M -j TieredStorageManager
```

上記以外の Hitachi Command Suite 製品のリソースの監視を無効にしていた場合は、同様にリソースの監視を有効にしてください。

関連項目

- 9.3 サービスの停止
- Device Manager および Tiered Storage Manager 以外にクラスタの管理対象から外す必要のあるサービスおよびリソースグループについて：各 Hitachi Command Suite 製品のマニュアル

(5) Tuning Manager サーバとのリモート接続およびポート番号の設定 (htmsetup コマンド)

Tuning Manager とのリモート接続の設定を変更したり、リモート接続に使用するポート番号を設定したりするには、htmsetup コマンドを使用します。

次の Tuning Manager とのリモート接続に関する設定を対話形式で設定します。

- リモート接続の有効、無効を切り替える（デフォルト値：無効）
- リモート接続が有効の場合に使用するポート番号を指定する（有効値：5001～65535、デフォルト値：24220）

Windows ファイアウォールがインストールされている OS の場合、リモート接続の有効、無効に合わせて、Windows ファイアウォールの例外への登録、削除も実行します。設定完了後は HiRDB が起動した状態になります。



重要 htmsetup コマンドは複数実行できません。

事前に完了しておく操作

- Administrator 権限（Windows の場合）または root（Solaris または Linux の場合）でのログイン
- ホスト設定ファイルへのホスト名と IP アドレスの登録（リモート接続を有効にする場合）
自マシンのホスト名と IP アドレスを登録してください。
- Hitachi Command Suite 製品のサービスの停止（参考：9.3 サービスの停止）
- ほかのコマンドが実行されていないことの確認

Hitachi Command Suite 共通コンポーネントの設定を変更するようなコマンドが実行されていないか、確認してください。

- クラスタの監視対象からの削除（クラスタ環境の場合）

実行系、待機系の Hitachi Command Suite 製品のサービス、およびリソースグループをクラスタの監視対象から外してください。

コマンドの形式

htmsetup

コマンドの格納先

Windows の場合

```
< Device Manager サーバのインストールフォルダ > %HiCommandServer%\tools  
%htmsetup.bat
```

Solaris または Linux の場合

```
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/tools/  
htmsetup.sh
```

(6) config.xml ファイルおよび configforclient.xml ファイルの設定

次の場合は、config.xml ファイルおよび configforclient.xml ファイルの設定内容を変更します。

- Tuning Manager の管理サーバと Device Manager の管理サーバの間にファイアウォールが設置されている場合
デフォルトでは任意の空きポート番号が使用される設定になっているため、特定のポート番号が使用されるように、ownPort パラメーターの設定を変更してください。それぞれのファイルの ownPort パラメーターには、それぞれ異なるポート番号の設定が必要です。指定できる値は 1024～65535 です。
なお、ほかのプロセスで使用されるポート番号との競合を避けるため、OS の自動割り当てポートは指定しないでください。ここで指定したポート番号は、ファイアウォールで例外登録が必要です。
- Device Manager の管理サーバに NIC が複数搭載されている場合
ownHost パラメーターに、Device Manager の管理サーバの IPv4 アドレスまたはホスト名のうち、Tuning Manager の管理サーバに接続されているネットワーク側の情報を指定してください。config.xml ファイルと configforclient.xml ファイルで、ownHost パラメーターには同じ値を設定してください。
- 13 台以上のストレージシステムから性能情報を取得する場合、または 1 日に 2 回以上性能情報を取得する場合
config.xml ファイルの logFileSize パラメーターの値を 30 に変更してください。

config.xml ファイルおよび configforclient.xml ファイルの格納先を次に示します。

Windows の場合

```
< Device Manager サーバのインストールフォルダ > %HiCommandServer%\vsa%\conf
```

Solaris または Linux の場合

```
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/vsa/conf
```

関連項目

- (1) ファイアウォールへの例外登録が必要なポート

5.2.5 管理クライアントの設定（ストレージシステムの性能情報の収集）

[分析] タブから Tuning Manager の Performance Reporter をラUNCHする場合は、レポート定義ファイルをインポートします。

最新のレポート定義ファイルは AnalyticsReportDefV750 です。レポート定義ファイルは、統合インストールメディア内の次の場所に格納されています。

```
<DVD ドライブ>:¥HTNM_SERVER¥Definitions¥Report_Definitions
```

ほかのレポート定義がインポートされている場合は削除してください。そのあと、最新のレポート定義ファイルをインポートしてください。

なお、[モビリティ] タブや [分析] タブの操作に必要なユーザーの操作権限も設定してください。

関連項目

- ユーザーの操作権限、Device Manager および Tiered Storage Manager でのライセンスの登録方法、および Device Manager のリソースグループおよびロールの設定方法について：マニュアル「*Hitachi Command Suite Software ユーザーズガイド*」
- Tuning Manager でのライセンスの登録方法および権限の設定方法について：マニュアル「*Hitachi Command Suite Tuning Manager Software 運用管理ガイド*」
- Tuning Manager の Performance Reporter にレポート定義をインポートする方法について：マニュアル「*Hitachi Command Suite Tuning Manager Software ユーザーズガイド*」

5.3 Universal Replicator の性能を分析するために必要な設定

Device Manager, Replication Manager, および Tuning Manager が連携すると、[レプリケーション] タブで Universal Replicator の性能情報を確認でき、Universal Replicator で発生する C/T デルタの悪化要因を分析できます。

分析に必要な情報は、Replication Manager や Tuning Manager から収集します。Replication Manager からは、コピーグループやペア管理サーバなどの構成情報、および C/T デルタやジャーナルボリューム使用率などの性能情報を収集します。Tuning Manager からは、ストレージシステムの構成情報、ストレージシステムのプロセッサの利用率やストレージシステムのキャッシュメモリーのうち、書き込み待ちデータの割合などの性能情報を収集します。

5.3.1 Universal Replicator の性能を分析するためのシステム構成

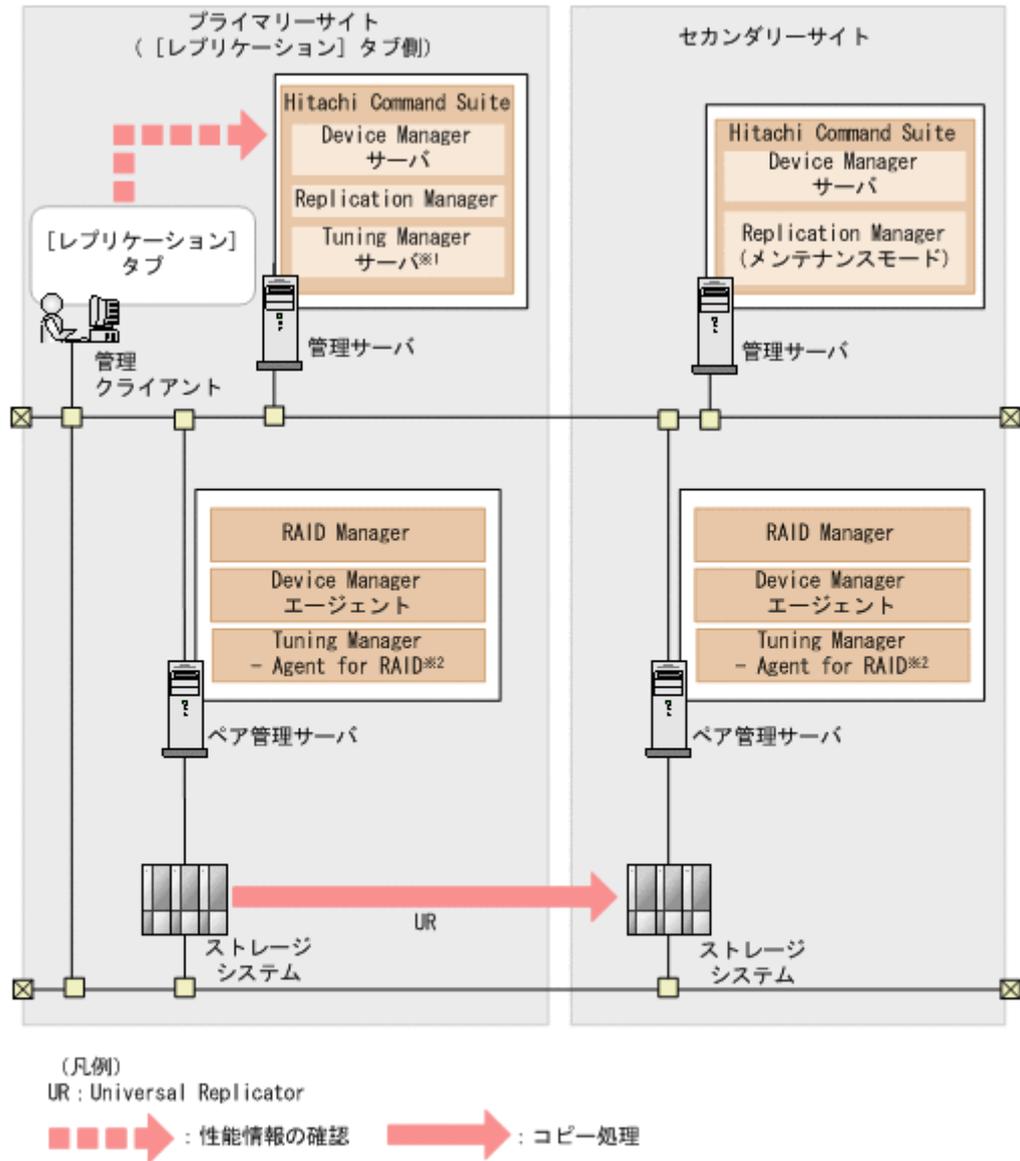
Universal Replicator の性能を分析するには、オープン系システムで Universal Replicator のコピーグループを管理するためのシステム構成であることや、Tuning Manager が設置された構成である必要があります。

管理クライアントは、プライマリーサイトとセカンダリーサイトの Device Manager サーバのどちらにも接続できますが、次の条件をすべて満たすように構成されているか確認してください。

- 管理クライアントから接続する Device Manager サーバと同じサイト ([レプリケーション] タブ側のサイト) 内に、Tuning Manager サーバを設置していること。
- [レプリケーション] タブ側とは別のサイトにある Replication Manager をメンテナンスモードにしていること。
- Tuning Manager - Agent for RAID を両方のサイトに設置していること。

管理クライアントからプライマリーサイトの Device Manager サーバに接続して、Universal Replicator の性能を分析する場合のシステム構成例を次に示します。

図 5-3 プライマリーサイトの Device Manager サーバに接続して性能分析する場合のシステム構成例



注※1 Device Managerとは異なるマシンにインストールされている場合もあります。
 注※2 Device Managerエージェントとは異なるマシンにインストールされている場合もあります。



重要 管理サーバの環境を新しいマシンに移行する場合は、収集した性能情報を引き継ぐための手順を実行する必要があります。手順どおりに実行しないと、性能情報のデータが消えるおそれがあります。詳細は、「ソフトウェア添付資料」を参照してください。



参考 次の操作を実行すると、[レプリケーション] タブで表示されていた C/T デルタやジャーナルボリューム使用率の履歴が表示されなくなります。

- ペア管理サーバを変更する
- ペア管理サーバの WWN を変更する
- ペア管理サーバの iSCSI イニシエーターの iSCSI ネームを変更する

関連項目

- Replication Manager のメンテナンスモードについて：マニュアル「Hitachi Command Suite Replication Manager Software システム構成ガイド」

5.3.2 Universal Replicator の性能を分析するための Device Manager の設定

Universal Replicator の性能を分析するには、Device Manager サーバの replication.properties ファイルにあるプロパティと rpmlib.properties ファイルにある rpmlib.rpm.port プロパティを設定します。

分析に必要な情報は、Replication Manager や Tuning Manager から定期的に収集できます。収集時間や収集間隔を変更する場合は、Device Manager サーバの replication.properties ファイルにあるプロパティを編集してください。

また、Replication Manager と RMI レジストリーとの通信に使用するポート番号を変更するために、Replication Manager サーバの base.properties ファイルにある base.rmi.port プロパティを変更した場合は、Device Manager サーバの rpmlib.properties ファイルにある rpmlib.rpm.port プロパティも変更してください。



重要 [レプリケーション] タブを使ったコピーグループ管理の運用中に、Device Manager サーバの ロケールを変更すると、[レプリケーション] タブで表示されるグラフが正しく表示されないおそれがあります。このため、ロケールを変更しないことをお勧めします。



参考 サマータイムが適用されている場合、分析に必要な情報の収集時間はサマータイムに従って調整されます。

関連項目

- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.15 Universal Replicator の性能分析に関するプロパティ \(replication.properties ファイル\)](#)
- [A.16.1 rpmlib.rpm.port](#)
- Replication Manager の base.properties ファイルにある base.rmi.port プロパティについて：マニュアル「*Hitachi Command Suite Replication Manager Software システム構成ガイド*」

5.3.3 Universal Replicator の性能を分析するための Replication Manager の設定

Universal Replicator の性能を分析するには、分析対象のコピーグループに対する Replication Manager での設定や、Replication Manager のプロパティの設定が完了している必要があります。

次の Replication Manager の設定が完了していることを確認してください。

- 分析対象のコピーグループに対して、C/T デルタのアラートを設定していること。
- Replication Manager の base.properties ファイルにある base.rmi.enabled プロパティの値に true を指定していること。

関連項目

- Replication Manager での設定：マニュアル「*Hitachi Command Suite Replication Manager Software ユーザーズガイド*」
- Replication Manager の base.properties ファイルにある base.rmi.enabled プロパティについて：マニュアル「*Hitachi Command Suite Replication Manager Software システム構成ガイド*」

5.3.4 Universal Replicator の性能を分析するための Tuning Manager の設定

Universal Replicator の性能を分析するには、Tuning Manager でストレージシステムの性能情報を収集するための設定が必要です。

さらに、PI_CLMS レコードについては、収集したパフォーマンスデータを Store データベースに記録するように次のどちらかの方法で設定してください。

- Performance Reporter の [サービス階層] 画面で Log プロパティを Yes にする。
- Performance Reporter の jpcasrec update コマンドを実行する。jpcasrec update コマンドのオプションに指定するパラメーターファイルには log パラメーターを指定し、値に Yes を指定する。

関連項目

- 5.2 ストレージシステムの性能情報を収集するために必要な設定
- Performance Reporter の [サービス階層] 画面や jpcasrec update コマンドでの設定方法：マニュアル「Hitachi Command Suite Tuning Manager Software 運用管理ガイド」

5.4 JP1/IM から Hitachi Command Suite 製品の GUI をラウンチするために必要な設定

Hitachi Command Suite 製品と JP1/IM が連携すると、JP1/IM の統合機能メニュー画面から、Hitachi Command Suite 製品の GUI をシングルサインオンでラウンチできます。

5.4.1 JP1/IM から Hitachi Command Suite 製品の GUI をラウンチするための前提環境

JP1/IM から Hitachi Command Suite 製品の GUI をシングルサインオンでラウンチできるようにするには、マシン環境を確認してください。

- 管理サーバの OS が Windows, Solaris (SPARC) または Red Hat Enterprise Linux であること。
- JP1/IM のバージョンが Version 7i 以降であること。
- JP1/IM - View をインストールするマシンには、Hitachi Command Suite 製品の GUI で前提としている OS および前提プログラムがインストールされていること。
- JP1/IM - View にログインするユーザーと同じアカウントが、事前に Hitachi Command Suite 製品に作成されていること。

パスワードには、6 文字以上の文字列を指定してください。ユーザー ID に使用できる文字は次のとおりです。

a~z A~Z 0~9 ! \$ - . @ _



参考 シングルサインオン機能を利用しない場合は、Hitachi Command Suite 製品のユーザー認証が必要です。JP1/IM の統合機能メニュー画面から Hitachi Command Suite 製品の GUI を起動するよう設定してください。

関連項目

- JP1/IM から Hitachi Command Suite 製品の GUI をラウンチする前提 OS や前提プログラムについて：ソフトウェア添付資料

- ・ シングルサインオン機能を利用しない場合に、JP1/IM の統合機能メニュー画面から Hitachi Command Suite 製品の GUI を起動する方法：JP1/IM のマニュアル

5.4.2 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするための設定

JP1/IM から Hitachi Command Suite 製品の GUI をシングルサインオンでラUNCHできるようにするには、JP1/IM - View の構成定義ファイルを作成します。

事前に完了しておく操作

- ・ 管理クライアントへの JP1/IM - View のインストール
詳細は、JP1/IM のマニュアルを参照してください。
- ・ 管理サーバへの JP1/Base と JP1/IM - Manager のインストールおよびセットアップ
詳細は、JP1/Base および JP1/IM のマニュアルを参照してください。

JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするには：

1. JP1/IM - View 用の構成定義ファイルのサンプルファイルをコピーします。

コピー元

Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%sample%
¥JP1_IM_conf
```

Solaris または Red Hat Enterprise Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/
sample/JP1_IM_conf
```

- ・ Device Manager 用サンプルファイル名：device_manager_ja.conf
- ・ Tiered Storage Manager 用サンプルファイル名：tieredstorage_manager_ja.conf
- ・ Replication Manager 用サンプルファイル名：replication_manager_ja.conf

コピー先

Windows の場合：

```
<JP1/IM - View のインストールフォルダ>%conf%¥function¥ja
```

Solaris または Red Hat Enterprise Linux の場合：

```
<JP1/IM - View のインストールディレクトリ>/conf/function/ja
```



注意

- ・ 管理サーバの OS が Solaris または Red Hat Enterprise Linux の場合は、ASCII モードでサンプルファイルを転送してください。
- ・ バージョン 5.x の Replication Monitor からアップグレードインストールした場合で、すでに JP1/IM と連携していたときは、従来使用していた replication_monitor_ja.conf ファイルを削除してください。

2. コピーしたサンプルファイルの arguments= で始まる行を実行環境に合わせて修正し、保存します。

Device Manager

```
arguments="http://<IP アドレス>:<ポート>/HiCommand/IMLogin?
jpluserid=%JCO_JP1USER%&jpltoken=%JCO_JP1TOKEN%&launchurl=http://<
IP アドレス>:<ポート>/DeviceManager/Login";
```

Tiered Storage Manager

```
arguments="http://<IP アドレス>:<ポート>/HiCommand/IMLogin?  
jpluserid=%JCO_JP1USER%&jpltoken=%JCO_JP1TOKEN%&launchurl=http://<  
IP アドレス>:<ポート>/TieredStorageManager/login.do";
```

Replication Manager

```
arguments="http://<IP アドレス>:<ポート>/HiCommand/IMLogin?  
jpluserid=%JCO_JP1USER%&jpltoken=%JCO_JP1TOKEN%&launchurl=http://<  
IP アドレス>:<ポート>/ReplicationManager/login.do";
```

URL のプロトコル, <IP アドレス>および<ポート>を, 次のように指定します。

URL のプロトコル

SSL 通信の場合は, https を指定します。

<IP アドレス>

管理サーバの IPv4 アドレスを指定します。IPv6 アドレスはサポートしていません。

<ポート>

HBase Storage Mgmt Web Service のポート番号を指定します。デフォルト値は, 非 SSL 通信の場合は 23015, SSL 通信の場合は 23016 です。

JP1/IM の統合機能メニュー画面から次のメニューを選択して, Hitachi Command Suite 製品の GUI が表示されれば, 正しく設定されています。

Device Manager

[ストレージ管理] – [ストレージエリア管理] – [ストレージハードウェア管理]

Tiered Storage Manager

[ストレージ管理] – [ストレージエリア管理] – [階層ストレージリソース管理]

Replication Manager

[ストレージ管理] – [ストレージエリア管理] – [ストレージレプリケーション管理]



注意 JP1/IM の統合機能メニュー画面では, ブラウザーの [戻る] [進む] ボタンおよびブラウザーの履歴を使った画面の移動をしないでください。

関連項目

- [5.4.1 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするための前提環境](#)

ログおよびアラートの設定

この章では、Hitachi Command Suite 製品でシステムの状態や障害を監視するために必要な設定について説明します。

- 6.1 統合ログの設定
- 6.2 監査ログを採取するために必要な設定
- 6.3 アラートの設定
- 6.4 SNMP トラップをログファイルに出力するための設定
- 6.5 イベント通知を使用するために必要な設定
- 6.6 JP1/IM でログを参照するために必要な設定

6.1 統合ログの設定

Hitachi Command Suite 共通コンポーネントは、ログ取得用の共通ライブラリーを提供しています。Hitachi Command Suite 製品は、このライブラリーを使用して、ログファイルにトレースログ情報を出力します。

6.1.1 トレースログファイルの設定 (Windows)

Hitachi Command Suite 共通コンポーネントのトレースログファイルのファイル数やファイルサイズを変更する場合は、Windows HNTRLib2 ユーティリティを使って設定します。



警告 トレースログファイルの設定を変更すると、共通トレースログを使用するそのほかのプログラム製品に影響が及びます。

事前に完了しておく操作

- Administrator 権限でのログイン

Hitachi Command Suite 共通コンポーネントのトレースログファイルを設定するには：

- 次の場所に格納されている Windows HNTRLib2 ユーティリティを実行します。
< Program Files フォルダ > ¥Hitachi¥HNTRLib2¥bin¥hntr2util.exe
- [Hitachi Network Objectplaza Trace Utility 2] ダイアログの [Number of Files] に、トレースログファイル数を指定します。
トレースログファイルは、最大 16 個設定できます。デフォルトは 4 個です。
- [Hitachi Network Objectplaza Trace Utility 2] ダイアログの [File Size] に、トレースログのファイルサイズを指定します。
トレースログのファイルサイズが指定した値になると、次のファイルに切り替えられます。
トレースログのファイルサイズは、8KB~4096KB で指定できます。デフォルトは 256KB です。[Buffer] の値よりも大きい値を指定してください。
- [OK] ボタンをクリックします。
- 変更を適用するために、OS を再起動します。

6.1.2 トレースログファイルの設定 (Solaris または Linux)

Hitachi Command Suite 共通コンポーネントのトレースログファイルのファイル数やファイルサイズを変更する場合は、ユーティリティプログラム (hntr2util) を使って設定します。



警告 トレースログファイルの設定を変更すると、共通トレースログを使用するそのほかのプログラム製品に影響が及びます。

事前に完了しておく操作

- root でのログイン

Hitachi Command Suite 共通コンポーネントのトレースログファイルを設定するには：

- 次の場所に格納されているユーティリティプログラムを実行します。
/opt/hitachi/HNTRLib2/bin/hntr2util
- メニューで、2 (Number of log files) を指定します。
- サブメニューで、トレースログファイル数を指定し、[Enter] キーを押します。
トレースログファイルは、最大 16 個設定できます。デフォルトは 4 個です。

4. メニューで、1 (Size of a log file) を指定します。
5. サブメニューで、トレースログのファイルサイズを指定し、[Enter] キーを押します。
 トレースログのファイルサイズが指定した値になると、次のファイルに切り替えられます。
 トレースログのファイルサイズは、8KB~4096KB で指定できます。デフォルトは 256KB です。
 [Size of buffer] の値よりも大きい値を指定してください。
6. 設定内容を確認して [e] キーを押したあと、[Enter] キーを押します。
7. 変更後の設定を保存するために、[y] キーを押して終了します。
8. 次のコマンドを実行して、メモリマップドファイルを削除します。

```
# rm /opt/hitachi/HNTRLib/mmap/hntrmmap.mm
```
9. 変更を適用するために、OS を再起動します。

6.1.3 Tiered Storage Manager CLI のログファイル採取の設定

管理サーバに Tiered Storage Manager CLI をインストールしている場合、hcmdsggetlogs コマンドで Tiered Storage Manager CLI のログファイルも一緒に採取できます。一括採取するためには、HtsmgetTI.properties ファイルでの環境設定が必要です。

Tiered Storage Manager CLI のログファイル採取を設定するには：

1. 次の場所に格納されている HtsmgetTI.properties ファイルのプロパティを設定します。

Windows の場合：

```
< Tiered Storage Manager サーバのインストールフォルダ > %SupportTools  
%CollectTool%
```

Solaris または Linux の場合：

```
< Tiered Storage Manager サーバのインストールディレクトリ > /SupportTools/  
CollectTool/
```

表 6-1 HtsmgetTI.properties ファイルで設定するプロパティ

プロパティ	説明
CLI_DIR	Tiered Storage Manager CLI がインストールされているディレクトリを指定してください。デフォルトのディレクトリは次のとおりです。 Windows の場合： <pre>< Tiered Storage Manager サーバのインストールフォルダ > %CLI</pre> Solaris または Linux の場合： <pre>< Tiered Storage Manager サーバのインストールディレクトリ > /CLI</pre>
SYSLOG	syslog の絶対パスを指定します。デフォルトのディレクトリは次のとおりです。 Solaris の場合： <pre>/var/adm/messages</pre> Linux の場合： <pre>/var/log/messages</pre>

6.2 監査ログを採取するために必要な設定

Hitachi Command Suite 製品では、法規制やセキュリティ評価基準、業界ごとの各種基準などに従っていることを監査者や評価者に証明するために、監査ログにユーザーの操作内容を記録できます。監査ログを採取するには、環境設定ファイル (auditlog.conf) を編集する必要があります。環境設定ファイルについては、「6.2.2 監査ログの環境設定ファイルの編集」を参照してください。

監査ログは、Windows の場合はイベントログファイル（アプリケーションログファイル）に出力され、Solaris または Linux の場合は syslog ファイルに出力されます。

日立のストレージ関連製品で採取できる監査ログを次の表に示します。

表 6-2 監査ログの種別と説明

種別	説明
StartStop	ハードウェアまたはソフトウェアの起動と終了を示す事象。 <ul style="list-style-type: none"> OS の起動と終了 ハードウェアコンポーネント（マイクロ含む）の起動と終了 ストレージシステム上のソフトウェア、SVP 上のソフトウェア、Hitachi Command Suite 製品の起動と終了
Failure	ハードウェアまたはソフトウェアの異常を示す事象。 <ul style="list-style-type: none"> ハードウェア障害 ソフトウェア障害（メモリーエラーなど）
LinkStatus	機器間のリンク状態を示す事象。 <ul style="list-style-type: none"> リンクアップまたはダウン
ExternalService	日立のストレージ関連製品と外部サービスとの通信結果を示す事象。 <ul style="list-style-type: none"> NTP サーバや DNS サーバなどとの通信 管理サーバとの通信（SNMP）
Authentication	機器、管理者、またはエンドユーザーが接続または認証を試みて成功または失敗したことを示す事象。 <ul style="list-style-type: none"> FC ログイン 機器認証（FC-SP 認証、iSCSI ログイン認証、SSL サーバ/クライアント認証） 管理者またはエンドユーザー認証
AccessControl	機器、管理者、またはエンドユーザーがリソースへのアクセスを試みて成功または失敗したことを示す事象。 <ul style="list-style-type: none"> 機器のアクセスコントロール 管理者またはエンドユーザーのアクセスコントロール
ContentAccess	重要なデータへのアクセスを試みて成功または失敗したことを示す事象。 <ul style="list-style-type: none"> NAS 上の重要なファイルまたは HTTP サポート時のコンテンツへのアクセス 監査ログファイルへのアクセス
ConfigurationAccess	管理者が許可された運用操作を実行し、操作が正常終了または失敗したことを示す事象。 <ul style="list-style-type: none"> 構成情報の参照または更新 アカウントの追加、削除などのアカウント設定の更新 セキュリティの設定 監査ログ設定の参照または更新
Maintenance	保守操作を実行し、操作が正常終了または失敗したことを示す事象。 <ul style="list-style-type: none"> ハードウェアコンポーネント増設または減設 ソフトウェアコンポーネント増設または減設
AnomalyEvent	しきい値のオーバーなどの異常が発生したことを示す事象。 <ul style="list-style-type: none"> ネットワークトラフィックのしきい値オーバー CPU 負荷のしきい値オーバー 内部に一時保存した監査ログの上限到達前通知やラップアラウンド 異常な通信の発生を示す事象。 <ul style="list-style-type: none"> 通常使用するポートへの SYN フラッド攻撃やプロトコル違反 未使用ポートへのアクセス（ポートスキャンなど）

採取できる監査ログは、製品ごとに異なります。

また、監査ログの出力内容については「13.3 監査ログの確認」を参照してください。

6.2.1 監査ログに出力される監査事象

Device Manager と Tiered Storage Manager では、次の種別の監査事象が監査ログに出力されま
す。

- StartStop
- Authentication
- ConfigurationAccess
- AccessControl
- ExternalService

それぞれの監査事象には、重要度 (Severity) が設定されています。重要度によって、出力する監
査ログをフィルタリングできます。

Device Manager と Tiered Storage Manager で監査ログに出力される監査事象を「表 6-3 監査ログ
に出力される監査事象 (種別が StartStop の場合)」～「表 6-7 監査ログに出力される監査事象 (種
別が ExternalService の場合)」に示します。そのほかの Hitachi Command Suite 製品で出力され
る監査ログについては、各製品のマニュアルを参照してください。

表 6-3 監査ログに出力される監査事象 (種別が StartStop の場合)

種別の説明	監査事象	Severity	メッセージ ID
ソフトウェアの起 動と終了	SSO サーバの起動成功	6	KAPM00090-I
	SSO サーバの起動失敗	3	KAPM00091-E
	SSO サーバの停止	6	KAPM00092-I

表 6-4 監査ログに出力される監査事象 (種別が Authentication の場合)

種別の説明	監査事象	Severity	メッセージ ID
管理者またはエン ドユーザーの認証	ログインの成功	6	KAPM01124-I
	ログインの成功 (外部認証サーバログイン)	6	KAPM02450-I
	ログインの失敗 (ユーザー ID またはパスワードに 誤りがある場合)	4	KAPM02291-W
	ログインの失敗 (ロック中のユーザーでログイン)	4	KAPM02291-W
	ログインの失敗 (存在しないユーザーでログイン)	4	KAPM02291-W
	ログインの失敗 (権限なし)	4	KAPM01095-E
	ログインの失敗 (認証失敗)	4	KAPM01125-E
	ログインの失敗 (外部認証サーバ認証失敗)	4	KAPM02451-W
	ログアウトの成功	6	KAPM08009-I
アカウントの自動 ロック	アカウントの自動ロック (認証の連続失敗またはア カウントの有効期限切れ)	4	KAPM02292-W

表 6-5 監査ログに出力される監査事象 (種別が ConfigurationAccess の場合)

種別の説明	監査事象	Severity	メッセージ ID
ユーザーの登録 (GUI)	ユーザーの登録成功	6	KAPM07230-I
	ユーザーの登録失敗	3	KAPM07240-E
ユーザーの削除 (GUI)	単一ユーザーの削除成功	6	KAPM07231-I
	単一ユーザーの削除失敗	3	KAPM07240-E
	複数ユーザーの削除成功	6	KAPM07231-I
	複数ユーザーの削除失敗	3	KAPM07240-E

種別の説明	監査事象	Severity	メッセージ ID
パスワードの変更 (管理者画面から変更)	管理者によるパスワード変更成功	6	KAPM07232-I
	管理者によるパスワード変更失敗	3	KAPM07240-E
パスワードの変更 (自ユーザー用画面から変更)	旧パスワードが正しいかを判断するための認証処理で失敗	3	KAPM07239-E
	ログインユーザー自身のパスワード変更成功 (自ユーザー画面から変更)	6	KAPM07232-I
	ログインユーザー自身のパスワード変更失敗 (自ユーザー画面から変更)	3	KAPM07240-E
プロフィールの変更	プロフィールの変更成功	6	KAPM07233-I
	プロフィールの変更失敗	3	KAPM07240-E
権限の変更	権限の変更成功	6	KAPM02280-I
	権限の変更失敗	3	KAPM07240-E
アカウントのロック	アカウントのロック成功※1	6	KAPM07235-I
	アカウントのロック失敗	3	KAPM07240-E
アカウントのロック解除	アカウントのロック解除成功※2	6	KAPM07236-I
	アカウントのロック解除失敗	3	KAPM07240-E
	hcmdsunlockaccount コマンドによるアカウントのロック解除成功	6	KAPM07236-I
	hcmdsunlockaccount コマンドによるアカウントのロック解除失敗	3	KAPM07240-E
認証方式変更	認証方式の変更成功	6	KAPM02452-I
	認証方式の変更失敗	3	KAPM02453-E
認可グループの追加 (GUI)	認可グループの追加成功	6	KAPM07247-I
	認可グループの追加失敗	3	KAPM07248-E
認可グループの削除 (GUI)	単一認可グループの削除成功	6	KAPM07249-I
	単一認可グループの削除失敗	3	KAPM07248-E
	複数認可グループの削除成功	6	KAPM07249-I
	複数認可グループの削除失敗	3	KAPM07248-E
認可グループの権限変更 (GUI)	認可グループの権限変更成功	6	KAPM07250-I
	認可グループの権限変更失敗	3	KAPM07248-E
ユーザーの登録 (GUI および CLI)	ユーザーの登録成功	6	KAPM07241-I
	ユーザーの登録失敗	3	KAPM07242-E
ユーザー情報の更新 (GUI および CLI)	ユーザー情報の更新成功	6	KAPM07243-I
	ユーザー情報の更新失敗	3	KAPM07244-E
ユーザーの削除 (GUI および CLI)	ユーザーの削除成功	6	KAPM07245-I
	ユーザーの削除失敗	3	KAPM07246-E
認可グループの登録 (GUI または CLI)	認可グループの登録成功	6	KAPM07251-I
	認可グループの登録失敗	3	KAPM07252-E
認可グループの削除 (GUI または CLI)	認可グループの削除成功	6	KAPM07253-I
	認可グループの削除失敗	3	KAPM07254-E

種別の説明	監査事象	Severity	メッセージID
認可グループの権限変更 (GUI または CLI)	認可グループの権限変更成功	6	KAPM07255-I
	認可グループの権限変更失敗	3	KAPM07256-E
ユーザーグループの登録 (CLI)	ユーザーグループの登録成功	6	KAPM07263-I
	ユーザーグループの登録失敗	3	KAPM07264-E
ユーザーグループの削除 (CLI)	ユーザーグループの削除成功	6	KAPM07265-I
	ユーザーグループの削除失敗	3	KAPM07266-E
ユーザーグループの更新 (CLI)	ユーザーグループの更新成功	6	KAPM07267-I
	ユーザーグループの更新失敗	3	KAPM07268-E
ロールの登録 (CLI)	ロールの登録成功	6	KAPM07269-I
	ロールの登録失敗	3	KAPM07270-E
ロールの削除 (CLI)	ロールの削除成功	6	KAPM07271-I
	ロールの削除失敗	3	KAPM07272-E
ロールの更新 (CLI)	ロールの更新成功	6	KAPM07273-I
	ロールの更新失敗	3	KAPM07274-E
ユーザーグループへのユーザーアカウントの割り当て (CLI)	ユーザーグループへのユーザーアカウントの割り当て成功	6	KAPM07275-I
	ユーザーグループへのユーザーアカウントの割り当て失敗	3	KAPM07276-E
ロールへのパーミッションの割り当て (CLI)	ロールへのパーミッションの割り当て成功	6	KAPM07277-I
	ロールへのパーミッションの割り当て失敗	3	KAPM07278-E
次の3項目の割り当て (CLI) ・ ユーザーグループおよび認可グループ ・ リソースグループ ・ ロール	次の3項目の割り当ての成功 ・ ユーザーグループおよび認可グループ ・ リソースグループ ・ ロール	6	KAPM07279-I
	次の3項目の割り当ての失敗 ・ ユーザーグループおよび認可グループ ・ リソースグループ ・ ロール	3	KAPM07280-E
データベースのバックアップまたはリストア	hcmsdbbackups コマンドによるバックアップ成功	6	KAPM05561-I
	hcmsdbbackups コマンドによるバックアップ失敗	3	KAPM05562-E
	hcmsbdb コマンドによる全体リストアの成功	6	KAPM05563-I
	hcmsbdb コマンドによる全体リストアの失敗	3	KAPM05564-E
	hcmsbdb コマンドによる部分リストアの成功	6	KAPM05565-I
	hcmsbdb コマンドによる部分リストアの失敗	3	KAPM05566-E
データベースのデータの入出力	hcmsdbmove コマンドによるデータ出力の成功	6	KAPM06543-I
	hcmsdbmove コマンドによるデータ出力の失敗	3	KAPM06544-E
	hcmsdbmove コマンドによるデータ入力成功	6	KAPM06545-I
	hcmsdbmove コマンドによるデータ入力失敗	3	KAPM06546-E
データベース領域の作成または削除	hcmsdbsetup コマンドによるデータベース領域の作成成功	6	KAPM06348-I
	hcmsdbsetup コマンドによるデータベース領域の作成失敗	3	KAPM06349-E

種別の説明	監査事象	Severity	メッセージ ID
	hcmdsdbsetup コマンドによるデータベース領域の削除成功	6	KAPM06350-I
	hcmdsdbsetup コマンドによるデータベース領域の削除失敗	3	KAPM06351-E
認証データの出入力	hcmdsauthmove コマンドによるデータ出力の成功	6	KAPM05832-I
	hcmdsauthmove コマンドによるデータ出力の失敗	3	KAPM05833-E
	hcmdsauthmove コマンドによるデータ入力 of 成功	6	KAPM05834-I
	hcmdsauthmove コマンドによるデータ入力 of 失敗	3	KAPM05835-E
Device Manager サーバの処理	リクエスト受理 (正常時)	6	KAIC51000-I KAIC51200-I KAIC51201-I
	リクエスト受理 (共通・異常時)	3	KAIC51400-E
	レスポンス送信 (正常時)	6	KAIC51100-I KAIC51300-I KAIC51301-I KAIC51302-I
	レスポンス送信 (異常時)	3	KAIC51500-E KAIC51700-E KAIC51701-E
関連製品の起動 (ラ ウンチ)	リクエスト受理 (正常時)	6	KAIC53000-I
	リクエスト受理 (異常時)	3	KAIC53200-E
	レスポンス送信 (正常時)	6	KAIC53100-I
	レスポンス送信 (異常時)	3	KAIC53300-E
Device Manager サーバ (CIM 経由) の処理	リクエスト受理 (正常時)	6	KAIC54000-I KAIC54200-I
	リクエスト受理 (異常時)	3	KAIC54400-E KAIC54600-E
	レスポンス送信 (正常時)	6	KAIC54100-I KAIC54300-I
	レスポンス送信 (異常時)	3	KAIC54500-E KAIC54700-E
ストレージドメイ ンの情報取得※3	全ストレージドメインの情報取得に成功	6	KATS90000-I
	全ストレージドメインの情報取得に失敗	4	KATS90001-W
	ストレージドメインの情報取得に成功	6	KATS90000-I
	ストレージドメインの情報取得に失敗	4	KATS90001-W
	全ストレージドメインの要約情報取得に成功	6	KATS90000-I
	全ストレージドメインの要約情報取得に失敗	4	KATS90001-W
	ストレージドメインの要約情報取得に成功	6	KATS90000-I
	ストレージドメインの要約情報取得に失敗	4	KATS90001-W
	ストレージドメインのリフレッシュ状態取得に成 功	6	KATS90000-I
	ストレージドメインのリフレッシュ状態取得に失 敗	4	KATS90001-W

種別の説明	監査事象	Severity	メッセージID
マイグレーショングループの情報取得※3	全マイグレーショングループの情報取得に成功	6	KATS90000-I
	全マイグレーショングループの情報取得に失敗	4	KATS90001-W
	マイグレーショングループの情報取得に成功	6	KATS90000-I
	マイグレーショングループの情報取得に失敗	4	KATS90001-W
	全マイグレーショングループの要約情報取得に成功	6	KATS90000-I
	全マイグレーショングループの要約情報取得に失敗	4	KATS90001-W
	マイグレーショングループの要約情報取得に成功	6	KATS90000-I
	マイグレーショングループの要約情報取得に失敗	4	KATS90001-W
ストレージシステムの情報取得※3	ストレージシステムの情報取得に成功	6	KATS90000-I
	ストレージシステムの情報取得に失敗	4	KATS90001-W
	エミュレーションタイプの情報取得に成功	6	KATS90000-I
	エミュレーションタイプの情報取得に失敗	4	KATS90001-W
タスクの情報取得※3	全タスクの情報取得に成功	6	KATS90000-I
	全タスクの情報取得に失敗	4	KATS90001-W
	タスクの情報取得に成功	6	KATS90000-I
	タスクの情報取得に失敗	4	KATS90001-W
	全タスクの要約情報取得に成功	6	KATS90000-I
	全タスクの要約情報取得に失敗	4	KATS90001-W
	タスクの要約情報取得に成功	6	KATS90000-I
	タスクの要約情報取得に失敗	4	KATS90001-W
ストレージの階層情報取得※3	全ストレージの階層情報取得に成功	6	KATS90000-I
	全ストレージの階層情報取得に失敗	4	KATS90001-W
	ストレージの階層情報取得に成功	6	KATS90000-I
	ストレージの階層情報取得に失敗	4	KATS90001-W
	全ストレージの階層要約情報の取得に成功	6	KATS90000-I
	全ストレージの階層要約情報の取得に失敗	4	KATS90001-W
	ストレージの階層要約情報の取得に成功	6	KATS90000-I
	ストレージの階層要約情報の取得に失敗	4	KATS90001-W
プールの情報取得※3	プールの情報取得に成功	6	KATS90000-I
	プールの情報取得に失敗	4	KATS90001-W
	検索条件に一致するプール数の取得に成功	6	KATS90000-I
	検索条件に一致するプール数の取得に失敗	4	KATS90001-W
キーストアーファイルの情報取得※3	キーストアーファイルの情報取得に成功	6	KATS90000-I
	キーストアーファイルの情報取得に失敗	4	KATS90001-W
ボリュームの情報取得※3	ボリュームの情報取得に成功	6	KATS90000-I
	ボリュームの情報取得に失敗	4	KATS90001-W
	検索条件に一致するボリューム数の取得に成功	6	KATS90000-I
	検索条件に一致するボリューム数の取得に失敗	4	KATS90001-W
	検索条件の取得に成功	6	KATS90000-I
	検索条件の取得に失敗	4	KATS90001-W
	ボリュームの要約情報取得に成功	6	KATS90000-I

種別の説明	監査事象	Severity	メッセージID
	ボリュームの要約情報取得に失敗	4	KATS90001-W
パリティグループの空き容量情報の取得※3	パリティグループの情報取得に成功	6	KATS90000-I
	パリティグループの情報取得に失敗	4	KATS90001-W
	検索条件の取得に成功	6	KATS90000-I
	検索条件の取得に失敗	4	KATS90001-W
	検索条件に一致するパリティグループ数の取得に成功	6	KATS90000-I
	検索条件に一致するパリティグループ数の取得に失敗	4	KATS90001-W
外部接続設定情報の取得※3	外部接続設定情報の取得に成功	6	KATS90000-I
	外部接続設定情報の取得に失敗	4	KATS90001-W
	パスグループの情報取得に成功	6	KATS90000-I
	パスグループの情報取得に失敗	4	KATS90001-W
ストレージドメインに対する操作※3	ストレージドメインの登録失敗	4	KATS90001-W
	ストレージドメインの削除失敗	4	KATS90001-W
	ストレージドメイン情報の更新成功	6	KATS90000-I
	ストレージドメイン情報の更新失敗	4	KATS90001-W
	ストレージドメインのリフレッシュ成功	6	KATS90000-I
	ストレージドメインのリフレッシュ失敗	4	KATS90001-W
マイグレーショングループに対する操作※3	マイグレーショングループへのボリューム追加成功	6	KATS90000-I
	マイグレーショングループへのボリューム追加失敗	4	KATS90001-W
	マイグレーション先として指定できるストレージ階層の一覧取得成功	6	KATS90000-I
	マイグレーション先として指定できるストレージ階層の一覧取得失敗	4	KATS90001-W
	マイグレーショングループの登録成功	6	KATS90000-I
	マイグレーショングループの登録失敗	4	KATS90001-W
	マイグレーショングループの削除成功	6	KATS90000-I
	マイグレーショングループの削除失敗	4	KATS90001-W
	マイグレーショングループ情報の更新成功	6	KATS90000-I
	マイグレーショングループ情報の更新失敗	4	KATS90001-W
	マイグレーションプランの作成成功	6	KATS90000-I
	マイグレーションプランの作成失敗	4	KATS90001-W
	マイグレーショングループからのボリューム削除成功	6	KATS90000-I
	マイグレーショングループからのボリューム削除失敗	4	KATS90001-W
	タスクに対する操作※3	タスクのキャンセル成功	6
タスクのキャンセル失敗		4	KATS90001-W
タスクの状態変更成功		6	KATS90000-I
タスクの状態変更失敗		4	KATS90001-W
マイグレーションタスクの登録成功		6	KATS90000-I
マイグレーションタスクの登録失敗		4	KATS90001-W

種別の説明	監査事象	Severity	メッセージID
	タスクの登録成功	6	KATS90000-I
	タスクの登録失敗	4	KATS90001-W
	タスクの削除成功	6	KATS90000-I
	タスクの削除失敗	4	KATS90001-W
	タスクの実行成功	6	KATS90000-I
	タスクの実行失敗	4	KATS90001-W
	タスク情報の更新成功	6	KATS90000-I
	タスク情報の更新失敗	4	KATS90001-W
ストレージ階層に対する操作※3	ストレージ階層の登録成功	6	KATS90000-I
	ストレージ階層の登録失敗	4	KATS90001-W
	ストレージ階層の削除成功	6	KATS90000-I
	ストレージ階層の削除失敗	4	KATS90001-W
	ストレージ階層情報の更新成功	6	KATS90000-I
	ストレージ階層情報の更新失敗	4	KATS90001-W

注※1

パスワードが設定されていないユーザーの認証方式を変更したことによるアカウントのロックについては、監査ログに記録されません。

注※2

ユーザーにパスワードを設定したことによるアカウントのロックの解除については、監査ログに記録されません。

注※3

Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI で操作した場合にだけ出力されます。

表 6-6 監査ログに出力される監査事象（種別が AccessControl の場合）

種別の説明	監査事象	Severity	メッセージID
ストレージドメインに対する操作失敗	ストレージドメインの変更権限なし	4	KATS90010-W
	ストレージドメインのリフレッシュ権限なし	4	KATS90010-W
ストレージ階層に対する操作失敗	ストレージ階層の作成権限なし	4	KATS90010-W
	ストレージ階層の削除権限なし	4	KATS90010-W
	ストレージ階層の変更権限なし	4	KATS90010-W
マイグレーショングループに対する操作失敗	マイグレーショングループの作成権限なし	4	KATS90010-W
	マイグレーショングループの削除権限なし	4	KATS90010-W
	マイグレーショングループの変更権限なし	4	KATS90010-W
	マイグレーショングループへのボリューム追加権限なし	4	KATS90010-W
	マイグレーショングループからのボリューム削除権限なし	4	KATS90010-W
タスクに対する操作失敗	タスクの作成権限なし	4	KATS90010-W
	タスクの削除権限なし	4	KATS90010-W
	タスクの変更権限なし	4	KATS90010-W
	タスクの実行権限なし	4	KATS90010-W

種別の説明	監査事象	Severity	メッセージ ID
	タスクのキャンセル権限なし	4	KATS90010-W
	タスクの中止権限なし	4	KATS90010-W

注

Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI で操作した場合にだけ出力されます。

表 6-7 監査ログに出力される監査事象（種別が ExternalService の場合）

種別の説明	監査事象	Severity	メッセージ ID
外部認証サーバとの通信	LDAP ディレクトリサーバとの通信成功	6	KAPM10116-I
	LDAP ディレクトリサーバとの通信失敗	3	KAPM10117-E
	RADIUS サーバとの通信成功	6	KAPM10118-I
	RADIUS サーバとの通信失敗（応答なし）	3	KAPM10119-E
	Kerberos サーバとの通信成功	6	KAPM10120-I
	Kerberos サーバとの通信失敗（応答なし）	3	KAPM10121-E
	DNS サーバとの通信成功	6	KAPM10122-I
	DNS サーバとの通信失敗（応答なし）	3	KAPM10123-E
外部認証サーバとの認証	LDAP ディレクトリサーバとの TLS ネゴシエーションに成功	6	KAPM10124-I
	LDAP ディレクトリサーバとの TLS ネゴシエーションに失敗	3	KAPM10125-E
	LDAP ディレクトリサーバでの情報検索用ユーザーの認証成功	6	KAPM10126-I
	LDAP ディレクトリサーバでの情報検索用ユーザーの認証失敗	3	KAPM10127-W
外部認証サーバでのユーザー認証	LDAP ディレクトリサーバでのユーザーの認証成功	6	KAPM10128-I
	LDAP ディレクトリサーバにユーザーが存在しない	4	KAPM10129-W
	LDAP ディレクトリサーバでのユーザーの認証失敗	4	KAPM10130-W
	RADIUS サーバでのユーザーの認証成功	6	KAPM10131-I
	RADIUS サーバでのユーザーの認証失敗	4	KAPM10132-W
	Kerberos サーバでのユーザーの認証成功	6	KAPM10133-I
	Kerberos サーバでのユーザーの認証失敗	4	KAPM10134-W
外部認証サーバから情報取得	LDAP ディレクトリサーバからユーザー情報の取得に成功	6	KAPM10135-I
	LDAP ディレクトリサーバからユーザー情報の取得に失敗	3	KAPM10136-E
	DNS サーバから SRV レコードの取得に成功	6	KAPM10137-I
	DNS サーバから SRV レコードの取得に失敗	3	KAPM10138-E

メッセージテキストの出力形式については「13.3.1 監査ログのメッセージテキスト」を参照してください。

メッセージ ID に対応するメッセージテキストについては、マニュアル「Hitachi Command Suite Software メッセージガイド」を参照してください。

6.2.2 監査ログの環境設定ファイルの編集

Hitachi Command Suite 製品の監査ログを採取するには、環境設定ファイル (auditlog.conf) を編集する必要があります。環境設定ファイルの Log.Event.Category に採取する監査事象の種別を設定することで、監査ログを取得できるようになります。

監査ログの環境設定ファイルの変更を反映するには、Hitachi Command Suite 製品のサービスを再起動する必要があります。



注意 監査ログは大量に出力されるおそれがあるので、ログサイズの変更、採取したログの退避、保管などを実施してください。

auditlog.conf ファイルの格納先を次に示します。

- Windows の場合：
 < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %conf%\sec
 %auditlog.conf
- Solaris または Linux の場合：
 < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /conf/sec/
 auditlog.conf

auditlog.conf ファイルに設定する項目を次の表に示します。

表 6-8 auditlog.conf ファイルに設定する項目

項目	説明
Log.Facility	syslog ファイルに監査ログメッセージを出力するときに使用される分類 (Facility) を数値で指定します。 Log.Facility と各監査事象に設定されている重要度 (Severity) を組み合わせた値が、syslog ファイル出力のフィルタリングに使用されます。監査ログに出力される重要度 (Severity) の値については、「表 6-3」～「表 6-7」を参照してください。Log.Facility に指定できる値については、「表 6-9」を参照してください。監査事象の重要度と syslog.conf ファイルの重要度の対応については、「表 6-10」を参照してください。 Log.Facility は、Solaris または Linux の場合だけに有効です。 Windows の場合、指定しても無視されます。また、指定できない値、または、数値ではない文字を指定した場合は、デフォルト値が仮定されます。 デフォルト値：1
Log.Event.Category	採取する監査事象の種別を指定します。複数指定する場合は、コンマ (,) で区切ります。その場合、種別とコンマの間はスペースを空けずに詰めて指定してください。指定されていない場合、監査ログは出力されません。指定できる種別については、「表 6-3」～「表 6-7」を参照してください。大文字、小文字は区別されません。指定できる種別以外の名称を指定した場合は、無視されます。 デフォルト値：指定なし
Log.Level	採取する監査事象の重要度 (Severity) を指定します。指定した値以下の重要度を持つ監査事象が、イベントログファイルに出力されます。 Hitachi Command Suite 製品で出力する監査事象および監査事象の重要度 (Severity) については、「表 6-3」～「表 6-7」を参照してください。監査事象の重要度とイベントログの種類への対応については、「表 6-10」を参照してください。 Log.Level は、Windows の場合だけに有効です。Solaris または Linux の場合、指定しても無視されます。また、指定できる値以外の数値、または、数値以外の文字を指定した場合は、デフォルト値が仮定されます。 指定できる値：0～7 (重要度 (Severity)) デフォルト値：6

次に Log.Facility に指定できる値と、対応する syslog.conf ファイルでの指定値を示します。

表 6-9 Log.Facility に指定できる値と syslog.conf での指定値の対応

Facility	対応する syslog.conf での指定値
1	user
2	mail*
3	daemon
4	auth*
6	lpr*
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

注※

指定はできますが、推奨しません。

次に監査事象の重要度、 syslog.conf ファイルの重要度の指定値およびイベントログの種類に対応を示します。

表 6-10 監査事象の重要度、 syslog.conf の重要度、 およびイベントログの種類に対応

監査事象の重要度	syslog.conf の重要度	イベントログの種類
0	emerg	エラー
1	alert	
2	crit	
3	err	
4	warning	警告
5	notice	情報
6	info	
7	debug	

次に auditlog.conf ファイルの例を示します。

```
# Specify an integer for Facility. (specifiable range: 1-23)
Log.Facility 1

# Specify the event category.
# You can specify any of the following:
# StartStop, Failure, LinkStatus, ExternalService,
# Authentication, AccessControl, ContentAccess,
# ConfigurationAccess, Maintenance, or AnomalyEvent.
Log.Event.Category Authentication,ConfigurationAccess

# Specify an integer for Severity. (specifiable range: 0-7)
Log.Level 6
```

この例の場合、 Authentication または ConfigurationAccess の監査事象が出力されます。 Windows の場合、「エラー」、「警告」および「情報」の監査ログが出力されます。 Solaris または

Linux の場合、分類が user として syslog.conf ファイルに定義された syslog ファイルに監査ログが出力されます。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

6.3 アラートの設定

Device Manager では、管理対象のストレージシステムやファイルサーバで発生した障害の情報を、アラートとして Device Manager GUI/CLI に表示します。

ストレージシステムのアラートは、受信内容をユーザーに E メールで自動通知することもできます。

6.3.1 Device Manager での障害検知

Device Manager では、管理対象のストレージシステムやファイルサーバの障害を、次の方法で検知します。

- ポーリング (デフォルト)
Device Manager が、ストレージシステムの稼働状況を定期的に監視し、障害を検知した場合にアラートとして表示します。アラートには発生部位と障害の概要が含まれています。
ポーリングの間隔は、Device Manager サーバの `server.dispatcher.daemon.pollingPeriod` プロパティで設定できます。
- SNMP トラップ (オプション)
ストレージシステムまたはファイルサーバから SNMP トラップを受信した時点で、SNMP トラップをアラートとして表示します。SNMP トラップには障害の発生部位だけでなく、発生場所の情報も含まれているため、障害要因を特定する際に便利です。なお、SNMP トラップを Device Manager で受信するためには、環境設定が必要です。

Device Manager で表示できるアラートは、ストレージシステムやファイルサーバによって異なります。それぞれのサポート有無を次の表に示します。

表 6-11 Device Manager で表示できるアラート

	管理対象	ポーリング	SNMP トラップ
ストレージシステム	Virtual Storage Platform	○	○
	Universal Storage Platform V/VM	○	○
	Hitachi USP	○	○
	SANRISE9900V	○	○
	HUS VM	○	○
	HUS100	○	×
	Hitachi AMS2000	○	×
	Hitachi SMS	○	×
	Hitachi AMS/WMS	○	×
	SANRISE9500V	○	×
	SMI-S enabled ストレージシステム	×	×

管理対象		ポーリング	SNMP トラップ
ファイルサーバ	Hitachi Virtual File Platform	×	○
	Hitachi NAS Platform	×	×

(凡例)

○ : サポート × : 非サポート

関連項目

- [6.3.2 SNMP トラップをアラートに表示するための設定](#)
- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.5.3 server.dispatcher.daemon.pollingPeriod](#)

6.3.2 SNMP トラップをアラートに表示するための設定

SNMP トラップをアラートに表示するには、次の設定が必要です。

- Device Manager で SNMP トラップを受信するための設定
 - 管理サーバの 162/udp ポートを Device Manager で使えるようにする
 - Device Manager サーバの `server.dispatcher.daemon.receiveTrap` プロパティに `true` を設定する
- SNMP トラップを Device Manager に通知するための設定
 - ストレージシステムの場合は、SNMP Agent で、トラップの通知対象マシンとして管理サーバの IP アドレスを設定する
 - Hitachi Virtual File Platform の場合は、Hitachi File Services Manager で、トラップの通知対象マシンとして管理サーバのホスト名または IP アドレスと、ポート番号 (162/udp) を設定する

上記の設定が完了すると、Device Manager サーバは、すべてのコミュニティの SNMP トラップを受信してアラートに表示します。

関連項目

- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.5.5 server.dispatcher.daemon.receiveTrap](#)

6.3.3 アラートを E メール通知するための操作フロー

ストレージシステムのアラートが発生した場合に、ユーザーに自動的に E メールを通知できます。管理クライアントにログインしていない状況でも、ストレージシステムの障害を知ることができます。

アラートを E メール通知するために必要な設定を次に示します。

1. SMTP サーバの環境設定
使用する SMTP サーバの設定手順に従って、Device Manager サーバが SMTP サーバに接続できるように設定します。
2. 受信ユーザーの登録
Device Manager GUI で、E メールを受信するユーザーを登録します。
3. アラート通知のプロパティ設定

Device Manager サーバのプロパティに、SMTP サーバの情報や通知元のメールアドレスなどを設定します。

4. SMTP 認証ユーザーアカウントの登録 (SMTP 認証を使用する場合)

Device Manager サーバに SMTP 認証ユーザーアカウントを登録します。イベント通知やヘルスチェック結果の通知で登録済みの場合、再登録は不要です。

5. アラート通知テンプレートのカスタマイズ (任意)

必要に応じてテンプレートファイルを編集し、Eメールの出力内容を設定します。



重要

- Device Manager が Eメールを送信するのは、アラート検出時の 1 回だけです。送信に失敗した場合、Eメールは再送されず、アラート情報および送信先の Eメールアドレスが、Device Manager のトレースログファイルに出力されます。
- Eメールを送信する前に Device Manager サーバのサービスが停止した場合、サービスが再起動しても Eメールは送信されません。サービスの再起動後に、CLI の GetAlerts コマンドまたは GUI で、対処していないアラートがないか確認してください。
- Device Manager サーバの管理対象ストレージシステムに対して、環境の構築や保守を実施すると、ストレージシステムでアラートが多数発生することがあります。事前に Device Manager サーバの server.mail.enabled プロパティに false を指定し、Eメール通知機能を無効にしておくことをお勧めします。

関連項目

- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.2.17 server.mail.enabled](#)

(1) SMTP サーバの設定

Device Manager サーバが SMTP サーバに接続できるように設定します。

SMTP サーバで、Device Manager サーバがサポートしている SMTP 認証の認証方式を指定してください。Device Manager サーバがサポートする SMTP 認証の認証方式は、LOGIN、PLAIN です。



重要

- SMTP サーバの認証方式が複数ある場合、Device Manager サーバは LOGIN、PLAIN の優先順で Eメールを送信します。SMTP サーバで LOGIN または PLAIN が指定されていない場合は、SMTP 認証を使用しないで Eメールを送信します。
- SMTP サーバで SMTP 認証の設定が無効な場合、Device Manager サーバ側で SMTP 認証の設定を有効にしても、Device Manager サーバは SMTP 認証を使用しないで Eメールを送信します。

(2) 受信ユーザーの登録

Eメールの受信ユーザーは、Device Manager GUI で登録します。

Eメールを受信するユーザーの条件は次のとおりです。条件を満たすユーザーに同じ内容の Eメールが送信されます。

- 対象のストレージシステムに対応するリソースグループが割り当てられていること。
- 割り当てたリソースグループに対する Device Manager のロールとして Modify が設定されていること。
- ユーザーのプロファイルに Eメールアドレスが登録されていること。

ユーザーアカウントを Hitachi Command Suite 製品に登録している場合に必要です。外部認可サーバでユーザーアカウントを管理している場合は、外部認可サーバで Eメールアドレスを登録してください。



参考 Device Manager サーバが送信する E メール の文字コードは Unicode (UTF-8) です。E メールを受信するユーザーは、Unicode (UTF-8) に対応したメールソフトを使用してください。

関連項目

- Device Manager GUI でのユーザー登録について：マニュアル「*Hitachi Command Suite Software ユーザーズガイド*」

(3) アラート通知のプロパティ設定

アラートを E メールで通知するには、Device Manager サーバの `server.properties` ファイルのプロパティに、SMTP サーバの情報や通知元のメールアドレスなどを設定する必要があります。

設定が必要なプロパティは次のとおりです。

- `server.mail.enabled`
- `server.mail.from`
- `server.mail.smtp.host`
- `server.mail.smtp.port`
- `server.mail.smtp.auth`
- `server.mail.errorsTo`
- `server.eventNotification.mail.to`
- `server.mail.alert.type`
- `server.mail.alert.status`

関連項目

- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.2.17 server.mail.enabled](#)
- [A.2.18 server.mail.from](#)
- [A.2.19 server.mail.smtp.host](#)
- [A.2.20 server.mail.smtp.port](#)
- [A.2.21 server.mail.smtp.auth](#)
- [A.2.22 server.mail.errorsTo](#)
- [A.2.23 server.eventNotification.mail.to](#)
- [A.2.24 server.mail.alert.type](#)
- [A.2.25 server.mail.alert.status](#)

(4) SMTP 認証ユーザーアカウントの Device Manager への登録

SMTP 認証を使用する場合は、SMTP 認証ユーザーのアカウントを `hdvmmmodmailuser` コマンドで Device Manager に登録します。イベント通知およびヘルスチェック結果の E メール通知で SMTP 認証ユーザーが設定済みの場合、再設定は不要です。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン
- Device Manager サーバの `server.mail.smtp.auth` プロパティの設定

true を指定してください。

事前に確認しておく情報

- リソースグループとして All Resources が割り当てられ、Device Manager のロールとして Admin が設定されている Device Manager のユーザー ID およびパスワード
- SMTP 認証に使用するユーザー ID およびパスワード

SMTP 認証ユーザーのアカウントを Device Manager に登録するには：

1. 次のコマンドを実行します。

Windows の場合：

```
< Device Manager サーバのインストールフォルダ > %HiCommandServer%\tools  
%Hdvmmodmailuser.bat -u < Device Manager のユーザー ID > -p < Device  
Manager のパスワード > < SMTP 認証ユーザー ID > [< SMTP 認証パスワード >]
```

Solaris または Linux の場合：

```
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/tools/  
hdvmmodmailuser.sh -u < Device Manager のユーザー ID > -p < Device  
Manager のパスワード > < SMTP 認証ユーザー ID > [< SMTP 認証パスワード >]
```

2. Hitachi Command Suite 製品のサービスを再起動します。



注意

- Device Manager サーバで SMTP 認証の設定を有効にしても、SMTP 認証ユーザーを登録していない場合、SMTP 認証を使用しないで、メールが送信されます。
 - Device Manager サーバに設定できる SMTP 認証ユーザーは、1 つだけです。コマンドを実行するたびに、設定されている SMTP 認証ユーザーの情報は更新されます。
 - Device Manager サーバで設定した SMTP 認証ユーザーの情報は削除できません。
-

関連項目

- [9.2 サービスの起動](#)
- [9.3 サービスの停止](#)
- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.2.21 server.mail.smtp.auth](#)

(5) アラート通知テンプレートのカスタマイズ

E メールの内容は、テンプレートファイル (mail-alert-detection.txt) で変更できます。テンプレートファイルを変更したあとは、Hitachi Command Suite 製品のサービスを再起動してください。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

次の場所に格納されているテンプレートファイル (mail-alert-detection.txt) を、テキストエディターで編集します。

Windows の場合：

```
< Device Manager サーバのインストールフォルダ > %HiCommandServer%\config
```

Solaris または Linux の場合：

< Device Manager サーバのインストールディレクトリ >/HiCommandServer/config

デフォルトの mail-alert-detection.txt ファイルを次に示します。

```
Subject:[DVM] Alert Notification
The following alert occurred.

MessageID: ${messageID}
Alert Type: ${alertType}
Source: ${source}
Status: ${status}
Component: ${component}
Description: ${description}
Recommended Action: ${recommendedAction}
Additional Info: ${additionalInfo}
Occurrence Time: ${occurrenceTime}

This message was sent automatically by the Device Manager server.
```

ヘッダー
空行
パラメーター
(出力有無を変更できる)

mail-alert-detection.txt ファイルは、次に示す条件をすべて満たすようにしてください。条件を満たさない場合、デフォルトの設定内容で E メールが送信されます。

- ファイル名およびファイルの格納先は変更しないでください。
- 1 行目にヘッダー、2 行目に空行、3 行目以降に本文および出力するパラメーターを指定してください。
- ヘッダーは「Subject:<メールの件名>」の形式で 1 つだけ指定してください。
- パラメーターは「\${<パラメーター名>）」の形式で指定してください。
パラメーター名は大文字と小文字が区別されます。
- UTF-8 エンコーディングで記述してください。
- ファイルサイズは 64KB 以内になるようにしてください。
- 各行の長さは改行文字を除いて 1024 バイト以内になるようにしてください。

mail-alert-detection.txt ファイルに指定できるパラメーターを次の表に示します。

表 6-12 mail-alert-detection.txt ファイルに指定できるパラメーター

パラメーター名	説明
messageID	アラート ID
alertType	アラートタイプ
source	ストレージシステム名
status	アラートの重要度
component	アラートが発生したストレージシステムの部位
description	問題の説明
recommendedAction	問題への対処方法
additionalInfo	補足情報
occurrenceTime	Device Manager サーバがアラート情報を取得した時刻 表示形式 : yyyy/mm/dd hh:mm:ss hh は 24 時間表示です。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

6.4 SNMP トラップをログファイルに出力するための設定

Device Manager では、ネットワーク上の機器で発生した SNMP トラップを受信し、ログファイルに出力します。Device Manager の管理対象のストレージシステムだけでなく、管理対象外の機器の SNMP トラップ (SNMP version1 限定) もログファイルに出力できます。

受信した SNMP トラップは、次のログファイルに出力されます。

- イベントログまたは syslog
- Hitachi Command Suite 共通トレースログファイル (hntr2n.log)
- Device Manager トレースログファイル (HDvMtracen.log)
- トレースログファイル (trace.log)
- エラーログファイル (error.log) ※

注※

重要度が、Error, Critical または Alert の場合だけ出力されます。SNMP トラップの重要度は、customizedsnmptrap.properties ファイルの customizedsnmptrap.customizelist プロパティに指定します。

SNMP トラップの情報のうち、ログファイルには次の情報が出力されます。

- トラップが受信されたことを示すメッセージ ID (プレフィックス : KAID)
- 送信元 (agent)
- Enterprise ID (enterprise)
- 一般トラップ番号 (generic)
- 固有トラップ番号 (specific)

JP1/IM などの統合管理ソフトウェアと連携すると、Device Manager で管理するストレージリソースも含めたネットワークリソース全体の稼働状況を一元的に監視できます。

関連項目

- [6.4.1 SNMP トラップをログファイルに出力するための設定](#)
- [6.6 JP1/IM でログを参照するために必要な設定](#)
- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.9.2 customizedsnmptrap.customizelist](#)

6.4.1 SNMP トラップをログファイルに出力するための設定

SNMP トラップを Device Manager で受信し、ログファイルに出力するためには、次の設定が必要です。

- Device Manager で SNMP トラップを受信するための設定※
 - 管理サーバの 162/udp ポートを Device Manager で使えるようにする
 - Device Manager サーバの server.dispatcher.daemon.receiveTrap プロパティに true を設定する
- SNMP トラップを Device Manager に通知するための設定※
 - SNMP 関連ソフトウェアで、トラップの通知対象マシンに管理サーバの情報を登録する
例えば、ストレージシステムの SNMP トラップを受信するためには、SNMP Agent での設定が必要です。

- SNMP トラップをログファイルに出力するための設定
 - `customizedsnmptrap.customizedSNMPTrapEnable` プロパティに `true` を設定する
 - `customizedsnmptrap.customizelist` プロパティにログファイルへの出力内容を設定する

注※ この設定は、SNMP トラップをアラートとして Device Manager GUI/CLI に表示する設定と同じです。

上記の設定が完了すると、Device Manager サーバは、すべてのコミュニティの SNMP トラップを受信してログファイルに出力します。

関連項目

- A.1.1 Device Manager サーバのプロパティの変更
- A.5.5 `server.dispatcher.daemon.receiveTrap`
- A.9.1 `customizedsnmptrap.customizedSNMPTrapEnable`
- A.9.2 `customizedsnmptrap.customizelist`

6.5 イベント通知を使用するために必要な設定

Tiered Storage Manager では、マイグレーションやシュレディングのタスク終了などユーザー操作とは異なるタイミングで発生する事象（イベント）の実行結果をメールでユーザーに通知できます。メールで通知できるイベントを次の表に示します。

表 6-13 メールで通知できる Tiered Storage Manager のイベント

イベント	説明
マイグレーションタスク終了	マイグレーションタスクの成功終了、失敗終了、または中止終了時に発生するイベント
シュレディングタスク終了	Tiered Storage Manager CLI で作成したシュレディングタスクの成功終了、失敗終了、または中止終了時に発生するイベント
ロックタスク終了	Tiered Storage Manager CLI で作成したロックタスクの成功終了、失敗終了、または中止終了時に発生するイベント
アンロックタスク終了	Tiered Storage Manager CLI で作成したアンロックタスクの成功終了、失敗終了、または中止終了時に発生するイベント
ボリュームロック期限満了	Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI で作成したマイグレーショングループに含まれるボリュームの、ボリュームロック期限が満了したときに発生するイベント
指定期間経過	Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI で作成したマイグレーショングループに対してユーザーが任意の期間（GUI：日付指定、CLI：日数指定）を設定し、その期間が経過したときに発生するイベント

通知先のメールアドレスの設定によって、通知対象となるイベントの範囲が次のように異なります。

- タスク作成時に設定する
GUI または CLI でマイグレーションやシュレディングなどのタスクを作成する際にメールアドレスを設定しておく、そのタスクの実行結果がユーザーに通知されるようになります。
- `server.properties` ファイルに設定する

server.properties ファイルの server.eventNotification.mail.to プロパティにメールアドレスを設定しておく、Tiered Storage Manager に関する全イベントの実行結果がユーザーに通知されるようになります。

- マイグレーショングループ作成時に設定する
Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI でマイグレーショングループを作成する際にメールアドレスを設定しておく、そのマイグレーショングループに関する全イベントの実行結果がユーザーに通知されるようになります。

それぞれの設定は独立しています。例えば、server.properties ファイルおよびマイグレーションタスク作成時に同一のメールアドレスを設定した場合、マイグレーションタスクが終了した際には、同じ内容のメールが 2 通送信されます。

6.5.1 イベント通知のためのプロパティの設定

Tiered Storage Manager に関するイベントの実行結果がメール通知されるようにするためには、Device Manager サーバの server.properties ファイルの次のプロパティに SMTP サーバの情報や通知元のメールアドレスなどを設定します。

- server.mail.enabled
- server.mail.from
- server.mail.smtp.host
- server.mail.smtp.port
- server.mail.smtp.auth
- server.mail.errorsTo
- server.eventNotification.mail.to



参考 Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI で実行したタスクについて通知する場合、Tiered Storage Manager サーバの server.properties ファイルにある次のプロパティに設定が必要です。

- server.mail.from
- server.mail.smtp.host
- server.mail.smtp.port
- server.mail.smtp.auth
- server.mail.errorsTo
- server.eventNotification.mail.to
- server.eventMonitoringIntervalInMinute

6.5.2 イベント通知テンプレートの編集

ユーザーにメールで通知する内容は、テンプレートファイルに設定されています。必要に応じてテンプレートファイルを編集し、項目の通知有無を変更できます。

テンプレートファイルは、イベントごとにあります。イベント別のテンプレートファイルを次の表に示します。

表 6-14 イベント通知メールのテンプレート

分類	イベント名	テンプレートファイル名
タスク終了	マイグレーションタスク終了	• [データマイグレーション] ウィザードで作成するマイグレーションタスクの場合※1 Windows の場合 :

分類	イベント名	テンプレートファイル名
		<p>< <i>Device Manager</i> サーバのインストールフォルダ>%HiCommandServer%config %mail-migrationtask-end.txt</p> <p>Solaris または Linux の場合： < <i>Device Manager</i> サーバのインストールディレクトリ>/HiCommandServer/ config/mail-migrationtask-end.txt</p> <ul style="list-style-type: none"> • Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI で作成するマイグレーションタスクの場合※2 <p>Windows の場合： < <i>Tiered Storage Manager</i> サーバのインストールフォルダ>%conf%mail- migrationtask-end.txt</p> <p>Solaris または Linux の場合： < <i>Tiered Storage Manager</i> サーバのインストールディレクトリ>/conf/mail- migrationtask-end.txt</p>
	シュレディングタスク終了※2	<ul style="list-style-type: none"> • Windows の場合： < <i>Tiered Storage Manager</i> サーバのインストールフォルダ>%conf%mail- shreddingtask-end.txt • Solaris または Linux の場合： < <i>Tiered Storage Manager</i> サーバのインストールディレクトリ>/conf/mail- shreddingtask-end.txt
	ロッキングタスク終了※2	<ul style="list-style-type: none"> • Windows の場合： < <i>Tiered Storage Manager</i> サーバのインストールフォルダ>%conf%mail- lockingtask-end.txt • Solaris または Linux の場合： < <i>Tiered Storage Manager</i> サーバのインストールディレクトリ>/conf/mail- lockingtask-end.txt
	アンロッキングタスク終了※2	<ul style="list-style-type: none"> • Windows の場合： < <i>Tiered Storage Manager</i> サーバのインストールフォルダ>%conf%mail- unlockingtask-end.txt • Solaris または Linux の場合： < <i>Tiered Storage Manager</i> サーバのインストールディレクトリ>/conf/mail- unlockingtask-end.txt
時間経過	ボリュームロック期限満了※2	<ul style="list-style-type: none"> • Windows の場合： < <i>Tiered Storage Manager</i> サーバのインストールフォルダ>%conf%mail-retention- term-expired.txt • Solaris または Linux の場合： < <i>Tiered Storage Manager</i> サーバのインストールディレクトリ>/conf/mail- retention-term-expired.txt
	指定期間経過※2	<ul style="list-style-type: none"> • Windows の場合： < <i>Tiered Storage Manager</i> サーバのインストールフォルダ>%conf%mail- migrationgroup-reminder.txt • Solaris または Linux の場合：

分類	イベント名	テンプレートファイル名
		< Tiered Storage Manager サーバのインストールディレクトリ >/conf/mail-migrationgroup-reminder.txt

注※1

テンプレートファイルのひな形は次の場所に格納されています。

- Windows の場合 :
< Device Manager サーバのインストールフォルダ >¥HiCommandServer¥template
- Solaris または Linux の場合 :
< Device Manager サーバのインストールディレクトリ >/HiCommandServer/template

注※2

テンプレートファイルのひな形は次の場所に格納されています。

- Windows の場合 :
< Tiered Storage Manager サーバのインストールフォルダ >¥template
- Solaris または Linux の場合 :
< Tiered Storage Manager サーバのインストールディレクトリ >/template

テンプレートに、イベントの種類に応じたパラメーターを指定することで、イベントの情報をメールに埋め込みます。

マイグレーションタスク終了のテンプレート (mail-migrationtask-end.txt) を例に、記述方法を次に示します。

```

Subject:[TSM] A migration task has finished. {Task : ${task}}
-----
The following migration task has finished:

Task : ${ task }
Task Type : ${ taskType }
Status : ${ status }
Description : ${ description }
User : ${ user }
Scheduled Time : ${ scheduledTime }
Completed Time : ${ completedTime }
Storage System : ${ storageSystem }
Migration Source (Host) : ${ migrationSourceHost }
Migration Source (LG) : ${ migrationSourceLG }
Migration Source (Pool) : ${ migrationSourcePool }
Migration Target (Tier) : ${ migrationTargetTier }
Migration Target (Pool) : ${ migrationTargetPool }
Advanced Option : ${ options }
Migrated Volumes : ${ migratedVolumes }

This message was sent automatically by the Tiered Storage Manager.

```

ヘッダー
空行

パラメーター
(出力有無を変更できる)

テンプレートファイルは、次に示す条件をすべて満たすように設定してください。

- 1行目にはヘッダー、2行目には空行を指定し、3行目以降に本文を指定してください。
- ヘッダーは「Subject:<メールの件名>」の形式で1つだけ指定してください。
- パラメーターは「\${<パラメーター名>}」の形式で指定してください。
- テンプレートファイルは、UTF-8エンコーディングで記述してください。
- テンプレートファイルのサイズは、64KB以内になるようにしてください。

- ・ テンプレートファイルの各行の長さは、改行文字を除いて 1024 バイト以内になるようにしてください。



重要 このテンプレートファイルの変更を有効にするには、Hitachi Command Suite 製品のサービスを再起動してください。

テンプレートに設定できるパラメーターは、イベントによって異なります。それぞれのパラメーターを「表 6-15 タスク終了イベントのパラメーター（[データマイグレーション] ウィザードで作成するマイグレーションタスク）」から「表 6-17 時間経過イベントのパラメーター」に示します。

表 6-15 タスク終了イベントのパラメーター（[データマイグレーション] ウィザードで作成するマイグレーションタスク）

パラメーター名	説明
task	タスク名
taskType	タスクの種類
status	タスクの状態
description	タスクの説明
user	タスク作成者のユーザ ID
scheduledTime	タスクの実行要求日時
completedTime	タスクの実行終了日時
storageSystem	ストレージシステム名
migrationSourceHost	マイグレーションソース：Host
migrationSourceLG	マイグレーションソース：Logical Group
migrationSourcePool	マイグレーションソース：Pool
migrationTargetTier	マイグレーションターゲット：Tier
migrationTargetPool	マイグレーションターゲット：Pool
options	オプション
migratedVolumes	マイグレーションされたボリュームの デバイス番号

表 6-16 タスク終了イベントのパラメーター（Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI で作成するタスク）

パラメーター名	説明
taskId	タスク ID
taskType	タスクの種類
taskStatus	タスクの状態
taskOwner	タスク作成者のユーザー ID
executionRequestTime	タスクの実行要求日時
endTime	タスクの実行終了日時
storageDomainName	ストレージドメイン名
migrationGroupName	マイグレーショングループ名
previousTargetStorageTierName	前回のマイグレーションの移動先ストレージ階層名
targetStorageTierName	移動先ストレージ階層名
eraseData	マイグレーション後のデータ消去有無
migratedVolumes	マイグレーションおよびデータ消去されたボリュームのデバイス番号

パラメーター名	説明
shreddingMethod	シュレディング方式
shreddedVolumes	シュレディングされたボリュームのデバイス番号
guardMode	ロックモード
retentionDays	保持期間（日数）
lockedVolumes	ロックされたボリュームのデバイス番号
unlockedVolumes	アンロックされたボリュームのデバイス番号
moveToMigrationGroupName	タスク完了後の移動先マイグレーショングループ名

表 6-17 時間経過イベントのパラメーター

パラメーター名	説明
storageDomainName	ストレージドメイン名
migrationGroupName	マイグレーショングループ名
expiredVolumes	期限が切れたボリュームのデバイス番号
remindAt	期間経過イベント発生予定日時
reminderDescription	期間経過イベント発生時の説明文

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止
- 各イベントのパラメーターの詳細について：マニュアル「*Hitachi Command Suite Tiered Storage Manager Software CLI リファレンスガイド*」

6.5.3 SMTP 認証ユーザーの設定

イベント通知機能を使用する場合、SMTP サーバに接続します。接続時に SMTP 認証を使用する場合は、`hdvmmmodmailuser` コマンドで **Device Manager** サーバに認証用のユーザーアカウントを設定する必要があります。



参考 Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI で実行したタスクについて通知する場合、`htsmmodmailuser` コマンドで Tiered Storage Manager サーバに認証用のユーザーアカウントを設定する必要があります。

(1) `hdvmmmodmailuser` コマンド

`hdvmmmodmailuser` コマンドを使用した SMTP 認証ユーザーの設定は、アラートおよびヘルスチェック結果の E メール通知と同じです。アラートまたはヘルスチェック結果の E メール通知で SMTP 認証ユーザーを設定した場合は、ここでの設定は不要です。

`hdvmmmodmailuser` コマンドの記述形式を次に示します。

形式

Windows の場合：

```
< Device Manager サーバのインストールフォルダ > %HiCommandServer%tools
%hdvmmmodmailuser.bat -u < Device Manager のユーザー ID > -p < Device Manager
のパスワード > < SMTP 認証ユーザー ID > [< SMTP 認証パスワード >]
```

Solaris または Linux の場合：

< *Device Manager* サーバのインストールディレクトリ > /HiCommandServer/tools/
hdvmmmodmailuser.sh -u < *Device Manager* のユーザー ID > -p < *Device Manager*
のパスワード > < *SMTP* 認証ユーザー ID > [< *SMTP* 認証パスワード >]

オプション

-u < *Device Manager* のユーザー ID >

リソースグループとして All Resources が割り当てられ、*Device Manager* のロールとして Admin が設定されているユーザー ID を指定してください。

-p < *Device Manager* のパスワード >

u オプションに指定した < *Device Manager* のユーザー ID > で *Device Manager* にログインするときのパスワードを指定してください。

< *SMTP* 認証ユーザー ID >

SMTP 認証に使用するユーザー ID を指定してください。

< *SMTP* 認証パスワード >

SMTP サーバにログインするときのパスワードを指定してください。



注意

- *Device Manager* サーバで *SMTP* 認証の設定を有効にしても、*SMTP* 認証ユーザーを登録していない場合、*SMTP* 認証を使用しないで、メールが送信されます。
- *Device Manager* サーバに設定できる *SMTP* 認証ユーザーは、1 つだけです。コマンドを実行するたびに、設定されている *SMTP* 認証ユーザーの情報は更新されます。
- *Device Manager* サーバで設定した *SMTP* 認証ユーザーの情報は削除できません。

なお、hdvmmmodmailuser コマンドで設定した内容を有効にするためには、hdvmmmodmailuser コマンドを実行したあと、Hitachi Command Suite 製品のサービスを再起動する必要があります。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

(2) htssmodmailuser コマンド

htssmodmailuser コマンドは、次の場所に移動してから実行してください。

- Windows の場合：

< *Tiered Storage Manager* サーバのインストールフォルダ > %bin

- Solaris または Linux の場合：

< *Tiered Storage Manager* サーバのインストールディレクトリ > /bin

htssmodmailuser コマンドの記述形式を次に示します。

形式

htssmodmailuser -u < *Tiered Storage Manager* のユーザー ID > -p < *Tiered Storage Manager* のパスワード > < *SMTP* 認証ユーザー ID > < *SMTP* 認証パスワード >

オプション

-u < *Tiered Storage Manager* のユーザー ID >

Device Manager のリソースグループとして All Resources が割り当てられ、*Tiered Storage Manager* の Admin 権限を持つユーザー ID を指定してください。

-p < *Tiered Storage Manager* のパスワード >
u オプションに指定した < *Tiered Storage Manager* のユーザー ID > で Tiered Storage Manager にログインするときのパスワードを指定してください。

< *SMTP 認証* ユーザー ID >

SMTP 認証に使用するユーザー ID を指定してください。

< *SMTP 認証* パスワード >

SMTP サーバにログインするときのパスワードを指定してください。

なお、htsmmodmailuser コマンドで設定した内容を有効にするためには、htsmmodmailuser コマンドを実行したあと、Hitachi Command Suite 製品のサービスを再起動する必要があります。



注意 次の両方の条件に当てはまる場合、tcsh または bash などの 257 バイト以上のコマンドが入力できるシェルから実行してください。

- Solaris または Linux 上で稼働している Tiered Storage Manager から htsmmodmailuser コマンドを実行する
- コマンド長が 256 バイトを超える

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

6.6 JP1/IM でログを参照するために必要な設定

Hitachi Command Suite 製品では、Windows、Solaris (SPARC) および Red Hat Enterprise Linux の場合だけ、JP1/IM との連携をサポートしています。

Device Manager と Tiered Storage Manager では、管理サーバのイベントログ (Windows の場合) または syslog (Solaris または Linux の場合) に出力されたログ情報を JP1/IM の統合コンソールで参照できます。

6.6.1 管理サーバが Windows の場合

管理サーバが Windows の場合のセットアップ手順は次のとおりです。各製品での手順の詳細については、JP1/IM および JP1/Base のマニュアルを参照してください。

1. 管理クライアントに JP1/IM - View をインストールしてください。
2. 管理サーバに JP1/Base と JP1/IM - Manager をインストールしてください。
3. JP1/Base の環境設定をしてください。
4. イベントログに出力された情報のうち、どのログを JP1/IM の統合コンソールに通知するかを JP1/Base の動作定義ファイル (nthevent.conf) に設定します。

JP1/Base の動作定義ファイルは次の場所に格納してください。

< *JP1/Base* のインストールフォルダ > %conf%\event\nthevent.conf

- Device Manager の場合

Device Manager が出力するすべてのログを JP1/IM の統合コンソールに通知する場合、nthevent.conf ファイルに次の内容を追加してください。

```
filter "Application"
  message '.*KAID.*'
end-filter
```

- Tiered Storage Manager の場合

Tiered Storage Manager が出力するすべてのログを JP1/IM の統合コンソールに通知する場合、nvent.conf ファイルに次の内容を追加してください。

```
filter "Application"
  message '.*KATS.*'
end-filter
```

5. JP1/Base EventlogTrap サービスを起動してください。

6.6.2 管理サーバが Solaris または Red Hat Enterprise Linux の場合

管理サーバが Solaris または Red Hat Enterprise Linux の場合のセットアップ手順は次のとおりです。各製品での手順の詳細については、JP1/IM および JP1/Base のマニュアルを参照してください。

1. 管理クライアントに JP1/IM - View をインストールしてください。
2. 管理サーバに JP1/Base と JP1/IM - Manager をインストールしてください。
3. JP1/Base の環境設定をしてください。
4. syslog ファイルに出力された情報のうち、どのログを JP1/IM の統合コンソールに通知するかを JP1/Base の動作定義ファイル (jevlog.conf) に設定します。

動作定義ファイルは次の場所に格納してください。

/etc/opt/jplbase/conf/jevlog.conf



重要

- syslog ファイルのデフォルトは、Solaris の場合は /var/adm/messages、Red Hat Enterprise Linux の場合は /var/log/messages です。
- 動作定義ファイルの名称を jevlog.conf 以外に変更することはできますが、その場合、jevlogstart コマンドでファイル名を指定する必要があります。詳細については、JP1/Base のマニュアルを参照してください。

動作定義ファイルの作成例を次に示します。

- Device Manager の場合 (Solaris)

```
FILETYPE =SEQ
RECTYPE =VAR '%n'
ACTDEF =<Error>0      ".*KAID.*-E"
ACTDEF =<Warning>0    ".*KAID.*-W"
ACTDEF =<Information>0 ".*KAID.*-I"
```

- Device Manager の場合 (Red Hat Enterprise Linux)

```
FILETYPE =SEQ2
ACTDEF =<Error>0 "KAID.*-E"
ACTDEF =<Warning>0 "KAID.*-W"
ACTDEF =<Information>0 "KAID.*-I"
```

- Tiered Storage Manager の場合 (Solaris)

```
FILETYPE =SEQ
RECTYPE =VAR '%n'
ACTDEF =<Error>0 ".*KATS.*-E"
ACTDEF =<Warning>0 ".*KATS.*-W"
ACTDEF =<Information>0 ".*KATS.*-I"
```

- Tiered Storage Manager の場合 (Red Hat Enterprise Linux)

```
FILETYPE =SEQ2
ACTDEF =<Error>0 ".*KATS.*-E"
ACTDEF =<Warning>0 ".*KATS.*-W"
ACTDEF =<Information>0 ".*KATS.*-I"
```

<Error>, <Warning>, <Information>の横の数字は JP1/IM に通知する際のイベント ID を指定します。指定できる範囲については、JP1/Base のマニュアルを参照してください。

5. jevlogstart コマンドを実行して、ログファイルトラップを起動してください。
Red Hat Enterprise Linux で jevlogstart コマンドを実行したとき、標準出力に表示された ID を控えておいてください。ログファイルトラップ機能を停止するために、その ID を指定する必要があります。

(例)

```
# /opt/jplbase/bin/jevlogstart <syslog ファイル>
```



重要 ログファイルトラップを停止するには、jevlogstop コマンドを使用します。

CIM/WBEM のセットアップ

この章では、Device Manager の CIM/WBEM 機能のセットアップについて説明します。

- 7.1 CIM/WBEM とは
- 7.2 Device Manager の CIM/WBEM 機能
- 7.3 ネームスペースの指定方法
- 7.4 CIM/WBEM 機能を使用するためのユーザーアカウント
- 7.5 CIM/WBEM 機能を利用するための設定
- 7.6 CIM/WBEM 機能でストレージシステムの性能情報を取得するための設定
- 7.7 SLP サービスの制御

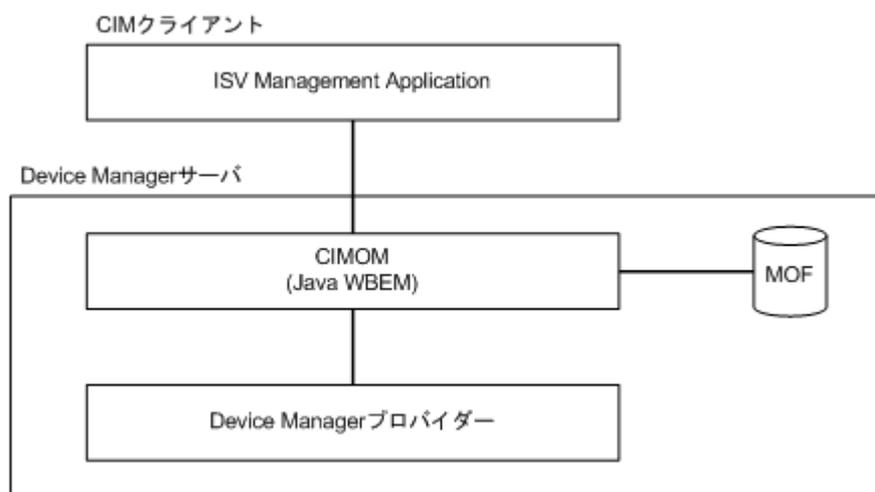
7.1 CIM/WBEM とは

Device Manager は、標準化団体 DMTF が定義した CIM および WBEM をサポートしています。CIM とは、ネットワーク環境にあるシステムを管理するための手法です。また、WBEM とは、ネットワークに接続されたホストやストレージシステムをはじめとした各種機器を、インターネットを通じて管理するための標準規格です。

Device Manager が使用する CIM モデルは、SNIA が提唱する SMI-S 仕様に準拠していて、SNIA-CTP に適合しています。CIM/WBEM 機能を使用すると、ベンダー、OS、プロトコルなどの環境の違いを意識しない標準的な手法で、ストレージシステムの構成や状態を管理できます。

Device Manager サーバの CIM モデルは、Device Manager が使用する MOF ファイルに定義されています。

図 7-1 Device Manager の CIM コンポーネント



CIM の関連情報は、次の URL で入手できます。

<http://www.dmtf.org/>

SMI-S の関連情報は、次の URL で入手できます。

<http://www.snia.org/>

7.2 Device Manager の CIM/WBEM 機能

Device Manager の CIM/WBEM を使用すると、SMI-S で規定された次の機能を利用できます。

オブジェクト操作機能

Device Manager が準拠している SMI-S の仕様では、ストレージネットワークを構成するストレージシステム、仮想ストレージシステム、スイッチ、ホストなどの機器に対するインターフェースが規定されています。各機器を管理する上で管理サービスが提供する必要がある機能は、機器ごとにプロファイルとしてまとめられています。

Device Manager の CIM/WBEM 機能が対象とするプロファイルは、Array プロファイルとそのサブプロファイルです。Array プロファイルには、ストレージシステムに対するインターフェースが規定されています。

インディケーション通知機能

インディケーションは、CIM で定義されるイベント通知機能です。CIM サーバで発生したイベント（CIM インスタンスの生成や削除など）の情報を示すインディケーションインスタンス

を、CIM クライアントに通知します。インディケーションの通知を受けるには、事前にインディケーションの送信先と送信条件を CIM サーバに登録する必要があります。登録方法については、SNIA のウェブサイトを参照してください。

Device Manager では、次に示すイベントの発生を通知します。

- ボリュームの作成
- ボリュームの削除
- LUN パスの割り当て
- LUN パスの解除

サービスディスカバリー機能

Device Manager では、SLP (Service Location Protocol) を用いたサービスディスカバリー機能を提供します。

SLP は、IETF で標準化が進められているプロトコルで、ネットワーク上で提供されているサービスを発見する仕組みを提供します。SLP については、RFC2608 を参照してください。

SLP のクライアントはサービスの種類を指定するだけで、利用できるサービスのアクセス情報 (URL など) やサービスの属性についての情報を取得できます。

Device Manager では、Device Manager サーバが SLP を用いて WBEM サービスの情報を通知します。

性能情報取得機能

Device Manager では、ストレージシステムの性能情報として、次の情報を取得します。

- ポートに関する情報
 - 総 I/O 数
 - データ転送量
- ボリュームに関する情報
 - 総 I/O 数
 - データ転送量
 - 読み込み I/O 数
 - キャッシュヒットした読み込み I/O 数
 - 書き込み I/O 数
 - キャッシュヒットした書き込み I/O 数

7.3 ネームスペースの指定方法

Device Manager では、バージョン 1.1.0~1.5.0 の SMI-S に対応しています。Device Manager (CIM サーバ) に接続するために必要なネームスペースを CIM クライアントで指定します。

ネームスペースは、次の形式で指定できます。

- SMI-S のバージョンを指定する。
root/smis/smisxx (xx はバージョン番号の略) を指定します。
例えば、バージョン 1.5.0 を指定する場合、root/smis/smis15 を指定します。
指定した SMI-S のバージョンに準拠したネームスペースのうち、最新のネームスペースが選択されます。
- 「最新」という条件で指定する。
root/smis/current を指定します。
最新のネームスペースが選択されます。

- interop を指定する。

SMI-S のバージョン 1.3.0 からは、ネームスペース interop をサポートします。ネームスペースに interop を指定すると、最新の管理サーバの情報を保持している Server プロファイルが指定されます。この Server プロファイルを経由して、各ベンダーのネームスペースにアクセスし、Array プロファイルおよびサブプロファイルの情報を取得します。

interop では、SMI-S のバージョン 1.3.0 以降に記載されている query だけを、CIM_IndicationFilter の Query プロパティに設定できます。



注意 05-80 以前のバージョンの Device Manager でサポートしていた dmxx (xx はバージョン番号の略) のネームスペースを指定する必要がある場合は、保守員に連絡してください。

表 7-1 ネームスペースおよび SMI-S のバージョンの対応

smisxx	ネームスペース		SMI-S のバージョン
	current	interop	
smis11	-	-	1.1.0
smis12	-	-	1.2.0
smis13	-	-	1.3.0
smis14	-	-	1.4.0
smis15	current	interop	1.5.0

(凡例) - : 該当なし

7.4 CIM/WBEM 機能を使用するためのユーザーアカウント

CIM/WBEM 機能を使用するユーザーには、All Resources を割り当てておく必要があります。また、Device Manager でのロールによって、実行できる CIM メソッドが異なります。

表 7-2 Device Manager でのロールと実行できる CIM メソッドの対応

Device Manager でのロール				CIM メソッド	
Admin	Modify	View	Peer	サービスメソッド	CIM オペレーション
●	●	●	-	○	○
-	●	●	-	○	○
-	-	●	-	×	○
-	-	-	●	×	○

(凡例)

- : ロールあり
- : ロールなし
- : CIM メソッドを実行できる
- × : CIM メソッドを実行できない

7.5 CIM/WBEM 機能を利用するための設定

Hitachi Command Suite の新規インストール時には、CIM/WBEM 機能は利用できる状態になっています。CIM/WBEM 機能を無効にしたあと、再度有効にするには、プロパティの変更やストレージシステムのリフレッシュが必要です。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン
- Device Manager へのストレージシステムの登録
ストレージシステムを登録する際には、分割ストレージ管理者ではなく、ストレージシステム全体の管理者のアカウントを使用してください。
- ポート番号の確認
Device Manager の CIM/WBEM 機能が使用するポート番号をほかのプログラムが使用していないか確認してください。同じポートを使用しているプログラムがある場合、どちらかのプログラムのポート番号を変更してください。
- CIMOM の停止 (Solaris の場合)
Solaris をインストールすると、CIMOM がシステムに組み込まれます。CIMOM が動作していると CIM/WBEM の起動に失敗することがあるため、次のコマンドを実行して停止してください。

```
# /etc/init.d/init.wbem stop
```


また、CIMOM が自動起動しないように inittab から削除してください。
- SLP デーモンのインストールの確認 (Solaris の場合)
pkginfo コマンドや Solaris の GUI を使って、SUNWslpr パッケージおよび SUNWslpu パッケージがインストールされていることを確認してください。
- 言語タグの設定 (サービスディスカバリー機能を使用する場合)
CIM クライアントで、言語タグを英語 (en) に設定してください。

CIM/WBEM 機能を利用するには :

1. Device Manager サーバの server.properties ファイルにある server.cim.support プロパティに、true を指定します。
2. 管理サーバの OS が Solaris の場合は、SLP デーモンの設定ファイルの名称を次のように変更して、システム起動時に SLP デーモンが自動的に起動するようにします。
変更前 : /etc/inet/slp.conf.example
変更後 : /etc/inet/slp.conf
そのあと、OS を再起動するか、SLP デーモンを起動してください。
3. Hitachi Command Suite 製品のサービスを再起動します。
Virtual Storage Platform, Universal Storage Platform V/VM または Hitachi USP に外部ストレージシステムが接続されている場合、Device Manager で管理している LDEV 数が多いと、サービスの起動処理に時間が掛かることがあります。
4. Device Manager GUI/CLI で、ストレージシステムをリフレッシュします。



注意

- CIM/WBEM 機能を無効にした状態でストレージシステムを削除した場合、手順 3 では、次の順序でサービスを再起動してください。
 1. server.properties ファイルの server.logicalview.initialsynchro プロパティを true に変更する。
 2. Hitachi Command Suite 製品のサービスを再起動する。
 3. server.properties ファイルの server.logicalview.initialsynchro プロパティを false に戻す。
- Device Manager GUI での設定操作で予約されたリソース (LDEV, パリティグループなど) に対して、CIM/WBEM 経由で操作を行った場合、設定が変更されたり、リソースが削除されたりすることがあります。

関連項目

- (2) Device Manager サーバで使用されるポート
- 7.7.2 SLP サービスの起動と停止
- 9.2 サービスの起動
- 9.3 サービスの停止
- A.2.10 server.cim.support
- A.2.16 server.logicalview.initialsynchro

7.5.1 CIM/WBEM 機能で使用するポートの変更

CIM/WBEM 機能で使用するポート番号を変更する場合は、Device Manager サーバのプロパティファイルを編集します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

ポートを変更するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. 次に示す Device Manager サーバのプロパティを編集して、ポート番号を設定します。
 - 非 SSL 通信の場合
server.properties ファイルの server.cim.http.port プロパティおよび cimxmlcpa.properties ファイルの HTTPPort プロパティ
 - SSL 通信の場合
server.properties ファイルの server.cim.https.port プロパティおよび cimxmlscpa.properties ファイルの HTTPSPort プロパティ
cimxmlscpa.properties ファイルには、必ず Ciphers プロパティも設定してください。
3. Hitachi Command Suite 製品のサービスを起動します。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止
- A.2.13 server.cim.http.port
- A.2.14 server.cim.https.port
- A.17.2 HTTPPort
- A.17.3 HTTPSPort

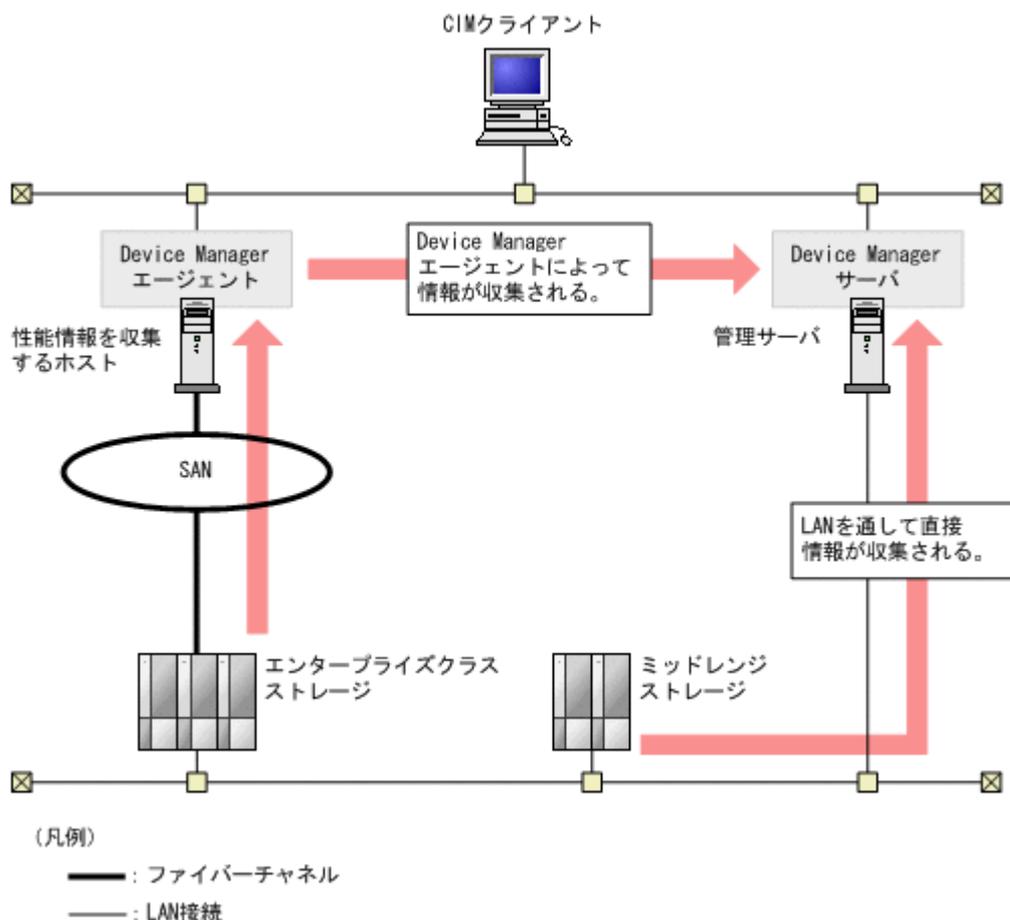
7.6 CIM/WBEM 機能でストレージシステムの性能情報を取得するための設定

ここでは、性能情報を取得するために必要なシステム構成および設定の手順について説明します。

7.6.1 CIM/WBEM 機能で性能情報を取得する場合のシステム構成

CIM/WBEM 機能で性能情報を取得する場合のシステム構成は、ストレージシステムの機種によって異なります。

図 7-2 ストレージシステムの性能情報を収集する場合のシステム構成例



ストレージシステム

性能情報の取得対象となるストレージシステムです。

エンタープライズクラスストレージ（Virtual Storage Platform, Universal Storage Platform V/VM または Hitachi USP）の性能情報は、ストレージシステム内のコマンドデバイスを利用して性能情報を収集するホスト（Device Manager エージェント）が情報を取得し、Device Manager サーバに通知します。

ミッドレンジストレージ（HUS100, Hitachi AMS2000, Hitachi SMS, Hitachi AMS/WMS または SANRISE9500V）の性能情報は、Device Manager サーバがストレージシステムから直接収集します。

性能情報を収集するホスト

エンタープライズクラスストレージ（Virtual Storage Platform, Universal Storage Platform V/VM または Hitachi USP）の性能情報を取得する場合に必要です。Virtual Storage Platform の場合はバージョン 7.0 以降、Universal Storage Platform V/VM または Hitachi USP の場合はバージョン 5.9 以降の Device Manager エージェントをインストールする必要があります。

性能情報を収集するホストは、管理サーバと同一マシンとする運用を推奨します。

性能情報を収集するホストを管理サーバとは別のマシンとする場合、性能情報を収集するホストとして利用できる OS は、Windows, Solaris, Linux だけです。HP-UX または AIX のホストでは性能情報を収集できません。

なお、Device Manager エージェントの `hdvmagt_setting` コマンドで一括管理構成の設定をしておくことを推奨します。

管理サーバ

バージョン 5.9 以降の Device Manager サーバがインストールされ、CIM/WBEM 機能が有効になっていることが必要です。

7.6.2 エンタープライズクラスストレージの性能情報を取得するための設定

エンタープライズクラスストレージ (Virtual Storage Platform, Universal Storage Platform V/VM または Hitachi USP) の性能情報を取得するための設定について説明します。

(1) ストレージシステムに必要な設定

各ストレージシステムにコマンドデバイスを用意し、性能情報を収集するホストに LUN パスを割り当てて、性能情報を収集するホストにコマンドデバイスを認識させます。

なお、Virtual Storage Platform または VP9500 の性能情報を収集する場合は、認証モードが無効になっているコマンドデバイスをホストに認識させてください。

(2) 性能情報を収集するホストに必要な設定

Device Manager エージェントをインストールし、コマンドデバイスを登録します。

性能情報を収集するには：

1. Device Manager エージェントおよび RAID Manager LIB をインストールします。

RAID Manager LIB は、Device Manager エージェントに同梱されています。ただし、ホストの OS が UNIX で、すでにホストに RAID Manager LIB がインストールされている場合、RAID Manager LIB は上書きされません。この場合は、次の表に示すバージョンの RAID Manager LIB をインストールしてください。

表 7-3 性能情報を収集する場合の RAID Manager LIB の前提バージョン

ストレージシステム	バージョン
Virtual Storage Platform	01-15-03/00 以降
VP9500	01.15.00 以降
Universal Storage Platform V/VM	01-12-03/03 以降
H20000/H24000	01.12.04 以降
Hitachi USP	01-12-03/03 以降
H10000/H12000	01.12.04 以降

2. Device Manager エージェントの `hdvmagt_setting` コマンドを実行して、一括管理構成の設定をします (推奨)。
3. `perf_findcmddev` コマンドを実行して、コマンドデバイスを登録します。



注意

- Device Manager エージェントをバージョン 6.3 以前から、バージョン 6.4 以降に更新インストールした場合、`perf_cmddev.properties` ファイルの設定は維持されます。SLPR 環境でストレージシステムを使用している場合は、更新インストール後に `perf_cmddev.properties` ファイルに定義された SLPR のコマンドデバイスの情報を更新してください。

- バージョン 6.3 以前の Device Manager エージェントを使用している場合、SLPR 環境でストレージシステムを使用するためには、perf_cmddev.properties ファイルを直接編集して SLPR のコマンドデバイスを定義してください。

関連項目

- (4) コマンドデバイスを登録する (perf_findcmddev コマンド)
- 11.3.4 Device Manager サーバの情報, HiScan コマンドの実行周期および RAID Manager または P9000 RAID Manager の情報の設定 (hdvmagt_setting コマンド)
- Device Manager エージェントのインストール方法: マニュアル「*Hitachi Command Suite Software* インストールガイド」

(3) Device Manager サーバで必要な設定

Device Manager サーバの server.properties ファイルにある server.cim.agent プロパティに、性能情報を収集するホスト (Device Manager エージェントをインストールしたマシン) のホスト名を指定します。



注意 server.cim.agent プロパティに設定したホスト名と、Device Manager に登録されているホスト名が一致していることを確認してください。一致していないと、性能情報を取得できません。

関連項目

- A.1.1 Device Manager サーバのプロパティの変更
- A.2.9 server.cim.agent

(4) コマンドデバイスを登録する (perf_findcmddev コマンド)

Device Manager エージェントでコマンドデバイスを登録するには、perf_findcmddev コマンドを実行します。コマンドデバイスを登録する場合は、write オプションを指定します。

事前に完了しておく操作

- Administrator 権限または root 権限のユーザーでのログイン

コマンドの形式

```
perf_findcmddev {write [-file <ファイル名>]|verify|view}
```

コマンドの格納先

Windows の場合:

```
< Device Manager エージェントのインストールフォルダ > \bin
```

Solaris または Linux の場合:

```
/opt/HDVM/HBaseAgent/bin
```

オプション

```
write [-file <ファイル名>]
```

ホストが認識しているすべてのコマンドデバイスの情報を、ファイルに出力します。

-file <ファイル名> を指定すると、コマンドデバイスの情報を、任意のファイルに出力します。ファイル名は絶対パスおよび相対パスで指定できます。-file <ファイル名> を指定しない場合、perf_cmddev.properties ファイルが上書きされます。

ホストが認識しているコマンドデバイスが検出されなかった場合、`perf_cmddev.properties` ファイルには、何も出力されません。

verify

`perf_cmddev.properties` ファイルで定義しているコマンドデバイスの情報と、ホストが認識しているコマンドデバイスの情報を照合します。ホストが複数のコマンドデバイスを認識している場合、各コマンドデバイスについて、実行結果を出力します。

- `perf_cmddev.properties` ファイルで定義済みのコマンドデバイスの情報と、ホストが認識しているコマンドデバイスの情報が一致している場合
The definition of the command device is valid.が表示されます。

- `perf_cmddev.properties` ファイルで定義済みのコマンドデバイスを、ホストが認識していない場合
メッセージ KAIC28615-W およびホストが認識していないコマンドデバイスの情報が出力されます。

- ホストが認識しているコマンドデバイスが、`perf_cmddev.properties` ファイルに定義されていない場合
メッセージ KAIC28616-W および定義されていないコマンドデバイスの情報を出力します。

なお、`perf_cmddev.properties` ファイルにバージョン 6.3 以前のフォーマットでコマンドデバイスの情報が定義されている場合、そのコマンドデバイスは SLPR0 に属していると見なされます。

view

`perf_cmddev.properties` ファイルに定義されているコマンドデバイスの情報を表示します。

`perf_cmddev.properties` ファイルに認識できない値が定義されている場合や、書式に従って定義されていない行では、UNKNOWN が表示されます。コメント行または空白行は表示しません。また、`perf_cmddev.properties` ファイルに値が定義されていない場合は、ヘッダーだけ表示されます。

出力例を次に示します。出力される内容は、`perf_cmddev.properties` ファイルの設定項目と同じです。

Raid ID	Serial#	SLPR#	LDEV#	Device	file name
R500	14050	0	345	¥¥.¥PhysicalDrive3	
R601	44332	1	456	¥¥.¥Volume{xxxxxxxx-xxxx-xxx-xxxxxxxx}	
R501	UNKNOWN	-	1045	¥¥.¥PhysicalDrive10	

関連項目

- (5) `perf_cmddev.properties` ファイルの形式

(5) `perf_cmddev.properties` ファイルの形式

`perf_cmddev.properties` ファイルを編集して、ストレージシステムのコマンドデバイスを定義できます。

`perf_cmddev.properties` ファイルの格納先

Windows の場合：

< *Device Manager* エージェントのインストールフォルダ > ¥mod¥hdvm¥config

Solaris または Linux の場合：

/opt/HDVM/HBaseAgent/mod/hdvm/config

perf_cmddev.properties ファイルの書式

次の書式で、1行に1つのコマンドデバイスを定義してください。

バージョン 6.4 以降の Device Manager エージェントを使用している場合：

```
< RAID ID > . < シリアル番号 > . [ < SLPR 番号 > . ] < LDEV 番号 > : < deviceFileName >
```

バージョン 6.3 以前の Device Manager エージェントを使用している場合：

```
< RAID ID > . < シリアル番号 > . < LDEV 番号 > : < deviceFileName >
```

表 7-4 perf_cmddev.properties ファイルの設定項目

設定項目	設定内容
< RAID ID >	次のどれかを指定します。 R700：Virtual Storage Platform または VP9500 の場合 R600：Universal Storage Platform V または H24000 の場合 R601：Universal Storage Platform VM または H20000 の場合 R500：Hitachi USP または H12000 の場合 R501：Hitachi NSC 55 または H10000 の場合
< シリアル番号 >	ストレージシステムのシリアル番号を 10 進数で指定します。
< SLPR 番号 >	コマンドデバイスが属する SLPR の番号を 10 進数で指定します。 SLPR を構築していない場合は 0 を指定してください。 この項目は省略できます。省略した場合（バージョン 6.3 以前の書式で定義した場合）は、SLPR を構築していないものと見なされます。
< LDEV 番号 >	コマンドデバイスの CU:LDEV 番号を 10 進数で指定します。
< deviceFileName >	ホストが認識しているコマンドデバイスの識別名（Physical Drive 番号、VolumeGUID、またはデバイスファイル名）を次の形式で指定します。* <ul style="list-style-type: none"> Windows の場合： ¥¥.¥PhysicalDrive ¥¥.¥Volume{ < GUID > } Solaris の場合： /dev/rdisk/cxtxdxs2 Linux の場合： /dev/sdx x は整数を示します。

注※

- Windows の PhysicalDrive 番号で指定した場合、または Linux の場合、OS の再起動によって PhysicalDrive 番号やデバイスファイル名が変更されることがあります。このため、OS の再起動後に、perf_findcmddev コマンドを実行して設定情報の確認、更新が必要です。Windows の場合は、VolumeGUID を指定すると、OS の再起動の影響を受けません。
- バージョン 6.3 以前の Device Manager エージェントを使用している場合、SLPR 環境ですべての SLPR の性能情報を取得するためには、perf_cmddev.properties ファイルに SLPR0 のコマンドデバイスを定義する必要があります。

同一ストレージシステム上のほかの SLPR のコマンドデバイスを複数定義する場合は、そのストレージシステムに関する定義の先頭行に SLPR0 のコマンドデバイスを定義してください。次の例では、Hitachi USP（シリアル番号：14050）の SLPR0 のコマンドデバイスとして、PhysicalDrive5（LDEV 番号：345）を定義しています。

```
R600.44332.456: ¥¥.¥PhysicalDrive3
R500.14050.345: ¥¥.¥PhysicalDrive5
R500.14050.346: ¥¥.¥PhysicalDrive6
R500.14050.347: ¥¥.¥PhysicalDrive10
R501.89832.780: ¥¥.¥PhysicalDrive15
```

7.6.3 ミッドレンジストレージの性能情報を取得するための設定

ミッドレンジストレージ (HUS100, Hitachi AMS2000, Hitachi SMS, Hitachi AMS/WMS または SANRISE9500V) の性能情報を取得するための設定について説明します。

(1) ストレージシステムに必要な設定

Device Manager GUI の Element Manager, Storage Navigator Modular または Storage Navigator Modular 2 で、性能統計情報を採取するための設定が必要です。

関連項目

- 性能統計情報採取の設定方法：各ストレージシステムのマニュアル

(2) 性能情報を取得するユーザーアカウントの登録 (hdvmodpolluser コマンド)

ストレージシステムで Account Authentication や Password Protection が有効になっている場合、性能情報取得中にストレージシステムがロックされ、ほかのユーザーがログインできなくなることがあります。Account Authentication が有効になっている場合は、性能情報取得用のユーザーアカウントをストレージシステムと Device Manager に登録すると、ストレージシステムをロックしないで性能情報を取得できます。

Device Manager に性能情報取得用のユーザーアカウントを登録するには、hdvmodpolluser コマンドを実行します。

Device Manager に登録できるユーザーアカウントは 1 つだけです。別のユーザーアカウントを指定して hdvmodpolluser コマンドを実行した場合は、以前の登録内容が上書きされます。

事前に完了しておく操作

- 参照権限だけを持つユーザーアカウントのストレージシステムへの登録
複数のストレージシステムの性能情報を取得する場合は、すべてのストレージシステムに同じユーザーアカウントを登録してください。

コマンドの形式

Windows の場合：

```
hdvmodpolluser { -u < Device Manager のユーザー ID > -p < Device Manager のパスワード > < 性能情報取得用のユーザー ID > < 性能情報取得用のパスワード > | -d }
```

Solaris の場合：

```
hdvmodpolluser.sh { -u < Device Manager のユーザー ID > -p < Device Manager のパスワード > < 性能情報取得用のユーザー ID > < 性能情報取得用のパスワード > | -d }
```

コマンドの格納先

Windows の場合：

```
< Device Manager サーバのインストールフォルダ > \HiCommandServer\tools
```

Solaris の場合：

```
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/tools
```

オプション

-u, -p

Device Manager のユーザー ID およびパスワードを指定します。指定するユーザーには、リソースグループとして All Resources が割り当てられ、Device Manager のロールとして Admin が設定されている必要があります。

<性能情報取得用のユーザー ID > , <性能情報取得用のパスワード>

ストレージシステムに登録した、参照権限だけを持つユーザーアカウントのユーザー ID およびパスワードを指定します。

-d

Device Manager に登録済みのユーザー情報を削除します。

7.7 SLP サービスの制御

サービスディスカバリー機能を使用する場合の SLP サービス（または SLP デーモン）の制御方法を説明します。なお、SLP サービス（または SLP デーモン）には、CIM/WBEM 機能で使用するポートがデフォルトで登録されます。

7.7.1 サービスディスカバリー機能を使用する場合の前提ソフトウェア

Windows または Red Hat Enterprise Linux の場合：

OpenSLP 1.0.11

OpenSLP は、Device Manager に同梱されているため、Device Manager をインストールすると、必要なファイルがコピーされます。OpenSLP の詳細については、OpenSLP のウェブサイト (<http://www.openslp.org/>) を参照してください。

Solaris の場合：

SUNWslpr パッケージおよび SUNWslpu パッケージ

Solaris をインストールすると、必要なパッケージがインストールされます。SUNWslpr パッケージおよび SUNWslpu パッケージの詳細については、Oracle 社のウェブサイト (<http://docs.sun.com/>) を参照してください。

SUSE Linux Enterprise Server の場合：

OpenSLP 1.2.0

OpenSLP は、SUSE Linux Enterprise Server システムに付属します。OpenSLP の詳細については、Novell 社のウェブサイト (<http://www.novell.com/>) を参照してください。

7.7.2 SLP サービスの起動と停止

ここでは、SLP サービス（または SLP デーモン）の起動および停止方法を説明します。

(1) SLP サービスの起動と停止 (Windows)

事前に完了しておく操作

- Administrator 権限でのログイン

SLP サービスの起動

次のどちらかを行ってください。

- [管理ツール] - [サービス] から、[Service Location Protocol] を選んで開始操作をする。

- コマンドプロンプトを起動して、OpenSLP の実行形式のファイルがあるフォルダに移動し、次のコマンドを実行する。

```
slpd -start
```

SLP サービスの停止

次のどちらかを行ってください。

- [管理ツール] - [サービス] から、[Service Location Protocol] を選んで停止操作をする。
- コマンドプロンプトを起動して、OpenSLP の実行形式のファイルがあるフォルダに移動し、次のコマンドを実行する。

```
slpd -stop
```

(2) SLP デーモンの起動と停止 (Solaris)

事前に完了しておく操作

- root 権限でのログイン

SLP デーモンの起動

次のコマンドを実行してください。

```
# /etc/init.d/slpd start
```

SLP デーモンの停止

次のコマンドを実行してください。

```
# /etc/init.d/slpd stop
```



注意 /etc/init.d/slpd stop コマンドを実行しても SLP デーモンが正常に停止しない場合は、次の手順を実行してください。

1. /etc/inet/slp.conf ファイルの名前を/etc/inet/slp.conf.example に戻す。
このとき、/etc/inet/slp.conf ファイルを残しておかないでください。
2. Solaris を再起動する。

(3) SLP デーモンの起動と停止 (Red Hat Enterprise Linux)

事前に完了しておく操作

- root 権限でのログイン

SLP デーモンの起動

次のコマンドを実行してください。

```
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/wsi/bin/  
slpd.sh start
```

SLP デーモンの停止

次のコマンドを実行してください。

```
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/wsi/bin/  
slpd.sh stop
```

(4) SLP デーモンの起動と停止 (SUSE Linux Enterprise Server)

事前に完了しておく操作

- root 権限でのログイン

SLP デーモンの起動

次のコマンドを実行してください。

```
# /usr/sbin/rcslpd start
```

SLP デーモンの停止

次のコマンドを実行してください。

```
# /usr/sbin/rcslpd stop
```

7.7.3 SLP サービスの解除

Hitachi Command Suite 製品のアンインストール時、SLP サービス (または SLP デーモン) の解除が必要になる場合があります。

次のようなメッセージが表示された場合、SLP サービスを手動で解除してください。

```
SLP サービスの解除に失敗しましたが、アンインストールを続行します。アンインストールしたあと、SLP サービスを解除してください。
```

```
Unable to release the SLP service, but the removal will continue. After the removal, release the SLP service.
```

(1) SLP サービスの解除 (Windows)

事前に完了しておく操作

- Administrator 権限でのログイン

SLP サービスを解除するには：

1. コマンドプロンプトを起動して、OpenSLP の実行形式のファイルがあるフォルダに移動します。
2. 次のコマンドを実行します。

```
slpd -remove
```

(2) SLP デーモンの解除 (Solaris)

事前に完了しておく操作

- root 権限でのログイン

SLP デーモンを解除するには：

1. 次のどちらかの方法を実行します。
 - /etc/init.d/slpd を削除する、またはリネームする。
 - /etc/inet/slp.conf を削除する、またはリネームする。

(3) SLP デーモンの解除 (Linux)

事前に完了しておく操作

- root 権限でのログイン

SLP デーモンを解除するには :

1. SLP デーモンを停止します。
2. /etc/init.d/slpd がある場合は、次のコマンドを実行して削除します。

```
# chkconfig --level 01345 slpd off
# chkconfig --del slpd
# rm -f /etc/init.d/slpd
```

7.7.4 OpenSLP のログに関する注意事項

SLP サービス (または SLP デーモン) のログ出力は単純増加のため、長期間運用するとディスクスペースを圧迫するおそれがあります。ログファイルを定期的にバックアップして、クリアしてください。デフォルトでは、SLP サービス (または SLP デーモン) の起動メッセージだけがログファイルに出力されます。

Windows の場合 :

`%WINDIR%slpd.log`

`%WINDIR%`には、Windows の環境変数 `WINDIR` (通常は、`C:\WINDOWS`) の値が入ります。

Linux の場合 :

< *Device Manager* サーバのインストールディレクトリ >/HiCommandServer/wsi/cfg/
slp.log

クラスタ環境でのセットアップ

Hitachi Command Suite 製品では、2 台の管理サーバを Active-standby 構成でクラスタリングできます。クラスタリングすることで Hitachi Command Suite 製品の可用性を向上できます。

ここでは、Hitachi Command Suite 製品をクラスタ環境で運用する場合のセットアップ方法について説明します。

- [8.1 管理サーバの環境の確認](#)
- [8.2 Windows でのセットアップ](#)
- [8.3 Solaris でのセットアップ](#)

8.1 管理サーバの環境の確認

管理サーバの環境によって、セットアップ方法が異なります。次の表を参照して、管理サーバの環境に応じたセットアップを開始してください。

表 8-1 管理サーバの環境ごとのセットアップ方法

管理サーバの環境		参照先	
		Windows	Solaris
管理サーバがクラスタ環境	Device Manager がインストールされていない	8.2.1	8.3.1
	Device Manager がインストールされている	8.2.2	8.3.2
管理サーバが非クラスタ環境	Device Manager がインストールされていない※	8.2.3	8.3.3
	Device Manager がインストールされている	8.2.3	8.3.3

注※

事前に Device Manager の新規インストールが必要です。

クラスタ環境をセットアップする際には、データベースの再作成およびバックアップをすることになります。管理サーバ上に次の空き容量があることを確認してください。

- データベースの再作成先に必要な空き容量：
< Hitachi Command Suite 共通コンポーネントのデータベース容量 > + < Device Manager サーバと同一ホストにインストールされている Device Manager サーバを含むすべての Hitachi Command Suite 製品のデータベース容量 >
- データベースのバックアップに必要な空き容量：
(< バックアップ対象となる Hitachi Command Suite 製品のデータベースサイズの総和 > + 1GB) × 2

Device Manager, Tiered Storage Manager, Replication Manager および Hitachi Command Suite 共通コンポーネントのデータベースの容量については、データベースファイルの格納先ディレクトリの容量をデータベースのサイズとしてください。ほかの Hitachi Command Suite 製品のデータベースの容量については、各製品のマニュアルを参照してください。



注意

- クラスタを構成するすべてのノードは、同じディスク構成にして、Hitachi Command Suite 製品のインストール先（ドライブ文字やパス名など）も同じにする必要があります。
- インストール後に、Hitachi Command Suite 製品の設定を変更する場合には、すべてのノードに同一の設定を実施してください。
- ここでは、クラスタ化するサービスの集まり（サービスのフェールオーバーの単位）をリソースグループと呼びます。

関連項目

- Hitachi Command Suite 製品のインストール方法：マニュアル「Hitachi Command Suite Software インストールガイド」

8.2 Windows でのセットアップ

ここでは、管理サーバの OS が Windows の場合に、Microsoft Cluster Service または Windows Server Failover Clustering を利用してクラスタ環境をセットアップする手順について説明します。

8.2.1 新規インストール (Windows)

ここでは、クラスタ構成の管理サーバに Hitachi Command Suite を新規インストールする方法を説明します。



注意 クラスタ環境のセットアップでは、Hitachi Command Suite のサービスの停止を伴う操作を実行します。セットアップ中は、Hitachi Command Suite にアクセスしないでください。

(1) 実行系ノードでの手順

実行系ノードに Hitachi Command Suite を新規インストールする場合の手順を次に示します。

1. クラスタ管理 IP アドレスと共有ディスクをオンラインにします。
2. ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、Hitachi Command Suite 製品のサービスおよびリソースグループをクラスタの管理対象から外します。



注意 次に示すリソースは管理対象から外さないでください。

- 共有ディスク
- クラスタ管理 IP アドレス
- 論理ホスト名

3. 実行系ノードに Hitachi Command Suite を新規インストールします。

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、次の条件に従ってください。

- 共有ディスクにアクセスできる状態にしたあとで、データベースの格納先に共有ディスク上のパスを指定する。
- 管理サーバの IP アドレスに論理ホスト名 (クラスタ管理 IP アドレスに割り当てられた仮想のホスト名) を指定する。

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されていない場合は、次の条件に従ってください。

- データベースの格納先に、ローカルディスク上のパスを指定する。
- 管理サーバの IP アドレスに、実行系ノードの IP アドレスを指定する。

4. 使用する製品のライセンスを GUI で登録します。

実行系ノードの IP アドレスにアクセスしてください。

インストールする製品ごとに、ライセンスキーの入力が必要です。

5. GUI を起動するための URL を論理ホスト名に変更します。

次のコマンドを実行して、論理ホスト名になっているかを確認します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdschgurl / print
```

論理ホスト名が指定されていない場合、次のコマンドを実行して URL を変更します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdschgurl / change http://<実行系ノードの IP アドレスまたはホスト名*>:<ポート番号> http://<論理ホスト名>:<ポート番号>
```

注※ インストール時に入力した値を指定します。

6. テキストエディターを使って、クラスタ設定ファイルを作成します。

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、この手順は不要です。

```
mode=online
virtualhost=<論理ホスト名>
onlinehost=<実行系ノードのホスト名>
standbyhost=<待機系ノードのホスト名>
```

作成したファイルは、cluster.conf というファイル名で、<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%conf に格納します。



注意

- mode には online を指定してください。
- virtualhost, onlinehost, standbyhost には IP アドレスは指定できません。ホスト名から IP アドレスの名前解決ができることを確認してください。
- virtualhost に指定する論理ホスト名には、有効でアクセスできる IP アドレスが割り当てられている必要があります。

7. server.properties ファイルを開き、server.http.host プロパティに論理ホスト名が指定されていることを確認します。

論理ホスト名が指定されていない場合は、論理ホスト名に変更してください。

```
<Device Manager サーバのインストールフォルダ>%HiCommandServer%config
%server.properties
```

8. データベースを共有ディスクに移行します。

その方法を手順 9～手順 11 で説明します。

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、データベースを共有ディスクに移行する手順は不要です。手順 12 に進んでください。

9. 次のコマンドを実行して、新規インストール後のデータベースをバックアップします。
障害が発生した場合に備えて、データベースをバックアップしておくことをお勧めします。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsbackups /dir <バックアップファイルの格納先フォルダ> /auto
```

dir

データベースのバックアップファイルを格納するローカルディスク上のフォルダを絶対パスで指定します。

dir オプションに指定するフォルダが空であることを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



重要 hcmdsbackups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先フォルダに database というフォルダが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

10. HiRDB が使用するポートをデフォルト (23032/tcp) 以外のポートに変更して運用している場合は、使用しているポート番号を控えておきます。

11. 次のコマンドを実行して、データベースを共有ディスクに移行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsdbclustersetup /createcluster /databasepath <データベースの再作成先
フォルダ> /exportpath <データベースの退避先フォルダ> /auto
```

createcluster

非クラスタ構成の Hitachi Command Suite 製品をクラスタ構成へ移行するためのオプションです。

databasepath

データベースの再作成先フォルダを指定します。共有ディスク上のフォルダを、63バイト以内の絶対パスで指定してください。

パスに使用できる文字を次に示します。そのほかに、円記号 (¥)、コロン (:) およびスラント (/) をパスの区切り文字として使用できます。

A~Z a~z 0~9 . _

exportpath

データベースの退避先フォルダを指定します。ローカルディスク上のフォルダを、63バイト以内の絶対パスで指定してください。パスに使用できる文字は、databasepathに指定できる文字と同じです。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



注意

- hcmdsdbclustersetup コマンドを実行すると、HiRDB が使用するポート番号の設定がデフォルト値 (23032/tcp) に戻ります。
- <データベースの退避先フォルダ>がすでにある場合は、フォルダの中を空にするか、フォルダを削除してください。
- hcmdsdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。
- hcmdsdbclustersetup コマンドが異常終了した状態でサーバを再起動すると、共有ディスクの接続先が待機系ノードに切り替わることがあります。

12. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスが停止していることを確認します。
13. [サービス] ウィンドウで次のプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service
 - HiCommandServer
 - HiCommand Tiered Storage Manager
14. クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスを登録しているリソースグループを選択し、右クリックメニューで待機系ノードに移動します。

関連項目

- 9.4 サービスの稼働状態の確認
- クラスタの管理対象から外す必要のあるサービスおよびリソースグループについて : 各 Hitachi Command Suite 製品のマニュアル
- Hitachi Command Suite のインストール方法 : マニュアル「*Hitachi Command Suite Software インストールガイド*」

(2) 待機系ノードでの手順

待機系ノードに Hitachi Command Suite を新規インストールする場合の手順を次に示します。

1. 待機系ノードに Hitachi Command Suite を新規インストールします。
インストールの際には、次の条件に従ってください。

- インストール先を実行系ノードと同じにしてください。
 - ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、管理サーバの IP アドレスに論理ホスト名（クラスタ管理 IP アドレスに割り当てられた仮想のホスト名）を指定してください。ほかの Hitachi Command Suite 製品でクラスタ環境が構築されていない場合は、待機系ノードの IP アドレスまたはホスト名を指定してください。
2. 使用する製品のライセンスを GUI で登録します。
待機系ノードの IP アドレスにアクセスしてください。
インストールする製品ごとに、ライセンスキーの入力が必要です。
 3. テキストエディターを使って、クラスタ設定ファイルを作成します。
ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、この手順は不要です。
クラスタ設定ファイルに指定する項目は次のとおりです。

```
mode=standby
virtualhost=<論理ホスト名>
onlinehost=<実行系ノードのホスト名>
standbyhost=<待機系ノードのホスト名>
```

作成したファイルは、cluster.conf というファイル名で、<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%conf に格納します。



注意

- mode には standby を指定してください。
- virtualhost, onlinehost, standbyhost には IP アドレスは指定できません。ホスト名から IP アドレスの名前解決ができることを確認してください。
- virtualhost に指定する論理ホスト名には、有効でアクセスできる IP アドレスが割り当てられている必要があります。

4. server.properties ファイルを開き、server.http.host プロパティに論理ホスト名が指定されていることを確認します。
論理ホスト名が指定されていない場合は、論理ホスト名に変更してください。
<Device Manager サーバのインストールフォルダ>%HiCommandServer%config
%server.properties
5. 共有ディスク上のデータベースを使用するように設定を変更します。
その方法を手順 6～手順 7 で説明します。
ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、共有ディスク上のデータベースを使用するように設定を変更する手順は不要です。手順 8 に進んでください。
6. HiRDB が使用するポートをデフォルト（23032/tcp）以外のポートに変更して運用している場合は、使用しているポート番号を控えておきます。
7. 次のコマンドを実行して、データベースを共有ディスクに移行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmsdbclustersetup /createcluster /databasepath <データベースの再作成先フォルダ> /exportpath <データベースの退避先フォルダ> /auto
```

createcluster

非クラスタ構成の Hitachi Command Suite 製品をクラスタ構成へ移行するためのオプションです。

databasepath

データベースの再作成先フォルダを指定します。実行系ノードで指定した<データベースの再作成先フォルダ>と同じフォルダを指定してください。

パスに使用できる文字を次に示します。そのほか、円記号 (¥)、コロン (:) およびスラッシュ (/) をパスの区切り文字として使用できます。

A~Z a~z 0~9 . _

exportpath

データベースの退避先フォルダを指定します。ローカルディスク上のフォルダを、63 バイト以内の絶対パスで指定してください。パスに使用できる文字は、databasepath に指定できる文字と同じです。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



注意

- hcmsdbclustersetup コマンドを実行すると、HiRDB が使用するポート番号の設定がデフォルト値 (23032/tcp) に戻ります。
- <データベースの退避先フォルダ>がすでにある場合は、フォルダの中を空にするか、フォルダを削除してください。
- hcmsdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。
- hcmsdbclustersetup コマンドが異常終了した状態でサーバを再起動すると、共有ディスクの接続先が待機系ノードに切り替わることがあります。

8. hcmsdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスが停止していることを確認します。
9. [サービス] ウィンドウで次のプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service
 - HiCommandServer
 - HiCommand Tiered Storage Manager

関連項目

- [9.4 サービスの稼働状態の確認](#)
- Hitachi Command Suite のインストール方法: マニュアル「*Hitachi Command Suite Software インストールガイド*」

(3) Microsoft Cluster Service の設定

Microsoft Cluster Service のリソースグループに、Device Manager および Tiered Storage Manager のリソースを登録します。

Microsoft Cluster Service の設定をする前に、次の作業を実施してください。

- クラスタ化するサービスの集まり (サービスフェールオーバーの単位) であるクラスタグループ (リソースグループ) を用意してください。
- 実行系と待機系で引き継ぎ可能な共有ディスクとクラスタ管理 IP アドレスを含めてリソースグループを構成してください。
- リソースの割り当て、削除および動作監視が Microsoft Cluster Service によって正常に制御できることを確認してください。

- すでに、ほかの Hitachi Command Suite 製品が登録されているリソースグループがあれば、そのリソースグループを使用してください。

リソースグループは、Hitachi Command Suite 製品に関連するリソースだけで構成してください。

Microsoft Cluster Service を設定するには：

- クラスタ管理アプリケーションで [新規作成] — [リソース] を選択し、表示される各ダイアログで、「表 8-2 HiRDB をリソースとして登録するための設定 (Microsoft Cluster Service の場合)」～「表 8-7 Tiered Storage Manager サーバをリソースとして登録するための設定 (Microsoft Cluster Service の場合)」に示す値を指定します。
- 設定が完了したら、クラスタ管理アプリケーションで、リソースを追加したリソースグループをオンラインにします。

(4) Microsoft Cluster Service に登録するリソースの値

Microsoft Cluster Service に Device Manager および Tiered Storage Manager のリソースを登録する場合は、次の表に示す値を設定してください。

表 8-2 HiRDB をリソースとして登録するための設定 (Microsoft Cluster Service の場合)

ダイアログ名	設定
[新しいリソース]	[名前]：HiRDB/ClusterService_HD0 (任意) [リソースの種類]：汎用サービス
[実行可能な所有者]	実行系ノードと待機系ノードが追加されていることを確認します。
[依存関係]	共有ディスクのドライブ、およびネットワーク名を登録します。
[汎用サービスパラメータ]	[サービス名]：HiRDBClusterService_HD0 [起動パラメータ]：何も指定しません。
[レジストリ レプリケーション]	何も指定しません。

表 8-3 HBase Storage Mgmt Common Service をリソースとして登録するための設定 (Microsoft Cluster Service の場合)

ダイアログ名	設定
[新しいリソース]	[名前]：HBase Storage Mgmt Common Service (任意) [リソースの種類]：汎用サービス
[実行可能な所有者]	実行系ノードと待機系ノードが追加されていることを確認します。
[依存関係]	HiRDB/ClusterService_HD0 を登録します。
[汎用サービスパラメータ]	[サービス名]：HBaseStgMgmtComService [起動パラメータ]：何も指定しません。
[レジストリ レプリケーション]	何も指定しません。

表 8-4 HBase Storage Mgmt Web Service をリソースとして登録するための設定 (Microsoft Cluster Service の場合)

ダイアログ名	設定
[新しいリソース]	[名前]：HBase Storage Mgmt Web Service (任意) [リソースの種類]：汎用サービス
[実行可能な所有者]	実行系ノードと待機系ノードが追加されていることを確認します。
[依存関係]	HBase Storage Mgmt Common Service を登録します。
[汎用サービスパラメータ]	[サービス名]：HBaseStgMgmtWebService [起動パラメータ]：何も指定しません。
[レジストリ レプリケーション]	何も指定しません。

表 8-5 HCS Device Manager Web Service をリソースとして登録するための設定 (Microsoft Cluster Service の場合)

ダイアログ名	設定
[新しいリソース]	[名前]: HCS Device Manager Web Service (任意) [リソースの種類]: 汎用サービス
[実行可能な所有者]	実行系ノードと待機系ノードが追加されていることを確認します。
[依存関係]	HBase Storage Mgmt Web Service を登録します。
[汎用サービスパラメータ]	[サービス名]: DeviceManagerWebService [起動パラメータ]: 何も指定しません。
[レジストリ レプリケーション]	何も指定しません。

表 8-6 HiCommandServer をリソースとして登録するための設定 (Microsoft Cluster Service の場合)

ダイアログ名	設定
[新しいリソース]	[名前]: HiCommandServer (任意) [リソースの種類]: 汎用サービス
[実行可能な所有者]	実行系ノードと待機系ノードが追加されていることを確認します。
[依存関係]	HBase Storage Mgmt Web Service を登録します。
[汎用サービスパラメータ]	[サービス名]: HiCommandServer [起動パラメータ]: 何も指定しません。
[レジストリ レプリケーション]	何も指定しません。

表 8-7 Tiered Storage Manager サーバをリソースとして登録するための設定 (Microsoft Cluster Service の場合)

ダイアログ名	設定
[新しいリソース]	[名前]: HiCommand Tiered Storage Manager (任意) [リソースの種類]: 汎用サービス
[実行可能な所有者]	実行系ノードと待機系ノードが追加されていることを確認します。
[依存関係]	HiCommandServer を登録します。
[汎用サービスパラメータ]	[サービス名]: HiCommandTieredStorageManager [起動パラメータ]: 何も指定しません。
[レジストリ レプリケーション]	何も指定しません。

(5) Windows Server Failover Clustering の設定

Windows Server Failover Clustering のリソースグループに、Device Manager および Tiered Storage Manager のリソースを登録します。

Windows Server Failover Clustering の設定をする前に、次の作業を実施してください。

- ・ クラスタ化するサービスの集まり (サービスフェールオーバーの単位) であるクラスタグループ (リソースグループ) を用意してください。
- ・ 実行系と待機系で引き継ぎ可能な共有ディスクとクライアントアクセスポイント (クラスタ管理 IP アドレスおよびネットワーク名) を含めてリソースグループを構成してください。
- ・ リソースの割り当て、削除および動作監視が Windows Server Failover Clustering によって正常に制御できることを確認してください。
- ・ すでに、ほかの Hitachi Command Suite 製品が登録されているリソースグループがあれば、そのリソースグループを使用してください。

リソースグループは、Hitachi Command Suite 製品に関連するリソースだけで構成してください。

Windows Server Failover Clustering を設定するには：

1. リソースグループの名称を右クリックして、[リソースの追加] - [汎用サービス] を選択します。[サービスの選択] 画面では、次のサービスを選択してください。
 - HiRDB/ClusterService_HD0
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service
 - HiCommandServer
 - HiCommand Tiered Storage Manager
 各サービスがリソースとして登録されます。
2. リソース名を右クリックして、[プロパティ] を選択します。
 それぞれのリソースで、「表 8-8 HiRDB/ClusterService_HD0 のプロパティの設定 (Windows Server Failover Clustering の場合)」～「表 8-13 HiCommand Tiered Storage Manager のプロパティの設定 (Windows Server Failover Clustering の場合)」に示された設定を指定します。
3. クラスタ管理アプリケーションで、リソースを追加したリソースグループをオンラインにします。

(6) Windows Server Failover Clustering に登録するリソースのプロパティ

Windows Server Failover Clustering に、Device Manager および Tiered Storage Manager のリソースのプロパティを登録する場合は、次の表に示す値を設定してください。

なお、Windows のバージョンによって表示されるタブが異なります。

表 8-8 HiRDB/ClusterService_HD0 のプロパティの設定 (Windows Server Failover Clustering の場合)

タブ名	設定
[全般]	[スタートアップパラメーター] (または [セットアップパラメータ]) : 何も指定しません (指定されている場合は削除してください)。
[依存関係]	共有ディスク、クライアントアクセスポイントを登録します。
[詳細なポリシー]	[実行可能な所有者] : 実行系ノードと待機系ノードが追加されていることを確認します。
[ポリシー]	何も指定しません。
[レジストリのレプリケーション]	何も指定しません。

表 8-9 HBase Storage Mgmt Common Service のプロパティの設定 (Windows Server Failover Clustering の場合)

タブ名	設定
[全般]	[スタートアップパラメーター] (または [セットアップパラメータ]) : 何も指定しません (指定されている場合は削除してください)。
[依存関係]	HiRDB/ClusterService_HD0 を登録します。
[詳細なポリシー]	[実行可能な所有者] : 実行系ノードと待機系ノードが追加されていることを確認します。

タブ名	設定
[ポリシー]	何も指定しません。
[レジストリのレプリケーション]	何も指定しません。

表 8-10 HBase Storage Mgmt Web Service のプロパティの設定 (Windows Server Failover Clustering の場合)

タブ名	設定
[全般]	[スタートアップパラメーター] (または [セットアップパラメータ]) : 何も指定しません (指定されている場合は削除してください)。
[依存関係]	HBase Storage Mgmt Common Service を登録します。
[詳細なポリシー]	[実行可能な所有者] : 実行系ノードと待機系ノードが追加されていることを確認します。
[ポリシー]	何も指定しません。
[レジストリのレプリケーション]	何も指定しません。

表 8-11 HCS Device Manager Web Service のプロパティの設定 (Windows Server Failover Clustering の場合)

タブ名	設定
[全般]	[スタートアップパラメーター] (または [セットアップパラメータ]) : 何も指定しません (指定されている場合は削除してください)。
[依存関係]	HBase Storage Mgmt Web Service を登録します。
[詳細なポリシー]	[実行可能な所有者] : 実行系ノードと待機系ノードが追加されていることを確認します。
[ポリシー]	何も指定しません。
[レジストリのレプリケーション]	何も指定しません。

表 8-12 HiCommandServer のプロパティの設定 (Windows Server Failover Clustering の場合)

タブ名	設定
[全般]	[スタートアップパラメーター] (または [セットアップパラメータ]) : 何も指定しません (指定されている場合は削除してください)。
[依存関係]	HBase Storage Mgmt Web Service を登録します。
[詳細なポリシー]	[実行可能な所有者] : 実行系ノードと待機系ノードが追加されていることを確認します。
[ポリシー]	何も指定しません。
[レジストリのレプリケーション]	何も指定しません。

表 8-13 HiCommand Tiered Storage Manager のプロパティの設定 (Windows Server Failover Clustering の場合)

タブ名	設定
[全般]	[スタートアップパラメーター] (または [セットアップパラメータ]) : 何も指定しません (指定されている場合は削除してください)。
[依存関係]	HiCommandServer を登録します。
[詳細なポリシー]	[実行可能な所有者] : 実行系ノードと待機系ノードが追加されていることを確認します。

タブ名	設定
[ポリシー]	何も指定しません。
[レジストリのレプリケーション]	何も指定しません。

8.2.2 アップグレードまたは上書きインストール (Windows)

ここでは、クラスタ構成の管理サーバに Hitachi Command Suite をアップグレードまたは上書きインストールする方法を説明します。



注意 クラスタ環境のセットアップでは、Hitachi Command Suite のサービスの停止を伴う操作を実行します。セットアップ中は、Hitachi Command Suite にアクセスしないでください。

(1) 準備作業

次の操作を実行してください。

1. 実行系ノードで、Hitachi Command Suite 製品のサービスを登録しているリソースグループをオンラインにします。
2. 実行系ノードのクラスタ管理アプリケーションで、次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service (バージョン 7.0 以降からアップグレードまたは上書きインストールした場合)
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
3. 実行系ノードで `hcmdssrv` コマンドを実行して、Hitachi Command Suite 共通コンポーネントのサービスを停止します。
4. 実行系ノードのクラスタ管理アプリケーションで、次のサービスをオフラインにします。
 - HiRDB/ClusterService_HD0
5. 待機系ノードで手順 1～手順 4 と同様の操作を実行します。
6. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを抑制します。実行系ノードまたは待機系ノードで、次のリソースの設定を変更します。
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service (バージョン 7.0 以降からアップグレードまたは上書きインストールした場合)
 - HiCommandServer
 - HiCommand Tiered Storage Manager
 - HiRDB/ClusterService_HD0
 - 上記以外に手順 2 でオフラインにしたサービス

Microsoft Cluster Service を使用する場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開しない] を選択します。

Windows Server Failover Clustering を使用する場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで、[リソースが失敗状態になった場合は、再起動しない] を選択します。

関連項目

- 9.3 サービスの停止

(2) 実行系ノードでの手順

実行系ノードにインストールされている Hitachi Command Suite をアップグレードまたは上書きインストールする場合の手順を次に示します。

1. 実行系ノードおよび待機系ノードから共有ディスクにアクセスできることを確認します。
2. Hitachi Command Suite をアップグレードまたは上書きインストールします。
[インストール前の確認] 画面で、[インストール前にデータベースをバックアップする] の設定が [はい] になっていることを確認してください。
[いいえ] になっている場合は、[設定編集] ボタンをクリックして [詳細インストール設定の編集] 画面を開きます。そのあと、[設定] メニューから [バックアップ] を選択して、[インストール前にデータベースをバックアップします。] チェックボックスをチェックしてください。
3. 次のコマンドを実行して、アップグレードまたは上書きインストール後のデータベースをバックアップします。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin  
%hcmdsbackups /dir <バックアップファイルの格納先フォルダ> /auto
```

dir

データベースのバックアップファイルを格納するローカルディスク上のフォルダを絶対パスで指定します。

dir オプションに指定するフォルダが空であることを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



重要 hcmdsbackups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先フォルダに database というフォルダが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

4. Hitachi Command Suite 製品のサービスが起動中の場合は、サービスを停止します。
5. [サービス] ウィンドウで次のプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service
 - HiCommandServer
 - HiCommand Tiered Storage Manager
6. クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスを登録しているリソースグループを選択し、右クリックメニューで待機系ノードに移動します。

関連項目

- 9.3 サービスの停止
- Hitachi Command Suite のインストール方法：マニュアル「*Hitachi Command Suite Software インストールガイド*」
- Replication Manager と Business Continuity Manager が連携している環境に Hitachi Command Suite をインストールする方法：マニュアル「*Hitachi Command Suite Replication Manager Software システム構成ガイド*」

(3) 待機系ノードでの手順

待機系ノードにインストールされている Hitachi Command Suite をアップグレードまたは上書きインストールする場合の手順を次に示します。

1. hcmdssrv コマンドを実行して、Hitachi Command Suite 共通コンポーネントのサービスを停止します。
2. Hitachi Command Suite をアップグレードまたは上書きインストールします。
3. Hitachi Command Suite 製品のサービスが起動中の場合は、サービスを停止します。
4. [サービス] ウィンドウで次のプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service
 - HiCommandServer
 - HiCommand Tiered Storage Manager
5. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを有効にします。次のリソースの設定を変更します。
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service (バージョン 7.0 以降からアップグレードまたは上書きインストールした場合)
 - HiCommandServer
 - HiCommand Tiered Storage Manager
 - HiRDB/ClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用する場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開する] を選択します。

Windows Server Failover Clustering を使用する場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで次の項目を選択します。

- [リソースが失敗状態になった場合は、現在のノードで再起動を試みる]
- [再起動に失敗した場合は、この役割のすべてのリソースをフェールオーバーする] (または [再起動に失敗した場合は、このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする])

6. Hitachi Command Suite 製品のサービスを登録しているリソースグループに HCS Device Manager Web Service を登録します。
7.0 よりも前のバージョンからアップグレードインストールした場合に登録が必要です。「表 8-5 HCS Device Manager Web Service をリソースとして登録するための設定 (Microsoft Cluster Service の場合)」または「表 8-11 HCS Device Manager Web Service のプロパティの設定 (Windows Server Failover Clustering の場合)」に従って設定してください。
7. クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスを登録しているリソースグループをオンラインにします。

関連項目

- 9.3 サービスの停止
- Hitachi Command Suite のインストール方法：マニュアル「*Hitachi Command Suite Software インストールガイド*」
- Replication Manager と Business Continuity Manager が連携している環境に Hitachi Command Suite をインストールする方法：マニュアル「*Hitachi Command Suite Replication Manager Software システム構成ガイド*」

8.2.3 クラスタ環境への変更 (Windows)

非クラスタ構成で Device Manager, Tiered Storage Manager または Replication Manager のシステムの運用を開始したあとで、クラスタ構成に変更したい場合は、次の手順で変更してください。ここでは、すでに運用中の Device Manager サーバ、Tiered Storage Manager サーバおよび Replication Manager サーバがインストールされたマシンを実行系ノードとする場合を想定して説明します。



注意 クラスタ環境のセットアップでは、Hitachi Command Suite のサービスの停止を伴う操作を実行します。セットアップ中は、Hitachi Command Suite にアクセスしないでください。

管理サーバの OS が Windows の場合に、運用開始後にクラスタ環境に変更する手順を次に示します。

1. Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager のサービスをいったん停止します。
2. 待機系ノードとなるマシンに Hitachi Command Suite をインストールします。
3. 使用する製品のライセンスを GUI で登録します。
待機系ノードの IP アドレスにアクセスしてください。
インストールする製品ごとに、ライセンスキーの入力が必要です。
4. 実行系ノードで次のコマンドを実行して、GUI を起動するための URL を論理ホスト名に変更します。
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin
%hcmdschgurl /change http://<実行系ノードの IP アドレスまたはホスト名>:<ポート番号> http://<論理ホスト名>:<ポート番号>
5. 実行系および待機系の各ノードで、テキストエディターを使って、クラスタ設定ファイルを作成します。
クラスタ設定ファイルに指定する項目は次のとおりです。
実行系ノードの場合

```
mode=online
virtualhost=<論理ホスト名>
```

```
onlinehost=<実行系ノードのホスト名>
standbyhost=<待機系ノードのホスト名>
```

待機系ノードの場合

```
mode=standby
virtualhost=<論理ホスト名>
onlinehost=<実行系ノードのホスト名>
standbyhost=<待機系ノードのホスト名>
```

作成したファイルは、cluster.conf というファイル名で、<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%conf に格納します。



注意

- mode には、実行系ノードの場合は online、待機系ノードの場合は standby を指定してください。
- virtualhost, onlinehost, standbyhost には IP アドレスは指定できません。ホスト名から IP アドレスの名前解決ができることを確認してください。
- virtualhost に指定する論理ホスト名には、有効でアクセスできる IP アドレスが割り当てられている必要があります。

6. 実行系および待機系の各ノードで、server.properties ファイルを開き、server.http.host プロパティに論理ホスト名を指定します。
<Device Manager サーバのインストールフォルダ>%HiCommandServer%config
%server.properties

7. 次のコマンドを実行して、実行系ノードでデータベースをバックアップします。
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsbackups /dir <バックアップファイルの格納先フォルダ> /auto

dir

データベースのバックアップファイルを格納するローカルディスク上のフォルダを絶対パスで指定します。

dir オプションに指定するフォルダが空であることを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



重要 hcmdsbackups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先フォルダに database というフォルダが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

8. HiRDB が使用するポートをデフォルト (23032/tcp) 以外のポートに変更して運用している場合は、使用しているポート番号を控えておきます。
9. 実行系ノードで次のコマンドを実行して、データベースを共有ディスクに移行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsdbclustersetup /createcluster /databasepath <データベースの再作成先
フォルダ> /exportpath <データベースの退避先フォルダ> /auto
```

createcluster

非クラスタ構成の Hitachi Command Suite 製品をクラスタ構成へ移行するためのオプションです。

databasepath

データベースの再作成先フォルダを指定します。共有ディスク上のフォルダを、63 バイト以内の絶対パスで指定してください。

パスに使用できる文字を次に示します。そのほかに、円記号 (¥)、コロン (:) およびスラント (/) をパスの区切り文字として使用できます。

A~Z a~z 0~9 . _

exportpath

データベースの退避先フォルダを指定します。ローカルディスク上のフォルダを、63バイト以内の絶対パスで指定してください。パスに使用できる文字は、databasepathに指定できる文字と同じです。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



注意

- hcmsdbclustersetup コマンドを実行すると、HiRDB が使用するポート番号の設定がデフォルト値 (23032/tcp) に戻ります。
- hcmsdbclustersetup コマンドを実行すると、Tuning Manager のリモート接続の設定が初期化されます。
- <データベースの退避先フォルダ>がすでにある場合は、フォルダの中を空にするか、フォルダを削除してください。
- hcmsdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。
- hcmsdbclustersetup コマンドが異常終了した状態でサーバを再起動すると、共有ディスクの接続先が待機系ノードに切り替わることがあります。

10. 待機系ノードで次のコマンドを実行して、共有ディスク上のデータベースを使用するように設定を変更します。

<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin

%hcmsdbclustersetup /createcluster /databasepath <データベースの再作成先フォルダ> /exportpath <データベースの退避先フォルダ> /auto

hcmsdbclustersetup コマンドに指定するオプションについては、手順 9 を参照してください。

databasepath には、実行系ノードで指定した<データベースの再作成先フォルダ>と同じフォルダを指定してください。

11. 実行系および待機系の各ノードで hcmsdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスが停止していることを確認します。
12. 実行系および待機系の各ノードで、次のサービスを手動で起動するよう変更します。
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service
 - HiCommandServer
 - HiCommand Tiered Storage Manager[サービス] ウィンドウ内で、各サービスのプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。
13. クラスタソフトウェアにリソースを登録します。

「(3) Microsoft Cluster Service の設定」または「(5) Windows Server Failover Clustering の設定」に従って、クラスタリソースを登録してください。
14. 非クラスタ環境で運用していた時に Tuning Manager とリモート接続していた場合は、必要に応じて、Tuning Manager のサービスを起動したあと、Tuning Manager と連携するための設定を再度実施します。

関連項目

- (2) Tuning Manager サーバとのリモート接続 (Microsoft Cluster Service または Windows Server Failover Clustering)
- 9.4 サービスの稼働状態の確認
- Tuning Manager のサービスを起動および停止する方法：インストールされている Tuning Manager に対応するバージョンのマニュアル
- Hitachi Command Suite のインストール方法：マニュアル「*Hitachi Command Suite Software インストールガイド*」

8.2.4 アンインストール (Windows)

ここでは、管理サーバの OS が Windows で、クラスタ構成となっている場合に Hitachi Command Suite をアンインストールする手順について説明します。

アンインストールの手順を次に示します。

1. Hitachi Command Suite 製品のサービスを登録しているリソースグループの所有者を待機系ノードから実行系ノードに移動します。
2. クラスタ管理アプリケーションで、次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
3. Hitachi Command Suite 製品のサービスを停止します。
4. クラスタ管理アプリケーションで、次のサービスをオフラインにします。
 - HiRDB/ClusterService_HD0
5. 次のサービスがほかのアプリケーションによって使用されていない場合は、クラスタ管理アプリケーションで、そのサービスを削除します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDB/ClusterService_HD0
6. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを抑制します。
手順 5 のサービスのうち、削除しないサービスについて、次の作業をします。
Microsoft Cluster Service を使用する場合：
リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開しない] を選択します。
Windows Server Failover Clustering を使用する場合：
リソース名を右クリックし、[プロパティ] - [ポリシー] タブで、[リソースが失敗状態になった場合は、再起動しない] を選択します。
7. 次のコマンドを実行して、データベースをバックアップします。

< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin
%hcmdsbackups /dir <バックアップファイルの格納先フォルダ> /auto

dir

データベースのバックアップファイルを格納するローカルディスク上のフォルダを絶対パスで指定します。

dir オプションに指定するフォルダが空であることを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



重要 hcmdsbackups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先フォルダに database というフォルダが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

8. hcmdsdrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
9. 実行系ノードで Hitachi Command Suite をアンインストールします。
10. 実行系ノードで、不要になったファイルやフォルダ（クラスタ環境内でのインストール中に作成されたファイルやフォルダなど）をすべて削除します。
11. クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスを登録していたリソースグループを待機系ノードに移動します。
12. 待機系ノードで Hitachi Command Suite をアンインストールします。
13. 待機系ノードで、不要になったファイルやフォルダ（クラスタ環境内でのインストール中に作成されたファイルやフォルダなど）をすべて削除します。
14. 次のリソースがほかのアプリケーションによって使用されていない場合は、クラスタ管理アプリケーションで、そのリソースをオフラインにしてから削除します。
 - IP アドレス
 - 共有ディスク
15. Hitachi Command Suite 製品のサービスを登録しているリソースグループが不要になった場合は、そのリソースグループも削除します。
16. 残したリソースグループを継続して使用する場合、フェールオーバーを有効にします。
手順 6 でフェールオーバーを抑制したリソースについて次の設定を行ってください。

Microsoft Cluster Service を使用する場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開する] を選択します。

Windows Server Failover Clustering を使用する場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで次の項目を選択します。

- [リソースが失敗状態になった場合は、現在のノードで再起動を試みる]
- [再起動に失敗した場合は、この役割のすべてのリソースをフェールオーバーする]（または [再起動に失敗した場合は、このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする]）

関連項目

- [9.3 サービスの停止](#)
- Hitachi Command Suite のアンインストール方法：マニュアル「*Hitachi Command Suite Software インストールガイド*」

8.3 Solaris でのセットアップ

ここでは、管理サーバの OS が Solaris の場合に、Veritas Cluster Server および Sun Cluster を利用してクラスタ環境をセットアップする手順について説明します。

8.3.1 新規インストール (Solaris)

ここでは、クラスタ構成の管理サーバに Hitachi Command Suite を新規インストールする方法を説明します。



注意 クラスタ環境のセットアップでは、Hitachi Command Suite のサービスの停止を伴う操作を実行します。セットアップ中は、Hitachi Command Suite にアクセスしないでください。

(1) 実行系ノードでの手順

実行系ノードに Hitachi Command Suite を新規インストールする場合の手順を次に示します。

1. クラスタ管理 IP アドレスと共有ディスクをオンラインにします。
2. ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、Hitachi Command Suite 製品のサービスおよびリソースグループをクラスタの管理対象から外します。



注意 次に示すリソースは管理対象から外さないでください。

- 共有ディスク
- クラスタ管理 IP アドレス
- 論理ホスト名

3. 実行系ノードに Hitachi Command Suite を新規インストールします。

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、次の条件に従ってください。

- 共有ディスクにアクセスできる状態にしたあとで、データベースの格納先に共有ディスク上のパスを指定する。
- 管理サーバの IP アドレスに論理ホスト名 (クラスタ管理 IP アドレスに割り当てられた仮想のホスト名) を指定する。

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されていない場合は、次の条件に従ってください。

- データベースの格納先に、ローカルディスク上のパスを指定する。
- 管理サーバの IP アドレスに、実行系ノードの IP アドレスを指定する。

4. 使用する製品のライセンスを GUI で登録します。

実行系ノードの IP アドレスにアクセスしてください。

インストールする製品ごとに、ライセンスキーの入力が必要です。

5. GUI を起動するための URL を論理ホスト名に変更します。

次のコマンドを実行して、論理ホスト名になっているかを確認します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/hcmdschgurl -print
```

論理ホスト名が指定されていない場合、次のコマンドを実行して URL を変更します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/hcmdschgurl -change http://<実行系ノードの IP アドレスまたはホスト名*>:<ポート番号> http://<論理ホスト名>:<ポート番号>
```

注※ インストール時に入力した値を指定します。

6. テキストエディターを使って、クラスタ設定ファイルを作成します。

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、この手順は不要です。

クラスタ設定ファイルに指定する項目は次のとおりです。

```
mode=online
virtualhost=<論理ホスト名>
onlinehost=<実行系ノードのホスト名>
standbyhost=<待機系ノードのホスト名>
```

作成したファイルは、cluster.conf というファイル名で、<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/conf に格納します。



注意

- mode には online を指定してください。
- virtualhost, onlinehost, standbyhost には IP アドレスは指定できません。ホスト名から IP アドレスの名前解決ができることを確認してください。
- virtualhost に指定する論理ホスト名には、有効でアクセスできる IP アドレスが割り当てられている必要があります。

7. server.properties ファイルを開き、server.http.host プロパティに論理ホスト名が指定されていることを確認します。

論理ホスト名が指定されていない場合は、論理ホスト名に変更してください。

```
<Device Manager サーバのインストールディレクトリ>/HiCommandServer/config/
server.properties
```

8. データベースを共有ディスクに移行します。

その方法を手順 9～手順 11 で説明します。

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、データベースを共有ディスクに移行する手順は不要です。手順 12 に進んでください。

9. 次のコマンドを実行して、新規インストール後のデータベースをバックアップします。

障害が発生した場合に備えて、データベースをバックアップしておくことをお勧めします。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/
hcmdsbackups -dir <バックアップファイルの格納先ディレクトリ> -auto
```

dir

データベースのバックアップファイルを格納するローカルディスク上のディレクトリを絶対パスで指定します。

dir オプションに指定するディレクトリが空であることを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



重要 hcmdsbacups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先ディレクトリに database というディレクトリが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

10. HiRDB が使用するポートをデフォルト (23032/tcp) 以外のポートに変更して運用している場合は、使用しているポート番号を控えておきます。

11. 次のコマンドを実行して、データベースを共有ディスクに移行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/
hcmdsdbclustersetup -createcluster -databasepath <データベースの再作成先
ディレクトリ> -exportpath <データベースの退避先ディレクトリ> -auto
```

createcluster

非クラスタ構成の Hitachi Command Suite 製品をクラスタ構成へ移行するためのオプションです。

databasepath

データベースの再作成先ディレクトリを指定します。共有ディスク上のディレクトリを、63 バイト以内の絶対パスで指定してください。

パスに使用できる文字を次に示します。そのほかに、スラント (/) をパスの区切り文字として使用できます。パス中に空白は指定できません。

A~Z a~z 0~9 . _

exportpath

データベースの退避先ディレクトリを指定します。ローカルディスク上のディレクトリを、63 バイト以内の絶対パスで指定してください。パスに使用できる文字は、databasepath に指定できる文字と同じです。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



注意

- hcmsdbclustersetup コマンドを実行すると、HiRDB が使用するポート番号の設定がデフォルト値 (23032/tcp) に戻ります。
- <データベースの退避先ディレクトリ>がすでにある場合は、ディレクトリの中を空にするか、ディレクトリを削除してください。
- hcmsdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。
- hcmsdbclustersetup コマンドが異常終了した状態でサーバを再起動すると、共有ディスクの接続先が待機系ノードに切り替わることがあります。

12. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスが停止していることを確認します。

13. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスがマシンの起動時に自動的に開始しないようにします。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdssrv -starttype manual -all
```

14. Device Manager サーバおよび Tiered Storage Manager サーバがマシンの起動時に自動的に開始しないようにします。次のファイルを別ディレクトリに移動するか、ファイル名を変更します。ファイル名を変更する場合は、変更後のファイル名の先頭文字に K と S は使用しないでください。

/etc/rc3.d/S99hicommand (Device Manager の場合)

/etc/rc3.d/S99htsmsserver (Tiered Storage Manager の場合)

15. Hitachi Command Suite 製品のサービスを登録しているリソースグループを待機系ノードに移動します。

Veritas Cluster Server の場合 :

Cluster Explorer ウィンドウで [Service Groups] タブを選択します。

Hitachi Command Suite 製品のサービスを登録しているリソースグループを右クリックして、コンテキストメニューから次の操作を順に実行します。

[Unfreeze] を選択します。

[Switch To] - [<ホスト名>] を選択します。

[Freeze] – [Temporary] を選択します。

Sun Cluster の場合：

次のコマンドを実行します。

```
/usr/cluster/bin/scswitch -z -g <リソースグループ名> -h <ホスト名>
```

関連項目

- 9.4 サービスの稼働状態の確認
- クラスタの管理対象から外す必要のあるサービスおよびリソースグループについて：各 Hitachi Command Suite 製品のマニュアル
- Hitachi Command Suite のインストール方法：マニュアル「*Hitachi Command Suite Software インストールガイド*」

(2) 待機系ノードでの手順

待機系ノードに Hitachi Command Suite を新規インストールする場合の手順を次に示します。

1. 待機系ノードに Hitachi Command Suite を新規インストールします。

インストールの際には、次の条件に従ってください。

- インストール先を実行系ノードと同じにしてください。
- ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合は、管理サーバの IP アドレスに論理ホスト名（クラスタ管理 IP アドレスに割り当てられた仮想のホスト名）を指定してください。ほかの Hitachi Command Suite 製品でクラスタ環境が構築されていない場合は、待機系ノードの IP アドレスまたはホスト名を指定してください。

2. 使用する製品のライセンスを GUI で登録します。

待機系ノードの IP アドレスにアクセスしてください。

インストールする製品ごとに、ライセンスキーの入力が必要です。

3. テキストエディターを使って、クラスタ設定ファイルを作成します。

ほかの Hitachi Command Suite 製品でクラスタ環境が構築されている場合、この手順は不要です。

クラスタ設定ファイルに指定する項目は次のとおりです。

```
mode=standby
virtualhost=<論理ホスト名>
onlinehost=<実行系ノードのホスト名>
standbyhost=<待機系ノードのホスト名>
```

作成したファイルは、cluster.conf というファイル名で、<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/conf に格納します。



注意

- mode には standby を指定してください。
- virtualhost, onlinehost, standbyhost には IP アドレスは指定できません。ホスト名から IP アドレスの名前解決ができることを確認してください。
- virtualhost に指定する論理ホスト名には、有効でアクセスできる IP アドレスが割り当てられている必要があります。

4. server.properties ファイルを開き、server.http.host プロパティに論理ホスト名が指定されていることを確認します。

論理ホスト名が指定されていない場合は、論理ホスト名に変更してください。

< *Device Manager* サーバのインストールディレクトリ > /HiCommandServer/config/
server.properties

- 共有ディスク上のデータベースを使用するように設定を変更します。

その方法を手順 6～手順 7 で説明します。

ほかの *Hitachi Command Suite* 製品でクラスタ環境が構築されている場合、共有ディスク上のデータベースを使用するように設定を変更する手順は不要です。手順 8 に進んでください。

- HiRDB* が使用するポートをデフォルト (23032/tcp) 以外のポートに変更して運用している場合は、使用しているポート番号を控えておきます。
- 次のコマンドを実行して、データベースを共有ディスクに移行します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdsdbclustersetup -createcluster -databasepath <データベースの再作成先  
ディレクトリ > -exportpath <データベースの退避先ディレクトリ > -auto
```

createcluster

非クラスタ構成の *Hitachi Command Suite* 製品をクラスタ構成へ移行するためのオプションです。

databasepath

データベースの再作成先ディレクトリを指定します。実行系ノードで指定した <データベースの再作成先ディレクトリ > と同じディレクトリを指定してください。

パスに使用できる文字を次に示します。そのほかに、スラント (/) をパスの区切り文字として使用できます。パス中に空白は指定できません。

A~Z a~z 0~9 . _

exportpath

データベースの退避先ディレクトリを指定します。ローカルディスク上のディレクトリを、63 バイト以内の絶対パスで指定してください。パスに使用できる文字は、databasepath に指定できる文字と同じです。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



注意

- hcmdsdbclustersetup コマンドを実行すると、*HiRDB* が使用するポート番号の設定がデフォルト値 (23032/tcp) に戻ります。
- <データベースの退避先ディレクトリ > がすでにある場合は、ディレクトリの中を空にするか、ディレクトリを削除してください。
- hcmdsdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。
- hcmdsdbclustersetup コマンドが異常終了した状態でサーバを再起動すると、共有ディスクの接続先が待機系ノードに切り替わることがあります。

- hcmdsdrv コマンドを実行して、*Hitachi Command Suite* 製品のサービスが停止していることを確認します。
- 次のコマンドを実行して、*Hitachi Command Suite* 製品のサービスがマシンの起動時に自動的に開始しないようにします。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdsdrv -starttype manual -all
```

- Device Manager* サーバおよび *Tiered Storage Manager* サーバがマシンの起動時に自動的に開始しないようにします。次のファイルを別ディレクトリに移動するか、ファイル名を変更しま

す。ファイル名を変更する場合は、変更後のファイル名の先頭文字に **K** と **S** は使用しないでください。

/etc/rc3.d/S99hicommand (Device Manager の場合)

/etc/rc3.d/S99htsmserver (Tiered Storage Manager の場合)

関連項目

- 9.4 サービスの稼働状態の確認
- Hitachi Command Suite のインストール方法: マニュアル「*Hitachi Command Suite Software インストールガイド*」

(3) スクリプトの作成 (Veritas Cluster Server の場合)

実行系ノードと待機系ノードで、Hitachi Command Suite のインストールと設定が終わったら、両方のノードで HiRDB 用のスクリプトを作成する必要があります。

1. HiRDB のサービスを Veritas Cluster Server から監視するためのダミーファイルを作成します。

ファイル名: <Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/HDB/.pdveritas

内容: 空のファイル

2. HiRDB のサービス用のリソースタイプを定義するスクリプトファイルを作成します。

ファイル名: /etc/VRTSvcs/conf/config/HiRDB_STypes.cf

内容: 次の内容でファイルを作成してください。

```
type HiRDB_S (  
  static str ArgList[] = { PDir, PdConfPath, Ld_Library_Path, DummyFilePath }  
  str PDir  
  str PdConfPath  
  str Ld_Library_Path  
  str DummyFilePath  
)
```

3. 次のコマンドを実行して、HiRDB 用のエージェントを定義します。

```
# mkdir /opt/VRTSvcs/bin/HiRDB_S
```

```
# cp /opt/VRTSvcs/bin/ScriptAgent /opt/VRTSvcs/bin/HiRDB_S/  
HiRDB_SAgent
```

4. HiRDB のサービスをオンラインにするために使用するスクリプトファイルを作成します。

ファイル名: /opt/VRTSvcs/bin/HiRDB_S/online

内容: 次の内容でファイルを作成してください。

```
#!/bin/sh  
PATH=/sbin:/usr/bin:/usr/sbin:/etc:/bin:/opt/VRTSvcs/bin:"$2"/bin  
export PATH  
PDDIR="$2"  
PDCONFPATH="$3"  
LD_LIBRARY_PATH="$4"  
export PDDIR PDCONFPATH LD_LIBRARY_PATH  
$PDDIR/bin/pdstart  
/bin/touch "$5"  
/bin/chmod 0400 "$5"
```

5. HiRDB のサービスをオフラインにするために使用するスクリプトファイルを作成します。

ファイル名: /opt/VRTSvcs/bin/HiRDB_S/offline

内容: 次の内容でファイルを作成してください。

```
#!/bin/sh
PATH=/sbin:/usr/bin:/usr/sbin:/etc:/bin:/opt/VRTSvcs/bin:"$2"/bin
export PATH
PDDIR="$2"
PDCONFPATH="$3"
LD_LIBRARY_PATH="$4"
export PDDIR PDCONFPATH LD_LIBRARY_PATH
$PDDIR/bin/pdstop -f -q
/bin/rm -f "$5"
```

6. HiRDB のサービスを監視するためのスクリプトファイルを作成します。

ファイル名 : /opt/VRTSvcs/bin/HiRDB_S/monitor

内容 : 次の内容でファイルを作成してください。

```
#!/bin/sh
if /bin/test -f "$5"
then
    exit 110
else
    exit 100
fi
```

7. 次のコマンドを実行して、作成したスクリプトに実行権限を割り当てます。

```
# chmod u+x /opt/VRTSvcs/bin/HiRDB_S/online
# chmod u+x /opt/VRTSvcs/bin/HiRDB_S/offline
# chmod u+x /opt/VRTSvcs/bin/HiRDB_S/monitor
```

(4) スクリプトの作成 (Sun Cluster の場合)

実行系ノードと待機系ノードで、Hitachi Command Suite のインストールと設定が終わったら、両方のノードで Hitachi Command Suite 共通コンポーネントのサービスをクラスタに登録するためのスクリプトを作成する必要があります。

次の 7 つのスクリプトを作成してください。

HCS Device Manager Web Service 用のスクリプト

ファイル名 : /etc/init.d/sc_hicommand-DM

内容 : 次の内容でファイルを作成してください。

```
#!/bin/sh
#
# Sample sc_hicommand-DM
#
# Usage: sc_hicommand-DM [start|stop|status]
#
# This Script executes /etc/init.d/hicommand-DM internally.
ALIVE_VALUE=0
DOWN_VALUE=1

exec_cmd() {
    echo `date +%y/%m/%d %H:%M:%S` " `exec    : $*"
    # Execute Command with operand
    $*
    # Set return value to RC
    RC=$?
    echo `date +%y/%m/%d %H:%M:%S` " `exec-end: $* (RC=$RC)"
    if [ $RC -ne 0 ]; then
        if [ $RC -ne 1 ]; then
            exit $RC
        fi
    fi
}

# Switch operation according to the first operand of this shell.
case $1 in
start)
```

```

exec_cmd "/etc/init.d/hicommand-DM start"
;;
stop)
exec_cmd "/etc/init.d/hicommand-DM stop"
;;
status)
/etc/init.d/hicommand-DM status
# The result is equal to 1
if [ $? -eq 1 ]; then
# running
RET_CODE=$ALIVE_VALUE
else
# not running
RET_CODE=$DOWN_VALUE
fi
exit $RET_CODE
;;
*)
echo "Invalid argument"
exit 1
esac
exit 0

```

HBase Storage Mgmt Web Service 用のスクリプト

ファイル名: /etc/init.d/sc_hicommand-CWS

内容: 次の内容でファイルを作成してください。

```

#!/bin/sh
#
# Sample sc_hicommand-CWS
#
# Usage: sc_hicommand-CWS [start|stop|status]
#
# This Script executes /etc/init.d/hicommand-CWS internally.
ALIVE_VALUE=0
DOWN_VALUE=1
exec_cmd() {
echo `date "+%y/%m/%d %H:%M:%S "` `exec      : $*`
# Execute Command with operand
$*
# Set return value to RC
RC=$?
echo `date "+%y/%m/%d %H:%M:%S "` `exec-end: $* (RC=$RC)`
if [ $RC -ne 0 ]; then
if [ $RC -ne 1 ]; then
exit $RC
fi
fi
}

# Switch operation according to the first operand of this shell.
case $1 in
start)
exec_cmd "/etc/init.d/hicommand-CWS start"
;;
stop)
exec_cmd "/etc/init.d/hicommand-CWS stop"
;;
status)
/etc/init.d/hicommand-CWS status
# The result is equal to 1
if [ $? -eq 1 ]; then
# running
RET_CODE=$ALIVE_VALUE
else
# not running
RET_CODE=$DOWN_VALUE
fi
exit $RET_CODE
;;
*)
echo "Invalid argument"
exit 1
esac

```

```
exit 0
```

HBase Storage Mgmt Common Service 用のスクリプト

ファイル名 : /etc/init.d/sc_hicommand-SSOS

内容 : 次の内容でファイルを作成してください。

```
#!/bin/sh
#
# Sample sc_hicommand-SSOS
#
# Usage: sc_hicommand-SSOS [start|stop|status]
#
# This Script executes /etc/init.d/hicommand-SSOS internally.
ALIVE_VALUE=0
DOWN_VALUE=1

exec_cmd() {
    echo `date "+%y/%m/%d %H:%M:%S "` `exec : $*`
    # Execute Command with operand
    $*
    # Set return value to RC
    RC=$?
    echo `date "+%y/%m/%d %H:%M:%S "` `exec-end: $* (RC=$RC)`
    if [ $RC -ne 0 ]; then
        if [ $RC -ne 1 ]; then
            exit $RC
        fi
    fi
}

# Switch operation according to the first operand of this shell.
case $1 in
start)
    exec_cmd "/etc/init.d/hicommand-SSOS start"
    ;;
stop)
    exec_cmd "/etc/init.d/hicommand-SSOS stop"
    ;;
status)
    /etc/init.d/hicommand-SSOS status
    # The result is equal to 1
    if [ $? -eq 1 ]; then
        # running
        RET_CODE=$ALIVE_VALUE
    else
        # not running
        RET_CODE=$DOWN_VALUE
    fi
    exit $RET_CODE
    ;;
*)
    echo "Invalid argument"
    exit 1
esac

exit 0
```

HiRDB の開始用スクリプト

ファイル名 : /etc/init.d/hirdb_start

内容 : 次の内容でファイルを作成してください。

```
#!/bin/sh

PATH=/usr/sbin:/usr/bin:$PDDIR/bin:../usr/cluster/bin
export PATH
PDDIR=<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/HDB
PDCONFPATH=$PDDIR/conf
LD_LIBRARY_PATH=$PDDIR/lib
PDHOST=<論理ホスト名>
export PDDIR PDCONFPATH LD_LIBRARY_PATH PDHOST
```

```
$PDDIR/bin/pdstart
/etc/init.d/hirdb_monitor
```

HiRDB の停止用スクリプト

ファイル名 : /etc/init.d/hirdb_stop

内容 : 次の内容でファイルを作成してください。

```
#!/bin/sh

PATH=/usr/sbin:/usr/bin:$PDDIR/bin:./usr/cluster/bin
export PATH
PDDIR=<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/HDB
PDCONFPATH=$PDDIR/conf
LD_LIBRARY_PATH=$PDDIR/lib
PDHOST=<論理ホスト名>
export PDDIR PDCONFPATH LD_LIBRARY_PATH PDHOST

$PDDIR/bin/pdstop -f -q
```

HiRDB の監視用スクリプト

ファイル名 : /etc/init.d/hirdb_probe

内容 : 次の内容でファイルを作成してください。

```
#!/bin/sh

ps -ef | grep root | grep pdprcd | awk -F' ' '{print $8}' | grep pdprcd
if [ $? = 0 ];then
    echo "exit 0"
    exit 0
else
    echo "exit 1"
    exit 1
fi
```

HiRDB の常駐スクリプト

ファイル名 : /etc/init.d/hirdb_monitor

内容 : 次の内容でファイルを作成してください。

```
#!/bin/sh

trap exit 5
while true
do
    sleep 5
done
exit
```

スクリプトを作成したあとで、次のコマンドを実行し、スクリプトファイルに実行権限を割り当ててください。

```
# chmod u+x <スクリプトファイル名>
```

(5) クラスタリソースの登録 (Veritas Cluster Server の場合)

クラスタリソースを登録する前に、次の作業を実施してください。

- ・ クラスタ化するサービスの集まり (サービスフェールオーバーの単位) であるクラスタグループ (リソースグループ) を用意してください。
- ・ 実行系と待機系で引き継ぎ可能な共有ディスクとクラスタ管理 IP アドレスを含めてリソースグループを構成してください。

- ・ リソースの割り当て、削除および動作監視が Veritas Cluster Server によって正常に制御できることを確認してください。
- ・ すでに、ほかの Hitachi Command Suite 製品が登録されているリソースグループがあれば、そのリソースグループを使用してください。
リソースグループは、Hitachi Command Suite 製品に関連するリソースだけで構成してください。

クラスタリソースを登録するには：

1. Java Console で Cluster Manager を起動します。
2. Veritas Cluster Server の設定ファイルを編集できる状態にします。
[File] メニューから [Open Configuration] を選択します。
3. 「(3) スクリプトの作成 (Veritas Cluster Server の場合)」で作成したファイルをインポートします。
[File] メニューから [Import Types] を選択します。
4. 次のファイルを選択して、[Import] を選択します。
/etc/VRTSvcs/conf/config/HiRDB_STypes.cf
5. Hitachi Command Suite 共通コンポーネント、Device Manager サーバおよび Tiered Storage Manager サーバのサービスをリソースとして登録します。
[Edit] メニューから、[Add], [Resource] の順に選択して [Add Resource] ダイアログを表示し、「表 8-14 HiRDB をリソースとして登録するための設定」～「表 8-19 Tiered Storage Manager サーバをリソースとして登録するための設定」の設定を行い [OK] を選択します。

表 8-14 HiRDB をリソースとして登録するための設定

項目名	設定内容
Resource Name	HiRDB (任意)
Resource Type	HiRDB_S
PdDir	< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /HDB
PdConfPath	< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /HDB/conf
Ld_Library_Path	< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /HDB/lib
DummyFilePath	< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /HDB/.pdveritas
Critical	False

表 8-15 HBase Storage Mgmt Common Service をリソースとして登録するための設定

項目名	設定内容
Resource Name	BaseCommonService (任意)
Resource Type	Application
Start Program Attribute	Scalar Values : /etc/init.d/hicommand-SSOS start
Stop Program Attribute	Scalar Values : /etc/init.d/hicommand-SSOS stop
PidFiles Attribute	/var/< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /tmp/HiCommand.pid

表 8-16 HBase Storage Mgmt Web Service をリソースとして登録するための設定

項目名	設定内容
Resource Name	BaseWebService (任意)
Resource Type	Application
Start Program Attribute	Scalar Values : /etc/init.d/hicommand-CWS start
Stop Program Attribute	Scalar Values : /etc/init.d/hicommand-CWS stop
PidFiles Attribute	/var/< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/httpsd/logs/httpd.pid

表 8-17 HCS Device Manager Web Service をリソースとして登録するための設定

項目名	設定内容
Resource Name	HCSDeviceManagerWebService (任意)
Resource Type	Application
Start Program Attribute	Scalar Values : /etc/init.d/hicommand-DM start
Stop Program Attribute	Scalar Values : /etc/init.d/hicommand-DM stop
PidFiles Attribute	/var/< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/tmp/DeviceManagerWebService.pid

表 8-18 HiCommandServer をリソースとして登録するための設定

項目名	設定内容
Resource Name	HiCommandServer (任意)
Resource Type	Application
Start Program Attribute	Scalar Values : /etc/init.d/hicommand start
Stop Program Attribute	Scalar Values : /etc/init.d/hicommand stop
Monitor Processes Attribute	Vector Values : /bin/sh < Device Manager サーバのインストールディレクトリ >/HiCommandServer/hicmdserver

表 8-19 Tiered Storage Manager サーバをリソースとして登録するための設定

項目名	設定内容
Resource Name	TieredStorageManager (任意)
Resource Type	Application
Start Program Attribute	Scalar Values : /etc/init.d/htsmsserver start
Stop Program Attribute	Scalar Values : /etc/init.d/htsmsserver stop
Monitor Processes Attribute	Vector Values : /bin/sh < Tiered Storage Manager サーバのインストールディレクトリ >/htsmservice



注意 Hitachi Command Suite 共通コンポーネントが起動中、何かの原因で強制終了した場合には、幾つかの一時ファイルが削除されずに残ってしまいます。これらのファイルが待機系ノードにある場合は、Hitachi Command Suite 共通コンポーネントが停止していても、Veritas Cluster Server のログに Hitachi Command Suite 共通コンポーネントをオフラインにできないという内容のエラーメッセージが出力されます。エラーは出力されますが、Hitachi Command Suite の動作には問題ありません。エラーが出力されないようにするには、次の手順を実行してください。

- hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスが停止していることを確認します。
- /var/< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/tmp ディレクトリの HiCommand.pid を削除してください。

- ・ /var/<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/httpd/logs ディレクトリの httpd.pid を削除してください。

6. リソースの依存関係を設定します。
次の順序で、Hitachi Command Suite 製品が登録されているリソースグループの各リソースの依存関係を設定します。下位のリソースが上位のリソースに依存しています。
 - 共有ディスクのデバイスファイル
 - 共有ディスクのマウントポイントおよび IP アドレス
 - HiRDB
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HCS Device Manager Web Service
 - HiCommandServer
 - Tiered Storage Manager上記のリソース名は、手順 5 で登録したリソース名で表示されます。
7. Veritas Cluster Server の設定ファイルに変更内容を保存します。
[File] メニューから [Save Configuration] を選択します。
8. Veritas Cluster Server の設定ファイルを閉じます。
[File] メニューから [Close Configuration] を選択します。
9. リソースを有効にして、Cluster Manager を終了します。

関連項目

- ・ 9.4 サービスの稼働状態の確認

(6) クラスタリソースの登録 (Sun Cluster の場合)

クラスタリソースを登録する前に、次の作業を実施してください。

- ・ クラスタ化するサービスの集まり (サービスフェールオーバーの単位) であるクラスタグループ (リソースグループ) を用意してください。
- ・ 実行系と待機系で引き継ぎ可能な共有ディスクとクラスタ管理 IP アドレスを含めてリソースグループを構成してください。
- ・ リソースの割り当て、削除および動作監視が Sun Cluster によって正常に制御できることを確認してください。
- ・ すでに、ほかの Hitachi Command Suite 製品が登録されているリソースグループがあれば、そのリソースグループを使用してください。
リソースグループは、Hitachi Command Suite 製品に関連するリソースだけで構成してください。

Sun Cluster では、Sun Cluster が提供する scrgadm コマンドを使用して、リソースを登録します。scrgadm コマンドの書式や使用方法については、Sun Cluster のマニュアルを参照してください。

クラスタリソースを登録するには：

1. HiRDB をリソースに登録します。
scrgadm コマンドのパラメーターには次の値を指定します。

表 8-20 HiRDB をリソースとして登録するためのパラメーターと設定値

項目名	設定内容
リソースタイプ	SUNW.gds
リソース名	HiRDB (任意)
関連するネットワーク	hdvm_ip
依存するリソース	SharedDisk
サービスの開始コマンド	/etc/init.d/hirdb_start*
サービスの停止コマンド	/etc/init.d/hirdb_stop*
サービスの監視コマンド	/etc/init.d/hirdb_probe*
使用するポート番号	23032/tcp (デフォルト)

注※ サービスの開始、停止、監視コマンドには、「(4) スクリプトの作成 (Sun Cluster の場合)」で作成したスクリプトを登録します。

コマンドの実行例を次に示します。

```
# /usr/cluster/bin/scrgadm -a -j HiRDB -g HiCommand -t SUNW.gds
-y Network_resources_used=hdvm_ip
-y Resource_dependencies=SharedDisk
-x Start_command="/etc/init.d/hirdb_start"
-x Stop_command="/etc/init.d/hirdb_stop"
-x Probe_command="/etc/init.d/hirdb_probe"
-y Port_list="23032/tcp"
```

2. HBase Storage Mgmt Common Service をリソースに登録します。

scrgadm コマンドのパラメーターには次の値を指定します。

表 8-21 HBase Storage Mgmt Common Service をリソースとして登録するためのパラメーターと設定値

項目名	設定内容
リソースタイプ	SUNW.gds
リソース名	BaseCommonService (任意)
関連するネットワーク	なし
依存するリソース	HiRDB
サービスの開始コマンド	/etc/init.d/sc_hicommand-SSOS start*
サービスの停止コマンド	/etc/init.d/sc_hicommand-SSOS stop*
サービスの監視コマンド	/etc/init.d/sc_hicommand-SSOS status*
使用するポート番号	23017/tcp (デフォルト)

注※ HBase Storage Mgmt Common Service をリソースに登録する前に、/etc/init.d/sc_hicommand-SSOS を作成してください。作成方法については、「(4) スクリプトの作成 (Sun Cluster の場合)」を参照してください。

コマンドの実行例を次に示します。

```
# /usr/cluster/bin/scrgadm -a -j BaseCommonService -g HiCommand
-t SUNW.gds
-y Resource_dependencies=HiRDB
-x Start_command="/etc/init.d/sc_hicommand-SSOS start"
-x Stop_command="/etc/init.d/sc_hicommand-SSOS stop"
-x Probe_command="/etc/init.d/sc_hicommand-SSOS status"
-y Port_list="23017/tcp"
```

3. HBase Storage Mgmt Web Service をリソースに登録します。

scrgadm コマンドのパラメーターには次の値を指定します。

表 8-22 HBase Storage Mgmt Web Service をリソースとして登録するためのパラメーターと設定値

項目名	設定内容
リソースタイプ	SUNW.gds
リソース名	BaseWebService (任意)
関連するネットワーク	hdvm_ip
依存するリソース	BaseCommonService
サービスの開始コマンド	/etc/init.d/sc_hicommand-CWS start [※]
サービスの停止コマンド	/etc/init.d/sc_hicommand-CWS stop [※]
サービスの監視コマンド	/etc/init.d/sc_hicommand-CWS status [※]
使用するポート番号	非 SSL の場合 : 23015/tcp (デフォルト) SSL の場合 : 23016/tcp (デフォルト)

注※ HBase Storage Mgmt Web Service をリソースに登録する前に、/etc/init.d/sc_hicommand-CWS を作成してください。作成方法については、「(4) スクリプトの作成 (Sun Cluster の場合)」を参照してください。

コマンドの実行例を次に示します。

```
# /usr/cluster/bin/scrgadm -a -j BaseWebService -g HiCommand -t SUNW.gds
-y Network_resources_used=hdvm_ip
-y Resource_dependencies=BaseCommonService
-x Start_command="/etc/init.d/sc_hicommand-CWS start"
-x Stop_command="/etc/init.d/sc_hicommand-CWS stop"
-x Probe_command="/etc/init.d/sc_hicommand-CWS status"
-y Port_list="23015/tcp"
```

4. HCS Device Manager Web Service をリソースに登録します。

scrgadm コマンドのパラメーターには次の値を指定します。

表 8-23 HCS Device Manager Web Service をリソースとして登録するためのパラメーターと設定値

項目名	設定内容
リソースタイプ	SUNW.gds
リソース名	HCSDeviceManagerWebService (任意)
関連するネットワーク	hdvm_ip
依存するリソース	BaseWebService
サービスの開始コマンド	/etc/init.d/sc_hicommand-CWS start [※]
サービスの停止コマンド	/etc/init.d/sc_hicommand-CWS stop [※]
サービスの監視コマンド	/etc/init.d/sc_hicommand-CWS status [※]
使用するポート番号	23025/tcp (デフォルト)

注※ HCS Device Manager Web Service をリソースに登録する前に、/etc/init.d/sc_hicommand-DM を作成してください。作成方法については、「(4) スクリプトの作成 (Sun Cluster の場合)」を参照してください。

コマンドの実行例を次に示します。

```
# /usr/cluster/bin/scrgadm -a -j HCSDeviceManagerWebService -g HiCommand -t
SUNW.gds
-y Network_resources_used=hdvm_ip
```

```

-y Resource_dependencies=BaseWebService
-x Start_command="/etc/init.d/sc_hicommand-DM start"
-x Stop_command="/etc/init.d/sc_hicommand-DM stop"
-x Probe_command="/etc/init.d/sc_hicommand-DM status"
-y Port_list="23025/tcp"

```

5. HiCommandServer をリソースに登録します。

scrgadm コマンドのパラメーターには次の値を指定します。

表 8-24 HiCommandServer をリソースとして登録するためのパラメーターと設定値

項目名	設定内容
リソースタイプ	SUNW.gds
リソース名	HiCommandServer (任意)
関連するネットワーク	hdvm_ip
依存するリソース	BaseWebService
サービスの開始コマンド	/etc/init.d/hicommand start
サービスの停止コマンド	/etc/init.d/hicommand stop
サービスの監視コマンド	/etc/init.d/hicommand status2
使用するポート番号	非 SSL の場合 : 2001/tcp (デフォルト) SSL の場合 : 2443/tcp (デフォルト)

コマンドの実行例を次に示します。

```

# /usr/cluster/bin/scrgadm -a -j HiCommandServer -g HiCommand -t SUNW.gds
-y Network_resources_used=hdvm_ip
-y Resource_dependencies=BaseWebService
-x Start_command="/etc/init.d/hicommand start"
-x Stop_command="/etc/init.d/hicommand stop"
-x Probe_command="/etc/init.d/hicommand status2"
-y Port_list=2001/tcp

```

6. HiCommand Tiered Storage Manager をリソースに登録します。

scrgadm コマンドのパラメーターには次の値を指定します。

表 8-25 HiCommand Tiered Storage Manager をリソースとして登録するためのパラメーターと設定値

項目名	設定内容
リソースタイプ	SUNW.gds
リソース名	TieredStorageManager (任意)
関連するネットワーク	hdvm_ip
依存するリソース	HiCommandServer
サービスの開始コマンド	< Tiered Storage Manager のインストールディレクトリ >/bin/htsmserver start
サービスの停止コマンド	< Tiered Storage Manager のインストールディレクトリ >/bin/htsmserver stop
サービスの監視コマンド	/usr/bin/pgrep htmservice
使用するポート番号	非 SSL の場合 : 20352/tcp (デフォルト) SSL の場合 : 24500/tcp (デフォルト)

コマンドの実行例を次に示します。

```

# /usr/cluster/bin/scrgadm -a -j TieredStorageManager -g HiCommand -t SUNW.gds

```

```
-y Network_resources_used=hdvm_ip
-y Resource_dependencies=HiCommandServer
-x Start_command="/opt/HiCommand/TieredStorageManager/bin/htsmsserver start"
-x Stop_command="/opt/HiCommand/TieredStorageManager/bin/htsmsserver stop"
-x Probe_command="/usr/bin/pgrep htmservice"
-y Port_list=20352/tcp
```

8.3.2 アップグレードまたは上書きインストール (Solaris)

ここでは、クラスタ構成の管理サーバに Hitachi Command Suite をアップグレードまたは上書きインストールする方法を説明します。



注意 クラスタ環境のセットアップでは、Hitachi Command Suite のサービスの停止を伴う操作を実行します。セットアップ中は、Hitachi Command Suite にアクセスしないでください。

(1) Veritas Cluster Server での準備作業

次の操作を実行してください。

1. 実行系ノードで、Hitachi Command Suite 製品のサービスを登録しているリソースグループをオンラインにします。
2. 実行系ノードで、次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service (バージョン 7.0 以降からアップグレードまたは上書きインストールした場合)
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
3. 実行系ノードで hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
4. 実行系ノードで、HiRDB のサービスをオフラインにします。
5. 待機系ノードで手順 1～手順 4 と同様の操作を実行します。
6. Veritas Cluster Server で、次に示すサービスを右クリックして、コンテキストメニューにある [Enabled] のチェックを外します。
実行系ノードまたは待機系ノードで実施してください。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service (バージョン 7.0 以降からアップグレードまたは上書きインストールした場合)
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDB
 - 上記以外に手順 2 でオフラインにしたサービス
7. 実行系ノードの Veritas Cluster Server で、Cluster Explorer ウィンドウの [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているリソースグループを右クリックして、コンテキストメニューから [Freeze] - [Temporary] を選択します。

関連項目

- 9.3 サービスの停止

(2) Sun Cluster での準備作業

実行系ノードおよび待機系ノードで次の操作を実行してください。

1. Hitachi Command Suite 製品のサービスを登録しているリソースグループをオンラインにします。
2. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント (HiRDB を除く)、Device Manager および Tiered Storage Manager のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j BaseWebService
# /usr/cluster/bin/scswitch -n -M -j HCSDeviceManagerWebService (バージョン 7.0 以降からアップグレードまたは上書きインストールした場合)
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j BaseCommonService
# /usr/cluster/bin/scswitch -n -M -j TieredStorageManager
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースの監視を無効にしてください。

3. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント (HiRDB を除く)、Device Manager および Tiered Storage Manager のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j HCSDeviceManagerWebService (バージョン 7.0 以降からアップグレードまたは上書きインストールした場合)
# /usr/cluster/bin/scswitch -n -j BaseWebService
# /usr/cluster/bin/scswitch -n -j BaseCommonService
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースを無効にしてください。

4. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
5. 次のコマンドを実行して、HiRDB のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

6. 次のコマンドを実行して、HiRDB のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

関連項目

- 9.3 サービスの停止

(3) 実行系ノードでの手順

実行系ノードにインストールされている Hitachi Command Suite をアップグレードまたは上書きインストールする場合の手順を次に示します。

1. 実行系ノードおよび待機系ノードから共有ディスクにアクセスできることを確認します。
2. Hitachi Command Suite をアップグレードまたは上書きインストールします。
インストーラーの指示に従って、アップグレードまたは上書きインストール前のデータベースをバックアップまたはエクスポートしてください。

3. 次のコマンドを実行して、アップグレードまたは上書きインストール後のデータベースをバックアップします。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdsbackups -dir <バックアップファイルの格納先ディレクトリ> -auto
```

dir

データベースのバックアップファイルを格納するローカルディスク上のディレクトリを絶対パスで指定します。

dir オプションに指定するディレクトリが空であることを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



重要 hcmdsbackups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先ディレクトリに database というディレクトリが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

4. Hitachi Command Suite 共通コンポーネントが起動中の場合は、hcmdssrv コマンドを実行して Hitachi Command Suite 製品のサービスを停止します。
5. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスがマシンの起動時に自動的に開始しないようにします。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdssrv -starttype manual -all
```

6. Device Manager サーバおよび Tiered Storage Manager サーバがマシンの起動時に自動的に開始しないようにします。次のファイルを別ディレクトリに移動するか、ファイル名を変更します。ファイル名を変更する場合は、変更後のファイル名の先頭文字に K と S は使用しないでください。

/etc/rc3.d/S99hicommand (Device Manager の場合)

/etc/rc3.d/S99htmsserver (Tiered Storage Manager の場合)

7. Hitachi Command Suite 製品のサービスを登録しているリソースグループを待機系ノードに移動します。

Veritas Cluster Server の場合 :

Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているリソースグループを右クリックして、コンテキストメニューから次の操作を順に実行します。

[Unfreeze] を選択します。

[Switch To] - [<ホスト名>] を選択します。

[Freeze] - [Temporary] を選択します。

Sun Cluster の場合 :

次のコマンドを実行します。

```
/usr/cluster/bin/scswitch -z -g <リソースグループ名> -h <ホスト名>
```

関連項目

- 9.3 サービスの停止
- Hitachi Command Suite のインストール方法 : マニュアル「*Hitachi Command Suite Software インストールガイド*」
- Replication Manager と Business Continuity Manager が連携している環境に Hitachi Command Suite をインストールする方法 : マニュアル「*Hitachi Command Suite Replication Manager Software システム構成ガイド*」

(4) 待機系ノードでの手順

待機系ノードにインストールされている Hitachi Command Suite をアップグレードまたは上書きインストールする場合の手順を次に示します。

1. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
2. Hitachi Command Suite をアップグレードまたは上書きインストールします。
3. Hitachi Command Suite 共通コンポーネントが起動中の場合は、hcmdssrv コマンドを実行して Hitachi Command Suite 製品のサービスを停止します。
4. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスがマシンの起動時に自動的に開始しないようにします。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdssrv -starttype manual -all
```

5. Device Manager サーバおよび Tiered Storage Manager サーバがマシンの起動時に自動的に開始しないようにします。次のファイルを別ディレクトリに移動するか、ファイル名を変更します。ファイル名を変更する場合は、変更後のファイル名の先頭文字に K と S は使用しないでください。

```
/etc/rc3.d/S99hicommand (Device Manager の場合)
```

```
/etc/rc3.d/S99htsmserver (Tiered Storage Manager の場合)
```

関連項目

- 9.3 サービスの停止
- Hitachi Command Suite のインストール方法：マニュアル「*Hitachi Command Suite Software インストールガイド*」
- Replication Manager と Business Continuity Manager が連携している環境に Hitachi Command Suite をインストールする方法：マニュアル「*Hitachi Command Suite Replication Manager Software システム構成ガイド*」

(5) クラスタリソースの設定 (Veritas Cluster Server の場合)

7.0 よりも前のバージョンからアップグレードインストールした場合には、HCS Device Manager Web Service をクラスタリソースとして登録する必要があります。クラスタリソースの登録の方法については、「(5) クラスタリソースの登録 (Veritas Cluster Server の場合)」を参照してください。

Veritas Cluster Server での設定の手順を次に示します。

1. Java Console で Cluster Manager を起動します。
2. Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているリソースグループを右クリックして、コンテキストメニューから [Unfreeze] を選択します。
3. Hitachi Command Suite 製品のサービスを登録しているリソースグループを右クリックして、コンテキストメニューから [Enable Resources] を選択します。
4. Veritas Cluster Server の設定ファイルに変更内容を保存します。[File] メニューから [Save Configuration] を選択します。
5. Veritas Cluster Server の設定ファイルを閉じます。[File] メニューから [Close Configuration] を選択します。
6. 実行系ノードで、Hitachi Command Suite 製品のサービスを登録しているリソースグループをオンラインにします。

(6) クラスタリソースの設定 (Sun Cluster の場合)

7.0 よりも前のバージョンからアップグレードインストールした場合には、HCS Device Manager Web Service のスクリプトを作成し、クラスタリソースとして登録する必要があります。スクリプトの作成方法については、「(4) スクリプトの作成 (Sun Cluster の場合)」を参照してください。クラスタリソースの登録の方法については、「(6) クラスタリソースの登録 (Sun Cluster の場合)」を参照してください。

Sun Cluster での設定の手順を次に示します。

1. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager のサービスおよび Tiered Storage Manager のサービスを有効にします。

```
# /usr/cluster/bin/scswitch -e -j HiRDB
# /usr/cluster/bin/scswitch -e -j BaseCommonService
# /usr/cluster/bin/scswitch -e -j BaseWebService
# /usr/cluster/bin/scswitch -e -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -j HiCommandServer
# /usr/cluster/bin/scswitch -e -j TieredStorageManager
```

上記以外の Hitachi Command Suite 製品のリソースを無効にしていた場合は、同様にリソースを有効にしてください。

2. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager のサービスおよび Tiered Storage Manager のサービスの監視を有効にします。

```
# /usr/cluster/bin/scswitch -e -M -j HiRDB
# /usr/cluster/bin/scswitch -e -M -j BaseCommonService
# /usr/cluster/bin/scswitch -e -M -j BaseWebService
# /usr/cluster/bin/scswitch -e -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer
# /usr/cluster/bin/scswitch -e -M -j TieredStorageManager
```

上記以外の Hitachi Command Suite 製品のリソースの監視を無効にしていた場合は、同様にリソースの監視を有効にしてください。

8.3.3 クラスタ環境への変更 (Solaris)

非クラスタ構成で Device Manager, Tiered Storage Manager または Replication Manager のシステムの運用を開始したあとで、クラスタ構成に変更したい場合は、次の手順で変更してください。ここでは、すでに運用中の Device Manager サーバ、Tiered Storage Manager サーバおよび Replication Manager サーバがインストールされたマシンを実行系ノードとする場合を想定して説明します。



注意 クラスタ環境のセットアップでは、Hitachi Command Suite のサービスの停止を伴う操作を実行します。セットアップ中は、Hitachi Command Suite にアクセスしないでください。

管理サーバの OS が Solaris の場合に、運用開始後にクラスタ環境に変更する手順を次に示します。

1. Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager のサービスをいったん停止します。
2. 待機系ノードとなるマシンに Hitachi Command Suite をインストールします。
3. GUI で待機系ノードにアクセスして、使用する製品のライセンスを登録します。
インストールする製品ごとに、ライセンスキーの入力が必要です。
4. 実行系ノードで次のコマンドを実行して、GUI を起動するための URL を論理ホスト名に変更します。

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/
hcmdschgurl /change http://<実行系ノードの IP アドレスまたはホスト名>:<ポート
番号> http://<論理ホスト名>:<ポート番号>

5. 実行系および待機系の各ノードで、テキストエディターを使ってクラスタ設定ファイルを作成します。

実行系ノードの場合

```
mode=online  
virtualhost=<論理ホスト名>  
onlinehost=<実行系ノードのホスト名>  
standbyhost=<待機系ノードのホスト名>
```

待機系ノードの場合

```
mode=standby  
virtualhost=<論理ホスト名>  
onlinehost=<実行系ノードのホスト名>  
standbyhost=<待機系ノードのホスト名>
```

作成したファイルは、cluster.conf というファイル名で、< Hitachi Command Suite 共通
コンポーネントのインストールディレクトリ > /conf に格納します。



注意

- mode には、実行系ノードの場合は online、待機系ノードの場合は standby を指定してください。
- virtualhost, onlinehost, standbyhost には IP アドレスは指定できません。ホスト名から IP アドレスの名前解決ができることを確認してください。
- virtualhost に指定する論理ホスト名には、有効でアクセスできる IP アドレスが割り当てられている必要があります。

6. 実行系および待機系の各ノードで、server.properties ファイルを開き、
server.http.host プロパティに論理ホスト名を指定します。
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/config/
server.properties

7. 次のコマンドを実行して、実行系ノードでデータベースをバックアップします。
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/
hcmdsbackups -dir <バックアップファイルの格納先ディレクトリ > -auto

dir

データベースのバックアップファイルを格納するローカルディスク上のディレクトリを絶対パスで指定します。

dir オプションに指定するディレクトリが空であることを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



重要 hcmdsbackups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先ディレクトリに database というディレクトリが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

8. HiRDB が使用するポートをデフォルト (23032/tep) 以外のポートに変更して運用している場合は、使用しているポート番号を控えておきます。
9. 次のコマンドを実行して、実行系ノードでデータベースを共有ディスクに移行します。

< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/
hcmdsdbclustersetup -createcluster -databasepath <データベースの再作成先
ディレクトリ > -exportpath <データベースの退避先ディレクトリ > -auto

createcluster

非クラスタ構成の Hitachi Command Suite 製品をクラスタ構成へ移行するためのオプションです。

databasepath

データベースの再作成先ディレクトリを指定します。共有ディスク上のディレクトリを、63 バイト以内の絶対パスで指定してください。

パスに使用できる文字を次に示します。そのほかに、スラント (/) をパスの区切り文字として使用できます。パス中に空白は指定できません。

A~Z a~z 0~9 . _

exportpath

データベースの退避先ディレクトリを指定します。ローカルディスク上のディレクトリを、63 バイト以内の絶対パスで指定してください。パスに使用できる文字は、databasepath に指定できる文字と同じです。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



注意

- hcmsdbclustersetup コマンドを実行すると、HiRDB が使用するポート番号の設定がデフォルト値 (23032/tcp) に戻ります。
- hcmsdbclustersetup コマンドを実行すると、Tuning Manager のリモート接続の設定が初期化されます。
- <データベースの退避先ディレクトリ>がすでにある場合は、ディレクトリの中を空にするか、ディレクトリを削除してください。
- hcmsdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。
- hcmsdbclustersetup コマンドが異常終了した状態でサーバを再起動すると、共有ディスクの接続先が待機系ノードに切り替わることがあります。

10. 待機系ノードで次のコマンドを実行して、共有ディスク上のデータベースを使用するように設定を変更します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmsdbclustersetup -createcluster -databasepath <データベースの再作成先  
ディレクトリ> -exportpath <データベースの退避先ディレクトリ> -auto
```

hcmsdbclustersetup コマンドに指定するオプションについては、手順 9 を参照してください。databasepath には、実行系ノードで指定した<データベースの再作成先ディレクトリ>と同じディレクトリを指定してください。

11. 実行系および待機系の各ノードで、hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスが停止していることを確認します。
12. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスがマシンの起動時に自動的に開始しないようにします。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdssrv -starttype manual -all
```

13. 実行系および待機系の各ノードで、Device Manager サーバおよび Tiered Storage Manager サーバがマシンの起動時に自動的に開始しないようにします。

次のファイルを別ディレクトリに移動するか、ファイル名を変更します。ファイル名を変更する場合は、変更後のファイル名の先頭文字に K と S は使用しないでください。

```
/etc/rc3.d/S99hicommand (Device Manager の場合)
```

```
/etc/rc3.d/S99htsmsserver (Tiered Storage Manager の場合)
```

14. クラスタ環境で必要な設定をします。
「(5) クラスタリソースの登録 (Veritas Cluster Server の場合)」または「(6) クラスタリソースの登録 (Sun Cluster の場合)」に従って、クラスタリソースを登録してください。
15. 非クラスタ環境で運用していた時に Tuning Manager とリモート接続していた場合は、必要に応じて、Tuning Manager のサービスを起動したあと、Tuning Manager と連携するための設定を再度実施します。

関連項目

- (3) Tuning Manager サーバとのリモート接続 (Veritas Cluster Server)
- (4) Tuning Manager サーバとのリモート接続 (Sun Cluster)
- 9.4 サービスの稼働状態の確認
- Tuning Manager のサービスを起動および停止する方法：インストールされている Tuning Manager に対応するバージョンのマニュアル
- Hitachi Command Suite のインストール方法：マニュアル「*Hitachi Command Suite Software インストールガイド*」

8.3.4 アンインストール (Solaris)

ここでは、管理サーバの OS が Solaris で、クラスタ構成となっている場合に、Hitachi Command Suite をアンインストールする手順について説明します。

(1) アンインストール (Veritas Cluster Server の場合)

アンインストールの手順を次に示します。

1. Cluster Manager (Java Console) を起動します。
2. Hitachi Command Suite 製品のサービスを登録しているリソースグループを、実行系ノードに移動します。
Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているリソースグループを右クリックして、コンテキストメニューから次の操作を順に実行します。
 - [Unfreeze] を選択します。
 - [Switch To] - [<ホスト名>] を選択します。
3. 次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
4. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
5. 次のサービスをオフラインにします。
 - HiRDB
6. 次のリソースがほかの製品で使われていない場合は削除します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer

- HCS Device Manager Web Service
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDB



注意 IP アドレスおよび共有ディスクのリソースは、この手順では削除しないでください。

7. 削除しないリソースについては、右クリックのコンテキストメニューから [Enabled] のチェックを外します。
8. Cluster Explorer ウィンドウの [Service Groups] タブを選択します。
9. Hitachi Command Suite 製品のサービスを登録しているリソースグループを右クリックして、コンテキストメニューから [Freeze] - [Temporary] を選択します。
10. 次のコマンドを実行して、データベースをバックアップします。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdsbackups -dir <バックアップファイルの格納先ディレクトリ > -auto
```

dir

データベースのバックアップファイルを格納するローカルディスク上のディレクトリを絶対パスで指定します。

dir オプションに指定するディレクトリが空であることを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



重要 hcmdsbackups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先ディレクトリに database というディレクトリが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

11. hcmdsdrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
12. 実行系ノードで Hitachi Command Suite をアンインストールします。



注意 クラスタ環境でのインストール中に作成された不要なディレクトリおよびファイルは手動で削除してください。

13. Hitachi Command Suite 製品のサービスを登録していたリソースグループを、待機系ノードに移動します。

Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録していたリソースグループを右クリックして、コンテキストメニューから次の操作を順に実行します。

- [Unfreeze] を選択します。
- [Switch To] - [<ホスト名>] を選択します。
- [Freeze] - [Temporary] を選択します。

14. 待機系ノードで Hitachi Command Suite をアンインストールします。



注意 クラスタ環境でのインストール中に作成された不要なディレクトリおよびファイルは手動で削除してください。

15. 次のリソースがほかの製品で使われていない場合は削除します。
 - IP アドレス
 - 共有ディスク

16. Hitachi Command Suite 製品のサービスを登録しているリソースグループが不要になった場合は、リソースグループを削除します。
17. リソースグループを削除しない場合は、Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているリソースグループを右クリックして、コンテキストメニューから [Unfreeze] を選択します。
18. 手順 7 で無効にしたリソースを有効にします。

関連項目

- 9.3 サービスの停止
- Hitachi Command Suite のアンインストール方法：マニュアル「*Hitachi Command Suite Software インストールガイド*」

(2) アンインストール (Sun Cluster の場合)

アンインストールの手順を次に示します。

1. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスを登録しているリソースグループを実行系ノードに移動します。


```
# /usr/cluster/bin/scswitch -z -g <リソースグループ名> -h <ホスト名>
```
2. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager および Tiered Storage Manager のリソースの監視を無効にします。


```
# /usr/cluster/bin/scswitch -n -M -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -M -j BaseWebService
# /usr/cluster/bin/scswitch -n -M -j BaseCommonService
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```
3. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント (HiRDB を除く)、Device Manager および Tiered Storage Manager のリソースを無効にします。


```
# /usr/cluster/bin/scswitch -n -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -j BaseWebService
# /usr/cluster/bin/scswitch -n -j BaseCommonService
```
4. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
5. 次のコマンドを実行して、HiRDB のリソースを無効にします。


```
# /usr/cluster/bin/scswitch -n -j HiRDB
```
6. 次のリソースがほかの製品で使われていない場合は削除します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDB



注意 IP アドレスおよび共有ディスクのリソースは、この手順では削除しないでください。

7. 次のコマンドを実行して、データベースをバックアップします。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdsbackups -dir <バックアップファイルの格納先ディレクトリ> -auto
```

```
dir
```

データベースのバックアップファイルを格納するローカルディスク上のディレクトリを絶対パスで指定します。

dir オプションに指定するディレクトリが空であることを確認してください。

```
auto
```

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。



重要 hcmdsbackups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先ディレクトリに database というディレクトリが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

8. hcmdsdrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
9. 実行系ノードで Hitachi Command Suite をアンインストールします。



注意 クラスタ環境でのインストール中に作成された不要なディレクトリおよびファイルは手動で削除してください。

10. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスを登録していたリソースグループを待機系ノードに移動します。
/usr/cluster/bin/scswitch -z -g <リソースグループ名> -h <ホスト名>
11. 待機系ノードで Hitachi Command Suite をアンインストールします。



注意 クラスタ環境でのインストール中に作成された不要なディレクトリおよびファイルは手動で削除してください。

12. 次のリソースがほかの製品で使われていない場合は削除します。
 - IP アドレス
 - 共有ディスク
13. Hitachi Command Suite 製品のサービスを登録しているリソースグループが不要になった場合は、リソースグループを削除します。
14. リソースグループを削除しない場合は、削除しなかったサービスに対して、次のコマンドを実行します。
/usr/cluster/bin/scswitch -e -j <サービス名>
/usr/cluster/bin/scswitch -e -M -j <サービス名>

関連項目

- 9.3 サービスの停止
- Hitachi Command Suite のアンインストール方法：マニュアル「*Hitachi Command Suite Software* インストールガイド」

サービスの起動と停止

この章では、管理サーバ上の Hitachi Command Suite 製品のサービスを起動したり停止したりする方法について説明します。

- 9.1 Hitachi Command Suite の常駐プロセス
- 9.2 サービスの起動
- 9.3 サービスの停止
- 9.4 サービスの稼働状態の確認

9.1 Hitachi Command Suite の常駐プロセス

Hitachi Command Suite (Device Manager, Tiered Storage Manager および Replication Manager) の運用では、常駐プロセスが OS 上で稼働していることが前提となります。

Device Manager, Tiered Storage Manager および Replication Manager の常駐プロセスを次の表に示します。

表 9-1 常駐プロセス (Windows の場合)

プロセス名	サービス名	機能
htsmService.exe	HiCommand Tiered Storage Manager	Tiered Storage Manager サーバ
HiCommandServer	HiCommandServer	Device Manager サーバ
hcmdssvctl.exe cjstartweb.exe	HBase Storage Mgmt Common Service	Hitachi Command Suite サブレットサービス Device Manager サーバとほかの Hitachi Command Suite 製品が同じマシンにインストールされている場合、HBase Storage Mgmt Common Service 以外のサービスのプロセスが、hcmdssvctl.exe および cjstartweb.exe という名称で起動されることがあります。
httpsd.exe	HBase Storage Mgmt Web Service	Hitachi Command Suite 共通 Web サービス このプロセスは複数起動されていることがあります。
httpsd.exe	HBase Storage Mgmt Web SSO Service ^{※1}	シングルサインオン用の Hitachi Command Suite 共通 Web サービス
hcmdssvctl.exe cjstartweb.exe	HCS Device Manager Web Service	Device Manager のサブレットサービス
hntr2mon.exe	Hitachi Network Objectplaza Trace	Hitachi Command Suite 共通トレースログ採取 (統合トレースログ情報の採取)
hntr2srv.exe	Monitor 2 Hitachi Network Objectplaza Trace Monitor 2 (x64) ^{※2}	Hitachi Command Suite 共通トレースサービス ([サービス] ウィンドウからのイベントの処理)
pdservice.exe ^{※3}	HiRDB/ EmbeddedEdition_HD0	HiRDB のプロセスサーバの制御

注※1

クラスタリソースへの登録はしないでください。

注※2

Windows (x64) の場合だけ表示されます。

注※3

常に起動していることが前提です。手動での停止や、クラスタリソースへの登録はしないでください。

表 9-2 常駐プロセス (Solaris または Linux の場合)

プロセス名	機能
htsmService	Tiered Storage Manager サーバ
hicmdserver	Device Manager サーバ Solaris の場合 : /bin/sh < Device Manager サーバのインストールディレクトリ > /HiCommandServer/hicmdserver Linux の場合 :

プロセス名	機能
	< Device Manager サーバのインストールディレクトリ > / HiCommandServer/hicmdserver
hcmdssso cjstartweb	Hitachi Command Suite サブレットサービス /bin/sh < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /CC/web/containers/HiCommand/hcmdssso < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /CC/web/bin/cjstartweb
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /httpsd/sbin/httpsd	Hitachi Command Suite 共通 Web サービス このプロセスは複数起動されていることがあります。
hcmdsdm cjstartweb	Device Manager のサブレットサービス /bin/sh < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /CC/web/containers/ DeviceManagerWebService/hcmdsdm < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /CC/web/bin/cjstartweb
/opt/hitachi/ HNTRLib2/bin/hntr2mon	Hitachi Command Suite 共通トレースログ採取 (統合トレースログ情報の採取)
pdprcd*	HiRDB のプロセスサーバプロセス

注※

常に起動していることが前提です。手動での停止や、クラスタリソースへの登録はしないでください。

関連項目

- [9.2 サービスの起動](#)
- [9.3 サービスの停止](#)
- [9.4 サービスの稼働状態の確認](#)
- [12.2.1 Host Data Collector の常駐プロセス](#)

9.2 サービスの起動

Windows メニューまたは hcmdssrv コマンドを使って、Hitachi Command Suite 製品のサービスを起動します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

サービスを起動するには：

1. 次の操作を実行します。

Windows の場合：

次のどれかの方法でサービスを起動します。

Windows XP, Windows Server 2003 R2, Windows Vista, Windows 7, Windows Server 2008 または Windows Server 2008 R2 の場合

[スタート] - [すべてのプログラム] - [Hitachi Command Suite] - [Manage Services] - [Start - HCS] を選択します。

Windows Server 2012 の場合

スタート画面からアプリケーションの一覧画面を表示し、[Hitachi Command Suite] の [Start - HCS] を選択します。

コマンドを実行する場合

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmdssrv /start
```

Solaris または Linux の場合 :

次のコマンドを実行します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdssrv -start
```

次のサービスが一括で起動され、各サービスを起動した結果が画面に表示されます。

- HiRDB
- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Web SSO Service (Windows の場合だけ)
- HCS Device Manager Web Service
- HiCommandServer
- HiCommand Tiered Storage Manager
- 同一マシンにインストールされた Hitachi Command Suite 製品のサービス



注意 05-70 より前のバージョンのほかの Hitachi Command Suite 製品のサービスは同時に起動しません。



参考 Hitachi Command Suite 製品のサービスを起動しても、Storage Navigator Modular 2 のサービスは起動しません。

Storage Navigator Modular 2 のサービスを起動するには、次の手順を実行してください。

Windows の場合 :

次のどちらかの方法を実行してください。

- [サービス] ウィンドウから、[SNM2 Server] - [サービスの開始] を選択する。
- コマンドプロンプトから次のコマンドを実行する。

```
net start snm2server
```

Solaris または Linux の場合 :

root でのログイン後、次のコマンドを実行してください。

```
/etc/init.d/snm2srv start
```

関連項目

- 05-70 より前のバージョンの Hitachi Command Suite 製品のサービスを起動する方法 : 各 Hitachi Command Suite 製品のバージョンに対応するマニュアル

9.3 サービスの停止

Windows メニューまたは `hcmdssrv` コマンドを使って、Hitachi Command Suite 製品のサービスを停止します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

サービスを停止するには：

1. 次の操作を実行します。

Windows の場合：

次のどれかの方法でサービスを停止します。

Windows XP, Windows Server 2003 R2, Windows Vista, Windows 7, Windows Server 2008 または Windows Server 2008 R2 の場合

[スタート] - [すべてのプログラム] - [Hitachi Command Suite] - [Manage Services] - [Stop - HCS] を選択します。

Windows Server 2012 の場合

スタート画面からアプリケーションの一覧画面を表示し、[Hitachi Command Suite] の [Stop - HCS] を選択します。

コマンドを実行する場合

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmdssrv /stop
```

Solaris または Linux の場合：

次のコマンドを実行します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdssrv -stop
```

次のサービスが一括で停止され、各サービスを停止した結果が画面に表示されます。

- HiRDB
- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Web SSO Service (Windows の場合だけ)
- HCS Device Manager Web Service
- HiCommandServer
- HiCommand Tiered Storage Manager
- 同一マシンにインストールされた Hitachi Command Suite 製品のサービス



注意

- 05-70 より前のバージョンのほかの Hitachi Command Suite 製品のサービスは同時に停止しません。
- Solaris または Linux 環境では、Hitachi Command Suite 共通コンポーネントの起動処理が完了していない状態で、Hitachi Command Suite 共通コンポーネントを停止しないでください。サービスの常駐プロセスが起動しているにも関わらずサービスの状態表示が停止していると表示されたり、サービスの停止ができなくなったりする場合があります。このような状態になった場合は、マシンを再起動してください。



参考 Hitachi Command Suite 製品のサービスを停止しても、Storage Navigator Modular 2 のサービスは停止しません。

Storage Navigator Modular 2 のサービスを停止するには、次の手順を実行してください。

Windows の場合 :

次のどちらかの方法を実行してください。

- ・ [サービス] ウィンドウから, [SNM2 Server] - [サービスの停止] を選択する。
- ・ コマンドプロンプトから次のコマンドを実行する。

```
net stop snm2server
```

Solaris または Linux の場合 :

root でのログイン後, 次のコマンドを実行してください。

```
/etc/init.d/snm2srv stop
```

関連項目

- ・ 05-70 より前のバージョンの Hitachi Command Suite 製品のサービスを停止する方法 : 各 Hitachi Command Suite 製品のバージョンに対応するマニュアル

9.4 サービスの稼働状態の確認

Windows メニューまたは `hcmdssrv` コマンドを使って, 各 Hitachi Command Suite 製品のサービスの稼働状態を確認します。

事前に完了しておく操作

- ・ Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

サービスの稼働状態を確認するには :

1. 次の操作を実行します。

Windows の場合 :

次のどれかの方法でサービスの稼働状態を確認します。

Windows XP, Windows Server 2003 R2, Windows Vista, Windows 7, Windows Server 2008 または Windows Server 2008 R2 の場合

[スタート] - [すべてのプログラム] - [Hitachi Command Suite] - [Manage Services] - [Status - HCS] を選択します。

Windows Server 2012 の場合

スタート画面からアプリケーションの一覧画面を表示し, [Hitachi Command Suite] の [Status - HCS] を選択します。

コマンドを実行する場合

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > \bin  
hcmdssrv /statusall
```

Solaris または Linux の場合 :

次のコマンドを実行します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdssrv -statusall
```

各サービスの稼働状態が画面に表示されます。

データベースの管理

この章では、Hitachi Command Suite 製品のデータベースをバックアップしたり、復元したりする方法について説明します。

- 10.1 データベースを管理する前に
- 10.2 データベースのバックアップ
- 10.3 データベースの復元
- 10.4 データベースの移行

10.1 データベースを管理する前に

バックアップと復元，エクスポートとインポートについて，機能の違いを次の表に示します。

表 10-1 バックアップ・復元とエクスポート・インポートの違い

項目	バックアップと復元	エクスポートとインポート
Hitachi Command Suite 製品のバージョンの条件	制限なし。	エクスポート元およびインポート先に，バージョン 05-50 以降の Hitachi Command Suite 製品がインストールされていること。
主な使用目的	サーバマシンに障害が発生したときに，現状の運用環境を復元すること。	サーバマシンを，別の OS のマシンなど現状とは異なる環境に移行すること。
対象となるデータ	<ul style="list-style-type: none"> Hitachi Command Suite 製品のデータベース Hitachi Command Suite 共通コンポーネントのデータベース 	<ul style="list-style-type: none"> Hitachi Command Suite 製品のデータベース Hitachi Command Suite 共通コンポーネントのデータベースに含まれるユーザー情報
マシン条件	<ul style="list-style-type: none"> バックアップ元マシンと復元先マシンで，インストールされている Hitachi Command Suite 製品の種類が一致していること バックアップ元マシンと復元先マシンで，インストールされている Hitachi Command Suite 製品のバージョンおよびリビジョンが一致していること 	<ul style="list-style-type: none"> インポート先マシンに，インポート対象の Hitachi Command Suite 製品がインストールされていること インポート先マシンにインストールされている Hitachi Command Suite 製品のバージョンおよびリビジョンが，エクスポート元と同じか，それ以上であること

以降で，各操作の手順を説明します。

10.2 データベースのバックアップ

データベースに障害が発生した場合，管理サーバを運用できなくなるおそれがあります。障害の発生に備えて，データベースのバックアップを定期的にとってください。

データベースをバックアップするときには，バックアップファイルを格納するディレクトリが必要です。バックアップファイルを格納するディレクトリには，バックアップ時に作成される一時ファイルの分も含めて次の空き容量が必要です。

必要な空き容量：

$$(\text{バックアップ対象となる Hitachi Command Suite 製品のデータベースサイズの総和} + 2.5\text{GB}) \times 2$$

例えば，Device Manager，Tiered Storage Manager，および Replication Manager を使用している環境の場合は，次のディレクトリの容量を考慮して，バックアップに必要な容量を見積もります。

- Device Manager のデータベースの格納先ディレクトリ
- Tiered Storage Manager のデータベースの格納先ディレクトリ
- Replication Manager のデータベースの格納先ディレクトリ
- Hitachi Command Suite 共通コンポーネントのデータベースの格納先ディレクトリ※

注※ Hitachi Command Suite 共通コンポーネントのデータベースの格納先ディレクトリには，BASE ディレクトリと SYS ディレクトリがあります。

ほかの Hitachi Command Suite 製品を使用している場合は，それらのデータベースの容量も考慮してください。



注意

- Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager のサービスをいったん停止しておく必要があります。データベースのバックアップが完了したあと、Tuning Manager のサービスを再開させてください。Tuning Manager のサービスを停止および起動する方法については、インストールされている Tuning Manager に対応するバージョンのマニュアルを参照してください。
- データベースのバックアップでは、Hitachi Command Suite のサービスの停止を伴う操作を実行します。バックアップ中は、Hitachi Command Suite にアクセスしないでください。

10.2.1 データベースのバックアップ（非クラスタ構成の場合）

管理サーバの OS が非クラスタ構成の場合に、データベースをバックアップする手順を説明します。

1. Administrator 権限または root 権限のユーザーで管理サーバにログインします。
2. hcmsbackups コマンドを実行してデータベースをバックアップします。

Windows の場合：

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmsbackups /dir <バックアップファイルの格納先フォルダ> /auto
```

Solaris または Linux の場合：

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmsbackups -dir <バックアップファイルの格納先ディレクトリ > -auto
```

dir

データベースのバックアップファイルを格納するローカルディスク上のディレクトリを絶対パスで指定します。Solaris または Linux の場合は、パスには空白を含めないようにしてください。

dir オプションに指定するディレクトリの下には、ファイルおよびサブディレクトリがないことを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。

hcmsbackups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先ディレクトリに database というディレクトリが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。



重要 dir オプションに指定したバックアップファイルの格納先ディレクトリに作成される database 以外のディレクトリには、Hitachi Command Suite 製品の設定ファイルがバックアップされます。管理サーバの障害によって Hitachi Command Suite 製品を再インストールすることになった場合には、バックアップされた設定ファイルで以前の設定内容を確認できます。

10.2.2 データベースのバックアップ（Microsoft Cluster Service または Windows Server Failover Clustering の場合）

管理サーバの OS が Windows でクラスタ構成の場合に、データベースをバックアップする手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースをバックアップしてください。

データベースをバックアップする手順を次に示します。

1. Administrator 権限のユーザーで管理サーバにログインします。

2. クラスタ管理アプリケーションで次のサービスを選択し、右クリックメニューでオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
3. `hcmdssrv /stop` コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。

そのあと `hcmdssrv /statusall` コマンドを実行して、サービスが停止していること、またはコマンドのリターンコードが 0 であることを確認してください。
4. クラスタ管理アプリケーションで、次のサービスをオフラインにします。
 - HiRDBClusterService_HD0
5. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを抑制します。次のリソースの設定を変更します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDBClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用している場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開しない] を選択します。

Windows Server Failover Clustering を使用している場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで、[リソースが失敗状態になった場合は、再起動しない] を選択します。

6. `hcmdsbackups` コマンドを実行してデータベースをバックアップします。


```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsbackups /dir <バックアップファイルの格納先フォルダ> /auto
```

`dir`

データベースのバックアップファイルを格納する共有ディスク上のフォルダを絶対パスで指定します。

`dir` オプションに指定するディレクトリの下には、ファイルおよびサブフォルダがないことを確認してください。

`auto`

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。

`hcmdsbackups` コマンドを実行すると、`dir` オプションに指定したバックアップファイルの格納先ディレクトリに `database` というディレクトリが作成され、データベースのバックアップファイルが `backup.hdb` というファイル名で格納されます。

7. `hcmdssrv /stop` コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
そのあと `hcmdssrv /statusall` コマンドを実行して、サービスが停止していること、またはコマンドのリターンコードが 0 であることを確認してください。
8. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを有効にします。
次のリソースの設定を変更します。

- HiCommand Tiered Storage Manager
- HiCommandServer
- HCS Device Manager Web Service
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDBClusterService_HD0
- 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用している場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開する] を選択します。

Windows Server Failover Clustering を使用している場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで次の項目を選択します。

- ・ [リソースが失敗状態になった場合は、現在のノードで再起動を試みる]
 - ・ [再起動に失敗した場合は、この役割のすべてのリソースをフェールオーバーする] (または [再起動に失敗した場合は、このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする])
9. クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスを登録しているリソースグループをオンラインにします。

関連項目

- ・ 9.2 サービスの起動
- ・ 9.3 サービスの停止

10.2.3 データベースのバックアップ (Veritas Cluster Server の場合)

管理サーバの OS が Solaris で、使用しているクラスタソフトウェアが Veritas Cluster Server の場合に、データベースをバックアップする手順を説明します。



注意 実行系ノード (`cluster.conf` ファイルの `mode` に `online` が設定されているマシン) でデータベースをバックアップしてください。

データベースをバックアップする手順を次に示します。

1. root 権限のユーザーで管理サーバにログインします。
2. Veritas Cluster Server で、次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service

- HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
3. `hcmdssrv -stop` コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。

そのあと `hcmdssrv -statusall` コマンドを実行して、サービスが停止していること、またはコマンドのリターンコードが 0 であることを確認してください。
 4. Veritas Cluster Server で、次のサービスをオフラインにします。
 - HiRDB
 5. 次のサービスを右クリックして、コンテキストメニューにある [Enabled] のチェックを外します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDB
 - 上記以外の Hitachi Command Suite 製品のリソース
 6. Cluster Explorer ウィンドウの [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Freeze] – [Temporary] を選択します。
 7. `hcmdsbbackups` コマンドを実行してデータベースをバックアップします。


```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/hcmdsbbackups -dir <バックアップファイルの格納先ディレクトリ> -auto
```

dir

データベースのバックアップファイルを格納する共有ディスク上のディレクトリを絶対パスで指定します。パスには空白を含めないようにしてください。

dir オプションに指定するディレクトリの下には、ファイルおよびサブディレクトリがないことを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。

`hcmdsbbackups` コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先ディレクトリに database というディレクトリが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。
 8. `hcmdssrv -stop` コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。

そのあと `hcmdssrv -statusall` コマンドを実行して、サービスが停止していること、またはコマンドのリターンコードが 0 であることを確認してください。
 9. Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Unfreeze] を選択します。
 10. Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Enable Resources] を選択します。
 11. Veritas Cluster Server で、リソースが登録されているグループをオンラインにします。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

10.2.4 データベースのバックアップ（Sun Cluster の場合）

管理サーバの OS が Solaris で、使用しているクラスタソフトウェアが Sun Cluster の場合に、データベースをバックアップする手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースをバックアップしてください。

データベースをバックアップする手順を次に示します。

1. root 権限のユーザーで管理サーバにログインします。
2. 次のコマンドを実行して、Tiered Storage Manager, Device Manager および Hitachi Command Suite 共通コンポーネント (HiRDB を除く) のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -M -j BaseWebService
# /usr/cluster/bin/scswitch -n -M -j BaseCommonService
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースの監視を無効にしてください。

3. 次のコマンドを実行して、Tiered Storage Manager, Device Manager および Hitachi Command Suite 共通コンポーネント (HiRDB を除く) のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -j BaseWebService
# /usr/cluster/bin/scswitch -n -j BaseCommonService
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースを無効にしてください。

4. hcmdssrv -stop コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。

そのあと hcmdssrv -statusall コマンドを実行して、サービスが停止していること、またはコマンドのリターンコードが 0 であることを確認してください。

5. 次のコマンドを実行して、HiRDB のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

6. 次のコマンドを実行して、HiRDB のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

7. hcmdsbackups コマンドを実行してデータベースをバックアップします。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/
hcmdsbackups -dir <バックアップファイルの格納先ディレクトリ > -auto
```

dir

データベースのバックアップファイルを格納する共有ディスク上のディレクトリを絶対パスで指定します。パスには空白を含めないようにしてください。

dir オプションに指定するディレクトリの下には、ファイルおよびサブディレクトリがないことを確認してください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。

hcmdsbackups コマンドを実行すると、dir オプションに指定したバックアップファイルの格納先ディレクトリに database というディレクトリが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

8. hcmdssrv -stop コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。

そのあと hcmdssrv -statusall コマンドを実行して、サービスが停止していること、またはコマンドのリターンコードが 0 であることを確認してください。

9. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager および Tiered Storage Manager のリソースを有効にします。

```
# /usr/cluster/bin/scswitch -e -j HiRDB
# /usr/cluster/bin/scswitch -e -j BaseCommonService
# /usr/cluster/bin/scswitch -e -j BaseWebService
# /usr/cluster/bin/scswitch -e -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -j HiCommandServer
# /usr/cluster/bin/scswitch -e -j TieredStorageManager
```

上記以外に Hitachi Command Suite 製品のリソースを無効にしていた場合は、同様にリソースを有効にしてください。

10. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager および Tiered Storage Manager の監視を有効にします。

```
# /usr/cluster/bin/scswitch -e -M -j HiRDB
# /usr/cluster/bin/scswitch -e -M -j BaseCommonService
# /usr/cluster/bin/scswitch -e -M -j BaseWebService
# /usr/cluster/bin/scswitch -e -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer
# /usr/cluster/bin/scswitch -e -M -j TieredStorageManager
```

上記以外に Hitachi Command Suite 製品のリソースの監視を無効にしていた場合は、同様にリソースの監視を有効にしてください。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

10.3 データベースの復元

データベースに障害が発生した場合、状況に応じて、次の方法で復元できます。

- データベースに不整合が生じた場合

hcmdsbackups コマンドでバックアップしておいたデータベースを使用して、復元できます。

データベースをバックアップした時点の管理サーバと、データベースを復元する時点の管理サーバとで、次のすべてが一致していることが前提です。

- インストールされている Hitachi Command Suite 製品の種類、バージョンおよびリビジョン
 - 各 Hitachi Command Suite 製品のインストール先
 - Hitachi Command Suite 共通コンポーネントのインストール先
 - 各 Hitachi Command Suite 製品のデータベースのインストール先
 - Hitachi Command Suite 共通コンポーネントのデータベースのインストール先
 - マシンの IP アドレスとホスト名
- データベースが破損した場合

hcmdsdbtrans コマンドでエクスポートしておいたデータベースを使用して、復元できます。データベースをエクスポートした時点の管理サーバと、データベースを復元する時点の管理サーバとで、インストールされている Hitachi Command Suite 製品の種類、バージョンおよびリビジョンが一致していることが前提です。

hcmdsdbrepair コマンドを実行すると、管理サーバにインストールされている全 Hitachi Command Suite 製品のデータベースは強制削除され、エクスポートしておいたデータベースに置き換わります。

10.3.1 データベース不整合時のデータベースの復元

データベースに不整合が生じた場合は、hcmdsbackups コマンドでバックアップしておいたデータベースを使用して、hcmdsdb コマンドで復元します。



注意

- 手順の途中で使用する hcmdbdb コマンドは、実行時に一時ファイルを作成します。バックアップファイルの格納先ディレクトリが次の条件を満たしていることを確認してください。
 - hcmdbdb コマンドを実行するユーザーに書き込み権限がある。
 - 格納しているバックアップファイルと同じ分の空き容量がある。
- Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager のサービスをいったん停止しておく必要があります。データベースの復元が完了したあと、Tuning Manager のサービスを再開させてください。Tuning Manager のサービスを停止および起動する方法については、インストールされている Tuning Manager に対応するバージョンのマニュアルを参照してください。
- データベースの復元では、Hitachi Command Suite のサービスの停止を伴う操作を実行します。復元中は、Hitachi Command Suite にアクセスしないでください。

(1) データベース不整合時のデータベースの復元（非クラスタ構成の場合）

管理サーバの OS が非クラスタ構成の場合に、データベースを復元する手順を説明します。

1. Administrator 権限または root 権限のユーザーで管理サーバにログインします。
2. hcmdbdb コマンドを実行してデータベースを復元します。

Windows の場合：

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin
%hcmdbdb /restore <バックアップファイル> /type <復元する Hitachi Command
Suite 製品の名称 > /auto
```

Solaris または Linux の場合：

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/
hcmdbdb -restore <バックアップファイル> -type <復元する Hitachi Command
Suite 製品の名称 > -auto
```

restore

hcmdsbackups コマンドで取得したデータベースのバックアップファイル (backup.hdb) を絶対パスで指定します。Solaris または Linux の場合、空白を含むパスは指定しないでください。

type

原則として、ALL を指定してください。管理サーバにインストールされているすべての Hitachi Command Suite 製品のデータベースが一括して復元されます。

障害などの理由によって、特定の Hitachi Command Suite 製品のデータベースしか復元できない場合は、次の表に従って復元対象の製品の名称を指定します。

表 10-2 データベースを復元する場合の type オプションの指定値 (非クラスタ構成の場合)

製品	指定値
Device Manager	DeviceManager
Tiered Storage Manager	TieredStorageManager
Replication Manager	ReplicationManager
そのほかの製品	それぞれの製品のマニュアルを参照

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。

- type オプションに DeviceManager を指定した場合は、Device Manager サーバの server.base.initialsynchro プロパティに true を設定します。
- type オプションに TieredStorageManager を指定した場合は、Tiered Storage Manager サーバの server.base.initialsynchro プロパティに true を設定します。
- Tuning Manager とリモート接続していた場合は、データベースの復元によって設定が初期化されるため、htmsetup コマンドを実行して再設定します。
- Hitachi Command Suite 製品のサービスを起動します。
- Device Manager サーバの server.base.initialsynchro プロパティを false に戻します。
- Tiered Storage Manager サーバの server.base.initialsynchro プロパティを false に戻します。
- type オプションに ALL または DeviceManager を指定した場合は、Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
- Replication Manager のセカンダリーサイトにある管理サーバでデータベースを復元した場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
- Device Manager の GUI で、Device Manager のタスクの状態を確認します。
完了していない、またはエラーになっているタスクがあれば、必要に応じてタスクを再作成するか、実行スケジュールを変更してください。
- Tiered Storage Manager のメッセージログを参照します。
リストア後、最初に Tiered Storage Manager を起動したとき、ログファイルに KATS50354-E メッセージが出力されているかを確認します。KATS50354-E には、状態が失敗に変更された Tiered Storage Manager のタスクのタスク ID が出力されます。
- KATS50354-E メッセージに示されているタスクのボリューム情報を参照して、Tiered Storage Manager のタスクが完了しているかを確認します。
マイグレーションタスクだけでなく、シュレディングタスク、ロックタスクが完了しているかどうかも確認してください。

- 完了していない Tiered Storage Manager のタスクを、必要に応じて再度タスクを作成して実行します。

関連項目

- (5) Tuning Manager サーバとのリモート接続およびポート番号の設定 (htmsetup コマンド)
- 9.2 サービスの起動

(2) データベース不整合時のデータベースの復元 (Microsoft Cluster Service または Windows Server Failover Clustering の場合)

管理サーバの OS が Windows でクラスタ構成の場合に、データベースを復元する手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースを復元してください。

- Administrator 権限のユーザーで管理サーバにログインします。
- クラスタ管理アプリケーションで次のサービスを選択し、右クリックメニューでオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
- hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
- クラスタ管理アプリケーションで、次のサービスをオフラインにします。
 - HiRDBClusterService_HD0
- クラスタ管理アプリケーションで、リソースグループのフェールオーバーを抑止します。次のリソースの設定を変更します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDBClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用している場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開しない] を選択します。

Windows Server Failover Clustering を使用している場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで、[リソースが失敗状態になった場合は、再起動しない] を選択します。

- hcmdsdb コマンドを実行してデータベースを復元します。

< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%\hcmdsdb /
restore <バックアップファイル> /type <復元する Hitachi Command Suite 製品の名称>

restore

hcmdsbackups コマンドで取得したデータベースのバックアップファイル (backup.hdb) を絶対パスで指定します。共有ディスクに保存したものを使用してください。

type

原則として、ALL を指定してください。管理サーバにインストールされているすべての Hitachi Command Suite 製品のデータベースが一括して復元されます。

障害などの理由によって、特定の Hitachi Command Suite 製品のデータベースしか復元できない場合は、次の表に従って復元対象の製品の名称を指定します。

表 10-3 データベースを復元する場合の type オプションの指定値 (Microsoft Cluster Service または Windows Server Failover Clustering の場合)

製品	指定値
Device Manager	DeviceManager
Tiered Storage Manager	TieredStorageManager
Replication Manager	ReplicationManager
その他の製品	それぞれの製品のマニュアルを参照

7. type オプションに DeviceManager を指定した場合は、実行系ノードおよび待機系ノードで、Device Manager サーバの server.base.initialsynchro プロパティに true を設定します。
8. type オプションに TieredStorageManager を指定した場合は、実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの server.base.initialsynchro プロパティに true を設定します。
9. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを有効にします。次のリソースの設定を変更します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDBClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用している場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開する] を選択します。

Windows Server Failover Clustering を使用している場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで次の項目を選択します。

- ・ [リソースが失敗状態になった場合は、現在のノードで再起動を試みる]
- ・ [再起動に失敗した場合は、この役割のすべてのリソースをフェールオーバーする] (または [再起動に失敗した場合は、このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする])

10. クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスを登録しているリソースグループをオンラインにします。
11. 実行系ノードおよび待機系ノードで、Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
12. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
13. `type` オプションに ALL または DeviceManager を指定した場合は、Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
14. Replication Manager のセカンダリーサイトにある管理サーバでデータベースを復元した場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
15. Device Manager の GUI で、Device Manager のタスクの状態を確認します。
完了していない、またはエラーになっているタスクがあれば、必要に応じてタスクを再作成するか、実行スケジュールを変更してください。
16. Tiered Storage Manager のメッセージログを参照します。
リストア後、最初に Tiered Storage Manager を起動したとき、ログファイルに KATS50354-E メッセージが出力されているかを確認します。KATS50354-E には、状態が失敗に変更された Tiered Storage Manager のタスクのタスク ID が出力されます。
17. KATS50354-E メッセージに示されているタスクのボリューム情報を参照して、Tiered Storage Manager のタスクが完了しているかを確認します。
マイグレーションタスクだけでなく、シュレディングタスク、ロックングタスクが完了しているかどうかを確認してください。
18. 完了していない Tiered Storage Manager のタスクを、必要に応じて再度タスクを作成して実行します。
19. Tuning Manager とリモート接続していた場合は、データベースの復元によって設定が初期化されるため、再設定します。
「(2) Tuning Manager サーバとのリモート接続 (Microsoft Cluster Service または Windows Server Failover Clustering)」に従って、Tuning Manager とのリモート接続を再設定してください。

関連項目

- 9.3 サービスの停止

(3) データベース不整合時のデータベースの復元 (Veritas Cluster Server の場合)

管理サーバの OS が Solaris で、使用しているクラスタソフトウェアが Veritas Cluster Server の場合に、データベースを復元する手順を説明します。



注意 実行系ノード (`cluster.conf` ファイルの `mode` に `online` が設定されているマシン) でデータベースを復元してください。

データベースを復元する手順を次に示します。

1. `root` 権限のユーザーで管理サーバにログインします。
2. Veritas Cluster Server で、次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service

- HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
3. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
 4. Veritas Cluster Server で、次のサービスをオフラインにします。
 - HiRDB
 5. 次のサービスを右クリックして、コンテキストメニューにある [Enabled] のチェックを外します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDB
 - 上記以外の Hitachi Command Suite 製品のリソース
 6. Cluster Explorer ウィンドウの [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Freeze] - [Temporary] を選択します。
 7. hcmdsdb コマンドを実行してデータベースを復元します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdsdb -restore <バックアップファイル> -type <復元する Hitachi Command Suite  
製品の名称 >
```

restore

hcmdsbackups コマンドで取得したデータベースのバックアップファイル (backup.hdb) を絶対パスで指定します。空白を含むパスは指定しないでください。共有ディスクに保存したものを使用してください。

type

原則として、ALL を指定してください。管理サーバにインストールされているすべての Hitachi Command Suite 製品のデータベースが一括して復元されます。

障害などの理由によって、特定の Hitachi Command Suite 製品のデータベースしか復元できない場合は、次の表に従って復元対象の製品の名称を指定します。

表 10-4 データベースを復元する場合の type オプションの指定値 (Veritas Cluster Server の場合)

製品	指定値
Device Manager	DeviceManager
Tiered Storage Manager	TieredStorageManager
Replication Manager	ReplicationManager
そのほかの製品	それぞれの製品のマニュアルを参照

8. type オプションに DeviceManager を指定した場合は、実行系ノードおよび待機系ノードで、Device Manager サーバの server.base.initialsynchro プロパティに true を設定します。

9. type オプションに TieredStorageManager を指定した場合は、実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの server.base.initialsynchro プロパティに true を設定します。
10. Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Unfreeze] を選択します。
11. Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Enable Resources] を選択します。
12. 実行系ノードおよび待機系ノードで、Device Manager サーバの server.base.initialsynchro プロパティを false に戻します。
13. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの server.base.initialsynchro プロパティを false に戻します。
14. type オプションに ALL または DeviceManager を指定した場合は、Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
15. Replication Manager のセカンダリーサイトにある管理サーバでデータベースを復元した場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
16. Device Manager の GUI で、Device Manager のタスクの状態を確認します。
完了していない、またはエラーになっているタスクがあれば、必要に応じてタスクを再作成するか、実行スケジュールを変更してください。
17. Tiered Storage Manager のメッセージログを参照します。
リストア後、最初に Tiered Storage Manager を起動したとき、ログファイルに KATS50354-E メッセージが出力されているかを確認します。KATS50354-E には、状態が失敗に変更された Tiered Storage Manager のタスクのタスク ID が出力されます。
18. KATS50354-E メッセージに示されているタスクのボリューム情報を参照して、Tiered Storage Manager のタスクが完了しているかを確認します。
マイグレーションタスクだけでなく、シュレディングタスク、ロッキングタスクが完了しているかどうかを確認してください。
19. 完了していない Tiered Storage Manager のタスクを、必要に応じて再度タスクを作成して実行します。
20. Tuning Manager とリモート接続していた場合は、データベースの復元によって設定が初期化されるため、再設定します。
「(3) Tuning Manager サーバとのリモート接続 (Veritas Cluster Server)」に従って、Tuning Manager とのリモート接続を再設定してください。

関連項目

- 9.3 サービスの停止

(4) データベース不整合時のデータベースの復元 (Sun Cluster の場合)

管理サーバの OS が Solaris で、使用しているクラスタソフトウェアが Sun Cluster の場合に、データベースを復元する手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースを復元してください。

データベースを復元する手順を次に示します。

1. root 権限のユーザーで管理サーバにログインします。

2. 次のコマンドを実行して、Tiered Storage Manager, Device Manager および Hitachi Command Suite 共通コンポーネント (HiRDB を除く) のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -M -j BaseWebService
# /usr/cluster/bin/scswitch -n -M -j BaseCommonService
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースの監視を無効にしてください。

3. 次のコマンドを実行して、Tiered Storage Manager, Device Manager および Hitachi Command Suite 共通コンポーネント (HiRDB を除く) のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -j BaseWebService
# /usr/cluster/bin/scswitch -n -j BaseCommonService
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースを無効にしてください。

4. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。

5. 次のコマンドを実行して、HiRDB のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

6. 次のコマンドを実行して、HiRDB のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

7. hcmdsdb コマンドを実行してデータベースを復元します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/
hcmdsdb -restore <バックアップファイル> -type <復元する Hitachi Command Suite
製品の名称 >
```

restore

hcmdsbackups コマンドで取得したデータベースのバックアップファイル (backup.hdb) を絶対パスで指定します。空白を含むパスは指定しないでください。共有ディスクに保存したものを使用してください。

type

原則として、ALL を指定してください。管理サーバにインストールされているすべての Hitachi Command Suite 製品のデータベースが一括して復元されます。

障害などの理由によって、特定の Hitachi Command Suite 製品のデータベースしか復元できない場合は、次の表に従って復元対象の製品の名称を指定します。

表 10-5 データベースを復元する場合の type オプションの指定値 (Sun Cluster の場合)

製品	指定値
Device Manager	DeviceManager
Tiered Storage Manager	TieredStorageManager
Replication Manager	ReplicationManager
そのほかの製品	それぞれの製品のマニュアルを参照

8. type オプションに DeviceManager を指定した場合は、実行系ノードおよび待機系ノードで、Device Manager サーバの server.base.initialsynchro プロパティに true を設定します。
9. type オプションに TieredStorageManager を指定した場合は、実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの server.base.initialsynchro プロパティに true を設定します。
10. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager および Tiered Storage Manager のリソースを有効にします。


```
# /usr/cluster/bin/scswitch -e -j HiRDB
# /usr/cluster/bin/scswitch -e -j BaseCommonService
# /usr/cluster/bin/scswitch -e -j BaseWebService
# /usr/cluster/bin/scswitch -e -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -j HiCommandServer
# /usr/cluster/bin/scswitch -e -j TieredStorageManager
```

 上記以外に Hitachi Command Suite 製品のリソースを無効にしていた場合は、同様にリソースを有効にしてください。
11. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager および Tiered Storage Manager の監視を有効にします。


```
# /usr/cluster/bin/scswitch -e -M -j HiRDB
# /usr/cluster/bin/scswitch -e -M -j BaseCommonService
# /usr/cluster/bin/scswitch -e -M -j BaseWebService
# /usr/cluster/bin/scswitch -e -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer
# /usr/cluster/bin/scswitch -e -M -j TieredStorageManager
```

 上記以外に Hitachi Command Suite 製品のリソースの監視を無効にしていた場合は、同様にリソースの監視を有効にしてください。
12. 実行系ノードおよび待機系ノードで、Device Manager サーバの server.base.initialsynchro プロパティを false に戻します。
13. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの server.base.initialsynchro プロパティを false に戻します。
14. type オプションに ALL または DeviceManager を指定した場合は Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
15. Replication Manager のセカンダリーサイトにある管理サーバでデータベースを復元した場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
16. Device Manager の GUI で、Device Manager のタスクの状態を確認します。
完了していない、またはエラーになっているタスクがあれば、必要に応じてタスクを再作成するか、実行スケジュールを変更してください。
17. Tiered Storage Manager のメッセージログを参照します。
リストア後、最初に Tiered Storage Manager を起動したとき、ログファイルに KATS50354-E メッセージが出力されているかを確認します。KATS50354-E には、状態が失敗に変更された Tiered Storage Manager のタスクのタスク ID が出力されます。
18. KATS50354-E メッセージに示されているタスクのボリューム情報を参照して、Tiered Storage Manager のタスクが完了しているかを確認します。
マイグレーションタスクだけでなく、シュレディングタスク、ロッキングタスクが完了しているかどうかを確認してください。

19. 完了していない Tiered Storage Manager のタスクを、必要に応じて再度タスクを作成して実行します。
20. Tuning Manager とリモート接続していた場合は、データベースの復元によって設定が初期化されるため、再設定します。
「(4) Tuning Manager サーバとのリモート接続 (Sun Cluster)」に従って、Tuning Manager とのリモート接続を再設定してください。

関連項目

- 9.3 サービスの停止

10.3.2 データベース破損時のデータベースの復元

データベースが破損した場合は、hcmdsdbtrans コマンドでエクスポートしておいたデータベースを使用して、hcmdsdbrepair コマンドで復元します。



注意

- Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager のサービスをいったん停止しておく必要があります。データベースの復元が完了したあと、Tuning Manager のサービスを再開させてください。Tuning Manager のサービスを停止および起動する方法については、インストールされている Tuning Manager に対応するバージョンのマニュアルを参照してください。
- データベースの復元では、Hitachi Command Suite のサービスの停止を伴う操作を実行します。復元中は、Hitachi Command Suite にアクセスしないでください。

(1) データベース破損時のデータベースの復元（非クラスタ構成の場合）

管理サーバの OS が非クラスタ構成の場合に、データベースを復元する手順を説明します。

1. Administrator 権限または root 権限のユーザーで管理サーバにログインします。
2. Hitachi Command Suite 製品のサービスを停止します。
3. hcmdsdbrepair コマンドを実行してデータベースを復元します。

Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin  
%hcmdsdbrepair /trans <エクスポートファイル>
```

Solaris または Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdsdbrepair -trans <エクスポートファイル>
```

trans

hcmdsdbtrans コマンドでエクスポートしたデータベースのアーカイブファイルを絶対パスで指定します。Solaris または Linux の場合、空白を含むパスは指定しないでください。

4. Device Manager サーバの server.base.initialsynchro プロパティに true を設定します。
5. Tiered Storage Manager サーバの server.base.initialsynchro プロパティに true を設定します。
6. Tuning Manager とリモート接続していた場合は、データベースの復元によって設定が初期化されるため、htmsetup コマンドを実行して再設定します。
7. Hitachi Command Suite 製品のサービスを起動します。

8. Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
9. Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
10. Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
11. Replication Manager のセカンダリーサイトにある管理サーバでデータベースを復元した場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
12. Device Manager の GUI で、Device Manager のタスクの状態を確認します。
完了していない、またはエラーになっているタスクがあれば、必要に応じてタスクを再作成するか、実行スケジュールを変更してください。
13. Tiered Storage Manager のメッセージログを参照します。
リストア後、最初に Tiered Storage Manager を起動したとき、ログファイルに `KATS50354-E` メッセージが出力されているかを確認します。`KATS50354-E` には、状態が失敗に変更された Tiered Storage Manager のタスクのタスク ID が出力されます。
14. `KATS50354-E` メッセージに示されているタスクのボリューム情報を参照して、Tiered Storage Manager のタスクが完了しているかを確認します。
マイグレーションタスクだけでなく、シュレディングタスク、ロックングタスクが完了しているかどうかとも確認してください。
15. 完了していない Tiered Storage Manager のタスクを、必要に応じて再度タスクを作成して実行します。
16. System アカウントのパスワードはデータベースの復元によって設定が初期化されるため、必要に応じて再設定します。

関連項目

- (5) Tuning Manager サーバとのリモート接続およびポート番号の設定 (`htmsetup` コマンド)
- 9.2 サービスの起動
- 9.3 サービスの停止
- System アカウントのパスワードの変更方法：マニュアル「*Hitachi Command Suite Software ユーザーズガイド*」

(2) データベース破損時のデータベースの復元 (Microsoft Cluster Service または Windows Server Failover Clustering の場合)

管理サーバの OS が Windows でクラスタ構成の場合に、データベースを復元する手順を説明します。



注意 実行系ノード (`cluster.conf` ファイルの `mode` に `online` が設定されているマシン) でデータベースを復元してください。

1. Administrator 権限のユーザーで管理サーバにログインします。
2. クラスタ管理アプリケーションで次のサービスを選択し、右クリックメニューでオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service

- HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
3. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
 4. クラスタ管理アプリケーションで、次のサービスをオフラインにします。
 - HiRDBClusterService_HD0
 5. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを抑制します。次のリソースの設定を変更します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDBClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用している場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開しない] を選択します。

Windows Server Failover Clustering を使用している場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで、[リソースが失敗状態になった場合は、再起動しない] を選択します。

6. hcmdsdbrepair コマンドを実行してデータベースを復元します。
 < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin
 %hcmdsdbrepair /trans <エクスポートファイル>

trans

hcmdsdbtrans コマンドでエクスポートしたデータベースのアーカイブファイルを絶対パスで指定します。

7. 実行系ノードおよび待機系ノードで、Device Manager サーバの server.base.initialsynchro プロパティに true を設定します。
8. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの server.base.initialsynchro プロパティに true を設定します。
9. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを有効にします。次のリソースの設定を変更します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDBClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用している場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開する] を選択します。

Windows Server Failover Clustering を使用している場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで次の項目を選択します。

- ・ [リソースが失敗状態になった場合は、現在のノードで再起動を試みる]
 - ・ [再起動に失敗した場合は、この役割のすべてのリソースをフェールオーバーする] (または [再起動に失敗した場合は、このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする])
10. クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスを登録しているリソースグループをオンラインにします。
 11. 実行系ノードおよび待機系ノードで、Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
 12. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
 13. Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
 14. Replication Manager のセカンダリーサイトにある管理サーバでデータベースを復元した場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
 15. Device Manager の GUI で、Device Manager のタスクの状態を確認します。
完了していない、またはエラーになっているタスクがあれば、必要に応じてタスクを再作成するか、実行スケジュールを変更してください。
 16. Tiered Storage Manager のメッセージログを参照します。
リストア後、最初に Tiered Storage Manager を起動したとき、ログファイルに KATS50354-E メッセージが出力されているかを確認します。KATS50354-E には、状態が失敗に変更された Tiered Storage Manager のタスクのタスク ID が出力されます。
 17. KATS50354-E メッセージに示されているタスクのボリューム情報を参照して、Tiered Storage Manager のタスクが完了しているかを確認します。
マイグレーションタスクだけでなく、シュレディングタスク、ロッキングタスクが完了しているかどうかも確認してください。
 18. 完了していない Tiered Storage Manager のタスクを、必要に応じて再度タスクを作成して実行します。
 19. Tuning Manager とリモート接続していた場合は、データベースの復元によって設定が初期化されるため、再設定します。
「(2) Tuning Manager サーバとのリモート接続 (Microsoft Cluster Service または Windows Server Failover Clustering)」に従って、Tuning Manager とのリモート接続を再設定してください。
 20. System アカウントのパスワードはデータベースの復元によって設定が初期化されるため、必要に応じて再設定します。

関連項目

- ・ [9.3 サービスの停止](#)
- ・ System アカウントのパスワードの変更方法：マニュアル「*Hitachi Command Suite Software ユーザーズガイド*」

(3) データベース破損時のデータベースの復元 (Veritas Cluster Server の場合)

管理サーバの OS が Solaris で、使用しているクラスタソフトウェアが Veritas Cluster Server の場合に、データベースを復元する手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースを復元してください。

データベースを復元する手順を次に示します。

1. root 権限のユーザーで管理サーバにログインします。
2. Veritas Cluster Server で、次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
3. hcmdsrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
4. Veritas Cluster Server で、次のサービスをオフラインにします。
 - HiRDB
5. 次のサービスを右クリックして、コンテキストメニューにある [Enabled] のチェックを外します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDB
 - 上記以外の Hitachi Command Suite 製品のリソース
6. Cluster Explorer ウィンドウの [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Freeze] - [Temporary] を選択します。
7. hcmsdbrepair コマンドを実行してデータベースを復元します。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/  
hcmsdbrepair -trans <エクスポートファイル>  
  
trans  
  
hcmsdbtrans コマンドでエクスポートしたデータベースのアーカイブファイルを絶対パスで指定します。空白を含むパスは指定しないでください。
```
8. 実行系ノードおよび待機系ノードで、Device Manager サーバの server.base.initialsynchro プロパティに true を設定します。
9. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの server.base.initialsynchro プロパティに true を設定します。

10. Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Unfreeze] を選択します。
11. Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Enable Resources] を選択します。
12. 実行系ノードおよび待機系ノードで、Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
13. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
14. Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
15. Replication Manager のセカンダリーサイトにある管理サーバでデータベースを復元した場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
16. Device Manager の GUI で、Device Manager のタスクの状態を確認します。
完了していない、またはエラーになっているタスクがあれば、必要に応じてタスクを再作成するか、実行スケジュールを変更してください。
17. Tiered Storage Manager のメッセージログを参照します。
リストア後、最初に Tiered Storage Manager を起動したとき、ログファイルに KATS50354-E メッセージが出力されているかを確認します。KATS50354-E には、状態が失敗に変更された Tiered Storage Manager のタスクのタスク ID が出力されます。
18. KATS50354-E メッセージに示されているタスクのボリューム情報を参照して、Tiered Storage Manager のタスクが完了しているかを確認します。
マイグレーションタスクだけでなく、シュレディングタスク、ロックングタスクが完了しているかどうかを確認してください。
19. 完了していない Tiered Storage Manager のタスクを、必要に応じて再度タスクを作成して実行します。
20. Tuning Manager とリモート接続していた場合は、データベースの復元によって設定が初期化されるため、再設定します。
「(3) Tuning Manager サーバとのリモート接続 (Veritas Cluster Server)」に従って、Tuning Manager とのリモート接続を再設定してください。
21. System アカウントのパスワードはデータベースの復元によって設定が初期化されるため、必要に応じて再設定します。

関連項目

- 9.3 サービスの停止
- System アカウントのパスワードの変更方法：マニュアル「Hitachi Command Suite Software ユーザーズガイド」

(4) データベース破損時のデータベースの復元 (Sun Cluster の場合)

管理サーバの OS が Solaris で使用しているクラスタソフトウェアが Sun Cluster の場合に、データベースを復元する手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースを復元してください。

データベースを復元する手順を次に示します。

1. root 権限のユーザーで管理サーバにログインします。
2. 次のコマンドを実行して、Tiered Storage Manager, Device Manager および Hitachi Command Suite 共通コンポーネント (HiRDB を除く) のリソースの監視を無効にします。


```
# /usr/cluster/bin/scswitch -n -M -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -M -j BaseWebService
# /usr/cluster/bin/scswitch -n -M -j BaseCommonService
```

 上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースの監視を無効にしてください。
3. 次のコマンドを実行して、Tiered Storage Manager, Device Manager および Hitachi Command Suite 共通コンポーネント (HiRDB を除く) のリソースを無効にします。


```
# /usr/cluster/bin/scswitch -n -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -j BaseWebService
# /usr/cluster/bin/scswitch -n -j BaseCommonService
```

 上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースを無効にしてください。
4. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
5. 次のコマンドを実行して、HiRDB のリソースの監視を無効にします。


```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```
6. 次のコマンドを実行して、HiRDB のリソースを無効にします。


```
# /usr/cluster/bin/scswitch -n -j HiRDB
```
7. hcmdsdbrepair コマンドを実行してデータベースを復元します。


```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/
hcmdsdrepair -trans <エクスポートファイル>
```

trans

hcmdsdbrtrans コマンドでエクスポートしたデータベースのアーカイブファイルを絶対パスで指定します。空白を含むパスは指定しないでください。
8. 実行系ノードおよび待機系ノードで、Device Manager サーバの server.base.initialsynchro プロパティに true を設定します。
9. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの server.base.initialsynchro プロパティに true を設定します。
10. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント, Device Manager および Tiered Storage Manager のリソースを有効にします。


```
# /usr/cluster/bin/scswitch -e -j HiRDB
# /usr/cluster/bin/scswitch -e -j BaseCommonService
# /usr/cluster/bin/scswitch -e -j BaseWebService
# /usr/cluster/bin/scswitch -e -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -j HiCommandServer
# /usr/cluster/bin/scswitch -e -j TieredStorageManager
```

 上記以外に Hitachi Command Suite 製品のリソースを無効にしていた場合は、同様にリソースを有効にしてください。

11. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager および Tiered Storage Manager の監視を有効にします。

```
# /usr/cluster/bin/scswitch -e -M -j HiRDB
# /usr/cluster/bin/scswitch -e -M -j BaseCommonService
# /usr/cluster/bin/scswitch -e -M -j BaseWebService
# /usr/cluster/bin/scswitch -e -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer
# /usr/cluster/bin/scswitch -e -M -j TieredStorageManager
```

上記以外に Hitachi Command Suite 製品のリソースの監視を無効にしていた場合は、同様にリソースの監視を有効にしてください。

12. 実行系ノードおよび待機系ノードで、Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
13. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
14. Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
15. Replication Manager のセカンダリーサイトにある管理サーバでデータベースを復元した場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
16. Device Manager の GUI で、Device Manager のタスクの状態を確認します。
完了していない、またはエラーになっているタスクがあれば、必要に応じてタスクを再作成するか、実行スケジュールを変更してください。
17. Tiered Storage Manager のメッセージログを参照します。
リストア後、最初に Tiered Storage Manager を起動したとき、ログファイルに `KATS50354-E` メッセージが出力されているかを確認します。`KATS50354-E` には、状態が失敗に変更された Tiered Storage Manager のタスクのタスク ID が出力されます。
18. `KATS50354-E` メッセージに示されているタスクのボリューム情報を参照して、Tiered Storage Manager のタスクが完了しているかを確認します。
マイグレーションタスクだけでなく、シュレディングタスク、ロックングタスクが完了しているかどうかを確認してください。
19. 完了していない Tiered Storage Manager のタスクを、必要に応じて再度タスクを作成して実行します。
20. Tuning Manager とリモート接続していた場合は、データベースの復元によって設定が初期化されるため、再設定します。
「(4) Tuning Manager サーバとのリモート接続 (Sun Cluster)」に従って、Tuning Manager とのリモート接続を再設定してください。
21. System アカウントのパスワードはデータベースの復元によって設定が初期化されるため、必要に応じて再設定します。

関連項目

- [9.3 サービスの停止](#)
- System アカウントのパスワードの変更方法：マニュアル「*Hitachi Command Suite Software ユーザーズガイド*」

10.4 データベースの移行

Hitachi Command Suite 製品を長期間使用していると、Hitachi Command Suite 製品のバージョンアップや管理対象となるオブジェクトの増加によって、今までよりも高性能なマシンが必要になる場合があります。このような場合、マシンの入れ替え作業の1つとしてデータベースを移行する必要があります。

Hitachi Command Suite 製品では、`hcmsdbtrans` コマンドを使用してデータベースを移行できます。`hcmsdbtrans` コマンドは、各 Hitachi Command Suite 製品のデータベースに格納されているすべての情報と、Hitachi Command Suite 共通コンポーネントが管理しているユーザー情報を移行するコマンドです。

`hcmsdbtrans` コマンドを使用すると、次に示すような、使用中の管理サーバとは異なる環境のマシンにもデータベースを移行できます。

- ・ 異なるプラットフォームのマシンへの移行
- ・ Hitachi Command Suite 製品のインストール先が異なるマシンへの移行
- ・ Hitachi Command Suite 製品のバージョンが移行元のバージョンよりも新しいマシンへの移行



重要 [レプリケーション] タブを使用している場合は、管理サーバの環境を新しいマシンに移行する際に、収集した性能情報を引き継ぐための手順を実行する必要があります。手順どおりに実行しないと、性能情報のデータが消えるおそれがあります。詳細は、「ソフトウェア添付資料」を参照してください。

10.4.1 データベースを移行する場合の注意事項

移行先と移行元の Hitachi Command Suite 製品のデータベース、種類、バージョン、およびユーザー情報についての注意事項を次に示します。

Hitachi Command Suite 製品のデータベース、種類、およびバージョンについての注意事項

- 移行元サーバに次の製品がインストールされている場合は、データベースをエクスポートする前に、移行元サーバおよび移行先サーバで、バージョン 6.0 以降へのアップグレードインストールが必要です。

Replication Monitor 5.x 以前

Tuning Manager 5.x 以前

バージョン 6.0 以降にアップグレードできない場合、またはデータベースの移行が不要の場合は、データベースのインポート対象から外してください。

- Tuning Manager のデータベースを移行する場合、次の制約があります。

Tuning Manager のデータベースは、移行元と移行先で同じ総容量に設定してください。データベースの総容量を変更する方法については、マニュアル「*Hitachi Command Suite Tuning Manager Software 運用管理ガイド*」を参照してください。

移行元と移行先のデータベースの構成 (Small または Medium) が同じか、または移行先のデータベースの構成が大きくなる組み合わせの場合に移行できます。

移行元のデータベースの構成で、管理対象となるリソース数が管理限界の 70% を超える場合には、同じデータベースの構成には移行できません。

- 移行元の管理サーバに Global Link Manager がインストールされている場合、データベースのインポート対象から外してください。Global Link Manager のデータベースの移行が必要なときは、移行先サーバにインストールされている Global Link Manager のバージョンに対応したマニュアルに従ってデータベースを移行してください。
- バージョン 6.x 以前の Device Manager がインストールされた環境でエクスポートしたデータベースを、バージョン 7.0 以降の環境にインポートできるのは、バージョン 7.0 以降の新規インストール後 1 回だけです。バージョン 7.0 以降の上書きインストール後や移行

先サーバでの運用開始後には、バージョン 6.x 以前のデータベースを再度インポートしないでください。

ユーザー情報についての注意事項

- 移行先にユーザー情報がある場合、そのユーザー情報は移行元のユーザー情報に置き換えられます。このため、すでに Hitachi Command Suite 製品のユーザー情報があるマシンへの移行は行わないでください。
- ユーザー情報が置き換えられるため、複数の管理サーバで稼働していた Hitachi Command Suite 製品を 1 台の管理サーバに集約するような移行はできません。

10.4.2 データベースを移行する流れ

データベースを移行する手順の流れは次のとおりです。

1. 移行先サーバに、データベースを移行する Hitachi Command Suite 製品をインストールします。
 2. hcmsdbtrans コマンドで移行元サーバでデータベースをエクスポートします。
 3. 移行元サーバから移行先サーバへアーカイブファイルを転送します。
 4. hcmsdbtrans コマンドで移行先サーバでデータベースをインポートします。
- 以降で、各手順の詳細を説明します。

10.4.3 移行先サーバへの Hitachi Command Suite 製品のインストール

移行先サーバに、データベースを移行する Hitachi Command Suite 製品をインストールしてください。移行先にインストールされていない Hitachi Command Suite 製品のデータベースは移行できません。移行先には、必要な Hitachi Command Suite 製品を漏れなくインストールしてください。

移行先サーバにインストールする Hitachi Command Suite 製品のバージョンは、移行元の Hitachi Command Suite 製品と同じか、それ以上にしてください。移行先にインストールされている Hitachi Command Suite 製品のバージョンがどれか 1 つでも移行元より古い場合、移行はできません。

10.4.4 移行元サーバでのデータベースのエクスポート

Hitachi Command Suite 製品のデータベースをエクスポートするときには、データベースの情報を一時的に格納するためのディレクトリと、アーカイブファイルを格納するディレクトリが必要です。それぞれのディレクトリには、次に示すディレクトリの合計サイズと同等の容量を確保してください。

- ・ インストールされている Hitachi Command Suite 製品の各データベースの格納先ディレクトリ
- ・ Hitachi Command Suite 共通コンポーネントのデータベースの格納先ディレクトリから SYS ディレクトリ以下を除いたもの



注意

- ・ データベースはアーカイブファイルとしてエクスポートされます。データベースの全体容量が 2GB を超えている場合、データベースのエクスポート時に、アーカイブファイルの作成に失敗します。この場合は、アーカイブファイルの代わりに、エクスポート時に収集されるデータベース情報を移行先に転送します。
- ・ Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager のサービスをいったん停止しておく必要があります。データベースのエクスポート

が完了したあと、**Tuning Manager** のサービスを再開させてください。**Tuning Manager** のサービスを停止および起動する方法については、インストールされている **Tuning Manager** に対応するバージョンのマニュアルを参照してください。

- データベースのエクスポートでは、**Hitachi Command Suite** のサービスの停止を伴う操作を実行します。エクスポート中は、**Hitachi Command Suite** にアクセスしないでください。

(1) データベースのエクスポート（非クラスタ構成の場合）

管理サーバの OS が非クラスタ構成の場合に、移行元サーバでデータベースをエクスポートする手順を次に示します。

- Administrator 権限または root 権限のユーザーで管理サーバにログインします。
- hcmsdbtrans コマンドを実行してデータベースをエクスポートします。

Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin  
%hcmsdbtrans /export /workpath <作業用フォルダ> /file <アーカイブファイ  
ル> /auto
```

Solaris または Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmsdbtrans -export -workpath <作業用ディレクトリ> -file <アーカイブ  
ファイル> -auto
```

workpath

データベース情報を一時的に配置するための作業用ディレクトリを、絶対パスで指定します。Solaris または Linux の場合、空白を含むパスは指定しないでください。ローカルディスクのディレクトリを指定してください。

workpath オプションに指定するディレクトリの下には、ファイルおよびサブディレクトリがないことを確認してください。

file

出力されるアーカイブファイルの名称を絶対パスで指定します。Solaris または Linux の場合は、パスに空白を含まないようにしてください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。

- アーカイブファイルを移行先サーバに転送します。
アーカイブファイルを作成できなかった場合、workpath オプションで指定したディレクトリに格納されているファイルをすべて転送してください。このとき、workpath オプションで指定したディレクトリ以下のファイル構成は変更しないでください。

(2) データベースのエクスポート（Microsoft Cluster Service または Windows Server Failover Clustering の場合）

管理サーバの OS が Windows でクラスタ構成の場合に、移行元サーバでデータベースをエクスポートする手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースをエクスポートしてください。

データベースをエクスポートする手順を次に示します。

- Administrator 権限のユーザーで管理サーバにログインします。

2. クラスタ管理アプリケーションで次のサービスを選択し、右クリックメニューでオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
3. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
4. クラスタ管理アプリケーションで、次のサービスをオフラインにします。
 - HiRDBClusterService_HD0
5. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを抑止します。次のリソースの設定を変更します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDBClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用している場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開しない] を選択します。

Windows Server Failover Clustering を使用している場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで、[リソースが失敗状態になった場合は、再起動しない] を選択します。

6. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを起動します。
7. hcmdbdbtrans コマンドを実行してデータベースをエクスポートします。
`<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>\bin
 %hcmdbdbtrans /export /workpath <作業用フォルダ> /file <アーカイブファイル
 >`

workpath

データベース情報を一時的に配置するための作業用フォルダを、絶対パスで指定します。ローカルディスクのフォルダを指定してください。workpath オプションに指定するフォルダの下には、ファイルおよびサブフォルダがないことを確認してください。

file

出力されるアーカイブファイルの名称を絶対パスで指定します。

8. アーカイブファイルを移行先サーバに転送します。
 アーカイブファイルを作成できなかった場合、workpath オプションで指定したフォルダに格納されているファイルをすべて転送してください。このとき、workpath オプションで指定したフォルダ以下のファイル構成は変更しないでください。

9. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
10. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを有効にします。
次のリソースの設定を変更します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDBClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用している場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開する] を選択します。

Windows Server Failover Clustering を使用している場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで次の項目を選択します。

- ・ [リソースが失敗状態になった場合は、現在のノードで再起動を試みる]
- ・ [再起動に失敗した場合は、この役割のすべてのリソースをフェールオーバーする] (または [再起動に失敗した場合は、このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする])

11. クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスを登録しているリソースグループをオンラインにします。

関連項目

- ・ 9.2 サービスの起動
- ・ 9.3 サービスの停止

(3) データベースのエクスポート (Veritas Cluster Server の場合)

管理サーバの OS が Solaris で、使用しているクラスタソフトウェアが Veritas Cluster Server の場合に、移行元サーバでデータベースをエクスポートする手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースをエクスポートしてください。

データベースをエクスポートする手順を次に示します。

1. root 権限のユーザーで管理サーバにログインします。
2. Veritas Cluster Server で、次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
3. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。

4. Veritas Cluster Server で、次のサービスをオフラインにします。
 - HiRDB
5. 次のサービスを右クリックして、コンテキストメニューにある [Enabled] のチェックを外します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDB
 - 上記以外の Hitachi Command Suite 製品のリソース
6. Cluster Explorer ウィンドウの [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Freeze] - [Temporary] を選択します。
7. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを起動します。
8. hcmsdbtrans コマンドを実行してデータベースをエクスポートします。


```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmsdbtrans -export -workpath <作業用ディレクトリ> -file <アーカイブファイル>
```

workpath

データベース情報を一時的に配置するための作業用ディレクトリを、絶対パスで指定します。空白を含むパスは指定しないでください。ローカルディスクのディレクトリを指定してください。workpath オプションに指定するディレクトリの下には、ファイルおよびサブディレクトリがないことを確認してください。

file

出力されるアーカイブファイルの名称を絶対パスで指定します。パスに空白を含まないようにしてください。
9. アーカイブファイルを移行先サーバに転送します。

アーカイブファイルを作成できなかった場合、workpath オプションで指定したディレクトリに格納されているファイルをすべて転送してください。このとき、workpath オプションで指定したディレクトリ以下のファイル構成は変更しないでください。
10. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
11. Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Unfreeze] を選択します。
12. Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Enable Resources] を選択します。
13. Veritas Cluster Server で、リソースが登録されているグループをオンラインにします。

関連項目

- [9.2 サービスの起動](#)
- [9.3 サービスの停止](#)

(4) データベースのエクスポート (Sun Cluster の場合)

管理サーバの OS が Solaris で、使用しているクラスタソフトウェアが Sun Cluster の場合に、移行元サーバでデータベースをエクスポートする手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースをエクスポートしてください。

データベースをエクスポートする手順を次に示します。

1. root 権限のユーザーで管理サーバにログインします。
2. 次のコマンドを実行して、Tiered Storage Manager, Device Manager および Hitachi Command Suite 共通コンポーネント (HiRDB を除く) のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -M -j BaseWebService
# /usr/cluster/bin/scswitch -n -M -j BaseCommonService
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースの監視を無効にしてください。

3. 次のコマンドを実行して、Tiered Storage Manager, Device Manager および Hitachi Command Suite 共通コンポーネント (HiRDB を除く) のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -j BaseWebService
# /usr/cluster/bin/scswitch -n -j BaseCommonService
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースを無効にしてください。

4. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
5. 次のコマンドを実行して、HiRDB のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

6. 次のコマンドを実行して、HiRDB のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

7. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを起動します。

8. hcmdsdbtrans コマンドを実行してデータベースをエクスポートします。

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/
hcmdsdbtrans -export -workpath <作業用ディレクトリ> -file <アーカイブファイル>
```

workpath

データベース情報を一時的に配置するための作業用ディレクトリを、絶対パスで指定します。空白を含むパスは指定しないでください。ローカルディスクのディレクトリを指定してください。

workpath オプションに指定するディレクトリの下には、ファイルおよびサブディレクトリがないことを確認してください。

file

出力されるアーカイブファイルの名称を絶対パスで指定します。パスに空白を含まないようにしてください。

9. アーカイブファイルを移行先サーバに転送します。
アーカイブファイルを作成できなかった場合、workpath オプションで指定したディレクトリに格納されているファイルをすべて転送してください。このとき、workpath オプションで指定したディレクトリ以下のファイル構成は変更しないでください。
10. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
11. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager および Tiered Storage Manager のリソースを有効にします。

```
# /usr/cluster/bin/scswitch -e -j HiRDB
# /usr/cluster/bin/scswitch -e -j BaseCommonService
# /usr/cluster/bin/scswitch -e -j BaseWebService
# /usr/cluster/bin/scswitch -e -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -j HiCommandServer
# /usr/cluster/bin/scswitch -e -j TieredStorageManager
```

上記以外に Hitachi Command Suite 製品のリソースを無効にしていた場合は、同様にリソースを有効にしてください。

12. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager および Tiered Storage Manager の監視を有効にします。

```
# /usr/cluster/bin/scswitch -e -M -j HiRDB
# /usr/cluster/bin/scswitch -e -M -j BaseCommonService
# /usr/cluster/bin/scswitch -e -M -j BaseWebService
# /usr/cluster/bin/scswitch -e -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer
# /usr/cluster/bin/scswitch -e -M -j TieredStorageManager
```

上記以外に Hitachi Command Suite 製品のリソースの監視を無効にしていた場合は、同様にリソースの監視を有効にしてください。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

10.4.5 移行先サーバでのデータベースのインポート

移行先サーバで、データベースをインポートする手順を次に示します。



注意

- Tuning Manager とリモート接続している場合は、Tuning Manager サーバがインストールされているマシンで、Tuning Manager のサービスをいったん停止しておく必要があります。データベースのインポートが完了したあと、Tuning Manager のサービスを再開させてください。Tuning Manager のサービスを停止および起動する方法については、インストールされている Tuning Manager に対応するバージョンのマニュアルを参照してください。
- データベースのインポートでは、Hitachi Command Suite のサービスの停止を伴う操作を実行します。インポート中は、Hitachi Command Suite にアクセスしないでください。

(1) データベースのインポート（非クラスタ構成の場合）

管理サーバの OS が非クラスタ構成の場合に、移行先サーバでデータベースをインポートする手順を次に示します。

1. Administrator 権限または root 権限のユーザーで管理サーバにログインします。
2. 移行元の管理サーバでプロパティにデフォルト値以外を設定していた場合は、必要に応じて、移行先サーバのプロパティファイルの設定値を見直してください。

データベースをインポートしても、プロパティファイルは移行先サーバに引き継がれません。

3. hcmsdbtrans コマンドを実行してデータベースをインポートします。

Windows の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin  
%hcmsdbtrans /import /workpath <作業用フォルダ> [/file <アーカイブ  
ファイル>] /type {ALL|<データベースを移行する Hitachi Command Suite 製品の  
名称>} /auto
```

Solaris または Linux の場合：

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmsdbtrans -import -workpath <作業用ディレクトリ> [-file <アーカイブ  
ファイル>] -type {ALL|<データベースを移行する Hitachi Command Suite 製品の  
名称>} -auto
```

workpath

アーカイブファイルを使用してインポートする場合：

アーカイブファイルを展開するためのディレクトリを、絶対パスで指定します。Solaris または Linux の場合、空白を含むパスは指定しないでください。ローカルディスクのディレクトリを指定してください。アーカイブファイルを使用する場合、file オプションの指定は必須です。

workpath オプションに指定するディレクトリの下には、ファイルおよびサブディレクトリがないことを確認してください。

アーカイブファイルを使用しないでインポートする場合：

移行元から転送したデータベース情報を格納したディレクトリを指定してください。転送したディレクトリ以下のファイル構成は変更しないでください。また、file オプションは指定しないでください。

file

移行元サーバから転送したデータベースのアーカイブファイルを、絶対パスで指定します。Solaris または Linux の場合、パスに空白を含まないようにしてください。workpath に指定したディレクトリに移行元から転送したデータベース情報が格納されている場合、このオプションを指定する必要はありません。

type

原則として、ALL を指定してください。ALL を指定すると、移行先にインストールされている Hitachi Command Suite 製品のデータベースが自動的に選択され、移行されます。

管理サーバのプログラム構成の違いなどの理由によって、特定の Hitachi Command Suite 製品のデータベースしか移行しない場合は、次の表に従って移行対象の製品の名称を指定します。複数の製品を指定する場合、コンマ (,) で区切って指定してください。

なお、type オプションを使用してデータベースを移行できるのは、指定したすべての製品のデータベースが、アーカイブファイルまたは workpath オプションに指定したディレクトリにあり、かつ、指定したすべての製品が移行先にインストールされている場合です。条件を満たさない製品が 1 つでもある場合、移行は実行されません。

表 10-6 データベースを移行する場合の type オプションの指定値 (非クラスタ構成の場合)

製品	指定値
Device Manager ^{※1※2}	DeviceManager
Tiered Storage Manager ^{※1}	TieredStorageManager
Replication Manager ^{※2}	ReplicationManager
そのほかの製品	それぞれの製品のマニュアルを参照

注※1 バージョン 7.0 以降の環境でエクスポートしたデータベースをインポートする場合は、Tiered Storage Manager のライセンスの有無に関係なく、Device Manager と Tiered Storage Manager のデータベースを必ず両方一緒にインポートしてください。

注※2 Replication Manager のデータベースをインポートする場合は、Device Manager のデータベースも必ず一緒にインポートしてください。

auto

Hitachi Command Suite 製品のサービスを自動的に起動/停止するオプションです。

4. Device Manager サーバの `server.base.initialsynchro` プロパティに `true` を指定します。
`hcmsdbtrans` コマンドでは、ユーザー情報以外の Hitachi Command Suite 共通コンポーネントのリポジトリを移行しないため、インポートした Device Manager のデータベースの情報に合わせてリポジトリの情報を同期する必要があります。
5. Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティに `true` を指定します。
6. Tuning Manager とリモート接続していた場合は、データベースのインポートによって設定が初期化されるため、`htmsetup` コマンドを実行して再設定します。
7. 移行先の Hitachi Command Suite 製品のサービスを起動します。
8. Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
9. Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
10. 次の場合には、Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
 - データベースをエクスポートしてから、インポートするまでの間にストレージシステムの構成を変更したとき
 構成を変更したストレージシステムをリフレッシュします。
 - 移行元と移行先で管理サーバにインストールされた Hitachi Command Suite 製品のバージョンが異なるとき
 Device Manager に登録されたすべてのストレージシステムをリフレッシュします。
11. Replication Manager のセカンダリーサイトにある管理サーバでデータベースをインポートした場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
12. データベースをバックアップします。
 運用再開後は、バージョン 6.4 以前にエクスポートしたアーカイブファイルはインポートできません。障害が発生した場合に備えて、インポート直後のデータベースをバックアップしておくことをお勧めします。

関連項目

- (5) Tuning Manager サーバとのリモート接続およびポート番号の設定 (htmsetup コマンド)
- 9.2 サービスの起動
- 10.2.1 データベースのバックアップ (非クラスタ構成の場合)

(2) データベースのインポート (Microsoft Cluster Service または Windows Server Failover Clustering の場合)

管理サーバの OS が Windows でクラスタ構成の場合に、移行先サーバでデータベースをインポートする手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースをインポートしてください。

データベースをインポートする手順を次に示します。

1. Administrator 権限のユーザーで管理サーバにログインします。
2. 移行元の管理サーバでプロパティにデフォルト値以外を設定していた場合は、必要に応じて、移行先の実行系ノードおよび待機系ノードでプロパティファイルの設定値を見直してください。
データベースをインポートしても、プロパティファイルは移行先サーバに引き継がれません。
3. クラスタ管理アプリケーションで次のサービスを選択し、右クリックメニューでオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
4. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
5. クラスタ管理アプリケーションで、次のサービスをオフラインにします。
 - HiRDBClusterService_HD0
6. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを抑制します。
次のリソースの設定を変更します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDBClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用している場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開しない] を選択します。

Windows Server Failover Clustering を使用している場合：

リソース名を右クリックし、[プロパティ] – [ポリシー] タブで、[リソースが失敗状態になった場合は、再起動しない] を選択します。

7. HiRDB を起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmdsdbsrv /start
```

8. hccmdsdbtrans コマンドを実行してデータベースをインポートします。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmdsdbtrans /import /workpath <作業用フォルダ> /file <アーカイブファイル  
> /type {ALL|<データベースを移行する Hitachi Command Suite 製品の名称>}
```

workpath

アーカイブファイルを使用してインポートする場合：

アーカイブファイルを展開するためのフォルダを、絶対パスで指定します。ローカルディスクのフォルダを指定してください。アーカイブファイルを使用する場合、file オプションの指定は必須です。

workpath オプションに指定するフォルダの下には、ファイルおよびサブフォルダがないことを確認してください。

アーカイブファイルを使用しないでインポートする場合：

移行元から転送したデータベース情報を格納したフォルダを指定してください。転送したフォルダ以下のファイル構成は変更しないでください。また、file オプションは指定しないでください。

file

移行元サーバから転送したデータベースのアーカイブファイルを、絶対パスで指定します。workpath に指定したフォルダに移行元から転送したデータベース情報が格納されている場合、このオプションを指定する必要はありません。

type

原則として、ALL を指定してください。ALL を指定すると、移行先にインストールされている Hitachi Command Suite 製品のデータベースが自動的に選択され、移行されます。

管理サーバのプログラム構成の違いなどの理由によって、特定の Hitachi Command Suite 製品のデータベースしか移行しない場合は、次の表に従って移行対象の製品の名称を指定します。複数の製品を指定する場合、コンマ (,) で区切って指定してください。

なお、type オプションを使用してデータベースを移行できるのは、指定したすべての製品のデータベースが、アーカイブファイルまたは workpath オプションに指定したフォルダにあり、かつ、指定したすべての製品が移行先にインストールされている場合です。条件を満たさない製品が 1 つでもある場合、移行は実行されません。

表 10-7 データベースを移行する場合の type オプションの指定値 (Microsoft Cluster Service または Windows Server Failover Clustering の場合)

製品	指定値
Device Manager ^{※1※2}	DeviceManager
Tiered Storage Manager ^{※1}	TieredStorageManager
Replication Manager ^{※2}	ReplicationManager
そのほかの製品	それぞれの製品のマニュアルを参照

注※1 バージョン 7.0 以降の環境でエクスポートしたデータベースをインポートする場合は、Tiered Storage Manager のライセンスの有無に関係なく、Device Manager と Tiered Storage Manager のデータベースを必ず両方一緒にインポートしてください。

注※2 Replication Manager のデータベースをインポートする場合は、Device Manager のデータベースも必ず一緒にインポートしてください。

9. 実行系ノードおよび待機系ノードで、Device Manager サーバの `server.base.initialsynchro` プロパティに `true` を指定します。
 `hcmdsdbtrans` コマンドでは、ユーザー情報以外の Hitachi Command Suite 共通コンポーネントのリポジトリを移行しないため、インポートした Device Manager のデータベースの情報に合わせてリポジトリの情報を同期する必要があります。
10. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティに `true` を指定します。
11. `hcmdssrv` コマンドを実行して、Hitachi Command Suite 製品のサービスを起動します。
12. クラスタ管理アプリケーションで、リソースグループのフェールオーバーを有効にします。
 次のリソースの設定を変更します。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDBClusterService_HD0
 - 上記以外の Hitachi Command Suite 製品のリソース

Microsoft Cluster Service を使用している場合：

リソース名を右クリックし、[プロパティ] - [詳細設定] タブで、[再開する] を選択します。

Windows Server Failover Clustering を使用している場合：

リソース名を右クリックし、[プロパティ] - [ポリシー] タブで次の項目を選択します。

- [リソースが失敗状態になった場合は、現在のノードで再起動を試みる]
- [再起動に失敗した場合は、この役割のすべてのリソースをフェールオーバーする] (または [再起動に失敗した場合は、このサービスまたはアプリケーションのすべてのリソースをフェールオーバーする])

13. クラスタ管理アプリケーションで、Hitachi Command Suite 製品のサービスを登録しているリソースグループをオンラインにします。
14. 実行系ノードおよび待機系ノードで、Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
15. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
16. 次の場合には、Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
 - データベースをエクスポートしてから、インポートするまでの間にストレージシステムの構成を変更したとき
 構成を変更したストレージシステムをリフレッシュします。
 - 移行元と移行先で管理サーバにインストールされた Hitachi Command Suite 製品のバージョンが異なるとき
 Device Manager に登録されたすべてのストレージシステムをリフレッシュします

17. Replication Manager のセカンダリーサイトにある管理サーバでデータベースをインポートした場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
18. データベースをバックアップします。
運用再開後は、バージョン 6.4 以前にエクスポートしたアーカイブファイルはインポートできません。障害が発生した場合に備えて、インポート直後のデータベースをバックアップしておくことをお勧めします。
19. Tuning Manager とリモート接続していた場合は、データベースのインポートによって設定が初期化されるため、再設定します。
「(2) Tuning Manager サーバとのリモート接続 (Microsoft Cluster Service または Windows Server Failover Clustering)」に従って、Tuning Manager とのリモート接続を再設定してください。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止
- 10.2.2 データベースのバックアップ (Microsoft Cluster Service または Windows Server Failover Clustering の場合)

(3) データベースのインポート (Veritas Cluster Server の場合)

管理サーバの OS が Solaris で、使用しているクラスタソフトウェアが Veritas Cluster Server の場合に、移行先サーバでデータベースをインポートする手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースをインポートしてください。

データベースをインポートする手順を次に示します。

1. root 権限のユーザーで管理サーバにログインします。
2. 移行元の管理サーバでプロパティにデフォルト値以外を設定していた場合は、必要に応じて、移行先の実行系ノードおよび待機系ノードでプロパティファイルの設定値を見直してください。
データベースをインポートしても、プロパティファイルは移行先サーバに引き継がれません。
3. Veritas Cluster Server で、次のサービスをオフラインにします。
 - HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - 上記以外の Hitachi Command Suite 製品のリソース
4. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。
5. Veritas Cluster Server で、次のサービスをオフラインにします。
 - HiRDB
6. 次のサービスを右クリックして、コンテキストメニューにある [Enabled] のチェックを外します。

- HiCommand Tiered Storage Manager
 - HiCommandServer
 - HCS Device Manager Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiRDB
 - 上記以外の Hitachi Command Suite 製品のリソース
7. Cluster Explorer ウィンドウの [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Freeze] - [Temporary] を選択します。
 8. HiRDB を起動します。
 < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/
 hcmsdbsrv -start
 9. hcmsdbtrans コマンドを実行してデータベースをインポートします。
 < Hitachi Command Suite 共通コンポーネントのインストールディレクトリ >/bin/
 hcmsdbtrans -import -workpath <作業用ディレクトリ> [-file <アーカイブファイル>] -type {ALL|<データベースを移行する Hitachi Command Suite 製品の名称>}

workpath

アーカイブファイルを使用してインポートする場合：

アーカイブファイルを展開するためのディレクトリを、絶対パスで指定します。空白を含むパスは指定しないでください。ローカルディスクのディレクトリを指定してください。アーカイブファイルを使用する場合、file オプションの指定は必須です。

workpath オプションに指定するディレクトリの下には、ファイルおよびサブディレクトリがないことを確認してください。

アーカイブファイルを使用しないでインポートする場合：

移行元から転送したデータベース情報を格納したディレクトリを指定してください。転送したディレクトリ以下のファイル構成は変更しないでください。また、file オプションは指定しないでください。

file

移行元サーバから転送したデータベースのアーカイブファイルを、絶対パスで指定します。パスに空白を含まないようにしてください。workpath に指定したディレクトリに移行元から転送したデータベース情報が格納されている場合、このオプションを指定する必要はありません。

type

原則として、ALL を指定してください。ALL を指定すると、移行先にインストールされている Hitachi Command Suite 製品のデータベースが自動的に選択され、移行されます。

管理サーバのプログラム構成の違いなどの理由によって、特定の Hitachi Command Suite 製品のデータベースしか移行しない場合は、次の表に従って移行対象の製品の名称を指定します。複数の製品を指定する場合、コンマ (,) で区切って指定してください。

なお、type オプションを使用してデータベースを移行できるのは、指定したすべての製品のデータベースが、アーカイブファイルまたは workpath オプションに指定したディレクトリにあり、かつ、指定したすべての製品が移行先にインストールされている場合です。条件を満たさない製品が 1 つでもある場合、移行は実行されません。

表 10-8 データベースを移行する場合の type オプションの指定値 (Veritas Cluster Server の場合)

製品	指定値
Device Manager ^{※1※2}	DeviceManager
Tiered Storage Manager ^{※1}	TieredStorageManager
Replication Manager ^{※2}	ReplicationManager
そのほかの製品	それぞれの製品のマニュアルを参照

注※1 バージョン 7.0 以降の環境でエクスポートしたデータベースをインポートする場合は、Tiered Storage Manager のライセンスの有無に関係なく、Device Manager と Tiered Storage Manager のデータベースを必ず両方一緒にインポートしてください。

注※2 Replication Manager のデータベースをインポートする場合は、Device Manager のデータベースも必ず一緒にインポートしてください。

10. 実行系ノードおよび待機系ノードで、Device Manager サーバの `server.base.initialsynchro` プロパティに `true` を指定します。
`hcmdsdbtrans` コマンドでは、ユーザー情報以外の Hitachi Command Suite 共通コンポーネントのリポジトリを移行しないため、インポートした Device Manager のデータベースの情報に合わせてリポジトリの情報を同期する必要があります。
11. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティに `true` を指定します。
12. `hcmdssrv` コマンドを実行して、Hitachi Command Suite 製品のサービスを起動します。
13. Cluster Explorer ウィンドウで [Service Groups] タブを選択します。Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Unfreeze] を選択します。
14. Hitachi Command Suite 製品のサービスを登録しているグループを右クリックして、コンテキストメニューから [Enable Resources] を選択します。
15. Veritas Cluster Server で、リソースが登録されているグループをオンラインにします。
16. 実行系ノードおよび待機系ノードで、Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
17. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
18. 次の場合には、Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
 - データベースをエクスポートしてから、インポートするまでの間にストレージシステムの構成を変更したとき
構成を変更したストレージシステムをリフレッシュします。
 - 移行元と移行先で管理サーバにインストールされた Hitachi Command Suite のバージョンが異なるとき
Device Manager に登録されたすべてのストレージシステムをリフレッシュします。
19. Replication Manager のセカンダリーサイトにある管理サーバでデータベースをインポートした場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。
20. データベースをバックアップします。

運用再開後は、バージョン 6.4 以前にエクスポートしたアーカイブファイルはインポートできません。障害が発生した場合に備えて、インポート直後のデータベースをバックアップしておくことをお勧めします。

21. **Tuning Manager** とリモート接続していた場合は、データベースのインポートによって設定が初期化されるため、再設定します。

「(3) Tuning Manager サーバとのリモート接続 (Veritas Cluster Server)」に従って、Tuning Manager とのリモート接続を再設定してください。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止
- 10.2.3 データベースのバックアップ (Veritas Cluster Server の場合)

(4) データベースのインポート (Sun Cluster の場合)

管理サーバの OS が Solaris で、使用しているクラスタソフトウェアが Sun Cluster の場合に、移行先サーバでデータベースをインポートする手順を説明します。



注意 実行系ノード (cluster.conf ファイルの mode に online が設定されているマシン) でデータベースをインポートしてください。

データベースをインポートする手順を次に示します。

1. root 権限のユーザーで管理サーバにログインします。
2. 移行元の管理サーバでプロパティにデフォルト値以外を設定していた場合は、必要に応じて、移行先の実行系ノードおよび待機系ノードでプロパティファイルの設定値を見直してください。
データベースをインポートしても、プロパティファイルは移行先サーバに引き継がれません。

3. 次のコマンドを実行して、Tiered Storage Manager, Device Manager および Hitachi Command Suite 共通コンポーネント (HiRDB を除く) のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -M -j BaseWebService
# /usr/cluster/bin/scswitch -n -M -j BaseCommonService
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースの監視を無効にしてください。

4. 次のコマンドを実行して、Tiered Storage Manager, Device Manager および Hitachi Command Suite 共通コンポーネント (HiRDB を除く) のリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -n -j BaseWebService
# /usr/cluster/bin/scswitch -n -j BaseCommonService
```

上記以外に Hitachi Command Suite 製品のリソースがある場合は、同様にリソースを無効にしてください。

5. hcmdssrv コマンドを実行して、Hitachi Command Suite 製品のサービスを停止します。

6. 次のコマンドを実行して、HiRDB のリソースの監視を無効にします。

```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

7. 次のコマンドを実行して、HiRDBのリソースを無効にします。

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

8. HiRDBを起動します。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdsdbsrv -start
```

9. hcmdsdbtrans コマンドを実行してデータベースをインポートします。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/bin/  
hcmdsdbtrans -import -workpath <作業用ディレクトリ> [-file <アーカイブファイ  
ル>] -type {ALL|<データベースを移行する Hitachi Command Suite 製品の名称>}
```

workpath

アーカイブファイルを使用してインポートする場合：

アーカイブファイルを展開するためのディレクトリを、絶対パスで指定します。空白を含むパスは指定しないでください。ローカルディスクのディレクトリを指定してください。アーカイブファイルを使用する場合、file オプションの指定は必須です。

workpath オプションに指定するディレクトリの下には、ファイルおよびサブディレクトリがないことを確認してください。

アーカイブファイルを使用しないでインポートする場合：

移行元から転送したデータベース情報を格納したディレクトリを指定してください。転送したディレクトリ以下のファイル構成は変更しないでください。また、file オプションは指定しないでください。

file

移行元サーバから転送したデータベースのアーカイブファイルを、絶対パスで指定します。パスに空白を含まないようにしてください。workpath に指定したディレクトリに移行元から転送したデータベース情報が格納されている場合、このオプションを指定する必要はありません。

type

原則として、ALL を指定してください。ALL を指定すると、移行先にインストールされている Hitachi Command Suite 製品のデータベースが自動的に選択され、移行されます。

管理サーバのプログラム構成の違いなどの理由によって、特定の Hitachi Command Suite 製品のデータベースしか移行しない場合は、次の表に従って移行対象の製品の名称を指定します。複数の製品を指定する場合、コンマ (,) で区切って指定してください。

なお、type オプションを使用してデータベースを移行できるのは、指定したすべての製品のデータベースが、アーカイブファイルまたは workpath オプションに指定したディレクトリにあり、かつ、指定したすべての製品が移行先にインストールされている場合です。条件を満たさない製品が1つでもある場合、移行は実行されません。

表 10-9 データベースを移行する場合の type オプションの指定値 (Sun Cluster の場合)

製品	指定値
Device Manager ^{※1※2}	DeviceManager
Tiered Storage Manager ^{※1}	TieredStorageManager
Replication Manager ^{※2}	ReplicationManager
その他の製品	それぞれの製品のマニュアルを参照

注※1 バージョン 7.0 以降の環境でエクスポートしたデータベースをインポートする場合は、Tiered Storage Manager のライセンスの有無に関係なく、Device Manager と Tiered Storage Manager のデータベースを必ず両方一緒にインポートしてください。

注※2 Replication Manager のデータベースをインポートする場合は、Device Manager のデータベースも必ず一緒にインポートしてください。

10. 実行系ノードおよび待機系ノードで、Device Manager サーバの `server.base.initialsynchro` プロパティに `true` を指定します。
`hcmdsdbtrans` コマンドでは、ユーザー情報以外の Hitachi Command Suite 共通コンポーネントのリポジトリを移行しないため、インポートした Device Manager のデータベースの情報に合わせてリポジトリの情報を同期する必要があります。
11. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティに `true` を指定します。
12. `hcmdssrv` コマンドを実行して、Hitachi Command Suite 製品のサービスを起動します。
13. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager および Tiered Storage Manager のリソースを有効にします。

```
# /usr/cluster/bin/scswitch -e -j HiRDB
# /usr/cluster/bin/scswitch -e -j BaseCommonService
# /usr/cluster/bin/scswitch -e -j BaseWebService
# /usr/cluster/bin/scswitch -e -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -j HiCommandServer
# /usr/cluster/bin/scswitch -e -j TieredStorageManager
```

上記以外に Hitachi Command Suite 製品のリソースを無効にしていた場合は、同様にリソースを有効にしてください。
14. 次のコマンドを実行して、Hitachi Command Suite 共通コンポーネント、Device Manager および Tiered Storage Manager の監視を有効にします。

```
# /usr/cluster/bin/scswitch -e -M -j HiRDB
# /usr/cluster/bin/scswitch -e -M -j BaseCommonService
# /usr/cluster/bin/scswitch -e -M -j BaseWebService
# /usr/cluster/bin/scswitch -e -M -j HCSDeviceManagerWebService
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer
# /usr/cluster/bin/scswitch -e -M -j TieredStorageManager
```

上記以外に Hitachi Command Suite 製品のリソースの監視を無効にしていた場合は、同様にリソースの監視を有効にしてください。
15. 実行系ノードおよび待機系ノードで、Device Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
16. 実行系ノードおよび待機系ノードで、Tiered Storage Manager サーバの `server.base.initialsynchro` プロパティを `false` に戻します。
17. 次の場合には、Device Manager の GUI または CLI でストレージシステムをリフレッシュします。
 - データベースをエクスポートしてから、インポートするまでの間にストレージシステムの構成を変更したとき
構成を変更したストレージシステムをリフレッシュします。
 - 移行元と移行先で管理サーバにインストールされた Hitachi Command Suite のバージョンが異なるとき
Device Manager に登録されたすべてのストレージシステムをリフレッシュします。
18. Replication Manager のセカンダリーサイトにある管理サーバでデータベースをインポートした場合、Replication Manager の GUI で最新の構成情報を取得して、プライマリーサイトの

Replication Manager とセカンダリーサイトの Device Manager のデータベースを同期させます。

19. データベースをバックアップします。

運用再開後は、バージョン 6.4 以前にエクスポートしたアーカイブファイルはインポートできません。障害が発生した場合に備えて、インポート直後のデータベースをバックアップしておくことをお勧めします。

20. Tuning Manager とリモート接続していた場合は、データベースのインポートによって設定が初期化されるため、再設定します。

「(4) Tuning Manager サーバとのリモート接続 (Sun Cluster)」に従って、Tuning Manager とのリモート接続を再設定してください。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止
- 10.2.4 データベースのバックアップ (Sun Cluster の場合)

Device Manager エージェントの運用

この章では、Device Manager エージェントを運用するために必要な設定や、Device Manager エージェントの操作について説明します。

- 11.1 Device Manager エージェントを運用するための前提条件
- 11.2 Device Manager エージェントの環境設定
- 11.3 Device Manager エージェントの操作
- 11.4 構成定義ファイルの利用
- 11.5 Device Manager エージェントのリモートインストール

11.1 Device Manager エージェントを運用するための前提条件

Device Manager エージェントを運用する上での前提条件や注意事項について説明します。

11.1.1 複数の NIC が搭載されたホストを使用する場合の前提条件

複数の NIC が搭載されたホストで Device Manager エージェントを動作させる場合の前提条件を次に示します。

- Device Manager エージェントの `server.properties` ファイルの `server.http.socket.agentAddress` プロパティに、Device Manager エージェントで使用する NIC の IP アドレスを指定してください。
- P-VOL を認識しているホストと S-VOL を認識しているホストの OS が Windows の場合、自ホストの優先 NIC に割り当てられた IP アドレスと、相手ホストから自ホストを名前解決した際の IP アドレスが同じになるように、それぞれのホストで NIC の優先順位を見直す必要があります。名前解決できない環境の場合は、Device Manager CLI または Replication Manager からコピーペアに対して操作した際にエラーになることがあります。

Windows Server 2003 R2 の場合は、次の手順で NIC の優先順位を変更してください。

- a. [スタート] – [設定] – [ネットワーク接続] を選択します。
- b. [詳細設定] – [詳細設定] – [アダプタとバインド] タブを選択し、NIC の優先順位を変更します。

Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 または Windows Server 2012 R2 の場合は、次の手順で NIC の優先順位を変更してください。

- a. [コントロールパネル] から、[ネットワークと共有センター] – [アダプターの設定の変更] を選択します。
- b. [詳細設定] – [詳細設定] – [アダプターとバインド] タブを選択し、NIC の優先順位を変更します。

[詳細設定] メニューが表示されていない場合は、[Alt] キーを押してメニューバーを表示させてから操作してください。

関連項目

- D.1.1 Device Manager エージェントのプロパティの変更
- D.6.5 `server.http.socket.agentAddress`

11.1.2 Device Manager エージェントを運用する場合の注意事項

Device Manager エージェントを運用する場合には、幾つかの注意事項があります。

- Device Manager エージェントをインストールしたあとに、下記の条件でホストの OS をバージョンアップした場合は、Device Manager エージェントを上書きインストールしてください。
 - Solaris 9 より前のバージョンから Solaris 9 以降にバージョンアップ
 - AIX 5.2 より前のバージョンから AIX 5.3 以降にバージョンアップ
 - HP-UX 11i v2 より前のバージョンから HP-UX 11i v2 以降にバージョンアップ
- ホストの OS が Windows の場合、Device Manager エージェントは、ドライブレター A または B が割り当てられたデバイスの情報を取得しません。Device Manager エージェントを使用して管理するデバイスには、C～Z のドライブレターを割り当ててください。

- AIX 7.1 または AIX 6.1 TL6 以降のホストで `rendev` コマンドを使用してデバイスファイル名を変更する場合、変更後の文字列には ASCII 印字可能文字だけを使用してください。ASCII 印字可能文字以外の文字が含まれると、Device Manager エージェントが正しく動作しません。
- `hdvm_info` 以外の Device Manager エージェントのコマンドを実行するためには、Administrator 権限またはスーパーユーザー権限が必要です。
- ホストで次の OS を使用している場合は、Device Manager エージェントのコマンドは、WOW64 用のコマンドプロンプトから実行してください。
Windows Server 2003 R2 (x64)
Windows Server 2008 (x64 および IPF)
Windows Server 2008 R2 (x64 および IPF)
Windows Server 2012 (x64)
Windows Server 2012 R2 (x64)
コマンドプロンプトの実行例を次に示します。
`C:\%WINDOVS%\SysWOW64\cmd.exe`
- Windows では、Device Manager エージェントのコマンドがインストールされるフォルダが自動的に環境変数 `PATH` に追加されます。このため、コマンドを実行するとき、コマンドが格納されているフォルダに移動する必要はありません。
- Device Manager エージェントを使用してストレージシステムで 256 以上の LUN を認識する Linux ホストを登録すると、KAIC03006-E のエラーメッセージが出力され、操作が失敗します。
ホストの OS が Linux の場合、Device Manager エージェントの管理対象ホストで認識するストレージシステムの 1 ポートごとの LU 数は 256 以下、LUN の範囲は 0~255 となるように指定してください。

11.2 Device Manager エージェントの環境設定

Device Manager エージェントの運用を開始するためには、環境設定が必要です。

必要に応じて次の設定をしてください。

- Java の実行環境の変更 (Windows または Linux)
Device Manager エージェントで使用する Java の実行環境を変更する場合に必要です。
- ファイアウォールへの例外登録 (Windows)
Device Manager エージェントのインストール後に Windows ファイアウォールを有効にした場合や、Device Manager エージェントで使用するポートを変更した場合に必要です。
- java プロセスの SED への例外登録 (AIX)
Device Manager エージェントのインストール後に、SED のモードを `all` に変更する場合に必要です。
- コピーペアを管理するために必要な設定
Device Manager または Replication Manager でコピーペアを管理する場合に必要です。
- ホストで管理する LU が 100 個以上ある場合に必要な設定
1 つのホストで認識している Device Manager 管理下の LU が 100 個以上ある場合に必要です。
- サービスの実行ユーザーの変更 (Windows)
Device Manager エージェントが起動する HORCM インスタンスを操作するため、Device Manager エージェントのサービスの実行ユーザーを、Administrator 権限を持つユーザーに変更する場合に必要です (デフォルト: LocalSystem)。

なお、Device Manager エージェントを新規インストールした際に、次に示す設定をしていない場合は、`hdvmagt_setting` コマンドを実行して必要な設定をしてください。

- Device Manager サーバの情報の設定（必須）
- Device Manager サーバへのホスト情報の通知周期の設定（任意）
- RAID Manager または P9000 RAID Manager の情報の設定（任意）

11.2.1 Device Manager エージェントで使用する Java の実行環境の変更 (javapath_setup コマンド)

ホストの OS が Windows または Linux の場合に、`javapath_setup` コマンドを実行して、Device Manager エージェントで使用する Java の実行環境を変更します。

事前に完了しておく操作

- Device Manager エージェントが前提とする Java の実行環境の確認
詳細は、「ソフトウェア添付資料」を参照してください。
- Administrator 権限（Windows の場合）または root（Linux の場合）でのログイン

事前に確認しておく情報

- 使用する Java の実行環境のインストールパス（特定の Java の実行環境を使用する場合）

コマンドの形式

```
javapath_setup {-set [new|bundle|<Java の実行環境のインストールパス>]|-check}
```

コマンドの格納先

Windows の場合

```
<Device Manager エージェントのインストールフォルダ>%bin
```

Linux の場合

```
/opt/HDVM/HBaseAgent/bin
```

オプション

`-set`

Java の実行環境を変更する場合に指定します。引数を省略した場合は、`new` を指定したものと見なされます。

- `new`
ホストにインストールされている Oracle JDK または Oracle JRE のうち、最新バージョンの Java の実行環境を使用するときに指定します。
同じバージョンの Java の実行環境がインストールされている場合は JDK が優先されません。
- `bundle`
Device Manager エージェントに同梱された Java の実行環境を使用するときに指定します。
- `<Java の実行環境のインストールパス>`
特定の Java の実行環境を使用するときに、インストールパスを絶対パスで指定します。

`-check`

ホストにインストールされている Oracle JDK または Oracle JRE のうち、最新バージョンの Java の実行環境を確認する場合に指定します。



注意

- ・ コマンド実行後は、Device Manager エージェントのサービスを再起動する必要があります。
- ・ 次の場合、32 ビット用の Java の実行環境を使用してください。
 - ・ ホストの OS が Windows のとき
 - ・ ホストの OS が Linux で、CIM/WBEM 機能を利用してエンタープライズクラスストレージの性能情報を取得するとき
 - ・ Dynamic Link Manager がホストにインストールされているとき
- ・ バージョン 7.0.1 以前からバージョンアップしたあとに、Java の実行環境を Device Manager エージェントに同梱された JRE から、Oracle JDK または Oracle JRE に変更した場合は、Device Manager エージェントを Windows ファイアウォールに例外登録する必要があります。

関連項目

- ・ [11.2.2 Device Manager エージェントの Windows ファイアウォールへの例外登録 \(firewall_setup コマンド\)](#)
- ・ [\(1\) Device Manager エージェントのサービスの起動、停止、稼働状態の確認 \(hbsasrv コマンド\)](#)

11.2.2 Device Manager エージェントの Windows ファイアウォールへの例外登録 (firewall_setup コマンド)

firewall_setup コマンドを実行して、Device Manager エージェントで使用するポートをファイアウォールに例外登録します。

Device Manager エージェントの server.properties ファイルにある次のプロパティに設定されているポートが例外登録されます。

- ・ server.agent.port プロパティに設定されたポート (デフォルト : 24041/tcp)
- ・ server.http.port プロパティに設定されたポート (デフォルト : 24042/tcp)
- ・ server.http.localPort プロパティに設定されたポート (デフォルト : 24043/tcp)

事前に完了しておく操作

- ・ Administrator 権限でのログイン

コマンドの形式

```
firewall_setup {-set|-unset}
```

コマンドの格納先

< Device Manager エージェントのインストールフォルダ > %bin

オプション

-set

ファイアウォールの例外登録を行う場合に指定します。

-unset

ファイアウォールの例外登録の設定を解除する場合に指定します。

関連項目

- D.6.1 server.agent.port
- D.6.2 server.http.localPort
- D.6.3 server.http.port

11.2.3 java プロセスの SED への例外登録 (AIX)

ホストの OS が AIX で、Device Manager エージェントのインストール後に SED のモードを all に変更した場合は、sedmgr コマンドを実行して、Device Manager エージェントが使用する java プロセスを SED に例外として登録する必要があります。

事前に確認しておく情報

- Device Manager エージェントが使用する Java の実行環境のインストールパス
Device Manager エージェントの server.properties ファイルにある server.agent.JRE.location プロパティで確認できます。

java プロセスを SED に例外登録するには：

1. 次のコマンドを実行して、Device Manager エージェントが使用する java プロセスを SED に例外として登録します。

```
# sedmgr -c exempt <Java の実行環境のインストールパス>/bin/java
```

上記のコマンドが成功した場合、実行結果は出力されません。

2. 次のコマンドを実行して、Device Manager エージェントが使用する java プロセスが、SED に例外として登録されていることを確認します。

```
# sedmgr -d <Java の実行環境のインストールパス>/bin/java
```

Device Manager エージェントが使用する java プロセスが SED に例外として登録されている場合、次のように表示されます。

```
<Java の実行環境のインストールパス>/bin/java : exempt
```

3. ホストを再起動します。

関連項目

- D.6.9 server.agent.JRE.location

11.2.4 コピーペアを管理するために必要な設定

Device Manager または Replication Manager でコピーペアを管理する場合、運用環境によっては Device Manager エージェントまたは Replicaiton Manager サーバのプロパティの設定値を変更する必要があります。

- RAID Manager または P9000 RAID Manager がデフォルト以外の場所にインストールされている場合、またはホストの OS が Windows で、RAID Manager または P9000 RAID Manager のインストールドライブと Device Manager エージェントのインストールドライブが異なる場合

Device Manager エージェントの server.properties ファイルにある server.agent.rm.location プロパティ

Device Manager エージェントの server.properties ファイルにある server.agent.rmxp.location プロパティ

- 管理対象のホストで、Device Manager サーバが管理するストレージシステムのコピーペアを一括管理したい場合

Device Manager エージェントの `server.properties` ファイルにある `server.agent.rm.centralizePairConfiguration` プロパティ



注意 構成定義ファイルにメインフレームボリュームのコピーペア定義を作成または追加する場合、コピーペアの管理方法は一括管理構成である必要があります。

- コピーペアを認識しているホストが仮想マシンの場合

Device Manager エージェントの `server.properties` ファイルにある `server.agent.rm.ignorePairStatus` プロパティ



注意 GUI または CLI で最新のコピーペア情報を確認したい場合は、コピーペアの管理方法に応じて、次のとおり対応してください。

通常構成：ストレージシステムをリフレッシュしてください。

一括管理構成：ペア管理サーバをリフレッシュしてください。

- 仮想コマンドデバイスに SVP を使用して、デバイスグループとして定義されたコピーペアを管理する場合

管理サーバに P-VOL および S-VOL を割り当てている構成の場合に設定が必要です。

Device Manager エージェントの `server.properties` ファイルにある `server.agent.rm.ignorePairStatus` プロパティ

GUI または CLI で最新のコピーペア情報を確認したい場合は、ストレージシステムをリフレッシュしてください。

- デバイスグループまたは仮想コマンドデバイスを使用して定義されたコピーペアを管理する場合

物理コマンドデバイスを使用した構成でコピーペアを管理する場合に比べて、RAID Manager または P9000 RAID Manager のコマンドの応答時間が増加するため、Device Manager エージェントで処理がエラー終了するおそれがあります。事前に次のプロパティの値を変更しておくことをお勧めします。

- Device Manager エージェントの `server.properties` ファイルにある `server.agent.rm.moduleTimeOut` プロパティ

1800 以上の値を設定してください。

- Device Manager エージェントの `agent.properties` ファイルにある `agent.rm.TimeOut` プロパティ

1800 以上の値を設定してください。

- Replicaiton Manager サーバの `agentif.properties` ファイルにある `hdvmagtif.MaxPollingCount` プロパティ

値に 100 を設定してください。

- Replicaiton Manager サーバの `agentif.properties` ファイルにある `hdvmagtif.PollingInterval` プロパティ

60 以上の値を設定してください。

- ペアを作成するときの、ペアボリュームの情報を記述する形式を HORCM_DEV 形式または HORCM_LDEV 形式のどちらかに統一したい場合

Device Manager エージェントの `server.properties` ファイルにある `server.agent.rm.pairDefinitionForm` プロパティ



注意 HUS100, Hitachi AMS2000, Hitachi SMS, Hitachi AMS/WMS または SANRISE9500V を使用してコピーペアを管理する場合、ペアボリュームの情報を HORCM_DEV 形式で記載していると、次の操作で時間が掛かることがあります。

- ホストのリフレッシュ

- ストレージシステムのリフレッシュ

このような場合は、HORCM_LDEV 形式に変更して運用することを推奨します。ただし、HORCM_LDEV 形式に変更する場合は、RAID Manager 01-17-03/04 以降または P9000 RAID Manager 01.17.04 以降がインストールされている必要があります。

- すでに RAID Manager または P9000 RAID Manager によって管理されているペアボリュームを Device Manager の操作対象から外したい場合

Device Manager エージェントの server.properties ファイルにある
server.agent.rm.exclusion.instance プロパティ

- ユーザーが作成した RAID Manager または P9000 RAID Manager の構成定義ファイルを Device Manager で使用できるように最適化したい場合

Device Manager エージェントの server.properties ファイルにある
server.agent.rm.optimization.userHorcmFile プロパティ

また、Replication Manager でコピーペアを管理する場合には、次のプロパティを設定する必要があります。適切な値が設定されていない場合は、メモリーヒープサイズの不足や Replication Manager の処理のタイムアウトが発生するおそれがあります。

- Device Manager エージェントの agent.properties ファイルにある agent.rm.TimeOut
プロパティ

動作確認をしながら設定値を調整してください。

- Device Manager エージェントの server.properties ファイルにある
server.agent.maxMemorySize プロパティ

1 台のホスト（ペア管理サーバ）が管理するペア数に応じた値を設定してください。デフォルトでは、64MB で動作します。ペア数が 5,000 個を超える場合は、2,500 個ごとに 64MB ずつ増やしたメモリーヒープサイズで動作するように値を設定してください。例えば、6,000 個のペアを管理するホストでは、server.agent.maxMemorySize プロパティの設定を「128」に変更してください。また、1 台のホストで正サイトと副サイトの構成定義ファイルを管理する場合には、ペア数を 2 倍した値を基に設定してください。

関連項目

- [D.1.1 Device Manager エージェントのプロパティの変更](#)
- [D.2.1 agent.rm.TimeOut](#)
- [D.6.7 server.agent.maxMemorySize](#)
- [D.6.15 server.agent.rm.centralizePairConfiguration](#)
- [D.6.17 server.agent.rm.exclusion.instance](#)
- [D.6.18 server.agent.rm.location](#)
- [D.6.19 server.agent.rm.optimization.userHorcmFile](#)
- [D.6.23 server.agent.rm.pairDefinitionForm](#)
- [D.6.25 server.agent.rm.ignorePairStatus](#)
- [D.6.27 server.agent.rm.moduleTimeOut](#)
- [D.6.31 server.agent.rmxp.location](#)
- Replication Manager サーバの agentif.properties ファイルにある hdvmagtif.MaxPollingCount プロパティおよび hdvmagtif.PollingInterval プロパティについて：マニュアル「*Hitachi Command Suite Replication Manager Software* システム構成ガイド」

11.2.5 ホストで 100 個以上の LU を管理する場合に必要な設定

1 台のホストで LU を 100 個以上管理する場合、管理対象の LU 数に応じて、Device Manager サーバが受信できるデータ長や、Device Manager エージェントのタイムアウト値などを変更する必要があります。

次に示すプロパティの設定値を変更します。設定する値は、ホストがボリュームマネージャーを使用しているかどうかによって異なります。

- Device Manager サーバが受信できるデータ長の最大値
Device Manager サーバの `server.properties` ファイルにある `server.http.entity.maxLength` プロパティ
- 情報をサーバに登録する処理のタイムアウト時間
Device Manager サーバの `server.properties` ファイルにある `server.http.server.timeOut` プロパティと `server.util.processTimeOut` プロパティ
- メモリーヒープサイズ
Device Manager エージェントの `server.properties` ファイルにある `server.agent.maxMemorySize` プロパティ



重要

- 環境によっては、目安値に従って設定しても問題を解消できないことがあります。設定値は環境に応じて調整してください。
- 次の場合は、目安値の 2~3 倍の値を設定してください。
Device Manager エージェントを再起動した直後に `HiScan` コマンドを実行するとき
`hldutil` コマンドと `HiScan` コマンドを同時に実行するとき
`HiScan` コマンドを同時に複数実行するとき

関連項目

- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.2.5 server.http.entity.maxLength](#)
- [D.1.1 Device Manager エージェントのプロパティの変更](#)
- [D.6.7 server.agent.maxMemorySize](#)
- [D.6.28 server.http.server.timeOut](#)
- [D.6.29 server.util.processTimeOut](#)

(1) ホストで 100 個以上の LU を管理する場合のプロパティの目安値 (ボリュームマネージャーを使用していないとき)

ボリュームマネージャーを使用しない場合のプロパティの目安値を次に示します。

表 11-1 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (ボリュームマネージャーを使用していないとき)

ホストが認識する Device Manager 管理 下の LU 数	<code>server.http.entity.maxLength</code> (単位: バイト)	<code>server.http.server.timeOut</code> (単位: 秒)	<code>server.util.processTimeOut</code> (単位: ミリ秒)
100	131,072 以上	600 (デフォルト値)	600,000 (デフォルト値)
256	153,600 以上	600	600,000
512	307,200 以上	600	600,000

ホストが認識する Device Manager 管理 下の LU 数	server.http.entity.maxLength (単位: バイト)	server.http.server.timeout (単位: 秒)	server.util.processTimeOut (単位: ミリ秒)
1,024	614,400 以上	1,200	1,200,000

関連項目

- ・ A.1.1 Device Manager サーバのプロパティの変更
- ・ A.2.5 server.http.entity.maxLength
- ・ D.1.1 Device Manager エージェントのプロパティの変更
- ・ D.6.28 server.http.server.timeout
- ・ D.6.29 server.util.processTimeOut

(2) ホストで 100 個以上の LU を管理する場合のプロパティの目安値 (ボリュームマネージャーを使用しているとき)

ボリュームマネージャーを使用する場合のプロパティの目安値を次に示します。

OS ごとに「表 11-2 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (Windows 環境でボリュームマネージャーを使用しているとき)」から「表 11-6 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (HP-UX 環境でボリュームマネージャーを使用しているとき)」に示します。各表は、HiScan コマンドの実行が 1 時間以内に完了する場合の設定値を記載しています。各表に示す LU 数、または論理ボリューム数を超える構成では、HiScan コマンドの実行に 1 時間以上掛かり HiScan コマンドが正常終了しないことがあるため、推奨できません。

表 11-2 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (Windows 環境でボリュームマネージャーを使用しているとき)

ホストが認識する Device Manager 管理 下の LU 数/論理ボ リューム数	server.http.entity.maxLength (単位: バイト)	server.http.server.timeout (単位: 秒)	server.util.processTimeOut (単位: ミリ秒)	server.agent.maxMemorySize (単位: MB)
88/10	230,000 以上	600 (デフォルト値)	600,000 (デフォルト値)	64
88/20	750,000 以上	600	600,000	64
100/200	12,000,000 以上	600	600,000	128
100/500	30,000,000 以上	600	600,000	384

表 11-3 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (Solaris 環境でボリュームマネージャーを使用しているとき)

ホストが認識する Device Manager 管理 下の LU 数/論理ボ リューム数	server.http.entity.maxLength (単位: バイト)	server.http.server.timeout (単位: 秒)	server.util.processTimeOut (単位: ミリ秒)	server.agent.maxMemorySize (単位: MB)
100/200	3,100,000 以上	600 (デフォルト値)	600,000 (デフォルト値)	128
100/500	7,200,000 以上	600	600,000	384
150/500	12,000,000 以上	600	600,000	512

ホストが認識する Device Manager 管理下の LU 数/論理ボリューム数	server.http.entity.maxLength (単位：バイト)	server.http.server.timeOut (単位：秒)	server.util.processTimeOut (単位：ミリ秒)	server.agent.maxMemorySize (単位：MB)
250/500	18,000,000 以上	600	600,000	768
500/1,000	36,000,000 以上	600	600,000	768
1,000/1,000	72,000,000 以上	1,200	600,000	768

表 11-4 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (AIX 環境でボリュームマネージャーを使用しているとき)

ホストが認識する Device Manager 管理下の LU 数/論理ボリューム数	server.http.entity.maxLength (単位：バイト)	server.http.server.timeOut (単位：秒)	server.util.processTimeOut (単位：ミリ秒)	server.agent.maxMemorySize (単位：MB)
100/200	2,500,000 以上	600 (デフォルト値)	600,000 (デフォルト値)	128
100/500	6,000,000 以上	600	600,000	384
175/500	11,000,000 以上	600	600,000	640
250/500	15,000,000 以上	600	600,000	768
500/1,000	19,000,000 以上	600	600,000	768
1,000/1,000	38,000,000 以上	600	600,000	768

表 11-5 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (Linux 環境でボリュームマネージャーを使用しているとき)

ホストが認識する Device Manager 管理下の LU 数/論理ボリューム数	server.http.entity.maxLength (単位：バイト)	server.http.server.timeOut (単位：秒)	server.util.processTimeOut (単位：ミリ秒)	server.agent.maxMemorySize (単位：MB)
100/50	748,000 以上	600 (デフォルト値)	600,000 (デフォルト値)	64
100/100	1,420,000 以上	600	600,000	64
100/256	3,600,000 以上	600	600,000	192
200/256	7,100,000 以上	600	600,000	512

表 11-6 ホストで 100 個以上の LU を管理する場合のプロパティ目安値 (HP-UX 環境でボリュームマネージャーを使用しているとき)

ホストが認識する Device Manager 管理下の LU 数/論理ボリューム数	server.http.entity.maxLength (単位：バイト)	server.http.server.timeOut (単位：秒)	server.util.processTimeOut (単位：ミリ秒)	server.agent.maxMemorySize (単位：MB)
100/50	745,000 以上	600 (デフォルト値)	600,000 (デフォルト値)	64
100/100	1,400,000 以上	600	600,000	64

ホストが認識する Device Manager 管理下の LU 数/論理ボリューム数	server.http.entity.maxLength (単位: バイト)	server.http.server.timeOut (単位: 秒)	server.util.processTimeOut (単位: ミリ秒)	server.agent.maxMemorySize (単位: MB)
100/256	3,500,000 以上	600	600,000	192
200/256	7,000,000 以上	600	600,000	512
500/1,000	40,000,000 以上	600	600,000	896
1,000/100	8,000,000 以上	600	600,000	192
1,000/500	42,000,000 以上	600	1,200,000	896

関連項目

- ・ [A.1.1 Device Manager サーバのプロパティの変更](#)
- ・ [A.2.5 server.http.entity.maxLength](#)
- ・ [D.1.1 Device Manager エージェントのプロパティの変更](#)
- ・ [D.6.7 server.agent.maxMemorySize](#)
- ・ [D.6.28 server.http.server.timeOut](#)
- ・ [D.6.29 server.util.processTimeOut](#)

11.2.6 Device Manager エージェントの常駐プロセス

Device Manager エージェントの運用では、常駐プロセスが OS 上で稼働していることが前提となります。

Device Manager エージェントの常駐プロセスを次に示します。

表 11-7 Device Manager エージェントの常駐プロセス (Windows)

プロセス名	サービス名	機能
hbsa_service.exe	HBsA Service	Device Manager エージェントのサービス

表 11-8 Device Manager エージェントの常駐プロセス (UNIX)

プロセス名	機能
hbsa_service	Device Manager エージェントのサービス

Device Manager エージェントのインストールが完了した時点では、Device Manager エージェントのサービスは起動した状態になっています。次の操作を行った場合には、Device Manager エージェントのサービスを再起動する必要があります。

- ・ Device Manager エージェントをインストールしたホストの IP アドレスを変更したとき
- ・ Device Manager エージェントをインストールしたホストに、HBA ドライバーまたは HBA API ライブラリーをインストールしたとき
- ・ Device Manager エージェントのプロパティファイルを変更したとき
- ・ 管理サーバで OS を再インストールしたあと、Hitachi Command Suite を新規インストールしたとき
- ・ RAID Manager または P9000 RAID Manager をインストールまたはアンインストールしたとき

- AIX または Linux で Dynamic Link Manager をインストールまたはアンインストールしたとき
- `hdvmagt_setting` コマンドの実行を中断したとき
- Device Manager エージェントで使用する Java の実行環境を変更したとき

(1) Device Manager エージェントのサービスの起動、停止、稼働状態の確認 (hbsasrv コマンド)

`hbsasrv` コマンドを実行して、Device Manager エージェントのサービスを起動または停止したり、Device Manager エージェントのサービスの稼働状態を確認します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

コマンドの形式

```
hbsasrv [start|stop [-f]|status]
```

コマンドの格納先

Windows の場合

< Device Manager エージェントのインストールフォルダ > %bin

Solaris, Linux, または HP-UX の場合

/opt/HDVM/HBaseAgent/bin

AIX の場合

/usr/HDVM/HBaseAgent/bin

オプション

`start`

Device Manager エージェントのサービスを起動します。

`stop`

Device Manager エージェントのサービスを停止します。

`-f` オプションを付けて実行すると、Device Manager エージェントのサービスを強制的に停止します。この場合、すべての処理が強制的に終了されますので、実行中のジョブの処理は保証されません。

`status`

Device Manager エージェントのサービスの稼働状態を表示します。



注意

- ホストマシンの性能や負荷状況によっては、`hbsasrv` コマンドが終了しても、Device Manager エージェントのサービスがすぐに停止しないことがあります。
- アドオンモジュールやバージョン 05-80 以降の Dynamic Link Manager が動作している場合、Device Manager エージェントのサービスを停止できないことがあります。この場合、KAIE62604-E のエラーメッセージが表示されます。アドオンモジュールおよび Dynamic Link Manager の動作が完了するまで待ち、再度コマンドを実行してください。
- `status` オプションを付けて実行した場合に表示されるバージョン情報は、Device Manager エージェントのバージョンではありません。Device Manager エージェントのバージョンを確認する場合は、`hdvm_info` コマンドを実行してください。

関連項目

- 11.3.3 Device Manager エージェントのバージョンの表示 (hdvm_info コマンド)

(2) サービスの実行ユーザーの変更 (Windows)

Device Manager エージェントのサービスを実行するユーザーを、Administrator 権限を持つユーザーに変更します。

事前に確認しておく情報

- 変更したいサービスの実行ユーザー (Administrator 権限を持つユーザー) のユーザー名とパスワード

サービスの実行ユーザーを変更するには：

- Device Manager エージェントのサービスを停止します。
- [管理ツール] - [サービス] を選択してサービスウィンドウを開きます。
- HBsA Service サービスを選択してから、[操作] - [プロパティ] を選択します。
- [ログオン] タブを選択し、[アカウント] を選択します。
- ユーザーとパスワードを設定します。
- サービスウィンドウから HBsA Service サービスを選択して開始します。

関連項目

- (1) Device Manager エージェントのサービスの起動、停止、稼働状態の確認 (hbsasrv コマンド)

11.3 Device Manager エージェントの操作

ここでは、Device Manager エージェントの操作について説明します。

11.3.1 エージェント機能の確認 (hbsa_modinfo コマンド)

使用できるアドオンモジュールの名称とバージョンを表示するには、hbsa_modinfo コマンドを実行します。

アドオンモジュールの名称とバージョンは、*V.R1.R2-MM* (*V*: バージョン番号, *R1* および *R2*: リビジョン番号, *MM*: 修正版番号) の形式で表示されます。アドオンモジュール名を指定して、そのモジュールが使用できる状態かどうかを確認することもできます。

該当するアドオンモジュールが見つからなかった場合は、アドオンモジュールが見つかりませんでしたという意味のメッセージが表示されますが、hbsa_modinfo コマンドは正常に終了します。

なお、Global Link Manager エージェントのバージョンが 6.2 の場合は、コマンド実行結果のアドオンモジュール名に HGLM Agent が表示されます。

また、アドオンモジュール名に hdlm が出力されるのは、OS が Windows で、Dynamic Link Manager エージェントのバージョンが 6.0 以降の場合だけです。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

コマンドの形式

hbsa_modinfo [<アドオンモジュール名>]

コマンドの格納先

Windows の場合

<Device Manager エージェントのインストールフォルダ>%bin

Solaris, Linux, または HP-UX の場合

/opt/HDVM/HBaseAgent/bin

AIX の場合

/usr/HDVM/HBaseAgent/bin

オプション

<アドオンモジュール名>

特定のアドオンモジュールの使用可否を確認する場合に、略称を次の形式で指定します。

hdlm : Dynamic Link Manager エージェント

hdvm : Device Manager エージェント

hglm : Global Link Manager エージェント

hptm : Protection Manager エージェント

hrpm : Replication Manager エージェント

hrpmap : Replication Manager Application エージェント

hbsa_modinfo コマンドで確認できるアドオンモジュールと機能概要を次に示します。

- Dynamic Link Manager エージェント
ホスト・ストレージシステム間のアクセス経路の監視と調整をします。
- Device Manager エージェント
ストレージシステムおよびホストの使用状況を収集します。
- Global Link Manager エージェント
ホスト・ストレージシステム間の DMP パス経路を監視します。
- Protection Manager エージェント
ストレージシステムの高速コピー機能を使用したバックアップ運用を簡略化します。
- Replication Manager エージェント
ストレージシステムのレプリケーションの状態を監視します。
- Replication Manager Application エージェント
ストレージシステムの高速コピー機能を使用したバックアップ運用を一元管理します。

11.3.2 Device Manager エージェントのレジストリーとファイルの削除 (hbsa_util コマンド)

ホストの OS が Windows の場合に、Device Manager エージェントのレジストリーとファイルを削除するには、hbsa_util コマンドを実行します。

事前に完了しておく操作

- Administrator 権限でのログイン

コマンドの形式

```
hbsa_util -cleanup
```

コマンドの格納先

< *Device Manager* エージェントのインストールフォルダ > %bin



参考 hbsa_util.exe ファイルは、統合インストールメディア中の次のフォルダにも格納されています。
< DVD-ROM ドライブ > %AGENTS%HDVM%Windows%HBsA

オプション

```
-cleanup
```

Device Manager エージェントのレジストリーとファイルを削除する場合に指定します。

11.3.3 Device Manager エージェントのバージョンの表示 (hdvm_info コマンド)

Device Manager エージェントのバージョンを表示するには、hdvm_info コマンドを実行します。

Device Manager エージェントのバージョンが *V.R1.R2-MM* (*V*: バージョン番号, *R1* および *R2*: リビジョン番号, *MM*: 修正版番号) の形式で表示されます。

コマンドの形式

```
hdvm_info
```

コマンドの格納先

Windows の場合

< *Device Manager* エージェントのインストールフォルダ > %bin

Solaris, Linux, または HP-UX の場合

```
/opt/HDVM/HBaseAgent/bin
```

AIX の場合

```
/usr/HDVM/HBaseAgent/bin
```

11.3.4 Device Manager サーバの情報, HiScan コマンドの実行周期および RAID Manager または P9000 RAID Manager の情報の設定 (hdvmagt_setting コマンド)

Device Manager サーバの情報, HiScan コマンドの自動実行の周期, および RAID Manager または P9000 RAID Manager を利用するための情報を設定するには、hdvmagt_setting コマンドを実行します。

次の情報を対話式に一括設定します。

表 11-9 hdvmagt_setting コマンドで設定する情報

項目	説明
Device Manager サーバの情報	IP アドレスまたはホスト名 IP アドレスを指定する場合は、IPv4 アドレスまたは IPv6 アドレスを使用できます。IPv6 アドレスは省略形も指定できます。

項目	説明
	<p>また、ホスト名を指定する場合は、次の条件を満たす必要があります。</p> <p>ホスト名の長さ：50 バイト以内 使用する文字：A～Z a～z 0～9 - _ . @</p> <p>ポート番号 デフォルトのポート番号は 2001 です。</p> <p>ユーザー ID とパスワード Device Manager サーバに登録された Device Manager エージェント用のユーザー ID とパスワードを指定します。Device Manager エージェント用のビルトインアカウントのユーザー ID は HaUser、デフォルトのパスワードは haset です。</p>
HiScan コマンドの実行周期	<p>HiScan コマンドを自動実行する周期を、次の 3 種類から選択します。</p> <ul style="list-style-type: none"> ・ 1 時間に 1 回 ・ 1 日に 1 回 ・ 1 週間に 1 回 <p>また、任意の実行時刻を指定できます。</p> <p>実行時刻を指定しない場合、1 時間周期であれば毎時 30 分に、1 日周期または 1 週間周期であれば午前 2 時 30 分に、HiScan コマンドが実行されます。</p> <p>Device Manager エージェントをインストールするホストが複数ある場合は、Device Manager サーバの負荷を軽減するために実行周期を 1 日周期または 1 週間周期に設定してください。また、複数のホスト情報が同時刻に Device Manager サーバに通知されないよう、ホスト間で実行時刻を調整してください。</p>
RAID Manager または P9000 RAID Manager を利用するための情報	<p>インストール先 RAID Manager または P9000 RAID Manager のインストールされているドライブまたはディレクトリを指定します。</p> <p>一括管理構成の指定 対象のホストで、コピーペアを一括管理するかどうかを設定します。</p>

事前に完了しておく操作

- ・ Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

事前に確認しておく情報

- ・ Device Manager サーバの IP アドレスまたはホスト名
- ・ Device Manager サーバのポート番号
 Device Manager サーバの server.properties ファイルにある server.http.port プロパティで確認できます。
- ・ Device Manager エージェント用のユーザー ID とパスワード
 Device Manager の PeerGroup に所属している必要があります。
- ・ RAID Manager または P9000 RAID Manager のインストール先

コマンドの形式

hdvmagt_setting

コマンドの格納先

Windows の場合

< Device Manager エージェントのインストールフォルダ > \bin

Solaris, Linux, または HP-UX の場合

```
/opt/HDVM/HBaseAgent/bin
```

AIX の場合

```
/usr/HDVM/HBaseAgent/bin
```



参考

- 現在設定されている HiScan コマンドの実行時刻は、HiScan.log ファイルの KAIC22805-I メッセージおよび KAIC22804-I メッセージの出力時刻から確認できます。HiScan.log ファイルの格納先は次のとおりです。

Windows の場合

```
<Device Manager エージェントのインストールフォルダ>%bin%logs
```

Solaris, Linux, または HP-UX の場合

```
/opt/HDVM/HBaseAgent/bin/logs
```

AIX の場合

```
/usr/HDVM/HBaseAgent/bin/logs
```

- Windows の場合、実行周期を設定すると exeHiScan.bat がタスクとして登録されます。

関連項目

- A.2.2 server.http.port

11.3.5 Device Manager サーバへのホスト情報の手動通知 (HiScan コマンド)

ホスト名, HBA の WWN, ファイルシステム, マウントポイント, ホストが接続している LU の情報などのホスト情報を Device Manager サーバに送信するには, HiScan コマンドを実行します。

ホストに接続されたストレージシステムの構成を変更した場合や, ホスト上のファイルシステムの構成を変更した場合などには, HiScan コマンドを手動で実行することで, 変更したホスト情報を Device Manager サーバに反映できます。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

事前に確認しておく情報

- Device Manager サーバの IP アドレスまたはホスト名
- Device Manager サーバのポート番号
- Device Manager エージェント用のユーザー ID とパスワード
Device Manager の PeerGroup に所属している必要があります。

コマンドの形式

ホスト情報を送信する場合

```
HiScan -s <送信先サーバ> [-u <ユーザー ID> -p <パスワード>] [{"-c <送信周期> | -t <出力ファイル名>"}]
```

送信したホスト情報をファイルに出力する場合

```
HiScan -t <出力ファイル名>
```

コマンドの格納先

Windows の場合

```
< Device Manager エージェントのインストールフォルダ > %bin
```

Solaris, Linux, または HP-UX の場合

```
/opt/HDVM/HBaseAgent/bin
```

AIX の場合

```
/usr/HDVM/HBaseAgent/bin
```

オプション

-s

送信先の Device Manager サーバを指定します。

送信先サーバに指定できる形式は次のとおりです。

```
< IP アドレス > [: < ポート番号 >]
```

```
< ホスト名 > [: < ポート番号 >]
```

```
localhost [: < ポート番号 >]
```

ポート番号を省略した場合は、Device Manager エージェントの server.properties ファイルにある server.server.serverPort プロパティに設定されたポート番号が使用されます。また、IPv6 形式の IP アドレスとポート番号を同時に指定する場合は、IPv6 アドレスを [] で囲んでください。

-u, -p

送信先の Device Manager サーバに登録され、PeerGroup に登録されたアカウントのユーザー ID とパスワードを指定します。

省略した場合は、Device Manager エージェントの server.properties ファイルにある server.server.authorization プロパティに定義されたユーザー ID とパスワードが使用されます。

-c

Device Manager サーバにホスト情報を送信する周期を指定します (単位: 秒)。強制的に終了するまで、指定した周期で Device Manager サーバにホスト情報を送信し続けます。10~2147483647 の値を指定します。

-t

Device Manager サーバに送信したホスト情報を XML 形式のファイルに出力します。ファイルはカレントディレクトリに出力されます。

ファイル名に次の文字は指定できません。

```
¥ / : , ; * ? " < > | $ % & ' ` ^
```

-s オプションと一緒に指定した場合は、Device Manager エージェントから送信した情報と Device Manager サーバからの応答メッセージがファイルに出力されます。



参考 Device Manager エージェントがインストールされているホストの情報は次のタイミングで Device Manager サーバに自動的に反映されます。

- HiScan コマンドが自動実行される時
- ホストマシンを起動したとき
- Device Manager の GUI からホスト情報を更新したとき

関連項目

- [D.6.12 server.server.authorization](#)

11.3.6 デバイス情報の取得 (hldutil コマンド)

ストレージシステムの LDEV やファイルシステムなどのデバイスの情報を取得するには、hldutil コマンドを実行します。

取得したデバイス情報を指定したフォーマットで表示したり、実行結果ログファイルに出力したり、過去のデバイス情報を表示したりできます。デバイス情報を表示する場合、オプションをすべて省略したときは、ホストに認識されているすべての LDEV の情報を表示します。

また、実行結果ログファイルをコピーしたり、削除したりして、デバイス情報を管理することもできます。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

コマンドの形式

デバイス情報を表示する場合

```
hldutil [-d [<ドライブ番号またはデバイススペシャルファイル名>] | -g [<ドライブグループ名>] | -l <LDEV 番号>.<シリアル番号>] [-p] [-q] [-nolog] [-s <ソートキー>...] [-serdec] [-k | -hf <ログファイル名> | -h <ログ番号>]
```

デバイス情報を管理する場合

```
hldutil {-h <ログ番号> -hb <ログファイル名> | -hrm { <ログ番号> | all } | -history <ログファイルの世代数>}
```

コマンドの格納先

Windows の場合

```
<Device Manager エージェントのインストールフォルダ>%util%bin
```

Solaris, Linux, または HP-UX の場合

```
/opt/HDVM/HBaseAgent/util/bin
```

AIX の場合

```
/usr/HDVM/HBaseAgent/util/bin
```

オプション

-d

ドライブ番号 (Windows の場合) またはデバイススペシャルファイル名 (UNIX の場合) で指定した LDEV の情報を表示します。ドライブ番号またはデバイススペシャルファイル名を省略した場合は、現在認識されているすべての LDEV の情報を表示します。

-g

ドライブグループ名で指定したドライブグループの情報を表示します。ドライブグループ名を省略した場合は、現在定義されているすべてのドライブグループの情報が表示されます。

-l

LDEV 番号とシリアル番号で指定した LDEV の情報を表示します。必ず LDEV 番号、シリアル番号の順で指定します。LDEV 番号とシリアル番号のどちらかを省略した場合、LDEV の情報は表示されません。

このオプションを指定した場合、表示項目が次のものに限定されます。

- Ldev# (LDEV 番号)
- Ser# (ストレージシステムのシリアル番号)
- Device (デバイススペシャルファイル名またはドライブ番号)
- Dg name (ドライブグループ名)
- fs (ファイルシステム)

-p

ドライブ情報に ShadowImage, TrueCopy, Copy-on-Write Snapshot, Thin Image, QuickShadow, または Universal Replicator で設定した P-VOL と S-VOL の情報を付けます。LDEV に P-VOL と S-VOL の情報が割り当てられていない場合は、このオプションを指定しても P-VOL と S-VOL の情報は表示されません。

-q

コマンドの実行結果を標準出力には出力しないで、実行結果ログファイルだけに出力します (quiet モード)。このオプションは、バックグラウンドでジョブを実行しながら最新の LDEV 情報を実行結果ログファイルに出力する場合に指定します。エラーメッセージは標準エラー出力に出力されます。

-nolog

コマンドの実行結果を標準出力に出力します。実行結果ログファイルは更新しません。

-s

LDEV 情報を ASCII コードの昇順で表示します。

複数のソートキーを指定する場合は、半角スペースで各ソートキーを区切ります。複数のソートキーを指定した場合は、指定順のソートキーでソートされます。ファイルシステム名をソートキーに指定した場合は、各 LDEV に含まれるファイルシステム名のうち、ASCII コードが最も小さいファイルシステム名で、LDEV 情報がソートされます。

このオプションを省略した場合は、コマンドが処理した情報の順序で LDEV 情報が表示されます。

-serdec

ストレージシステムのシリアル番号を 10 進数で表示します。

-k

最新の実行結果ログファイルの内容を標準出力に出力します。

標準出力への出力にはハードウェアへのアクセスは生じません。ただし、実行結果ログファイルにドライブ情報が記録されていない場合は、ドライブ情報を取得し、標準出力と実行結果ログファイルに出力されます。

-hf

指定した実行結果ログファイルの内容を標準出力に出力します。

標準出力への出力にはハードウェアへのアクセスは生じません。

-h

指定したログ番号の実行結果ログファイルの内容を標準出力に出力します。

標準出力への出力にはハードウェアへのアクセスは生じません。

このオプションと -hb オプションを一緒に指定すると、実行結果ログファイルのコピーを作成します。-h オプションでコピー元の実行結果ログファイル名のログ番号を指定し、-hb オプションでコピー先を指定します。

-hb

実行結果ログファイルのコピーを作成します。このオプションは必ず-h オプションと一緒に指定します。

-h オプションでコピー元の実行結果ログファイル名のログ番号を指定し、-hb オプションでコピー先を指定します。コピー先のファイル名は絶対パスまたは相対パスで指定します。

-hrm

指定したログ番号の実行結果ログファイルを削除します。all を指定すると、デフォルトのログ格納用ディレクトリからすべての実行結果ログファイルが削除されます。

-history

実行結果ログファイルの世代数を指定します。指定できる世代数は1から64です。デフォルト値は32です。指定した値は、次に実行結果ログファイルが作成された際に有効になります。



注意 LUの追加や削除など、ホストの環境を変更したあとすぐに hldutil コマンドを実行すると、ホストの変更内容を認識できないことがあります。この場合、しばらく待ってから再度 hldutil コマンドを実行してください。

関連項目

- (3) hldutil コマンドで指定できるソートキー

(1) hldutil コマンドで表示される情報

hldutil コマンドを実行した場合に表示される情報を、出力順で次の表に示します。

OS や指定したオプションによって、表示される項目は異なります。

表 11-10 hldutil コマンドで表示される情報

表示項目	意味
Dg name	ドライブグループ名
Device	ドライブ番号 (Windows の場合)
	デバイススペシャルファイル名 (UNIX の場合)
fs	ファイルシステム名
P/S※1	P-VOL, S-VOL の区別
Vend.	ベンダー名
Prod.	プロダクト名
Port#	ポート番号 (DKC 側)
Tid#※2	ターゲット ID (ホスト側 SCSI インターフェース)
Lun#※2	LU 番号 (ホスト側 SCSI インターフェース)
Ldev#	LDEV 番号 (DKC 側)
Ser#	ストレージシステムのシリアル番号
RaidID	ストレージシステムの機種を表す文字列
RG#	パリティグループ番号
PortWWN※3	Port WWN 名
NodeWWN※3	Node WWN 名
iSCSIName	iSCSI イニシエーターの iSCSI ネーム

注※1

ホストが仮想マシンの場合、P-VOL や S-VOL の構成を変更したあとに hldutil コマンドを実行すると、情報が正しく表示されないことがあります。仮想化サーバを再起動すると、正しい情報が表示されます。

注※2

HP-UX 11i v3 の一貫性のある特殊デバイス (persistent device special file) の場合、この項目は出力されません。

注※3

NPIV を使用して仮想マシンに仮想 WWN を割り当てている場合、仮想化サーバの物理 WWN が出力されます。

(2) hldutil コマンドで表示される RaidID が表すストレージシステムの機種

hldutil コマンドで表示される RaidID は、ストレージシステムの機種を表す文字列です。

RaidID とストレージシステムの機種の対応を次の表に示します。

表 11-11 hldutil コマンドで表示される RaidID とストレージシステムの機種の対応

RaidID	ストレージシステムの機種
71	Hitachi WMS 100 または BR50
73	Hitachi AMS 200 または BR150
75	Hitachi AMS 500
77	Hitachi AMS 1000 または Hitachi TMS1000
81	Hitachi SMS 100
82	Hitachi SMS 110
83	Hitachi AMS 2010, Hitachi AMS 2100 または BR1600 シリーズ
85	Hitachi AMS 2300
87	Hitachi AMS 2500
91	HUS110 または BR1650S
92	HUS130 または BR1650E
93	HUS150
D60H	SANRISE9580V
HM70	HUS VM
R450	SANRISE9980V または SANRISE H1024
R451	SANRISE9970V または SANRISE H128
R500	Hitachi USP 100, Hitachi USP 600 または Hitachi USP 1100
R501	Hitachi NSC 55
R600	Universal Storage Platform V
R601	Universal Storage Platform VM
R700	Virtual Storage Platform

(3) hldutil コマンドで指定できるソートキー

hldutil コマンドの -s オプションにソートキーを指定すると、取得した LDEV 情報をソートできます。

hldutil コマンドで指定できるソートキーを次に示します。

表 11-12 hldutil コマンドで指定できるソートキー

ソートキー	説明
dg	ドライブグループ名でソートします。
fs	ファイルシステム名でソートします。
iscsin	iSCSI イニシエーターの iSCSI ネームでソートします。
ldev	LDEV 番号でソートします。
lun	LU 番号でソートします。
port	ポート番号でソートします。
prod	プロダクト名でソートします。
rg	パリティグループ番号でソートします。
rid	ストレージシステムの機種を表す文字列でソートします。
ser	ストレージシステムのシリアル番号でソートします。
tid	ターゲット ID でソートします。
vend	ベンダー名でソートします。
wwnn	Node WWN 名でソートします。
wwnp	Port WWN でソートします。

11.4 構成定義ファイルの利用

Device Manager では、ユーザーが作成した RAID Manager または P9000 RAID Manager の構成定義ファイルを利用して、コピーペアを管理できます。

11.4.1 構成定義ファイルを利用するための前提環境

構成定義ファイルを利用するためには、RAID Manager または P9000 RAID Manager がインストールされているホストでの環境設定が必要です。

- Device Manager エージェントのインストール
- Device Manager サーバの情報の設定
- Device Manager でコピーペアを管理するための設定

関連項目

- [11.2.4 コピーペアを管理するために必要な設定](#)
- [11.3.4 Device Manager サーバの情報、HiScan コマンドの実行周期および RAID Manager または P9000 RAID Manager の情報の設定 \(hdvماغt_setting コマンド\)](#)
- [11.4.2 構成定義ファイルの編集](#)

11.4.2 構成定義ファイルの編集

horcmXX.conf ファイルを編集して、ストレージシステムをリフレッシュします。

構成定義ファイルを編集するには：

1. horcmXX.conf ファイルを開きます。
構成定義ファイルは、Device Manager エージェントの server.properties ファイルの server.agent.rm.horcmSource プロパティで指定されたディレクトリに格納されています。

デフォルトの格納場所は次のとおりです。

Windows の場合

システムフォルダ (環境変数"%windir%"で表されるフォルダ)

UNIX の場合

/etc ディレクトリ

horcmXX.conf ファイルが存在しない場合は、新規に作成してください。

2. 記述規則に沿って、パラメーターを設定します。
3. Device Manager GUI/CLI を使用して、構成定義ファイルに記述したコピーペアボリュームが存在するストレージシステムをリフレッシュします。



重要

- Device Manager がサポートしていないパラメーターを使用すると、構成定義ファイルが不正であると見なされ、処理が正常に実行されません。また、サポートしているパラメーターであっても、一部の記述形式をサポートしていない場合があります。サポートしていない形式で項目を指定した場合も構成定義ファイルは不正と見なされるので注意してください。
- Device Manager エージェントでは、コピーペアの情報を取得する際に次のインスタンス番号および UDP ポート番号を一時的に使用します。そのため、構成定義ファイルのインスタンス番号および UDP ポート番号を指定する場合は、その値と重複しないようにしてください。
 - インスタンス番号：900～998 (デフォルト)
 - UDP ポート番号：53232～53330 (デフォルト)これらのインスタンス番号または UDP ポート番号を使用した場合、システムログまたはイベントログに、RAID Manager または P9000 RAID Manager のエラー情報が出力されることがあります。



参考 Device Manager エージェントが一時的に使用するインスタンス番号および UDP ポート番号は、server.properties ファイルにある server.agent.rm.temporaryInstance プロパティおよび server.agent.rm.temporaryPort プロパティで変更できます。

関連項目

- 11.4.1 構成定義ファイルを利用するための前提環境
- 11.4.4 構成定義ファイルを利用する上での注意事項
- D.2.4 agent.rm.horcmInstance
- D.2.5 agent.rm.horcmService
- D.6.21 server.agent.rm.temporaryInstance
- D.6.22 server.agent.rm.temporaryPort
- D.6.26 server.agent.rm.horcmSource

(1) Device Manager がサポートしている構成定義ファイルのパラメーター

Device Manager がサポートしていないパラメーターを使用すると、構成定義ファイルが不正であると見なされ、処理が正常に実行されません。

Device Manager では、次のパラメーターをサポートしています。

- HORCM_MON
- HORCM_CMD
- HORCM_DEV
- HORCM_LDEV
- HORCM_INST

- HORCM_INSTP
- HORCM_CTQM※

注※

Device Manager エージェントのバージョンが 6.2 以降の場合だけサポートしています。ただし、ペアの作成時または操作時に、構成定義ファイルに HORCM_CTQM が定義されていても Device Manager エージェントは無視して動作します。Device Manager エージェントが構成定義ファイルに HORCM_CTQM の定義を追加したり、既存の定義にペアグループを追加したりすることはありません。ただし、ペアの削除時に、削除するペアグループと同名のグループがある場合、HORCM_CTQM の定義からグループを削除します。

関連項目

- (2) 構成定義ファイルの記述規則
- (3) HORCM_MON パラメーターの記述形式
- (4) HORCM_CMD パラメーターの記述形式
- (5) HORCM_DEV パラメーターの記述形式
- (6) HORCM_LDEV パラメーターの記述形式
- (7) HORCM_INST パラメーターの記述形式
- (8) HORCM_INSTP パラメーターの記述形式

(2) 構成定義ファイルの記述規則

構成定義ファイルが記述規則に沿って作成されていない場合、Device Manager では構成定義ファイルを不正と見なします。

次の規則に従って、構成定義ファイルを作成してください。

- 構成定義ファイルには、スペースだけの行を含むことはできません。
- Device Manager エージェントのバージョンが 05-50 以前の場合、パラメーターの開始行以外には、"H"で始まり、次の文字列を含む行があってははいけません。
HORCM_MON, HORCM_CMD, HORCM_DEV, HORCM_LDEV, HORCM_INST, HORCM_INSTP, HORCM_CTQM, HORCM_LDEVG, HORCM_ALLOW_INST
- Device Manager エージェントのバージョンが 7.0.0~7.0.1 の場合、構成定義ファイルの HORCM_CMD パラメーターに仮想コマンドデバイスの定義があってははいけません。
- 構成定義ファイルは、次の規則に従って作成されている必要があります。
 - HORCM_MON が定義されていること
 - HORCM_DEV または HORCM_LDEV の少なくともどちらか一方が定義されていること
 - HORCM_INST または HORCM_INSTP の少なくともどちらか一方が定義されていること
 - HORCM_ALLOW_INST が定義されていないこと

関連項目

- (1) Device Manager がサポートしている構成定義ファイルのパラメーター
- (3) HORCM_MON パラメーターの記述形式
- (4) HORCM_CMD パラメーターの記述形式
- (5) HORCM_DEV パラメーターの記述形式
- (6) HORCM_LDEV パラメーターの記述形式

- (7) HORCM_INST パラメーターの記述形式
- (8) HORCM_INSTP パラメーターの記述形式

(3) HORCM_MON パラメーターの記述形式

HORCM_MON パラメーターには、自ホストのマシン情報や、コピーペアボリュームの障害の監視間隔を指定します。

- ip_address
IP アドレス (Device Manager エージェントのバージョン 5.9 以降は IPv6 もサポート)、ホスト名、"NONE", または "NONE6" を指定します。なお、Replication Manager を使用して構成定義ファイルを生成した場合、常にホスト名で指定されます (Replication Manager は Device Manager エージェントを利用して、構成定義ファイルを参照します)。
 - Device Manager サーバで管理されているホストの情報を指定してください。
 - IP アドレスのバージョン (IPv6 または IPv4) は、HORCM_INST または HORCM_INSTP の ip_address と一致させてください。
 - IPv6 で運用する場合は、IP アドレスで指定してください。ホスト名を指定した場合は、IPv4 で動作します。
OS が Windows Server 2003 R2 の場合、IPv6 アドレスを指定できません。Windows Server 2003 R2 で IPv6 を使用する場合は、NONE6 を指定してください。
 - ip_address に指定できる値を次に示します。一部の形式は、ホストを特定できないため、ip_address には指定できません。

表 11-13 HORCM_MON パラメーターの ip_address に指定できる値

値	Device Manager エージェントのバージョン		
	5.9 以降	05-80	05-70 以前
IP アドレス	○	○	○
ホスト名	○	○	○
NONE	△	△	×
"_NONE_"	×	×	×
NONE6	△	×	×
"_NONE6_"	×	×	×
ループバックの IP アドレス (127.0.0.1 ~127.255.255.254)	△	△	×
ループバックのホスト名 (localhost)	△	△	×
クラスタの仮想 IP アドレス	×	×	×
クラスタの仮想マシン名	×	×	×

(凡例)

○：指定できる。

△：Device Manager CLI でコピーペアを管理する場合には指定できる。Device Manager GUI または Replication Manager からコピーペアを操作する場合は指定できない。

×：指定できない。

- service
ポート名称またはポート番号を指定します。
 - ポート名称を指定する場合、半角 15 文字以内で指定する必要があります。また、ポート番号への名前変換ができる環境である必要があります。

- ポート番号を指定する場合、0～65535 の数値で指定する必要があります。
- poll
10 ミリ秒単位の数値または"-1"を指定します。
- timeout
タイムアウト時間を 10 ミリ秒単位で指定します。

表 11-14 HORCM_MON パラメーターの記述形式のサポート状況

バージョン	指定項目			
	ip_address	service	poll	timeout
6.1 以降	○	○	○	○
5.9～6.0	○	ポート番号指定だけサポート。	○	○
05-80	IP アドレス、ホスト名、"NONE"の指定だけサポート。	ポート番号指定だけサポート。	○	○
05-70 以前	IP アドレス、ホスト名の指定だけサポート。	ポート番号指定だけサポート。	○	○

(凡例)

○ : すべての記述形式をサポート

関連項目

- 11.4.2 構成定義ファイルの編集
- (2) 構成定義ファイルの記述規則
- (7) HORCM_INST パラメーターの記述形式
- (8) HORCM_INSTP パラメーターの記述形式
- 11.4.4 構成定義ファイルを利用する上での注意事項

(4) HORCM_CMD パラメーターの記述形式

HORCM_CMD パラメーターには、ストレージシステム上のコマンドデバイスを指定します。

- dev_name
必ず、ホストで認識されているコマンドデバイスを指定してください。同一装置内のコマンドデバイスを複数指定したり、複数装置のコマンドデバイスを指定したりすることもできます。
Windows の場合は、IPCMD 形式、PhysicalDrive 形式、GUID 形式、または CMD 形式でコマンドデバイスを指定します。

IPCMD 形式

¥¥.¥IPCMD-<仮想コマンドデバイスの IP アドレス>-<ポート番号>[-<ストレージシステムのユニット ID >]

PhysicalDrive 形式

¥¥.¥PhysicalDrive < Windows によって定義されるドライブ番号 >

Device Manager エージェントのバージョンが 04-30 以前の場合は、大文字と小文字を区別して指定する必要があります。

GUID 形式

¥¥.¥Volume{ < GUID > }

CMD 形式

¥¥.¥CMD-<シリアル番号>[-<LDEV 番号>[-<ポート名称>[-<ホストグループ番号>]]]

シリアル番号および論理デバイス番号は 10 進数で指定する必要があります。ホストグループ番号は、Device Manager エージェントのバージョンが 05-60 以降の場合は 0~254 の値を、05-50 以前の場合は 0~127 の値を指定する必要があります。

UNIX の場合は、IPCMD 形式、CMD 形式またはスペシャルファイルでコマンドデバイスを指定します。

IPCMD 形式

¥¥.¥IPCMD-<仮想コマンドデバイスの IP アドレス>-<ポート番号>[-<ストレージシステムのユニット ID >]

CMD 形式

¥¥.¥CMD-<シリアル番号>[-<LDEV 番号>[-<ポート名称>[-<ホストグループ番号>]]]<HINT >

シリアル番号および論理デバイス番号は 10 進数で指定する必要があります。ホストグループ番号は、Device Manager エージェントのバージョンが 05-60 以降の場合は 0~254 の値を、05-50 以前の場合は 0~127 の値を指定する必要があります。

HINT は、次のように指定します。

Solaris : /dev/rdisk/

AIX : /dev/rhdisk

Linux : /dev/sd

HP-UX : /dev/rdisk/または/dev/rdisk/disk

表 11-15 HORCM_CMD パラメーターの記述形式のサポート状況

バージョン		指定項目
		dev_name
7.4.1 以降	Windows の場合	○
	UNIX の場合	○
7.1~7.4.0	Windows の場合	○
	UNIX の場合	スペシャルファイルによる指定、または IPCMD 形式による指定だけサポート。
05-10~7.0	Windows の場合	IPCMD 形式以外をサポート。
	UNIX の場合	スペシャルファイルによる指定だけサポート。
05-00	Windows の場合	IPCMD 形式、CMD 形式以外の記述形式をサポート。
	UNIX の場合	スペシャルファイルによる指定だけサポート。
04-30 以前	Windows の場合	IPCMD 形式、CMD 形式、GUID 形式以外の記述形式をサポート。
	UNIX の場合	スペシャルファイルによる指定だけサポート。

(凡例)

○ : すべての記述形式をサポート

関連項目

- 11.4.2 構成定義ファイルの編集
- (2) 構成定義ファイルの記述規則
- 11.4.4 構成定義ファイルを利用する上での注意事項

(5) HORCM_DEV パラメーターの記述形式

HORCM_DEV パラメーターには、コピーペアとなるボリュームが存在するストレージシステムの情報を指定します。

- dev_group
グループ名称を指定します。
 - 同一ホストの構成定義ファイル間では同じ dev_group と dev_name の組み合わせを重複して指定できません。
 - 半角 31 文字以内で指定する必要があります。また、ハイフン (-) で始まる文字列は指定できません。
- dev_name
ペア論理ボリューム名称を指定します。
 - 1 つの構成定義ファイル内では同じ dev_name を重複して指定できません。
 - 半角 31 文字以内で指定する必要があります。また、ハイフン (-) で始まる文字列は指定できません。
- port#
ポート名称を指定します。
port# にポート名称を指定し、続けてホストグループ番号を指定する場合、Device Manager エージェントのバージョンで指定できる値が異なります。Device Manager エージェントのバージョンが 05-60 以降の場合は 0~254 の値を、Device Manager エージェントのバージョンが 05-50 以前の場合は 0~127 の値を指定する必要があります。
- targetID
SCSI/Fibre のターゲット ID を指定します。
- LU#
SCSI/Fibre の論理ユニット番号を指定します。
- MU#
ミラー記述子を数値または h 付加で指定します。省略して空白のままにしておくこともできます。
MU# に指定できる値は、Device Manager エージェントのバージョンとコピータイプによって次のように異なります。

Device Manager エージェントのバージョンが 7.4.0 以降の場合

ShadowImage : 0~2

Copy-on-Write Snapshot : 0~63

Thin Image : 0~63

TrueCopy : 指定なし

Universal Replicator : 指定なし※, 0※, h1, h2, h3

注※

値を指定しない場合または 0 を指定した場合は、TrueCopy でマルチターゲット構成のペアを作成できません。

Device Manager エージェントのバージョンが 6.0～7.3.1 の場合

ShadowImage : 0～2

Copy-on-Write Snapshot : 0～63

TrueCopy : 指定なし

Universal Replicator : 指定なし※, 0※, h1, h2, h3

注※

値を指定しない場合または 0 を指定した場合は、TrueCopy でマルチターゲット構成のペアを作成できません。

Device Manager エージェントのバージョンが 04-20～5.9 の場合

ShadowImage : 0～2

Copy-on-Write Snapshot : 0～31

TrueCopy : 指定なし

Universal Replicator : h1, h2, h3

Device Manager エージェントのバージョンが 04-00 または 04-10 の場合

ShadowImage : 0～2

Copy-on-Write Snapshot : 0～13

TrueCopy : 指定なし

Universal Replicator : h1, h2, h3

Device Manager エージェントのバージョンが 03-50 以前の場合

ShadowImage : 0～2

Copy-on-Write Snapshot : 0～13

TrueCopy : 指定なし

表 11-16 HORCM_DEV パラメーターの記述形式のサポート状況

バージョン	指定項目					
	dev_group	dev_name	port#	targetID	LU#	MU#
04-00 以降	○	○	○	○	○	○
03-50 以前	○	○	○	○	○	ミラー記述子, 省略 (空白), または数値による指定だけサポート。

(凡例)

○ : すべての記述形式をサポート

関連項目

- 11.4.2 構成定義ファイルの編集
- (2) 構成定義ファイルの記述規則
- 11.4.4 構成定義ファイルを利用する上での注意事項

(6) HORCM_LDEV パラメーターの記述形式

HORCM_LDEV パラメーターには、コピーペアが存在するストレージシステムの情報とボリュームの情報を指定します。

- dev_group

グループ名称を指定します。

- 同一ホストの構成定義ファイル間では同じ dev_group と dev_name の組み合わせを重複して指定できません。
- 半角 31 文字以内で指定する必要があります。また、ハイフン (-) で始まる文字列は指定できません。
- dev_name
ペア論理ボリューム名称を指定します。
 - 1 つの構成定義ファイル内では同じ dev_name を重複して指定できません。
 - 半角 31 文字以内で指定する必要があります。また、ハイフン (-) で始まる文字列は指定できません。
- Serial#
ストレージシステムの装置番号を 10 進数またはシリアル番号:ジャーナル ID 形式で指定します。
- CU:LDEV (LDEV#)
LDEV 番号を 10 進数, 16 進数, または CU:LDEV 形式で指定します。
LDEV# の指定例を示します。

10 進数の場合

260

16 進数の場合

0x104

CU:LDEV 形式の場合

01:04

- MU#
ミラー記述子を数値または h 付加で指定します。省略して空白のままにしておくこともできます。
MU# に指定できる値は、Device Manager エージェントのバージョンとコピータイプによって次のように異なります。

Device Manager エージェントのバージョンが 7.4.0 以降の場合

ShadowImage : 0~2

Copy-on-Write Snapshot : 0~63

Thin Image : 0~63

TrueCopy : 指定なし

Universal Replicator : 0※, h1, h2, h3

注※

指定した場合、TrueCopy でマルチターゲット構成のペアを作成できません。

Device Manager エージェントのバージョンが 6.0~7.3.1 の場合

ShadowImage : 0~2

Copy-on-Write Snapshot : 0~63

TrueCopy : 指定なし

Universal Replicator : 0※, h1, h2, h3

注※

指定した場合、TrueCopy でマルチターゲット構成のペアを作成できません。

Device Manager エージェントのバージョンが 5.9 以前の場合

ShadowImage : 0~2

Copy-on-Write Snapshot : 0~31

TrueCopy : 指定なし

Universal Replicator : h1, h2, h3

表 11-17 HORCM_LDEV パラメーターの記述形式のサポート状況

バージョン	指定項目				
	dev_group	dev_name	Serial#	CU:LDEV (LDEV#)	MU#
6.2 以降	○	○	○	○	○
6.1~05-60	○	○	○	シリアル番号:ジャーナル ID 形式以外の記述形式を サポート。	○
05-50 以前	×	×	×	×	×

(凡例)

○ : すべての記述形式をサポート

× : すべての記述形式が非サポート

関連項目

- [11.4.2 構成定義ファイルの編集](#)
- [\(2\) 構成定義ファイルの記述規則](#)
- [11.4.4 構成定義ファイルを利用する上での注意事項](#)

(7) HORCM_INST パラメーターの記述形式

HORCM_INST パラメーターには、相手ホストのマシン情報を指定します。

- dev_group
HORCM_DEV パラメーターまたは HORCM_LDEV パラメーターの dev_group に指定した内容を指定します。
 - 1つの dev_group に対して同一ホストの複数の ip_address を指定することはできません。
 - 半角 31 文字以内で指定する必要があります。また、ハイフン (-) で始まる文字列は指定できません。
- ip_address
IP アドレス (Device Manager エージェントのバージョン 5.9 以降は IPv6 もサポート)、ホスト名、"NONE", または "NONE6" を指定します。"NONE" または "NONE6" を指定するとローカルホストを指定したものと見なされます。ただし、Replication Manager を使用して、既存の構成定義ファイルに新規グループを追加した場合は、常にホスト名が指定されます。
 - Device Manager サーバで管理されているホストの情報を指定してください。
 - IP アドレスのバージョン (IPv6 または IPv4) は、HORCM_MON の ip_address と一致させてください。
 - IPv6 で運用する場合は、IP アドレスを指定してください。ホスト名を指定した場合は、IPv4 で動作します。
 - ip_address に指定できる値を次に示します。一部の形式は、ホストを特定できないため、ip_address には指定できません。

表 11-18 HORCM_INST パラメーターの ip_address に指定できる値

値	Device Manager エージェントのバージョン	
	05-80 以降	05-70 以前
IP アドレス	○	○
ホスト名	○	○
ループバックの IP アドレス (127.0.0.1 ～127.255.255.254)	△	×
ループバックのホスト名 (localhost)	△	×
クラスタの仮想 IP アドレス	×	×
クラスタの仮想マシン名	×	×

(凡例)

○：指定できる。

△：Device Manager CLI でコピーペアを管理する場合には指定できる。Device Manager GUI または Replication Manager からコピーペアを操作する場合は指定できない。

×：指定できない。

- service

ポート名称またはポート番号を指定します。

- ポート名称を指定する場合、半角 15 文字以内で指定する必要があります。また、ポート番号への名前変換ができる環境である必要があります。
- ポート番号を指定する場合、0～65535 の数値で指定する必要があります。

表 11-19 HORCM_INST パラメーターの記述形式のサポート状況

バージョン	指定項目		
	dev_group	ip_address	service
7.0 以降	○	○	○
6.1～6.4	○	IP アドレス、ホスト名の指定だけサポート。	○
6.0 以前	○	IP アドレス、ホスト名の指定だけサポート。	ポート番号指定だけサポート。

(凡例)

○：すべての記述形式をサポート

関連項目

- 11.4.2 構成定義ファイルの編集
- (2) 構成定義ファイルの記述規則
- (3) HORCM_MON パラメーターの記述形式
- (5) HORCM_DEV パラメーターの記述形式
- (6) HORCM_LDEV パラメーターの記述形式
- 11.4.4 構成定義ファイルを利用する上での注意事項

(8) HORCM_INSTP パラメーターの記述形式

HORCM_INSTP パラメーターには、相手ホストのマシン情報とパスグループ ID を指定します。

- dev_group
HORCM_DEV パラメーターまたは HORCM_LDEV パラメーターの dev_group に指定した内容を指定します。
 - 1つの dev_group に対して同一ホストの複数の ip_address を指定することはできません。
 - 半角 31 文字以内で指定する必要があります。また、ハイフン (-) で始まる文字列は指定できません。
- ip_address
IP アドレス、ホスト名、"NONE", または"NONE6"を指定します。"NONE"または"NONE6"を指定するとローカルホストを指定したものと見なされます。ただし、Replication Manager を使用して、既存の構成定義ファイルに新規グループを追加した場合は、常にホスト名が指定されます。
 - Device Manager サーバで管理されているホストの情報を指定してください。
 - IP アドレスのバージョン (IPv6 または IPv4) は、HORCM_MON の ip_address と一致させてください。
 - IPv6 で運用する場合は、IP アドレスを指定してください。ホスト名を指定した場合は、IPv4 で動作します。
 - ip_address に指定できる値を次に示します。一部の形式は、ホストを特定できないため、ip_address には指定できません。

表 11-20 HORCM_INSTP パラメーターの ip_address に指定できる値

値	Device Manager エージェントのバージョン
	7.6.0 以降
IP アドレス	○
ホスト名	○
ループバックの IP アドレス (127.0.0.1~127.255.255.254)	△
ループバックのホスト名 (localhost)	△
クラスタの仮想 IP アドレス	×
クラスタの仮想マシン名	×

(凡例)

○：指定できる。

△：Device Manager CLI でコピーペアを管理する場合には指定できる。Device Manager GUI または Replication Manager からコピーペアを操作する場合は指定できない。

×：指定できない。

- service
ポート名称またはポート番号を指定します。
 - ポート名称を指定する場合、半角 15 文字以内で指定する必要があります。また、ポート番号への名前変換ができる環境である必要があります。
 - ポート番号を指定する場合、0~65535 の数値で指定する必要があります。
- pathID
パスグループ ID を 1~255 の 10 進数で指定します。
 - 1つのコピーグループに複数のパスグループ ID を指定することはできません。
 - パスグループ ID を指定しない場合 (CU Free の場合) は、HORCM_INST パラメーターを使用してください。

表 11-21 HORCM_INSTP パラメーターの記述形式のサポート状況

バージョン	指定項目
	すべてのパラメーター
7.6.0 以降	○
6.2～7.5.0	△
6.1 以前	×

(凡例)

○：すべての記述形式をサポート

△：ペアの作成時または操作時に指定されていても無視される。ペアの削除時に、削除するペアグループと同名のグループがある場合、HORCM_INSTP の定義からグループが削除される。

×：すべての記述形式が非サポート

関連項目

- 11.4.2 構成定義ファイルの編集
- (2) 構成定義ファイルの記述規則
- (3) HORCM_MON パラメーターの記述形式
- (5) HORCM_DEV パラメーターの記述形式
- (6) HORCM_LDEV パラメーターの記述形式
- (7) HORCM_INST パラメーターの記述形式
- 11.4.4 構成定義ファイルを利用する上での注意事項

11.4.3 構成定義ファイルの格納場所の変更

RAID Manager または P9000 RAID Manager の構成定義ファイルの格納場所を変更する場合は、格納場所のパスを Device Manager エージェントの `server.properties` ファイルの `server.agent.rm.horcSource` プロパティに設定します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

構成定義ファイルの格納場所を変更するには：

1. `hbsasrv` コマンドを実行して、Device Manager エージェントのサービスを停止します。
2. RAID Manager のコマンドを実行して、ユーザーが手動で起動した HORCM インスタンスをすべて停止します。
3. 構成定義ファイルの格納場所を変更します。
4. Device Manager エージェントの `server.properties` ファイルの `server.agent.rm.horcSource` プロパティに、手順 3 で変更した格納場所のパスを指定します。
5. `hbsasrv` コマンドを実行して、Device Manager エージェントのサービスを起動します。

関連項目

- (1) Device Manager エージェントのサービスの起動、停止、稼働状態の確認 (`hbsasrv` コマンド)
- D.6.26 `server.agent.rm.horcSource`

11.4.4 構成定義ファイルを利用する上での注意事項

RAID Manager または P9000 RAID Manager の構成定義ファイルを利用して、コピーペアを管理する場合の注意事項を次に示します。

構成定義ファイルを編集した場合

Device Manager を使用して構成定義ファイルを作成または変更した場合は、構成定義ファイルの内容は自動的に Device Manager サーバに通知されます。

ただし、Replication Manager を使用したり、手動で直接構成定義ファイルを編集したりするなど、Device Manager を使用しないで構成定義ファイルを作成または変更した場合は、Device Manager サーバに構成定義ファイルの情報を手動通知する必要があります。

Device Manager の GUI または CLI を使用してストレージシステムのリフレッシュを実行すると、構成定義ファイルの情報が Device Manager サーバに通知されます。構成定義ファイルに記述したコピーペアボリュームが属するストレージシステムをリフレッシュしてください。

構成定義ファイルを最適化する場合

server.properties ファイルの server.agent.rm.optimization.userHorcmFile プロパティに true が指定されている場合、Device Manager エージェントのサービス起動時およびコピーペアの操作時に、Device Manager エージェントによって構成定義ファイルの内容が最適化されます。このとき、次の点に注意してください。

- 構成定義ファイルのバックアップについて
最適化処理の実行時には、元の構成定義ファイル horcmXX.conf を horcmXX.conf.bk としてバックアップします。バックアップファイルは 1 世代しか作成されないため、最適化処理が 2 回以上実行されると、ユーザーが作成したオリジナルの構成定義ファイルは失われます。必要に応じてバックアップを作成してください。
- コマンドデバイスの定義に追加されるコメントについて
RAID Manager または P9000 RAID Manager の構成定義ファイルに対して最適化処理が実施されると、コマンドデバイスを定義している行の 1 行前にコマンドデバイスのユニット ID、論理デバイス番号およびシリアル番号がコメントとして追加されます。このとき、次の点に注意してください。
 - ・ Device Manager エージェントが追加されたコメントを参照するので、コメントの内容を変更しないでください。
 - ・ Device Manager エージェントが管理している構成定義ファイルをコピーして、新たに構成定義ファイルを作成する場合、コメントは削除してください。

コピーペアを削除する場合

管理クライアントからコピーペアの削除を実行する場合、対象となる構成定義ファイルのコピーペアの定義がすべて削除されるときには、構成定義ファイルも削除されます。構成定義ファイルを削除したくない場合は、削除実行前に構成定義ファイルをバックアップしておいてください。

関連項目

- ・ 11.4.2 構成定義ファイルの編集
- ・ D.6.19 server.agent.rm.optimization.userHorcmFile

11.5 Device Manager エージェントのリモートインストール

JP1/NETM/DM は、ネットワークを利用して、ソフトウェアの配布やクライアントの資源管理を実現するシステムです。JP1/NETM/DM を使用すると、複数のホストに Device Manager エージェントを一括インストールできます。

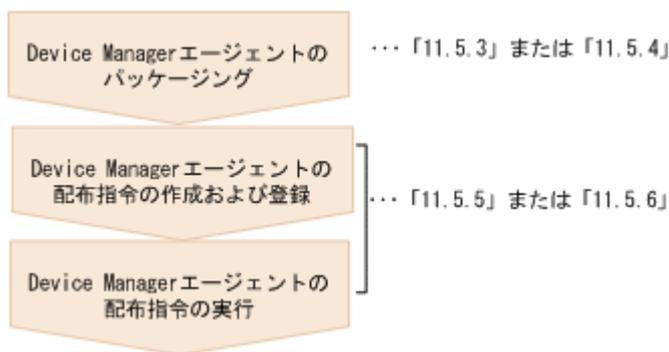
11.5.1 Device Manager エージェントをリモートインストールするための操作フロー

JP1/NETM/DM を使用して、Device Manager エージェントをリモートインストールするには、次の操作が必要です。

- Device Manager エージェントのパッケージング
資源登録システムから配布管理システムへ Device Manager エージェントを登録(パッケージング) します。
- 配布指令の作成および登録
配布管理システムに登録された資源 (Device Manager エージェント) を配布先システムにコピーするための指令を作成および登録します。
- 配布指令の実行
登録された配布指令を実行して、Device Manager エージェントをインストールします。

リモートインストールの操作の流れを次の図に示します。

図 11-1 リモートインストールの流れ

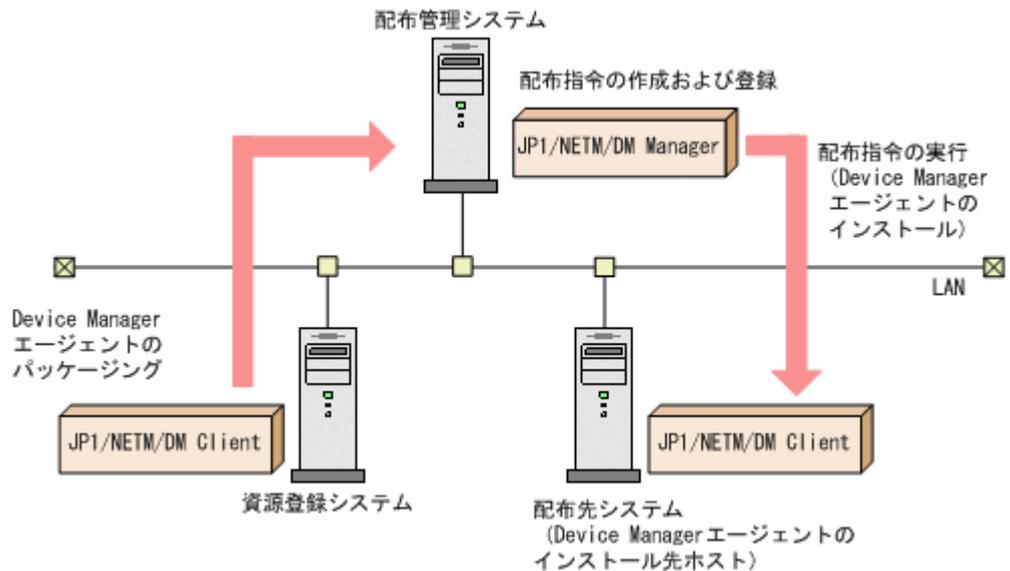


11.5.2 Device Manager エージェントをリモートインストールする場合のシステム構成

JP1/NETM/DM を使用して、Device Manager エージェントをリモートインストールするには、リモートインストール環境が構築されている必要があります。

JP1/NETM/DM を使用して、Device Manager エージェントをリモートインストールする場合のシステム構成を次の図に示します。

図 11-2 JP1/NETM/DM を使用するためのシステム構成



- 配布管理システム
ソフトウェアの配布状況や配布先の状態を管理するシステムです。JP1/NETM/DM Manager (Windows の場合はバージョン 07-00 以降, Solaris の場合はバージョン 06-73 以降) がインストールされている必要があります。
- 資源登録システム
ソフトウェア資源を登録するシステムです。JP1/NETM/DM Client (バージョン 07-00 以降) がインストールされている必要があります。
- 配布先システム
ソフトウェアの配布先となるシステムです。JP1/NETM/DM Client (バージョン 07-00 以降) と Device Manager エージェント (Windows の場合はバージョン 04-10 以降, UNIX の場合はバージョン 04-00 以降) がインストールされている必要があります。

関連項目

- JP1/NETM/DM Manager と JP1/NETM/DM Client のインストール, およびリモートインストール環境の構築方法について: JP1/NETM/DM のマニュアル

11.5.3 Device Manager エージェントのパッケージング (Windows)

Device Manager エージェントをパッケージングするには, JP1_NETM_DM Client の [JP1/NETM/DM パッケージ] ウィンドウから実行します。

事前に完了しておく操作

- Administrator 権限でのログイン

Device Manager エージェントをパッケージングするには:

1. 統合インストールメディアを挿入します。
2. Device Manager エージェントのインストーラーが格納されているフォルダ以下のファイルおよびサブフォルダをすべて任意の場所にコピーします。
3. [スタート] - [すべてのプログラム] - [JP1_NETM_DM Client] - [ソフトウェア パッケージ] を選択し, JP1/NETM/DM にログオンします。

4. [JP1/NETM/DM パッケージ] ウィンドウの [ファイル] ウィンドウから、手順 2. でコピーしたフォルダを選択します。
5. [実行] - [パッケージング] を選択します。
6. [JP1/NETM/DM パッケージング] ダイアログで、環境に合わせて各項目を設定し、[パッケージ実行] を選択します。

関連項目

- 11.5.5 Device Manager エージェントの配布指令の作成、登録および実行 (Windows)
- [JP1/NETM/DM パッケージング] ダイアログの設定項目について : JP1/NETM/DM のマニュアル

11.5.4 Device Manager エージェントのパッケージング (UNIX)

Device Manager エージェントをパッケージングするには、登録ファイルとインストーラー実行シェルを作成し、rdscm コマンドを実行します。

Device Manager エージェントをパッケージングするには :

1. 統合インストールメディアを挿入し、マウントします。
2. Device Manager エージェントのインストーラーが格納されているディレクトリ以下のファイルおよびサブディレクトリを次のコマンドですべてコピーします。
ここでは <DVD のマウントディレクトリ>/AGENTS/HDvM/Solaris と仮定します。
cp -r <DVD のマウントディレクトリ>/AGENTS/HDvM/Solaris /* /var/tmp/HDvM-Agent
3. 資源登録システムに、root 権限でログインします。
4. 登録ファイルとインストーラー実行シェルを作成します。
パッケージを実行するには、登録ファイル (HDvM_Agt_regfile) とインストーラー実行シェル (HDvM_Agt_install) を作成する必要があります。
HDvM_Agt_regfile と HDvM_Agt_install のサンプルファイルは、Device Manager エージェントのインストーラーと同じディレクトリに格納されています。このサンプルファイルは編集しないで使用できます。



重要 デフォルトでは、配布先システムの起動時にインストールされますが、登録ファイルを編集することで、PUSH 型で Device Manager エージェントをインストールするように指定できます。

5. 次のコマンドを実行して、配布管理システムへ Device Manager エージェントを登録します。
chmod 711 /var/tmp/HDvM-Agent/HDvM_Agt_install
rdscm -k <JP1/NETM/DM Manager のパスワード> -d <ソフトウェアディレクトリ>
<登録ファイル>
<ソフトウェアディレクトリ>
資源登録システムに格納されている Device Manager エージェントのディレクトリのパスを指定します。
<登録ファイル>
手順 2. でコピーした HDvM_Agt_regfile ファイルのパスを指定します。
実行例を次に示します。
rdscm -k <JP1/NETM/DM Manager のパスワード> -d ./HDvM-Agent /var/tmp/HDvM-Agent/HDvM_Agt_regfile



参考 Device Manager エージェントの製品に同梱されている登録ファイルのサンプルファイルをそのまま使用する場合、配布先システムが UNIX のときは、/var/tmp を一時的な格納場所とします。

関連項目

- 11.5.6 Device Manager エージェントの配布指令の作成，登録および実行（Solaris）
- 登録ファイルの詳細について：JP1/NETM/DM のマニュアル

11.5.5 Device Manager エージェントの配布指令の作成，登録および実行（Windows）

Device Manager エージェントの配布指令を作成，登録および実行するには，JP1/NETM/DM Manager のリモートインストールマネージャのウィンドウから実行します。

事前に完了しておく操作

- Device Manager エージェントのパッケージング
- Administrator 権限でのログイン

配布指令を作成，登録および実行するには：

1. [スタート] - [すべてのプログラム] - [JP1_NETM_DM Manager] - [リモートインストールマネージャ] を選択します。
2. [システム構成] ウィンドウで，[ファイル] - [新規作成] - [ジョブ定義] を選択します。
3. [ジョブ定義] ウィンドウで，[ファイル] - [ジョブ定義の新規作成] を選択します。
4. ジョブの種別選択で「パッケージのインストール」を選択します。
5. [ジョブの作成] ダイアログで，環境に合わせて各項目を設定し，[保存] を選択します。



重要 [保存&実行] を選択すると，保存と同時にジョブが実行されます。

6. [ジョブ定義] ウィンドウで，手順 5. で登録したジョブを選択します。
7. [実行] - [ジョブの実行] を選択します。



注意 配布先システムのシャットダウン時を指定したリモートインストールはできません。

関連項目

- 11.5.3 Device Manager エージェントのパッケージング（Windows）
- [ジョブの作成] ダイアログの設定項目について：JP1/NETM/DM のマニュアル

11.5.6 Device Manager エージェントの配布指令の作成，登録および実行（Solaris）

Device Manager エージェントの配布指令を作成，登録および実行するには，rdsdmind コマンドを実行します。

事前に完了しておく操作

- Device Manager エージェントのパッケージング

事前に確認しておく情報

- 配布先のホスト名

配布指令を作成、登録および実行するには：

1. 配布管理システムに、root 権限でログインします。
2. 次のコマンドを実行して、登録されているパッケージの一覧を表示し、配布指令を作成するパッケージを確認します。

```
# rdsdmsrc -c
```

コマンドの実行例を次に表示します。

```
# rdsdmsrc -c
KDDH3043-I : Displaying the list of packages.
C 1
C.HC 1
C.HC.HDvM-Agent_SOL.0600.0000
```

3. 次のコマンドを実行して、配布指令を登録します。

```
# rdsdmind -d -a 配布先ホスト名 -s インストールするパッケージ名 -p F
```

パッケージ名の例を次に示します。

- Solaris リソース名称
C.HC.HDvM-Agent_SOL
- AIX リソース名称
C.HC.HDvM-Agent_AIX
- Linux リソース名称
C.HC.HDvM-Agent_LNX
- HP-UX リソース名称
C.HC.HDvM-Agent_HP

コマンドの実行例を次に示します。

```
# rdsdmind -d -a host1 -s C.HC.HDvM-Agent_SOL.0600.0000 -p F
KDDH3023-I : Completed registering a job.
```

4. 次に示すコマンドを実行して、登録した Device Manager エージェントをインストールします。

```
# rdsdmind -x
```

コマンドの実行例を次に示します。

```
# rdsdmind -x
KDDH3027-I : Received a job execution request.
```



注意 配布先システムのシャットダウン時を指定したリモートインストールはできません。

関連項目

- 11.5.4 Device Manager エージェントのパッケージング (UNIX)

11.5.7 リモートインストールの実行結果の戻り値

Windows 環境に Device Manager エージェントをリモートインストールした場合、実行結果の戻り値は、JP1/NETM/DM Manager のジョブ実行状況ウィンドウから表示される詳細情報ダイアログで確認できます。

リモートインストールに失敗した場合、JP1/NETM/DM Manager のジョブ実行状況ウィンドウから表示される詳細情報ダイアログで、保守コードを確認してください。保守コードの左から 9 番目と 10 番目の数字にリモートインストールの実行結果の戻り値が表示されます。この操作は JP1/NETM/DM Manager がインストールされている配布管理システムで実行します。

リモートインストールの実行結果の戻り値一覧を、次の表に示します。

表 11-22 リモートインストールの実行結果の戻り値

戻り値	説明	対処
00	正常終了	なし。
90	Device Manager エージェントのインストールで失敗しました。	<p>次の原因が考えられます。</p> <ul style="list-style-type: none"> • ディスクの空き容量が不足しています。十分な容量を確保してから、再度インストールを実行してください。 • リモートインストールする OS がサポートされていません。OS を確認してください。 • Device Manager エージェント以外のインストール処理またはアンインストール処理を実行中です。実行中の処理が完了してから、再度インストールを実行してください。 • Java の実行環境を提供するプログラムが動作しません。 ホストの OS に Device Manager エージェントの前提パッチが適用されているか確認してください。また、server.properties ファイルの server.agent.JRE.location プロパティに指定されているインストールパスに、Device Manager エージェント用の Java の実行環境を提供するプログラムがインストールされているかを確認してください。 <p>UNIX の場合は次の原因も考えられます。</p> <ul style="list-style-type: none"> • Device Manager エージェントが前提とする Java の実行環境を提供するプログラムがインストールされていません。インストールしてから、再度 Device Manager エージェントのインストールを実行してください。 • インストーラーの実行ファイルの権限を変更できませんでした。インストーラーの実行ファイルを含むディレクトリ内のすべてのファイルおよびサブディレクトリを、権限を変更できる場所に移動してから、再度インストールを実行してください。
91	リモートインストール先のディレクトリの設定値が不正です。	リモートインストール先のディレクトリを正しく設定し、再度インストールを実行してください。
93	Device Manager エージェントのインストールには成功しましたが、他 PP と連携するための設定に失敗しました。	<p>Protection Manager - Console がインストールされている環境の場合、hptmguinst.exe または hptmguinst.sh を実行してください。エラーメッセージを確認し、エラーに対処してから再度インストールを実行してください。</p> <p>Dynamic Link Manager の GUI がインストールされている環境の場合、保守員に連絡してください。</p> <p>OS が Solaris または HP-UX の場合は、Global Link Manager エージェントのインストールに失敗しているおそれがあります。再度インストー</p>

戻り値	説明	対処
		ルを実行してください。それでも失敗する場合は、保守員に連絡してください。
95	Device Manager エージェント機能のセットアップには成功しましたが、Replication Manager エージェント機能のセットアップでエラーが発生しました。	サポート OS および前提パッチを確認したあと、再度実行してください。再度問題が発生した場合は、保守員に連絡してください。
96	実行したユーザーには Administrator 権限がありません。	Administrator 権限があるユーザー ID で再度実行してください。
98	新しいバージョンの Device Manager エージェントがインストールされているため、ダウングレードできません。	なし。
99	Device Manager エージェントまたは関連プログラムが動作中です。	KAIC25111-W~KAIC25113-W メッセージに従って対処してください。

関連項目

- [D.6.9 server.agent.JRE.location](#)
- リモートインストールの実行結果を確認する方法について：JP1/NETM/DM のマニュアル

Host Data Collector のセットアップ

ここでは、Host Data Collector のセットアップ方法について説明します。

- [12.1 Host Data Collector のインストール](#)
- [12.2 Host Data Collector の環境設定](#)
- [12.3 Host Data Collector のアンインストール](#)

12.1 Host Data Collector のインストール

ここでは、管理サーバとは別のマシンに Host Data Collector をインストールする手順を説明します。

12.1.1 Host Data Collector のインストール条件

Host Data Collector のインストール時に指定する項目（インストール先のパスやポート番号）にはデフォルト値が用意されています。

デフォルト値が用意されている項目では、デフォルト値を使用することをお勧めします。

デフォルト値とは異なる設定にする場合は、次の表に示す条件を確認し、指定する値をあらかじめ決めておいてください。

表 12-1 Host Data Collector のインストール中に入力する情報

項目	説明	
インストール先	Host Data Collector のインストール先です。デフォルトは次のとおりです。 Windows の場合 < Program Files フォルダ > ¥Hitachi Solaris または Linux の場合 /opt/Hitachi インストール先をデフォルト以外のパスに変更する場合は、次の条件を満たすインストール先を用意してください。 ・ 絶対パスの長さ：64 バイト以内 ・ 指定できる文字： Windows の場合 A~Z a~z 0~9 . _ () 半角スペース ¥ : Solaris または Linux の場合 A~Z a~z 0~9 _ / ・ そのほかの条件（Windows の場合）： ○ 半角スペースを 2 文字以上続けて指定しないでください。 ○ 半角スペースはフォルダ名の先頭と末尾には指定できません。 ○ ドライブ直下（例えば、D:¥）を指定しないでください。 ○ Windows（IPF または x64）では、環境変数%ProgramFiles%に設定されているフォルダを指定しないでください。	
ポート番号	RMI レジストリーのポート番号	RMI レジストリーの非 SSL 通信用のポート番号です。 デフォルト：22098/tcp
	RMI サーバのポート番号	RMI サーバの非 SSL 通信用のポート番号です。 デフォルト：22099/tcp
	クラスローダー用ポート番号	クラスローダーの非 SSL 通信用のポート番号です。 デフォルト：22100/tcp

関連項目

- ・ [12.1.2 Host Data Collector のインストール（Windows）](#)
- ・ [12.1.3 Host Data Collector のインストール（Solaris または Linux）](#)

12.1.2 Host Data Collector のインストール（Windows）

統合インストールメディアを使用して、Host Data Collector をインストールします。

事前に完了しておく操作

- ・ マシン要件および前提プログラムの確認
詳細は、「ソフトウェア添付資料」を参照してください。
- ・ Host Data Collector および管理サーバの Hitachi Command Suite 製品のバージョンの確認
 - Device Manager で Host Data Collector を使用してホストを管理する場合、Host Data Collector のバージョンは、管理サーバにインストールされた Device Manager サーバのバージョンと同じか、より新しいバージョンである必要があります。ただし、Host Data Collector のバージョンが 7.5.0 以降の場合、Device Manager サーバのバージョンも 7.5.0 以降である必要があります。
 - 複数のマシンに Host Data Collector をインストールして運用する場合、各マシンの Host Data Collector のバージョンが一致している必要があります。
- ・ Administrator 権限でのログイン

事前に確認しておく情報

- ・ インストール先のパス（新規インストール時）
- ・ Host Data Collector で使用するポート番号（新規インストール時）

Host Data Collector をインストールするには：

1. 統合インストールメディアを挿入します。
2. 表示されたウィンドウの「Host Data Collector」横にある [Install] ボタンをクリックします。
ウィンドウが表示されない場合は、インストーラー（setup.exe）を直接実行してください。
インストーラーは、<DVD ドライブ>:\\$AGENTS\HHDC\Windows フォルダに格納されています。
3. インストールウィザードの指示に従って、各画面で必要な情報を指定します。

インストールが完了すると、[インストール完了] 画面が表示されます。また、Host Data Collector のサービス（Host Data Collector Base Service）が OS に登録されます。



参考

- ・ Host Data Collector のインストーラーは、Device Manager GUI からダウンロードすることもできます。
- ・ バージョン 7.4.1 以前の Host Data Collector がシステムドライブ以外にインストールされている場合、バージョン 7.5.0 以降にアップグレードインストールすると、Host Data Collector のインストールドライブ直下に temp フォルダが作成されます。不要な場合は削除してください。



重要 アップグレードインストールした場合は、管理サーバの Hitachi Command Suite 製品のサービスを再起動する必要があります。

関連項目

- ・ 9.2 サービスの起動
- ・ 9.3 サービスの停止
- ・ 12.1.1 Host Data Collector のインストール条件
- ・ 12.1.5 管理サーバへの Host Data Collector マシンの登録

12.1.3 Host Data Collector のインストール（Solaris または Linux）

統合インストールメディアを使用して、Host Data Collector をインストールします。

事前に完了しておく操作

- マシンの要件および前提プログラムの確認
詳細は、「ソフトウェア添付資料」を参照してください。
- Host Data Collector および管理サーバの Hitachi Command Suite 製品のバージョンの確認
 - Device Manager で Host Data Collector を使用してホストを管理する場合、Host Data Collector のバージョンは、管理サーバにインストールされた Device Manager サーバのバージョンと同じか、より新しいバージョンである必要があります。ただし、Host Data Collector のバージョンが 7.5.0 以降の場合、Device Manager サーバのバージョンも 7.5.0 以降である必要があります。
 - 複数のマシンに Host Data Collector をインストールして運用する場合、各マシンの Host Data Collector のバージョンが一致している必要があります。
- root でのログイン

事前に確認しておく情報

- インストール先のパス（新規インストール時）
- Host Data Collector で使用するポート番号（新規インストール時）

Host Data Collector をインストールするには：

- 統合インストールメディアを挿入します。
自動的にマウントされない場合は、/mnt/dvdrom ディレクトリにマウントしてください。
- インストーラー（setup.sh）が格納されているディレクトリに移動します。
インストーラーは、<DVD-ROMのマウントディレクトリ>/AGENTS/HHDC/<プラットフォーム名>ディレクトリに格納されています。
- 次のコマンドを実行します。
./setup.sh
- 表示されたメッセージに従って操作します。

インストールが完了すると、次のメッセージが表示されます。

```
Host Data Collector installation completed successfully.
```



参考 Host Data Collector のインストーラーは、Device Manager GUI からダウンロードすることもできます。



重要 アップグレードインストールした場合は、管理サーバの Hitachi Command Suite 製品のサービスを再起動する必要があります。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止
- 12.1.1 Host Data Collector のインストール条件
- 12.1.5 管理サーバへの Host Data Collector マシンの登録

12.1.4 Host Data Collector を運用する場合の注意事項

Host Data Collector を運用する場合には、幾つかの注意事項があります。

Host Data Collector を使用してストレージシステムで 256 以上の LUN を認識する Linux ホストを登録すると、KAIC03006-E のエラーメッセージが出力され、操作が失敗します。ホストの OS が Linux の場合、Host Data Collector の管理対象ホストで認識するストレージシステムの 1 ポートごとの LU 数は 256 以下、LUN の範囲は 0~255 となるように指定してください。

また、クラスタ構成の場合は次の点にも注意してください。

- ・ クラスタを構成する全ノードは、同じディスク構成にして、Host Data Collector のインストール先（ドライブ名やパス名）も同じにする必要があります。
- ・ インストール後に Host Data Collector の設定を変更する場合は、全ノードで同一の設定にしてください。
- ・ 実行系ノードで動作している状態でも、待機系ノードの Host Data Collector のサービス（Host Data Collector Base Service）は常に起動した状態にしておく必要があります。

12.1.5 管理サーバへの Host Data Collector マシンの登録

Host Data Collector を管理サーバとは別のマシンにインストールした場合には、Device Manager サーバの `hostdatacollectors.properties` ファイルのプロパティに、Host Data Collector をインストールしたマシンの情報を登録する必要があります。

管理サーバに Host Data Collector マシンの情報を登録することで、ホストを登録したり、各ホストでのボリュームの使用状況を確認したりできるようになります。

事前に完了しておく操作

- ・ Administrator 権限（Windows の場合）または root（Solaris または Linux の場合）でのログイン
- ・ 管理サーバへの Hitachi Command Suite のインストール
- ・ ホストへの Host Data Collector のインストール
- ・ Host Data Collector マシンの OS が Solaris または Linux の場合、Host Data Collector マシンの名前解決の設定（DNS サーバまたは `hosts` ファイルの設定）

事前に確認しておく情報

- ・ Host Data Collector をインストールしたマシンの情報
 - IP アドレスまたはホスト名
 - RMI レジストリーのポート番号
`hdcbase.properties` ファイルの `hdc.common.rmi.registryPort` プロパティまたは `hdc.common.rmi.ssl.registryPort` プロパティで確認できます。
 - RMI サーバのポート番号
`hdcbase.properties` ファイルの `hdc.common.rmi.serverPort` プロパティまたは `hdc.common.rmi.ssl.serverPort` プロパティで確認できます。
 - クラスローダーのポート番号
`hdcbase.properties` ファイルの `hdc.common.http.serverPort` プロパティまたは `hdc.common.https.serverPort` プロパティで確認できます。

Host Data Collector マシンを管理サーバに登録するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. Device Manager サーバの `hostdatacollectors.properties` ファイルにある次のプロパティに、Host Data Collector をインストールしたマシンの情報を設定します。

hdc.rmiregistry プロパティ
hdc.rmiserver プロパティ
hdc.classloader プロパティ

3. Hitachi Command Suite 製品のサービスを起動します。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止
- A.12.2 hdc.rmiregistry
- A.12.3 hdc.rmiserver
- A.12.4 hdc.classloader
- C.2.4 hdc.common.rmi.registryPort
- C.2.5 hdc.common.rmi.serverPort
- C.2.6 hdc.common.http.serverPort
- C.2.7 hdc.common.rmi.ssl.registryPort
- C.2.8 hdc.common.rmi.ssl.serverPort
- C.2.9 hdc.common.https.serverPort

12.2 Host Data Collector の環境設定

ここでは、Host Data Collector の環境設定について説明します。

12.2.1 Host Data Collector の常駐プロセス

Host Data Collector の常駐プロセスには、Host Data Collector のサービスプロセスと JavaVM のサービスプロセスがあります。

Host Data Collector の常駐プロセスを「表 12-2 Host Data Collector の常駐プロセス (Windows)」から「表 12-3 Host Data Collector の常駐プロセス (Solaris または Linux)」に示します。

表 12-2 Host Data Collector の常駐プロセス (Windows)

プロセス名	サービス名	機能
HdcProcessController.exe	Host Data Collector Base Service	Host Data Collector のサービス

表 12-3 Host Data Collector の常駐プロセス (Solaris または Linux)

プロセス名	機能
< Host Data Collector のインストールディレクトリ > /HDC/Base/internal/bin/HdcAdapter.sh	Host Data Collector のサービスの Adapter プロセス※
< Host Data Collector のインストールディレクトリ > /HDC/Base/internal/bin/HdcService.sh	Host Data Collector のサービスの Service プロセス
< Host Data Collector のインストールディレクトリ > /HDC/Base/internal/bin/HdcRMI.sh	Host Data Collector のサービスの RMI プロセス
< Java の実行環境のインストールパス > /bin/java	JavaVM (Adapter) ※

プロセス名	機能
< Java の実行環境のインストールパス >/bin/java	JavaVM (Service)
< Java の実行環境のインストールパス >/bin/java	JavaVM (RMI)

注※

Host Data Collector の `hdcbase.properties` ファイルの `hdc.adapter.adapterProcessNum` プロパティに設定されている Adapter プロセスの数だけ常駐します。



重要 クラスタ構成の場合、実行系ノードで動作している状態でも、待機系ノードの Host Data Collector のサービス (Host Data Collector Base Service) は常に起動した状態にしておく必要があります。

関連項目

- ・ [9.1 Hitachi Command Suite の常駐プロセス](#)

(1) サービスの起動 (Host Data Collector)

`controlservice` コマンドを使って、Host Data Collector のサービスを起動します。

事前に完了しておく操作

- ・ Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

Host Data Collector のサービスを起動するには :

1. 次のコマンドを実行します。

Windows の場合 :

```
< Host Data Collector のインストールフォルダ >%HDC%Base%bin
%controlservice.exe start
```

Solaris または Linux の場合 :

```
< Host Data Collector のインストールディレクトリ >/HDC/Base/bin/
controlservice.sh start
```

関連項目

- ・ [12.2.1 Host Data Collector の常駐プロセス](#)
- ・ [\(2\) サービスの停止 \(Host Data Collector\)](#)
- ・ [\(3\) サービスの稼働状態の確認 \(Host Data Collector\)](#)

(2) サービスの停止 (Host Data Collector)

`controlservice` コマンドを使って、Host Data Collector のサービスを停止します。

事前に完了しておく操作

- ・ Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

Host Data Collector のサービスを停止するには :

1. 次のコマンドを実行します。

Windows の場合 :

```
<Host Data Collector のインストールフォルダ>%HDC%Base%bin  
%controlservice.exe stop
```

Solaris または Linux の場合 :

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/bin/  
controlservice.sh stop
```

関連項目

- 12.2.1 Host Data Collector の常駐プロセス
- (1) サービスの起動 (Host Data Collector)
- (3) サービスの稼働状態の確認 (Host Data Collector)

(3) サービスの稼働状態の確認 (Host Data Collector)

controlservice コマンドを使って、Host Data Collector のサービスの稼働状態を確認します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

Host Data Collector のサービスの稼働状態を確認するには :

1. 次のコマンドを実行します。

Windows の場合 :

```
<Host Data Collector のインストールフォルダ>%HDC%Base%bin  
%controlservice.exe state
```

Solaris または Linux の場合 :

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/bin/  
controlservice.sh state
```

関連項目

- 12.2.1 Host Data Collector の常駐プロセス
- (1) サービスの起動 (Host Data Collector)
- (2) サービスの停止 (Host Data Collector)

12.2.2 Host Data Collector のファイアウォールへの例外登録 (Windows)

Host Data Collector の運用開始後に Windows ファイアウォールを有効にした場合や、Host Data Collector で使用するポートを変更した場合は、手でファイアウォールの例外登録をする必要があります。

(1) Host Data Collector のサービスの例外登録 (非 SSL 通信用)

firewall_setup コマンドを使って、Host Data Collector のサービスで使用する非 SSL 通信用のポートをファイアウォールに例外登録します。

Host Data Collector の hdcbase.properties ファイルにある次のプロパティに設定されているポートが例外登録されます。例外登録名はすべて Host Data Collector Base です。

- `hdc.common.rmi.registryPort` プロパティ (デフォルト値 : 22098/tcp)
- `hdc.common.rmi.serverPort` プロパティ (デフォルト値 : 22099/tcp)
- `hdc.common.http.serverPort` プロパティ (デフォルト値 : 22100/tcp)

事前に完了しておく操作

- Administrator 権限でのログイン

コマンドの形式

```
firewall_setup.bat {add|del}
```

コマンドの格納先

< *Host Data Collector* のインストールフォルダ > %HDC%Base%bin

オプション

add

ファイアウォールの例外登録を行う場合に指定します。

del

ファイアウォールの例外登録の設定を解除する場合に指定します。

関連項目

- (2) [Host Data Collector のサービスの例外登録 \(SSL 通信用\)](#)
- [C.2.4 hdc.common.rmi.registryPort](#)
- [C.2.5 hdc.common.rmi.serverPort](#)
- [C.2.6 hdc.common.http.serverPort](#)

(2) Host Data Collector のサービスの例外登録 (SSL 通信用)

`netsh` コマンドを使って、Host Data Collector のサービスで使用する SSL 通信用のポートをファイアウォールに例外登録します。

事前に完了しておく操作

- Administrator 権限でのログイン

事前に確認しておく情報

- `hdc.common.rmi.ssl.registryPort` プロパティに設定されているポート番号 (デフォルト値 : 22104/tcp)
- `hdc.common.rmi.ssl.serverPort` プロパティに設定されているポート番号 (デフォルト値 : 22105/tcp)
- `hdc.common.https.serverPort` プロパティに設定されているポート番号 (デフォルト値 : 22106/tcp)

Host Data Collector のサービスを例外登録するには :

1. ポートごとに次のコマンドを実行します。

Windows Server 2003 または Windows Server 2003 R2 の場合

```
netsh firewall add portopening protocol=TCP port=<ポート番号>
name="Host Data Collector Base" mode=ENABLE
```

Windows Server 2008, Windows Server 2008 R2 または Windows Server 2012 の場合

```
netsh advfirewall firewall add rule name="Host Data Collector Base"
dir=in action=allow localport=<ポート番号> protocol=TCP
```

2. 設定を有効にするために、Host Data Collector のサービスを再起動します。



参考 次のコマンドを実行すると登録内容を確認できます。

Windows Server 2003 または Windows Server 2003 R2 の場合

```
netsh firewall show portopening
```

Windows Server 2008, Windows Server 2008 R2 または Windows Server 2012 の場合

```
netsh advfirewall firewall show rule name=all
```

関連項目

- (1) サービスの起動 (Host Data Collector)
- (2) サービスの停止 (Host Data Collector)
- (1) Host Data Collector のサービスの例外登録 (非 SSL 通信用)
- C.2.7 hdc.common.rmi.ssl.registryPort
- C.2.8 hdc.common.rmi.ssl.serverPort
- C.2.9 hdc.common.https.serverPort

12.2.3 Host Data Collector で使用する Java の実行環境の変更

Host Data Collector の運用開始後に使用する Java の実行環境を変更する場合は、使用する Java の実行環境のインストールパスを Host Data Collector の `javaconfig.properties` ファイルの `javapathlocation` プロパティに設定します。

事前に完了しておく操作

- Host Data Collector が前提とする Java の実行環境の確認
詳細は、「ソフトウェア添付資料」を参照してください。
- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

事前に確認しておく情報

- 使用する Java の実行環境のインストールパス

Host Data Collector で使用する Java の実行環境を変更するには：

1. Host Data Collector のサービスを停止します。
2. Host Data Collector の `javaconfig.properties` ファイルの `javapathlocation` プロパティに、使用する Java の実行環境のインストールパスを絶対パスで設定します。
3. Host Data Collector のサービスを起動します。

Host Data Collector で使用する Java の実行環境が、指定したパスの `bin` ディレクトリにある Java の実行環境に変更されます。

関連項目

- (1) サービスの起動 (Host Data Collector)
- (2) サービスの停止 (Host Data Collector)
- C.4.1 javapathlocation

12.2.4 Host Data Collector マシンに複数の IP アドレスがある場合の設定

Host Data Collector マシンが複数の IP アドレスを持っている場合、Host Data Collector の `hdcbase.properties` ファイルの `hdc.service.rmi.registryIPAddress` プロパティに、Device Manager サーバとの通信で使用する IP アドレスを指定してください。

関連項目

- C.2.10 `hdc.service.rmi.registryIPAddress`

12.2.5 Host Data Collector のバージョンの確認

`hdc_info` コマンドを使って、Host Data Collector のバージョンを確認します。

Host Data Collector のバージョンを確認するには：

1. 次のコマンドを実行します。

Windows の場合：

```
< Host Data Collector のインストールフォルダ > %HDC%Base%bin%hdc_info.exe
```

Solaris または Linux の場合：

```
< Host Data Collector のインストールディレクトリ > /HDC/Base/bin/hdc_info.sh
```

12.3 Host Data Collector のアンインストール

Host Data Collector でホストを管理する必要がなくなったら、Host Data Collector をアンインストールします。Host Data Collector をアンインストールすると、プロパティファイルやログファイルなどが削除されます。

12.3.1 Host Data Collector のアンインストール (Windows)

Host Data Collector でホストを管理する必要がなくなったら、Windows の [プログラムと機能] メニューから、Host Data Collector をアンインストールします。

事前に完了しておく操作

- Administrator 権限でのログイン

Host Data Collector をアンインストールするには：

1. [コントロールパネル] - [プログラムと機能] - [Host Data Collector] を選択し、[アンインストール] ボタンをクリックします。
2. アンインストールウィザードの指示に従って操作します。

アンインストールが完了すると [アンインストール完了] 画面が表示されます。



参考 システムドライブ以外にインストールされているバージョン 7.4.1 以前の Host Data Collector をアンインストールすると、Host Data Collector がインストールされていたドライブ直下に temp フォルダが残ることがあります。不要な場合は削除してください。

12.3.2 Host Data Collector のアンインストール（Solaris または Linux）

Host Data Collector でホストを管理する必要がなくなったら、`.unsetup.sh` コマンドを実行して、Host Data Collector をアンインストールします。

事前に完了しておく操作

- root でのログイン

Host Data Collector をアンインストールするには：

1. 次のコマンドを実行します
 < Host Data Collector のインストールディレクトリ >/HDC/Base/bin/.unsetup.sh
2. 表示されたメッセージに従って操作します。

アンインストールが完了すると、次のメッセージが表示されます。

```
Host Data Collector removal completed successfully.
```

トラブルシューティング

この章では、Device Manager および Tiered Storage Manager の運用中に発生した問題の解決策やログファイルの参照方法について説明します。

- 13.1 一般的な問題と解決策
- 13.2 トラブル発生時に採取が必要な保守情報
- 13.3 監査ログの確認

13.1 一般的な問題と解決策

ここでは、Device Manager や Tiered Storage Manager の環境設定や運用中に発生するおそれがあるトラブルの事例とその要因、対処を説明します。

13.1.1 管理サーバで発生したトラブルへの対処方法（Device Manager）

Device Manager に起因するトラブルが発生した場合の対処方法を示します。

(1) Device Manager の GUI にログインできない

Device Manager の GUI にログインできない場合、ユーザーアカウントのロックを解除してください。

要因

ユーザーアカウントがロックされているおそれがあります。

対処方法

User Management の Admin 権限を持っていないユーザーの場合：

User Management の Admin 権限を持つユーザーに、アカウントのロックを解除するよう依頼してください。

User Management の Admin 権限を持っているユーザーの場合：

User Management の Admin 権限を持つほかのユーザーにアカウントのロックを解除するよう依頼するか、`hcmdsunlockaccount` コマンドを実行して自分自身のアカウントのロックを解除してください。

関連項目

- ・ 3.2.4 アカウントロックの解除

(2) Hitachi Command Suite 共通コンポーネントまたは Device Manager サーバのサービスを起動できない

Hitachi Command Suite 共通コンポーネントまたは Device Manager サーバのサービスを起動できない場合、デスクトップヒープの領域を変更してください。

要因

デスクトップヒープが不足しているおそれがあります。

対処方法

レジストリーを編集して、デスクトップヒープの領域を変更してください。

関連項目

- ・ デスクトップヒープの領域の変更方法：Microsoft 社の Web サイト

(3) 管理サーバの起動後や Hitachi Command Suite 製品のサービスの起動後に Device Manager サーバにアクセスできない

管理サーバの起動後や Hitachi Command Suite 製品のサービスの起動後に、GUI や CLI から Device Manager サーバにアクセスできない場合、Device Manager のデータベースへの接続リトライ回数とリトライ間隔を延長してください。

要因

Device Manager トレースログファイルに KAIC03100-E が出力されている場合、Device Manager サーバからデータベースへの接続処理がタイムアウトしています。

対処方法

Device Manager のデータベースへの接続リトライ回数とリトライ間隔を延長します。

Device Manager サーバの `database.properties` ファイルにある、次のプロパティの値を変更してください。

- `dbm.startingCheck.retryCount`
- `dbm.startingCheck.retryPeriod`

関連項目

- [A.1.1 Device Manager サーバのプロパティの変更](#)
- [A.3.2 dbm.startingCheck.retryCount](#)
- [A.3.3 dbm.startingCheck.retryPeriod](#)

(4) Hitachi Virtual File Platform の SNMP トラップを受信できない

Hitachi Virtual File Platform の SNMP トラップを受信できない場合、管理サーバの IP アドレスやホスト名などの設定内容を、Hitachi File Services Manager と Device Manager 間で一致させてください。

要因

次の設定が Hitachi File Services Manager と Device Manager 間で一致していないおそれがあります。

- 管理サーバの IP アドレスまたはホスト名
- 管理サーバのポート番号
- ファイルサーバ名（ノードの IP アドレスまたはホスト名）

対処方法

次の設定を見直してください。

- SNMP トラップの通知先に、管理サーバの IP アドレスおよびホスト名が登録されているか
- SNMP トラップの通知先に、Device Manager の SNMP トラップ受信ポートが登録されているか
- Device Manager に登録されたファイルサーバ名が、Hitachi File Services Manager に登録されているノードの IP アドレスおよびホスト名と一致しているか
ファイルサーバ名の形式：<ノードのホスト名>@<ノードの IP アドレス>

(5) ストレージシステムの構成変更やリフレッシュがエラー終了した

ミッドレンジストレージに対する構成変更やリフレッシュがエラー終了し、KAIC05310-E メッセージまたは KAIC06299-E メッセージが出力された場合、ミッドレンジストレージと Device Manager サーバ間の通信タイムアウト時間を延長してください。

要因

Device Manager サーバからストレージシステムへの接続処理がタイムアウトしているおそれがあります。

対処方法

次の手順でストレージシステムと Device Manager サーバ間の通信タイムアウト時間を延長してください。

なお、通信タイムアウト時間は、次の値のうち、小さい値が適用されます。

- 管理サーバの OS に設定された値
 - lanconf.inf ファイルの ConnectionTimeout プロパティの値
1. lanconf.inf ファイルの ConnectionTimeout プロパティの値を運用環境に合わせて変更します。

指定できる値の範囲は 1~60 (秒) です。

Windows の場合

```
<Device Manager サーバのインストールフォルダ>\lib\HSNMAPI\lanconf.inf
```

Solaris または Linux の場合

```
<Device Manager サーバのインストールディレクトリ>/lib/HSNMAPI/  
lanconf.inf
```

2. Hitachi Command Suite 製品のサービスを再起動します。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

13.1.2 管理サーバで発生したトラブルへの対処方法 (Tiered Storage Manager)

Tiered Storage Manager に起因するトラブルが発生した場合の対処方法を示します。

ここでは、管理クライアントからの操作は、Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI からの操作だけを示します。

(1) Tiered Storage Manager サーバの起動に失敗した

Tiered Storage Manager サーバの起動に失敗した場合、要因に対応する対処を実施してください。

要因

- Device Manager, または Hitachi Command Suite 共通コンポーネントが起動していません。
- 実行ユーザーに管理者権限がありません。
- プロパティファイルが誤っています。

対処方法

Device Manager または Hitachi Command Suite 共通コンポーネントが起動していない場合：

Device Manager および Hitachi Command Suite 共通コンポーネントを起動してください。

実行ユーザーに管理者権限がない場合：

OS の管理者権限を持つユーザーで実行し直してください。

プロパティファイルが誤っている場合：

コマンドログまたはメッセージログを参考に、プロパティファイルを修正してください。

(2) Tiered Storage Manager サーバが停止しない

Tiered Storage Manager サーバが停止しない場合、要因に対応する対処を実施してください。

要因

- ・ 停止処理中にサーバに異常が発生しました。
- ・ 実行ユーザーに管理者権限がありません。

対処方法

停止処理中にサーバに異常が発生した場合：

Tiered Storage Manager サーバを停止してから約 10 分経過したあと、さらに停止処理に必要な時間が経過しても停止しないときは、次のコマンドを実行してください。

Windows の場合：

```
< Tiered Storage Manager サーバのインストールフォルダ > %bin%htsmsserver  
forcestop
```

Solaris または Linux の場合：

```
< Tiered Storage Manager サーバのインストールディレクトリ > /bin/htsmsserver  
forcestop
```

実行ユーザーに管理者権限がない場合：

OS の管理者権限を持つユーザーで実行し直してください。

(3) Tiered Storage Manager サーバで異常終了したりクラスタ環境でフェールオーバーが発生したりする

強制終了や予期しないエラーで Tiered Storage Manager サーバが異常終了したり、クラスタ環境でフェールオーバーが発生したりする場合は、データベースの情報とストレージシステムの状態の整合性を回復してください。

要因

データベースの情報とストレージシステムの状態に不整合が発生しました。

対処方法

次の手順でデータベースの情報とストレージシステムの状態の整合性を回復してください。

1. Hitachi Command Suite 製品のサービスを再起動したあと、Device Manager ですべてのストレージシステムをリフレッシュしてください。
2. Tiered Storage Manager サーバの異常終了時に、マイグレーションタスクの作成またはキャンセル操作をしていた場合は、操作し直してください。キャンセル操作でエラーが発生した場合、ストレージシステムをリフレッシュしてください。

3. 実行中のマイグレーションタスクが失敗した場合は、再度ストレージシステムをリフレッシュしてください。そのあと、タスクの状態に応じて、次のとおり対処してください。

タスクの状態が「データ消去失敗」の場合：

マイグレーションは完了し、移動元と移動先の LDEV 番号は付け替わっています。移動先 LDEV 番号が付いた移動元ボリュームの状態を確認して、ボリュームの状態に応じて対処してください。データ消去に失敗した場合、移動先 LDEV 番号が付いた移動元には元のデータが残っています。

- 移動先 LDEV 番号が付いたボリュームが閉塞状態になっているときは、Storage Navigator を利用して該当するボリュームをフォーマットしてください。
- 移動先 LDEV 番号が付いたボリュームが閉塞状態になっていないときは、該当するボリュームのデータが消去されないで残っているおそれがあります。

データを消去する必要があるときには、フォーマットするか、次の手順でデータを消去してください。LDEV 10:01 を 20:01 にマイグレーションしたとして説明します（移動元ボリュームはマイグレーションによって LDEV 番号が 20:01 に付け替わっています）。

1. 20:01 に LUN パスを設定し、ホストに割り当てます。
2. 割り当てたホストから”0” データをボリュームサイズ分書き込み、20:01 のデータを消去します。
3. 20:01 の LUN パスを解除します。

タスクの状態が「マイグレーション失敗」の場合：

エラーの要因によっては、ストレージシステムでマイグレーションが完了していても、Tiered Storage Manager や Device Manager ではマイグレーション失敗終了として扱われているおそれがあります。このとき、次の手順で対処してください。

- a. Device Manager ですべてのストレージシステムをリフレッシュし、Tiered Storage Manager と Device Manager の管理情報を最新状態に更新します。
予約されたまま残っているボリュームがあれば、リフレッシュ中に解除されます。
- b. マイグレーション失敗終了状態になっているマイグレーションタスクのボリューム情報を表示して、マイグレーション実行前か実行後かを確認します。
このとき、マイグレーション元のすべての LDEV について、パリティグループ名とストレージシステム名を確認してください。
- c. マイグレーションが実行されていない LDEV があつた場合、エラーになった要因を取り除いたあと、再度マイグレーションタスクを作成して、マイグレーションを実行します。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

(4) データベースに障害が発生し Tiered Storage Manager の操作ができない

データベースに障害が発生し、Tiered Storage Manager で操作できない場合、バックアップしておいたデータベースを復元してください。

要因

データベースに障害が発生したため、リポジトリにアクセスできません。

対処方法

バックアップしておいたデータベースを復元してください。

関連項目

- ・ 10.3 データベースの復元

13.1.3 ホストで発生したトラブルへの対処方法

Device Manager エージェントに起因するトラブルが発生した場合の対処方法を示します。

(1) HiScan コマンドを実行しても、Device Manager サーバにホスト情報を登録できない

HiScan コマンドを実行しても、エラーメッセージが出力されて Device Manager サーバにホスト情報を登録できない場合、要因に対応する対処を実施してください。

要因

KAIC22019-E のエラーメッセージが出力される場合：

次の要因が考えられます。

- ホストが認識している Device Manager の管理下のボリュームへの LUN パスが、断線などの理由によって無効になっているおそれがあります。
- 1つのホストで認識している Device Manager 管理下の LU が 100 個以上ある場合に発生することがあります。

KAIC22009-E, KAIC22014-E, または KAIC22048-E のエラーメッセージが出力される場合：

1つのホストで認識している Device Manager 管理下の LU が 100 個以上ある場合に発生することがあります。

対処方法

ホストが認識している Device Manager の管理下のボリュームへの LUN パスが無効になっている場合：

無効になっている LUN パスを復旧させるか、無効になっている LUN パスを認識しないように OS の設定を変更してください。

1つのホストで認識している Device Manager 管理下の LU が 100 個以上ある場合：

ホストで 100 個以上の LU を管理する場合に必要な設定をしてください。

関連項目

- ・ 11.2.5 ホストで 100 個以上の LU を管理する場合に必要な設定

(2) 通信エラーが発生して、ほかの Hitachi Command Suite 製品の処理が停止した

通信エラーが発生して、ほかの Hitachi Command Suite 製品の処理が停止した場合、数分待つてから、処理を再度実行してください。

要因

Device Manager エージェントのインストールが終了した直後や、Device Manager エージェントのサービスが起動された直後に、ほかの Hitachi Command Suite 製品から Device Manager エージェントにアクセスしたおそれがあります。

対処方法

数分待つてから、処理を再度実行してください。

(3) [プログラムと機能] 画面に [HBase Agent] が 2 つ表示されている

Windows 環境で、Device Manager エージェントまたは Dynamic Link Manager がインストールされているマシンの [プログラムと機能] 画面に [HBase Agent] が 2 つ表示されている場合は、hbsa_util コマンドを実行して、Device Manager エージェントのレジストリーとファイルを削除してください。

関連項目

- 11.3.2 Device Manager エージェントのレジストリーとファイルの削除 (hbsa_util コマンド)

(4) [プログラムと機能] 画面に [HBase Agent] が残っている

Windows 環境で、Device Manager エージェントと Dynamic Link Manager の両方をアンインストールしたにも関わらず、[プログラムと機能] 画面に [HBase Agent] が残っている場合は、hbsa_util コマンドを実行して、Device Manager エージェントのレジストリーとファイルを削除してください。

関連項目

- 11.3.2 Device Manager エージェントのレジストリーとファイルの削除 (hbsa_util コマンド)

(5) JavaVM が異常終了する

Windows (x64 および IPF) の環境で、JavaVM が異常終了する場合は、Server.cmd ファイルを編集してください。

要因

動作している Device Manager エージェントに対して、Device Manager と連携するほかのプログラムが頻繁にアクセスしたおそれがあります。

対処方法

次の手順に従って、Server.cmd ファイルを編集してください。

- 次の場所に格納されている Server.cmd ファイルをテキストエディターで開きます。
< Device Manager エージェントのインストールフォルダ > %agent%\bin\Server.cmd
- Java 起動オプションに -Djava.compiler=NONE を追加します。

Server.cmd ファイルの編集例を次に示します。

```
.java -Dalet.msclang -Djava.compiler=NONE %1 %2 -classpath
"C:\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar\agent4.jar;C:\Program Files
\HITACHI\HDVM\HBaseAgent\agent\jar\jdom.jar;C:\Program Files\HITACHI
\HDVM\HBaseAgent\agent\jar\xerces.jar;C:\Program Files\HITACHI\HDVM\HBaseAgent
\agent
\jar\servlet.jar;C:\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar
\log4j-1.2.3.jar" com.Hitachi.soft.HiCommand.DVM.agent4.as.
export.Server %*
exit /b %ERRORLEVEL%
```

(6) ホストで OutOfMemory エラーが発生し、しばらく時間が経過しても応答がない

ホストリフレッシュなどを実行したときにホストで OutOfMemory エラーが発生し、しばらく時間が経過しても応答がない場合、要因に対応する対処を実施してください。

要因

- 1つのホストで認識している Device Manager 管理下の LU が 100 個以上ある場合に発生することがあります。
- HiScan コマンドの -t オプションで指定したログファイル、または HiScan.msg ファイルに次のエラーメッセージが出力されている場合は、Device Manager サーバの負荷が高くなっているため、発生することがあります。

```
<html><head><title>400 Bad request</title>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
</head><body>
<h1>400 Bad request</h1>
<p><strong>ServiceConnection#0: java.lang.OutOfMemoryError</strong>
</body></html>
```

HiScan.msg ファイルの格納場所は次のとおりです。

Windows の場合

< Device Manager エージェントのインストールフォルダ >¥bin¥logs¥

Solaris, Linux, または HP-UX の場合

/opt/HDVM/HBaseAgent/bin/logs/

AIX の場合

/usr/HDVM/HBaseAgent/bin/logs/

対処方法

- 1つのホストで認識している Device Manager 管理下の LU が 100 個以上ある場合、ホストで 100 個以上の LU を管理する場合に必要な設定をしてください。
- Device Manager サーバの負荷が高くなっている場合、次のとおり対処してください。
 - Device Manager サーバのメモリーヒープサイズを変更してください。
 - 複数ホストで HiScan コマンドの実行時間が重なっているときは、hdvmagt_setting コマンドを使用して実行周期を設定してください。

関連項目

- [1.3.3 メモリーヒープサイズの変更 \(Device Manager サーバ\)](#)
- [11.2.5 ホストで 100 個以上の LU を管理する場合に必要な設定](#)
- [11.3.4 Device Manager サーバの情報, HiScan コマンドの実行周期および RAID Manager または P9000 RAID Manager の情報の設定 \(hdvmagt_setting コマンド\)](#)
- [11.3.5 Device Manager サーバへのホスト情報の手動通知 \(HiScan コマンド\)](#)

(7) Device Manager の GUI にファイルシステム名が表示されない

Solaris 環境で Device Manager の GUI にファイルシステム名が表示されない場合、バージョン 4.0 以降の VxVM を使用してください。

要因

バージョン 4.0 より前の VxVM を使用している場合、デバイス名をエンクロージャに基づいて命名したとき、Device Manager エージェントは、ファイルシステムと LUN との対応を Device Manager サーバに通知しません。

対処方法

ファイルシステムと LUN との対応を確認したい場合は、バージョン 4.0 以降の VxVM を使用してください。

(8) ストレージシステムの構成変更が Device Manager サーバに反映されない

ストレージシステムの構成変更が Device Manager サーバに反映されない場合、hldutil コマンドや HiScan コマンドを実行して、最新の情報を Device Manager サーバに反映してください。

要因

LU の登録や削除など、ストレージシステムの構成を変更した直後は、OS が変更を認識しないことがあります。このとき、Device Manager エージェントは古い情報を Device Manager サーバに通知します。

対処方法

1. hldutil コマンドを実行して最新の情報を確認する。
2. ホストの OS を再起動する。
3. HiScan コマンドを実行する。

関連項目

- 11.3.5 Device Manager サーバへのホスト情報の手動通知 (HiScan コマンド)
- 11.3.6 デバイス情報の取得 (hldutil コマンド)

(9) Device Manager エージェントの機能が使用できない

RAID Manager と P9000 RAID Manager を同一ディレクトリにインストールしている環境で Device Manager エージェントの機能が使用できない場合は、RAID Manager と P9000 RAID Manager をインストールし直してください。

要因

RAID Manager と P9000 RAID Manager を同一ディレクトリにインストールしている場合、RAID Manager をインストールしたあとに、P9000 RAID Manager をインストールした環境で Device Manager エージェントを使用すると発生することがあります。

対処方法

RAID Manager と P9000 RAID Manager をインストールし直してください。

RAID Manager と P9000 RAID Manager をアンインストールしたあと、P9000 RAID Manager を先にインストールしてから、RAID Manager をインストールしてください。

関連項目

- RAID Manager のアンインストール手順およびインストール手順 : RAID Manager のマニュアル
- P9000 RAID Manager のアンインストール手順およびインストール手順 : P9000 RAID Manager のマニュアル

(10) 対処不要なエラー

次のエラーが発生した場合、対処は不要です。

- 複数の HiScan コマンドが同時に実行されたときに、イベントログまたはシステムログに次のメッセージが出力された。
 - [HORCM_005] Could not create endpoint for remote connection.
 - [HORCM_007] Illegal parameter values in HORCM configuration file.
- ペア状態の S-VOL をマウントしているときに、Windows のイベントログにイベント ID : 51 またはイベント ID : 57 の次のメッセージが出力された。
 - イベント ID : 51
ページング操作中にデバイス ¥Device¥Harddisknn¥DRn 上でエラーが検出されました。
(n は数字を示します)
 - イベント ID : 57
データをトランザクション ログにフラッシュできませんでした。障害が発生する可能性があります。
- Device Manager エージェントの HiScan コマンドの実行周期が、実行系ノードと待機系ノードで同じ時間に設定されているときに、AIX の待機系ノードのエラーログ上に SC_DISK_ERR2 (Device Busy) や HSDRV_RSV_CONFLICT が出力された。
この現象は、共有ディスクに対する I/O 負荷が高くなった場合にまれに発生することがあります。
共有ディスクは実行系ノードが正常にディスク予約 (Reserve) をしているため、システムには問題ありません。共有ディスクの情報は実行系ノードで動作している Device Manager エージェントから取得されているので、Device Manager の運用についても問題ありません。
- Linux 環境で、rpm -v コマンドを実行したらエラーになった。

13.2 トラブル発生時に採取が必要な保守情報

障害要因を特定できない場合や、障害を回復できない場合には、保守情報を用意して、障害対応窓口に連絡してください。

トラブル発生時には、原因特定のために次の情報が必要です。

- 障害に伴うシステムの状況
- 障害の発生日時
- 障害の発生場面
- 管理サーバやホストなどのネットワーク構成
- 管理サーバやホストなどの OS
- 障害が発生したマシンの保守情報
 - 管理サーバの保守情報
 - Host Data Collector マシンの保守情報
Host Data Collector を使用していて、かつ Host Data Collector が管理サーバとは別のマシンにインストールされている場合は、Host Data Collector がインストールされたマシンの保守情報も取得する必要があります。管理サーバに Host Data Collector がインストールされている場合は、hcmdsgetlogs コマンドを実行すると、Host Data Collector の保守情報も自動的に取得されます。
 - ホストの保守情報
- Java VM のスレッドダンプ

次に示す問題が発生した場合、原因を見つけるために HBase Storage Mgmt Common Service と HCS Device Manager Web Service のスレッドダンプが必要になります。

- GUI を起動しても Device Manager ログインウィンドウが表示されない
- Device Manager へのログイン後、Device Manager メインウィンドウが表示されない
- Tuning Manager から Device Manager サーバを起動しても Device Manager メインウィンドウが表示されない



重要 システム構成や障害の発生場面によっては、障害解析のために、ほかのプログラムのログファイルも必要になります。

- [モビリティ] タブや [分析] タブで性能情報を参照している場合
PFM - Manager, Tuning Manager サーバ, PFM - Base および Tuning Manager - Agent for RAID のログファイルが必要です。
- [レプリケーション] タブで性能情報を参照している場合
Replication Manager サーバ, PFM - Manager, Tuning Manager サーバ, PFM - Base および Tuning Manager - Agent for RAID のログファイルが必要です。
- Device Manager で仮想化サーバを管理している場合
仮想化ソフトウェア, vMA および VMware vCenter Server のログファイルが必要です。
- Device Manager で Hitachi Virtual File Platform を管理している場合
Hitachi File Services Manager のログファイルが必要です。
- Device Manager と Compute Systems Manager 間で業務サーバ (ホスト) のマシン情報を同期している場合
Compute Systems Manager のログファイルが必要です。

関連項目

- Device Manager と Tiered Storage Manager 以外のログファイルの取得方法 : 各プログラムのマニュアル

13.2.1 管理サーバの保守情報の取得 (hcmdsgetlogs コマンド)

管理サーバの保守情報を取得するには、hcmdsgetlogs コマンドを実行します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

コマンドの形式

Windows :

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > \bin  
hcmdsgetlogs /dir < フォルダ名 > [/types < Hitachi Command Suite 製品の名称 >  
[ < Hitachi Command Suite 製品の名称 > ...]] [/arc < アーカイブファイル名 >] [/logtypes < ログファイル種別 > [ < ログファイル種別 > ...]]
```

Solaris または Linux :

```
< Hitachi Command Suite 共通コンポーネントのインストールディレクトリ > /bin/  
hcmdsgetlogs -dir < ディレクトリ名 > [-types < Hitachi Command Suite 製品の名称 > [ < Hitachi Command Suite 製品の名称 > ...]] [-arc < アーカイブファイル名 >] [-logtypes < ログファイル種別 > [ < ログファイル種別 > ...]]
```



注意 hcmdsgetlogs コマンドは、2 つ以上同時に実行しないでください。

オプション

dir

採取した保守情報を格納するローカルディスク上のディレクトリを絶対パスで指定します。あらかじめディレクトリを作成している場合は、ディレクトリを空にしてください。

指定できるパスの最大長は 41 バイトです。パスには一部の特殊文字を除いた ASCII 印字可能文字コードを指定できます。指定できない特殊文字を示します。

¥ / : , ; * ? " < > | \$ % & ' `

ただし、パスの区切り文字として、Windows の場合は円記号 (¥)、コロン (:) およびスラント (/)、Solaris または Linux の場合はスラント (/) を使用できます。パスの末尾にはパスの区切り文字を指定しないでください。

Windows の場合、パス中に空白を指定するときは、パスを引用符 (") で囲んで指定してください。Solaris または Linux の場合は、パス中に空白は指定できません。

types

障害などの理由によって、特定の Hitachi Command Suite 製品の保守情報しか取得できない場合に、次の表に従って取得対象の製品の名称を指定します。複数の製品名を指定する場合は、空白文字で区切ってください。

表 13-1 保守情報を取得する場合の type オプションの指定値

製品	指定値
Device Manager	DeviceManager
Tiered Storage Manager	TieredStorageManager
Replication Manager	ReplicationManager
その他の製品	それぞれの製品のマニュアルを参照

このオプションを指定する場合、logtypes オプションでログファイルの種別に log を含めて指定してください。

このオプションを省略した場合、同一管理サーバにインストールされている全 Hitachi Command Suite 製品の保守情報が取得されます。

arc

作成されるアーカイブファイルの名前を指定します。このオプションを省略した場合、ファイル名は「HiCommand_log」になります。

ファイル名には一部の特殊文字を除いた ASCII 印字可能文字コードを指定できます。指定できない特殊文字を次に示します。Solaris または Linux の場合、空白は指定できません。

¥ / : , ; * ? " < > | \$ % & ' `

logtypes

障害などの理由によって、特定のログファイルしか取得できない場合に、取得対象のログファイルの種別を指定します。

log : .jar ファイルと .hdb.jar ファイルだけを取得する場合に指定します。

db : .db.jar ファイルだけを取得する場合に指定します。

csv : .csv.jar ファイルだけを取得する場合に指定します。

複数の種別を指定する場合は、空白文字で区切ってください。

このオプションを省略した場合、すべてのログファイルが取得されます。

このコマンドを実行すると、メッセージ KAPM05318-I または KAPM05319-E が出力されます。また、保守情報（ログファイルとデータベースファイル）が取得され、dir オプションで指定したディレクトリの下に 4 つのアーカイブファイル（.jar, .hdb.jar, .db.jar および.csv.jar）が作成されます。



参考 メッセージ KAPM05318-I または KAPM05319-E が出力されない場合、dir オプションで指定するディレクトリに十分な空き容量がないため、hcmsggetlogs コマンドが途中で終了しています。dir オプションで指定するディレクトリに十分な空き容量を確保したあとで、再度 hcmsggetlogs コマンドを実行してください。

13.2.2 Host Data Collector マシンの保守情報の取得（hdc_gettras コマンド）

Host Data Collector マシンの保守情報を取得するには、hdc_gettras コマンドを実行します。

事前に完了しておく操作

- Administrator 権限（Windows の場合）または root（Solaris または Linux の場合）でのログイン

コマンドの形式

Windows の場合：

```
< Host Data Collector のインストールフォルダ > %HDC%\Base\bin\hdc_gettras.bat -o  
< フォルダ名 > [-f]
```

Solaris または Linux の場合：

```
< Host Data Collector のインストールディレクトリ > /HDC/Base/bin/hdc_gettras.sh  
-o < ディレクトリ名 > [-f]
```

- ○
保守情報の出力先を、絶対パスまたはカレントディレクトリからの相対パスで指定します。パスには一部の特殊文字を除いた ASCII 印字可能文字コードを指定できます。指定できない特殊文字を示します。
¥ / : , ; * ? " < > | \$ % & ' ` ^
ただし、パスの区切り文字として、Windows の場合は円記号（¥）、コロン（:）およびスラント（/）、Solaris または Linux の場合はスラント（/）を使用できます。
- f
○ オプションで指定したディレクトリがすでに存在する場合に、強制的に上書きするときに指定します。

次の場所に保守情報が出力されます。

Windows の場合：

```
< o オプションに指定したフォルダ > %hdcResult
```

Solaris または Linux の場合：

```
< o オプションに指定したディレクトリ > /hdcResult
```

13.2.3 Host Data Collector 管理対象ホストの保守情報の取得（hdc_target_gettras コマンド）

Host Data Collector の管理対象の通常ホストまたは仮想マシンで保守情報を取得するには、hdc_target_gettras コマンドを実行します。

事前に完了しておく操作

- ホストへのファイルのコピー

Host Data Collector がインストールされたマシンから、管理対象のホストに次のファイルをコピーします。

Windows の場合：

```
<Host Data Collector のインストールフォルダ>%Base%bin  
%hdc_target_gettras.bat
```

UNIX の場合：

```
<Host Data Collector のインストールディレクトリ>/Base/bin/  
hdc_target_gettras.sh
```

- Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

コマンドの形式

Windows の場合：

```
hdc_target_gettras.bat -o <フォルダ名> [-f]
```

UNIX の場合：

```
hdc_target_gettras.sh -o <ディレクトリ名> [-f]
```

- o
保守情報の出力先を、絶対パスまたはカレントディレクトリからの相対パスで指定します。パスには一部の特殊文字を除いた ASCII 印字可能文字コードを指定できます。指定できない特殊文字を示します。
¥ / : , ; * ? " < > | \$ % & ' ` ^
ただし、パスの区切り文字として、Windows の場合は円記号 (¥)，コロン (:) およびスラント (/)，UNIX の場合はスラント (/) を使用できます。
- f
o オプションで指定したディレクトリがすでに存在する場合に、強制的に上書きするときに指定します。

次の場所に保守情報が出力されます。

Windows の場合：

```
<o オプションに指定したフォルダ>%target_hdcResult
```

UNIX の場合：

```
<o オプションに指定したディレクトリ>/target_hdcResult
```

13.2.4 Device Manager エージェントの保守情報の取得 (TIC コマンド)

Device Manager エージェントの管理対象の通常ホストまたは仮想マシンで保守情報を取得するには、TIC コマンドを実行します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

コマンドの形式

Windows の場合

```
TIC.bat [-outdir <フォルダ名> [-f] [-d [<アドオンモジュール名>]]]
```

Solaris または HP-UX の場合

```
TIC.sh [-outdir <ディレクトリ名> [-f] [-d [<アドオンモジュール名>]]]
```

AIX または Linux の場合

```
TIC.sh [-outdir <ディレクトリ名> [-f]]
```

コマンドの格納先

Windows の場合

```
<Device Manager エージェントのインストールフォルダ>%bin
```

Solaris, Linux, または HP-UX の場合

```
/opt/HDVM/HBaseAgent/bin
```

AIX の場合

```
/usr/HDVM/HBaseAgent/bin
```

オプション

-outdir

保守情報の出力先を、絶対パスまたはカレントディレクトリからの相対パスで指定します。

パスの区切り文字を除き、次の文字は指定できません。

```
¥ / : , ; * ? " < > | $ % & ` ` ^
```

このオプションを省略した場合、TIC コマンドの格納先が指定されたものとして動作します。

-f

-outdir オプションで指定したディレクトリがすでに存在する場合、強制的に上書きするときに指定します。

-d

特定のアドオンモジュールの障害情報を取得対象から外したい場合に、略称を次の形式で指定します。

hglm : Global Link Manager エージェント (Windows, Solaris または HP-UX の場合だけ)

hrpmap : Replication Manager Application エージェント (Windows の場合だけ)

複数指定する場合はコンマ (,) で区切ります。アドオンモジュール名を省略した場合は、

Global Link Manager エージェントと **Replication Manager Application** エージェントの障害情報は取得されません。

次の場所に保守情報が出力されます。

Windows の場合 :

```
<-outdir オプションに指定したフォルダ>%resultDir
```

UNIX の場合 :

```
<-outdir オプションに指定したディレクトリ>/resultDir
```

13.2.5 HBase Storage Mgmt Common Service のスレッドダンプ取得 (Windows)

HBase Storage Mgmt Common Service のスレッドダンプを取得するには、dump という名前のファイルを作成したあと、HBase Storage Mgmt Common Service を再起動します。

HBase Storage Mgmt Common Service のスレッドダンプを取得するには :

1. < *Hitachi Command Suite* 共通コンポーネントのインストールフォルダ > %CC%\web
¥containers¥HiCommand に、dump という名前のファイルを作成します。
2. Windows の [サービス] ウィンドウにアクセスします。
3. HBase Storage Mgmt Common Service を停止します。
4. [サービス] ウィンドウから、HBase Storage Mgmt Common Service を開始します。

Hitachi Command Suite に同梱された JDK を使用している場合は javacorexxx .xxxx .txt ファイルが、Oracle JDK を使用している場合は HiCommand.log ファイルが、次のフォルダへ出力されます。

< *Hitachi Command Suite* 共通コンポーネントのインストールフォルダ > %CC%\web
¥containers¥HiCommand

Oracle JDK を使用している場合、出力されるたびに HiCommand.log ファイルは上書きされます。出力後は別名で保存しておくことをお勧めします。

13.2.6 HCS Device Manager Web Service のスレッドダンプ取得 (Windows)

HCS Device Manager Web Service のスレッドダンプを取得するには、dump という名前のファイルを作成したあと、HCS Device Manager Web Service を再起動します。

HCS Device Manager Web Service のスレッドダンプを取得するには :

1. < *Hitachi Command Suite* 共通コンポーネントのインストールフォルダ > %CC%\web
¥containers¥DeviceManagerWebService に、dump という名前のファイルを作成します。
2. Windows の [サービス] ウィンドウにアクセスします。
3. HCS Device Manager Web Service を停止します。
4. [サービス] ウィンドウから、HCS Device Manager Web Service を開始します。

Hitachi Command Suite に同梱された JDK を使用している場合は javacorexxx .xxxx .txt ファイルが、Oracle JDK を使用している場合は DeviceManagerWebService.log ファイルが、次のフォルダへ出力されます。

< *Hitachi Command Suite* 共通コンポーネントのインストールフォルダ > %CC%\web
¥containers¥DeviceManagerWebService

Oracle JDK を使用している場合、出力されるたびに DeviceManagerWebService.log ファイルは上書きされます。出力後は別名で保存しておくことをお勧めします。

13.2.7 HBase Storage Mgmt Common Service のスレッドダンプ取得 (Solaris または Linux)

HBase Storage Mgmt Common Service のスレッドダンプを取得するには、kill コマンドを実行したあと、Hitachi Command Suite 製品のサービスを再起動します。

事前に完了しておく操作

- Hitachi Command Suite に同梱された JDK への切り替え (Oracle JDK を使用している場合)

HBase Storage Mgmt Common Service のスレッドダンプを取得するには :

1. 次のコマンドを実行します。

```
# kill -3 <PID >
```

<PID >は、<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/CC/web/containers/HiCommand/logs/cjstdout.log ファイルに書き込まれている Process ID です。

cjstdout.log ファイルには複数の Process ID が書き込まれていますが、最後に書き込まれている Process ID を指定してください。

2. Hitachi Command Suite 製品のサービスを再起動します。

javacorexxx .xxxx .txt ファイルが次のディレクトリへ出力されます。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>/CC/web/containers/HiCommand
```

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

13.2.8 HCS Device Manager Web Service のスレッドダンプ取得 (Solaris または Linux)

HCS Device Manager Web Service のスレッドダンプを取得するには、kill コマンドを実行したあと、Hitachi Command Suite 製品のサービスを再起動します。

事前に完了しておく操作

- Hitachi Command Suite に同梱された JDK への切り替え (Oracle JDK を使用している場合)

HCS Device Manager Web Service のスレッドダンプを取得するには：

1. 次のコマンドを実行します。

```
# kill -3 <PID >
```

<PID >は、<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/CC/web/containers/DeviceManagerWebService/logs/cjstdout.log ファイルに書き込まれている Process ID です。

cjstdout.log ファイルには複数の Process ID が書き込まれていますが、最後に書き込まれている Process ID を指定してください。

2. Hitachi Command Suite 製品のサービスを再起動します。

javacorexxx .xxxx .txt ファイルが次のディレクトリへ出力されます。

```
<Hitachi Command Suite 共通コンポーネントのインストールディレクトリ>/CC/web/containers/DeviceManagerWebService
```

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

13.3 監査ログの確認

- Windows の場合：

Windows のイベントログに次の形式で出力されます。

```
<プログラム名> [<プロセス ID >]: <メッセージ部>
```

- Solaris または Linux の場合 :

syslog ファイルに次の形式で出力されます。

```
<日付・時刻> <サーバ名 (または, IP アドレス)> <プログラム名> [<プロセス ID >]: <メッセージ部>
```

<メッセージ部>の出力形式と内容を説明します。



重要 <メッセージ部>には、半角で 953 文字まで表示されます。

メッセージ部の出力形式

```
<統一識別子>, <統一仕様リビジョン番号>, <通番>, <メッセージ ID >, <日付・時刻>, <検出エンティティ>, <検出場所>, <監査事象の種別>, <監査事象の結果>, <監査事象の結果サブジェクト識別情報>, <ハードウェア識別情報>, <発生場所情報>, <ロケーション識別情報>, <FQDN >, <冗長化識別情報>, <エージェント情報>, <リクエスト送信元ホスト>, <リクエスト送信元ポート番号>, <リクエスト送信先ホスト>, <リクエスト送信先ポート番号>, <一括操作識別子>, <ログ種別情報>, <アプリケーション識別情報>, <予約領域>, <メッセージテキスト>
```

表 13-2 メッセージ部出力される情報

項目※1	内容
統一識別子	「CELFSS」固定
統一仕様リビジョン番号	「1.1」固定
通番	監査ログのメッセージの通番
メッセージ ID	メッセージ ID 詳細については、「6.2.1」を参照してください。
日付・時刻	メッセージが出力された日付と時刻 「yyyy-mm-ddThh:mm:ss <タイムゾーン>」の形式で出力されます。
検出エンティティ	コンポーネント名やプロセス名
検出場所	ホスト名
監査事象の種別	事象の種別
監査事象の結果	事象の結果
監査事象の結果サブジェクト識別情報	事象に応じた、アカウント ID、プロセス ID または IP アドレス
ハードウェア識別情報	ハードウェアの型名や製番
発生場所情報	ハードウェアのコンポーネントの識別情報
ロケーション識別情報	ロケーション識別情報
FQDN	完全修飾ドメイン名
冗長化識別情報	冗長化識別情報
エージェント情報	エージェント情報
リクエスト送信元ホスト	リクエストの送信元のホスト名
リクエスト送信元ポート番号	リクエストの送信元のポート番号
リクエスト送信先ホスト	リクエストの送信先のホスト名
リクエスト送信先ポート番号	リクエストの送信先のポート番号

項目※1	内容
一括操作識別子※2	プログラム内で操作の通番
ログ種別情報	「BasicLog」または「DetailLog」
アプリケーション識別情報	プログラムの識別情報
予約領域	出力されません。予約領域です。
メッセージテキスト	監査事象に応じた内容 表示できない文字は、アスタリスク (*) に置き換えて出力されます。詳細については、「13.3.1」を参照してください。

注※1

監査事象によっては、出力されない項目もあります。

注※2

Tiered Storage Manager の監査ログのうち、メッセージテキストの中に配列の情報が出力される場合は、最初に配列の開始を示す基本ログが出力され、次に配列の要素ごとに詳細ログが1行ずつ出力され、末尾に配列の終了を示す基本ログが出力されます。

出力例

```

...,i,BasicLog,,, ".....NumSD=n, Start SDs"
...,i,DetailLog,,, "SD[1]=(domainId-1,domainName-1)"
...,i,DetailLog,,, "SD[2]=(domainId-2,domainName-2)"
.....
...,i,DetailLog,,, "SD[n]=(domainId-n,domainName-n)"
...,i,BasicLog,,, "End SDs"

```

ただし、配列の長さが1の場合は、詳細ログには出力しないで、基本ログに出力します。

監査事象「ログイン」で出力されるメッセージ部の例

```

CELFSS,1.1,0,KAPM01124-I,2006-05-15T14:08:23.1+09:00,HBase-SSO,management-
host,Authentication,Success,uid=system,,,,,,,,,BasicLog,,, "The login process
has completed properly."

```

Device Manager サーバの監査事象「リクエスト受理」で出力されるメッセージ部の例

```

CELFSS,1.1,10,KAIC51000-I,2006-03-17T12:45:00.0+09:00,DvM_Srv, TestServer,
ConfigurationAccess,Success,uid=system,,,,,from=12.228.23.124,,,,,BasicLog,DvM
_GUI,, "123456789 ModPort<SA info='R500-14000'><Port info='0,0,,1,'></Port></
SA>"

```

13.3.1 監査ログのメッセージテキスト

監査ログ中のメッセージテキストは、監査事象ごとに形式が異なります。ここでは、監査事象ごとにメッセージテキストの形式を説明します。メッセージテキストの形式で[]で囲んだ項目は、出力されないことがあります。

(1) Hitachi Command Suite 共通コンポーネントの処理として出力される場合

発生した監査事象の内容が、文字列で出力されます。

メッセージテキストの詳細については、マニュアル「Hitachi Command Suite Software メッセージガイド」を参照してください。次にメッセージテキストの例を示します。

ログイン時の例

```

"The login process has completed properly."

```

(2) Device Manager サーバの処理として出力される場合

構成変更、情報取得などのサーバの処理に関するリクエスト受理時、およびレスポンス送信時の情報が出力されます。メッセージテキストの形式とその内容を説明します。

リクエスト受理時（正常時）

```
<ユニーク ID > <詳細メッセージ>
```

レスポンス送信時（正常時）

```
<ユニーク ID >[ <ステータス>][ <リクエスト操作開始ユニーク ID >]
```

リクエスト受理時またはレスポンス送信時（異常時）

```
<ユニーク ID > <エラーメッセージ ID >
```

表 13-3 Device Manager サーバリクエスト受理時またはレスポンス送信時に出力される情報

項目	内容
ユニーク ID	リクエストごとに一意な ID です。レスポンス送信時は、対応するリクエストのユニーク ID です。SVP 経由の処理の場合、この ID は SVP 側の監査ログにも出力されます。
詳細メッセージ	リクエストの詳細な内容です。詳細については、「13.3.2」を参照してください。
ステータス	リクエストと操作が非同期である場合、ポーリングの結果を示す文字列です。出力される文字列を次に示します。 <ul style="list-style-type: none">COMPLETED：操作成功PROCESSING：操作中FAILED：操作失敗
リクエスト操作開始ユニーク ID	リクエストと操作が非同期である場合、リクエストとその操作に対するポーリングの結果を対応付ける一意な ID です。この ID は、リクエスト受理時の詳細メッセージに、GetRequestStatus（コマンド：Get、ターゲット：RequestStatus）の RequestStatus エレメントの属性として出力されるメッセージ ID と対応しています。詳細メッセージについては、「13.3.2」を参照してください。
エラーメッセージ ID	エラーメッセージ ID です。メッセージ ID の詳細については、マニュアル「Hitachi Command Suite Software メッセージガイド」を参照してください。

次に、リクエスト受理時（正常時）、および、レスポンス送信時（異常時）に出力されるメッセージテキストの例を示します。

リクエスト受理時（正常時）の例

```
"123456789 AddLUN<SA info='D700-75010421'><Path info=',,0,4,15,0,'><LDEV info='D700-75010421-31,, '/><LDEV info='D700-75010421-34,, '/></Path><Path info=',,1,1,15,0,31' /><Path info=',,16,6,15,0,31' /><Path info=',,0,4,15,1,35' /></SA>"
```

レスポンス送信時（異常時）の例

```
"123456789 KAIC01014-E"
```

(3) 関連製品の起動情報として出力される場合

関連製品の起動（ラUNCH）に関するリクエスト受理時、およびレスポンス送信時の情報が出力されます。メッセージテキストの形式とその内容を説明します。

リクエスト受理時（正常時）

<ユニーク ID > [<ラUNCHセッション ID >] [<ラUNCH先識別子 >]

レスポンス送信時（正常時）

<ユニーク ID > [<ラUNCHセッション ID >]

リクエスト受理時またはレスポンス送信時（異常時）

<ユニーク ID > [<ラUNCHセッション ID >] <エラーメッセージ ID >

表 13-4 ラUNCHリクエスト受理時またはレスポンス送信時に出力される情報

項目	内容
ユニーク ID	リクエストごとに一意な ID です。レスポンス送信時は、対応するリクエストのユニーク ID です。SVP 経由の処理の場合、この ID は SVP 側の監査ログにも出力されます。
ラUNCHセッション ID	形式: "lsessionID=..." ラUNCH用セッション ID が出力されます。ある特定のアプリケーションをラUNCHする場合に、GUI と Device Manager サーバの間で複数回のリクエスト・レスポンスのやり取りが行われるときに出力されます。ラUNCHセッション ID が出力されるアプリケーションについては、「表 13-5」を参照してください。ラUNCH対象のストレージシステムが、Virtual Storage Platform, Universal Storage Platform V/VM または HUS VM のときは出力されません。
ラUNCH先識別子	形式: "loid=..." ラUNCH対象を識別する情報が出力されます。初回のリクエスト受理時のときだけに出力されます。ラUNCH識別子の内容は、起動するアプリケーションによって異なります。詳細については、「表 13-5」を参照してください。
エラーメッセージ ID	エラーメッセージ ID です。 メッセージ ID の詳細については、マニュアル「Hitachi Command Suite Software メッセージガイド」を参照してください。

次の表に、ラUNCHセッション ID の有無とラUNCH先識別子の内容を、ラUNCHされるアプリケーションごとに示します。

表 13-5 ラUNCHセッション ID の有無とラUNCH識別子の内容

アプリケーション種別	ストレージシステム	セッション ID の有無	ラUNCH識別子の内容
Element Manager	Virtual Storage Platform	無	ラUNCH対象のストレージシステムを特定する情報です。内容は、StorageArray エレメントのエレメント識別子※1と同様です。詳細については、「表 13-17」の StorageArray エレメントの属性値出力順を参照してください。※2
	Universal Storage Platform V/VM	無	
	Hitachi USP	有	
	SANRISE9900V	有	
	HUS VM	無	
	HUS100	無	
	Hitachi AMS2000	無	
	Hitachi SMS	無	
	Hitachi AMS/WMS	無	
	SANRISE9500V	無	
Protection Manager	--	無	ラUNCH対象ホストマシンを特定する情報です。内容は、Host エレメントのエレメント識別子※1と同様です。詳細について

アプリケーション種別	ストレージシステム	セッションIDの有無	ラウンチ識別子の内容
			では、「表 13-17」の Host エレメントの属性値出力順を参照してください。

注※1

エレメント識別子は、エレメントを一意に特定するための属性値です。

注※2

Element Manager から SANRISE9900V を操作した場合だけ、IP アドレスが表示されます (出力例: loid=10.208.110.110)。

次に、ラウンチリクエスト受理時 (正常時)、およびレスポンス送信時 (正常時) に出力されるメッセージテキストの例を示します。

リクエスト受理時 (正常時) の例

```
"123456789 lsessionID=a7e770671b8 loid=R500-14000"
```

レスポンス送信時 (正常時) の例

```
"123456789 lsessionID=a7e770671b8"
```

(4) Device Manager サーバ (CIM 経由) の処理として出力される場合

CIM サービスメソッドのリクエスト受理時、またはレスポンス送信時の情報が出力されます。メッセージテキストの形式とその内容を説明します。

リクエスト受理時 (正常時)

```
<ユニーク ID> <メソッド名> <入力パラメーター> <オブジェクトパス>
```

レスポンス送信時 (正常時および異常時)

```
<ユニーク ID> <リターンコード> <出力パラメーター>
```

レスポンス送信時 (非同期処理によってジョブが生成された場合)

```
<ユニーク ID> return=4096 <オブジェクトパス>
```



注意 非同期処理によってジョブが生成された場合の完了通知は、監査ログに出力されません。

表 13-6 Device Manager サーバ (CIM 経由) リクエスト受理時またはレスポンス送信時に出力される情報

項目	内容
ユニーク ID	リクエストごとに一意な ID です。レスポンス送信時は、対応するリクエストのユニーク ID です。SVP 経由の処理の場合、この ID は SVP 側の監査ログにも出力されます。
メソッド名	リクエストされたメソッド名です。
入力パラメーター	形式: "inParams={...}" リクエストされたメソッドに引き渡された入力パラメーターが出力されます。
オブジェクトパス	形式: "objectPath=..."

項目	内容
	リクエストされたメソッドに引き渡されたオブジェクトパスが出力されます。
リターンコード	形式:"return=..." リクエストされたメソッドの実行結果としてリターンコードが出力されます。
出力パラメーター	形式:"outParams={...}" リクエストされたメソッドの実行結果として、引き渡されたパラメーターの内容が出力されます。

次に、Device Manager サーバ (CIM 経由) のリクエスト受理時 (正常時)、およびレスポンス送信時 (正常時) に出力されるメッセージテキストの例を示します。

リクエスト受理時 (正常時) の例

```
"123456789 GetSupportedSizeRange inParams={ElementType=3,Goal=//192.168.0.1/
root/smis/current:HITACHI_StorageSetting.InstanceID='RAID5'} objectPath=/root/
smis/current:HITACHI_StoragePool.InstanceID='AMS500.75010421'"
```

レスポンス送信時 (正常時) の例

```
"123456789 return=0
outParams={MinimumVolumeSize=1024,MaximumVolumeSize=248139692,VolumeSizeDivisor=
1024}"
```

(5) Tiered Storage Manager の処理として出力される場合

Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI で操作した場合に出力される監査ログのメッセージテキストの出力形式および出力される情報を次に示します。

```
<メッセージ本文> <操作種別 (OP)>, <操作対象 (Res)>[, <失敗理由 (RC)>]
[, <ストレージドメイン情報 (SD)>][, <ストレージシステム情報 (SS)>]
[, <マイグレーショングループ情報 (MG)>]
[, <タスク完了後の移動先マイグレーショングループ情報 (MG_moveTo)>]
[, <ストレージ階層情報 (ST)>][, <プール情報 (PO)>][, <ボリューム情報 (VL)>]
[, <ボリュームペア (VP)>][, <空き容量情報 (FS)>][, <外部接続設定情報 (EM)>]
[, <バスグループ情報 (PG)>][, <エミュレーションタイプ情報 (EM)>][, <タスク情報 (TK)>]
[, <監査事象ごとのオプション (opt)>]
```

注

<失敗理由 (RC)>以降の項目は、出力される場合と、出力されない場合があります。

表 13-7 監査ログのメッセージテキストに出力される項目 (メッセージ本文、操作種別および操作対象)

項目	内容	出力形式
メッセージ本文	事象を説明するメッセージ	メッセージ本文が出力されます。出力されるメッセージについては、「表 13-9」を参照してください。
操作種別 (OP)	Tiered Storage Manager サーバに対する操作要求の種類 1. 操作 ID (OpId) 2. 操作名 (OpName)	OP= (OpId,OpName) OpId, OpName については、「表 13-10」を参照してください。
操作対象 (Res)	操作の対象となるリソース (資源) の種類 1. リソース ID (ResId) 2. リソース名 (ResName)	Res= (ResId,ResName) ResId, ResName については、「表 13-11」を参照してください。

表 13-8 監査ログのメッセージテキストに出力される項目（追加情報）

項目	内容	出力形式
失敗理由 (RC)	失敗事象の場合に、その理由・原因を示すエラーコード	RC=KATSppmmm-z メッセージ内容については、マニュアル「Hitachi Command Suite Software メッセージガイド」を参照してください。
ストレージドメイン情報 (SD)	1 個の場合 1. ストレージドメイン ID (id) 2. ストレージドメイン名 (name)	SD= (id,name)
	複数の場合 1. 要素数 (n) 2. ストレージドメイン ID (id) 3. ストレージドメイン名 (name)	NumSD=n, Start SDs SD[1]= (id-1,name-1) ... SD[n]= (id-n,name-n) End SDs
	ストレージドメイン情報の数 (n)	NumSD=n
ストレージシステム情報 (SS)	1. ストレージシステム名 (name) 2. 論理 DKC 番号 (ldkc)	SS= (,name,ldkc)
	ストレージシステム情報の数 (n)	NumSS=n
マイグレーショングループ情報 (MG)	1 個の場合 1. マイグレーショングループ ID (id) 2. マイグレーショングループ名 (name)	MG= (id,name)
	複数の場合 1. 要素数 (n) 2. マイグレーショングループ ID (id) 3. マイグレーショングループ名 (name)	NumMG=n, Start MGs MG[1]= (id-1,name-1) ... MG[n]= (id-n,name-n) End MGs
	マイグレーショングループ情報の数 (n)	NumMG=n
タスク完了後の移動先マイグレーショングループ情報 (MG_moveTo)	1. マイグレーショングループ ID (id) 2. マイグレーショングループ名 (name)	MG_moveTo= (id,name)
ストレージ階層情報 (ST)	1 個の場合 1. ストレージ階層 ID (id) 2. ストレージ階層名 (name)	ST= (id,name)
	複数の場合 1. 要素数 (n) 2. ストレージ階層 ID (id) 3. ストレージ階層名 (name)	NumST=n, Start STs ST[1]= (id-1,name-1) ... ST[n]= (id-n,name-n) End STs
	ストレージ階層の数 (n)	NumST=n
プール情報 (PO)	ストレージドメイン ID (id)	SD= (id,)
	プール数 (n)	NumPO=n
ボリューム情報 (VL)	1 個の場合 1. コントローラー論理デバイス番号 (devnum) 2. LU または LDEV のオブジェクト ID (id)	VL= (devnum,id)
	複数の場合 1. 要素数 (n)	NumVL=n, Start VLs VL[1]= (devnum-1,id-1) ...

項目	内容	出力形式
	2. コントローラー論理デバイス番号 (devnum) 3. LUまたはLDEVのオブジェクトID (id)	VL[n]= (devnum-n,id-n) End VLs
	ボリュームの数 (n)	NumVL=n
ボリュームペア (VP)	1 個の場合 1. 移動元ボリュームのコントローラー論理デバイス番号 (sdevnum) 2. 移動元 LDEV のオブジェクト ID (sid) 3. 移動先ボリュームのコントローラー論理デバイス番号 (tdevnum) 4. 移動先 LDEV のオブジェクト ID (tid)	VP= (sdevnum,sid,tdevnum,tid)
	複数の場合 1. 要素数 (n) 2. 移動元ボリュームのコントローラー論理デバイス番号 (sdevnum) 3. 移動元 LDEV のオブジェクト ID (sid) 4. 移動先ボリュームのコントローラー論理デバイス番号 (tdevnum) 5. 移動先 LDEV のオブジェクト ID (tid)	NumVP=n, Start VPs VP[1]= (sdevnum-1,sid-1,tdevnum-1,tid-1) ... VP[n]= (sdevnum-n,sid-n,tdevnum-n,tid-n) End VPs
	ボリュームペア数 (n)	NumVP=n
空き容量情報 (FS)	1 個の場合 1. パリティグループ名 (agname) 2. 空き容量番号 (fnum)	FS= (agname,fnum)
	複数の場合 空き容量情報数 (n)	NumFS=n
外部接続設定情報 (EM)	外部接続設定情報数 (n)	NumEM=n
パスグループ情報 (PG)	1 個の場合 パスグループ ID (id)	PG= (id)
	複数の場合 パスグループ情報数 (n)	NumPG=n
エミュレーションタイプ情報 (EM)	エミュレーションタイプ情報数 (n)	NumEM=n
タスク情報 (TK)	マイグレーションタスクの場合 1. タスク ID (id) 2. タスク種別 (type) =0 3. データ消去の有無 (erase) Y : データ消去あり N : データ消去なし	TK= (id,0,erase)
	ロッキングタスクの場合 1. タスク ID (id) 2. タスク種別 (type) =2 3. ロック状態 (mode) ReadOnly : Read Only Protect : Protect 4. ロック期限 (days)	TK= (id,2,mode,days)
	アンロッキングタスクの場合 1. タスク ID (id) 2. タスク種別 (type) =3	TK= (id,3)

項目	内容	出力形式
	シュレディングタスクの場合 1. タスク ID (id) 2. タスク種別 (type) =4 3. シュレディング方式 (method) 0 : Zero Once 1 : DOD	TK= (id,4,method)
	タスク情報が複数ある場合 1. タスクの数 2. タスク ID (id) 3. タスク種別 (type) 0 : マイグレーションタスク 2 : ロッキングタスク 3 : アンロッキングタスク 4 : シュレディングタスク	NumTK=n, Start TKs TK[1]= (id-1,type-1) ... TK[n]= (id-n,type-n) End TKs
監査事象ごとのオプション (opt)	CancelTask の場合 強制キャンセルかどうか (emergency) Y : emergency 指定あり N : emergency 指定なし	opt= (emergency)
	Add Volume の場合 移動許可 (moveFromMigrationGroup) Y : 移動許可する N : 移動許可しない	opt= (moveFromMigrationGroup)
	Change Task の場合 1.変更後のタスクの状態 (status) 0x01020600: タスク実行中 0x02030000: 取消 0x02040000: 中止 0x02050000: 即時中止 2.強制的に変更するかどうか (emergency) Y : emergency 指定あり N : emergency 指定なし	opt= (status,emergency)

表 13-9 監査ログに出力されるメッセージ

メッセージ ID	メッセージ (アプリケーション固有情報)	内容
KATS90000-I	The operation requested by the client has completed.	監査ログが複数行にわたる場合、ログの先頭行であることを示します。 Tiered Storage Manager が管理する資源へのアクセスに成功したことによって、Configuration Access 種別の監査事象が発生しました。
KATS90001-W	The operation requested by the client has failed.	監査ログが複数行にわたる場合、ログの先頭行であることを示します。 Tiered Storage Manager が管理する資源へのアクセスに失敗したことによって、Configuration Access 種別の監査事象が発生しました。
KATS90010-W	The user does not have permission for the operation.	実行権限がないため、Tiered Storage Manager が管理する資源へのアクセスに失敗したことによって、Access Control 種別の監査事象が発生しました。

メッセージ ID	メッセージ (アプリケーション固有情報)	内容
KATS90020-I	KATS90000-I メッセージの継続行が出力されます。	監査ログが複数行にわたる場合、ログの継続行であることを示します。 Tiered Storage Manager が管理する資源へのアクセスに成功したことによって、 Configuration Access 種別の監査事象が発生しました。
KATS90021-W	KATS90001-W メッセージの継続行が出力されます。	監査ログが複数行にわたる場合、ログの継続行であることを示します。 Tiered Storage Manager が管理する資源へのアクセスに失敗したことによって、 Configuration Access 種別の監査事象が発生しました。
KATS90030-I	KATS90000-I メッセージの最終行が出力されます。	監査ログが複数行にわたる場合、ログの最終行であることを示します。 Tiered Storage Manager が管理する資源へのアクセスに成功したことによって、 Configuration Access 種別の監査事象が発生しました。
KATS90031-W	KATS90001-W メッセージの最終行が出力されます。	監査ログが複数行にわたる場合、ログの最終行であることを示します。 Tiered Storage Manager が管理する資源へのアクセスに失敗したことによって、 Configuration Access 種別の監査事象が発生しました。

表 13-10 監査ログに出力される操作種別 (OP) の意味

OpId	OpName	意味
10	Get	情報取得
11	Get_summary	要約情報取得
12	Get_num	情報の個数だけ取得
20	Create	作成
30	Delete	削除
40	Modify	更新
50	Add	追加
60	Remove	除去
70	Change	(状態の) 変更
80	Execute	実行
90	Refresh	リフレッシュ
100	Cancel	キャンセル
110	Stop	中止
120	Choose	選択
130	Check	チェック

表 13-11 監査ログに出力される操作対象 (Res) の意味

ResId	ResName	正式名称	意味
10	LC	License	ライセンス情報
20	SD	Storage Domain	ストレージドメイン

ResId	ResName	正式名称	意味
21	RS	Refresh Status	ストレージのリフレッシュ状態
30	MG	Migration Group	マイグレーショングループ
40	ST	Storage Tier	ストレージ階層
50	MP	Migration Plan	マイグレーションプラン
60	SS	Subsystem	ストレージシステム
70	TK	Task	タスク
80	VL	Volume	ボリューム
90	VP	Volume Pair	ボリュームペア
100	VR	Volume Range	ボリュームの検索範囲
110	LOG	Logger Info	ログ出力に関する情報
120	PO	Pool	プール
130	KS	Key Store	キーストアファイル情報
140	FS	Free Space	空き容量
150	FSR	Free Space Range	空き容量の検索範囲
160	EXM	External Mapping	外部接続設定情報
170	PG	Path Group	パスグループ
180	EM	Emulation	エミュレーション

監査ログの出力例を次に示します。

```
TSMgr[00000974]:CELFSS,1.1,1,KATS90000-I,2006-11-09T19:58:45.4+09:00,TSM_Srv,
Hostname1,ConfigurationAccess,Success,uid=user01,,,,,,,,,,,,BasicLog,,, "The
operation requested by the client has completed. OP=(30,Delete), Res=(20,SD),
SD=(DMLhc2idzx,Domain-A) "
```

13.3.2 Device Manager サーバリクエスト受理詳細メッセージ

Device Manager サーバが、リクエストを受理したときに出力される詳細メッセージの出力形式を次に示します。[]で囲んだ項目は、出力されないことがあります。

```
<コマンド><ターゲット>[ <オプション>][ <パラメーター>]
```

詳細メッセージに出力される情報を次の表に示します。

表 13-12 詳細メッセージに出力される情報

項目	内容
コマンド	リソースに対する操作（追加、削除、変更、参照など）を表す文字列（3文字）です。出力される文字列の意味については、「(1)」を参照してください。
ターゲット	操作内容を特定する情報です。出力されるターゲットとその内容については、「(2)」を参照してください。
オプション	操作内容を特定する情報です。オプションが指定されたときだけ出力されます。出力されるオプションの意味については、「(3)」を参照してください。複数のオプションが指定された場合、セミコロン (;) で区切って出力されません。
パラメーター	操作内容、対象リソースを特定する情報です。リクエストで指定されたときだけ出力されます。タグ形式で出力されます。出力されるパラメーターについては「(4)」を参照してください。

出力される情報について項目ごとに以降で説明します。

(1) 詳細メッセージに出力されるコマンド

詳細メッセージに出力されるコマンドを次の表に示します。

表 13-13 詳細メッセージに出力されるコマンド

出力文字列	正式名	操作
Add	Add	追加
Del	Delete	削除
Get	Get	取得
Imp	Import	インポート
Ivk	Invoke	SMI-S enabled ストレージシステムに対する操作全般
Mod	Modify	変更
Set	Set	設定

(2) 詳細メッセージに出力されるターゲット

詳細メッセージに出力されるターゲットの内容を次の表に示します。

表 13-14 詳細メッセージに出力されるターゲット

出力文字列	正式名	操作内容
Alerts	Alerts	アラート情報の参照・削除
ArrGrp	ArrayGroup	パリティグループの構成変更
ArrRsrv	ArrayReservation	ストレージシステム予約の設定・情報取得
CFForRep	ConfigFileForReplication	RAID Manager 用構成ファイルの作成
COMEFSP	CreateOrModifyElementFromStoragePool	SMI-S enabled ストレージシステムでのボリューム作成
ConfChange	ConfigurationChange	Device Manager サーバへの構成変更通知
DataRetentions	DataRetentions	データ保護情報の設定・取得
ExpPaths	ExposePaths	SMI-S enabled ストレージシステムでの LUN パス設定
ExtArrGrp	ExternalArrayGroup	外部パリティグループの設定
Host	Host	ホストの設定・参照
HostI	HostInfo	ホスト (エージェント) の構成変更・参照
HostRef	HostRefresh	HostInfo の更新
HostScan	HostScan	ホストの自動設定
HostVol	HostVolume	ホストのボリューム情報を Device Manager サーバへ通知
HSD	HostStorageDomain	ホストグループまたは iSCSI ターゲットの構成変更
ISCSIForHSD	ISCSINameForHostStorageDomain	iSCSI ターゲットに属する iSCSI ネームの変更
JrnlPool	JournalPool	プールの構成変更
LDEVForVolMig	LDEVForVolumeMigration	LDEV の VolumeMigration 属性の設定・情報取得
LGrp	LogicalGroup	論理グループの設定・参照
LU	LogicalUnit	論理ユニットの構成変更
LUFormat	LogicalUnitFormat	論理ユニット中の全 LDEV のフォーマット
LUN	LUN	LUN パスの構成変更
LUSE	LUSE	拡張 LDEV の構成変更

出力文字列	正式名	操作内容
Msgs	Messages	メッセージ
ObjLabel	ObjectLabel	LDEV のラベルの設定・削除
ObjName	ObjectName	Device Manager 中で使用するオブジェクトの名称設定
Port	Port	ポートの構成変更
PortCtrl	PortController	ポートコントローラーの構成変更
Rep	Replication	ペアの構成変更
RepCtrlPair	ReplicationControllerPair	ペアの構成情報参照および変更
ReqStatus	RequestStatus	コマンドの状態の返却
SA	StorageArray	ストレージシステムの追加, 削除, および情報取得
ShrnkPoolPrgrss	ShrinkingPoolProgress	DP プールの縮小の進捗取得
SmrtFldr	SmartFolder	論理グループの参照
SpareDrive	SpareDrive	スペアドライブの構成変更
SrvI	ServerInfo	Device Manager サーバの情報取得
SSOpt	StorageSystemOption	ストレージシステム単位のオプション設定
Subscrbr	Subscriber	イベントリスナーの追加・削除
TrngPlcy	TieringPolicy	階層ポリシーの構成変更
URLLink	URLLink	URL Link 情報の構成変更
User	User	ユーザーの設定・参照
VolFmtPrgrss	VolumeFormatProgress	ボリュームのノーマルフォーマットの進捗取得
VolMig	VolumeMigration	移動プランの設定・情報取得
VolShred	VolumeShredding	シュレディング機能の実行要求・情報取得
VRpu	VResourcePartitionUnit	仮想 ID を用いたデータ移行に使用しているリソースグループの構成変更
VVol	VirtualVolume	DP ボリュームの設定
WWN	WorldWideName	WWN の削除
WWNForHSD	WWNForHostStorageDomain	ホストグループに属する WWN の構成変更
WWNForLUN	WWNForLUN	LUN の WWN の構成変更
ZPRVol	ZeroPageReclaimVolume	ゼロページ破棄の進捗情報の取得

注

表中にない文字が出力されることもあります。

(3) 詳細メッセージに出力されるオプション

詳細メッセージに出力されるオプションの内容を次の表に示します。

表 13-15 詳細メッセージに出力されるオプション

出力文字列	操作内容
add	<ul style="list-style-type: none"> ターゲットが Replication の場合 コピーペアを追加する。 ターゲットが ReplicationControllerPair の場合 既存の RCU に論理パスを追加する。 ターゲットが VResourcePartitionUnit の場合 仮想 ID を用いたデータ移行用のリソースグループに, LDEV を追加する。

出力文字列	操作内容
all	<ul style="list-style-type: none"> ターゲットが StorageArray の場合 SMI-S enabled ストレージシステムも情報取得の対象にする。 ターゲットが URLLink の場合 SMI-S enabled ストレージシステムの管理サーバの URL も取得の対象にする。
auto	HDP プールの作成または拡張時に、PDEV を自動的に選択する。
assign	DP プールと DP ボリュームを関連づける。
bulk	容量または個数を指定して、複数のボリュームを作成する。
changerank	外部ボリュームの階層ランクを変更する。
datastore	仮想化サーバのデータストア容量の情報だけを更新する。
delete	<ul style="list-style-type: none"> ターゲットが Replication の場合 コピーペアを削除する。 ターゲットが ReplicationControllerPair の場合 既存の RCU から論理パスを削除する。 ターゲットが VResourcePartitionUnit の場合 仮想 ID を用いたデータ移行用のリソースグループから、LDEV を削除する。
dividebycap	容量を指定して、複数のボリュームを作成する。
dividebynum	個数を指定して、複数のボリュームを作成する。
encrypt	<ul style="list-style-type: none"> ターゲットが ArrayGroup の場合 暗号化されたパリティグループを作成する。 ターゲットが JournalPool の場合 暗号化された HDP プールを作成する。
exist	既存の仮想パリティグループに、DP ボリュームを作成する。
expand	DM-LU を拡張する。
force	<ul style="list-style-type: none"> ターゲットが LUSE の場合 ボリュームとホストグループ間またはボリュームと iSCSI ターゲット間のパスがすでに存在する論理ユニットで LUSE を作成する。 ターゲットが Virtual Volume の場合 DP プールと関連づけられている DP ボリュームに対し、関連づけの解除と DP ボリュームの削除を同時に実行する。 ターゲットが ExternalArrayGroup の場合 Device Manager に登録されていない外部ストレージシステムのボリューム（外部ボリューム）を設定する。
HORCMInfo	構成定義ファイル情報だけを更新する。
inband2	Thin Image のコピーペアを操作する。
iSCSINameDiscard	設定されている iSCSI ネームを破棄する。
lusekeep	LUSE を保持する。
merge	複数のホストに割り当てられた WWN または iSCSI ネームを 1 つのホストに統合する。
nameSync:false	<ul style="list-style-type: none"> ターゲットが JournalPool の場合 DP プール名をストレージシステムに反映しない。 ターゲットが ObjectLabel の場合 ボリュームラベルをストレージシステムに反映しない。
nameSync:true	<ul style="list-style-type: none"> ターゲットが JournalPool の場合 DP プール名をストレージシステムに反映する。 ターゲットが ObjectLabel の場合 ボリュームラベルをストレージシステムに反映する。
noformat	フォーマットをしないで、論理ユニットを作成する。
nolabelbefore	すでにラベルを設定している場合は、エラーとする。

出力文字列	操作内容
numOfLUs:< n >	作成するボリュームまたは DP ボリュームの数。< n >は作成するボリュームまたは DP ボリュームの数。
numOfPDEVs:< n >	HDP プールを構成する PDEV 数。
overwrite	<ul style="list-style-type: none"> ターゲットが Host の場合 同名のホストがあったとき、上書きする。 ターゲットが ObjectLabel の場合 すでに設定しているラベルを削除してから、ラベルを設定する。 ターゲットが VResourcePartitionUnit の場合 同じ仮想 ID 情報を持つ LDEV があったとき、上書きする。
private	プライベート論理グループの情報を取得する。
public	パブリック論理グループの情報を取得する。
quickformat	<ul style="list-style-type: none"> ターゲットが LogicalUnit の場合 論理ユニットを作成し、クイックフォーマットを実行する。 ターゲットが LogicalUnitFormat の場合 論理ユニットのクイックフォーマットを実行する。
refreshable	ロールとして Modify が設定されているストレージシステムだけをレスポンスで返却する。
remainMigraion	完了したプランのプランステータスを、ストレージシステム (SVP) に残す。
restore	副ボリュームのデータを、正ボリュームにコピーする。
resync	正ボリュームのデータを、副ボリュームにコピーする。
smi-s	<ul style="list-style-type: none"> ターゲットが ObjectName の場合 SMI-S enabled ストレージシステムの名称を対象にする。 ターゲットが StorageArray の場合 SMI-S enabled ストレージシステムだけを対象にする。 ターゲットが URLLink の場合 SMI-S enabled ストレージシステムの管理サーバの URL だけを対象にする。
split	ペアを分割する。
suspend	Universal Replicator で、3DC ペアを作成する。
takeOverWWN	指定した WWN がすでに登録されている WWN と重複したため、WWN を置き換えるか、既存の WWN を保持する。
unassign	DP プールと DP ボリュームの関連づけを解除する。
update	既存のペア構成を変更する。
validate:false	ペアの変更時に HORCM ファイルを検証しない。
validate:true	ペアの変更時に HORCM ファイルを検証する。
waitingViewSynchro	データベースの更新処理が終了したら、完了レスポンスを返却する。
ZeroPageReclaim	ゼロページを破棄する。

(4) 詳細メッセージに出力されるパラメーター

詳細メッセージに出力されるパラメーターの形式は次のとおりです。

パラメーター形式 1 (入れ子型)

```
<<エレメント> <属性>>[<パラメーター 1 ><パラメーター 2 >...<パラメーター n >]</エレメント>>
```

<エレメント>で示される開始・終了タグの間に、そのエレメントに依存するパラメーターが出力されます。該当するパラメーターがない場合は、出力されません。

パラメーター形式 2 (単独型)

```
<<エレメント> <属性>/>
```

詳細メッセージに出力されるパラメーターの情報を次の表に示します。

表 13-16 詳細メッセージに出力されるパラメーターの情報

項目	内容
エレメント	エレメント名を示す文字列です。出力されるエレメントとその内容については、「表 13-17」を参照してください。ただし、「表 13-17」にない文字が出力されることもあります。
属性	形式: "info='...'" エレメントに対して指定された属性値が出力されます。複数個出力される場合は、コンマ (,) で区切られます。属性値は、文字列または数値で出力されます。 対応する属性が未指定、または属性値に何も指定されていなかった場合、値は出力されません。すべての属性が未指定、または属性値に何も指定されていなかった場合、この項目は出力されません。 属性値にアポストロフィ (') またはコンマ (,) が含まれる場合、疑問符 (?) で置換されます。 属性値の出力順については、「表 13-17」を参照してください。

エレメントの内容と対応する属性値の出力順を次の表に示します。

表 13-17 エレメントの内容と対応する属性値の出力順

出力文字列	正式名と内容	属性値出力順 ^{*1}
Alert	Alert (Device Manager またはストレージシステムで発生したエラー情報)	アラート番号 number
Alerts	Alerts (Alert エレメントの集まり)	-
ArrGrp	ArrayGroup (ストレージシステムのパーティティグループに関する情報)	<モデル名 ^{*2} - シリアル番号 - シャーシ番号 - パリティグループ番号>, パリティグループが位置するシャーシ番号, パリティグループ番号, パリティグループの RAID レベル, CLPR 番号, エミュレーションモード, 外部パーティティグループのオプション情報, タイプ <model ^{*2} - serialnum - chassis - number>, chassis, number, raidType, clprNumber, emulation, volumeType, type
ArrRsrv	ArrayReservation (ストレージシステムのロック情報)	<モデル名 ^{*2} - シリアル番号>, <モデル名 ^{*2} - シリアル番号> <model ^{*2} - serialnum>, <model ^{*2} - serialnum>
ArrV	ArrayValue (Param で指定したパラメーターが配列型の場合に値を指定するエレメント)	ArrayValue で指定する値 value
ChangedItem	ChangedItem (Device Manager で変更されたデータに関する情報)	-

出力文字列	正式名と内容	属性値出力順 ^{※1}
ChangeI	ChangeInfo (ストレージシステム構成のバージョン情報)	LDEV 情報のバージョン, ポート情報のバージョン, LU 情報のバージョン, LUSE 情報のバージョン, LUN 情報のバージョン, ホストのモード情報のバージョン, DCR 情報のバージョン, CVS 情報のバージョン, SSID 情報のバージョン, CHA 情報のバージョン versionOfLDEV, versionOfPort, versionOfLogicalUnit, versionOfLUSE, versionOfLUNSecurity, versionOfHostMode, versionOfDCR, versionOfCVS, versionOfSSID, versionOfCHA
CIMInvk	CIMInvoker (CIM インスタンスを特定するエレメント)	メソッドを実行するサービスクラスのオブジェクトパス objectPath
CommandComplete	CommandComplete (Get Request Status コマンド発行時にクライアントが必要とする情報)	-
CommParas	CommParameters (ストレージシステムにアクセスする方法に関する情報)	-
Comp	Component (ストレージシステムの構成に関する情報)	-
Cond	Condition (Filter エレメントと同時に使用して, Get コマンドの結果を限定する)	LU の種別, LDEV のエレメント識別子, LDEV の種別, ホストの格納ステータス, Alert のソース, ホスト種別, ジャーナルボリュームの CLPR 番号, ホストのエレメント識別子, ジャーナルプール識別子, DP プールボリューム ID, 指定した WWN または iSCSI ネームからアクセスできるボリューム, LDEV のタイプ, 対象のストレージシステムのオブジェクト ID, MCU モデル, MCU のシリアル番号, HDT ボリューム ^{※5} の階層割り当てポリシー, 仮想ストレージシステムのファミリー, 仮想ストレージシステムのシリアル番号, 仮想ポート ID, 仮想ホストグループ ID, 仮想デバイス番号 ^{※4} , スナップショットグループの ID, スナップショットグループの名前 type, childID, volumeKind, host, source, hostType, clprNumber, assocID, poolFunction, dpPoolID, accessibleWWN, substance, targetArray, masterArrayType, masterSerialNumber, tierLevel, vArrayFamily, vSerialNumber, vPortID, vDomainID, vDevNum ^{※4} , snapshotGroupID, snapshotGroupName
ConfChange	ConfigurationChange (ストレージシステムの構成変更情報を Device Manager サーバへ通知)	ユーザー ID, 通知種別, シリアル番号, プロダクト名 ^{※2} , 発生日時, IP アドレス user, type, serialNumber, arrayType ^{※2} , date, ipAddress
ConfigChange	ConfigChange (Device Manager サーバで変更されたデータに関する情報)	-
ConfigF	ConfigFile	<ホスト ID - HORCM インスタンス番号> <hostID - instanceNumber>

出力文字列	正式名と内容	属性値出力順 ^{※1}
	(RAID Manager のコンフィグファイルに関する情報)	
DataRetention	DataRetention (データ保護情報)	-
DataRetentions	DataRetentions (LDEV のデータ保護情報)	-
DS	Datastore (データストアの情報)	-
ErrI	ErrorInfo (ストレージシステムで発生したエラーの情報)	ストレージシステムで発生したエラーのエラーコード, エラー発生日時 errorCode, date
ErrList	ErrorList (ErrorInfo エレメントを含むリスト)	ErrorInfo エレメントの個数 errorCount
ExternalDevice	ExternalDevice (外部ボリュームの情報)	-
ExtPathI	ExternalPathInfo (外部ストレージシステムのアクセス情報)	<モデル名 ^{※2} - シリアル番号 - シャーシ番号 - パリティグループ番号 - 外部ストレージシステムのポートの WWN - 外部 LU の LUN - External ポートのポート ID - 優先度> ^{※3} , 外部ストレージシステムのポートの WWN, 外部 LU の LUN, External ポートのポート ID, パスグループ ID <model ^{※2} - serialnum - chassis - number - externalWWN - externalLun - portID - priority> ^{※3} , externalWWN, externalLun, portID, pathGroupID
ExtS	ExternalStorage	-
F	File (ログファイル名に関する情報)	ログファイルの名前 name
Filt	Filter (Get コマンドの結果を限定する)	-
FreeLUN	FreeLUN (ホストグループまたは iSCSI ターゲットの LUN 空き情報)	-
FreeSpace	FreeSpace (ストレージシステムのパリティグループの空き容量に関する情報)	<モデル名 ^{※2} - シリアル番号 - シャーシ番号 - パリティグループ番号 - パリティグループ内のフリースペースのインデックス番号> <model ^{※2} - serialnum - chassis - number - fsControlIndex>
FSys	FileSystem (Device Manager エージェントから取得したファイルシステムの情報)	デバイスファイル名, マウントポイント, ファイルシステムのタイプ, ファイルシステムのサイズ, , ファイルシステムの使用率, , ファイルシステムの削除可否, ファイルシステムの拡張可否, , , , , , , , , deviceFileName, mountPoint, type, size, , percentUsed, , , deletable, expandable, , , , , , , ,

出力文字列	正式名と内容	属性値出力順 ^{※1}
FSys	FileSystem (ファイルサーバから取得したファイルシステムの情報)	,,, ファイルシステムのサイズ, ファイルシステムの使用量, ファイルシステムの使用率, ファイルシステムの空き容量, ファイルシステムの空き容量率, ,, ファイルシステムに関連する EVS 名, ファイルシステムの状態, ファイルシステムのラベル, マウントポイントの数, ファイルシステムが属している StoragePool のラベル, 最小リテンション期間, 最大リテンション期間, 自動コミット期間, デフォルトリテンション期間 ,,, size, usedSize, percentUsed, freeSize, percentFree, ,, evs, status, label, numberOfMountPoints, storagePool, minRetentionPeriod, maxRetentionPeriod, autoCommitPeriod, defaultRetentionPeriod
Host	Host (論理ボリュームが使用するホスト情報)	<ホスト ID>, ホスト名, ホストの IP アドレス, ホストの IPv6 用の IP アドレス, ホストのタイプ, 操作対象ホスト名, ホストの OS タイプ <hostID>, name, ipAddress, ipv6Address, hostType, targetName, osType
HostI	HostInfo (LU とホスト間のアクセスに関する情報)	<ホスト名 - ホスト SCSI バス番号 - ターゲット ID - ボリュームのホストでの LU 番号>, ホストに接続しているストレージシステムのタイプ (モデル) ^{※2} , ホストに接続しているストレージシステムのシリアル番号, HostInfo オブジェクトの表示名, ホストの IP アドレス, ホストの IPv6 用の IP アドレス, LUN のマウントポイント, ポート ID, ホストグループまたは iSCSI ターゲットのドメイン ID, 論理ユニットのデバイス番号 ^{※4} , HBA 上のポート WWN, マウントするファイルシステムのタイプ, ファイルシステム名, LUN の容量, LUN の使用率, iSCSI イニシエーターの iSCSI ネーム <name - osScsiBus - osScsiID - osLun>, arrayType ^{※2} , serialNumber, name, ipAddress, ipv6Address, mountPoint, portID, domainID, devNum ^{※4} , portWWN, fileType, fileName, sizeInMB, percentUsed, portISCSIName
HostModeOpt	HostModeOption (ホストモードオプションの情報)	-
HostVol	HostVolume (Device Manager エージェントから取得したボリューム情報)	デバイスファイル名, メーカー名称, モデル名 ^{※2} , シリアル番号, ポート番号, デバイス番号 ^{※4} , 識別番号, ホスト名称, IP アドレス, ホストの IPv6 用の IP アドレス, マウントポイント, SCSI バスの番号, SCSI バス接続識別番号, LU 番号, HBA のノード WWN, HBA のポート WWN, ストレージシステムのポートの WWN, ファイルシステムのタイプ, ファイルシステム名称, ボリュームサイズ, ボリューム使用率, LU ペアタイプ, Dynamic Link Manager が管理するデバイスファイルの名称, Dynamic Link Manager が管理する LUN バスの本数, LU のペアタイプ (Universal Replicator), Dynamic Link Manager 以外のバス管理ソフトウェアで管理するデバイスファイルの LUN バス本数, Dynamic Link Manager 以外のバス管理ソフトウェアで管理するデバイスファイルの名称, iSCSI イニシエーターの iSCSI ネーム, inquiry の HostGroupID (0~254) ,, ,

出力文字列	正式名と内容	属性値出力順 ^{※1}
		deviceFileName, vendorID, model ^{※2} , serialNumber, port, devNum ^{※4} , hsDeviceID, name, , ipAddress, ipv6Address, mountPoint, OSscsiBus, OSscsiID, OSlun, hbaWWN, portWWN, subsystemPortWWN, fileSystemType, fileSystemName, sizeInMB, percentUsed, pairType, dlmPathName, numberOfDlmPath, pairTypeTCMirror, numberOfPath, relatedPathName, portISCSIName, hostGroupID, , ,
HostVol	HostVolume (ファイルサーバから取得したボリューム情報)	, メーカー名称, モデル名 ^{※2} , シリアル番号, ポート番号, デバイス番号 ^{※4} , , ホスト名称, クラスタ名, IP アドレス, ホストの IPv6 用の IP アドレス, , SCSI バスの番号, SCSI バス接続識別番号, LU 番号, , HBA のノード WWN, , , , ボリュームサイズ, ボリューム使用率, , , , , iSCSI イニシエーターの iSCSI ネーム, inquiry の HostGroupID (0~254), ホストタイプ, ボリュームの用途, ファイルサーバの管理サーバの IP アドレス, ファイルサーバのタイプ, ファイルサーバのクラスタ ID , vendorID, model ^{※2} , serialNumber, port, devNum ^{※4} , , name, cluster, ipAddress, ipv6Address, , OSscsiBus, OSscsiID, OSlun, , portWWN, , , sizeInMB, percentUsed, , , , , portISCSIName, hostGroupID, hostType, usage, managerIpaddress, fileServerDisplayType, clusterID
HSD	HostStorageDomain (ホストグループまたは iSCSI ターゲットに関する情報)	<モデル名 ^{※2} - シリアル番号 - ポート ID - ドメイン ID>, ポート ID, ドメイン ID, ホストグループまたは iSCSI ターゲットの新しいホスト接続モード, 新しいホスト接続モードのリスト, ホスト接続モードのオプション, ホストグループ名または iSCSI ターゲット名, ホストグループまたは iSCSI ターゲットのニックネーム, 操作対象のホストグループまたは iSCSI ターゲットの名前, 操作対象のホストグループまたは iSCSI ターゲットのポート ID, ドメインタイプ, iSCSI ターゲットの iSCSI ネーム, プラットフォーム, ミドルウェア, 交替パス, フェールオーバー, 追加パラメーター <model ^{※2} - serialnum - portID - domainID>, portID, domainID, hostMode, hostMode2, hostModeOption, name, nickname, targetNickname, targetPortID, domainType, iSCSIName, platform, middleware, alternatePath, failover, additionalParameter
IPAddress	IPAddress (ポートコントローラーの IP アドレス)	-
ISCSIName	ISCSIName (iSCSI ネームの情報)	iSCSI イニシエーターの iSCSI ネーム, iSCSI イニシエーターのニックネーム, 操作対象の iSCSI イニシエーターのニックネーム iscsiname, nickname, targetNickname
JrnlPool	JournalPool (ジャーナルグループ情報)	<モデル名 ^{※2} - シリアル番号 - ジャーナルプール識別子 - プール ID>, 名前, ジャーナルプール識別子, プール ID, DP プールの使用率のしきい値 1, DP プールの使用率のしきい値 2, DP プールの使用率のしきい値 2 のモード, ジャーナルボリュームへの流入制限, データあふれ監視時間 (秒), リモートパス監視時間の単位, リモートパス監視時間, リ

出力文字列	正式名と内容	属性値出力順※1
		<p>モータバス監視時間の転送, キャッシュの使用, 回線速度, デルタリシンク失敗時の処理, RAID レベル, 警告予約率, 最大予約率, 予約率の警告通知有無, 階層配置の有無, HDT の自動実行モード, 自動モニタリングの実行周期, 自動モニタリングの開始時刻, 自動モニタリングの終了時刻, 自動モニタリングの HDT の再配置のモニターモード, 自動モニタリングの HDT プールの I/O 負荷情報, 自動モニタリングの稼働状態, 自動モニタリングの最終開始日時, 自動モニタリングの最終終了日時, 自動モニタリングの階層再配置の実行状態, 自動モニタリングの階層再配置の進捗率, 自動モニタリングの階層再配置で使用するモニタリング情報, HDT プールの階層の数, レプリケーション枯渇警告しきい値, レプリケーションデータ解放しきい値, 仮想化超過限界しきい値超過時のボリューム操作可否</p> <p><model※2 - serialnum - poolFunction - poolID>, name, poolFunction, poolID, threshold, threshold2, threshold2mode, inflowControl, dataOverflowWatch, unitOfPathWatchTime, pathWatchTime, forwardPathWatchTime, useOfCache, speedOfLine, deltaResyncFailure, raidLevel, overProvisioningWarning, overProvisioningLimit, volumeThresholdFlag, tierControl, autoMigration, migrationInterval, monitorStartTime, monitorEndTime, monitoringMode, monitorsSideState, monitoringState, lastMonitorStartDate, lastMonitorEndDate, relocationState, relocationProgress, relocateUseMonitor, numberOfTiers, ThresholdRepDepAlert, ThresholdRepDataReleased, overProvisioningLimitEnforcement</p>
JrnlPoolTier	JournalPoolTier (HDT プールの階層情報)	<p><モデル名※2 - シリアル番号, ジャーナルプール識別子, プール ID, 階層 ID>, 階層 ID, 新規割り当て用空き領域率, 再配置用バッファ領域率</p> <p><model※2 - serialnum - poolFunction - poolID - tierID>, tierID, bufSpaceForNewPageAssignment, bufSpaceForTierRelocation</p>
LDEV	LDEV (LDEV に関する情報)	<p><モデル名※2 - シリアル番号 - LDEV のデバイス番号※4>, LDEV の LBA, CLPR 番号, ストライプサイズ, HDT ボリューム※5 の階層割り当てポリシー, DM-LU の拡張に使用されるパリティグループが位置するシャーシ番号, DM-LU の拡張に使用されるパリティグループのパリティグループ番号, HDT ボリューム※5 の階層再配置の有無</p> <p><model※2 - serialnum - devnum※4>, lba, clprNumber, stripeSizeInKB, tierLevel, chassis, number, tierRelocation</p>
LDKC	LogicalDKC (ストレージシステムの論理 DKC)	-
LGrp	LogicalGroup (ホスト, ボリューム, またはほかの論理グループをグループビン グ)	<p><論理グループ ID>, 名前, 説明, <親グループの論理グループの要素識別子>, 操作対象論理グループ名, 親論理グループ名</p> <p><groupID>, name, description, <parentID>, targetLogicalPath, parentLogicalPath</p>
LicenseKey	LicenseKey	<モデル名※2 - シリアル番号 - LicenseKeyID>

出力文字列	正式名と内容	属性値出力順 ^{※1}
	(プログラムを使用できるようにするために必要なキーコード)	<model ^{※2} - serialnum - PPID>
LU	LogicalUnit (LUを表す情報)	<モデル名 ^{※2} - シリアル番号 - 論理デバイス番号 ^{※4} >, 論理ユニットに含まれている LDEV の番号 ^{※4} , ボリュームサイズ, エミュレーションモード, ポートコントローラーのデフォルトの数, コマンドデバイスとして使用されているかの有無, コマンドデバイスセキュリティが設定されているかの有無, 論理ユニットがコマンドデバイスとして使用されている場合のユーザー認証モードの有無, DP プールボリューム ID, DP プールのしきい値, Differential Management LU かどうか, 外部ボリュームの階層ランク <model ^{※2} - serialnum - devnum ^{※4} >, devNum ^{※4} , capacityInKB, emulation, defaultPortController, commandDevice, commandDeviceSecurity, commandDeviceAuth, dpPoolID, threshold, differentialManagement, externalTierRank
LVol	LogicalVolume (論理ボリュームの情報)	名前, サイズ, 論理ボリュームの削除可否, 論理ボリュームの拡張可否, 論理ボリュームのタイプ name, size, deletable, expandable, type
MFRepI	MFReplicationInfo (メインフレームボリュームのレプリケーションに関する情報)	<PVOL シリアル番号 - PVOLLDEV 番号 ^{※4} - SVOL シリアル番号 - SVOLLDEV 番号 ^{※4} >, P-VOL のストレージシステムのタイプ ^{※2} , P-VOL が属しているストレージシステムのシリアル番号, P-VOL のデバイス番号 ^{※4} , P-VOL パスを管理する HORCM 構成ファイル内のポート番号, S-VOL のストレージシステムのタイプ ^{※2} , S-VOL が属しているストレージシステムのシリアル番号, S-VOL のデバイス番号 ^{※4} , S-VOL パスを管理する HORCM 構成ファイル内のポート番号, S-VOL が属するプール ID, コピーの種類 ^{※6} , P-VOL の MU 番号, P-VOL のフェンスレベル <pvolSerialNumber - pvolDevNum ^{※4} - svolSerialNumber - svolDevNum ^{※4} >, pvolArrayType ^{※2} , pvolSerialNumber, pvolDevNum ^{※4} , pvolPortID, svolArrayType ^{※2} , svolSerialNumber, svolDevNum ^{※4} , svolPortID, svolPoolID, replicationFunction ^{※6} , muNumber, fenceLevel
MFVolI	MFVolumeInfo (メインフレームホストと LDEV 間のアクセス情報)	-
MountPoint	MountPoint (マウントポイントの情報)	名前, プロトコル, ディレクトリパス, 共有容量, 共有容量の使用量, 共有容量の使用率, CIFS 共有名 name, protocol, path, shareCapacityInMB, shareUsedCapacityInMB, shareCapacityPercentUsed, cifsShareName
Msg	Message (非同期メッセージ)	-
Msgs	Messages (Message エlement をグルーピング)	待ち時間 (秒) timeToWait
ObjLabel	ObjectLabel	オブジェクト ID, オブジェクトに設定するラベル

出力文字列	正式名と内容	属性値出力順 ^{※1}
	(Device Manager サーバのオブジェクトのラベル設定)	targetID, label
ObjName	ObjectName (Device Manager サーバのオブジェクト名設定)	<対象エレメント名 - 対象エレメント識別子>, 名前 注意事項: <対象エレメント名>および<対象エレメント識別子>は, ObjectName 属性以外のエレメント名とエレメント識別子を示しています。エレメント識別子に対する構成要素は, <対象エレメント名>に対応する属性値出力順を参照してください。 <対象エレメント名 - 対象エレメント識別子>, name
PairedJrnlPool	PairedJournalPool (Universal Replicator のジャーナルプールとペアになっているジャーナルプール)	<モデル名 ^{※2} - シリアル番号 - ジャーナルプール識別子 - プール ID - MU 番号 ^{※3} , MU 番号, 形成コピー転送レート <model ^{※2} - serialNumber - poolFunction - poolID - muNumber ^{※3} , muNumber, transferRate
PairedPortController	PairedPortController (NAS 構成上でペアになっている CHIP)	-
PairedVol	PairedVolume (HostVolume とペアになっている相手ペアボリュームの情報)	レプリケーション操作種別 ^{※6} , ボリュームタイプ, ボリューム装置製番, ボリューム装置機種 ^{※2} , ボリュームの論理デバイス番号 ^{※4} , ペアの状態, フェンスレベル, ペアの対象 S-VOL に対する P-VOL の MU 番号 replicationFunction ^{※6} , otherPairType, otherPairSerialNumber, otherPairArrayType ^{※2} , otherPairDevNum ^{※4} , status, fenceLevel, muNumber
Para	Parameter (名前と値の対)	パラメーターの名前, パラメーターの値 ^{※2} name, value ^{※2}
Part	Partition (パーティションの情報)	名称, ボリュームグループ名, パーティションの容量 name, volumeGroupName, sizeInMB
Path	Path (ホストとホストグループ間またはホストと iSCSI ターゲット間のパスに関する情報)	<モデル名 ^{※2} - シリアル名 - ポート ID - ドメイン ID - 論理デバイス番号 ^{※4} >, 名前, ポート ID, ホストグループまたは iSCSI ターゲットのドメイン ID, 操作対象のホストグループまたは iSCSI ターゲットの名前, SCSI ID, ホストとホストグループ間またはホストと iSCSI ターゲット間のパスに割り当てられている LUN, 論理ユニットを識別するためのデバイス番号 ^{※4} , 操作対象のホストグループまたは iSCSI ターゲットのポート ID, 操作対象のホストグループまたは iSCSI ターゲットの ID, 操作対象のホストグループまたは iSCSI ターゲットのニックネーム, 操作対象のデバイス番号 ^{※4} <model ^{※2} - serialnum - portID - domainID - devnum ^{※4} >, name, portID, domainID, domainNickname, scsiID, lun, devNum ^{※4} , targetPortID, targetDomainID, targetDomainNickname, targetDevNum ^{※4}
PDEV	PDEV (PDEV に関する情報)	<モデル名 ^{※2} - シリアル番号 - PDEV の ID>, ドライブタイプ, ドライブサイズ, フォームファクタ

出力文字列	正式名と内容	属性値出力順※1
		<model※2 - serialnum - PDEVID>, diskType, diskModelSize, formFactor
Port	Port (ポートに関する情報)	<モデル名※2 - シリアル番号 - ポート ID>, ファイバーチャネルポートのアドレス, ファイバーチャネルトポロジー, iSCSI ポートに対して LUN セキュリティが有効か無効か, iSCSI ポートオプション, チャネルスピード, iSCSI ポートの IP アドレス, ポートのサブネットマスク, iSCSI ポートのゲートウェイの IP アドレス, iSCSI ポート番号, キープアライブタイム, iSCSI ポートの属性, IPv6 の状態, リンクローカルアドレスの設定種別, リンクローカルアドレス, グローバルアドレスの設定種別, グローバルアドレス 1, グローバルアドレス 2, IPv6 のゲートウェイアドレス, MTU の設定, VLAN の状態, VLAN ID, Window Scale <model※2 - serialnum - portID>, fibreAddress, topology, lunSecurityEnabled, portOption, channelSpeed, ipAddress, subnetMask, gateway, portNumber, keepAliveTime, portRole, ipv6SettingMode, linklocalSettingMode, linklocalAddress, globalSettingMode, globalAddress1, globalAddress2, gatewayForIPv6, mtu, vlanSettingMode, vlanId, windowScale
PortCtrl	PortController (ストレージシステムのポートコントローラーに関する情報)	<モデル名※2 - シリアル番号 - ポートコントローラー ID>, モード <model※2 - serialnum - controllerID>, mode
Prm	Param (CIMInvoker で指定したメソッドのパラメーターを指定するエレメント)	実行するメソッドのパラメーター名, このパラメーターで指定する値の型, パラメーターで指定する値 name, type, value
RDArrGrp	RelatedDistributedArrayGroup	-
RepCon	ReplicationConnection (MCU と RCU 間の通信に関する情報)	MCU 側のポート名, RCU 側のポート名 masterPortDisplayName, remotePortDisplayName
RepCtrlPair	ReplicationControllerPair (MCU および RCU に関する情報)	<MCU 機種 - MCU 装置製番 - MCU の CU 番号 - RCU の ArrayFamily - RCU 装置製番 - RCU の SSID, RCU のパスグループ ID>, MCU モデル, MCU のシリアル番号, MCU の CU 番号, RCU モデル, RCU のシリアル番号, RCU の SSID, RCU の CU 番号, ペアのタイプ, RCU のパスのグループ ID, 回線の帯域 <masterArrayType - masterSerialNumber - masterControllerID - remoteArrayFamily - remoteSerialNumber - remoteSSID - remotePathGroupID>, masterArrayType, masterSerialNumber, masterControllerID, remoteArrayFamily, remoteSerialNumber, remoteSSID, remoteControllerID, pairType, remotePathGroupID, bandwidth
RepGrp	ReplicationGroup (HORCM インスタンスグループに関する情報)	<レプリケーショングループ ID>, RAID Manager が使用するコピーグループの名前, P-VOL を認識するホストのホスト ID, P-VOL を管理する HORCM インスタンスの情報

出力文字列	正式名と内容	属性値出力順 ^{※1}
		<p>スタンス番号, P-VOL を管理する HORCM インスタンスのポート番号, S-VOL を識別するホストのホスト ID, S-VOL を管理する HORCM インスタンスのインスタンス番号, S-VOL を管理する HORCM インスタンスのポート番号, コピーの種類^{※6}, P-VOL のフェンスレベル, コピーペース</p> <p><replicationGroupID>, groupName, pvolHostID, pvolInstanceNumber, pvolPortNumber, svolHostID, svolInstanceNumber, svolPortNumber, replicationFunction^{※6}, fenceLevel, copyTrackSize</p>
RepI	ReplicationInfo (レプリケーションに関する情報)	<p><PVOL シリアル番号 - PVOLLDEV 番号^{※4} - SVOL シリアル番号 - SVOLLDEV 番号^{※4}>, RAID Manager が使用するコピーペアの名前, P-VOL のストレージシステムのタイプ^{※2}, P-VOL が属しているストレージシステムのシリアル番号, P-VOL のデバイス番号^{※4}, P-VOL パスを管理する HORCM 構成ファイル内のポート番号, P-VOL が属するプール ID, S-VOL のストレージシステムのタイプ^{※2}, S-VOL が属しているストレージシステムのシリアル番号, S-VOL のデバイス番号^{※4}, S-VOL パスを管理する HORCM 構成ファイル内のポート番号, S-VOL が属するプール ID, コピーの種類^{※6}, P-VOL の MU 番号, P-VOL のフェンスレベル, コピーペース, P-VOL の管理データ用 DP プールのプール ID, S-VOL の管理データ用 DP プールのプール ID, スナップショットグループの ID</p> <p><pvolSerialNumber - pvolDevNum^{※4} - svolSerialNumber - svolDevNum^{※4}>, pairName, pvolArrayType^{※2}, pvolSerialNumber, pvolDevNum^{※4}, pvolPortID, pvolPoolID, svolArrayType^{※2}, svolSerialNumber, svolDevNum^{※4}, svolPortID, svolPoolID, replicationFunction^{※6}, muNumber, fenceLevel, copyTrackSize, pvolMngAreaPoolID, svolMngAreaPoolID, snapshotGroupID</p>
ReqStatus	RequestStatus (直前のリクエストの状態を返す)	<p>メッセージ ID</p> <p>messageID</p>
RPort	RelatedPort (ほかのポートの属性が変更された際に、属性が変更されるポート)	-
RSIMI	RSIMInfo (ストレージシステムの RSIM 情報)	<p>RSIM 情報の RSIM ID</p> <p>RSIMID</p>
RsltObj	ResultObject (ListView エlement で表示される一覧中の「1 行」)	-
SA	StorageArray (ストレージシステム情報)	<p><モデル名^{※2} - シリアル番号></p> <p><model^{※2} - serialnum></p>
SIMI	SIMInfo	<p>SIM 情報の SIMID</p> <p>SIMID</p>

出力文字列	正式名と内容	属性値出力順 ^{※1}
	(ストレージシステムの SIM 情報)	
SizeCond	SizeCondition (SearchCondition の内の件数指定条件)	先頭から読み飛ばす件数, 取得する件数 offset, size
SlctCond	SelectCondition (SelectItem エレメントがまとめられた要素)	下位の SelectItem エレメントが表す条件を連結する条件演算子 operator
SlctItem	SelectItem (SearchCondition の内のフィルター条件)	フィルター条件のキー値, key 属性と value 属性の関係を表す演算子, フィルター条件の値 ^{※2} key, operator, value ^{※2}
SmrtFldr	SmartFolder (論理グループに関する情報)	<論理グループ ID>, 論理グループのパス <groupID>, logicalPath
SortCond	SortCondition (SortItem がまとめられた要素)	-
SortItem	SortItem (SearchCondition の内のソート条件)	ソートキーとなるカラム名, ソート順, ソートの優先順位 key, order, priority
SrchCond	SearchCondition (ListView を取得するときの検索条件)	-
SrcHost	SourceHost (移行元ホストの情報)	<ホスト ID>, ホスト名 <hostID>, name
SrvI	ServerInfo (Device Manager サーバの情報)	-
SsGrp	SnapshotGroup (スナップショットグループに関する情報)	<モデル名 ^{※2} - シリアル番号 - スナップショットグループの ID>, ストレージシステムのタイプ, シリアル番号, スナップショットグループの ID, スナップショットグループの名前, コピーペアで実行される操作のタイプ ^{※6} , コンシステンシーグループの ID <model ^{※2} - serialNumber - groupID>, arrayType, serialNumber, groupID, groupName, replicationFunction ^{※6} , ctGrp
SSOpt	StorageSystemOption (ストレージシステムに設定されているオプションに関する情報)	オプション名, オプションの値 name, value
SsSummary	SnapshotSummary (Copy-on-Write Snapshot の P-VOL に関する情報)	-
Subscrbr	Subscriber (通知予定トピック)	-
TargetPort	TargetPort (外部ストレージシステムのポート)	外部ストレージシステムのポートの WWN targetPortAddress

出力文字列	正式名と内容	属性値出力順 ^{※1}
Timestamp	Timestamp (Device Manager サーバでメッセージが生成された時刻)	-
Topic	Topic (メッセージトピックの名称)	通知情報 name
TrngPlcy	TieringPolicy (HDT ボリューム ^{※5} の階層ポリシーに関する情報)	<モデル名 ^{※2} , シリアル番号, 階層ポリシー ID>, 階層 1 に対する最大容量しきい値, 階層 1 に対する最小容量しきい値, 階層 3 に対する最大容量しきい値, 階層 3 に対する最小容量しきい値 <model ^{※2} , serialNumber, policyID>, allocationThresholdT1Max, allocationThresholdT1Min, allocationThresholdT3Max, allocationThresholdT3Min
URLLink	URLLink (Hitachi Command Suite オブジェクトとアプリケーションのリンク)	<関連エレメント識別子・識別 ID>, アプリケーションまたは Web ページを起動するのに必要な URL, アプリケーション名, <リンク先関連エレメント識別子・リンク先識別 ID>, 補足説明, ファイルサーバのホスト名 <linkedID - nameID>, url, name, <linkedID - nameID>, description, linkedHostName
User	User (Device Manager の 1 ユーザーアカウント情報)	ユーザー ID, パスワード, ユーザーと関連づけられているリソースグループ名, ユーザーと関連づけられているリソースグループに対する権限, ユーザー名, 補足説明 loginID, password, groupName, role, fullName, description
VD	VirtualDisk (仮想ドライブの情報)	-
VHSD	VHostStorageDomain (仮想ホストストレージドメインの情報)	-
VLDEV	VLDEV (LDEV に関する仮想情報)	<モデル名 ^{※2} - シリアル番号 - 仮想 ID を用いたデータ移行用のリソースグループの ID - デバイス番号 ^{※4} >, デバイス番号 ^{※4} , 仮想デバイス番号 ^{※4} , 仮想エミュレーションタイプ, 仮想 SSID, 仮想 LUSE を構成する要素数, 仮想 CVS 設定有無 <model ^{※2} - serialNumber - ResourcePartitionUnitID - devNum ^{※4} >, devNum ^{※4} , vDevNum ^{※4} , vEmulation, vSSID, vLUSE, vCVS
VM	VM (仮想マシンの情報)	-
VolCon ^{※3}	VolumeConnection (割り当てられた LDEV と、それに一致する外部 LU に関する情報)	<割り当てられた LU のモデル名 ^{※2} - 割り当てられた LU の装置製番 - 割り当てられた LU のデバイス番号 ^{※4} > <mappedArrayType ^{※2} - mappedSerialNumber - mappedDevNum ^{※4} >
VolFmtPrgrss	VolumeFormatProgress (ボリュームのフォーマットの進捗)	-

出力文字列	正式名と内容	属性値出力順 ^{※1}
VolGrp	VolumeGroup (ボリュームグループの情報)	タイプ, 名前, ボリュームグループの容量, ボリュームグループに属するドライブ数 type, name, size, numberOfDisk
VolMig	VolumeMigration (マイグレーションプランに関する情報)	<モデル名 ^{※2} - シリアル番号 - 移動元 LDEV 番号 ^{※4} - 移動先 LDEV 番号 ^{※4} >, 移動操作オーナー ID, 移動元デバイス番号 ^{※4} , 移動先デバイス番号 ^{※4} <model ^{※2} - serialnum - sourceDevNum ^{※4} - targetDevNum ^{※4} >, ownerId, sourceDevNum ^{※4} , targetDevNum ^{※4}
VolShred	VolumeShredding (シュレッディング機能に関する情報)	シュレッディングのオーナー ID ownerID
VPort	VPort (仮想ポートの情報)	-
VRpu	VResourcePartitionUnit (仮想 ID を用いたデータ移行に使用しているリソースグループの情報)	<モデル名 ^{※2} - シリアル番号 - 仮想 ID を用いたデータ移行用のリソースグループの ID> <model ^{※2} - serialNumber - ResourcePartitionUnitID>
WritingPattern	WritingPattern (書き込み 1 回分の書き込みパターン情報)	シュレッディングが指定されたときの書き込みパターン pattern
WritingPatterns	WritingPatterns (VolumeShredding 1 回分の全書き込みパターン情報)	-
WWN	WorldWideName (ホストの HBA 情報)	WorldWideName, ニックネーム, 操作対象ホストグループ名, WorldWideName wwn, nickname, targetNickname, wwnString

(凡例)

- : 属性値出力なし

<...> : 属性の 1 つを表すエレメント識別子。内容が複数の要素で構成される場合、ハイフン (-) で連結されます。

注※1

下段は、Device Manager 内部で使用される名称による出力順です。

注※2

ストレージシステム種別として、「表 13-18 ストレージシステム種別 共通出力名称一覧」に示す共通出力名称で出力されます。

注※3

ObjectName エレメントの<対象エレメント識別子>として出力される場合の属性値出力順です。エレメントの属性値としては、<対象エレメント識別子>は出力されません。

注※4

Virtual Storage Platform, Universal Storage Platform V/VM および HUS VM の場合は、LDKC 番号, CU および LDEV 番号を組み合わせた数値 (=LDKC*65536+CU*256+LDEV)

が出力されます。SANRISE9900V および Hitachi USP の場合は、CU と LDEV 番号を組み合わせた数値 (=CU*256+LDEV) が出力されます。

HUS100, Hitachi SMS, Hitachi AMS/WMS および SANRISE9500V の場合は LU 番号が出力されます。

注※5

HDT プールから作成 (HDT プールと関連づけ) する仮想ボリュームです。

注※6

レプリケーション操作種別属性は、「表 13-19 レプリケーション操作種別属性 共通出力名称一覧」に示す共通出力名称で出力されます。

表 13-18 ストレージシステム種別 共通出力名称一覧

共通出力名称	対応ストレージシステム種別
D600	SANRISE9500V
D700	Hitachi AMS/WMS
D800	Hitachi AMS2000
D850	HUS100
HM700	HUS VM
R450	SANRISE9900V
R500	Hitachi USP
R600	Universal Storage Platform V/VM
R700	Virtual Storage Platform
S800	Hitachi SMS

表 13-19 レプリケーション操作種別属性 共通出力名称一覧

共通出力名称	対応製品
Local Copy	ShadowImage
Remote Copy (Async)	TrueCopy Async
Remote Copy (Jrnl)	Universal Replicator
Remote Copy (Sync)	TrueCopy Sync
SnapShot	QuickShadow Copy-on-Write Snapshot
SnapShot (Fast)	Thin Image

13.3.3 Tiered Storage Manager のユーザー操作と監査ログの対応

ここでは、Tiered Storage Manager での操作時に出力される監査ログについて説明します。

(1) GUI 操作と監査ログの対応

監査ログの出力内容から、Legacy モードの Tiered Storage Manager GUI で実行した内容を推定する方法を次に示します。

1. Tiered Storage Manager が出力した監査ログを抽出します (プログラム名が「TSMgr」であるもの)。

GUI の操作による監査ログは、Tiered Storage Manager が出力する監査ログのうち、アプリケーション識別情報が「TSM_GUI」となっているものです。

複数のユーザーが同時刻に Tiered Storage Manager にアクセスしている場合、「サブジェクト識別情報」に出力されるユーザー ID によってフィルタリングできます。

2. 監査ログの出力内容と「表 13-20 GUI 操作と、監査ログに出力される主要情報の対応」を突き合わせて、マッチするパターンを見つけることで、GUI の操作を推定します。

監査ログの出力内容のうち、Get 系の情報は、画面更新などのために頻繁に呼ばれるため、これだけを見てユーザー操作を特定することはできません。一方 Tiered Storage Manager の各種資源に対する作成、更新、削除などの操作については、監査ログの中にその操作に対応した出力情報があります。「表 13-20 GUI 操作と、監査ログに出力される主要情報の対応」には、これらの操作を特定するための主要な情報だけを示しています。「キー」欄に○印の付いている監査ログ情報によって、ユーザー操作を特定できます。実際の監査ログには、これらの情報の前後に、Get 系の監査ログが出力されます。

ユーザーが操作するとき直接指定するのは、ストレージドメイン名やマイグレーショングループ名などの「名称」です。しかし、Tiered Storage Manager サーバが出力する監査ログには、ストレージドメイン ID やマイグレーショングループ ID などの Tiered Storage Manager 内部で管理する「ID」しか出ないものがあります。この場合、その監査ログ情報だけを見ても「ID」に対応する「名称」はわかりませんが、その近くに出力されている監査ログを調べれば、「ID」と「名称」の両方の情報を出力しているものがありますので、それによって対応を調べられます。

新規に作成するものは、「Create xx」の監査事象の情報に、両方の情報が出力されています。既存のものに対する操作の場合は、GUI または CLI が選択対象に関する情報を知るために、事前に「Get 系のリクエスト」を発行していますので、そこから両方の情報を取得できます。

ID に対応する名称を調べる方法を、ストレージドメインを更新（リフレッシュ）する場合を例にして、次に示します。

(例)

OP=(10,Get), Res=(20,SD), SD=(domainId,domainName)...(1) (ドメイン選択)

OP=(90,Refresh), Res=(20,SD), SD=(domainId,...)(2) (ドメインをリフレッシュ)

(2)の情報だけを見ると domainId しかわかりませんが、直前の(1)を見ると対応する domainName がわかります。

表 13-20 GUI 操作と、監査ログに出力される主要情報の対応

GUI 操作	キー	OpName※	ResName※	追加情報※	特記事項
ログイン	○	Get	LC	—	—
ストレージドメイン一覧表示	○	Get	SD	NumSD	—
ストレージドメイン詳細情報表示	○	Get	SD	SD	—
	—	Get	RS	SD	—
ストレージ階層一覧表示	○	Get	ST	SD, NumST	—
ストレージ階層詳細情報表示	○	Get	ST	SD, ST	—
マイグレーショングループ作成	○	Create	MG	SD, MG	—
マイグレーショングループ編集	○	Modify	MG	SD, MG	—
マイグレーショングループ削除	○	Delete	MG	MG	—

GUI 操作	キー	OpName※	ResName※	追加情報※	特記事項
マイグレーショングループ一覧表示	○	Get	MG	SD, NumMG	—
マイグレーショングループ詳細表示	○	Get	MG	SD, MG	—
マイグレーショングループへのボリューム追加	○	Add	VL	MG, VL	追加ボリューム数分出力されます
マイグレーショングループからのボリューム削除	○	Remove	VL	MG, VL	削除ボリューム数分出力されます
ボリューム検索	—	Get	VR	SD	—
	○	Get_num	VL	NumVL	—
	○	Get	VL	SD, NumVL	—
プール検索	○	Get_num	PO	NumPO	—
	○	Get	PO	SD, NumPO	—
タスク検索	○	Get_summary	TK	NumTK	—
マイグレート MG	○	Create	MP	SD, MG, ST	—
マイグレーションタスク作成	○	Create	TK	TK, SD, MG, ST, NumVP, VPs	—
タスク実行	○	Execute	TK	TK	—
タスク一覧表示	○	Get_summary	TK	NumTK	—
タスク詳細表示	○	Get	TK	TK	—
タスクキャンセル	○	Cancel	TK	TK	—
タスク中止	○	Change	TK	TK	—
タスク変更	○	Modify	TK	TK	—
タスク削除	○	Delete	TK	TK	—

(凡例)

- : 主キー
- : 該当なし

注※

詳細については「表 13-7 監査ログのメッセージテキストに出力される項目（メッセージ本文、操作種別および操作対象）」～「表 13-11 監査ログに出力される操作対象（Res）の意味」を参照してください。

(2) CLI 操作と監査ログの対応

監査ログの出力内容から CLI で実行した内容を推定する方法を次に示します。

1. Tiered Storage Manager が出力した監査ログを抽出します（プログラム名が「TSMgr」であるもの）。

CLI コマンド実行による監査ログは、Tiered Storage Manager が出力する監査ログのうち、アプリケーション識別情報が「TSM_CLI」のものであります。

複数のユーザーが同時刻に Tiered Storage Manager にアクセスしている場合、「サブジェクト識別情報」に出力されるユーザー ID によってフィルタリングできます。

2. 監査ログの出力内容と「表 13-21 CLI コマンドと、監査ログに出力される情報の対応」を突き合わせて、マッチするパターンを見つけることで、CLI コマンドを推定します。
- Get で始まるコマンド以外は、「キー」欄に○印の付いている監査ログ情報によって、入力されたコマンドを特定できます。

表 13-21 CLI コマンドと、監査ログに出力される情報の対応

CLI コマンド	キー※1	OpName※2	ResName※2	追加情報※2	特記事項
AddVolumeToMigrationGroup	○	Add	VL	SD, MG, VL	—
	—	Get	MG	SD, MG	—
	—	Get	SD	SD	—
	—	Get	VL	SD, NumVL	—
CancelTask	○	Cancel	TK	TK	—
CreateLockingTask	○	Create	TK	TK, SD, MG, NumVL, VLs	TK=(id,2,...)
	—	Execute	TK	TK	—
	—	Get	TK	TK	—
CreateMigrationGroup	—	Get	SD	SD	—
	○	Create	MG	SD, MG	—
CreateMigrationPlan	—	Get	ST	SD, NumST, [STs]	—
	○	Create	MP	SD, MG, ST	—
CreateMigrationTask	○	Create	TK	TK, SD, MG, ST, NumVP, VPs	TK=(id,0,...)
	—	Execute	TK	TK	--execute 指定あり
	—	Get	TK	TK	--execute 指定あり
CreateShreddingTask	○	Create	TK	TK, SD, MG, NumVL, VLs	TK=(id,4,...)
	—	Execute	TK	TK	--execute 指定あり
	—	Get	TK	TK	--execute 指定あり
CreateStorageDomain	○	Create	SD	SD, SS	—
CreateStorageTier	—	Get	SD	SD	—
	○	Create	ST	SD, ST	—
CreateUnlockingTask	○	Create	TK	TK, SD, MG, NumVL, VLs	TK=(id,3,...)
	—	Execute	TK	TK	--execute 指定あり
	—	Get	TK	TK	--execute 指定あり
DeleteMigrationGroup	—	Get	MG	SD, MG	—
	○	Delete	MG	MG	—
DeleteStorageDomain	—	Get	SD	SD	—
	○	Delete	SD	SD	—
DeleteStorageTier	—	Get	ST	SD, ST	—

CLI コマンド	キー※1	OpName※2	ResName※2	追加情報※2	特記事項
	○	Delete	ST	SD, ST	—
DeleteTasks	—	Get	TK	{TK NumTK}	--force 指定なし
	○	Delete	TK	{TK NumTK, TKs}	—
ExecuteTask	○	Execute	TK	TK	—
GetFreeSpaces	—	Get	SS	NumSS	—
	—	Get_num	FS	SS, NumFS	subsystemname パラメーターで指定したストレージシステムの数だけ取得
	○	Get	FS	SS, NumFS	subsystemname パラメーターで指定したストレージシステムの数だけ取得
GetMigrationGroups	○	Get	MG	SD, NumMG, [MGs]	—
GetPools	—	Get_num	PO	NumPO	—
	—	Get	SD	SD	—
	○	Get	PO	SD, NumPO	—
GetStorageDomains	○	Get	SD	NumSD, [SDs]	—
	—	Get	RS	NumSD, SDs	—
GetStorageTiers	○	Get	ST	SD, NumST, [STs]	—
	—	Get	SD	SD	—
GetTasks	○	Get	TK	{TK NumTK}	—
GetVolumes	—	Get_num	VL	NumVL	—
	—	Get	SD	SD	10,000 件ずつ分割取得
	○	Get	VL	SD, NumVL	10,000 件ずつ分割取得
ModifyMigrationGroup	—	Get	MG	SD, MG	—
	○	Modify	MG	SD, MG	—
ModifyStorageDomain	—	Get	SD	SD	—
	○	Modify	SD	SD	—
ModifyStorageTier	—	Get	ST	SD, ST	—
	○	Modify	ST	SD, ST	—
ModifyTask	—	Get	TK	TK	—
	○	Modify	TK	TK	—

CLI コマンド	キー※1	OpName※2	ResName※2	追加情報※2	特記事項
Refresh	—	Get_summar y	SD	NumSD	ストレージド メイン名の指 定あり
	○	Refresh	SD	SD	—
RemoveVolumeFromMigrati onGroup	—	Get_summar y	SD	SD	—
	—	Get	MG	SD, MG	—
	—	Get	VL	SD, NumVL	—
	○	Remove	VL	SD, MG, VL	—
StopTask	○	Change	TK	TK	opt = (0x02040000 , または 0x02050000)

(凡例)

- : 主キー
- : 該当なし

注※1

コマンドを推定する際に、キーとなる監査ログです。

注※2

詳細については「表 13-7 監査ログのメッセージテキストに出力される項目（メッセージ本文、操作種別および操作対象）」～「表 13-11 監査ログに出力される操作対象（Res）の意味」を参照してください。

Device Manager サーバのプロパティ

ここでは、Device Manager サーバのプロパティファイルについて説明します。

- A.1 Device Manager サーバのプロパティファイル
- A.2 Device Manager サーバの構成情報に関するプロパティ (server.properties ファイル)
- A.3 Device Manager のデータベースに関するプロパティ (database.properties ファイル)
- A.4 Device Manager のログ出力に関するプロパティ (logger.properties ファイル)
- A.5 Device Manager のスレッドに関するプロパティ (dispatcher.properties ファイル)
- A.6 Device Manager の MIME に関するプロパティ (mime.properties ファイル)
- A.7 Device Manager の GUI に関するプロパティ (client.properties ファイル)
- A.8 Device Manager のセキュリティに関するプロパティ
- A.9 Device Manager の SNMP トラップのログ出力に関するプロパティ (customizedsnmptrap.properties ファイル)
- A.10 Device Manager からラUNCHするアプリケーションに関するプロパティ (launchapp.properties ファイル)
- A.11 ホストとの通信に関するプロパティ (host.properties ファイル)
- A.12 Host Data Collector との連携に関するプロパティ (hostdatacollectors.properties ファイル)
- A.13 マイグレーションに関するプロパティ (migration.properties ファイル)
- A.14 Tuning Manager との連携に関するプロパティ (tuningmanager.properties ファイル)
- A.15 Universal Replicator の性能分析に関するプロパティ (replication.properties ファイル)
- A.16 Replication Manager との連携に関するプロパティ (rpmlib.properties ファイル)

- A.17 CIM/WBEM 機能に関するプロパティ (jserver.properties ファイル, cimxmlcpa.properties ファイル, cimxmlscpa.properties ファイル)

A.1 Device Manager サーバのプロパティファイル

Device Manager サーバのプロパティファイルには、Device Manager の構成情報に関するプロパティファイルやデータベースに関するプロパティファイルなどがあります。

Device Manager サーバのプロパティファイルを次の表に示します。

表 A-1 Device Manager サーバのプロパティファイル

プロパティファイル	説明
server.properties ファイル	Device Manager サーバの構成情報に関するプロパティファイルです。 警告： 専門知識のある方以外は、これらの属性を最適化する操作は実行しないでください。僅かな変更でも Device Manager サーバのパフォーマンスに重大な影響が出るおそれがあります。
database.properties ファイル	Device Manager のデータベースに関するプロパティファイルです。 警告： 専門知識のある方以外は、これらの属性を最適化する操作は実行しないでください。僅かな変更でも Device Manager サーバのパフォーマンスに重大な影響が出るおそれがあります。
logger.properties ファイル	Device Manager のログ出力に関するプロパティファイルです。
dispatcher.properties ファイル	Device Manager のスレッドに関するプロパティファイルです。
mime.properties ファイル	Device Manager の MIME (Multipurpose Internet Mail Extensions) に関するプロパティファイルです。
client.properties ファイル	Device Manager の GUI に関するプロパティファイルです。
customizedsnmptrap.properties ファイル	Device Manager の SNMP トラップのログ出力に関するプロパティファイルです。
launchapp.properties ファイル	Device Manager からラウンチするアプリケーションに関するプロパティファイルです。
host.properties ファイル	ホストとの通信に関するプロパティファイルです。
hostdatacollectors.properties ファイル	Host Data Collector との連携に関するプロパティファイルです。
migration.properties ファイル	マイグレーションに関するプロパティファイルです。
tuningmanager.properties ファイル	Tuning Manager との連携に関するプロパティファイルです。
replication.properties ファイル	Universal Replicator の性能分析に関するプロパティファイルです。
rpmlib.properties ファイル	Replication Manager との連携に関するプロパティファイルです。
• jserver.properties ファイル • cimxmlcpa.properties ファイル • cimxmlscpa.properties ファイル	CIM/WBEM 機能に関するプロパティファイルです。



注意

- 通常、Device Manager サーバのプロパティファイルの設定値は特に変更する必要はありません。

値を変更すると、サーバの故障や不具合の原因となることがあるので、十分に注意してください。結果の予測に必要な専門知識がないユーザーは、値を変更しないでください。

- デフォルト値は新規インストールした際に設定される値です。
- 上書きインストールまたはアップグレードインストールした場合、**Device Manager** サーバのプロパティファイルの設定値は、インストール前の値が引き継がれます。

A.1.1 Device Manager サーバのプロパティの変更

Device Manager サーバのプロパティファイルは、テキストエディターを使用して編集します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

Device Manager サーバのプロパティを変更するには：

1. Hitachi Command Suite 製品のサービスを停止します。
2. テキストエディターで、**Device Manager** サーバのプロパティファイルに適切な値を設定します。
3. Hitachi Command Suite 製品のサービスを起動します。

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

A.1.2 Device Manager サーバのプロパティファイルの記述規則

プロパティファイルは、Java プロパティファイル形式です。

プロパティファイルは、次の記述規則に従って作成されている必要があります。

- 各プロパティは、`foo.bar=12345` のように、「=」で区切られた名前と値の対で指定します。
- 個々のプロパティは、行区切り文字 (改行) で区切ります。
- 行頭に番号記号 (#) がある場合、その行は注釈行になります。
- リテラル (文字列または数値) を引用符で囲む必要はありません。
- 円記号 (\$) はエスケープ文字を表す予約文字になります。**Windows** では、絶対パス名を表すときに円記号 (\$) を含むので、「\$\$」と指定する必要があります。
例えば、ファイルパス名 `C:\HiCommand\docroot\foo.bar` は、`C:\\HiCommand\\docroot\\foo.bar` と入力します。プロパティの指定では、そのほかの文字にはエスケープ文字「\$」を付ける必要はありません。
- プロパティファイル内に同じプロパティ名で複数の設定がされている場合、ファイルの最後に設定したプロパティの値が有効になります。
- 行末に円記号 (\$) がある場合、次の行は継続行になります。

A.2 Device Manager サーバの構成情報に関するプロパティ (server.properties ファイル)

構成情報に関するプロパティは、`server.properties` ファイルに含まれています。

- Windows の場合 :
`<Device Manager サーバのインストールフォルダ>%HiCommandServer%config
server.properties`
- Solaris または Linux の場合 :
`<Device Manager サーバのインストールディレクトリ>/HiCommandServer/config/
server.properties`

A.2.1 server.http.host

管理サーバ (Device Manager サーバ) のホスト名または IP アドレスを指定します。

IP アドレスを指定する場合の入力形式は次のとおりです。

IPv4 の場合 :

`x.x.x.x` (x は 0~255)

IPv6 の場合 :

コロン付きの 16 進数で指定します。省略形も使用できます。使用できる IPv6 アドレスはグローバルアドレスだけです。

ホスト名および IP アドレスは、クライアント (GUI, CLI およびストレージシステム) からアクセスできる値を指定する必要があります。

デフォルト : インストール時に指定した管理サーバのホスト名または IP アドレス (URL の登録処理でエラーが発生した場合は localhost が設定されます)



注意

- Device Manager がインストールされているサーバマシンが、NIC を複数搭載している場合、クライアント (GUI, CLI およびストレージシステム) が接続されているネットワーク側の IP アドレスを指定してください。ホスト名は指定しないでください。
- クラスタ環境の場合は、クラスタ管理 IP アドレスを指定する必要があります。
- Device Manager で SMI-S enabled ストレージシステムを管理している場合、このプロパティの設定値を変更したときには、管理対象の SMI-S enabled ストレージシステムをリフレッシュする必要があります。

A.2.2 server.http.port

Device Manager サーバが非 SSL で通信する際に使用するポートを指定します。

標準の Web サーバに使用されるポートは通常 80 ですが、このポートですでにイントラネットサーバが稼働しているおそれがあります。ほかのサービスと競合するおそれがあるので、小さい数字のポートは避けてください。通常は、1024~49151 のポートを選択します。

このプロパティにスペースを設定すると、ポートに 80 が割り当てられます。

デフォルト : 2001



注意 このプロパティの値を変更したら、次の設定も変更する必要があります。

- DeviceManager エージェントに登録された Device Manager のポート番号 (hdvماغt_setting コマンド)
- Tiered Storage Manage サーバの hdvm.port プロパティ
- Replication Manager に登録された情報取得元の Device Manager サーバのポート番号 (Device Manager サーバと非 SSL で通信している場合)
- ファイルサーバ管理ソフトウェアに登録された Device Manager サーバのポート番号
- Sun Cluster に登録された Device Manager サーバのポート番号 (管理サーバをクラスタ構成にしている場合)

- 管理クライアントのポップアップブロック設定 (Internet Explorer 6 を使用している場合)
 - Device Manager CLI の HiCommandCLI.properties ファイルの HiCommandCLI.serverurl プロパティ (Device Manager サーバと非 SSL で通信している場合)
-

関連項目

- (6) クラスタリソースの登録 (Sun Cluster の場合)
- 11.3.4 Device Manager サーバの情報, HiScan コマンドの実行周期および RAID Manager または P9000 RAID Manager の情報の設定 (hdvmagt_setting コマンド)
- B.1.1 Tiered Storage Manager サーバのプロパティの変更
- B.5.2 hdvm.port
- ファイルサーバ管理ソフトウェアでのポート番号の変更方法：ファイルサーバのマニュアル

A.2.3 server.https.port

Device Manager サーバが SSL で通信する際に使用するポートを指定します。

セキュア Web サーバ用のポートは通常 443 です。すでにこのポートでセキュアイントラネットサーバが稼働していることがあるため、1024~49151 のポートを専用 (ミドルウェア) HTTP サーバに使用することを推奨します。HTTP リスナー用に指定したポートとは異なる値を割り当ててください。

デフォルト：2443



注意 このプロパティの値を変更したら、次の設定も変更する必要があります。

- Replication Manager に登録された情報取得元の Device Manager サーバのポート番号 (Device Manager サーバと SSL で通信している場合)
 - Sun Cluster に登録された Device Manager サーバのポート番号 (管理サーバをクラスタ構成にしている場合)
 - 管理クライアントのポップアップブロックの設定 (Internet Explorer 6 を使用している場合)
 - Device Manager CLI の HiCommandCLI.properties ファイルの HiCommandCLI.serverurl プロパティ (Device Manager サーバと SSL で通信している場合)
-

関連項目

- (6) クラスタリソースの登録 (Sun Cluster の場合)

A.2.4 server.rmi.port

Device Manager の RMI サーバ機能が使用するポートを指定します。

ほかのサービスと競合するおそれがあるので、小さい数字のポートは避けてください。通常は、1024~65535 のポートを選択します。

デフォルト：23055



注意 このプロパティの値を変更した場合は、Device Manager サーバの client.rmi.port プロパティと Tiered Storage Manager の hdvm.rmi.port プロパティも同じ値に変更してください。

関連項目

- A.7.1 client.rmi.port
- B.5.4 hdvm.rmi.port

A.2.5 server.http.entity.maxLength

Device Manager サーバが許容する HTTP 要求エンティティの最大長をバイト単位で指定します。

通常、この設定を変更する必要はありません。この設定では、異常に大きなデータ量のエンティティを持つ要求を制限することで、サービス妨害攻撃やバッファのオーバーフローをねらった攻撃を防ぐのに役立ちます。Device Manager サーバがこれより長いポスト要求を検出すると、クライアントにエラー応答を送り、その要求の詳細をログに記録します。

デフォルト：1310720



重要 Device Manager に、ファイルシステムやストレージプールなどの数が多いファイルサーバを登録すると、ファイルサーバから送信された情報が Device Manager に正しく反映されないことがあります。その場合は、デフォルトよりも大きな値に変更してください。

A.2.6 server.base.home

Device Manager のインストーラーによって設定される Hitachi Command Suite 共通コンポーネントのインストールディレクトリです。

通常、この設定を変更する必要はありません。

デフォルト：インストーラーによって設定された値

A.2.7 server.horcconfigfile.hostname

Device Manager が構成定義ファイルを編集するときに、IP アドレス (ipaddress) とホスト名 (hostname) のどちらを使用するかを指定します。

デフォルト：ipaddress



注意

- ・ コピーペアを作成したときに設定していた IP アドレス、またはホスト名を変更するとコピーペアの操作ができなくなる場合があります。この場合は、構成定義ファイルの変更やストレージシステムのリフレッシュなどを実行する必要があります。
- ・ このプロパティの設定は Replicaiton Manager では無視されます。Replicaiton Manager で構成定義ファイルを編集するときは、常にホスト名が使用されます。

関連項目

- ・ 1.6.5 コピーペアを管理する場合の注意事項

A.2.8 server.base.initialsynchro

Device Manager の起動時に管理情報データベースと表示情報 (Hitachi Command Suite 共通コンポーネントのリポジトリ) を同期するかどうかを指定します。

true に設定すると、情報が同期されます。false に設定すると、情報は同期されません。

デフォルト：false



注意 このプロパティを true に設定した場合、情報の同期には、数分掛かることがあります。プロパティを変更してすぐに Device Manager にログインしようとする、エラーになる場合があります。この場合は、同期が完了するのを待って、ログインしてください。

A.2.9 server.cim.agent

ストレージシステムの性能情報取得機能を使用する場合に、Device Manager エージェントがインストールされているマシンのホスト名を指定します。

このプロパティを指定しない場合、性能情報は取得できません。

デフォルト：なし

A.2.10 server.cim.support

CIM サポートを有効にするかどうかを指定します。

CIM を実行する場合に、このプロパティを true に設定する必要があります。

デフォルト：true

A.2.11 server.cim.support.job

ボリュームの作成と解除、LUN パスの設定と解除、LUN へのセキュリティの設定と解除、および LUSE の作成と解除などのメソッドを、非同期処理で実行するか、同期処理で実行するかを指定します。

このプロパティを true に設定すると、メソッドは非同期処理で実行され、false に設定すると、同期処理で実行されます。CIM クライアントがジョブ制御のサブプロファイルをサポートしていない場合、false を指定します。

このプロパティに、true または false 以外の文字列を設定した場合、およびこのプロパティが存在しない場合、メソッドは非同期処理で実行されます。

デフォルト：true

A.2.12 server.cim.support.protocol

CIM 機能で使用するポートのオープン/クローズを指定します。

指定できる値の範囲は、1～3 です。指定する値によって、非 SSL 用の通信ポート（デフォルト：5988/tcp）と SSL 用通信ポート（デフォルト：5989/tcp）をオープンするかどうかが変わります。

1：非 SSL 通信用のポートはオープンし、SSL 通信用のポートはクローズします。

2：非 SSL 通信用のポートはクローズし、SSL 通信用のポートはオープンします。

3：非 SSL 通信用のポートと、SSL 通信用のポートの両方がオープンします。

デフォルト：3

関連項目

- [A.2.13 server.cim.http.port](#)
- [A.2.14 server.cim.https.port](#)

A.2.13 server.cim.http.port

CIM 機能で使用する非 SSL 通信用のポートを指定します。

デフォルト：5988



注意 このプロパティの値を変更した場合は、Device Manager サーバの HTTPPort プロパティも同じ値に変更してください。

関連項目

- A.2.12 server.cim.support.protocol
- A.17.2 HTTPPort

A.2.14 server.cim.https.port

CIM 機能で使用する SSL 通信用のポートを指定します。

デフォルト : 5989



注意 このプロパティの値を変更した場合は、Device Manager サーバの HTTPSPort プロパティも同じ値に変更してください。

関連項目

- A.2.12 server.cim.support.protocol
- A.17.3 HTTPSPort

A.2.15 server.configchange.enabled

GUI からラウンチしたストレージ管理ツール (Element Manager) でストレージシステムの構成を変更した際に、データベース上のストレージシステム情報も自動的に更新 (リフレッシュ) するかどうかを指定します。

true を指定すると、Virtual Storage Platform、Universal Storage Platform V/VM、Hitachi USP、SANRISE9900V または HUS VM の場合は、構成変更の直後にデータベース上のストレージシステム情報が自動的にリフレッシュされます。また、HUS100、Hitachi AMS2000、Hitachi SMS、Hitachi AMS/WMS または SANRISE9500V の場合は、次のプロパティに指定した間隔で構成が変更されたかがチェックされ、変更時にはデータベース上のストレージシステム情報が自動的にリフレッシュされます。

HUS100、Hitachi AMS2000 または Hitachi SMS の場合

```
server.dispatcher.snm2.configchange.pollingPeriod プロパティ
```

Hitachi AMS/WMS または SANRISE9500V の場合

```
server.dispatcher.configchange.pollingPeriod プロパティ
```

false を指定した場合は、自動的にリフレッシュされません。

デフォルト : true

関連項目

- A.5.6 server.dispatcher.snm2.configchange.pollingPeriod
- A.5.7 server.dispatcher.configchange.pollingPeriod

A.2.16 server.logicalview.initialsynchro

Device Manager サーバを起動した際に、データベース内のストレージシステムの情報と、GUI や CIM/WBEM 機能で表示する情報を強制的に同期するかどうかを指定します。

true を指定した場合は同期されます。false を指定した場合は同期されません。

デフォルト : false

A.2.17 server.mail.enabled

アラート、イベント、およびヘルスチェック結果をユーザーに E メールで通知するかどうかを指定します。

E メールで通知する場合は true を指定してください。E メールで通知しない場合は false を指定してください。

デフォルト : true



注意 このプロパティに true を設定した場合は、server.mail.smtp.host プロパティも設定してください。

関連項目

- [A.2.19 server.mail.smtp.host](#)

A.2.18 server.mail.from

アラート、イベント、およびヘルスチェック結果をユーザーに E メール通知する場合に、通知元（差出人）のメールアドレスを指定します。

運用環境によっては、ドメイン名がないアドレスからの E メールを受信できないことがあります。プロパティの設定値を変更するか、Eメールの設定（SMTP サーバや通知先のメールフィルターなど）を変更してください。

値を指定していない場合または値が不正であった場合は、デフォルト値が設定されます。

デフォルト : hdvmserver

A.2.19 server.mail.smtp.host

SMTP サーバのホスト名または IP アドレスを指定します。

アラート、イベント、およびヘルスチェック結果をユーザーに E メール通知する場合に、設定が必要です。IP アドレスを指定する場合、IPv4 または IPv6 のどちらかで指定します。

デフォルト : なし



注意 このプロパティを設定した場合は、server.mail.enabled プロパティに true を指定してください。

関連項目

- [A.2.17 server.mail.enabled](#)

A.2.20 server.mail.smtp.port

SMTP サーバのポート番号を指定します。

アラート、イベント、およびヘルスチェック結果をユーザーに E メール通知する場合に、設定が必要です。

指定できる値の範囲は 0～65535 です。

デフォルト：25

A.2.21 server.mail.smtp.auth

アラート、イベント、およびヘルスチェック結果をユーザーに E メール通知する場合に、SMTP 認証を使用するかどうかを指定します。

SMTP 認証を使用する場合は true を指定してください。SMTP 認証を使用しない場合は false を指定してください。

デフォルト：false

A.2.22 server.mail.errorsTo

アラート、イベント、およびヘルスチェック結果の通知メールが配信エラーとなったときに送信される配信不能通知の送信先メールアドレスを指定します。

このプロパティを指定していない場合は、Device Manager サーバの server.properties ファイルの server.mail.from に指定したメールアドレスに送信されます。ただし、配信不能通知が送信される条件は、SMTP サーバの設定によって異なります。SMTP サーバの設定を確認してください。

デフォルト：なし

関連項目

- [A.2.18 server.mail.from](#)

A.2.23 server.eventNotification.mail.to

アラートおよびイベントの通知メールの送信先メールアドレスを指定します。

このプロパティに設定するメールアドレスには、すべてのアラートおよびイベントについて、E メール通知されます。

デフォルト：なし

A.2.24 server.mail.alert.type

アラートをユーザーに E メール通知する場合に、通知するアラートのタイプを指定します。

指定できる値は次のとおりです。

- Trap：SNMP トラップで検知した障害情報だけを通知します。
- Server：Device Manager による定期監視で検知した障害情報だけを通知します。
- All：SNMP トラップで検知した障害情報と、Device Manager による定期監視で検知した障害情報の両方を通知します。同じ障害であっても、SNMP トラップで検知した障害情報と Device Manager による定期監視で検知した障害情報の両方について、それぞれ E メールが送信されます。

デフォルト：Trap

A.2.25 server.mail.alert.status

アラートをユーザーに E メール通知する場合に、通知するアラートの重要度を指定します。

Device Manager サーバはこのプロパティで指定した重要度以上のアラートを通知します。指定できる値は、重要度の低い順に、Normal, Service, Moderate, Serious, Acute です。

デフォルト : Moderate

A.2.26 server.subsystem.ssid.availableValues

Device Manager にストレージシステムを登録する際、ストレージシステムに対して自動的に設定する SSID の値の範囲を指定します。

このプロパティは、Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, SANRISE9900V および HUS VM で有効です。

指定できる値は次のとおりです。

- 4~FFFD の 16 進数 : 連続した複数の値を指定する場合は、ハイフン (-) で範囲を指定します。連続していない複数の値を指定する場合は、コンマ (,) で区切って指定します。大文字小文字は区別されません。範囲が重複して指定されている場合、その論理和を指定値とします。
- All : All を指定すると、指定できる全範囲を指定することになります。大文字小文字は区別されません。

値を指定しない場合、SSID の自動設定は行いません。

デフォルト : All

A.2.27 server.smisclient.indication.port

SMI-S プロバイダーからインディケーション通知を受信する際に使用するポート番号を指定します。

指定できる値の範囲は、1024~49151 です。

このプロパティの設定値を変更した場合、Device Manager で管理している SMI-S enabled ストレージシステムをリフレッシュする必要があります。

デフォルト : 5983

A.2.28 server.agent.differentialrefresh.manual.enabled

ストレージシステムの手動リフレッシュ時に、前回のリフレッシュ時点から構成に変化があったリソースについてだけ、データベースの情報を更新するかどうかを指定します。

このプロパティは、リフレッシュ対象のストレージシステムが Virtual Storage Platform または HUS VM の場合だけ有効です。

true を指定した場合、前回のリフレッシュ時点から構成に変化がないリソースについてはデータベースの更新が省略されるため、リフレッシュ処理を効率化できます。

構成が変化したかどうかに関わらず、ストレージシステム上のすべてのリソースの情報をデータベースに反映する場合には、false を指定します。

デフォルト : true

A.2.29 server.agent.differentialrefresh.periodical.enabled

ストレージシステムの自動リフレッシュ時に、前回のリフレッシュ時点から構成に変化があったリソースについてだけ、データベースの情報を更新するかどうかを指定します。

このプロパティは、リフレッシュ対象のストレージシステムが Virtual Storage Platform または HUS VM の場合だけ有効です。

true を指定した場合、前回のリフレッシュ時点から構成に変化がないリソースについてはデータベースの更新が省略されるため、リフレッシュ処理を効率化できます。

構成が変化したかどうかに関わらず、ストレージシステム上のすべてのリソースの情報をデータベースに反映する場合には、false を指定します。

デフォルト : true

A.2.30 server.logicalGroupMapping.updateInterval

ヘルスチェックの際に論理グループのボリューム構成情報の取得処理を省略する場合に、その期間を指定します (分単位)。

デフォルトでは、常に最新のボリューム構成情報を基に論理グループのヘルスチェックレポートが作成されます。Device Manager 管理下のボリューム数が多い場合は、論理グループのボリューム構成情報の取得処理に時間が掛かることがあります。論理グループのボリューム構成が頻繁に変わらない環境では、この処理を省略し、前回取得したボリューム構成情報を基にヘルスチェックを実施することで、レポート作成に掛かる時間を短縮できます。

このプロパティはデフォルトでは存在しないため、次の形式で指定してください。

```
server.logicalGroupMapping.updateInterval=<時間>
```

ヘルスチェック後、指定した期間が経過するまでは、その期間内に実行されたヘルスチェックでは、前回取得したボリューム構成情報を基にレポートが作成されます。

A.3 Device Manager のデータベースに関するプロパティ (database.properties ファイル)

データベースに関するプロパティは、database.properties ファイルに含まれています。

- Windows の場合 :
< Device Manager サーバのインストールフォルダ >¥HiCommandServer¥config
¥database.properties
- Solaris または Linux の場合 :
< Device Manager サーバのインストールディレクトリ > /HiCommandServer /config/
database.properties

このプロパティファイルには、Device Manager サーバのデータベースとの接続の確立に関する設定が含まれています。Device Manager サーバを稼働する前には、これらの設定を正しく入力し、Database Management System (DBMS) を起動する必要があります。サーバが DBMS に接続できない場合には、エラーログにエントリが書き込まれます (デフォルトディレクトリは、logs ディレクトリ)。この情報は、新規インストールのトラブルシューティング時に役立ちます。

A.3.1 dbm.traceSQL

SQL をトレースログに出力するかどうかを指定します。

true を設定すると、SQL を出力します。false を設定すると、SQL を出力しません。

デフォルト : false

A.3.2 dbm.startingCheck.retryCount

Device Manager サーバの起動時に、DBMS の起動確認をリトライする回数を指定します。

指定できる値の範囲は、0~100 です。通常、この設定を変更する必要はありません。

デフォルト : 18

A.3.3 dbm.startingCheck.retryPeriod

Device Manager サーバの起動時に、DBMS の起動確認をリトライする間隔を秒単位で指定します。

指定できる値の範囲は、0~60 (秒) です。通常、この設定を変更する必要はありません。

デフォルト : 10 (秒)

A.4 Device Manager のログ出力に関するプロパティ (logger.properties ファイル)

ログ出力に関するプロパティは、logger.properties ファイルに含まれています。

- Windows の場合 :
< Device Manager サーバのインストールフォルダ >¥HiCommandServer¥config
¥logger.properties
- Solaris または Linux の場合 :
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/config/
logger.properties

このプロパティファイルには、各種ログファイルの操作およびエラーログの名前、場所、および出力レベルなど、Device Manager サーバのロギングモジュールを構成する設定一式が含まれています。また、このファイルを使用して、デバッグおよび診断を目的としたトレースロギングを構成することもできます。

A.4.1 logger.loglevel

trace.log, error.log, CIMOMTrace.log および SMISClientTrace.log の出力レベルを指定します。

このフィールドで使用できる値は、詳細度が高い順に DEBUG, INFO, WARN, ERROR, および FATAL です。デフォルト値の場合、INFO, WARN, ERROR, および FATAL のエントリーが trace.log に出力されます。この場合、DEBUG のエントリーはログに出力されません。

デフォルト : INFO

A.4.2 logger.MaxBackupIndex

access.log, cim_access.log, error.log, service.log, stdout.log, stderr.log, statuscheck.log, trace.log, CIMOMTrace.log および SMISClientTrace.log の最大バックアップ数を指定します。

ログファイルが `logger.MaxFileSize` プロパティで指定された最大長に達すると、`access.log.1` のようにカウンターが追加された形式にファイル名が変更されます。ログファイルがさらに作成されると、指定された数のバックアップログファイルが作成されるまで、カウンターが増加していきます（例えば、`access.log.1` は `access.log.2` になります）。指定された数のバックアップログファイルが作成されたあとは、新しいバックアップログファイルが作成されるたびに、最も古いバックアップログファイルが削除されます。

指定できる値の範囲は、1～20 です。

デフォルト：10

関連項目

- [A.4.3 logger.MaxFileSize](#)

A.4.3 logger.MaxFileSize

`access.log`, `cim_access.log`, `error.log`, `service.log`, `stdout.log`, `stderr.log`, `statuscheck.log`, `trace.log`, `CIMOMTrace.log` および `SMISClientTrace.log` の最大サイズを指定します。

ログファイルのサイズが指定値を超えた場合は、新しいログファイルが作成されます。キロバイト単位の場合は **KB**、メガバイト単位の場合は **MB** と指定しないかぎり、指定したサイズはバイト単位であると見なされます。

指定できる値の範囲は、512KB～32MB です。

デフォルト：1MB

A.4.4 logger.hicommandbase.loglevel

Hitachi Command Suite 共通コンポーネントによって `HDvMtracen.log`, `HDvMGuiTracen.log` および `HDvMGuiMessage n .log` (n はファイルのバックアップ数を表す整数です) に書き込まれる操作（トレース）およびエラーログの出力レベルを指定します。

各ロギングイベントには、そのタイプ（エラー、警告、および情報）とは無関係に独自の出力レベルがあります。使用できるレベルは、重要度が低い順に 30, 20, 10, および 0 です。プロダクションシステムのデフォルトのログ出力レベルは、20 です。これは、ロギングイベントレベル 20, 10, および 0 のメッセージは `HDvMtrace1.log` に書き込まれますが、ロギングイベントレベル 30 のメッセージは書き込まれないことを意味します。

デフォルト：20

A.4.5 logger.hicommandbase.sysloglevel

Hitachi Command Suite 共通コンポーネントによってイベントログ（Windows）または `syslog`（Solaris または Linux）に書き込まれるトレースログとエラーログの出力レベルを指定します。

各ロギングイベントには、そのタイプ（エラー、警告、および情報）とは無関係に独自の出力レベルがあります。使用できるレベルは、重要度が低い順に 30, 20, 10, および 0 です。プロダクションシステムのデフォルトのログ出力レベルは、0 です。これは、ロギングイベントレベル 0 のメッセージだけがイベントログ（Windows）または `syslog`（Solaris または Linux）に書き込まれ、ロギングイベントレベル 30, 20, および 10 のメッセージは書き込まれないことを意味します。通常は、デフォルト値の使用を推奨します。

デフォルト：0

A.4.6 logger.hicommandbase.MaxBackupIndex

Hitachi Command Suite 共通コンポーネントによって HDvMtracen.log, HDvMGuiTracen.log および HDvMGuiMessagen.log に書き込まれる操作（トレース）およびエラーログの最大バックアップ数を指定します（*n* はファイルのバックアップ数を表す整数です）。

ログファイルが logger.hicommandbase.MaxFileSize プロパティで指定されたサイズに達すると、HDvMtrace2.log のようにカウンターが追加されたファイルが作成されます。ログファイルの数がこのプロパティで指定した値に達すると、最も古いファイルから上書きされます。

指定できる値の範囲は、1～16 です。

デフォルト：10

関連項目

- [A.4.7 logger.hicommandbase.MaxFileSize](#)

A.4.7 logger.hicommandbase.MaxFileSize

Hitachi Command Suite 共通コンポーネントによって HDvMtracen.log, HDvMGuiTracen.log および HDvMGuiMessagen.log に書き込まれる操作（トレース）およびエラーログの最大サイズを指定します（*n* はファイルのバックアップ数を表す整数です）。

キロバイト単位の場合は KB, メガバイト単位の場合は MB, ギガバイトの場合は GB と指定しないかぎり、指定したサイズはバイト単位であると見なされます。

有効な値は、4096～2147483647（2GB 未満）です。

デフォルト：5MB

A.5 Device Manager のスレッドに関するプロパティ (dispatcher.properties ファイル)

スレッドに関するプロパティは、dispatcher.properties ファイルに含まれています。

- Windows の場合：
< *Device Manager* サーバのインストールフォルダ >¥HiCommandServer¥config
¥dispatcher.properties
- Solaris または Linux の場合：
< *Device Manager* サーバのインストールディレクトリ > /HiCommandServer/config/
dispatcher.properties

このプロパティファイルには、Device Manager サーバのディスパッチャーレイヤーの操作を構成する設定一式が含まれています。例えば、各種バックグラウンドプロセス（デーモン）の微調整やサービスエージェントに対するスレッド優先度の最適化などをするプロパティがあります。

A.5.1 server.dispatcher.message.timeout

保留されている応答メッセージが期限切れになる（ページされる）までのタイムアウトを分単位で指定します。

保留メッセージには、クライアントによるポーリングおよび Device Manager 通知サービスを介したクライアントへの送信がまだ行われていない長期実行プロセス（ストレージシステムの追加など）からの応答があります。

デフォルト：15（分）

A.5.2 server.dispatcher.message.timeout.in.processing

何らかの理由で完了していない GUI や CLI の処理のタイムアウト時間を分単位で指定します。

デフォルト：720（分）

A.5.3 server.dispatcher.daemon.pollingPeriod

コンポーネント状態と構成バージョンを確認するバックグラウンドのスレッドのポーリング間隔を分単位で指定します。

0 を指定すると、ポーリングは無効になります。

デフォルト：5（分）



注意 HUS100, Hitachi AMS2000 または Hitachi SMS の場合、ポーリングの実行時に、ストレージシステムの I/O 性能に影響が出る場合があります。影響を少なくしたい場合は、ポーリング間隔を大きくするか、ポーリングを無効にしてください。

A.5.4 server.dispatcher.traps.purgePeriod

古くなった SNMP トラップまたはアラートのパージ間隔を分単位で指定します。

0 を指定すると、サーバからのトラップのパージが無効になります。

デフォルト：5（分）

A.5.5 server.dispatcher.daemon.receiveTrap

ストレージシステムやスイッチなどのネットワークリソースで出力された SNMP トラップを Device Manager で受信するかどうかを指定します。

受信する場合は true を、受信しない場合は false を指定してください。

SNMP トラップの受信には 162/udp が使用されます。Hitachi Command Suite を新規インストールした際に 162/udp が使用されていない場合は、自動的に true が設定されます。

デフォルト：true

A.5.6 server.dispatcher.snm2.configchange.pollingPeriod

GUI からラウンチされた Storage Navigator Modular 2 で、HUS100, Hitachi AMS2000 または Hitachi SMS の構成が変更されたかどうかを、Device Manager サーバがチェックする間隔を秒単位に指定します。

server.configchange.enabled プロパティに true が設定されていると、Device Manager サーバがストレージシステムの構成変更を検知した場合には、データベース上のストレージシステム情報が自動的に更新（リフレッシュ）されます。

指定できる範囲は、0～3600（秒）です。0 を指定した場合は、ストレージシステムの構成が変更されても、Device Manager サーバは検知できないため、データベース上のストレージシステム情報はリフレッシュされません。

デフォルト：300（秒）

関連項目

- [A.2.15 server.configchange.enabled](#)

A.5.7 server.dispatcher.configchange.pollingPeriod

Element Manager で SANRISE9500V または Hitachi AMS/WMS の構成が変更されたかどうかを、Device Manager サーバがチェックする間隔を秒単位に指定します。

server.configchange.enabled プロパティに true が設定されていると、Device Manager サーバがストレージシステムの構成変更を検知した場合には、データベース上のストレージシステム情報が自動的に更新（リフレッシュ）されます。

指定できる範囲は、0～3600（秒）です。0 を指定した場合は、ストレージシステムの構成が変更されても、Device Manager サーバは検知できないため、データベース上のストレージシステム情報はリフレッシュされません。

デフォルト：60（秒）

関連項目

- [A.2.15 server.configchange.enabled](#)

A.5.8 server.dispatcher.daemon.configUpdate.detection.interval

Virtual Storage Platform, Universal Storage Platform V/VM または HUS VM の構成が Device Manager 以外のストレージ管理ツール（RAID Manager や SVP など）で変更されたかどうかを、Device Manager サーバがチェックする間隔を分単位で指定します。

Virtual Storage Platform, Universal Storage Platform V/VM または HUS VM の構成変更を Device Manager サーバが検知した場合には、Device Manager の GUI に警告メッセージが表示されます。

指定できる範囲は 0～1440（分）です。0 を指定した場合、Device Manager サーバは、Virtual Storage Platform, Universal Storage Platform V/VM または HUS VM の構成が変更されたかどうかをチェックしません。

デフォルト：10（分）



注意

- GUI に警告メッセージが表示されていた場合は、該当するストレージシステムの情報を手動でリフレッシュしてください。

なお、ストレージシステムの構成変更後にユーザーが手動でリフレッシュを実行し忘れた場合に備えて、データベース上の情報が自動的に更新されるよう設定することもできます。次のプロパティを設定してください。

server.dispatcher.daemon.autoSynchro.doRefresh プロパティ

server.dispatcher.daemon.autoSynchro.type プロパティ

- Device Manager サーバでは、次の構成変更については検知できません。
 - LDEV の状態（正常や閉塞、コピー中など）が変更される
 - コピーペアを作成、変更または削除するまた、Universal Storage Platform V/VM で LDEV のアクセス属性（Read/Write や Read Only, Protect など）を変更した場合も検知できません。
- Device Manager サーバでは、次の契機にもストレージシステムの構成が変更されたものとして扱われます。
 - SVP を再起動する
 - Storage Navigator に表示されているストレージシステムの構成情報を更新する

- ・ クラスタ構成の SVP を、実行系から待機系、または待機系から実行系に切り替える
- ・ DKC の電源を入れる
- ・ DP プールの構成が変更される※
- ・ Copy-on-Write Snapshot または Thin Image のデータプールの構成が変更される※

注※

Virtual Storage Platform または HUS VM の場合、
`server.dispatcher.daemon.configUpdate.detection.variable.enabled` プロパティを
`false` にすると、プールの構成変更については Device Manager の GUI に警告メッセージが表示されない
ようになります。

関連項目

- ・ [A.5.9 server.dispatcher.daemon.autoSynchro.doRefresh](#)
- ・ [A.5.10 server.dispatcher.daemon.autoSynchro.type](#)
- ・ [A.5.14 server.dispatcher.daemon.configUpdate.detection.variable.enabled](#)

A.5.9 server.dispatcher.daemon.autoSynchro.doRefresh

Device Manager サーバが Virtual Storage Platform, Universal Storage Platform V/VM または HUS VM の構成が変更されていることを検知した場合に、データベース上のそのストレージシステムの情報を自動的にリフレッシュするかどうかを指定します。

`true` を指定した場合、Device Manager サーバが検知したあと、ユーザーが手動でリフレッシュしなかったときには、`server.dispatcher.daemon.autoSynchro.type` プロパティに指定された周期でデータベース上の Virtual Storage Platform, Universal Storage Platform V/VM または HUS VM の情報が自動的にリフレッシュされます。`false` を指定した場合は、自動的にリフレッシュされません。

デフォルト : `true`



注意 `true` を指定した場合、Virtual Storage Platform, Universal Storage Platform V/VM または HUS VM の情報だけがデータベースに反映されます。Virtual Storage Platform, Universal Storage Platform V/VM または HUS VM のコマンドデバイスを認識しているホストの構成定義ファイルの情報は反映されません。

関連項目

- ・ [A.5.10 server.dispatcher.daemon.autoSynchro.type](#)

A.5.10 server.dispatcher.daemon.autoSynchro.type

データベース上のストレージシステム情報を自動的に更新 (リフレッシュ) する周期を次のどれかの形式で指定します。

H : 一定の時間ごとに自動リフレッシュする場合に指定します。

`server.dispatcher.daemon.autoSynchro.interval` プロパティで間隔を指定してください。

D : 1 日に 1 回、特定の時刻に自動リフレッシュする場合に指定します。

`server.dispatcher.daemon.autoSynchro.startTime` プロパティで時刻を指定してください。

W : 週に 1 回、特定の曜日の特定の時刻に自動リフレッシュする場合に指定します。

`server.dispatcher.daemon.autoSynchro.dayOfWeek` プロパティで曜日を、
`server.dispatcher.daemon.autoSynchro.startTime` プロパティで時刻を指定してください。

このプロパティは、`server.dispatcher.daemon.autoSynchro.doRefresh` プロパティで `true` を指定した場合にだけ有効になります。

デフォルト：D

関連項目

- [A.5.9 server.dispatcher.daemon.autoSynchro.doRefresh](#)
- [A.5.11 server.dispatcher.daemon.autoSynchro.dayOfWeek](#)
- [A.5.12 server.dispatcher.daemon.autoSynchro.startTime](#)
- [A.5.13 server.dispatcher.daemon.autoSynchro.interval](#)

A.5.11 server.dispatcher.daemon.autoSynchro.dayOfWeek

データベース上のストレージシステム情報を自動的に更新（リフレッシュ）する曜日を次のどれかの形式で指定します。

Sun Mon Tue Wed Thu Fri Sat

このプロパティは `server.dispatcher.daemon.autoSynchro.type` プロパティで `w` を指定した場合にだけ有効になります。また、管理サーバのタイムゾーンの設定に従って、自動リフレッシュが実行されます。

デフォルト：Fri

関連項目

- [A.5.10 server.dispatcher.daemon.autoSynchro.type](#)

A.5.12 server.dispatcher.daemon.autoSynchro.startTime

データベース上のストレージシステム情報の自動更新（リフレッシュ）を開始する時刻を「`hh:mm`」の形式で指定します。

`hh` は 00～23 の範囲で、`mm` は 00～59 の範囲で指定します。このプロパティは `server.dispatcher.daemon.autoSynchro.type` プロパティで `D` または `w` を指定した場合にだけ有効になります。また、管理サーバのタイムゾーンの設定に従って、自動リフレッシュが実行されます。

デフォルト：23:00

関連項目

- [A.5.10 server.dispatcher.daemon.autoSynchro.type](#)

A.5.13 server.dispatcher.daemon.autoSynchro.interval

データベース上のストレージシステム情報を自動的に更新（リフレッシュ）する間隔を時間単位で指定します。

指定できる範囲は 1～24（時間）です。

このプロパティは `server.dispatcher.daemon.autoSynchro.type` プロパティで `H` を指定した場合にだけ有効になります。

デフォルト：24（時間）

関連項目

- [A.5.10 server.dispatcher.daemon.autoSynchro.type](#)

A.5.14

server.dispatcher.daemon.configUpdate.detection.variable.enabled

Device Manager サーバが Virtual Storage Platform または HUS VM の構成が変更されているかどうかをチェックする際に、DP プールや Copy-on-Write Snapshot のデータプールの利用率など、値が逐次変化する項目についても監視対象にするかどうかを指定します。

true を指定した場合は、監視対象になり、値の変化を検知した際には Device Manager の GUI に警告メッセージが表示されます。false を指定した場合、次の変更については監視対象にはならないで、警告メッセージも表示されません。

- 次のボリュームの利用率の変化
 - HDP ボリューム
 - HDP プール
 - HDT プール
 - Copy-on-Write Snapshot のデータプール
 - Thin Image のデータプール
- 次のボリュームの利用率の閾値の変更
 - HDP プール
 - HDT プール
 - Copy-on-Write Snapshot のデータプール
 - Thin Image のデータプール
- 次のボリュームの最大予約容量の変更
 - HDP プール
 - HDT プール
 - Copy-on-Write Snapshot のデータプール
 - Thin Image のデータプール
- HDT プールのモニタリングモードの変更
- HDT プールの性能モニタリングと階層再配置に関する設定変更
- HDT ボリュームの階層ポリシーに関する設定変更
HDT ボリュームとは、HDT プールから作成 (HDT プールと関連づけ) する仮想ボリュームです。

なお、このプロパティは、

server.dispatcher.daemon.configUpdate.detection.interval プロパティで 0 以外を指定した場合にだけ有効になります。

デフォルト : false

関連項目

- [A.5.8 server.dispatcher.daemon.configUpdate.detection.interval](#)

A.5.15 server.dispatcher.daemon.autoSynchro.performance.doRefresh

[モビリティ] タブに表示される性能情報を自動的に更新（リフレッシュ）するかどうかを指定します。

true を指定した場合、htnm.infoAcquirePeriod プロパティに指定した周期で、server.dispatcher.daemon.autoSynchro.performance.startTime プロパティに指定した時刻に自動リフレッシュされます。

false を指定した場合、自動的にリフレッシュされません。性能情報をリフレッシュしたい場合は、次のどちらかの方法を実行します。

- GUI の場合
[ストレージシステム更新] 画面で、[性能情報を更新する] チェックボックスをチェックして、ストレージシステムをリフレッシュします。
- CLI の場合
RefreshPerformanceData コマンドを実行します。

デフォルト：true

関連項目

- [A.5.16 server.dispatcher.daemon.autoSynchro.performance.startTime](#)
- [A.14.1 htnm.infoAcquirePeriod](#)

A.5.16 server.dispatcher.daemon.autoSynchro.performance.startTime

[モビリティ] タブに表示される性能情報を更新する時刻を「*hh:mm*」の形式で指定します。

hh は 00～23 の範囲で、*mm* は 00～59 の範囲で指定します。このプロパティは、server.dispatcher.daemon.autoSynchro.performance.doRefresh プロパティで true を指定した場合にだけ有効になります。

デフォルト：00:10

関連項目

- [A.5.15 server.dispatcher.daemon.autoSynchro.performance.doRefresh](#)

A.5.17

server.dispatcher.daemon.autoSynchro.logicalGroup.doRefresh

論理グループの情報を自動的に更新するかどうかを指定します。

true を指定すると、次のタイミングで自動的に更新されます。

- ストレージシステムの登録
- ストレージシステムのリフレッシュ
- ストレージシステムの削除
- 性能情報の自動更新 (htnm.infoAcquirePeriod で指定した周期)
- 論理グループの作成および編集
- ユーザーグループの作成、編集および削除
- リソースグループの編集および削除

なお、論理グループの情報が自動的に更新されるのは、上記の操作を GUI で実行した場合だけです。

true を指定しても上記の操作を CLI で実行した場合、または false を指定した場合、論理グループの情報は自動的に更新されません。情報を更新する場合は、[モビリティ] タブの [論理グループ] で論理グループを選択し、[データ更新] ボタンをクリックしてください。

デフォルト : true

関連項目

- A.14.1 htnm.infoAcquirePeriod

A.6 Device Manager の MIME に関するプロパティ (mime.properties ファイル)

MIME に関するプロパティは、mime.properties ファイルに含まれています。

- Windows の場合 :
< *Device Manager* サーバのインストールフォルダ > %HiCommandServer%\config
mime.properties
- Solaris または Linux の場合 :
< *Device Manager* サーバのインストールディレクトリ > /HiCommandServer/config/
mime.properties

このプロパティファイルには、Device Manager サーバによって認識されるすべての MIME タイプの翻訳/検索テーブルが含まれています。検索テーブル内の各プロパティは、特定の拡張子をそのファイルの MIME タイプに割り当てます。通常、この設定を変更する必要はありません。また、このファイルへの追加は、専門知識のあるシステム管理者だけがするようにしてください。

A.7 Device Manager の GUI に関するプロパティ (client.properties ファイル)

GUI に関するプロパティは、client.properties ファイルに含まれています。

- Windows の場合 :
< *Device Manager* サーバのインストールフォルダ > %HiCommandServer%\config
client.properties
- Solaris または Linux の場合 :
< *Device Manager* サーバのインストールディレクトリ > /HiCommandServer/config/
client.properties

このプロパティファイルには、Device Manager の GUI の表示および操作に関する設定が含まれています。

A.7.1 client.rmi.port

Device Manager の RMI サーバのポート番号を指定します。

Device Manager サーバの server.rmi.port プロパティに指定した値と同じ値を指定する必要があります。

デフォルト : 23055

関連項目

- A.2.4 server.rmi.port

A.7.2 client.migration.use.legacymode

Tiered Storage Manager GUI から、バージョン 7.1.0 以前に作成したマイグレーショングループを使ったマイグレーションを実行するかどうかを指定します。

マイグレーショングループを使ったマイグレーションを実行する場合は、true を指定します。true を指定すると、[ツール] - [Legacy Tiered Storage Manager] から、マイグレーショングループを使ったマイグレーション用の画面 (Legacy モードの GUI) を起動できるようになります。

false を指定した場合、マイグレーショングループを使ったマイグレーションは Tiered Storage Manager GUI からできません。

デフォルト : false



参考

- バージョン 7.1.1 以降では、マイグレーション前に移動元のボリュームをマイグレーショングループとして定義する必要がなくなりました。
- true を指定した場合でも、[よく使うタスク] や [モビリティ] タブなどで [データマイグレーション] を選択すると、マイグレーションウィザードで移動元と移動先のボリュームを直接指定してマイグレーションできます。
- true と false のどちらかを指定しても、Tiered Storage Manager CLI からはマイグレーショングループを使ったマイグレーションができます。



注意 このプロパティが false の場合、マイグレーショングループを使って作成したマイグレーションタスクは、[タスク&アラート] タブの [タスク一覧] で参照・操作できません。そのため、プロパティを true から false に変更する場合は、未完了のマイグレーションタスクが残っていないか確認してください。残っている場合は、次のどちらかの方法でタスクを終了させてください。

- タスクを即時実行する
- タスクをキャンセルし、プロパティを false に変更したあと、[データマイグレーション] ウィザードでタスクを再作成する

A.8 Device Manager のセキュリティに関するプロパティ

このマニュアルでは、以下の内容は、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制により非公開となっています。以下の内容については、製品に付属するマニュアルをご覧ください。

A.9 Device Manager の SNMP トラップのログ出力に関するプロパティ (customizedsnmptrap.properties ファイル)

SNMP トラップのログ出力に関するプロパティは、customizedsnmptrap.properties ファイルに含まれています。

- Windows の場合 :

< Device Manager サーバのインストールフォルダ >¥HiCommandServer¥config
¥customizedsnmptrap.properties

- Solaris または Linux の場合 :

< Device Manager サーバのインストールディレクトリ >/HiCommandServer/config/
customizedsnmptrap.properties

A.9.1 customizedsnmptrap.customizedSNMPTrapEnable

Device Manager で受信した SNMP トラップをログファイルに出力するかどうかを指定します。

出力する場合は true, 出力しない場合は false を指定します。

true を指定した場合は, customizedsnmptrap.customizelist プロパティも設定してください。

デフォルト : false



重要 server.dispatcher.daemon.receiveTrap プロパティに true を指定している場合, 同じ事象に関するストレージシステムの SNMP トラップについては, ログファイルに二重に出力されることがあります。

関連項目

- A.5.5 server.dispatcher.daemon.receiveTrap

A.9.2 customizedsnmptrap.customizelist

Device Manager で受信した SNMP トラップをログファイルに出力する際の重要度や出力形式を指定します。

customizedsnmptrap.customizelist プロパティの指定形式を次に示します。

```
customizedsnmptrap.customizelist = ¥  
< EnterpriseID1 > : < 一般トラップ番号 1 > : < 固有トラップ番号 1 > : < 重要度 1 > : < 出力内容 1 > , ¥  
< EnterpriseID2 > : < 一般トラップ番号 2 > : < 固有トラップ番号 2 > : < 重要度 2 > : < 出力内容 2 > , ¥  
...  
< EnterpriseIDn > : < 一般トラップ番号 n > : < 固有トラップ番号 n > : < 重要度 n > : < 出力内容 n >
```

表 A-2 customizedsnmptrap.customizelist プロパティで指定する項目

項目	形式	説明
EnterpriseID	ドット表現 (例) .1.3.6.1.4.116.3.11.1.2	省略できません。
一般トラップ番号	0~6 の数値	省略できません。
固有トラップ番号	数値	省略できません。
重要度	次に示すどれかの文字列で各トラップの重要度を指定します。 次に示す文字列以外は指定できません。 <ul style="list-style-type: none">• Information• Warning• Error• Critical• Alert• Null	省略できます。省略時は Null を指定したと見なされます。 メッセージ ID のインジケータは次のとおり出力されます。 <ul style="list-style-type: none">• Information : -I• Warning : -W• Error/Critical/Alert : -E• Null : ログを出力しない
出力内容	次の文字列 (変数) で出力内容を指定します。	省略できます。省略時は \$a\$e\$g\$s の内容が出力されます。

項目	形式	説明
	次に示す文字列以外は指定できません。 <ul style="list-style-type: none"> • \$a • \$e • \$g • \$s • \$n (n=1以上の整数) 	重要度に Null を指定した場合この項目への指定は無効になります。各変数の出力内容は次のとおりです。 <ul style="list-style-type: none"> • \$a: エージェントアドレス (ドット形式) • \$e: EnterpriseID (ドット形式) • \$g: 一般トラップ番号 • \$s: 固有トラップ番号 • \$n (n=1以上の整数): n 番目のバリエーションの値

- 項目を省略した場合でも、区切り文字のコロン (:) は入力してください。
- 複数の定義を指定する場合、コンマ (,) を区切り文字として使用してください。ただし、最後のエントリーの終わりにはコンマ (,) を入力しないでください。
- 途中で改行したい場合は、その行の終わりに円記号 (¥) を入力してください。円記号 (¥) のあとの改行は無視されます。

customizedsnmptrap.customizelist プロパティの指定例を、次に示します。

```
customizedsnmptrap.customizelist = ¥
.1.2.3:6:1:Information:$a$e$g$s$1$2, ¥
.1.3.6.1.4.1.2854:6:1:Warning:$e$a$s$3$2$1$g, ¥
.1.3.6.1.4.1.116.3.11.4.1.1:6:1:Error:$a$s, ¥
.1.3.6.1.4.1.116.3.11.4.1.1:6:100:Information:$a$s
```

デフォルト: なし



注意 このプロパティが指定されていない場合、customizedsnmptrap.customizedSNMPTrapEnable プロパティに true が設定されていても、SNMP トラップの情報はログに出力されません。

関連項目

- [A.9.1 customizedsnmptrap.customizedSNMPTrapEnable](#)

A.10 Device Manager からラUNCHするアプリケーションに関するプロパティ (launchapp.properties ファイル)

ラUNCHするアプリケーションに関するプロパティは、launchapp.properties ファイルに含まれています。

- Windows の場合 :
`<Device Manager サーバのインストールフォルダ>¥HiCommandServer¥config¥launchapp.properties`
- Solaris または Linux の場合 :
`<Device Manager サーバのインストールディレクトリ>/HiCommandServer/config/launchapp.properties`

このプロパティファイルには、ラUNCHされるアプリケーションがインストールされているサーバの情報が含まれています。

A.10.1 launchapp.snm2.url

クライアントの Web ブラウザーからラUNCH実行する Storage Navigator Modular 2 の Web サーバの URL を指定します。

このプロパティは、対象のストレージシステムが SANRISE9500V および Hitachi AMS/WMS の場合に指定します。

次に、Storage Navigator Modular 2 の Web サーバの URL を指定した例を示します。

```
launchapp.snm2.url=http://192.168.17.235:23015/program/StorageNavigatorModular/applet
```

デフォルト：なし



注意

- IPv6 アドレスは使用できません。IPv6 環境ではホスト名で指定してください。
- 管理サーバに NIC が複数搭載されている場合、URL 内の IP アドレスには、管理クライアント (GUI) が接続されているネットワーク側の IP アドレスを指定してください。ホスト名は指定しないでください。

A.10.2 launchapp.snm2.rmi.port

Storage Navigator Modular 2 で、RMI の通信に使用するポート番号を変更した場合、このプロパティに変更後のポート番号を指定します。

変更後のポート番号を指定しないと、Device Manager は Storage Navigator Modular 2 との連携ができません。有効な値は、1～65535 です。

このプロパティは、対象のストレージシステムが、SANRISE9500V および Hitachi AMS/WMS の場合に指定します。

Storage Navigator Modular (for Web) と同じマシン上で動作させる場合、Storage Navigator Modular (for Web) と Storage Navigator Modular 2 の RMI の通信に使用するポート番号には、同じ番号を指定しないでください。

デフォルト：なし

関連項目

- Storage Navigator Modular 2 で設定した通信用ポート番号の参照方法および変更方法：
Storage Navigator Modular 2 のマニュアル

A.10.3 launchapp.elementmanager.role.mode

Element Manager を使用して、ストレージシステムのユーザーアカウントおよび監査ログを管理できる Device Manager のユーザーの権限を指定します。

指定できる値は 0 または 1 です。指定する値によって、Element Manager でストレージシステムのユーザーアカウントおよび監査ログを管理できる Device Manager のユーザーの権限が次のとおり変わります。

0：Admin または Modify 権限を持つユーザーだけが管理できます。

1：Admin 権限を持つユーザーだけが管理できます。

デフォルト：0



注意 HUS100, Hitachi AMS2000, Hitachi SMS, および Hitachi AMS/WMS の場合は, Account Authentication が有効である必要があります。

A.10.4 launchapp.elementmanager.usehostname

Element Manager をラウンチしてエンタープライズクラスストレージまたは HUS VM に接続する場合, Element Manager の URL にホスト名を表示するかどうかを指定します。

true を指定すると, 対象のストレージシステムをホスト名で指定して Device Manager に登録した場合, Element Manager の URL にホスト名を表示します。false を指定した場合, Element Manager の URL に IP アドレスを表示します。

デフォルト: true

A.11 ホストとの通信に関するプロパティ (host.properties ファイル)

ホストとの通信に関するプロパティは, host.properties ファイルに含まれています。

- Windows の場合 :
< Device Manager サーバのインストールフォルダ > %HiCommandServer%\config
%host.properties
- Solaris または Linux の場合 :
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/config/
host.properties

A.11.1 host.mf.agent.connection.timeout

Device Manager サーバが, Mainframe Agent との通信処理をタイムアウトするまでの時間を秒単位で指定します。

有効な値は, 0, 30~3600 (秒) です。0 を指定した場合, タイムアウトしません。専門知識のあるシステム管理者が, Mainframe Agent に対して, パフォーマンスを微調整する場合だけ, この設定を変更してください。

デフォルト: 300

A.11.2 host.agent.access.timeoutForRpm

Replication Manager サーバが Device Manager サーバ経由で Device Manager エージェントからホスト情報を取得する際の通信タイムアウト時間を分単位で指定します。

有効な値は, 1~1440 (分) です。

デフォルト: 15

A.12 Host Data Collector との連携に関するプロパティ (hostdatacollectors.properties ファイル)

Host Data Collector との連携に関するプロパティは, hostdatacollectors.properties ファイルに含まれています。

- Windows の場合 :
`<Device Manager サーバのインストールフォルダ>%HiCommandServer%config
%hostdatacollectors.properties`
- Solaris または Linux の場合 :
`<Device Manager サーバのインストールディレクトリ>/HiCommandServer/config/
hostdatacollectors.properties`

A.12.1 hdc.request.timeout

Device Manager サーバから Host Data Collector に対するリクエスト処理のタイムアウト値を指定します (単位: ミリ秒)。

1000~86400000 の値を設定できます。

Device Manager サーバが複数の Host Data Collector と通信する場合は、すべての Host Data Collector との通信に適用されます。

デフォルト: 1800000

A.12.2 hdc.rmiregistry

Host Data Collector がインストールされたマシンの IP アドレスまたはホスト名と、RMI レジストリーのポート番号を次の形式で指定します。

`<IP アドレスまたはホスト名>:[<ポート番号>], <IP アドレスまたはホスト名>:[<ポート番号>], ...`

IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず角括弧 ([]) で囲んでください。

ポート番号は、hdcbase.properties ファイルの hdc.common.rmi.registryPort プロパティまたは hdc.common.rmi.ssl.registryPort プロパティに指定した値と一致している必要があります。ポート番号を省略した場合、hdc.usessl プロパティの値が false のときは 22098 を、true のときは 22104 を指定したものと見なされます。

Host Data Collector がインストールされたマシンが複数台ある場合は、台数分、Host Data Collector の情報を指定する必要があります。

デフォルト値:

管理サーバの OS が Host Data Collector の前提 OS である場合: 127.0.0.1:22098

管理サーバの OS が Host Data Collector の前提 OS ではない場合: なし



注意 Host Data Collector がインストールされたマシンの IP アドレスまたはホスト名は、hdc.rmiregistry プロパティ、hdc.rmiserver プロパティおよび hdc.classloader プロパティですべて同じにしてください。また、Host Data Collector がインストールされたマシンに複数の IP アドレスが割り当てられている場合、Host Data Collector の hdcbase.properties ファイルの hdc.service.rmi.registryIPAddress プロパティも同じ値にしてください。

関連項目

- [A.12.3 hdc.rmiserver](#)
- [A.12.4 hdc.classloader](#)
- [A.12.5 hdc.usessl](#)
- [C.2.4 hdc.common.rmi.registryPort](#)
- [C.2.7 hdc.common.rmi.ssl.registryPort](#)

- [C.2.10 hdc.service.rmi.registryIPAddress](#)

A.12.3 hdc.rmiservert

Host Data Collector がインストールされたマシンの IP アドレスまたはホスト名と、RMI サーバのポート番号を次の形式で指定します。

< IP アドレスまたはホスト名 > : [< ポート番号 >] , < IP アドレスまたはホスト名 > : [< ポート番号 >] , ...

IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず角括弧 ([]) で囲んでください。

ポート番号は、Host Data Collector の `hdc.common.rmi.serverPort` プロパティまたは `hdc.common.rmi.ssl.serverPort` プロパティに指定した値と一致している必要があります。ポート番号を省略した場合、`hdc.usessl` プロパティの値が `false` のときは 22099 を、`true` のときは 22105 を指定したものと見なされます。

Host Data Collector がインストールされたマシンが複数台ある場合は、台数分、Host Data Collector の情報を指定する必要があります。

デフォルト値 :

管理サーバの OS が Host Data Collector の前提 OS である場合 : 127.0.0.1:22099

管理サーバの OS が Host Data Collector の前提 OS ではない場合 : なし



注意 Host Data Collector がインストールされたマシンの IP アドレスまたはホスト名は、`hdc.rmiregistry` プロパティ、`hdc.rmiservert` プロパティおよび `hdc.classloader` プロパティですべて同じにしてください。また、Host Data Collector がインストールされたマシンに複数の IP アドレスが割り当てられている場合、Host Data Collector の `hdcbase.properties` ファイルの `hdc.service.rmi.registryIPAddress` プロパティも同じ値にしてください。

関連項目

- [A.12.2 hdc.rmiregistry](#)
- [A.12.4 hdc.classloader](#)
- [A.12.5 hdc.usessl](#)
- [C.2.5 hdc.common.rmi.serverPort](#)
- [C.2.8 hdc.common.rmi.ssl.serverPort](#)
- [C.2.10 hdc.service.rmi.registryIPAddress](#)

A.12.4 hdc.classloader

Host Data Collector がインストールされたマシンの IP アドレスまたはホスト名と、クラスローダーのポート番号を次の形式で指定します。

< IP アドレスまたはホスト名 > : [< ポート番号 >] , < IP アドレスまたはホスト名 > : [< ポート番号 >] , ...

IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず角括弧 ([]) で囲んでください。

ポート番号は、Host Data Collector の `hdc.common.http.serverPort` プロパティまたは `hdc.common.https.serverPort` プロパティに指定した値と一致している必要があります。ポート番号を省略した場合、`hdc.usessl` プロパティの値が `false` のときは 22100 を、`true` のときは 22106 を指定したものと見なされます。

Host Data Collector がインストールされたマシンが複数台ある場合は、台数分、Host Data Collector の情報を指定する必要があります。

デフォルト値：

管理サーバの OS が Host Data Collector の前提 OS である場合：127.0.0.1:22100

管理サーバの OS が Host Data Collector の前提 OS ではない場合：なし



注意 Host Data Collector がインストールされたマシンの IP アドレスまたはホスト名は、hdc.rmiregistry プロパティ、hdc.rmiserver プロパティおよびhdc.classloader プロパティですべて同じにしてください。また、Host Data Collector がインストールされたマシンに複数の IP アドレスが割り当てられている場合、Host Data Collector のhdcbase.properties ファイルのhdc.service.rmi.registryIPAddress プロパティも同じ値にしてください。

関連項目

- [A.12.2 hdc.rmiregistry](#)
- [A.12.3 hdc.rmiserver](#)
- [A.12.5 hdc.usessl](#)
- [C.2.6 hdc.common.http.serverPort](#)
- [C.2.9 hdc.common.https.serverPort](#)
- [C.2.10 hdc.service.rmi.registryIPAddress](#)

A.12.5 hdc.usessl

Host Data Collector マシンと Device Manager サーバ間を SSL で通信するかどうかを指定します。

SSL で通信する場合は true を指定してください。非 SSL で通信する場合は false を指定してください。

Host Data Collector がインストールされたマシンが複数台ある場合、このプロパティの設定はすべての Host Data Collector マシンとの通信に適用されます。

デフォルト：false

A.13 マイグレーションに関するプロパティ (migration.properties ファイル)

マイグレーションに関するプロパティは、migration.properties ファイルに含まれています。

- Windows の場合：
< Device Manager サーバのインストールフォルダ > \HiCommandServer\config
migration.properties
- Solaris または Linux の場合：
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/config/
migration.properties

A.13.1 migration.dataErase.defaultValue

[データマイグレーション] ウィザードを起動した際の [シュレディング] チェックボックスの状態を指定します。

true を設定した場合：

[シユレヱディング] チェックボックスが選択された状態になります。

false を設定した場合：

[シユレヱディング] チェックボックスが選択されていない状態になります。

情報漏洩を防ぐため、マイグレーション後は移動元ボリュームのデータを消去することをお勧めします。

デフォルト：false

A.13.2 migration.plan.candidateVolumeCountLimit

マイグレーションプランを作成するときに表示される候補ボリューム数を絞り込むかどうかを指定します。

true を設定すると、候補ボリューム数を絞り込みます。false を設定すると、候補ボリューム数を絞り込みません。

デフォルト：true

A.13.3 migration.plan.candidateCapacityGroupDisplayMaxCount

マイグレーションプランを作成するときに、移動元ボリュームと同じ容量のボリュームに加えて、移動元ボリュームよりも容量が大きいボリュームを何番目まで候補ボリュームとして表示させるかを指定します。

指定できる値の範囲は、0～10 です。0 を指定した場合は、移動元ボリュームと同じ容量のボリュームだけ表示されます。

デフォルト：4



注意

- 移動元ボリュームよりも容量が大きいボリュームを移動先に指定した場合は、マイグレーションの実行前に、移動先ボリュームがいったん削除され、移動元ボリュームと同じ容量のボリュームに再作成されます。そのため、同じ容量のボリュームに移動する場合よりも、マイグレーションタスクの実行に時間が掛かります。
 - 移動先ボリュームを再作成すると、移動元ボリュームとの容量の差だけ、パリティグループの空き容量が増加します。例えば、10GB の移動元ボリュームに対して、30GB のボリュームを移動先に指定した場合は、パリティグループの空き容量が 20GB 増加します。そのため、できるだけ移動元ボリュームとの容量の差が小さいボリュームを移動先に指定することをお勧めします。
-

A.13.4 migration.multiExecution

1 つのストレージシステム内で同時に実行できるマイグレーションペアの数を指定します。

指定できる値の範囲は、1～64 です。

デフォルト：8

A.14 Tuning Manager との連携に関するプロパティ (tuningmanager.properties ファイル)

Tuning Manager との連携に関するプロパティは、tuningmanager.properties ファイルに含まれています。

- Windows の場合 :
`<Device Manager サーバのインストールフォルダ>%HiCommandServer%config
%tuningmanager.properties`
- Solaris または Linux の場合 :
`<Device Manager サーバのインストールディレクトリ>/HiCommandServer/config/
tuningmanager.properties`

A.14.1 htm.infoAcquirePeriod

パリティグループの利用率やボリュームの IOPS などの性能情報の集計単位を指定します。

指定方法は次の 3 とおりです。

- day : 性能情報を日単位で集計します。
- week : 性能情報を週単位で集計します。Tuning Manager では月曜日から日曜日を 1 週間としています。
- month : 性能情報を月単位で集計します。Tuning Manager では 1 日から月末日を 1 か月としています。

表示されるのは、集計が完了した性能情報です。そのため、day を指定した場合は 1 日前の性能情報、week を指定した場合は先週の性能情報、month を指定した場合は先月の性能情報が表示されます。週や月の途中でストレージシステムをリフレッシュしても、同じ情報が表示されます。

デフォルト : day

A.14.2 htm.servers

接続する Tuning Manager サーバの数を指定します。

指定できる値の範囲は、0~50 です。

デフォルト : 0

A.14.3 htm.server*n*.host

アクセスする Tuning Manager サーバのホスト名または IP アドレスを指定します。

プロパティ名の *n* には、「0」から「*htm.servers* プロパティで指定した値 - 1」までの値を指定します。

- Device Manager サーバと Tuning Manager サーバが同一マシンの場合
Tuning Manager サーバと Hitachi Command Suite 共通コンポーネント間の通信方式によって設定する値が異なります。
 - http で通信するとき
ループバックアドレス (127.0.0.1 または localhost) を指定してください。
 - https で通信するとき
Hitachi Command Suite 共通コンポーネントのサーバ証明書の CN に指定したホスト名を指定してください。大文字、小文字の区別も同じにしてください。
- Device Manager サーバと Tuning Manager サーバが別マシンの場合
アクセスする Tuning Manager サーバのホスト名または IPv4 アドレスを指定してください。IPv6 アドレスは指定できません。

デフォルト : なし

A.14.4 htnm.server*n*.protocol

Tuning Manager サーバと Hitachi Command Suite 共通コンポーネント間の通信方式に応じて、http または https を指定します。

デフォルト：http

なお、プロパティ名の *n* には、「*htnm.servers* プロパティで指定した値 - 1」までの値を指定します。

A.14.5 htnm.server*n*.port

アクセスする Tuning Manager サーバの HBase Storage Mgmt Web Service のポート番号を指定します。

htnm.server.*n*.protocol に http を指定した場合は、非 SSL 用の HBase Storage Mgmt Web Service のポート番号を指定します。htnm.server.*n*.protocol に https を指定した場合は、SSL 用の HBase Storage Mgmt Web Service のポート番号を指定します。

デフォルト：なし

なお、プロパティ名の *n* には、「*htnm.servers* プロパティで指定した値 - 1」までの値を指定します。

関連項目

- [A.14.4 htnm.server*n*.protocol](#)

A.14.6 htnm.flashMode

[分析] タブから Tuning Manager の履歴レポートをラウンチする場合、履歴レポートのチャートの表示形式を指定します。

true を指定すると、チャートを Adobe Flash Player で表示します。false を指定すると、チャートを画像 (PNG 形式) で表示します。

デフォルト：true

A.14.7 hdvm.analytics.disabled

[分析] タブを非表示にします。

このプロパティはデフォルトでは存在しません。

[分析] タブを表示しない場合は、tuningmanager.properties ファイルに、次のとおり指定してください。

```
hdvm.analytics.disabled=true
```

A.14.8 hdvm.analytics.healthcheck.excludeMainframe

メインフレームボリュームをヘルスチェックの分析対象にする場合に指定します。

デフォルトでは、メインフレームボリュームはヘルスチェックで分析されません。メインフレームボリュームも分析する場合は、このプロパティを指定してください。なお、このプロパティはデフォルトでは存在しないため、tuningmanager.properties ファイルに、次のとおり指定してください。

```
hdvm.analytics.healthcheck.excludeMainframe=false
```

A.14.9 hdvm.analytics.healthcheck.notification.exportreport.locale

ヘルスチェック結果を E メールで通知する場合、ヘルスチェックレポートを添付するときの PDF ファイルのロケールを指定します。

デフォルトでは、Device Manager サーバのロケールが指定されます。Device Manager サーバのロケールに日本語以外の言語が指定されている場合は、英語が指定されます。

Device Manager サーバのロケールとは別に PDF ファイルのロケールを指定する場合は、このプロパティでロケールを指定してください。このプロパティに ja を指定すると日本語、en を指定すると英語のロケールが指定されます。

このプロパティはデフォルトでは存在しないため、次の形式で指定してください。

```
hdvm.analytics.healthcheck.notification.exportreport.locale=<ロケール値>
```

A.15 Universal Replicator の性能分析に関するプロパティ (replication.properties ファイル)

Universal Replicator の性能分析に関するプロパティは、replication.properties ファイルに含まれています。

- Windows の場合 :

```
<Device Manager サーバのインストールフォルダ>%HiCommandServer%config  
%replication.properties
```

- Solaris または Linux の場合 :

```
<Device Manager サーバのインストールディレクトリ>/HiCommandServer/config/  
replication.properties
```

A.15.1 server.dispatcher.daemon.replication.config.doUpdate

プライマリーサイトとセカンダリーサイトのストレージシステム、コピーグループ、コピーペア、およびペア管理サーバの構成情報を定期的に収集するかどうかを指定します。

true を指定すると、構成情報を定期的に収集します。

デフォルトでは、毎日 2:00 に構成情報を収集します。

ヘルスチェックや Tuning Manager のポーリングの実行中に収集時刻を指定している場合は、収集時刻を変更することをお勧めします。

また、Replication Manager の構成情報の更新が完了してから構成情報を収集するように、収集時刻を指定することをお勧めします。Replication Manager の構成情報の更新が完了した時刻は、Replication Manager のイベントログから確認できます。

収集間隔や収集時刻を変更したい場合は、次のプロパティを編集してください。

- server.dispatcher.daemon.replication.config.updateInterval プロパティ : 収集間隔
- server.dispatcher.daemon.replication.config.offset プロパティ : 収集開始時刻の時

- `server.dispatcher.daemon.replication.config.minute` プロパティ：収集開始時刻の分

`false` を指定した場合は、定期的には収集しません。この場合は、[レプリケーション] タブで構成情報を収集してください。

デフォルト：true

関連項目

- [A.15.2 server.dispatcher.daemon.replication.config.updateInterval](#)
- [A.15.3 server.dispatcher.daemon.replication.config.offset](#)
- [A.15.4 server.dispatcher.daemon.replication.config.minute](#)
- Replication Manager のイベントログについて：マニュアル「*Hitachi Command Suite Replication Manager Software ユーザーズガイド*」

A.15.2 server.dispatcher.daemon.replication.config.updateInterval

プライマリーサイトとセカンダリーサイトのストレージシステム、コピーグループ、コピーペア、およびペア管理サーバの構成情報を収集する間隔を指定します。

指定できる値は、8、12、または 24（時間）です。

このプロパティは、`server.dispatcher.daemon.replication.config.doUpdate` プロパティで `true` を指定した場合にだけ有効になります。

デフォルト：24（時間）

関連項目

- [A.15.1 server.dispatcher.daemon.replication.config.doUpdate](#)

A.15.3 server.dispatcher.daemon.replication.config.offset

プライマリーサイトとセカンダリーサイトのストレージシステム、コピーグループ、コピーペア、およびペア管理サーバの構成情報を収集する開始時刻の時を指定します。

`server.dispatcher.daemon.replication.config.updateInterval` プロパティに 8 または 12 を指定した場合は、1 日に構成情報を複数回収集するため、1 日の最初に収集する開始時刻の時を指定します。

例えば、このプロパティに 3 を指定すると、次のように構成情報を収集します。

- `server.dispatcher.daemon.replication.config.updateInterval` プロパティに 8 を指定した場合
毎日 3:00、11:00、19:00 に収集します。
- `server.dispatcher.daemon.replication.config.updateInterval` プロパティに 12 を指定した場合
毎日 3:00、15:00 に収集します。
- `server.dispatcher.daemon.replication.config.updateInterval` プロパティに 24 を指定した場合
毎日 3:00 に収集します。

0～23 の範囲で、`server.dispatcher.daemon.replication.config.updateInterval` プロパティに指定した値よりも小さい値を指定してください。

このプロパティは、`server.dispatcher.daemon.replication.config.doUpdate` プロパティで `true` を指定した場合にだけ有効になります。

デフォルト：2

関連項目

- [A.15.1 server.dispatcher.daemon.replication.config.doUpdate](#)
- [A.15.2 server.dispatcher.daemon.replication.config.updateInterval](#)

A.15.4 server.dispatcher.daemon.replication.config.minute

プライマリーサイトとセカンダリーサイトのストレージシステム、コピーグループ、コピーペア、およびペア管理サーバの構成情報を収集する開始時刻の分を指定します。

指定できる範囲は、0～59（分）です。

このプロパティは、`server.dispatcher.daemon.replication.config.doUpdate` プロパティで `true` を指定した場合にだけ有効になります。

デフォルト：0（分）

関連項目

- [A.15.1 server.dispatcher.daemon.replication.config.doUpdate](#)

A.15.5

server.dispatcher.daemon.replication.performance.rpm.updateInterval

C/T デルタやジャーナルボリューム使用率などの性能情報を、Replication Manager から収集する間隔を分単位で指定します。

3～60 の範囲で、60 の約数を指定してください。

デフォルト：5（分）

A.15.6

server.dispatcher.daemon.replication.performance.tnm.updateInterval

ストレージシステムのプロセッサの利用率や、ストレージシステムのキャッシュメモリーのうち、書き込み待ちデータの割合などの性能情報を、Tuning Manager から収集する間隔を指定します。

指定できる値は、4, 8, 12, または 24（時間）です。

デフォルト：4（時間）

A.15.7 server.dispatcher.daemon.replication.performance.tnm.offset

ストレージシステムのプロセッサの利用率や、ストレージシステムのキャッシュメモリーのうち、書き込み待ちデータの割合などの性能情報を、Tuning Manager から収集する開始時刻の時を指定します。

`server.dispatcher.daemon.replication.performance.tnm.updateInterval` プロパティに 4, 8, または 12 を指定した場合は、1 日に性能情報を複数回収集するため、1 日の最初に収集する開始時刻の時を指定します。

例えば、このプロパティに 2 を指定すると、次のように性能情報を収集します。

- `server.dispatcher.daemon.replication.performance.tnm.updateInterval` プロパティに 4 を指定した場合
毎日 2:00, 6:00, 10:00, 14:00, 18:00, 22:00 に収集します。
- `server.dispatcher.daemon.replication.performance.tnm.updateInterval` プロパティに 8 を指定した場合
毎日 2:00, 10:00, 18:00 に収集します。
- `server.dispatcher.daemon.replication.performance.tnm.updateInterval` プロパティに 12 を指定した場合
毎日 2:00, 14:00 に収集します。
- `server.dispatcher.daemon.replication.performance.tnm.updateInterval` プロパティに 24 を指定した場合
毎日 2:00 に収集します。

0～23 の範囲で、

`server.dispatcher.daemon.replication.performance.tnm.updateInterval` プロパティに指定した値よりも小さい値を指定してください。

ヘルスチェックや **Tuning Manager** のポーリングの実行中に収集時刻を指定している場合は、収集時刻を変更することをお勧めします。

デフォルト：3

関連項目

- [A.15.6 server.dispatcher.daemon.replication.performance.tnm.updateInterval](#)

A.15.8 server.dispatcher.daemon.replication.performance.tnm.minute

ストレージシステムのプロセッサの利用率や、ストレージシステムのキャッシュメモリーのうち、書き込み待ちデータの割合などの性能情報を、**Tuning Manager** から収集する開始時刻の分を指定します。

指定できる範囲は、0～59（分）です。

デフォルト：5（分）

A.15.9 hdvm.replication.disabled

[レプリケーション] タブを非表示にします。

このプロパティはデフォルトでは存在しません。

[レプリケーション] タブを表示しない場合は、`replication.properties` ファイルに、次のとおり指定してください。

```
hdvm.replication.disabled=true
```

A.16 Replication Manager との連携に関するプロパティ (rpmllib.properties ファイル)

Replication Manager との連携に関するプロパティは、rpmllib.properties ファイルに含まれています。

- Windows の場合：
< Device Manager サーバのインストールフォルダ >¥HiCommandServer¥config
¥rpmllib.properties
- Solaris または Linux の場合：
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/config/
rpmllib.properties

A.16.1 rpmllib.rpm.port

Replication Manager サーバとの連携に使用するポート番号を指定します。

ポート番号は、Replication Manager サーバの base.properties ファイルにある base.rmi.port プロパティの値と合わせてください。

デフォルト：25200

関連項目

- Replication Manager サーバの base.properties ファイルにある base.rmi.port プロパティについて：マニュアル「Hitachi Command Suite Replication Manager Software システム構成ガイド」

A.17 CIM/WBEM 機能に関するプロパティ (jserver.properties ファイル, cimxmlcpa.properties ファイル, cimxmlscpa.properties ファイル)

CIM/WBEM 機能に関するプロパティは、jserver.properties ファイル, cimxmlcpa.properties ファイル, および cimxmlscpa.properties ファイルに含まれています。

- jserver.properties ファイルの格納先
 - Windows の場合：
< Device Manager サーバのインストールフォルダ >¥HiCommandServer¥config
 - Solaris または Linux の場合：
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/config
- cimxmlcpa.properties ファイルおよび cimxmlscpa.properties ファイルの格納先
 - Windows の場合：
< Device Manager サーバのインストールフォルダ >¥HiCommandServer¥wsi¥server
¥jserver¥bin
 - Solaris または Linux の場合：
< Device Manager サーバのインストールディレクトリ > /HiCommandServer/wsi/
server/jserver/bin

A.17.1 com.wbemsolutions.jserver.bindto

1 台の管理サーバに複数の IP アドレスが割り当てられている場合に、SLP に登録する IP アドレスを指定します。

CIM クライアントからアクセスできる IP アドレスを指定する必要があります。

このプロパティは、jserver.properties ファイルに指定します。

com.wbemsolutions.jserver.bindto プロパティはデフォルトでは存在しないため、次の形式でプロパティを指定してください。

com.wbemsolutions.jserver.bindto=<IP アドレス>

A.17.2 HTTPPort

非 SSL 通信の場合に、CIM/WBEM 機能で使用するポート番号を指定します。

このプロパティは、cimxmlcpa.properties ファイルに指定します。cimxmlcpa.properties ファイルはデフォルトでは存在しないため、ファイルを新規作成し、次の形式でプロパティを指定してください。

HTTPPort=<ポート番号>



注意

- このプロパティの値を変更した場合は、Device Manager サーバの server.cim.http.port プロパティも同じ値に変更してください。
- cimxmlcpa.properties ファイルは、Device Manager サーバのサービスを起動した際に削除されます。ポート変更の際は、そのつど cimxmlcpa.properties ファイルを新規作成してください。

関連項目

- [A.2.13 server.cim.http.port](#)

A.17.3 HTTPSPort

SSL 通信の場合に、CIM/WBEM 機能で使用するポート番号を指定します。

このプロパティは、cimxmlscpa.properties ファイルに指定します。

cimxmlscpa.properties ファイルはデフォルトでは存在しないため、ファイルを新規作成し、次の形式でプロパティを指定してください。

HTTPSPort=<ポート番号>



注意

- cimxmlscpa.properties ファイルには、Ciphers プロパティも必ず指定してください。
- このプロパティの値を変更した場合は、Device Manager サーバの server.cim.https.port プロパティも同じ値に変更してください。
- cimxmlscpa.properties ファイルは、Device Manager サーバのサービスを起動した際に削除されます。ポート変更の際は、そのつど cimxmlscpa.properties ファイルを新規作成してください。

関連項目

- [A.2.14 server.cim.https.port](#)

Tiered Storage Manager サーバのプロパティ

ここでは、Tiered Storage Manager サーバのプロパティファイルについて説明します。

- B.1 Tiered Storage Manager サーバのプロパティファイル
- B.2 Tiered Storage Manager サーバの動作に関するプロパティ (server.properties ファイル)
- B.3 Tiered Storage Manager の GUI に関するプロパティ (client.properties ファイル)
- B.4 Tiered Storage Manager のデータベースに関するプロパティ (database.properties ファイル)
- B.5 Tiered Storage Manager から Device Manager サーバへのアクセスに関するプロパティ (devicemanager.properties ファイル)
- B.6 Tiered Storage Manager のログ出力に関するプロパティ (logger.properties ファイル)
- B.7 Tiered Storage Manager のセキュリティに関するプロパティ

B.1 Tiered Storage Manager サーバのプロパティファイル

Tiered Storage Manager サーバのプロパティファイルには、Tiered Storage Manager サーバの動作に関するプロパティファイルや Device Manager サーバへのアクセスに関するプロパティファイルなどがあります。Tiered Storage Manager サーバのプロパティファイルは、Tiered Storage Manager CLI または Legacy モードの Tiered Storage Manager GUI からの操作（処理）にだけ適用されます。

Tiered Storage Manager サーバのプロパティファイルを次の表に示します。

表 B-1 Tiered Storage Manager サーバのプロパティファイル

プロパティファイル	説明
server.properties ファイル	Tiered Storage Manager サーバの動作に関するプロパティファイルです。
client.properties ファイル	Tiered Storage Manager の GUI に関するプロパティファイルです。
database.properties ファイル	Tiered Storage Manager のデータベースに関するプロパティファイルです。
devicemanager.properties ファイル	Tiered Storage Manager から Device Manager サーバへのアクセスに関するプロパティファイルです。
logger.properties ファイル	Tiered Storage Manager のログ出力に関するプロパティファイルです。



注意

- 誤った指定をした場合は、プロパティの読み込みに失敗し、起動できません。指定を誤ったプロパティは、コマンドログまたはメッセージログに出力されます。
- クラスタ構成の場合、特別な理由がないかぎり、実行系ノードと待機系ノードのプロパティファイルの内容は同じにしてください。
- デフォルト値は新規インストールした際に設定される値です。

B.1.1 Tiered Storage Manager サーバのプロパティの変更

Tiered Storage Manager サーバのプロパティファイルは、テキストエディターを使用して編集します。

事前に完了しておく操作

- Administrator 権限（Windows の場合）または root（Solaris または Linux の場合）でのログイン

Tiered Storage Manager サーバのプロパティを変更するには：

- Hitachi Command Suite 製品のサービスを停止します。
- テキストエディターで、Tiered Storage Manager サーバのプロパティファイルに適切な値を設定します。
- Hitachi Command Suite 製品のサービスを起動します。



参考 Tiered Storage Manager サーバのプロパティを新規インストール時の設定に戻す場合には、次の場所に格納されているひな形を使ってください。

Windows の場合：

< Tiered Storage Manager サーバのインストールフォルダ > \template

Solaris または Linux の場合 :

< *Tiered Storage Manager* サーバのインストールディレクトリ > /template

関連項目

- 9.2 サービスの起動
- 9.3 サービスの停止

B.1.2 Tiered Storage Manager サーバのプロパティファイルの記述規則

プロパティファイルは、Java プロパティファイル形式です。

プロパティファイルは、次の記述規則に従って作成されている必要があります。

- 各プロパティは、foo.bar=12345 のように、「=」で区切られた名前と値の対で指定します。
- 個々のプロパティは、行区切り文字（改行）で区切ります。
- 行頭に番号記号（#）がある場合、その行は注釈行になります。
- リテラル（文字列または数値）を引用符で囲む必要はありません。
- 円記号（¥）はエスケープ文字を表す予約文字になります。Windows では、絶対パス名を表すときに円記号（¥）を含むので、「¥¥」と指定する必要があります。

例えば、ファイルパス名 C:¥¥HiCommand¥¥docroot¥¥foo.bar は、C:¥¥HiCommand¥¥docroot ¥¥foo.bar と入力します。プロパティの指定では、そのほかの文字にはエスケープ文字「¥」を付ける必要はありません。

- プロパティファイル内に同じプロパティ名で複数の設定がされている場合、ファイルの最後に設定したプロパティの値が有効になります。
- 行末に円記号（¥）がある場合、次の行は継続行になります。

B.2 Tiered Storage Manager サーバの動作に関するプロパティ（server.properties ファイル）

Tiered Storage Manager サーバの動作に関するプロパティは、server.properties ファイルに含まれています。

- Windows の場合 :
< *Tiered Storage Manager* サーバのインストールフォルダ > ¥conf¥server.properties
- Solaris または Linux の場合 :
< *Tiered Storage Manager* サーバのインストールディレクトリ > /conf/
server.properties

B.2.1 server.rmi.secure

Tiered Storage Manager サーバと CLI クライアント間を SSL で通信するかどうかを指定します。

SSL で通信するよう指定すると、Tiered Storage Manager サーバと CLI クライアント間のデータ転送を暗号化できます。

指定できる値は 1 から 4 です。

1 : 非 SSL で通信します。

2 : SSL で通信します。

3 : 高度なセキュリティ設定の SSL で通信します。

4 : 高度なセキュリティ設定で、かつ使用する暗号方式 (Cipher Suite) をセキュリティポリシーに合わせて制限した状態で SSL で通信します。使用する暗号方式は `server.rmi.security.enabledCipherSuites` プロパティで設定します。

デフォルト : 1

B.2.2 server.rmi.port

Tiered Storage Manager サーバが処理要求を受け付ける RMI ポート番号 (非 SSL 通信用) を指定します。

指定できる値の範囲は、1~65535 です。

このプロパティは、`server.rmi.secure` プロパティに 1 を指定した場合に有効になります。

デフォルト : 20352



注意 このプロパティの値を変更したら、次の設定も変更する必要があります。

- Tiered Storage Manager CLI の `htsmcli.properties` ファイルの `htsmserver.location` プロパティ (Tiered Storage Manager サーバと非 SSL で通信している場合)
 - Sun Cluster に登録された Tiered Storage Manager サーバのポート番号 (管理サーバをクラスタ構成にしている場合)
-

関連項目

- (6) クラスタリソースの登録 (Sun Cluster の場合)
- B.2.1 `server.rmi.secure`

B.2.3 server.rmi.security.port

Tiered Storage Manager サーバが処理要求を受け付ける RMI ポート番号 (SSL 通信用) を指定します。

指定できる値の範囲は、1~65535 です。

このプロパティは、`server.rmi.secure` プロパティに 2, 3 または 4 を指定した場合に有効になります。

デフォルト : 24500



注意 このプロパティの値を変更したら、次の設定も変更する必要があります。

- Tiered Storage Manager CLI の `htsmcli.properties` ファイルの `htsmserver.location` プロパティ (Tiered Storage Manager サーバと SSL で通信している場合)
 - Sun Cluster に登録された Tiered Storage Manager サーバのポート番号 (管理サーバをクラスタ構成にしている場合)
-

関連項目

- (6) クラスタリソースの登録 (Sun Cluster の場合)
- B.2.1 `server.rmi.secure`

B.2.4 server.base.initialsynchro

Tiered Storage Manager サーバが起動したときに、ナビゲーションツリーに含まれている Tiered Storage Manager の構成情報と、Hitachi Command Suite 共通コンポーネントのデータベースとの同期を取るかどうかを指定します。

指定できる値はブール値です。true に設定すると、同期を取ります。false に設定すると、同期を取りません。

Tiered Storage Manager のデータベースを個別にリストアすると、Tiered Storage Manager サーバの再起動時に Tiered Storage Manager のストレージ構成情報と Hitachi Command Suite 共通コンポーネントのデータベースとの不整合が発生することがあります。その場合は、true を指定してください。

デフォルト：false

B.2.5 server.mail.smtp.host

イベント通知メール送信時にアクセスする SMTP サーバのホスト名または IP アドレスを指定します。

IPv6 アドレスを入力する場合は、IPv6 アドレスを [] で囲んでください。

デフォルト：なし

B.2.6 server.mail.from

イベント通知メールの通知元（差出人）のメールアドレスを指定します。

運用環境によっては、ドメイン名がないアドレスからの E メールを受信できないこともあります。プロパティの設定値を変更するか、SMTP サーバの環境設定を変更してください。

デフォルト：htsmserver

B.2.7 server.mail.errorsTo

イベント通知メールが配信エラーとなったときに送信される配信不能通知の送信先メールアドレスを指定します。

このプロパティを指定していない場合は、server.mail.from に指定したメールアドレスに送信されます。ただし、配信不能通知が送信される条件は、SMTP サーバの設定によって異なります。SMTP サーバの設定を確認してください。

デフォルト：なし

関連項目

- [B.2.6 server.mail.from](#)

B.2.8 server.mail.smtp.port

イベント通知メール送信時にアクセスする SMTP サーバのポート番号を指定します。

指定できる値の範囲は、1～65535 です。

デフォルト：25

B.2.9 server.mail.smtp.auth

イベント通知メール送信時に SMTP 認証をするかどうかを指定します。

指定する値はブール値です。true に設定すると、SMTP 認証をします。false に設定すると、SMTP 認証をしません。ただし、SMTP 認証をする設定にしても、使用するメールサーバが SMTP 認証に対応していない場合、SMTP 認証をしないでメールが送信されます。使用するメールサーバの仕様を確認して、SMTP 認証の設定をしてください。

デフォルト : false

B.2.10 server.eventNotification.mail.to

イベント通知メールの送信先メールアドレスを指定します。

このプロパティに設定するメールアドレスには、すべてのイベントの通知メールが送られます。

デフォルト : なし

B.2.11 server.eventMonitoringIntervallnMinute

イベント通知メールを送信するイベントのうち、ボリュームロック期限満了および指定期間経過の監視間隔を分単位で指定します。

指定できる値の範囲は、1~35,791 です。

デフォルト : 720

B.2.12 server.migration.multiExecution

1 つのストレージシステム内で同時に実行できるマイグレーションペアの数を指定します。

指定できる値の範囲は、1~64 です。

デフォルト : 8

B.2.13 server.checkOutVolumeRange

ボリューム検索や、ストレージ階層の定義で検索条件を指定したとき、検索条件で指定した値が指定できる値であることをチェックするかどうかを指定します。

指定できる値はブール値です。true に設定すると、チェックします。false に設定すると、チェックしません。

デフォルト : true



注意 false に設定すると、検索条件をチェックしません。false に設定した場合は、検索条件を間違えないよう十分注意してください。通常は、デフォルト (true : 検索条件をチェックする) のままにしてください。

B.2.14 server.migration.dataErase.defaultValue

[マイグレーション] ウィザードを起動した際の [移動元ボリュームのデータ消去] チェックボックスの状態、および CreateMigrationTask コマンドで erasedata パラメーターの指定を省略した場合の動作を指定します。

指定できる値はブール値です。

true を設定した場合：

[マイグレーション] ウィザードは [移動元ボリュームのデータ消去] チェックボックスが選択された状態で起動します。また、CreateMigrationTask コマンドで `erasedata` パラメーターを省略した場合は Yes を指定したものとして動作します。

false を設定した場合：

[マイグレーション] ウィザードの初期表示では [移動元ボリュームのデータ消去] チェックボックスが選択されていない状態で起動します。また、CreateMigrationTask コマンドで `erasedata` パラメーターを省略した場合は No を指定したものとして動作します。

情報漏洩を防ぐため、マイグレーション後は移動元ボリュームのデータを消去することをお勧めします。

デフォルト：false

B.2.15 server.migrationPlan.candidateVolumeCountLimit

マイグレーションプランを作成するときに表示される候補ボリューム数を絞り込むかどうか、指定します。

指定できる値はブール値です。true に設定すると、候補ボリューム数を絞り込みます。false に設定すると、候補ボリューム数を絞り込みません。

デフォルト：true

B.2.16

server.migrationPlan.candidateCapacityGroupDisplayMaxCount

マイグレーションプランを作成するとき、移動元ボリュームと同じ容量のボリュームに加えて、移動元ボリュームよりも容量が大きいボリュームを何番目まで候補ボリュームとして表示させるかを指定します。

指定できる値の範囲は、0～10 です。0 を指定した場合は、移動元ボリュームと同じ容量のボリュームだけ表示されます。

デフォルト：4



注意

- 移動元ボリュームよりも容量が大きいボリュームを移動先に指定した場合は、マイグレーションの実行前に、移動先ボリュームがいったん削除され、移動元ボリュームと同じ容量のボリュームに再作成されます。そのため、同じ容量のボリュームに移動する場合よりも、マイグレーションタスクの実行に時間が掛かります。
 - 移動先ボリュームを再作成すると、移動元ボリュームとの容量の差だけ、パリティグループの空き容量が増加します。例えば、10GB の移動元ボリュームに対して、30GB のボリュームを移動先に指定した場合は、パリティグループの空き容量が 20GB 増加します。そのため、できるだけ移動元ボリュームとの容量の差が小さいボリュームを移動先に指定することをお勧めします。
-

B.2.17 server.migration.maxRetryCount

Tiered Storage Manager サーバがストレージシステムへタスク実行の要求をリトライするときの最大リトライ回数を指定します。

ユーザーがストレージシステムの構成を変更していたり Modify モードでストレージシステムを操作していたりするために、ストレージシステムが要求を一時的に受け付けなくなった場合、5 分ごとにストレージシステムへ要求をリトライできます。

指定できる値の範囲は、0~2,147,483,647 です。0 を指定した場合は、リトライされません。

デフォルト：5

B.3 Tiered Storage Manager の GUI に関するプロパティ (client.properties ファイル)

GUI に関するプロパティは、client.properties ファイルに含まれています。

- Windows の場合：
< Tiered Storage Manager サーバのインストールフォルダ > %conf%\client.properties
- Solaris または Linux の場合：
< Tiered Storage Manager サーバのインストールディレクトリ > /conf/
client.properties

B.3.1 client.ldev.rowsperpage.retain.enabled

ソータブルテーブルの 1 ページ当たりの表示行数を変更した場合に、その設定を保持するかどうかを指定します。

このプロパティで true を指定すると、あるユーザーがあるソータブルテーブルで表示行数を変更した場合には、次に同じユーザーが同じソータブルテーブルを参照した際にも前回変更した行数で初期表示されます。設定した表示行数はユーザーアカウントごと、ソータブルテーブルごとに保持されます。

false を指定した場合は、1 ページ当たり 25 行表示された状態でソータブルテーブルが初期表示されます。

デフォルト：true



重要 設定値を true から false に変更しても、各ユーザーが変更した表示行数の設定は Tiered Storage Manager サーバに保存されています。再度、true を設定した場合には、以前にユーザーが設定した表示行数でソータブルテーブルが初期表示されます。

B.4 Tiered Storage Manager のデータベースに関するプロパティ (database.properties ファイル)

データベースに関するプロパティは、database.properties ファイルに含まれています。

- Windows の場合：
< Tiered Storage Manager サーバのインストールフォルダ > %conf%\
%database.properties
- Solaris または Linux の場合：
< Tiered Storage Manager サーバのインストールディレクトリ > /conf/
database.properties

B.4.1 dbm.traceSQL

トレースログに SQL を出力するかどうかを指定します。

指定できる値はブール値です。true に設定すると、SQL を出力します。false に設定すると、SQL を出力しません。

デフォルト : false

B.5 Tiered Storage Manager から Device Manager サーバへのアクセスに関するプロパティ (devicemanager.properties ファイル)

Device Manager サーバへのアクセスに関するプロパティは、devicemanager.properties ファイルに含まれています。

- Windows の場合 :
 < Tiered Storage Manager サーバのインストールフォルダ > ¥conf
 ¥devicemanager.properties
- Solaris または Linux の場合 :
 < Tiered Storage Manager サーバのインストールディレクトリ > /conf/
 devicemanager.properties

B.5.1 hdvm.protocol

Device Manager サーバにアクセスするときに使用するプロトコルを指定します。

デフォルト : http

B.5.2 hdvm.port

アクセスする Device Manager サーバのポート番号を指定します。

Device Manager サーバの server.http.port プロパティに指定した値と同じ値を指定する必要があります。

デフォルト : 2001

関連項目

- [A.2.2 server.http.port](#)

B.5.3 hdvm.timeout

アクセスする Device Manager サーバと通信するときのタイムアウトまでの時間をミリ秒で指定します。

0 を指定すると、タイムアウトしない設定になります。

指定できる値の範囲は、0~2,147,483,647 です。

デフォルト : 0

B.5.4 hdvm.rmi.port

Device Manager の RMI サーバのポート番号を指定します。

Device Manager サーバの server.rmi.port プロパティに指定した値と同じ値を指定する必要があります。

デフォルト : 23055

関連項目

- A.2.4 server.rmi.port

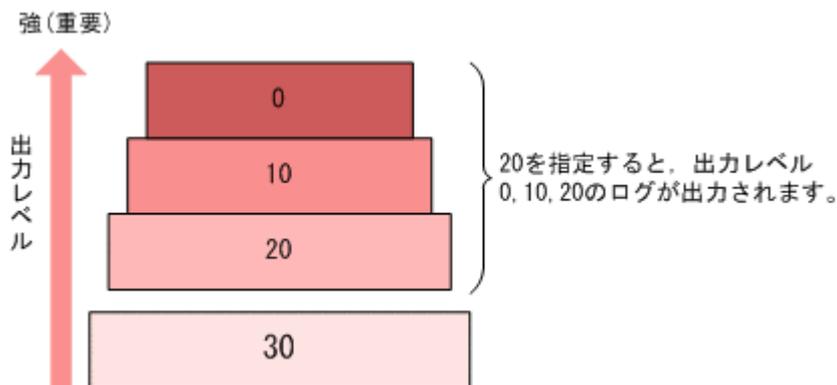
B.6 Tiered Storage Manager のログ出力に関するプロパティ (logger.properties ファイル)

ログ出力に関するプロパティは、logger.properties ファイルに含まれています。

- Windows の場合：
 < Tiered Storage Manager サーバのインストールフォルダ > \conf \logger.properties
- Solaris または Linux の場合：
 < Tiered Storage Manager サーバのインストールディレクトリ > /conf /
 logger.properties

出力レベルのしきい値に指定した値と出力されるメッセージの関係を次の図に示します。

図 B-1 出力レベルのしきい値に指定した値と出力されるメッセージの関係



B.6.1 logger.messageLogLevel

Tiered Storage Manager が出力するメッセージログに対して、出力レベルのしきい値を指定します。

このプロパティが対象とするログは、Tiered Storage Manager サーバのメッセージログ (HTSMServerMessage.log) および GUI のメッセージログ (HTSMGuiMessage.log) です。

Tiered Storage Manager では、ログ出力メッセージの内容に応じた出力レベルが用意されています。このプロパティで指定した値以下の出力レベルのメッセージが、メッセージログに出力されません。

指定できる値の範囲は、0~30 です。デフォルトでの運用をお勧めします。ただし、出力レベルが 30 で出力されるメッセージはないため、30 を指定しても 20 を指定した場合と出力されるメッセージに差異はありません。

デフォルト : 20

表 B-2 メッセージログの出力レベル

メッセージ種別	出力レベル	メッセージ説明
エラー	0	管理サーバの運用に影響を与えるエラーが発生した。
	10	操作ミスなどによる実行エラーが発生した。

メッセージ種別	出力レベル	メッセージ説明
警告	20	制限があるものの実行できるエラーが発生した。
情報	0	管理サーバや GUI の動作に関する情報が発生した。
	20	操作ごとの処理に関する情報が発生した。

B.6.2 logger.tracelogLevel

Tiered Storage Manager が出力するトレースログに対して、出力レベルのしきい値を指定します。

このプロパティが対象とするログは、Tiered Storage Manager サーバのトレースログ (HTSMServerTracen.log) および GUI のトレースログ (HTSMGuiTracen.log) です。

Tiered Storage Manager では、ログ出力メッセージの内容に応じた出力レベルが用意されています。このプロパティで指定した値以下の出力レベルのメッセージが、トレースログに出力されます。

指定できる値の範囲は、0～30 です。デフォルトでの運用をお勧めします。

デフォルト：20

表 B-3 トレースログの出力レベル

メッセージ種別	出力レベル	メッセージ説明
エラー	0	管理サーバや Servlet の運用に影響を与えるエラーが発生した。
	10	操作ミスなどによる実行エラーが発生した。
警告	20	制限があるものの実行できるエラーが発生した。
情報	0	管理サーバや管理クライアントの動作に関する情報が発生した。
	10	ほかのプログラムやマシンとのやり取りに関する情報が発生した。
	20	主要なメソッドの開始や停止、主要なオブジェクトの作成や削除に関する情報が発生した。
	30	詳細な情報が発生した。

B.6.3 logger.syslogLevel

Tiered Storage Manager が出力するイベントログまたは syslog に対して、出力レベルのしきい値を指定します。

イベントログおよび syslog は、メッセージログの中で特に重要なメッセージを出力します。このプロパティで指定した値以下の出力レベルのメッセージが、イベントログまたは syslog に出力されます。

指定できる値の範囲は、0～30 です。デフォルトでの運用をお勧めします。

デフォルト：0

B.6.4 logger.serverMessageFileCount

Tiered Storage Manager サーバが出力するメッセージログの最大バックアップ数を指定します。

指定できる値の範囲は、2～16 です。

ログファイルが logger.serverMessageMaxFileSize プロパティで指定された最大長に達すると、HTSMServerMessage2.log のようにカウンターが追加された形式にファイル名が変更されます。ログファイルはカウンターの順に使用され、ログ情報が書き込まれます。最後のファイルまで終わると、先頭のファイルに上書きされる「ラウンドロビン方式」になっています。

また、Tiered Storage Manager サーバが起動したときは、前回のサーバ停止が正常停止、異常停止に関係なく、最新ファイルの続きから書き込みが続けられます。

デフォルト：10

関連項目

- [B.6.8 logger.serverMessageMaxFileSize](#)

B.6.5 logger.serverTraceFileCount

Tiered Storage Manager サーバが出力するトレースログの最大バックアップ数を指定します。

指定できる値の範囲は、2～16 です。

ログファイルが `logger.serverTraceMaxFileSize` プロパティで指定された最大長に達すると、HTSMServerTrace2.log のようにカウンターが追加された形式にファイル名が変更されます。ログファイルはカウンターの順に使用され、ログ情報が書き込まれます。最後のファイルまで終わると、先頭のファイルに上書きされる「ラウンドロビン方式」になっています。

また、Tiered Storage Manager サーバが起動したときは、前回のサーバ停止が正常停止、異常停止に関係なく、最新ファイルの続きから書き込みが続けられます。

デフォルト：10

関連項目

- [B.6.9 logger.serverTraceMaxFileSize](#)

B.6.6 logger.guiMessageFileCount

GUI が出力するメッセージログの最大バックアップ数を指定します。

指定できる値の範囲は、2～16 です。

ログファイルが `logger.guiMessageMaxFileSize` プロパティで指定された最大長に達すると、HTSMGuiMessage2.log のようにカウンターが追加された形式にファイル名が変更されます。ログファイルはカウンターの順に使用され、ログ情報が書き込まれます。最後のファイルまで終わると、先頭のファイルに上書きされる「ラウンドロビン方式」になっています。

また、Tiered Storage Manager サーバが起動したときは、前回のサーバ停止が正常停止、異常停止に関係なく、最新ファイルの続きから書き込みが続けられます。

デフォルト：10

関連項目

- [B.6.10 logger.guiMessageMaxFileSize](#)

B.6.7 logger.guiTraceFileCount

GUI が出力するトレースログの最大バックアップ数を指定します。

指定できる値の範囲は、2～16 です。

ログファイルが `logger.guiTraceMaxFileSize` プロパティで指定された最大長に達すると、HTSMGuiTrace2.log のようにカウンターが追加された形式にファイル名が変更されます。ログ

ファイルはカウンターの順に使用され、ログ情報が書き込まれます。最後のファイルまで終わると、先頭のファイルに上書きされる「ラウンドロビン方式」になっています。

また、Tiered Storage Manager サーバが起動したときは、前回のサーバ停止が正常停止、異常停止に関係なく、最新ファイルの続きから書き込みが続けられます。

デフォルト：10

関連項目

- [B.6.11 logger.guiTraceMaxFileSize](#)

B.6.8 logger.serverMessageMaxFileSize

Tiered Storage Manager サーバが出力するメッセージログ (HTSMServerMessage`n`.log) の最大サイズを指定します。

指定できる値の範囲は、32,768 バイト (32KB) ～2,147,483,647 バイト (2,048MB) です。このプロパティを指定する場合、キロバイト単位の場合は KB、メガバイト単位の場合は MB を指定してください。単位がないとバイト単位と判断されます。

デフォルト：1,048,576 (1MB)

B.6.9 logger.serverTraceMaxFileSize

Tiered Storage Manager サーバが出力するトレースログ (HTSMServerTrace`n`.log) の最大サイズを指定します。

指定できる値の範囲は、32,768 バイト (32KB) ～2,147,483,647 バイト (2,048MB) です。このプロパティを指定する場合、キロバイト単位の場合は KB、メガバイト単位の場合は MB を指定してください。単位がないとバイト単位と判断されます。

デフォルト：5,242,880 (5MB)

B.6.10 logger.guiMessageMaxFileSize

GUI が出力するメッセージログ (HTSMGuiMessage`n`.log) の最大サイズを指定します。

指定できる値の範囲は、32,768 バイト (32KB) ～2,147,483,647 バイト (2,048MB) です。このプロパティを指定する場合、キロバイト単位の場合は KB、メガバイト単位の場合は MB を指定してください。単位がないとバイト単位と判断されます。

デフォルト：1,048,576 (1MB)

B.6.11 logger.guiTraceMaxFileSize

GUI が出力するトレースログ (HTSMGuiTrace`n`.log) の最大サイズを指定します。

指定できる値の範囲は、32,768 バイト (32KB) ～2,147,483,647 バイト (2,048MB) です。このプロパティを指定する場合、キロバイト単位の場合は KB、メガバイト単位の場合は MB を指定してください。単位がないとバイト単位と判断されます。

デフォルト：5,242,880 (5MB)

B.7 Tiered Storage Manager のセキュリティに関するプロパティ

このマニュアルでは、以下の内容は、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制により非公開となっています。以下の内容については、製品に付属するマニュアルをご覧ください。

Host Data Collector のプロパティ

ここでは、Host Data Collector のプロパティファイルについて説明します。

- C.1 Host Data Collector のプロパティファイル
- C.2 Host Data Collector の動作に関するプロパティ (hdcbase.properties ファイル)
- C.3 Host Data Collector のログ出力に関するプロパティ (logger.properties ファイル)
- C.4 Host Data Collector の Java 環境に関するプロパティ (javaconfig.properties ファイル)

C.1 Host Data Collector のプロパティファイル

Host Data Collector のプロパティファイルには、Host Data Collector の動作に関するプロパティファイルやログ出力に関するプロパティファイルなどがあります。

Host Data Collector のプロパティファイルを次の表に示します。

表 C-1 Host Data Collector のプロパティファイル

プロパティファイル	説明
hdcbase.properties ファイル	Host Data Collector の動作に関するプロパティファイルです。
logger.properties ファイル	Host Data Collector のログ出力に関するプロパティファイルです。
javaconfig.properties ファイル	Host Data Collector の Java 環境に関するプロパティファイルです。

C.1.1 Host Data Collector のプロパティの変更

Host Data Collector のプロパティファイルは、テキストエディターを使用して編集します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (Solaris または Linux の場合) でのログイン

Host Data Collector のプロパティを変更するには：

1. Host Data Collector のサービスを停止します。
2. テキストエディターで、Host Data Collector のプロパティファイルに適切な値を設定します。
3. Host Data Collector のサービスを起動します。

関連項目

- (1) サービスの起動 (Host Data Collector)
- (2) サービスの停止 (Host Data Collector)

C.2 Host Data Collector の動作に関するプロパティ (hdcbase.properties ファイル)

Host Data Collector の動作に関するプロパティは、hdcbase.properties ファイルに含まれています。

- Windows の場合：
< Host Data Collector のインストールフォルダ > \HDC\Base\config
hdcbase.properties
- Solaris または Linux の場合：
< Host Data Collector のインストールディレクトリ > /HDC/Base/config/
hdcbase.properties

C.2.1 hdc.service.localport

Service プロセスと Adapter プロセス間で通信する際の Service プロセス側のポート番号を指定します。

指定できる値の範囲は、1～65535 です。

デフォルト：22110

C.2.2 hdc.adapter.adapterProcessNum

同一ホスト内で起動する Adapter プロセスの数を指定します。

指定できる値の範囲は、1～10 です。

デフォルト：1

C.2.3 hdc.adapter.localport

Service プロセスと Adapter プロセス間で通信する際の Adapter プロセス側のポート番号を指定します。

Adapter プロセスを複数起動する場合は、ポート番号をコンマ (,) で区切ってください。指定できるポート番号の数は、最大 10 個です。Adapter プロセスの起動数よりポート番号の数が多い場合は、起動数分だけ有効になります。

指定できる値の範囲は、1～65535 です。

デフォルト：22111,22112,22113,22114,22115,22116,22117,22118,22119,22120

関連項目

- [C.2.2 hdc.adapter.adapterProcessNum](#)

C.2.4 hdc.common.rmi.registryPort

RMI レジストリーの非 SSL 通信用のポート番号を指定します。

指定できる値の範囲は、1～65535 です。このポートは、Host Data Collector の内部通信でも使用されます。

デフォルト：22098



重要 このプロパティの値を変更した場合は、次の設定が必要です。

- `firewall_setup` コマンドでファイアウォールの例外登録を再設定する (`hdc.ssl.secure` プロパティの値が 1 または 2 の場合)
 - Device Manager サーバの `hdc.rmiregistry` プロパティに同じ値を設定する (Host Data Collector と Device Manager サーバ間を非 SSL で通信している場合)
-

関連項目

- (1) Host Data Collector のサービスの例外登録 (非 SSL 通信用)
- [A.12.2 hdc.rmiregistry](#)
- [C.2.13 hdc.ssl.secure](#)

C.2.5 hdc.common.rmi.serverPort

RMI サーバの非 SSL 通信用のポート番号を指定します。

指定できる値の範囲は、1～65535 です。

デフォルト : 22099



重要 このプロパティの値を変更した場合は、次の設定が必要です。

- `firewall_setup` コマンドでファイアウォールの例外登録を再設定する (`hdc.ssl.secure` プロパティの値が 1 または 2 の場合)
 - Device Manager サーバの `hdc.rmiserver` プロパティに同じ値を設定する (Host Data Collector と Device Manager サーバ間を非 SSL で通信している場合)
-

関連項目

- (1) Host Data Collector のサービスの例外登録 (非 SSL 通信用)
- [A.12.3 hdc.rmiserver](#)
- [C.2.13 hdc.ssl.secure](#)

C.2.6 hdc.common.http.serverPort

クラスローダーの非 SSL 通信用のポート番号を指定します。

指定できる値の範囲は、1～65535 です。

デフォルト : 22100



重要 このプロパティの値を変更した場合は、次の設定が必要です。

- `firewall_setup` コマンドでファイアウォールの例外登録を再設定する (`hdc.ssl.secure` プロパティの値が 1 または 2 の場合)
 - Device Manager サーバの `hdc.classloader` プロパティに同じ値を設定する (Host Data Collector と Device Manager サーバ間を非 SSL で通信している場合)
-

関連項目

- (1) Host Data Collector のサービスの例外登録 (非 SSL 通信用)
- [A.12.4 hdc.classloader](#)
- [C.2.13 hdc.ssl.secure](#)

C.2.7 hdc.common.rmi.ssl.registryPort

RMI レジストリーの SSL 通信用のポート番号を指定します。

指定できる値の範囲は、1～65535 です。

デフォルト : 22104



重要 このプロパティの値を変更した場合は、次の設定が必要です。

- `netsh` コマンドでファイアウォールの例外登録を再設定する (`hdc.ssl.secure` プロパティの値が 2 または 3 の場合)
 - Device Manager サーバの `hdc.rmiregistry` プロパティに同じ値を設定する (Host Data Collector と Device Manager サーバ間を SSL で通信している場合)
-

関連項目

- (2) Host Data Collector のサービスの例外登録 (SSL 通信用)
- A.12.2 hdc.rmiregistry
- C.2.13 hdc.ssl.secure

C.2.8 hdc.common.rmi.ssl.serverPort

RMI サーバの SSL 通信用のポート番号を指定します。

指定できる値の範囲は、1～65535 です。

デフォルト：22105



重要 このプロパティの値を変更した場合は、次の設定が必要です。

- netsh コマンドでファイアウォールの例外登録を再設定する (hdc.ssl.secure プロパティの値が 2 または 3 の場合)
 - Device Manager サーバの hdc.rmiserver プロパティに同じ値を設定する (Host Data Collector と Device Manager サーバ間を SSL で通信している場合)
-

関連項目

- (2) Host Data Collector のサービスの例外登録 (SSL 通信用)
- A.12.3 hdc.rmiserver
- C.2.13 hdc.ssl.secure

C.2.9 hdc.common.https.serverPort

クラスローダーの SSL 通信用のポート番号を指定します。

指定できる値の範囲は、1～65535 です。

デフォルト：22106



重要 このプロパティの値を変更した場合は、次の設定が必要です。

- netsh コマンドでファイアウォールの例外登録を再設定する (hdc.ssl.secure プロパティの値が 2 または 3 の場合)
 - Device Manager サーバの hdc.classloader プロパティに同じ値を設定する (Host Data Collector と Device Manager サーバ間を SSL で通信している場合)
-

関連項目

- (2) Host Data Collector のサービスの例外登録 (SSL 通信用)
- A.12.4 hdc.classloader
- C.2.13 hdc.ssl.secure

C.2.10 hdc.service.rmi.registryIPAddress

Host Data Collector マシンが複数の IP アドレスを持っている場合、Device Manager サーバとの通信で使用する IP アドレスを指定します。

IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を使用できます。

IP アドレスは、Device Manager サーバの `hostdatacollectors.properties` ファイルにある次のプロパティに指定する値と同じにしてください。

- `hdc.rmiregistry` プロパティ
- `hdc.rmiserver` プロパティ
- `hdc.classloader` プロパティ

デフォルト値：なし※

注※ 指定されていない場合、Host Data Collector が取得した IP アドレスで動作します。

関連項目

- [A.12.2 hdc.rmiregistry](#)
- [A.12.3 hdc.rmiserver](#)
- [A.12.4 hdc.classloader](#)

C.2.11 `hdc.service.fileCleanup.startTime`

Host Data Collector が管理対象のホストから収集したホスト情報のファイルを削除する時刻を「`hhmm`」の形式で指定します。

`hh` は 00～23 の範囲で、`mm` は 00～59 の範囲で指定します。

デフォルト：2300

C.2.12 `hdc.adapter.esx.timeout`

Host Data Collector が管理対象の仮想化サーバから情報を取得する際のタイムアウト値を秒単位で指定します。

指定できる値の範囲は、0～2147483647 です。

デフォルト：1200

C.2.13 `hdc.ssl.secure`

Host Data Collector と Device Manager サーバ間の通信でオープンするポートを指定します。

指定できる値の範囲は、1～3 です。

- 1：非 SSL 通信用のポートだけオープンします。
- 2：非 SSL 通信用のポートと、SSL 通信用のポートの両方がオープンします。
- 3：SSL 通信用のポートだけオープンします。

`hdc.ssl.secure` プロパティの値とオープンするポート番号の対応は、次のとおりです。

表 C-2 `hdc.ssl.secure` プロパティの値とオープンするポート番号の対応

<code>hdc.ssl.secure</code> プロパティの値	オープンするポート番号（デフォルト）	
1	RMI レジストリー	22098/tcp
	RMI サーバ	22099/tcp
	クラスローダー	22100/tcp
2	RMI レジストリー	22098/tcp, 22104/tcp

hdc.ssl.secure プロパティの値	オープンするポート番号 (デフォルト)	
	RMI サーバ	22099/tcp, 22105/tcp
	クラスローダー	22100/tcp, 22106/tcp
3	RMI レジストリー	22098/tcp, 22104/tcp
	RMI サーバ	22105/tcp
	クラスローダー	22106/tcp

注

RMI レジストリーの非 SSL 通信用のポート (デフォルト: 22098/tcp) は、Host Data Collector の内部通信でも使用するため、常にオープンします。

デフォルト: 1

関連項目

- C.2.4 hdc.common.rmi.registryPort
- C.2.5 hdc.common.rmi.serverPort
- C.2.6 hdc.common.http.serverPort
- C.2.7 hdc.common.rmi.ssl.registryPort
- C.2.8 hdc.common.rmi.ssl.serverPort
- C.2.9 hdc.common.https.serverPort

C.3 Host Data Collector のログ出力に関するプロパティ (logger.properties ファイル)

Host Data Collector のログ出力に関するプロパティは、logger.properties ファイルに含まれています。

- Windows の場合 :
`<Host Data Collector のインストールフォルダ>%HDC%Base%config
%logger.properties`
- Solaris または Linux の場合 :
`<Host Data Collector のインストールディレクトリ>/HDC/Base/config/
logger.properties`

C.3.1 logger.trace.level

Host Data Collector が出力するトレースログの出力レベルを指定します。

このプロパティで指定した値以下の出力レベルのメッセージが、トレースログに出力されます。

表 C-3 トレースログの出力レベル

メッセージ種別	出力レベル	メッセージ説明
ERROR	0	エラー
WARNING	10	警告
INFO	30	情報
-	40	デバッグ

指定できる値は、0、10、30 および 40 です。

デフォルト：30

C.3.2 logger.trace.maxFileSize

Host Data Collector のトレースログの最大サイズを指定します。

キロバイト単位の場合は KB、メガバイト単位の場合は MB、ギガバイト単位の場合は GB と指定しないかぎり、指定したサイズはバイト単位であると見なされます。

指定できる値の範囲は、4096～2147483647 です。

デフォルト：5242880

C.3.3 logger.trace.numOfFiles

Host Data Collector のトレースログの最大バックアップファイル数を指定します。

ログファイルが logger.trace.maxFileSize プロパティで指定された最大長に達すると、カウンターが追加された形式にファイル名が変更されます。ログファイルがさらに作成されると、指定された数のバックアップログファイルが作成されるまで、カウンターが増加していきます。指定された数のバックアップログファイルが作成されたあとは、新しいバックアップログファイルが作成されるたびに、最も古いバックアップログファイルが削除されます。

指定できる値の範囲は、2～16 です。

デフォルト：10

関連項目

- [C.3.2 logger.trace.maxFileSize](#)

C.3.4 logger.iotrace.maxFileSize

通信トレースログの最大サイズを指定します。

キロバイト単位の場合は KB、メガバイト単位の場合は MB、ギガバイト単位の場合は GB と指定しないかぎり、指定したサイズはバイト単位であると見なされます。

指定できる値の範囲は、4096～2147483647 です。

デフォルト：5242880

C.3.5 logger.iotrace.numOfFiles

Host Data Collector の通信トレースログの最大バックアップファイル数を指定します。

ログファイルが logger.iotrace.maxFileSize プロパティで指定された最大長に達すると、カウンターが追加された形式にファイル名が変更されます。ログファイルがさらに作成されると、指定された数のバックアップログファイルが作成されるまで、カウンターが増加していきます。指定された数のバックアップログファイルが作成されたあとは、新しいバックアップログファイルが作成されるたびに、最も古いバックアップログファイルが削除されます。

指定できる値の範囲は、2～16 です。

デフォルト：10

関連項目

- C.3.4 logger.iotrace.maxFileSize

C.4 Host Data Collector の Java 環境に関するプロパティ (javaconfig.properties ファイル)

Host Data Collector の Java 環境に関するプロパティは、javaconfig.properties ファイルに含まれています。

- Windows の場合：
 <Host Data Collector のインストールフォルダ>%HDC%Base%config
 %javaconfig.properties
- Solaris または Linux の場合：
 <Host Data Collector のインストールディレクトリ>/HDC/Base/config/
 javaconfig.properties

C.4.1 javapathlocation

Host Data Collector で使用する Java の実行環境の格納場所を絶対パスで指定します。

パス中に空白文字が含まれる場合、パスを引用符 (") で囲む必要はありません。

デフォルト：

Windows または Linux の場合：なし (Host Data Collector に同梱された Java の実行環境が使用されます)

Solaris の場合：インストール時に検出された Java の実行環境のパス



Device Manager エージェントのプロパティ

ここでは、Device Manager エージェントのプロパティファイルについて説明します。

- D.1 Device Manager エージェントのプロパティファイル
- D.2 Device Manager エージェントと Replication Manager サーバとの連携に関するプロパティ (agent.properties ファイル)
- D.3 Device Manager エージェントの hldutil コマンドの動作に関するプロパティ (hldutil.properties ファイル)
- D.4 Device Manager エージェントのログ出力に関するプロパティ (logger.properties ファイル)
- D.5 Device Manager エージェントのプログラム情報に関するプロパティ (programproductinfo.properties ファイル)
- D.6 Device Manager エージェントの動作に関するプロパティ (server.properties ファイル)

D.1 Device Manager エージェントのプロパティファイル

Device Manager エージェントのプロパティファイルには、Device Manager エージェントの動作に関するプロパティファイルや Replication Manager サーバとの連携に関するプロパティファイルなどがあります。

Device Manager エージェントのプロパティファイルを次の表に示します。

表 D-1 Device Manager エージェントのプロパティファイル

プロパティファイル	説明
agent.properties ファイル	Device Manager エージェントと Replication Manager サーバとの連携に関するプロパティファイルです。
hldutil.properties ファイル	Device Manager エージェントの hldutil コマンドの動作に関するプロパティファイルです。
logger.properties ファイル	Device Manager エージェントのログ出力に関するプロパティファイルです。
programproductinfo.properties ファイル	Device Manager エージェントのプログラム情報に関するプロパティファイルです。
server.properties ファイル	Device Manager エージェントの動作に関するプロパティファイルです。



注意 デフォルトは新規インストールした際に設定される値です。

D.1.1 Device Manager エージェントのプロパティの変更

Device Manager エージェントのプロパティファイルは、テキストエディターを使用して編集します。

事前に完了しておく操作

- Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

Device Manager エージェントのプロパティを変更するには：

- hbsasrv コマンドを実行して、Device Manager エージェントのサービスを停止します。
- テキストエディターで、Device Manager エージェントのプロパティファイルに適切な値を設定します。
- hbsasrv コマンドを実行して、Device Manager エージェントのサービスを起動します。

関連項目

- (1) Device Manager エージェントのサービスの起動、停止、稼働状態の確認 (hbsasrv コマンド)

D.2 Device Manager エージェントと Replication Manager サーバとの連携に関するプロパティ (agent.properties ファイル)

Replication Manager サーバとの連携に関するプロパティは、agent.properties ファイルに含まれています。

- Windows の場合
 < *Device Manager* エージェントのインストールフォルダ > %mod%\hrpm\config
 %agent.properties
- Solaris, Linux, または HP-UX の場合
 /opt/HDVM/HBaseAgent/mod/hrpm/config/agent.properties
- AIX の場合
 /usr/HDVM/HBaseAgent/mod/hrpm/config/agent.properties



重要 Device Manager エージェントでは、Replication Manager でコピーペアの状態を監視するために、監視用の構成定義ファイルとインスタンスを独自に作成・管理しています。
監視用 HORCM インスタンスとは、Device Manager エージェントが利用する RAID Manager または P9000 RAID Manager のインスタンスのことです。また、監視用 HORCM ファイルとは、その RAID Manager または P9000 RAID Manager の構成定義ファイルのことです。

D.2.1 agent.rm.TimeOut

Device Manager エージェントが使用する RAID Manager または P9000 RAID Manager のコマンドの応答待ち時間を指定します (単位: 秒)。

0~86400 の値を設定できます。0 はタイムアウトがないことを意味します。

デフォルト: 600

通常は設定されている値を変更する必要のないパラメーターです。値を変更するためには、Device Manager エージェントに関する詳しい知識が必要です。

D.2.2 agent.rm.everytimeShutdown

監視用 HORCM インスタンスを毎回停止するかどうかを指定します。

true または false で指定します。true の場合、毎回停止します。false の場合、停止しません。

デフォルト: false

通常は設定されている値を変更する必要のないパラメーターです。値を変更するためには、Device Manager エージェントに関する詳しい知識が必要です。

D.2.3 agent.rm.shutdownWait

監視用 HORCM インスタンスを停止するときの待ち時間を指定します (単位: 秒)。

1~60 の値を設定できます。

デフォルト: 5

D.2.4 agent.rm.horcmlInstance

監視用 HORCM ファイルのインスタンス番号を指定します。

0~4094 の値を設定できます。ほかの RAID Manager または P9000 RAID Manager の構成定義ファイルのインスタンス番号と重複しないように設定する必要があります。

デフォルトでは、Device Manager エージェントが 900~998 の値を使用しますので、その値と重複しないように設定してください。

デフォルト: 4094



参考 Device Manager エージェントが使用するインスタンス番号は、`server.properties` ファイルにある `server.agent.rm.temporaryInstance` プロパティで変更できます。

関連項目

- [D.6.21 server.agent.rm.temporaryInstance](#)

D.2.5 agent.rm.horcmService

監視用 HORCM ファイルの UDP ポート番号を指定します。

0~65535 の値を設定できます。ほかのアプリケーションのポート番号と重複しないように設定する必要があります。

デフォルトでは、Device Manager エージェントが 53232~53330 の値を使用しますので、その値と重複しないように設定してください。

デフォルト : 54323



参考 Device Manager エージェントが使用する UDP ポート番号は、`server.properties` ファイルにある `server.agent.rm.temporaryPort` プロパティで変更できます。

関連項目

- [D.6.22 server.agent.rm.temporaryPort](#)

D.2.6 agent.logger.loglevel

Replication Manager エージェント機能のログファイルの出力レベルを指定します。

ここで設定してある値以上のレベルのログが出力されます。設定できる値は、重要度の低い順に示すと次のとおりです。

DEBUG, INFO, WARN, ERROR, FATAL

デフォルト : INFO

D.2.7 agent.logger.MaxBackupIndex

Replication Manager エージェント機能のログファイルの世代数を指定します。

1~20 の値を設定できます。ログファイルの数がこの値に達すると、先頭のファイルから順に再利用されます。

デフォルト : 5

ログファイルの出力量は、Replication Manager で管理しているコピーペアの数に依存します。ログファイルの出力量は次の計算式で求められます。

$\langle \text{出力されるログファイルの情報量 (MB/週間)} \rangle = 0.75 \times \langle \text{コピーペア数} \rangle + 4$

出力される容量と、保持期間を考慮して、`agent.logger.MaxBackupIndex` と `agent.logger.MaxFileSize` の値を設定してください。なお、対象のホスト (ペア管理サーバ) で管理しているコピーペア数は、Replication Manager の [`<コピーグループ名>`] サブウィンドウで確認できます。

関連項目

- [D.2.8 agent.logger.MaxFileSize](#)

D.2.8 agent.logger.MaxFileSize

Replication Manager エージェント機能のログファイルのサイズを指定します。

512KB～32MB の値を設定できます。バイト単位、KB 単位、または MB 単位で指定できます。数字に KB、MB のどちらも指定していないと、バイト単位で指定したと見なされます。

デフォルト：5MB

ログファイルの出力量は、Replication Manager で管理しているコピーペアの数に依存します。ログファイルの出力量は次の計算式で求められます。

$\langle \text{出力されるログファイルの情報量 (MB/週間)} \rangle = 0.75 \times \langle \text{コピーペア数} \rangle + 4$

出力される容量と、保持期間を考慮して、agent.logger.MaxBackupIndex と agent.logger.MaxFileSize の値を設定してください。なお、対象のホスト（ペア管理サーバ）で管理しているコピーペア数は、Replication Manager の [<コピーグループ名>] サブウィンドウで確認できます。

関連項目

- [D.2.7 agent.logger.MaxBackupIndex](#)

D.3 Device Manager エージェントの hldutil コマンドの動作に関するプロパティ（hldutil.properties ファイル）

hldutil コマンドの動作に関するプロパティは、hldutil.properties ファイルに含まれています。

- Windows の場合
`<Device Manager エージェントのインストールフォルダ>%util%bin
%hldutil.properties`
- Solaris, Linux, または HP-UX の場合
`/opt/HDVM/HBaseAgent/util/bin/hldutil.properties`
- AIX の場合
`/usr/HDVM/HBaseAgent/util/bin/hldutil.properties`

D.3.1 agent.util.hpux.displayDsf

ホストの OS が HP-UX 11i v3 の場合、hldutil コマンドを実行したときに表示されるデバイスファイル名の形式を指定します。

disk を指定する場合

hldutil コマンドを実行すると、disk デバイスファイルが表示されます。

ctd を指定する場合

hldutil コマンドを実行すると、ctd デバイスファイルが表示されます。

mix を指定する場合

hdutil コマンドを実行すると、disk デバイスファイルおよび ctd デバイスファイルの両デバイスファイルが表示されます。

上記以外の値を指定した場合は、mix を指定したと見なされます。このプロパティを HP-UX 11i v2 以前のバージョンの OS で指定することはできません。また、ほかの OS で指定することもできません。

デフォルト : mix

D.4 Device Manager エージェントのログ出力に関するプロパティ (logger.properties ファイル)

Device Manager エージェントのログ出力に関するプロパティは、logger.properties ファイルに含まれています。

- Windows の場合
 < Device Manager エージェントのインストールフォルダ > %agent%config
 %logger.properties
- Solaris, Linux, または HP-UX の場合
 /opt/HDVM/HBaseAgent/agent/config/logger.properties
- AIX の場合
 /usr/HDVM/HBaseAgent/agent/config/logger.properties



重要 access.log ファイル、error.log ファイル、service.log ファイルおよび trace.log ファイルの出力先は次のとおりです。

Windows の場合

 < Device Manager エージェントのインストールフォルダ > %agent%logs%

Solaris, Linux, または HP-UX の場合

 /opt/HDVM/HBaseAgent/agent/logs/

AIX の場合

 /usr/HDVM/HBaseAgent/agent/logs/

D.4.1 logger.loglevel

trace.log ファイルと error.log ファイルの出力レベルを指定します。

このフィールドで使用できる値は、詳細度が高い順に DEBUG, INFO, WARN, ERROR および FATAL です。デフォルト値の場合、DEBUG のエントリはログに出力されないで、INFO, WARN, ERROR, および FATAL のエントリはログに出力されます。

デフォルト : INFO

D.4.2 logger.MaxBackupIndex

access.log ファイル、error.log ファイル、service.log ファイルおよび trace.log ファイルの最大バックアップファイル数を指定します。

ログファイルが logger.MaxFileSize プロパティで指定された最大長に達すると、access.log.1 のようにカウンターが追加された形式にファイル名が変更されます。ログファイルがさらに作成されると、指定された数のバックアップログファイルが作成されるまで、カウンター

が増加していきます（例えば、`access.log.1` が `access.log.2` になります）。指定された数のバックアップログファイルが作成されたあとは、新しいバックアップログファイルが作成されるたびに、最も古いバックアップログファイルが削除されます。

指定できる値の範囲は、1～20 です。

デフォルト：10

ログファイルの出力量は、**Replication Manager** で管理しているコピーペアの数に依存します。ログファイルの出力量は次の計算式で求められます。

$\text{＜出力されるログファイルの情報量 (MB/週間)＞} = 0.8 \times \text{＜コピーペア数＞} + 25$

出力される容量と、保持期間を考慮して、`logger.MaxBackupIndex` と `logger.MaxFileSize` の値を設定してください。

なお、対象のホスト（ペア管理サーバ）で管理しているコピーペア数は、**Replication Manager** の [`＜コピーグループ名＞`] サブウィンドウで確認できます。

関連項目

- [D.4.3 logger.MaxFileSize](#)

D.4.3 logger.MaxFileSize

`access.log` ファイル、`error.log` ファイル、`service.log` ファイルおよび `trace.log` ファイルの最大サイズを指定します。

ログファイルのサイズが指定値を超えた場合は、新しいログファイルが作成されます。

キロバイト単位るとき **KB**、メガバイト単位るとき **MB** と指定しないかぎり、指定したサイズは、バイト単位であると見なされます。指定できる値の範囲は、512KB～32MB です。

デフォルト：5MB

ログファイルの出力量は、**Replication Manager** で管理しているコピーペアの数に依存します。ログファイルの出力量は次の計算式で求められます。

$\text{＜出力されるログファイルの情報量 (MB/週間)＞} = 0.8 \times \text{＜コピーペア数＞} + 25$

出力される容量と、保持期間を考慮して、`logger.MaxBackupIndex` と `logger.MaxFileSize` の値を設定してください。

なお、対象のホスト（ペア管理サーバ）で管理しているコピーペア数は、**Replication Manager** の [`＜コピーグループ名＞`] サブウィンドウで確認できます。

関連項目

- [D.4.2 logger.MaxBackupIndex](#)

D.5 Device Manager エージェントのプログラム情報に関するプロパティ（`programproductinfo.properties` ファイル）

プログラム情報に関するプロパティは、`programproductinfo.properties` ファイルに含まれています。

ホストの OS が Windows の場合にだけ存在します。

```
< Device Manager エージェントのインストールフォルダ > %agent%config  
%programproductinfo.properties
```

D.5.1 veritas.volume.manager.version

Windows にインストールされている VxVM のバージョンを指定します。

Windows 環境に VxVM がインストールされている場合、VxVM のバージョンをこのプロパティに設定してください。バージョンは、*x.x* の形式で指定します。

デフォルト：なし

D.6 Device Manager エージェントの動作に関するプロパティ (server.properties ファイル)

Device Manager エージェントの動作に関するプロパティは、`server.properties` ファイルに含まれています。

- Windows の場合
 < Device Manager エージェントのインストールフォルダ > %agent%config
 %server.properties
- Solaris, Linux, または HP-UX の場合
 /opt/HDVM/HBaseAgent/agent/config/server.properties
- AIX の場合
 /usr/HDVM/HBaseAgent/agent/config/server.properties

D.6.1 server.agent.port

Device Manager エージェントのデーモンプロセス (またはサービス) で使用するポートを指定します。

ほかのサービスと競合するおそれがあるので、小さい数字のポートは避けてください。通常は、1024~49151 の範囲で指定します。バージョン 05-80 より前の Dynamic Link Manager がインストールされている場合は 23013 を設定してください。

なお、ホストの OS が Windows の場合、使用するポートを変更したら、`firewall_setup` コマンドでファイアウォールの例外登録を再設定してください。

デフォルト：24041

D.6.2 server.http.localPort

Device Manager エージェントのデーモンプロセスと Web サーバプロセスとの間の通信に使用するポートを指定します。

ほかのサービスと競合するおそれがあるので、小さい数字のポートは避けてください。通常は、1024~49151 の範囲で指定します。

なお、ホストの OS が Windows の場合、使用するポートを変更したら、`firewall_setup` コマンドでファイアウォールの例外登録を再設定してください。

デフォルト：24043

D.6.3 server.http.port

Device Manager エージェントの Web サーバ機能が使用するポートを指定します。

ほかのサービスと競合するおそれがあるので、小さい数字のポートは避けてください。通常は、1024～49151 の範囲を選択します。バージョン 05-80 より前の Dynamic Link Manager がインストールされている場合は 23011 を設定してください。

なお、ホストの OS が Windows の場合、使用するポートを変更したら、`firewall_setup` コマンドでファイアウォールの例外登録を再設定してください。

デフォルト：24042

D.6.4 server.http.host

Device Manager エージェントの Web サーバ機能が動作するホストのホスト名を指定します。

デフォルト：localhost

D.6.5 server.http.socket.agentAddress

Device Manager エージェントが Device Manager サーバに通知する IP アドレスを指定します。

Device Manager エージェントが Device Manager サーバに通知する IP アドレスを限定するため、通知する IP アドレスを指定してください。

IPv6 環境で運用する場合は、グローバルアドレスを指定してください。サイトローカルアドレスまたはリンクローカルアドレスを指定した場合は IPv4 アドレスで動作します。

指定する IP アドレスのバージョンは `server.http.socket.bindAddress` と合わせてください。

ここで指定した IP アドレスは、RAID Manager または P9000 RAID Manager の構成定義ファイルの作成や編集でも使用されます。RAID Manager または P9000 RAID Manager と併用する場合は、指定したアドレスで RAID Manager または P9000 RAID Manager のインスタンス間で通信ができることを確認しておいてください。

デフォルト：なし※

注※ 指定されていない場合、Device Manager エージェントが取得した IP アドレスで動作します。IP アドレスが複数ある場合は、Device Manager エージェントが API によって取得した 1 つ目の IP アドレスで動作します。

関連項目

- [D.6.6 server.http.socket.bindAddress](#)

D.6.6 server.http.socket.bindAddress

Device Manager エージェントが 2 つ以上のネットワークインターフェース (NIC) を搭載したプラットフォーム上で動作する場合、Device Manager エージェントが要求を受け付ける NIC を指定します。

受け付けるインターフェースを限定したい場合には、Device Manager エージェントが受け付ける IP アドレスを指定してください。

IPv6 環境で運用する場合は、グローバルアドレスを指定してください。サイトローカルアドレスまたはリンクローカルアドレスを指定した場合はデフォルト値で動作します。

指定する IP アドレスのバージョンは `server.http.socket.agentAddress` と合わせてください。

デフォルト：なし（Device Manager エージェントはすべての NIC で要求を受け付けます）

関連項目

- [D.6.5 server.http.socket.agentAddress](#)

D.6.7 server.agent.maxMemorySize

Device Manager エージェントの Web サーバ機能のプロセスの最大メモリーヒープサイズを指定します（単位：MB）。

32～4096 の範囲で指定します。

デフォルト：指定なし※

注※ 64MB で動作します。Solaris（x64 Edition（AMD64））の場合は、物理メモリーの 1/4 または 1GB のどちらか小さい方で動作します。



注意 Device Manager と Replication Manager の両方を使用している場合は、それぞれに必要なメモリーサイズの合計値を指定してください。

関連項目

- Device Manager で必要なメモリーサイズの詳細：[11.2.5 ホストで 100 個以上の LU を管理する場合に必要な設定](#)
- Replication Manager で必要なメモリーサイズの詳細：[11.2.4 コピーペアを管理するために必要な設定](#)

D.6.8 server.agent.shutDownTime

Device Manager エージェントの Web サーバ機能が最後の HTTP/XML メッセージを送信または受信してから停止するまでの時間を指定します（単位：ミリ秒）。

1～9223372036854775807 の範囲で指定します。

Device Manager エージェントの性能に関する最新の知識がない場合は、このプロパティを編集しないでください。

デフォルト：600000

D.6.9 server.agent.JRE.location

Device Manager エージェント用の Java の実行環境を提供するプログラムのインストール先を絶対パスで指定します。

Windows の場合は、パスの区切り文字にスラント (*/*) を指定してください。

デフォルト：Device Manager エージェントが使用している Java の実行環境のインストールパス



注意

- ホストの OS が Windows または Linux の場合、プロパティの指定がないときは、Device Manager エージェントに同梱された Java の実行環境が使用されます。
- 次の場合、32 ビット用の Java の実行環境を使用してください。

- ・ホストの OS が Windows のとき
 - ・ホストの OS が Linux で、CIM/WBEM 機能を利用してエンタープライズクラスストレージの性能情報を取得するとき
 - ・Dynamic Link Manager がホストにインストールされているとき
-

D.6.10 server.http.entity.maxLength

Device Manager エージェントの Web サーバ機能が許容する HTTP 要求エンティティの最大長を指定します (単位: バイト)。

通常、この設定を変更する必要はありません。この設定では、異常に大きなデータ量のエンティティを持つ要求を制限することで、サービス妨害攻撃やバッファオーバーフローをねらった攻撃を防ぐのに役立ちます。Device Manager エージェントがこれより長いポスト要求を検出すると、リモートにエラー応答を送り、その要求の詳細をログに記録します。

デフォルト: 32768

D.6.11 server.http.security.clientIP

Device Manager エージェントに接続できる IPv4 および IPv6 のアドレスを指定します。

この設定は、接続できる IP アドレスを制限することで、サービス妨害攻撃やバッファオーバーフローをねらった攻撃を防ぐのに役立ちます。

IPv4 アドレスの場合はアスタリスク (*) をワイルドカード文字として使用できます。IP アドレスを複数指定する場合は、コンマ (,) で区切ります。

191.0.0.2 と 192.168.0.0~192.168.255.255 の接続を許可する場合の指定例を次に示します。

```
server.http.security.clientIP=191.0.0.2, 192.168.*.*
```

2001::203:baff:fe36:109a と 2001::203:baff:fe5b:7bac の接続を許可する場合の指定例を次に示します。

```
server.http.security.clientIP=2001::203:baff:fe36:109a,  
2001::203:baff:fe5b:7bac
```

デフォルト: 指定なし (すべての IP アドレスが接続できます)

D.6.12 server.server.authorization

このプロパティには、Device Manager サーバの認証に使用するユーザー ID とパスワードが格納されています。

このプロパティは暗号化されているため、テキストエディターでは編集できません。このプロパティを編集するためには、hdvmagt_setting コマンドを使用します。

デフォルト: なし

D.6.13 server.server.serverIPAddress

Device Manager サーバの IP アドレスまたはホスト名を指定します。

IP アドレスを指定する場合

IPv4 の場合、ドット付きの 10 進数で指定します。

IPv6 の場合、コロン付きの 16 進数で指定します。省略形も使用できます。IPv6 アドレスでの指定例を次に示します。

```
server.server.serverIPAddress=2001::214:85ff:fe02:e53b
```

ホスト名を指定する場合

ホスト名は 50 バイト以内の文字列で指定できます。使用できる文字を次に示します。

```
a~z A~Z 0~9 - . @ _
```

デフォルト : 255.255.255.255

D.6.14 server.server.serverPort

Device Manager エージェントの接続先の Device Manager サーバのポートを指定します。

一般的な規則として 1024~49151 の範囲で指定できますが、Device Manager サーバの server.http.port プロパティに指定した値と同じ値を指定する必要があります。

デフォルト : 2001

関連項目

- [A.2.2 server.http.port](#)

D.6.15 server.agent.rm.centralizePairConfiguration

コピーペアを管理するとき、ホストごとにコピーペアを管理するか、1 台のホストですべてのコピーペアを一括管理するかを指定します。

disable

ホストごとにコピーペアを管理する、通常構成の場合に指定します。通常構成では、各ホストに Device Manager エージェントと RAID Manager または P9000 RAID Manager をインストールする必要があります。

通常構成でホストが異なる LU 同士をコピーペアとする場合は、それぞれの LU が各ホストで認識されていることを確認してください。

enable

1 台のホスト（ペア管理サーバ）ですべてのコピーペアを管理する、一括管理構成の場合に指定します。一括管理構成では、ペア管理サーバに Device Manager エージェントと RAID Manager または P9000 RAID Manager をインストールすれば、そのほかのホストには Device Manager エージェントをインストールするだけで運用できます。

一括管理構成では、ペア管理サーバが各ストレージシステムのコマンドデバイスを認識していれば、各ストレージシステムのホストが認識していない LU も含めて、すべての LU を使用してコピーペアを作成できます。

デフォルト : disable

D.6.16 server.agent.rm.cuLdevForm

ペアを作成する際、構成定義ファイルにペアボリュームの情報を HORCM_LDEV 形式で記載する場合の LDEV 番号の出力形式を指定します。

指定を省略した場合は、10 進数で出力されます。

DECIMAL

10 進数で出力する場合に指定します。

CULDEV

CU:LDEV 形式で出力する場合に指定します。

HEXA

16 進数で出力する場合に指定します。

このプロパティは、Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, SANRISE9900V または HUS VM にコピーペアを作成する場合にだけ有効です。また、対象のコピーペアのコマンドデバイスに仮想コマンドデバイスを使用している場合 (HORCM_CMD パラメーターに IPCMD 形式でコマンドデバイスを設定している場合) は、設定した値に関係なく 10 進数で出力されます。

デフォルト : CULDEV

D.6.17 server.agent.rm.exclusion.instance

Device Manager エージェントがインストールされているホスト上で、すでに RAID Manager または P9000 RAID Manager によって管理されているペアボリュームを Device Manager の操作対象から外す場合に、RAID Manager または P9000 RAID Manager のインスタンス番号を指定します。

Device Manager の操作対象から外した場合は、Replication Manager でも操作対象外になります。複数のインスタンス番号を指定する場合は、個々の番号をコンマ (,) で区切ります。Device Manager エージェントからは、このプロパティで指定したインスタンス番号を持つ RAID Manager または P9000 RAID Manager を操作できません。

デフォルト : なし

D.6.18 server.agent.rm.location

RAID Manager がデフォルト以外の場所にインストールされている場合、またはホストの OS が Windows で RAID Manager のインストールドライブと Device Manager エージェントのインストールドライブが異なる場合に、RAID Manager のインストールディレクトリを指定します。

Windows の場合は、パスの区切り文字にスラント (/) を指定してください。

デフォルト (Windows の場合) : < Device Manager エージェントのインストールドライブ > / HORCM

デフォルト (UNIX の場合) : /HORCM

D.6.19 server.agent.rm.optimization.userHorcmFile

ユーザーが作成した RAID Manager または P9000 RAID Manager の構成定義ファイルを最適化の対象とするかどうかを指定します。

RAID Manager または P9000 RAID Manager の構成定義ファイルを最適化の対象とする場合は、true を指定します。この場合、ユーザーが作成した RAID Manager または P9000 RAID Manager の構成定義ファイルを、Device Manager で使用できるよう更新します。このほか、次に示す最適化処理を実施します。最適化処理は、Device Manager エージェントの起動時およびペア操作で構成定義ファイルが更新されるタイミングで実施されます。

- コマンドデバイスにユニット ID, LDEV 番号およびシリアル番号をコメントとして追加する
- シリアル番号がコメントに記載されているコマンドデバイスがボリューム名の変更などによって使用できない状態の場合、使用できるコマンドデバイスに変更する

- ホストがストレージシステム内の複数のコマンドデバイスと接続されている状態で、一部のコマンドデバイスしか指定されていない場合、残りのコマンドデバイスを予備のコマンドデバイスとして設定する
- 使われていないコマンドデバイスを削除する
- コマンドデバイス、ペアボリュームの CU 番号、LDEV 番号を `cu:ldev` の形式でコメントとして追加する
- SLPR 環境で同一ストレージシステムのコマンドデバイスの定義が複数ある場合、コマンドデバイスの定義を並び替える
- 構成定義ファイルの `HORCM_MON` パラメーターの `poll` に、`server.agent.rm.horcm.poll` プロパティに設定された値を反映する

デフォルト：false

D.6.20 server.agent.rm.horcm.poll

構成定義ファイルの `HORCM_MON` パラメーターの `poll` に設定する値（コピーペアをモニタリングする間隔）を 10 ミリ秒単位で指定します。

モニタリングしない場合は -1 を指定してください。

このプロパティに指定した値は、次のタイミングで構成定義ファイルに反映されます。

- ペアを作成または追加したとき
- 構成定義ファイルが最適化されたとき

デフォルト：なし※

注※ 構成定義ファイルが新規作成された際は `poll` に 1000 が設定されます。また、既存の構成定義ファイルにペアが追加された際や、構成定義ファイルが最適化された際には、元の設定値が維持されます。

D.6.21 server.agent.rm.temporaryInstance

Device Manager エージェントがコピーペアの情報を取得する際に、一時的に使用する構成定義ファイルのインスタンス番号を指定します。

0～3997 の範囲で指定します。

<指定した値>～<指定した値>+98 のインスタンス番号が使用されます。

デフォルト：900

D.6.22 server.agent.rm.temporaryPort

Device Manager エージェントがコピーペアの情報を取得する際に、一時的に使用する構成定義ファイルの UDP ポート番号を指定します。

1～65437 の範囲で指定します。

<指定した値>～<指定した値>+98 の UDP ポート番号が使用されます。

デフォルト：53232

D.6.23 server.agent.rm.pairDefinitionForm

ペアを作成するとき、構成定義ファイルにペアボリュームの情報を HORCM_DEV 形式で記述するか、HORCM_LDEV 形式で記述するかを指定します。

HORCM_DEV 形式に統一したい場合は HORCM_DEV、HORCM_LDEV 形式に統一したい場合は HORCM_LDEV を指定します。HORCM_LDEV 形式で運用することを推奨します。

ただし、メインフレームボリュームのコピーペアを作成するとき、プロパティで指定している形式に関係なく、HORCM_LDEV 形式で構成定義ファイルに記述します。

デフォルト：HORCM_LDEV

Device Manager エージェントは、次に示す条件によって、ペアを作成するとき構成定義ファイルに記述する形式を決定します。

- 既存の構成定義ファイルに HORCM_DEV 形式または HORCM_LDEV 形式のどちらで記述されているか
- ペアを作成する対象のグループが新規のグループか既存のグループか

Device Manager エージェントが HORCM_DEV 形式または HORCM_LDEV 形式のどちらで記述するかを決める条件を次の表に示します。

表 D-2 Device Manager エージェントが構成定義ファイルに記述する形式を決める条件

既存の構成定義ファイルの記述	ペアの操作	構成定義ファイルに記述する形式
記述なし	新規のコピーグループにペアを作成する場合	プロパティで形式を指定している場合： プロパティで設定した形式 プロパティで形式を指定していない場合： HORCM_DEV 形式
HORCM_DEV 形式で記述されている場合	既存のコピーグループにペアを追加する場合	プロパティで指定している形式に関係なく HORCM_DEV 形式
	新規のコピーグループにペアを作成する場合	プロパティで形式を指定している場合： プロパティで設定した形式 プロパティで形式を指定していない場合： HORCM_DEV 形式
HORCM_LDEV 形式で記述されている場合	既存のコピーグループにペアを追加する場合	プロパティで指定している形式に関係なく HORCM_LDEV 形式
	新規のコピーグループにペアを作成する場合	プロパティで形式を指定している場合： プロパティで設定した形式 プロパティで形式を指定していない場合： HORCM_LDEV 形式
HORCM_DEV 形式の記述と HORCM_LDEV 形式の記述の両方が混在する場合	HORCM_DEV 形式で記述された既存のコピーグループにペアを追加する場合	プロパティで指定している形式に関係なく HORCM_DEV 形式
	HORCM_LDEV 形式で記述された既存のコピーグループにペアを追加する場合	プロパティで指定している形式に関係なく HORCM_LDEV 形式
	HORCM_DEV 形式と HORCM_LDEV 形式の両方で記述された既存のコピーグループにペアを追加する場合	プロパティで形式を指定している場合： プロパティで設定した形式

既存の構成定義ファイルの記述	ペアの操作	構成定義ファイルに記述する形式
		プロパティで形式を指定していない場合： HORCM_DEV 形式
	新規のコピーグループにペアを作成する場合	プロパティで形式を指定している場合： プロパティで設定した形式 プロパティで形式を指定していない場合： HORCM_DEV 形式



注意 HORCM_LDEV を指定する場合、RAID Manager 01-17-03/04 以降または P9000 RAID Manager 01.17.04 以降がインストールされている必要があります。RAID Manager のバージョンが 01-17-03/04 より前、または P9000 RAID Manager のバージョンが 01.17.04 より前のときに HORCM_LDEV を指定すると、「ペアの作成に失敗しました。ホスト"<ホスト名>"のエラー詳細："<エラーの詳細>"というメッセージが表示され、ペアの作成に失敗します。

D.6.24 server.agent.rm.userAuthentication

コマンドデバイスの認証モードが有効になっていることをチェックするかどうかを指定します。

true を指定した場合、認証モードが有効になっていることをチェックします。false を指定した場合はチェックしません。

デフォルト：true



注意 false を指定する場合は、Device Manager エージェントがインストールされているホストに、認証モードが有効なコマンドデバイスが 1 つも接続されていないことを確認してください。コマンドデバイスの認証モードが有効になっている状態で false を指定した場合、ペア状態の取得やペア操作が正常に行えません。

D.6.25 server.agent.rm.ignorePairStatus

Device Manager エージェントから管理サーバにホスト情報を送信する際、コピーペア情報を省くかどうかを指定します。

コピーペア情報を省く場合は true を、省かない場合は false を指定します。

次のマシンでは true を指定してください。

- コピーペアが割り当てられている仮想マシン
- 仮想コマンドデバイスに SVP を使用して、デバイスグループとして定義されたコピーペアを管理する場合の管理サーバ
管理サーバに P-VOL および S-VOL を割り当てている構成の場合に設定が必要です。

デフォルト：false

D.6.26 server.agent.rm.horcmSource

RAID Manager または P9000 RAID Manager の構成定義ファイルをデフォルト以外の場所に格納する場合、構成定義ファイルの格納場所を絶対パスで指定します。

パスは次の規則に従って指定してください。

- Windows の場合、パスの区切り文字にスラント (/) を指定してください。
- Windows の場合、パス中に空白文字が含まれるときは、パスを引用符 (") で囲む必要はありません。

- ・ シンボリックリンクは指定できません。

デフォルト：なし※

注※ 指定されていない場合、次に示すデフォルトの格納場所が指定されたものとして動作します。

Windows の場合

システムフォルダ（環境変数"%windir%"で表されるフォルダ）

UNIX の場合

/etc ディレクトリ

関連項目

- ・ [11.4.3 構成定義ファイルの格納場所の変更](#)

D.6.27 server.agent.rm.moduleTimeOut

Device Manager エージェントが RAID Manager または P9000 RAID Manager のコマンドを実行したときに、コマンド実行結果が戻されるまでのタイムアウト値を指定します（単位：秒）。

あるコマンドを実行するのにこのプロパティの設定値より長い時間が掛かった場合、Device Manager エージェントは、コマンド実行中にエラーが発生したと判断します。

専門知識のあるシステム管理者が Device Manager エージェントのペア構成機能のパフォーマンスを微調整する場合だけ、この設定値を変更してください。

デフォルト：600

D.6.28 server.http.server.timeOut

HiScan コマンドの実行、サービスの再起動、ホストリフレッシュの実行などによって Device Manager サーバにホスト情報を登録する場合の、Device Manager サーバからの応答待ち時間の最大値を指定します（単位：秒）。

このプロパティで指定された時間を超えても Device Manager サーバから応答がない場合は異常と判断し、HiScan コマンドが異常終了します。

100～3600 の範囲で指定します。最小値より小さい値を指定した場合は 100、最大値より大きい値を指定した場合は 3600 が指定されたものとして動作します。

デフォルト：600

D.6.29 server.util.processTimeOut

Device Manager エージェントが正常実行と見なす外部プログラムの実行時間を指定します（単位：ミリ秒）。

外部プログラムの実行時間がこのプロパティで指定した時間より長い場合、Device Manager エージェントはそのプログラムを異常と判断して、プログラムを終了します。このプロパティの値が小さ過ぎると、正常に動作している外部プログラムが停止される場合があります。Device Manager エージェントの性能に関する最新の知識がない場合は、このプロパティを編集しないでください。

デフォルト：600000

D.6.30 server.agent.evtwait.timeout

リモートペアをリストアする際に、pair 状態になるまでの待ち時間を指定します（単位：秒）。

指定した時間を過ぎた場合には処理がエラーになります。

1～1999999 の範囲で指定します。

デフォルト：3600

D.6.31 server.agent.rmexp.location

P9000 RAID Manager がデフォルト以外の場所にインストールされている場合、またはホストの OS が Windows で P9000 RAID Manager のインストールドライブと Device Manager エージェントのインストールドライブが異なる場合に、P9000 RAID Manager のインストールディレクトリを指定します。

Windows の場合は、パスの区切り文字にスラント (/) を指定してください。

デフォルト (Windows の場合) : < Device Manager エージェントのインストールドライブ > / HORCM

デフォルト (UNIX の場合) : /HORCM

このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報を示します。

- E.1 関連マニュアル
- E.2 このマニュアルでの表記
- E.3 このマニュアルで使用している略語
- E.4 KB（キロバイト）などの単位表記について

E.1 関連マニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

- *Hitachi Command Suite Software ユーザーズガイド* (3020-3-W02)
- *Hitachi Command Suite Software CLI リファレンスガイド* (3020-3-W03)
- *Hitachi Command Suite Tiered Storage Manager Software CLI リファレンスガイド* (3020-3-W04)
- *Hitachi Command Suite Software メッセージガイド* (3020-3-W05)
- *Hitachi Command Suite Software インストールガイド* (3020-3-W07)
- *Hitachi Command Suite Software Mainframe Agent ユーザーズガイド* (3020-3-W09)
- *Hitachi Command Suite Software Plug-in for Virtualization Server Provisioning ユーザーズガイド* (3020-3-W25)
- *Hitachi Command Suite Tuning Manager Software 運用管理ガイド* (3020-3-W41)
- *Hitachi Command Suite Tuning Manager Software インストールガイド* (3020-3-W42)
- *Hitachi Command Suite Tuning Manager Software ユーザーズガイド* (3020-3-W43)
- *Hitachi Command Suite Tuning Manager - Agent for RAID* (3020-3-W44)
- *Hitachi Command Suite Replication Manager Software ユーザーズガイド* (3020-3-W81)
- *Hitachi Command Suite Replication Manager Software システム構成ガイド* (3020-3-W82)

E.2 このマニュアルでの表記

このマニュアルでは、製品の名称を省略して表記しています。このマニュアルでの表記と、製品の正式名称または意味を次に示します。

表記	製品名
AIX 5.2	AIX 5L Version 5.2
AIX 5.3	AIX 5L Version 5.3
Business Continuity Manager	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none">• Hitachi Business Continuity Manager Basic• Hitachi Business Continuity Manager Extended CT Group• Hitachi Business Continuity Manager UR 4x4 Extended CTG• Hitachi Business Continuity Manager UR 4x4 Extended CTG Software
BR150	BladeSymphony 専用エントリークラスディスクアレイ装置 BR150
BR1600	エントリークラスディスクアレイ装置 BR1600
BR1600E	エントリークラスディスクアレイ装置 BR1600E
BR1600S	エントリークラスディスクアレイ装置 BR1600S
BR1600 シリーズ	エントリークラスディスクアレイ装置 BR1600 シリーズ
BR1650E	エントリークラスディスクアレイ装置 BR1650E
BR1650S	エントリークラスディスクアレイ装置 BR1650S
BR50	BladeSymphony 専用エントリークラスディスクアレイ装置 BR50
Compute Systems Manager	Hitachi Compute Systems Manager
Copy-on-Write Snapshot	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none">• Hitachi Copy-on-Write Snapshot Software• Copy-on-Write Snapshot• Copy-on-write SnapShot

表記	製品名
	<ul style="list-style-type: none"> Snapshot XP
DAMP	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> ディスクアレイ管理プログラム 2 Disk Array Management Program 2
Device Manager	Hitachi Device Manager
Dynamic Link Manager	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Dynamic Link Manager Hitachi Dynamic Link Manager EX
Dynamic Provisioning	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Dynamic Provisioning Software Dynamic Provisioning Thin Provisioning
Firefox	Firefox®
Global Link Manager	Hitachi Global Link Manager
H128	SANRISE H128
H1024	SANRISE H1024
H10000	Hitachi Universal Storage Platform H10000
H12000	Hitachi Universal Storage Platform H12000
H20000	Hitachi Universal Storage Platform H20000
H24000	Hitachi Universal Storage Platform H24000
H48/H512	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> SANRISE H48 SANRISE H512
H128/H1024	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> SANRISE H128 SANRISE H1024
H10000/H12000	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Universal Storage Platform H10000 Hitachi Universal Storage Platform H12000
H20000/H24000	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Universal Storage Platform H20000 Hitachi Universal Storage Platform H24000
HAM	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi High Availability Manager Hitachi High Availability Manager Software
HDP	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Dynamic Provisioning Thin Provisioning
HDT	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Dynamic Tiering Software P9000 Smart Tiers
Hitachi AMS	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Adaptable Modular Storage シリーズ BladeSymphony 専用エントリークラスディスクアレイ装置 BR150
Hitachi AMS/WMS	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Adaptable Modular Storage シリーズ Hitachi Tape Modular Storage シリーズ Hitachi Workgroup Modular Storage シリーズ BladeSymphony 専用エントリークラスディスクアレイ装置 BR150 BladeSymphony 専用エントリークラスディスクアレイ装置 BR50

表記	製品名
Hitachi AMS 200	Hitachi Adaptable Modular Storage 200
Hitachi AMS 500	Hitachi Adaptable Modular Storage 500
Hitachi AMS 1000	Hitachi Adaptable Modular Storage 1000
Hitachi AMS 2000	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Hitachi Adaptable Modular Storage 2000 シリーズ エントリークラスディスクアレイ装置 BR1600 シリーズ
Hitachi AMS 2010	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Hitachi Adaptable Modular Storage 2010 エントリークラスディスクアレイ装置 BR1600S
Hitachi AMS 2100	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Hitachi Adaptable Modular Storage 2100 エントリークラスディスクアレイ装置 BR1600 エントリークラスディスクアレイ装置 BR1600E
Hitachi AMS 2300	Hitachi Adaptable Modular Storage 2300
Hitachi AMS 2500	Hitachi Adaptable Modular Storage 2500
Hitachi NSC 55	Hitachi Network Storage Controller 55
Hitachi SMS	Hitachi Simple Modular Storage シリーズ
Hitachi TMS	Hitachi Tape Modular Storage シリーズ
Hitachi TMS1000	Hitachi Tape Modular Storage 1000
Hitachi USP	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Hitachi Universal Storage Platform Hitachi Network Storage Controller Hitachi Universal Storage Platform H12000 Hitachi Universal Storage Platform H10000
Hitachi USP 100	Hitachi Universal Storage Platform 100
Hitachi USP 600	Hitachi Universal Storage Platform 600
Hitachi USP 1100	Hitachi Universal Storage Platform 1100
Hitachi WMS	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Hitachi Workgroup Modular Storage シリーズ BladeSymphony 専用エントリークラスディスクアレイ装置 BR50
Hitachi WMS 100	Hitachi Workgroup Modular Storage 100
HORCM	Hitachi Open Remote Copy Manager
HUS100	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Hitachi Unified Storage 150 Hitachi Unified Storage 130 Hitachi Unified Storage 110 エントリークラスディスクアレイ装置 BR1650 シリーズ
HUS110	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Hitachi Unified Storage 110 エントリークラスディスクアレイ装置 BR1650S
HUS130	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Hitachi Unified Storage 130 エントリークラスディスクアレイ装置 BR1650E
HUS150	Hitachi Unified Storage 150
HUS VM	Hitachi Unified Storage VM
H シリーズ	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Hitachi Virtual Storage Platform VP9500 Hitachi Universal Storage Platform H24000 Hitachi Universal Storage Platform H20000

表記	製品名
	<ul style="list-style-type: none"> Hitachi Universal Storage Platform H12000 Hitachi Universal Storage Platform H10000 SANRISE H1024 SANRISE H512 SANRISE H128 SANRISE H48
JDK	Java Development Kit
JP1/AJS2 - Scenario Operation	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> JP1/Automatic Job Management System 2 - Scenario Operation Manager JP1/Automatic Job Management System 2 - Scenario Operation View
JP1/IM	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> JP1/Integrated Management - Manager JP1/Integrated Management - View JP1/Integrated Manager - Central Console JP1/Integrated Manager - Console View JP1/Integrated Manager - View
JP1/IM - Manager	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> JP1/Integrated Management - Manager JP1/Integrated Manager - Central Console
JP1/IM - View	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> JP1/Integrated Management - View JP1/Integrated Manager - Console View JP1/Integrated Manager - View
JRE	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Java Runtime Environment Java 2 Runtime Environment
Linux	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Red Hat Enterprise Linux[®] SUSE Linux[®] Enterprise Server Oracle Linux[®]
Mainframe Agent	Hitachi Device Manager Mainframe Agent
P9000 RAID Manager	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> RAID Manager XP P9000 RAID Manager
PFM - Base	JP1/Performance Management - Base
PFM - Manager	JP1/Performance Management - Manager
Performance Monitor	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Performance Management - Base Monitor Performance Monitor
Protection Manager	Hitachi Protection Manager
QuickShadow	Hitachi QuickShadow
RAID Manager	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> RAID Manager RAID Manager XP P9000 RAID Manager
Replication Manager	Hitachi Replication Manager
Replication Monitor	JP1/HiCommand Replication Monitor
SANRISE9500V	SANRISE9500V シリーズ
SANRISE9900V	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> SANRISE9900V シリーズ

表記	製品名
	<ul style="list-style-type: none"> • SANRISE H1024 • SANRISE H128
ShadowImage	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> • Business Copy XP • Business Copy/Snapshot • Business Copy for Mainframe • Hitachi Open Multiple RAID Coupling Feature • Hitachi ShadowImage • Hitachi ShadowImage for Mainframe • Hitachi ShadowImage Software • Hitachi ShadowImage Software for Mainframe • ShadowImage • ShadowImage in-system replication
Storage Navigator	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> • Storage Navigator • Remote Web Console
Storage Navigator Modular 2	Hitachi Storage Navigator Modular 2
SUSE Linux Enterprise Server	SUSE Linux® Enterprise Server
Thin Image	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> • Fast Snap • Hitachi Thin Image
Tiered Storage Manager	Hitachi Tiered Storage Manager
TrueCopy	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> • Continuous Access XP Asynchronous • Continuous Access XP Synchronous • Continuous Access Synchronous • Continuous Access Synchronous for Mainframe • Hitachi Open Remote Copy • Hitachi Open Remote Copy Asynchronous • Hitachi TrueCopy • Hitachi TrueCopy Asynchronous • Hitachi TrueCopy Asynchronous for Mainframe • Hitachi TrueCopy Basic • Hitachi TrueCopy for Mainframe • Hitachi TrueCopy Software • Hitachi TrueCopy Software for Mainframe • TrueCopy • TrueCopy Asynchronous • TrueCopy Extended Distance • TrueCopy remote replication • 日立同期リモートコピー(SRC: Synchronous Remote Copy)
TrueCopy Async	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> • Continuous Access XP Asynchronous • Hitachi Open Remote Copy Asynchronous • Hitachi TrueCopy Asynchronous • Hitachi TrueCopy Asynchronous for Mainframe • TrueCopy Asynchronous • TrueCopy Extended Distance
TrueCopy Sync	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> • Continuous Access XP Synchronous • Continuous Access Synchronous

表記	製品名
	<ul style="list-style-type: none"> Continuous Access Synchronous for Mainframe Hitachi Open Remote Copy Hitachi TrueCopy Hitachi TrueCopy Basic Hitachi TrueCopy for Mainframe Hitachi TrueCopy Software Hitachi TrueCopy Software for Mainframe TrueCopy TrueCopy remote replication 日立同期リモートコピー(SRC: Synchronous Remote Copy)
Tuning Manager	Hitachi Tuning Manager
Universal Replicator	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Continuous Access XP Journal Continuous Access Journal Continuous Access Journal for Mainframe Hitachi Universal Replicator for Mainframe Hitachi Universal Replicator Software Hitachi Universal Replicator Software for Mainframe Universal Replicator
Universal Storage Platform V	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Universal Storage Platform V Hitachi Universal Storage Platform H24000
Universal Storage Platform V/VM	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Universal Storage Platform V Hitachi Universal Storage Platform VM Hitachi Universal Storage Platform H24000 Hitachi Universal Storage Platform H20000
Universal Storage Platform VM	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Universal Storage Platform VM Hitachi Universal Storage Platform H20000
Universal Volume Manager	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Universal Volume Manager External Storage XP
UNIX	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Solaris AIX Linux[®] HP-UX
Veritas Cluster Server	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> VERITAS Cluster Server 4.0 VERITAS Cluster Server 4.1 MP2 Veritas Cluster Server 5.0 MP1
Virtual Partition Manager	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Virtual Partition Manager Hitachi Virtual Partition Manager Software Disk/Cache Partition
Virtual Storage Platform	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Hitachi Virtual Storage Platform Hitachi Virtual Storage Platform VP9500
vMA	VMware vSphere [®] Management Assistant
VMware	VMware [®]
VMware ESX	次の製品を区別する必要がない場合の表記です。

表記	製品名
	<ul style="list-style-type: none"> VMware vSphere® ESX VMware vSphere® ESXi™
VMware vCenter Server	VMware vCenter™ Server
VP9500	Hitachi Virtual Storage Platform VP9500
VxVM	Veritas Volume Manager
エンタープライズクラスストレージ	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> Virtual Storage Platform Universal Storage Platform V/VM Hitachi USP SANRISE9900V
ミッドレンジストレージ	<p>次の製品を区別する必要がない場合の表記です。</p> <ul style="list-style-type: none"> HUS100 Hitachi AMS2000 Hitachi SMS Hitachi AMS/WMS SANRISE9500V

E.3 このマニュアルで使用している略語

このマニュアルで使用する主な英略語を次に示します。

略語	正式名称
AES	Advanced Encryption Standard
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CHA	CHannel Adapter
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIM	Common Information Model
CIMOM	CIM Object Manager
CLI	Command Line Interface
CLPR	Cache Logical PaRtition
CN	Common Name
CPU	Central Processing Unit
CSR	Certificate Signing Request
CSV	Comma Separated Value
CU	Control Unit
CVS	Custom Volume Size
DBMS	DataBase Management System
DCR	Dynamic Cache Residency
DER	Distinguished Encoding Rules
DKC	DisK Controller
DM-LU	Differential Management LU
DMP	Dynamic MultiPathing

略語	正式名称
DMTF	Distributed Management Task Force
DN	Distinguished Name
DNS	Domain Name System
DoS	Denial of Services
EVS	Enterprise Virtual Server
FC	Fibre Channel
FC-SP	Fibre Channel - Security Protocol
FCoE	Fibre Channel over Ethernet
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GUI	Graphical User Interface
HBA	Host Bus Adapter
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
I/O	Input/Output
ID	IDentifier
IETF	Internet Engineering Task Force
IOPS	Input Output Per Second
IP	Internet Protocol
IP-SAN	Internet Protocol Storage Area Network
IPF	Itanium [®] Processor Family
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
iSCSI	Internet Small Computer System Interface
JAR	Java ARchiver
LAN	Local Area Network
LBA	Logical Block Addressing
LDAP	Lightweight Directory Access Protocol
LDEV	Logical DEvice
LDKC	Logical DisK Controller
LU	Logical Unit
LUN	Logical Unit Number
LUSE	Logical Unit Size Expansion
MCU	Main Control Unit
MOF	Managed Object Format
MU	Multiple Unit
NAS	Network Attached Storage
NAT	Network Address Translation
NIC	Network Interface Card
NPIV	N Port ID Virtualization
NTP	Network Time Protocol
OS	Operating System
P-VOL	Primary VOLume

略語	正式名称
PAP	Password Authentication Protocol
PDEV	Physical DEvice
PEM	Privacy Enhanced Mail
PID	Process ID
PNG	Portable Network Graphics
PP	Program Product
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RCU	Remote Control Unit
RDN	Relative Distinguished Name
RFC	Request For Comments
RMI	Remote Method Invocation
S-VOL	Secondary VOLume
SAN	Storage Area Network
SCSI	Small Computer System Interface
SED	Stack Execution Disable
SIM	Service Information Message
SLP	Service Location Protocol
SLPR	Storage Logical PaRtition
SMI-S	Storage Management Initiative - Specification
SMTP	Simple Mail Transfer Protocol
SNIA	Storage Networking Industry Association
SNIA-CTP	SNIA Conformance Testing Program
SNMP	Simple Network Management Protocol
SP	Service Pack
SRV	SeRVice
SSH	Secure SHell
SSID	Storage System ID
SSL	Secure Sockets Layer
SSO	Single Sign - On
SVP	SerVice Processor
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
V-VOL	Virtual VOLume
WAN	Wide Area Network
WBEM	Web - Based Enterprise Management
WWN	World Wide Name
XML	eXtensible Markup Language

E.4 KB（キロバイト）などの単位表記について

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 $1,024$ バイト、 $1,024^2$ バイト、 $1,024^3$ バイト、 $1,024^4$ バイトです。

索引

A

account.lock.num 120
agent.logger.loglevel 476
agent.logger.MaxBackupIndex 476
agent.logger.MaxFileSize 477
agent.properties ファイル 474
agent.rm.everytimeShutdown 475
agent.rm.horcmInstance 475
agent.rm.horcmService 476
agent.rm.shutdownWait 475
agent.rm.TimeOut 475
agent.util.hpux.displayDsf 477
auditlog.conf ファイル 167

C

C/T デルタ
分析 149
CIM/WBEM 188
CIM/WBEM 機能
Device Manager 188
設定 190
ユーザーアカウント設定 190
cimxmlcpa.properties ファイル 447
cimxmlsca.properties ファイル 447
client.ldev.rowsperpage.retain.enabled 456
client.migration.use.legacyMode 432
client.properties ファイル 431, 456
client.rmi.port 431
com.wbemsolutions.jservice.bindto 448
Compute Systems Manager 63
config.xml ファイル 148
configforclient.xml ファイル 148
customizedsnmptrap.customizedSNMPTrapEnable
433
customizedsnmptrap.customizelist 433
customizedsnmptrap.properties ファイル 432

D

database.properties ファイル 421, 456
dbm.startingCheck.retryCount 422
dbm.startingCheck.retryPeriod 422
dbm.traceSQL 421, 456
Device Manager CLI
パスワード 128
Device Manager エージェント 31
環境設定 303
常駐プロセス 312
前提バージョン 81
ファイアウォール 305
プロパティファイル 474
ポート 90
保守情報の取得 [ホスト] 371
Device Manager エージェントのサービス
稼働状態の確認 313
起動 313
停止 313
Device Manager サーバ 31
プロパティファイル 411
ポート 87
devicemanager.properties ファイル 457
dispatcher.properties ファイル 424
Dynamic Link Manager 63

E

Element Manager
使用 130
設定 131
設定の解除 133
E メール通知
アラート 170
イベント 176
受信ユーザーの登録 171
テンプレートのカスタマイズ [アラート] 173

F

firewall_setup コマンド 305

G

Global Link Manager 63

H

hbsa_modinfo コマンド 314

hbsa_util コマンド 315

hbsasrv コマンド 313

hcmdsbanner コマンド 125, 126

hcmdsgetlogs コマンド 368

hcmdsunlockaccount コマンド 121

hdc.adapter.adapterProcessNum 465

hdc.adapter.esx.timeout 468

hdc.adapter.localport 465

hdc.classloader 438

hdc.common.http.serverPort 466

hdc.common.https.serverPort 467

hdc.common.rmi.registryPort 465

hdc.common.rmi.serverPort 466

hdc.common.rmi.ssl.registryPort 466

hdc.common.rmi.ssl.serverPort 467

hdc.request.timeout 437

hdc.rmiregistry 437

hdc.rmiserver 438

hdc.service.fileCleanup.startTime 468

hdc.service.localport 465

hdc.service.rmi.registryIPAddress 467

hdc.ssl.secure 468

hdc.usessl 439

hdcbase.properties ファイル 464

hdvm.analytics.disabled 442

hdvm.analytics.healthcheck.excludeMainframe 442

hdvm.analytics.healthcheck.notification.exportreport.

locale 443

hdvm.port 457

hdvm.protocol 457

hdvm.replication.disabled 446

hdvm.rmi.port 457

hdvm.timeout 457

hdvm_info コマンド 316

hdvmagt_setting コマンド 316

hdvmmodmailuser コマンド

アラート通知 172

イベント通知 181

hdvmmodpolluser コマンド 198

HiScan.log ファイル 318

HiScan.msg ファイル 365

HiScan コマンド 318

Hitachi Command Suite 共通コンポーネント 31

ポート 86

ポートの変更 92

ログ出力 156

Hitachi File Services Manager 63

hldutil.properties ファイル 477

hldutil コマンド 320

HORCM_CMD 328

HORCM_DEV 330

HORCM_INST 333

HORCM_INSTP 334

HORCM_LDEV 331

HORCM_MON 327

Host Data Collector 31

アンインストール 355

アンインストール [Solaris または Linux] 356

アンインストール [Windows] 355

インストール 346

インストール [Solaris または Linux] 347

インストール [Windows] 346

インストール条件 346

環境設定 350

管理サーバへの登録 349

常駐プロセス 350

バージョンの確認 355

ファイアウォール 352

プロパティファイル 464

ポート 89

保守情報の取得 370

保守情報の取得 [ホスト] 370

Host Data Collector のサービス

稼働状態の確認 352

起動 351

停止 351

例外登録 352, 353

host.agent.access.timeoutForRpm 436

host.mf.agent.connection.timeout 436

host.properties ファイル 436

hostdatacollectors.properties ファイル 436

htmsetup コマンド 147

Microsoft Cluster Service または Windows Server

Failover Clustering 142

Sun Cluster 145

Veritas Cluster Server 144

非クラスタ環境 141

htnm.flashMode 442

htnm.infoAcquirePeriod 441

htnm.server.n.host 441

htnm.server.n.port 442

htnm.server.n.protocol 442

htnm.servers 441
HtsmgetTI.properties ファイル 157
htsmmodmailuser コマンド 182
HTTPPort 448
HTTPSPort 448

I

IETF 189
IPv6
 移行 108
 グローバルアドレス 108
 グローバルユニークローカルアドレス 108
 サイトローカルアドレス 108
 ストレージシステムとの連携 109
 リンクローカルアドレス 108
IP アドレス
 変更 111

J

Java
 変更 [Device Manager エージェント] 304
 変更 [Host Data Collector] 354
javaconfig.properties ファイル 471
javapath_setup コマンド 304
javapathlocation 471
JDK
 変更 [Device Manager サーバ] 40
JP1/IM 63, 183
 Hitachi Command Suite 製品の GUI のラウンチ 152
JP1/NETM/DM 63
 配布指令 341
 パッケージング 339, 340
jserver.properties ファイル 447

L

launchapp.elementmanager.role.mode 435
launchapp.elementmanager.usehostname 436
launchapp.properties ファイル 434
launchapp.snm2.rmi.port 435
launchapp.snm2.url 435
Legacy モード 432
Linux
 ファイアウォールの例外登録 96
logger.guiMessageFileCount 460
logger.guiMessageMaxFileSize 461
logger.guiTraceFileCount 460
logger.guiTraceMaxFileSize 461
logger.hicommandbase.loglevel 423
logger.hicommandbase.MaxBackupIndex 424

logger.hicommandbase.MaxFileSize 424
logger.hicommandbase.sysloglevel 423
logger.iotrace.maxFileSize 470
logger.iotrace.numOfFiles 470
logger.loglevel 422, 478
logger.MaxBackupIndex 422, 478
logger.MaxFileSize 423, 479
logger.messageLogLevel 458
logger.properties ファイル 422, 458, 469, 478
logger.serverMessageFileCount 459
logger.serverMessageMaxFileSize 461
logger.serverTraceFileCount 460
logger.serverTraceMaxFileSize 461
logger.syslogLevel 459
logger.trace.level 469
logger.trace.maxFileSize 470
logger.trace.numOfFiles 470
logger.tracelogLevel 459

M

migration.dataErase.defaultValue 439
migration.multiExecution 440
migration.plan.candidateCapacityGroupDisplayMaxCount 440
migration.plan.candidateVolumeCountLimit 440
migration.properties ファイル 439
mime.properties ファイル 431

N

NIC
 複数の NIC のネットワーク設定 107
npivmapping.properties ファイル 52

O

OutOfMemory エラー 364

P

P9000 RAID Manager 32
password.check.userID 119
password.min.length 118
password.min.lowercase 118
password.min.numeric 118
password.min.symbol 119
password.min.uppercase 118
perf_cmddev.properties ファイル 196
perf_findcmddev コマンド 195
programproductinfo.properties ファイル 479

R

RAID Manager 32
Replication Manager 63
Replication Manager サーバ 31
replication.properties ファイル 443
rpmlib.properties ファイル 447
rpmlib.rpm.port 447

S

server.agent.differentialrefresh.manual.enabled 420
server.agent.differentialrefresh.periodical.enabled 421
server.agent.evtwait.timeout 490
server.agent.JRE.location 482
server.agent.maxMemorySize 482
server.agent.port 480
server.agent.rm.centralizePairConfiguration 484
server.agent.rm.cuLdevForm 484
server.agent.rm.exclusion.instance 485
server.agent.rm.horcm.poll 486
server.agent.rm.horcmSource 488
server.agent.rm.ignorePairStatus 488
server.agent.rm.location 485
server.agent.rm.moduleTimeOut 489
server.agent.rm.optimization.userHorcmFile 485
server.agent.rm.pairDefinitionForm 487
server.agent.rm.temporaryInstance 486
server.agent.rm.temporaryPort 486
server.agent.rm.userAuthentication 488
server.agent.rmxp.location 490
server.agent.shutDownTime 482
server.base.home 415
server.base.initialsynchro 415, 453
server.checkOutVolumeRange 454
server.cim.agent 416
server.cim.http.port 416
server.cim.https.port 417
server.cim.support 416
server.cim.support.job 416
server.cim.support.protocol 416
server.configchange.enabled 417
server.dispatcher.configchange.pollingPeriod 426
server.dispatcher.daemon.autoSynchro.dayOfWeek 428
server.dispatcher.daemon.autoSynchro.doRefresh 427
server.dispatcher.daemon.autoSynchro.interval 428
server.dispatcher.daemon.autoSynchro.logicalGroup.doRefresh 430
server.dispatcher.daemon.autoSynchro.performance.doRefresh 430
server.dispatcher.daemon.autoSynchro.performance.startTime 430
server.dispatcher.daemon.autoSynchro.startTime 428
server.dispatcher.daemon.autoSynchro.type 427
server.dispatcher.daemon.configUpdate.detection.interval 426
server.dispatcher.daemon.configUpdate.detection.variable.enabled 429
server.dispatcher.daemon.pollingPeriod 425
server.dispatcher.daemon.receiveTrap 425
server.dispatcher.daemon.replication.config.doUpdate 443
server.dispatcher.daemon.replication.config.minute 445
server.dispatcher.daemon.replication.config.offset 444
server.dispatcher.daemon.replication.config.updateInterval 444
server.dispatcher.daemon.replication.performance.rpm.updateInterval 445
server.dispatcher.daemon.replication.performance.tnm.minute 446
server.dispatcher.daemon.replication.performance.tnm.offset 445
server.dispatcher.daemon.replication.performance.tnm.updateInterval 445
server.dispatcher.message.timeout 424
server.dispatcher.message.timeout.in.processing 425
server.dispatcher.snm2.configchange.pollingPeriod 425
server.dispatcher.traps.purgePeriod 425
server.eventMonitoringIntervalInMinute 454
server.eventNotification.mail.to 419, 454
server.horcmconfigfile.hostname 415
server.http.entity.maxLength 415, 483
server.http.host 413, 481
server.http.localPort 480
server.http.port 413, 481
server.http.security.clientIP 483
server.http.server.timeOut 489
server.http.socket.agentAddress 481
server.http.socket.bindAddress 481
server.https.port 414
server.logicalGroupMapping.updateInterval 421
server.logicalview.initialsynchro 417
server.mail.alert.status 420
server.mail.alert.type 419
server.mail.enabled 418
server.mail.errorsTo 419, 453
server.mail.from 418, 453
server.mail.smtp.auth 419, 454
server.mail.smtp.host 418, 453
server.mail.smtp.port 418, 453
server.migration.dataErase.defaultValue 454
server.migration.maxRetryCount 455
server.migration.multiExecution 454

server.migrationPlan.candidateCapacityGroupDisplayMaxCount 455

server.migrationPlan.candidateVolumeCountLimit 455

server.properties ファイル

- Device Manager エージェント 480
- Device Manager サーバ 412
- Tiered Storage Manager サーバ 451

server.rmi.port 414, 452

server.rmi.secure 451

server.rmi.security.port 452

server.server.authorization 483

server.server.serverIPAddress 483

server.server.serverPort 484

server.smisclient.indication.port 420

server.subsystem.ssid.availableValues 420

server.util.processTimeOut 489

SLP サービス

- 解除 201
- 起動 199
- 制御 199
- 停止 199

SMTP サーバ 171

SMTP 認証ユーザー 172, 181

SNMP トラップ

- アラート 170
- ログファイル出力 175

Storage Navigator Modular 2

- 前提条件 130

SVP 32

System アカウント

- ロックに関する設定 120

T

TIC コマンド 371

Tiered Storage Manager CLI

- パスワード 128
- ログファイル 157

Tiered Storage Manager サーバ 31

- プロパティファイル 450
- ポート 88

Tuning Manager 63

- リモート接続 [Microsoft Cluster Service または Windows Server Failover Clustering] 142
- リモート接続 [Sun Cluster] 145
- リモート接続 [Veritas Cluster Server] 144
- リモート接続 [非クラスタ環境] 141

tuningmanager.properties ファイル 440

U

Universal Replicator

- 性能分析 149

Universal Replicator の性能分析

- Device Manager の設定 151
- Replication Manager の設定 151
- Tuning Manager の設定 152
- システム構成 149

URL

- 変更 114

V

veritas.volume.manager.version 480

vMA

- 仮想化サーバの監視構成 55

W

Windows

- ファイアウォールの例外登録 96

あ

アラート 169

- Eメール通知 170
- SNMP トラップ 170

アラート通知

- SMTP サーバ 171

アンインストール

- Host Data Collector 355
- Host Data Collector [Solaris または Linux] 356
- Host Data Collector [Windows] 355

い

移行

- IPv6 108
- データベース 280
- 一括管理構成 65, 484

イベント通知

- SMTP 認証ユーザーの設定 181
- テンプレートのカスタマイズ 177
- プロパティの設定 177

インストール

- Host Data Collector 346
- Host Data Collector [Solaris または Linux] 347
- Host Data Collector [Windows] 346
- リモートインストール 338

インストール条件

- Host Data Collector 346

インポート
データベース 287

え

エクスポート
データベース 281

お

オープンホスト 42

か

仮想 WWN

登録 52

仮想化サーバ 42

vMA での監視構成 55

前提環境 [Host Data Collector] 53

前提環境 [vMA] 54

仮想コマンドデバイスサーバ 65

仮想マシン 42

構成変更時に必要な作業 53

前提環境 [Device Manager エージェント] 48

前提環境 [Host Data Collector] 45

環境設定

Device Manager エージェント 303

Host Data Collector 350

監査ログ

Device Manager サーバ 377

Device Manager サーバ [CIM 経由] 379

Hitachi Command Suite 共通コンポーネント 376

syslog ファイル 158

イベントログファイル 158

確認 374

環境設定ファイルの編集 167

監査事象 159

関連製品 377

出力内容の対応 [CLI コマンド] 405

出力内容の対応 [GUI 操作] 403

詳細メッセージ 385

設定 157

メッセージテキスト 376

リクエスト [Device Manager] 385

管理クライアント 30

制限 126

管理サーバ 30

システム要件 37

保守情報の取得 368

ホスト名の変更 110

く

クラスタ環境への変更

Hitachi Command Suite [Solaris] 242

Hitachi Command Suite [Windows] 217

クラスタ構成

アップグレードまたは上書きインストール [Solaris]
238

アップグレードまたは上書きインストール
[Windows] 214

アンインストール [Solaris] 245

アンインストール [Windows] 220

クラスタ環境への変更 [Solaris] 242

クラスタ環境への変更 [Windows] 217

新規インストール [Solaris] 222

新規インストール [Windows] 205

け

警告バナー 124

メッセージの削除 125

メッセージの作成と登録 124

メッセージの条件 124

こ

構成定義ファイル 308

格納場所の変更 336

記述規則 326

サポートしているパラメーター 325

前提環境 324

注意事項 337

編集 324

コピーペア

Device Manager エージェントの前提バージョン 81

一括管理構成 65

システム構成 65

ストレージシステム 64

ストレージシステムの要件 78

設定 [Device Manager エージェント] 306

通常構成 65

さ

サービス

Hitachi Command Suite 製品 249

実行ユーザーの変更 [Device Manager エージェント]
314

サービスプロセッサ 32

し

- 資源登録システム 339
- システム構成 30
 - SVP 構成 73, 75
 - 一括管理構成 68
 - 仮想コマンドデバイス構成 71
 - コピーペアの管理 65
 - 性能情報 193
 - 通常構成 66
- システム要件
 - 管理サーバ 37
- 条件
 - メッセージ [警告バナー] 124
- 常駐プロセス 250
 - Device Manager エージェント 312
 - Host Data Collector 350
- 新規インストール
 - Hitachi Command Suite [Solaris] 222
 - Hitachi Command Suite [Windows] 205

す

- ストレージシステム 31
 - コピーペア 64
 - コピーペアを管理する場合の要件 78
 - 性能情報の収集 134
 - 性能情報の取得 [CIM/WBEM 機能] 192
 - ポート 90

せ

- 性能情報
 - システム構成 193
 - ストレージシステム 134
 - ストレージシステム [CIM/WBEM 機能] 192
 - 設定 194, 198
- 性能分析
 - Universal Replicator 149
- 前提環境
 - 仮想化サーバ [Host Data Collector] 53
 - 仮想化サーバ [vMA] 54
 - 仮想マシン [Device Manager エージェント] 48
 - 仮想マシン [Host Data Collector] 45
 - 構成定義ファイルの利用 324
 - 通常ホスト [Device Manager エージェント] 45
 - 通常ホスト [Host Data Collector] 43
- 前提条件
 - Storage Navigator Modular 2 130

つ

- 通常構成 65, 484
- 通常ホスト 42
 - 前提環境 [Device Manager エージェント] 45
 - 前提環境 [Host Data Collector] 43

て

- データベース
 - 移行 280
 - インポート 287
 - エクスポート 281
 - バックアップ 256
 - 復元 262

と

- 統合ログ
 - 設定 156

ね

- ネームスペース 189
- ネットワーク
 - ブリッジ 107
- ネットワーク構成 32

は

- 配布管理システム 339
- 配布先システム 339
- パスワード
 - Device Manager CLI 128
 - Tiered Storage Manager CLI 128
- バックアップ
 - データベース 256
- パラメーター
 - 構成定義ファイル 325

ふ

- ファイアウォール
 - Device Manager エージェント 305
 - Host Data Collector 352
 - 設定 96
 - 例外登録 96
 - 例外登録 [Linux] 96
 - 例外登録 [Windows] 96
- ファイルサーバ 42
- 復元
 - データベース 262

ブリッジ

ネットワークの設定 107

プロパティ

変更 [Device Manager エージェント] 474

変更 [Device Manager サーバ] 412

変更 [Host Data Collector] 464

変更 [Tiered Storage Manager サーバ] 450

プロパティファイル

Device Manager エージェント 474

Device Manager サーバ 411

Host Data Collector 464

Tiered Storage Manager サーバ 450

記述規則 412, 451

へ

ペア管理サーバ 31, 65, 484

ほ

ポート

Device Manager エージェント 90

Device Manager サーバ 87

Hitachi Command Suite 共通コンポーネント 86

Host Data Collector 89

Tiered Storage Manager サーバ 88

ストレージシステム 90

変更 92

変更 [CIM/WBEM 機能] 192

例外登録 96

保守情報

Device Manager エージェントの管理対象ホスト 371

Host Data Collector 370

Host Data Collector の管理対象ホスト 370

管理サーバ 368

ホスト 31, 41

バージョンアップ 302

ホスト管理ソフトウェア 42

ホスト名

変更 110

め

メインフレームホスト 42

メインフレームボリューム 58

ヘルスチェック 442

メッセージテキスト

監査ログ 376

メモリーヒープサイズ

変更 [Device Manager サーバ] 39

変更 [Hitachi Command Suite 共通コンポーネント]

38

ゆ

ユーザーアカウント

アカウントロック 119

アカウントロックの解除 121

アカウントロックポリシー 120

アカウントロックポリシーの設定 120

パスワードポリシー 118

パスワードポリシーの設定 118

り

リモートインストール 338

実行結果の戻り値 342

配布指令 341

パッケージング 339, 340

リモート接続

Tuning Manager [Microsoft Cluster Service または
Windows Server Failover Clustering] 142

Tuning Manager [Sun Cluster] 145

Tuning Manager [Veritas Cluster Server] 144

Tuning Manager [非クラスタ環境] 141

れ

例外登録

Host Data Collector のサービス 352, 353

ろ

ログ

参照 183

ログファイル

SNMP トラップ 175

Tiered Storage Manager CLI 157

ロック

System アカウント 120

アカウントロックの解除 121

ユーザーアカウント 120