

Hitachi Command Suite

システム構成ガイド

3021-9-008-F0

対象製品

Hitachi Device Manager 8.7.4

Hitachi Tiered Storage Manager 8.7.4

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

HITACHI, BladeSymphony, HiRDB, JP1 は、株式会社日立製作所の商標または登録商標です。

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 は、米国およびその他の国における Adobe 社の登録商標または商標です。

Adobe AIR と AIR は、米国およびその他の国における Adobe 社の登録商標または商標です。

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

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

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/またはその他の国における Intel Corporation またはその子会社の商標です。

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 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。

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、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。

Red Hat, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the United States and other countries. Linux[®] is the registered trademark of Linus Torvalds in the U.S. and other countries.

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。

SQL 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。

UNIX は、The Open Group の商標です。

Veritas, Veritas ログおよび Veritas は、米国およびその他の国における Veritas Technologies LLC またはその関連会社の商標または登録商標です。

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

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。

その他記載の会社名、製品名などは、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/>).

Java is a registered trademark of Oracle and/or its affiliates.

HITACHI
Inspire the Next

株式会社 日立製作所



発行

2020年7月 3021-9-008-F0

著作権

All Rights Reserved. Copyright© 2014, 2020, Hitachi, Ltd.

目次

はじめに.....	21
対象読者.....	22
マニュアルの構成.....	22
マイクロソフト製品の表記について.....	23
このマニュアルで使用している記号.....	24
ストレージシステムのサポートについて.....	25
ストレージシステムのサポート終了について.....	25
OS, 仮想化ソフトウェア, ブラウザーなどのサポートについて.....	25
エンドユーザライセンスについて.....	26
1.概要.....	27
1.1 システム構成.....	29
1.2 セキュリティ構成.....	32
1.2.1 セキュリティについての一般的なリスク.....	32
1.2.2 Device Manager で推奨するセキュリティ構成.....	33
1.3 管理サーバおよび Host Data Collector マシンのシステム要件.....	33
1.3.1 管理リソース数の上限.....	33
1.3.2 メモリーヒープサイズの変更.....	34
1.3.3 管理サーバの JDK の変更.....	35
1.3.4 Host Data Collector の Java の実行環境の変更.....	36
1.4 Device Manager で管理できるホスト.....	37
1.5 Device Manager のホスト管理ソフトウェア.....	38
1.6 通常ホストのシステム要件.....	39
1.6.1 通常ホストの前提環境.....	39
1.7 仮想マシンのシステム要件.....	41
1.7.1 仮想マシンの前提環境.....	42
1.7.2 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.....	45
1.7.3 仮想マシンの構成変更時に必要な作業.....	47
1.8 仮想化サーバのシステム要件.....	48
1.8.1 仮想化サーバの前提環境.....	48
1.8.2 仮想化サーバを管理対象にするための操作フロー.....	50
1.8.3 仮想化サーバの運用に関する注意事項.....	50
1.9 メインフレームホストのシステム要件.....	50
1.9.1 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.....	51
1.10 ファイルサーバのシステム要件.....	51

1.10.1 NAS Platform の前提環境	51
1.10.2 Hitachi Virtual File Platform および Hitachi Capacity Optimization の前提環境	53
1.10.3 ファイルサーバを管理対象にするための操作フロー	54
1.10.4 ファイルサーバの運用に関する注意事項	54
1.11 NAS モジュールのシステム要件	55
1.11.1 NAS モジュールを管理対象にするための操作フロー	55
1.11.2 NAS モジュールの運用に関する注意事項	55
1.12 関連製品	56
1.13 Device Manager でのコピーペア管理	57
1.14 コピーペアを管理する場合のシステム構成（一括管理構成）	58
1.15 コピーペアを管理する場合のシステム構成（一括管理構成以外）	62
1.15.1 各ホストでコピーペアを管理する場合のシステム構成	63
1.15.2 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	66
1.15.3 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）	70
1.15.4 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）	73
1.16 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	75
1.17 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	76
1.18 コピーペアを管理する場合の注意事項	80
1.19 高可用性システムの構築	84
1.19.1 高可用性システムを構築するための構成例	86
1.19.2 高可用性システムを構築するための要件（VSP 5000 シリーズの場合）	87
1.19.3 高可用性システムを構築するための要件（VSP G1000, G1500 または VSP F1500 の場合）	89
1.19.4 高可用性システムを構築するための要件（VSP G100, G200, G400, G600, G800 および VSP F400, F600, F800 の場合）	92
1.19.5 高可用性システムを構築するための要件（VSP G150, G350, G370, G700, G900 および VSP F350, F370, F700, F900 の場合）	95
1.20 コマンドを実行する場合の注意事項	98
2.ネットワーク構成に応じた設定	99
2.1 Hitachi Command Suite 製品で使用されるポート	100
2.1.1 Hitachi Command Suite 共通コンポーネントで使用されるポート	100
2.1.2 Device Manager サーバで使用されるポート	101
2.1.3 Tiered Storage Manager サーバで使用されるポート	102
2.1.4 Host Data Collector で使用されるポート	103
2.1.5 Device Manager エージェントで使用されるポート	104
2.1.6 ストレージシステムで使用されるポート	104
2.2 Hitachi Command Suite 共通コンポーネントで使用されるポートの変更	107
2.3 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録	113
2.3.1 Device Manager および Tiered Storage Manager でファイアウォールへの例外登録が必要なポート	113
2.3.2 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録（Windows）	128
2.3.3 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録（Red Hat Enterprise Linux 5 または Red Hat Enterprise Linux 6）	129
2.3.4 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録（Red Hat Enterprise Linux 7 または Oracle Linux 7）	129
2.4 Host Data Collector でのファイアウォールへの例外登録（Windows）	130
2.4.1 Host Data Collector でのサービスの例外登録（非 SSL 通信用）	130

2.4.2 Host Data Collector でのサービスの例外登録 (SSL 通信用)	131
2.5 IP アドレスが複数ある場合のネットワーク設定.....	132
2.5.1 管理サーバでブリッジ機能を使用する場合のネットワークの設定.....	132
2.5.2 Host Data Collector マシンに複数の IP アドレスがある場合の設定.....	133
2.6 IPv6 環境で運用する場合の Device Manager の設定.....	133
2.6.1 Device Manager を IPv6 環境に移行するときの設定.....	133
2.6.2 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.....	135
2.7 管理サーバの IP アドレスまたはホスト名の変更.....	135
2.7.1 管理サーバのホスト名の変更.....	135
2.7.2 管理サーバの IP アドレスの変更.....	137
2.7.3 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.....	138
2.8 Hitachi Command Suite 製品の URL の変更 (hcmds64chgurl コマンド)	140
3. ユーザーアカウントを管理するために必要な設定.....	143
3.1 パスワードポリシーとは.....	144
3.1.1 パスワードポリシーの設定.....	144
3.2 アカウントロックとは.....	145
3.2.1 アカウントロックポリシーとは.....	146
3.2.2 アカウントロックポリシーの設定.....	146
3.2.3 System アカウントのロックに関する設定.....	147
3.2.4 アカウントロックの解除.....	147
4. 外部認証サーバでのユーザー管理.....	149
4.1 外部認証サーバとの連携とは.....	150
4.2 外部認可サーバとの連携とは.....	150
4.3 外部認証サーバでユーザー認証するための操作フロー.....	151
4.3.1 LDAP ディレクトリサーバでユーザー認証するための操作フロー.....	151
4.3.2 RADIUS サーバでユーザー認証するための操作フロー.....	154
4.3.3 Kerberos サーバでユーザー認証するための操作フロー.....	156
4.4 Hitachi Command Suite 製品のアカウントの条件.....	157
4.5 ユーザーエントリのデータ構造とは.....	158
4.5.1 BaseDN とは.....	158
4.5.2 階層構造モデルとは.....	158
4.5.3 フラットモデルとは.....	159
4.6 複数の外部認証サーバと連携している場合の構成.....	160
4.7 外部認証サーバと外部認可サーバの登録.....	162
4.7.1 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目.....	163
4.7.2 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定例.....	168
4.7.3 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目.....	170
4.7.4 RADIUS サーバで認証する場合の exauth.properties ファイルの設定例.....	175
4.7.5 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目.....	176
4.7.6 Kerberos サーバで認証する場合の exauth.properties ファイルの設定例.....	181
4.8 情報検索用のユーザーアカウントとは.....	182
4.8.1 情報検索用のユーザーアカウントの条件.....	182
4.8.2 情報検索用のユーザーアカウントの登録.....	184
4.8.3 情報検索用のユーザーアカウントの削除.....	185
4.8.4 情報検索用ユーザーアカウントを登録済みの LDAP ディレクトリサーバの確認.....	186
4.9 共有秘密鍵の登録.....	186

4.9.1 共有秘密鍵の削除.....	187
4.9.2 共有秘密鍵が登録されている RADIUS サーバの確認.....	187
4.10 外部認証サーバおよび外部認可サーバとの接続確認.....	188
4.11 外部認証サーバとの連携設定に使用するコマンドに関する注意事項.....	190
4.12 Kerberos 認証に使用できる暗号タイプ.....	190
5.通信に関するセキュリティ設定.....	193
5.1 Device Manager および Tiered Storage Manager のセキュリティ通信路.....	194
5.1.1 Device Manager サーバのデフォルトの証明書.....	199
5.1.2 管理サーバと管理クライアント (GUI) 間のセキュリティ通信のための操作フロー.....	201
5.1.3 管理サーバと管理クライアント (Device Manager CLI) 間のセキュリティ通信のための操作フロー.....	203
5.1.4 管理サーバと管理クライアント (Tiered Storage Manager CLI) 間のセキュリティ通信のための操作フロー.....	204
5.1.5 LDAP ディレクトリサーバと管理サーバ間のセキュリティ通信のための操作フロー.....	205
5.1.6 Device Manager サーバと Replication Manager サーバ間のセキュリティ通信のための操作フロー.....	206
5.1.7 Tuning Manager サーバと Device Manager サーバ間のセキュリティ通信のための操作フロー.....	207
5.1.8 Host Data Collector マシンと管理サーバ間のセキュリティ通信のための操作フロー.....	208
5.1.9 仮想化サーバと Host Data Collector 間のセキュリティ通信のための操作フロー.....	210
5.1.10 管理サーバと Device Manager エージェント間のセキュリティ通信のための操作フロー.....	211
5.1.11 ストレージシステムと管理サーバ間のセキュリティ通信のための操作フロー.....	212
5.1.12 管理サーバとストレージシステム (VSP G1000, G1500 または VSP F1500) 間のセキュリティ通信のための操作フロー.....	213
5.1.13 管理サーバとストレージシステム (VSP 5000 シリーズ) 間のセキュリティ通信のための操作フロー.....	214
5.1.14 管理サーバとストレージシステム (VSP Gx00 モデルまたは VSP Fx00 モデル) 間のセキュリティ通信のための操作フロー.....	214
5.1.15 SMI-S プロバイダーと管理サーバ間のセキュリティ通信のための操作フロー.....	216
5.1.16 Tuning Manager サーバと Tuning Manager API クライアント間のセキュリティ通信のための操作フロー.....	216
5.1.17 ストレージシステムと管理クライアント (GUI) 間のセキュリティ通信のための操作フロー.....	217
5.1.18 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー (オブジェクト操作).....	218
5.1.19 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー (オブジェクト操作の相互認証).....	219
5.1.20 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー (インディケーション通知).....	220
5.1.21 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー (インディケーション通知の相互認証).....	221
5.1.22 トラストストア.....	222
5.2 SSL サーバの構築 (Hitachi Command Suite 共通コンポーネント).....	224
5.2.1 Hitachi Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成.....	224
5.2.2 Hitachi Command Suite 共通コンポーネントのサーバ証明書の認証局への申請.....	227
5.2.3 SSL/TLS を有効にする場合の user_httpsd.conf ファイルの編集.....	227
5.2.4 証明書の有効期限の確認 (Hitachi Command Suite 共通コンポーネント).....	231
5.3 SSL サーバの構築 (Device Manager サーバ).....	232
5.3.1 Device Manager サーバのキーペアと自己署名証明書の作成.....	232
5.3.2 Device Manager サーバの SSL/TLS の有効化.....	235
5.3.3 Device Manager サーバの証明書発行要求の作成.....	236
5.3.4 Device Manager サーバのサーバ証明書の認証局への申請.....	237
5.3.5 Device Manager サーバのキーストアへのサーバ証明書のインポート.....	238
5.3.6 Device Manager サーバのキーペア情報の参照 (標準モード).....	239
5.3.7 Device Manager サーバのキーペア情報の参照 (詳細モード).....	239

5.3.8 Device Manager サーバのキーストアーからのキーペアの削除.....	240
5.3.9 Device Manager サーバのキーペアのパスワードの変更.....	241
5.3.10 Device Manager サーバのキーストアーパスワードの変更.....	241
5.3.11 Device Manager サーバのトラストストアへの証明書のインポート.....	242
5.3.12 Device Manager サーバのトラストストア情報の参照（標準モード）.....	242
5.3.13 Device Manager サーバのトラストストア情報の参照（詳細モード）.....	243
5.3.14 Device Manager サーバのトラストストアからのサーバ証明書の削除.....	244
5.3.15 Device Manager サーバのトラストストアパスワードの変更.....	245
5.3.16 Device Manager サーバのサーバ証明書の確認.....	245
5.4 SSL サーバの構築（Host Data Collector）.....	246
5.4.1 Host Data Collector のキーペアおよび証明書発行要求の作成.....	246
5.4.2 Host Data Collector のサーバ証明書の認証局への申請.....	247
5.4.3 Host Data Collector のサーバ証明書のキーストアーへのインポート.....	248
5.4.4 Host Data Collector のサーバ証明書の確認.....	249
5.5 SSL クライアントの構築.....	249
5.5.1 Device Manager サーバのトラストストアファイルのダウンロード.....	249
5.5.2 Device Manager CLI で使用するトラストストアファイルの作成.....	250
5.5.3 Device Manager サーバの自己署名証明書のエクスポート.....	250
5.5.4 Web ブラウザーへの証明書のインポート（Internet Explorer の場合）.....	251
5.5.5 Web ブラウザーへの証明書のインポート（Firefox の場合）.....	252
5.5.6 Web ブラウザーへの証明書のインポート（Google Chrome の場合）.....	252
5.5.7 ポップアップブロックの設定変更.....	253
5.5.8 Device Manager CLI の実行マシンでの SSL/TLS の有効化.....	253
5.5.9 Tiered Storage Manager サーバのトラストストアファイルのダウンロード.....	254
5.5.10 Tiered Storage Manager CLI の実行マシンでの SSL/TLS の有効化.....	255
5.5.11 Hitachi Command Suite 共通コンポーネントのトラストストアへの証明書のインポート.....	256
5.5.12 LDAP ディレクトリサーバのサーバ証明書の条件.....	258
5.5.13 Hitachi Command Suite 共通コンポーネントのトラストストアにインポートされた証明書の確認.....	258
5.5.14 Hitachi Command Suite 共通コンポーネントのトラストストアにインポートされた証明書の削除.....	259
5.5.15 Replication Manager サーバと Device Manager サーバ間の通信プロトコルの変更.....	260
5.5.16 Device Manager サーバのトラストストアへの証明書のインポート.....	260
5.5.17 Device Manager サーバのトラストストアにインポートされた証明書の確認.....	261
5.5.18 Host Data Collector のトラストストアへの証明書のインポート.....	262
5.5.19 Host Data Collector のトラストストアにインポートされた証明書の確認.....	263
5.5.20 Host Data Collector のトラストストアパスワードの変更.....	263
5.5.21 仮想化サーバの登録情報の変更.....	264
5.5.22 Device Manager エージェントのトラストストアへのサーバ証明書のインポート.....	265
5.5.23 Device Manager エージェントのトラストストアにインポートされたサーバ証明書の確認.....	266
5.5.24 Device Manager エージェントのトラストストアパスワードの変更.....	267
5.5.25 Device Manager エージェントのトラストストアにインポートされたサーバ証明書の削除.....	268
5.5.26 ストレージシステムの登録情報の変更.....	269
5.6 SSL サーバおよび SSL クライアントの構築（CIM サーバ）.....	269
5.6.1 オブジェクト操作用のキーストアーファイルの作成.....	269
5.6.2 オブジェクト操作用の MOF ファイルの編集.....	270
5.6.3 オブジェクト操作用のサーバ証明書のエクスポート.....	271
5.6.4 オブジェクト操作に対する相互認証の有効化.....	272
5.6.5 オブジェクト操作用のクライアント証明書のインポート.....	273
5.6.6 インディケーション通知用のキーストアーファイルの作成.....	274
5.6.7 インディケーション通知用の MOF ファイルの編集.....	275
5.6.8 インディケーション通知用のクライアント証明書のエクスポート.....	276

5.6.9 インディケーション通知に対する相互認証の有効化.....	277
5.6.10 インディケーション通知用のサーバ証明書のインポート.....	277
5.6.11 CIM サーバの自己署名証明書の確認.....	278
5.6.12 製品同梱されたオブジェクト操作用の自己署名証明書.....	279
5.6.13 相互認証の無効化.....	279
5.7 SSL サーバおよび SSL クライアントの構築 (CIM クライアント)	280
5.7.1 CIM クライアントのキーペアと自己署名証明書の作成.....	280
5.7.2 CIM クライアントのサーバ証明書またはクライアント証明書のエクスポート.....	281
5.7.3 CIM クライアントへのサーバ証明書またはクライアント証明書のインポート.....	281
6.関連製品と連携するために必要な設定.....	283
6.1 Storage Navigator Modular 2 と連携するために必要な設定.....	284
6.1.1 Storage Navigator Modular 2 と連携するための前提条件.....	284
6.1.2 Element Manager を使用するための設定.....	285
6.1.3 Element Manager を使用するための設定の解除.....	287
6.2 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.....	288
6.2.1 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.....	289
6.2.2 ストレージシステムの性能情報を収集するための操作フロー.....	291
6.2.3 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.....	293
6.2.4 エンタープライズクラスストレージ, VSP Gx00 モデル, VSP Fx00 モデルおよび HUS VM の性能情報を収集するための設定.....	294
6.2.5 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.....	296
6.2.6 Tuning Manager サーバとのリモート接続 (非クラスタ環境)	297
6.2.7 Tuning Manager サーバとのリモート接続 (Windows のクラスタ環境)	298
6.2.8 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)	299
6.2.9 config.xml ファイルおよび configforclient.xml ファイルの設定.....	300
6.2.10 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)	301
6.3 [レプリケーション] タブで Universal Replicator の性能を分析するために必要な設定.....	302
6.3.1 [レプリケーション] タブで Universal Replicator の性能を分析するためのシステム構成.....	302
6.3.2 [レプリケーション] タブで Universal Replicator の性能を分析するための設定の流れ.....	305
6.3.3 RMI 通信で使用するポート番号を Device Manager サーバに設定する.....	306
6.3.4 ストレージシステムのインスタンス環境を構築する.....	306
6.3.5 PFM - Manager のホスト名を設定する.....	307
6.3.6 Tuning Manager - Agent for RAID のインスタンスを起動する.....	307
6.3.7 Tuning Manager とリモート接続するためにプロパティを設定する.....	308
6.3.8 [レプリケーション] タブで分析するための性能情報を収集するように設定する.....	309
6.3.9 [レプリケーション] タブで分析するための性能情報の収集時間や収集間隔を変更する.....	309
6.3.10 Universal Replicator の性能を分析する際の注意事項.....	310
6.4 [レプリケーション] タブでレプリケーション管理機能を利用するために必要な設定.....	310
6.4.1 [レプリケーション] タブでレプリケーション管理機能を利用する場合のシステム構成 (複数サイト構成).....	311
6.4.2 [レプリケーション] タブでレプリケーション管理機能を利用するための設定の流れ.....	313
6.4.3 管理サーバやペア管理サーバに必要な製品をインストールする.....	314
6.4.4 RMI 通信で使用するポート番号を Device Manager サーバに設定する.....	314
6.4.5 副サイトの Replication Manager をメンテナンスモードにする.....	315
6.5 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.....	315
6.5.1 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.....	315
6.5.2 JP1/IM から Hitachi Command Suite 製品の GUI をラウンチするための設定.....	316

7.ログおよびアラートの設定.....	319
7.1 Hitachi Command Suite 共通トレースログの設定.....	320
7.1.1 Hitachi Command Suite 共通トレースログファイルの設定 (Windows)	320
7.1.2 Hitachi Command Suite 共通トレースログファイルの設定 (Linux)	320
7.2 アラートの設定.....	321
7.2.1 Device Manager での障害検知.....	321
7.2.2 SNMP トラップをアラートに表示するための設定.....	323
7.2.3 SNMP トラップ受信ユーザーを登録する (SNMP v3)	325
7.2.4 SNMP トラップ受信ユーザーを管理するためのコマンド (hdvmsnmpuser) の形式 (SNMP v3)	325
7.2.5 アラートを E メール通知するための操作フロー.....	327
7.2.6 SMTP サーバの設定.....	328
7.2.7 受信ユーザーの設定.....	328
7.2.8 アラート通知のプロパティ設定.....	328
7.2.9 SMTP 認証ユーザーアカウントを Device Manager に登録する.....	329
7.2.10 アラート通知テンプレートのカスタマイズ.....	330
7.3 SNMP トラップをログファイルに出力するための設定.....	332
7.3.1 SNMP トラップをログファイルに出力するための設定.....	333
7.4 Device Manager のイベント通知を使用するために必要な設定.....	334
7.4.1 Device Manager のイベント通知のためのプロパティの設定	335
7.4.2 SMTP 認証ユーザーの設定 (hdvmodmailuser コマンド)	335
7.4.3 Device Manager のイベント通知テンプレートの編集.....	336
7.5 Tiered Storage Manager のイベント通知を使用するために必要な設定.....	338
7.5.1 Tiered Storage Manager のイベント通知のためのプロパティの設定.....	339
7.5.2 SMTP 認証ユーザーの設定 (htsmmodmailuser コマンド)	340
7.5.3 Tiered Storage Manager のイベント通知テンプレートの編集.....	341
7.6 JP1/IM でログを参照するために必要な設定.....	346
7.6.1 管理サーバが Windows の場合.....	346
7.6.2 管理サーバが Red Hat Enterprise Linux の場合.....	347
8.CIM/WBEM のセットアップ.....	349
8.1 CIM/WBEM とは.....	350
8.2 Device Manager の CIM/WBEM 機能.....	350
8.3 ネームスペースの指定方法.....	351
8.4 CIM/WBEM 機能を使用するためのユーザーアカウント.....	352
8.5 CIM/WBEM 機能を利用するための設定をする.....	352
8.5.1 CIM/WBEM 機能で使用するポートを変更する.....	354
8.6 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.....	354
8.6.1 CIM/WBEM 機能で性能情報を取得する場合のシステム構成.....	355
8.6.2 Virtual Storage Platform, Universal Storage Platform V/VM または Hitachi USP の性能情報を取得する ための設定をする.....	356
8.6.3 コマンドデバイスを登録するためのコマンド (perf_findcmddev) の形式.....	357
8.6.4 perf_cmddev.properties ファイルの形式.....	359
8.6.5 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をする.....	360
8.6.6 性能情報を取得するユーザーアカウントを登録するためのコマンド (hdvmodpolluser) の形式..	361
8.7 SLP サービスの制御.....	361
8.7.1 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.....	362
8.7.2 SLP サービスを起動する (Windows)	362
8.7.3 SLP サービスを停止する (Windows)	362
8.7.4 SLP デーモンを起動する (Red Hat Enterprise Linux または Oracle Linux)	363

8.7.5 SLP デーモンを停止する (Red Hat Enterprise Linux または Oracle Linux)	363
8.7.6 SLP サービスを解除する (Windows)	363
8.7.7 SLP デーモンを解除する (Linux)	364
8.7.8 OpenSLP のログに関する注意事項	364
9. サービスの起動と停止	365
9.1 Hitachi Command Suite のサービスの起動と停止	366
9.1.1 Hitachi Command Suite の常駐プロセス	366
9.1.2 Hitachi Command Suite のサービスの起動	367
9.1.3 Hitachi Command Suite のサービスの停止	369
9.1.4 Hitachi Command Suite のサービスの稼働状態の確認	370
9.2 Host Data Collector のサービスの起動と停止	371
9.2.1 Host Data Collector の常駐プロセス	371
9.2.2 Host Data Collector のサービスの起動	372
9.2.3 Host Data Collector のサービスの停止	373
9.2.4 Host Data Collector のサービスの稼働状態の確認	373
9.3 クラスタ管理アプリケーションに登録されている Hitachi Command Suite 製品のサービス	374
10. データベースの管理	377
10.1 データベースを管理する前に	378
10.2 データベースのバックアップ	378
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)	379
10.2.2 データベースのバックアップ (Windows のクラスタ構成の場合)	380
10.2.3 データベースのバックアップ (Red Hat Enterprise Linux のクラスタ構成の場合)	382
10.3 データベースの復元	383
10.3.1 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)	384
10.3.2 データベース不整合時のデータベースの復元 (Windows のクラスタ構成の場合)	386
10.3.3 データベース不整合時のデータベースの復元 (Red Hat Enterprise Linux のクラスタ構成の場合)	388
10.3.4 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)	390
10.3.5 データベース破損時のデータベースの復元 (Windows のクラスタ構成の場合)	391
10.3.6 データベース破損時のデータベースの復元 (Red Hat Enterprise Linux のクラスタ構成の場合)	393
10.4 データベースの移行	395
10.4.1 データベースを移行する場合の注意事項	395
10.4.2 データベースを移行する流れ	396
10.4.3 移行先サーバへの Hitachi Command Suite 製品のインストール	396
10.4.4 移行元サーバでデータベースをエクスポートする (非クラスタ構成の場合)	396
10.4.5 移行元サーバでデータベースをエクスポートする (Windows のクラスタ構成の場合)	398
10.4.6 移行元サーバでデータベースをエクスポートする (Red Hat Enterprise Linux のクラスタ構成の場合)	400
10.4.7 移行先サーバでデータベースをインポートする (非クラスタ構成の場合)	402
10.4.8 移行先サーバでデータベースをインポートする (Windows のクラスタ構成の場合)	404
10.4.9 移行先サーバでデータベースをインポートする (Red Hat Enterprise Linux のクラスタ構成の場合)	407
11. Device Manager エージェントの運用	411
11.1 Device Manager エージェントを運用するための前提条件	412
11.1.1 Device Manager エージェントで通常ホストを管理する場合の前提環境	412
11.1.2 Device Manager エージェントで仮想マシンを管理する場合の前提環境	413
11.1.3 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	414

11.1.4 Device Manager エージェントを運用する場合の注意事項.....	415
11.2 Device Manager エージェントの環境設定.....	416
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) ...	416
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)	418
11.2.3 java プロセスの SED への例外登録 (AIX)	418
11.2.4 コピーペアを管理するために必要な設定.....	419
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.....	422
11.2.6 Device Manager エージェントの常駐プロセス.....	425
11.2.7 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) ...	426
11.2.8 Device Manager エージェントのサービスの実行ユーザーの変更 (Windows)	427
11.3 Device Manager エージェントの操作.....	427
11.3.1 エージェント機能の確認 (hbsa_modinfo コマンド)	427
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)	429
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)	429
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 RAID	430
Manager XP の情報の設定 (hdvmagt_setting コマンド)	430
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)	433
11.3.6 デバイス情報の取得 (hldutil コマンド)	435
11.3.7 hldutil コマンドで表示される情報.....	438
11.4 構成定義ファイルの利用	439
11.4.1 構成定義ファイルを利用するための前提環境.....	439
11.4.2 構成定義ファイルの編集.....	440
11.4.3 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.....	441
11.4.4 構成定義ファイルの記述規則.....	441
11.4.5 HORCM_MON パラメーターの記述形式.....	442
11.4.6 HORCM_CMD パラメーターの記述形式.....	444
11.4.7 HORCM_VCMD パラメーターの記述形式.....	446
11.4.8 HORCM_DEV パラメーターの記述形式.....	446
11.4.9 HORCM_LDEV パラメーターの記述形式.....	448
11.4.10 HORCM_INST パラメーターの記述形式.....	450
11.4.11 HORCM_INSTP パラメーターの記述形式.....	452
11.4.12 構成定義ファイルの格納場所の変更.....	454
11.4.13 構成定義ファイルを利用する上での注意事項.....	454
11.5 Device Manager エージェントのリモートインストール.....	455
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.....	455
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.....	456
11.5.3 Device Manager エージェントのパッケージング (Windows)	457
11.5.4 Device Manager エージェントのパッケージング (UNIX)	457
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)	458
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)	459
11.5.7 リモートインストールの実行結果の戻り値.....	460
12.Hitachi Command Suite の監査ログ.....	463
12.1 監査ログを採取するために必要な設定.....	464
12.1.1 監査ログに出力される監査事象.....	465
12.1.2 監査ログの環境設定ファイルの編集.....	473
12.2 監査ログの確認.....	476
12.3 監査ログのメッセージ部に出力されるメッセージテキスト.....	478
12.3.1 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.....	478
12.3.2 Device Manager サーバの処理として出力される場合.....	478

12.3.3 Device Manager GUI の処理として出力される場合	479
12.3.4 関連製品の起動情報として出力される場合	479
12.3.5 Device Manager サーバ (CIM 経由) の処理として出力される場合	481
12.3.6 Tiered Storage Manager の処理として出力される場合	482
12.4 監査ログのメッセージ部に出力される詳細メッセージ	487
12.4.1 詳細メッセージに出力されるコマンド	488
12.4.2 詳細メッセージに出力されるターゲット	488
12.4.3 詳細メッセージに出力されるオプション	490
12.4.4 詳細メッセージに出力されるパラメーター	493
12.5 Tiered Storage Manager CLI のユーザー操作と監査ログの対応	508
13.トラブルシューティング	513
13.1 管理サーバで発生したトラブルへの対処方法 (Device Manager)	514
13.1.1 Device Manager の GUI にログインできない	514
13.1.2 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	514
13.1.3 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	515
13.1.4 Hitachi Virtual File Platform および Hitachi Capacity Optimization の SNMP トラップを受信できない	515
13.1.5 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	516
13.2 管理サーバで発生したトラブルへの対処方法 (Tiered Storage Manager)	516
13.2.1 Tiered Storage Manager サーバの起動に失敗した	517
13.2.2 Tiered Storage Manager サーバが停止しない	517
13.2.3 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	518
13.2.4 データベースに障害が発生し Tiered Storage Manager の操作ができない	519
13.3 ホストで発生したトラブルへの対処方法	519
13.3.1 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	519
13.3.2 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	520
13.3.3 [プログラムと機能] 画面に [HBase Agent] が2つ表示されている	520
13.3.4 [プログラムと機能] 画面に [HBase Agent] が残っている	520
13.3.5 JavaVM が異常終了する	521
13.3.6 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	521
13.3.7 Device Manager の GUI にファイルシステム名が表示されない	522
13.3.8 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	523
13.3.9 Device Manager エージェントの機能が使用できない	523
13.3.10 対処不要なエラー	523
13.4 トラブル発生時に採取が必要な保守情報	524
13.4.1 管理サーバの保守情報の取得 (hcnds64getlogs コマンド)	525
13.4.2 Tiered Storage Manager CLI のログファイル採取の設定	527
13.4.3 Host Data Collector マシンの保守情報の取得 (hdc_getras コマンド)	528
13.4.4 Host Data Collector 管理対象ホストの保守情報の取得 (hdc_target_getras コマンド)	528
13.4.5 Device Manager エージェントの保守情報の取得 (TIC コマンド)	529
13.4.6 HCS Device Manager Web Service のスレッドダンプ取得 (Windows)	531
13.4.7 HCS Device Manager Web Service のスレッドダンプ取得 (Linux)	531
付録 A Device Manager サーバのプロパティ	533
A.1 Device Manager サーバのプロパティファイル	535
A.1.1 Device Manager サーバのプロパティの変更	536

A.1.2 Device Manager サーバのプロパティファイルの記述規則.....	536
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)	537
A.2.1 server.http.host.....	537
A.2.2 server.http.port.....	537
A.2.3 server.https.port.....	538
A.2.4 server.rmi.port.....	539
A.2.5 server.http.entity.maxLength.....	539
A.2.6 server.base.home.....	539
A.2.7 server.horcmconfigfile.hostname.....	540
A.2.8 server.base.initialsynchro.....	540
A.2.9 server.cim.agent.....	540
A.2.10 server.cim.support.....	540
A.2.11 server.cim.support.job.....	540
A.2.12 server.cim.support.protocol.....	541
A.2.13 server.cim.http.port.....	541
A.2.14 server.cim.https.port.....	541
A.2.15 server.configchange.enabled.....	542
A.2.16 server.logicalview.initialsynchro.....	542
A.2.17 server.mail.enabled.storagesystem.....	542
A.2.18 server.mail.enabled.fileserver.....	543
A.2.19 server.mail.from.....	543
A.2.20 server.mail.smtp.host.....	543
A.2.21 server.mail.smtp.port.....	543
A.2.22 server.mail.smtp.auth.....	544
A.2.23 server.mail.errorsTo.....	544
A.2.24 server.eventNotification.mail.to.....	544
A.2.25 server.mail.alert.type.storagesystem.....	544
A.2.26 server.mail.alert.status.....	545
A.2.27 server.subsystem.ssid.availableValues.....	545
A.2.28 server.agent.differentialrefresh.manual.enabled.....	545
A.2.29 server.agent.differentialrefresh.periodical.enabled.....	545
A.2.30 server.logicalGroupMapping.updateInterval.....	546
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)	546
A.3.1 dbm.traceSQL.....	546
A.3.2 dbm.startingCheck.retryCount.....	546
A.3.3 dbm.startingCheck.retryPeriod.....	547
A.4 Device Manager のログ出力に関するプロパティ (logger.properties ファイル)	547
A.4.1 logger.loglevel.....	547
A.4.2 logger.MaxBackupIndex.....	547
A.4.3 logger.MaxFileSize.....	548
A.4.4 logger.hicommandbase.loglevel.....	548
A.4.5 logger.hicommandbase.sysloglevel.....	548
A.4.6 logger.hicommandbase.MaxBackupIndex.....	548
A.4.7 logger.hicommandbase.MaxFileSize.....	549
A.5 Device Manager のスレッドに関するプロパティ (dispatcher.properties ファイル)	549
A.5.1 server.dispatcher.message.timeout.....	549
A.5.2 server.dispatcher.message.timeout.in.processing.....	549
A.5.3 server.dispatcher.daemon.pollingPeriod.....	549
A.5.4 server.dispatcher.traps.purgePeriod.....	550
A.5.5 server.dispatcher.daemon.receiveTrap.....	550
A.5.6 server.dispatcher.snm2.configchange.pollingPeriod.....	550
A.5.7 server.dispatcher.configchange.pollingPeriod.....	550
A.5.8 server.dispatcher.daemon.configUpdate.detection.interval.....	551
A.5.9 server.dispatcher.daemon.autoSynchro.doRefresh.....	552

A.5.10	server.dispatcher.daemon.autoSynchro.type.....	552
A.5.11	server.dispatcher.daemon.autoSynchro.dayOfWeek.....	553
A.5.12	server.dispatcher.daemon.autoSynchro.startTime.....	553
A.5.13	server.dispatcher.daemon.autoSynchro.interval.....	553
A.5.14	server.dispatcher.daemon.configUpdate.detection.variable.enabled.....	553
A.5.15	server.dispatcher.daemon.autoSynchro.performance.doRefresh.....	554
A.5.16	server.dispatcher.daemon.autoSynchro.performance.startTime.....	555
A.5.17	server.dispatcher.daemon.autoSynchro.logicalGroup.doRefresh.....	555
A.5.18	server.dispatcher.daemon.logicalGroupMappingUpdate.startTime.....	556
A.6	Device Manager の MIME に関するプロパティ (mime.properties ファイル)	556
A.7	Device Manager の GUI に関するプロパティ (client.properties ファイル)	556
A.7.1	client.rmi.port.....	556
A.7.2	client.launch.em.secure.....	557
A.7.3	client.externaltask.sn.fetch.enable.....	557
A.7.4	client.externaltask.sn.fetch.pollinginterval.....	557
A.8	Device Manager のセキュリティに関するプロパティ (server.properties ファイルと cimxmlscpa.properties ファイル)	558
A.8.1	server.http.security.clientIP.....	558
A.8.2	server.http.security.clientIPv6.....	559
A.8.3	server.https.security.keystore.....	559
A.8.4	server.http.security.unprotected.....	560
A.8.5	server.https.security.truststore.....	560
A.8.6	server.https.enabledCipherSuites.....	560
A.8.7	server.https.protocols.....	561
A.8.8	Ciphers.....	561
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).....	562
A.9.1	customizedsnmptrap.customizedSNMPTrapEnable.....	563
A.9.2	customizedsnmptrap.customizelist.....	563
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)	564
A.10.1	launchapp.snm2.url.....	565
A.10.2	launchapp.snm2.rmi.port.....	565
A.10.3	launchapp.elementmanager.role.mode.....	565
A.10.4	launchapp.elementmanager.usehostname.....	566
A.11	ホストとの通信に関するプロパティ (host.properties ファイル)	566
A.11.1	host.mf.agent.connection.timeout.....	566
A.11.2	host.agent.access.timeoutForRpm.....	566
A.12	Host Data Collector との連携に関するプロパティ (hostdatacollectors.properties ファイル)	566
A.12.1	hdc.request.timeout.....	567
A.12.2	hdc.rmiregistry.....	567
A.12.3	hdc.rmiserver.....	568
A.12.4	hdc.classloader.....	568
A.12.5	hdc.usessl.....	569
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)	569
A.13.1	migration.dataErase.defaultValue.....	570
A.13.2	migration.plan.candidateVolumeCountLimit.....	570
A.13.3	migration.plan.candidateCapacityGroupDisplayMaxCount.....	570
A.13.4	migration.multiExecution.....	570
A.13.5	migration.volumeDelete.defaultValue.....	571
A.14	Tuning Manager との連携に関するプロパティ (tuningmanager.properties ファイル)	571
A.14.1	htnm.infoAcquirePeriod.....	571
A.14.2	htnm.servers.....	571

A.14.3	htnm.server.n.host.....	572
A.14.4	htnm.server.n.protocol.....	572
A.14.5	htnm.server.n.port.....	572
A.14.6	htnm.flashMode.....	572
A.14.7	hdvm.analytics.report.pdf.showLogo.....	573
A.14.8	hdvm.analytics.disabled.....	573
A.14.9	hdvm.analytics.healthcheck.excludeMainframe.....	573
A.14.10	hdvm.analytics.healthcheck.notification.exportreport.locale.....	573
A.14.11	htnm.agent.use.cipher.type.....	574
A.15	[レプリケーション] タブに関するプロパティ (replication.properties ファイル)	574
A.15.1	server.dispatcher.daemon.replication.config.doUpdate.....	574
A.15.2	server.dispatcher.daemon.replication.config.updateInterval.....	575
A.15.3	server.dispatcher.daemon.replication.config.offset.....	575
A.15.4	server.dispatcher.daemon.replication.config.minute.....	576
A.15.5	server.dispatcher.daemon.replication.performance.rpm.updateInterval.....	576
A.15.6	server.dispatcher.daemon.replication.performance.tnm.updateInterval.....	576
A.15.7	server.dispatcher.daemon.replication.performance.tnm.offset.....	576
A.15.8	server.dispatcher.daemon.replication.performance.tnm.minute.....	577
A.15.9	hdvm.replication.disabled.....	577
A.16	Replication Manager との連携に関するプロパティ (rpm.lib.properties ファイル)	577
A.16.1	rpm.lib.rpm.port.....	578
A.17	CIM/WBEM 機能に関するプロパティ (jsvc.properties ファイル, cimxmlcpa.properties ファイル, cimxmlscpa.properties ファイル)	578
A.17.1	com.wbemsolutions.jsvc.bindto.....	578
A.17.2	HTTPPort.....	579
A.17.3	HTTPSPort.....	579
付録 B	Tiered Storage Manager サーバのプロパティ	581
B.1	Tiered Storage Manager サーバのプロパティファイル.....	582
B.1.1	Tiered Storage Manager サーバのプロパティの変更.....	582
B.1.2	Tiered Storage Manager サーバのプロパティファイルの記述規則.....	583
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)	583
B.2.1	server.rmi.port.....	583
B.2.2	server.rmi.security.port.....	584
B.2.3	server.base.initialsynchro.....	584
B.2.4	server.mail.smtp.host.....	584
B.2.5	server.mail.from.....	585
B.2.6	server.mail.errorsTo.....	585
B.2.7	server.mail.smtp.port.....	585
B.2.8	server.mail.smtp.auth.....	585
B.2.9	server.eventNotification.mail.to.....	585
B.2.10	server.eventMonitoringIntervalInMinute.....	585
B.2.11	server.migration.multiExecution.....	586
B.2.12	server.checkOutVolumeRange.....	586
B.2.13	server.migration.dataErase.defaultValue.....	586
B.2.14	server.migrationPlan.candidateVolumeCountLimit.....	586
B.2.15	server.migrationPlan.candidateCapacityGroupDisplayMaxCount.....	587
B.2.16	server.migration.maxRetryCount.....	587
B.3	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)	587
B.3.1	dbm.traceSQL.....	587
B.4	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)	588
B.4.1	hdvm.protocol.....	588

B.4.2 hdvm.port.....	588
B.4.3 hdvm.timeout.....	588
B.4.4 hdvm.rmi.port.....	588
B.5 Tiered Storage Manager のログ出力に関するプロパティ (logger.properties ファイル)	589
B.5.1 logger.messageLogLevel.....	589
B.5.2 logger.traceLogLevel.....	590
B.5.3 logger.syslogLevel.....	590
B.5.4 logger.serverMessageFileCount.....	590
B.5.5 logger.serverTraceFileCount.....	591
B.5.6 logger.guiMessageFileCount.....	591
B.5.7 logger.guiTraceFileCount.....	591
B.5.8 logger.serverMessageMaxFileSize.....	592
B.5.9 logger.serverTraceMaxFileSize.....	592
B.5.10 logger.guiMessageMaxFileSize.....	592
B.5.11 logger.guiTraceMaxFileSize.....	592
B.6 Tiered Storage Manager のセキュリティに関するプロパティ (server.properties ファイル)	592
B.6.1 server.rmi.secure.....	593
B.6.2 server.rmi.security.enabledCipherSuites.....	593
B.6.3 server.rmi.security.protocols.....	594
付録 C Host Data Collector のプロパティ	595
C.1 Host Data Collector のプロパティファイル.....	596
C.1.1 Host Data Collector のプロパティの変更.....	596
C.2 Host Data Collector の動作に関するプロパティ (hdcbase.properties ファイル)	596
C.2.1 hdc.service.localport.....	597
C.2.2 hdc.adapter.adapterProcessNum.....	597
C.2.3 hdc.adapter.localport.....	597
C.2.4 hdc.common.rmi.registryPort.....	597
C.2.5 hdc.common.rmi.serverPort.....	598
C.2.6 hdc.common.http.serverPort.....	598
C.2.7 hdc.common.rmi.ssl.registryPort.....	599
C.2.8 hdc.common.rmi.ssl.serverPort.....	599
C.2.9 hdc.common.https.serverPort.....	599
C.2.10 hdc.service.rmi.registryIPAddress.....	600
C.2.11 hdc.service.fileCleanup.startTime.....	600
C.2.12 hdc.adapter.esx.timeout.....	600
C.2.13 hdc.ssl.secure.....	601
C.2.14 hdc.ssl.esx.certCheck.....	601
C.2.15 hdc.common.bindServerIPAddress.....	602
C.2.16 hdc.common.allowIPAddressList.....	602
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)	603
C.3.1 logger.trace.level.....	603
C.3.2 logger.trace.maxFileSize.....	603
C.3.3 logger.trace.numOfFiles.....	604
C.3.4 logger.iotrace.maxFileSize.....	604
C.3.5 logger.iotrace.numOfFiles.....	604
C.4 Host Data Collector の Java 環境に関するプロパティ (javaconfig.properties ファイル)	604
C.4.1 javapathlocation.....	605
C.5 Host Data Collector のセキュリティに関するプロパティ (hdcbase.properties ファイル)	605
C.5.1 hdc.ssl.ciphers.....	605
C.5.2 hdc.ssl.esx.enabledTLSv1.....	606

付録 D Device Manager エージェントのプロパティ.....	607
D.1 Device Manager エージェントのプロパティファイル.....	608
D.1.1 Device Manager エージェントのプロパティの変更.....	608
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)	609
D.2.1 agent.rm.TimeOut.....	609
D.2.2 agent.rm.everytimeShutdown.....	609
D.2.3 agent.rm.shutdownWait.....	609
D.2.4 agent.rm.horcmlInstance.....	610
D.2.5 agent.rm.horcmlService.....	610
D.2.6 agent.rm.horcmlRange.....	611
D.2.7 agent.logger.loglevel.....	611
D.2.8 agent.logger.MaxBackupIndex.....	611
D.2.9 agent.logger.MaxFileSize.....	612
D.2.10 agent.rm.lunPathCheck.....	612
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).....	612
D.3.1 agent.util.hpux.displayDsf.....	613
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)	613
D.4.1 logger.loglevel.....	614
D.4.2 logger.MaxBackupIndex.....	614
D.4.3 logger.MaxFileSize.....	614
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))	615
D.5.1 veritas.volume.manager.version.....	615
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)	615
D.6.1 server.agent.port.....	616
D.6.2 server.http.localPort.....	616
D.6.3 server.http.port.....	616
D.6.4 server.http.host.....	616
D.6.5 server.http.socket.agentAddress.....	617
D.6.6 server.http.socket.bindAddress.....	617
D.6.7 server.agent.maxMemorySize.....	618
D.6.8 server.agent.shutDownTime.....	618
D.6.9 server.agent.JRE.location.....	618
D.6.10 server.http.entity.maxLength.....	619
D.6.11 server.http.security.clientIP.....	619
D.6.12 server.server.authorization.....	619
D.6.13 server.server.serverIPAddress.....	619
D.6.14 server.server.serverPort.....	620
D.6.15 server.agent.rm.centralizePairConfiguration.....	620
D.6.16 server.agent.rm.cuLdevForm.....	620
D.6.17 server.agent.rm.exclusion.instance.....	621
D.6.18 server.agent.rm.location.....	621
D.6.19 server.agent.rm.optimization.userHorcmFile.....	621
D.6.20 server.agent.rm.horcml.poll.....	622
D.6.21 server.agent.rm.temporaryInstance.....	622
D.6.22 server.agent.rm.temporaryPort.....	622
D.6.23 server.agent.rm.pairDefinitionForm.....	622
D.6.24 server.agent.rm.userAuthentication.....	624
D.6.25 server.agent.rm.ignorePairStatus.....	624
D.6.26 server.agent.rm.horcmlSource.....	625
D.6.27 server.agent.rm.moduleTimeOut.....	625
D.6.28 server.server.ssl.hdvm.....	625
D.6.29 server.http.server.timeOut.....	626

D.6.30 server.util.processTimeOut.....	626
D.6.31 server.agent.evtwait.timeout.....	626
D.6.32 server.agent.snapshotEvtwait.timeout.....	626
D.6.33 server.agent.rmxp.location.....	626
D.7 Device Manager エージェントが接続するコマンドデバイスに関するプロパティファイル (rgcmddev.properties ファイル)	627
付録 E 管理クライアントに関するセキュリティ設定.....	629
E.1 警告バナーとは.....	630
E.1.1 警告バナーに表示するメッセージの条件.....	630
E.1.2 警告バナーに表示するメッセージの作成と登録.....	630
E.1.3 警告バナーからのメッセージの削除.....	632
E.2 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.....	632
付録 F コピーペア定義の移行.....	635
F.1 コピーペア定義の移行とは.....	636
F.2 コピーペア定義を移行するための前提条件.....	638
F.3 コピーペア定義をデバイスグループ定義に移行する.....	640
F.4 ペア定義移行コマンドで使用するプロパティ.....	641
付録 G このマニュアルの参考情報.....	645
G.1 関連マニュアル.....	646
G.2 このマニュアルでの表記.....	646
G.3 このマニュアルで使用している略語.....	653
G.4 KB（キロバイト）などの単位表記について.....	656
索引.....	657



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
- ストレージシステムのサポートについて
- ストレージシステムのサポート終了について
- OS, 仮想化ソフトウェア, ブラウザーなどのサポートについて
- エンドユーザライセンスについて

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 外部認証サーバでのユーザー管理

外部認証サーバでユーザー認証する方法について説明しています。

第5章 通信に関するセキュリティ設定

Hitachi Command Suite 製品で利用できる通信に関するセキュリティ設定について説明しています。

第6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7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8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 Hitachi Command Suite の監査ログ

Device Manager および Tiered Storage Manager の監査ログを採取するために必要な設定や、監査ログで確認できる情報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保守情報の取得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 管理クライアントに関するセキュリティ設定

管理クライアントに関するセキュリティ設定について説明しています。

付録 F コピーペア定義の移行

構成定義ファイルで管理されるコピーペア定義をストレージシステム上のデバイスグループ定義に移行する方法について説明しています。

付録 G 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®

表記	製品名
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 Server® 2008 Microsoft® Windows Server® 2008 R2 Microsoft® Windows Server® 2012 Microsoft® Windows Server® 2012 R2
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

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。

ストレージシステムのサポートについて

Hitachi Virtual Storage Platform E990 については、特に記載がない場合、Hitachi Virtual Storage Platform F900 に対する記載を参照してください。マニュアルでの表記については、「[G.2 このマニュアルでの表記](#)」を参照してください。

ストレージシステムのサポート終了について

次に示すストレージシステムのサポートを終了しました。サポートを終了したストレージシステムに関するマニュアル中の記載は無視してください。マニュアルでの表記については、「[G.2 このマニュアルでの表記](#)」を参照してください。

バージョン 8.6.1 からサポート終了

- Hitachi Universal Storage Platform 100
- Hitachi Universal Storage Platform 600
- Hitachi Universal Storage Platform 1100
- Hitachi Universal Storage Platform H10000
- Hitachi Universal Storage Platform H12000
- Hitachi network Storage Controller

バージョン 8.5.3 からサポート終了

- Hitachi Adaptable Modular Storage シリーズ
 - Hitachi Adaptable Modular Storage 1000
 - Hitachi Adaptable Modular Storage 500
 - Hitachi Adaptable Modular Storage 200
 - BladeSymphony 専用エントリークラスディスクアレイ装置 BR150
- Hitachi Workgroup 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 BR50
- Hitachi Tape Modular Storage シリーズ

OS, 仮想化ソフトウェア, ブラウザーなどのサポートについて

OS, 仮想化ソフトウェア, ブラウザーなどの最新のサポート状況は、「ソフトウェア添付資料」を参照してください。

サポートが終了したソフトウェアに関するマニュアル中の記載は無視してください。

新しいバージョンをサポートしたソフトウェアについては、特に記載がないかぎり、従来サポートしているバージョンと同等のものとしてサポートします。

エンドユーザライセンスについて

デスクトップアプリケーションの GUI には、Adobe AIR を使用しています。

- Prohibitions against distribution and/or copying of the Object Code Redistributables separately from a Developer Application.
- Prohibitions against creating modifications and/or derivative works of, and against decompiling and reverse engineering, the Object Code Redistributables;
- A disclaimer of indirect, special, incidental, punitive, and consequential damages, and of all applicable statutory warranties, to the full extent allowed by law;
- A provision indicating ownership of the Sample Code, SDK Source Files and Object Code Redistributables by HARMAN and its licensors.

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。

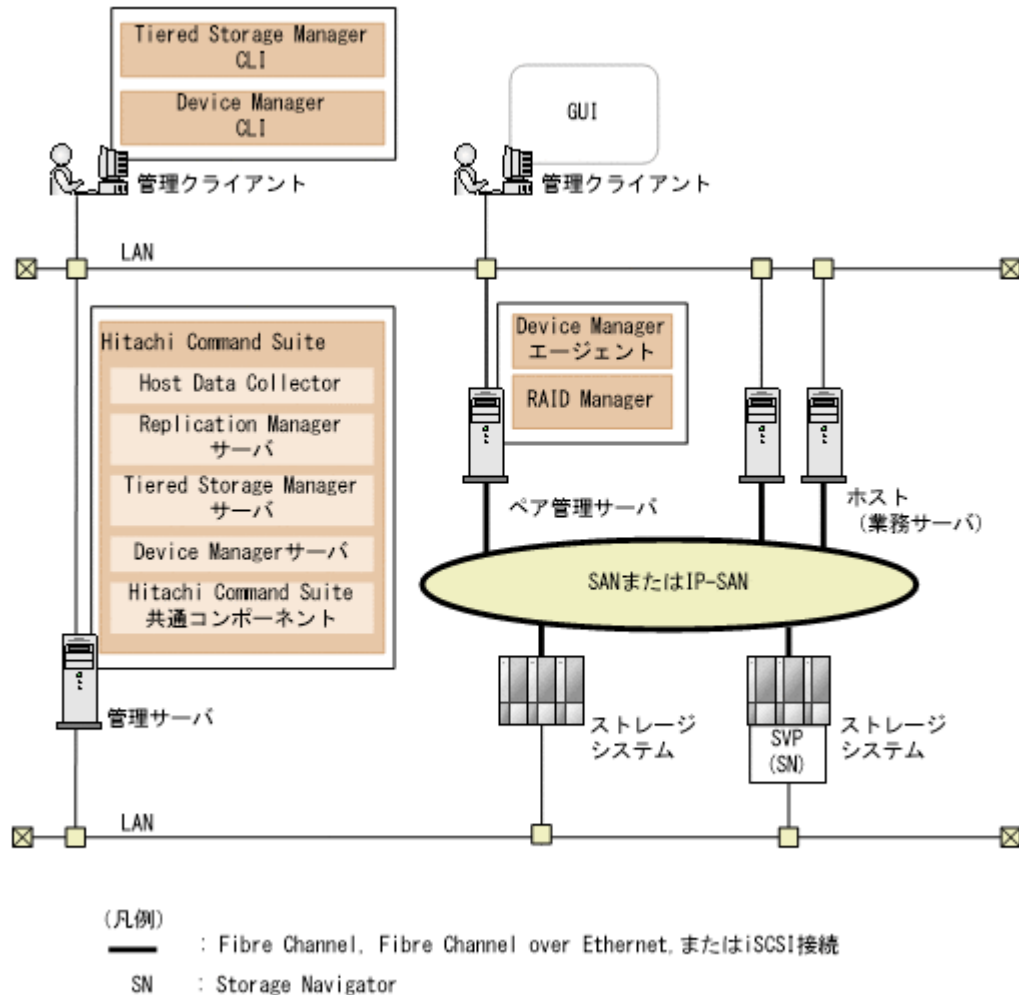
- 1.1 システム構成
- 1.2 セキュリティ構成
- 1.3 管理サーバおよび Host Data Collector マシンのシステム要件
- 1.4 Device Manager で管理できるホスト
- 1.5 Device Manager のホスト管理ソフトウェア
- 1.6 通常ホストのシステム要件
- 1.7 仮想マシンのシステム要件
- 1.8 仮想化サーバのシステム要件
- 1.9 メインフレームホストのシステム要件
- 1.10 ファイルサーバのシステム要件
- 1.11 NAS モジュールのシステム要件
- 1.12 関連製品
- 1.13 Device Manager でのコピーペア管理
- 1.14 コピーペアを管理する場合のシステム構成（一括管理構成）
- 1.15 コピーペアを管理する場合のシステム構成（一括管理構成以外）
- 1.16 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
- 1.17 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

- 1.18 コピーペアを管理する場合の注意事項
- 1.19 高可用性システムの構築
- 1.20 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 基本的なシステム構成



管理クライアント

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

GUI

グラフィカルユーザーインターフェースです。

Device Manager を操作する GUI には、次の二種類があります。

- デスクトップアプリケーションの GUI (Adobe AIR 環境で動作する GUI)
- Web アプリケーションの GUI (Web ブラウザーの Adobe Flash Player 環境で動作する GUI)

GUI についてはマニュアル「*Hitachi Command Suite ユーザーズガイド*」を参照してください。

Device Manager CLI および Tiered Storage Manager CLI

コマンドラインプロンプトから実行するコマンドラインインターフェースです。

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。

Hitachi Command Suite は、次のコンポーネントから構成され、常に一緒にインストールおよびアンインストールされます。

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 製品で共通する機能を提供するコンポーネントです。

Device Manager サーバ

Device Manager で、ストレージシステムのボリュームを管理するために必要なコンポーネントです。

Tiered Storage Manager サーバ

Tiered Storage Manager で、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に必要なコンポーネントです。

Replication Manager サーバ

Replication Manager で、ストレージシステムのボリュームを複製するために必要な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。



ヒント

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

ペア管理サーバ

コピーペアの構成や状態などの情報を収集し、管理するためのマシンです。次のプログラムをインストールします。

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するために必要なプログラムです。

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も必要です。

RAID Manager または RAID Manager XP

ストレージシステム上のコピーペアを制御するために必要なプログラムです。

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。

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。次に示す機種のストレージシステムを管理できます。

- エンタープライズクラスストレージ
VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, Virtual Storage Platform, Universal Storage Platform V/VM および Hitachi USP のストレージシステムの総称です。

- VSP Gx00 モデル
- VSP Fx00 モデル
- HUS VM
- ミッドレンジストレージ
HUS100, Hitachi AMS2000, Hitachi SMS, Hitachi AMS/WMS のストレージシステムの総称です。

SVP

ストレージシステムを管理するためのコンピュータです。エンタープライズクラスストレージ、VSP Gx00 モデル、VSP Fx00 モデル、または HUS VM の場合に使用されます。エンタープライズクラスストレージ、または HUS VM の場合、ストレージシステムに搭載されています。VSP Gx00 モデルまたは VSP Fx00 モデルの場合、ストレージシステムの管理機能を提供するサーバを SVP として設置して使用します。



メモ

VSP 5000 シリーズ、VSP G1000, G1500, VSP F1500, VSP Gx00 モデル、または VSP Fx00 モデルを使用する場合、管理サーバと SVP の時刻を合わせてください。

Storage Navigator

Device Manager のコンポーネントです。ストレージシステムの構成やリソースの設定をより詳細な条件で行うための機能を提供します。

ネットワーク (LAN および SAN)

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 SAN または IP-SAN を構成します。

システム構成を検討する場合、次の点に注意してください。

- 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 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 サーバを用意してください。
- Device Manager エージェントのバージョンが 8.1.1 以前の場合、次の OS では、Device Manager エージェントをインストールすると、Global Link Manager エージェントも自動的にインストールされます。
 - Windows
 - 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。

1.2 セキュリティ構成

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP および HUS VM は, SVP と通信します。

SVP には, 次の 2 種類の Ethernet アダプターがあります。

- プライベート (内部) Ethernet LAN 用アダプター
ストレージシステム内の通信に使用されます。
- パブリック LAN 用アダプター
ストレージシステムの外部にあるほかのコンピュータのアプリケーションが, SVP と通信するために使用されます。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。



警告

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 を接続しないでください。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, および Hitachi AMS/WMS を, パブリックネットワークに接続する場合には注意が必要です。

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。

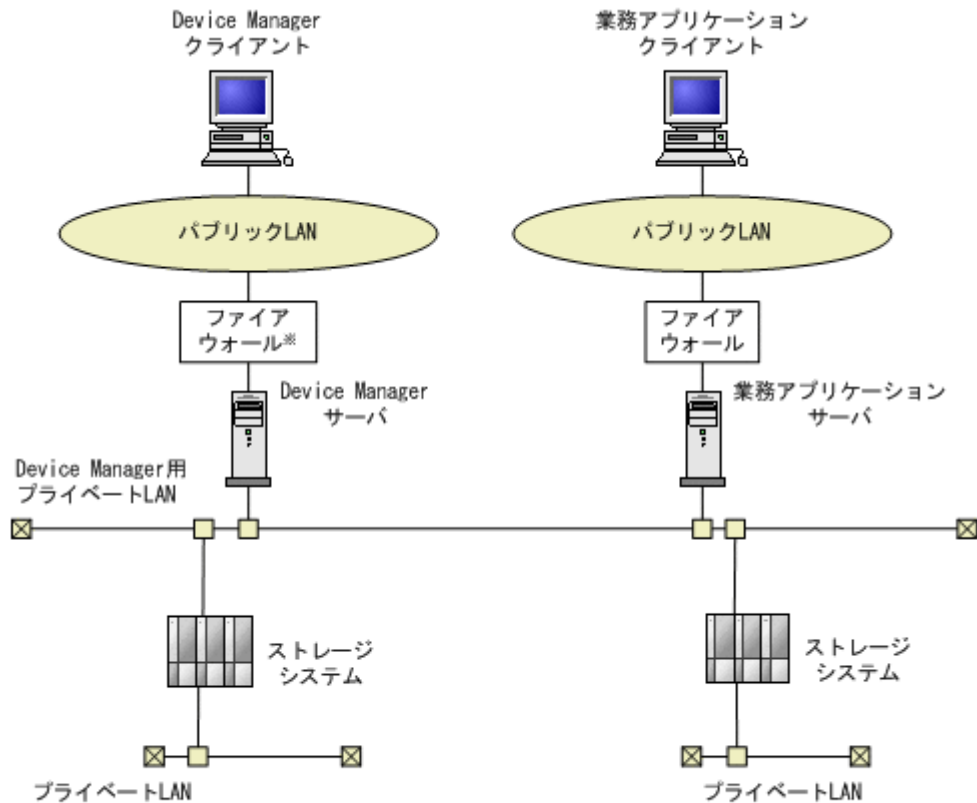
管理用の LAN の構成に関するガイドラインを以下に示します。

- 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 Device Manager で推奨するセキュリティ構成

管理サーバをデュアルホームにするか、NIC を 2 つ搭載してください。一方の NIC を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の LAN に接続し、もう一方の NIC を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 2 管理用の LAN を分離し、ファイアウォールを設置した構成](#)」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てください。

図 2 管理用の LAN を分離し、ファイアウォールを設置した構成



注※ Device Manager は、NAT1には対応していません。

1.3 管理サーバおよび Host Data Collector マシンのシステム要件

ここでは管理サーバ、および管理サーバと異なるマシンにインストールした Host Data Collector 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 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 数とパス数 ^{※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>

関連タスク

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

関連参照

- [付録 A.2.11 server.cim.support.job](#)

1.3.2 メモリーヒープサイズの変更

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（Linux の場合）を編集します。

前提条件

次の情報の確認

- 管理対象となる LDEV 数

表 2 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		
	512MB	1024MB	2048MB
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または NAS モジュールの構成（ファイルサーバまたは NAS モジュールを管理対象にする場合）
ファイルサーバまたは NAS モジュールの台数に応じて、次のとおりメモリーヒープサイズを設定してください。
 - ファイルサーバまたは NAS モジュールを 1 台管理する場合
メモリーヒープサイズは 1024MB を設定してください。
 - ファイルサーバまたは NAS モジュールを 2 台以上管理する場合
メモリーヒープサイズは 2048MB 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。

操作手順

- 次のファイルをテキストエディターで開きます。

Window の場合

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager
%HiCommandServer%Server.ini
```

Linux の場合

```
<Hitachi Command Suite のインストールディレクトリ>/hicommand.sh
```

- メモリーヒープサイズを変更します。
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
```

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

1.3.3 管理サーバの 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、hcmds64chgjdk コマンドを実行します。

前提条件

- 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。



メモ

- 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 製品に同梱された JDK に切り替えてください。

操作手順

- Hitachi Command Suite 製品のサービスを停止します。
- 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 のインストールフォルダ>%Base64%bin  
%hcmds64chgjdk
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/  
hcmds64chgjdk
```

3. 次の場合は、hcmds64keytool ユーティリティ (Windows の場合) または keytool ユーティリティ (Linux の場合) で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、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 サーバ間で SSL/TLS 通信を使用している場合
4. Hitachi Command Suite 製品のサービスを起動します。
 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。

関連タスク

- [5.5.11 Hitachi Command Suite 共通コンポーネントのトラストストアへの証明書のインポート](#)
- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

1.3.4 Host Data Collector の Java の実行環境の変更

Host Data Collector マシン (管理サーバと異なるマシン) の 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。

前提条件

- 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 (Linux の場合) でのログイン
- 管轄ポリシーファイルのインストール (Host Data Collector を SSL サーバとして使用する場合)
使用する Java の実行環境のバージョンに応じた Java Cryptography Extension (JCE) の無制限強度の管轄ポリシーファイル (Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files) をダウンロードし、インストールする必要があります。
管轄ポリシーファイルは、Oracle 社の Web サイトからダウンロードしてください。インストール方法は、管轄ポリシーファイルに付属するドキュメントを参照してください。
- 次の情報の確認
 - 使用する Java の実行環境のインストールパスの確認

操作手順

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。

操作結果

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。

関連タスク

- [9.2.2 Host Data Collector のサービスの起動](#)
- [9.2.3 Host Data Collector のサービスの停止](#)

関連参照

- [付録 C.4.1 javapathlocation](#)

1.4 Device Manager で管理できるホスト

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。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 3 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 Capacity Optimization	
	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。



メモ

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。

1.5 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 4 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※	Y	Y	Y	--	--
Device Manager エージェント※	Y	Y	--	--	--
Mainframe Agent	--	--	--	Y	--
ファイルサーバ管理ソフトウェア	--	--	--	--	Y

(凡例)

- Y : 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 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。
オープンホストを管理する場合、Device Manager のホスト管理ソフトウェアとして Host Data Collector を使用することを推奨します。



ヒント

Host Data Collector は、ホスト情報収集のためのモジュールとモジュール実行用のスクリプトを、管理対象ホストの次の場所に転送します。

Windows ホストの場合：admin\$（ファイル共有プロトコル、SMB プロトコルによる通信）

UNIX ホストの場合：/tmp（SSH プロトコルによる通信）

Host Data Collector は、転送したモジュール実行用のスクリプトを実行して、管理対象ホストの情報を収集します。

管理対象ホストでは、Host Data Collector によるリモート操作を許可するための環境設定が必要です。

- 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。
- 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。



メモ

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。

ただし、Compute Systems Manager から Linux ホストに su コマンドを利用する方法でアクセスしている場合、Device Manager では sudo コマンドを実行できるように設定する必要があります。sudo コマンドの設定方法については、通常ホストの前提環境について説明している個所を参照してください。



ヒント ホスト管理ソフトウェアの管理対象ホストの詳細については、ソフトウェア添付資料を参照してください。

関連参照

- [1.6.1 通常ホストの前提環境](#)

1.6 通常ホストのシステム要件

Host Data Collector 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。



メモ

- ホストの OS が Linux で Device-Mapper マルチパス機能 (DM-Multipath) を使用する場合、`/etc/multipath.conf` ファイルの `multipaths` セクションで、`alias` 属性にマルチパスデバイスの別名を設定するときは、次の文字を使用してください。
`A~Z a~z 0~9 - _ . @`
- 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。
- Solaris マルチパス機能 (MPxIO) が有効な Solaris ホストの場合、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 LUN の範囲は 0~255 となるように指定してください。LUN が 256 以上の場合、次の問題が発生します。
 - LUN が 256 以上の LDEV の情報が収集されない。
 - コマンドデバイスの LUN が 256 以上の場合、Replication Manager でコピーペア構成定義の操作を行ったときに、KAVN00451-E のエラーメッセージが出力され、操作が失敗する。

1.6.1 通常ホストの前提環境

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。
- Windows の Application Experience サービスの [スタートアップの種類] が [手動] または [自動] に設定されている。
- ホストが Active Directory のメンバーとして管理されている場合、次に示すドメインのグループポリシーが [未構成] または [無効] に設定されている。
[Windows コンポーネント] - [アプリケーションの互換性] - [プログラム互換性アシスタントを終了する]

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。



メモ

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。
- リモートから一般ユーザーアカウント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。
- 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)。
- 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。



メモ

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。



メモ

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)
-



ヒント Host Data Collector のセットアップ方法については、マニュアル「*Hitachi Command Suite* インストールガイド」を参照してください。

1.7 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。

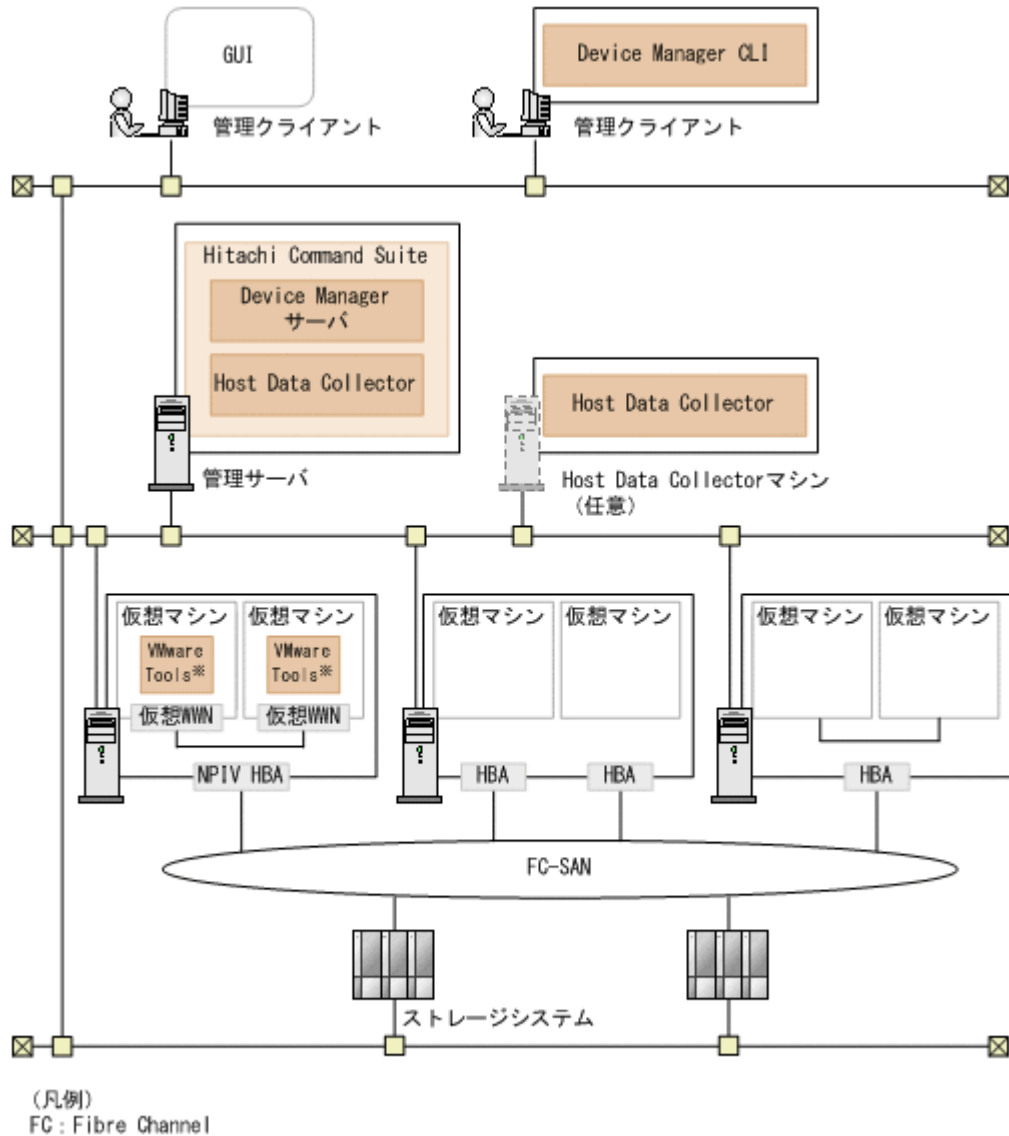
- 仮想マシンごとに仮想 HBA が割り当てられている構成 (NPIV HBA を使用している場合) (推奨)
- 仮想マシンごとに HBA が割り当てられている構成
- 複数の仮想マシンで HBA を共有している構成

Host Data Collector 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。

1.7.1 仮想マシンの前提環境

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 3 仮想マシンの前提環境



注※ 仮想化ソフトウェアにVMware ESXi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。



ヒント Host Data Collector のセットアップ方法については、マニュアル「Hitachi Command Suite インストールガイド」を参照してください。仮想化サーバの登録方法については、マニュアル「Hitachi Command Suite ユーザーズガイド」またはマニュアル「Hitachi Command Suite CLI リファレンスガイド」を参照してください。

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。
- Windows の Application Experience サービスの [スタートアップの種類] が [手動] または [自動] に設定されている。
- ホストが Active Directory のメンバーとして管理されている場合、次に示すドメインのグループポリシーが [未構成] または [無効] に設定されている。
[Windows コンポーネント] - [アプリケーションの互換性] - [プログラム互換性アシスタントを終了する]
- 仮想化ソフトウェアに VMware ESXi を使用し、かつ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

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。
- 仮想化ソフトウェアに VMware ESXi を使用し、かつ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



メモ

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。
- リモートから一般ユーザーアカウント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。
- 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。

- 仮想化ソフトウェアに VMware ESXi を使用し、かつ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



メモ

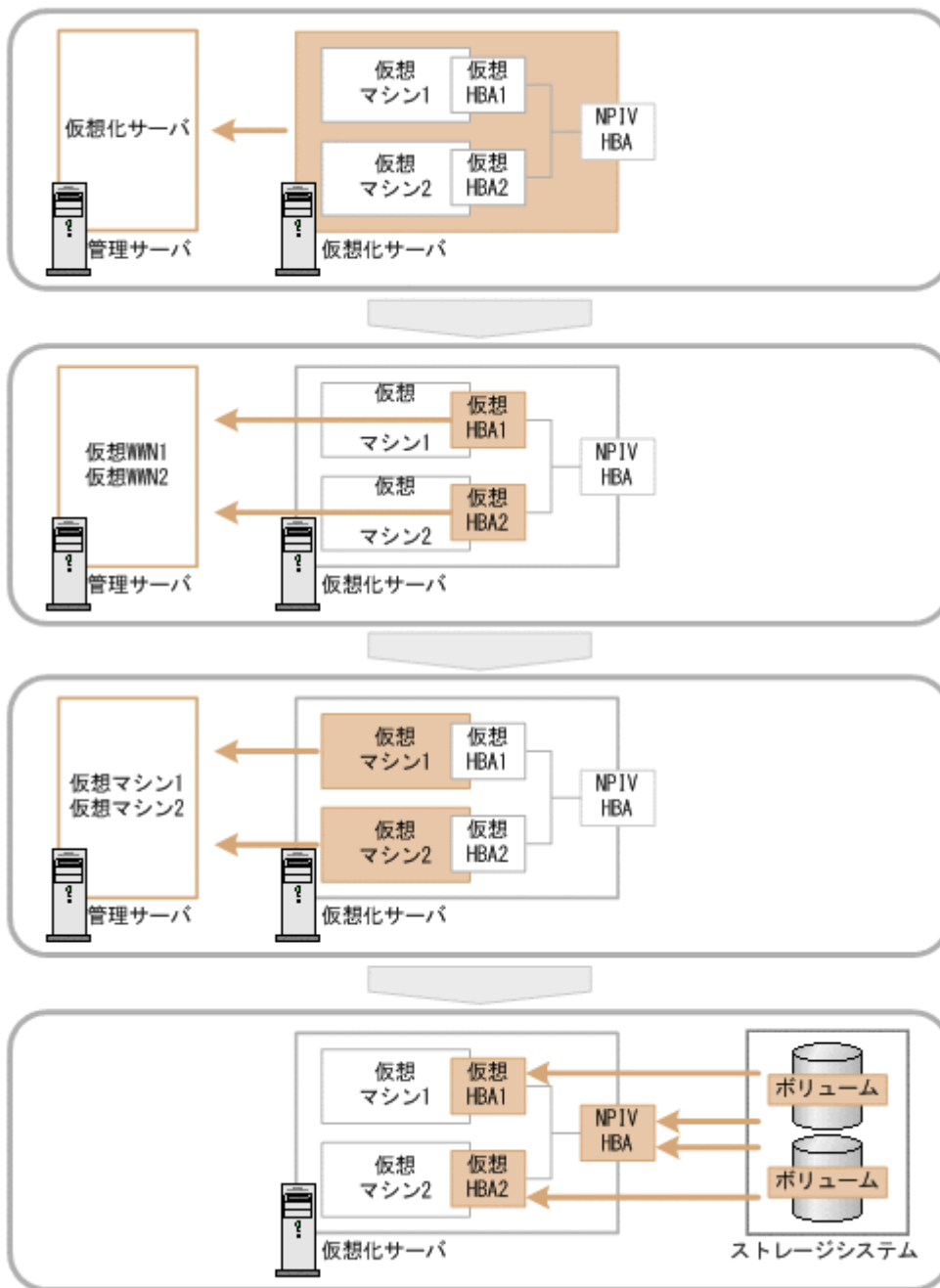
一般ユーザーアカウントで Device Manager に登録したホストを、root アカウントを使って二重に登録しないでください。

1.7.2 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)

図 4 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)

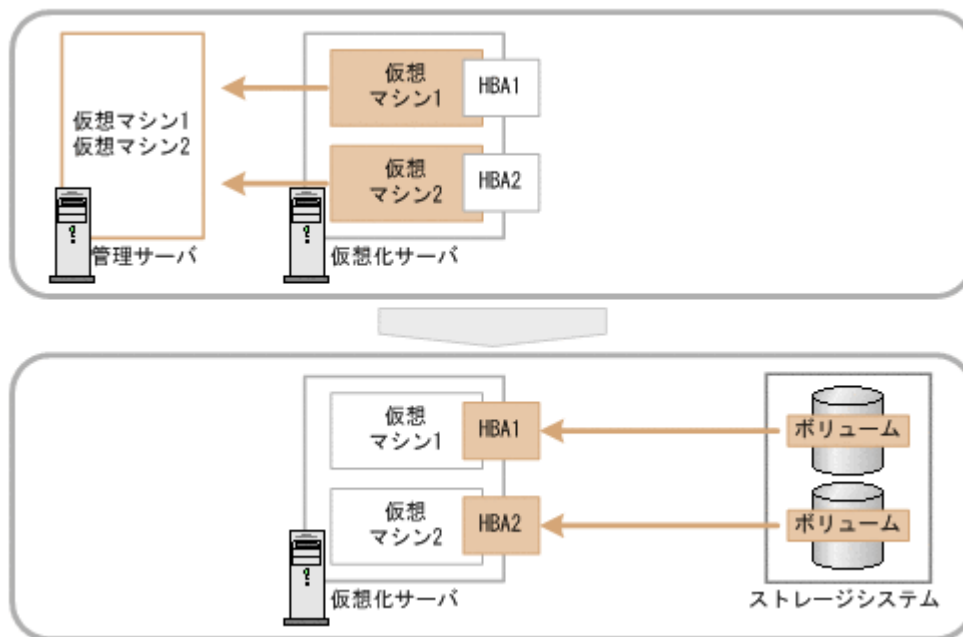


1. ボリュームの使用状況を管理したい仮想マシンが稼働する仮想化サーバを Device Manager に登録します。
仮想化サーバの登録方法は、マニュアル「Hitachi Command Suite ユーザーズガイド」またはマニュアル「Hitachi Command Suite CLI リファレンスガイド」を参照してください。
2. ボリュームの使用状況を管理したい各仮想マシンを Device Manager に通常ホストとして登録します。

3. 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。
ボリュームの LUN パスは、仮想化サーバ（物理 WWN）と仮想マシン（仮想 WWN）で、ポートが一致している必要があります。
4. 仮想化サーバを再起動します。

仮想マシンごとに HBA が割り当てられている構成

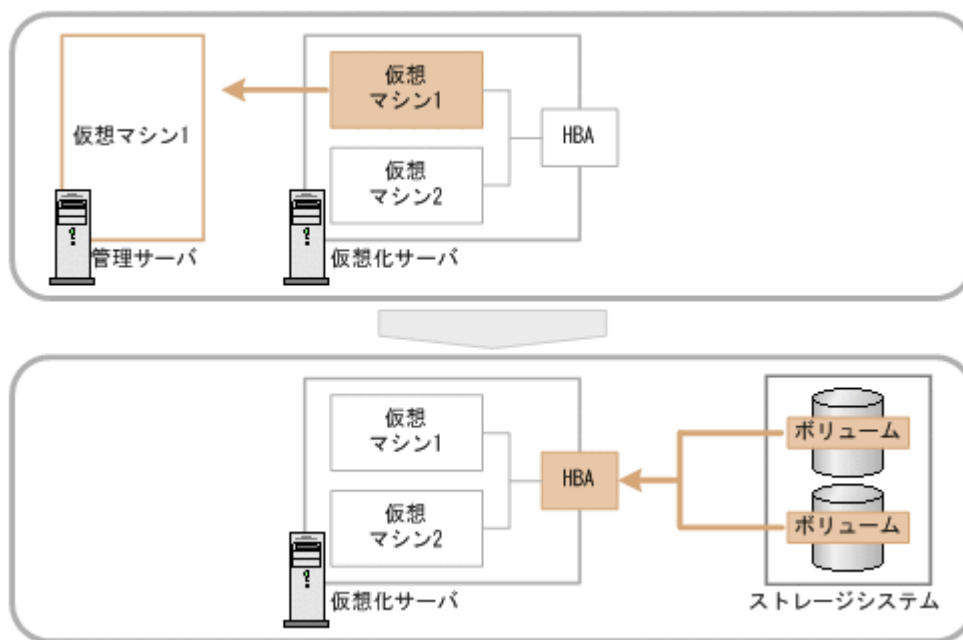
図 5 仮想マシンにボリュームを割り当てるための操作フロー（仮想マシンごとに HBA が割り当てられている構成）



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。
仮想化サーバの登録方法は、マニュアル「Hitachi Command Suite ユーザーズガイド」またはマニュアル「Hitachi Command Suite CLI リファレンスガイド」を参照してください。
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 6 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。
仮想化サーバの登録方法は、マニュアル「*Hitachi Command Suite ユーザーズガイド*」またはマニュアル「*Hitachi Command Suite CLI リファレンスガイド*」を参照してください。
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。



メモ

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。

関連参照

- [1.7.3 仮想マシンの構成変更時に必要な作業](#)

1.7.3 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。

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

仮想 WWN を追加または変更した場合

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してください。

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

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：

```
< Hitachi Command Suite のインストールフォルダ > ¥DeviceManager  
¥HiCommandServer¥config¥npivmapping.properties
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/  
config/npivmapping.properties
```

1.8 仮想化サーバのシステム要件

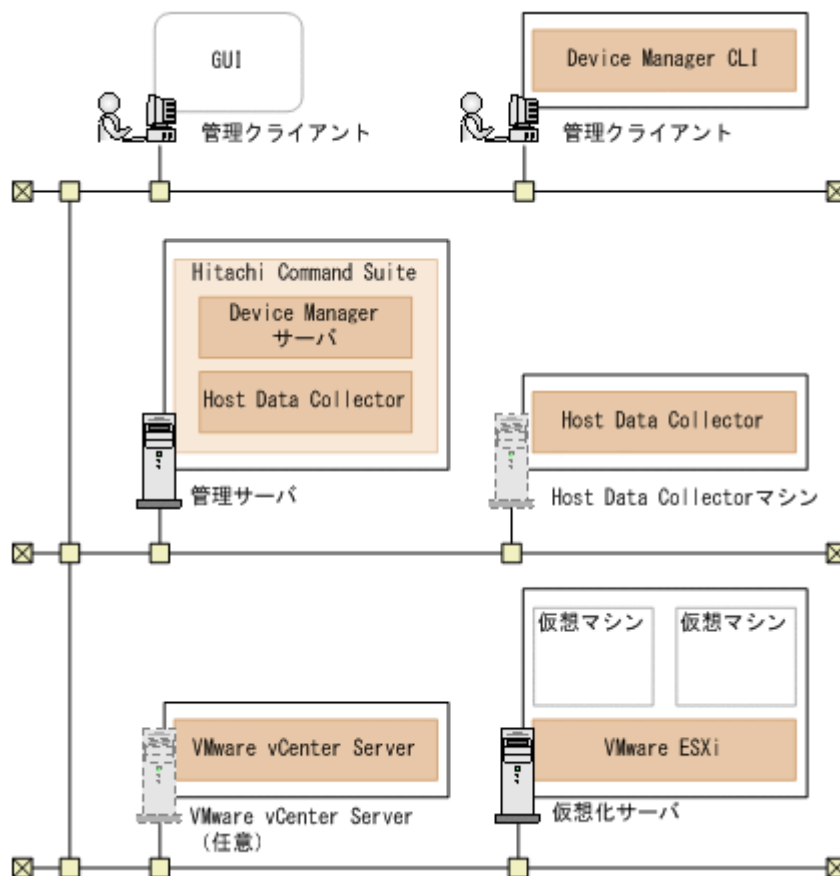
Device Manager は、Host Data Collector を使用して、仮想化サーバのマシン情報および仮想化サーバに割り当てられているボリュームの情報を収集します。

1.8.1 仮想化サーバの前提環境

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 ESXi 5.x または VMware ESXi 6.x です。

図 7 仮想化サーバの前提環境 (Host Data Collector で管理する場合)



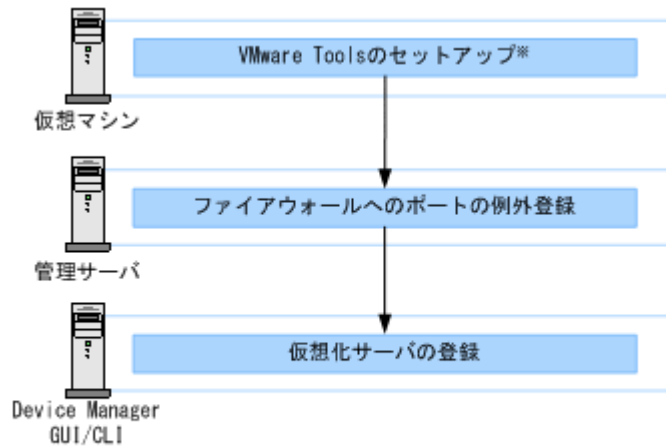
- Host Data Collector は、管理サーバにインストールする Hitachi Command Suite に同梱されているほか、管理サーバ以外のマシンにインストールすることもできます。なお、Host Data Collector マシンを複数台設置する場合は、各マシンにインストールされた Host Data Collector のバージョンおよびリビジョンを同じにしてください。
- 仮想化サーバ上の仮想マシンに仮想 HBA が割り当てられている場合は、その仮想マシンに VMware Tools をインストールする必要があります。
- Host Data Collector マシ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

Host Data Collector のセットアップ方法については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。

1.8.2 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 8 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。

1.8.3 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 で仮想化サーバの情報をリフレッシュしてください。
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、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 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 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。
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。

1.9 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。

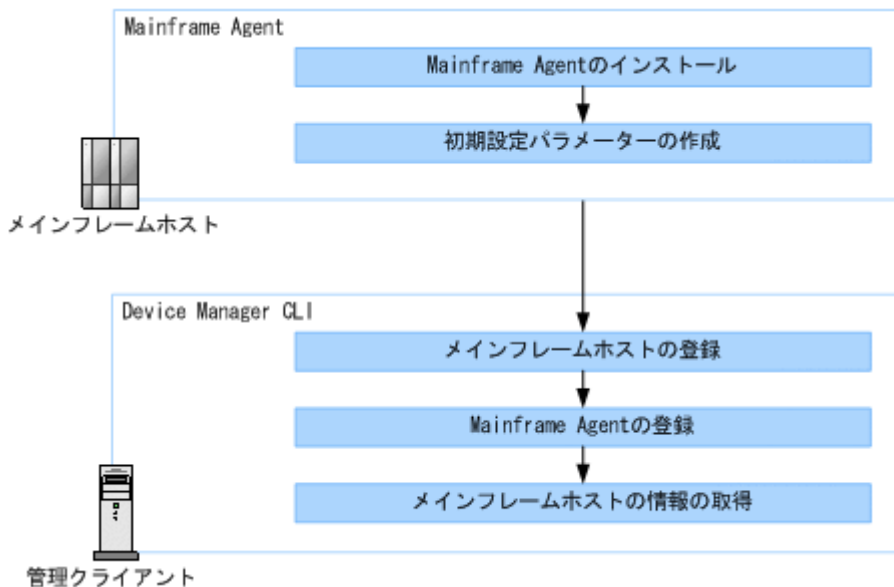
- メインフレームボリュームの使用状況やストレージシステムの論理 DKC シリアル番号の参照 (Device Manager)
- メインフレームボリュームのマイグレーションやシュレディング (Tiered Storage Manager)

1.9.1 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。

Device Manager CLI での環境設定方法は、マニュアル「*Hitachi Command Suite CLI リファレンスガイド*」を参照してください。Mainframe Agent での環境設定方法は、マニュアル「*Hitachi Command Suite Mainframe Agent ユーザーズガイド*」を参照してください。

図 9 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



1.10 ファイルサーバのシステム要件

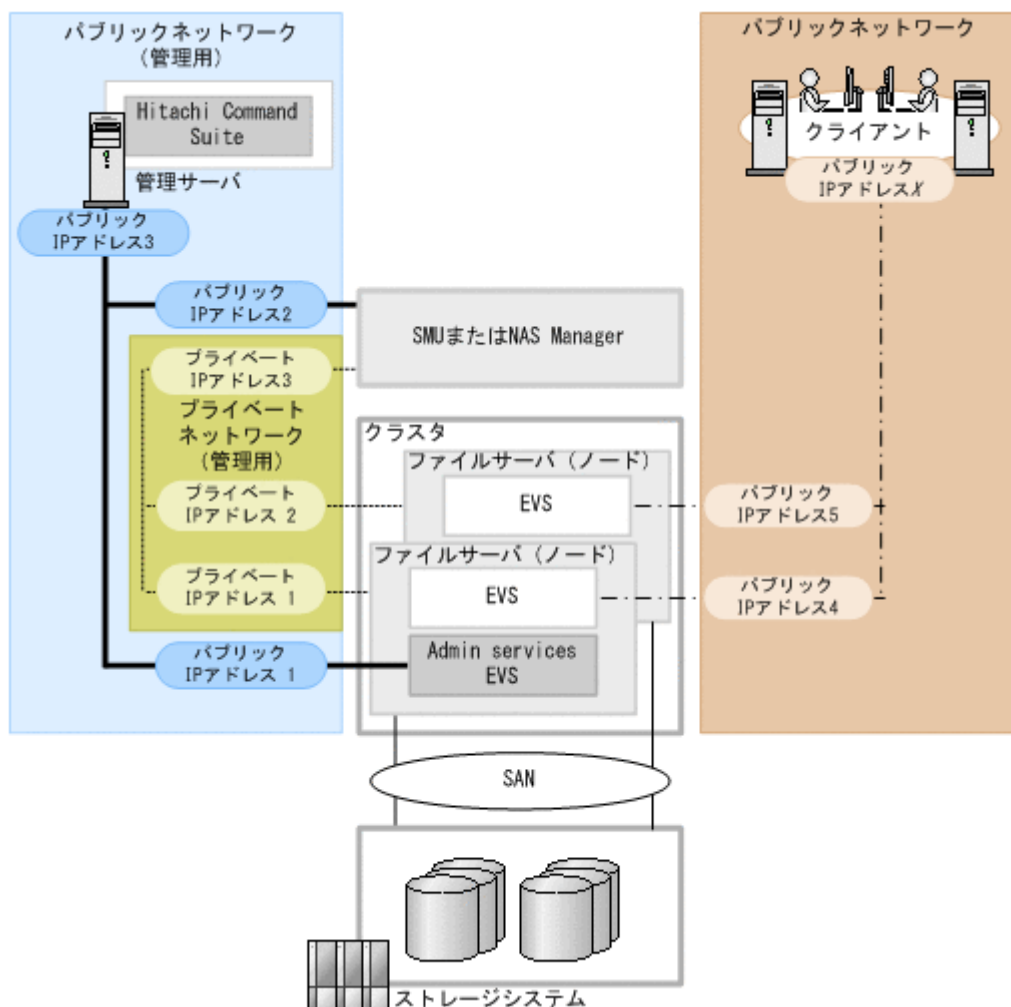
Device Manager では、ストレージシステムのボリュームをファイルサーバに割り当てたり、ファイルサーバの情報を確認したりできます。

1.10.1 NAS Platform の前提環境

Device Manager で NAS Platform を管理するためには、管理サーバが次のプログラムと通信できるシステム構成にする必要があります。

- System Management Unit (SMU) または NAS Manager
- Admin services EVS

図 10 NAS Platform の前提環境



- 管理サーバは、次のプログラムと通信できるネットワーク上に設置してください。
 - SMU または NAS Manager
 - Admin services EVS
- SMU または NAS Manager 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。
- 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 または NAS Manager の [EVS Management] ページで確認できません。
IP アドレスの確認方法については、NAS Platform のマニュアルを参照してください。
 - 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。



メモ

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。

1.10.2 Hitachi Virtual File Platform および Hitachi Capacity Optimization の前提環境

Device Manager で Hitachi Virtual File Platform および Hitachi Capacity Optimization 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 5 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 とは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		Y	Y
ファイルサーバの登録, 管理		Y	Y
ファイルサーバへのボリュームの割り当て		Y	Y
ファイルシステムの作成, 拡張および削除		Y	--
ファイル共有の追加, 編集および解除		Y	--
[ダッシュボード] での情報確認	ファイルシステムの容量情報の確認	Y	Y
	スナップショットの容量情報および階層ファイルシステムの使用状況の確認※	Y	--
ファイルサーバのアラート監視		Y	Y

(凡例)

- Y : 実行できる
- : 実行できない

注※

Hitachi Virtual File Platform の場合だけ確認できます。

Hitachi File Services Manager のインストール方法および環境設定については、ファイルサーバのマニュアルを参照してください。Hitachi File Services Manager の前提バージョンについては、ソフトウェア添付資料を参照してください。

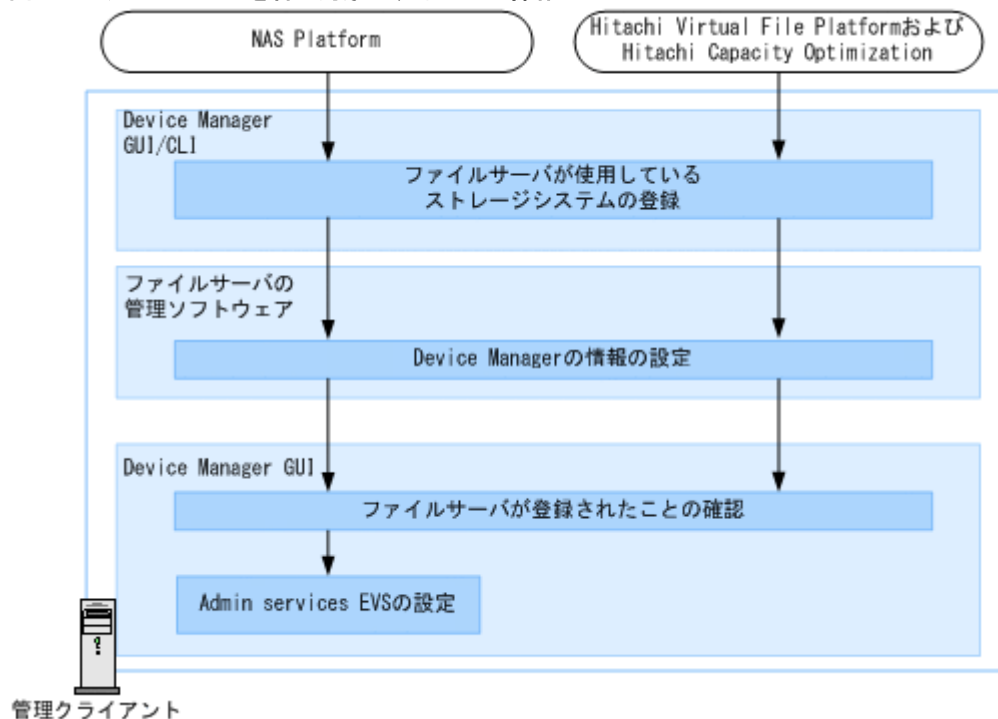
関連概念

- [7.2 アラートの設定](#)

1.10.3 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 11 ファイルサーバを管理対象にするための操作フロー



ファイルサーバで使用できるストレージシステムおよびファイルサーバ管理ソフトウェアでの設定方法については、ファイルサーバのマニュアルを参照してください。

Device Manager GUI/CLI での設定方法については、マニュアル「*Hitachi Command Suite ユーザーズガイド*」またはマニュアル「*Hitachi Command Suite CLI リファレンスガイド*」を参照してください。

1.10.4 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。
- 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 または NAS Manager 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 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。
SMU または NAS Manager での設定方法については、NAS Platform のマニュアルを参照してください。
- Hitachi Virtual File Platform および Hitachi Capacity Optimization 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。

Hitachi File Services Manager での設定方法については、ファイルサーバのマニュアルを参照してください。

関連タスク

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

関連参照

- ・ [付録 A.2.5 server.http.entity.maxLength](#)

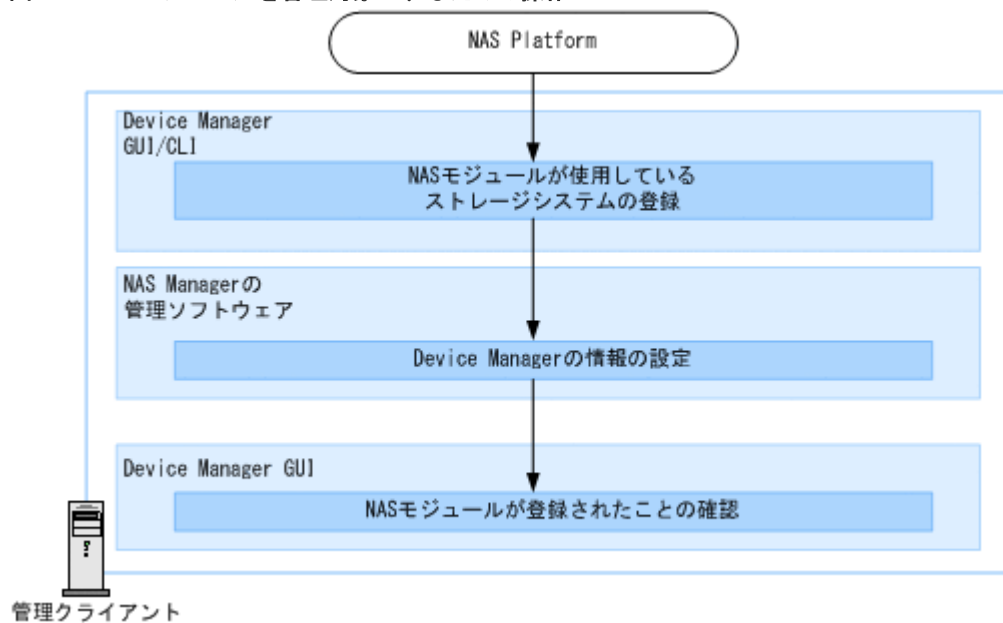
1.11 NAS モジュールのシステム要件

Device Manager では、ストレージシステムのボリュームを NAS モジュールに割り当てたり、NAS モジュールの情報を確認したりできます。

1.11.1 NAS モジュールを管理対象にするための操作フロー

Device Manager で NAS モジュール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、NAS Manager 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 12 NAS モジュールを管理対象にするための操作フロー



Device Manager GUI/CLI での設定方法については、マニュアル「*Hitachi Command Suite ユーザーズガイド*」またはマニュアル「*Hitachi Command Suite CLI リファレンスガイド*」を参照してください。

1.11.2 NAS モジュールの運用に関する注意事項

NAS モジュールの運用に関する注意事項は次のとおりです。

- ・ NAS Platform では、NAS モジュールの情報は毎日 AM 3:00 に Device Manager のデータベースに反映されます。

NAS Manager 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 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。

NAS Manager での設定方法については、NAS Platform のマニュアルを参照してください。

- ストレージシステムとは別に存在する NAS Manager と Device Manager が連携する場合、連携できる NAS Manager は 1 台だけです。

1.12 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 および Hitachi Capacity Optimization 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, 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。

関連概念

- [6.5 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするために必要な設定](#)
- [7.6 JP1/IM でログを参照するために必要な設定](#)

1.13 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。

- [レプリケーション] タブを使用する場合
1つのサイトだけではなく複数のサイトにわたるレプリケーションの構成を管理できます。各サイトは、1台の管理サーバとペア管理サーバ、複数のストレージシステムから構成されます。離れた場所にある別のサイトとの間で TrueCopy や Universal Replicator のペアを構成し、ディザスタリカバリーに備えた運用ができます。
作成済みのレプリケーション構成に対して、[レプリケーション] タブの操作だけでディザスタリカバリーテストを実施することもできます。
[レプリケーション] タブを使用するには、Replication Manager のライセンスが必要です。
以降の説明では、レプリケーション管理機能の前提となるコピーペア管理のシステム構成や要件について説明します。レプリケーション管理機能を利用する場合の複数のサイトと連携した構成や必要な設定については、[レプリケーション] タブでレプリケーション管理機能を利用するために必要な設定について説明している章を参照してください。
- Device Manager GUI から Replication Manager GUI をラUNCHして使用する場合
1つのサイトだけではなく複数のサイトにわたるレプリケーションの構成を管理し、ディザスタリカバリーに備えた運用ができます。
Replication Manager Application Agent を導入することで、Exchange Server や SQL Server でボリュームのレプリケーションも管理できます。
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が、複数のサイトにわたるレプリケーションの管理はできません。
- Device Manager CLI を使用する場合
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が、複数のサイトにわたるレプリケーションの管理はできません。



ヒント

Device Manager では、2台のストレージシステム上で global-active device の機能を利用し、可用性の高いシステムを構築できます。

関連概念

- [1.19 高可用性システムの構築](#)

- [6.4 \[レプリケーション\] タブでレプリケーション管理機能を利用するために必要な設定](#)

関連参照

- [1.14 コピーペアを管理する場合のシステム構成（一括管理構成）](#)
- [1.15 コピーペアを管理する場合のシステム構成（一括管理構成以外）](#)
- [1.16 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](#)
- [1.18 コピーペアを管理する場合の注意事項](#)
- [1.17 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](#)

1.14 コピーペアを管理する場合のシステム構成（一括管理構成）

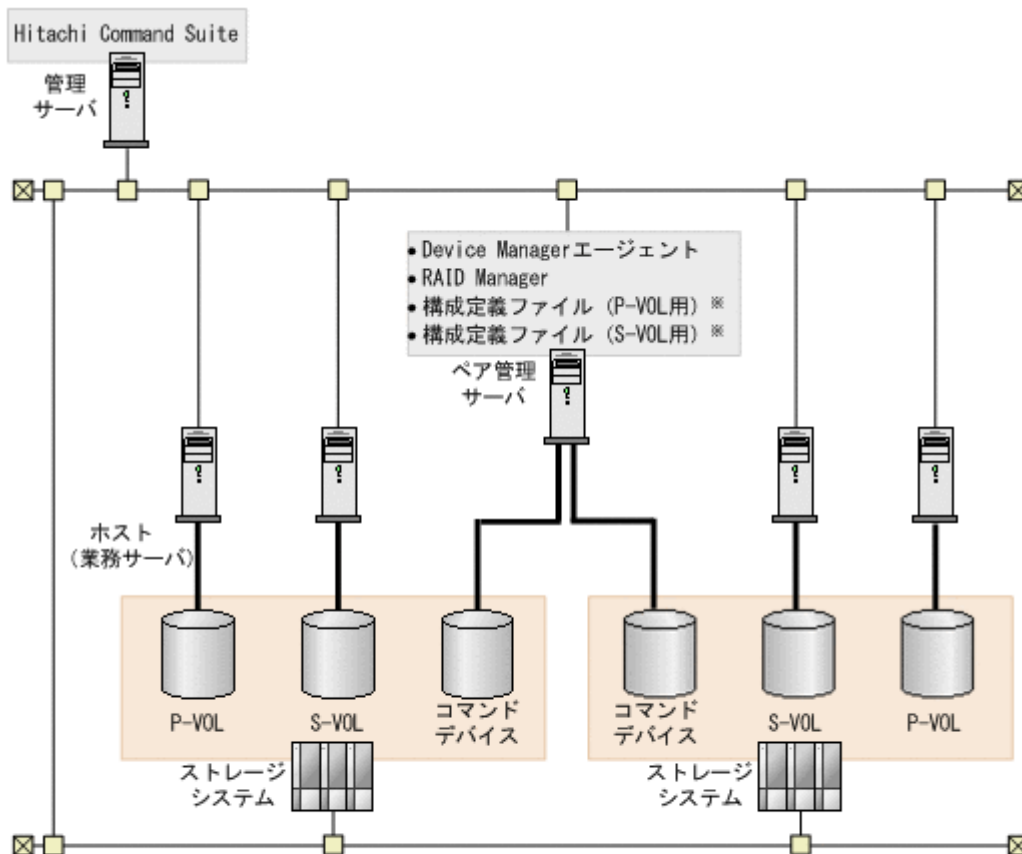
ホスト（業務サーバ）とは別に、1台のマシンにコマンドデバイスをファイバーチャネル接続して、コピーペアを一括管理する構成です。

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。また、ファイルサーバや NAS モジュールに割り当てられたボリュームのコピーペアも管理できます。

[レプリケーション] タブを使用してコピーペアを管理する場合は、システム構成が一括管理構成である必要があります。

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 13 コピーペア管理のシステム構成例（一括管理構成）



(凡例)

— : Fibre Channel

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。
RAID Manager は最新のバージョンを利用することを推奨します。
Device Manager エージェントのバージョンが 8.0 以前で、RAID Manager 01-32-03/XX 以降、または XP7 RAID Manager 01.32.XX 以降 を利用する場合は、Device Manager エージェントを 8.0.1 以降にアップグレードインストールしてください。
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 RAID Manager XP の両方をインストールする必要があります。RAID Manager のインストール手順については、RAID Manager のマニュアルを参照してください。

- 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。
- 仮想ストレージマシンに属するコマンドデバイスと仮想ストレージマシンに属さないコマンドデバイスが、同時にペア管理サーバに接続されていないこと。



ヒント

ホストが P-VOL、S-VOL を認識していること、またはペア管理サーバがコマンドデバイスを認識していることを確認するには、Device Manager エージェントの `h1dutil` コマンドを使用してください。



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は、次の点に注意してください。

- 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。
- 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、ストレージシステムに対してユーザー認証が完了している必要があります。
Device Manager エージェントのバージョンが 8.0.1 以降で、かつ Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用している場合、ユーザー認証は自動的に行われるため、手動でユーザー認証を行う必要はありません。

リソースグループの条件 (VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、VSP Fx00 モデル、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)
- ・リソースグループにコマンドデバイスが登録され、各ユーザーに割り当てられていること。
- ・ペア管理サーバに、ストレージシステムのリソースグループが 0 (VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルの場合は、デフォルトの仮想ストレージマシンのリソースプール) のコマンドデバイスが接続されていて、そのコマンドデバイスの情報が Device Manager エージェントの rgcmddev.properties ファイルに定義されていること。
- ・コマンドデバイスの認証モードが有効であること。
- ・ストレージシステムのリソースグループ ID が 0 (VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルのときは、デフォルトの仮想ストレージマシンのリソースプール) のすべてのコマンドデバイスに対して、ユーザー認証が完了していること。
Device Manager エージェントのバージョンが 8.0.1 以降で、かつ Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用している場合、ユーザー認証は自動的に行われるため、手動でユーザー認証を行う必要はありません。

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルで仮想ストレージマシンを作成してリソース管理している場合の条件

- ・ユーザーの管理対象の仮想ストレージマシンに、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)
- ・コマンドデバイスおよびジャーナルボリュームが、デフォルトの仮想ストレージマシン上に作成されたリソースグループに登録され、ユーザーに割り当てられていること。



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。

関連タスク

- ・ [付録 D.1.1 Device Manager エージェントのプロパティの変更](#)

関連参照

- ・ [1.16 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](#)
- ・ [1.17 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](#)
- ・ [11.3.6 デバイス情報の取得 \(hldutil コマンド\)](#)
- ・ [付録 D.6.15 server.agent.rm.centralizePairConfiguration](#)
- ・ [付録 D.7 Device Manager エージェントが接続するコマンドデバイスに関するプロパティファイル \(rgcmddev.properties ファイル\)](#)

1.15 コピーペアを管理する場合のシステム構成（一括管理構成以外）

一括管理構成以外のシステム構成を次に示します。

- 各ホストでコピーペアを管理する構成
各ホスト（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、ホストごとにコピーペアを管理する構成です。
- 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 VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、VSP Fx00 モデル、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。



メモ

コマンドデバイスの認証モードが有効に設定されている場合、および仮想コマンドデバイスに SVP を使用していて、かつ構成定義ファイルでコピーペアを定義している場合、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、ストレージシステムに対してユーザー認証が完了している必要があります。

次の両方の条件を満たす場合、Device Manager サーバから取得したユーザーアカウントで自動的にユーザー認証が実行されます。

- Device Manager エージェントのバージョンが 8.0.1 以降のとき
 - Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用しているとき
- そのほかの場合、RAID Manager のコマンド (raidcom -login) を実行して、手動でユーザー認証を行ってください。手動でユーザー認証を行う場合は、次の点に注意してください。
- 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。
 - 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。



メモ

- 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。

関連概念

- [5.1.10 管理サーバと Device Manager エージェント間のセキュリティ通信のための操作フロー](#)

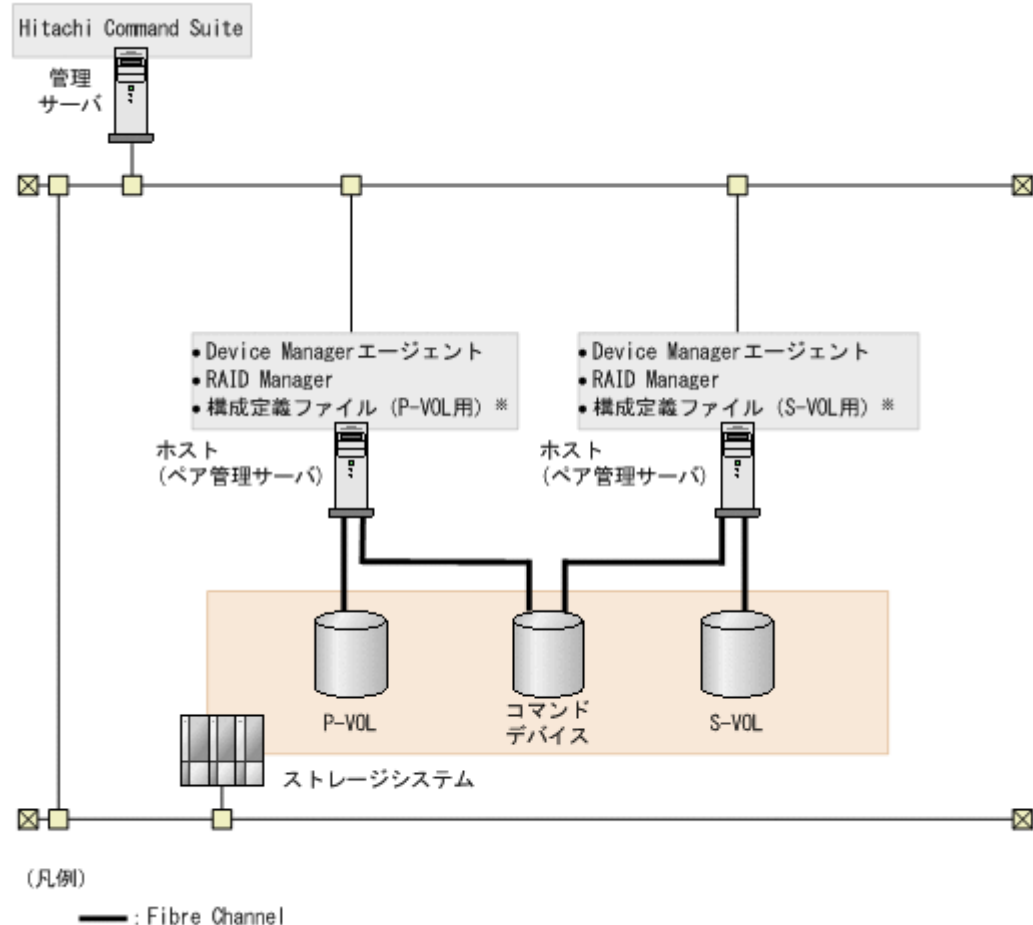
関連参照

- 1.18 コピーペアを管理する場合の注意事項
- 付録 D.6.24 server.agent.rm.userAuthentication

1.15.1 各ホスト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（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 14 コピーペア管理のシステム構成例（各ホストでコピーペアを管理する場合）



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（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。
 - 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。
RAID Manager は最新のバージョンを利用することを推奨します。
Device Manager エージェントのバージョンが 8.0 以前で、RAID Manager 01-32-03/XX 以降、または XP7 RAID Manager 01.32.XX 以降 を利用する場合は、Device Manager エージェントを 8.0.1 以降にアップグレード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 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 RAID Manager XP の両方をインストールする必要があります。
RAID Manager のインストール手順については、RAID Manager のマニュアルを参照してください。
- 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 (ペア管理サーバ) 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 (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。
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。
- 仮想ストレージマシンに属するコマンドデバイスと仮想ストレージマシンに属さないコマンドデバイスが、同時にペア管理サーバに接続されていないこと。



ヒント

ホスト（ペア管理サーバ）が P-VOL、S-VOL およびコマンドデバイスを認識していることを確認するには、**Device Manager** エージェントの `hldutil` コマンドを使用してください。



注意

認証モードが有効なコマンドデバイスがホスト（ペア管理サーバ）に接続されている場合は、次の点に注意してください。

- ・ 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。
- ・ **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、ストレージシステムに対してユーザー認証が完了している必要があります。
Device Manager エージェントのバージョンが 8.0.1 以降で、かつ **Device Manager** サーバと **Device Manager** エージェント間の通信に SSL/TLS を利用している場合、ユーザー認証は自動的に行われるため、手動でユーザー認証を行う必要はありません。

リソースグループの条件（VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、VSP Fx00 モデル、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）
- ・ リソースグループにコマンドデバイスが登録され、各ユーザーに割り当てられていること。
- ・ ホストに、ストレージシステムのリソースグループ ID が 0（VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデルの場合は、デフォルトの仮想ストレージマシンのリソースプール）のコマンドデバイスが接続されていて、そのコマンドデバイスの情報が **Device Manager** エージェントの `rgcmddev.properties` ファイルに定義されていること。
- ・ コマンドデバイスの認証モードが有効であること。
- ・ ストレージシステムのリソースグループ ID が 0（VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデルのときは、デフォルトの仮想ストレージマシンのリソースプール）のすべてのコマンドデバイスに対して、ユーザー認証が完了していること。
Device Manager エージェントのバージョンが 8.0.1 以降で、かつ **Device Manager** サーバと **Device Manager** エージェント間の通信に SSL/TLS を利用している場合、ユーザー認証は自動的に行われるため、手動でユーザー認証を行う必要はありません。

VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデルで仮想ストレージマシンを作成してリソース管理している場合の条件

- ・ ユーザーの管理対象の仮想ストレージマシンに、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）

- ・ コマンドデバイスおよびジャーナルボリュームが、デフォルトの仮想ストレージマシン上に作成されたリソースグループに登録され、ユーザーに割り当てられていること。



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。

関連タスク

- ・ [付録 D.1.1 Device Manager エージェントのプロパティの変更](#)

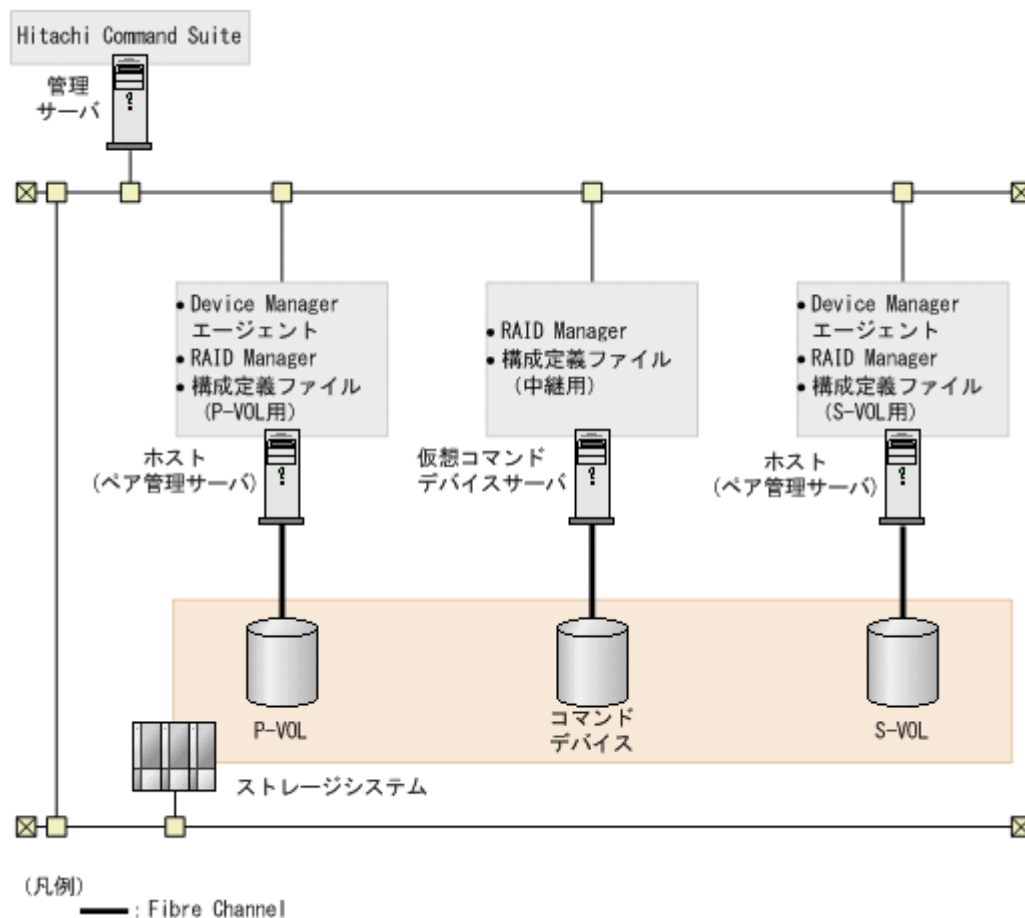
関連参照

- ・ [1.16 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](#)
- ・ [1.17 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](#)
- ・ [11.3.6 デバイス情報の取得 \(hldutil コマンド\)](#)
- ・ [付録 D.7 Device Manager エージェントが接続するコマンドデバイスに関するプロパティファイル \(rgcmddev.properties ファイル\)](#)

1.15.2 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（ペア管理サーバ）、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 15 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 (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。
RAID Manager は最新のバージョンを利用することを推奨します。
Device Manager エージェントのバージョンが 8.0 以前で、**RAID Manager 01-32-03/XX** 以降、または **XP7 RAID Manager 01.32.XX** 以降 を利用する場合は、**Device Manager** エージェントを 8.0.1 以降にアップグレードインストールしてください。
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 **RAID Manager XP** の両方をインストールする必要があります。
RAID Manager のインストール手順については、**RAID Manager** のマニュアルを参照してください。
- ホスト (ペア管理サーバ) 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。
RAID Manager は最新のバージョンを利用することを推奨します。
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 **RAID Manager XP** の両方をインストールする必要があります。
RAID Manager のインストール手順については、**RAID Manager** のマニュアルを参照してください。
- 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、ホスト (ペア管理サーバ) 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。また、コピーペアの状態を監視するため、**Replication Manager** エージェントで使用しているインスタンスからのアクセスを許可する必要があります。次に示す監視用 HORCM ファイルのインスタンス番号も設定してください。
監視用 HORCM ファイルのインスタンス番号は、**RAID Manager** または **XP7 RAID Manager** のバージョンによって異なります。
 - **RAID Manager** のバージョンが 01-32-03/XX 以降、または **XP7 RAID Manager** のバージョンが 01.32.XX 以降の場合
Device Manager エージェントの agent.properties ファイルにある agent.rm.horcmInstance プロパティと agent.rm.horcmRange プロパティの値から算出した次の範囲のインスタンス番号 (デフォルトでは、1948~2047) です。意図的に拒否したいインスタンス番号を設定する必要はありません。
上限値: < agent.rm.horcmInstance プロパティで指定した値 >
下限値: < agent.rm.horcmInstance プロパティで指定した値 > - < agent.rm.horcmRange プロパティで指定した値 > + 1
 - **RAID Manager** のバージョンが 01-32-03/XX より前、または **XP7 RAID Manager** のバージョンが 01.32.XX より前の場合

Device Manager エージェントの `agent.rm.horcInstance` プロパティで指定した値、および `agent.rm.horcInstance` プロパティで指定した値 > -1 のインスタンス番号を設定してください (デフォルトでは、2046 と 2047)。

- ・ 認証モードが有効なコマンドデバイスが仮想コマンドデバイスサーバに接続されている場合は、次の点に注意してください。
 - ・ 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。
 - ・ 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、ストレージシステムに対してユーザー認証が完了している必要があります。
- Device Manager エージェントのバージョンが 8.0.1 以降で、かつ Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用している場合、ユーザー認証は自動的に行われるため、手動でユーザー認証を行う必要はありません。

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 (ペア管理サーバ) に認識されていること。
P-VOL と S-VOL は別のペア管理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 (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。
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。
- ・ 仮想ストレージマシンに属するコマンドデバイスと仮想ストレージマシンに属さないコマンドデバイスが、同時にペア管理サーバに接続されていないこと。



ヒント

ホスト (ペア管理サーバ) が P-VOL、S-VOL を認識していること、または仮想コマンドデバイスサーバがコマンドデバイスを認識していることを確認するには、Device Manager エージェントの `hldutil` コマンドを使用してください。

リソースグループの条件 (VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、VSP Fx00 モデル、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)

- ・ リソースグループにコマンドデバイスが登録され、各ユーザーに割り当てられていること。
- ・ 仮想コマンドデバイスサーバに、ストレージシステムのリソースグループが 0 (VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルの場合は、デフォルトの仮想ストレージマシンのリソースプール) のコマンドデバイスが接続されていて、そのコマンドデバイスの情報が Device Manager エージェントの rgcmddev.properties ファイルに定義されていること。
- ・ コマンドデバイスの認証モードが有効であること。
- ・ ストレージシステムのリソースグループ ID が 0 (VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルのときは、デフォルトの仮想ストレージマシンのリソースプール) のすべてのコマンドデバイスに対して、ユーザー認証が完了していること。

Device Manager エージェントのバージョンが 8.0.1 以降で、かつ Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用している場合、ユーザー認証は自動的に行われるため、手動でユーザー認証を行う必要はありません。

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おくことをお勧めします。

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルで仮想ストレージマシンを作成してリソース管理している場合の条件

- ・ ユーザーの管理対象の仮想ストレージマシンに、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 またはコピーグループに定義された Thin Image ペアを管理する場合)
- ・ コマンドデバイスおよびジャーナルボリュームが、デフォルトの仮想ストレージマシン上に作成されたリソースグループに登録され、ユーザーに割り当てられていること。



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。

関連タスク

- ・ [付録 D.1.1 Device Manager エージェントのプロパティの変更](#)

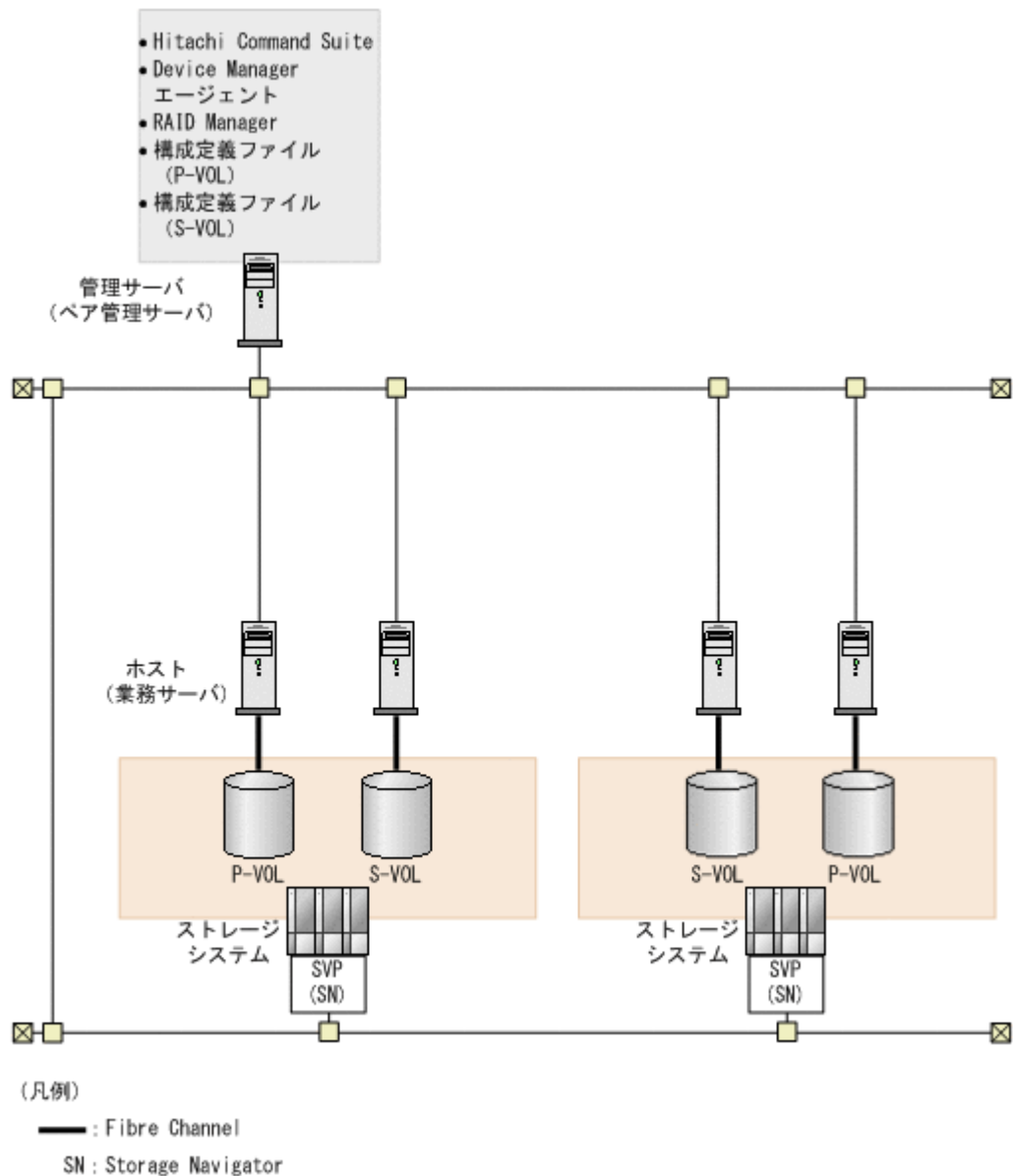
関連参照

- ・ [1.16 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](#)
- ・ [1.17 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](#)
- ・ [11.3.6 デバイス情報の取得 \(hldutil コマンド\)](#)
- ・ [付録 D.2.4 agent.rm.horcmInstance](#)
- ・ [付録 D.2.6 agent.rm.horcmRange](#)
- ・ [付録 D.7 Device Manager エージェントが接続するコマンドデバイスに関するプロパティファイル \(rgcmddev.properties ファイル\)](#)

1.15.3 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 16 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 (ペア管理サーバ) 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。
RAID Manager は最新のバージョンを利用することを推奨します。

Device Manager エージェントのバージョンが 8.0 以前で、RAID Manager 01-32-03/XX 以降、または XP7 RAID Manager 01.32.XX 以降 を利用する場合は、Device Manager エージェントを 8.0.1 以降にアップグレードインストールしてください。

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 RAID Manager XP の両方をインストールする必要があります。

RAID Manager のインストール手順については、RAID Manager のマニュアルを参照してください。

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 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。



ヒント

ホスト (業務サーバ) が P-VOL、S-VOL を認識していることを確認するには、Device Manager エージェントの hldutil コマンドを使用してください。

リソースグループの条件 (VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、VSP Fx00 モデル、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。

VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデルで仮想ストレージマシンを作成してリソース管理している場合の条件

- ユーザーの管理対象の仮想ストレージマシンに、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)
- ジャーナルボリュームが、デフォルトの仮想ストレージマシン上に作成されたリソースグループに登録され、ユーザーに割り当てられていること。



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、ストレージシステムに対してユーザー認証が完了している必要があります。

Device Manager エージェントのバージョンが 8.0.1 以降で、かつ Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用している場合、ユーザー認証は自動的に行われるため、手動でユーザー認証を行う必要はありません。

- 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。
-

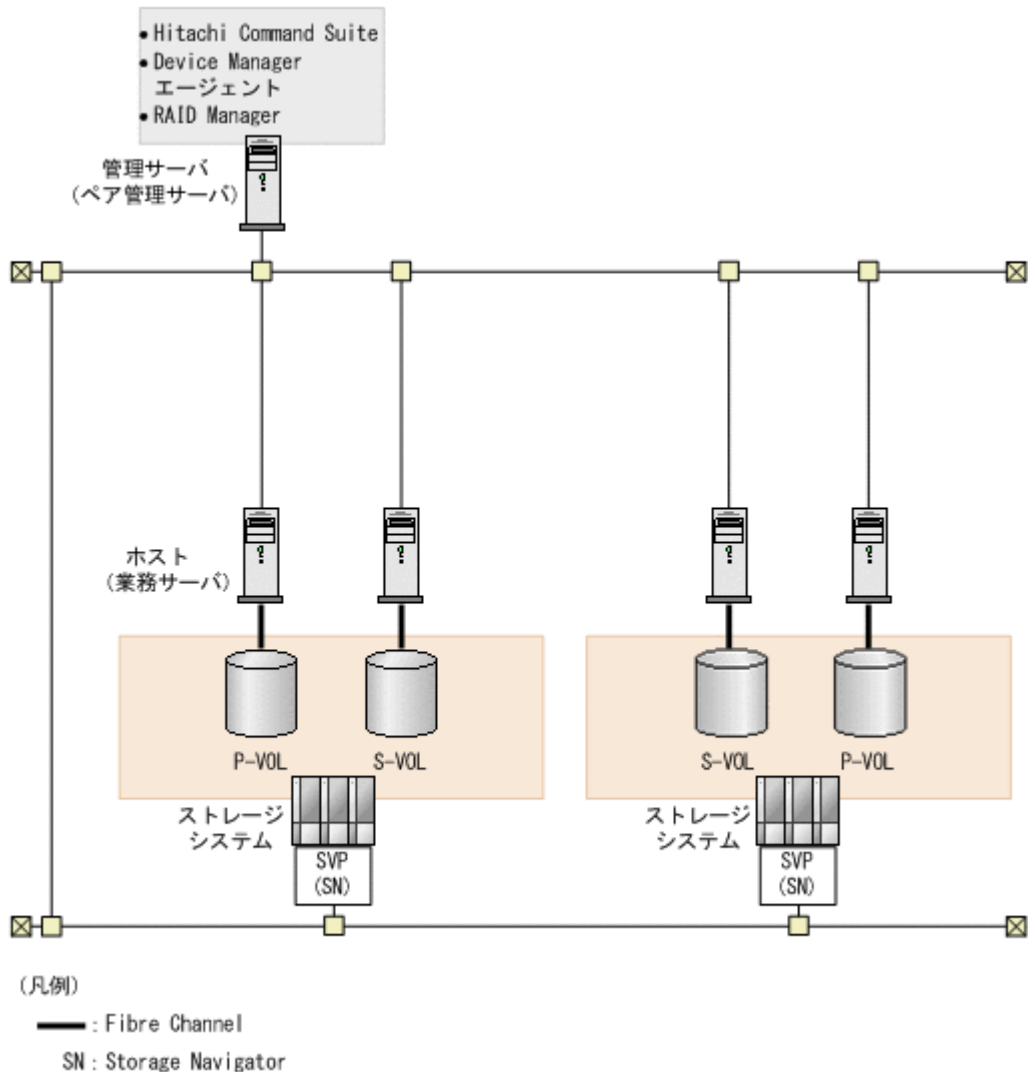
関連参照

- [1.16 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](#)
- [1.17 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](#)
- [11.3.6 デバイス情報の取得 \(hldutil コマンド\)](#)

1.15.4 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 17 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（ペア管理サーバ）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。
RAID Manager は最新のバージョンを利用することを推奨します。
Device Manager エージェントのバージョンが 8.0 以前で、RAID Manager 01-32-03/XX 以降、または XP7 RAID Manager 01.32.XX 以降を利用する場合は、Device Manager エージェントを 8.0.1 以降にアップグレードインストールしてください。
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 RAID Manager XP の両方をインストールする必要があります。

RAID Manager のインストール手順については、RAID Manager のマニュアルを参照してください。

- 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。



ヒント

ホスト（業務サーバ）が P-VOL、S-VOL を認識していることを確認するには、Device Manager エージェントの `hldutil` コマンドを使用してください。

リソースグループの条件（VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、VSP Fx00 モデル、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てをお勧めします。

VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデルで仮想ストレージマシンを作成してリソース管理している場合の条件

- ユーザーの管理対象の仮想ストレージマシンに、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)
- ・ジャーナルボリュームが、デフォルトの仮想ストレージマシン上に作成されたリソースグループに登録され、ユーザーに割り当てられていること。



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。

関連概念

- ・ [5.1.6 Device Manager サーバと Replication Manager サーバ間のセキュリティ通信のための操作フロー](#)

関連タスク

- ・ [付録 D.1.1 Device Manager エージェントのプロパティの変更](#)

関連参照

- ・ [1.16 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](#)
- ・ [1.17 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](#)
- ・ [11.3.6 デバイス情報の取得 \(hldutil コマンド\)](#)
- ・ [付録 D.6.15 server.agent.rm.centralizePairConfiguration](#)
- ・ [付録 D.6.25 server.agent.rm.ignorePairStatus](#)

1.16 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

コピーペアを管理するためには、ストレージシステムの環境構築が必要です。

次の要件に従ってストレージシステムを環境構築してください。詳細については、各ストレージシステムのマニュアルを参照してください。



ヒント

リモートパス、ジャーナルグループ、プールおよび V-VOL については、[レプリケーション] タブを使用して設定できます。詳細は、マニュアル「Hitachi Command Suite ユーザーズガイド」を参照してください。

- ・ リモートパス
Universal Replicator または TrueCopy を利用してコピーペアの操作をする場合、ストレージシステム間でリモートパスを設定しておく必要があります。
- ・ ジャーナルグループ
Universal Replicator を利用してコピーペアの操作をする場合、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。
- ・ プール

Copy-on-Write Snapshot, Thin Image または TrueCopy Extended Distance を利用してコピーペアの操作をする場合、プールを設定しておく必要があります。

HUS100 では DP プール, Hitachi AMS2000 および Hitachi AMS/WMS ではデータプールと呼びます。

- DM-LU

次の場合, DM-LU を設定しておく必要があります。

- HUS100 で, TrueCopy remote replication または ShadowImage を使用する場合
- Hitachi AMS2000 および Hitachi AMS/WMS で, TrueCopy remote replication, TrueCopy Extended Distance, Copy-on-Write Snapshot, または ShadowImage を使用する場合

- V-VOL

Copy-on-Write Snapshot または Thin Image を利用してコピーペアの操作をする場合, S-VOL 用に仮想ボリューム (V-VOL) を作成する必要があります。

次の順序で準備してください。

1. プールの作成
2. V-VOL の作成



注意

- ストレージシステムを環境構築したあと, 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。
- VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, 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。
- エンタープライズクラスストレージの場合, Device Manager CLI でメインフレームボリュームのコピーペア (Universal Replicator, TrueCopy および ShadowImage のコピーペア) の構成を確認できます。
- 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, コマンドデバイスの認証モードを有効にする必要があります。
また, ペア管理サーバで `raidcom -login` コマンドを実行して, ユーザー認証を行う必要があります。
Device Manager エージェントのバージョンが 8.0.1 以降で, かつ Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用している場合, ユーザー認証は自動的に行われるため, 手動でユーザー認証を行う必要はありません。

1.17 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 6 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
VSP 5000 シリーズ	8.7.0 以降
VSP G1000	8.0 以降
VSP G1500	8.5.0 以降
VSP F1500	8.5.0 以降
VSP G100	8.1.4 以降
VSP G200, G400, G600	8.1.2 以降
VSP F400, F600	
VSP G800	8.2.0 以降
VSP F800	
VSP G130	8.5.0-09 以降
VSP G150, G350, G370, G700, G900	8.5.0-08 以降
VSP F350, F370, F700, F900	8.5.0-08 以降
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 7 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 (TrueCopy Sync および Universal Replicator による 3DC デルタリシンク構成)	05-50 以降
	状態表示 (global-active device および Universal Replicator による 3DC デルタリシンク構成)	8.1.4 以降
	状態変更	05-60 以降
	状態変更 (global-active device および Universal Replicator による 3DC デルタリシンク構成)	8.1.4 以降
TrueCopy	状態表示	02-30 以降
	状態表示 (TrueCopy Extended Distance)	05-10 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
	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
global-active device	状態表示 (global-active device ペアが DP ボリュームの場合)	8.0.1 以降
	状態表示 (global-active device ペアが基本ボリュームの場合)	8.1.4 以降
	状態変更 (global-active device ペアが DP ボリュームの場合)	8.0.1 以降
	状態変更 (global-active device ペアが基本ボリュームの場合)	8.1.4 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 8 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
VSP 5000 シリーズ	8.7.0 以降
VSP G1000	8.0 以降
VSP G1500	8.5.0 以降
VSP F1500	8.5.0 以降
VSP G100	8.1.4 以降
VSP G200, G400, G600	8.1.2 以降
VSP F400, F600	
VSP G800	8.2.0 以降
VSP F800	

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
VSP G130	8.5.0-09 以降
VSP G150, G350, G370, G700, G900	8.5.0-08 以降
VSP F350, F370, F700, F900	8.5.0-08 以降
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
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)	
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	
Hitachi Workgroup Modular Storage 100	04-10 以降

関連参照

- [1.14 コピーペアを管理する場合のシステム構成（一括管理構成）](#)
- [1.15.1 各ホストでコピーペアを管理する場合のシステム構成](#)
- [1.15.2 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](#)
- [1.15.3 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）](#)
- [1.15.4 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）](#)

1.18 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。

仮想マシンをペア管理サーバとして使用する場合

- Device Manager では、仮想マシンをペア管理サーバとして使用する場合、仮想マシンのシステム要件を満たす必要があります。ただし、[レプリケーション] タブでは、仮想 HBA を割り当てていない仮想マシンであっても、同仮想マシンをペア管理サーバとして使用できます。この場合、同仮想マシンと、同仮想マシンが属する仮想化サーバの両方を Device Manager に登録してください。
なお、[レプリケーション] タブを使用するには、Replication Manager のライセンスが必要です。

RAID Manager 01-32-03/XX 以降、または XP7 RAID Manager 01.32.XX 以降を使用する場合

- RAID Manager 01-32-03/XX 以降、または XP7 RAID Manager 01.32.XX 以降では、1つの構成定義ファイルに仮想 ID と物理 ID の両方のペア定義を混在して指定できません。仮想 ID のペア定義は仮想 ID 用の構成定義ファイルに、物理 ID のペア定義は物理 ID 用の構成定義ファイルに別々に定義する必要があります。
仮想 ID 用の構成定義ファイルと物理 ID 用の構成定義ファイルは、次の規則に従って作成してください。
 - 物理 ID 用の構成定義ファイルに、HORCM_VCMD パラメーターは定義できません。
 - 仮想 ID 用の構成定義ファイルに、HORCM_VCMD パラメーターを定義します。
 - 仮想 ID 用の構成定義ファイルに、HORCM_DEV パラメーターは定義できません。
 - 仮想ストレージマシンをサポートしていないストレージシステムのペアは、物理 ID 用の構成定義ファイルに定義します。
 - 仮想 ID 用の構成定義ファイルに、複数のストレージシステムのコマンドデバイスを定義することはできません。仮想 ID 用の構成定義ファイルは、ストレージシステムごとに作成してください。

RAID Manager 01-32-03/XX より前、または XP7 RAID Manager 01.32.XX より前からアップグレードインストールした場合、上記の規則に従っていないときは、既存の構成定義ファイルを手動で作成し直す必要があります。

- 仮想 ID を使用してコピーペアを管理する場合、Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用していないときは、ストレージシステムと仮想ストレージマシンの両方に対してユーザー認証が必要です。
ユーザー認証を実施していないと、次の操作では仮想 ID を使用したコピーペアの状態は更新されません。
 - HiScan コマンドを実行したとき（手動実行および自動実行）
 - Device Manager GUI/CLI でホスト情報を更新したとき

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルで、仮想 ID を使用することで異なるストレージシステム間でシリアル番号が重複する構成になる場合

- RAID Manager 01-32-03/XX より前、または XP7 RAID Manager 01.32.XX より前を使用している場合、それぞれのストレージシステムのコマンドデバイスは、別々のペア管理サーバに接続してください。
- RAID Manager 01-32-03/XX 以降、または XP7 RAID Manager 01.32.XX 以降を使用している場合、次のどちらかの条件に当てはまる構成定義ファイルは、別々のペア管理サーバで管理してください。
 - 仮想 ID 用の構成定義ファイルで、HORCM_VCMD に定義しているシリアル番号が、物理 ID 用の構成定義ファイルに定義されているストレージシステムのシリアル番号と一致するとき
 - 仮想 ID 用の構成定義ファイルが複数あり、HORCM_VCMD に定義されているシリアル番号が一致するとき

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルで、仮想ストレージマシンを用いてデータ移行をした場合

- global-active device の機能を利用する場合を除き、仮想ボリュームを物理 ID で運用したいときは、コピーペアの管理方法は一括管理構成にしてください。
- 構成定義ファイルを移行後の環境に合わせて再作成してください。
 - RAID Manager のバージョンが 01-32-03/XX より前、または XP7 RAID Manager のバージョンが 01.32.XX より前の場合、HORCM_LDEV パラメーターの Serial#, devNum, portName には、仮想 ID または物理 ID を指定できます。
 - RAID Manager のバージョンが 01-32-03/XX 以降、または XP7 RAID Manager のバージョンが 01.32.XX 以降の場合は、仮想 ID のペア定義は仮想 ID 用の構成定義ファイルに、物理 ID のペア定義は物理 ID 用の構成定義ファイルに別々に定義する必要があります。
 - HORCM_CMD パラメーターには、ストレージシステムリソースグループ ID が 0 (デフォルトの仮想ストレージマシンのリソースプール) のコマンドデバイスを指定します。
- VSP G1000 のマイクロコードのバージョンが 80-02-01-XX/XX より前の場合、コマンドデバイスの認証モードを有効にしてください。

次の場合、コマンドデバイスの認証モードが無効でも、仮想ストレージマシンのボリュームを使用してコピーペアを操作できます。

 - VSP 5000 シリーズ
 - VSP G1000 のマイクロコードのバージョンが 80-02-01-XX/XX 以降
 - VSP G1500
 - VSP F1500
 - VSP Gx00 モデル
 - VSP Fx00 モデル

ただし、VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルに認証モードが有効なコマンドデバイスと認証モードが無効なコマンドデバイスが存在し、かつ同一ペア管理サーバに接続されている場合は、同一ペア管理サーバで認識するすべてのコマンドデバイスの認証モードを有効にする必要があります。
次の場合、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 ペアを管理する場合
- global-active device ペアを管理する場合
- 仮想ストレージマシン以外でリソースグループ内のペアを管理する場合
- 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、ユーザー認証が完了している必要があります。
Device Manager エージェントのバージョンが 8.0.1 以降で、かつ Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用している場合、ユーザー認証は自動的に行われるため、手動でユーザー認証を行う必要はありません。

Virtual Storage Platform または HUS VM で、仮想 ID を用いてデータ移行をした場合

- コピーペアの管理方法は、一括管理構成にしてください。
- 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てください。
- 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、ユーザー認証が完了している必要があります。
Device Manager エージェントのバージョンが 8.0.1 以降で、かつ Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用している場合、ユーザー認証は自動的に行われるため、手動でユーザー認証を行う必要はありません。

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

- 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。

Device Manager サーバの server.properties ファイルにある server.horcmconfigfile.hostname プロパティの値を変更した場合

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。

1. 自ホストの構成定義ファイルを修正する。
2. 自ホスト上の Device Manager エージェントを再起動する。
3. 相手ホストの構成定義ファイルを修正する。
4. 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 で制御する場合

コピーペアの P-VOL を認識しているペア管理サーバ上の構成定義ファイルと S-VOL を認識しているペア管理サーバ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ペア管理サーバで管理する場合、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。

- Device Manager エージェントのバージョンが 05-60 以前の場合：
 - 同一ペア管理サーバ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
- Device Manager エージェントのバージョンが 05-70 以降の場合：
 - 同一ペア管理サーバ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

Device Manager CLI で作成した構成定義ファイルを RAID Manager で使用する場合

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す。

- 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、ペア管理サーバ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、ペア管理サーバで削除してください。

関連概念

- [11.2.4 コピーペアを管理するために必要な設定](#)
- [11.4 構成定義ファイルの利用](#)

関連参照

- [1.7 仮想マシンのシステム要件](#)

- 1.13 Device Manager でのコピーペア管理
- 付録 A.2.7 server.horcconfigfile.hostname

1.19 高可用性システムの構築

Device Manager では、2 台のストレージシステム上で global-active device の機能を利用し、両方のストレージシステムで I/O を受け付けられるようにすることで、可用性の高いシステムを構築できます。

global-active device の機能は VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデルで利用できます。

正側のストレージシステムと副側のストレージシステムの組み合わせによる混在の可否を、次の表に示します。

表 9 正側および副側のストレージシステムの組み合わせによる混在の可否

正側のストレージシステム	副側のストレージシステム						
	VSP 5000 シリーズ	VSP G1000 (マイクロコードのバージョン: 80-04-2X-XX/XX 以降), VSP G1500, VSP F1500	VSP G1000 (マイクロコードのバージョン: 80-04-2X-XX/XX より前)	VSP G100, VSP G200, VSP G400, VSP G600, VSP G800 (マイクロコードのバージョン: 83-01-2X-XX/XX 以降)	VSP F400, VSP F600, VSP F800 (マイクロコードのバージョン: 83-04-0X-XX/XX 以降)	VSP G150, VSP G350, VSP G370, VSP G700, VSP G900, VSP F350, VSP F370, VSP F700, VSP F900	VSP E990
VSP 5000 シリーズ	Y	--	--	--	--	--	--
VSP G1000 (マイクロコードのバージョン: 80-04-2X-XX/XX 以降), VSP G1500, VSP F1500	--	Y	Y	--	--	--	--
VSP G1000 (マイクロコードのバージョン: 80-04-2X-XX/XX より前)	--	Y	Y	--	--	--	--
VSP G100, VSP G200, VSP G400, VSP	--	--	--	Y	Y	--	--

正側のストレージシステム	副側のストレージシステム						
	VSP 5000 シリーズ	VSP G1000 (マイクロコードのバージョン: 80-04-2X-XX/XX 以降), VSP G1500, VSP F1500	VSP G1000 (マイクロコードのバージョン: 80-04-2X-XX/XX より前)	VSP G100, VSP G200, VSP G400, VSP G600, VSP G800 (マイクロコードのバージョン: 83-01-2X-XX/XX 以降)	VSP F400, VSP F600, VSP F800 (マイクロコードのバージョン: 83-04-0X-XX/XX 以降)	VSP G150, VSP G350, VSP G370, VSP G700, VSP G900, VSP F350, VSP F370, VSP F700, VSP F900	VSP E990
G600, VSP G800 (マイクロコードのバージョン: 83-01-2X-XX/XX 以降)							
VSP F400, VSP F600, VSP F800 (マイクロコードのバージョン: 83-04-0X-XX/XX 以降)	--	--	--	Y	Y	--	--
VSP G150, VSP G350, VSP G370, VSP G700, VSP G900, VSP F350, VSP F370, VSP F700, VSP F900	--	--	--	--	--	Y	--
VSP E990	--	--	--	--	--	--	Y

(凡例)

Y: 混在できる

--: 混在できない



ヒント

[レプリケーション] タブを使用すると、1つのサイトだけではなく複数のサイトにわたる高可用性システムの構成も管理できます。

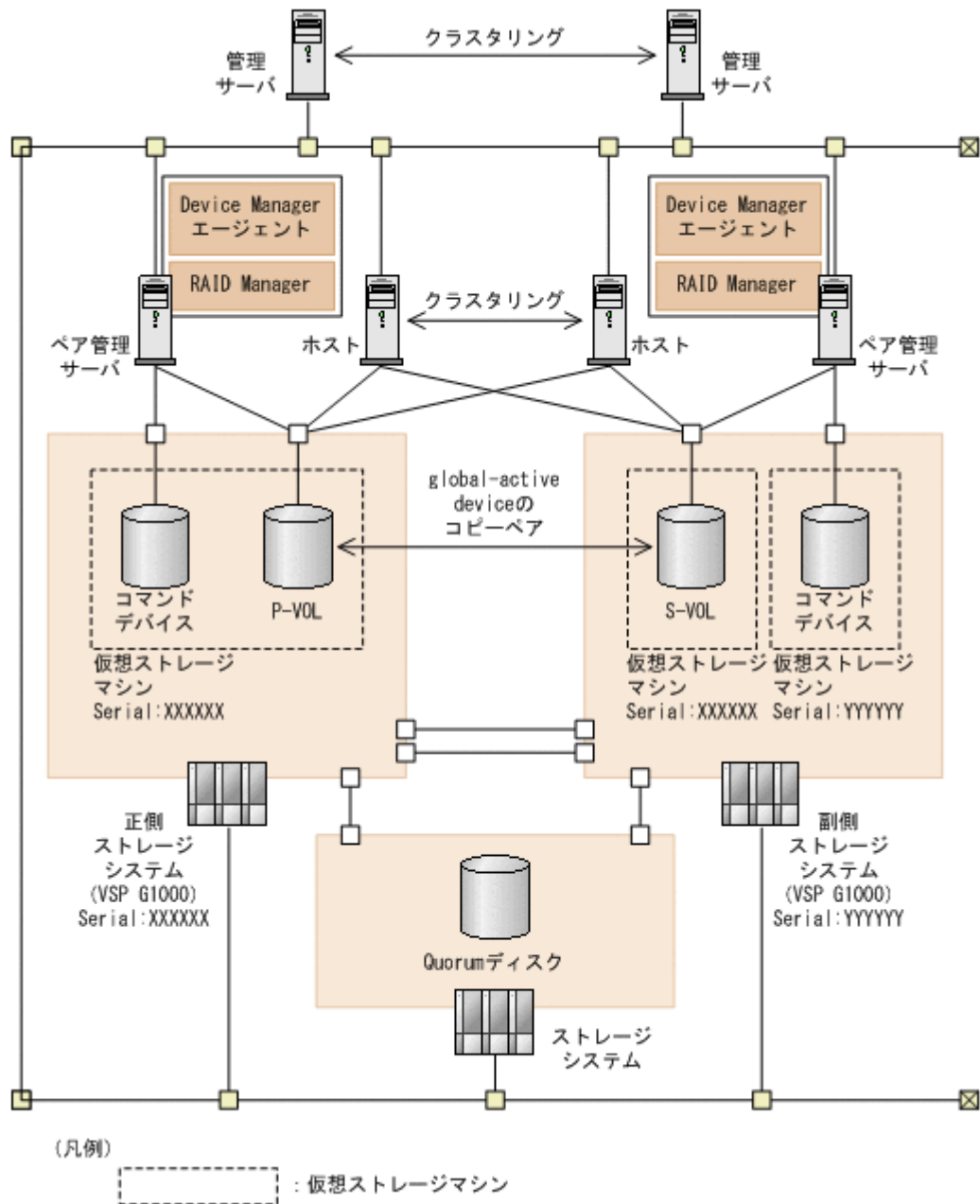
関連概念

- [6.4 \[レプリケーション\] タブでレプリケーション管理機能を利用するために必要な設定](#)

1.19.1 高可用性システムを構築するための構成例

高可用性システムを構築するためのシステム構成の例を次の図に示します。

図 18 高可用性システムの構成例



この図では、ホストをクラスタ構成にするとともに、2 台の VSP G1000 を global-active device の機能を利用して二重化することで、業務システムの可用性を高めています。global-active device のコピーペアのうち、どちらのボリュームが最新の情報を保持しているかを記録する Quorum ディスクを別のストレージシステムで提供することで、ストレージシステムの障害発生時にも業務を継続できます。さらに、Hitachi Command Suite の管理サーバをクラスタ構成にすることで、管理サーバに障害が発生してもストレージシステムの管理を継続できます。

1.19.2 高可用性システムを構築するための要件（VSP 5000 シリーズの場合）

次の要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などを構築してください。

管理サーバの要件

- Replication Manager のライセンスが登録されていること。
- 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 および S-VOL を認識しているホスト
 - 正側のペア管理サーバ
 - 副側のペア管理サーバ
 - 正側のストレージシステム
 - 副側のストレージシステム
 - Quorum ディスク用の外部ストレージシステム（Device Manager CLI を使用して高可用性システムを構築する場合）

ホスト（業務サーバ）の要件

- パス管理ソフトウェアがインストールされていること。



メモ

ホストの OS が HP-UX 11i v3 でネイティブマルチパス機能を使用している場合は、事前に次のコマンドを実行してレガシー DSF に対するマルチパス機能を無効にしてください。

```
scsimgr save_attr -a leg_mpath_enable=false
```

ストレージシステムの要件（正側、副側共通）

- global-active device の前提ソフトウェアをインストールし、ライセンスが有効であること。
- 正側のストレージシステムと副側のストレージシステム間が 2 本以上のファイバーチャネルまたは iSCSI で接続されていて、正側のストレージシステムと副側のストレージシステム間で双方向のリモートパスが設定されていること。
- 正側のストレージシステムと副側のストレージシステムの両方に、Quorum ディスク用の外部ボリュームがあり、同一の Quorum ディスク ID が設定されていること。
- ストレージシステムのキャッシュと共用メモリーが十分にあること。

前提ソフトウェア、キャッシュおよび共用メモリーについては、global-active device のマニュアルを参照してください。

Quorum ディスク用の外部ストレージシステムの要件

- 正側のストレージシステムと Quorum ディスク用の外部ストレージシステム間、副側のストレージシステムと Quorum ディスク用の外部ストレージシステム間がそれぞれファイバーチャネル接続または iSCSI 接続されていること。
- 正側のストレージシステム、副側のストレージシステムの External ポートと Quorum ディスク用の外部ストレージシステムのポート間で外部パスが設定されていること。

ペア管理サーバの要件（正側，副側共通）

- バージョン 8.7.0 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 01-50-03/XX 以降の RAID Manager がインストールされていること。
RAID Manager のインストール手順については、RAID Manager のマニュアルを参照してください。
- 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。

ペアボリュームの要件

- 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 および S-VOL の両方がオープンボリュームであること。
- P-VOL および S-VOL の両方が DP ボリューム，または基本ボリューム（内部ボリュームまたは外部ボリューム）であること。
- P-VOL および S-VOL のボリュームの種別（DP ボリューム，内部ボリュームまたは外部ボリューム）が同じであること。
- P-VOL が所属する仮想ストレージマシンのモデル名とシリアル番号が，S-VOL が所属する仮想ストレージマシンのモデル名とシリアル番号と同じであること。

コマンドデバイスの要件

- コマンドデバイスセキュリティが設定されていないこと。
- デフォルトの仮想ストレージマシンに所属していること。
- ストレージシステム内のリソースを分割管理している場合，ホスト（ペア管理サーバ）に，ストレージシステムのリソースグループ ID が 0（デフォルトの仮想ストレージマシンのリソースプール）のコマンドデバイスが接続されていて，そのコマンドデバイスの情報が Device Manager エージェントの `rgcmddev.properties` ファイルに定義されていること。
- コマンドデバイスの認証モードが有効であること。
- Device Manager の GUI または CLI から `global-active device` ペアに対する操作を実行する前には，ストレージシステムに対してユーザー認証が完了していること。



ヒント

ホストおよびペア管理サーバが，P-VOL，S-VOL，またはコマンドデバイスを認識していることを確認するには，Device Manager エージェントの `hldutil` コマンドを使用してください。



メモ

ストレージシステムに対してユーザー認証を行う方法を次に示します。

自動でユーザー認証を行う

Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用しているとき，Device Manager サーバから取得したユーザーアカウントで自動的にユーザー認証が実行されます。

手動でユーザー認証を行う

RAID Manager のコマンド (`raidcom -login`) を実行して，ユーザー認証を行ってください。

手動でユーザー認証を行う場合は，次の点に注意してください。

- 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。
- 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。



ヒント

デフォルトの仮想ストレージマシンとは、次の両方の条件を満たす仮想ストレージマシンのことです。

- ・ 仮想ストレージマシンのモデル名が、所属するストレージシステムのモデル名と同じである。
- ・ 仮想ストレージマシンのシリアル番号が、所属するストレージシステムのシリアル番号と同じである。



注意

次の要件も確認してください。

- ・ nondisruptive migration 機能を利用してデータ移行をしたボリュームで global-active device のコピーペアを作成する場合、nondisruptive migration 機能でのデータ移行が完了していること。
データ移行が完了していることを確認してから、コピーペアを作成してください。

リモートパスの設定、ペア管理サーバの設定、Quorum ディスクの設定および仮想ストレージマシンについては、マニュアル「*Hitachi Command Suite ユーザーズガイド*」または「*Hitachi Command Suite CLI リファレンスガイド*」を参照してください。

関連概念

- ・ [5.1.10 管理サーバと Device Manager エージェント間のセキュリティ通信のための操作フロー](#)

関連参照

- ・ [11.3.6 デバイス情報の取得 \(hldutil コマンド\)](#)
- ・ [付録 D.7 Device Manager エージェントが接続するコマンドデバイスに関するプロパティファイル \(rgcmddev.properties ファイル\)](#)

1.19.3 高可用性システムを構築するための要件（VSP G1000, G1500 または VSP F1500 の場合）

次の要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などを構築してください。

管理サーバの要件

- ・ Replication Manager のライセンスが登録されていること。
- ・ 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 および S-VOL を認識しているホスト
 - 正側のペア管理サーバ
 - 副側のペア管理サーバ
 - 正側のストレージシステム
 - 副側のストレージシステム
 - Quorum ディスク用の外部ストレージシステム (Device Manager CLI を使用して高可用性システムを構築する場合)

ホスト（業務サーバ）の要件

- ・ パス管理ソフトウェアがインストールされていること。



メモ

- ホストの OS が HP-UX 11i v3 でネイティブマルチパス機能を使用している場合は、事前に次のコマンドを実行してレガシー DSF に対するマルチパス機能を無効にしてください。
`scsimgr save_attr -a leg_mpath_enable=false`
- ホストの OS が Windows または AIX で MPIO 機能を使用している場合、VSP G1000（マイクロコードのバージョンが 80-04-0X-XX/XX 以降）、VSP G1500 または VSP F1500 のときは、ホストグループのホストモードオプションに 102 を設定してください。

ストレージシステムの要件（正側、副側共通）

- global-active device の前提ソフトウェアをインストールし、ライセンスが有効であること。
- 正側のストレージシステムと副側のストレージシステム間が 2 本以上のファイバーチャネルまたは iSCSI で接続されていて、正側のストレージシステムと副側のストレージシステム間で双方向のリモートパスが設定されていること。
- 正側のストレージシステムと副側のストレージシステムの両方に、Quorum ディスク用の外部ボリュームがあり、同一の Quorum ディスク ID が設定されていること。
- ストレージシステムのキャッシュと共用メモリーが十分にあること。

前提ソフトウェア、キャッシュおよび共用メモリーについては、global-active device のマニュアルを参照してください。

Quorum ディスク用の外部ストレージシステムの要件

- 正側のストレージシステムと Quorum ディスク用の外部ストレージシステム間、副側のストレージシステムと Quorum ディスク用の外部ストレージシステム間がそれぞれファイバーチャネル接続または iSCSI 接続されていること。
- 正側のストレージシステム、副側のストレージシステムの External ポートと Quorum ディスク用の外部ストレージシステムのポート間で外部パスが設定されていること。

ペア管理サーバの要件（正側、副側共通）

- VSP G1000 の場合、バージョン 8.0.1 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。VSP G1500 または VSP F1500 の場合、バージョン 8.5.0 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 01-32-03/XX 以降の RAID Manager、またはバージョン 01.32.XX 以降の XP7 RAID Manager がインストールされていること。
RAID Manager のインストール手順については、RAID Manager のマニュアルを参照してください。
- 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。

ペアボリュームの要件

- 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 および S-VOL の両方がオープンボリュームであること。
- P-VOL および S-VOL の両方が DP ボリューム、または基本ボリューム（内部ボリュームまたは外部ボリューム）であること。
- P-VOL および S-VOL のボリュームの種別（DP ボリューム、内部ボリュームまたは外部ボリューム）が同じであること。

- ・ P-VOL が所属する仮想ストレージマシンのモデル名とシリアル番号が、S-VOL が所属する仮想ストレージマシンのモデル名とシリアル番号と同じであること。

コマンドデバイスの要件

- ・ コマンドデバイスセキュリティが設定されていないこと。
- ・ デフォルトの仮想ストレージマシンに所属していること。
- ・ ストレージシステム内のリソースを分割管理している場合、ホスト（ペア管理サーバ）に、ストレージシステムのリソースグループ ID が 0（デフォルトの仮想ストレージマシンのリソースプール）のコマンドデバイスが接続されていて、そのコマンドデバイスの情報が Device Manager エージェントの rgcmddev.properties ファイルに定義されていること。
- ・ コマンドデバイスの認証モードが有効であること。
- ・ Device Manager の GUI または CLI から global-active device ペアに対する操作を実行する前には、ストレージシステムに対してユーザー認証が完了していること。



ヒント

ホストおよびペア管理サーバが、P-VOL、S-VOL、またはコマンドデバイスを認識していることを確認するには、Device Manager エージェントの hldutil コマンドを使用してください。



メモ

ストレージシステムに対してユーザー認証を行う方法を次に示します。

自動でユーザー認証を行う

Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用しているとき、Device Manager サーバから取得したユーザーアカウントで自動的にユーザー認証が実行されます。

手動でユーザー認証を行う

RAID Manager のコマンド (raidcom -login) を実行して、ユーザー認証を行ってください。

手動でユーザー認証を行う場合は、次の点に注意してください。

- ・ 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。
- ・ 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。



ヒント

デフォルトの仮想ストレージマシンとは、次の両方の条件を満たす仮想ストレージマシンのことです。

- ・ 仮想ストレージマシンのモデル名が、所属するストレージシステムのモデル名と同じである。
- ・ 仮想ストレージマシンのシリアル番号が、所属するストレージシステムのシリアル番号と同じである。



注意

VSP G1000 の場合、次の要件も確認してください。

- ・ 基本ボリューム（内部ボリュームまたは外部ボリューム）を使用して global-active device のコピーペアを作成する場合は、次の要件も満たす必要があります。
 - ・ 正側と副側の両方のストレージシステム（VSP G1000）のマイクロコードのバージョンが 80-02-4X-XX/XX 以降であること。
 - ・ Device Manager エージェントのバージョンが 8.1.4 以降であること。
- ・ global-active device、Universal Replicator のコピーペアおよび Universal Replicator のデルタリシンクペアを使用した構成（3DC デルタリシンク構成）の場合は、次の要件も満たす必要があります。
 - ・ 正側と副側の両方のストレージシステム（VSP G1000）のマイクロコードのバージョンが 80-02-4X-XX/XX 以降であること。
 - ・ Device Manager エージェントのバージョンが 8.1.4 以降であること。

- ・RAID Manager のバージョンが 01-32-03/09 以降, または XP7 RAID Manager のバージョンが 01.32.09 以降であること。
 - ・コンシステンシーグループ ID を使用して global-active device ペアを操作する場合は, 次の要件も満たす必要があります。
 - ・正側と副側の両方のストレージシステム (VSP G1000) のマイクロコードのバージョンが 80-02-2X-XX/XX 以降であること。
 - ・Device Manager エージェントのバージョンが 8.1.2 以降であること。
 - ・RAID Manager のバージョンが 01-32-03/07 以降, または XP7 RAID Manager のバージョンが 01.32.07 以降であること。
 - ・nondisruptive migration 機能を利用してデータ移行をしたボリュームで global-active device のコピーペアを作成する場合は, 次の要件も満たす必要があります。
 - ・正側と副側の両方のストレージシステム (VSP G1000) のマイクロコードのバージョンが 80-02-01-XX/XX 以降であること。
 - ・Device Manager エージェントのバージョンが 8.1 以降であること。
 - ・nondisruptive migration 機能でのデータ移行が完了していること。
- データ移行が完了していることを確認してから, コピーペアを作成してください。



注意

VSP G1500 または VSP F1500 の場合, 次の要件も確認してください。

- ・global-active device, Universal Replicator のコピーペアおよび Universal Replicator のデルタリシンクペアを使用した構成 (3DC デルタリシンク構成) の場合, RAID Manager のバージョンが 01-32-03/09 以降, または XP7 RAID Manager のバージョンが 01.32.09 以降であること。
 - ・コンシステンシーグループ ID を使用して global-active device ペアを操作する場合は, RAID Manager のバージョンが 01-32-03/07 以降, または XP7 RAID Manager のバージョンが 01.32.07 以降であること。
 - ・nondisruptive migration 機能を利用してデータ移行をしたボリュームで global-active device のコピーペアを作成する場合は, nondisruptive migration 機能でのデータ移行が完了していること。
- データ移行が完了していることを確認してから, コピーペアを作成してください。

リモートパスの設定, ペア管理サーバの設定, Quorum ディスクの設定および仮想ストレージマシンについては, マニュアル「*Hitachi Command Suite ユーザーズガイド*」または「*Hitachi Command Suite CLI リファレンスガイド*」を参照してください。

関連概念

- ・ [5.1.10 管理サーバと Device Manager エージェント間のセキュリティ通信のための操作フロー](#)

関連参照

- ・ [11.3.6 デバイス情報の取得 \(hldutil コマンド\)](#)
- ・ [付録 D.7 Device Manager エージェントが接続するコマンドデバイスに関するプロパティファイル \(rgcmddev.properties ファイル\)](#)

1.19.4 高可用性システムを構築するための要件 (VSP G100, G200, G400, G600, G800 および VSP F400, F600, F800 の場合)

次の要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などを構築してください。

管理サーバの要件

- ・ Replication Manager のライセンスが登録されていること。
- ・ 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 および S-VOL を認識しているホスト

- 正側のペア管理サーバ
- 副側のペア管理サーバ
- 正側のストレージシステム
- 副側のストレージシステム
- Quorum ディスク用の外部ストレージシステム (Device Manager CLI を使用して高可用性システムを構築する場合)

ホスト (業務サーバ) の要件

- パス管理ソフトウェアがインストールされていること。



メモ

- ホストの OS が HP-UX 11i v3 でネイティブマルチパス機能を使用している場合は、事前に次のコマンドを実行してレガシー DSF に対するマルチパス機能を無効にしてください。
`scsimgr save_attr -a leg_mpath_enable=false`
- ホストの OS が Windows または AIX で MPIO 機能を使用している場合、VSP G100, G200, G400, G600 および VSP G800 のマイクロコードのバージョンが 83-03-0X-XX/XX 以降、または VSP F400, F600 および VSP F800 のときは、ホストグループのホストモードオプションに 102 を設定してください。

ストレージシステムの要件 (正側, 副側共通)

- global-active device の前提ソフトウェアをインストールし、ライセンスが有効であること。
- 正側のストレージシステムと副側のストレージシステム間が 2 本以上のファイバーチャネルまたは iSCSI で接続されていて、正側のストレージシステムと副側のストレージシステム間で双方向のリモートパスが設定されていること。
- 正側のストレージシステムと副側のストレージシステムの両方に、Quorum ディスク用の外部ボリュームがあり、同一の Quorum ディスク ID が設定されていること。
- ストレージシステムのキャッシュと共用メモリーが十分にあること。

前提ソフトウェア、キャッシュおよび共用メモリーについては、global-active device のマニュアルを参照してください。

Quorum ディスク用の外部ストレージシステムの要件

- 正側のストレージシステムと Quorum ディスク用の外部ストレージシステム間、副側のストレージシステムと Quorum ディスク用の外部ストレージシステム間がそれぞれファイバーチャネル接続または iSCSI 接続されていること。
- 正側のストレージシステム、副側のストレージシステムのポートと Quorum ディスク用の外部ストレージシステムのポート間で外部パスが設定されていること。

ペア管理サーバの要件 (正側, 副側共通)

- バージョン 8.2.0 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 01-34-03/XX 以降の RAID Manager, またはバージョン 01.34.XX 以降の XP7 RAID Manager がインストールされていること。
RAID Manager のインストール手順については、RAID Manager のマニュアルを参照してください。
- 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。

ペアボリュームの要件

- 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 および S-VOL の両方がオープンボリュームであること。
- P-VOL および S-VOL の両方が DP ボリューム, または基本ボリューム (内部ボリュームまたは外部ボリューム) であること。
- P-VOL および S-VOL のボリュームの種別 (DP ボリューム, 内部ボリュームまたは外部ボリューム) が同じであること。
- P-VOL が所属する仮想ストレージマシンのモデル名とシリアル番号が, S-VOL が所属する仮想ストレージマシンのモデル名とシリアル番号と同じであること。

コマンドデバイスの要件

- コマンドデバイスセキュリティが設定されていないこと。
- デフォルトの仮想ストレージマシンに所属していること。
- ストレージシステム内のリソースを分割管理している場合, ホスト (ペア管理サーバ) に, ストレージシステムのリソースグループ ID が 0 (デフォルトの仮想ストレージマシンのリソースプール) のコマンドデバイスが接続されていて, そのコマンドデバイスの情報が Device Manager エージェントの `rgcmddev.properties` ファイルに定義されていること。
- コマンドデバイスの認証モードが有効であること。
- Device Manager の GUI または CLI から `global-active device` ペアに対する操作を実行する前には, ストレージシステムに対してユーザー認証が完了していること。



ヒント

ホストおよびペア管理サーバが, P-VOL, S-VOL, またはコマンドデバイスを認識していることを確認するには, Device Manager エージェントの `hldutil` コマンドを使用してください。



メモ

ストレージシステムに対してユーザー認証を行う方法を次に示します。

自動でユーザー認証を行う

Device Manager サーバと Device Manager エージェント間の通信に SSL/TLS を利用しているとき, Device Manager サーバから取得したユーザーアカウントで自動的にユーザー認証が実行されます。

手動でユーザー認証を行う

RAID Manager のコマンド (`raidcom -login`) を実行して, ユーザー認証を行ってください。

手動でユーザー認証を行う場合は, 次の点に注意してください。

- 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。
- 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。



ヒント

デフォルトの仮想ストレージマシンとは, 次の両方の条件を満たす仮想ストレージマシンのことです。

- 仮想ストレージマシンのモデル名が, 所属するストレージシステムのモデル名と同じである。
- 仮想ストレージマシンのシリアル番号が, 所属するストレージシステムのシリアル番号と同じである。



注意

次の場合は、正側と副側の両方のストレージシステムのマイクロコードのバージョンが 83-03-0X-XX/XX 以降である必要があります。

- 基本ボリューム（内部ボリュームまたは外部ボリューム）を使用して global-active device のコピーペアを作成する場合
- global-active device, Universal Replicator のコピーペアおよび Universal Replicator のデルタリシンクペアを使用した構成（3DC デルタリシンク構成）の場合
この場合は、正側と副側の両方のストレージシステムが VSP G800 または VSP F800 であることも必要です。
- コンシステンシーグループ ID を使用して global-active device ペアを操作する場合
- nondisruptive migration 機能を利用してデータ移行をしたボリュームで global-active device のコピーペアを作成する場合
この場合は、nondisruptive migration 機能でのデータ移行が完了したことを確認してから、コピーペアを作成してください。

リモートパスの設定、ペア管理サーバの設定、Quorum ディスクの設定および仮想ストレージマシンについては、マニュアル「*Hitachi Command Suite ユーザーズガイド*」または「*Hitachi Command Suite CLI リファレンスガイド*」を参照してください。

関連概念

- [5.1.10 管理サーバと Device Manager エージェント間のセキュリティ通信のための操作フロー](#)

関連参照

- [11.3.6 デバイス情報の取得 \(hldutil コマンド\)](#)
- [付録 D.7 Device Manager エージェントが接続するコマンドデバイスに関するプロパティファイル \(rgcmddev.properties ファイル\)](#)

1.19.5 高可用性システムを構築するための要件（VSP G150, G350, G370, G700, G900 および VSP F350, F370, F700, F900 の場合）

次の要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などを構築してください。

管理サーバの要件

- Replication Manager のライセンスが登録されていること。
- 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 および S-VOL を認識しているホスト
 - 正側のペア管理サーバ
 - 副側のペア管理サーバ
 - 正側のストレージシステム
 - 副側のストレージシステム
 - Quorum ディスク用の外部ストレージシステム（Device Manager CLI を使用して高可用性システムを構築する場合）

ホスト（業務サーバ）の要件

- パス管理ソフトウェアがインストールされていること。



メモ

- ホストの OS が HP-UX 11i v3 でネイティブマルチパス機能を使用している場合は、事前に次のコマンドを実行してレガシー DSF に対するマルチパス機能を無効にしてください。
`scsimgr save_attr -a leg_mpath_enable=false`
- ホストの OS が Windows または AIX で MPIO 機能を使用している場合、ホストグループのホストモードオプションに 102 を設定してください。

ストレージシステムの要件（正側、副側共通）

- global-active device の前提ソフトウェアをインストールし、ライセンスが有効であること。
- 正側のストレージシステムと副側のストレージシステム間が 2 本以上のファイバーチャネルまたは iSCSI で接続されていて、正側のストレージシステムと副側のストレージシステム間で双方向のリモートパスが設定されていること。
- 正側のストレージシステムと副側のストレージシステムの両方に、Quorum ディスク用の外部ボリュームがあり、同一の Quorum ディスク ID が設定されていること。
- ストレージシステムのキャッシュと共用メモリーが十分にあること。

前提ソフトウェア、キャッシュおよび共用メモリーについては、global-active device のマニュアルを参照してください。

Quorum ディスク用の外部ストレージシステムの要件

- 正側のストレージシステムと Quorum ディスク用の外部ストレージシステム間、副側のストレージシステムと Quorum ディスク用の外部ストレージシステム間がそれぞれファイバーチャネル接続または iSCSI 接続されていること。
- 正側のストレージシステム、副側のストレージシステムのポートと Quorum ディスク用の外部ストレージシステムのポート間で外部パスが設定されていること。

ペア管理サーバの要件（正側、副側共通）

- バージョン 8.5.0-08 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 01-45-03/XX 以降の RAID Manager、またはバージョン 01.45.XX 以降の XP7 RAID Manager がインストールされていること。
RAID Manager のインストール手順については、RAID Manager のマニュアルを参照してください。
- 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。

ペアボリュームの要件

- 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 および S-VOL の両方がオープンボリュームであること。
- P-VOL および S-VOL の両方が DP ボリューム、または基本ボリューム（内部ボリュームまたは外部ボリューム）であること。
- P-VOL および S-VOL のボリュームの種別（DP ボリューム、内部ボリュームまたは外部ボリューム）が同じであること。
- P-VOL が所属する仮想ストレージマシンのモデル名とシリアル番号が、S-VOL が所属する仮想ストレージマシンのモデル名とシリアル番号と同じであること。

コマンドデバイスの要件

- コマンドデバイスセキュリティが設定されていないこと。
- デフォルトの仮想ストレージマシンに所属していること。
- ストレージシステム内のリソースを分割管理している場合、ホスト（ペア管理サーバ）に、ストレージシステムのリソースグループ ID が 0（デフォルトの仮想ストレージマシンのリソースプール）のコマンドデバイスが接続されていて、そのコマンドデバイスの情報が **Device Manager** エージェントの `rgcmddev.properties` ファイルに定義されていること。
- コマンドデバイスの認証モードが有効であること。
- **Device Manager** の GUI または CLI から **global-active device** ペアに対する操作を実行する前には、ストレージシステムに対してユーザー認証が完了していること。



ヒント

ホストおよびペア管理サーバが、P-VOL、S-VOL、またはコマンドデバイスを認識していることを確認するには、**Device Manager** エージェントの `hldutil` コマンドを使用してください。



メモ

ストレージシステムに対してユーザー認証を行う方法を次に示します。

自動でユーザー認証を行う

Device Manager サーバと **Device Manager** エージェント間の通信に SSL/TLS を利用しているとき、**Device Manager** サーバから取得したユーザーアカウントで自動的にユーザー認証が実行されます。

手動でユーザー認証を行う

RAID Manager のコマンド (`raidcom -login`) を実行して、ユーザー認証を行ってください。

手動でユーザー認証を行う場合は、次の点に注意してください。

- 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。
- 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。



ヒント

デフォルトの仮想ストレージマシンとは、次の両方の条件を満たす仮想ストレージマシンのことです。

- 仮想ストレージマシンのモデル名が、所属するストレージシステムのモデル名と同じである。
- 仮想ストレージマシンのシリアル番号が、所属するストレージシステムのシリアル番号と同じである。



注意

次の要件も確認してください。

- **global-active device**、**Universal Replicator** のコピーペアおよび **Universal Replicator** のデルタリシンクペアを使用した構成（3DC デルタリシンク構成）の場合
この場合は、正側と副側の両方のストレージシステムが **VSP G900** または **VSP F900** であることも必要です。
- コンシステンシーグループ ID を使用して **global-active device** ペアを操作する場合
- **nondisruptive migration** 機能を利用してデータ移行をしたボリュームで **global-active device** のコピーペアを作成する場合
この場合は、**nondisruptive migration** 機能でのデータ移行が完了したことを確認してから、コピーペアを作成してください。

リモートパスの設定、ペア管理サーバの設定、**Quorum** ディスクの設定および仮想ストレージマシンについては、マニュアル「*Hitachi Command Suite ユーザーズガイド*」または「*Hitachi Command Suite CLI リファレンスガイド*」を参照してください。

1.20 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 Hitachi Command Suite 製品で使用されるポート
- 2.2 Hitachi Command Suite 共通コンポーネントで使用されるポートの変更
- 2.3 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録
- 2.4 Host Data Collector でのファイアウォールへの例外登録 (Windows)
- 2.5 IP アドレスが複数ある場合のネットワーク設定
- 2.6 IPv6 環境で運用する場合の Device Manager の設定
- 2.7 管理サーバの IP アドレスまたはホスト名の変更
- 2.8 Hitachi Command Suite 製品の URL の変更 (hcnds64chgurl コマンド)

2.1 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。



ヒント

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。

2.1.1 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 10 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
22015/tcp [※]	管理クライアント (GUI) と通信する際に、HBase 64 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。
22016/tcp	管理クライアント (GUI) と SSL で通信する際に、HBase 64 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。
22017/tcp～22030/tcp 22033/tcp 22034/tcp	Hitachi Command Suite 共通コンポーネントで予約済みのポートです。
22031/tcp	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。
22032/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。 このポート番号は変更できます。
22035/tcp 22037/tcp 22038/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。
22036/tcp	Hitachi Command Suite 共通コンポーネントの内部通信 (ネーミングサービス) で使用されます。 このポート番号は変更できます。
22121/tcp 22123/tcp 22124/tcp	HCS Device Manager Web Service で使用されるポートです。 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。
22122/tcp	HCS Device Manager Web Service で使用されるポートです。 Hitachi Command Suite 共通コンポーネントの内部通信 (ネーミングサービス) で使用されます。 このポート番号は変更できます。

ポート番号	説明
24235/tcp～24242/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。

注※

SSL を設定している場合でも使用されます。外部から管理サーバへの非 SSL 通信を遮断するには、`user_httpsd.conf` ファイルの編集が必要です。

関連概念

- [2.3 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録](#)

関連タスク

- [2.2 Hitachi Command Suite 共通コンポーネントで使用されるポートの変更](#)
- [5.2.3 SSL/TLS を有効にする場合の user_httpsd.conf ファイルの編集](#)

2.1.2 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 11 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（VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、VSP Fx00 モデル、Virtual Storage Platform、Universal Storage Platform V/VM、Hitachi USP および HUS VM）やファイルサーバから 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 <code>server.properties</code> ファイルにある <code>server.http.port</code> プロパティで変更できます。
2443/tcp	Device Manager サーバの内部通信、管理クライアント（GUI および CLI）との SSL 通信、およびストレージシステム（VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデル）との SSL 通信で使用されます。 このポートは、Device Manager サーバの <code>server.properties</code> ファイルにある <code>server.https.port</code> プロパティで変更できます。
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。

ポート番号	説明
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。
24230/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。

関連概念

- [2.3 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録](#)

関連タスク

- [8.5.1 CIM/WBEM 機能で使用するポートを変更する](#)
- [付録 A.1.1 Device Manager サーバのプロパティの変更](#)

関連参照

- [6.2.8 Tuning Manager サーバとのリモート接続およびポート番号の設定 \(htmsetup コマンド\)](#)
- [6.2.9 config.xml ファイルおよび configforclient.xml ファイルの設定](#)
- [付録 A.2.2 server.http.port](#)
- [付録 A.2.3 server.https.port](#)
- [付録 A.2.4 server.rmi.port](#)

2.1.3 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 12 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。

関連タスク

- [付録 B.1.1 Tiered Storage Manager サーバのプロパティの変更](#)

関連参照

- [付録 B.2.1 server.rmi.port](#)
- [付録 B.2.2 server.rmi.security.port](#)

2.1.4 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 13 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。

関連タスク

- [付録 C.1.1 Host Data Collector のプロパティの変更](#)

関連参照

- [付録 C.2.1 hdc.service.localport](#)
- [付録 C.2.3 hdc.adapter.localport](#)
- [付録 C.2.4 hdc.common.rmi.registryPort](#)
- [付録 C.2.5 hdc.common.rmi.serverPort](#)
- [付録 C.2.6 hdc.common.http.serverPort](#)
- [付録 C.2.7 hdc.common.rmi.ssl.registryPort](#)

- [付録 C.2.8 hdc.common.rmi.ssl.serverPort](#)
- [付録 C.2.9 hdc.common.https.serverPort](#)

2.1.5 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 14 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 <code>server.properties</code> ファイルにある <code>server.agent.port</code> 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 <code>server.properties</code> ファイルにある <code>server.http.port</code> 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 <code>server.properties</code> ファイルにある <code>server.http.localPort</code> プロパティで変更できます。

関連タスク

- [付録 D.1.1 Device Manager エージェントのプロパティの変更](#)

関連参照

- [付録 D.6.1 server.agent.port](#)
- [付録 D.6.2 server.http.localPort](#)
- [付録 D.6.3 server.http.port](#)

2.1.6 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 15 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
VSP 5000 シリーズ	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 Storage Navigator 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。
	11099/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。

対象ストレージシステム	ポート番号	説明
	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。
VSP G1000 VSP G1500 VSP F1500 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 Storage Navigator 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。
VSP Gx00 モデル (SVP) VSP Fx00 モデル (SVP)	443/tcp	管理クライアント (GUI) から SSL で Storage Navigator 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す。
	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す。
	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す。
	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す。 1 台の SVP から複数のストレージシステムを同時に接続している場合、接続しているストレージシステムの数だけポートが使用されます。デフォルトでは 51100/tcp~51335/tcp の範囲で使用されます。実際に SVP で使用されているポート番号を確認する場合は、VSP Gx00 モデルまたは VSP Fx00 モデルのマニュアルを参照してください。
VSP Gx00 モデル (コントローラー) VSP Fx00 モデル (コントローラー)	443/tcp	管理クライアント (GUI) から SSL で maintenance utility 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。
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。
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。
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す。
	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す。
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。
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。

対象ストレージシステム	ポート番号	説明
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。

VSP Gx00 モデル (SVP) または VSP Fx00 モデル (SVP) で使用されるポート番号を変更した場合には、Device Manager で次の設定が必要です。

- ファイアウォールの例外登録を設定し直す
- 変更後のポート番号を Device Manager に設定する
1099/tcp を変更した場合には、Device Manager GUI の [ストレージシステム編集] 画面または Device Manager CLI の AddStorageArray コマンドで、変更後のポート番号を設定してください。443/tcp を変更した場合には、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てください。

ミッドレンジストレージ (HUS100, Hitachi SMS, Hitachi AMS2000, Hitachi AMS/WMS) で使用されるポート番号 (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、時間が掛かることがあります。

ポート番号の変更方法および services ファイルの設定方法については、各ストレージシステムのマニュアルを参照してください。

2.2 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。

操作手順

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。

表 16 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
22015/tcp	Windows の場合 : < Hitachi Command Suite のインストールフォルダ > \Base64\UCPSB\httpsd\conf\user_httpsd.conf ^{*1} Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/httpsd/conf/user_httpsd.conf ^{*1}	Listen
22016/tcp	Windows の場合 : < Hitachi Command Suite のインストールフォルダ > \Base64\UCPSB\httpsd\conf\user_httpsd.conf ^{*1} Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/httpsd/conf/user_httpsd.conf ^{*1}	<ul style="list-style-type: none"> • VirtualHost <ホスト名> : <ポート> • Listen^{*2}
22031/tcp	Windows の場合 : < Hitachi Command Suite のインストールフォルダ > \Base64\UCPSB\httpsd\conf\user_hssso_httpsd.conf Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/httpsd/conf/user_hssso_httpsd.conf	Listen 127.0.0.1:<ポート番号>
22032/tcp	Windows の場合 : < Hitachi Command Suite のインストールフォルダ > \Base64\HDB\CONF\emb\HiRDB.ini Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > /Base64/HDB/conf/emb/HiRDB.ini	PDNAMEPORT
	Windows の場合 : < Hitachi Command Suite のインストールフォルダ > \Base64\HDB\CONF\pdsys Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > /Base64/HDB/conf/pdsys	pd_name_port
	Windows の場合 :	pd_name_port

デフォルト のポート番 号	設定ファイル	変更場所
	<p>< Hitachi Command Suite のインストールフォルダ > \Base64\database\work\def_pdsys</p> <p>Linux の場合 :</p> <p>< Hitachi Command Suite のインストールディレクトリ > /Base64/database/work/def_pdsys</p>	
22035/tcp	<p>Windows の場合 :</p> <p>< Hitachi Command Suite のインストールフォルダ > \Base64\uCPSB\CC\web\redirector\workers.properties</p> <p>Linux の場合 :</p> <p>< Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/CC/web/redirector/workers.properties</p>	worker.HBase64StgMgmtSSOService.port
	<p>Windows の場合 :</p> <p>< Hitachi Command Suite のインストールフォルダ > \Base64\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties</p> <p>Linux の場合 :</p> <p>< Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties</p>	webserver.connector.ajp13.port
22036/tcp	<p>Windows の場合 :</p> <p>< Hitachi Command Suite のインストールフォルダ > \Base64\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties</p> <p>Linux の場合 :</p> <p>< Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties</p>	ejbserver.rmi.naming.port
22037/tcp	<p>Windows の場合 :</p> <p>< Hitachi Command Suite のインストールフォルダ > \Base64\uCPSB\CC\server\usrconf\ejb</p>	ejbserver.http.port

デフォルトのポート番号	設定ファイル	変更場所
	¥HBase64StgMgmtSSOService ¥usrconf.properties Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties	
22038/tcp	Windows の場合 : < Hitachi Command Suite のインストールフォルダ > ¥Base64¥uCPSB¥CC¥server¥usrconf¥ejb¥HBase64StgMgmtSSOService¥usrconf.properties Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties	ejbserver.rmi.remote.listener.port
22121/tcp	Windows の場合 : < Hitachi Command Suite のインストールフォルダ > ¥Base64¥uCPSB¥CC¥web¥redirector¥workers.properties Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/CC/web/redirector/workers.properties	worker.DeviceManagerWebService.port
	Windows の場合 : < Hitachi Command Suite のインストールフォルダ > ¥Base64¥uCPSB¥CC¥server¥usrconf¥ejb¥DeviceManagerWebService¥usrconf.properties Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/CC/server/usrconf/ejb/DeviceManagerWebService/usrconf.properties	webserver.connector.ajp13.port
22122/tcp	Windows の場合 : < Hitachi Command Suite のインストールフォルダ > ¥Base64¥uCPSB¥CC	ejbserver.rmi.naming.port

デフォルト のポート番 号	設定ファイル	変更場所
	¥server¥usrconf¥ejb ¥DeviceManagerWebService ¥usrconf.properties Linux の場合 : < Hitachi Command Suite のインストー ルディレクトリ > /Base64/uCPSB/CC/ server/usrconf/ejb/ DeviceManagerWebService/ usrconf.properties	
22123/tcp	Windows の場合 : < Hitachi Command Suite のインストー ルフォルダ > ¥Base64¥uCPSB¥CC ¥server¥usrconf¥ejb ¥DeviceManagerWebService ¥usrconf.properties Linux の場合 : < Hitachi Command Suite のインストー ルディレクトリ > /Base64/uCPSB/CC/ server/usrconf/ejb/ DeviceManagerWebService/ usrconf.properties	ejbserver.http.port
22124/tcp	Windows の場合 : < Hitachi Command Suite のインストー ルフォルダ > ¥Base64¥uCPSB¥CC ¥server¥usrconf¥ejb ¥DeviceManagerWebService ¥usrconf.properties Linux の場合 : < Hitachi Command Suite のインストー ルディレクトリ > /Base64/uCPSB/CC/ server/usrconf/ejb/ DeviceManagerWebService/ usrconf.properties	ejbserver.rmi.remote.listene r.port

注※1

httpsd.conf ファイルは編集しないでください。

注※2

SSL が有効の場合に外部から管理サーバへの非 SSL 通信を遮断するには、
user_httpsd.conf ファイルの Listen 22015 行を編集する必要があります。



メモ

次のポート番号に変更しないでください。

1, 7, 9, 11, 13, 15, 17, 19, 20, 21, 22, 23, 25, 37, 42, 43, 53, 77, 79, 87, 95,
101, 102, 103, 104, 109, 110, 111, 113, 115, 117, 119, 123, 135, 139, 143, 179,

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。
 - 22015/tcp (HBase 64 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。
 - 22016/tcp (SSL 対応の HBase 64 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。

次の作業

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。

- Element Manager を使用して、Hitachi AMS/WMS を操作する場合 (23015/tcp および 23016/tcp)
lauchapptool 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 (22015/tcp および 22016/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。
- JP1/IM と連携している場合 (22015/tcp および 22016/tcp)
JP1/IM の統合機能メニュー画面から、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 の統合機能メニュー定義ファイルを変更する必要があります。
- Hitachi Virtual File Platform および Hitachi Capacity Optimization 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。
Hitachi File Services Manager での設定方法については、ファイルサーバのマニュアルを参照してください。

関連概念

- [6.5 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするための必要な設定](#)

関連タスク

- [2.8 Hitachi Command Suite 製品の URL の変更 \(hcnds64chgurl コマンド\)](#)
- [5.2.3 SSL/TLS を有効にする場合の user_httpsd.conf ファイルの編集](#)
- [5.5.7 ポップアップブロックの設定変更](#)
- [6.1.2 Element Manager を使用するための設定](#)

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)
- [付録 A.1.1 Device Manager サーバのプロパティの変更](#)

関連参照

- [2.1.1 Hitachi Command Suite 共通コンポーネントで使用されるポート](#)
- [付録 A.14.5 htnm.server.n.port](#)

2.3 Device Manager および Tiered Storage Manager での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。



メモ

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、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。

2.3.1 Device Manager および Tiered Storage Manager で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 17 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 18 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 19 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 20 管理サーバ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 21 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 22 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 23 ファイルサーバまたは NAS モジュールを運用する場合にファイアウォールで例外登録が必要なポート番号](#)
- [表 24 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 25 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 26 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 27 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 28 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 29 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 30 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 31 ペア管理サーバを使用してコピーペアを管理する場合にファイアウォールで例外登録が必要なポート番号](#)

表 17 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)	22015/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)	22016/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 18 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"> • VSP 5000 シリーズ • VSP G1000 • VSP G1500 • VSP F1500 	162/udp	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	
	<ul style="list-style-type: none"> • VSP Gx00 モデル (コン トローラー) • VSP Fx00 モ デル (コント ローラー) • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • HUS VM 			
any/tcp	管理サーバ	443/tcp ^{*1}	<ul style="list-style-type: none"> • VSP 5000 シ リーズ • VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 モデル (SVP) • VSP Fx00 モデル (SVP) • Virtual Storage Platform • HUS VM 	-
any/tcp	管理サーバ	1099/ tcp ^{*1}	<ul style="list-style-type: none"> • VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 モデル (SVP) • VSP Fx00 モデル (SVP) • Virtual Storage Platform • Universal Storage Platform V/VM 	-

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"> Hitachi USP HUS VM 	
any/tcp	管理サーバ	2000/tcp ^{*2}	<ul style="list-style-type: none"> Hitachi AMS/WMS 	-
any/tcp	管理サーバ	2000/tcp ^{*2}	<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 ^{*2}	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、ファイアウォールを設定してください。
any/tcp	<ul style="list-style-type: none"> VSP 5000 シリーズ VSP G1000 VSP G1500 VSP F1500 VSP Gx00 モデル (SVP) VSP Fx00 モデル (SVP) 	2443/tcp ^{*2}	管理サーバ	VSP G1000, G1500 または VSP F1500 の場合、RAID Manager および SVP へのログイン時に Hitachi Command Suite でユーザーアカウントを認証しているときに設定が必要です。
any/tcp	管理サーバ	8443/tcp	<ul style="list-style-type: none"> NAS モジュールを搭載した VSP G400, G600, G800 (コントローラー) NAS モジュールを搭載した VSP F400, F600, F800 (コントローラー) 	内部 NAS Manager ^{*3} を使用する場合に設定が必要です。
any/tcp	管理サーバ	11099/tcp	<ul style="list-style-type: none"> VSP 5000 シリーズ 	-
any/tcp	管理サーバ	20443/tcp	<ul style="list-style-type: none"> NAS モジュールを搭載した VSP G400, G600, G800 	内部 NAS Manager ^{*3} を使用する場合に設定が必要です。

通信元		通信先		備考
ポート番号	マシン	ポート番号	マシン	
			(コントローラー) <ul style="list-style-type: none"> NAS モジュールを搭載した VSP F400, F600, F800 (コントローラー) 	
any/tcp	管理サーバ	28355/tcp ^{※2}	<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 ^{※1}	<ul style="list-style-type: none"> VSP 5000 シリーズ VSP G1000 VSP G1500 VSP F1500 VSP Gx00 モデル (SVP) VSP Fx00 モデル (SVP) Virtual Storage Platform Universal Storage Platform V/VM Hitachi USP 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 ^{※1}	<ul style="list-style-type: none"> VSP 5000 シリーズ VSP G1000 VSP G1500 VSP F1500 	通信先のストレージシステムが VSP Gx00 モデルまたは VSP Fx00 モデルの場合、1 台の SVP から複数のストレージシステムを同時に接続しているときは、接続しているストレージシステムの数だけポートが使用されるため、使用されているすべてのポートに対して設定が必要です。デフォルトでは 51100/tcp～51335/tcp の範囲で使用されます。実際に SVP で使用されているポート番号を確認する

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"> • VSP Gx00 モデル (SVP) • VSP Fx00 モデル (SVP) • Virtual Storage Platform 	場合は、VSP Gx00 モデルまたは VSP Fx00 モデルのマニュアルを確認してください。

(凡例)

-: 該当なし

注※1

VSP Gx00 モデル (SVP) または VSP Fx00 モデル (SVP) の場合、ポート番号は変更できません。

注※2

ポート番号は変更できます。

注※3

NAS モジュールを搭載したストレージシステムの内部に存在している NAS Manager です。

表 19 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"> • VSP 5000 シリーズ • VSP G1000 • VSP G1500 • VSP F1500 • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • HUS VM 	
any/tcp	管理クライアント (GUI)	443/tcp ^{※1}	<ul style="list-style-type: none"> • VSP 5000 シリーズ • VSP G1000 	SSL で Storage Navigator を使用する場合に設定が必要です。

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"> • VSP G1500 • VSP F1500 • VSP Gx00 モデル (SVP およびコン トローラー) • VSP Fx00 モ デル (SVP お よびコント ローラー) • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • HUS VM 	
any/tcp	管理クライアント (GUI)	1099/ tcp ^{※1}	<ul style="list-style-type: none"> • VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 モデル (SVP) • VSP Fx00 モ デル (SVP) • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • HUS VM 	-
any/tcp	管理クライアント (GUI)	11099/tcp	<ul style="list-style-type: none"> • VSP 5000 シ リーズ 	-
any/tcp	管理クライアント (GUI)	20443/tcp	<ul style="list-style-type: none"> • NAS モジュ ールを搭載 した VSP G400, G600, G800 (コント ローラー) 	内部 NAS Manager ^{※2} を使用する場合に設定 が必要です。

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"> NAS モジュールを搭載した VSP F400, F600, F800 (コントローラー) 	
any/tcp	管理クライアント (GUI)	51099/tcp ^{*1}	<ul style="list-style-type: none"> VSP 5000 シリーズ VSP G1000 VSP G1500 VSP F1500 VSP Gx00 モデル (SVP) VSP Fx00 モデル (SVP) Virtual Storage Platform Universal Storage Platform V/VM Hitachi USP HUS VM 	
any/tcp	管理クライアント (GUI)	51100/tcp ^{*1}	<ul style="list-style-type: none"> VSP 5000 シリーズ VSP G1000 VSP G1500 VSP F1500 VSP Gx00 モデル (SVP) VSP Fx00 モデル (SVP) Virtual Storage Platform Universal Storage Platform V/VM HUS VM 	通信先のストレージシステムが VSP Gx00 モデルまたは VSP Fx00 モデルの場合、1 台の SVP から複数のストレージシステムを同時に接続しているときは、接続しているストレージシステムの数だけポートが使用されるため、使用されているすべてのポートに対して設定が必要です。デフォルトでは 51100/tcp～51335/tcp の範囲で使用されます。実際に SVP で使用されているポート番号を確認する場合は、VSP Gx00 モデルまたは VSP Fx00 モデルのマニュアルを確認してください。
any/tcp	管理クライアント (GUI)	161/udp	<ul style="list-style-type: none"> VSP 5000 シリーズ 	管理クライアントを SNMP マネージャーとして使用する場合に設定が必要です。

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"> ・ VSP G1000 ・ VSP G1500 ・ VSP F1500 ・ VSP Gx00 モデル (コン トローラー) ・ VSP Fx00 モ デル (コント ローラー) 	
any/tcp	管理クライアント (GUI)	427/tcp	<ul style="list-style-type: none"> ・ VSP 5000 シ リーズ ・ VSP G1000 ・ VSP G1500 ・ VSP F1500 ・ VSP Gx00 モデル (SVP) ・ VSP Fx00 モ デル (SVP) 	SMI-S 機能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)	5443/tcp	<ul style="list-style-type: none"> ・ VSP 5000 シ リーズ ・ VSP G1000 ・ VSP G1500 ・ VSP F1500 	SSL で raidinf コマンドを使用する場合に 設定が必要です。
any/tcp	管理クライアント (GUI)	5989/tcp	<ul style="list-style-type: none"> ・ VSP 5000 シ リーズ ・ VSP G1000 ・ VSP G1500 ・ VSP F1500 ・ VSP Gx00 モデル (SVP) ・ VSP Fx00 モ デル (SVP) 	SMI-S 機能を使用する場合に設定が必要で す。
any/tcp	<ul style="list-style-type: none"> ・ VSP 5000 シ リーズ ・ VSP G1000 ・ VSP G1500 ・ VSP F1500 	162/udp	管理クライアント (GUI)	管理クライアントを SNMP マネージャーとし て使用する場合に設定が必要です。

(凡例)

- : 該当なし

注※1

VSP Gx00 モデル (SVP) または VSP Fx00 モデル (SVP) の場合、ポート番号は変更できません。

注※2

NAS モジュールを搭載したストレージシステムの内部に存在している NAS Manager です。

表 20 管理サーバ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	<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 21 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 ESXiVMware ESXi 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	VMware ESXi	非 SSL 通信の場合に設定が必要です。
any/tcp	管理サーバ	5989/tcp	VMware ESXi	SSL 通信の場合に設定が必要です。

表 22 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 23 ファイルサーバまたは NAS モジュールを運用する場合に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)	443/tcp	外部 NAS Manager※ ¹	-
any/tcp	<ul style="list-style-type: none">Hitachi Virtual File PlatformHitachi Capacity OptimizationNAS Platform	2001/tcp※ ²	管理サーバ	-
any/tcp	外部 NAS Manager※ ¹	2001/tcp※ ²	管理サーバ	-
any/tcp	管理サーバ	8443/tcp	NAS Platform	-

(凡例)

- : 該当なし

注※1

ストレージシステムとは別に存在する NAS Manager です。

注※2

ポート番号は変更できます。

表 24 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	Tuning Manager の管理サーバ	22015/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	24230/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。

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	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。

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 パラメーターに設定したポート番号を登録してください。

表 25 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。 <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 非 SSL 通信のとき
any/tcp	管理サーバ	22099/tcp [※]	Host Data Collector をインストールしたマシン	
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 26 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 ESXi VMware ESXi 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	443/tcp	<ul style="list-style-type: none"> VMware ESXi VMware ESXi 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。
any/tcp	Host Data Collector をインストールしたマシン	445/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。

注※

ポート番号は変更できます。

表 27 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	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 28 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	-

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	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 29 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 ボリュームロック期限の満了 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 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 30 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	389/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。

表 31 ペア管理サーバを使用してコピーペアを管理する場合に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"> • 通常ホスト • 仮想マシン 	31001/udp	<ul style="list-style-type: none"> • VSP 5000 シリーズ • VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 モデル • VSP Fx00 モデル • Virtual Storage Platform • HUS VM 	-

(凡例)

- : 該当なし

関連タスク

- [2.3.2 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録 \(Windows\)](#)
- [2.3.3 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録 \(Red Hat Enterprise Linux 5 または Red Hat Enterprise Linux 6\)](#)

関連参照

- [6.2.9 config.xml ファイルおよび configforclient.xml ファイルの設定](#)

2.3.2 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録 (Windows)

hcmds64fwcancel 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。

操作手順

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 のインストールフォルダ>%Base64%bin%hcmds64fwcancel
```

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。

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

表 32 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	<Hitachi Command Suite のインストールフォルダ> %DeviceManager %HiCommandServer %HiCommandServer.exe
Tiered Storage Manager サーバ	Tiered Storage Manager(htsmService)	<Hitachi Command Suite のインストールフォルダ> %TieredStorageManager%bin %htsmService.exe
JDK	Device Manager - HBase64(java)	<Hitachi Command Suite のインストールフォルダ> %Base64%uCPsB%hjdk%jdk %jre%bin%java.exe*
	Tiered Storage Manager - HBase64(java)	<Hitachi Command Suite のインストールフォルダ> %Base64%uCPsB%hjdk%jdk %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。

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。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [2.3.1 Device Manager および Tiered Storage Manager でファイアウォールへの例外登録が必要なポート](#)

2.3.3 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録（Red Hat Enterprise Linux 5 または Red Hat Enterprise Linux 6）

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。

操作手順

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 2443:tcp 22015:tcp



メモ 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。

関連参照

- [2.3.1 Device Manager および Tiered Storage Manager でファイアウォールへの例外登録が必要なポート](#)

2.3.4 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録（Red Hat Enterprise Linux 7 または Oracle Linux 7）

`firewalld` サービスの管理コマンドである `firewall-cmd` コマンドを使用して、ゾーンを適用したポートに対し、Hitachi Command Suite で使用されるポート番号を指定します。

操作手順

1. ゾーンを適用したポートに対し、有効にするサービス名を指定します。
デフォルトゾーンにサービス名を指定し、OS 再起動後も設定を有効にする例を次に示します。
`firewall-cmd --permanent --add-service=<サービス名>`

- ・ <サービス名>
非 SSL 通信の場合は http, SSL 通信の場合は https を指定します。
- 2. ゾーンを適用したポートに対し、通信を許可するポート番号として、Hitachi Command Suite で使用されるポート番号、およびそのポート番号とのプロトコルの組み合わせを指定します。デフォルトゾーンにポート番号とプロトコルの組み合わせを指定し、OS 再起動後も設定を有効にする例を次に示します。
firewall-cmd --permanent --add-port=<ポート番号>/<プロトコル>
- ・ <ポート番号>
Hitachi Command Suite で使用されるポート番号を指定します。
- ・ <プロトコル>
tcp または udp を指定します。

関連参照

- ・ [2.3.1 Device Manager および Tiered Storage Manager でファイアウォールへの例外登録が必要なポート](#)

2.4 Host Data Collector で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、手動でファイアウォールの例外登録をする必要があります。

2.4.1 Host Data Collector で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)
- ・ hdc.service.localport プロパティ (デフォルト値: 22110/tcp)
- ・ hdc.adapter.localport プロパティ (デフォルト値: 22111/tcp~22120/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。

関連タスク

- [2.4.2 Host Data Collector](#) でのサービスの例外登録 (SSL 通信用)

関連参照

- [付録 C.2.1 hdc.service.localport](#)
- [付録 C.2.3 hdc.adapter.localport](#)
- [付録 C.2.4 hdc.common.rmi.registryPort](#)
- [付録 C.2.5 hdc.common.rmi.serverPort](#)
- [付録 C.2.6 hdc.common.http.serverPort](#)

2.4.2 Host Data Collector で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。

前提条件

- Administrator 権限でのログイン
- 次の情報の確認
 - `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)

操作手順

1. ポートごとに次のコマンドを実行します。

```
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。



ヒント

次のコマンドを実行すると登録内容を確認できます。

```
netsh advfirewall firewall show rule name=all
```

関連タスク

- [9.2.2 Host Data Collector](#) のサービスの起動
- [9.2.3 Host Data Collector](#) のサービスの停止
- [2.4.1 Host Data Collector](#) でのサービスの例外登録 (非 SSL 通信用)

関連参照

- 付録 C.2.7 `hdc.common.rmi.ssl.registryPort`
- 付録 C.2.8 `hdc.common.rmi.ssl.serverPort`
- 付録 C.2.9 `hdc.common.https.serverPort`

2.5 IP アドレスが複数ある場合のネットワーク設定

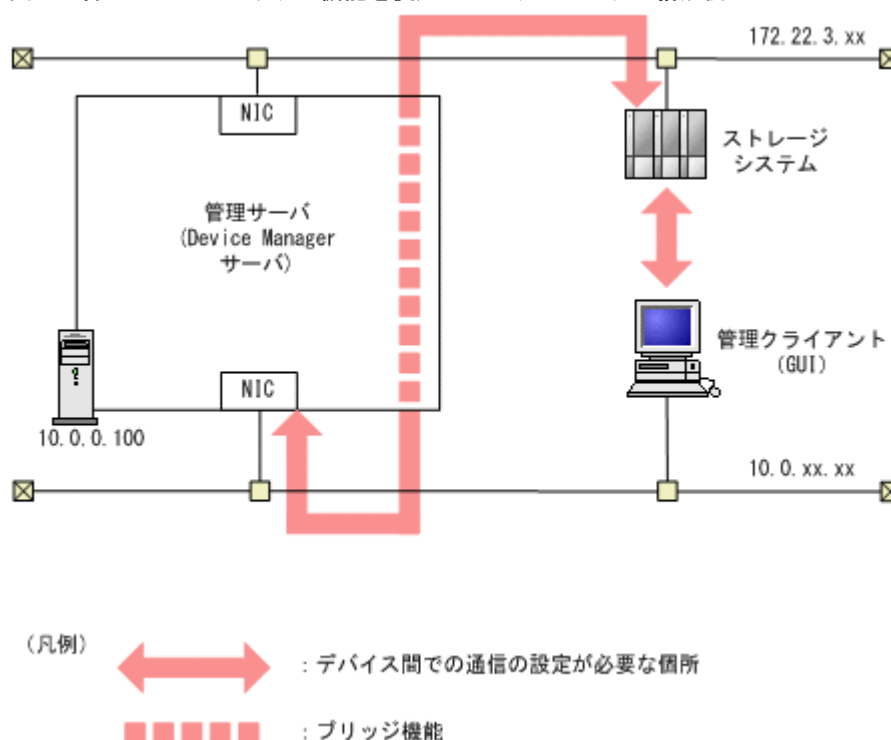
複数のネットワーク構成の場合の通信設定について説明します。

2.5.1 管理サーバで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 19 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。

- ストレージシステムと、管理クライアントの間
- ストレージシステムと、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 19 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)

関連タスク

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

関連参照

- [付録 A.2.1 server.http.host](#)
- [付録 A.10.1 launchapp.snm2.url](#)

2.5.2 Host Data Collector マシンに複数の IP アドレスがある場合の設定

管理サーバとは別にインストールした Host Data Collector のマシンが複数の 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。

関連参照

- [付録 C.2.10 hdc.service.rmi.registryIPAddress](#)

2.6 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。
- Element Manager を使用して、Hitachi AMS/WMS 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。

関連参照

- [6.1 Storage Navigator Modular 2 と連携するために必要な設定](#)

2.6.1 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、user_httpsd.conf ファイルを編集します。



メモ

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。
ただし、インストール後に Hitachi File Services Manager や 32bit 版 Storage Navigator Modular 2 と連携する場合は、次のファイルの設定で、IPv6 での通信が有効になっていることを確認してください。

- Windows の場合：

< Hitachi File Services Manager または 32bit 版 Storage Navigator Modular 2 のインストールフォルダ >¥Base¥httpsd¥conf¥httpsd.conf

- Linux の場合 :
< Hitachi File Services Manager または 32bit 版 Storage Navigator Modular 2 のインストールディレクトリ >/Base/httpsd/conf/httpsd.conf

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. user_httpsd.conf ファイルを開きます。
user_httpsd.conf ファイルの格納先を次に示します。

- Windows の場合 :
< Hitachi Command Suite のインストールフォルダ >¥Base64¥uCPSB¥httpsd¥conf ¥user_httpsd.conf
- Linux の場合 :
< Hitachi Command Suite のインストールディレクトリ >/Base64/uCPSB/httpsd/conf/ user_httpsd.conf



メモ

user_httpsd.conf ファイルと同じ場所に格納されている httpsd.conf ファイルは編集しないでください。

ただし、Hitachi File Services Manager や 32bit 版 Storage Navigator Modular 2 と連携している場合は、次の場所に格納されている httpsd.conf ファイルも編集してください。

Windows の場合 :

< Hitachi File Services Manager または 32bit 版 Storage Navigator Modular 2 のインストールフォルダ >¥Base¥httpsd¥conf¥httpsd.conf

Linux の場合 :

< Hitachi File Services Manager または 32bit 版 Storage Navigator Modular 2 のインストールディレクトリ >/Base/httpsd/conf/httpsd.conf

user_httpsd.conf ファイルの編集と同じ手順で編集してください。ただし、ポート番号は HBase Storage Mgmt Web Service のポート番号 (非 SSL 通信の場合は 23015 (デフォルト)、SSL 通信の場合は 23016 (デフォルト)) を指定してください。

-
3. 「#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。



注意

- 非 SSL 通信の場合、SSLDisable 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。

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

2.6.2 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/VM 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。

操作手順

1. 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/VM 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。

関連タスク

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

関連参照

- [付録 A.2.1 server.http.host](#)

2.7 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。

2.7.1 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 (Linux の場合)、`user_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。

前提条件

- 次の情報の確認
 - 変更後の管理サーバのホスト名
ホスト名は 128 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。



ヒント 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。

操作手順

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

2. 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。
 - 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
 - 管理サーバと CIM クライアント間
 - 管理サーバとストレージシステム（VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデル）間

3. 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. `user_httpsd.conf` ファイルを編集します。

`ServerName` ディレクティブの値を変更後のホスト名に変更します。

- Windows の場合：


```
<Hitachi Command Suite のインストールフォルダ>%Base64%uCPsB%httpsd%conf%user_httpsd.conf
```
- Linux の場合：


```
<Hitachi Command Suite のインストールディレクトリ>/Base64/uCPsB/httpsd/conf/user_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` ディレクティブの値を変更後のホスト名に変更します。



メモ `httpsd.conf` ファイルおよび `hssso_httpsd.conf` ファイルは編集しないでください。

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 のインストールフォルダ>%Base64%conf%cluster.conf
```
- Linux の場合：


```
<Hitachi Command Suite のインストールディレクトリ>/Base64/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。

関連概念

- [10.2 データベースのバックアップ](#)

関連タスク

- [2.8 Hitachi Command Suite 製品の URL の変更 \(hcmds64chgurl コマンド\)](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)
- [9.1.4 Hitachi Command Suite のサービスの稼働状態の確認](#)

関連参照

- [2.7.3 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](#)

2.7.2 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、`user_httpsd.conf` ファイルを編集したあと、マシンを再起動します。

前提条件

次の情報の確認

- 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。

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. `user_httpsd.conf` ファイルを編集します。

`ServerName` ディレクティブに変更前の 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 のインストールフォルダ > \Base64\uCPSB\httpsd\conf
user_httpsd.conf
- Linux の場合 :
< Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/httpsd/
conf/user_httpsd.conf



メモ

- `httpsd.conf` ファイルは編集しないでください。
 - `user_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。

関連概念

- [10.2 データベースのバックアップ](#)

関連タスク

- [2.8 Hitachi Command Suite 製品の URL の変更 \(hcnds64chgurl コマンド\)](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)
- [9.1.4 Hitachi Command Suite のサービスの稼働状態の確認](#)

関連参照

- [2.7.3 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](#)

2.7.3 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。
Replication Manager 情報取得元の登録方法については、マニュアル「*Hitachi Command Suite Replication Manager ユーザーズガイド*」を参照してください。
- Element Manager を使用して、Hitachi AMS/WMS を操作する場合
`lauchapptool` 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リポジトリの所在登録を変更する方法については、マニュアル「*Hitachi Command Suite Tuning Manager 運用管理ガイド*」を参照してください。
- 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

- NAS Platform の場合は、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 SMU, NAS Manager, または NAS Platform CLI で変更してください。
設定する IP アドレスの形式 (IPv6 または IPv4) は、次の形式に合わせてください。

表 33 設定する管理サーバの IP アドレスの形式 (NAS Platform の SNMP トラップの設定)

条件		IP アドレスの形式 (IPv6 または IPv4)
Admin services EVS から SNMP トラップを送信するように、NAS Platform CLI で設定している		Admin services EVS の IP アドレスの形式に合わせる
Admin services EVS から SNMP トラップを送信しないように、NAS Platform CLI で設定している	ファイルシステムをマウントする EVS がある	ファイルシステムをマウントする EVS の IP アドレスの形式に合わせる
	ファイルシステムをマウントする EVS がない	ファイルサーバ (ノード) の IP アドレスの形式に合わせる

- Hitachi Virtual File Platform および Hitachi Capacity Optimization の場合は、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。
ファイルサーバの SNMP トラップ通知先の変更方法については、ファイルサーバのマニュアルを参照してください。
- VSP 5000 シリーズを操作する場合
Device Manager GUI の [ストレージシステム編集] 画面で、ユーザーアカウント認証を設定し直してください。
- VSP G1000, G1500 または VSP F1500 で、RAID Manager および SVP へのログイン時に Hitachi Command Suite でユーザーアカウントを認証している場合
Device Manager に同梱されたデフォルトの証明書以外を使用して Device Manager とストレージシステム間でセキュリティ通信をしているときは、Device Manager GUI の [ストレージシステム編集] 画面で、ユーザーアカウント認証を設定し直してください。
- VSP Gx00 モデルまたは VSP Fx00 モデルを操作する場合
Device Manager に同梱されたデフォルトの証明書以外を使用して Device Manager とストレージシステム間でセキュリティ通信をしているときは、Device Manager GUI の [ストレージシステム編集] 画面で、ユーザーアカウント認証を設定し直してください。
- 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、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 の統合機能メニュー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。

Device Manager, Tiered Storage Manager および Replication Manager 以外で必要になる設定については、各 Hitachi Command Suite 製品のマニュアルを参照してください。

関連概念

- [6.5 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするために必要な設定](#)

関連タスク

- [4.7 外部認証サーバと外部認可サーバの登録](#)

- [6.1.2 Element Manager](#) を使用するための設定
- [9.1.2 Hitachi Command Suite](#) のサービスの起動
- [9.1.3 Hitachi Command Suite](#) のサービスの停止
- [付録 A.1.1 Device Manager](#) サーバのプロパティの変更

関連参照

- [6.2.9 config.xml](#) ファイルおよび [configforclient.xml](#) ファイルの設定
- [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 [RAID Manager XP](#) の情報の設定 ([hdvmagt_setting](#) コマンド)
- [付録 A.2.1 server.http.host](#)

2.8 Hitachi Command Suite 製品の URL の変更 (hcnds64chgurl コマンド)

GUI に登録されている各 Hitachi Command Suite 製品の URL を hcnds64chgurl コマンドで変更します。

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 hcnds64chgurl コマンドで変更する必要があります。

- HBase 64 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

操作手順

1. hcnds64chgurl コマンドを実行します。

Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>%Base64%\bin\hcnds64chgurl
{/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>}
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/
hcnds64chgurl {-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。



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://hostname:22015
- 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>

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 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 または Windows Server 2012 R2 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>
user_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：22015）、SSL 通信の場合は、SSL 通信用のポート番号（デフォルト：22016）を指定してください。
user_httpsd.conf ファイルの格納先は次のとおりです。
<Hitachi Command Suite のインストールフォルダ>%Base64%uCPSB%httpsd%conf
%user_httpsd.conf

関連概念

- [5.1.2 管理サーバと管理クライアント（GUI）間のセキュリティ通信のための操作フロー](#)

関連タスク

- [2.2 Hitachi Command Suite 共通コンポーネントで使用されるポートの変更](#)
- [2.7.1 管理サーバのホスト名の変更](#)
- [2.7.2 管理サーバの IP アドレスの変更](#)

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

3.1 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。

操作手順

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 のインストールフォルダ>\Base64\conf\sec  
security.conf
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/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 34 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

項目	説明
password.min.numeric	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。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



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。
- 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。

操作結果

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。

3.2 アカウントロックとは

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。



ヒント

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。

操作手順

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 のインストールフォルダ >¥Base64¥conf¥sec
¥security.conf
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/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 35 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



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。

操作結果

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。

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。

操作手順

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 のインストールフォルダ>\Base64\conf\user.conf
 - Linux の場合：
<Hitachi Command Suite のインストールディレクトリ>/Base64/conf/user.conf
- user.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。

操作結果

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。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

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、hcmds64unlockaccount コマンドで解除できます。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 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。
- 次の情報の確認

- 。 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

操作手順

1. hcmds64unlockaccount 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 のインストールフォルダ > ¥Base64¥bin  
¥hcmds64unlockaccount [/user <ユーザー ID > /pass <パスワード >]
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/  
hcmd64unlockaccount [-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。



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、アンパサンド (&)、縦線 (|) またはアクセントコンフлекс (^) が含まれる場合は、記号 1 文字ごとに引用符 (") で囲むか、アクセントコンフлекс (^) でエスケープしてください。
 - 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。
-

外部認証サーバでのユーザー管理

この章では、外部認証サーバでユーザー認証する方法について説明します。

- 4.1 外部認証サーバとの連携とは
- 4.2 外部認可サーバとの連携とは
- 4.3 外部認証サーバでユーザー認証するための操作フロー
- 4.4 Hitachi Command Suite 製品のアカウントの条件
- 4.5 ユーザーエントリーのデータ構造とは
- 4.6 複数の外部認証サーバと連携している場合の構成
- 4.7 外部認証サーバと外部認可サーバの登録
- 4.8 情報検索用のユーザーアカウントとは
- 4.9 共有秘密鍵の登録
- 4.10 外部認証サーバおよび外部認可サーバとの接続確認
- 4.11 外部認証サーバとの連携設定に使用するコマンドに関する注意事項
- 4.12 Kerberos 認証に使用できる暗号タイプ

4.1 外部認証サーバとの連携とは

Hitachi Command Suite 製品では、外部認証サーバに登録されているユーザーアカウントを使って、GUI にログインしたり、CLI を実行したりできます。

外部認証サーバと連携すると、Hitachi Command Suite 製品でのログインパスワードの管理やアカウントの制御が不要になります。

Hitachi Command Suite 製品では、次の外部認証サーバとの連携をサポートしています。

- LDAP ディレクトリサーバ
- RADIUS サーバ
- Kerberos サーバ

4.2 外部認可サーバとの連携とは

外部認証サーバでユーザー認証を行う場合には、外部認可サーバも併用することで、管理サーバ (Hitachi Command Suite 製品) に対するアクセス可否を外部認可サーバで制御できます。

外部認可サーバとも連携する場合、Hitachi Command Suite 製品では、ユーザーを外部認可サーバのグループ (認可グループ) ごとに管理するため、Hitachi Command Suite 製品での個々のユーザーのアカウント管理や権限設定が不要になります。

Hitachi Command Suite 製品では、LDAP ディレクトリサーバ (Active Directory) との連携をサポートしています。

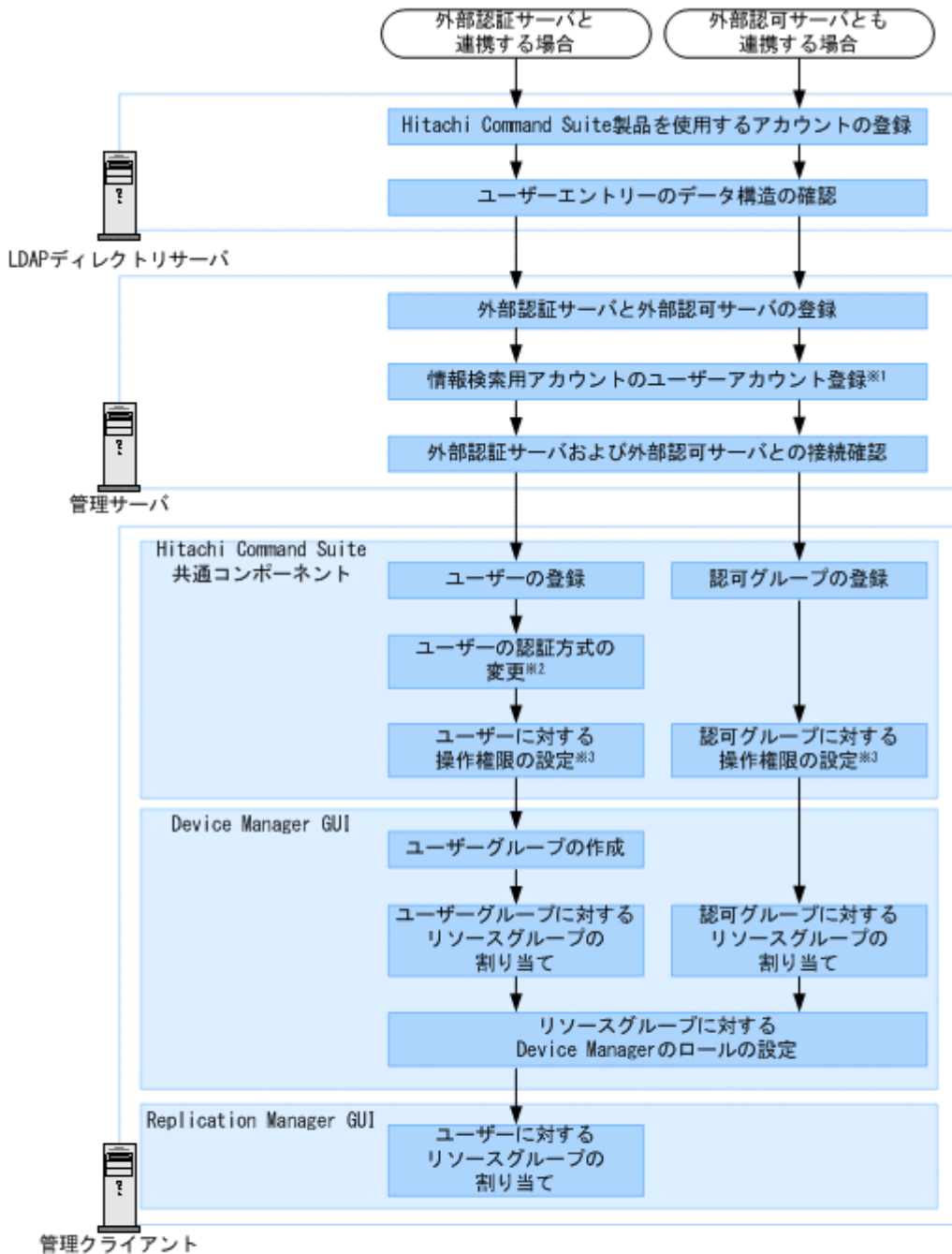
4.3 外部認証サーバでユーザー認証するための操作フロー

外部認証サーバで一元管理されているユーザーアカウントを使って、Hitachi Command Suite 製品の GUI や CLI を使用できるようにするためには、外部認証サーバ、管理サーバおよび管理クライアントで環境設定が必要です。

4.3.1 LDAP ディレクトリサーバでユーザー認証するための操作フロー

LDAP ディレクトリサーバでユーザー認証するためには、Hitachi Command Suite 製品で、管理サーバへの外部認証サーバの登録や認証対象のアカウントの登録などが必要です。

図 20 LDAP ディレクトリサーバでユーザー認証するための操作フロー



注※1 外部認証サーバとだけ連携する場合、ユーザーエントリーのデータ構造がフラットモデルのときは、不要な操作です。

注※2 既存のユーザーの認証方式を変更する場合に必要な操作です。

注※3 ユーザーの作業範囲に応じて操作権限を設定します。

- ユーザー管理 (User Management)
- Device Manager以外のHitachi Command Suite製品
CLIを使用してTiered Storage Managerを運用するユーザーに対しては、ロールに加えて、Tiered Storage Managerの権限も付与する必要があります。



メモ

- Hitachi Command Suite 製品の運用開始後に、外部認可サーバと連携したシステム構成に切り替える場合は、Hitachi Command Suite 共通コンポーネントに登録されている同名のユーザー ID は削除するか、変更してください。ユーザー ID にドメイン名が含まれている場合 (例: user1@example.com) も同様に、同名のユーザー ID を削除するか、変更してください。同名のユーザー ID が登録されている場合、そのユーザー

ーが Hitachi Command Suite 製品にログインした際には, Hitachi Command Suite 共通コンポーネントでの認証 (内部認証) となります。

- **Replication Manager** では, 認可グループに所属するユーザーにリソースグループとして All Resources が自動的に割り当てられます。また, 認可グループに対して **Modify** 権限を設定した場合, その認可グループに所属するユーザーのユーザーロールは **Storage Administrator** になります (変更はできません)。
 - 登録した認可グループのネストグループに属するユーザーも, 認可グループに設定されたロール (権限) で Hitachi Command Suite 製品を操作できるようになります。
 - LDAP ディレクトリサーバと管理サーバとの通信に **StartTLS** を使用する場合は, セキュリティ通信のための環境設定が別途必要です。
 - 管理クライアントでの作業については, マニュアル「*Hitachi Command Suite ユーザーズガイド*」またはマニュアル「*Hitachi Command Suite Replication Manager ユーザーズガイド*」を参照してください。
-

関連概念

- [4.5 ユーザーエントリーのデータ構造とは](#)
- [4.8 情報検索用のユーザーアカウントとは](#)
- [5.1 Device Manager および Tiered Storage Manager のセキュリティ通信路](#)

関連タスク

- [4.7 外部認証サーバと外部認可サーバの登録](#)
- [4.10 外部認証サーバおよび外部認可サーバとの接続確認](#)

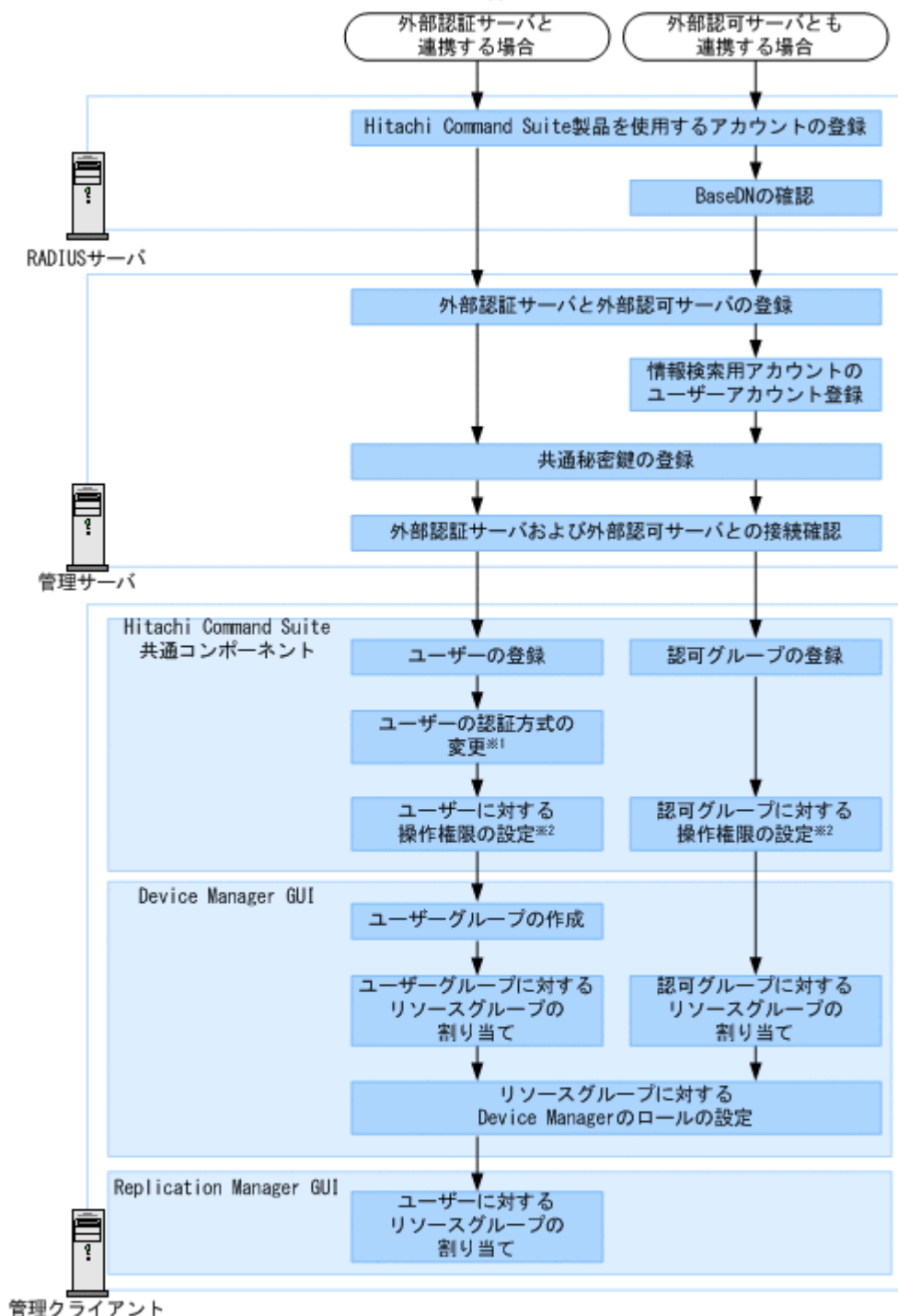
関連参照

- [4.4 Hitachi Command Suite 製品のアカウントの条件](#)

4.3.2 RADIUS サーバでユーザー認証するための操作フロー

RADIUS サーバでユーザー認証するためには、Hitachi Command Suite 製品で、管理サーバへの外部認証サーバの登録や認証対象のアカウントの登録などが必要です。

図 21 RADIUS サーバでユーザー認証するための操作フロー



注※1 既存のユーザーの認証方式を変更する場合に必要な操作です。

注※2 ユーザーの作業範囲に応じて操作権限を設定します。

- ユーザー管理 (User Management)
- Device Manager以外のHitachi Command Suite製品
CLIを使用してTiered Storage Managerを運用するユーザーに対しては、ロールに加えて、Tiered Storage Managerの権限も付与する必要があります。



メモ

- Hitachi Command Suite 製品の運用開始後に、外部認可サーバと連携したシステム構成に切り替える場合は、Hitachi Command Suite 共通コンポーネントに登録されている同名のユーザー ID は削除するか、変更してください。同名のユーザー ID が登録されている場合、そのユーザーが Hitachi Command Suite 製品にログインした際には、Hitachi Command Suite 共通コンポーネントでの認証（内部認証）となります。
- Replication Manager では、認可グループに所属するユーザーにリソースグループとして All Resources が自動的に割り当てられます。また、認可グループに対して Modify 権限を設定した場合、その認可グループに所属するユーザーのユーザーロールは Storage Administrator になります（変更はできません）。
- 登録した認可グループのネストグループに属するユーザーも、認可グループに設定されたロール（権限）で Hitachi Command Suite 製品を操作できるようになります。
- LDAP ディレクトリサーバと管理サーバとの通信に StartTLS を使用する場合は、セキュリティ通信のための環境設定が別途必要です。
- 管理クライアントでの作業については、マニュアル「Hitachi Command Suite ユーザーズガイド」またはマニュアル「Hitachi Command Suite Replication Manager ユーザーズガイド」を参照してください。

関連概念

- [4.5 ユーザーエントリーのデータ構造とは](#)
- [4.8 情報検索用のユーザーアカウントとは](#)
- [5.1 Device Manager および Tiered Storage Manager のセキュリティ通信路](#)

関連タスク

- [4.7 外部認証サーバと外部認可サーバの登録](#)
- [4.9 共有秘密鍵の登録](#)
- [4.10 外部認証サーバおよび外部認可サーバとの接続確認](#)

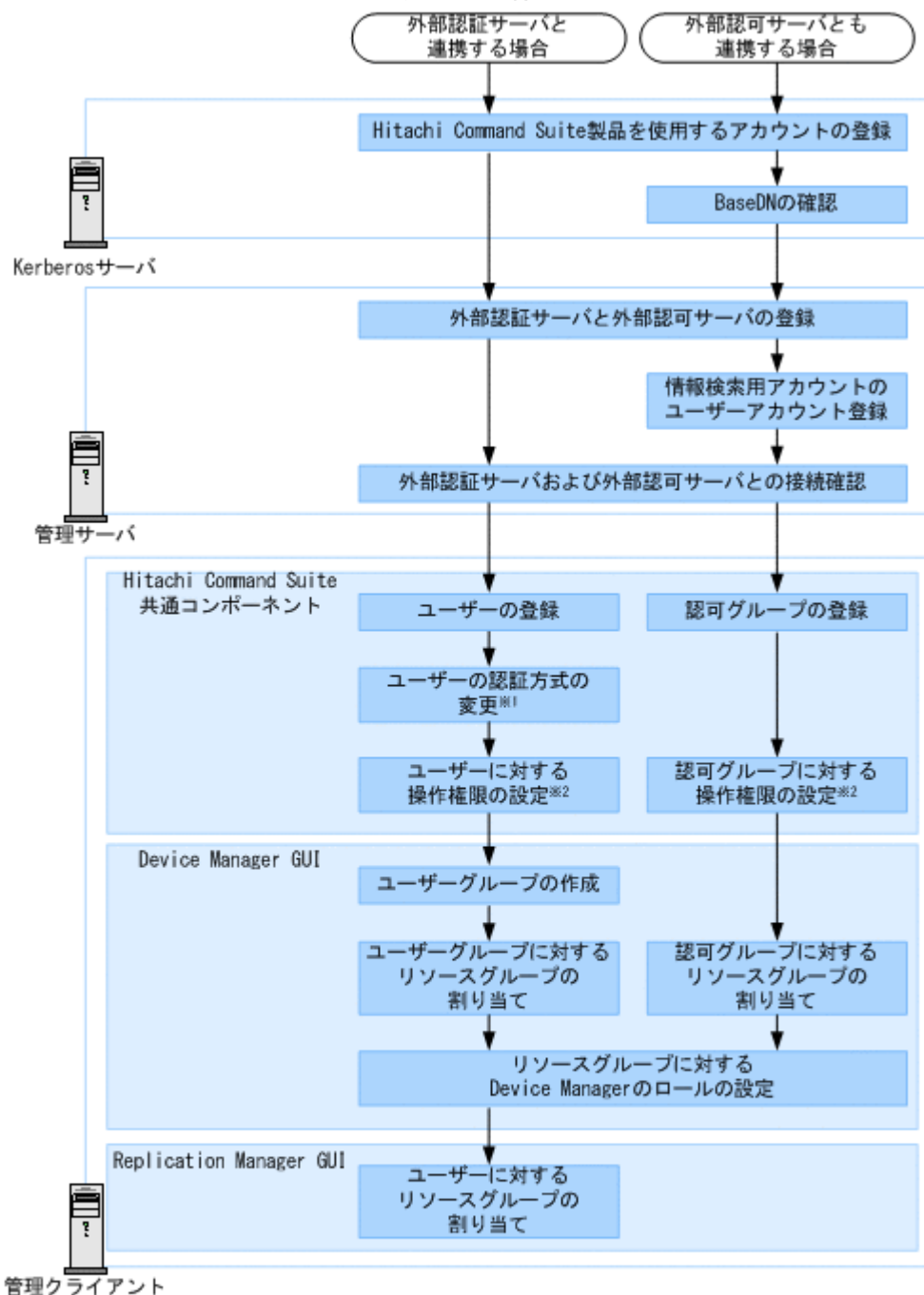
関連参照

- [4.4 Hitachi Command Suite 製品のアカウントの条件](#)

4.3.3 Kerberos サーバでユーザー認証するための操作フロー

Kerberos サーバでユーザー認証するためには、Hitachi Command Suite 製品で、管理サーバへの外部認証サーバの登録や認証対象のアカウントの登録などが必要です。

図 22 Kerberos サーバでユーザー認証するための操作フロー



注※1 既存のユーザーの認証方式を変更する場合に必要な操作です。

注※2 ユーザーの作業範囲に応じて操作権限を設定します。

- ユーザー管理 (User Management)
- Device Manager以外のHitachi Command Suite製品
CLIを使用してTiered Storage Managerを運用するユーザーに対しては、ロールに加えて、Tiered Storage Managerの権限も付与する必要があります。



メモ

- Hitachi Command Suite 製品の運用開始後に、外部認証サーバと連携したシステム構成に切り替える場合は、Hitachi Command Suite 共通コンポーネントに登録されている同名のユーザー ID は削除するか、変更してください。ユーザー ID にレルム名が含まれている場合（例：user1@EXAMPLE.COM）も同様に、同名のユーザー ID を削除するか、変更してください。同名のユーザー ID が登録されている場合、そのユーザーが Hitachi Command Suite 製品にログインした際には、Hitachi Command Suite 共通コンポーネントでの認証（内部認証）となります。
- Replication Manager では、認可グループに所属するユーザーにリソースグループとして All Resources が自動的に割り当てられます。また、認可グループに対して Modify 権限を設定した場合、その認可グループに所属するユーザーのユーザーロールは Storage Administrator になります（変更はできません）。
- 登録した認可グループのネストグループに属するユーザーも、認可グループに設定されたロール（権限）で Hitachi Command Suite 製品を操作できるようになります。
- LDAP ディレクトリサーバと管理サーバとの通信に StartTLS を使用する場合は、セキュリティ通信のための環境設定が別途必要です。
- 管理クライアントでの作業については、マニュアル「Hitachi Command Suite ユーザーズガイド」またはマニュアル「Hitachi Command Suite Replication Manager ユーザーズガイド」を参照してください。

関連概念

- [4.5 ユーザーエントリーのデータ構造とは](#)
- [4.8 情報検索用のユーザーアカウントとは](#)
- [5.1 Device Manager および Tiered Storage Manager のセキュリティ通信路](#)

関連タスク

- [4.7 外部認証サーバと外部認可サーバの登録](#)
- [4.10 外部認証サーバおよび外部認可サーバとの接続確認](#)

関連参照

- [4.4 Hitachi Command Suite 製品のアカウントの条件](#)

4.4 Hitachi Command Suite 製品のアカウントの条件

Hitachi Command Suite 製品を使用するユーザーのアカウント（ユーザー ID およびパスワード）は、外部認証サーバと Hitachi Command Suite 製品の両方で使用できる文字で構成されている必要があります。

次の条件をすべて満たすように、ユーザーアカウントを設定してください。

- 256 バイト以内であること。
- 次の文字を使用していること。
A~Z a~z 0~9 ! # \$ % & ' () * + - . = @ ¥ ^ _ |

Hitachi Command Suite 製品では、ユーザー ID の大文字と小文字の違いは区別されません。また、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に従ってください。

4.5 ユーザーエントリーのデータ構造とは

LDAP ディレクトリサーバのユーザーエントリーのデータ構造には階層構造モデルとフラットモデルがあります。

LDAP ディレクトリサーバでユーザー認証を行う場合、管理サーバに登録する LDAP ディレクトリサーバの情報や管理サーバで必要な作業がデータ構造によって異なるため、ユーザーエントリーがどちらに該当しているかを確認してください。

また、LDAP ディレクトリサーバでユーザー認証・認可する場合には、ユーザーを検索する起点となるエントリー（BaseDN）についても確認してください。

4.5.1 BaseDN とは

認証および認可の際にユーザーを検索する起点となるエントリーを BaseDN といいます。

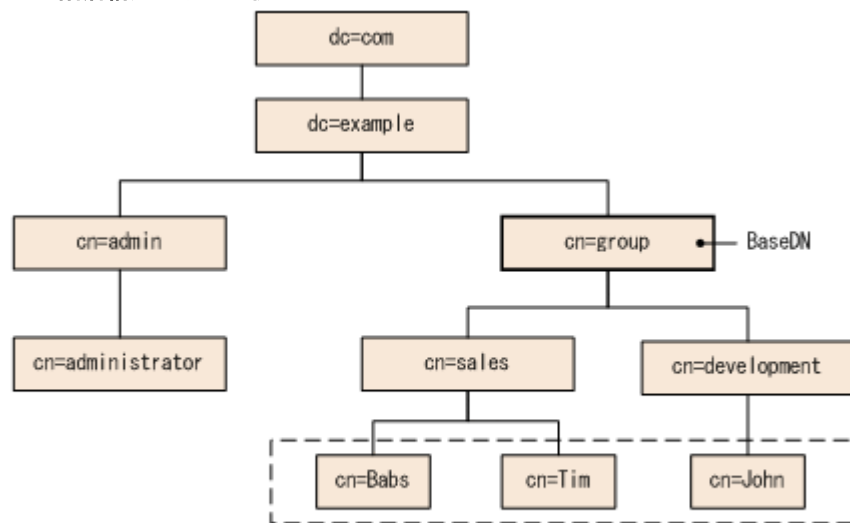
BaseDN より下の階層のユーザーエントリーが認証・認可の対象となります。Hitachi Command Suite 製品で認証・認可したいユーザーをすべて含むエントリーであることが必要です。BaseDN は、管理サーバに LDAP ディレクトリサーバの情報を登録する際に必要になります。

4.5.2 階層構造モデルとは

BaseDN より下の階層が分岐していて、かつ別の階層下にユーザーエントリーが登録されているデータ構造の場合は階層構造モデルになります。

階層構造モデルの場合は、BaseDN より下のエントリーを対象に、ログイン ID とユーザー属性値が等しいエントリーが検索されます。次の図に階層構造モデルの例を示します。

図 23 階層構造モデルの例



(凡例) [-----]: 認証対象のユーザーエントリー

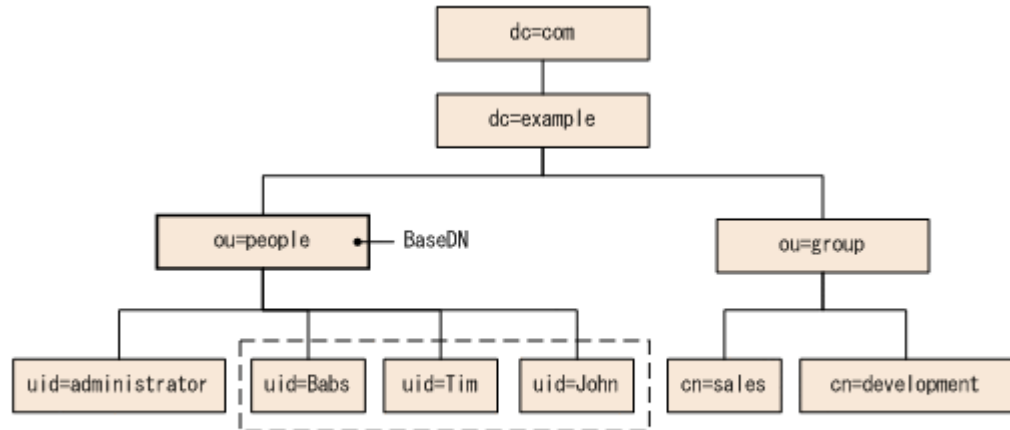
点線で囲まれた範囲が、認証の対象となるユーザーエントリーです。この例では、対象のユーザーエントリーが「cn=sales」と「cn=development」の2つのエントリーにわたって属しているので、BaseDNは「cn=group,dc=example,dc=com」となります。

4.5.3 フラットモデルとは

BaseDN より下に分岐がなく、かつ直下にユーザーエントリーが登録されているデータ構造の場合はフラットモデルになります。

フラットモデルの場合は、BaseDN より下のエントリーを対象に、ログイン ID と BaseDN を組み合わせた DN を持つエントリーが認証されます。次の図にフラットモデルの例を示します。

図 24 フラットモデルの例



(凡例) [---]: 認証対象のユーザーエントリー

点線で囲まれた範囲が、認証の対象となるユーザーエントリーです。この例では、認証対象のすべてのユーザーエントリーが「ou=people」の直下に属しているため、BaseDN は「ou=people,dc=example,dc=com」となります。

ただし、次のどちらかに該当する場合は、データ構造がフラットモデルであっても、階層構造モデルの場合の説明に従って設定してください。

- Hitachi Command Suite 製品のユーザー ID として、RDN の属性以外のユーザー属性値を使用する
ユーザーエントリーの RDN の属性値以外のユーザー属性値（Windows のログオン ID など）をユーザー ID として使用する場合には、階層構造モデルの場合の認証方法の設定が必要です。
- ユーザーエントリーの RDN の属性値に、Hitachi Command Suite 製品のユーザー ID として使用できない文字が使われている
フラットモデルの場合の認証では、ユーザーエントリーの RDN の属性値を Hitachi Command Suite 製品のユーザー ID として使用します。そのため、Hitachi Command Suite 製品のユーザー ID として使用できない文字が使われている場合は、フラットモデルの場合の認証を行うことができません。
使用できる RDN の例：
uid=John123S
cn=John_Smith
使用できない RDN の例：
uid=John:123S（コロン（:）が使用されている）
cn=John Smith（スペースが使用されている）

4.6 複数の外部認証サーバと連携している場合の構成

複数の外部認証サーバと連携している場合、冗長構成またはマルチドメイン構成でユーザー認証します。

それぞれの外部認証サーバで同一のユーザー情報を管理する構成を、冗長構成と呼びます。ある外部認証サーバに障害が発生しても、ほかの外部認証サーバでユーザー認証できます。

外部認証サーバごとに異なるユーザー情報を管理する構成を、マルチドメイン構成と呼びます。ドメイン名を含んでいるユーザー ID でログインすると、入力したドメインの外部認証サーバでユーザー認証されます。外部認証サーバが Kerberos サーバの場合は、レルムごとに異なるユーザー情報を管理することで、マルチドメイン構成と同様の構成にできます。

冗長構成およびマルチドメイン構成に対応している外部認証サーバは次のとおりです。

表 36 冗長構成およびマルチドメイン構成のサポート状況

外部認証サーバ	冗長構成	マルチドメイン構成
LDAP ディレクトリサーバ	Y※1	Y※1
RADIUS サーバ	Y	-
Kerberos サーバ	Y	Y※2

(凡例)

Y : サポートしている

- : サポートしていない

注※1

冗長構成またはマルチドメイン構成のどちらか一方の構成にできます。

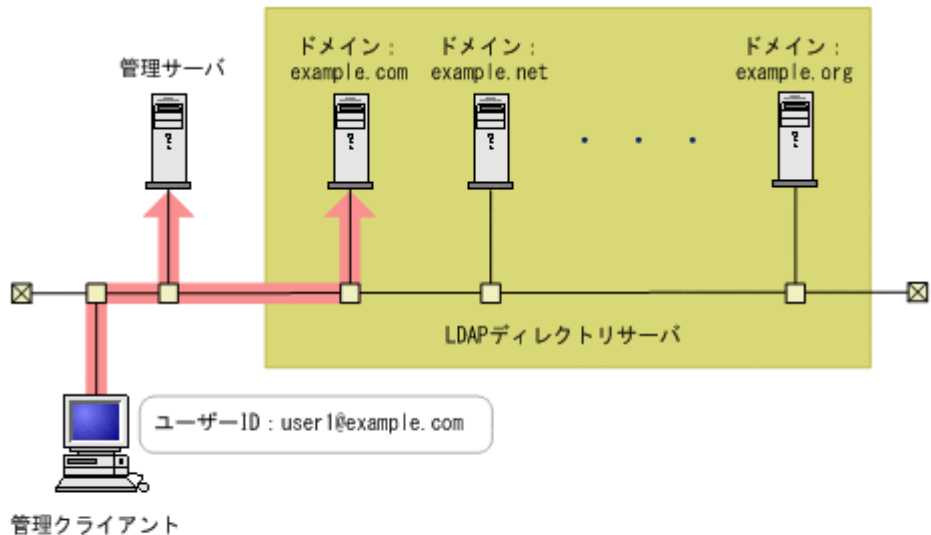
注※2


レルムごとに異なるユーザー情報を管理することで、マルチドメイン構成と同様の構成にできます。

マルチドメイン構成の LDAP ディレクトリサーバでユーザー認証する場合、ログイン時に入力したユーザー ID にドメイン名を含んでいるかどうかで、ユーザー認証の処理が異なります。

ドメイン名を含んでいるユーザー ID でログインすると、次の図に示すように、入力したドメインの LDAP ディレクトリサーバでユーザー認証されます。

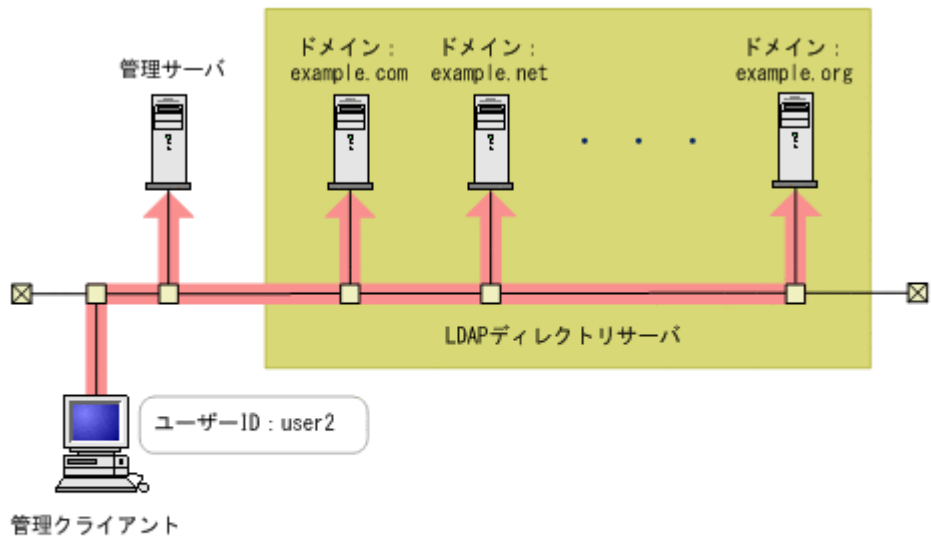
図 25 マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいるユーザー ID の場合）




(凡例)
 : ユーザー認証の処理

ドメイン名を含んでいないユーザー ID でログインすると、次の図に示すように、連携しているすべての LDAP ディレクトリサーバへ順にユーザー認証ができるまで認証処理が実行されます。このとき、多数の LDAP ディレクトリサーバと連携していると、ユーザー認証に時間が掛かるため、ドメイン名を含んでいるユーザー ID でログインすることをお勧めします。

図 26 マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいないユーザー ID の場合）



(凡例)
 : ユーザー認証の処理

4.7 外部認証サーバと外部認可サーバの登録

exauth.properties ファイルに、使用する外部認証サーバの種類やサーバ識別名、外部認証サーバと外部認可サーバのマシン情報などを設定します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- exauth.properties ファイルのひな形のコピー

Windows の場合 :

```
<Hitachi Command Suite のインストールフォルダ>%Base64%sample%conf%  
%exauth.properties
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/sample/conf/  
exauth.properties
```

- ユーザーエントリーのデータ構造の確認 (認証方式が LDAP の場合)
- LDAP ディレクトリサーバの OS での DNS サーバの環境設定*
- DNS サーバの SRV レコードへの LDAP ディレクトリサーバ情報の登録*
- 次の情報の確認
 - 共通
 - 外部認証サーバの種類
 - 認証方式が LDAP の場合
 - 外部認証サーバおよび外部認可サーバのマシン情報 (ホスト名または IP アドレス, ポート番号)
 - BaseDN
 - LDAP ディレクトリサーバが管理する外部認可サーバ用のドメイン名 (外部認可サーバと連携する場合)
 - LDAP ディレクトリサーバが管理するマルチドメイン構成用のドメイン名 (マルチドメイン構成の場合)
 - 認証方式が RADIUS の場合
 - 外部認証サーバおよび外部認可サーバのマシン情報 (ホスト名または IP アドレス, ポート番号)
 - 認証プロトコル
 - 管理サーバのホスト名または IP アドレス
 - LDAP ディレクトリサーバが管理するドメイン名 (外部認可サーバと連携する場合)
 - BaseDN (外部認可サーバと連携する場合)
 - 認証方式が Kerberos の場合
 - 外部認証サーバおよび外部認可サーバのマシン情報 (ホスト名または IP アドレス, ポート番号)
 - レルム名
 - LDAP ディレクトリサーバが管理するドメイン名 (外部認可サーバと連携する場合)
 - BaseDN (外部認可サーバと連携する場合)

注※ LDAP ディレクトリサーバの情報を DNS サーバに照会する場合に必要な作業です。

操作手順

1. コピーした `exauth.properties` ファイルに必要な事項を指定します。
2. `exauth.properties` ファイルを次の場所に格納します。

Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>\Base64\conf  
exauth.properties
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/conf/  
exauth.properties
```

3. `auth.ocsp.enable` プロパティと `auth.ocsp.responderURL` プロパティの設定値を変更した場合には、Hitachi Command Suite 製品のサービスを再起動します。
それ以外のプロパティまたは属性の設定値を変更した場合は、直ちに変更後の値が有効になります。

関連概念

- [4.5 ユーザーエントリーのデータ構造とは](#)
- [4.6 複数の外部認証サーバと連携している場合の構成](#)

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

4.7.1 LDAP ディレクトリサーバで認証する場合の `exauth.properties` ファイルの設定項目

`exauth.properties` ファイルには、使用する外部認証サーバの種類やサーバ識別名、外部認証サーバのマシン情報などを設定します。

- 共通のプロパティ
[表 37 LDAP ディレクトリサーバで認証する場合の `exauth.properties` ファイルの設定項目 \(共通項目\)](#)
- 外部認証サーバと外部認可サーバのプロパティ
接続先の LDAP ディレクトリサーバの情報を `exauth.properties` ファイルに直接指定する場合と、DNS サーバに照会する場合とで設定する項目が異なります。
 - LDAP ディレクトリサーバの情報を直接指定する場合
[表 38 LDAP ディレクトリサーバで認証する場合の `exauth.properties` ファイルの設定項目 \(外部認証サーバの情報を直接指定するとき\)](#)
[表 39 LDAP ディレクトリサーバで認証する場合の `exauth.properties` ファイルの設定項目 \(外部認証サーバと StartTLS で通信するとき\)](#)
 - LDAP ディレクトリサーバの情報を DNS サーバに照会する場合
[表 40 LDAP ディレクトリサーバで認証する場合の `exauth.properties` ファイルの設定項目 \(外部認証サーバの情報を DNS サーバに照会するとき\)](#)



メモ

- プロパティの設定値は、大文字と小文字を区別してください。
- 管理サーバと LDAP ディレクトリサーバとの間の通信に StartTLS を使用する場合は、`exauth.properties` ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する必要があります。

- DNS サーバに接続先の LDAP ディレクトリサーバを照会する場合は、ユーザーがログインする際に処理に時間が掛かることがあります。
- 接続先の LDAP ディレクトリサーバがマルチドメイン構成の場合、DNS サーバに LDAP ディレクトリサーバを照会できません。

表 37 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）

プロパティ名	説明
auth.server.type	外部認証サーバの種類です。ldap を指定します。 デフォルト値：internal（外部認証サーバと連携しない場合）
auth.server.name	LDAP ディレクトリサーバのサーバ識別名を指定します。接続プロトコルやポート番号などの設定（「 表 38 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき） 」および「 表 40 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき） 」）を LDAP ディレクトリサーバごとに区別するために付ける任意の名称です。初期値として「ServerName」が設定されています。必ず 1 つ以上のサーバ識別名を指定してください。サーバ識別名を複数指定する場合は、サーバ識別名をコンマ（,）で区切って指定します。同じサーバ識別名は重複して登録しないでください。 指定できる値：64 バイト以内の次の文字列 0～9 A～Z a～z ! # () + - . = @ [] ^ _ { } ~ デフォルト値：なし
auth.ldap.multi_domain	LDAP ディレクトリサーバのサーバ識別名を複数指定する場合、各サーバがマルチドメイン構成であるか、冗長構成であるかを指定します。 マルチドメイン構成の場合は true を指定します。 冗長構成の場合は false を指定します。 デフォルト値：false
auth.group.mapping	外部認可サーバとも連携するかどうかを指定します。 連携する場合は true を指定します。 連携しない場合は false を指定します。 デフォルト値：false

表 38 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）

属性	説明
protocol ^{*1}	LDAP ディレクトリサーバ接続のプロトコルです。この項目は必須です。 平文による通信の場合は ldap、StartTLS による通信の場合は tls を指定します。 tls を指定する場合には、LDAP ディレクトリサーバで次のどれかの暗号方式を使用できることを事前に確認してください。 <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA 指定できる値：ldap または tls

属性	説明
	デフォルト値：なし
host ^{※2}	LDAP ディレクトリサーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。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。この項目は必須です。 デフォルト値：なし
port	LDAP ディレクトリサーバのポート番号です。指定するポートが、LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120 (秒) デフォルト値：15
attr	認証で使用するユーザー ID の値が定義されている属性名 (Attribute Type) です。 <ul style="list-style-type: none"> 階層構造モデルの場合 ユーザーを一意に特定できる値が格納されている属性名を指定します。この属性に格納された値を Hitachi Command Suite 製品のユーザー ID として使用します。^{※3} 例えば、Active Directory を使用している場合で、Windows のログオン ID をユーザー ID として使用したいときは、Windows のログオン ID が値として定義されている属性名の sAMAccountName を指定します。 フラットモデルの場合 ユーザーエントリーの RDN の属性名を指定します。 例えば、ユーザーの DN が uid=John,ou=People,dc=example,dc=com の場合、uid=John の属性名である uid を指定します。 初期値として sAMAccountName が設定されています。この項目は必須です。 デフォルト値：なし
basedn	LDAP ディレクトリサーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認証の対象となります。指定した値は LDAP ディレクトリサーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。 <ul style="list-style-type: none"> 階層構造モデルの場合 検索対象のユーザーエントリーをすべて含む階層の DN です。 フラットモデルの場合 検索対象のユーザーエントリーより 1 つ上の階層の DN です。 この項目は必須です。DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。 空白文字 # + ; , < = > ¥ デフォルト値：なし
retry.interval	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60 (秒) デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。

属性	説明
	指定できる値：0～50 デフォルト値：20
domain.name	LDAP ディレクトリサーバが管理する外部認可サーバ用のドメインの名称です。 外部認可サーバとも連携する場合、この項目は必須です。 デフォルト値：なし
domain	LDAP ディレクトリサーバが管理するマルチドメイン構成用のドメインの名称です。 ログイン時に、この属性で指定したドメイン名をユーザー ID に含めると、指定したドメインに属する LDAP ディレクトリサーバが認証先となります。 LDAP ディレクトリサーバのサーバ識別名ごとにドメイン名を指定する際に、ドメイン名を重複しないように指定してください。大文字小文字は区別されません。 マルチドメイン構成の場合、この項目は必須です。 デフォルト値：なし
dns_lookup	false を指定します。 デフォルト値：false

注

各属性は、次のように指定します。

auth.ldap.<auth.server.name に指定した値>.<属性>=<値>

注※1

LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合には、Hitachi Command Suite 共通コンポーネントのセキュリティ設定が必要です。

注※2

LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合は、host 属性には LDAP ディレクトリサーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。

注※3

Hitachi Command Suite 製品のユーザー ID として使用できない文字列が値に含まれていない属性を指定してください。

表 39 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバと StartTLS で通信するとき）

プロパティ名	説明
auth.ocsp.enable	LDAP ディレクトリサーバと StartTLS で通信する場合に、OCSP レスポンダーを使用して LDAP ディレクトリサーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を、検証しない場合は false を指定します。 デフォルト値：false
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に、OCSP レスポンダーの URL を指定します。省略した場合は、AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値：なし

表 40 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）

属性	説明
protocol	LDAP ディレクトリサーバ接続のプロトコルです。この項目は必須です。 指定できる値：ldap デフォルト値：なし
port	LDAP ディレクトリサーバのポート番号です。指定するポートが、LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：15
attr	認証で使用するユーザー ID の値が定義されている属性名（Attribute Type）です。 <ul style="list-style-type: none"> 階層構造モデルの場合 ユーザーを一意に特定できる値が格納されている属性名を指定します。この属性に格納された値を Hitachi Command Suite 製品のユーザー ID として使用します。* 例えば、Active Directory を使用している場合で、Windows のログオン ID をユーザー ID として使用したいときは、Windows のログオン ID が値として定義されている属性名の sAMAccountName を指定します。 フラットモデルの場合 ユーザーエントリーの RDN の属性名を指定します。 例えば、ユーザーの DN が uid=John,ou=People,dc=example,dc=com の場合、uid=John の属性名である uid を指定します。 初期値として sAMAccountName が設定されています。この項目は必須です。 デフォルト値：なし
basedn	LDAP ディレクトリサーバの情報を検索する際に、起点となるエントリーの DN（BaseDN）です。この DN より下の階層のユーザーエントリーが認証の対象となります。指定した値は LDAP ディレクトリサーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。 <ul style="list-style-type: none"> 階層構造モデルの場合 検索対象のユーザーエントリーをすべて含む階層の DN です。 フラットモデルの場合 検索対象のユーザーエントリーより 1 つ上の階層の DN です。 この項目は必須です。DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。 空白文字 # + ; , < = > ¥ デフォルト値：なし
retry.interval	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60（秒） デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。

属性	説明
	指定できる値：0～50 デフォルト値：20
domain.name	LDAP ディレクトリサーバが管理する外部認可サーバ用のドメインの名称です。 この項目は必須です。 デフォルト値：なし
dns_lookup	true を指定します。 ただし、次の属性に値が設定されている場合は、DNS サーバには照会されず、ユーザーが指定した値を使用して LDAP ディレクトリサーバに接続されます。 <ul style="list-style-type: none"> auth.ldap.<auth.server.name に指定した値>.host auth.ldap.<auth.server.name に指定した値>.port デフォルト値：false

注

各属性は、次のように指定します。

auth.ldap.<auth.server.name に指定した値>.<属性>=<値>

注※

Hitachi Command Suite 製品のユーザー ID として使用できない文字列が値に含まれていない属性を指定してください。

4.7.2 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定例

LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定例を次に示します。

- LDAP ディレクトリサーバの情報を直接指定する場合（外部認証サーバとだけ連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.dns_lookup=false
```

- LDAP ディレクトリサーバを DNS サーバに照会する場合（外部認証サーバとだけ連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```


- LDAP ディレクトリサーバの情報を直接指定する場合（外部認可サーバとも連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=false
```

- LDAP ディレクトリサーバを DNS サーバに照会する場合（外部認可サーバとも連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- 冗長構成の場合

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=false
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
```

- マルチドメイン構成の場合

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=true
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
```

```
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

4.7.3 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目

exauth.properties ファイルには、使用する外部認証サーバの種類やサーバ識別名、外部認証サーバのマシン情報などを設定します。

- 共通のプロパティ
[表 41 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）](#)
- 外部認証サーバのプロパティ
RADIUS サーバごとに設定します。
[表 42 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの設定）](#)
- 外部認可サーバのプロパティ
外部認可サーバとも連携する場合に必要な設定です。LDAP ディレクトリサーバの情報をドメインごとに設定します。
接続先の LDAP ディレクトリサーバの情報を直接指定する場合と、DNS サーバに照会する場合とで exauth.properties ファイルに設定する項目が異なります。
 - LDAP ディレクトリサーバの情報を直接指定する場合
[表 43 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）](#)
[表 44 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を直接指定するとき）](#)
[表 45 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）](#)
 - LDAP ディレクトリサーバの情報を DNS サーバに照会する場合
[表 43 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）](#)
[表 46 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）](#)



メモ

- プロパティの設定値は、大文字と小文字を区別してください。
- 管理サーバと LDAP ディレクトリサーバとの間の通信に StartTLS を使用する場合は、exauth.properties ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する必要があります。
- DNS サーバに接続先の LDAP ディレクトリサーバを照会する場合は、ユーザーがログインする際に処理に時間が掛かることがあります。

表 41 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）

プロパティ名	説明
auth.server.type	外部認証サーバの種類です。radius を指定します。 デフォルト値：internal（外部認証サーバと連携しない場合）
auth.server.name	RADIUS サーバのサーバ識別名を指定します。接続プロトコルやポート番号などの設定（表 42 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの設定））を RADIUS サーバごとに区別するために付ける任意の名称です。初期値として「ServerName」が設定されています。必ず 1 つ以上のサーバ識別名を指定してください。RADIUS サーバを冗長構成にする場合は、各サーバのサーバ識別名をコンマ（,）で区切って指定します。サーバ識別名は重複して登録しないでください。 指定できる値：64 バイト以内の次の文字列 0～9 A～Z a～z ! # () + - . = @ [] ^ _ { } ~ デフォルト値：なし
auth.group.mapping	外部認可サーバとも連携するかどうかを指定します。 連携する場合は true を指定します。 連携しない場合は false を指定します。 デフォルト値：false

表 42 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの設定）

属性	説明
protocol	RADIUS サーバ認証に使用する認証プロトコルです。この項目は必須です。 指定できる値：PAP または CHAP デフォルト値：なし
host ^{*1}	RADIUS サーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。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。この項目は必須です。 デフォルト値：なし
port	RADIUS サーバの認証用ポート番号です。指定するポートが RADIUS サーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：1812
timeout	RADIUS サーバと接続するときの接続待ち時間です。 指定できる値：1～65535（秒） デフォルト値：1
retry.times	RADIUS サーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。 指定できる値：0～50 デフォルト値：3
attr.NAS-Identifier ^{*2}	Device Manager の管理サーバのホスト名です。RADIUS サーバが管理サーバを識別するために使用します。初期値として、管理サーバのホスト名が設定されています。 指定できる値：253 バイト以内の次の文字列

属性	説明
	0~9 A~Z a~z ! " # \$ % & ' () * + , - . / : ; < = > ? @ [¥] ^ _ ` { } ~ デフォルト値：なし
attr.NAS-IP-Address ^{※2}	Device Manager の管理サーバの IPv4 アドレスです。RADIUS サーバが管理サーバを識別するために使用します。 IPv4 アドレスの形式が不正な場合、この属性は無効です。 デフォルト値：なし
attr.NAS-IPv6-Address ^{※2}	Device Manager の管理サーバの IPv6 アドレスです。RADIUS サーバが管理サーバを識別するために使用します。IPv6 アドレスは必ず角括弧 ([]) で囲んでください。 IPv6 アドレスの形式が不正な場合、この属性は無効です。 デフォルト値：なし

注

各属性は、次のように指定します。

auth.radius.<auth.server.name に指定した値>.<属性>=<値>

注※1

同一マシンで稼働する外部認可サーバとも連携し、かつ LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合は、host 属性には LDAP ディレクトリサーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。

注※2

attr.NAS-Identifier, attr.NAS-IP-Address, attr.NAS-IPv6-Address はどれか 1 つを必ず指定してください。

表 43 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）

属性	説明
domain.name	LDAP ディレクトリサーバが管理するドメインの名称です。外部認可サーバとも連携する場合、この項目は必須です。 デフォルト値：なし
dns_lookup	LDAP ディレクトリサーバの情報を DNS サーバに照会するかどうかを指定します。 exauth.properties ファイルに LDAP ディレクトリサーバの情報を直接指定する場合は false を指定します。 DNS サーバに照会する場合は、true を指定します。 ただし、次の属性に値が設定されている場合は、DNS サーバには照会されず、ユーザーが指定した値を使用して LDAP ディレクトリサーバに接続されます。 <ul style="list-style-type: none"> auth.group.<ドメイン名>.host auth.group.<ドメイン名>.port デフォルト値：false

注

各属性は、次のように指定します。

auth.radius.<auth.server.name に指定した値>.<属性>=<値>

表 44 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を直接指定するとき）

属性	説明
protocol ^{※1}	<p>LDAP ディレクトリサーバ接続のプロトコルです。</p> <p>平文による通信の場合は ldap, StartTLS による通信の場合は tls を指定します。</p> <p>tls を指定する場合には, LDAP ディレクトリサーバで次のどれかの暗号方式を使用できることを事前に確認してください。</p> <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA <p>指定できる値: ldap または tls デフォルト値: ldap</p>
host ^{※2}	<p>外部認証サーバと外部認可サーバが異なるマシンで稼働している場合に, LDAP ディレクトリサーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合, IP アドレスへの名前解決ができることを事前に確認してください。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。</p> <p>省略した場合は, 外部認証サーバと外部認可サーバが同一マシンで稼働しているものと見なされます。</p> <p>デフォルト値: なし</p>
port	<p>LDAP ディレクトリサーバのポート番号です。指定するポートが, LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。</p> <p>指定できる値: 1~65535 デフォルト値: 389</p>
basedn	<p>LDAP ディレクトリサーバの情報を検索する際に, 起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認可の対象となります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。</p> <p>DN は RFC4514 の規約に従って指定してください。例えば, 次の文字が DN に含まれる場合は, 1 文字ごとに円記号 (¥) でエスケープする必要があります。</p> <p>空白文字 # + ; , < = > ¥</p> <p>指定した値は LDAP ディレクトリサーバにそのまま渡されるため, BaseDN にエスケープが必要な文字が含まれる場合は, 正しくエスケープしてください。</p> <p>省略した場合は, Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。</p> <p>デフォルト値: なし</p>
timeout	<p>LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合, タイムアウトしないで, 通信エラーが発生するまで待ち続けます。</p> <p>指定できる値: 0~120 (秒) デフォルト値: 15</p>
retry.interval	<p>LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。</p> <p>指定できる値: 1~60 (秒) デフォルト値: 1</p>

属性	説明
retry.times	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。 指定できる値：0～50 デフォルト値：20

注

各属性は、次のように指定します。

auth.group.<ドメイン名>.<属性>=<値>

<ドメイン名>には、auth.radius.<auth.server.name に指定した値>.domain.name の値を指定します。

注※1

LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合には、Hitachi Command Suite 共通コンポーネントのセキュリティ設定が必要です。

注※2

外部認証サーバと外部認可サーバが別のマシンで稼働していて、かつ LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合は、host 属性には LDAP ディレクトリサーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。

表 45 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）

プロパティ名	説明
auth.ocsp.enable	LDAP ディレクトリサーバと StartTLS で通信する場合に、OCSP レスポンダーを使用して LDAP ディレクトリサーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を、検証しない場合は false を指定します。 デフォルト値：false
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に、OCSP レスポンダーの URL を指定します。省略した場合は、AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値：なし

表 46 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）

属性	説明
protocol	LDAP ディレクトリサーバ接続のプロトコルです。 指定できる値：ldap デフォルト値：ldap
port	LDAP ディレクトリサーバのポート番号です。指定するポートが、LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
basedn	LDAP ディレクトリサーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認可の対象となる。

属性	説明
	<p>ります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。</p> <p>DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。</p> <p>空白文字 # + ; , < = > ¥</p> <p>指定した値は LDAP ディレクトリサーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。</p> <p>省略した場合は、Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。</p> <p>デフォルト値：なし</p>
timeout	<p>LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。</p> <p>指定できる値：0~120 (秒)</p> <p>デフォルト値：15</p>
retry.interval	<p>LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。</p> <p>指定できる値：1~60 (秒)</p> <p>デフォルト値：1</p>
retry.times	<p>LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。</p> <p>指定できる値：0~50</p> <p>デフォルト値：20</p>

注

各属性は、次のように指定します。

auth.group.<ドメイン名>.<属性>=<値>

<ドメイン名>には、auth.radius.<auth.server.name に指定した値>.domain.name の値を指定します。

4.7.4 RADIUS サーバで認証する場合の exauth.properties ファイルの設定例

RADIUS サーバで認証する場合の exauth.properties ファイルの設定例を次に示します。

- 外部認証サーバとだけ連携する場合

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=false
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
```

- 外部認可サーバの情報を直接設定する場合

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
```

```

auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=false
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.host=ldap.example.com
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20

```

- 外部認証サーバを DNS サーバに照会する場合

```

auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=true
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20

```

- 冗長構成の場合

```

auth.server.type=radius
auth.server.name=ServerName1,ServerName2
auth.group.mapping=false
auth.radius.ServerName1.protocol=PAP
auth.radius.ServerName1.host=radius1.example.com
auth.radius.ServerName1.port=1812
auth.radius.ServerName1.timeout=1
auth.radius.ServerName1.retry.times=3
auth.radius.ServerName1.attr.NAS-IP-Address=127.0.0.1
auth.radius.ServerName2.protocol=PAP
auth.radius.ServerName2.host=radius2.example.com
auth.radius.ServerName2.port=1812
auth.radius.ServerName2.timeout=1
auth.radius.ServerName2.retry.times=3
auth.radius.ServerName2.attr.NAS-IP-Address=127.0.0.1

```

4.7.5 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目

exauth.properties ファイルには、使用する外部認証サーバの種類やサーバ識別名、外部認証サーバのマシン情報などを設定します。

- 共通のプロパティ
[表 47 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）](#)
- 外部認証サーバのプロパティ
 Kerberos サーバごとに設定します。
 接続先の Kerberos サーバの情報を直接指定する場合と、DNS サーバに照会する場合とで exauth.properties ファイルに設定する項目が異なります。
 - Kerberos サーバの情報を直接指定する場合

表 48 Kerberos サーバで認証する場合の `exauth.properties` ファイルの設定項目 (外部認証サーバの情報を直接指定するとき)

- Kerberos サーバの情報を DNS サーバに照会する場合
表 49 Kerberos サーバで認証する場合の `exauth.properties` ファイルの設定項目 (外部認証サーバの情報を DNS サーバに照会するとき)
- 外部認可サーバのプロパティ
Kerberos サーバの情報を直接指定し、かつ外部認可サーバとも連携する場合にだけ必要な設定です。レルムごとに指定します。
表 50 Kerberos サーバで認証する場合の `exauth.properties` ファイルの設定項目 (外部認可サーバの設定)
表 51 Kerberos サーバで認証する場合の `exauth.properties` ファイルの設定項目 (外部認可サーバと StartTLS で通信するとき)



メモ

- プロパティの設定値は、大文字と小文字を区別してください。
- 管理サーバと LDAP ディレクトリサーバとの間の通信に StartTLS を使用する場合は、`exauth.properties` ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する必要があります。
- DNS サーバに接続先の LDAP ディレクトリサーバを照会する場合は、ユーザーがログインする際に処理に時間が掛かることがあります。

表 47 Kerberos サーバで認証する場合の `exauth.properties` ファイルの設定項目 (共通項目)

プロパティ名	説明
<code>auth.server.type</code>	外部認証サーバの種類です。kerberos を指定します。 デフォルト値: internal (外部認証サーバと連携しない場合)
<code>auth.group.mapping</code>	外部認可サーバとも連携するかどうかを指定します。 連携する場合は true を指定します。 連携しない場合は false を指定します。 デフォルト値: false

表 48 Kerberos サーバで認証する場合の `exauth.properties` ファイルの設定項目 (外部認証サーバの情報を直接指定するとき)

属性	説明
<code>default_realm</code>	デフォルトのレルム名を指定します。GUI のログイン画面でレルム名を省略してユーザー ID を入力した場合に、この項目で指定したレルムに所属するユーザーとして認証されます。この項目は必須です。 デフォルト値: なし
<code>dns_lookup_kdc</code>	false を指定します。 デフォルト値: false
<code>default_tkt_enctypes</code>	Kerberos 認証に使用する暗号タイプを指定します。このプロパティは、管理サーバの OS が Windows の場合にだけ有効です。 次の暗号タイプを使用できます。 <ul style="list-style-type: none"> • aes128-cts • rc4-hmac • des3-cbc-sha1 • des-cbc-md5

属性	説明
	<ul style="list-style-type: none"> des-cbc-crc 複数指定する場合は、コンマ (,) で区切ってください。 指定した暗号タイプのうち、管理サーバの OS と Kerberos サーバの両方でサポートされているものが使用されます。 デフォルト：なし (DES-CBC-MD5 での認証)
clockskew	管理サーバと Kerberos サーバ間の時刻の差の許容範囲を指定します。この値よりも時刻に差がある場合、認証エラーになります。 指定できる値：0～300 (秒) デフォルト値：300
timeout	Kerberos サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120 (秒) デフォルト値：3
realm_name	レalm識別名を指定します。レalmごとに Kerberos サーバの情報を区別するために付ける任意の名称です。必ず 1 つ以上のレalm識別名を指定してください。レalm識別名を複数指定する場合は、レalm識別名をコンマ (,) で区切って指定します。同じレalm識別名は重複して登録しないでください。 デフォルト値：なし
< realm_name に指定した値 >.realm	Kerberos サーバに設定してあるレalm名を指定します。この項目は必須です。 デフォルト値：なし
< realm_name に指定した値 >.kdc*	Kerberos サーバの情報を次の形式で指定します。 <ホスト名または IP アドレス>[:<ポート番号>] この項目は必須です。 <ホスト名または IP アドレス> ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。 IP アドレスは、IPv4 アドレスで指定してください。IPv6 環境では、ホスト名で指定してください。ただし、ループバックアドレス (localhost または 127.0.0.1) を指定しないでください。 <ポート番号> 指定するポートが Kerberos サーバで待ち受けポート番号として設定されていることを事前に確認してください。ポート番号を省略した場合、または指定したポート番号が Kerberos サーバで使用できないポート番号である場合は、88 を指定したと見なされます。 Kerberos サーバを冗長構成にする場合は、次のようにコンマ (,) で区切って指定します。 <ホスト名または IP アドレス>[:<ポート番号>], <ホスト名または IP アドレス>[:<ポート番号>], ...

注

各属性は、次のように指定します。
 auth.kerberos.<属性>=<値>

注※

外部認可サーバの接続プロトコルに StartTLS を使用する場合は、外部認可サーバのサーバ証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。

表 49 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認証サーバの情報を DNS サーバに照会するとき)

属性	説明
default_realm	デフォルトのレルム名を指定します。GUI のログイン画面でレルム名を省略してユーザー ID を入力した場合に、この項目で指定したレルムに所属するユーザーとして認証されます。この項目は必須です。 デフォルト値：なし
dns_lookup_kdc	true を指定します。この項目は必須です。 ただし、次のすべての属性に値を設定していると、Kerberos サーバは DNS サーバに照会されません。 <ul style="list-style-type: none"> • realm_name • <realm_name に指定した値>.realm • <realm_name に指定した値>.kdc
default_tkt_enctypes	Kerberos 認証に使用する暗号タイプを指定します。このプロパティは、管理サーバの OS が Windows の場合にだけ有効です。 次の暗号タイプを使用できます。 <ul style="list-style-type: none"> • aes128-cts • rc4-hmac • des3-cbc-sha1 • des-cbc-md5 • des-cbc-crc 複数指定する場合は、コンマ (,) で区切ってください。 指定した暗号タイプのうち、管理サーバの OS と Kerberos サーバの両方でサポートされているものが使用されます。 デフォルト：なし (DES-CBC-MD5 での認証)
clockskew	管理サーバと Kerberos サーバ間の時刻の差の許容範囲を指定します。この値よりも時刻に差がある場合、認証エラーになります。 指定できる値：0～300 (秒) デフォルト値：300
timeout	Kerberos サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120 (秒) デフォルト値：3

注

各属性は、次のように指定します。
auth.kerberos.<属性>=<値>

表 50 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認可サーバの設定)

属性	説明
protocol*	LDAP ディレクトリサーバ接続のプロトコルです。 平文による通信の場合は ldap、StartTLS による通信の場合は tls を指定します。Kerberos サーバの情報を直接指定する場合にだけ、StartTLS で通信できます。 tls を指定する場合には、LDAP ディレクトリサーバで次のどれかの暗号方式を使用できることを事前に確認してください。

属性	説明
	<ul style="list-style-type: none"> • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA 指定できる値：ldap または tls デフォルト値：ldap
port	LDAP ディレクトリサーバのポート番号です。指定するポートが、LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
basedn	LDAP ディレクトリサーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認可の対象となります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。 DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。 空白文字 # + ; , < = > ¥ 指定した値は LDAP ディレクトリサーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。 省略した場合は、Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。 デフォルト値：なし
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120 (秒) デフォルト値：15
retry.interval	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60 (秒) デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。 指定できる値：0～50 デフォルト値：20

注

各属性は、次のように指定します。

auth.group.<レルム名>.<属性>=<値>

<レルム名>には auth.kerberos.<realm_name に指定した値>.realm の値を指定します。

注※

LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合には、Hitachi Command Suite 共通コンポーネントのセキュリティ設定が必要です。

表 51 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認可サーバと StartTLS で通信するとき)

プロパティ名	説明
auth.ocsp.enable	LDAP ディレクトリサーバと StartTLS で通信する場合に、OCSP レスポンダーを使用して LDAP ディレクトリサーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を、検証しない場合は false を指定します。 デフォルト値: false
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に、OCSP レスポンダーの URL を指定します。省略した場合は、AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値: なし

4.7.6 Kerberos サーバで認証する場合の exauth.properties ファイルの設定例

Kerberos サーバで認証する場合の exauth.properties ファイルの設定例を次に示します。

- Kerberos サーバの情報を直接指定する場合 (外部認可サーバと連携しないとき)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

- Kerberos サーバを DNS サーバに照会する場合 (外部認可サーバと連携しないとき)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- Kerberos サーバの情報を直接指定する場合 (外部認可サーバとも連携するとき)

```
auth.server.type=kerberos
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- Kerberos サーバを DNS サーバに照会する場合（外部認可サーバとも連携するとき）

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- 冗長構成の場合

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos.example.com:88,kerberos.example.net:88
```

- レalm識別名を複数指定した場合

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1,S2
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos1.example.com:88,kerberos1.example.net:88
auth.kerberos.S2.realm=EXAMPLE.NET
auth.kerberos.S2.kdc=kerberos2.example.com:88,kerberos2.example.net:88
```

4.8 情報検索用のユーザーアカウントとは

情報検索用のユーザーアカウントとは、認証・認可対象のアカウントが存在するか LDAP ディレクトリサーバ内の情報を検索する際に使用されるユーザーアカウントです。

次の運用を行う場合には、管理サーバに情報検索用のユーザーアカウントを登録しておく必要があります。

- LDAP ディレクトリサーバを外部認証サーバとして利用し、データ構造が階層モデルの場合
- LDAP ディレクトリサーバを外部認可サーバとして利用する場合※

上記以外の場合は、認証・認可時にユーザー情報の検索を行わないため、この作業は不要です。すでに登録されている場合は、削除してください。

注※

GUI で認可グループを Hitachi Command Suite 製品に登録する際に、認可グループの Distinguished Name が外部認可サーバに登録されているか確認したい場合、System アカウントなど Hitachi Command Suite 製品に登録されたユーザー ID で操作するためには、情報検索用のユーザーアカウントを管理サーバに登録しておく必要があります。

4.8.1 情報検索用のユーザーアカウントの条件

情報検索用のユーザーアカウントの条件は、認証方式によって異なります。

次の条件を満たすユーザーアカウントを LDAP ディレクトリサーバに準備してください。

認証方式が LDAP の場合

- `exauth.properties` ファイルの `auth.ldap.<auth.server.name に指定した値>.basedn` で指定した DN にバインドできること
- `exauth.properties` ファイルの `auth.ldap.<auth.server.name に指定した値>.basedn` で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- `exauth.properties` ファイルの `auth.ldap.<auth.server.name に指定した値>.basedn` で指定した DN を参照できること
- `exauth.properties` ファイルの `auth.ldap.<auth.server.name に指定した値>.basedn` で指定した DN 下にある認可グループを参照できること (外部認可サーバとも連携するとき)
- `exauth.properties` ファイルの `auth.ldap.<auth.server.name に指定した値>.basedn` で指定した DN 下にある認可グループの属性と、認可グループのネストグループの属性を検索できること (外部認可サーバとも連携するとき)

認証方式が RADIUS の場合

- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN にバインドできること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN を参照できること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN 下にある認可グループを参照できること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN 下にある認可グループの属性と、認可グループのネストグループの属性を検索できること

認証方式が Kerberos の場合

- `exauth.properties` ファイルの `auth.group.<レルム名>.basedn` で指定した DN にバインドできること
- `exauth.properties` ファイルの `auth.group.<レルム名>.basedn` で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- `exauth.properties` ファイルの `auth.group.<レルム名>.basedn` で指定した DN を参照できること
- `exauth.properties` ファイルの `auth.group.<レルム名>.basedn` で指定した DN 下にある認可グループを参照できること
- `exauth.properties` ファイルの `auth.group.<レルム名>.basedn` で指定した DN 下にある認可グループの属性と、認可グループのネストグループの属性を検索できること

4.8.2 情報検索用のユーザーアカウントの登録

hcnds64ldapuser コマンドを実行して、情報検索用のユーザーアカウントを管理サーバに登録します。

前提条件

- LDAP ディレクトリサーバへの情報検索用のユーザーアカウントの登録
- 次の情報の確認
 - 情報検索用ユーザーの DN とパスワード
 - LDAP ディレクトリサーバのサーバ識別名または外部認可サーバ用のドメイン名（認証方式が LDAP の場合）
exauth.properties ファイルの auth.server.name プロパティに指定したサーバ識別名または auth.ldap.<auth.server.name に指定した値>.domain.name プロパティに指定したドメイン名を指定します。
 - RADIUS サーバのドメイン名（認証方式が RADIUS の場合）
exauth.properties ファイルの auth.radius.<auth.server.name に指定した値>.domain.name に指定したドメイン名を指定します。
 - Kerberos サーバのレルム名（認証方式が Kerberos の場合）
exauth.properties ファイルで Kerberos サーバの情報を直接指定した場合は、auth.kerberos.default_realm の値、または auth.kerberos.<auth.kerberos.realm_name 値>.realm の値を指定します。
exauth.properties ファイルで Kerberos サーバの情報を DNS サーバに照会するように設定した場合は、DNS サーバに登録されたレルム名を指定します。

操作手順

1. hcnds64ldapuser コマンドを実行します。

Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>%Base64%bin  
%hcnds64ldapuser /set /dn <情報検索用ユーザーの DN > [/pass <情報検索  
用ユーザーのパスワード>] /name <名前>
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/  
hcnds64ldapuser -set -dn <情報検索用ユーザーの DN > [-pass <情報検索用  
ユーザーのパスワード>] -name <名前>
```

- <情報検索用ユーザーの DN >
DN は RFC4514 の規約に従って指定してください。例えば、次の文字が含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。
空白文字 # + , ; < => ¥
- <情報検索用ユーザーのパスワード>
大文字と小文字の違いも含めて、LDAP ディレクトリサーバに登録しているパスワードと完全に一致している必要があります。pass オプションを省略してコマンドを実行すると、対話形式でパスワードを入力できます。



メモ

- LDAP ディレクトリサーバでは DN やパスワードに引用符 (") を使用できますが、管理サーバには DN およびパスワードに引用符 (") が含まれていないユーザーアカウントを登録してください。
- Active Directory が提供する dsquery コマンドでユーザーの DN を確認できます。dsquery コマンドを使用して、ユーザー「administrator」の DN を確認する場合の実行例と実行結果を次に示します。

```
dsquery user -name administrator
"CN=administrator,CN=admin,DC=example,DC=com"
```
- DN が「cn=administrator,cn=admin,dc=example,com」の場合など、DN にコンマ (,) が含まれる場合は次のように指定します。
Windows の場合：

```
hcnds64ldapuser /set /dn
"cn=administrator,cn=admin,dc=example¥,com" /pass
administrator_pass /name ServerName
```


Linux の場合：

```
hcnds64ldapuser -set -dn
"cn=administrator,cn=admin,dc=example¥¥,com" -pass
administrator_pass -name ServerName
```

関連参照

- [4.11 外部認証サーバとの連携設定に使用するコマンドに関する注意事項](#)

4.8.3 情報検索用のユーザーアカウントの削除

hcnds64ldapuser コマンドを実行して、情報検索用のユーザーアカウントを管理サーバから削除します。

前提条件

次の情報の確認

- LDAP ディレクトリサーバのサーバ識別名または外部認可サーバ用のドメイン名（認証方式が LDAP の場合）
- RADIUS サーバのドメイン名（認証方式が RADIUS の場合）
- Kerberos サーバのレルム名（認証方式が Kerberos の場合）

操作手順

- hcnds64ldapuser コマンドを実行します。

Windows の場合：

```
< Hitachi Command Suite のインストールフォルダ > ¥Base64¥bin
¥hcnds64ldapuser /delete /name <名前>
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/
hcnds64ldapuser -delete -name <名前>
```

関連参照

- [4.11 外部認証サーバとの連携設定に使用するコマンドに関する注意事項](#)

4.8.4 情報検索用ユーザーアカウントを登録済みの LDAP ディレクトリサーバの確認

hcnds64ldapuser コマンドを実行して、情報検索用ユーザーアカウントを管理サーバに登録済みの LDAP ディレクトリサーバを確認します。

操作手順

1. hcnds64ldapuser コマンドを実行します。

Windows の場合：

```
< Hitachi Command Suite のインストールフォルダ >%Base64%\bin  
%hcnds64ldapuser /list
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ >/Base64/bin/  
hcnds64ldapuser -list
```

4.9 共有秘密鍵の登録

hcnds64radiussecret コマンドを実行して、RADIUS サーバの共有秘密鍵 (shared secret) を管理サーバに登録します。

前提条件

次の情報の確認

- 共有秘密鍵
- RADIUS サーバのサーバ識別名
exauth.properties ファイルの auth.server.name プロパティに指定するサーバ識別名と一致している必要があります。

操作手順

1. hcnds64radiussecret コマンドを実行します。

Windows の場合：

```
< Hitachi Command Suite のインストールフォルダ >%Base64%\bin  
%hcnds64radiussecret [/set <共有秘密鍵>] /name <RADIUS サーバのサーバ識別名 >
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ >/Base64/bin/  
hcnds64radiussecret [-set <共有秘密鍵>] -name <RADIUS サーバのサーバ識別名 >
```

- set オプションを省略してコマンドを実行すると、対話形式で共有秘密鍵を入力できます。

関連参照

- [4.11 外部認証サーバとの連携設定に使用するコマンドに関する注意事項](#)

4.9.1 共有秘密鍵の削除

hcmds64radiussecret コマンドを実行して、共有秘密鍵 (shared secret) を削除します。

前提条件

次の情報の確認

- RADIUS サーバのサーバ識別名

操作手順

1. hcmds64radiussecret コマンドを実行します。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ >¥Base64¥bin  
¥hcmds64radiussecret /delete /name < RADIUS サーバのサーバ識別名 >
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/  
hcmds64radiussecret -delete -name < RADIUS サーバのサーバ識別名 >
```

関連参照

- [4.11 外部認証サーバとの連携設定に使用するコマンドに関する注意事項](#)

4.9.2 共有秘密鍵が登録されている RADIUS サーバの確認

hcmds64radiussecret コマンドを実行して、共有秘密鍵 (shared secret) を管理サーバに登録済みの RADIUS サーバを確認します。

操作手順

1. hcmds64radiussecret コマンドを実行します。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ >¥Base64¥bin  
¥hcmds64radiussecret /list
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/  
hcmds64radiussecret -list
```

操作結果

RADIUS サーバのサーバ識別名が表示されます。

関連参照

- [4.11 外部認証サーバとの連携設定に使用するコマンドに関する注意事項](#)

4.10 外部認証サーバおよび外部認可サーバとの接続確認

hcnds64checkauth コマンドを実行して、管理サーバから外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。Tuning Manager とリモート接続している場合は、Device Manager サーバがインストールされているマシンで実行してください。

前提条件

- 外部認証サーバと外部認可サーバの登録
- 次の情報の確認
 - 認証方式が LDAP の場合
LDAP ディレクトリサーバに登録されているユーザーアカウントを確認してください。ユーザー ID は、exauth.properties ファイルの auth.ldap.<auth.server.name に指定した値>.attr で指定した属性に格納されている値を指定してください。
 - 認証方式が RADIUS の場合
RADIUS サーバに登録されているユーザーアカウントを確認してください。
 - 認証方式が Kerberos の場合
外部認証サーバとだけ連携する場合：
Hitachi Command Suite 製品に登録されていて、かつ認証方式が Kerberos のユーザーアカウントを確認してください。
外部認可サーバとも連携する場合：
Hitachi Command Suite 製品に登録されていないユーザーアカウントを確認してください。
なお、exauth.properties ファイルの default_realm で設定したレルム名とは異なるレルムに所属するユーザーを指定する場合、ユーザーが所属するレルムも確認してください。exauth.properties ファイルでレルム名を複数指定した場合、指定したレルム名をすべて確認してください。
なお、ユーザー ID またはパスワードの先頭に、Windows の場合はスラント (/)、Linux の場合はハイフン (-) が含まれるユーザーアカウントは使用できません。

操作手順

- hcnds64checkauth コマンドを実行します。

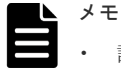
Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>%Base64%bin  
%hcnds64checkauth [/user <ユーザー ID > /pass <パスワード>] [/summary]
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/  
hcnds64checkauth [-user <ユーザー ID > -pass <パスワード>] [-summary]
```

- 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。
- summary オプションを指定すると、コマンド実行時に表示される確認メッセージが簡略化されます。



メモ

- ・ 認証方式が Kerberos の場合、`exauth.properties` ファイルでレルム名を複数指定したときは、レルムごとに接続確認してください。また、ユーザー ID は次の形式で指定してください。
 - ・ `exauth.properties` ファイルの `default_realm` で設定したレルム名とは異なるレルムに所属するユーザーを指定する場合：
＜ユーザー ID＞@＜レルム名＞
 - ・ `exauth.properties` ファイルの `default_realm` で設定したレルムに所属するユーザーを指定する場合：
レルム名を省略して入力できます。
- ・ 認証方式が LDAP でマルチドメイン構成の場合、`hcnds64checkauth` コマンドを実行すると、連携しているすべての外部認証サーバに対してチェックし外部認証サーバごとにチェック結果が表示されます。
`hcnds64checkauth` コマンドで指定したユーザーアカウントが登録されていない外部認証サーバでは、チェック結果のフェーズ 3 でユーザーアカウントが登録されていないことを示すエラーメッセージが表示され、フェーズ 3 での確認で失敗することがあります。
この場合、接続確認したい外部認証サーバごとに、外部認証サーバに登録されているユーザーアカウントで確認してください。

操作結果

`exauth.properties` ファイルの設定や、外部認証サーバおよび外部認可サーバとの接続状況がチェックされ、結果がフェーズごとに表示されます（全 4 フェーズ）。各フェーズでの確認が正常に終了した場合、次のメッセージが表示されます。

```
KAPM15004-I The result of the configuration check of Phase <phase-number> was normal.
```

フェーズ 1

`exauth.properties` ファイルの共通のプロパティが正しく設定されているかチェックします。

フェーズ 2

`exauth.properties` ファイルの外部認証サーバと外部認可サーバのプロパティが正しく設定されているかチェックします。

フェーズ 3

外部認証サーバに接続できるかチェックします。

フェーズ 4

外部認可サーバとも連携するよう設定されている場合に、外部認可サーバに接続できるか、および認可グループを検索できるかをチェックします。

エラーが発生した場合は、マニュアル「*Hitachi Command Suite* メッセージ」で出力されたメッセージ ID を検索し、要因や対処方法を確認してください。

関連参照

- ・ [4.7 外部認証サーバと外部認可サーバの登録](#)
- ・ [4.11 外部認証サーバとの連携設定に使用するコマンドに関する注意事項](#)

4.11 外部認証サーバとの連携設定に使用するコマンドに関する注意事項

外部認証サーバと連携するための設定で実行するコマンドの引数に、コマンドラインの制御文字が含まれる場合には、コマンドラインの仕様に従い正しくエスケープしてください。

また、円記号 (¥) はコマンドラインでは特殊な扱いとなるため、引数に円記号 (¥) が含まれる場合には注意が必要です。

hcnds64ldapuser コマンド、hcnds64radiussecret コマンド、および hcnds64checkauth コマンドを実行する際のエスケープ方法は次のとおりです。

Windows の場合：

次の文字が含まれる場合は、引数を引用符 (") で囲むか、1文字ごとにアクサンシルコンプレックス (^) でエスケープしてください。

空白文字 & | ^ < > ()

円記号 (¥) は、次に続く文字によってはエスケープ文字として扱われることがあります。このため、引数に円記号 (¥) と上記の文字が含まれる場合には、引用符 (") で囲まないで、上記文字を1文字ごとにアクサンシルコンプレックス (^) でエスケープしてください。

また、引数の末尾に円記号 (¥) がある場合は、円記号 (¥) でエスケープしてください。

Linux の場合：

次の文字が含まれる場合は、引数を引用符 (") で囲むか、1文字ごとに円記号 (¥) でエスケープしてください。

空白文字 # & ' () ~ ¥ ` < > ; |

ただし、円記号 (¥) は、引用符 (") で囲われていてもエスケープ文字として扱われます。引数に円記号 (¥) が含まれる場合には、必ず円記号 (¥) でエスケープしてください。

例えば、hcnds64radiussecret コマンドで登録する共有秘密鍵が「secret01¥」の場合は、次のとおりエスケープしてください。

Windows の場合：

```
hcnds64radiussecret /set secret01¥¥ /name ServerName
```

Linux の場合：

次のどちらかの形式で指定してください。

```
hcnds64radiussecret -set secret01¥¥ -name ServerName
```

```
hcnds64radiussecret -set "secret01¥¥" -name ServerName
```

4.12 Kerberos 認証に使用できる暗号タイプ

Hitachi Command Suite 製品でサポートされている暗号タイプを使用できるように Kerberos サーバを構築してください。

Hitachi Command Suite 製品で、Kerberos 認証に使用できる暗号タイプ (encryption types) は次のとおりです。

- AES256-CTS-HMAC-SHA1-96
- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC

- DES3-CBC-SHA1
- DES-CBC-CRC
- DES-CBC-MD5

通信に関するセキュリティ設定

この章では、Hitachi Command Suite 製品で利用できる通信に関するセキュリティ設定について説明します。

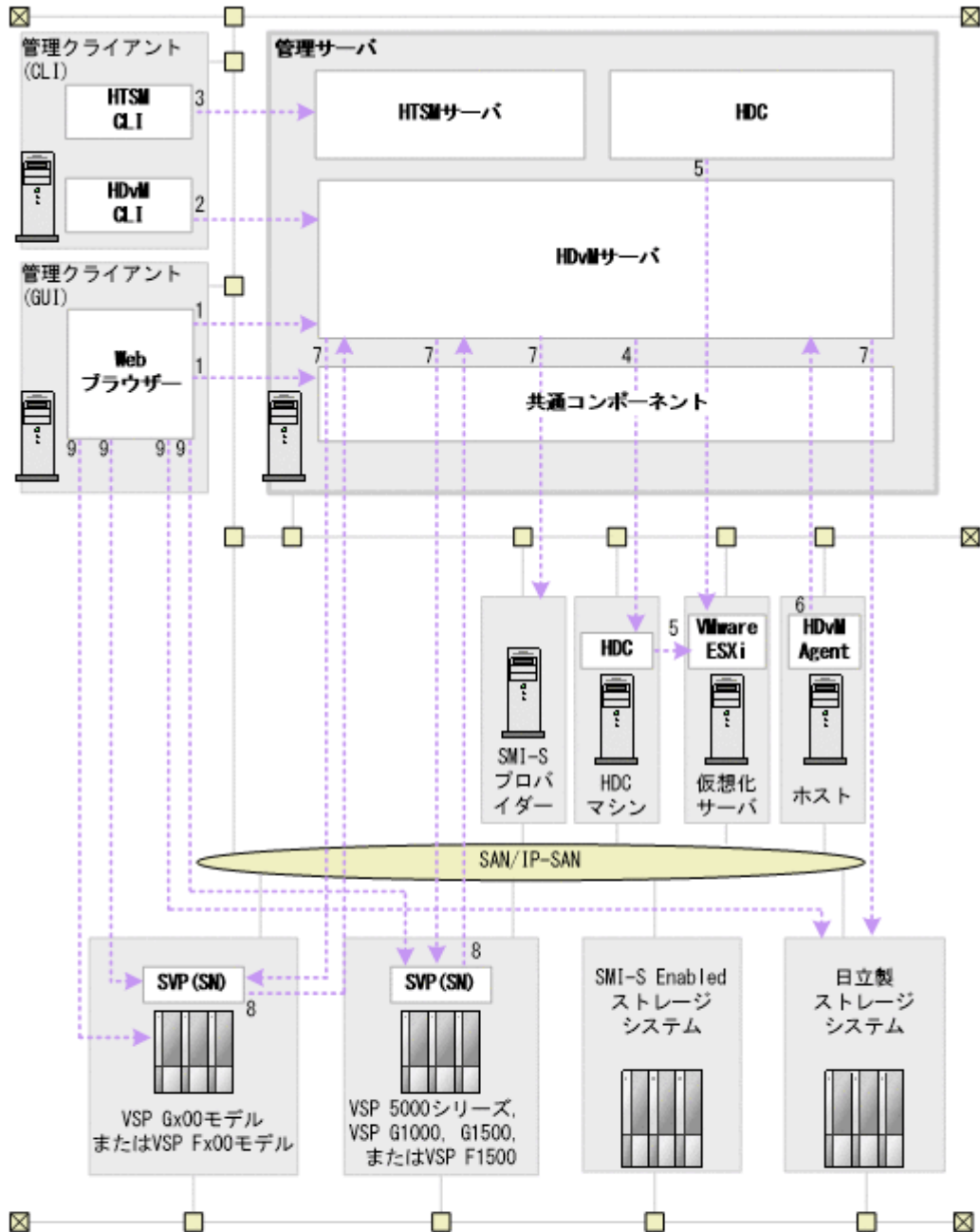
- 5.1 Device Manager および Tiered Storage Manager のセキュリティ通信路
- 5.2 SSL サーバの構築 (Hitachi Command Suite 共通コンポーネント)
- 5.3 SSL サーバの構築 (Device Manager サーバ)
- 5.4 SSL サーバの構築 (Host Data Collector)
- 5.5 SSL クライアントの構築
- 5.6 SSL サーバおよび SSL クライアントの構築 (CIM サーバ)
- 5.7 SSL サーバおよび SSL クライアントの構築 (CIM クライアント)

5.1 Device Manager および Tiered Storage Manager のセキュリティ通信路

Device Manager および Tiered Storage Manager ではマシン間でセキュリティ通信を利用できません。

Device Manager および Tiered Storage Manager のセキュリティ通信路について、次の 2 つの図に示します。

図 27 Device Manager および Tiered Storage Manager のセキュリティ通信路 (1/2)



(凡例)

---▶ : SSLクライアントからSSLサーバへの接続

HDvM : Hitachi Device Manager

HTSM : Hitachi Tiered Storage Manager

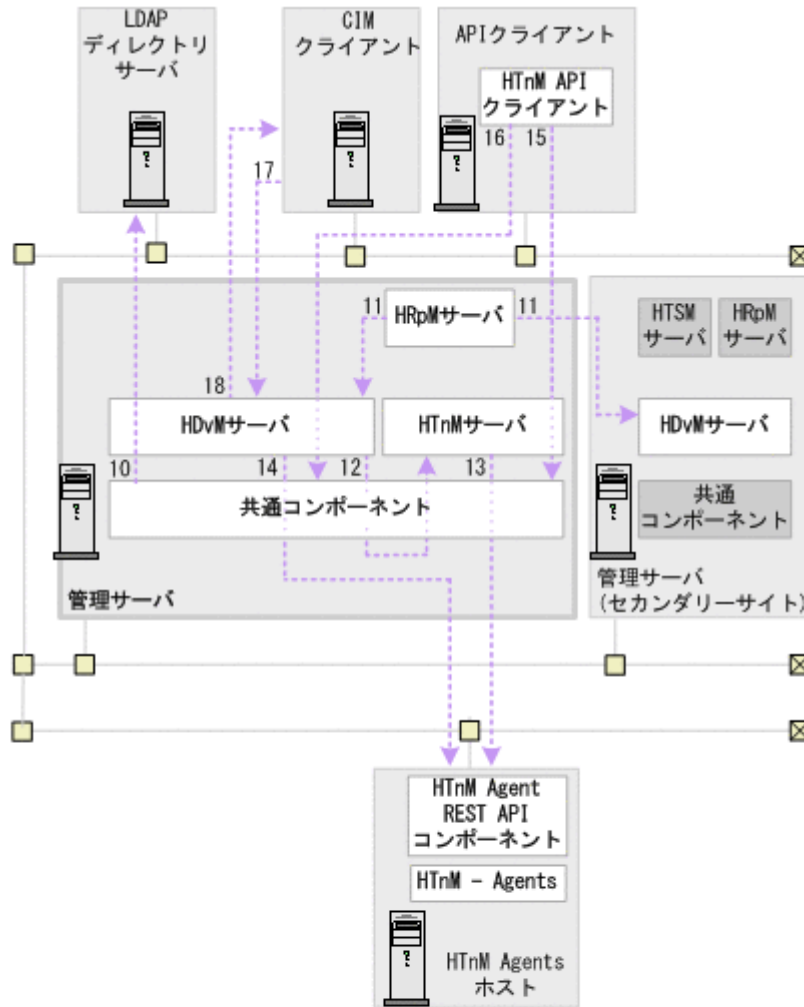
共通コンポーネント : Hitachi Command Suite共通コンポーネント

HDC : Host Data Collector

HDvM Agent : Device Managerエージェント

SN : Storage Navigator

図 28 Device Manager および Tiered Storage Manager のセキュリティ通信路 (2/2)



(凡例)

---> : SSLクライアントからSSLサーバへの接続

HDvM : Hitachi Device Manager

HTSM : Hitachi Tiered Storage Manager

HRpM : Hitachi Replication Manager

HTnM : Hitachi Tuning Manager

共通コンポーネント : Hitachi Command Suite共通コンポーネント

Device Manager および Tiered Storage Manager で利用できるセキュリティ通信路について、次に示します。表中の項番は、図中の番号と対応しています。

表 52 Device Manager および Tiered Storage Manager で利用できるセキュリティ通信路

項番	SSL サーバ	SSL クライアント	備考
1	管理サーバ <ul style="list-style-type: none"> Hitachi Command Suite 共通コンポーネント Device Manager サーバ 	管理クライアント (GUI)	-

項番	SSL サーバ	SSL クライアント	備考
2	管理サーバ (Device Manager サーバ)	管理クライアント (Device Manager CLI)	-
3	管理サーバ (Tiered Storage Manager サーバ)	管理クライアント (Tiered Storage Manager CLI)	-
4	Host Data Collector マシン	管理サーバ (Device Manager サーバ)	-
5	仮想化サーバ	Host Data Collector マシン	-
6	管理サーバ (Device Manager サーバ)	Device Manager エージェントマシン	-
7	ストレージシステム <ul style="list-style-type: none"> • VSP 5000 シリーズ • VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 モデル • VSP Fx00 モデル • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • HUS VM • HUS100 • Hitachi AMS2000 • Hitachi SMS • SMI-S enabled ストレージシステム (SMI-S プロバイダー) 	管理サーバ (Device Manager サーバ)	VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP および HUS VM との通信は常にセキュリティ通信が使用されます。 管理サーバ (Device Manager サーバ) は TLS バージョン 1.0, TLS バージョン 1.1, または, TLS バージョン 1.2 を利用可能です。 セキュリティ通信で使用するプロトコルは, ストレージシステムによって利用できる条件が異なります。詳細は, 各ストレージシステムのマニュアルを参照してください。また, HUS100, Hitachi AMS2000, および Hitachi SMS とのセキュリティ通信で, TLS バージョン 1.2 を利用したい場合は, Device Manager のバージョンが 8.6.1-01 以降である必要があります。
8	管理サーバ (Device Manager サーバ)	ストレージシステム (VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデル)	次の場合は Device Manager サーバとストレージシステム (VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデル) 間でセキュリティ通信を利用するための設定が必要です。 <ul style="list-style-type: none"> • VSP G1000, G1500 または VSP F1500 で, RAID Manager および SVP へのログイン時に Hitachi Command Suite でユーザーアカウントを認証する場合 • VSP 5000 シリーズを操作する場合

項番	SSL サーバ	SSL クライアント	備考
			<ul style="list-style-type: none"> VSP Gx00 モデルまたは VSP Fx00 モデルを操作する場合 VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルの場合、デフォルトではセキュリティ通信の設定が有効になります。
9	ストレージシステム	管理クライアント (GUI)	<p>Device Manager GUI から Storage Navigator, Storage Navigator Modular 2, または maintenance utility を使用する場合に、管理クライアントの Web ブラウザーとストレージシステム間でセキュリティ通信を利用できます。ストレージシステムが VSP Gx00 モデルまたは VSP Fx00 モデルの場合、管理クライアント (GUI) から、SVP またはコントローラーに対するセキュリティ通信を利用できます。デフォルトではセキュリティ通信の設定が有効になります。</p>
10	LDAP ディレクトリサーバ	管理サーバ (Hitachi Command Suite 共通コンポーネント)	-
11	Device Manager サーバ	Replication Manager サーバ	複数サイト構成の場合でも、各副サイト (Device Manager サーバ) と正サイト (Replication Manager サーバ) 間でセキュリティ通信を利用できます。
12	Tuning Manager サーバ	Device Manager サーバ	Device Manager サーバと Tuning Manager サーバが同じ管理サーバにインストールされている場合にセキュリティ通信を利用できます。Device Manager サーバと Tuning Manager サーバが異なる管理サーバにインストールされている場合については、マニュアル「 <i>Hitachi Command Suite Tuning Manager 運用管理ガイド</i> 」の SSL の設定について説明している箇所を参照してください。
13	Tuning Manager Agents	Tuning Manager サーバ	<ul style="list-style-type: none"> Tuning Manager API の利用時にセキュリティ通信を利用できます。 「図 28 Device Manager および Tiered Storage Manager のセキュリティ通信路 (2/2)」の Tuning Manager Agent REST API コンポーネントは、Tuning Manager API の使用時に必要なコンポーネントで、Tuning Manager - Agent REST Web Service と Tuning Manager - Agent REST Application Service の総称です。 セキュリティ通信の設定手順については、マニュアル「<i>Hitachi Command Suite Tuning Manager - Agents</i>」の SSL の設定について説明している箇所を参照してください。
14	Tuning Manager Agents	Device Manager サーバ	<ul style="list-style-type: none"> Tuning Manager のアラート機能の使用時にセキュリティ通信を利用できます。Device Manager サーバと Tuning Manager サーバが同じ管理サーバにインストールされている場合は、項番 13 と同じ経路になるため項番 13 を設定していれば、追加の設定は不要です。

項番	SSL サーバ	SSL クライアント	備考
			<ul style="list-style-type: none"> セキュリティ通信の設定手順については、マニュアル「<i>Hitachi Command Suite Tuning Manager - Agents</i>」の SSL の設定について説明している個所を参照してください。
15	Tuning Manager サーバ	Tuning Manager API クライアント	Device Manager サーバと Tuning Manager サーバが異なる管理サーバにインストールされている場合のセキュリティ通信の設定手順については、マニュアル「 <i>Hitachi Command Suite Tuning Manager 運用管理ガイド</i> 」の SSL の設定について説明している個所を参照してください。
16	Device Manager サーバ	Tuning Manager API クライアント	<ul style="list-style-type: none"> Tuning Manager のアラート機能の使用時にセキュリティ通信を利用できます。Device Manager サーバと Tuning Manager サーバが同じ管理サーバにインストールされている場合は、項番 15 と同じ経路になるため項番 15 を設定していれば、追加の設定は不要です。 Device Manager サーバと Tuning Manager サーバが異なる管理サーバにインストールされている場合のセキュリティ通信の設定手順については、マニュアル「<i>Hitachi Command Suite Tuning Manager 運用管理ガイド</i>」の SSL の設定について説明している個所を参照してください。
17	管理サーバ (Device Manager サーバ)	CIM クライアント	オブジェクト操作でセキュリティ通信を利用できます。さらにセキュリティを強化するために、相互認証を設定することもできます。
18	CIM クライアント	管理サーバ (Device Manager サーバ)	インディケーション通知でセキュリティ通信を利用できます。さらにセキュリティを強化するために、相互認証を設定することもできます。

(凡例)

- : 該当なし

5.1.1 Device Manager サーバのデフォルトの証明書

Device Manager のバージョン 8.1.3 以降では、Device Manager を新規インストールした場合、または Device Manager サーバの証明書が存在しない状態でアップグレードインストールをした場合、デフォルトの証明書がキーストアーに登録され、SSL/TLS 通信の設定が有効になります。

デフォルトの証明書は、ストレージシステム (VSP G1000, G1500, VSP F1500, VSP Gx00 モデルおよび VSP Fx00 モデル) と Hitachi Command Suite の間でユーザーアカウント認証の連携をする際の通信路を暗号化するための自己署名証明書です。HiKeytool を使って証明書の内容を表示し、セキュリティの要件を満たしているか確認してください。よりセキュリティを高めるために別の自己署名証明書または認証局の署名済みの証明書を使用する場合は、デフォルトの証明書を削除して SSL/TLS 通信の設定をやり直してください。

ストレージシステム (VSP G1000, G1500, VSP F1500, VSP Gx00 モデルおよび VSP Fx00 モデル) 以外のコンポーネントと Device Manager サーバ間でセキュリティ通信を利用する場合は、デフォルトの証明書を削除して SSL/TLS 通信の設定をやり直してください。



メモ

- デフォルトの証明書の内容を確認する、またはキーストアーから削除するには、HiKeytool を使用してください。
 - デフォルトの証明書を Device Manager サーバの通信相手のトラストストアにインポートしないでください。インポートした場合、通信に失敗します。
-

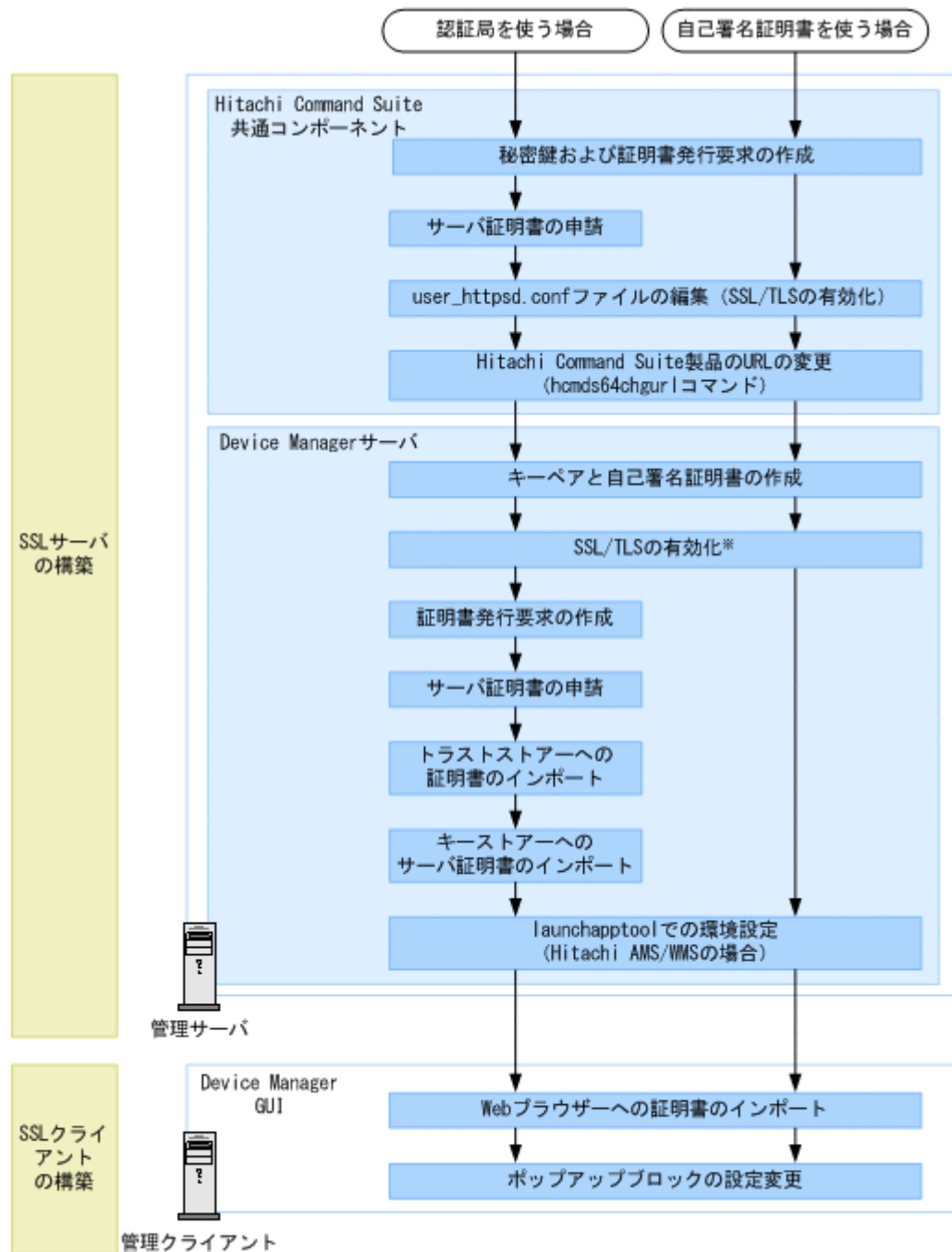
関連タスク

- [5.3.7 Device Manager サーバのキーペア情報の参照 \(詳細モード\)](#)
- [5.3.8 Device Manager サーバのキーストアーからのキーペアの削除](#)

5.1.2 管理サーバと管理クライアント（GUI）間のセキュリティ通信のための操作フロー

管理サーバで Hitachi Command Suite 共通コンポーネントと Device Manager サーバのサーバ証明書を作成し、管理クライアント（GUI）の Web ブラウザーにインポートする必要があります。

図 29 管理サーバと管理クライアント（GUI）間のセキュリティ通信のための操作フロー



注※ デフォルトではSSL/TLSが有効に設定されます。



メモ

- Device Manager サーバでのサーバ証明書の作成およびインポートは、Device Manager GUI の Element Manager から Storage Navigator や Storage Navigator Modular 2 を使用しない場合には不要です。

- Web ブラウザーへ証明書をインポートする際に、著名な認証局を使用する場合、証明書が Web ブラウザーにすでにインポートされていることもあります。その場合、証明書を改めてインポートする必要はありません。
 - SSL/TLS 通信で使用する暗号方式を制限したい場合は、Device Manager サーバの `server.properties` ファイルにある `server.https.enabledCipherSuites` プロパティの値を変更してください。
-

関連概念

- [5.2 SSL サーバの構築 \(Hitachi Command Suite 共通コンポーネント\)](#)
- [5.3 SSL サーバの構築 \(Device Manager サーバ\)](#)
- [5.5 SSL クライアントの構築](#)

関連タスク

- [2.8 Hitachi Command Suite 製品の URL の変更 \(hcmds64chgurl コマンド\)](#)
- [6.1.2 Element Manager を使用するための設定](#)
- [付録 A.1.1 Device Manager サーバのプロパティの変更](#)

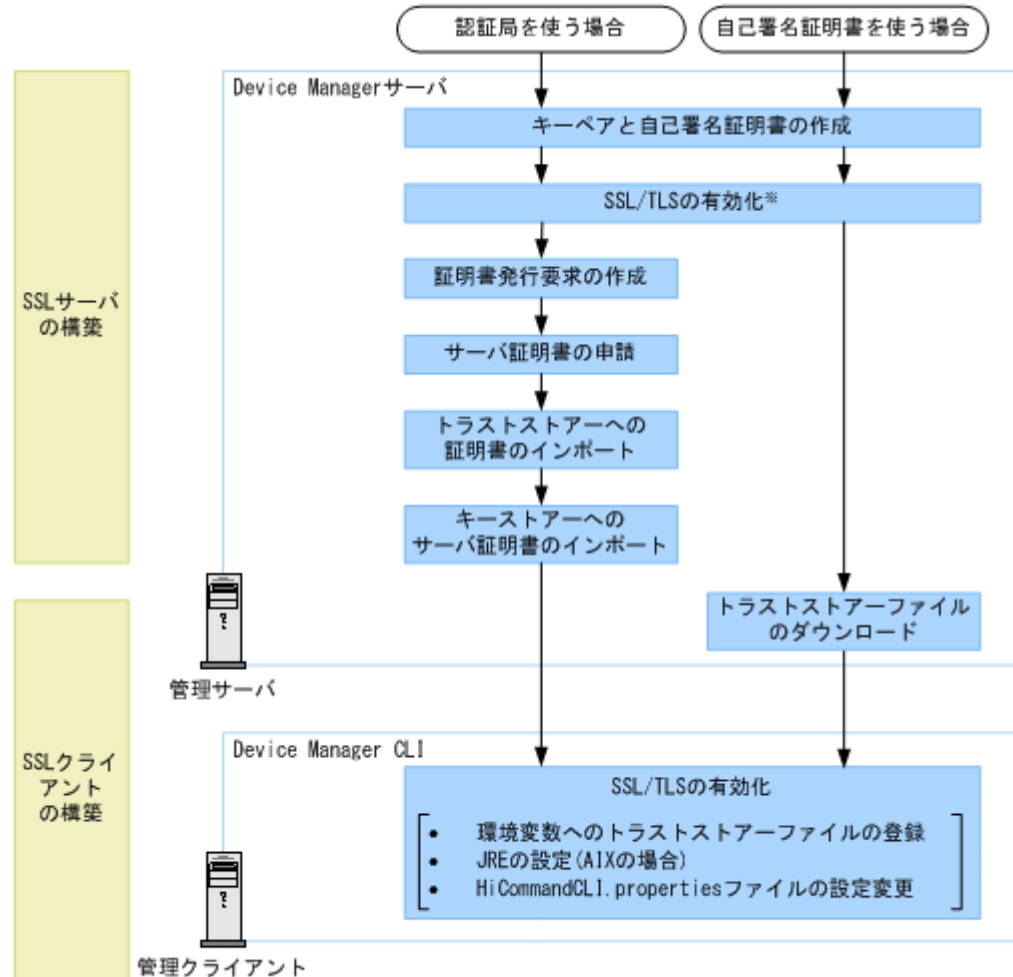
関連参照

- [付録 A.8.6 server.https.enabledCipherSuites](#)

5.1.3 管理サーバと管理クライアント (Device Manager CLI) 間のセキュリティ通信のための操作フロー

管理サーバで Device Manager サーバのサーバ証明書を作成し、管理クライアント (Device Manager CLI) で SSL/TLS を有効化する必要があります。

図 30 管理サーバと管理クライアント (Device Manager CLI) 間のセキュリティ通信のための操作フロー



注※ デフォルトではSSL/TLSが有効に設定されます。



メモ

SSL/TLS 通信で使用する暗号方式を制限したい場合は、Device Manager サーバの `server.properties` ファイルにある `server.https.enabledCipherSuites` プロパティの値を変更してください。

関連概念

- [5.3 SSL サーバの構築 \(Device Manager サーバ\)](#)
- [5.5 SSL クライアントの構築](#)

関連タスク

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

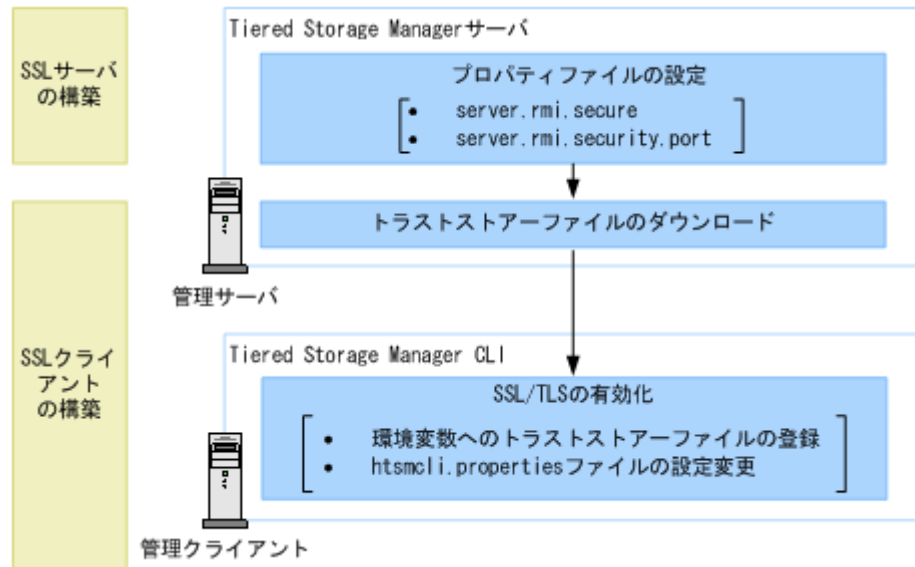
関連参照

- [付録 A.8.6 server.https.enabledCipherSuites](#)

5.1.4 管理サーバと管理クライアント（Tiered Storage Manager CLI）間のセキュリティ通信のための操作フロー

管理サーバと管理クライアント（Tiered Storage Manager CLI）間の SSL/TLS 通信には、Tiered Storage Manager サーバに同梱された自己署名証明書を使用します。管理サーバで Tiered Storage Manager サーバのプロパティを設定し、管理クライアント（Tiered Storage Manager CLI）で SSL/TLS を有効化する必要があります。

図 31 管理サーバと管理クライアント（Tiered Storage Manager CLI）間のセキュリティ通信のための操作フロー



メモ

SSL/TLS 通信で使用する暗号方式を制限したい場合は、Tiered Storage Manager サーバの `server.properties` ファイルにある `server.rmi.secure` プロパティの値を変更してください。

関連概念

- 5.5 SSL クライアントの構築

関連タスク

- 付録 B.1.1 Tiered Storage Manager サーバのプロパティの変更

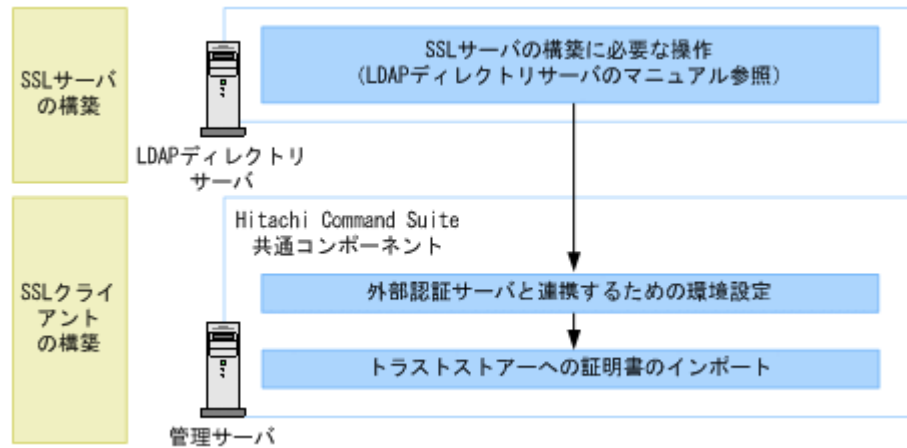
関連参照

- 付録 B.6.1 `server.rmi.secure`
- 付録 B.2.2 `server.rmi.security.port`
- 付録 B.6.2 `server.rmi.security.enabledCipherSuites`

5.1.5 LDAP ディレクトリサーバと管理サーバ間のセキュリティ通信のための操作フロー

管理サーバで外部認証サーバと連携するための設定をしたあと、証明書をトラストストア（ldapcacerts）にインポートする必要があります。

図 32 LDAP ディレクトリサーバと管理サーバ間のセキュリティ通信のための操作フロー



なお、LDAP ディレクトリサーバのサーバ証明書が著名な認証局で発行されている場合は、認証局の証明書がトラストストア（jssecacerts）にすでにインポートされていることがあります。その場合、証明書を改めて ldapcacerts にインポートする必要はありません。

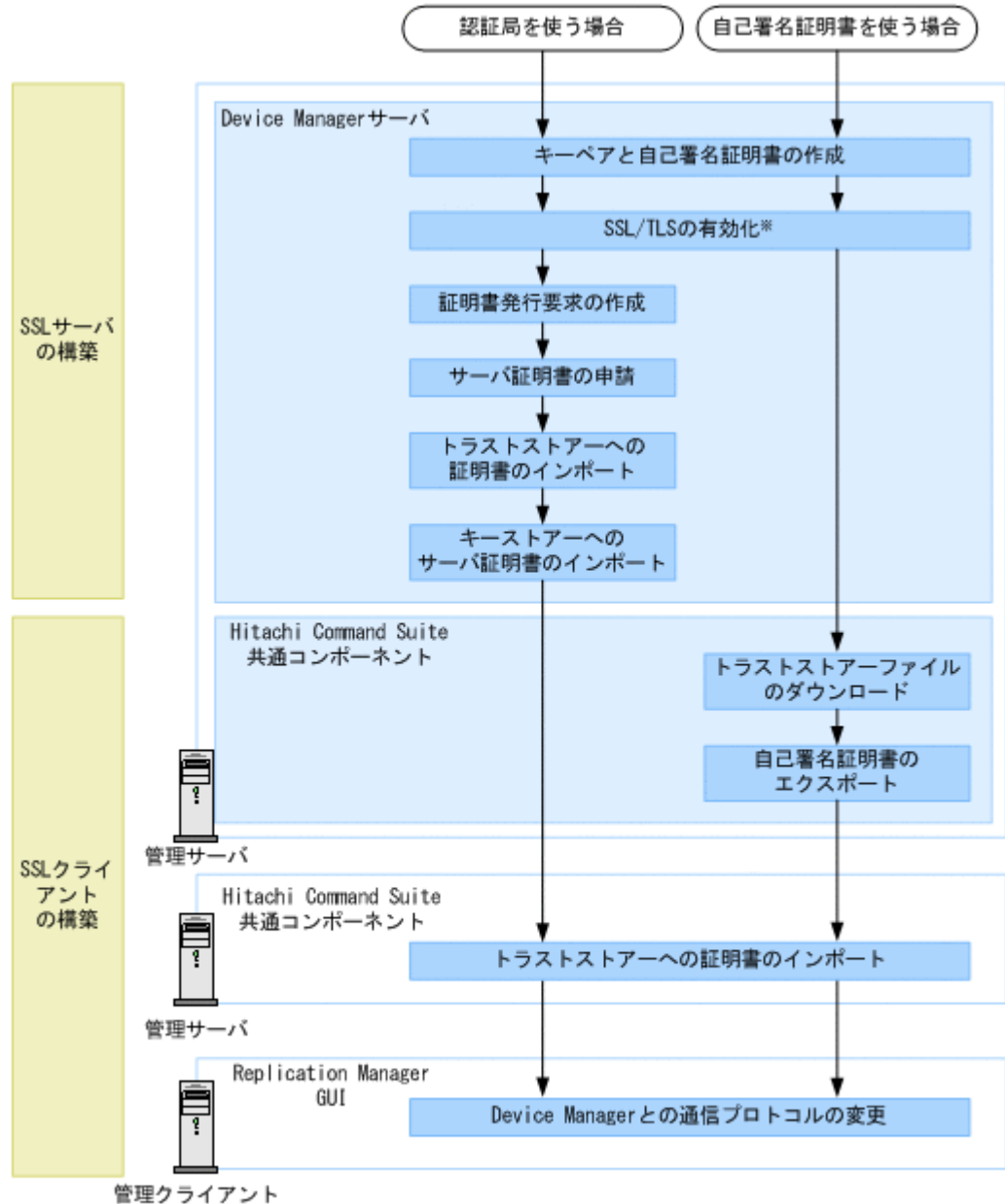
関連概念

- [4.3.1 LDAP ディレクトリサーバでユーザー認証するための操作フロー](#)
- [5.5 SSL クライアントの構築](#)

5.1.6 Device Manager サーバと Replication Manager サーバ間のセキュリティ通信のための操作フロー

管理サーバで Device Manager サーバのサーバ証明書を作成し、トラストストア（jssecacerts）にインポートします。

図 33 Device Manager サーバと Replication Manager サーバ間のセキュリティ通信のための操作フロー



注※ デフォルトではSSL/TLSが有効に設定されます。

なお、著名な認証局を使用する場合、認証局の証明書がトラストストア（jssecacerts）にすでにインポートされていることもあります。その場合、証明書を改めてインポートする必要はありません。



メモ

- SSL/TLS 通信で使用する暗号方式を制限したい場合は、Device Manager サーバの `server.properties` ファイルにある `server.https.enabledCipherSuites` プロパティの値を変更してください。

- 複数サイト構成の場合は、各副サイトで作成した Device Manager サーバのサーバ証明書を正サイトに安全な方法で転送し、トラストストア（jssecacerts）にインポートします。

関連概念

- [5.3 SSL サーバの構築（Device Manager サーバ）](#)
- [5.5 SSL クライアントの構築](#)

関連タスク

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

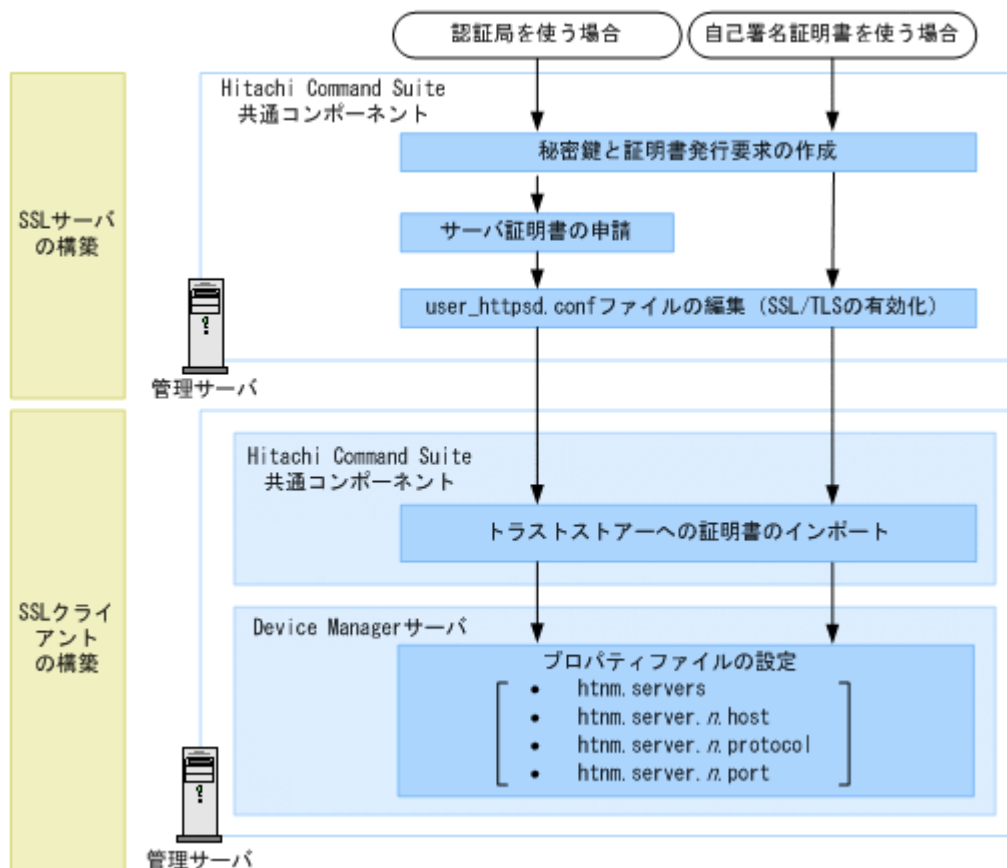
関連参照

- [付録 A.8.6 server.https.enabledCipherSuites](#)

5.1.7 Tuning Manager サーバと Device Manager サーバ間のセキュリティ通信のための操作フロー

管理サーバで Hitachi Command Suite 共通コンポーネントのサーバ証明書を作成し、トラストストア（jssecacerts）にインポートします。

図 34 Tuning Manager サーバと Device Manager サーバ間のセキュリティ通信のための操作フロー



なお、著名な認証局を使用する場合、証明書がトラストストア（jssecacerts）にすでにインポートされていることもあります。その場合、証明書を改めてインポートする必要はありません。

関連概念

- [5.2 SSL サーバの構築（Hitachi Command Suite 共通コンポーネント）](#)

- ・ 5.5 SSL クライアントの構築

関連タスク

- ・ 付録 A.1.1 Device Manager サーバのプロパティの変更

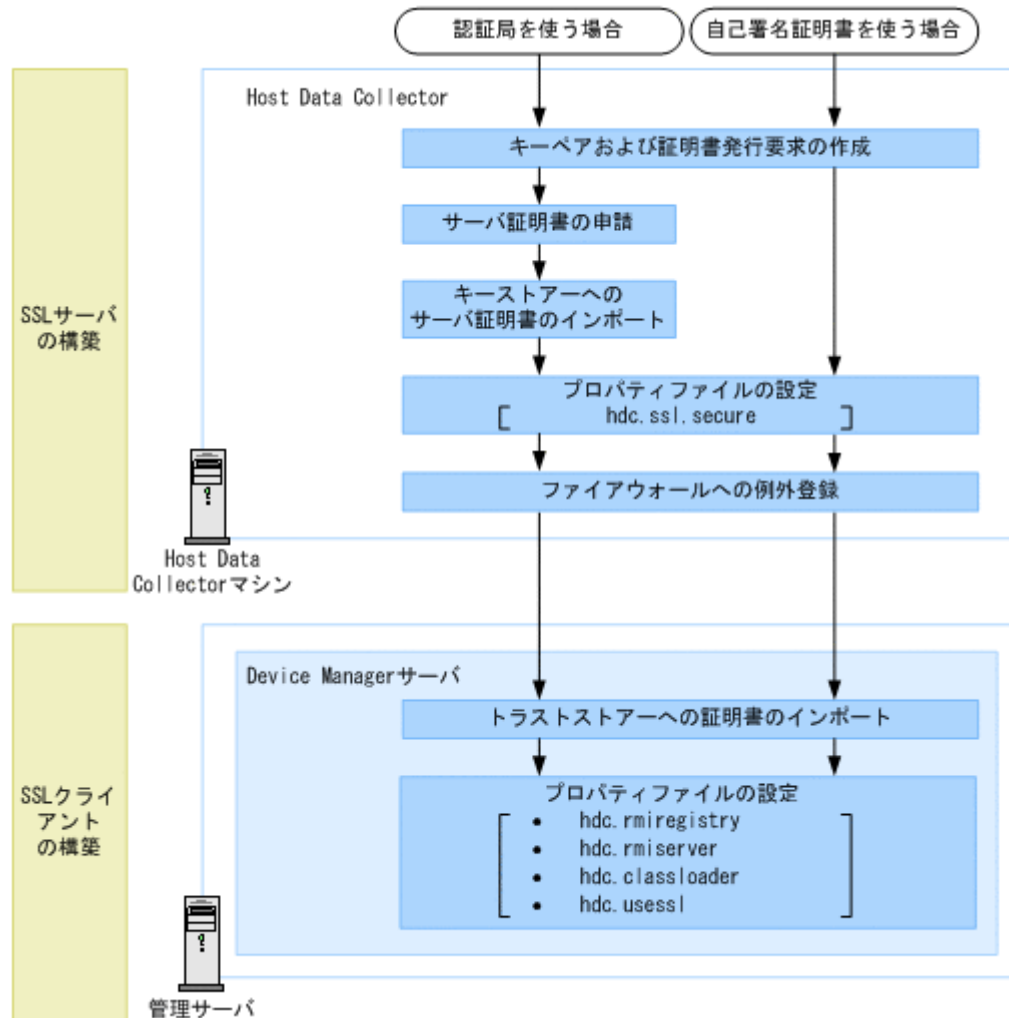
関連参照

- ・ 付録 A.14.2 htnm.servers
- ・ 付録 A.14.3 htnm.server.n.host
- ・ 付録 A.14.4 htnm.server.n.protocol
- ・ 付録 A.14.5 htnm.server.n.port

5.1.8 Host Data Collector マシンと管理サーバ間のセキュリティ通信のための操作フロー

Host Data Collector マシンで Host Data Collector のサーバ証明書を作成し、トラストストア (dvmcacerts) にインポートします。

図 35 Host Data Collector マシンと管理サーバ間のセキュリティ通信のための操作フロー



メモ

- ・ SSL/TLS 通信で使用する暗号方式を制限したい場合は、Host Data Collector の `hdcbase.properties` ファイルにある `hdc.ssl.ciphers` プロパティの値を変更してください。

- Host Data Collector がインストールされたマシンが複数台ある場合は、管理サーバと全 Host Data Collector マシンとの通信プロトコル (SSL/非 SSL) を合わせる必要があります。
 - Host Data Collector の Java の実行環境を変更している場合は、使用する Java の実行環境のバージョンに応じた Java Cryptography Extension (JCE) の無制限強度の管轄ポリシーファイル (Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files) をダウンロードし、インストールする必要があります。
管轄ポリシーファイルは、Oracle 社の Web サイトからダウンロードしてください。インストール方法は、管轄ポリシーファイルに付属するドキュメントを参照してください。
-

関連概念

- [2.4 Host Data Collector でのファイアウォールへの例外登録 \(Windows\)](#)
- [5.4 SSL サーバの構築 \(Host Data Collector\)](#)

関連タスク

- [5.3.11 Device Manager サーバのトラストストアへの証明書のインポート](#)
- [付録 A.1.1 Device Manager サーバのプロパティの変更](#)
- [付録 C.1.1 Host Data Collector のプロパティの変更](#)

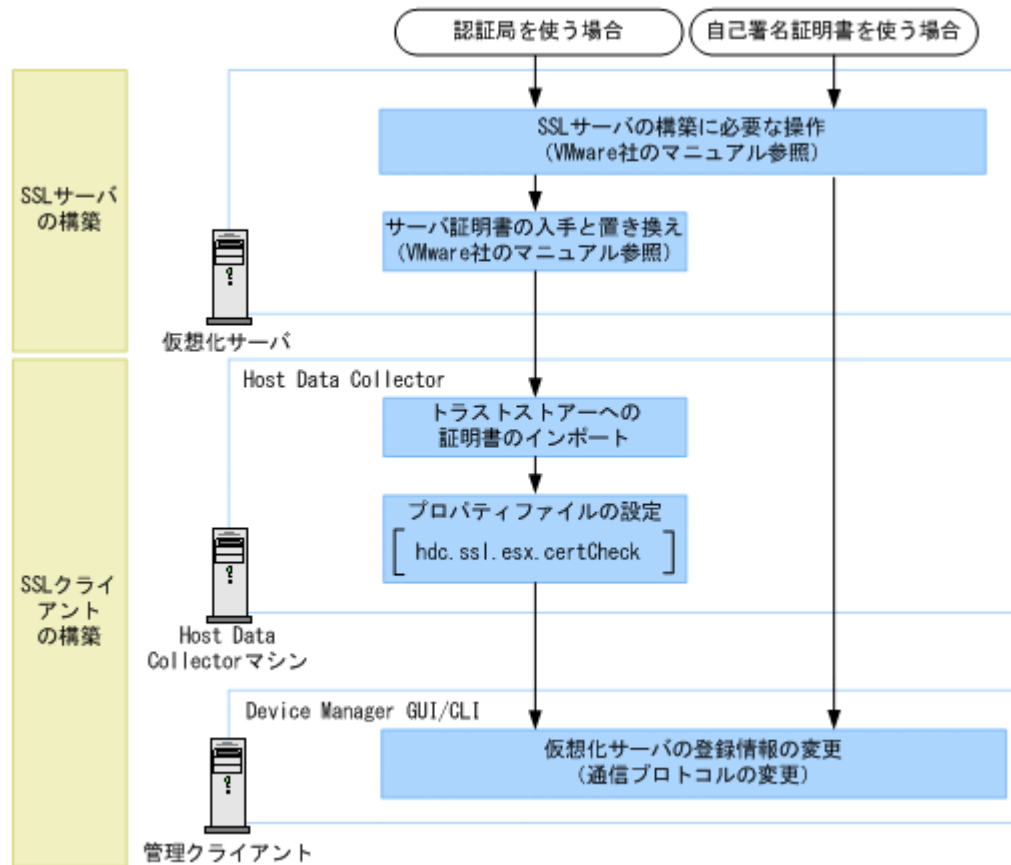
関連参照

- [付録 A.12.2 hdc.rmiregistry](#)
- [付録 A.12.3 hdc.rmiserver](#)
- [付録 A.12.4 hdc.classloader](#)
- [付録 A.12.5 hdc.usessl](#)
- [付録 C.2.13 hdc.ssl.secure](#)
- [付録 C.5.1 hdc.ssl.ciphers](#)

5.1.9 仮想化サーバと Host Data Collector 間のセキュリティ通信のための操作フロー

仮想化サーバで SSL サーバを構築したあと、Device Manager の GUI または CLI で仮想化サーバとの通信プロトコルを変更する必要があります。

図 36 仮想化サーバと Host Data Collector 間のセキュリティ通信のための操作フロー



メモ

デフォルトでは、仮想化サーバと Host Data Collector 間は、自己署名証明書を使用して SSL で通信する設定になっています。この設定を変更するには、次のとおり操作してください。

- 運用テストなどの目的で、非 SSL で通信する構成に変更する場合
Device Manager の GUI または CLI で通信プロトコルを変更する前に、VMware ESXi または VMware vCenter Server で、Web プロキシサービスのセキュリティ設定 (proxy.xml ファイル) を変更してください。
- 認証局で署名されたサーバ証明書を使用する場合
認証局に申請して、仮想化サーバのサーバ証明書を入手してください。証明書発行要求 (CSR) を作成する際は、サブジェクトの別名 (Subject Alternative Names) に発行元の仮想化サーバの IP アドレスを指定してください。
Host Data Collector で管理する仮想化サーバに VMware ESXi を含む場合、仮想化サーバのサーバ証明書を発行した認証局からルート認証局までの全認証局の証明書がチェーンされた状態で、サーバ証明書が必要です。
入手したサーバ証明書は、仮想化サーバにインポートされている自己署名証明書と置き換えてください。詳細は、VMware 社のマニュアルを参照してください。

関連タスク

- [5.5.18 Host Data Collector のトラストストアへの証明書のインポート](#)
- [5.5.21 仮想化サーバの登録情報の変更](#)

- ・ 付録 C.1.1 Host Data Collector のプロパティの変更

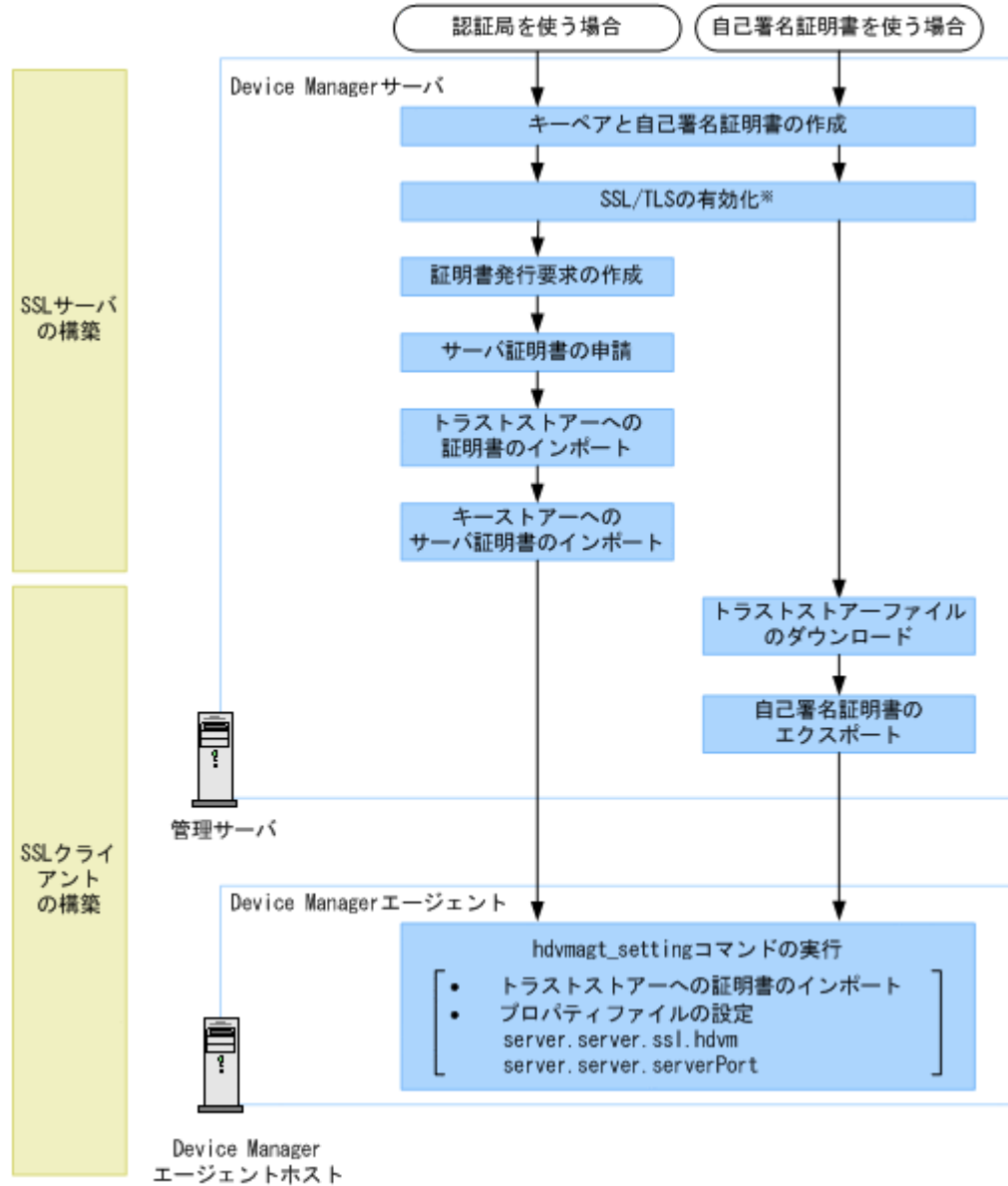
関連参照

- ・ 付録 C.2.14 hdc.ssl.esx.certCheck

5.1.10 管理サーバと Device Manager エージェント間のセキュリティ通信のための操作フロー

管理サーバで Device Manager のサーバ証明書を作成し、トラストストアにインポートします。

図 37 管理サーバと Device Manager エージェント間のセキュリティ通信のための操作フロー



注※ デフォルトではSSL/TLSが有効に設定されます。

バージョン 8.2.0 以降の Device Manager エージェントでは、Device Manager エージェントの新規インストール時にも Device Manager エージェントのトラストストアへの証明書のインポートおよびプロパティファイルの設定ができます。Device Manager エージェントのインストール方法については、マニュアル「Hitachi Command Suite インストールガイド」を参照してください。



メモ

- SSL/TLS 通信で使用する暗号方式を制限したい場合は、Device Manager サーバの `server.properties` ファイルにある `server.https.enabledCipherSuites` プロパティの値を変更してください。
- Device Manager エージェントの Java の実行環境を変更している場合は、使用する Java の実行環境のバージョンに応じた Java Cryptography Extension (JCE) の無制限強度の管轄ポリシーファイル (Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files) をダウンロードし、インストールする必要があります。
管轄ポリシーファイルは、Oracle 社または IBM 社の Web サイトからダウンロードしてください。インストール方法は、管轄ポリシーファイルに付属するドキュメントを参照してください。



メモ

バージョン 8.2.0 より前の Device Manager エージェントを使用している場合は、手動で Device Manager エージェントのトラストストアへの証明書のインポートおよびプロパティファイルの設定をしてください。

関連概念

- [5.3 SSL サーバの構築 \(Device Manager サーバ\)](#)

関連タスク

- [5.5.1 Device Manager サーバのトラストストアファイルのダウンロード](#)
- [5.5.3 Device Manager サーバの自己署名証明書のエクスポート](#)
- [付録 A.1.1 Device Manager サーバのプロパティの変更](#)

関連参照

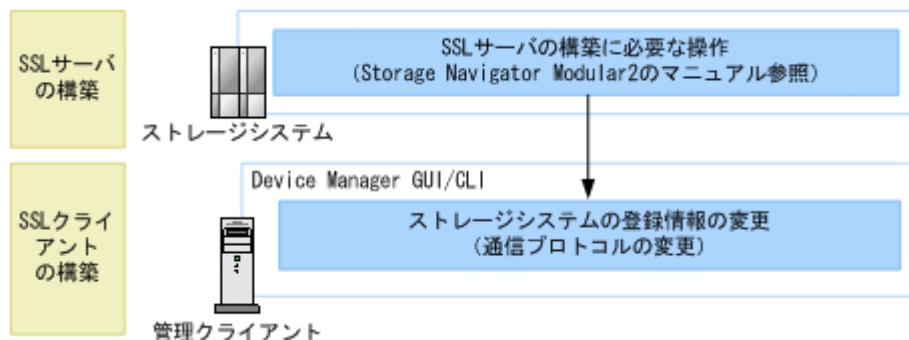
- [11.3.4 Device Manager サーバの情報, HiScan コマンドの実行周期および RAID Manager または RAID Manager XP の情報の設定 \(hdvmagt_setting コマンド\)](#)
- [付録 A.8.6 server.https.enabledCipherSuites](#)
- [付録 D.6.14 server.server.serverPort](#)
- [付録 D.6.28 server.server.ssl.hdvm](#)

5.1.11 ストレージシステムと管理サーバ間のセキュリティ通信のための操作フロー

HUS100, Hitachi AMS2000 または Hitachi SMS と管理サーバの通信に SSL/TLS を使用するためには、Device Manager の GUI または CLI でストレージシステムとの通信プロトコルを変更する必要があります。

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP および HUS VM との通信では常に SSL/TLS が使用されるため、Device Manager での環境設定は不要です。

図 38 ストレージシステムと管理サーバ間のセキュリティ通信のための操作フロー



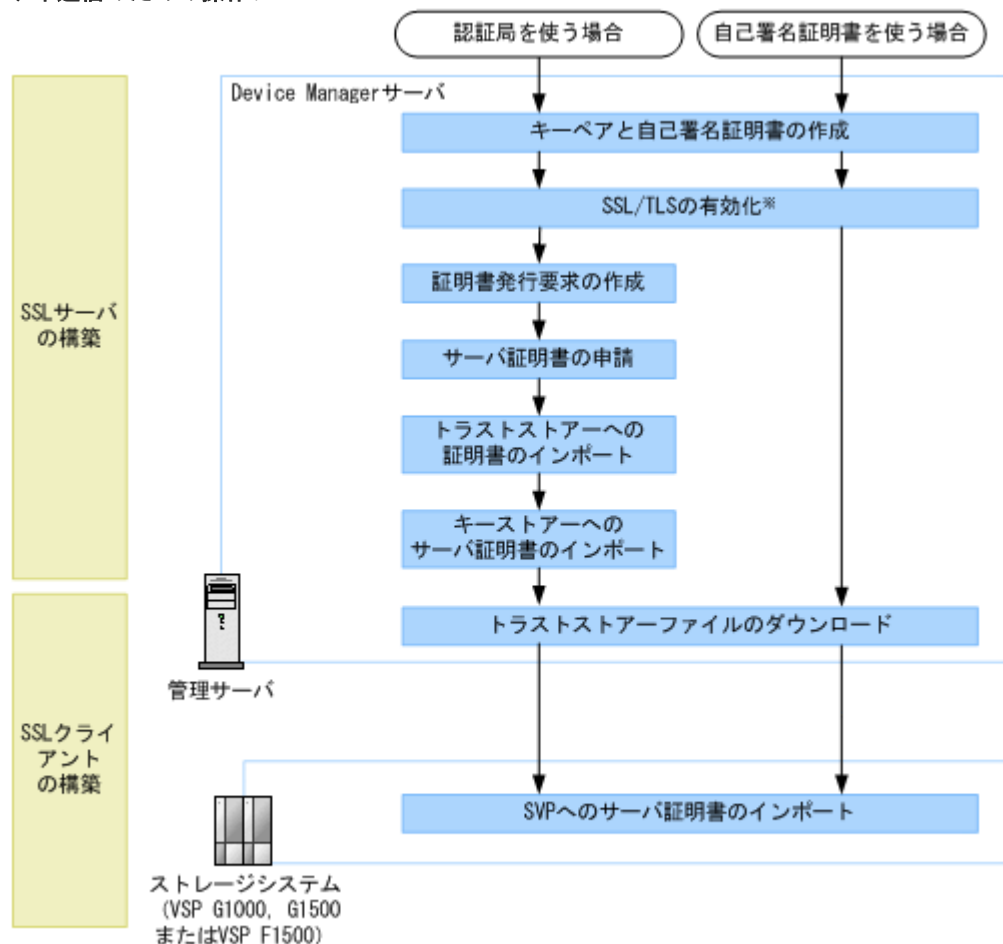
関連タスク

- 5.5.26 ストレージシステムの登録情報の変更

5.1.12 管理サーバとストレージシステム (VSP G1000, G1500 または VSP F1500) 間のセキュリティ通信のための操作フロー

RAID Manager および SVP へのログイン時に Hitachi Command Suite でユーザーアカウントを認証する際のセキュリティを高めたい場合、デフォルトの証明書を削除して、Device Manager サーバのサーバ証明書を作成し、SVP にインポートする必要があります。Device Manager サーバのサーバ証明書の作成時に指定したホスト名から、Device Manager サーバの IP アドレスへの名前解決ができるように、SVP で設定をしてください。

図 39 管理サーバとストレージシステム (VSP G1000, G1500 または VSP F1500) 間のセキュリティ通信のための操作フロー



SVP での設定方法については、ストレージシステムのマニュアルを参照してください。

関連概念

- 5.1.1 Device Manager サーバのデフォルトの証明書
- 5.3 SSL サーバの構築 (Device Manager サーバ)

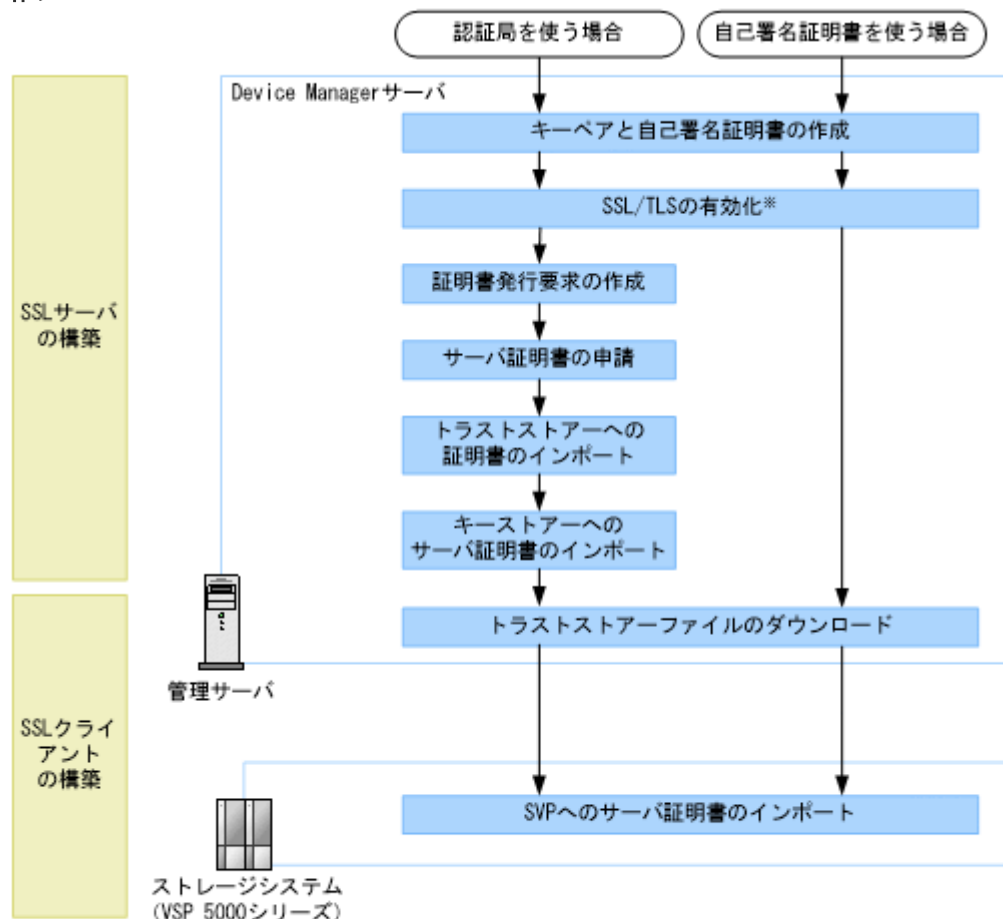
関連タスク

- 5.5.1 Device Manager サーバのトラストストアファイルのダウンロード

5.1.13 管理サーバとストレージシステム（VSP 5000 シリーズ）間のセキュリティ通信のための操作フロー

VSP 5000 シリーズでは、Device Manager サーバのデフォルトの証明書を削除後、Device Manager サーバのサーバ証明書を作成し、SVP にインポートする必要があります。Device Manager サーバのサーバ証明書の作成時に指定したホスト名から、Device Manager サーバの IP アドレスへの名前解決ができるように、SVP で設定をしてください。

図 40 管理サーバとストレージシステム（VSP 5000 シリーズ）間のセキュリティ通信のための操作フロー



注※ デフォルトではSSL/TLSが有効に設定されます。

SVP での設定方法については、ストレージシステムのマニュアルを参照してください。



ヒント

VSP 5000 シリーズを管理するために、Device Manager サーバのサーバ証明書を作成した場合、既に管理している VSP G1000, G1500, VSP F1500, VSP Gx00 モデル、または VSP Fx00 モデルとのセキュリティ通信を見直す必要があります。

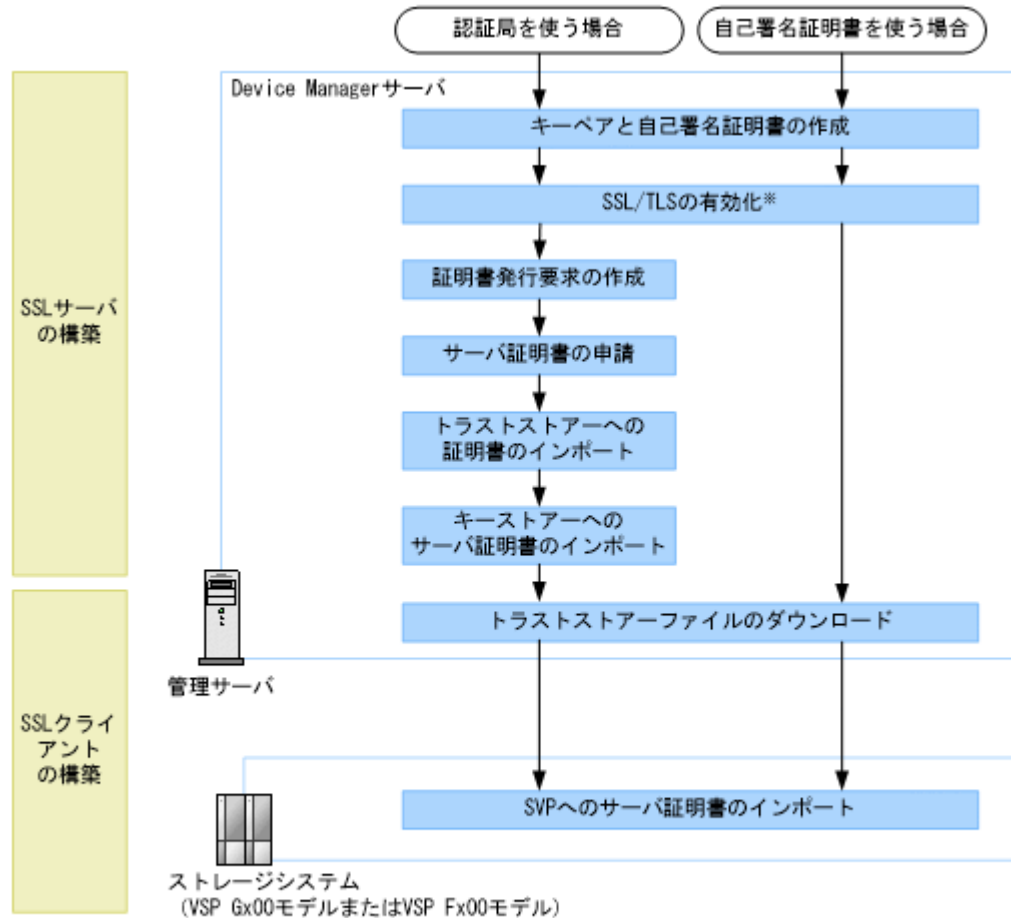
詳細は、各ストレージシステムの管理サーバとストレージシステム間のセキュリティ通信のための操作フローを参照してください。

5.1.14 管理サーバとストレージシステム（VSP Gx00 モデルまたは VSP Fx00 モデル）間のセキュリティ通信のための操作フロー

VSP Gx00 モデルまたは VSP Fx00 モデルは、デフォルトで管理サーバと暗号化通信ができるよう設定されているため、デフォルトのサーバ証明書を使用する場合は、設定は不要です。ストレージ

システムを操作する際に発生する通信のセキュリティを高めたい場合、デフォルトの証明書を削除して、Device Manager サーバのサーバ証明書を作成し、SVP にインポートする必要があります。Device Manager サーバのサーバ証明書の作成時に指定したホスト名から、Device Manager サーバの IP アドレスへの名前解決ができるように、SVP で設定をしてください。

図 41 管理サーバとストレージシステム（VSP Gx00 モデルまたは VSP Fx00 モデル）間のセキュリティ通信のための操作フロー



注※ デフォルトではSSL/TLSが有効に設定されます。

SVP での設定方法については、ストレージシステムのマニュアルを参照してください。

関連概念

- [5.1.1 Device Manager サーバのデフォルトの証明書](#)
- [5.3 SSL サーバの構築 \(Device Manager サーバ\)](#)

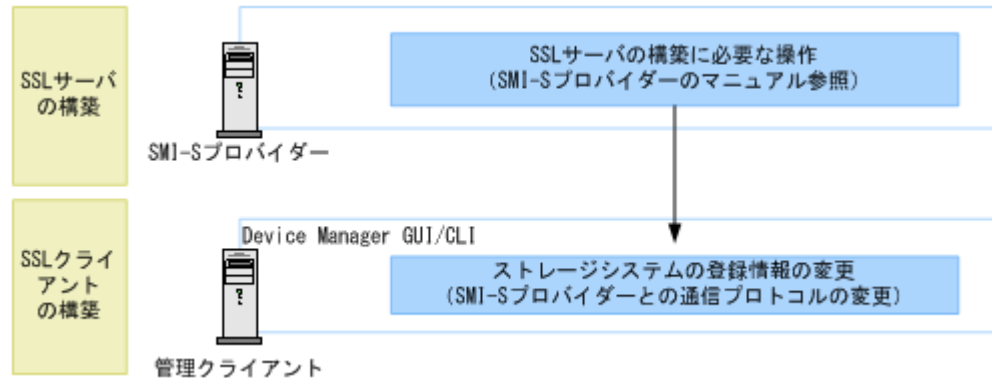
関連タスク

- [5.5.1 Device Manager サーバのトラストストアファイルのダウンロード](#)

5.1.15 SMI-S プロバイダーと管理サーバ間のセキュリティ通信のための操作フロー

SMI-S プロバイダーで環境を構築し、Device Manager の GUI または CLI で SMI-S プロバイダーとの通信プロトコルを変更する必要があります。

図 42 SMI-S プロバイダーと管理サーバ間のセキュリティ通信のための操作フロー



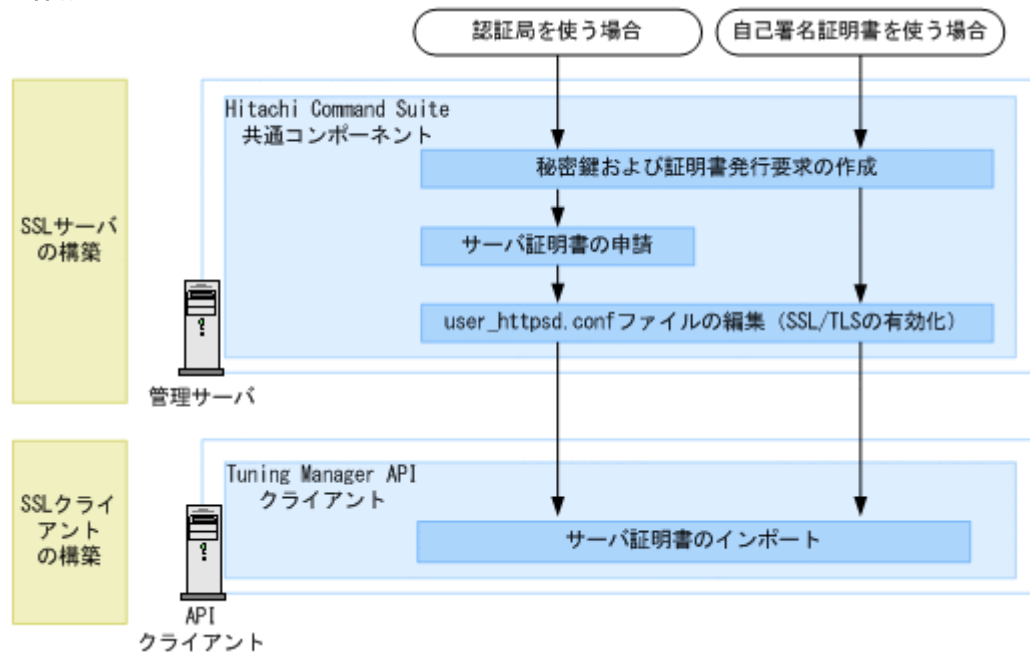
関連概念

- 5.5 SSL クライアントの構築

5.1.16 Tuning Manager サーバと Tuning Manager API クライアント間のセキュリティ通信のための操作フロー

Tuning Manager サーバと Device Manager サーバが同じ管理サーバにインストールされている場合、管理サーバで Hitachi Command Suite 共通コンポーネントのサーバ証明書を作成し、Tuning Manager API クライアントにインポートします。API クライアント側での SSL 通信の設定については、各クライアントの環境に応じて実施してください。

図 43 Tuning Manager サーバと Tuning Manager API クライアント間のセキュリティ通信のための操作フロー



メモ

このマニュアルでは、Tuning Manager サーバと Device Manager サーバが同じ管理サーバにインストールされている場合の SSL 通信の設定手順について説明します。Tuning Manager サーバと Device Manager サーバが異なる管理サーバにインストールされている場合は、マニュアル「Hitachi Command Suite Tuning Manager 運用管理ガイド」を参照してください。

関連概念

- ・ 5.2 SSL サーバの構築 (Hitachi Command Suite 共通コンポーネント)

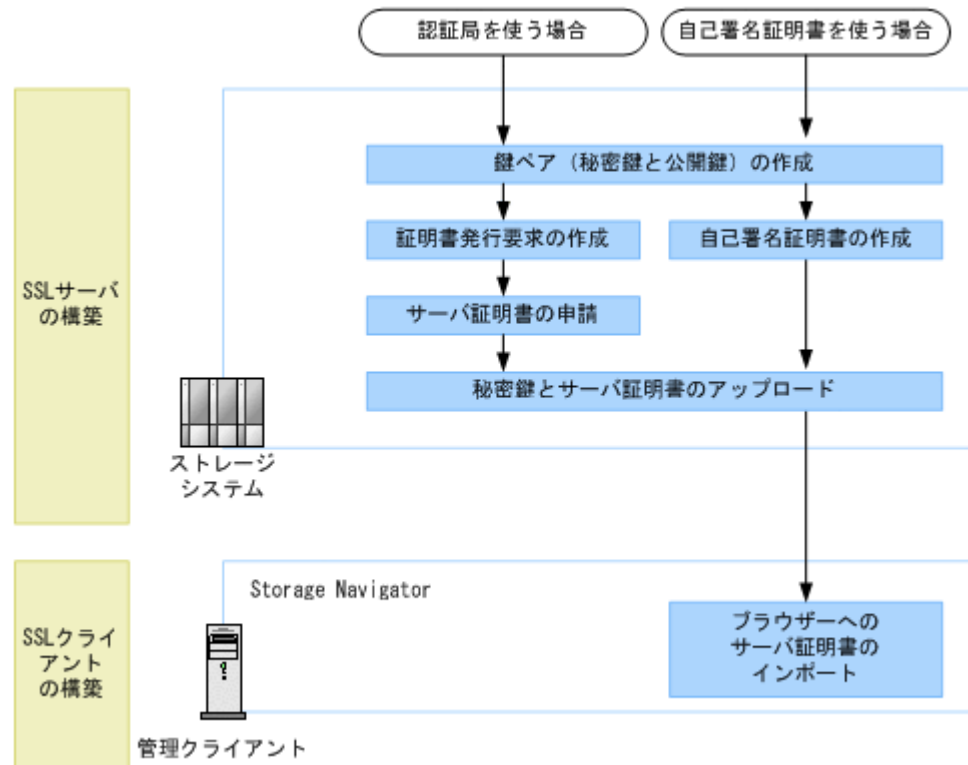
5.1.17 ストレージシステムと管理クライアント (GUI) 間のセキュリティ通信のための操作フロー

Device Manager GUI から Storage Navigator, Storage Navigator Modular 2, または maintenance utility を使用してストレージシステムを操作する場合、ストレージシステムに格納されているデフォルトのサーバ証明書を使用したセキュリティ通信が利用できます。

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, Virtual Storage Platform または HUS VM を操作する場合は、Device Manager GUI から Storage Navigator または maintenance utility を起動すると Web ブラウザーに証明書の警告メッセージが表示されますが、無視してください。この警告メッセージが表示されても、ストレージシステムと Device Manager GUI 間の通信は暗号化されています。Storage Navigator の起動時に表示される警告メッセージエラーを解消するには、次の操作フローに従ってストレージシステムのサーバ証明書を再作成してください。サーバ証明書の Common Name には、ストレージシステムのホスト名を指定してください。このホスト名は、Device Manager GUI で登録する際に指定するストレージシステムのホスト名と一致している必要があります。VSP Gx00 モデルまたは VSP Fx00 モデルの場合は、SVP のホスト名を指定してください。

maintenance utility の場合、Device Manager GUI で VSP Gx00 モデルまたは VSP Fx00 モデルのコントローラーを IP アドレスで登録するため、警告メッセージの表示を解消できません。

図 44 ストレージシステムと管理クライアント (GUI) 間のセキュリティ通信のための操作フロー





ヒント

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, または VSP Fx00 モデル を操作する場合, よりセキュリティを高めるために, Device Manager GUI から Storage Navigator に送信する情報を簡略化することもできます。

Storage Navigator に送信する情報を簡略化するには, Device Manager サーバの `client.properties` ファイルにある `client.launch.em.secure` プロパティに `true` を指定してください。

サーバ証明書の作成およびインポート方法については, ストレージシステムのマニュアルを参照してください。

関連タスク

- 付録 A.1.1 Device Manager サーバのプロパティの変更

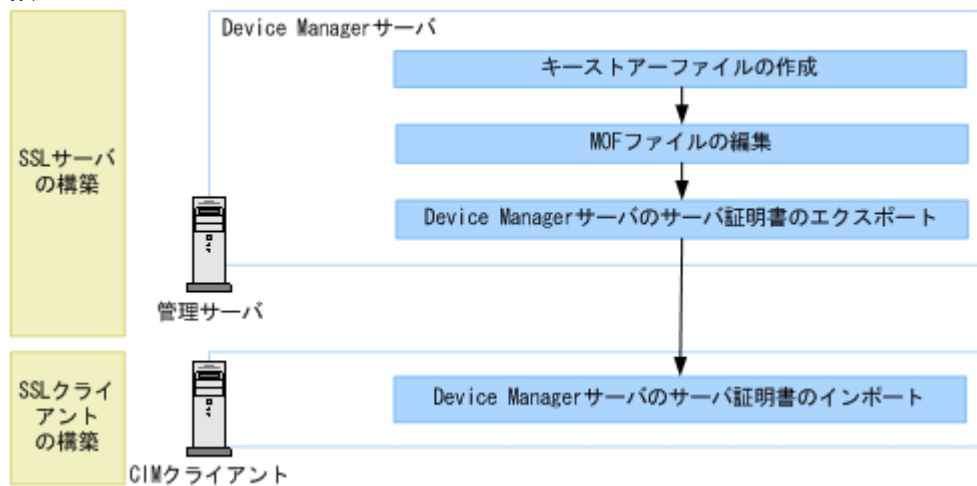
関連参照

- 付録 A.7.2 `client.launch.em.secure`

5.1.18 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー (オブジェクト操作)

オブジェクト操作で SSL サーバ認証するためには, Device Manager サーバで作成したサーバ証明書を CIM クライアントにインポートする必要があります。

図 45 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー (オブジェクト操作)



メモ

SSL/TLS 通信で使用する暗号方式を制限したい場合は, `cimxmlscpa.properties` ファイルを新規に作成して, `Ciphers` プロパティに値を指定してください。

関連概念

- 5.6 SSL サーバおよび SSL クライアントの構築 (CIM サーバ)
- 5.7 SSL サーバおよび SSL クライアントの構築 (CIM クライアント)

関連タスク

- 付録 A.1.1 Device Manager サーバのプロパティの変更

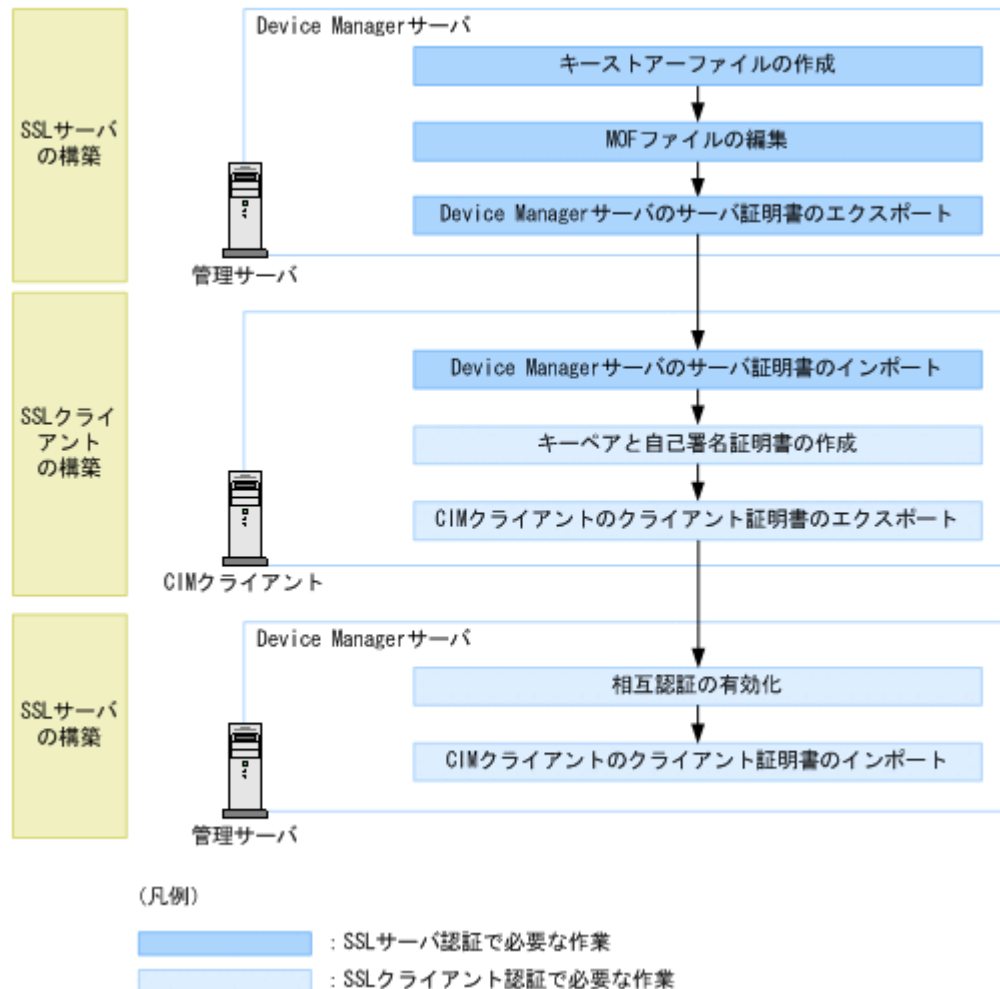
関連参照

- 付録 A.8.8 `Ciphers`

5.1.19 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー（オブジェクト操作の相互認証）

SSL サーバ認証のために、Device Manager サーバのサーバ証明書を CIM クライアントにインポートします。また、SSL クライアント認証のために、CIM クライアントのクライアント証明書を Device Manager サーバにインポートします。

図 46 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー（オブジェクト操作の相互認証）



メモ

SSL/TLS 通信で使用している暗号方式を制限したい場合は、`cimxmlscpa.properties` ファイルを新規に作成して、`Ciphers` プロパティに値を指定してください。

関連概念

- ・ [5.6 SSL サーバおよび SSL クライアントの構築（CIM サーバ）](#)
- ・ [5.7 SSL サーバおよび SSL クライアントの構築（CIM クライアント）](#)

関連タスク

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

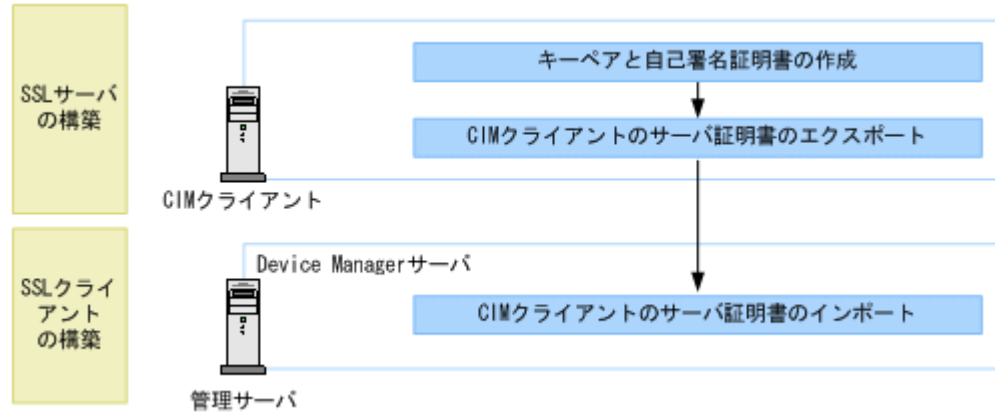
関連参照

- ・ [付録 A.8.8 Ciphers](#)

5.1.20 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー（インディケーション通知）

インディケーション通知で SSL サーバ認証するためには、CIM クライアントで作成したサーバ証明書を Device Manager サーバにインポートする必要があります。

図 47 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー（インディケーション通知）



メモ

SSL/TLS 通信で使用する暗号方式を制限したい場合は、`cimxmlscpa.properties` ファイルを新規に作成して、`Ciphers` プロパティに値を指定してください。

関連概念

- ・ [5.6 SSL サーバおよび SSL クライアントの構築（CIM サーバ）](#)
- ・ [5.7 SSL サーバおよび SSL クライアントの構築（CIM クライアント）](#)

関連タスク

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

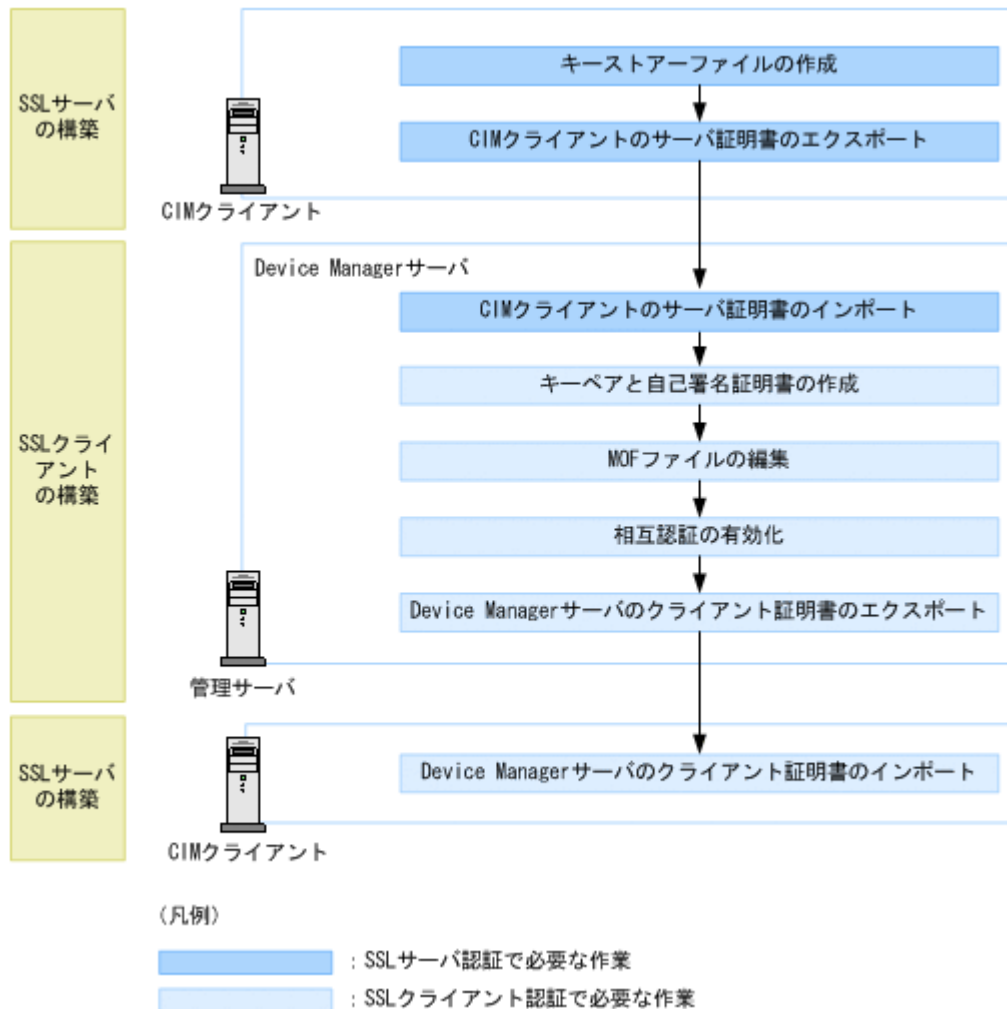
関連参照

- ・ [付録 A.8.8 Ciphers](#)

5.1.21 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー（インディケーション通知の相互認証）

SSL サーバ認証のために、CIM クライアントのサーバ証明書を Device Manager サーバにインポートします。また、SSL クライアント認証のために、Device Manager サーバのクライアント証明書を CIM クライアントにインポートします。

図 48 管理サーバと CIM クライアント間のセキュリティ通信のための操作フロー（インディケーション通知の相互認証）



メモ

SSL/TLS 通信で使用する暗号方式を制限したい場合は、`cimxmlscpa.properties` ファイルを新規に作成して、`Ciphers` プロパティに値を指定してください。

関連概念

- ・ [5.6 SSL サーバおよび SSL クライアントの構築（CIM サーバ）](#)
- ・ [5.7 SSL サーバおよび SSL クライアントの構築（CIM クライアント）](#)

関連タスク

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

関連参照

- ・ [付録 A.8.8 Ciphers](#)

5.1.22 トラストストア

トラストストアの格納場所を次に示します。

- `jssecacerts`

Hitachi Command Suite 共通コンポーネントのトラストストアです。次の通信路で SSL/TLS を使用する場合に、`jssecacerts` に、証明書をインポートします。

- Device Manager サーバと Replication Manager サーバ間
- Tuning Manager サーバと Device Manager サーバ間

Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>%Base64%uCPsB%jdk%jre%lib%security%jssecacerts
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/uCPsB/jdk/jre/lib/security/jssecacerts
```

- `ldapcacerts`

Hitachi Command Suite 共通コンポーネントのトラストストアです。LDAP ディレクトリサーバと StartTLS 通信する場合には、`ldapcacerts` に証明書をインポートします。

Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>%Base64%conf%sec%ldapcacerts
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/conf/sec/ldapcacerts
```

- `dvmcacerts`

Device Manager サーバのトラストストアです。

管理サーバと管理クライアント (GUI) 間の通信に使用する Device Manager サーバのサーバ証明書を認証局に申請した場合には、証明書を `dvmcacerts` にインポートします。

また、Host Data Collector マシンと Device Manager サーバ間で SSL/TLS 通信する場合に、Host Data Collector のサーバ証明書を `dvmcacerts` にインポートします。

Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager%HiCommandServer%dvmcacerts
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/dvmcacerts
```



メモ

- トラストストアファイルは、Device Manager サーバの `server.properties` ファイルにある `server.https.security.truststore` プロパティで変更できます。

- 初期パスワードは changeit です。変更する場合は、必ず HiKeytool を使用してください。ほかのツールやコマンドを使って変更した場合、HiKeytool でサーバ証明書のインポートや参照ができなくなります。
-

- hdccacerts

Host Data Collector のトラストストアです。

仮想化サーバと Host Data Collector 間の通信に使用する仮想化サーバのサーバ証明書を認証局に申請した場合には、証明書を hdccacerts にインポートします。デフォルトパスワードは changeit です。

Windows の場合 :

```
< Host Data Collector のインストールフォルダ > %HDC%\Base\config\hdccacerts
```

Linux の場合 :

```
< Host Data Collector のインストールディレクトリ > /HDC/Base/config/  
hdccacerts
```

- hdvmcacerts

Device Manager エージェントのトラストストアです。

管理サーバと Device Manager エージェント間で SSL/TLS 通信する場合に、Device Manager サーバのサーバ証明書を hdvmcacerts にインポートします。デフォルトパスワードは changeit 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%\config  
%hdvmcacerts
```

UNIX の場合 :

```
< Device Manager エージェントのインストールディレクトリ > /agent/config/  
hdvmcacerts
```

- .truststore

Device Manager サーバのオブジェクト操作のトラストストアです。オブジェクト操作の SSL サーバ認証で CIM クライアントと通信する際に使用されます。デフォルトパスワードは trustssl です。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%\wsi%\server%\jserver%\bin%\truststore
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/wsi/  
server/jserver/bin/.truststore
```

- indtruststore

Device Manager サーバのインディケーション通知用のトラストストアです。インディケーション通知の SSL クライアント認証で CIM クライアントと通信する際に使用されます。

Windows の場合 :

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager
%HiCommandServer%wsi%server%jserver%bin%indtruststore
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/wsi/
server/jserver/bin/indtruststore
```

- Java Web Start のトラストストアー

Windows の場合 :

```
<Program Files フォルダ>%Java%<JRE バージョン>%bin%cacerts
```

Linux の場合 :

```
/usr/java/<JRE バージョン>/javaws/cacerts
```

HP-UX の場合 :

```
/opt/<JRE バージョン>/jre/javaws/cacerts
```

関連タスク

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

関連参照

- [付録 A.8.5 server.https.security.truststore](#)

5.2 SSL サーバの構築 (Hitachi Command Suite 共通コンポーネント)

Hitachi Command Suite 共通コンポーネントを SSL サーバとして使用するためには、秘密鍵とサーバ証明書を準備し、それぞれの格納場所を `user_httpsd.conf` ファイルに設定する必要があります。

5.2.1 Hitachi Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成

Hitachi Command Suite 共通コンポーネントで秘密鍵および証明書発行要求 (CSR) を作成するには、`hcnds64ssltool` コマンドを使用します。

`hcnds64ssltool` コマンドを実行すると、RSA 暗号および楕円曲線暗号 (ECC) に対応した 2 種類の秘密鍵、証明書発行要求、および自己署名証明書が作成されます。証明書発行要求は、PEM 形式で作成されます。なお、自己署名証明書は暗号化通信のテストなどの目的でだけ使用することをお勧めします。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 次の情報の確認
 - 証明書発行要求の要件 (認証局に確認)
 - 管理クライアントで使用する Web ブラウザーのバージョン
管理クライアント (GUI) で使用する Web ブラウザーが、サーバ証明書の署名アルゴリズムに対応している必要があります。
 - 既存の秘密鍵、証明書発行要求、および自己署名証明書の格納先 (再作成する場合)

出力先パスに同じ名称のファイルがある場合、ファイルを上書きして作成できません。再作成する場合は、既存の格納先以外に出力してください。

操作手順

1. 次のコマンドを実行します。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > %Base64%bin%hcmds64ssltool  
[/key <秘密鍵ファイル>] [/csr <証明書発行要求ファイル>] [/cert <自己署名証明書ファイル>] [/certtext <自己署名証明書の内容ファイル>] [/validity  
<有効日数>] [/dname <DN >] [/sigalg <RSA 暗号用のサーバ証明書の署名  
アルゴリズム>] [/eccsigalg <楕円曲線暗号用のサーバ証明書の署名アルゴリズム  
>] [/ecckeysize <楕円曲線暗号用の秘密鍵のキーサイズ>]
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/  
hcmds64ssltool [-key <秘密鍵ファイル>] [-csr <証明書発行要求ファイル>]  
[-cert <自己署名証明書ファイル>] [-certtext <自己署名証明書の内容ファイル  
>] [-validity <有効日数>] [-dname <DN >] [-sigalg <RSA 暗号用のサ  
ーバ証明書の署名アルゴリズム>] [-eccsigalg <楕円曲線暗号用のサーバ証明書の  
署名アルゴリズム>] [-ecckeysize <楕円曲線暗号用の秘密鍵のキーサイズ>]
```

オプション

key

秘密鍵の出力先パスを絶対パスで指定します。

RSA 暗号用の秘密鍵は指定したファイル名で出力されます。楕円曲線暗号用の秘密鍵は指定したファイル名の先頭に ecc- が付いて出力されます。

オプションの指定を省略すると、httpsdkey.pem ファイルおよび ecc-httpsdkey.pem ファイルが出力されます。*

csr

証明書発行要求の出力先パスを絶対パスで指定します。

RSA 暗号用の証明書発行要求は指定したファイル名で出力されます。楕円曲線暗号用の証明書発行要求は指定したファイル名の先頭に ecc- が付いて出力されます。

オプションの指定を省略すると、httpsd.csr ファイルおよび ecc-httpsd.csr ファイルが出力されます。*

cert

自己署名証明書の出力先パスを絶対パスで指定します。

RSA 暗号用の自己署名証明書は指定したファイル名で出力されます。楕円曲線暗号用の自己署名証明書は指定したファイル名の先頭に ecc- が付いて出力されます。

オプションの指定を省略すると、httpsd.pem ファイルおよび ecc-httpsd.pem ファイルが出力されます。*

certtext

自己署名証明書の内容 (テキスト形式) の出力先パスを絶対パスで指定します。

RSA 暗号用の自己署名証明書の内容は指定したファイル名で出力されます。楕円曲線暗号用の自己署名証明書の内容は指定したファイル名の先頭に ecc- が付いて出力されます。

オプションの指定を省略すると、httpsd.txt ファイルおよび ecc-httpsd.txt ファイルが出力されます。*

validity

自己署名証明書の有効期間を日数で指定します。このオプションを指定すると、RSA 暗号用と楕円曲線暗号用で同じ内容が指定されます。指定を省略した場合は、有効期間は 3650 日になります。

dname

自己署名証明書と証明書発行要求に記述する DN を指定します。オプションの指定を省略すると、対話形式で DN を指定できます。

DN は属性型と属性値を等号 (=) でまとめ、各属性をコンマ (,) で区切って指定します。DN には引用符 (") および円記号 (¥) は指定できません。また、DN の属性値は RFC2253 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープしてください。

DN の先頭または末尾の空白文字

DN の先頭の番号記号 (#)

DN に含まれる正符号 (+), コンマ (,), セミコロン (;), 始め山括弧 (<), 等号 (=) および終わり山括弧 (>)

DN に指定する属性型および属性値を次の表に示します。

表 53 DN に指定する属性型および属性値

属性型	属性型の正式名称	属性値
CN	Common Name	管理サーバ (HBase 64 Storage Mgmt Web Service) のホスト名を指定します。この項目は必須です。 管理クライアント (GUI) から管理サーバ (Hitachi Command Suite 共通コンポーネントの HBase 64 Storage Mgmt Web Service) に接続するときに使用するホスト名 (FQDN 形式でも可) を指定します。管理サーバをクラスタ環境で運用している場合には、論理ホスト名を指定してください。
OU	Organizational Unit Name	組織の構成単位名を指定します。
O	Organization Name	組織名を指定します。この項目は必須です。
L	Locality Name	市区町村名または地域名を指定します。
ST	State or Province Name	都道府県名を指定します。
ST	State or Province Name	州名を指定します。
C	Country Name	2 文字の国コードを指定します。

sigalg

RSA 暗号用のサーバ証明書の署名アルゴリズムを指定します。SHA256withRSA または SHA1withRSA を指定できます。指定を省略した場合、署名アルゴリズムは SHA256withRSA になります。

eccsigalg

楕円曲線暗号用のサーバ証明書の署名アルゴリズムを指定します。SHA512withECDSA, SHA384withECDSA, SHA256withECDSA または SHA1withECDSA を指定できます。指定を省略した場合、署名アルゴリズムは SHA384withECDSA になります。

ecckeysize

楕円曲線暗号用の秘密鍵のキーサイズをビットで指定します。256 または 384 を指定できます。指定を省略した場合、キーサイズは 384 ビットになります。
RSA 暗号用の秘密鍵のキーサイズは 2048 ビット（固定）です。

注※

オプションの指定を省略すると、次の場所にファイルが出力されます。

Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>\Base64\uCPSB\httpsd\conf\ssl\server\
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/uCPSB/httpsd/conf/ssl/server/
```

5.2.2 Hitachi Command Suite 共通コンポーネントのサーバ証明書の認証局への申請

作成した Hitachi Command Suite 共通コンポーネントの証明書発行要求（CSR）を認証局に送信し、電子署名を受けます。

前提条件

- Hitachi Command Suite 共通コンポーネントの証明書発行要求の作成
- 次の情報の確認
 - 認証局への申請方法や対応状況
X.509 PEM 形式のサーバ証明書を発行してもらう必要があります。申請方法については、使用する認証局の Web サイトなどで確認してください。
また、証明書の署名アルゴリズムに、認証局が対応していることを確認してください。

操作手順

1. 作成した証明書発行要求を認証局に送付します。

操作結果

認証局からの返答は保存しておいてください。



メモ

認証局が発行する証明書には有効期限があります。期限が切れる前に再発行してもらう必要があります。証明書の有効期限は、`hcmds64checkcerts` コマンドを使用して確認してください。

関連タスク

- [5.2.4 証明書の有効期限の確認（Hitachi Command Suite 共通コンポーネント）](#)

5.2.3 SSL/TLS を有効にする場合の user_httpsd.conf ファイルの編集

Hitachi Command Suite 共通コンポーネントの SSL/TLS を有効にする場合は、`user_httpsd.conf` ファイルを編集します。

前提条件

- Hitachi Command Suite 共通コンポーネントの秘密鍵の作成（SSL/TLS の有効化に必要）※
- Hitachi Command Suite 共通コンポーネントのサーバ証明書の準備（SSL/TLS の有効化に必要）※

認証局から返送されたサーバ証明書を準備します。暗号化通信のテストなどの目的の場合は、自己署名証明書でもかまいません。

- 次の情報の確認
 - 証明書発行要求の Common Name に設定したホスト名 (SSL/TLS の有効化に必要)

注※

次の場所にコピーしておくことをお勧めします。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > \Base64\uCPSB\httpsd\conf
\ssl\server
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/httpsd/
conf/ssl/server
```

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. user_httpsd.conf ファイルを編集します。

user_httpsd.conf ファイルの格納場所

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > \Base64\uCPSB\httpsd\conf
\user_httpsd.conf
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/httpsd/
conf/user_httpsd.conf
```

user_httpsd.conf ファイルの例 (デフォルト)

```

ServerName <管理サーバのホスト名>
Listen 22015          ●————— 非SSL通信用のポート番号
#Listen [::]:22015   ●————— 非SSL通信用のポート番号 (IPv6環境用)
#Listen 127.0.0.1:22015
SSLDisable
#Listen 22016        ●————— SSL通信用のポート番号
#Listen [::]:22016   ●————— SSL通信用のポート番号 (IPv6環境用)
#<VirtualHost *:22016> ●————— SSL通信用のポート番号
# ServerName <管理サーバのホスト名>
# SSLEnable
# SSLProtocol TLSv12
# SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDSA-AES128-GCM-
SHA256:ECDSA-AES256-SHA384:ECDSA-AES128-SHA256:ECDSA-
AES256-SHA:ECDSA-AES128-SHA:AES256-SHA:AES128-
SHA256:AES128-SHA:DES-CBC3-SHA
# SSLRequireSSL
# SSLCertificateKeyFile "<Hitachi Command Suiteのインストールフォルダ>
/Base64/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem"
# SSLCertificateFile "<Hitachi Command Suiteのインストールフォルダ>
/Base64/uCPSB/httpsd/conf/ssl/server/httpsd.pem"
# SSLECCCertificateKeyFile "<Hitachi Command Suiteのインストールフォルダ>
/Base64/uCPSB/httpsd/conf/ssl/server/ecc-httpsdkey.pem"
# SSLECCCertificateFile "<Hitachi Command Suiteのインストールフォルダ>/Base64/
uCPSB/httpsd/conf/ssl/server/ecc-httpsd.pem"
# SSLCACertificateFile "<Hitachi Command Suiteのインストールフォルダ>
/Base64/uCPSB/httpsd/conf/ssl/cacert/anycert.pem"
#</VirtualHost>
#HWSLogSSLVerbose On

```

SSL/TLS の有効化に必要な設定



メモ

ディレクティブを編集する際は、次の点に注意してください。

- ディレクティブを重複して指定しないでください。
- 1つのディレクティブの途中で改行しないでください。
- 各ディレクティブに指定するパスには、シンボリックリンクやジャンクションを指定しないでください。
- 各ディレクティブに指定する証明書および秘密鍵ファイルには、PEM形式のファイルを指定してください。
- httpsd.conf ファイルおよび hssso_httpsd.conf ファイルは編集しないでください。

- 次の行頭の番号記号 (#) を削除します。

```

ServerName <ホスト名>
Listen 22015
#Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
  ServerName <ホスト名>
  SSLEnable
  SSLProtocol TLSv12
  SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-
ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA:AES256-SHA256:AES256-
SHA:AES128-SHA256:AES128-SHA:DES-CBC3-SHA
  SSLRequireSSL
  SSLCertificateKeyFile "<Hitachi Command Suiteのインストールフォルダ>
/Base64/uCPSB/httpd/conf/ssl/server/httpdkey.pem"
  SSLCertificateFile "<Hitachi Command Suiteのインストールフォルダ>
/Base64/uCPSB/httpd/conf/ssl/server/httpd.pem"
  SSLECCertificateKeyFile "<Hitachi Command Suiteのインストールフォルダ>
/Base64/uCPSB/httpd/conf/ssl/server/ecc-httpdkey.pem"
  SSLECCertificateFile "<Hitachi Command Suiteのインストールフォルダ>
/Base64/uCPSB/httpd/conf/ssl/server/ecc-httpd.pem"
  # SSLCACertificateFile "<Hitachi Command Suiteのインストールフォルダ>
/Base64/uCPSB/httpd/conf/ssl/cacert/anycert.pem"
</VirtualHost>
HWSLogSSLVerbose On

```

行頭の番号記号 (#) を削除 (13か所)

RSA 暗号だけを使用する場合、SSLECCertificateKeyFile ディレクティブおよび SSLECCertificateFile ディレクティブの行頭の番号記号 (#) を削除する必要はありません。

- 先頭行の ServerName ディレクティブと<VirtualHost>タグ内の ServerName ディレクティブに、証明書発行要求の Common Name に設定したホスト名 (クラスタ環境の場合は論理ホスト名) を指定します。大文字, 小文字の区別も同じにしてください。
- SSLCertificateKeyFile ディレクティブに, RSA 暗号の Hitachi Command Suite 共通コンポーネントの秘密鍵ファイルを絶対パスで指定します。
- SSLCertificateFile ディレクティブに, RSA 暗号の Hitachi Command Suite 共通コンポーネントのサーバ証明書を絶対パスで指定します。
- SSLECCertificateKeyFile ディレクティブに, 楕円曲線暗号の Hitachi Command Suite 共通コンポーネントの秘密鍵ファイルを絶対パスで指定します。RSA 暗号だけを使用する場合, この設定は不要です。
- SSLECCertificateFile ディレクティブに, 楕円曲線暗号の Hitachi Command Suite 共通コンポーネントのサーバ証明書を絶対パスで指定します。RSA 暗号だけを使用する場合, この設定は不要です。
- Hitachi Command Suite 共通コンポーネントのサーバ証明書を発行した認証局が中間認証局の場合は, SSLCACertificateFile ディレクティブの行頭の番号記号 (#) を削除して, すべての中間認証局の証明書を絶対パスで指定します。複数の証明書をテキストエディターで連結させることで, 1つのファイルに複数の証明書を混在させることができます。
- IPv6 環境の場合, #Listen [::]:22016 の行頭の番号記号 (#) を削除します。



メモ

- SSL を有効にする場合や Device Manager を IPv6 環境で運用する場合でも、Listen 22015 の行を削除したり、コメント行にしたりしないでください。
外部から管理サーバへの非 SSL 通信を遮断したい場合は、Listen 22015 と Listen [::]:22015 の行頭に番号記号 (#) を追記してコメント行にしたあと、#Listen 127.0.0.1:22015 の行頭の番号記号を削除してください。ただし、Hitachi File Services Manager や Storage Navigator Modular 2 と連携しているときは、この設定をすると正常に連携できなくなることがあります。これらの製品と連携している場合、各製品のドキュメントで外部からの非 SSL 通信の遮断をサポートしているかを確認し、ドキュメントに従い設定してください。
- Hitachi Command Suite をバージョン 8.2.1 以前からアップグレードインストールしても、user_httpsd.conf ファイルに楕円曲線暗号の内容は反映されません。楕円曲線暗号を使用する場合、次の場所に格納されているサンプルファイルから、SSLRequiredCiphers ディレクティブ、SSLECCertificateKeyFile ディレクティブおよび SSLECCertificateFile ディレクティブの内容をコピーして使用してください。
Windows の場合：
`<Hitachi Command Suite のインストールフォルダ>%Base64%sample%httpsd.conf%user_httpsd.conf`
Linux の場合：
`<Hitachi Command Suite のインストールディレクトリ>/Base64/sample/httpsd/conf/user_httpsd.conf`
- Hitachi File Services Manager や 32bit 版 Storage Navigator Modular 2 と連携している場合に SSL/TLS を有効にするときは、次の場所に格納されている httpsd.conf ファイルも編集してください。
Windows の場合：
`<Hitachi File Services Manager または 32bit 版 Storage Navigator Modular 2 のインストールフォルダ>%Base%httpsd%conf%httpsd.conf`
Linux の場合：
`<Hitachi File Services Manager または 32bit 版 Storage Navigator Modular 2 のインストールディレクトリ>/Base/httpsd/conf/httpsd.conf`
編集方法については、Hitachi File Services Manager または Storage Navigator Modular 2 のマニュアルを参照してください。



ヒント

SSL/TLS を無効にするには、user_httpsd.conf ファイルの例（デフォルト）を参考に、Listen 22016 から HWSLogSSLVerbose On までの行頭に番号記号 (#) を追記して、コメント行にしてください。

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

5.2.4 証明書の有効期限の確認 (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サーバ証明書や認証局の証明書の有効期限を確認するには、hcmds64checkcerts コマンドを使用します。

サーバ証明書には有効期限があります。有効期限切れに注意してください。

前提条件

- user_httpsd.conf ファイルの編集
hcnds64checkcerts コマンドでは、user_httpsd.conf ファイルで指定している証明書の有効期限が確認できます。このため、user_httpsd.conf ファイルに次の証明書のパスを指定してください。
 - Hitachi Command Suite 共通コンポーネントのサーバ証明書
RSA 暗号および楕円曲線暗号の証明書を使用している場合、それぞれで指定が必要です。
 - すべての中間認証局の証明書
- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン

操作手順

1. 次のコマンドを実行して、証明書の有効期限を確認してください。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > %Base64%\bin  
%hcnds64checkcerts { [/days <日数>] [/log] | /all }
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/  
hcnds64checkcerts { [-days <日数>] [-log] | -all }
```

days

有効期限切れの証明書があるか確認する日付を、コマンドの実行日からの日数で指定します。指定できる値の範囲は 30~3652 (10 年) です。このオプションを指定すると、指定した日数以内に有効期限が切れる証明書、およびすでに有効期限が切れている証明書が表示されます。オプションの指定を省略すると、日数に 30 が指定されます。

log

表示対象の証明書がある場合、イベントログ (Windows) または syslog (Linux) に警告メッセージが出力されます。このコマンドを OS のタスクや cron などに登録して、定期的に証明書の有効期限を確認する場合、このオプションを指定してください。

all

user_httpsd.conf ファイルで指定したすべての証明書の有効期限が表示されます。

関連タスク

- [5.2.3 SSL/TLS を有効にする場合の user_httpsd.conf ファイルの編集](#)

5.3 SSL サーバの構築 (Device Manager サーバ)

Device Manager サーバを SSL サーバとして使用するためには、秘密鍵とサーバ証明書を準備する必要があります。

5.3.1 Device Manager サーバのキーペアと自己署名証明書の作成

Device Manager サーバのキーペアと自己署名証明書を作成するには、HiKeytool のメインメニューから [SSL configuration for Device Manager Server] - [Make KeyPair/Self-Signed Certificate] を選択します。

暗号および Java セキュリティの分野に精通しているか、特に指定がある場合を除き、デフォルト値を使用してください。なお、自己署名証明書は暗号化通信のテストなどの目的でだけ使用することをお勧めします。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 既存のキーペアの削除 (再作成する場合)
キーストアーに格納できるキーペアは 1 つだけです。複数のキーペアが格納されていると、Device Manager サーバをセキュアモードで使用する際に問題が発生するおそれがあります。
- 次の情報の確認
 - 管理クライアントで使用する Web ブラウザーのバージョン
管理クライアント (GUI) で使用する Web ブラウザーが、サーバ証明書の署名アルゴリズムに対応している必要があります。

操作手順

1. 次のとおり実行して、HiKeytool を起動します。

Windows の場合

```
< Hitachi Command Suite のインストールフォルダ > ¥DeviceManager  
¥HiCommandServer¥HiKeytool.bat
```

Linux の場合

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/  
HiKeytool.sh
```

2. メインメニューで、1 ([SSL configuration for Device Manager Server]) を指定します。
3. サーバ用メインメニューで、1 ([Make KeyPair/Self-Signed Certificate]) を指定します。
4. ホスト名を指定します。
管理クライアントから管理サーバに接続するとき使用するホスト名 (FQDN 形式でも可) を指定します。クラスタ環境で管理サーバを運用している場合は、論理ホスト名を指定してください。
使用しているマシンが LAN または WAN の別名で認識される場合を除き、デフォルト値を使用してください。別名で認識される場合には、Device Manager サーバが認識される名前を指定する必要があります。
手順 4～手順 9 で指定する値に、円記号 (¥) は指定できません。
5. 組織の構成単位を指定します。
デフォルト値を推奨しますが、Marketing のようにわかりやすい別の名前も使用できます。
6. 組織名を指定します。
通常はデフォルト値のホスト名を使用しますが、会社名など別の名前も使用できます。
7. 市区町村名または地域名を指定します。
8. 都道府県名を指定します。
9. 2 文字の国コードを指定します。
10. キーエイリアスを指定します。
手順 4 で指定したホスト名と同じ文字列を指定してください。
11. 秘密鍵のパスワードを指定します。
12. キーアルゴリズムを指定します。
RSA だけがサポートされています。
13. キーサイズを指定します。

2048 ビットだけがサポートされています。

14. 署名アルゴリズムを指定します。

SHA256withRSA, SHA1withRSA および MD5withRSA がサポートされています。

15. キーペアと自己署名証明書の有効日数を指定します。

16. キーストアパスワードを指定します (最低 6 文字)。

17. 変更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。

HiKeytool でセキュリティ設定を続けて実施する場合、設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば、変更が有効になります。

操作結果

キーペアと自己署名証明書が作成され、Device Manager サーバのキーストアファイル (デフォルト: keystore) に登録されます。

Windows の場合

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%keystore
```

Linux の場合

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/keystore
```



ヒント

Device Manager サーバのキーストアファイルは、Device Manager サーバの server.properties ファイルにある server.https.security.keystore プロパティで変更できます。

```
>1  
  
Enter Server Name [default=example]:example.com  
Enter Organizational Unit [default=Device Manager Administration]:  
Enter Organization Name [default=example]:Hitachi  
Enter your City or Locality:Yokohama  
Enter your State or Province:Kanagawa  
Enter your two-character country-code [default=JP]:  
Enter Key Alias [default=example]:example.com  
  
Passwords must only contain characters (A-Z,a-z), digits (0-9) and  
whitespaces.  
Do not enter special characters for your password!  
This may render your keystore damaged or unusable!  
  
Enter Key Password (6 characters minimum) [default=passphrase]:  
Enter Key Algorithm [default=RSA]:  
Enter Key Size [default=2048]:  
Enter Signature Algorithm [default=SHA256withRSA]:  
Enter number of days valid [default=365]:  
  
Passwords must only contain characters (A-Z,a-z), digits (0-9) and  
whitespaces.  
Do not enter special characters for your password!  
This may render your keystore damaged or unusable!
```

```
Enter KeyStore Password (6 characters minimum) [default=passphrase]:  
  
Creating new X500Name for  
example.com...  
  
Creating the Device Manager Server KeyPair for example.com at:  
C:\Program Files\HiCommand\DeviceManager\HiCommandServer\keystore  
<this can take up to a minute>  
Updating KeyStore password in server.properties ...  
Saving new KeyStore password to disk...  
Updating keypass in server properties...  
Saving new keypass to disk...  
  
All done.
```

関連タスク

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

関連参照

- [付録 A.8.3 server.https.security.keystore](#)

5.3.2 Device Manager サーバの SSL/TLS の有効化

Device Manager サーバの SSL/TLS を有効にするには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Set Device Manager Server Security Level] を選択します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- Device Manager サーバの自己署名証明書とキーペアの作成

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、2 ([Set Device Manager Server Security Level]) を指定します。
3. 2 ([TLS/SSL]) を指定します。
4. 変更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。

HiKeytool でセキュリティ設定を続けて実施する場合、設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば、変更が有効になります。

操作結果

```
>2  
  
Current Device Manager Server Security Level = User Logon (Basic  
Authentication)  
  
Options:  
1) User Logon (Basic Authentication)  
2) TLS/SSL (Secure Sockets)  
Enter selection: [default=2]:2  
  
Device Manager Server Security level set to: TLS/SSL Secure Socket  
You must restart the Device Manager Server for this change to take  
effect.
```

5.3.3 Device Manager サーバの証明書発行要求の作成

Device Manager サーバで証明書発行要求 (CSR) を作成するには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Generate CSR] を選択します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- Device Manager サーバのキーペアの作成
- Device Manager サーバでの SSL/TLS の有効化

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、3 ([Generate CSR]) を指定します。

操作結果

証明書発行要求が、次の場所に <ホスト名>.csr というファイル名で保存されます。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > ¥DeviceManager
¥HiCommandServer
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer
```

```
>3
```

```
Generating CSR...
CSR has been written to disk and saved at:
C:¥Program Files¥HiCommand¥DeviceManager¥HiCommandServer¥example.com.csr
All done!
```

作成される証明書発行要求の例を次に示します。

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC0zCCAbsCAQAwgY0xCzAJBgNVBAYTAKpQMREwDwYDVQQIEWhLYW5hZ2F3YTERMA8GA1UEB
xMIWW9rb2hhbWExEjAQBgNVBAoTCVMxMDM4NDc3MzEwMC4GA1UECxMnSG1Db21tYW5kIERl
dm1jZSBNYW5hZ2VyeIEFkbWluaXN0cmF0aW9uMRlwEAYDVQQDEWlTMTAzODQ3NzMwggEiMA0GCSq
GSIsb3DQEB
:
省略
:
wEYfCLrKBtlGrzv9eRpclQIs5bRbzM9S4KGPwbnYKym31281m6MiN27U7t0XW0oI73xC/
jJVlK25+s0tVyerx09zVYvtirW02Q+H4KUEq6tJHo79nY5W2OCVsWr/Vuyh
+XvbVtVnLI8oVPkMUIFnhOQijq+VPSaSlKjiba6NA/+jgT4Fe0dfq31zJ8ELIN/
YtlKCl8txEhO2MXwOQ==
-----END NEW CERTIFICATE REQUEST-----
```



メモ

実際の CSR にはキャリッジリターンや改行が余計に含まれています。これらがないと、認証局への送信時に正しく処理されません。

5.3.4 Device Manager サーバのサーバ証明書の認証局への申請

認証局へのサーバ証明書の申請は、通常、オンラインで行えます。作成した Device Manager サーバの証明書発行要求 (CSR) を任意の認証局に送信し、電子署名を受けます。

前提条件

- Device Manager サーバの証明書発行要求の作成
- 次の情報の確認
 - 認証局への申請方法や対応状況
X.509 DER 形式または X.509 PEM 形式のサーバ証明書を発行してもらう必要があります。申請方法については、使用する認証局の Web サイトなどで確認してください。

操作手順

1. 作成した証明書発行要求を認証局に送付します。

操作結果

認証局で発行されたサーバ証明書は、通常、E メールで送付されます。次の場所に <ホスト名>.cer というファイル名で保存しておくことをお勧めします。

Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>\DeviceManager  
\HiCommandServer
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer
```

認証局によっては、サーバ証明書が .cer 拡張子付きの添付書類として返送されることがあります。また、認証局が応答を Eメールの本文にテキストとして埋め込んで返送してきた場合は、テキストエディターを使用して応答を新規ファイルに保存してください。



メモ

- 認証局からの返答は保存しておいてください。
- 認証局が発行する証明書には有効期限があります。期限が切れる前に再発行してもらう必要があります。証明書の有効期限は、HiKeytool を使用して確認してください。
- 認証局によってサーバ証明書に設定された有効日数は、HiKeytool で設定した値よりも優先されます。キーペアとそれに関連するサーバ証明書の期限が切れると、SSL/TLS を介した安全な接続を確立できなくなります。サーバ証明書を更新する必要がある期日を書き留めておいてください。

次に認証局で発行されたサーバ証明書の例を示します。

```
-----BEGIN CERTIFICATE-----  
MIIDMDCCApmgAwIBAgIDOBcYMA0GCSqGSIb3DQEBAUAMIGHMQswCQYDVQQGEwJa  
QTEiMCAGA1UECBZRk9SIFRFU1RJTkcgUUVVSUE9TRVMgT05MWTEdMBsGA1UEChMU  
VGhhd3RlIENlcnRpZmljYXRpb24xZnZAVBgNVBAsTD1RlRFU1QgVEVTVCBURVNUMRww  
:  
省略  
:  
ADANBgkqhkiG9w0BAQQFAAOBgQBtzeFG4IfvpPnA7G/khD4rrT1TvjbK4Y1pcROM  
cel43uUfKgNYgY35UukoNtd120XOoudLwKvJu5JK7846zWIbEJmCr5BYlmywZuao  
MQdXMyPOUnqucgg44/JG2F27xqP4atWEZsN1j5R7XGGXi4RPAO5Y0YbbbvMJD0QR
```

関連タスク

- [5.3.16 Device Manager サーバのサーバ証明書の確認](#)

5.3.5 Device Manager サーバのキーストアーへのサーバ証明書のインポート

Device Manager サーバのキーストアーに、認証局で発行されたサーバ証明書をインポートするには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Import Digitally Signed Certificate] を選択します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 既存のキーペアの削除
キーストアーに格納できるキーペアは 1 つだけです。複数のキーペアが格納されていると、Device Manager サーバをセキュアモードで使用する際に問題が発生するおそれがあります。
- Device Manager サーバのサーバ証明書の入手
- 証明書のインポート
サーバ証明書を発行した認証局から、中間認証局、ルート認証局に至る全認証局の証明書を、Device Manager サーバのトラストストアにインポートします。

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、4 ([Import Digitally Signed Certificate]) を指定します。
3. サーバ証明書の格納場所を絶対パスで指定します。
4. 変更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。
HiKeytool でセキュリティ設定を続けて実施する場合、設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば、変更が有効になります。

操作結果

サーバ証明書が Device Manager サーバのキーストアーファイル (デフォルト: keystore) にインポートされます。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > \DeviceManager
\HiCommandServer\keystore
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/keystore
```



ヒント

Device Manager サーバのキーストアーファイルは、Device Manager サーバの server.properties ファイルにある server.https.security.keystore プロパティで変更できます。

```
>4
```

```
Preparing to import digitally signed certificate.
```

```
Enter the location of the digitally signed certificate
[default=C:\Program
Files\HiCommand\DeviceManager\HiCommandServer\example.com.cer]:
Beginning import...

Digitally signed certificate imported. You must restart the Device
Manager
Server for the changes to take effect.
```

関連タスク

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

関連参照

- [付録 A.8.3 server.https.security.keystore](#)

5.3.6 Device Manager サーバのキーペア情報の参照（標準モード）

Device Manager サーバのキーストアーに登録されたキーペアの情報を標準モードで参照するには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Display contents of Device Manager Server KeyStore] を選択します。

前提条件

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

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、5 ([Display contents of Device Manager Server KeyStore]) を指定します。

操作結果

キーペアのエイリアス名、作成日、MD5 Fingerprints が次のように表示されます。

```
>5
Listing Contents of Device Manager Server KeyStore

Alias
=====
1) example.com, Tue Apr 01 09:48:02 JST 2008
   MD5 Fingerprints:FC:59:A5:8A:5A:27:5E:70:E4:6B:21:30:39:D1:00:1D
```

5.3.7 Device Manager サーバのキーペア情報の参照（詳細モード）

Device Manager サーバのキーストアーに登録されたキーペアの情報を詳細モードで参照するには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Display verbose contents of Device Manager Server KeyStore] を選択します。

前提条件

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

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、6 ([Display verbose contents of Device Manager Server KeyStore]) を指定します。

操作結果

キーペアの詳細情報が次のように表示されます。

```
>6
Listing Contents of Device Manager Server KeyStore
1)
alias: example.com
Certificate chain length: 1
Issued by: example.com: Hitachi
Server Name: example.com
Organizational Unit: Device Manager Administration
Organization: Hitachi
Locality: Yokohama
State: Kanagawa
Country: JP
Created: Tue Apr 01 09:48:02 JST 2008
Entry Type: Key Entry
Certificate Version: 1
Serial Number: 47f18642
Valid from: Tue Apr 01 09:48:02 JST 2008
Valid to: Wed Apr 01 09:48:02 JST 2009
Certificate: VALID
MD5 Fingerprints: FC:59:A5:8A:5A:27:5E:70:E4:6B:21:30:39:D1:00:1D
SHA1 Fingerprints:
F7:C4:2D:F3:E3:F3:5A:AB:E1:57:D1:E8:9C:80:07:89:2C:2A:48:7A
```

5.3.8 Device Manager サーバのキーストアーからのキーペアの削除

Device Manager サーバのキーストアーからキーペアを削除するには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Delete an entry from the Device Manager Server KeyStore] を選択します。

前提条件

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

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、7 ([Delete an entry from the Device Manager Server KeyStore]) と指定します。
3. 削除するキーペアの番号を指定します。
4. 表示されたメッセージを確認して、[y] キーを押します。
5. 変更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。

HiKeytool でセキュリティ設定を続けて実施する場合、設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば、変更が有効になります。

操作結果

```
>7
Delete an entry from the Device Manager Server KeyStore.

Alias
=====
1) example.com, Tue Apr 01 09:48:02 JST 2008
   MD5 Fingerprints:FC:59:A5:8A:5A:27:5E:70:E4:6B:21:30:39:D1:00:1D
Enter number of alias to delete (0 to abort) [default=0]:1
Delete example.com [1] ? [default=No]:y
```


5.3.9 Device Manager サーバのキーペアのパスワードの変更

Device Manager サーバのキーペアのパスワードを変更するには、HiKeytool のメインメニュー [SSL configuration for Device Manager Server]-[Change Device Manager Server KeyPair/Self-Signed Certificate Keypass] を選択します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 次の情報の確認
 - Device Manager サーバのキーストアパスワード
 - Device Manager サーバのキーペアの現在のパスワード

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、8 ([Change Device Manager Server KeyPair/Self-Signed Certificate Keypass]) を指定します。
3. Device Manager サーバのキーストアパスワードを指定します。
4. 現在のキーペアのパスワードを指定します。
5. 新しいキーペアのパスワードを指定します。
使用できる文字は次のとおりです。
A~Z a~z 0~9 空白文字
大文字と小文字は区別されます。ほかの文字を指定すると、キーストアを使用できなくなります。
6. 新しいパスワードを再指定します。
7. 変更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。
HiKeytool でセキュリティ設定を続けて実施する場合、設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば、変更が有効になります。

5.3.10 Device Manager サーバのキーストアパスワードの変更

Device Manager サーバのキーストアのパスワードを変更するには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Change Device Manager Server KeyStore Password] を選択します。

前提条件

次の情報の確認

- Device Manager サーバの現在のキーストアパスワード

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、9 ([Change Device Manager Server KeyStore Password]) を指定します。
3. 現在の Device Manager サーバのキーストアパスワードを指定します。
4. 新しいキーストアパスワードを指定します。
使用できる文字は次のとおりです。
A~Z a~z 0~9 空白文字

大文字と小文字は区別されます。ほかの文字を指定すると、キーストアーを使用できなくなります。

5. 新しいパスワードを再指定します。
6. 変更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。
HiKeytool でセキュリティ設定を続けて実施する場合、設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば、変更が有効になります。

5.3.11 Device Manager サーバのトラストストアへの証明書のインポート

Device Manager サーバのトラストストアに、証明書をインポートするには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Import Certificate to Device Manager Server TrustStore] を選択します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 証明書の入手
X.509 DER 形式または X.509 PEM 形式の証明書が必要です。サーバ証明書を発行した認証局から、中間認証局、ルート認証局に至る全認証局の証明書を準備してください。

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、10 ([Import Certificate to Device Manager Server TrustStore]) を指定します。
3. インポートする証明書のエイリアス名を指定します。
4. インポートする証明書の絶対パスを指定します。
5. インポートする証明書が複数ある場合は、手順 2～手順 4 を繰り返します。
6. 変更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。
HiKeytool でセキュリティ設定を続けて実施する場合、設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば、変更が有効になります。

関連参照

- [5.1.22 トラストストア](#)

5.3.12 Device Manager サーバのトラストストア情報の参照 (標準モード)

Device Manager サーバのトラストストアに登録されたサーバ証明書の情報を標準モードで参照するには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Display contents of Device Manager Server TrustStore] を選択します。

前提条件

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

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、11 ([Display contents of Device Manager Server TrustStore]) を指定します。

操作結果

サーバ証明書のエイリアス名、作成日、および MD5 Fingerprints が表示されます。

```
>11
Listing Contents of Device Manager Server TrustStore

Alias
=====
1) verisignclass3ca, Fri Nov 25 12:04:38 JST 2005
   MD5 Fingerprints:10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
2) verisignclass3g2ca, Fri Nov 25 12:04:37 JST 2005
   MD5 Fingerprints:A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:5C:E9
3) verisignclass2g2ca, Fri Nov 25 12:04:35 JST 2005
   MD5 Fingerprints:2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
4) verisignclass1g2ca, Fri Nov 25 12:04:34 JST 2005
   MD5 Fingerprints:DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:41:83
5) verisignclass3g3ca, Fri Nov 25 12:04:37 JST 2005
   MD5 Fingerprints:CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:57:44:61:92:09
6) verisignclass2g3ca, Fri Nov 25 12:04:36 JST 2005
   MD5 Fingerprints:F8:BE:C4:63:22:C9:A8:46:74:8B:B8:1D:1E:4A:2B:F6
7) verisignclass1g3ca, Fri Nov 25 12:04:34 JST 2005
   MD5 Fingerprints:B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:95:73
8) verisignclass1ca, Fri Nov 25 12:04:35 JST 2005
   MD5 Fingerprints:97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62
9) verisignserverca, Fri Nov 25 12:04:38 JST 2005
   MD5 Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
10) verisignclass2ca, Fri Nov 25 12:04:36 JST 2005
    MD5 Fingerprints:B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:77:3E
```

関連参照

- [5.1.22 トラストストア](#)

5.3.13 Device Manager サーバのトラストストア情報の参照（詳細モード）

Device Manager サーバのトラストストアに登録されたサーバ証明書の情報を詳細モードで参照するには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Display verbose contents of Device Manager Server TrustStore] を選択します。

前提条件

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

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、12 ([Display verbose contents of Device Manager Server TrustStore]) を指定します。

操作結果

サーバ証明書の詳細情報が次のように表示されます。

```
>12
Listing Contents of Device Manager Server TrustStore

1)
alias: verisignclass3ca
Issued by: "VeriSign, Inc."
Organizational Unit: Class 3 Public Primary Certification Authority
Organization: "VeriSign, Inc."
```

```
Country: US
Created: Fri Nov 25 12:04:38 JST 2005
Entry Type: Trusted Certificate
Certificate Version: 1
Serial Number: 70bae41d10d92934b638ca7b03ccbabf
Valid from: Mon Jan 29 09:00:00 JST 1996
Valid to: Wed Aug 02 08:59:59 JST 2028
Certificate: VALID
MD5 Fingerprints: 10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
SHA1 Fingerprints:
74:2C:31:92:E6:07:E4:24:EB:45:49:54:2B:E1:BB:C5:3E:61:74:E2
```

関連参照

- [5.1.22 トラストストア](#)

5.3.14 Device Manager サーバのトラストストアからのサーバ証明書の削除

Device Manager サーバのトラストストアに登録されたサーバ証明書を削除するには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Delete an entry from the Device Manager Server TrustStore] を選択します。

前提条件

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

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、13 ([Delete an entry from the Device Manager Server TrustStore]) を指定します。
3. 削除するサーバ証明書の番号を指定します。
4. 表示されたメッセージを確認して、[y] キーを押します。
5. 変更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。

HiKeytool でセキュリティ設定を続けて実施する場合、設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば、変更が有効になります。

操作結果

指定したエントリが削除され、Device Manager サーバのトラストストアの内容が再び表示されます。削除が完了したことを確認してください。

```
>13
Delete an entry from the Device Manager Server TrustStore.

Alias
=====
1) verisignclass3ca, Fri Nov 25 12:04:38 JST 2005
   MD5 Fingerprints:10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
2) verisignclass3g2ca, Fri Nov 25 12:04:37 JST 2005
   MD5 Fingerprints:A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:5C:E9
3) verisignclass2g2ca, Fri Nov 25 12:04:35 JST 2005
   MD5 Fingerprints:2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
4) verisignclass1g2ca, Fri Nov 25 12:04:34 JST 2005
   MD5 Fingerprints:DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:41:83
5) verisignclass3g3ca, Fri Nov 25 12:04:37 JST 2005
   MD5 Fingerprints:CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:57:44:61:92:09
6) verisignclass2g3ca, Fri Nov 25 12:04:36 JST 2005
   MD5 Fingerprints:F8:BE:C4:63:22:C9:A8:46:74:8B:B8:1D:1E:4A:2B:F6
7) verisignclass1g3ca, Fri Nov 25 12:04:34 JST 2005
```

```
MD5 Fingerprints:B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:95:73
8) verisignclass1ca, Fri Nov 25 12:04:35 JST 2005
MD5 Fingerprints:97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62
9) verisignserverca, Fri Nov 25 12:04:38 JST 2005
MD5 Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
10) verisignclass2ca, Fri Nov 25 12:04:36 JST 2005
MD5 Fingerprints:B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:77:3E

Enter number of alias to delete (0 to abort) [default=0]:1

Delete verisignclass3ca [1] ? [default=No]:
```

関連参照

- [5.1.22 トラストストア](#)

5.3.15 Device Manager サーバのトラストストアパスワードの変更

Device Manager サーバのトラストストアパスワードを変更するには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Change Device Manager Server TrustStore Password] を選択します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 次の情報の確認
 - Device Manager サーバのトラストストアの現在のパスワード

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、14 ([Change Device Manager Server TrustStore Password]) を指定します。
3. 現在のトラストストアパスワードを指定します。
4. 新しいトラストストアパスワードを指定します。
使用できる文字は次のとおりです。
A~Z a~z 0~9 空白文字
大文字と小文字は区別されます。ほかの文字を指定すると、キーストアーを使用できなくなります。
5. 新しいパスワードを再指定します。
6. 変更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。
HiKeytool でセキュリティ設定を続けて実施する場合、設定ごとに再起動する必要はありません。HiKeytool での設定がすべて終了した時点で再起動すれば、変更が有効になります。

関連参照

- [5.1.22 トラストストア](#)

5.3.16 Device Manager サーバのサーバ証明書の確認

Device Manager サーバのサーバ証明書を確認するには、HiKeytool を使用します。

サーバ証明書には有効期限があります。有効期限切れに注意してください。

前提条件

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

操作手順

1. HiKeytool を起動し、メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
2. サーバ用メインメニューで、6 ([Display verbose contents of Device Manager Server KeyStore]) を指定します。

操作結果

サーバ証明書の詳細情報が表示されます。「Valid to:」行を確認してください。

関連タスク

- [5.3.7 Device Manager サーバのキーペア情報の参照 \(詳細モード\)](#)

5.4 SSL サーバの構築 (Host Data Collector)

Host Data Collector を SSL サーバとして使用するためには、キーペアとサーバ証明書を準備する必要があります。

5.4.1 Host Data Collector のキーペアおよび証明書発行要求の作成

Host Data Collector マシンでキーペアと証明書発行要求を作成するには、hdc_ssltool コマンドを使用します。証明書発行要求および自己署名証明書は、秘密鍵のキーサイズ 2048 ビット、キーアルゴリズム RSA、署名アルゴリズム SHA256withRSA で作成されます。なお、自己署名証明書は暗号化通信のテストなどの目的でだけ使用することをお勧めします。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- Host Data Collector の既存のキーストアファイルの削除 (再作成する場合)
Host Data Collector で作成できるキーストアファイルは 1 つだけです。

操作手順

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_ssltool.bat -key <キーストアファイル名> -csr <証明書発行要求ファイル>  
-keypass <秘密鍵のパスワード> -storepass <キーストアパスワード>  
> [-cert <自己署名証明書ファイル>] [-validity <有効日数>] [-dname <DN >]
```

Linux の場合 :

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/bin/  
hdc_ssltool.sh -key <キーストアファイル名> -csr <証明書発行要求ファイル>  
-keypass <秘密鍵のパスワード> -storepass <キーストアパスワード>  
[-cert <自己署名証明書ファイル>] [-validity <有効日数>] [-dname <DN >]
```

オプション

key

キーストアファイルの出力先を絶対パスで指定します。

csr

証明書発行要求の出力先を絶対パスで指定します。

keypass

秘密鍵のパスワードを 6 文字以上で指定します。

keypass オプションと storepass オプションには、同じパスワードを指定してください。

storepass

キーストアのパスワードを 6 文字以上で指定します。

storepass オプションと keypass オプションには、同じパスワードを指定してください。

cert

自己署名証明書の出力先を絶対パスで指定します。

validity

自己署名証明書の有効期間を日数で指定します。指定を省略した場合、有効期間は 3650 日になります。

dnname

自己署名証明書と証明書発行要求に記述する DN を指定します。dnname オプションの指定を省略してコマンドを実行すると、対話形式で DN を指定できます。

関連タスク

- [5.2.1 Hitachi Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成](#)

5.4.2 Host Data Collector のサーバ証明書の認証局への申請

認証局へのサーバ証明書の申請は、通常、オンラインで行えます。作成した Host Data Collector の証明書発行要求 (CSR) を認証局に送信し、電子署名を受けます。

前提条件

- Host Data Collector の証明書発行要求の作成
 - 次の情報の確認
 - 認証局への申請方法や対応状況
- 利用する認証局が SHA256withRSA での署名に対応していることを確認してください。申請方法については、使用する認証局の Web サイトなどで確認してください。

操作手順

1. 作成した証明書発行要求を認証局に送付します。

操作結果

認証局で発行されたサーバ証明書は、通常、Eメールで送付されます。認証局からの返答は保存しておいてください。



メモ

認証局が発行する証明書には有効期限があります。期限が切れる前に再発行してもらう必要があります。証明書の有効期限は、keytool ユーティリティを使用して確認してください。

関連タスク

- [5.4.4 Host Data Collector のサーバ証明書の確認](#)

5.4.3 Host Data Collector のサーバ証明書のキーストアーへのインポート

Host Data Collector のキーストアーにサーバ証明書をインポートするには、keytool ユーティリティを使用します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 認証局の証明書の入手
サーバ証明書を発行した認証局から、中間認証局、ルート認証局に至る全認証局の証明書が必要です。
- 認証局で署名された Host Data Collector のサーバ証明書の入手
- 次の情報の確認
 - キーストアーファイルの情報
自己署名証明書の作成時に用意したキーストアーファイルの情報が必要です。
 - 絶対パス
 - アクセスパスワード

操作手順

1. 次のコマンドを実行して、認証局の証明書をインポートします。

Windows の場合：

```
<Host Data Collector のインストールフォルダ>%HDC%Base%uCP%jdk%jre%bin%keytool -import -alias <エイリアス名> -keystore <キーストアーファイル名> -file <証明書のファイル名>
```

Linux の場合：

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/uCP%jdk%jre/bin/keytool -import -alias <エイリアス名> -keystore <キーストアーファイル名> -file <証明書のファイル名>
```

- alias：キーストアー内で証明書を識別するための名称を指定します。
認証局の証明書のエイリアス名には、hdc 以外の任意の名称を指定してください。
 - keystore：キーストアーファイルを絶対パスで指定します。
 - file：認証局の証明書の格納場所を絶対パスで指定します。
2. 次のコマンドを実行して、Host Data Collector のサーバ証明書をインポートします。

Windows の場合：

```
<Host Data Collector のインストールフォルダ>%HDC%Base%uCP%jdk%jre%bin%keytool -import -alias hdc -keystore <キーストアーファイル名> -file <証明書のファイル名>
```

Linux の場合：

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/uCP%jdk%jre/bin/keytool -import -alias hdc -keystore <キーストアーファイル名> -file <証明書のファイル名>
```

- alias：キーストアー内でサーバ証明書を識別するための名称を指定します。
Host Data Collector のサーバ証明書のエイリアス名には、hdc を必ず指定してください。
- keystore：キーストアーファイルを絶対パスで指定します。
- file：サーバ証明書の格納場所を絶対パスで指定します。

5.4.4 Host Data Collector のサーバ証明書の確認

Host Data Collector のサーバ証明書を確認するには、keytool ユーティリティを使用します。サーバ証明書には有効期限があります。有効期限切れに注意してください。

操作手順

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%uCPSB%jdk%jre%bin%keytool -printcert -v -file <証明書のファイル名>
```

Linux の場合：

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/uCPSB/jdk/jre/bin/keytool -printcert -v -file <証明書のファイル名>
```

5.5 SSL クライアントの構築

SSL/TLS で通信するためには、SSL サーバで作成されたサーバ証明書を SSL クライアントにインポートする必要があります。

5.5.1 Device Manager サーバのトラストストアファイルのダウンロード

Web ブラウザー経由で、Device Manager サーバのトラストストアファイル (HiCommandCerts) をダウンロードします。

前提条件

- Device Manager サーバのサーバ証明書のインポート (認証局が発行したサーバ証明書を使用する場合)
 - トラストストアへの証明書のインポート
 - キーストアへのサーバ証明書のインポート
- Device Manager サーバの自己署名証明書の作成 (自己署名証明書を使用する場合)
自己署名証明書は暗号化通信のテストなどの目的でだけ使用することをお勧めします。
- 次の情報の確認
 - Device Manager サーバの非 SSL 通信用のポート番号 (デフォルト : 2001)
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 のユーザーアカウント

操作手順

1. 管理サーバで Web ブラウザーや OS のコマンドなどを使用して、次の URL からトラストストアファイルをダウンロードします。

ユーザーアカウントを指定してダウンロードしてください。

```
http://<ループバックの IP アドレスまたはループバックのホスト名>:<Device Manager サーバのポート番号>/service/HiCommandCerts
```

関連タスク

- [5.3.1 Device Manager サーバのキーペアと自己署名証明書の作成](#)

- [5.3.5 Device Manager サーバのキーストアへのサーバ証明書のインポート](#)
- [5.3.11 Device Manager サーバのトラストストアへの証明書のインポート](#)

関連参照

- [付録 A.2.2 server.http.port](#)

5.5.2 Device Manager CLI で使用するトラストストアファイルの作成

Device Manager CLI で使用するトラストストアファイルを作成するには、keytool ユーティリティを使用して、認証局の証明書がインポートされたトラストストアファイルを作成する必要があります。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 認証局の証明書の入手
Device Manager サーバのサーバ証明書を発行した認証局から、ルート認証局までの全認証局の証明書がチェインされた状態で必要です。

操作手順

1. 次のコマンドを実行して、認証局の証明書がインポートされたトラストストアファイルを作成します。

Windows の場合

```
<Hitachi Command Suite のインストールフォルダ>%Base64%uCPSB%jdk%jre%bin
%keytool -import -trustcacerts -alias <エイリアス名> -keystore <トラストストアファイル名> -file <証明書のファイル名>
```

Linux の場合

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/
uCPSB/jdk/jre/bin/keytool -import -trustcacerts -alias <エイリアス名>
> -keystore <トラストストアファイル名> -file <証明書のファイル名>
```

- alias: トラストストア内で証明書を識別するための名称を指定します。任意の名称を指定してください。
- keystore: トラストストアファイルを絶対パスで指定します。
- file: 認証局の証明書の格納場所を絶対パスで指定します。

関連タスク

- [5.3.4 Device Manager サーバのサーバ証明書の認証局への申請](#)

5.5.3 Device Manager サーバの自己署名証明書のエクスポート

ダウンロードしたトラストストアファイル (HiCommandCerts) から、Device Manager サーバの自己署名証明書をエクスポートするには、hcnds64keytool ユーティリティ (Windows の場合) または keytool ユーティリティ (Linux の場合) を使用します。

前提条件

- Device Manager サーバのトラストストアファイルのダウンロード
- 次の情報の確認

- Device Manager サーバのキーペアのエイリアス名
HiKeytool で確認できます。

操作手順

1. 次のコマンドを実行します。

Windows の場合 :

```
<Hitachi Command Suite のインストールフォルダ>%Base64%bin
%hcnds64keytool -export -keystore <トラストストアファイル> -alias <
エイリアス名> -file <サーバ証明書>
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/
uCPSB/jdk/bin/keytool -export -keystore <トラストストアファイル> -
alias <エイリアス名> -file <サーバ証明書>
```

- keystore : トラストストアファイルのパスを指定します。
 - alias : キーペアのエイリアス名を指定します。
 - file : 出力する自己署名証明書ファイルのパスを指定します。
2. Device Manager サーバのトラストストアファイルのパスワードには何も入力しないで、
[Enter] キーを押します。

関連タスク

- [5.3.6 Device Manager サーバのキーペア情報の参照 \(標準モード\)](#)

5.5.4 Web ブラウザーへの証明書のインポート (Internet Explorer の場合)

GUI を使用するためには、証明書を管理クライアント (GUI) の Web ブラウザーにインポートしておく必要があります。

前提条件

- 証明書の入手
認証局を使用する場合は、次のサーバ証明書を発行した認証局から、ルート認証局までの全認証局の証明書がチェーンされた状態で必要です。
 - Hitachi Command Suite 共通コンポーネント
 - Device Manager サーバ

操作手順

1. Internet Explorer を起動し、[ツール] - [インターネット オプション] を選択します。
[ツール] 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。
2. [コンテンツ] タブで [証明書] ボタンをクリックし、Web ブラウザーに証明書をインポートします。

関連タスク

- [5.2.1 Hitachi Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成](#)
- [5.2.2 Hitachi Command Suite 共通コンポーネントのサーバ証明書の認証局への申請](#)
- [5.3.4 Device Manager サーバのサーバ証明書の認証局への申請](#)

5.5.5 Web ブラウザーへの証明書のインポート（Firefox の場合）

GUI を使用するためには、証明書を管理クライアント（GUI）の Web ブラウザーにインポートしておく必要があります。

前提条件

- 証明書の入手
認証局を使用する場合は、次のサーバ証明書を発行した認証局から、ルート認証局までの全認証局の証明書がチェーンされた状態で必要です。
 - Hitachi Command Suite 共通コンポーネント
 - Device Manager サーバ

操作手順

1. Firefox を起動し、次のメニューを選択します。

Windows :

[ツール] - [オプション]

Linux :

[編集] - [設定]

2. [詳細] を選択します。
3. [暗号化] タブで [証明書を表示] ボタンをクリックし、Web ブラウザーに証明書をインポートします。

関連タスク

- [5.2.1 Hitachi Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成](#)
- [5.2.2 Hitachi Command Suite 共通コンポーネントのサーバ証明書の認証局への申請](#)
- [5.3.4 Device Manager サーバのサーバ証明書の認証局への申請](#)

5.5.6 Web ブラウザーへの証明書のインポート（Google Chrome の場合）

GUI を使用するためには、証明書を管理クライアント（GUI）の Web ブラウザーにインポートしておく必要があります。

前提条件

- 証明書の入手
認証局を使用する場合は、次のサーバ証明書を発行した認証局から、ルート認証局までの全認証局の証明書がチェーンされた状態で必要です。
 - Hitachi Command Suite 共通コンポーネント
 - Device Manager サーバ

操作手順

1. Google Chrome を起動し、[Google Chrome の設定] - [設定] を選択します。
2. [詳細設定を表示] をクリックします。
3. [HTTPS/SSL] メニューの [証明書の管理] ボタンをクリックし、Web ブラウザーに証明書をインポートします。

関連タスク

- [5.2.1 Hitachi Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成](#)

- [5.2.2 Hitachi Command Suite 共通コンポーネントのサーバ証明書の認証局への申請](#)
- [5.3.4 Device Manager サーバのサーバ証明書の認証局への申請](#)

5.5.7 ポップアップブロックの設定変更

Hitachi Command Suite 製品の URL を SSL 通信用に変更したら、Web ブラウザーのポップアップブロックの設定にも、SSL 通信用の URL を登録する必要があります。

前提条件

- Hitachi Command Suite 製品の URL の変更
- 次の情報の確認
 - 管理サーバの IP アドレスまたはホスト名

操作手順

1. Web ブラウザーのポップアップブロックの設定で、許可する Web サイトのアドレスに次の URL を登録します。

`https://<管理サーバの IP アドレスまたはホスト名>`

関連タスク

- [2.8 Hitachi Command Suite 製品の URL の変更 \(hcmds64chgurl コマンド\)](#)

5.5.8 Device Manager CLI の実行マシンでの SSL/TLS の有効化

Device Manager CLI で使用するトラストストアファイルの格納場所を環境変数 `HDVM_CLI_CERTS_PATH` に設定します。

また、`HiCommandCLI.properties` ファイルに `HiCommandCLI.serverurl` プロパティや `secure` プロパティを設定しておくこと、Device Manager CLI を実行する際に、`URL` や `secure (s)` オプションの指定を省略できます。

前提条件

- トラストストアファイルの作成（認証局を使う場合）
認証局の証明書がインポートされたトラストストアファイルを作成してください。作成したトラストストアファイルのファイル名を `HiCommandCerts` に変更して、Device Manager CLI の実行ファイル (`HiCommandCLI.bat`) が格納されたディレクトリに保存してください。
- Device Manager サーバのトラストストアファイルの入手（自己署名証明書を使う場合）
安全な方法で管理サーバから取得し、ファイル名を変えないで、Device Manager CLI の実行ファイル (`HiCommandCLI.bat`) が格納されたディレクトリに保存してください。
- Device Manager CLI での Java 環境の設定
次の両方の条件を満たす環境では、Device Manager サーバと Device Manager CLI 間の通信に SSL/TLS を使用するに当たり、Device Manager CLI で使用する Java 環境を変更する必要があります。
 - Device Manager サーバがインストールされた管理サーバから Device Manager CLI を実行する。
 - Hitachi Command Suite に同梱された JDK を Device Manager CLI で使用している。
詳細は、マニュアル「*Hitachi Command Suite CLI リファレンスガイド*」を参照してください。
- 次の情報の確認

- 管理サーバの IP アドレスまたはホスト名
Device Manager サーバのサーバ証明書に設定されている Common Name を確認してください。
- Device Manager サーバの SSL 通信のポート番号（デフォルト：2443）
Device Manager サーバの server.properties ファイルにある server.https.port プロパティで確認できます。

操作手順

1. 環境変数 HDVM_CLI_CERTS_PATH に、トラストストアファイルの絶対パス（ファイル名を含む）を指定します。
2. HiCommandCLI.properties ファイルの設定を変更します。
HiCommandCLI.properties ファイルは、Device Manager CLI の実行ファイル（HiCommandCLI.bat）が格納されたディレクトリに格納されています。

- HiCommandCLI.serverurl プロパティ
Device Manager サーバの URL を次の形式で設定します。

```
HiCommandCLI.serverurl=https://<管理サーバの IP アドレスまたはホスト名>:  
<Device Manager サーバの SSL 通信のポート番号>/service
```

- secure プロパティ
true を設定します。雛型には secure プロパティが記載されていないため、次のとおり追記してください。

```
##### OPTIONS #####  
secure=true
```

関連参照

- [付録 A.2.3 server.https.port](#)

5.5.9 Tiered Storage Manager サーバのトラストストアファイルのダウンロード

Web ブラウザー経由で、Tiered Storage Manager サーバのトラストストアファイル（TieredStorageManagerCerts）をダウンロードします。

前提条件

- Tiered Storage Manager サーバの server.properties ファイルの設定
 - server.rmi.secure プロパティ
 - server.rmi.security.port プロパティ
- 次の情報の確認
 - HBase 64 Storage Mgmt Web Service の非 SSL 通信のポート番号（デフォルト：22015）
user_httpsd.conf ファイルで確認できます。
 - Tiered Storage Manager のユーザーアカウント

操作手順

1. 管理サーバで Web ブラウザーや OS のコマンドなどを使用して、次の URL からトラストストアファイルをダウンロードします。

ユーザーアカウントを指定してダウンロードしてください。

```
http://<ループバックの IP アドレスまたはループバックのホスト名>:<HBase 64  
Storage Mgmt Web Service のポート番号>/TieredStorageManager/  
TieredStorageManagerCerts
```

関連タスク

- [2.2 Hitachi Command Suite 共通コンポーネントで使用されるポートの変更](#)
- [付録 B.1.1 Tiered Storage Manager サーバのプロパティの変更](#)

関連参照

- [付録 B.2.2 server.rmi.security.port](#)
- [付録 B.6.1 server.rmi.secure](#)

5.5.10 Tiered Storage Manager CLI の実行マシンでの SSL/TLS の有効化

Tiered Storage Manager サーバのトラストストアファイル (TieredStorageManagerCerts) の格納場所を環境変数 HTSM_CLI_CERTS_PATH に設定します。

また、htsmcli.properties ファイルに htmsserver.location プロパティや option.secure プロパティを設定しておくこと、Tiered Storage Manager CLI を実行する際に、Tiered Storage Manager サーバのロケーションや secure (s) オプションの指定を省略できます。

前提条件

- Tiered Storage Manager サーバのトラストストアファイルの入手
安全な方法で管理サーバから取得しておきます。
- htsmcli.properties ファイルの雛型のコピー
次の場所にある雛型を任意の場所にコピーして使用してください。ただし、Windows の場合、ドライブ直下にはコピーしないでください。
 - 管理クライアントで Tiered Storage Manager CLI を実行する場合
Windows :
<システムドライブ>%TieredStorageManager%< Tiered Storage Manager のバージョン>%CLI%
Solaris, HP-UX または Linux :
/opt/TieredStorageManager/< Tiered Storage Manager のバージョン>/CLI/
 - 管理サーバで Tiered Storage Manager CLI を実行する場合
Windows :
<Hitachi Command Suite のインストールフォルダ>%TieredStorageManager
%CLI%
Linux :
<Hitachi Command Suite のインストールディレクトリ>/
TieredStorageManager/CLI/
- 環境変数 HTSM_CLI_HOME の設定
htsmcli.properties ファイルの格納ディレクトリを設定します。Windows の場合、パスは次の規則に従って指定してください。
 - パスを引用符 (") やアポストロフィ (') で囲まないでください。

- パスの終端にはパス区切り文字 (¥) を指定しないでください。
- パス区切り文字 (¥) は円記号でエスケープしてください。
- 次の情報の確認
 - 管理サーバのホスト名または IP アドレス
 - Tiered Storage Manager サーバの SSL 通信用のポート番号 (デフォルト : 24500)
Tiered Storage Manager サーバの `server.properties` ファイルにある `server.rmi.security.port` プロパティで確認できます。

操作手順

1. 環境変数 `HTSM_CLI_CERTS_PATH` に、トラストストアファイルの絶対パス (ファイル名を含む) を指定します。
サーバ証明書の格納先ディレクトリをカレントディレクトリにして Tiered Storage Manager CLI を実行する運用の場合は、`HTSM_CLI_CERTS_PATH` の設定は省略できます。
2. `htsmcli.properties` ファイルの設定を変更します。

- `htsmserver.location` プロパティ
Tiered Storage Manager サーバのロケーションを次の形式で指定します。

```
htsmserver.location=rmi://<管理サーバの IP アドレスまたはホスト名>:<Tiered Storage Manager サーバの SSL 通信用のポート番号>/HTSMserver
```

- `option.secure` プロパティ
`true` を設定します。雛型には `option.secure` プロパティが記載されていないため、次のとおり追記してください。

```
##### OPTIONS #####
option.secure=true
```

関連タスク

- [2.2 Hitachi Command Suite 共通コンポーネントで使用されるポートの変更](#)

関連参照

- [付録 B.2.2 server.rmi.security.port](#)

5.5.11 Hitachi Command Suite 共通コンポーネントのトラストストアへの証明書のインポート

証明書をトラストストア (`ldapcacerts` または `jssecacerts`) にインポートするには、`hcnds64keytool` ユーティリティ (Windows の場合) または `keytool` ユーティリティ (Linux の場合) を使用します。

前提条件

- 証明書の準備
安全な方法で取得してください。
- LDAP ディレクトリサーバとの通信に使う場合
LDAP ディレクトリサーバのサーバ証明書を発行した認証局から、ルート認証局までの全認証局の証明書がチェーンされた状態で必要です。Hitachi Command Suite 製品の要件に合ったものである必要があります。

- **Replication Manager** サーバとの通信に使う場合
 認証局を使うとき：
Device Manager サーバのサーバ証明書を発行した認証局から、ルート認証局までの全認証局の証明書がチェーンされた状態で必要です。
 自己署名証明書を使うとき：
Device Manager サーバの自己署名証明書をトラストストアファイルからエクスポートしておく必要があります。
- **Tuning Manager** サーバとの通信に使う場合
 認証局を使うとき：
Hitachi Command Suite 共通コンポーネントのサーバ証明書を発行した認証局から、ルート認証局までの全認証局の証明書がチェーンされた状態で必要です。
 自己署名証明書を使うとき：
Hitachi Command Suite 共通コンポーネントの自己署名証明書が必要です。
- 次の情報の確認
 - トラストストアファイルのパス
 - トラストストアへのアクセスパスワード（トラストストアがすでに存在する場合）

操作手順

1. 次のコマンドを実行します。

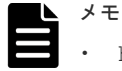
Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>%Base64%bin
%hcms64keytool -import -alias <エイリアス名> -file <証明書> -
keystore <トラストストアファイル名> -storepass <トラストストアへのア
クセスパスワード>
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/
uCPSE/jdk/bin/keytool -import -alias <エイリアス名> -file <証明書>
-keystore <トラストストアファイル名> -storepass <トラストストアへの
アクセスパスワード>
```

- **alias**：トラストストア内で証明書を識別するための名称を指定します。
 サーバ証明書が複数ある場合は、トラストストア内で使用されていない任意のエイリアス名を指定してください。
- **file**：証明書を指定します。
- **keystore**：インポート先のトラストストアファイルのパスを指定します。存在しない場合は、自動的に作成されます。
LDAP ディレクトリサーバのサーバ証明書は、`ldapcacerts` にインポートすることをお勧めします。ほかのプログラムと証明書を共有する場合は `jssecacerts` にインポートしてもかまいません。
Replication Manager サーバと **Device Manager** サーバ間、または **Tuning Manager** サーバと **Device Manager** サーバ間の通信で使用する証明書は、`jssecacerts` にインポートしてください。
- **storepass**：トラストストアへのアクセスパスワードを指定します。



メモ

- ・ hcmts64keytool ユーティリティまたは keytool ユーティリティで、トラストストア内のユニーク名、トラストストアのファイル名、およびパスワードを指定するときには、次の点に注意してください。
 - ・ ファイル名には次の記号を使用しないでください。
: , ; * ? " < > | -
 - ・ ファイル名は 255 バイト以内の文字列にしてください。
 - ・ トラストストア内のユニーク名、およびパスワードには引用符 (") を含めないでください。

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

関連タスク

- ・ [5.2.1 Hitachi Command Suite 共通コンポーネントの秘密鍵および証明書発行要求の作成](#)
- ・ [5.2.2 Hitachi Command Suite 共通コンポーネントのサーバ証明書の認証局への申請](#)
- ・ [5.3.4 Device Manager サーバのサーバ証明書の認証局への申請](#)
- ・ [9.1.2 Hitachi Command Suite のサービスの起動](#)
- ・ [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- ・ [5.1.22 トラストストア](#)

5.5.12 LDAP ディレクトリサーバのサーバ証明書の条件

管理サーバと LDAP ディレクトリサーバ間を StartTLS で通信する場合には、入手した LDAP ディレクトリサーバのサーバ証明書が次の条件を満たしていることを確認してください。

- ・ exauth.properties ファイルの次の属性に、LDAP ディレクトリサーバのサーバ証明書の CN (Subject 欄の CN) が設定されていること。
 - 認証方式が LDAP の場合
auth.ldap.<auth.server.name に指定した値>.host
 - 認証方式が RADIUS で、外部認可サーバとも連携する場合
外部認証サーバと外部認可サーバが同一マシンで稼働しているとき：
auth.radius.<auth.server.name に指定した値>.host
外部認証サーバと外部認可サーバが別のマシンで稼働しているとき：
auth.group.<ドメイン名>.host
 - 認証方式が Kerberos で、外部認可サーバとも連携する場合
auth.kerberos.<auth.kerberos.realm_name に指定した値>.kdc

関連タスク

- ・ [4.7 外部認証サーバと外部認可サーバの登録](#)

5.5.13 Hitachi Command Suite 共通コンポーネントのトラストストアにインポートされた証明書の確認

Hitachi Command Suite 共通コンポーネントのトラストストア (ldapcacerts または jssecacerts) にインポートされた証明書を確認するには、hcmts64keytool ユーティリティ (Windows の場合) または keytool ユーティリティ (Linux の場合) を使用します。

前提条件

次の情報の確認

- トラストストアファイルのパス
- トラストストアへのアクセスパスワード

操作手順

1. 次のコマンドを実行します。

Windows の場合 :

```
<Hitachi Command Suite のインストールフォルダ>%Base64%bin  
%hcmds64keytool -list -v -keystore <トラストストアファイル名> -  
storepass <トラストストアへのアクセスパスワード>
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/  
uCPSE/jdk/bin/keytool -list -v -keystore <トラストストアファイル名>  
-storepass <トラストストアへのアクセスパスワード>
```

- keystore : 証明書が格納されているトラストストアファイルのパスを指定します。
- storepass : トラストストアへのアクセスパスワードを指定します。

関連参照

- [5.1.22 トラストストア](#)

5.5.14 Hitachi Command Suite 共通コンポーネントのトラストストアにインポートされた証明書の削除

Hitachi Command Suite 共通コンポーネントのトラストストア (ldapcacerts または jssecacerts) にインポートされた証明書を削除するには、hcmds64keytool ユーティリティ (Windows の場合) または keytool ユーティリティ (Linux の場合) を使用します。

前提条件

次の情報の確認

- 削除する証明書のエイリアス名
- トラストストアファイルのパス
- トラストストアへのアクセスパスワード

操作手順

1. 次のコマンドを実行します。

Windows の場合 :

```
<Hitachi Command Suite のインストールフォルダ>%Base64%bin  
%hcmds64keytool -delete -alias <エイリアス名> -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/  
uCPSE/jdk/bin/keytool -delete -alias <エイリアス名> -keystore <トラ
```

```
ストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

- alias : 証明書のエイリアス名を指定します。
- keystore : 証明書が格納されているトラストストアファイルのパスを指定します。
- storepass : トラストストアへのアクセスパスワードを指定します。

関連タスク

- [5.5.13 Hitachi Command Suite 共通コンポーネントのトラストストアにインポートされた証明書の確認](#)

関連参照

- [5.1.22 トラストストア](#)


5.5.15 Replication Manager サーバと Device Manager サーバ間の通信プロトコルの変更

Replication Manager サーバと Device Manager サーバ間の通信プロトコルは、Replication Manager GUI の [Device Manager の編集] 画面で変更します。

前提条件

- 名前解決の設定
管理クライアントで、正サイトの管理サーバに関して、ホスト名から IP アドレスへ名前解決ができるようにしてください（例：管理クライアントの hosts ファイルへの登録）。
- トラストストア（jssecacerts）への Device Manager サーバのサーバ証明書のインポート
- 次の情報の確認
 - 接続する Device Manager サーバの IP アドレスまたはホスト名
 - 接続する Device Manager サーバの SSL 用のポート番号（デフォルト：2443）
接続する Device Manager サーバの server.properties ファイルにある server.https.port プロパティで確認できます。

操作手順

1. Device Manager の GUI の [設定] メニューから [レプリケーション管理] を選択します。
2. [エクスプローラ] メニューで、[管理者メニュー] - [情報取得元] をクリックします。
3. 表示されたツリーで [Device Manager] を選択します。
4. SSL/TLS で通信する Device Manager の  アイコンをクリックします。
5. [Device Manager の編集] 画面で通信プロトコルとポート番号を変更します。

関連参照

- [付録 A.2.3 server.https.port](#)

5.5.16 Device Manager サーバのトラストストアへの証明書のインポート

証明書を Device Manager サーバのトラストストアにインポートするには、HiKeytool のメインメニューで [SSL configuration for Device Manager Server] - [Import Certificate to Device Manager Server TrustStore] を選択します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 証明書の準備
安全な方法で取得してください。
 - 認証局を使う場合
Host Data Collector のサーバ証明書を発行した認証局から、ルート認証局までの全認証局の証明書がチェインされた状態で必要です。
 - 自己署名証明書を使う場合
Host Data Collector の自己署名証明書が必要です。

操作手順

1. 次のとおり実行して、HiKeytool を起動します。

Windows の場合

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager  
%HiCommandServer%HiKeytool.bat
```

Linux の場合

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/  
HiKeytool.sh
```

2. メインメニューで 1 ([SSL configuration for Device Manager Server]) を指定します。
3. サーバ用メインメニューで、10 ([Import Certificate to Device Manager Server TrustStore]) を指定します。
4. インポートする証明書のエイリアス名を指定します。
5. インポートする証明書の絶対パスを指定します。
6. インポートする証明書が複数ある場合は、手順 1～手順 5 を繰り返します。
7. 変更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。

関連タスク

- [5.4.1 Host Data Collector のキーペアおよび証明書発行要求の作成](#)
- [5.4.2 Host Data Collector のサーバ証明書の認証局への申請](#)
- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [5.1.22 トラストストア](#)

5.5.17 Device Manager サーバのトラストストアにインポートされた証明書の確認

Device Manager サーバのトラストストアにインポートされた証明書を確認するには、HiKeytool を使用します。

証明書の確認方法には、標準モードおよび詳細モードがあります。必要に応じて使い分けてください。

関連タスク

- [5.3.12 Device Manager サーバのトラストストア情報の参照 \(標準モード\)](#)
- [5.3.13 Device Manager サーバのトラストストア情報の参照 \(詳細モード\)](#)

5.5.18 Host Data Collector のトラストストアへの証明書のインポート

仮想化サーバの証明書を Host Data Collector のトラストストアにインポートするには、keytool ユーティリティを使用します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- サーバ証明書の入手と置き換え
認証局に申請して、仮想化サーバのサーバ証明書を入手してください。証明書発行要求 (CSR) を作成する際は、サブジェクトの別名 (Subject Alternative Names) に発行元の仮想化サーバの IP アドレスを指定してください。
Host Data Collector で管理する仮想化サーバに VMware ESXi を含む場合、仮想化サーバのサーバ証明書を発行した認証局からルート認証局までの全認証局の証明書がチェーンされた状態で、サーバ証明書が必要です。
入手したサーバ証明書は、仮想化サーバにインポートされている自己署名証明書と置き換えてください。詳細は、VMware 社のマニュアルを参照してください。

操作手順

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%uCPsB%jdk%jre  
%bin%keytool -import -alias <エイリアス名> -keystore <トラストストア  
ファイル名> -file <サーバ証明書>
```

Linux の場合 :

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/  
uCPsB/jdk/jre/bin/keytool -import -alias <エイリアス名> -keystore  
<トラストストアファイル名> -file <サーバ証明書>
```

- alias : トラストストア内で証明書を識別するための名称を指定します。
- keystore : インポート先のトラストストアファイルとして、次のパスを指定します。

Windows の場合 :

```
<Host Data Collector のインストールフォルダ>%HDC%Base%config%hdccacerts
```

Linux の場合 :

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/config/  
hdccacerts
```

- file : サーバ証明書ファイルを絶対パスで指定します。

2. トラストストアパスワードを入力します。
デフォルトパスワードは changeit です。

関連参照

- [5.1.22 トラストストア](#)

5.5.19 Host Data Collector のトラストストアーにインポートされた証明書の確認

トラストストアーにインポートされた証明書を確認するには、keytool ユーティリティを使用します。

前提条件

次の情報の確認

- トラストストアーへのアクセスパスワード

操作手順

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%uCPSE%jdk%jre%bin%keytool -list -alias <エイリアス名> -keystore <トラストストアーファイル名>
```

Linux の場合：

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/uCPSE/jdk/jre/bin/keytool -list -alias <エイリアス名> -keystore <トラストストアーファイル名>
```

- alias：トラストストアー内で証明書を識別するための名称を指定します。
- keystore：証明書が格納されているトラストストアーファイルとして、次のパスを指定します。

Windows の場合：

```
<Host Data Collector のインストールフォルダ>%HDC%Base%config%hdccacerts
```

Linux の場合：

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/config/hdccacerts
```

2. トラストストアーパスワードを入力します。
デフォルトパスワードは changeit です。

関連参照

- [5.1.22 トラストストアー](#)

5.5.20 Host Data Collector のトラストストアーパスワードの変更

Host Data Collector のトラストストアーパスワードを変更するには、keytool ユーティリティを使用します。

前提条件

- トラストストアーへのアクセスパスワード

操作手順

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%uCPSE%jdk%jre
%bin%keytool -storepasswd -keystore <トラストストアファイル名>
```

Linux の場合 :

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/
uCPSE/jdk/jre/bin/keytool -storepasswd -keystore <トラストストアフ
ァイル名>
```

- keystore : パスワードを変更するトラストストアファイルとして、次のパスを指定しま
す。

Windows の場合 :

```
<Host Data Collector のインストールフォルダ>%HDC%Base%config%hdccacerts
```

Linux の場合 :

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/config/
hdccacerts
```

2. 現在のトラストストアパスワードを指定します。
デフォルトパスワードは changeit です。
3. 新しいトラストストアパスワードを指定します。
使用できる文字は次のとおりです。
A~Z a~z 0~9 空白文字
大文字と小文字は区別されます。
新しいパスワードは 6 文字以上を指定してください。
4. 新しいトラストストアパスワードを再指定します。

関連参照

- [5.1.22 トラストストア](#)

5.5.21 仮想化サーバの登録情報の変更

Device Manager サーバと仮想化サーバ間の通信プロトコルは、Device Manager GUI の [ホスト
編集] 画面または Device Manager CLI の ModifyVirtualizationServer コマンドで変更しま
す。

ここでは、Device Manager GUI を使って登録情報を変更する方法を説明します。

ModifyVirtualizationServer コマンドについては、マニュアル「*Hitachi Command Suite
CLI リファレンスガイド*」を参照してください。

前提条件

- 仮想化サーバでの SSL サーバの構築
詳細は、VMware 社のマニュアルを参照してください。

操作手順

1. [管理] タブで [管理リソース] を選択します。
2. [ホスト] タブで対象の仮想化サーバを選択し、[ホスト編集] ボタンをクリックします。
3. [ホスト編集] 画面で、通信プロトコルを変更します。

5.5.22 Device Manager エージェントのトラストストアへのサーバ証明書のインポート

Device Manager サーバのサーバ証明書を Device Manager エージェントのトラストストアにインポートするには、`hdvmagt_setting` コマンドを使用します。

`hdvmagt_setting` コマンドで次の設定ができます。

- Device Manager サーバのサーバ証明書が Device Manager エージェントのトラストストアにインポートされます。
- Device Manager エージェントの次のプロパティファイルが設定されます。
 - `server.server.ssl.hdvm`
`true` を設定します。
 - `server.server.serverPort`
SSL 通信のポート番号を設定します。

前提条件

- Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン
- サーバ証明書の入手
管理サーバで作成されたサーバ証明書を安全な方法で取得します。
 - Device Manager サーバのサーバ証明書
暗号化通信のテストなどの目的で自己署名証明書を使用する場合は、トラストストアファイル (HiCommandCerts) からサーバ証明書をエクスポートしておく必要があります。
- 次の情報の確認
 - Device Manager エージェントのトラストストアへのアクセスパスワード (デフォルトパスワードを変更している場合)
 - 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 (Device Manager サーバと非 SSL で通信している場合) または `server.https.port` プロパティ (Device Manager サーバと SSL で通信している場合) 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。

操作手順

1. 次のコマンドを実行して、対話形式で SSL 通信の設定をします。

Windows の場合 :

```
< Device Manager エージェントのインストールフォルダ > %bin%hdvmagt_setting
```

Linux の場合 :

```
< Device Manager エージェントのインストールディレクトリ > /bin/  
hdvmagt_setting
```

Solaris, または HP-UX の場合 :

```
/opt/HDVM/HBaseAgent/bin/hdvmagt_setting
```

AIX の場合 :

```
/usr/HDVM/HBaseAgent/bin/hdvmagt_setting
```

関連タスク

- [5.3.4 Device Manager サーバのサーバ証明書の認証局への申請](#)

関連参照

- [5.1.22 トラストストア](#)
- [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 RAID Manager XP の情報の設定 \(hdvmagt_setting コマンド\)](#)

5.5.23 Device Manager エージェントのトラストストアにインポートされたサーバ証明書の確認

トラストストアにインポートされたサーバ証明書を確認するには、`hbsa_keytool` ユーティリティ (Windows の場合) または `keytool` ユーティリティ (UNIX の場合) を使用します。

前提条件

次の情報の確認

- トラストストアへのアクセスパスワード

操作手順

1. 次のコマンドを実行します。

Windows の場合 :

```
< Device Manager エージェントのインストールフォルダ > %bin%hbsa_keytool -list -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

Linux の場合 :

```
< Device Manager エージェントのインストールディレクトリ > /agent/JRE1.5/bin/keytool -list -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

Solaris, AIX および HP-UX の場合 :

```
< JDK または JRE のインストールディレクトリ > /bin/keytool -list -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

- `keystore` : サーバ証明書が格納されているトラストストアファイルとして、次のパスを指定します。

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%hdvmcacerts
```

UNIX の場合 :

```
< Device Manager エージェントのインストールディレクトリ > /agent/config/hdvmcacerts
```

- `storepass` : トラストストアへのアクセスパスワードを指定します。

関連参照

- [5.1.22 トラストストア](#)

5.5.24 Device Manager エージェントのトラストストアパスワードの変更

Device Manager エージェントのトラストストアパスワードを変更するには、`hbsa_keytool` ユーティリティ (Windows の場合) または `keytool` ユーティリティ (UNIX の場合) を使用します。

前提条件

- トラストストアへのアクセスパスワード

操作手順

1. 次のコマンドを実行します。

Windows の場合 :

```
< Device Manager エージェントのインストールフォルダ > %bin%hbsa_keytool -storepasswd -keystore <トラストストアファイル名 >
```

Linux の場合 :

```
< Device Manager エージェントのインストールディレクトリ > /agent/JRE1.5/bin/keytool -storepasswd -keystore <トラストストアファイル名 >
```

Solaris, AIX および HP-UX の場合 :

```
< JDK または JRE のインストールディレクトリ > /bin/keytool -storepasswd -keystore <トラストストアファイル名 >
```

- `keystore` : パスワードを変更するトラストストアファイルとして、次のパスを指定します。

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%hdmvcacerts
```

UNIX の場合 :

```
< Device Manager エージェントのインストールディレクトリ > /agent/config/hdmvcacerts
```

2. 現在のトラストストアパスワードを指定します。
3. 新しいトラストストアパスワードを指定します。
使用できる文字は次のとおりです。
A~Z a~z 0~9 空白文字
大文字と小文字は区別されます。
新しいパスワードは 6 文字以上を指定してください。
4. 新しいトラストストアパスワードを再指定します。

関連参照

- [5.1.22 トラストストア](#)

5.5.25 Device Manager エージェントのトラストストアにインポートされたサーバ証明書の削除

トラストストアにインポートされたサーバ証明書を削除するには、`hbsa_keytool` ユーティリティ (Windows の場合) または `keytool` ユーティリティ (UNIX の場合) を使用します。

前提条件

次の情報の確認

- 削除するサーバ証明書のエイリアス名
- トラストストアへのアクセスパスワード

操作手順

1. 次のコマンドを実行します。

Windows の場合 :

```
< Device Manager エージェントのインストールフォルダ >%bin%hbsa_keytool -delete -alias <エイリアス名> -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

Linux の場合 :

```
< Device Manager エージェントのインストールディレクトリ >/agent/JRE1.5/bin/keytool -delete -alias <エイリアス名> -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

Solaris, AIX および HP-UX の場合 :

```
< JDK または JRE のインストールディレクトリ >/bin/keytool -delete -alias <エイリアス名> -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

- `alias` : サーバ証明書のエイリアス名を指定します。
- `keystore` : サーバ証明書が格納されているトラストストアファイルとして、次のパスを指定します。

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%hvmcacerts
```

UNIX の場合 :

```
< Device Manager エージェントのインストールディレクトリ >/agent/config/hvmcacerts
```

- `storepass` : トラストストアへのアクセスパスワードを指定します。

関連タスク

- [5.5.23 Device Manager エージェントのトラストストアにインポートされたサーバ証明書の確認](#)

関連参照

- [5.1.22 トラストストア](#)

5.5.26 ストレージシステムの登録情報の変更

Device Manager サーバとストレージシステム間の通信プロトコルは、Device Manager GUI の [ストレージシステム編集] 画面または Device Manager CLI の AddStorageArray コマンドで変更します。

ここでは、Device Manager GUI を使って登録情報を変更する方法を説明します。

AddStorageArray コマンドについては、マニュアル「*Hitachi Command Suite CLI リファレンスガイド*」を参照してください。

前提条件

- ストレージシステムでの SSL サーバの構築
詳細は、Storage Navigator Modular 2 のマニュアルを参照してください。
- ストレージシステムのリフレッシュ
- 次の情報の確認（SMI-S enabled ストレージシステムの場合）
 - SMI-S プロバイダーとの通信ポート（デフォルト：5989）

操作手順

1. [管理] タブで [管理リソース] を選択します。
2. [ストレージシステム] タブで対象のストレージシステムを選択し、[ストレージシステム編集] ボタンをクリックします。
3. [ストレージシステム編集] 画面で、通信プロトコルと通信ポートを変更します。

5.6 SSL サーバおよび SSL クライアントの構築（CIM サーバ）

オブジェクト操作で SSL サーバ認証を使用する場合には、Device Manager サーバでサーバ証明書を作成し、CIM クライアントにインポートする必要があります。相互認証を使用する場合は、CIM クライアントでクライアント証明書を作成し、Device Manager サーバにインポートする必要があります。

また、インディケーション通知で SSL サーバ認証を使用する場合には、CIM クライアントでサーバ証明書を作成し、Device Manager サーバにインポートする必要があります。相互認証を使用する場合は、Device Manager サーバでクライアント証明書を作成し、CIM クライアントにインポートする必要もあります。

5.6.1 オブジェクト操作のキーストアーファイルの作成

オブジェクト操作のキーストアーファイルを作成するには、hcnds64keytool ユーティリティ（Windows の場合）または keytool ユーティリティ（Linux の場合）を使用します。

前提条件

- オブジェクト操作の既存のキーストアーファイルの削除

Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager  
%HiCommandServer%wsi%server%jserver%bin%.keystore
```

Linux の場合：

< Hitachi Command Suite のインストールディレクトリ >/HiCommandServer/wsi/
server/jserver/bin/.keystore

操作手順

1. 次のコマンドを実行して、オブジェクト操作用のキーストアーファイルを作成します。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ >%Base64%bin%hcmds64keytool  
-genkey -keystore <キーストアーファイル名> -storepass <キーストアーパス  
ワード> -alias <エイリアス名> -dname <エンティティの識別名> -validity  
<証明書の有効期限> -keypass <秘密鍵のパスワード> -keyalg <キーアルゴリ  
ズム> -sigalg <署名アルゴリズム> -keysize <キーサイズ>
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ >/Base64/uCPSB/jdk/bin/  
keytool -genkey -keystore <キーストアーファイル名> -storepass <キース  
トアーパスワード> -alias <エイリアス名> -dname <エンティティの識別名> -  
validity <証明書の有効期限> -keypass <秘密鍵のパスワード> -keyalg <キ  
ーアルゴリズム> -sigalg <署名アルゴリズム> -keysize <キーサイズ>
```

- keystore : オブジェクト操作用のキーストアーファイル (.keystore : 固定) を指定して
ください。
 - storepass, keypass : 同じパスワードを指定してください。
2. WSIEncryptString.jar を実行して、キーストアーパスワードを暗号化します。
WSIEncryptString.jar は次の場所に格納されています。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ >%DeviceManager  
%HiCommandServer%wsi%server%jserver%lib%
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ >/HiCommandServer/wsi/  
server/jserver/lib/
```

```
java -jar WSIEncryptString.jar <キーストアーパスワード>
```

操作結果

キーストアーパスワードを暗号化した文字列が表示されます。この文字列をオブジェクト操作用の MOF ファイルに設定します。

5.6.2 オブジェクト操作用の MOF ファイルの編集

WSIEncryptString.jar で暗号化したキーストアーパスワードをオブジェクト操作用の MOF ファイルに指定し、コンパイルします。

前提条件

- オブジェクト操作用のキーストアーファイルの作成
- 次の情報の確認

- WSIEncryptString.jar で暗号化したキーストアパスワード

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. オブジェクト操作用の MOF ファイル (CIMXMLSCOMATLSSettingData_instances.mof) に、WSIEncryptString.jar で暗号化したキーストアパスワードを設定します。

MOF ファイルは、次の場所に格納されています。

Windows の場合：

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager
%HiCommandServer%wsi%server%jserver%mofof%wbemserver
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/wsi/
server/jserver/mof/wbemserver
```

KeyStorePassword の XXXXXXXX 部分に、暗号化したキーストアパスワードを設定してください。

```
instance of HITACHI_CIMXMLSCOMATLSSettingData {
    InstanceID          =
HITACHI:HITACHI_CIMXMLSCOMATLSSettingData:001";
    ElementName         = "CIM-XML Client Adapter TLS Settings";
    MutualAuthenticationRequired = false;
    KeyStoreFile        = "{0}/jserver/bin/.keystore";
    KeyStorePassword    = "XXXXXXXX";
    TrustStoreFile      = "{0}/jserver/bin/.truststore";
};
```

3. mofcomp コマンドを実行して、オブジェクト操作用の MOF ファイルをコンパイルします。

Windows の場合：

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager
%HiCommandServer%wsi%bin%mofofcomp.bat
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ > /
HiCommandServer/wsi/bin/mofcomp
```

```
mofcomp -m -o ..%server%jserver%logr ..%server%jserver%mofof%wbemserver
%CIMXMLSCOMATLSSettingData_instances.mof
```

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

5.6.3 オブジェクト操作用のサーバ証明書のエクスポート

オブジェクト操作用の Device Manager サーバのサーバ証明書をキーストアファイル (.keystore) からエクスポートするには、HiKeytool のメインメニューで [SSL configuration for SMI-S] - [Export Server's Certificate from KeyStore for Object Operations] を選択します。

前提条件

- オブジェクト操作の MOF ファイルの編集
- 次の情報の確認
 - オブジェクト操作のキーストアパスワード
 - オブジェクト操作のサーバ証明書のエイリアス名

操作手順

1. 次のとおり実行して、HiKeytool を起動します。

Windows の場合

```
< Hitachi Command Suite のインストールフォルダ > ¥DeviceManager  
¥HiCommandServer¥HiKeytool.bat
```

Linux の場合

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/  
HiKeytool.sh
```

2. メインメニューで、2 ([SSL configuration for SMI-S]) を指定します。
3. SMI-S 用メインメニューで、5 ([Export Server's Certificate from KeyStore for Object Operations]) を指定します。
4. キーストアパスワード、エイリアス名、およびオブジェクト操作のサーバ証明書の出力先を指定します。

```
Enter keystore-password:serverssl  
Enter alias:foocorpserver  
Enter authentication-filename (absolute path):c:¥tmp¥server.cer
```

5.6.4 オブジェクト操作に対する相互認証の有効化

オブジェクト操作に対する相互認証を有効にするには、HiKeytool のメインメニューで [SSL configuration for SMI-S] - [Set Security Level for Object Operations] を選択します。

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. 次のとおり実行して、HiKeytool を起動します。

Windows の場合

```
< Hitachi Command Suite のインストールフォルダ > ¥DeviceManager  
¥HiCommandServer¥HiKeytool.bat
```

Linux の場合

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/  
HiKeytool.sh
```

3. メインメニューで、2 ([SSL configuration for SMI-S]) を指定します。
4. SMI-S 用メインメニューで、1 ([Set Security Level for Object Operations]) を指定します。
5. 2 ([SSL with two-way authentication]) を指定します。
オブジェクト操作の MOF ファイルがコンパイルされ、SMI-S 用メインメニューに戻ります。

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

```
You must stop the Device Manager Server before specifying this setting.  
1) SSL without two-way authentication  
2) SSL with two-way authentication  
  
>2
```



メモ

「The compilation of the MOF file failed.」というメッセージが表示された場合、次の場所にある全ファイルを集めて保守員に連絡してください。

Windows の場合：

```
< Hitachi Command Suite のインストールフォルダ > ¥DeviceManager ¥HiCommandServer ¥wsi  
¥server ¥jserver ¥mof ¥wbemserver
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/wsi/server/  
jserver/mof/wbemserver
```

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

5.6.5 オブジェクト操作のクライアント証明書のインポート

オブジェクト操作の相互認証で使用する CIM クライアントのクライアント証明書をトラストストアファイル (.truststore) にインポートするには、HiKeytool のメインメニューで [SSL configuration for SMI-S] - [Import Client's Certificate to TrustStore for Object Operations] を選択します。

前提条件

- CIM クライアントのオブジェクト操作のクライアント証明書の入手
- 既存のオブジェクト操作のトラストストアファイル (.truststore) の削除

操作手順

1. 次のとおり実行して、HiKeytool を起動します。

Windows の場合

```
< Hitachi Command Suite のインストールフォルダ > ¥DeviceManager  
¥HiCommandServer ¥HiKeytool.bat
```

Linux の場合

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/  
HiKeytool.sh
```

2. メインメニューで、2 ([SSL configuration for SMI-S]) を指定します。
3. SMI-S 用メインメニューで、3 ([Import Client's Certificate to TrustStore for Object Operations]) を指定します。
4. エイリアス名、トラストストアのパスワード、およびオブジェクト操作のクライアント証明書の絶対パスを指定します。

```
Enter alias:foocorpclient  
Enter truststore-password:trustssl
```

```
Enter authentication-filename (absolute path) : c:\%tmp%\client.cer
```

関連タスク

- [5.7.2 CIM クライアントのサーバ証明書またはクライアント証明書のエクスポート](#)

関連参照

- [5.1.22 トラストストア](#)

5.6.6 インディケーション通知用のキーストアファイルの作成

インディケーション通知用のキーストアファイルを作成するには、hcnds64keytool ユーティリティ (Windows の場合) または keytool ユーティリティ (Linux の場合) を使用します。

前提条件

- インディケーション通知用の既存のキーストアファイルの削除 (再作成する場合)

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%\wsi\server\jserver\bin\indkeystore
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/wsi/  
server/jserver/bin/indkeystore
```

操作手順

1. 次のコマンドを実行して、インディケーション通知用のキーストアファイルを作成します。

Windows の場合

```
< Hitachi Command Suite のインストールフォルダ > %Base64%\bin\hcnds64keytool  
-genkey -keystore <キーストアファイル名> -storepass <キーストアパ  
スワード> -alias <エイリアス名> -dname <エンティティの識別名> -validity  
<証明書の有効期限> -keypass <秘密鍵のパスワード> -keyalg <キーアルゴリ  
ズム> -sigalg <署名アルゴリズム> -keysize <キーサイズ>
```

Linux の場合

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/jdk/bin/  
keytool -genkey -keystore <キーストアファイル名> -storepass <キース  
トアパスワード> -alias <エイリアス名> -dname <エンティティの識別名> -  
validity <証明書の有効期限> -keypass <秘密鍵のパスワード> -keyalg <キ  
ーアルゴリズム> -sigalg <署名アルゴリズム> -keysize <キーサイズ>
```

- keystore : インディケーション通知用のキーストアファイル (indkeystore : 固定) を指定してください。
 - storepass, keypass : 同じパスワードを指定してください。
2. WSIEncryptString.jar を実行して、キーストアパスワードを暗号化します。
WSIEncryptString.jar は次の場所に格納されています。

Windows の場合 :

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager
%HiCommandServer%wsi%server%jserver%lib%
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/wsi/
server/jserver/lib/
```

```
java -jar WSIEncryptString.jar <キーストアパスワード>
```

操作結果

キーストアパスワードを暗号化した文字列が表示されます。この文字列をインディケーション通知用の MOF ファイルに設定します。

5.6.7 インディケーション通知用の MOF ファイルの編集

WSIEncryptString.jar で暗号化したキーストアパスワードをインディケーション通知用の MOF ファイルに指定し、コンパイルします。

前提条件

- インディケーション通知用のキーストアファイルの作成
- 次の情報の確認
 - WSIEncryptString.jar で暗号化したキーストアパスワード

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. インディケーション通知用の MOF ファイル (CIMXMLSIndicationHandlerTLSSettingData_instances.mof) に、WSIEncryptString.jar で暗号化したキーストアパスワードを設定し、MutualAuthenticationRequired の値を true に変更します。

MOF ファイルは、次の場所に格納されています。

Windows の場合 :

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager
%HiCommandServer%wsi%server%jserver%moF%wbemserver
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/wsi/
server/jserver/mof/wbemserver
```

KeyStorePassword の XXXXXXXX 部分に、暗号化したキーストアパスワードを設定してください。

```
instance of HITACHI_CIMXMLSIndicationHandlerTLSSettingData {
    InstanceID          =
    "HITACHI:HITACHI_CIMXMLSIndicationHandlerTLSSettingData:001";
    ElementName         = "CIM_XML-TLS Indication Handler Settings";
    MutualAuthenticationRequired = true;
    KeyStoreFile        = "{0}/jserver/bin/indkeystore";
    KeyStorePassword    = "XXXXXXX";
    TrustStoreFile      = "{0}/jserver/bin/indtruststore";
};
```

3. mofcomp コマンドを実行して、インディケーション通知用の MOF ファイルをコンパイルします。

Windows の場合：

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%wsi%bin%mofcomp.bat
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ > /  
HiCommandServer/wsi/bin/mofcomp
```

```
mofcomp -m -o ..%server%jserver%logr ..%server%jserver%hof%wbemserver  
%CIMXMLSIndicationHandlerTLSSettingData_instances.mof
```

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

5.6.8 インディケーション通知用のクライアント証明書のエクスポート

インディケーション通知の相互認証で使用するクライアント証明書をキーストアファイル (indkeystore) からエクスポートするには、HiKeytool のメインメニューで [SSL configuration for SMI-S] - [Export Server's Certificate from KeyStore for Event Indications] を選択します。

前提条件

- インディケーション通知用の MOF ファイルの編集
- 次の情報の確認
 - インディケーション通知用のキーストアパスワード
 - インディケーション通知用のクライアント証明書のエイリアス名

操作手順

1. 次のとおり実行して、HiKeytool を起動します。

Windows の場合

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%HiKeytool.bat
```

Linux の場合

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/  
HiKeytool.sh
```

2. メインメニューで、2 ([SSL configuration for SMI-S]) を指定します。
3. SMI-S 用メインメニューで、6 ([Export Server's Certificate from KeyStore for Event Indications]) を指定します。
4. キーストアパスワード、エイリアス名、およびインディケーション通知用のクライアント証明書の出力先を指定します。

```
Enter keystore-password:serverindtrust  
Enter alias:foocorpindserver
```

```
Enter authentication-filename (absolute path) : c:\%tmp%\serverind.cer
```

5.6.9 インディケーション通知に対する相互認証の有効化

インディケーション通知に対する相互認証を有効にするには、HiKeytool のメインメニューで [SSL configuration for SMI-S] - [Set Security Level for Event Indications] を選択します。

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. 次のとおり実行して、HiKeytool を起動します。

Windows の場合

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%\HiKeytool.bat
```

Linux の場合

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/  
HiKeytool.sh
```

3. メインメニューで、2 ([SSL configuration for SMI-S]) を指定します。
4. SMI-S 用メインメニューで、2 ([Set Security Level for Event Indications]) を指定します。
5. 2 ([SSL with two-way authentication]) を指定します。
インディケーション通知の MOF ファイルがコンパイルされ、SMI-S 用メインメニューに戻ります。
6. Hitachi Command Suite 製品のサービスを起動します。

```
You must stop the Device Manager Server before specifying this setting.  
1) SSL without two-way authentication  
2) SSL with two-way authentication  
>2
```



メモ

「The compilation of the MOF file failed.」というメッセージが表示された場合、次の場所にある全ファイルを収集して保守員に連絡してください。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager%\HiCommandServer%\wsi  
%server%\jserver%\mof%
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/wsi/server/  
jserver/mof/
```

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

5.6.10 インディケーション通知用のサーバ証明書のインポート

インディケーション通知用の CIM クライアントのサーバ証明書をトラストストアファイル (indtruststore) にインポートするには、HiKeytool のメインメニューで [SSL configuration for SMI-S] - [Import Client's Certificate to TrustStore for Event Indications] を選択します。

前提条件

- CIM クライアントのインディケーション通知用のサーバ証明書の入手
- 既存のインディケーション通知用のトラストストアファイル (indtruststore) の削除

操作手順

1. 次のとおり実行して、HiKeytool を起動します。

Windows の場合

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%HiKeytool.bat
```

Linux の場合

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/  
HiKeytool.sh
```

2. メインメニューで、2 ([SSL configuration for SMI-S]) を指定します。
3. SMI-S 用メインメニューで、4 ([Import Client's Certificate to TrustStore for Event Indications]) を指定します。
4. エイリアス名、トラストストアのパスワード、および CIM クライアントのサーバ証明書の絶対パスを指定します。

```
Enter alias:foocorpindclient  
Enter truststore-password:indtrust  
Enter authentication-filename(absolute path):c:%tmp%clientind.cer
```

関連タスク

- [5.7.2 CIM クライアントのサーバ証明書またはクライアント証明書のエクスポート](#)

関連参照

- [5.1.22 トラストストア](#)

5.6.11 CIM サーバの自己署名証明書の確認

Device Manager サーバ (CIM サーバ) のオブジェクト操作またはインディケーション通知用の自己署名証明書を確認するには、hcnds64keytool ユーティリティ (Windows の場合) または keytool ユーティリティ (Linux の場合) を使用します。

前提条件

次の情報の確認

- キーストアパスワード

操作手順

1. 次のコマンドを実行します。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > %Base64%bin%hcnds64keytool  
-list -keystore <キーストアファイル名> -storepass <キーストアパスワ  
ード>
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/jdk/bin/  
keytool -list -keystore <キーストアーファイル名> -storepass <キースト  
アーパスワード>
```

- keystore : 対象のキーストアーファイルを指定します。
- storepass : キーストアーパスワードを指定します。

5.6.12 製品同梱されたオブジェクト操作の自己署名証明書

Device Manager に同梱されているオブジェクト操作の自己署名証明書の署名アルゴリズムは SHA256withRSA、キーサイズは 2048 ビットです。

Device Manager に同梱されているオブジェクト操作の自己署名証明書は、次のキーストアーファイル (キーストアーパスワード : wbemssl) に格納されています。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%wsi%server%jserver%bin%.keystore
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/wsi/  
server/jserver/bin/.keystore
```

5.6.13 相互認証の無効化

オブジェクト操作またはインディケーション通知の相互認証を無効にするには、HiKeytool を使用します。

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. 次のとおり実行して、HiKeytool を起動します。

Windows の場合

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%HiKeytool.bat
```

Linux の場合

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/  
HiKeytool.sh
```

3. メインメニューで、2 ([SSL configuration for SMI-S]) を指定します。
4. SMI-S 用メインメニューで、1 ([Set Security Level for Object Operations]) または 2 ([Set Security Level for Event Indications]) を指定します。
5. 1 ([SSL without two-way authentication]) を指定します。
MOF ファイルがコンパイルされ、SMI-S 用メインメニューに戻ります。
6. Hitachi Command Suite 製品のサービスを起動します。

You must stop the Device Manager Server before specifying this setting.
1) SSL without two-way authentication
2) SSL with two-way authentication

**メモ**

「The compilation of the MOF file failed.」というメッセージが表示された場合、次の場所にある全ファイルを集めて保守員に連絡してください。

Windows の場合：

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager%HiCommandServer%wsi%server%jserver%mof%
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/wsi/server/jserver/mof/
```

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

5.7 SSL サーバおよび SSL クライアントの構築（CIM クライアント）

オブジェクト操作で SSL サーバ認証を使用する場合には、Device Manager サーバでサーバ証明書を作成し、CIM クライアントにインポートする必要があります。相互認証を使用する場合は、CIM クライアントでクライアント証明書を作成し、Device Manager サーバにインポートする必要があります。

また、インディケーション通知で SSL サーバ認証を使用する場合には、CIM クライアントでサーバ証明書を作成し、Device Manager サーバにインポートする必要があります。相互認証を使用する場合は、Device Manager サーバでクライアント証明書を作成し、CIM クライアントにインポートする必要があります。

5.7.1 CIM クライアントのキーペアと自己署名証明書の作成

CIM クライアントでキーペアと自己署名証明書を作成するには、keytool ユーティリティを使用します。

前提条件

- CIM クライアントマシンへの Java のインストール

操作手順

1. 次のコマンドを実行して、キーペアと自己署名証明書を作成します。

```
keytool -genkey -keystore <キーストアファイル名> -storepass <キーストアパスワード> -alias <エイリアス名> -dname <エンティティの識別名> -validity <証明書の有効期限> -keypass <秘密鍵のパスワード> -keyalg <キーアルゴリズム> -sigalg <署名アルゴリズム> -keysize <キーサイズ>
```

- ファイル名には次の記号を使用しないでください。
: , ; * ? " < > |
- ファイル名は 255 バイト以内の文字列にしてください。
- エイリアス名、およびパスワードには引用符 (") を含めないでください。
- storepass, keypass には、同じパスワードを指定してください。

2. 次のコマンドを実行して、作成されたキーペアと自己署名証明書の内容を確認します。
`keytool -list -keystore <キーストアファイル名> -storepass <キーストアパスワード>`

5.7.2 CIM クライアントのサーバ証明書またはクライアント証明書のエクスポート

CIM クライアントのキーストアファイルから CIM クライアントのサーバ証明書またはクライアント証明書をエクスポートするには、keytool ユーティリティを使用します。

前提条件

- CIM クライアントマシンへの Java のインストール
- CIM クライアントのサーバ証明書の作成
- 次の情報の確認
 - CIM クライアントのキーストアファイルのパス
 - CIM クライアントのサーバ証明書のエイリアス名
 - CIM クライアントのキーストアのパスワード

操作手順

1. 次のコマンドを実行して、CIM クライアントのサーバ証明書またはクライアント証明書をエクスポートします。
`keytool -export -keystore <キーストアファイル名> -storepass <キーストアパスワード> -alias <エイリアス名> -file <証明書のファイル名>`
2. 次のコマンドを実行して、エクスポートされたサーバ証明書またはクライアント証明書の内容を確認します。
`keytool -printcert -v -file <証明書のファイル名>`

5.7.3 CIM クライアントへのサーバ証明書またはクライアント証明書のインポート

CIM クライアントのトラストストアに Device Manager サーバのサーバ証明書またはクライアント証明書をインポートするには、keytool ユーティリティを使用します。

前提条件

- CIM クライアントマシンへの Java のインストール
- Device Manager サーバ (CIM サーバ) のサーバ証明書の入手
- 次の情報の確認
 - CIM クライアントのトラストストアのパスワード

操作手順

1. 次のコマンドを実行して、Device Manager サーバのサーバ証明書またはクライアント証明書をインポートします。
`keytool -import -alias <エイリアス名> -keystore <トラストストアファイル名> -storepass <トラストストアパスワード> -trustcacerts -file <証明書のファイル名>`
- ファイル名には次の記号を使用しないでください。

: , ; * ? " < > |

- ファイル名は 255 バイト以内の文字列にしてください。

2. 次のコマンドを実行して、トラストストアファイルの内容を確認します。

```
keytool -list -keystore <トラストストアファイル名> -storepass <トラストストアパスワード>
```

関連タスク

- [5.6.3 オブジェクト操作のサーバ証明書のエクスポート](#)
- [5.6.8 インディケーション通知用のクライアント証明書のエクスポート](#)

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。

- 6.1 Storage Navigator Modular 2 と連携するために必要な設定
- 6.2 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
- 6.3 [レプリケーション] タブで Universal Replicator の性能を分析するために必要な設定
- 6.4 [レプリケーション] タブでレプリケーション管理機能を利用するために必要な設定
- 6.5 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHするために必要な設定

6.1 Storage Navigator Modular 2 と連携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、ミッドレンジストレージの Element Manager である Storage Navigator Modular 2 をラUNCHできます。

Element Manager を使って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。

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

Storage Navigator Modular 2 利用時の前提条件を次に示します。

- Storage Navigator Modular 2 をインストールする前に、ソフトウェア添付資料の Hitachi Command Suite のインストール後に Hitachi File Services Manager や Storage Navigator Modular 2 をインストールして連携する場合の注意事項を確認してください。
- 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 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UNCH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。



注意

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)。

6.1.2 Element Manager を使用するための設定

Element Manager で Hitachi AMS/WMS 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。

操作手順

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 :
`< Hitachi Command Suite のインストールフォルダ > %DeviceManager
%HiCommandServer%tools%launchapptool.bat`
- Linux の場合 :
`< Hitachi Command Suite 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、「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。

3. 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。

4. 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
```

**注意**

- ・ 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。

5. 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
```

6. 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。

7. launchapptool を終了します。

```
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):
```

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。

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。

関連タスク

- ・ [9.1.2 Hitachi Command Suite のサービスの起動](#)
- ・ [9.1.3 Hitachi Command Suite のサービスの停止](#)

6.1.3 Element Manager を使用するための設定の解除

Element Manager で Hitachi AMS/WMS 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。

操作手順

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 :

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%tools%launchapptool.bat
```

- Linux の場合 :

```
< Hitachi Command Suite 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):
```

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

6.2 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、パー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。

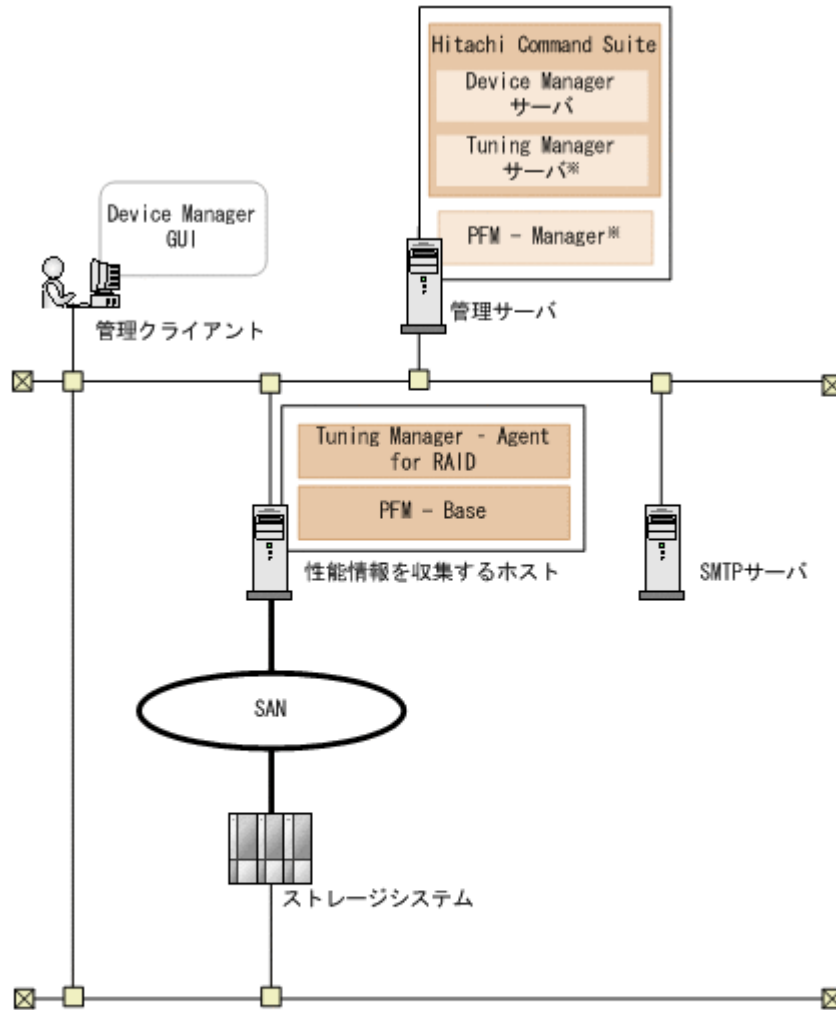
また、Device Manager と Tuning Manager が連携すると、[分析] タブで次のことができます。

- 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。

6.2.1 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 49 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。

Tuning Manager - Agent for RAID の設定方法については、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。

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。

Tuning Manager サーバの設定方法については、マニュアル「*Hitachi Command Suite Tuning Manager インストールガイド*」を参照してください。

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。

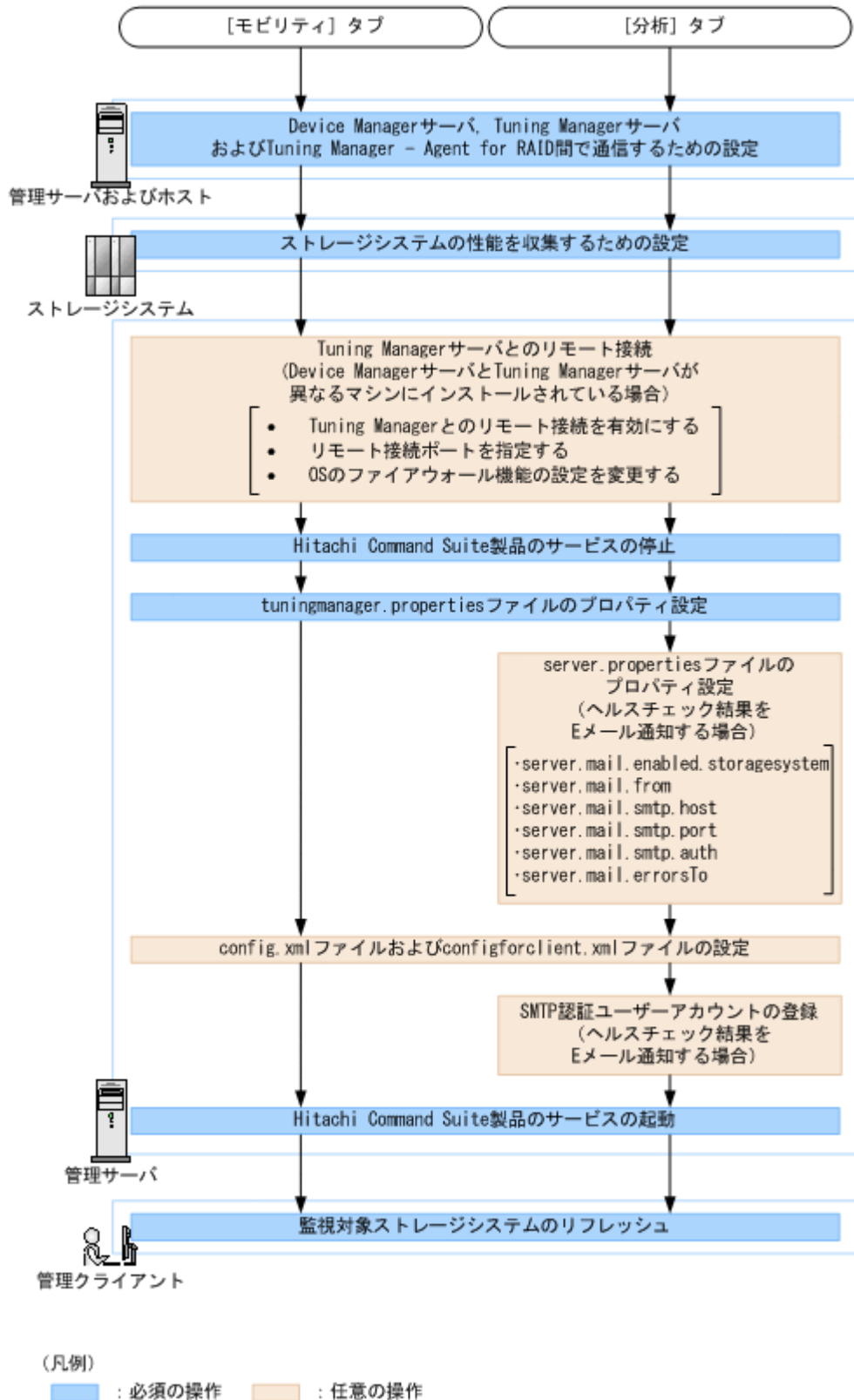
関連タスク

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

6.2.2 ストレージシステムの性能情報を収集するための操作フロー

ストレージシステムの性能情報を収集するには、管理サーバ、性能情報を収集するホスト、およびストレージシステムで環境設定をしたあと、管理クライアント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。

図 50 ストレージシステムの性能情報を収集するための操作フロー





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。
- クラスタの設定で `hcms64dbclustersetup` 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。
- 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。
`hcms64dbtrans`
`hcms64backups` および `hcms64db -restore` の組み合わせ
`hcms64dbtrans` および `hcms64dbrepair` の組み合わせ



メモ

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。



ヒント

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、システムは次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=22015` (接続する Tuning Manager サーバの HBase 64 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。

関連タスク

- [6.2.6 Tuning Manager サーバとのリモート接続 \(非クラスタ環境\)](#)
- [6.2.7 Tuning Manager サーバとのリモート接続 \(Windows のクラスタ環境\)](#)
- [7.2.9 SMTP 認証ユーザーアカウントを Device Manager に登録する](#)
- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [6.2.3 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](#)
- [6.2.4 エンタープライズクラスストレージ、VSP Gx00 モデル、VSP Fx00 モデルおよび HUS VM の性能情報を収集するための設定](#)
- [6.2.5 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](#)
- [6.2.9 config.xml ファイルおよび configforclient.xml ファイルの設定](#)

- 付録 A.2.17 `server.mail.enabled.storagesystem`
- 付録 A.2.19 `server.mail.from`
- 付録 A.2.20 `server.mail.smtp.host`
- 付録 A.2.21 `server.mail.smtp.port`
- 付録 A.2.22 `server.mail.smtp.auth`
- 付録 A.2.23 `server.mail.errorsTo`
- 付録 A.14 Tuning Manager との連携に関するプロパティ (`tuningmanager.properties` ファイル)

6.2.3 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 サーバが使用するポート番号については, マニュアル「*Hitachi Command Suite Tuning Manager* インストールガイド」を参照してください。Tuning Manager - Agent for RAID が使用するポート番号については, マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。
- [分析] タブで特定の操作をする場合, Performance データベースや Tuning Manager API の設定が前提条件を満たしていること。
操作ごとに必要な設定について, 次の表に示します。

表 54 [分析] タブでの操作に必要な Performance データベースおよび Tuning Manager API の設定

操作	Performance データベースの種別	Tuning Manager API を利用を有効にするための設定
[性能問題特定] ウィザードでの分析対象期間を 72 分より長く, 間隔を分単位に設定する	Hybrid Store	不要
	Store データベース	必要
MP ブレードまたは MP ユニットの性能を分析する	Hybrid Store	不要
	Store データベース	必要
ホストごとに性能を分析する	Hybrid Store	不要

Performance データベースの種別は, バージョン 8.1.3 以降の Tuning Manager - Agent for RAID でサポートしている Hybrid Store にすることをお勧めします。Performance データベースを Hybrid Store にすると, Tuning Manager API の利用が有効になります。

Performance データベースの移行および Tuning Manager - Agent for RAID のインストールについては, マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。

Performance データベースの種別が Store データベースの場合, Tuning Manager API の利用を有効にするには `htmrestctrl` コマンドを実行します。`htmrestctrl` コマンドについては, マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。

- 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、jpc hosts ファイルに IP アドレスを設定し、jpc hosts 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。

Tuning Manager サーバの設定方法については、マニュアル「*Hitachi Command Suite Tuning Manager インストールガイド*」を参照してください。Tuning Manager - Agent for RAID の設定方法については、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。



ヒント

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選択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。

関連概念

- [2.3 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録](#)
- [5.1.7 Tuning Manager サーバと Device Manager サーバ間のセキュリティ通信のための操作フロー](#)

関連タスク

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

関連参照

- [付録 A.5.16 server.dispatcher.daemon.autoSynchro.performance.startTime](#)

6.2.4 エンタープライズクラスストレージ、VSP Gx00 モデル、VSP Fx00 モデルおよび 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、VSP Gx00 モデル、VSP Fx00 モデルおよび 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、VSP Gx00 モデル、VSP Fx00 モデルおよび 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については、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。
 - 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。
コマンドデバイスの設定方法については、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。
 - Tuning Manager - Agent for RAID のインスタンス環境を構築する際に、インスタンス情報の Method for Collecting の値に 1 または 3 を指定していること。
Device Manager は Method for Collecting に 2 を指定して構築した Tuning Manager - Agent for RAID のインスタンスとは連携できません。
インスタンス環境の設定方法については、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。
 - 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。
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は、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。
 - ヘルスチェックを実行する場合、次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。
 - PI_CLMS レコード (Universal Storage Platform V/VM および Hitachi USP の場合は設定不要)
 - 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
- レコードの保存期間は Tuning Manager の Performance Reporter で設定してください。レコードの保存期間の設定方法については、マニュアル「*Hitachi Command Suite Tuning Manager 運用管理ガイド*」を参照してください。
設定するレコードの保存期間を「[表 55 ヘルスチェックを実行するためのレコードの保存期間 \(エンタープライズクラスストレージ, VSP Gx00 モデル, VSP Fx00 モデルおよび HUS VM の場合\)](#)」に示します。

表 55 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, VSP Gx00 モデル, VSP Fx00 モデルおよび HUS VM の場合)

Performance データベースの種類	プロパティ名	設定値
Store データベースバージョン 1.0	Product Interval - Hour Drawer	Month
	Product Interval - Day Drawer	Year
Store データベースバージョン 2.0	Period - Hour Drawer (Day)	9 以上

Performance データベースの種類	プロパティ名	設定値
	Period - Day Drawer (Week)	5 以上
Hybrid Store	Retention - hourly	216 以上
	Retention - daily	35 以上



ヒント

ホストごとに性能分析する場合は、分析したい期間に合わせて PI_LDS レコードの保存期間を設定してください。

6.2.5 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, および Hitachi AMS/WMS) 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。

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については、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。

- 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。

Tuning Manager - Agent for RAID 専用のアカウントの作成方法については、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。

- 次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
- PI_CLCS レコード
- PI_CLPS レコード
- 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

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は、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。

- ヘルスチェックを実行する場合、次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。

- 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

レコードの保存期間は Tuning Manager の Performance Reporter で設定してください。レコードの保存期間の設定方法については、マニュアル「*Hitachi Command Suite Tuning Manager 運用管理ガイド*」を参照してください。

設定するレコードの保存期間を「[表 56 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。

表 56 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)

Performance データベースの種類	プロパティ名	設定値
Store データベースバージョン 1.0	Product Interval - Hour Drawer	Month
	Product Interval - Day Drawer	Year
Store データベースバージョン 2.0	Period - Hour Drawer (Day)	9 以上
	Period - Day Drawer (Week)	5 以上
Hybrid Store	Retention - hourly	216 以上
	Retention - daily	35 以上



ヒント

ホストごとに性能分析する場合は、分析したい期間に合わせて PI_LDS レコードの保存期間を設定してください。

6.2.6 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。

前提条件

- 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

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 (Linux の場合) でのログイン

操作手順

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：24230) 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。

関連タスク

- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [2.3.1 Device Manager および Tiered Storage Manager でファイアウォールへの例外登録が必要なポート](#)

6.2.7 Tuning Manager サーバとのリモート接続（Windows のクラスタ環境）

Windows のクラスタ環境で 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、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。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。

前提条件

- 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

操作手順

1. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスをオフラインにします。

```
< Hitachi Command Suite のインストールフォルダ > %Base64%ClusterSetup  
%hcnds64clustersrvstate /soff /r <リソースグループ名 >
```

```
soff
```

クラスタ管理アプリケーションのリソースグループに登録された Hitachi Command Suite 製品のサービスをオフラインにして、フェールオーバーを抑制するためのオプションです。

```
r
```

リソースグループ名を指定します。

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：24230）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。
5. Hitachi Command Suite 製品のサービスを停止します。
6. 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。
7. 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。
8. Hitachi Command Suite 製品のサービスを停止します。
9. 次のコマンドを実行して、リソースグループおよび Hitachi Command Suite 製品のサービスをオンラインにします。

```
< Hitachi Command Suite のインストールフォルダ > %Base64%ClusterSetup  
%hcnds64clustersrvstate /son /r <リソースグループ名 >
```

son

クラスタ管理アプリケーションに設定されたリソースグループをオンラインにして、フェールオーバーを有効にするためのオプションです。

r

リソースグループ名を指定します。

関連タスク

- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [9.3 クラスタ管理アプリケーションに登録されている Hitachi Command Suite 製品のサービス](#)

6.2.8 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：24230）

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。



メモ

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（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
- 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

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager  
%HiCommandServer%tools%htmsetup.bat
```

Linux の場合

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/tools/  
htmsetup.sh
```

関連タスク

- [9.1.3 Hitachi Command Suite のサービスの停止](#)

6.2.9 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。
- Device Manager に RMI 通信できるホストを制限したい場合
Device Manager に RMI 通信できるホストを制限する事で、外部ホストからのサービス妨害攻撃やバッファオーバーフローを狙った攻撃を防ぐのに役立ちます。
以下の設定をしてください。以下の全ての設定について config.xml ファイルと configforclient.xml ファイルで、同じ値を設定してください。
 - Tuning Manager サーバと Device Manager サーバを同一ホストにインストールしている場合
ownHostLoopback パラメーター※の値を true に指定してください。また、ownHost パラメーターに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。
注※ ownHostLoopback パラメーターの定義は、<vserver-connection>タグ配下に追加してください。
 - Tuning Manager サーバと Device Manager サーバを別ホストにインストールしている場合

allowHosts パラメーター※に、Tuning Manager server の IP アドレスまたはホスト名を指定してください。IP アドレスの指定は、IPv4 アドレスまたは IPv6 アドレスが使用できます。

また、ownHostLoopback パラメーターを true に変更していた場合は、ownHostLoopback パラメーターに false を指定してください（デフォルト：false）。Tuning Manager の管理サーバに NIC が複数搭載されており、かつホスト名ではなく IP アドレスを指定する場合、Device Manager と通信可能な全ての IP アドレスをコンマ (,) で区切って指定してください。

Device Manager サーバが複数の Tuning Manager サーバと通信する場合は、すべての Tuning Manager サーバの IP アドレスまたはホスト名をコンマ (,) で区切りつけて指定してください。

Device Manager サーバと同一ホストにインストールしている Tuning Manager サーバについては、指定は不要です。

注※ allowHosts パラメーターの定義は、<vserver-connection>タグ配下に追加してください。

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

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager  
%HiCommandServer%vsa%conf
```

Linux の場合

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/vsa/conf
```

関連参照

- [2.3.1 Device Manager および Tiered Storage Manager でファイアーウォールへの例外登録が必要なポート](#)

6.2.10 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、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 AnalyticsReportDefV840 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。

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は、マニュアル「*Hitachi Command Suite ユーザーズガイド*」を参照してください。

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は、マニュアル「*Hitachi Command Suite Tuning Manager 運用管理ガイド*」を参照してください。

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は、マニュアル「*Hitachi Command Suite Tuning Manager ユーザーズガイド*」を参照してください。

6.3 [レプリケーション] タブで 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。

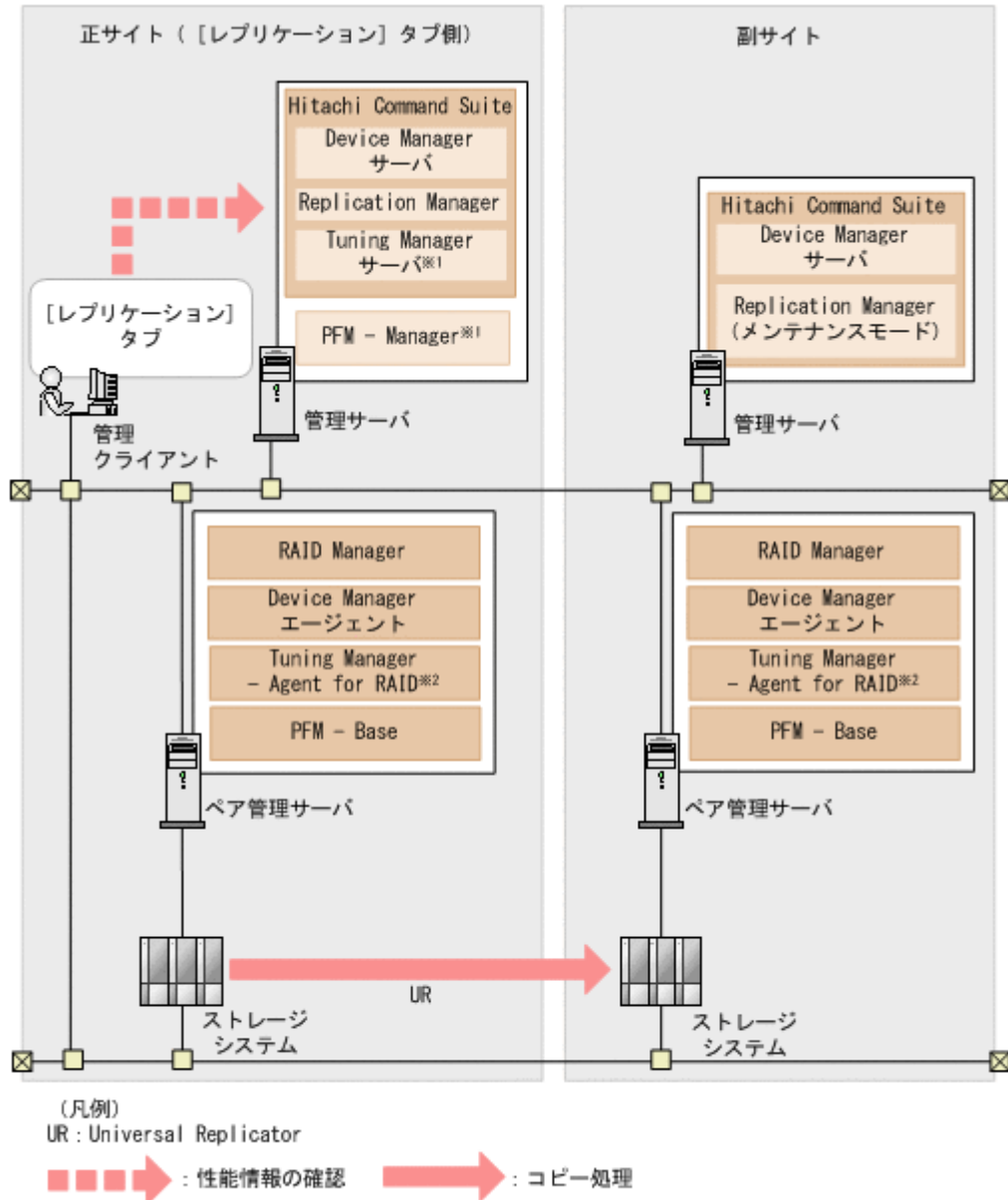
6.3.1 [レプリケーション] タブで Universal Replicator の性能を分析するためのシステム構成

[レプリケーション] タブで Universal Replicator の性能を分析するには, 次を示すプログラムが必要です。Replication Manager を導入済みで, すでに Universal Replicator の運用をしていることを前提とします。

- Device Manager
- Replication Manager
- Tuning Manager
- Tuning Manager - Agent for RAID

[レプリケーション] タブで Universal Replicator の性能を分析するためのシステム構成例を次に示します。

図 51 管理クライアントから正サイトの 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サーバとは異なるマシンにインストールされている場合があります。
 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があります。

各プログラムの要件を次に示します。[レプリケーション] タブを利用する場合、管理クライアントからは正サイトと副サイトのどちらかの Device Manager サーバに接続できます。

- 管理クライアントから接続する Device Manager サーバと同じ管理サーバで稼働する Replication Manager で、性能分析対象の Universal Replicator ペアの C/T デルタを確認できること。
- 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内に、Tuning Manager サーバが 1 つ以上稼働していること。
- 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接続する Device Manager サーバとは別のサイト (図の例では副サイト) にある Replication Manager をメンテナンスモードにしていること。

Replication Manager のメンテナンスモードについては、マニュアル「*Hitachi Command Suite Replication Manager システム構成ガイド*」を参照してください。

- 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設定になっていること。
 - 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 サーバが使用するポート番号については、マニュアル「*Hitachi Command Suite Tuning Manager インストールガイド*」を参照してください。Tuning Manager - Agent for RAID が使用するポート番号については、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。
 - 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 サーバを Device Manager サーバとは別のマシンにインストールする場合、Device Manager サーバと Tuning Manager サーバ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。
- Tuning Manager - Agent for RAID で Tuning Manager API の利用を有効にしていること。
Performance データベースの種別は、バージョン 8.1.3 以降の Tuning Manager - Agent for RAID でサポートしている Hybrid Store にすることをお勧めします。Performance データベースを Hybrid Store にすると、Tuning Manager API の利用が有効になります。
Performance データベースの移行および Tuning Manager - Agent for RAID のインストールについては、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。
Performance データベースの種別が Store データベースの場合、Tuning Manager API の利用を有効にするには htmrestctrl コマンドを実行します。htmrestctrl コマンドについては、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。



メモ

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。



ヒント

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

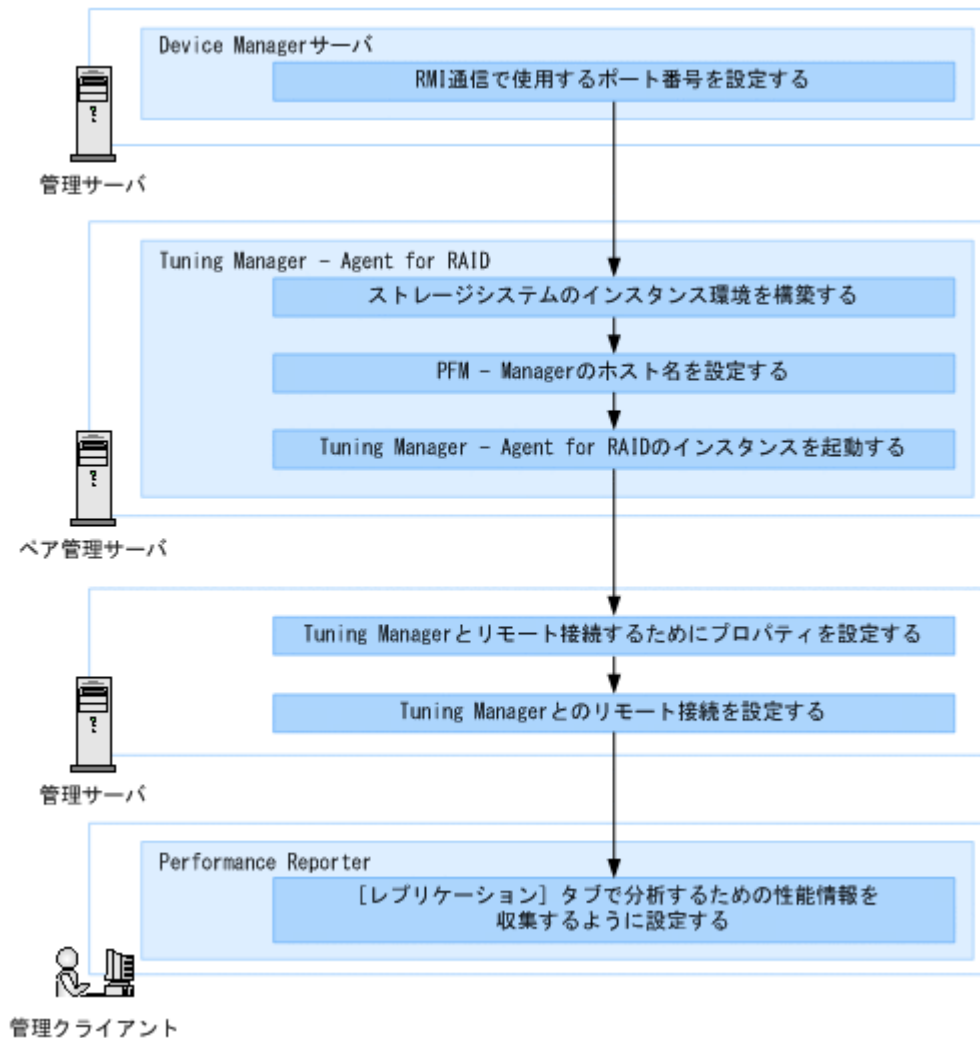
関連概念

- [2.3 Device Manager および Tiered Storage Manager でのファイアウォールの例外登録](#)

6.3.2 [レプリケーション] タブで Universal Replicator の性能を分析するための設定の流れ

レプリケーションタブで Universal Replicator の性能を分析するためには、管理サーバでの Device Manager、Replication Manager および Tuning Manager の設定、ペア管理サーバでの Tuning Manager - Agent for RAID の設定がそれぞれ必要です。

図 52 レプリケーションタブで Universal Replicator の性能を分析するための設定の流れ



関連タスク

- 6.2.6 Tuning Manager サーバとのリモート接続 (非クラスタ環境)
- 6.2.7 Tuning Manager サーバとのリモート接続 (Windows のクラスタ環境)
- 6.3.3 RMI 通信で使用するポート番号を Device Manager サーバに設定する
- 6.3.4 ストレージシステムのインスタンス環境を構築する
- 6.3.5 PFM - Manager のホスト名を設定する
- 6.3.6 Tuning Manager - Agent for RAID のインスタンスを起動する
- 6.3.7 Tuning Manager とリモート接続するためにプロパティを設定する
- 6.3.8 [レプリケーション] タブで分析するための性能情報を収集するように設定する

6.3.3 RMI 通信で使用するポート番号を Device Manager サーバに設定する

[レプリケーション] タブを利用するには、Replication Manager との連携で RMI 通信を使用する必要がありますため、RMI 通信で使用するポート番号を Device Manager サーバに設定します。

前提条件

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

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. Device Manager サーバの `rpmlib.properties` ファイルにある `rpmlib.rpm.port` プロパティを設定します。

Replication Manager の `base.properties` ファイルにある `base.rmi.port` プロパティに設定されているポート番号を入力してください。 `base.rmi.port` プロパティの値 (デフォルト: 25200) を変更していない場合は、設定不要です。

`base.properties` ファイルは次の場所に格納されています。

Windows の場合 :

< Hitachi Command Suite のインストールフォルダ > \ReplicationManager\conf

Linux の場合 :

< Hitachi Command Suite のインストールディレクトリ > /ReplicationManager/
conf

Replication Manager の `base.properties` ファイルおよび `base.rmi.port` プロパティについては、マニュアル「*Hitachi Command Suite Replication Manager システム構成ガイド*」を参照してください。

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [付録 A.16.1 rpmlib.rpm.port](#)

6.3.4 ストレージシステムのインスタンス環境を構築する

分析対象の正ストレージシステムと副ストレージシステムを Tuning Manager - Agent for RAID で監視するために、ペア管理サーバでストレージシステムごとにインスタンス環境を構築します。

前提条件

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

操作手順

1. `jpctdlistraid` コマンドを実行して、分析対象のストレージシステムのコマンドデバイスを確認します。

`DEVICE_FILE` の値を確認してください。

jpctdlistraid コマンドについては、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。

2. `jpccconf inst setup` コマンドを対話形式で実行して、分析対象のストレージシステムのインスタンス環境を構築します。

インスタンスは、1つのストレージシステムにつき1つ作成してください。

対話形式で次のインスタンス情報を入力してください。

- Storage Model : 2
- Method for Collecting : 1 または 3
- Command Device File Name : 手順 1 の `jpctdlistraid` コマンドで確認した `DEVICE_FILE` の値
- Unassigned Open Volume Monitoring : Y
- Mainframe Volume Monitoring : 任意の値
- Store Version : 指定なし

`jpccconf inst setup` コマンドについては、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」およびマニュアル「*JPI/Performance Management リファレンス*」を参照してください。

3. `jpctdchkinst` コマンドを実行して、設定したインスタンス情報の内容を確認します。

[Check result]に KAVF18850-I メッセージが出力されていれば、問題ありません。

`jpctdchkinst` コマンドについては、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」を参照してください。

6.3.5 PFM - Manager のホスト名を設定する

ペア管理サーバで、Tuning Manager - Agent for RAID が管理されている PFM - Manager のホスト名を設定します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 次の情報の確認
 - PFM - Manager がインストールされているマシンのホスト名

操作手順

1. `jpccconf mgrhost define` コマンドを実行します。

`jpccconf mgrhost define` コマンドについては、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」およびマニュアル「*JPI/Performance Management リファレンス*」を参照してください。

6.3.6 Tuning Manager - Agent for RAID のインスタンスを起動する

ペア管理サーバで Tuning Manager - Agent for RAID を起動して、構築したインスタンス環境を Tuning Manager - Agent for RAID で運用できるようにします。

前提条件

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

操作手順

1. `jpcspm start` コマンドを実行して、Tuning Manager - Agent for RAID の対象インスタンスを起動します。
`jpcspm start` コマンドについては、マニュアル「*Hitachi Command Suite Tuning Manager - Agents*」およびマニュアル「*JPI/Performance Management リファレンス*」を参照してください。
2. `jpctool service list` コマンドを実行して、対象インスタンスの状態を確認します。
インスタンスの状態が次の条件を満たしていることを確認してください。
 - 1つのインスタンスにつき、サービス名に DA1 と DS1 が登録されていること。
 - DA1 と DS1 の Status が Active になっていること。`jpctool service list` コマンドについては、マニュアル「*JPI/Performance Management リファレンス*」を参照してください。

6.3.7 Tuning Manager とリモート接続するためにプロパティを設定する

Device Manager サーバと Tuning Manager が異なるマシンにインストールされている場合は、リモート接続する必要があるため、Device Manager サーバの `tuningmanager.properties` ファイルのプロパティを設定します。

前提条件

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

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. Device Manager サーバの `tuningmanager.properties` ファイルにある次のプロパティを設定します。
 - `htnm.servers`
 - `htnm.server.n.host`
 - `htnm.server.n.protocol`
 - `htnm.server.n.port``n` には、「0」から「`<htnm.servers` プロパティで指定した値 $> - 1$ 」までの値を指定します。
3. Hitachi Command Suite 製品のサービスを起動します。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [付録 A.14.2 htnm.servers](#)
- [付録 A.14.3 htnm.server.n.host](#)
- [付録 A.14.4 htnm.server.n.protocol](#)
- [付録 A.14.5 htnm.server.n.port](#)

6.3.8 [レプリケーション] タブで分析するための性能情報を収集するように設定する

[レプリケーション] タブで分析できるメトリックの性能情報を収集するには、Tuning Manager の Performance Reporter で、Tuning Manager - Agent for RAID のパフォーマンスデータを記録するように、各メトリックに対応するレコードごとにプロパティを変更します。

操作手順

1. Performance Reporter の Agent Collector サービスのプロパティ画面を表示します。
パフォーマンスデータの記録方法を変更するために、Performance Reporter の Agent Collector サービスのプロパティ画面を表示する方法については、マニュアル「*Hitachi Command Suite Tuning Manager 運用管理ガイド*」を参照してください。
2. [サービスのプロパティ] の [Interval Records] ノードを展開します。
3. レコードを選択して、[Log] プロパティを [Yes] に変更します。
設定が必要なメトリックとレコードの対応を次の表に示します。

表 57 [レプリケーション] タブで分析するために設定が必要なメトリックとレコードの対応

メトリック	レコード	
プロセッサ利用率	PI_PRCs ^{*1}	
キャッシュ書き込み待ち率	PI_CLMS ^{*2}	
ポートデータ流出量	PI_PTS ^{*1}	
正ジャーナルデータ流入量	PI_JNLS	
正ジャーナルデータ流出量		
正ジャーナル書き込み IOPS		
正ジャーナル読み込み処理時間		
正ジャーナル書き込みブロックサイズ		
副ジャーナルデータ取得時間		
副ジャーナル転送・処理時間		
正ボリュームデータ流入量		PI_LDS ^{*1}

注※1

デフォルトでは、[Log] プロパティが [Yes] に設定されています。

注※2

Tuning Manager - Agent for RAID のバージョンが 8.1.1 以降の場合、デフォルトでは、[Log] プロパティが [Yes] に設定されています。

6.3.9 [レプリケーション] タブで分析するための性能情報の収集時間や収集間隔を変更する

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が、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。



メモ

次の場合、定期収集は実行されません。

- Device Manager GUI/CLI での構成情報や性能情報の収集中

- ・ 定期収集の実行中に、次の収集開始時刻になった場合

前提条件

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

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. Device Manager サーバの replication.properties ファイルにあるプロパティを設定します。
3. Hitachi Command Suite 製品のサービスを起動します。

関連タスク

- ・ [9.1.2 Hitachi Command Suite のサービスの起動](#)
- ・ [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- ・ [付録 A.15 \[レプリケーション\] タブに関するプロパティ \(replication.properties ファイル\)](#)

6.3.10 Universal Replicator の性能を分析する際の注意事項

[レプリケーション] タブで Universal Replicator の性能を分析する際の注意事項について説明します。

- ・ 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。
- ・ 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。

6.4 [レプリケーション] タブでレプリケーション管理機能を利用するために必要な設定

[レプリケーション] タブのレプリケーション管理機能を使用すると、1つのサイトだけではなく複数のサイトにわたるレプリケーションの構成を管理できます。

各サイトは、1台の管理サーバとペア管理サーバ、複数のストレージシステムから構成されます。[レプリケーション] タブを使用することで、遠隔地にある別のサイトとの間で TrueCopy や Universal Replicator のペアを構成し、ディザスタリカバリーに備えた運用ができます。

ここでは、レプリケーション管理機能を利用する場合の複数のサイトと連携した構成や必要な設定について説明します。

レプリケーション管理機能の前提となるコピーペア管理のシステム構成や要件については、コピーペア管理について説明している章を参照してください。高可用性システムを構築するためのシステム構成や要件については、高可用性システムの構築について説明している章を参照してください。

関連概念

- ・ [1.19 高可用性システムの構築](#)

関連参照

- ・ [1.14 コピーペアを管理する場合のシステム構成 \(一括管理構成\)](#)

- 1.15 コピーペアを管理する場合のシステム構成（一括管理構成以外）
- 1.16 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
- 1.18 コピーペアを管理する場合の注意事項
- 1.17 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

6.4.1 [レプリケーション] タブでレプリケーション管理機能を利用する場合のシステム構成（複数サイト構成）

レプリケーション管理機能を利用する場合の複数のサイトと連携したシステム構成例を次に示します。

図 53 レプリケーション管理機能を利用する場合のシステム構成例（2 サイト構成）

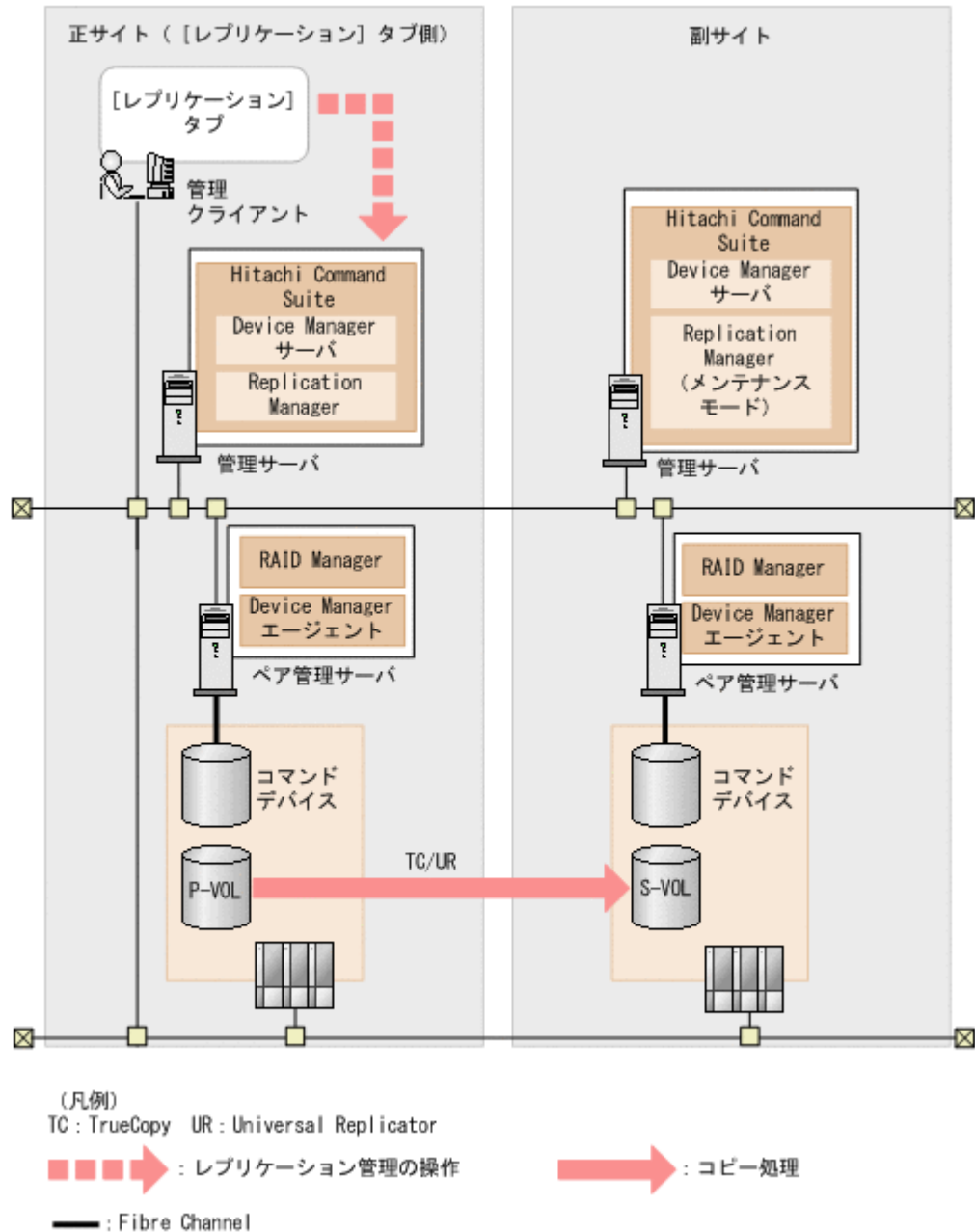
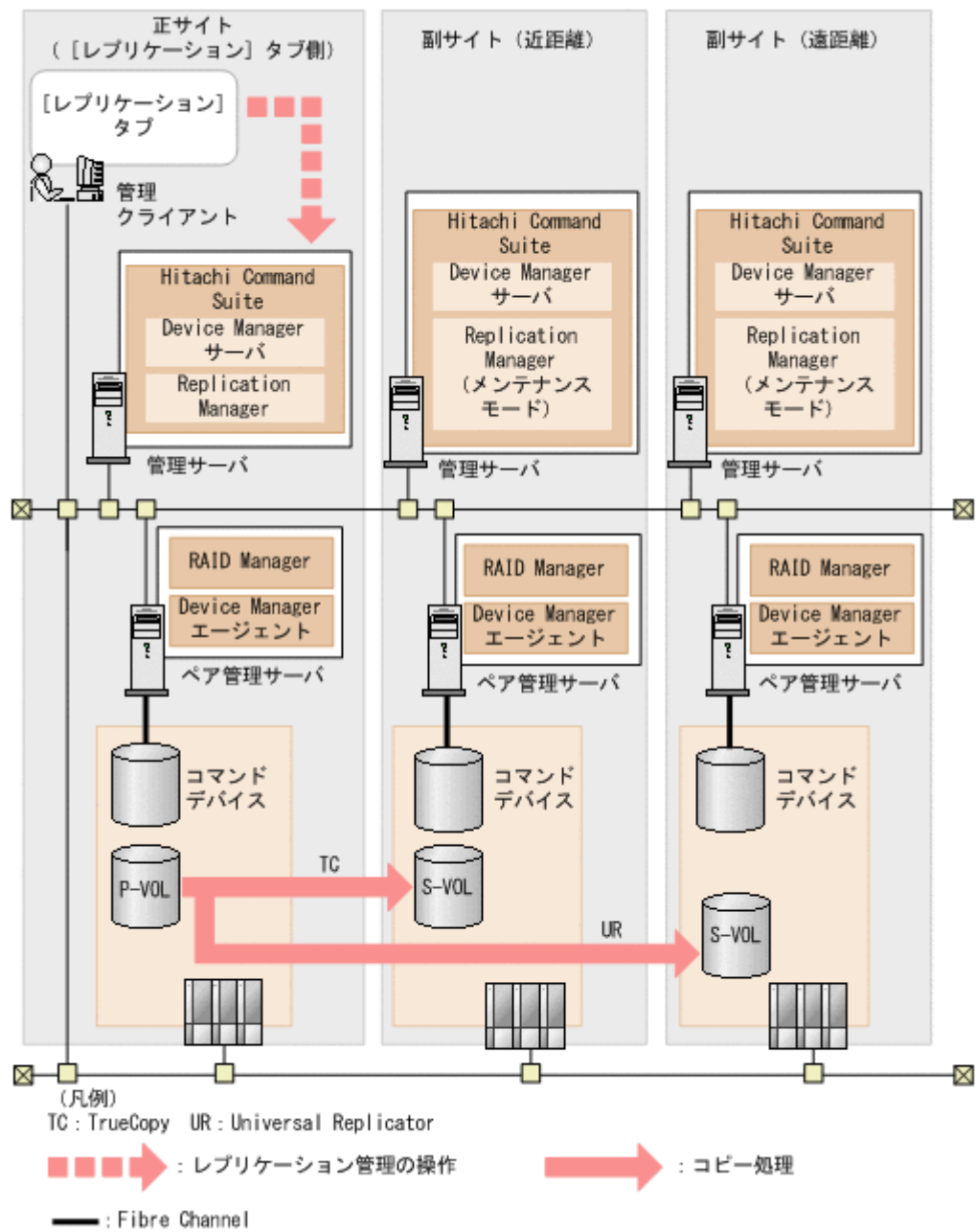


図 54 レプリケーション管理機能を利用する場合のシステム構成例 (3 サイト構成)



6.4.2 [レプリケーション] タブでレプリケーション管理機能を利用するための設定の流れ

[レプリケーション]タブでレプリケーション管理機能を利用するための設定の流れについて説明します。

図 55 [レプリケーション] タブでレプリケーション管理機能を利用するための設定の流れ (1 サイト構成)

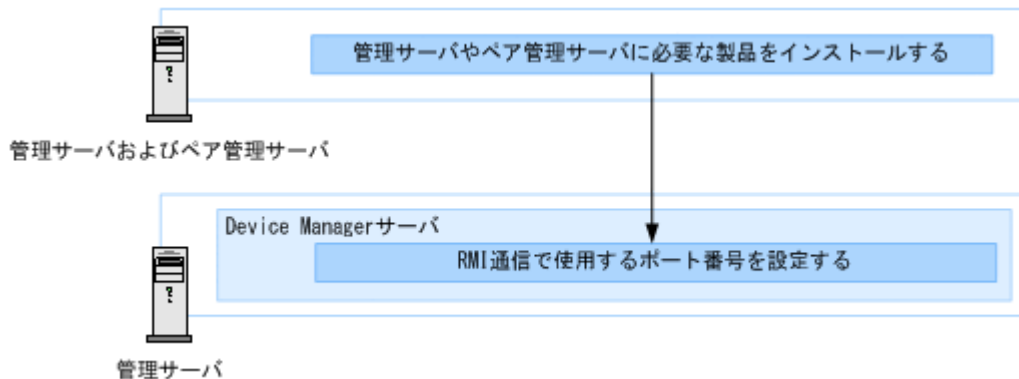
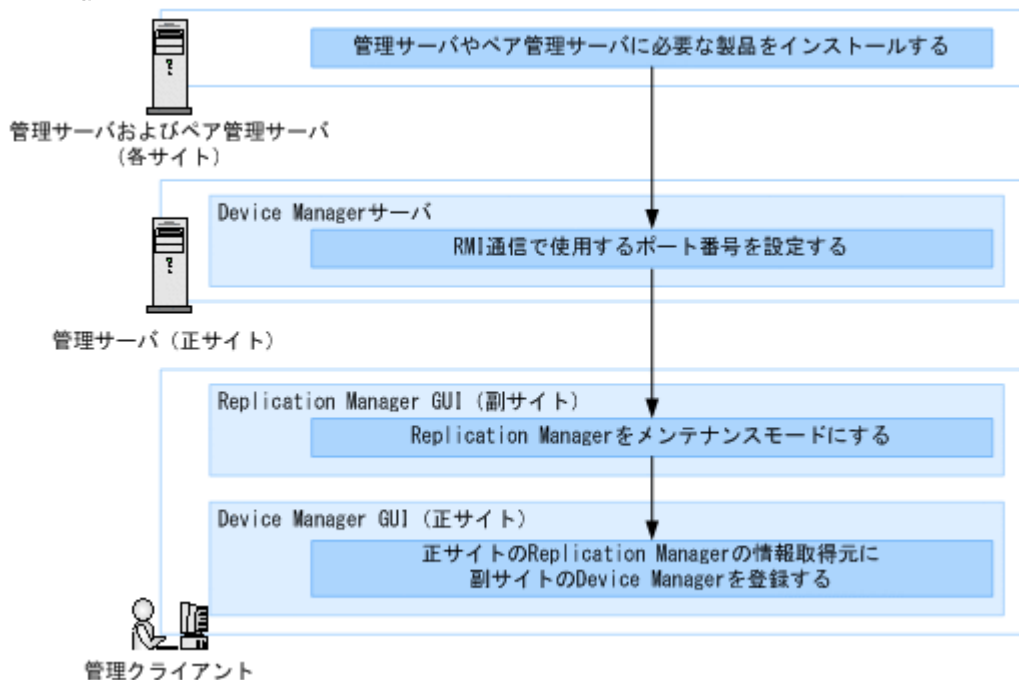


図 56 [レプリケーション] タブでレプリケーション管理機能を利用するための設定の流れ (複数サイト構成)



正サイトの Replication Manager の情報取得元に副サイトの Device Manager を登録するには、[レプリケーション] タブを使用します。詳細は、マニュアル「Hitachi Command Suite ユーザーズガイド」を参照してください。

関連タスク

- 6.4.3 管理サーバやペア管理サーバに必要な製品をインストールする
- 6.4.4 RMI 通信で使用するポート番号を Device Manager サーバに設定する
- 6.4.5 副サイトの Replication Manager をメンテナンスモードにする

6.4.3 管理サーバやペア管理サーバに必要な製品をインストールする

システム構成に従って、管理サーバやペア管理サーバに必要な製品をインストールしてください。

操作手順

1. 管理サーバに Hitachi Command Suite をインストールします。
Hitachi Command Suite のインストール方法については、マニュアル「*Hitachi Command Suite* インストールガイド」を参照してください。
2. ペア管理サーバに RAID Manager および Device Manager エージェントをインストールします。
RAID Manager のインストール方法については、RAID Manager のマニュアルを参照してください。
Device Manager エージェントのインストール方法については、マニュアル「*Hitachi Command Suite* インストールガイド」を参照してください。

6.4.4 RMI 通信で使用するポート番号を Device Manager サーバに設定する

[レプリケーション] タブを利用するには、Replication Manager との連携で RMI 通信を使用する必要があるため、RMI 通信で使用するポート番号を Device Manager サーバに設定します。

前提条件

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

操作手順

1. Hitachi Command Suite 製品のサービスを停止します。
2. Device Manager サーバの `rpmlib.properties` ファイルにある `rpmlib.rpm.port` プロパティを設定します。
Replication Manager の `base.properties` ファイルにある `base.rmi.port` プロパティに設定されているポート番号を入力してください。 `base.rmi.port` プロパティの値 (デフォルト: 25200) を変更していない場合は、設定不要です。
`base.properties` ファイルは次の場所に格納されています。

Windows の場合 :

< Hitachi Command Suite のインストールフォルダ > \ReplicationManager\conf

Linux の場合 :

< Hitachi Command Suite のインストールディレクトリ > /ReplicationManager/
conf

Replication Manager の `base.properties` ファイルおよび `base.rmi.port` プロパティについては、マニュアル「*Hitachi Command Suite Replication Manager* システム構成ガイド」を参照してください。

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [付録 A.16.1 rpmlib.rpm.port](#)

6.4.5 副サイトの Replication Manager をメンテナンスモードにする

複数サイト構成の場合、副サイトの Replication Manager の動作モードをメンテナンスモードに変更します。

前提条件

副サイトの Device Manager の GUI へのログイン

操作手順

1. Device Manager の GUI の [設定] メニューから [レプリケーション管理] を選択します。
2. [エクスプローラ] メニューで、[管理者メニュー] - [メンテナンス] をクリックします。
3. [モード変更] ボタンをクリックします。
4. メッセージを確認し、メンテナンスモードに変更します。

6.5 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCH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UNCHできます。

6.5.1 JP1/IM から Hitachi Command Suite 製品の GUI をラUNCH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UNCHできるようにするには、マシン環境を確認してください。

- 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 ! \$ - . @ _



ヒント

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。

JP1/IM から Hitachi Command Suite 製品の GUI をラUNCHする前提 OS や前提プログラムについては、「ソフトウェア添付資料」を参照してください。

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 を起動する方法については、JP1/IM のマニュアルを参照してください。

6.5.2 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 の統合機能メニュー定義ファイルを作成します。

前提条件

- 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。

操作手順

1. JP1/IM - View 用の統合機能メニュー定義ファイルのサンプルファイルを JP1/IM - View がインストールされているマシンにコピーします。

コピー元

Windows の場合 :

< Hitachi Command Suite のインストールフォルダ > ¥Base64¥sample¥JP1_IM_conf

Red Hat Enterprise Linux の場合 :

< Hitachi Command Suite のインストールディレクトリ > /Base64/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



注意

- 管理サーバの OS が 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 64 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 22015, SSL 通信の場合は 22016 です。

操作結果

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]

関連参照

- [6.5.1 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。

- 7.1 Hitachi Command Suite 共通トレースログの設定
- 7.2 アラートの設定
- 7.3 SNMP トラップをログファイルに出力するための設定
- 7.4 Device Manager のイベント通知を使用するために必要な設定
- 7.5 Tiered Storage Manager のイベント通知を使用するために必要な設定
- 7.6 JP1/IM でログを参照するために必要な設定

7.1 Hitachi Command Suite 共通トレースログの設定

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。

7.1.1 Hitachi Command Suite 共通トレースログファイルの設定 (Windows)

Hitachi Command Suite 共通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

設定を変更すると、Hitachi Command Suite 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。

前提条件

- Administrator 権限でのログイン

操作手順

- 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。

7.1.2 Hitachi Command Suite 共通トレースログファイルの設定 (Linux)

Hitachi Command Suite 共通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

設定を変更すると、Hitachi Command Suite 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。

前提条件

- root でのログイン

操作手順

- 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

2. メニューで、2 ([Number of log files]) を指定します。
3. 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/HNTRLlib/mmap/hntrmmap.mm
```
9. 変更を適用するために、OS を再起動します。

7.2 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。アラートは E メールでも通知できます。

7.2.1 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やファイルサーバ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。



メモ

ポーリングでは、部位ごとに、前回のポーリング時の障害レベルと異なる障害レベルを検知した場合にのみアラートを検知します。このため、以下の場合に障害が検知できないことがあります。

- 既に障害が発生している部位で発生した障害レベルが同じ障害
- ポーリング間隔の間に発生し、回復した障害

また、ポーリング間隔の間に同じ部位で複数の障害が発生した場合、1つの障害にまとめられません。



ヒント

- ポーリングでは、Device Manager がストレージシステムやファイルサーバから受領した稼働状況をそのままアラートとして表示します。
- ポーリングでは、Device Manager サーバが停止中に発生した障害が Device Manager の再起動後も継続している場合、検知できることがあります

- 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。



メモ

SNMP トラップ受信では、Device Manager サーバが停止中に発生した障害はアラートとして表示できません。



ヒント

Device Manager がストレージシステムやファイルサーバから受信した SNMP トラップをそのままアラートとして表示します。

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 58 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	アラートのメール通知
ストレージシステム	VSP 5000 シリーズ	Y	v1, v3	Y
	VSP G1000	Y	v1, v3 ^{*1}	Y
	VSP G1500	Y	v1, v3	Y
	VSP F1500	Y	v1, v3	Y
	VSP Gx00 モデル	Y	v1, v3 ^{*2}	Y
	VSP Fx00 モデル	Y	v1, v3 ^{*2}	Y
	Virtual Storage Platform	Y	v1	Y
	Universal Storage Platform V/VM	Y	v1	Y
	Hitachi USP	Y	v1	Y
	HUS VM	Y	v1	Y
	HUS100	Y	--	Y
	Hitachi AMS2000	Y	--	Y
	Hitachi SMS	Y	--	Y
	Hitachi AMS/WMS	Y	--	Y
	SMI-S enabled ストレージシステム	--	--	--
ファイルサーバ	Hitachi Virtual File Platform	--	v2c	--
	Hitachi Capacity Optimization	--	v2c	--
	NAS Platform	Y ^{*3}	v1 ^{*3}	Y ^{*3}

(凡例)

Y : サポート

-- : 非サポート

- v1 : SNMP v1 をサポート
- v2c : SNMP v2c をサポート
- v3 : SNMP v3 をサポート

注※1

VSP G1000 のマイクロコードのバージョンが、80-03-0X-XX/XX 以降の場合に SNMP v3 をサポートします。

注※2

VSP Gx00 モデルおよび VSP Fx00 モデルのマイクロコードのバージョンが、83-01-2X-XX/XX 以降の場合に SNMP v3 をサポートします。
NAS モジュールの場合、SNMP v1 だけをサポートします。

注※3

ファイルサーバの場合、障害情報を検知するには、次の条件をどちらも満たしている必要があります。

- ・ NAS Platform のバージョンが 12.2 以降であること
- ・ Admin services EVS が設定されていること



メモ

- ・ ファイルサーバまたは NAS モジュールの場合、ポーリングと SNMP トラップでは、障害を検知するタイミングが異なりますが、アラートに表示される内容は同じです。5 分間隔より短い間隔でアラートを取得したい場合だけ、SNMP トラップの設定をしてください。デフォルトでは、5 分間隔のポーリングでアラートを取得しています。
- ・ ストレージシステムの場合、ポーリングと SNMP ラップでは、障害を検知するタイミングだけでなく、障害レベルも異なることがあります。これは、発生場所とその発生部位の障害が与える障害部位への影響度によって、障害部位の障害レベルが異なるためです。
- ・ ポーリングと SNMP ラップの両方で同じ障害を検知している場合、それぞれをアラートとして表示します。ただし、同一の障害であっても、前述のとおり、ポーリングと SNMP トラップで障害レベルが異なることがあります。

関連概念

- ・ [7.2.2 SNMP トラップをアラートに表示するための設定](#)

関連タスク

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

関連参照

- ・ [付録 A.5.3 server.dispatcher.daemon.pollingPeriod](#)

7.2.2 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。

- ・ rpm パッケージのインストール (Linux の場合)
SNMP トラップを受信するために必要な rpm パッケージをインストールしてください。必要な rpm パッケージの詳細は、「ソフトウェア添付資料」を参照してください。
- ・ 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 v3を使用する場合は、hdvmsnmpuser コマンドで、SNMP トラップ受信ユーザーの認証情報の登録および暗号化の設定をする
- 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 (SNMP v1, SNMP v3 共通)
 - SNMP v3を使用する場合は、SNMP Agent で、SNMP トラップ受信ユーザーの認証情報の登録および暗号化の設定をする
管理サーバと同じ内容を設定してください。認証情報の登録および暗号化の設定方法については、マニュアル「*SNMP Agent ユーザガイド*」を参照してください。
 - NAS Platform の場合は、SMU, NAS Manager, または NAS Platform CLI 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
設定する IP アドレスの形式 (IPv6 または IPv4) は、次の形式に合わせてください。

表 59 設定する管理サーバの IP アドレスの形式 (NAS Platform の SNMP トラップの設定)

条件		IP アドレスの形式 (IPv6 または IPv4)
Admin services EVS から SNMP トラップを送信するように、NAS Platform CLI で設定している		Admin services EVS の IP アドレスの形式に合わせる
Admin services EVS から SNMP トラップを送信しないように、NAS Platform CLI で設定している	ファイルシステムをマウントする EVS がある	ファイルシステムをマウントする EVS の IP アドレスの形式に合わせる
	ファイルシステムをマウントする EVS がない	ファイルサーバ (ノード) の IP アドレスの形式に合わせる

- Hitachi Virtual File Platform および Hitachi Capacity Optimization 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

SNMP v1 または SNMP v2c で、Device Manager とストレージシステムまたはファイルサーバ間の通信をする場合、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。

SNMP v3 で、Device Manager とストレージシステム間の通信をするときは、SNMP トラップ受信ユーザーに設定された認証情報に基づいて、すべての SNMP トラップを受信してアラートに表示します。

関連タスク

- [7.2.3 SNMP トラップ受信ユーザーを登録する \(SNMP v3\)](#)
- [付録 A.1.1 Device Manager サーバのプロパティの変更](#)

関連参照

- [付録 A.5.5 server.dispatcher.daemon.receiveTrap](#)

7.2.3 SNMP トラップ受信ユーザーを登録する (SNMP v3)

Device Manager でストレージシステムからの SNMP v3 トラップを受信するためには、SNMP トラップ受信ユーザーの登録が必要です。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 次の情報の確認
 - hdvmsnmpuser コマンド実行時に Device Manager との認証に使うユーザーアカウント 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 およびパスワードを確認します。

操作手順

1. Device Manager サーバで hdvmsnmpuser コマンドを実行します。

なお、hdvmsnmpuser コマンドで設定した内容を有効にするために、Device Manager サーバを再起動する必要はありません。

関連参照

- [7.2.4 SNMP トラップ受信ユーザーを管理するためのコマンド \(hdvmsnmpuser\) の形式 \(SNMP v3\)](#)

7.2.4 SNMP トラップ受信ユーザーを管理するためのコマンド (hdvmsnmpuser) の形式 (SNMP v3)

SNMP トラップ受信ユーザーの情報を設定するには、hdvmsnmpuser コマンドを実行します。

hdvmsnmpuser コマンドでは、ユーザー情報の登録、変更、削除、および取得ができます。

コマンドの形式

ユーザー情報を登録する場合：

```
hdvmsnmpuser -u <Device Manager のユーザー ID> -p <Device Manager のパスワード> add --user_name <SNMP トラップ受信ユーザー名> --security_level <セキュリティレベル> [--auth_protocol <認証プロトコル> --auth_password <認証パスワード> [--encrypt_protocol <暗号化プロトコル> --encrypt_key <暗号キー> ] ]
```

ユーザー情報を変更する場合：

```
hdvmsnmpuser -u <Device Manager のユーザー ID> -p <Device Manager のパスワード> modify --user_name <SNMP トラップ受信ユーザー名> [--security_level <セキュリティレベル> ] [--auth_protocol <認証プロトコル> ] [--auth_password <認証パスワード> ] [--encrypt_protocol <暗号化プロトコル> --encrypt_key <暗号キー> ]
```

ユーザー情報を削除する場合：

```
hdvmsnmpuser -u <Device Manager のユーザー ID> -p <Device Manager のパスワード> delete --user_name <SNMP トラップ受信ユーザー名>
```

ユーザー情報を取得する場合

```
hdvmsnmpuser -u <Device Manager のユーザー ID> -p <Device Manager のパスワード> get [--user_name <SNMP トラップ受信ユーザー名> ]
```

コマンドの格納先

Windows の場合 :

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager  
%HiCommandServer%tools%hdvmsnmpuser.bat
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/tools/  
hdvmsnmpuser.sh
```

オプション

SNMP トラップ受信ユーザー名、認証パスワード、および暗号キーに使用できる文字は次のとおりです。

A~Z a~z 0~9 空白文字 半角記号

次の記号は使用できません。

¥ , / : ; * ? " < > | & % ^

大文字と小文字は区別されます。文字列の先頭または末尾に空白文字を指定しないでください。

-u <Device Manager のユーザー ID> , -p <Device Manager のパスワード>

Device Manager のユーザー ID およびパスワードを指定します。

--user_name <SNMP トラップ受信ユーザー名>

SNMP トラップ受信ユーザー名を指定します。指定できる最大文字数は 32 文字です。ユーザー情報を取得する場合、このオプションで指定した SNMP トラップ受信ユーザーの情報を出力します。このオプションを省略したときは、DeviceManager サーバに登録されているすべての SNMP トラップ受信ユーザーの情報を出力します。

--security_level <セキュリティレベル>

セキュリティレベルを指定します。指定できる値は次のとおりです。

authPriv (認証も暗号化もする)
authNoPriv (認証するが暗号化はしない)
noAuthNoPriv (認証も暗号化もしない)

--auth_protocol <認証プロトコル>

認証時に使用するプロトコルとして、SHA または MD5 を指定します。このオプションは、--security_level に authPriv または authNoPriv を設定する場合に指定します。

--auth_password <認証パスワード>

認証用のパスワードを指定します。VSP 5000 シリーズ、VSP G1000、G1500、または VSP F1500 の場合は、8 文字以上 180 文字以下で指定します。VSP Gx00 モデルまたは VSP Fx00 モデルの場合は、8 文字以上 64 文字以下で指定します。

このオプションは、`--security_level` に `authPriv` または `authNoPriv` を設定する場合に指定します。

`--encrypt_protocol` <暗号化プロトコル>

通信時に使用する暗号化プロトコルとして、AES または DES を指定します。

このオプションは、`--security_level` に `authPriv` を設定する場合に指定します。

`--encrypt_key` <暗号キー>

暗号化された情報を復元するためのキーを指定します。VSP 5000 シリーズ、VSP G1000、G1500、または VSP F1500 の場合は、8 文字以上 180 文字以下で指定します。VSP Gx00 モデルまたは VSP Fx00 モデルの場合は、8 文字以上 64 文字以下で指定します。

このオプションは、`--security_level` に `authPriv` を設定する場合に指定します。

また、`--encrypt_protocol` を設定する場合は、必ず指定します。

7.2.5 アラートを E メール通知するための操作フロー

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やファイルサーバ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。

操作手順

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. 受信ユーザーの設定

Device Manager GUI を使用して、E メールを受信するユーザーアカウントを設定します。

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。



メモ

- 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やファイルサーバに対して、環境の構築や保守を実施すると、ストレージシステムやファイルサーバ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.storagesystem` プロパティや `server.mail.enabled.fileserver` 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。

関連タスク

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

関連参照

- [付録 A.2.17 server.mail.enabled.storagesystem](#)
- [付録 A.2.18 server.mail.enabled.fileserver](#)

7.2.6 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。



メモ

- 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。

7.2.7 受信ユーザーの設定

Device Manager GUI を使用して、E メールを受信するユーザーアカウントを設定します。

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。

- 管理対象のリソース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。
Device Manager GUI でのユーザーアカウントの設定については、マニュアル「*Hitachi Command Suite ユーザーズガイド*」を参照してください。



ヒント

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。

7.2.8 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.storagesystem
- server.mail.enabled.fileserver
- 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.storagesystem`
- `server.mail.alert.status`

関連タスク

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

関連参照

- [付録 A.2.17 server.mail.enabled.storagesystem](#)
- [付録 A.2.18 server.mail.enabled.fileserver](#)
- [付録 A.2.19 server.mail.from](#)
- [付録 A.2.20 server.mail.smtp.host](#)
- [付録 A.2.21 server.mail.smtp.port](#)
- [付録 A.2.22 server.mail.smtp.auth](#)
- [付録 A.2.23 server.mail.errorsTo](#)
- [付録 A.2.24 server.eventNotification.mail.to](#)
- [付録 A.2.25 server.mail.alert.type.storagesystem](#)
- [付録 A.2.26 server.mail.alert.status](#)

7.2.9 SMTP 認証ユーザーアカウントを Device Manager に登録する

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。



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。

前提条件

- Administrator 権限 (Windows の場合) または root (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。
- 次の情報の確認
 - 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

操作手順

1. 次のコマンドを実行します。

Windows の場合 :

```
< Hitachi Command Suite のインストールフォルダ > ¥DeviceManager  
¥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 >]
```

Linux の場合 :

```
< Hitachi Command Suite 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 >]
```

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)
- [付録 A.1.1 Device Manager サーバのプロパティの変更](#)

関連参照

- [付録 A.2.22 server.mail.smtp.auth](#)

7.2.10 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 (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 :

```
< Hitachi Command Suite のインストールフォルダ > ¥DeviceManager  
¥HiCommandServer¥config
```

Linux の場合 :

```
< Hitachi Command Suite 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。



メモ

mail-alert-detection.txt ファイルを保存する際に、バイトオーダーマーク (BOM) を付与しないでください。

mail-alert-detection.txt ファイルに BOM が付与されていると、KAIC18797-E のエラーメッセージが出力され、Eメールの送信に失敗します。

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 60 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	アラートの種別
source	アラートの発生元 ストレージシステムまたは NAS モジュールの場合は、ストレージシステム名 ファイルサーバの場合は、クラスタ名またはノード名
status	アラートの重要度
component	問題が発生したコンポーネント ストレージシステムまたは NAS モジュールの場合は、アラートが発生したストレージシステムの部位 ファイルサーバの場合は、File Controller
description	アラートの説明

パラメーター名	説明
recommendedAction	アラートへの対処方法
additionalInfo	補足情報
occurrenceTime	ストレージシステムの場合は、Device Manager サーバがアラート情報を取得した時刻 ファイルサーバまたは NAS モジュールの場合は、アラートが発生した時刻 表示形式：yyyy/mm/dd hh:mm:ss hh は 24 時間表示です。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

7.3 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 v1, SNMP v3 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。

関連概念

- [7.3.1 SNMP トラップをログファイルに出力するための設定](#)
- [7.6 JP1/IM でログを参照するために必要な設定](#)

関連タスク

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

関連参照

- [付録 A.9.2 customizedsnmptrap.customizelist](#)

7.3.1 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 v3 を使用する場合は、`hdvmsnmpuser` コマンドで、SNMP トラップ受信ユーザーの認証情報の登録および暗号化の設定をする
- 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 v3 を使用する場合は、SNMP Agent で、SNMP トラップ受信ユーザーの認証情報の登録および暗号化の設定をする
管理サーバと同じ内容を設定してください。認証情報の登録および暗号化の設定方法については、マニュアル「*SNMP Agent ユーザガイド*」を参照してください。
- 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。

SNMP v1 または SNMP v2c で、Device Manager とストレージシステムまたはファイルサーバ間の通信をする場合、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に出力します。

SNMP v3 で、Device Manager とストレージシステム間の通信をする場合、SNMP トラップ受信ユーザーに設定された認証情報に基づいて、すべての SNMP トラップを受信してログに出力します。

関連タスク

- [7.2.3 SNMP トラップ受信ユーザーを登録する \(SNMP v3\)](#)
- [付録 A.1.1 Device Manager サーバのプロパティの変更](#)

関連参照

- [付録 A.5.5 server.dispatcher.daemon.receiveTrap](#)

- [付録 A.9.1 customizedsnmptrap.customizedSNMPTrapEnable](#)
- [付録 A.9.2 customizedsnmptrap.customizelist](#)

7.4 Device Manager のイベント通知を使用するために必要な設定

Device Manager GUI では、一部を除くすべての事象（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。

ただし、次の HCS タスクはメール通知が行われません。

- HDT プールのモニタリングスケジュールのテンプレート編集
- HDT プールのモニタリングスケジュールのテンプレート削除

Device Manager GUI のタスク作成時に E メール通知を有効にした場合、次の宛先へ実行結果が通知されます。

- Device Manager GUI のタスクを作成する際に設定したメールアドレス
- Device Manager サーバの `server.properties` ファイルにある `server.eventNotification.mail.to` プロパティに設定したメールアドレス

イベントを E メールで通知するためには、次の設定が必要です。アラートを E メールで通知するための設定をすでにしている場合は、1~4 の設定は不要です。

操作手順

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。

2. 受信ユーザーの設定（任意）

ログインユーザーの E メールアドレスを登録しておくことで、Device Manager GUI でタスクを作成する際にメールアドレスが自動的に入力されます。

3. イベン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 認証ユーザーの設定

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。

5. イベント通知のテンプレート編集（任意）

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てください。

関連タスク

- [7.4.1 Device Manager のイベント通知のためのプロパティの設定](#)
- [7.4.2 SMTP 認証ユーザーの設定（hdvmmmodmailuser コマンド）](#)
- [7.4.3 Device Manager のイベント通知テンプレートの編集](#)

関連参照

- [7.2.6 SMTP サーバの設定](#)
- [7.2.7 受信ユーザーの設定](#)

- [付録 A.2.24 server.eventNotification.mail.to](#)

7.4.1 Device Manager のイベント通知のためのプロパティの設定

Device Manager に関するイベントの実行結果が E メールで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.storagesystem`
- `server.mail.from`
- `server.mail.smtp.host`
- `server.mail.smtp.port`
- `server.mail.smtp.auth`
- `server.mail.errorsTo`
- `server.eventNotification.mail.to`

関連参照

- [付録 A.2.17 server.mail.enabled.storagesystem](#)
- [付録 A.2.19 server.mail.from](#)
- [付録 A.2.20 server.mail.smtp.host](#)
- [付録 A.2.21 server.mail.smtp.port](#)
- [付録 A.2.22 server.mail.smtp.auth](#)
- [付録 A.2.23 server.mail.errorsTo](#)
- [付録 A.2.24 server.eventNotification.mail.to](#)

7.4.2 SMTP 認証ユーザーの設定 (hdvmmmodmailuser コマンド)

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。

`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 :

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager
%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 >]
```

Linux の場合 :

```
< Hitachi Command Suite 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。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

7.4.3 Device Manager の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次の場所に格納されています。

Windows の場合：

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager  
%HiCommandServer%config\mail-taskStatusNotification.txt
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ > /HiCommandServer/config/  
mail-taskStatusNotification.txt
```



ヒント

テンプレートファイル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：

```
< Hitachi Command Suite のインストールフォルダ > %DeviceManager%HiCommandServer  
%template%\mail-taskStatusNotification.txt
```

Linux の場合：

テンプレートに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。

テンプレートファイル (mail-taskStatusNotification.txt) の記述例を次に示します。

```

Subject:[$ {productName.short}] $ {taskType} task has finished. (Task : $ {task}, Status : $ {status})
ヘッダー
空行
The following task has finished:
Task : $ { task }
Task Type : $ { taskType }
Status : $ { status }
Description : $ { description }
User : $ { user }
Scheduled Time : $ { scheduledTime }
Completed Time : $ { completedTime }
Message : $ { message }
} パラメーター
(出力有無を変更できる)
This message was sent automatically by the
${productName}.

```

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。



メモ

テンプレートファイルを保存する際に、バイトオーダーマーク (BOM) を付与しないでください。テンプレートファイルに BOM が付与されていると、KAIC18797-E のエラーメッセージが出力され、Eメールの送信に失敗します。

テンプレートに設定できるパラメーターを次に示します。

表 61 タスク終了イベントのパラメーター

パラメーター名	説明	ヘッダー	コンテンツ
task	タスク名	Y	Y
taskType	タスクの種類	Y	Y
status	タスクの状態	Y	Y
description	タスクの説明	--	Y
user	タスク作成者のユーザー ID	--	Y
scheduledTime	タスクの実行要求日時	--	Y
completedTime	タスクの実行終了日時	--	Y
message	エラーメッセージ	--	Y
productName	製品名称	--	Y

パラメーター名	説明	ヘッダー	コンテンツ
productName.short	製品名称 (略称)	Y	Y

(凡例)

Y : 指定できる。

-- : 指定できない。

7.5 Tiered Storage Manager の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せん。

メールで通知できるイベントを次の表に示します。

表 62 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
ロッキングタスク終了	Tiered Storage Manager CLI で作成したロッキ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
アンロッキングタスク終了	Tiered Storage Manager CLI で作成したアンロッキ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
ボリュームロック期限満了	Tiered Storage Manager CLI 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 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 (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方法によって, 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
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通知先のメールアドレスを設定することで, 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。
- Device Manager および Tiered Storage Manager の 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 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。

イベントを E メール通知するためには、次の設定が必要です。アラートを E メール通知するための設定をすでに行っている場合は、1~2 の設定は不要です。

操作手順

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。

2. 受信ユーザーの設定 (任意)

ログインユーザーの E メールアドレスを登録しておく、Device Manager GUI でタスクを作成する際にメールアドレスが自動的に入力されます。

3. イベント通知のプロパティ設定

Device Manager サーバおよび Tiered Storage 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 認証ユーザーの設定

接続時に SMTP 認証を使用する場合は、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。

タスクの種類によって使用するコマンドが異なります。Device Manager GUI で実行したタスクについては、`hdvmodmailuser` コマンドを実行してください。Tiered Storage Manager CLI で実行したタスクについては、`htsmmodmailuser` コマンドを実行してください。

5. イベント通知のテンプレート編集 (任意)

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てください。

関連タスク

- [7.4.2 SMTP 認証ユーザーの設定 \(hdvmodmailuser コマンド\)](#)
- [7.5.1 Tiered Storage Manager のイベント通知のためのプロパティの設定](#)
- [7.5.2 SMTP 認証ユーザーの設定 \(htsmmodmailuser コマンド\)](#)
- [7.5.3 Tiered Storage Manager のイベント通知テンプレートの編集](#)

関連参照

- [7.2.6 SMTP サーバの設定](#)
- [7.2.7 受信ユーザーの設定](#)
- [付録 B.2.9 server.eventNotification.mail.to](#)

7.5.1 Tiered Storage Manager の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.storagesystem`
- `server.mail.from`

- `server.mail.smtp.host`
- `server.mail.smtp.port`
- `server.mail.smtp.auth`
- `server.mail.errorsTo`
- `server.eventNotification.mail.to`



ヒント

Tiered Storage Manager CLI 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`

関連参照

- [付録 A.2.17 server.mail.enabled.storagesystem](#)
- [付録 A.2.19 server.mail.from](#)
- [付録 A.2.20 server.mail.smtp.host](#)
- [付録 A.2.21 server.mail.smtp.port](#)
- [付録 A.2.22 server.mail.smtp.auth](#)
- [付録 A.2.23 server.mail.errorsTo](#)
- [付録 A.2.24 server.eventNotification.mail.to](#)
- [付録 B.2.5 server.mail.from](#)
- [付録 B.2.4 server.mail.smtp.host](#)
- [付録 B.2.7 server.mail.smtp.port](#)
- [付録 B.2.8 server.mail.smtp.auth](#)
- [付録 B.2.6 server.mail.errorsTo](#)
- [付録 B.2.9 server.eventNotification.mail.to](#)
- [付録 B.2.10 server.eventMonitoringIntervalInMinute](#)

7.5.2 SMTP 認証ユーザーの設定 (htsmmodmailuser コマンド)

Tiered Storage Manager CLI で実行したタスクについてイベント通知機能を使用する場合、`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。

`htsmmodmailuser` 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 :
 < *Hitachi Command Suite* のインストールフォルダ > \TieredStorageManager\bin
- Linux の場合 :
 < *Hitachi Command Suite* のインストールディレクトリ > /TieredStorageManager/bin

htsmmodmailuser コマンドの記述形式を次に示します。

形式

```
htsmmodmailuser -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。

- 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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

7.5.3 Tiered Storage Manager の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 63 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	<ul style="list-style-type: none">• [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： < Hitachi Command Suite のインストールフォルダ > ¥DeviceManager ¥HiCommandServer¥config¥mail-migrationtask-end.txt

分類	イベント名	テンプレートファイル名
		<p>Linux の場合 :</p> <p>< Hitachi Command Suite 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 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 :</p> <p>< Hitachi Command Suite のインストールフォルダ > %TieredStorageManager%conf %mail-migrationtask-end.txt</p> <p>Linux の場合 :</p> <p>< Hitachi Command Suite のインストールディレクトリ > / TieredStorageManager / 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 : < Hitachi Command Suite のインストールフォルダ > %TieredStorageManager%conf %mail-shreddingtask-end.txt • Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > / TieredStorageManager / conf / mail-shreddingtask-end.txt
	ロックタスク終了※2	<ul style="list-style-type: none"> • Windows の場合 : < Hitachi Command Suite のインストールフォルダ > %TieredStorageManager%conf %mail-lockingtask-end.txt • Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > / TieredStorageManager / conf / mail-lockingtask-end.txt
	アンロックタスク終了※2	<ul style="list-style-type: none"> • Windows の場合 : < Hitachi Command Suite のインストールフォルダ > %TieredStorageManager%conf %mail-unlockingtask-end.txt • Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > / TieredStorageManager / 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 : < Hitachi Command Suite のインストールフォルダ > %TieredStorageManager%conf %mail-retention-term-expired.txt • Linux の場合 : < Hitachi Command Suite のインストールディレクトリ > / TieredStorageManager / conf / mail-retention-term-expired.txt
	指定期間経過※2	<ul style="list-style-type: none"> • Windows の場合 :

分類	イベント名	テンプレートファイル名
		<p>< <i>Hitachi Command Suite</i> のインストールフォルダ > ¥TieredStorageManager¥conf¥mail-migrationgroup-reminder.txt</p> <ul style="list-style-type: none"> Linux の場合 : < <i>Hitachi Command Suite</i> のインストールディレクトリ > /TieredStorageManager/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 :
< *Hitachi Command Suite* のインストールフォルダ > ¥DeviceManager¥HiCommandServer¥template
- Linux の場合 :
< *Hitachi Command Suite* 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 :
< *Hitachi Command Suite* のインストールフォルダ > ¥TieredStorageManager¥template
- Linux の場合 :
< *Hitachi Command Suite* のインストールディレクトリ > /TieredStorageManager/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。各イベントのパラメーターの詳細については、マニュアル「*Hitachi Command Suite Tiered Storage Manager CLI* リファレンスガイド」を参照してください。

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。



メモ

- テンプレートファイルファイルを保存する際に、バイトオーダーマーク（BOM）を付与しないでください。テンプレートファイルにBOMが付与されていると、KAIC18797-Eのエラーメッセージが出力され、Eメールの送信に失敗します。
- 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次に示します。

表 64 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ー 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

パラメーター名	説明
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 65 タスク終了イベントのパラメーター (Tiered Storage Manager CLI 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
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 66 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

パラメーター名	説明
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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

7.6 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 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 (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。

7.6.1 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。

操作手順

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 (ntevent.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%ntevent.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、ntevent.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、ntevent.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。

7.6.2 管理サーバが Red Hat Enterprise Linux の場合

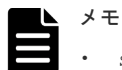
管理サーバが Red Hat Enterprise Linux の場合のセットアップ手順は次のとおりです。各製品での手順の詳細については、JP1/IM および JP1/Base のマニュアルを参照してください。

操作手順

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



- syslog ファイルのデフォルトは、/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せんが、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

```
FILETYPE =SEQ2
ACTDEF =<Error>0 "KAID.*-E"
ACTDEF =<Warning>0 "KAID.*-W"
ACTDEF =<Information>0 "KAID.*-I"
```

- Tiered Storage Manager の場合

```
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。
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>
```



- 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。

- 8.1 CIM/WBEM とは
- 8.2 Device Manager の CIM/WBEM 機能
- 8.3 ネームスペースの指定方法
- 8.4 CIM/WBEM 機能を使用するためのユーザーアカウント
- 8.5 CIM/WBEM 機能を利用するための設定をする
- 8.6 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
- 8.7 SLP サービスの制御

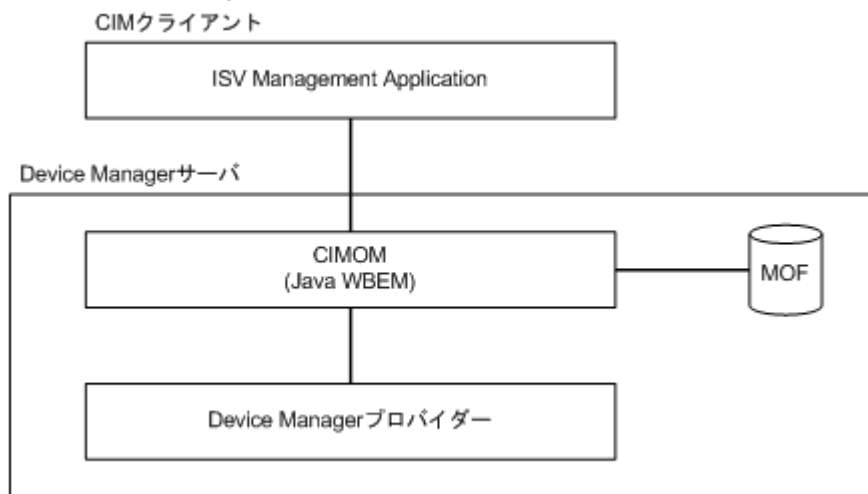
8.1 CIM/WBEM とは

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 57 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/>

8.2 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のある機能は、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

8.3 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。

表 67 ネームスペースおよび SMI-S のバージョンの対応

ネームスペース			SMI-S のバージョン
<code>smisxx</code>	<code>current</code>	<code>interop</code>	
<code>smis11</code>	-	-	1.1.0
<code>smis12</code>	-	-	1.2.0
<code>smis13</code>	-	-	1.3.0
<code>smis14</code>	-	-	1.4.0
<code>smis15</code>	<code>current</code>	<code>interop</code>	1.5.0

(凡例) - : 該当なし

8.4 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 68 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	
	サービスマソッド	CIM オペレーション
Admin または Modify	Y	Y
View または Peer	--	Y

(凡例)

Y : CIM メソッドを実行できる

-- : CIM メソッドを実行できない

8.5 CIM/WBEM 機能を利用するための設定をする

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。

前提条件

- Administrator 権限 (Windows の場合) または root (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。
- SLP サービスまたは SLP デーモンの起動（サービスディスカバリー機能を使用する場合）
- 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。

操作手順

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. **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 USP00 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。
3. **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。

関連概念

- [8.7 SLP サービスの制御](#)

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [2.1.2 Device Manager サーバで使用されるポート](#)
- [付録 A.2.10 server.cim.support](#)
- [付録 A.2.16 server.logicalview.initialsynchro](#)

8.5.1 CIM/WBEM 機能で使用するポートを変更する

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。

前提条件

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

操作手順

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。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [付録 A.2.13 server.cim.http.port](#)
- [付録 A.2.14 server.cim.https.port](#)
- [付録 A.8.8 Ciphers](#)
- [付録 A.17.2 HTTPPort](#)
- [付録 A.17.3 HTTPSPort](#)

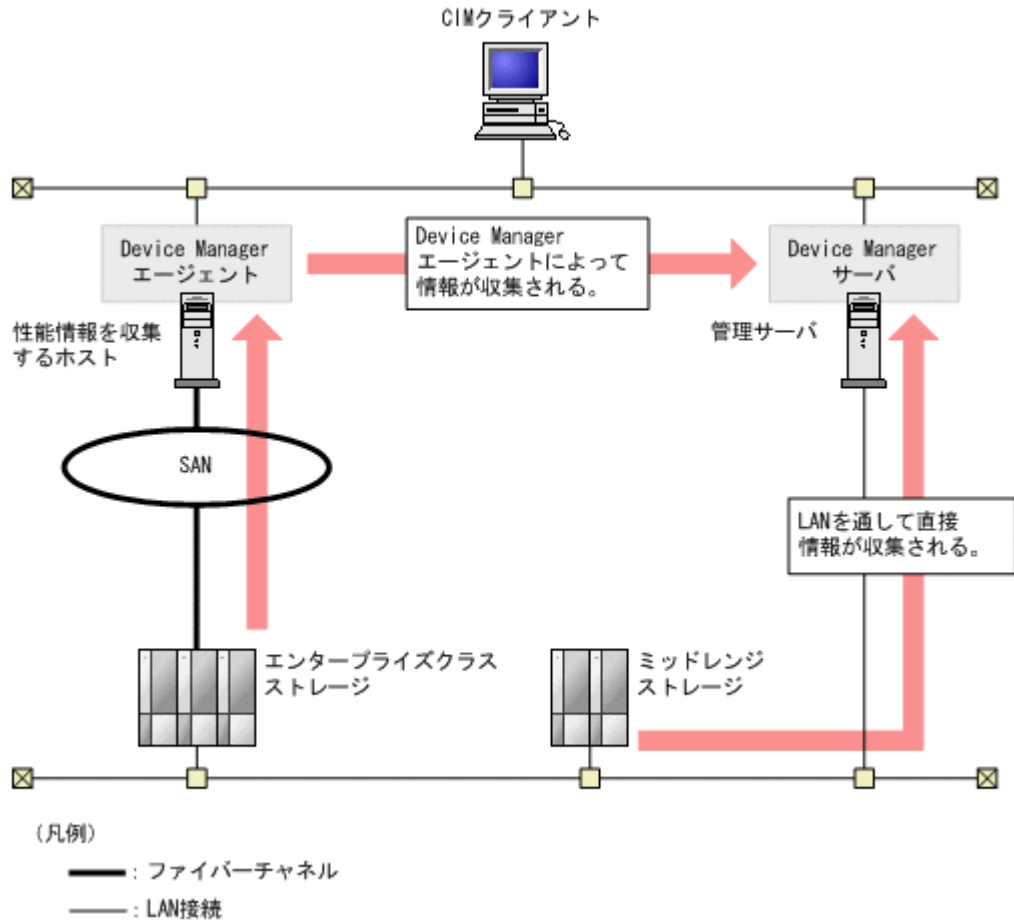
8.6 CIM/WBEM 機能でストレージシステムの性能情報を取得するための設定

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。

8.6.1 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 58 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。

Virtual Storage Platform, Universal Storage Platform V/V M 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 または Hitachi AMS/WMS) 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

Virtual Storage Platform, Universal Storage Platform V/V M 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/V M 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。

8.6.2 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をする

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。

前提条件

Administrator 権限または root 権限のユーザーでのログイン

操作手順

1. 性能情報を収集する対象となる各ストレージシステムにコマンドデバイスを用意します。
2. 性能情報を収集するホストにコマンドデバイスを割り当てて、ホストに認識させます。

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。

3. 性能情報を収集するホストに Device Manager エージェントおよび RAID Manager LIB をインストールします。

Device Manager エージェントのインストール方法については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。

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 69 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

4. 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)。
5. `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。

6. 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。

関連タスク

- 付録 A.1.1 Device Manager サーバのプロパティの変更

関連参照

- 8.6.3 コマンドデバイスを登録するためのコマンド (perf_findcmddev) の形式
- 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 RAID Manager XP の情報の設定 (hdvmagt_setting コマンド)
- 付録 A.2.9 server.cim.agent

8.6.3 コマンドデバイスを登録するためのコマンド (perf_findcmddev) の形式

Device Manager エージェントでコマンドデバイスを登録したり、コマンドデバイスの情報を表示したりするコマンド (perf_findcmddev) の形式を示します。

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

Linux の場合 :

< Device Manager エージェントのインストールディレクトリ > /bin

Solaris の場合 :

/opt/HDVM/HBaseAgent/bin

オプション

```
write [-file <ファイル名>]
```

コマンドデバイスを登録する場合に指定します。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
R600 14050 0 345 ¥¥.¥PhysicalDrive3
R601 44332 1 456 ¥¥.¥Volume{xxxxxxxx-xxxx-xxx-xxxxxxxx}
R600 UNKNOWN - 1045 ¥¥.¥PhysicalDrive10
```

関連参照

- [8.6.4 perf_cmddev.properties ファイルの形式](#)

8.6.4 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

Linux の場合：

< Device Manager エージェントのインストールディレクトリ > /mod/hdvm/config

Solaris 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 70 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 : ¥¥.¥PhysicalDrivex ¥¥.¥Volume{ < GUID > }

設定項目	設定内容
	<ul style="list-style-type: none"> • Solaris の場合 : /dev/rdisk/cxtxs2 • 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、Universal Storage Platform V (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。

```
R700.44332.456: ¥¥.¥PhysicalDrive3
R600.14050.345: ¥¥.¥PhysicalDrive5
R600.14050.346: ¥¥.¥PhysicalDrive6
R600.14050.347: ¥¥.¥PhysicalDrive10
R601.89832.780: ¥¥.¥PhysicalDrive15
```

8.6.5 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をする

ミッドレンジストレージ (HUS100, Hitachi AMS2000, Hitachi SMS または Hitachi AMS/WMS) の性能情報を取得するための設定について説明します。

操作手順

1. 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をします。
性能統計情報採取の設定方法については、各ストレージシステムのマニュアルを参照してください。
2. ストレージシステムで Account Authentication が有効になっている場合、参照権限だけを持つ情報収集用のユーザーアカウントを作成します。
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場合があります。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。
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。
3. hdvmmmodpolluser コマンドを実行して、Device Manager に性能情報取得用のユーザーアカウントを登録します。

関連参照

- 8.6.6 性能情報を取得するユーザーアカウントを登録するためのコマンド (hdvmmmodpolluser) の形式

8.6.6 性能情報を取得するユーザーアカウントを登録するためのコマンド (hdvmmmodpolluser) の形式

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ためのコマンド (hdvmmmodpolluser) の形式を示します。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 hdvmmmodpolluser 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。

コマンドの形式

Windows の場合 :

```
hdvmmmodpolluser { -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 :

```
< Hitachi Command Suite のインストールフォルダ > ¥DeviceManager  
¥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。

8.7 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。

8.7.1 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

Device Manager でサービスディスカバリー機能を使用するには、前提ソフトウェアが必要です。

表 71 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

OS	前提ソフトウェア	備考
Windows Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6	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。
Red Hat Enterprise Linux 7 Oracle Linux 7	OpenSLP 2.0.0	OpenSLP は、各 OS に付属します。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。

8.7.2 SLP サービスを起動する (Windows)

Windows メニューまたは `slpd` コマンドを使用して、SLP サービスを起動します。

前提条件

Administrator 権限でのログイン

操作手順

- 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
```

8.7.3 SLP サービスを停止する (Windows)

Windows メニューまたは `slpd` コマンドを使用して、SLP サービスを停止します。

前提条件

Administrator 権限でのログイン

操作手順

- 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
```

8.7.4 SLP デーモンを起動する (Red Hat Enterprise Linux または Oracle Linux)

slpd コマンドまたは systemctl コマンドを使用して、SLP デーモンを起動します。

前提条件

root 権限でのログイン

操作手順

1. 次のコマンドを実行してください。

Red Hat Enterprise Linux 5 または Red Hat Enterprise Linux 6 の場合

```
<Hitachi Command Suite のインストールディレクトリ>/  
HiCommandServer/wsi/bin/slpd.sh start
```

Red Hat Enterprise Linux 7 または Oracle Linux 7 の場合

```
# systemctl start slpd.service
```

8.7.5 SLP デーモンを停止する (Red Hat Enterprise Linux または Oracle Linux)

slpd コマンドまたは systemctl コマンドを使用して、SLP デーモンを停止します。

前提条件

root 権限でのログイン

操作手順

1. 次のコマンドを実行してください。

Red Hat Enterprise Linux 5 または Red Hat Enterprise Linux 6 の場合

```
<Hitachi Command Suite のインストールディレクトリ>/  
HiCommandServer/wsi/bin/slpd.sh stop
```

Red Hat Enterprise Linux 7 または Oracle Linux 7 の場合

```
# systemctl stop slpd.service
```

8.7.6 SLP サービスを解除する (Windows)

Hitachi Command Suite 製品のアンインストール時、SLP サービス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。
```

前提条件

Administrator 権限でのログイン

操作手順

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
```

8.7.7 SLP デーモンを解除する (Linux)

Hitachi Command Suite 製品のアンインストール時、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 デーモン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。

前提条件

root 権限でのログイン

操作手順

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
```

8.7.8 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 :

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/wsi/cfg/  
slp.log
```

サービスの起動と停止

この章では、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 のサービスの起動と停止
- 9.2 Host Data Collector のサービスの起動と停止
- 9.3 クラスタ管理アプリケーションに登録されている Hitachi Command Suite 製品のサービス

9.1 Hitachi Command Suite のサービスの起動と停止

ここでは、Device Manager、Tiered Storage Manager および Replication Manager 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。

9.1.1 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 72 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 cjstartsv.exe	HBase 64 Storage Mgmt SSO Service	シングルサインオン用の Hitachi Command Suite J2EE サービス
httpsd.exe rotatelog.exe	HBase 64 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 rotatelog.exe	HBase 64 Storage Mgmt Web SSO Service	シングルサインオン用の Hitachi Command Suite 共通 Web サービス
hcmdssvctl.exe cjstartsv.exe	HCS Device Manager Web Service	Device Manager の J2EE サービス
hntr2mon.exe hntr2srv.exe	Hitachi Network Objectplaza Trace Monitor 2 Hitachi Network Objectplaza Trace Monitor 2 (x64)	Hitachi Command Suite 共通トレースログ採取 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*	HiRDB/ EmbeddedEdition _HD1	HiRDB のプロセスサーバの制御

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。

表 73 常駐プロセス (Linux の場合)

プロセス名	機能
htsmService	Tiered Storage Manager サーバ
hicmdserver	Device Manager サーバ < Hitachi Command Suite のインストールディレクトリ > / HiCommandServer/hicmdserver

プロセス名	機能
hcs_hssso cjstartsv	シングルサインオン用の Hitachi Command Suite J2EE サービス < Hitachi Command Suite のインストールディレクトリ > /Base64/ uCPsb/CC/web/containers/HBase64StgMgmtSSOService/ hcs_hssso < Hitachi Command Suite のインストールディレクトリ > /Base64/ uCPsb/CC/web/bin/cjstartweb
httpsd rotatelog	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。 < Hitachi Command Suite のインストールディレクトリ > /Base64/ uCPsb/httpsd/sbin/httpsd < Hitachi Command Suite のインストールディレクトリ > /Base64/ uCPsb/httpsd/sbin/rotatelog
httpsd rotatelog	シングルサインオン用の Hitachi Command Suite 共通 Web サービス < Hitachi Command Suite のインストールディレクトリ > /Base64/ uCPsb/httpsd/sbin/httpsd < Hitachi Command Suite のインストールディレクトリ > /Base64/ uCPsb/httpsd/sbin/rotatelog
hcs_dm cjstartsv	Device Manager の J2EE サービス /bin/sh < Hitachi Command Suite のインストールディレクトリ > / Base64/uCPsb/CC/server/repository/ DeviceManagerWebService/hcs_dm < Hitachi Command Suite のインストールディレクトリ > /Base64/ uCPsb/CC/server/bin/cjstartsv
/opt/hitachi/ HNTRLib2/bin/hntr2mon	Hitachi Command Suite 共通トレースログ採取
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。

関連概念

- [9.2.1 Host Data Collector の常駐プロセス](#)

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)
- [9.1.4 Hitachi Command Suite のサービスの稼働状態の確認](#)

9.1.2 Hitachi Command Suite のサービスの起動

Windows メニューまたは hcmds64srv コマンドを使って、Hitachi Command Suite のサービスを起動します。

前提条件

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

操作手順

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 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 または Windows Server 2012 R2 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 のインストールフォルダ > %Base64%\bin\hcmds64srv /start
```

Linux の場合 :

次のコマンドを実行します。

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/hcmdssrv -start
```



メモ

Hitachi File Services Manager や 32bit 版 Storage Navigator Modular 2 と連携している場合、コマンドを実行して Hitachi Command Suite 製品のサービスを起動するときは、次のコマンドも実行してください。

- Windows の場合 :

```
< Hitachi File Services Manager または Storage Navigator Modular 2 のインストールフォルダ > %Base%\bin\hcmdssrv /start
```

- Linux の場合 :

```
< Hitachi File Services Manager または Storage Navigator Modular 2 のインストールディレクトリ > /Base/bin/hcmdssrv -start
```



ヒント

Hitachi Command Suite 製品のサービスを起動しても、32bit 版 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
```

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
```

操作結果

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 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt Web SSO Service
- 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

9.1.3 Hitachi Command Suite のサービスの停止

Windows メニューまたは `hcmds64srv` コマンドを使って、Hitachi Command Suite のサービスを停止します。

前提条件

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

操作手順

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 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 または Windows Server 2012 R2 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 のインストールフォルダ > %Base64%\bin\hcmds64srv /
stop
```

Linux の場合 :

次のコマンドを実行します。

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/hcmd64srv
-stop
```



注意

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。



メモ

Hitachi File Services Manager や 32bit 版 Storage Navigator Modular 2 と連携している場合、コマンドを実行して Hitachi Command Suite 製品のサービスを停止するときは、次のコマンドも実行してください。

- Windows の場合 :

<Hitachi File Services Manager または Storage Navigator Modular 2 のインストールフォルダ>%Base%\bin\hcmdssrv /stop

- Linux の場合 :

<Hitachi File Services Manager または Storage Navigator Modular 2 のインストールディレクトリ>/Base/bin/hcmdssrv -stop



ヒント

Hitachi Command Suite 製品のサービスを停止しても、32bit 版 Storage Navigator Modular 2 のサービスは停止しません。

32bit 版 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
```

- 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
```

操作結果

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 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt Web SSO Service
- 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

9.1.4 Hitachi Command Suite のサービスの稼働状態の確認

Windows メニューまたは hcmds64srv コマンドを使って、各 Hitachi Command Suite のサービスの稼働状態を確認します。

前提条件

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

操作手順

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 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 または Windows Server 2012 R2 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 のインストールフォルダ > %Base64%\bin\hcmds64srv /  
statusall
```

Linux の場合 :

次のコマンドを実行します。

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/hcmd64srv  
-statusall
```

操作結果

各サービスの稼働状態が画面に表示されます。

9.2 Host Data Collector のサービスの起動と停止

ここでは、Host Data Collector 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。

9.2.1 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 74 Host Data Collector の常駐プロセス \(Windows\)](#)」から「[表 75 Host Data Collector の常駐プロセス \(Linux\)](#)」に示します。

表 74 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 HdcAdapter.exe* HdcRMI.exe HdcService.exe	Host Data Collector Base Service	Host Data Collector のサービス

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。

表 75 Host Data Collector の常駐プロセス (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

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/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) ※
< 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。



メモ

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。

関連概念

- [9.1.1 Hitachi Command Suite の常駐プロセス](#)

関連参照

- [付録 C.2.2 hdc.adapter.adapterProcessNum](#)

9.2.2 Host Data Collector のサービスの起動

controlservice コマンドを使って、Host Data Collector のサービスを起動します。

前提条件

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

操作手順

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
```

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
```

関連概念

- [9.2.1 Host Data Collector の常駐プロセス](#)

関連タスク

- [9.2.3 Host Data Collector のサービスの停止](#)
- [9.2.4 Host Data Collector のサービスの稼働状態の確認](#)

9.2.3 Host Data Collector のサービスの停止

`controlservice` コマンドを使って、Host Data Collector のサービスを停止します。

前提条件

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

操作手順

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
```

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
```

関連概念

- [9.2.1 Host Data Collector の常駐プロセス](#)

関連タスク

- [9.2.2 Host Data Collector のサービスの起動](#)
- [9.2.4 Host Data Collector のサービスの稼働状態の確認](#)

9.2.4 Host Data Collector のサービスの稼働状態の確認

`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。

前提条件

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

操作手順

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
```

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
```

関連概念

- [9.2.1 Host Data Collector の常駐プロセス](#)

関連タスク

- [9.2.2 Host Data Collector のサービスの起動](#)
- [9.2.3 Host Data Collector のサービスの停止](#)

9.3 クラスタ管理アプリケーションに登録されている Hitachi Command Suite 製品のサービス

ここでは、hcmds64clustersrvstate コマンドが対象としている Hitachi Command Suite 製品のサービスについて説明します。

Windows のクラスタ環境で、Tuning Manager サーバとリモート接続する場合やデータベースをバックアップする場合などに、次の表に示すサービスを一括でオンラインまたはオフラインにします。

表 76 管理サーバでクラスタ管理アプリケーションに登録されている Hitachi Command Suite 製品のサービス

製品名	サービス表示名	サービス名	備考
Hitachi Command Suite 共通コンポーネント	HiRDB/ClusterService_HD1	HiRDBClusterService_HD1	-
	HBase 64 Storage Mgmt Web Service	HBase64StgMgmtWebService	-
	HBase 64 Storage Mgmt Web SSO Service	HBase64StgMgmtWebSSOService	-
	HBase 64 Storage Mgmt SSO Service	HBase64StgMgmtSSOService	-
Device Manager	HCS Device Manager Web Service	DeviceManagerWebService64	-
	HiCommandServer	HiCommandServer	-
	HiCommand Tiered Storage Manager	HiCommandTieredStorageManager	-
Tuning Manager サーバ	HCS Tuning Manager REST Application Service	TuningManagerRESTService	-
	HiCommand Performance Reporter	PerformanceReporter64	-
	HiCommand Suite TuningManager	HiCommandTuningManager64	-
Compute Systems Manager	HCS Compute Systems Manager Web Service	ComputeSystemsManagerWebService64	-
	DeploymentManager PXE Management	PxeSvc	デプロイメントマネージャーをインストールしている場合に使用するサービスです。
	DeploymentManager PXE Mtftp	PxeMtftp	デプロイメントマネージャーをインストールしている場合に使用するサービスです。

製品名	サービス表示名	サービス名	備考
	DeploymentManager Transfer Management	ftsvc	デプロイメン トマネージャ ーをインスト ールしている 場合に使用す るサービスで す。

(凡例)

- : 該当なし

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 77 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のマシンで、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"> インポート先のマシンに、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 インポート先の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：

$$(\text{バックアップ対象となる Hitachi Command Suite 製品のデータベースサイズの総和} + 4.6\text{GB}) \times 2$$

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。



メモ

バックアップソフトウェアで Hitachi Command Suite 製品が使用するデータベース関連のファイルにアクセスすると、I/O 遅延やファイル排他などで障害が発生することがあります。

バックアップソフトウェアで Hitachi Command Suite のインストールディレクトリを含めてバックアップしたい場合は、Hitachi Command Suite 製品のすべてのサービスを停止したあとに、バックアップしてください。

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。

操作手順

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. hcmds64backups 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 のインストールフォルダ>%Base64%bin  
%hcmd64backups /dir <バックアップファイルの格納先フォルダ> /auto
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/  
hcmd64backups -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。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。

hcmd64backups 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。



メモ

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せん。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。



メモ

hcms64backups コマンドに続けて、以下のいずれかのコマンドを実行する場合、hcms64backups コマンドに auto オプションは指定しないでください。

- hcms64dbtrans
- hcms64srv /stop または hcms64srv -stop
- hcms64db
- hcms64backups

hcms64backups コマンドに auto オプションを指定しないときは、hcms64backups コマンドを実行する前に、以下のコマンドを順に実行してください。また、すべての作業が終了後、hcms64srv /start コマンドまたは hcms64srv -start 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。

Windows の場合：

1. <Hitachi Command Suite のインストールフォルダ>%Base64%\bin\hcms64srv /stop
2. <Hitachi Command Suite のインストールフォルダ>%Base64%\bin\hcms64dbsrv /start

Linux の場合：

1. <Hitachi Command Suite のインストールディレクトリ>/Base64/bin/hcms64srv -stop
2. <Hitachi Command Suite のインストールディレクトリ>/Base64/bin/hcms64dbsrv -start

10.2.2 データベースのバックアップ（Windows のクラスタ構成の場合）

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。

前提条件

Administrator 権限でのログイン

操作手順

1. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスをオフラインにします。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%\ClusterSetup\hcms64clustersrvstate /soff /r <リソースグループ名>
```

soff

クラスタ管理アプリケーションのリソースグループに登録された Hitachi Command Suite 製品のサービスをオフラインにして、フェールオーバーを抑制するためのオプション

ンです。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。

r

リソースグループ名を指定します。

2. hcmds64backups 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 のインストールフォルダ>%Base64%bin  
%hcmds64backups /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。

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。

hcmds64backups 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。

3. hcmds64srv /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 hcmds64srv /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. 次のコマンドを実行して、リソースグループおよび Hitachi Command Suite 製品のサービスをオンラインにします。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%ClusterSetup  
%hcmds64clustersrvstate /son /r <リソースグループ名>
```

son

クラスタ管理アプリケーションに設定されたリソースグループをオンラインにして、フェールオーバーを有効にするためのオプションです。

r

リソースグループ名を指定します。



メモ

hcmds64backups コマンドに続けて、以下のいずれかのコマンドを実行する場合、hcmds64backups コマンドに auto オプションは指定しないでください。

- hcmds64dbtrans
- hcmds64srv /stop または hcmds64srv -stop
- hcmds64db
- hcmds64backups

hcmds64backups コマンドに auto オプションを指定しないときは、hcmds64backups コマンドを実行する前に、以下のコマンドを順に実行してください。また、すべての作業が終了後、hcmds64srv /start 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。

```
1. <Hitachi Command Suite のインストールフォルダ>%Base64%bin%hcmds64srv /  
stop
```

2. <Hitachi Command Suite のインストールフォルダ>/Base64/bin/hcmds64dsrv /
start

関連タスク

- [9.1.3 Hitachi Command Suite のサービスの停止](#)
- [9.1.4 Hitachi Command Suite のサービスの稼働状態の確認](#)

関連参照

- [9.3 クラスタ管理アプリケーションに登録されている Hitachi Command Suite 製品のサービス](#)

10.2.3 データベースのバックアップ（Red Hat Enterprise Linux のクラスタ構成の場合）

管理サーバの OS が Red Hat Enterprise Linux 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。

前提条件

- root 権限でのログイン
- 次の情報の確認
 - サービスグループに登録するために作成したスクリプトのファイル名
Hitachi Command Suite 製品のサービスをサービスグループに登録する方法については、マニュアル「*Hitachi Command Suite* インストールガイド」を参照してください。

操作手順

1. Hitachi Command Suite 製品のサービスをサービスグループから削除します。
詳細については、マニュアル「*Hitachi Command Suite* インストールガイド」を参照してください。
2. 実行系ノードにサービスグループが移動している事を確認します。
移動していない場合は、実行系ノードにサービスグループを移動してください。
3. hcmds64srv -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ます。
4. hcmds64backups 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 のインストールディレクトリ>/Base64/bin/hcmds64backups  
-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。

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。

hcmds64backups 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。

5. hcmds64srv -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 hcmds64srv -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。

6. 手順 1 で削除した Hitachi Command Suite 製品のサービスを、再度サービスグループに登録します。
7. Hitachi Command Suite 製品のサービスを登録したサービスグループを起動します。
詳細については、マニュアル「*Hitachi Command Suite* インストールガイド」を参照してください。



メモ

hcmds64backups コマンドに続けて、以下のいずれかのコマンドを実行する場合、hcmds64backups コマンドに auto オプションは指定しないでください。

- hcmds64dbtrans
- hcmds64srv -stop
- hcmds64db
- hcmds64backups

hcmds64backups コマンドに auto オプションを指定しないときは、hcmds64backups コマンドを実行する前に、以下のコマンドを順に実行してください。また、すべての作業が終了後、hcmds64srv -start 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。

1. <Hitachi Command Suite のインストールディレクトリ>/Base64/bin/hcmds64srv -stop
2. <Hitachi Command Suite のインストールディレクトリ>/Base64/bin/hcmds64dsrv -start

関連タスク

- [9.1.3 Hitachi Command Suite のサービスの停止](#)
- [9.1.4 Hitachi Command Suite のサービスの稼働状態の確認](#)

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
hcmds64backups 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、復元できません。
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
 hcmds64dbtrans 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、復元できません。
 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。
 hcmds64dbrepair 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（非クラスタ構成の場合）

管理サーバ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。



注意

- 手順の途中で使用する hcmds64db 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。
 - hcmds64db 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。
 Tuning Manager とリモート接続していて、Tuning Manager のアラート機能を使用していた場合は、データベースの復元後、アラート定義情報を同期する必要があります。アラート定義情報の同期については、マニュアル「Hitachi Command Suite Tuning Manager API リファレンスガイド」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。

操作手順

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. hcmds64db 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 のインストールフォルダ >%Base64%\bin\hcmd64db /
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
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ >%Base64%/bin/hcmd64db
-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
```


hcmds64backups 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。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 78 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
その他の製品	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 の副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、正サイトの Replication Manager と副サイトの 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。
- 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。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)

関連参照

- [6.2.8 Tuning Manager サーバとのリモート接続およびポート番号の設定 \(htmsetup コマンド\)](#)

10.3.2 データベース不整合時のデータベースの復元（Windows のクラスタ構成の場合）

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。
- 手順の途中で使用する hcmds64db 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。
 - hcmds64db 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。

Tuning Manager とリモート接続していて、Tuning Manager のアラート機能を使用していた場合は、データベースの復元後、アラート定義情報を同期する必要があります。アラート定義情報の同期については、マニュアル「*Hitachi Command Suite Tuning Manager API リファレンスガイド*」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。

前提条件

Administrator 権限でのログイン

操作手順

1. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスをオフラインにします。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%ClusterSetup  
%hcmds64clustersrvstate /soff /r <リソースグループ名>
```

```
soff
```

クラスタ管理アプリケーションのリソースグループに登録された Hitachi Command Suite 製品のサービスをオフラインにして、フェールオーバーを抑制するためのオプションです。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。

```
r
```

リソースグループ名を指定します。

2. hcmds64db コマンドを実行してデータベースを復元します。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%bin%hcmds64db /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

hcmds64backups 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 79 データベースを復元する場合の type オプションの指定値 (Windows の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

- 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。
- 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。
- 次のコマンドを実行して、リソースグループおよび Hitachi Command Suite 製品のサービスをオンラインにします。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%ClusterSetup  
%hcmds64clustersrvstate /son /r <リソースグループ名>
```

son

クラスタ管理アプリケーションに設定されたリソースグループをオンラインにして、フェールオーバーを有効にするためのオプションです。

r

リソースグループ名を指定します。

- 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。
- 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。
- 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 の副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、正サイトの Replication Manager と副サイトの 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。

12. 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。

13. 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。
14. 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。

関連タスク

- [6.2.7 Tuning Manager サーバとのリモート接続 \(Windows のクラスタ環境\)](#)

関連参照

- [9.3 クラスタ管理アプリケーションに登録されている Hitachi Command Suite 製品のサービス](#)

10.3.3 データベース不整合時のデータベースの復元 (Red Hat Enterprise Linux のクラスタ構成の場合)

管理サーバの OS が Red Hat Enterprise Linux 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。
- 手順の途中で使用する hcmds64db 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。
 - hcmds64db 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。
- 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。

前提条件

- root 権限でのログイン
- 次の情報の確認
 - サービスグループに登録するために作成したスクリプトのファイル名
Hitachi Command Suite 製品のサービスをサービスグループに登録する方法については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。

操作手順

1. Hitachi Command Suite 製品のサービスをサービスグループから削除します。
詳細については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。
2. 実行系ノードにサービスグループが移動している事を確認します。
移動していない場合は、実行系ノードにサービスグループを移動してください。
3. hcmds64db コマンドを実行してデータベースを復元します。

<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/hcmds64db -
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

hcmds64backups 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 80 データベースを復元する場合の type オプションの指定値 (Red Hat Enterprise
Linux の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

4. 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。
5. 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。
6. Hitachi Command Suite 製品のサービスを起動します。
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 プロパティを false に戻します。
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 プロパティを false に戻します。
9. Hitachi Command Suite 製品のサービスを再起動します。
10. 手順 1 で削除した Hitachi Command Suite 製品のサービスを、再度サービスグループに登録し
ます。
11. Hitachi Command Suite 製品のサービスを登録したサービスグループを起動します。
詳細については、マニュアル「Hitachi Command Suite インストールガイド」を参照してくだ
さい。
12. 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。
13. Replication Manager の副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、正サイトの Replication Manager
と副サイトの Device Manager のデータベースを同期させます。
14. 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。
15. 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。

16. 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。
17. 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。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

10.3.4 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。



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。
Tuning Manager とリモート接続していて、Tuning Manager のアラート機能を使用していた場合は、データベースの復元後、アラート定義情報を同期する必要があります。アラート定義情報の同期については、マニュアル「*Hitachi Command Suite Tuning Manager API リファレンスガイド*」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。

操作手順

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. hcnds64dbrepair 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 のインストールフォルダ > %Base64%bin  
%hcnds64dbrepair /trans <エクスポートファイル >
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/  
hcnds64dbrepair -trans <エクスポートファイル >
```

trans

hcnds64dbtrans 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。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 の副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、正サイトの Replication Manager と副サイトの 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。
System アカウントのパスワードの変更方法については、マニュアル「*Hitachi Command Suite ユーザーズガイド*」を参照してください。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [6.2.8 Tuning Manager サーバとのリモート接続およびポート番号の設定 \(htmsetup コマンド\)](#)

10.3.5 データベース破損時のデータベースの復元 (Windows のクラスタ構成の場合)

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。
- 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。

Tuning Manager とリモート接続して、Tuning Manager のアラート機能を使用していた場合は、データベースの復元後、アラート定義情報を同期する必要があります。アラート定義情報の同期については、マニュアル「*Hitachi Command Suite Tuning Manager API リファレンスガイド*」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。

前提条件

Administrator 権限でのログイン

操作手順

1. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスをオフラインにします。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%ClusterSetup  
%hcnds64clustersrvstate /soff /r <リソースグループ名>
```

soff

クラスタ管理アプリケーションのリソースグループに登録された Hitachi Command Suite 製品のサービスをオフラインにして、フェールオーバーを抑制するためのオプションです。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。

r

リソースグループ名を指定します。

2. hcnds64dbrepair コマンドを実行してデータベースを復元します。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%bin%hcnds64dbrepair /  
trans <エクスポートファイル>
```

trans

hcnds64dbtrans 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。

3. 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。
4. 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。
5. 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、リソースグループおよび Hitachi Command Suite 製品のサービスをオンラインにします。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%ClusterSetup  
%hcnds64clustersrvstate /son /r <リソースグループ名>
```

son

クラスタ管理アプリケーションに設定されたリソースグループをオンラインにして、フェールオーバーを有効にするためのオプションです。

r

リソースグループ名を指定します。

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 プロパティを false に戻します。
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 プロパティを false に戻します。
9. 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。

10. Replication Manager の副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、正サイトの Replication Manager と副サイトの Device Manager のデータベースを同期させます。
11. 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。
12. 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。
13. 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。
14. 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。
15. 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。
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。
System アカウントのパスワードの変更方法については、マニュアル「Hitachi Command Suite ユーザーズガイド」を参照してください。

関連タスク

- [6.2.7 Tuning Manager サーバとのリモート接続 \(Windows のクラスタ環境\)](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [9.3 クラスタ管理アプリケーションに登録されている Hitachi Command Suite 製品のサービス](#)

10.3.6 データベース破損時のデータベースの復元 (Red Hat Enterprise Linux のクラスタ構成の場合)

管理サーバの OS が Red Hat Enterprise Linux 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。
- 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。

前提条件

- root 権限でのログイン
 - 次の情報の確認
 - サービスグループに登録するために作成したスクリプトのファイル名
- Hitachi Command Suite 製品のサービスをサービスグループに登録する方法については、マニュアル「Hitachi Command Suite インストールガイド」を参照してください。

操作手順

1. Hitachi Command Suite 製品のサービスをサービスグループから削除します。
詳細については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。
2. 実行系ノードにサービスグループが移動している事を確認します。
移動していない場合は、実行系ノードにサービスグループを移動してください。
3. hcmds64dbrepair コマンドを実行してデータベースを復元します。

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/  
hcmds64dbrepair -trans <エクスポートファイル>  
  
trans  
  
hcmds64dbtrans 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。
```
4. 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。
5. 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。
6. Hitachi Command Suite 製品のサービスを起動します。
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 プロパティを false に戻します。
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 プロパティを false に戻します。
9. Hitachi Command Suite 製品のサービスを再起動します。
10. 手順 1 で削除した Hitachi Command Suite 製品のサービスを、再度サービスグループに登録し
ます。
11. Hitachi Command Suite 製品のサービスを登録したサービスグループを起動します。
詳細については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してくだ
さい。
12. 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。
13. Replication Manager の副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、正サイトの Replication Manager
と副サイトの Device Manager のデータベースを同期させます。
14. 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。
15. 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。
16. 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。
17. 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。
18. 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。
System アカウントのパスワードの変更方法については、マニュアル「*Hitachi Command Suite
ユーザーズガイド*」を参照してください。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

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、`hcmds64dbtrans` コマンドを使用してデータベースを移行できます。`hcmds64dbtrans` 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。

`hcmds64dbtrans` 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



メモ

[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 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。

操作手順

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. hcmds64dbtrans 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. hcmds64dbtrans 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 移行元サーバでデータベースをエクスポートする(非クラスタ構成の場合)

管理サーバ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。

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。アーカイブファイルの作成先のディスク容量が不足している場合、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手動で移行先に転送してください。
- 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。

操作手順

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. hcmds64dbtrans 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 のインストールフォルダ > %Base64%bin  
%hcmds64dbtrans /export /workpath <作業用フォルダ> /file <アーカイブフ  
ファイル> /auto
```

Linux の場合 :

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/  
hcmds64dbtrans -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。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。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。

3. 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。



メモ

hcmts64dbtrans コマンドに続けて、以下のコマンドを実行する場合、hcmts64dbtrans コマンドに auto オプションは指定しないでください。

- hcmts64dbtrans
- hcmts64srv /stop または hcmts64srv -stop
- hcmts64db
- hcmts64backups

hcmts64dbtrans コマンドに auto オプションを指定しないときは、hcmts64dbtrans コマンドを実行する前に、以下のコマンドを順に実行してください。また、すべての作業が終了後、hcmts64srv /start コマンドまたは hcmts64srv -start 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。

Windows の場合：

1. <Hitachi Command Suite のインストールフォルダ>%Base64%\bin\hcmts64srv /stop

2. <Hitachi Command Suite のインストールフォルダ>%Base64%\bin\hcmts64bsrv /start

Linux の場合：

1. <Hitachi Command Suite のインストールディレクトリ>/Base64/bin/hcmts64srv -stop

2. <Hitachi Command Suite のインストールディレクトリ>/Base64/bin/hcmts64bsrv -start

10.4.5 移行元サーバでデータベースをエクスポートする (Windows のクラスタ構成の場合)

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。

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

- 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。
- データベースはアーカイブファイルとしてエクスポートされます。アーカイブファイルの作成先のディスク容量が不足している場合、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手動で移行先に転送してください。
- 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。

前提条件

Administrator 権限でのログイン

操作手順

1. 次のコマンドを実行して、**Hitachi Command Suite** 製品のサービスをオフラインにします。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%ClusterSetup  
%hcnds64clustersrvstate /soff /r <リソースグループ名>
```

soff

クラスタ管理アプリケーションのリソースグループに登録された **Hitachi Command Suite** 製品のサービスをオフラインにして、フェールオーバーを抑制するためのオプションです。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。

r

リソースグループ名を指定します。

2. hcnds64dbtrans 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 のインストールフォルダ>%Base64%bin%hcnds64dbtrans /  
export /workpath <作業用フォルダ> /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。

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。

3. 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。

4. hcnds64srv 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、リソースグループおよび **Hitachi Command Suite** 製品のサービスをオンラインにします。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%ClusterSetup  
%hcnds64clustersrvstate /son /r <リソースグループ名>
```

son

クラスタ管理アプリケーションに設定されたリソースグループをオンラインにして、フェールオーバーを有効にするためのオプションです。

r

リソースグループ名を指定します。



メモ

hcmds64dbtrans コマンドに続けて、以下のコマンドを実行する場合、hcmds64dbtrans コマンドに auto オプションは指定しないでください。

- hcmd64dbtrans
- hcmd64srv /stop
- hcmd64db
- hcmd64backups

hcmds64dbtrans コマンドに auto オプションを指定しないときは、hcmds64dbtrans コマンドを実行する前に、以下のコマンドを順に実行してください。また、すべての作業が終了後、hcmds64srv /start 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。

Windows の場合：

1. <Hitachi Command Suite のインストールフォルダ>%Base64%bin%hcmd64srv /stop
2. <Hitachi Command Suite のインストールフォルダ>%Base64%bin%hcmd64dsrv /start

関連タスク

- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [9.3 クラスタ管理アプリケーションに登録されている Hitachi Command Suite 製品のサービス](#)

10.4.6 移行元サーバでデータベースをエクスポートする（Red Hat Enterprise Linux のクラスタ構成の場合）

管理サーバの OS が Red Hat Enterprise Linux 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。

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

- 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。
- データベースはアーカイブファイルとしてエクスポートされます。アーカイブファイルの作成先のディスク容量が不足している場合、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手動で移行先に転送してください。

- 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。
-

前提条件

- root 権限でのログイン
- 次の情報の確認
 - サービスグループに登録するために作成したスクリプトのファイル名
Hitachi Command Suite 製品のサービスをサービスグループに登録する方法については、マニュアル「*Hitachi Command Suite* インストールガイド」を参照してください。

操作手順

1. Hitachi Command Suite 製品のサービスをサービスグループから削除します。
詳細については、マニュアル「*Hitachi Command Suite* インストールガイド」を参照してください。
2. 実行系ノードにサービスグループが移動している事を確認します。
移動していない場合は、実行系ノードにサービスグループを移動してください。
3. hcmds64dbtrans 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 のインストールディレクトリ>/Base64/bin/hcmds64dbtrans
-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。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。

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. 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。
5. hcmds64srv 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. 手順 1 で削除した Hitachi Command Suite 製品のサービスを、再度サービスグループに登録します。
7. Hitachi Command Suite 製品のサービスを登録したサービスグループを起動します。
詳細については、マニュアル「*Hitachi Command Suite* インストールガイド」を参照してください。



メモ

hcmds64dbtrans コマンドに続けて、以下のコマンドを実行する場合、hcmds64dbtrans コマンドに auto オプションは指定しないでください。

- hcmds64dbtrans
- hcmds64srv -stop

- hcms64db
- hcms64backups

hcms64dbtrans コマンドに auto オプションを指定しないときは、hcms64dbtrans コマンドを実行する前に、以下のコマンドを順に実行してください。また、すべての作業が終了後、hcms64srv -start 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。

1. <Hitachi Command Suite のインストールディレクトリ>/Base64/bin/hcms64srv -stop
2. <Hitachi Command Suite のインストールディレクトリ>/Base64/bin/hcms64dsrv -start

関連タスク

- [9.1.3 Hitachi Command Suite のサービスの停止](#)

10.4.7 移行先サーバでデータベースをインポートする(非クラスタ構成の場合)

管理サーバ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。



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。
Tuning Manager とリモート接続していて、Tuning Manager のアラート機能を使用していた場合は、データベースのインポート後、アラート定義情報を同期する必要があります。アラート定義情報の同期については、マニュアル「Hitachi Command Suite Tuning Manager API リファレンスガイド」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。

操作手順

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. hcms64dbtrans 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 のインストールフォルダ>%Base64%bin
%hcms64dbtrans /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
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/
hcms64dbtrans -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。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。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 81 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。

hcnds64dbtrans 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 の副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、正サイトの Replication Manager と副サイトの 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。

関連タスク

- ・ [9.1.2 Hitachi Command Suite のサービスの起動](#)
- ・ [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）](#)

関連参照

- ・ [6.2.8 Tuning Manager サーバとのリモート接続およびポート番号の設定 \(htmsetup コマンド\)](#)

10.4.8 移行先サーバでデータベースをインポートする（Windows のクラスタ構成の場合）

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。
- ・ 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。
Tuning Manager とリモート接続していて、Tuning Manager のアラート機能を使用していた場合は、データベースのインポート後、アラート定義情報を同期する必要があります。アラート定義情報の同期について

は、マニュアル「*Hitachi Command Suite Tuning Manager API* リファレンスガイド」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。

前提条件

- Administrator 権限でのログイン
- プロパティファイルの設定値の見直し（移行先の実行系ノードおよび待機系ノード）
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。このため、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、必要に応じて設定値を見直してください。

操作手順

1. 次のコマンドを実行して、Hitachi Command Suite 製品のサービスをオフラインにします。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%ClusterSetup  
%hcnds64clustersrvstate /soff /r <リソースグループ名>
```

soff

クラスタ管理アプリケーションのリソースグループに登録された Hitachi Command Suite 製品のサービスをオフラインにして、フェールオーバーを抑制するためのオプションです。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。

r

リソースグループ名を指定します。

2. hcnds64dbtrans 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 のインストールフォルダ>%Base64%bin%hcnds64dbtrans /  
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
```

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 82 データベースを移行する場合の type オプションの指定値 (Windows の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。

3. 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。
`hcnds64dbtrans` 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。
4. 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。
5. 次のコマンドを実行して、リソースグループおよび Hitachi Command Suite 製品のサービスをオンラインにします。

```
<Hitachi Command Suite のインストールフォルダ>%Base64%ClusterSetup
%hcnds64clustersrvstate /son /r <リソースグループ名>
```

son

クラスタ管理アプリケーションに設定されたリソースグループをオンラインにして、フェールオーバーを有効にするためのオプションです。

r

リソースグループ名を指定します。

6. 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。
7. 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。
8. 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
9. Replication Manager の副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、正サイトの Replication Manager と副サイトの Device Manager のデータベースを同期させます。
 10. データベースをバックアップします。
 11. 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。

関連タスク

- [6.2.7 Tuning Manager サーバとのリモート接続 \(Windows のクラスタ環境\)](#)
- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [10.2.2 データベースのバックアップ \(Windows のクラスタ構成の場合\)](#)

関連参照

- [9.3 クラスタ管理アプリケーションに登録されている Hitachi Command Suite 製品のサービス](#)

10.4.9 移行先サーバでデータベースをインポートする (Red Hat Enterprise Linux のクラスタ構成の場合)

管理サーバの OS が Red Hat Enterprise Linux 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。

前提条件

- root 権限でのログイン
- プロパティファイルの設定値の見直し (移行先の実行系ノードおよび待機系ノード)
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。このため、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、必要に応じて設定値を見直してください。
- 次の情報の確認
 - サービスグループに登録するために作成したスクリプトのファイル名
Hitachi Command Suite 製品のサービスをサービスグループに登録する方法については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。

操作手順

1. Hitachi Command Suite 製品のサービスをサービスグループから削除します。
詳細については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。
2. 実行系ノードにサービスグループが移動している事を確認します。

移動していない場合は、実行系ノードにサービスグループを移動してください。

3. hcmds64dbtrans 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 のインストールディレクトリ>/Base64/bin/hcmd64dbtrans
-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。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。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 83 データベースを移行する場合の type オプションの指定値 (Red Hat Enterprise Linux の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. 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。
 `hcmds64dbtrans` 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. 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。
6. Hitachi Command Suite 製品のサービスを起動します。
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` プロパティを `false` に戻します。
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` プロパティを `false` に戻します。
9. Hitachi Command Suite 製品のサービスを再起動します。
10. 手順 1 で削除した Hitachi Command Suite 製品のサービスを、再度サービスグループに登録します。
11. Hitachi Command Suite 製品のサービスを登録したサービスグループを起動します。
 詳細については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。
12. 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
13. Replication Manager の副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、正サイトの Replication Manager と副サイトの Device Manager のデータベースを同期させます。
14. データベースをバックアップします。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)
- [10.2.3 データベースのバックアップ \(Red Hat Enterprise Linux のクラスタ構成の場合\)](#)

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。



メモ

- ホストの OS が Linux で Device-Mapper マルチパス機能 (DM-Multipath) を使用する場合、`/etc/multipath.conf` ファイルの `multipaths` セクションで、`alias` 属性にマルチパスデバイスの別名を設定するときは、次の文字を使用してください。
A~Z a~z 0~9 - _ . @
- 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。
- Solaris マルチパス機能 (MPxIO) が有効な Solaris ホストの場合、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 LUN の範囲は 0~255 となるように指定してください。LUN が 256 以上の場合、次の問題が発生します。
 - LUN が 256 以上の LDEV の情報が収集されない。
 - コマンドデバイスの LUN が 256 以上の場合、Replication Manager でコピーペア構成定義の操作を行ったときに、KAVN00451-E のエラーメッセージが出力され、操作が失敗する。

11.1.1 Device Manager エージェントで通常ホストを管理する場合の前提環境

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、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。

Device Manager エージェントのセットアップ方法については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。

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。



メモ

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)

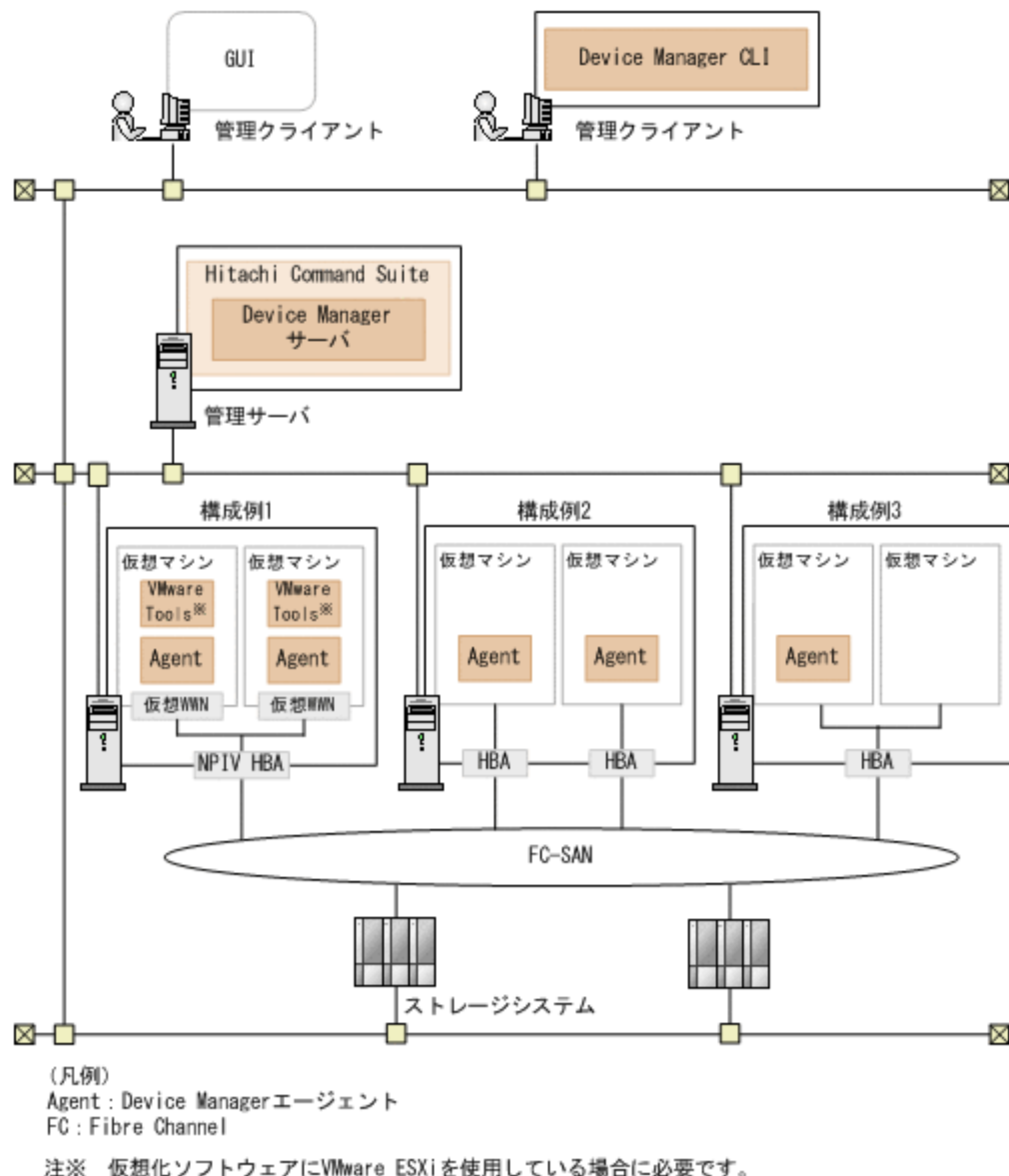
11.1.2 Device Manager エージェントで仮想マシンを管理する場合の前提環境

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。

仮想マシンへの HBA の割り当て方法ごとに、次の 3 つの構成があります。それぞれの構成で、前提環境が異なります。

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

図 59 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)



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) (推奨) : 図中の構成例 1

単独の HBA の構成で、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管理します。

- 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 ESXi 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。
- 仮想化ソフトウェアに VMware ESXi を使用している場合は、同一の物理環境で稼働する VMware ESXi も Host Data Collector を使用して Device Manager に登録してください。Host Data Collector を使用してホストを登録する方法についてはマニュアル「*Hitachi Command Suite ユーザーズガイド*」を参照してください。
- 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。

Device Manager エージェントのセットアップ方法については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。

仮想マシンごとに HBA が割り当てられている構成 : 図中の構成例 2

HBA が割り当てられている仮想マシンごとに Device Manager エージェントをインストールして管理します。

- 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。
- 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。
- 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。

Device Manager エージェントのセットアップ方法については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。

複数の仮想マシンで HBA を共有している構成 : 図中の構成例 3

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管理します。

- 仮想マシンごとに Device Manager エージェントをインストールすることはできません。
- 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。
- 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。

Device Manager エージェントのセットアップ方法については、マニュアル「*Hitachi Command Suite インストールガイド*」を参照してください。

11.1.3 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。

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。

次の手順で NIC の優先順位を変更してください。

1. [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。
2. [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。

関連タスク

- [付録 D.1.1 Device Manager エージェントのプロパティの変更](#)

関連参照

- [付録 D.6.5 server.http.socket.agentAddress](#)

11.1.4 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、次の条件でホストの 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 10 より前のバージョンから Solaris 10 以降にバージョンアップ
 - AIX 6.1 より前のバージョンから AIX 6.1 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 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:¥WINDOWS¥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。

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 RAID Manager XP 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
- 管轄ポリシーファイルのインストール (Device Manager サーバと Device Manager エージェント間でセキュリティ通信する場合)
使用する Java の実行環境のバージョンに応じた Java Cryptography Extension (JCE) の無制限強度の管轄ポリシーファイル (Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files) をダウンロードし、インストールする必要があります。
管轄ポリシーファイルは、Oracle 社または IBM 社の Web サイトからダウンロードしてください。インストール方法は、管轄ポリシーファイルに付属するドキュメントを参照してください。

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

< Device Manager エージェントのインストールディレクトリ > /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 の場合
 - ホストの OS が Linux で、CIM/WBEM 機能を利用して 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ホストの OS が Red Hat Enterprise Linux 7 以降、Oracle Linux 7 以降、または SUSE Linux Enterprise Server 12 以降のときは、64 ビット用の Java の実行環境を使用してください。
- Dynamic Link Manager がホストにインストールされているときに指定できる Java の実行環境については、Dynamic Link Manager のマニュアルを参照してください。
- 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。

関連参照

- [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 \(firewall_setup コマンド\)](#)
- [11.2.7 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。

関連参照

- [付録 D.6.1 server.agent.port](#)
- [付録 D.6.2 server.http.localPort](#)
- [付録 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。

前提条件

次の情報の確認

- 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。

操作手順

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。

関連参照

- [付録 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 Replication 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 RAID Manager XP 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 RAID Manager XP 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 RAID Manager を使用している場合は、Device Manager エージェントの `server.properties` ファイルにある `server.agent.rm.location` プロパティに、RAID Manager のインストールディレクトリを設定してください。RAID Manager XP を使用している場合は、Device Manager エージェントの `server.properties` ファイルにある `server.agent.rmxp.location` プロパティに、RAID Manager XP のインストールディレクトリを設定してください。
- 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` プロパティに、`enable` を設定してください。



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` プロパティに、`true` を設定してください。



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。

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。

各ホストでコピーペアを管理する構成：ストレージシステム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` プロパティに、`true` を設定してください。

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 RAID Manager XP 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。

- Replication 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。

- Replication 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。

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は、マニュアル「*Hitachi Command Suite Replication Manager* システム構成ガイド」を参照してください。

- 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` プロパティに、HORCM_DEV または HORCM_LDEV を設定してください。



注意

HUS100, Hitachi AMS2000, Hitachi SMS または Hitachi AMS/WMS 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、RAID Manager 01-17-03/04 以降または XP7 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 RAID Manager XP 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 プロパティに、Device Manager の操作対象から外したい RAID Manager または RAID Manager XP のインスタンス番号を設定してください。
- ユーザーが作成した RAID Manager または RAID Manager XP 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 プロパティに、true を設定してください。
- ホスト（ペア管理サーバ）に複数の IP アドレスがある場合
Device Manager エージェントの server.properties ファイルにある server.http.socket.agentAddress プロパティに、Device Manager エージェントが Device Manager サーバに通知する IP アドレスを設定してください。

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。

関連タスク

- [付録 D.1.1 Device Manager エージェントのプロパティの変更](#)

関連参照

- [付録 D.2.1 agent.rm.TimeOut](#)
- [付録 D.6.5 server.http.socket.agentAddress](#)
- [付録 D.6.7 server.agent.maxMemorySize](#)
- [付録 D.6.15 server.agent.rm.centralizePairConfiguration](#)

- [付録 D.6.17 server.agent.rm.exclusion.instance](#)
- [付録 D.6.18 server.agent.rm.location](#)
- [付録 D.6.19 server.agent.rm.optimization.userHorcmFile](#)
- [付録 D.6.23 server.agent.rm.pairDefinitionForm](#)
- [付録 D.6.25 server.agent.rm.ignorePairStatus](#)
- [付録 D.6.27 server.agent.rm.moduleTimeOut](#)
- [付録 D.6.33 server.agent.rmxp.location](#)

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 エージェントの `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



メモ

- 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

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ときのプロパティの目安値を次に示します。

表 84 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.maxL ength</code> (単位：バイト)	<code>server.http.server.time Out</code> (単位：秒)	<code>server.util.processTime Out</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

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ときのプロパティの目安値を、OS ごとに「[表 85 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 89 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 85 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 86 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
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 87 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.process TimeOut (単位: ミリ秒)	server.agent.max MemorySize (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 88 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.process TimeOut (単位: ミリ秒)	server.agent.max MemorySize (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 89 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.process TimeOut (単位: ミリ秒)	server.agent.max MemorySize (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
100/256	3,500,000 以上	600	600,000	192
200/256	7,000,000 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)
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

関連タスク

- [付録 A.1.1 Device Manager サーバのプロパティの変更](#)
- [付録 D.1.1 Device Manager エージェントのプロパティの変更](#)

関連参照

- [付録 A.2.5 server.http.entity.maxLength](#)
- [付録 D.6.7 server.agent.maxMemorySize](#)
- [付録 D.6.29 server.http.server.timeOut](#)
- [付録 D.6.30 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 90 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 91 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 RAID Manager XP 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

11.2.7 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
```

Linux の場合

```
< Device Manager エージェントのインストールディレクトリ > /bin
```

Solaris 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。

関連参照

- [11.3.3 Device Manager エージェントのバージョンの表示 \(hdvm_info コマンド\)](#)

11.2.8 Device Manager エージェントの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。

前提条件

次の情報の確認

- 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

操作手順

1. Device Manager エージェントのサービスを停止します。
2. [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。
3. 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。
4. [ログオン] タブを選択し、[アカウント] を選択します。
5. ユーザーとパスワードを設定します。
6. 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。

関連参照

- [11.2.7 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

Linux の場合

<Device Manager エージェントのインストールディレクトリ>/bin

Solaris 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度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度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



ヒント

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
```

統合インストールメディアの中から取得する場合は、Administrator 権限で保護されたフォルダ内に新規にフォルダを作成し、そのフォルダへ hbsa_util.exe ファイルを移動してから実行してください。

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
```

Linux の場合

```
< Device Manager エージェントのインストールディレクトリ >/bin
```

Solaris または HP-UX の場合

```
/opt/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 RAID Manager XP 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 RAID Manager XP 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。

Device Manager エージェントのバージョンが 8.2.0 以降の場合, Device Manager サーバと Device Manager エージェント間でセキュリティ通信を利用するときは, hdvmagt_setting コマンドで次の設定ができます。

- Device Manager サーバのサーバ証明書を Device Manager エージェントのトラストストアにインポートする
- Device Manager エージェントのプロパティファイルを設定する
 - server.server.ssl.hdvm
true を設定します。
 - server.server.serverPort
SSL 通信のポート番号を設定します。

次の情報を対話式に一括設定します。

表 92 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	<p><i>IP アドレスまたはホスト名</i></p> <p>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。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><i>SSL 通信の設定</i></p> <p>Device Manager サーバと Device Manager エージェント間で SSL 通信をする場合は, 次の情報を指定します。</p> <ul style="list-style-type: none"> • Device Manager サーバのサーバ証明書の格納先ディレクトリ指定したディレクトリ内のすべての証明書ファイルがインポート対象になります。サブディレクトリ以下は対象外になります。指定する値は, 次の条件を満たす必要があります。 絶対パス名の長さ: 64 バイト以内 使用する文字 (Windows): A~Z a~z 0~9 . () 空白文字 使用する文字 (UNIX): A~Z a~z 0~9 _ / • Device Manager エージェントのトラストストアのアクセスパスワード パスワードは大文字と小文字が区別されます。デフォルトパスワードは changeit です。

項目	説明
	<p>ポート番号</p> <p>Device Manager サーバ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 2001, SSL 通信の場合は 2443 です。デフォルト値以外を設定している場合は、現在設定している値が表示されます。</p> <p>ユーザー ID とパスワード</p> <p>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。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 RAID Manager XP を利用するための情報	<p>インストール先</p> <p>RAID Manager または RAID Manager XP 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</p> <p>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
- サーバ証明書の入手 (SSL 通信の設定をする場合)
 - 管理サーバで作成されたサーバ証明書を安全な方法で取得します。
 - Device Manager サーバのサーバ証明書
 - 暗号化通信のテストなどの目的で自己署名証明書を使用する場合は、トラストストアファイル (HiCommandCerts) からサーバ証明書をエクスポートしておく必要があります。



メモ

Device Manager サーバのデフォルトの証明書は、ストレージシステム (VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデル) と Hitachi Command Suite の間でユーザーアカウント認証の連携をする際の通信路を暗号化するための自己署名証明書です。Device Manager サーバと Device Manager エージェント間で SSL 通信をする場合は、別の自己署名証明書または認証局の署名済みの証明書を使用してください。

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 エージェントのトラストストアへのアクセスパスワード (デフォルトパスワードを変更している場合)
- 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 (Device Manager サーバと非 SSL で通信している場合) または `server.https.port` プロパティ (Device Manager サーバと SSL で通信している場合) 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 RAID Manager XP 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

Linux の場合

< Device Manager エージェントのインストールディレクトリ > /bin

Solaris または HP-UX の場合

/opt/HDVM/HBaseAgent/bin

AIX の場合

/usr/HDVM/HBaseAgent/bin



ヒント

- 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
Linux の場合
< Device Manager エージェントのインストールディレクトリ > /bin/logs
Solaris または HP-UX の場合
< Device Manager エージェントのインストールディレクトリ > /opt/HDVM/HBaseAgent/bin/logs
AIX の場合
< Device Manager エージェントのインストールディレクトリ > /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。
- トラストストアにインポートされたサーバ証明書のエイリアス名は、hdvm <yyyymmdd> <hhmmss> <処理番号> となります。

関連概念

- [5.1.10 管理サーバと Device Manager エージェント間のセキュリティ通信のための操作フロー](#)

関連参照

- [5.1.22 トラストストア](#)
- [5.3.4 Device Manager サーバのサーバ証明書の認証局への申請](#)
- [付録 A.2.2 server.http.port](#)
- [付録 A.2.3 server.https.port](#)
- [付録 D.6.14 server.server.serverPort](#)
- [付録 D.6.28 server.server.ssl.hdvm](#)

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
```

Linux の場合

```
<Device Manager エージェントのインストールディレクトリ>/bin
```

Solaris 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。



ヒント

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時
- Device Manager の GUI からホスト情報を更新した時

関連参照

- [付録 D.6.12 server.server.authorization](#)
- [付録 D.6.14 server.server.serverPort](#)

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

Linux の場合

< Device Manager エージェントのインストールディレクトリ > /util/bin

Solaris 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, Universal Replicator, または global-active device 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。

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。

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。

hldutil コマンドで指定できるソートキーを次に示します。

表 93 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。

ソートキー	説明
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。

-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。

-hlf

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。

11.3.7 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 94 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 詳細については、「 表 95 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 」を参照してください。
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。

表 95 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

RaidID	ストレージシステムの機種
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 AMS2010, Hitachi AMS2100 または BR1600 シリーズ
85	Hitachi AMS2300
87	Hitachi AMS2500
91	HUS110 または BR1650S
92	HUS130 または BR1650E
93	HUS150
HM70	HUS VM
HM82	VSP G100, G130, G150, G200, G350, G370 または VSP F350, F370
HM84	VSP G400, G600, G700 または VSP F400, F600, F700
HM86	VSP G800, G900 または VSP F800, F900
HM90	VSP E990
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
R800	VSP G1000, G1500, または VSP F1500
R900	VSP 5000 シリーズ

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 RAID Manager XP 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 RAID Manager XP 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

関連概念

- [11.2.4 コピーペアを管理するために必要な設定](#)

関連タスク

- [11.4.2 構成定義ファイルの編集](#)

関連参照

- [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 RAID Manager XP の情報の設定 \(hdvmagt_setting コマンド\)](#)

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。

操作手順

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

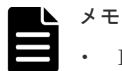
システムフォルダ (環境変数"%windir%"で表されるフォルダ)

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。



- 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 RAID Manager XP のエラー情報が出力されることがあります。



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.tmporaryInstance プロパティおよび server.agent.rm.tmporaryPort プロパティで変更できます。

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。

関連参照

- [11.4.1 構成定義ファイルを利用するための前提環境](#)
- [11.4.13 構成定義ファイルを利用する上での注意事項](#)
- [付録 D.2.4 agent.rm.horcmInstance](#)

- [付録 D.2.5 agent.rm.horcmService](#)
- [付録 D.6.21 server.agent.rm.temporaryInstance](#)
- [付録 D.6.22 server.agent.rm.temporaryPort](#)
- [付録 D.6.26 server.agent.rm.horcmSource](#)

11.4.3 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_VCMD
- 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。

関連参照

- [11.4.4 構成定義ファイルの記述規則](#)
- [11.4.5 HORCM_MON パラメーターの記述形式](#)
- [11.4.6 HORCM_CMD パラメーターの記述形式](#)
- [11.4.7 HORCM_VCMD パラメーターの記述形式](#)
- [11.4.8 HORCM_DEV パラメーターの記述形式](#)
- [11.4.9 HORCM_LDEV パラメーターの記述形式](#)
- [11.4.10 HORCM_INST パラメーターの記述形式](#)
- [11.4.11 HORCM_INSTP パラメーターの記述形式](#)

11.4.4 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は、"H"で始まり、次の文字列を含む行があってはけません。
HORCM_MON, HORCM_CMD, HORCM_VCMD, 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
- 構成定義ファイルの HORCM_DEV パラメーターに仮想 ID の定義があってはけません。
- **RAID Manager 01-32-03/XX** 以降、または **XP7 RAID Manager 01.32.XX** 以降を使用している場合、HORCM_VCMD パラメーターが定義されている構成定義ファイルに HORCM_DEV パラメーター、または仮想ストレージマシンをサポートしていないストレージシステムのコピーペア定義があってはけません。
- **RAID Manager 01-32-03/XX** 以降、または **XP7 RAID Manager 01.32.XX** 以降を使用している場合、HORCM_VCMD パラメーターが定義されている構成定義ファイルに複数のストレージシステムのコマンドデバイスの定義があってはけません。

関連参照

- [11.4.3 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](#)
- [11.4.5 HORCM_MON パラメーターの記述形式](#)
- [11.4.6 HORCM_CMD パラメーターの記述形式](#)
- [11.4.7 HORCM_VCMD パラメーターの記述形式](#)
- [11.4.8 HORCM_DEV パラメーターの記述形式](#)
- [11.4.9 HORCM_LDEV パラメーターの記述形式](#)
- [11.4.10 HORCM_INST パラメーターの記述形式](#)
- [11.4.11 HORCM_INSTP パラメーターの記述形式](#)

11.4.5 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。
 - **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。

- 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 96 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	Y	Y	Y
ホスト名	Y	Y	Y
NONE	Y*	Y*	--
"__NONE__"	--	--	--
NONE6	Y*	--	--
"__NONE6__"	--	--	--
ループバックの IP アドレス (127.0.0.1 ～127.255.255.254)	Y*	Y*	--
ループバックのホスト名 (localhost)	Y*	Y*	--
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)

Y : 指定できる。

-- : 指定できない。

注※ : 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。

- 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 97 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	Y	Y	Y	Y
5.9～6.0	Y	ポート番号指定だけサポート。	Y	Y
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。	Y	Y

バージョン	指定項目			
	ip_address	service	poll	timeout
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。	Y	Y

(凡例)

Y：すべての記述形式をサポート

関連タスク

- [11.4.2 構成定義ファイルの編集](#)

関連参照

- [11.4.4 構成定義ファイルの記述規則](#)
- [11.4.10 HORCM_INST パラメーターの記述形式](#)
- [11.4.11 HORCM_INSTP パラメーターの記述形式](#)
- [11.4.13 構成定義ファイルを利用する上での注意事項](#)

11.4.6 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 98 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	Y
	UNIX の場合	Y
7.1~7.4.0	Windows の場合	Y
	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)

Y : すべての記述形式をサポート

関連タスク

- [11.4.2 構成定義ファイルの編集](#)

関連参照

- [11.4.4 構成定義ファイルの記述規則](#)
- [11.4.13 構成定義ファイルを利用する上での注意事項](#)

11.4.7 HORCM_VCMD パラメーターの記述形式

HORCM_VCMD パラメーターには、操作対象の仮想ストレージマシンのシリアル番号を指定します。

- Serial#
仮想ストレージマシンのシリアル番号を指定します。

表 99 HORCM_VCMD 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
	Serial#
8.0.1 以降	Y※1
8.0	Y※2
7.6.1 以前	--

(凡例)

- Y：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

注※1

RAID Manager 01-32-03/XX 以降、または XP7 RAID Manager 01.32.XX 以降を使用している場合、Device Manager エージェントから HORCM_VCMD の定義を変更できます。

注※2

Device Manager エージェントからは HORCM_VCMD の定義の変更はできません。

関連タスク

- [11.4.2 構成定義ファイルの編集](#)

関連参照

- [11.4.4 構成定義ファイルの記述規則](#)
- [11.4.13 構成定義ファイルを利用する上での注意事項](#)

11.4.8 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 8.0.1 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※, h0※, h1, h2, h3

global-active device : 指定なし, h0, h1, h2, h3

注※

値を指定しない場合、0 または h0 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 7.4.0~8.0 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 100 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	Y	Y	Y	Y	Y	Y
03-50 以前	Y	Y	Y	Y	Y	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)

Y : すべての記述形式をサポート

関連タスク

- [11.4.2 構成定義ファイルの編集](#)

関連参照

- [11.4.4 構成定義ファイルの記述規則](#)
- [11.4.13 構成定義ファイルを利用する上での注意事項](#)

11.4.9 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 8.0.1 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※, h0※, h1, h2, h3

global-active device : 指定なし, h0, h1, h2, h3

注※

値を指定しない場合, 0 または h0 を指定した場合, 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 7.4.0~8.0 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, 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、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 101 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#
6.4 以降	Y	Y	Y	Y	Y
6.3~6.2	Y	Y	Y	Y※	Y
6.1~05-60	Y	Y	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。	Y※	Y
05-50 以前	--	--	--	--	--

(凡例)

Y : 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

注※ : 16 進数または CU:LDEV 形式の場合、参照または削除だけできる。

関連タスク

- [11.4.2 構成定義ファイルの編集](#)

関連参照

- [11.4.4 構成定義ファイルの記述規則](#)
- [11.4.13 構成定義ファイルを利用する上での注意事項](#)

11.4.10 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), またはホスト名を指定します。

- 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_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 102 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	Y	Y
ホスト名	Y	Y
ループバックの IP アドレス (127.0.0.1 ~127.255.255.254)	Y*	--
ループバックのホスト名 (localhost)	Y*	--
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)

Y : 指定できる。

-- : 指定できない。

注※ : 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。

- 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 103 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	Y	Y	Y
6.1~6.4	Y	IP アドレス, ホスト名の指定だけサポート。	Y
6.0 以前	Y	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)

Y:すべての記述形式をサポート

関連タスク

- 11.4.2 構成定義ファイルの編集

関連参照

- 11.4.4 構成定義ファイルの記述規則
- 11.4.5 HORCM_MON パラメーターの記述形式
- 11.4.8 HORCM_DEV パラメーターの記述形式
- 11.4.9 HORCM_LDEV パラメーターの記述形式
- 11.4.13 構成定義ファイルを利用する上での注意事項

11.4.11 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、またはホスト名を指定します。
 - 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_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 104 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	Y
ホスト名	Y
ループバックの IP アドレス (127.0.0.1～127.255.255.254)	Y*
ループバックのホスト名 (localhost)	Y*
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)

Y：指定できる。

--：指定できない。

注※：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。

- 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 105 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	Y
6.2～7.5.0	Y*
6.1 以前	--

(凡例)

Y：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

注※：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。

関連タスク

- [11.4.2 構成定義ファイルの編集](#)

関連参照

- [11.4.4 構成定義ファイルの記述規則](#)
- [11.4.5 HORCM_MON パラメーターの記述形式](#)
- [11.4.8 HORCM_DEV パラメーターの記述形式](#)
- [11.4.9 HORCM_LDEV パラメーターの記述形式](#)
- [11.4.10 HORCM_INST パラメーターの記述形式](#)
- [11.4.13 構成定義ファイルを利用する上での注意事項](#)

11.4.12 構成定義ファイルの格納場所の変更

RAID Manager または RAID Manager XP 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.horcmSource` プロパティに設定します。

前提条件

Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

操作手順

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。
HORCM インスタンスの停止方法については、RAID Manager のマニュアルを参照してください。
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.horcmSource` 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。

関連参照

- [11.2.7 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 \(hbsasrv コマンド\)](#)
- [付録 D.6.26 server.agent.rm.horcmSource](#)

11.4.13 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 RAID Manager XP 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 RAID Manager XP 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際には、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。

関連タスク

- [11.4.2 構成定義ファイルの編集](#)

関連参照

- [付録 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。

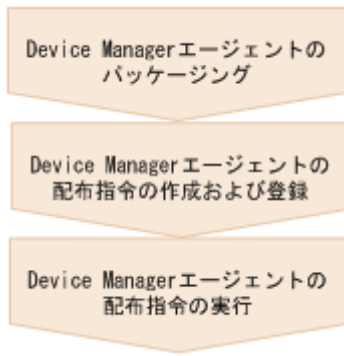
11.5.1 Device Manager エージェントをリモートインストールするための操作フロー

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 60 リモートインストールの流れ



関連タスク

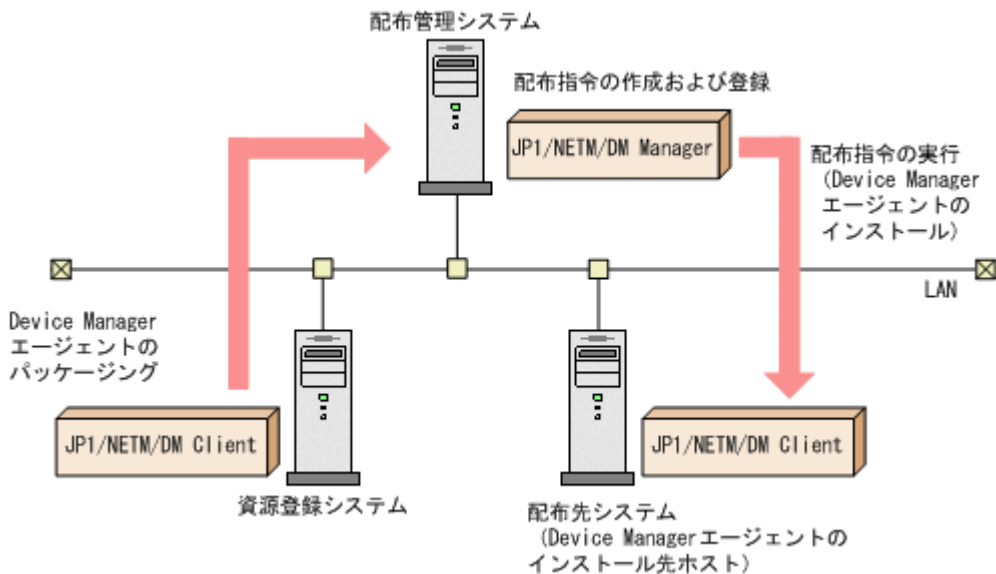
- 11.5.3 Device Manager エージェントのパッケージング (Windows)
- 11.5.4 Device Manager エージェントのパッケージング (UNIX)
- 11.5.5 Device Manager エージェントの配布指令の作成, 登録および実行 (Windows)
- 11.5.6 Device Manager エージェントの配布指令の作成, 登録および実行 (Solaris)

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 61 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。

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。

前提条件

Administrator 権限でのログイン

操作手順

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。

関連タスク

- [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 \(Windows\)](#)

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。

操作手順

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。



メモ

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。



ヒント

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。

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
```

関連タスク

- [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 \(Solaris\)](#)

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。

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。

前提条件

- 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

操作手順

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。



メモ

[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。

関連タスク

- [11.5.3 Device Manager エージェントのパッケージング \(Windows\)](#)

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。

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。

前提条件

- Device Manager エージェントのパッケージング
- 次の情報の確認
 - 配布先のホスト名

操作手順

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。

```
# rdsdmrsc -c
```

コマンドの実行例を次に表示します。

```
# rdsdmrsc -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。
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.
```

関連タスク

- [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 106 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。

戻り値	説明	対処
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。	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。 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。
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。

関連参照

- [付録 D.6.9 server.agent.JRE.location](#)

Hitachi Command Suite の監査ログ

この章では、Device Manager および Tiered Storage Manager の監査ログを採取するために必要な設定や、監査ログで確認できる情報について説明します。

- 12.1 監査ログを採取するために必要な設定
- 12.2 監査ログの確認
- 12.3 監査ログのメッセージ部に出力されるメッセージテキスト
- 12.4 監査ログのメッセージ部に出力される詳細メッセージ
- 12.5 Tiered Storage Manager CLI のユーザー操作と監査ログの対応

12.1 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、「[12.1.2 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、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 107 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">Fibre Channel ログイン機器認証 (Fibre Channel - Security Protocol 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

種別	説明
	<ul style="list-style-type: none"> 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「[12.2 監査ログの確認](#)」を参照してください。

12.1.1 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せん。

- 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 108 監査ログに出力される監査事象（種別が StartStop の場合）](#)」～「[表 112 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 108 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 109 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
	ログアウトの失敗	4	KAPM01126-W
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
SNMP v3 トラップ受信時のユーザー認証	ユーザー認証の成功	6	KAIC52000-I
	ユーザー認証の失敗	3	KAIC52100-E

表 110 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
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
プロファイルの変更	プロファイルの変更成功	6	KAPM07233-I
	プロファイルの変更失敗	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

種別の説明	監査事象	Severity	メッセージ ID
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
	hcnds64unlockaccount コマンドによるアカウントのロック解除成功	6	KAPM07236-I
	hcnds64unlockaccount 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
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

種別の説明	監査事象	Severity	メッセージID
	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	hcmds64backups コマンドまたは hcmdsb64db コマンドによるバックアップ成功	6	KAPM05561-I
	hcmds64backups コマンドまたは hcmdsb64db コマンドによるバックアップ失敗	3	KAPM05562-E
	hcmdsb64db コマンドによる全体リストアの成功	6	KAPM05563-I
	hcmdsb64db コマンドによる全体リストアの失敗	3	KAPM05564-E
	hcmdsb64db コマンドによる部分リストアの成功	6	KAPM05565-I
	hcmdsb64db コマンドによる部分リストアの失敗	3	KAPM05566-E
データベースのエクスポートまたはインポート	データベースのエクスポートに成功	6	KAPM06543-I
	データベースのエクスポートに失敗	3	KAPM06544-E
	データベースのインポートに成功	6	KAPM06545-I
	データベースのインポートに失敗	3	KAPM06546-E
データベース領域の作成または削除	データベース領域の作成成功	6	KAPM06348-I
	データベース領域の作成失敗	3	KAPM06349-E
	データベース領域の削除成功	6	KAPM06350-I
	データベース領域の削除失敗	3	KAPM06351-E
認証データの入出力	hcmdsb64authmove コマンドによるデータ出力の成功	6	KAPM05832-I
	hcmdsb64authmove コマンドによるデータ出力の失敗	3	KAPM05833-E
	hcmdsb64authmove コマンドによるデータ入力 の成功	6	KAPM05834-I
	hcmdsb64authmove コマンドによるデータ入力 の失敗	3	KAPM05835-E

種別の説明	監査事象	Severity	メッセージ ID
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
タスクに対する操作 (GUI)	タスク操作の成功	6	KAIC15984-I
	タスク操作の失敗	3	KAIC15985-E
ストレージシステムの構成変更 (GUI)	ストレージシステムの構成変更成功	6	KAIC15986-I
	ストレージシステムの構成変更失敗	3	KAIC15987-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
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

種別の説明	監査事象	Severity	メッセージID
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
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
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
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
キーストアファイ ルの情報取得※3	キーストアファイルの情報取得に成功	6	KATS90000-I
	キーストア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
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
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

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	KATS90000-I
	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
	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 で操作した場合にだけ出力されます。

表 111 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
	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 で操作した場合にだけ出力されます。

表 112 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

種別の説明	監査事象	Severity	メッセージ ID
	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「[12.3 監査ログのメッセージ部出力される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* メッセージ」を参照してください。

12.1.2 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 のインストールフォルダ>%Base64%conf%sec%auditlog.conf

- Linux の場合 :

<Hitachi Command Suite のインストールディレクトリ>/Base64/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 113 auditlog.conf ファイルに設定する項目

項目	説明
Log.Facility	<p>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。</p> <p>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 108 監査ログに出力される監査事象 (種別が StartStop の場合)」～「表 112 監査ログに出力される監査事象 (種別が ExternalService の場合)」を参照してください。Log.Facility に指定できる値については、「表 114 Log.Facility に指定できる値と syslog.conf での指定値の対応」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 115 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」を参照してください。</p> <p>Log.Facility 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。</p> <p>デフォルト値：1</p>
Log.Event.Category	<p>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 108 監査ログに出力される監査事象 (種別が StartStop の場合)」～「表 112 監査ログに出力される監査事象 (種別が ExternalService の場合)」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。</p> <p>デフォルト値：指定なし</p>
Log.Level	<p>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。</p> <p>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 108 監査ログに出力される監査事象 (種別が StartStop の場合)」～「表 112 監査ログに出力される監査事象 (種別が ExternalService の場合)」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の対応については、「表 115 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」を参照してください。</p> <p>Log.Level は、Windows の場合だけに有効です。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。</p> <p>指定できる値：0～7 (重要度 (Severity))</p> <p>デフォルト値：6</p>

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 114 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*

Facility	対応する syslog.conf での指定値
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の対応を示します。

表 115 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

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。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。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)

- 9.1.3 Hitachi Command Suite のサービスの停止

12.2 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。また、イベントログのソースは "HBase64 Event", イベント ID は "1" です。

<プログラム名> [<プロセス ID >]: <メッセージ部>

- Linux の場合 :
syslog ファイルに次の形式で出力されます。

<syslog ヘッダー部> <メッセージ部>

<syslog ヘッダー部>のフォーマットは、OS の環境設定に依存します。例えば、rsyslog を使用している場合、/etc/rsyslog.conf ファイルに\$ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format を指定すると、RFC5424 対応の形式で出力されます。

<メッセージ部>の出力形式と内容を説明します。



メモ

<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 116 メッセージ部に出力される情報

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、「 12.1.1 監査ログに出力される監査事象 」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

項目※1	内容
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
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、「 12.3 監査ログのメッセージ部に出力されるメッセージテキスト 」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
was successful. (session ID = <セッション ID >)"

```

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,1.1,17,KAIC51000-  
I,2016-08-26T21:36:41.5+09:00,DvM_Srv,AHO,ConfigurationAccess,Success,uid  
=system,,,,,from=127.0.0.1,,,,BasicLog,DvM_CLI,, "662627265 ModPort<SA  
info='R800-50932'><Port info='R800-50932-0,,Fabric(on)? Point-to-  
Point,1,,,,,,,,,,,,,'></Port></SA>"
```

12.3 監査ログのメッセージ部出力されるメッセージテキスト

監査ログ中のメッセージ部出力される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。

12.3.1 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* メッセージ」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 was successful. (session ID = <セッション ID >)"
```

12.3.2 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 117 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、「 12.4 監査ログのメッセージ部出力される詳細メッセージ 」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。

項目	内容
	<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	<p>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。</p> <p>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、「12.4 監査ログのメッセージ部に出力される詳細メッセージ」を参照してください。</p>
エラーメッセージ ID	<p>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 メッセージ」を参照してください。</p>

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"
```

12.3.3 Device Manager GUI 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 メッセージ](#)」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。

タスク登録時の例

```
The task operation (registerTask) succeeded. (task name=<タスク名>)
```

12.3.4 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 118 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

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。
ラウンチセッション ID	形式: "lsessionID=..." ラウンチ用セッション ID が出力されます。ある特定のアプリケーションをラウンチする場合に、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。ラウンチセッション ID が出力されるアプリケーションについては、「 表 119 ラウンチセッション ID の有無とラウンチ識別子の内容 」を参照してください。ラウンチ対象のストレージシステムが、Hitachi USP のときに出力されます。
ラウンチ先識別子	形式: "loid=..." ラウンチ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。ラウンチ識別子の内容は、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 119 ラウンチセッション ID の有無とラウンチ識別子の内容 」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「 <i>Hitachi Command Suite</i> メッセージ」を参照してください。

次の表に、ラウンチセッション ID の有無とラウンチ先識別子の内容を、ラウンチされるアプリケーションごとに示します。

表 119 ラウンチセッション ID の有無とラウンチ識別子の内容

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	ラウンチ識別子の内容
Element Manager	Universal Storage Platform V/VM	無	ラウンチ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※と同様です。詳細については、「 表 131 エレメントの内容と対応する属性値の出力順 」の StorageArray エレメントの属性値出力順を参照してください。
	Hitachi USP	有	
	HUS100	無	
	Hitachi AMS2000	無	
	Hitachi SMS	無	
	Hitachi AMS/WMS	無	
Protection Manager	--	無	ラウンチ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※と同様です。詳細については、「 表 131 エレメントの内容と対応する属性値の出力順 」の Host エレメントの属性値出力順を参照してください。

注※

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。

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"
```

12.3.5 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 120 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=..." 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=0outParams={MinimumVolumeSize=1024,MaximumVolumeSize=248139692,VolumeSizeDivisor=1024}"
```

12.3.6 Tiered Storage Manager の処理として出力される場合

Tiered Storage Manager CLI 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) >][, <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 121 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 123 監査ログに出力されるメッセージ 」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 124 監査ログに出力される操作種別 (OP) の意味 」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 125 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。

表 122 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

項目	内容	出力形式
		メッセージ内容については、マニュアル「Hitachi Command Suite メッセージ」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)	VL= (devnum,id)

項目	内容	出力形式
	2. LU または LDEV のオブジェクト ID (id)	
	複数の場合 1. 要素数 (n) 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)	NumVL=n, Start VLs VL[1]= (devnum-1,id-1) ... 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)	空き容量情報数 (n)	NumFS=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)	TK= (id,3)

項目	内容	出力形式
	2. タスク種別 (type) =3	
	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	opt= (status,emergency)
	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	

表 123 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。

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
		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。
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 124 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

表 125 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
20	SD	Storage Domain	ストレージドメイン
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
110	LOG	Logger Info	ログ出力に関する情報
120	PO	Pool	プール
130	KS	Key Store	キーストアーファイル情報
140	FS	Free Space	空き容量

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=(DM1hc2idzx,Domain-A) "
```

12.4 監査ログのメッセージ部に出力される詳細メッセージ

Device Manager サーバがリクエストを受理した場合、監査ログのメッセージ部のメッセージテキストに詳細メッセージとして操作内容が出力されます。

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 126 詳細メッセージに出力される情報

項目	内容
コマンド	リソースに対しての操作（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、「 12.4.1 詳細メッセージに出力されるコマンド 」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、「 12.4.2 詳細メッセージに出力されるターゲット 」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、「 12.4.3 詳細メッセージに出力されるオプション 」を参照してください。

項目	内容
	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 ます。
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「 12.4.4 詳細メッセージに出力されるパラメーター 」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。

12.4.1 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 127 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

12.4.2 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 128 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
AclRel	AclRelation	リソースグループ, ユーザーグループおよびロールの関 係によって構成される認可情報の作成・削除・取得・変 更
AclRol	AclRole	ロールの一覧の取得
AclRsrcGrp	AclResourceGroup	リソースグループの作成・削除・情報取得・変更
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
CpyGrp	CopyGroup	コピーグループの情報取得
DataRetentions	DataRetentions	データ保護情報の設定・取得

出力文字列	正式名	操作内容
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
LDEVForALUA	LDEVForALUA	LDEV の ALUA 属性の変更
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
MntrDt	MonitoringData	I/O モニタリング情報の適用・取得
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
PortVisibleWWN	PortVisibleWWN	ポートにログインしているホスト (HBA) の WWN の情報取得
PRpu	PResourcePartitionUnit	リソースグループの構成変更
QrmDsk	QuorumDisk	Quorum ディスク ID の設定・削除
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
RepPrfmnc	ReplicationPerformance	コピーグループの構成情報および性能情報の更新
RepPrfmncDt	ReplicationPerformanceData	Universal Replicator の性能情報の取得
RepStatus	ReplicationStatus	global-active device ペアの状態の取得
ReqStatus	RequestStatus	コマンドの状態の返却
ResrcName	ResourceName	ストレージシステムのラベル情報の取得
SA	StorageArray	ストレージシステムの追加, 削除, および情報取得
ShrnkPoolPrgrs	ShrinkingPoolProgress	DP プールの縮小の進捗取得

出力文字列	正式名	操作内容
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
SSupervisor	StorageSupervisor	SVP が管理するストレージシステムの情報取得
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
VLDEV	VLDEV	仮想 LDEV の追加・削除
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	仮想リソースグループの構成変更
VSA	VStorageArray	仮想ストレージマシンの構成情報取得
VSrv	VirtualizationServer	仮想化サーバまたは VMware vCenter Server に関する情報取得
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。

12.4.3 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 129 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 仮想リソースグループに、仮想 LDEV を追加する。
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

出力文字列	操作内容
	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。
applyMonitorDataAndRelocate	S-VOL に適用した I/O モニタリング情報を基に、HDT プールの階層再配置を実行する。
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。
ctg	コンシステンシーグループ ID を設定する。
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 仮想リソースグループから、仮想 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 VirtualVolume 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。 ターゲットが VResourcePartitionUnit の場合 仮想 LDEV が所属する仮想リソースグループを強制削除する。 ターゲットが MonitoringData の場合 コピーペアの構成に関係なく、I/O モニタリング情報を適用または取得する。
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。
mapVAttr	仮想 LDEV に仮想 LDEV 情報を設定する。

出力文字列	操作内容
mapVID	仮想 LDEV に仮想デバイス番号を設定する。
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。
move	<ul style="list-style-type: none"> ターゲットが PResourcePartitionUnit の場合 リソースグループの各リソースを別のリソースグループに移動する。 ターゲットが VResourcePartitionUnit の場合 仮想 LDEV を別の仮想リソースグループに移動する。
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。
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 同じ仮想デバイス番号を持つ 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。
refreshconfiguration	コピーグループの性能情報と構成情報を同時に更新する。
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。
reverse	正ボリュームと副ボリュームの関係を逆転させてからコピーペアを削除する。
setMode	仮想 LDEV の操作モードを設定する。

出力文字列	操作内容
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。
startMonitor	性能モニタリングを開始する。
startRelocation	ハードウェア階層再配置を開始する。
stopMonitor	性能モニタリングを停止する。
stopRelocation	ハードウェア階層再配置を停止する。
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。
unmapVAttr	仮想 LDEV から仮想 LDEV 情報を削除する。
unmapVID	仮想 LDEV から仮想デバイス番号を削除する。
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。
withoutVAttr	仮想 LDEV に仮想 LDEV 情報を設定しない。
withoutVID	仮想 LDEV に仮想デバイス番号を設定しない。
ZeroPageReclaim	ゼロページを破棄する。

12.4.4 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 130 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 131 エレメントの内容と対応する属性値の出力順 」を参照してください。ただし、「 表 131 エレメントの内容と対応する属性値の出力順 」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 131 エレメントの内容と対応する属性値の出力順 」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 131 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
AclRel	AclRelation (リソースグループ、ユーザーグループおよびロールの関係によって構成される認可情報)	ユーザーグループの ID, リソースグループのオブジェクト ID
AclRol	AclRole (ロールの情報)	ロールの短縮名
AclRsrcGrp	AclResourceGroup (リソースグループの情報)	<モデル名 ^{*1} - シリアル番号 - リソースグループの ID>, リソースグループ名, 説明, ストレージシステムのオブジェクト ID, 仮想ストレージマシンのオブジェクト ID
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
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リティグループに関する情報)	<モデル名 ^{*1} - 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, 外部パリティグループのオプション情報, タイプ
ArrRsrv	ArrayReservation (ストレージシステムのロック情報)	<モデル名 ^{*1} - シリアル番号>, <モデル名 ^{*1} - シリアル番号>
ArrV	ArrayValue	ArrayValue で指定する値

出力文字列	正式名と内容	属性値出力順
	(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)	
ChangedItem	ChangedItem (Device Manager で変更されたデータに関する情報)	-
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
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
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, MCU モデル, MCU のシリアル番号, HDT ボリューム ^{*4} の階層割り当てポリシー, 仮想ストレージマシンのファミリー, 仮想ストレージマシンのシリアル番号, 仮想ポート ID, 仮想ホストグループ ID, 仮想デバイス番号 ^{*3} , 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, 仮想ストレージマシンのタイプ, ポートの種類, リソースの最初の並び番号, リソースの個数, ストレージシステムのオブジェクト ID, 仮想ストレージマシンのオブジェクト ID, ID (LDEV ID, ホストグループのドメイン ID, または iSCSI ターゲットのドメイン ID) がリソースに割り当て済みかどうか, コンシステンシーグループ ID, メインフレームボリュームのコンシステンシーグループ ID, コピーの種類 ^{*5}
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 ^{*1} , 発生日時, IP アドレス

出力文字列	正式名と内容	属性値出力順
ConfigChange	ConfigChange (Device Manager サーバで変更されたデータに関する情報)	-
ConfigF	ConfigFile (RAID Manager のコンフィグファイルに関する情報)	<ホスト ID - HORCM インスタンス番号>
CpyGrp	CopyGroup (コピーグループの情報)	<P-VOL 側の WWN または P-VOL 側のホスト ID - P-VOL 側の HORCM インスタンス番号 - S-VOL 側の WWN または S-VOL 側のホスト ID - S-VOL 側の HORCM インスタンス番号 - コピーグループ名>
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
ErrList	ErrorList (ErrorInfo エレメントを含むリスト)	ErrorInfo エレメントの個数
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 ^{*1} - 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 ^{>*2} , 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
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
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 ^{*1} - 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>

出力文字列	正式名と内容	属性値出力順
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, , , , , , , ,
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
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
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) *1, 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*3, 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
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*6, シリアル番号, ポート番号, ポート名, デバイス番号*3, 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) , , , , , , ボリューム ID, global-active device のペアタイプ, 物理モデル名*6, 物理シリアル番号, 物理ポート番号, 物理ポート名
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*6, シリアル番号, ポート番号, , デバイス番号*3, , ホスト名称, 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

出力文字列	正式名と内容	属性値出力順
		続識別番号, LU 番号, HBA のポート 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), クラスタ名, ホストタイプ, ファイルサーバの管理サーバの IP アドレス, ボリュームの用途, ファイルサーバのタイプ, ファイルサーバのクラスタ ID, , , , ,
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*1 - 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, ALUA のパスの優先度
HSDID	HostStorageDomainID (ホストストレージドメインの ID に関する情報)	<ポートのユニークキー - ドメイン ID>
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
JrnlPool	JournalPool (ジャーナルグループ情報)	<モデル名*1 - 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 プールのしきい値 1, DP プールのしきい値 2, DP プールのしきい値 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), リモートバス監視時間の単位, リモートバス監視時間, リモート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, 手動モニタリングの HDT プールの I/O 負荷情報, 手動モニタリングの稼働状態, 手動モニタリングの最終開始日時, 手動モニタリングの最終終了日時, 手動モニタリングの階層再配置の実行状態, 手動モニタリングの階層再配置の進捗率, 手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, HDT プールの階層再配置速度, DP プール枯渇による DP ボリュームへの I/O 失敗時に DP ボリュームを保護するかどうか (Protect 属性にするかどうか), DP プールボリューム閉塞による DP ボリュームへの I/O 失敗時に DP ボリュームを保護す

出力文字列	正式名と内容	属性値出力順
		るかどうか (Protect 属性にするかどうか), active flash が有効か無効か
JrnlPoolDriveAttr	JournalPoolDriveAttr (DP プールボリュームのドライブ属性に関する情報)	-
JrnlPoolTier	JournalPoolTier (HDT プールの階層情報)	<モデル名 ^{*1} ・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
LDEV	LDEV (LDEV に関する情報)	<モデル名 ^{*1} ・シリアル番号・LDEV のデバイス番号 ^{*3} >, LDEV の LBA, CLPR 番号, ストライプサイズ, HDT ボリューム ^{*4} 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ン番号, 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 ^{*4} の階層再配置の有無, 階層割り当てポリシーの新規ページ割り当て HDT ボリューム情報, 優先再配置指定情報, DP ボリュームの容量を DP プールからページ予約するかどうか, ALUA 属性が有効か無効か, T10 PI 属性が有効か無効か
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ピング)	<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
LicenseKey	LicenseKey (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)	<モデル名 ^{*1} ・シリアル番号・LicenseKeyID>
LogSet	LogSettings (ストレージシステムに設定されている, 監査ログの Syslog 設定・FTP 設定に関する情報, およびアラートの SNMP 設定に関する情報)	-
LU	LogicalUnit (LU を表す情報)	<モデル名 ^{*1} ・シリアル番号・論理デバイス番号 ^{*3} >, 論理ユニットに含まれている LDEV の番号 ^{*3} , 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, 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デバイスグループ定義の有無, 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
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

出力文字列	正式名と内容	属性値出力順
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 ^{※3} ・SVOL シリアル番号・SVOLLDEV 番号 ^{※3} >, P-VOL のストレージシステムのタイプ ^{※1} , 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 ^{※3} , 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 ^{※1} , 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 ^{※3} , 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 ^{※5} , コピー状態, P-VOL の MU 番号, P-VOL のフェンスレベル, メインフレームボリュームのコンシステンシーグループ ID
MFVolI	MFVolumeInfo (メインフレームホストと LDEV 間のアクセス情報)	-
MntrDt	MonitorData (I/O モニタリング情報)	HDT ボリュームの転送情報, I/O モニタリング情報のセッションデータ, I/O モニタリング情報の取得の成功可否
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
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)
ObjLabel	ObjectLabel (Device Manager サーバのオブジェクトのラベル設定)	オブジェクト ID, オブジェクトに設定するラベル
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。
EgMntrDt	PageMonitorData (ページごとの I/O モニタリング情報)	ページ番号, I/O モニタリングの読み込み情報, I/O モニタリングの書き込み情報, シーケンシャルデータに対する I/O モニタリング情報, I/O モニタリング情報の加重平均 (短期間), I/O モニタリング情報の加重平均 (長期間), I/O モニタリング情報のデータ保証コード
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 ^{※1} ・シリアル番号・ジャーナルプール識別子・プール ID・MU 番号 ^{※2} >, MU 番号, 形成コピー転送レート
PairedPortController	PairedPortController	-

出力文字列	正式名と内容	属性値出力順
	(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 ^{※5} , 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 ^{※1} , ボリュームの論理デバイス番号 ^{※3} , 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
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 ^{※1}
PArrGrp	PArrayGroup (リソースグループに属するパリティグループの情報)	シャーシ番号, パリティグループ番号
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
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 ^{※1} - シリアル名 - ポート ID - ドメイン ID - 論理デバイス番号 ^{※3} >, 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 ^{※3} , 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 ^{※3}
PDEV	PDEV (PDEV に関する情報)	<モデル名 ^{※1} - 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
PHSD	PHostStorageDomain (リソースグループに属するホストグループの情報)	ポート ID, ホストグループ ID
PLDEV	PLDEV (リソースグループに属する LDEV の情報)	LDEV のデバイス番号
Port	Port (ポートに関する情報)	<モデル名 ^{※1} - 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, Selective ACK モードが有効か無効か, Delayed ACK モードが有効か無効か, Window Scale Option の設定値

出力文字列	正式名と内容	属性値出力順
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 ^{*1} ・シリアル番号・ポートコントローラー ID>, モード
PPort	PPort (リソースグループに属するポートの情報)	ポート ID
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
PRpu	PResourcePartitionUnit (リソースグループの構成変更)	<モデル名 ^{*1} ・シリアル番号・リソースグループの ID >
QrmDsk	QuorumDisk (Quorum ディスクに関する情報)	<モデル名 ^{*1} ・シリアル番号・Quorum ディスク ID>, Quorum ディスク ID, Quorum ディスクのデバイス番号 ^{*3} , Quorum ディスクを共有する相手側ストレージシステムのファミリー, Quorum ディスクを共有する相手側ストレージシステムのシリアル番号, Quorum ディスク監視停止時の Read 応答保証時間 (秒)
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, RCU 側の iSCSI ポートの IP アドレス, RCU 側の iSCSI ポート番号
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 のバスのグループ ID, 回線の帯域
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 インスタンスのインスタンス番号, 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 ^{*5} , P-VOL のフェンスレベル, コピーペース, Quorum ディスク ID, コンシステンシーグループ ID
RepI	ReplicationInfo (レプリケーションに関する情報)	<PVOL シリアル番号・PVOLLDEV 番号 ^{*3} ・SVOL シリアル番号・SVOLLDEV 番号 ^{*3} >, 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 ^{*1} , 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 ^{*3} , P-VOL パスを管理する HORCM 構成ファイル内のポート番号, HORCM 構成ファイル内の P-VOL が属しているストレージシステムのシリアル番号, HORCM 構成ファイル内の P-VOL の

出力文字列	正式名と内容	属性値出力順
		デバイス番号, 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*1, 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*3, S-VOL パスを管理する HORCM 構成ファイル内のポート番号, HORCM 構成ファイル内の S-VOL が属しているストレージシステムのシリアル番号, HORCM 構成ファイル内の S-VOL のデバイス番号, S-VOL が属するプール ID, コピーの種類*5, P-VOL の MU 番号, P-VOL のフェンスレベル, コピーベース, 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, Quorum ディスク ID, コンシステンシーグループ ID
RepPrfmncPrmtrs	ReplicationPerformanceParameters (Universal Replicator の性能情報の取得に関する情報)	<P-VOL 側の WWN または P-VOL 側のホスト ID - P-VOL 側の HORCM インスタンス番号 - S-VOL 側の WWN または S-VOL 側のホスト ID - S-VOL 側の HORCM インスタンス番号 - コピーグループ名>, ホスト名, HORCM インスタンス番号, コピーグループ名, 性能情報の取得開始日時, 性能情報の取得終了日時
ReqStatus	RequestStatus (直前のリクエストの状態を返す)	メッセージ ID
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)	RSIM 情報の RSIM ID
RsltObj	ResultObject (ListView エレメント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)	<モデル名*1 - シリアル番号>
SIMI	SIMInfo (ストレージシステムの SIM 情報)	SIM 情報の SIMID
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
SlctCond	SelectCondition (SelectedItem 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
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*1
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

出力文字列	正式名と内容	属性値出力順
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
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
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*1 - 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*5, コンシステンシーグループの ID
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
SsSummary	SnapshotSummary (Copy-on-Write Snapshot の P-VOL に関する情報)	-
SSupervisor	StorageSupervisor (SVP に関する情報)	SVP の IP アドレス, SVP が管理するストレージシステムのファミリー, SVP が管理するストレージシステムのファミリーの表示名, SVP の RMI レジストリーのポート番号
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
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
TrngPlcy	TieringPolicy (HDT ボリューム*4 の階層ポリシーに関する情報)	<モデル名*1 - シリアル番号 - 階層ポリシー ID>, 階層ポリシー名, 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
URLLink	URLLink (Hitachi Command Suite オブジェクトとア	<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

出力文字列	正式名と内容	属性値出力順
	アプリケーションのリンク)	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
User	User (Device Manager の 1 ユーザーアカウント情報)	ユーザー ID, 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
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 (仮想 LDEV に関する情報)	<モデル名*1・シリアル番号・仮想リソースグループの ID・デバイス番号*3>, デバイス番号*3, 仮想デバイス番号*3, 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, 仮想 LDEV の操作モード
VM	VM (仮想マシンの情報)	-
VolCon ^{※2}	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*1・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*3>
VolFmtPrgrss	VolumeFormatProgress (ボリュームのノーマルフォーマットの進捗)	-
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
VolID	VolumeID (ボリュームの ID に関する情報)	<ストレージシステムのユニークキー・LDEV のデバイス番号>
VolMig	VolumeMigration (マイグレーションプランに関する情報)	<モデル名*1・シリアル番号・移動元 LDEV 番号*3・移動先 LDEV 番号*3>, 移動操作オーナー ID, 移動元デバイス番号*3, 移動先デバイス番号*3
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
VPort	VPort (仮想ポートの情報)	-
VRpu	VResourcePartitionUnit (仮想リソースグループの情報)	<モデル名*1・シリアル番号・仮想リソースグループの ID>, リソースグループ名, 仮想ストレージマシンのタイプ, 仮想ストレージマシンのファミリー, 仮想ストレージマシンのシリアル番号
VSA	VStorageArray (仮想ストレージマシンの構成情報)	<仮想ストレージマシンのファミリーまたは仮想ストレージマシンのタイプ*1・仮想ストレージマシンのシリアル番号>, リソースグループ名
VSrv	VirtualizationServer	-

出力文字列	正式名と内容	属性値出力順
	(仮想化サーバに関する情報)	
VSrvMan	virtualizationservermanager (VMware vCenter Server に関する情報)	-
WritingPattern	WritingPattern (書き込み 1 回分の書き込みパターン情報)	シュレディングが指定されたときの書き込みパターン
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

(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

ストレージシステム種別として、「[表 132 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※2

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※3

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, 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 番号を組み合わせさせた数値 (=LDKC*65536+CU*256+LDEV) が出力されます。

Hitachi USP の場合は, CU と LDEV 番号を組み合わせさせた数値 (=CU*256+LDEV) が出力されます。

HUS100, Hitachi SMS および Hitachi AMS/WMS の場合は LU 番号が出力されます。

注※4

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※5

レプリケーション操作種別属性は、「[表 133 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。

注※6

ストレージシステム種別として、「[表 134 ストレージシステム種別 共通出力名称一覧 \(RaidID が出力される場合\)](#)」に示す共通出力名称で出力されます。

表 132 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
D700	Hitachi AMS/WMS
D800	Hitachi AMS2000
D850	HUS100
HM700	HUS VM
HM800	VSP G100, G200, G400, G600, G800, または VSP F400, F600, F800
HM850	VSP G130, G150, G350, G370, G700, G900, または VSP F350, F370, F700, F900
R500	Hitachi USP
R600	Universal Storage Platform V/VM
R700	Virtual Storage Platform
R800	VSP G1000, G1500 または VSP F1500
R900	VSP 5000 シリーズ
S800	Hitachi SMS

表 133 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
Local Copy for Mainframe	Hitachi ShadowImage for Mainframe
Remote Copy (Async)	TrueCopy Async
Remote Copy (Async) for Mainframe	Hitachi TrueCopy Asynchronous for Mainframe
Remote Copy (Ha)	global-active device
Remote Copy (Jrnl)	Universal Replicator
Remote Copy (Jrnl) for Mainframe	Hitachi Universal Replicator for Mainframe
Remote Copy (Sync)	TrueCopy Sync
Remote Copy (Sync) for Mainframe	Hitachi TrueCopy for Mainframe
SnapShot	Copy-on-Write Snapshot
SnapShot (Fast)	Thin Image

表 134 ストレージシステム種別 共通出力名称一覧 (RaidID が出力される場合)

共通出力名称 (RaidID)	対応ストレージシステム種別
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

共通出力名称 (RaidID)	対応ストレージシステム種別
82	Hitachi SMS 110
83	Hitachi AMS2010, Hitachi AMS2100 または BR1600 シリーズ
85	Hitachi AMS2300
87	Hitachi AMS2500
91	HUS110 または BR1650S
92	HUS130 または BR1650E
93	HUS150
HM70	HUS VM
HM82	VSP G100, G130, G150, G200, G350, G370 または VSP F350, F370
HM84	VSP G400, G600, G700 または VSP F400, F600, F700
HM86	VSP G800, G900 または VSP F800, F900
HM90	VSP E990
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
R800	VSP G1000, G1500 または VSP F1500
R900	VSP 5000 シリーズ

12.5 Tiered Storage Manager CLI のユーザー操作と監査ログの対応

ここでは、Tiered Storage Manager CLI での操作時に出力される監査ログについて説明します。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。

操作手順

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 135 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「Y」が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 135 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	Y	Add	VL	SD, MG, VL	—
	--	Get	MG	SD, MG	—
	--	Get	SD	SD	—
	--	Get	VL	SD, NumVL	—
CancelTask	Y	Cancel	TK	TK	—
CreateLockingTask	Y	Create	TK	TK, SD, MG, NumVL, VLs	TK=(id,2,...)
	--	Execute	TK	TK	—
	--	Get	TK	TK	—
CreateMigrationGroup	--	Get	SD	SD	—
	Y	Create	MG	SD, MG	—
CreateMigrationPlan	--	Get	ST	SD, NumST, [STs]	—
	Y	Create	MP	SD, MG, ST	—
CreateMigrationTask	Y	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	Y	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	Y	Create	SD	SD, SS	—
CreateStorageTier	--	Get	SD	SD	—
	Y	Create	ST	SD, ST	—
CreateUnlockingTask	Y	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	—
	Y	Delete	MG	MG	—
DeleteStorageDomain	--	Get	SD	SD	—

CLI コマンド	キー※1	OpName※2	ResName※2	追加情報※2	特記事項
	Y	Delete	SD	SD	—
DeleteStorageTier	--	Get	ST	SD, ST	—
	Y	Delete	ST	SD, ST	—
DeleteTasks	--	Get	TK	{TK NumTK}	--force 指定なし
	Y	Delete	TK	{TK NumTK, TKs}	—
ExecuteTask	Y	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
	Y	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	Y	Get	MG	SD, NumMG, [MGs]	—
GetPools	--	Get_num	PO	NumPO	—
	--	Get	SD	SD	—
	Y	Get	PO	SD, NumPO	—
GetStorageDomains	Y	Get	SD	NumSD, [SDs]	—
	--	Get	RS	NumSD, SDs	—
GetStorageTiers	Y	Get	ST	SD, NumST, [STs]	—
	--	Get	SD	SD	—
GetTasks	Y	Get	TK	{TK NumTK}	—
GetVolumes	--	Get_num	VL	NumVL	—
	--	Get	SD	SD	10,000 件ずつ分割取得
	Y	Get	VL	SD, NumVL	10,000 件ずつ分割取得
ModifyMigrationGroup	--	Get	MG	SD, MG	—
	Y	Modify	MG	SD, MG	—
ModifyStorageDomain	--	Get	SD	SD	—
	Y	Modify	SD	SD	—
ModifyStorageTier	--	Get	ST	SD, ST	—
	Y	Modify	ST	SD, ST	—
ModifyTask	--	Get	TK	TK	—

CLI コマンド	キー※1	OpName※2	ResName※2	追加情報※2	特記事項
	Y	Modify	TK	TK	—
Refresh	--	Get_summary	SD	NumSD	ストレージドメイン名の指定あり
	Y	Refresh	SD	SD	—
RemoveVolumeFromMigrationGroup	--	Get_summary	SD	SD	—
	--	Get	MG	SD, MG	—
	--	Get	VL	SD, NumVL	—
	Y	Remove	VL	SD, MG, VL	—
StopTask	Y	Change	TK	TK	opt = (0x02040000, または 0x02050000)

(凡例)

- Y : 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 121 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 125 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。

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保守情報の取得方法について説明します。

- 13.1 管理サーバで発生したトラブルへの対処方法 (Device Manager)
- 13.2 管理サーバで発生したトラブルへの対処方法 (Tiered Storage Manager)
- 13.3 ホストで発生したトラブルへの対処方法
- 13.4 トラブル発生時に採取が必要な保守情報

13.1 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。

13.1.1 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、`hcmds64unlockaccount` 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。

関連タスク

- ・ [3.2.4 アカウントロックの解除](#)

13.1.2 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。

デスクトップヒープの領域の変更方法については、Microsoft 社の Web サイトを参照してください。

13.1.3 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`

関連タスク

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

関連参照

- [付録 A.3.2 dbm.startingCheck.retryCount](#)
- [付録 A.3.3 dbm.startingCheck.retryPeriod](#)

13.1.4 Hitachi Virtual File Platform および Hitachi Capacity Optimization の SNMP トラップを受信できない

Hitachi Virtual File Platform および Hitachi Capacity Optimization 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>

13.1.5 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

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager  
%HiCommandServer%lib%HSNMAPI%lanconf.inf
```

Linux の場合

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/lib/  
HSNMAPI/lanconf.inf
```

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

13.2 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 からの操作だけを示します。

13.2.1 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。

13.2.2 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：

```
< Hitachi Command Suite のインストールフォルダ > %TieredStorageManager%\bin  
%htsmsserver forcestop
```

Linux の場合：

```
< Hitachi Command Suite のインストールディレクトリ > /  
TieredStorageManager/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。

13.2.3 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。データ消去到失敗した場合、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。

1. 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。
2. 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。

3. マイグレーションが実行されていない LDEV があった場合、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。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

13.2.4 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。

関連概念

- [10.3 データベースの復元](#)

13.3 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。

13.3.1 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。

関連概念

- [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](#)

13.3.2 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。

13.3.3 [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。

関連参照

- [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 \(hbsa_util コマンド\)](#)

13.3.4 [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。

関連参照

- [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 \(hbsa_util コマンド\)](#)

13.3.5 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。

1. 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
2. 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%
```

13.3.6 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\

Linux の場合

< *Device Manager* エージェントのインストールディレクトリ > /bin/logs/

Solaris 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。

関連概念

- [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](#)

関連タスク

- [1.3.2 メモリーヒープサイズの変更](#)

関連参照

- [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 RAID Manager XP 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 \(HiScan コマンド\)](#)

13.3.7 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。

13.3.8 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。

関連参照

- [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 \(hldutil コマンド\)](#)

13.3.9 Device Manager エージェントの機能が使用できない

RAID Manager と RAID Manager XP 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 RAID Manager XP をインストールし直してください。

要因

RAID Manager と RAID Manager XP 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、RAID Manager XP 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 RAID Manager XP をインストールし直してください。

RAID Manager と RAID Manager XP をアンインストールしたあと、RAID Manager XP 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。

13.3.10 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¥Harddisk¥n¥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。

13.4 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、hcnds64getlogs 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 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



メモ

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 または Hitachi Capacity Optimization 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。

Device Manager と Tiered Storage Manager 以外のログファイルの取得方法については、各プログラムのマニュアルを参照してください。

13.4.1 管理サーバの保守情報の取得 (hcmds64getlogs コマンド)

管理サーバの保守情報を取得するには、hcmds64getlogs 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 (Linux の場合) でのログイン

コマンドの形式

Windows :

```
<Hitachi Command Suite のインストールフォルダ>%Base64%bin  
%hcmds64getlogs /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> ...]]
```

Linux :

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/  
hcmds64getlogs -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

hcmds64getlogs コマンドは、2 つ以上同時に実行しないでください。



メモ

Hitachi File Services Manager や Storage Navigator Modular 2 と連携している場合は、types オプションおよび logtypes オプションを省略して実行すると、Hitachi File Services Manager や Storage Navigator Modular 2 の保守情報も収集できます。

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 (/)、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。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 136 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
そのほかの製品	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_64」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。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。



メモ

大規模なシステム環境で [レプリケーション] タブを使用している場合は、保守情報の取得に時間が掛かり、保守情報のファイルサイズが大きくなります。このため、hcmds64getlogs コマンドの実行時に、次のオプションを指定して保守情報を取得することをお勧めします。

Windows :

```
<Hitachi Command Suite のインストールフォルダ>%Base64%bin%hcmds64getlogs /dir <フォルダ名> /logtypes log csv
```

Linux :

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/hcmds64getlogs -dir <ディレクトリ名> -logtypes log csv
```

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。



ヒント

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、hcmds64getlogs 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 hcmds64getlogs コマンドを実行してください。

13.4.2 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、hcmds64getlogs 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。

操作手順

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 :

```
<Hitachi Command Suite のインストールフォルダ>%TieredStorageManager  
%SupportTools%CollectTool%
```

Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/TieredStorageManager/  
SupportTools/CollectTool/
```

表 137 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 : <Hitachi Command Suite のインストールフォルダ> %TieredStorageManager%CLI Linux の場合 : <Hitachi Command Suite のインストールディレクトリ>/ TieredStorageManager/CLI
SYSLOG	Linux の場合に 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。 /var/log/messages

13.4.3 Host Data Collector マシンの保守情報の取得 (hdc_getras コマンド)

Host Data Collector マシンの保守情報を取得するには、hdc_getras 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 (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_getras.bat -o  
<フォルダ名> [-f]
```

Linux の場合 :

```
<Host Data Collector のインストールディレクトリ>/HDC/Base/bin/hdc_getras.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 (/)、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
```

Linux の場合 :

```
<o オプションに指定したディレクトリ>/hdcResult
```

13.4.4 Host Data Collector 管理対象ホストの保守情報の取得 (hdc_target_getras 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_getras 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]
```

- ○

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

○ 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
```

13.4.5 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
```

Linux の場合

```
<Device Manager エージェントのインストールディレクトリ>/bin
```

Solaris 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
```

13.4.6 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。

操作手順

1. < Hitachi Command Suite のインストールフォルダ > ¥Base64¥uCPSB¥CC¥server¥public ¥ejb¥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。

操作結果

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 のインストールフォルダ > ¥Base64¥uCPSB¥CC¥server¥public ¥ejb¥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。

13.4.7 HCS Device Manager Web Service のスレッドダンプ取得 (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。

操作手順

1. 次のコマンドを実行します。

```
# kill -3 < PID >
```

< PID > は、< Hitachi Command Suite のインストールディレクトリ > /Base64/ uCPSB/CC/server/public/ejb/DeviceManagerWebService/logs/CC/ maintenance/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。

操作結果

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、次のディレクトリへ出力されます。

```
< Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/CC/server/ public/ejb/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。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

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 (server.properties ファイルと cimxmlsca.properties ファイル)
- 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 [レプリケーション] タブ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 138 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。
<ul style="list-style-type: none"> • server.properties ファイル • cimxmlscpa.properties ファイル 	Device Manager のセキュリティ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UNCH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	[レプリケーション] タブ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。
<ul style="list-style-type: none"> • jserver.properties ファイル 	CIM/WBEM 機能に関するプロパティファイルです。

プロパティファイル	説明
<ul style="list-style-type: none"> cimxmlcpa.properties ファイル cimxmlscpa.properties ファイル 	



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。

前提条件

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

操作手順

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

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：
 <Hitachi Command Suite のインストールフォルダ>%DeviceManager
 %HiCommandServer%config%server.properties
- Linux の場合：
 <Hitachi Command Suite 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。
- 次の場合、このプロパティの設定値を変更したときには、Device Manager GUI の [ストレージシステム編集] 画面で、ユーザーアカウント認証を設定し直してください。
 - VSP G1000, G1500 または VSP F1500 で、RAID Manager および SVP へのログイン時に Hitachi Command Suite でユーザーアカウントを認証している場合
 - VSP 5000 シリーズ, VSP Gx00 モデルまたは VSP Fx00 モデルを操作する場合

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。

- Device Manager エージェントに登録された Device Manager のポート番号 (hdvmagt_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
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。
- 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)

関連タスク

- [5.5.7 ポップアップブロックの設定変更](#)
- [5.5.8 Device Manager CLI の実行マシンでの SSL/TLS の有効化](#)
- [5.5.15 Replication Manager サーバと Device Manager サーバ間の通信プロトコルの変更](#)
- [付録 B.1.1 Tiered Storage Manager サーバのプロパティの変更](#)

関連参照

- [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 RAID Manager XP の情報の設定 \(hdvmagt_setting コマンド\)](#)
- [付録 B.4.2 hdvm.port](#)

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。

- Device Manager エージェントに登録された Device Manager のポート番号 (hdvmagt_setting コマンド)
- 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)
- 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)

次の場合、このプロパティの設定値を変更したときには、Device Manager GUI の [ストレージシステム編集] 画面で、ユーザーアカウント認証を設定し直してください。

- VSP G1000, G1500 または VSP F1500 で、RAID Manager および SVP へのログイン時に Hitachi Command Suite でユーザーアカウントを認証している場合

- ・ VSP 5000 シリーズ, VSP Gx00 モデルまたは VSP Fx00 モデルを操作する場合

関連タスク

- ・ [5.5.7 ポップアップブロックの設定変更](#)
- ・ [5.5.8 Device Manager CLI の実行マシンでの SSL/TLS の有効化](#)
- ・ [5.5.15 Replication Manager サーバと Device Manager サーバ間の通信プロトコルの変更](#)

関連参照

- ・ [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 RAID Manager XP の情報の設定 \(hdvmagt_setting コマンド\)](#)

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。

関連参照

- ・ [付録 A.7.1 client.rmi.port](#)
- ・ [付録 B.4.4 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狙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 : 3000000



メモ

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 Replication Manager では無視されます。

関連参照

- [1.18 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 機能を有効にする場合は、このプロパティに true を設定してください。CIM 機能を無効にする場合は、このプロパティに false を設定してください。

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

関連参照

- [付録 A.2.13 server.cim.http.port](#)
- [付録 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。

関連参照

- [付録 A.2.12 server.cim.support.protocol](#)
- [付録 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。

関連参照

- [付録 A.2.12 server.cim.support.protocol](#)
- [付録 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、Universal Storage Platform V/VM または Hitachi USP 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 または Hitachi AMS/WMS 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 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

関連参照

- [付録 A.5.6 server.dispatcher.snm2.configchange.pollingPeriod](#)
- [付録 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.storagesystem

次の内容をユーザーに E メールで通知するかどうかを指定します。

- ストレージシステムのアラート
- Device Manager GUI, Tiered Storage Manager のイベント
- ヘルスチェック結果

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。

関連参照

- [付録 A.2.20 server.mail.smtp.host](#)

A.2.18 server.mail.enabled.fileserver

ファイルサーバまたは NAS モジュールのアラートをユーザーに 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。

ファイルサーバまたは NAS モジュールの場合、ポーリングと SNMP トラップでは、障害を検知するタイミングが異なりますが、アラートに表示される内容は同じです。そのため、`true` を指定すると、どちらのアラートも E メールで通知されます。

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。

関連参照

- [付録 A.2.20 server.mail.smtp.host](#)

A.2.19 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.2.20 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.storagesystem` または `server.mail.enabled.fileserver` プロパティに `true` を指定してください。

関連参照

- [付録 A.2.17 server.mail.enabled.storagesystem](#)
- [付録 A.2.18 server.mail.enabled.fileserver](#)

A.2.21 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.2.22 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.2.23 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

関連参照

- [付録 A.2.19 server.mail.from](#)

A.2.24 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.2.25 server.mail.alert.type.storagesystem

ストレージシステムの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 によるポーリング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 によるポーリング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 によるポーリング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.2.26 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.2.27 server.subsystem.ssid.availableValues

Device Manager でボリュームを作成する際、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、VSP 5000 シリーズ、VSP G1000, G1500, VSP F1500, VSP Gx00 モデル、VSP Fx00 モデル、Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP 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.2.28 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 VSP 5000 シリーズ、VSP G1000, G1500, VSP F1500, VSP Gx00 モデル、VSP Fx00 モデル、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 VSP 5000 シリーズ、VSP G1000, G1500, VSP F1500, VSP Gx00 モデル、VSP Fx00 モデル、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 (分単位) >
```

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 :
 <Hitachi Command Suite のインストールフォルダ>%DeviceManager
 %HiCommandServer%config%database.properties
- Linux の場合 :
 <Hitachi Command Suite 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：
 <Hitachi Command Suite のインストールフォルダ>%DeviceManager
 %HiCommandServer%config%logger.properties
- Linux の場合：
 <Hitachi Command Suite 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

関連参照

- [付録 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。キロバイト単位のときは **KB**、メガバイト単位のときは **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 HDvMGuiMessagen.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 (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 (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

関連参照

- [付録 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 n .log, HDvMGuiTracen n .log および HDvMGuiMessage n .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:

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager  
%HiCommandServer%config%dispatcher.properties
```

- Linux の場合:

```
<Hitachi Command Suite 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 性能に影響が出ることがあります。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ペ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ペ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UNCH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)

関連参照

- 付録 A.2.15 server.configchange.enabled

A.5.7 server.dispatcher.configchange.pollingPeriod

Element Manager で 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)

関連参照

- [付録 A.2.15 server.configchange.enabled](#)

A.5.8 server.dispatcher.daemon.configUpdate.detection.interval

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, 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。

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, 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, VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, 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 (Universal Storage Platform V/VM の場合だけ)
 - 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 (VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, Virtual Storage Platform, または Universal Storage Platform V/VM の場合だけ)
 - 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※

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, 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。

関連参照

- [付録 A.5.9 server.dispatcher.daemon.autoSynchro.doRefresh](#)

- [付録 A.5.10 server.dispatcher.daemon.autoSynchro.type](#)
- [付録 A.5.14 server.dispatcher.daemon.configUpdate.detection.variable.enabled](#)

A.5.9 server.dispatcher.daemon.autoSynchro.doRefresh

Device Manager サーバが VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, 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 VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, 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, VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, 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。VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, VSP Fx00 モデル, 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。

関連参照

- [付録 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

関連参照

- [付録 A.5.9 server.dispatcher.daemon.autoSynchro.doRefresh](#)
- [付録 A.5.11 server.dispatcher.daemon.autoSynchro.dayOfWeek](#)

- [付録 A.5.12 server.dispatcher.daemon.autoSynchro.startTime](#)
- [付録 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

関連参照

- [付録 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

関連参照

- [付録 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）

関連参照

- [付録 A.5.10 server.dispatcher.daemon.autoSynchro.type](#)

A.5.14

server.dispatcher.daemon.configUpdate.detection.variable.enabled

Device Manager サーバが VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、VSP Fx00 モデル、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しきい値の変更
 - 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

関連参照

- [付録 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選択して, 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

関連参照

- [付録 A.5.16 server.dispatcher.daemon.autoSynchro.performance.startTime](#)
- [付録 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

関連参照

- [付録 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

関連参照

- [付録 A.14.1 htnm.infoAcquirePeriod](#)

A.5.18

server.dispatcher.daemon.logicalGroupMappingUpdate.startTime

[分析] タブの MP ブレード/ユニット分析画面に表示される、ポリシーが所属する論理グループの一覧をバックグラウンドで収集するタスクの実行開始時刻を「*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。

デフォルト : 02:00

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 :
 <Hitachi Command Suite のインストールフォルダ>%DeviceManager
 %HiCommandServer%config%mime.properties
- Linux の場合 :
 <Hitachi Command Suite 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 :
 <Hitachi Command Suite のインストールフォルダ>%DeviceManager
 %HiCommandServer%config%client.properties
- Linux の場合 :
 <Hitachi Command Suite 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

関連参照

- [付録 A.2.4 server.rmi.port](#)

A.7.2 client.launch.em.secure

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, または VSP Fx00 モデル を操作する場合, Device Manager GUI から Storage Navigator を起動する際に, セキュリティを高めるために Storage Navigator に送信する情報を簡略化するかどうかを指定します。

true を指定した場合, Storage Navigator に送信する情報を簡略化します。この場合, 次の設定が必要です。

- ストレージシステムと管理クライアント (GUI) 間のセキュリティ通信の設定を有効にすること。
自己署名証明書または認証局の署名済みのサーバ証明書を使用してください。
- Device Manager GUI でストレージシステムを登録する際に, ホスト名で登録すること。
サーバ証明書の Common Name に設定されているホスト名で登録してください。ストレージシステムを登録する方法については, マニュアル「*Hitachi Command Suite ユーザーズガイド*」を参照してください。

false を指定した場合, Storage Navigator に送信する情報を簡略化しません。

デフォルト: false

関連概念

- [5.1.17 ストレージシステムと管理クライアント \(GUI\) 間のセキュリティ通信のための操作フロー](#)

A.7.3 client.externaltask.sn.fetch.enable

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, または VSP Fx00 モデル における Storage Navigator での操作のタスクを Device Manager で監視するかどうかを指定します。おもに Storage Navigator の操作で構成変更を行う場合だけ, false を指定してください。

true を指定した場合, Device Manager が Storage Navigator での操作のタスクを監視し, Device Manager GUI で Storage Navigator での操作のタスクを表示できます。また, Storage Navigator での操作のタスクによる構成変更を自動的に Device Manager のデータベースに反映します。この構成変更を Device Manager のデータベースに反映する間は, 該当ストレージシステムがロックされ, Storage Navigator の操作ができなくなることがあります。

false を指定した場合, Device Manager は Storage Navigator での操作のタスクを監視しません。この場合, Storage Navigator での操作のタスクによる構成変更を Device Manager のデータベースに反映するには, 手動でのストレージシステムの更新が必要です。

デフォルト: true

関連参照

- [付録 A.7.4 client.externaltask.sn.fetch.pollinginterval](#)

A.7.4 client.externaltask.sn.fetch.pollinginterval

VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデル, または VSP Fx00 モデル における Storage Navigator での操作のタスクを Device Manager で監視する場合, タスクの監視間隔を秒単位で指定します。指定できる範囲は 1~86400 (秒) です。

このプロパティは `client.externaltask.sn.fetch.enable` プロパティで `true` を指定した場合だけ有効になります。

デフォルト : 5 (秒)

関連参照

- [付録 A.7.3 client.externaltask.sn.fetch.enable](#)

A.8 Device Manager のセキュリティに関するプロパティ (server.properties ファイルと cimxmlscpa.properties ファイル)

セキュリティに関するプロパティは、`server.properties` ファイルおよび `cimxmlscpa.properties` ファイルに含まれています。

- `server.properties` ファイル
 - Windows の場合 :
< *Hitachi Command Suite* のインストールフォルダ > %DeviceManager%HiCommandServer%config%server.properties
 - Linux の場合 :
< *Hitachi Command Suite* のインストールディレクトリ > /HiCommandServer/config/server.properties
- `cimxmlscpa.properties` ファイル
 - Windows の場合 :
< *Hitachi Command Suite* のインストールフォルダ > %DeviceManager%HiCommandServer%wsi%server%jserver%bin%cimxmlscpa.properties
 - Linux の場合 :
< *Hitachi Command Suite* のインストールディレクトリ > /HiCommandServer/wsi/server/jserver/bin/cimxmlscpa.properties

A.8.1 server.http.security.clientIP

Device Manager サーバに接続できる IPv4 アドレスを指定します。

`server.http.security.clientIP` プロパティは `server.properties` ファイルに存在します。

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のオーバーフローを狙った攻撃を防ぐのに役立ちます。

172.16.0.1 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=172.16.0.1,192.168.*.*
```

1 つの IP アドレスで複数の接続元を指定する場合には、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。無効な IP アドレスや空白文字 (スペース) は無視されます。

デフォルト : *.*.*.* (すべての IP アドレスが接続できます)



注意

- Device Manager サーバをインストールしたマシンを示す IP アドレス（ローカルループバックアドレス）は、設定する必要はありません。このプロパティでは、ローカルループバックアドレスからは常に Device Manager サーバに接続できるものと見なされます。
- Hitachi Command Suite 共通コンポーネントの環境定義ファイル `user_httpsd.conf` にも IP アドレスを登録する必要があります。

関連タスク

- [付録 E.2 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](#)

A.8.2 server.http.security.clientIPv6

Device Manager サーバに接続できる IPv6 アドレスを指定します。

`server.http.security.clientIPv6` プロパティは `server.properties` ファイルに存在します。

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狙った攻撃を防ぐのに役立ちます。

`12AB:0:0:CD30::~12AB:0:0:CD3F:FFFF:FFFF:FFFF:FFFF` の接続を許可する場合の指定例を次に示します。

```
server.http.security.clientIPv6=12AB:0:0:CD30::/60
```

CIDR 形式で範囲を指定できます。IP アドレスを複数指定する場合は、コンマ (,) で区切ります。無効な IP アドレスの指定や空白文字（スペース）は無視されます。

デフォルト：`:::`（すべての IP アドレスが接続できます）



注意

- Device Manager サーバをインストールしたマシンを示す IP アドレス（ローカルループバックアドレス）は、設定する必要はありません。このプロパティでは、ローカルループバックアドレスからは常に Device Manager サーバに接続できるものと見なされます。
- Hitachi Command Suite 共通コンポーネントの環境定義ファイル `user_httpsd.conf` にも IP アドレスを登録する必要があります。

関連タスク

- [付録 E.2 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](#)

A.8.3 server.https.security.keystore

SSL または TLS で暗号化された通信の確立に使用されるキーペアとサーバ証明書を格納するキーストアファイルの名前を指定します。

`server.https.security.keystore` プロパティは `server.properties` ファイルに存在しません。

Device Manager のバージョン 8.1.3 以降では、Device Manager を新規インストールした場合、または Device Manager サーバの証明書が存在しない状態でアップグレードインストールをした場合、Device Manager サーバのキーストアには、VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、および VSP Fx00 モデルに対するユーザーアカウント認証用のデフォルトの証明書が格納されています。VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、および VSP Fx00 モデルとの通信をよりセキュアにしたい場合、またはほかの用途

でセキュリティ通信をする場合は、キーペアと自己署名証明書または信頼された証明書をキーストアにインポートし直してください。

デフォルト : keystore

関連概念

- [5.1.1 Device Manager サーバのデフォルトの証明書](#)

A.8.4 server.http.security.unprotected

サーバのドキュメントルートにある保護していないファイルリソースを指定します。

server.http.security.unprotected プロパティは server.properties ファイルに存在します。

複数のファイルリソースを指定する場合は、各項目をコンマ (,) で区切ります。スペースは無視されます。ファイルまたはディレクトリが未保護として指定されている場合、サーバのセキュリティモード設定に関わらず、これらはアクセス制御リストチェック (ユーザー認証) から除かれます。アスタリスクをワイルドカード文字として使用することで、ディレクトリ全体 (ネストされたサブディレクトリも含む) を未保護としてフラグを設定できます。スペースを指定した場合には、すべてのリソースが保護されます。この結果、Device Manager へのすべての要求にユーザー認証が必要になります。

このプロパティは、ユーザー認証を必要とせず、誰でも index.html フロントページを Web ブラウザーに表示できるようにします。さらに重要なことは、Java Web Start アプリケーションが、一連のログオンダイアログを表示せずに JAR ファイルを更新し、(HiCommand.jnlp ファイルを介して) エンドユーザーのシステムに展開できることです。同様に、手順ごとに独立した認証を必要とせず、GUI のヘルプファイル (および特定のクライアントインストール情報) を Web ブラウザーに表示できます。通常、この設定を変更する必要はありません。

デフォルト : index.html, HiCommand/*, webstart/*, images/*, style/*, docs/*, favicon.ico, vasa/*

A.8.5 server.https.security.truststore

Device Manager サーバのトラストストアファイルを指定します。

server.https.security.truststore プロパティは server.properties ファイルに存在します。

デフォルト : dvmcacerts



メモ

このプロパティは、HiKeytool で変更できません。値を変更するには、server.properties ファイルで値を編集する必要があります。

A.8.6 server.https.enabledCipherSuites

次の SSL/TLS 通信で使用する暗号方式 (Cipher Suite) をコンマ (,) で区切って指定します。

- Device Manager サーバと Device Manager GUI (Web ブラウザー) 間
- Device Manager サーバと Device Manager CLI 間
- Device Manager サーバと Device Manager エージェント間
- Device Manager サーバと Replication Manager サーバ間

`server.https.enabledCipherSuites` プロパティは `server.properties` ファイルに存在します。

指定できる暗号方式は次のとおりです。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

デフォルト : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256

A.8.7 server.https.protocols

次の SSL/TLS 通信で使用するプロトコルをコンマ (,) で区切って指定します。

- Device Manager サーバと Device Manager GUI (Web ブラウザー) 間
- Device Manager サーバと Device Manager CLI 間
- Device Manager サーバと Device Manager エージェント間
- Device Manager サーバと Replication Manager サーバ間

`server.https.protocols` プロパティは `server.properties` ファイルに存在します。

指定できるプロトコルは次のとおりです。

- TLSv1
- TLSv1.1
- TLSv1.2

指定したプロトコルのうち、暗号強度の高いプロトコルから使用されます。

デフォルト : TLSv1, TLSv1.1, TLSv1.2

A.8.8 Ciphers

Device Manager サーバと CIM クライアント間 (オブジェクト操作とインディケーション通知) の SSL/TLS 通信で使用する暗号方式 (Cipher Suite) をコンマ (,) で区切って指定します。

指定できる暗号方式は次のとおりです。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

デフォルトで使用される暗号方式は次のとおりです。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

cimxmlscpa.properties ファイルおよび Ciphers プロパティは、デフォルトでは存在しません。使用する暗号方式を制限する場合は、cimxmlscpa.properties ファイルを新規作成し、Ciphers プロパティを次の形式で追記してください。

Ciphers = <暗号方式>, <暗号方式>, ...



注意

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。このため、設定した値を控えておくことをお勧めします。

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 :
 <Hitachi Command Suite のインストールフォルダ>%DeviceManager
 %HiCommandServer%config%customizedsnmptrap.properties
- Linux の場合 :

<Hitachi Command Suite 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



メモ

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。

関連参照

- 付録 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 139 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">InformationWarningErrorCriticalAlertNull	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に出力されます。 <ul style="list-style-type: none">Information : -IWarning : -WError/Critical/Alert : -ENull : ログを出力しない

項目	形式	説明
出力内容	次の文字列 (変数) で出力内容を指定します。 次に示す文字列以外は指定できません。 <ul style="list-style-type: none"> • \$a • \$e • \$g • \$s • \$n (n=1 以上の整数) 	省略できます。省略時は\$a\$e\$g\$sの内容が出力されます。 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 番目のバリアブルバインディングの値

- 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。

関連参照

- [付録 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 :
 - <Hitachi Command Suite のインストールフォルダ>¥DeviceManager
 - ¥HiCommandServer¥config¥launchapp.properties
- Linux の場合 :
 - <Hitachi Command Suite 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、ラウンチ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 ブラウザーからラウンチ実行する 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 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 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

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

Device Manager GUI から Storage Navigator を使用してエンタープライズクラスストレージ、VSP Gx00 モデル、VSP Fx00 モデルまたは HUS VM に接続する場合、Storage Navigator 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、Storage Navigator の URL にホスト名を表示します。false を指定した場合、Storage Navigator 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 :
 < Hitachi Command Suite のインストールフォルダ >¥DeviceManager
 ¥HiCommandServer¥config¥host.properties
- Linux の場合 :
 < Hitachi Command Suite 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 :
 < Hitachi Command Suite のインストールフォルダ >¥DeviceManager
 ¥HiCommandServer¥config¥hostdatacollectors.properties

- Linux の場合：
 < Hitachi Command Suite 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。

関連参照

- [付録 A.12.3 hdc.rmiserver](#)
- [付録 A.12.4 hdc.classloader](#)
- [付録 A.12.5 hdc.usessl](#)
- [付録 C.2.4 hdc.common.rmi.registryPort](#)
- [付録 C.2.7 hdc.common.rmi.ssl.registryPort](#)
- [付録 C.2.10 hdc.service.rmi.registryIPAddress](#)

A.12.3 hdc.rmiserver

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.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。

関連参照

- [付録 A.12.2 hdc.rmiregistry](#)
- [付録 A.12.4 hdc.classloader](#)
- [付録 A.12.5 hdc.usessl](#)
- [付録 C.2.5 hdc.common.rmi.serverPort](#)
- [付録 C.2.8 hdc.common.rmi.ssl.serverPort](#)
- [付録 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。

関連参照

- [付録 A.12.2 `hdc.rmiregistry`](#)
- [付録 A.12.3 `hdc.rmiserver`](#)
- [付録 A.12.5 `hdc.usessl`](#)
- [付録 C.2.6 `hdc.common.http.serverPort`](#)
- [付録 C.2.9 `hdc.common.https.serverPort`](#)
- [付録 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：
 <Hitachi Command Suite のインストールフォルダ>%DeviceManager
 %HiCommandServer%config%migration.properties
- Linux の場合：
 <Hitachi Command Suite 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 :

[シュレディング] 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 :

[シュレディング] 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、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.13.5 migration.volumeDelete.defaultValue

[データマイグレーション] ウィザードを起動した際の [削除] 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 :

[削除] 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 :

[削除] チェックボックスが選択されていない状態になります。

デフォルト : false

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 :

```
<Hitachi Command Suite のインストールフォルダ>%DeviceManager  
%HiCommandServer%config\tuningmanager.properties
```

- Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/config/  
tuningmanager.properties
```

A.14.1 htnm.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 htnm.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 htm.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、「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。

A.14.5 htm.server.n.port

アクセスする Tuning Manager サーバの HBase 64 Storage Mgmt Web Service のポート番号を指定します。

htm.server.n.protocol に http を指定した場合は、非 SSL 用の HBase 64 Storage Mgmt Web Service のポート番号を指定します。htm.server.n.protocol に https を指定した場合は、SSL 用の HBase 64 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、「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。

関連参照

- [付録 A.14.4 htm.server.n.protocol](#)

A.14.6 htm.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。

デスクトップアプリケーションの GUI (Adobe AIR 環境で動作する GUI) を使用する場合、`htnm.flashMode` プロパティの値は無視されます。この場合、履歴レポートのチャートは画像 (PNG 形式) で表示します。

デフォルト : `true`

A.14.7 `hdvm.analytics.report.pdf.showLogo`

[分析] タブでエクスポートする PDF ファイルの表紙および目次に、ロゴやコピーライトなどを出力するかどうかを指定します。

次の項目を出力する場合は `true`、出力しない場合は `false` を指定します。

- 表紙
 - 「Hitachi」のロゴ
 - コピーライト
 - 製品名称の文頭の「Hitachi」
- 目次
 - 製品名称の文頭の「Hitachi」

デフォルト : `true`

A.14.8 `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.14.9 `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.14.10 `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.14.11 htm.agent.use.cipher.type

Tuning Manager Agent REST API コンポーネントへアクセスするときに使用する暗号方式を指定します。

指定方法は次のとおりです。

- SUITEB128 : 楕円曲線暗号 (ECC) を利用するときに設定します。Oracle JDK を使用する場合はこちらを設定してください。
- SUITEB192 : 楕円曲線暗号 (ECC) を利用するときに設定します。
- RSA : RSA を利用するときに設定します。

デフォルト : RSA

A.15 [レプリケーション] タブに関するプロパティ (replication.properties ファイル)

[レプリケーション] タブ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 :
<Hitachi Command Suite のインストールフォルダ>%DeviceManager
%HiCommandServer%config%replication.properties
- Linux の場合 :
<Hitachi Command Suite 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

正サイトと副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。Replication Manager のイベントログについては、マニュアル「Hitachi Command Suite Replication Manager ユーザーズガイド」を参照してください。

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、Device Manager GUI/CLI で構成情報を収集してください。

デフォルト：true

関連参照

- [付録 A.15.2 `server.dispatcher.daemon.replication.config.updateInterval`](#)
- [付録 A.15.3 `server.dispatcher.daemon.replication.config.offset`](#)
- [付録 A.15.4 `server.dispatcher.daemon.replication.config.minute`](#)

A.15.2 `server.dispatcher.daemon.replication.config.updateInterval`

正サイトと副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）

関連参照

- [付録 A.15.1 `server.dispatcher.daemon.replication.config.doUpdate`](#)

A.15.3 `server.dispatcher.daemon.replication.config.offset`

正サイトと副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間を指定します。

`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間を指定します。

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

関連参照

- [付録 A.15.1 server.dispatcher.daemon.replication.config.doUpdate](#)
- [付録 A.15.2 server.dispatcher.daemon.replication.config.updateInterval](#)

A.15.4 server.dispatcher.daemon.replication.config.minute

正サイトと副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）

関連参照

- [付録 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

関連参照

- [付録 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 (`rpmlib.properties` ファイル)

Replication Manager との連携に関するプロパティは、`rpmlib.properties` ファイルに含まれています。

- Windows の場合 :
`<Hitachi Command Suite のインストールフォルダ>%DeviceManager
%HiCommandServer%config%rpmlib.properties`
- Linux の場合 :

<Hitachi Command Suite 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。

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は、マニュアル「Hitachi Command Suite Replication Manager システム構成ガイド」を参照してください。

デフォルト：25200

A.17 CIM/WBEM 機能に関するプロパティ (jservice.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、jservice.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。

- jservice.properties ファイルの格納先
 - Windows の場合：
<Hitachi Command Suite のインストールフォルダ>%DeviceManager
%HiCommandServer%config
 - Linux の場合：
<Hitachi Command Suite 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：
<Hitachi Command Suite のインストールフォルダ>%DeviceManager
%HiCommandServer%wsi%jservice%jservice%bin
 - Linux の場合：
<Hitachi Command Suite のインストールディレクトリ>/HiCommandServer/wsi/
server/jservice/bin

A.17.1 com.wbemsolutions.jservice.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、jservice.properties ファイルに指定します。

com.wbemsolutions.jservice.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.jservice.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。

関連参照

- [付録 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。

関連参照

- [付録 A.2.14 server.cim.https.port](#)
- [付録 A.8.8 Ciphers](#)

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 のデータベースに関するプロパティ (database.properties ファイル)
- B.4 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.5 Tiered Storage Manager のログ出力に関するプロパティ (logger.properties ファイル)
- B.6 Tiered Storage Manager のセキュリティに関するプロパティ (server.properties ファイル)

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 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 140 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。
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。
server.properties ファイル	Tiered Storage Manager のセキュリティ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。

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：

```
<Hitachi Command Suite のインストールフォルダ>%TieredStorageManager  
%template
```

Linux の場合：

```
<Hitachi Command Suite のインストールディレクトリ>/TieredStorageManager/  
template
```

前提条件

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

操作手順

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

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

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：
＜Hitachi Command Suite のインストールフォルダ＞¥TieredStorageManager¥conf¥server.properties
- Linux の場合：
＜Hitachi Command Suite のインストールディレクトリ＞/TieredStorageManager/conf/server.properties

B.2.1 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場合は、Tiered Storage Manager CLI の `htsmcli.properties` ファイルの `htsmserver.location` プロパティも見直してください。

関連タスク

- [5.5.10 Tiered Storage Manager CLI の実行マシンでの SSL/TLS の有効化](#)

関連参照

- [付録 B.6.1 server.rmi.secure](#)

B.2.2 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場合は、Tiered Storage Manager CLI の `htsmcli.properties` ファイルの `htsmserver.location` プロパティも見直してください。

関連タスク

- [5.5.10 Tiered Storage Manager CLI の実行マシンでの SSL/TLS の有効化](#)

関連参照

- [付録 B.6.1 server.rmi.secure](#)

B.2.3 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。

`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.2.4 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.2.5 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：htsmsserver

B.2.6 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

関連参照

- [付録 B.2.5 server.mail.from](#)

B.2.7 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.2.8 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。

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.2.9 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.2.10 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.2.11 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の最大値を指定します。

指定できる値の範囲は、1～64です。

デフォルト：8



メモ マイグレーションペアは、指定した数に達するまで1ペアずつストレージシステムに登録され、実行されます。しかし、次のマイグレーションペアをストレージシステムに登録するまでの間に、以前のマイグレーションペアの実行が完了する場合（例えば、小容量のボリュームのマイグレーションペアが含まれる場合）は、同時に実行されているマイグレーションペアの数が指定された数まで達しないことがあります。

B.2.12 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。

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.2.13 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。

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.2.14 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。

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.2.15

server.migrationPlan.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。

B.2.16 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：
＜Hitachi Command Suite のインストールフォルダ＞¥TieredStorageManager¥conf¥database.properties
- Linux の場合：
＜Hitachi Command Suite のインストールディレクトリ＞/TieredStorageManager/conf/database.properties

B.3.1 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。

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.4 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 :
 <Hitachi Command Suite のインストールフォルダ>%TieredStorageManager%conf
 %devicemanager.properties
- Linux の場合 :
 <Hitachi Command Suite のインストールディレクトリ>/TieredStorageManager/
 conf/devicemanager.properties

B.4.1 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.4.2 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

関連参照

- [付録 A.2.2 server.http.port](#)

B.4.3 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.4.4 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

関連参照

- [付録 A.2.4 server.rmi.port](#)

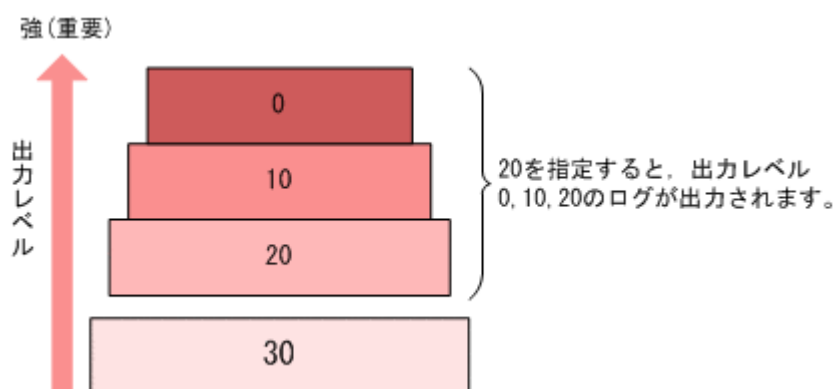
B.5 Tiered Storage Manager のログ出力に関するプロパティ (logger.properties ファイル)

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：
 <Hitachi Command Suite のインストールフォルダ>%TieredStorageManager%conf
 ¥logger.properties
- Linux の場合：
 <Hitachi Command Suite のインストールディレクトリ>/TieredStorageManager/
 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 62 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.5.1 logger.messageLogLevel

HTSMServerMessage`n`.log ファイルおよび HTSMGuiMessage`n`.log ファイルに出力されるログの出力レベルを指定します。

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 141 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。
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.5.2 logger.tracelogLevel

HTSMServerTracen.log ファイルおよび HTSMGuiTracen.log ファイルに出力されるログの出力レベルを指定します。

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 142 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.5.3 logger.syslogLevel

Tiered Storage Manager が出力するイベントログまたは syslog に出力されるログの出力レベルを指定します。

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。

デフォルト：0

B.5.4 logger.serverMessageFileCount

HTSMServerMessageN.log ファイル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

関連参照

- 付録 B.5.8 logger.serverMessageMaxFileSize

B.5.5 logger.serverTraceFileCount

HTSMServerTrace n .log ファイル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

関連参照

- [付録 B.5.9 logger.serverTraceMaxFileSize](#)

B.5.6 logger.guiMessageFileCount

HTSMGuiMessage n .log ファイル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

関連参照

- [付録 B.5.10 logger.guiMessageMaxFileSize](#)

B.5.7 logger.guiTraceFileCount

HTSMGuiTrace n .log ファイル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

関連参照

- [付録 B.5.11 logger.guiTraceMaxFileSize](#)

B.5.8 logger.serverMessageMaxFileSize

HTSMServerMessage`n`.log ファイル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.5.9 logger.serverTraceMaxFileSize

HTSMServerTrace`n`.log ファイル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.5.10 logger.guiMessageMaxFileSize

HTSMGuiMessage`n`.log ファイル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.5.11 logger.guiTraceMaxFileSize

HTSMGuiTrace`n`.log ファイル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 Tiered Storage Manager のセキュリティに関するプロパティ (server.properties ファイル)

Tiered Storage Manager のセキュリティ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 :
<Hitachi Command Suite のインストールフォルダ>%TieredStorageManager%conf
%server.properties
- Linux の場合 :
<Hitachi Command Suite のインストールディレクトリ>/TieredStorageManager/
conf/server.properties

B.6.1 server.rmi.secure

Tiered Storage Manager サーバと管理クライアント (Tiered Storage Manager CLI) 間を SSL で通信するかどうかを指定します。

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。署名アルゴリズムは MD5withRSA です。

3 : SSL で通信します。署名アルゴリズムは SHA256withRSA です。

4 : 署名アルゴリズムは SHA256withRSA 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 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



注意

使用する暗号方式をセキュリティポリシーに合わせて設定できるため、SSL で通信する場合は 4 を指定することを推奨します。

関連参照

- [付録 B.6.2 server.rmi.security.enabledCipherSuites](#)

B.6.2 server.rmi.security.enabledCipherSuites

Tiered Storage Manager サーバと管理クライアント (Tiered Storage Manager CLI) 間を SSL/TLS 通信する場合、暗号方式 (Cipher Suite) をコンマ (,) で区切って指定します。

このプロパティは、`server.properties` ファイルの `server.rmi.secure` プロパティに 4 が指定されている場合にだけ有効です。

指定できる暗号方式は次のとおりです。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

デフォルト : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384,

TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256

関連参照

- [付録 B.6.1 server.rmi.secure](#)

B.6.3 server.rmi.security.protocols

Tiered Storage Manager サーバと管理クライアント (Tiered Storage Manager CLI) 間を SSL/TLS 通信する場合、プロトコルをコンマ (,) で区切って指定します。

指定できるプロトコルは次のとおりです。

- TLSv1
- TLSv1.1
- TLSv1.2

指定したプロトコルのうち、暗号強度の高いプロトコルから使用されます。

デフォルト : TLSv1, TLSv1.1, TLSv1.2

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.5 Host Data Collector のセキュリティに関するプロパティ (hdcbase.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 143 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。
hdcbase.properties ファイル	Host Data Collector のセキュリティ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。

前提条件

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

操作手順

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。

関連タスク

- [9.2.2 Host Data Collector のサービスの起動](#)
- [9.2.3 Host Data Collector のサービスの停止](#)

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
- 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



メモ

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
-

関連タスク

- [2.4.1 Host Data Collector](#) でのサービスの例外登録（非 SSL 通信用）

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



メモ

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
-

関連タスク

- [2.4.1 Host Data Collector](#) でのサービスの例外登録（非 SSL 通信用）

関連参照

- [付録 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



メモ

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)

関連タスク

- [2.4.1 Host Data Collector](#) でのサービスの例外登録 (非 SSL 通信用)

関連参照

- [付録 A.12.2 hdc.rmiregistry](#)
- [付録 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



メモ

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)

関連タスク

- [2.4.1 Host Data Collector](#) でのサービスの例外登録 (非 SSL 通信用)

関連参照

- [付録 A.12.3 hdc.rmiserver](#)
- [付録 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



メモ

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)

関連タスク

- [2.4.1 Host Data Collector](#) でのサービスの例外登録 (非 SSL 通信用)

関連参照

- [付録 A.12.4 hdc.classloader](#)
- [付録 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



メモ

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)

関連タスク

- [2.4.2 Host Data Collector](#) でのサービスの例外登録 (SSL 通信用)

関連参照

- [付録 A.12.2 hdc.rmiregistry](#)
- [付録 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



メモ

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)

関連タスク

- [2.4.2 Host Data Collector](#) でのサービスの例外登録 (SSL 通信用)

関連参照

- [付録 A.12.3 hdc.rmiserver](#)
- [付録 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。



メモ

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)

関連タスク

- [2.4.2 Host Data Collector](#) でのサービスの例外登録 (SSL 通信用)

関連参照

- [付録 A.12.4 hdc.classloader](#)
- [付録 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。

関連参照

- [付録 A.12.2 hdc.rmiregistry](#)
- [付録 A.12.3 hdc.rmiserver](#)
- [付録 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 144 `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
	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

関連参照

- [付録 C.2.4 `hdc.common.rmi.registryPort`](#)
- [付録 C.2.5 `hdc.common.rmi.serverPort`](#)
- [付録 C.2.6 `hdc.common.http.serverPort`](#)
- [付録 C.2.7 `hdc.common.rmi.ssl.registryPort`](#)
- [付録 C.2.8 `hdc.common.rmi.ssl.serverPort`](#)
- [付録 C.2.9 `hdc.common.https.serverPort`](#)

C.2.14 hdc.ssl.esx.certCheck

仮想化サーバと Host Data Collector 間での SSL 通信に、認証局で署名されたサーバ証明書を使用する場合、証明書の有効性をチェックするかどうかを指定します。

Host Data Collector で実行できる、証明書の有効性のチェックは、次のとおりです。

- サーバ証明書が有効期限内かどうかの確認

- サーバ証明書のチェーンの検証
- サーバ証明書のサブジェクトの別名 (Subject Alternative Names) の確認

証明書の有効性をチェックする場合は 1 を、証明書の有効性をチェックしない場合は 0 を指定してください。

デフォルト : 0

C.2.15 hdc.common.bindServerIPAddress

Host Data Collector が RMI 通信を受け付ける IP アドレスを指定します。

Host Data Collector と通信を行う Device Manager サーバが同一ホストにインストールされている構成でこのプロパティにループバックアドレスを指定することで、Host Data Collector への RMI 通信を実行できるのは同一ホストからのみとなります。

外部ホストからのサービス妨害攻撃やバッファオーバーフローを狙った攻撃を防ぐのに役立ちます。

デフォルト値 : なし※

注※ 指定されていない場合、hdc.service.rmi.registryIPAddress プロパティで指定した IP アドレスで通信を行います。



注意

- このプロパティは非 SSL 通信だけを対象とします。このプロパティを使用する際は、SSL の設定は非 SSL のみ (hdc.ssl.secure=1) としてください。
このプロパティにループバックアドレスを指定した場合、ローカル通信だけに制限されるため、非 SSL 通信であっても外部ホストからの攻撃を防ぐことができます。
- Host Data Collector を Device Manager サーバとは別のホストにインストールしている場合、または SSL 通信が必要な場合は、hdc.common.allowIPAddressList プロパティを使用してください。
- このプロパティを指定した場合、hdc.service.rmi.registryIPAddress プロパティの指定値は無効となります。
- このプロパティを指定する場合、Device Manager サーバの hostdatacollectors.properties ファイルに記載する hdc.rmiregistry プロパティ、hdc.rmiserver プロパティ、hdc.classloader プロパティの IP アドレスも同じ値にしてください。

関連参照

- [付録 A.12.2 hdc.rmiregistry](#)
- [付録 A.12.3 hdc.rmiserver](#)
- [付録 A.12.4 hdc.classloader](#)
- [付録 C.2.10 hdc.service.rmi.registryIPAddress](#)
- [付録 C.2.13 hdc.ssl.secure](#)
- [付録 C.2.16 hdc.common.allowIPAddressList](#)

C.2.16 hdc.common.allowIPAddressList

Host Data Collector の RMI 通信への接続を許可する Device Manager サーバの IPv4 および IPv6 の IP アドレスを指定します。

この設定は、接続を許可する 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狙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。

```
hdc.common.allowIPAddressList=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。

```
hdc.common.allowIPAddressList=2001::203:baff:fe36:109a,2001::203:baff:fe5b:7bac
```

デフォルト値：なし (すべての IP アドレスが接続できます)

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
- 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 145 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

関連参照

- [付録 C.3.2 logger.trace.maxFileSize](#)

C.3.4 logger.ioTRACE.maxFileSize

Host Data Collector の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

関連参照

- [付録 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

- 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 :

なし (Host Data Collector に同梱された Java の実行環境が使用されます)

C.5 Host Data Collector のセキュリティに関するプロパティ (hdcbase.properties ファイル)

セキュリティ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`
- 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.5.1 hdc.ssl.ciphers

Device Manager サーバと Host Data Collector 間を SSL/TLS で通信する場合、暗号方式 (Cipher Suite) をコンマ (,) で区切って指定します。

使用できる暗号方式は次のとおりです。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

デフォルト :

`TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256`

C.5.2 hdc.ssl.esx.enabledTLSv1

仮想化サーバと Host Data Collector 間を SSL/TLS 通信する場合に、TLS バージョン 1.0 の使用を許容するかどうかを指定します。

指定できる値は、0 または 1 です。

0 : TLS バージョン 1.0 の使用を抑止します。

1 : TLS バージョン 1.0 の使用を許容します。

デフォルト : 1



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.7 Device Manager エージェントが接続するコマンドデバイスに関するプロパティファイル (rgcmddev.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 146 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。
rgcmddev.properties ファイル	Device Manager エージェントが接続するコマンドデバイス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。

前提条件

Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン

操作手順

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. 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。
3. 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。

関連参照

- [11.2.7 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
- Linux の場合
 < Device Manager エージェントのインストールディレクトリ > /mod/hrpm/config/agent.properties
- Solaris 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



メモ

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 RAID Manager XP 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 RAID Manager XP 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 RAID Manager XP 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の上限値を指定します。

1～2047 の値を設定できます。ほかの RAID Manager または RAID Manager XP 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：2047

監視用 HORCM ファイルのインスタンス番号は、RAID Manager または XP7 RAID Manager のバージョンによって異なります。

RAID Manager のバージョンが 01-32-03/XX 以降、または XP7 RAID Manager のバージョンが 01.32.XX 以降の場合

このプロパティと agent.rm.horcmlInstance プロパティの値から算出した次の範囲のインスタンス番号が使用されます。デフォルトでは、1948～2047 です。

インスタンス番号の上限値：<このプロパティで指定した値>

インスタンス番号の下限値：<このプロパティで指定した値>-<agent.rm.horcmlInstance プロパティで指定した値>+1

RAID Manager のバージョンが 01-32-03/XX より前、または XP7 RAID Manager のバージョンが 01.32.XX より前の場合

このプロパティで指定した値、および<このプロパティで指定した値>-1 のインスタンス番号が使用されます。デフォルトでは、2046 と 2047 です。

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。



ヒント

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。

関連参照

- [付録 D.2.6 agent.rm.horcmlInstance](#)
- [付録 D.6.21 server.agent.rm.temporaryInstance](#)

D.2.5 agent.rm.horcmlService

監視用 HORCM ファイルの UDP ポート番号の上限値を指定します。

2～65535 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：54323

監視用 HORCM ファイルのポート番号は、RAID Manager または XP7 RAID Manager のバージョンによって異なります。

RAID Manager のバージョンが 01-32-03/XX 以降、または XP7 RAID Manager のバージョンが 01.32.XX 以降の場合

このプロパティと agent.rm.horcmlInstance プロパティの値から算出した次の範囲のポート番号が使用されます。デフォルトでは、54224～54323 です。

ポート番号の上限値：<このプロパティで指定した値>

ポート番号の下限値: <このプロパティで指定した値> - <agent.rm.horcmRange プロパティで指定した値> + 1

RAID Manager のバージョンが 01-32-03/XX より前、または XP7 RAID Manager のバージョンが 01.32.XX より前の場合

このプロパティで指定した値、および <このプロパティで指定した値> - 1 のポート番号が使用されます。デフォルトでは、54322 と 54323 です。

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。



ヒント

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。

関連参照

- [付録 D.2.6 agent.rm.horcmRange](#)
- [付録 D.6.22 server.agent.rm.temporaryPort](#)

D.2.6 agent.rm.horcmRange

監視用 HORCM ファイルのインスタンス番号、および UDP ポート番号の数を指定します。

このプロパティは、RAID Manager のバージョンが 01-32-03/XX 以降、または XP7 RAID Manager のバージョンが 01.32.XX 以降の場合にだけ有効です。

10~1000 の値を設定できます。設定する値は、次の計算式で算出した値よりも大きな値を設定してください。

$2 \times (2 + \text{仮想ストレージマシンを構築するストレージシステムの数})$

デフォルト : 100

関連参照

- [付録 D.2.4 agent.rm.horcmInstance](#)
- [付録 D.2.5 agent.rm.horcmService](#)

D.2.7 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.2.8 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。

$\text{<出力されるログファイルの情報量 (MB/週間)> = 0.75 \times \text{<コピーペア数>} + 4$

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。

関連参照

- [付録 D.2.9 agent.logger.MaxFileSize](#)

D.2.9 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。

$\text{<出力されるログファイルの情報量 (MB/週間)> = 0.75 \times \text{<コピーペア数>} + 4$

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。

関連参照

- [付録 D.2.8 agent.logger.MaxBackupIndex](#)

D.2.10 agent.rm.lunPathCheck

監視用 HORCM インスタンスが管理するボリュームの LUN パスの構成変更を監視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、LUN パスの構成変更を監視します。false の場合、LUN パスの構成を変更したときは、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。

デフォルト：false

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`

- Linux の場合
`< Device Manager エージェントのインストールディレクトリ >/util/bin/hldutil.properties`
- Solaris 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

hldutil 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。

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`
- Linux の場合
`< Device Manager エージェントのインストールディレクトリ >/agent/config/logger.properties`
- Solaris 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`



メモ

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%`

Linux の場合

< Device Manager エージェントのインストールディレクトリ > /agent/logs/

Solaris 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。

<出力されるログファイルの情報量 (MB/週間) > = 0.8 × <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。

関連参照

- [付録 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。

<出力されるログファイルの情報量 (MB/週間) > = 0.8 × <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。

関連参照

- [付録 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
- Linux の場合
 <Device Manager エージェントのインストールディレクトリ>/agent/config/
 server.properties
- Solaris 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。

指定するホスト名は、IP アドレスへの名前解決ができることを事前に確認してください。

デフォルト：localhost



注意

次の場合、Device Manager の管理対象ホストに変更前と変更後のホストが両方登録されているときは、変更前のホストを削除してください。

- このプロパティの値を変更してから Device Manager エージェントのサービスを再起動した場合
 - このプロパティの値を変更している環境で、Device Manager エージェントをバージョン 8.5.0 以降にアップグレードインストールした場合
-

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。

IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を指定できます。

IPv4 アドレスを指定した場合は、指定した IPv4 アドレスと、同一 NIC に設定された IPv6 アドレス^{*1}の両方を通知します。IPv6 アドレスを指定した場合は、指定した IPv6 アドレスと、同一 NIC に設定された IPv4 アドレス^{*1}の両方を通知します。

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 RAID Manager XP 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 RAID Manager XP と併用する場合は、指定したアドレスで RAID Manager または RAID Manager XP 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^{*2}

注^{*1} Device Manager エージェントが取得した 1 つ目の IP アドレスを通知します。

注^{*2} 指定されていない場合、Device Manager エージェントが取得した IPv4 アドレスおよび IPv6 アドレスを通知します。IPv4 アドレスおよび IPv6 アドレスが複数ある場合は、Device Manager エージェントが取得した 1 つ目の IP アドレスを通知します。

関連参照

- [付録 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 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)

関連参照

- [付録 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。

関連概念

- [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](#)
- [11.2.4 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 または Solaris の場合
 - ホストの OS が Linux で、CIM/WBEM 機能を利用して 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ホストの OS が Red Hat Enterprise Linux 7 以降、Oracle Linux 7 以降、または SUSE Linux Enterprise Server 12 以降のときは、64 ビット用の Java の実行環境を使用してください。
 - Dynamic Link Manager がホストにインストールされているときに指定できる Java の実行環境については、Dynamic Link Manager のマニュアルを参照してください。
-

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狙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: 262144

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狙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 (Device Manager サーバと非 SSL で通信している場合) または `server.https.port` プロパティ (Device Manager サーバと SSL で通信している場合) で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

関連参照

- [付録 A.2.2 server.http.port](#)
- [付録 A.2.3 server.https.port](#)

D.6.15 server.agent.rm.centralizePairConfiguration

コピーペアを管理するとき、各ホストで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

各ホスト (ペア管理サーバ) でコピーペアを管理する構成の場合に指定します。

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。

デフォルト : disable

関連概念

- [1.15 コピーペアを管理する場合のシステム構成 \(一括管理構成以外\)](#)

関連参照

- [1.14 コピーペアを管理する場合のシステム構成 \(一括管理構成\)](#)

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、VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、VSP Fx00 モデル、Virtual Storage Platform、Universal Storage Platform V/VM、Hitachi USP

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 RAID Manager XP 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 RAID Manager XP 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 RAID Manager XP 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 RAID Manager XP 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 RAID Manager XP 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 RAID Manager XP 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.rmtemporaryInstance

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.rmtemporaryPort

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、次の場合は、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。

- ・ メインフレームボリュームのコピーペアを作成する場合
- ・ VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデルで仮想ストレージマシンのボリュームを使用してコピーペアを作成する場合

- VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500 または VSP Gx00 モデルで global-active device のコピーペアを作成する場合

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に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 147 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 XP7 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 XP7 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



メモ

VMware Tools のサービスまたはプロセスが起動している状態で、Device Manager エージェントを仮想マシンにインストールしたとき、server.agent.rm.ignorePairStatus プロパティの値は true に変更されます。

D.6.26 server.agent.rm.horcmSource

RAID Manager または RAID Manager XP 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

関連タスク

- [11.4.12 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 RAID Manager XP 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.server.ssl.hdvm

Device Manager エージェントと 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。

デフォルト：false



メモ

true を指定し、かつ Device Manager エージェントの Java の実行環境を変更している場合は、使用する Java の実行環境のバージョンに応じた Java Cryptography Extension (JCE) の無制限強度の管轄ポリシーファイル (Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files) をダウンロードし、インストールする必要があります。

管轄ポリシーファイルは、Oracle 社または IBM 社の Web サイトからダウンロードしてください。インストール方法は、管轄ポリシーファイルに付属するドキュメントを参照してください。

D.6.29 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.6.30 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すぎると、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.6.31 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.6.32 server.agent.snapshotEvtwait.timeout

Copy-on-Write Snapshot もしくは Thin Image ペアを作成、リシンク、またはリストアする際に、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.6.33 server.agent.rmcp.location

RAID Manager XP 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 XP 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 XP 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.7 Device Manager エージェントが接続するコマンドデバイスに関するプロパティファイル（rgcmddev.properties ファイル）

ストレージシステムが VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデル、VSP Fx00 モデル、Virtual Storage Platform、または HUS VM で、ストレージシステム内のリソースを分割している場合、rgcmddev.properties ファイルに、ストレージシステムのリソースグループ ID が 0（VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデルの場合は、デフォルトの仮想ストレージマシンのリソースプール）のコマンドデバイスを指定します。

- Windows の場合
 < Device Manager エージェントのインストールフォルダ > %mod%hdvm%config
 %rgcmddev.properties
- Linux の場合
 < Device Manager エージェントのインストールディレクトリ > /mod/hdvm/config/
 rgcmddev.properties
- Solaris または HP-UX の場合
 /opt/HDVM/HBaseAgent/mod/hdvm/config/rgcmddev.properties
- AIX の場合
 /usr/HDVM/HBaseAgent/mod/hdvm/config/rgcmddev.properties

コマンドデバイスを、次の形式で定義してください。同一装置内のリソースグループ ID が 0（VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500、VSP Gx00 モデルまたは VSP Fx00 モデルの場合は、デフォルトの仮想ストレージマシンのリソースプール）の複数のコマンドデバイスを定義した場合、いちばん下の行に定義されたコマンドデバイスだけが有効になります。

```
< RAID ID > . < シリアル番号 > . < LDEV 番号 >
```

RAID ID

ストレージシステムを、次の形式で指定します。

- R900 : VSP 5000 シリーズの場合
- HM90 : VSP E990 の場合
- R800 : VSP G1000、G1500 または VSP F1500 の場合
- HM82 : G100、G130、G150、G200、G350、G370 または VSP F350、F370 の場合
- HM84 : VSP G400、G600、G700 または VSP F400、F600、F700 の場合
- HM86 : VSP G800、G900 または VSP F800、F900 の場合
- R700 : Virtual Storage Platform の場合
- HM70 : HUS VM 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。VSP 5000 シリーズ、VSP G1000、G1500、VSP F1500 または Virtual Storage Platform の場合は 5 桁、VSP Gx00 モデル、VSP Fx00 モデルまたは HUS VM の場合はモデル名を含めて 6 桁で指定してください。

LDEV 番号

コマンドデバイスの CU:LDEV 番号を 16 進数で指定します。ストレージシステムのリソースグループ ID が 0 (VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルの場合は, デフォルトの仮想ストレージマシンのリソースプール) のコマンドデバイスを指定してください。

同一装置の複数の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, 構成定義ファイルの HORCM_CMD パラメーターには, 1 行に複数のコマンドデバイスを指定できます。1 行に複数のコマンドデバイスが指定されている場合, RAID Manager は先頭のコマンドデバイスから使用します。

Device Manager エージェントでは, 装置内のすべてのリソースに対する操作を可能とするため, ストレージシステムのリソースグループ ID が 0 (VSP 5000 シリーズ, VSP G1000, G1500, VSP F1500, VSP Gx00 モデルまたは VSP Fx00 モデルの場合は, デフォルトの仮想ストレージマシンのリソースプール) のコマンドデバイスを使用する必要があります。そのため, ペア管理サーバが複数のコマンドデバイスを認識している場合は, rgcmddev.properties ファイルで指定した LDEV 番号のコマンドデバイスが HORCM_CMD パラメーターの先頭に来るように, Device Manager エージェントが並び替えを行います。

(例)

VSP G1000 (シリアル番号 : 310051) のコマンドデバイス (PhysicalDrive1 (LDEV 番号 : 00:01) と PhysicalDrive2 (LDEV 番号 : 00:02)) がペア管理サーバで認識されている場合の例を示します。

通常, PhysicalDrive 番号やデバイスファイル名を基に, HORCM_CMD パラメーターは次のように定義されます。

```
HORCM_CMD
#dev_name          dev_name          dev_name
#UnitID 0 (LDEV# 00:01 00:02 Serial# 310051)
¥¥.¥PhysicalDrive1 ¥¥.¥PhysicalDrive2
```

rgcmddev.properties ファイルに 「R800.310051.00:02」と指定した場合, LDEV 番号 : 00:02 のコマンドデバイスが HORCM_CMD パラメーターの先頭に定義されます。

```
HORCM_CMD
#dev_name          dev_name          dev_name
#UnitID 0 (LDEV# 00:02 00:01 Serial# 310051)
¥¥.¥PhysicalDrive2 ¥¥.¥PhysicalDrive1
```



管理クライアントに関するセキュリティ設定

ここでは、管理クライアントに関するセキュリティ設定について説明します。

- E.1 警告バナーとは
- E.2 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

E.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。

E.1.1 警告バナーに表示するメッセージの条件

hcmds64banner 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。

E.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、hcmds64banner コマンドを実行して登録します。

前提条件

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

操作手順

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 のインストールフォルダ > ¥Base64 ¥sample ¥resource
- Linux の場合：
< Hitachi Command Suite のインストールディレクトリ > /Base64/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。<br>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. `hcmds64banner` 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 のインストールフォルダ>%Base64%bin%hcmds64banner /  
add /file <ファイル名> [/locale <ロケール名>]
```

• Linux の場合 :

```
<Hitachi Command Suite のインストールディレクトリ>/Base64/bin/  
hcmds64banner -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。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。



メモ 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、`hcmds64banner` コマンドを実行すると、上書き更新されます。



ヒント

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
 - `hcmds64banner` 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。
-

操作結果

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せん。

E.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 `hcms64banner` コマンドを実行します。

前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- 次の情報の確認
 - 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)

操作手順

1. `hcms64banner` コマンドを実行します。

- Windows の場合 :
< Hitachi Command Suite のインストールフォルダ > \Base64\bin\hcms64banner / delete [/locale <ロケール名 >]
- Linux の場合 :
< Hitachi Command Suite のインストールディレクトリ > /Base64/bin/hcms64banner -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。



ヒント

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
 - `hcms64banner` 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。

E.2 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、`user_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。

前提条件

次の情報の確認

- 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)

操作手順

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, user_httpsd.conf ファイルの最終行に登録します。

user_httpsd.conf ファイルの格納先

- Windows の場合 :
< Hitachi Command Suite のインストールフォルダ > \Base64\uCPSB\httpsd\conf\user_httpsd.conf
- Linux の場合 :
< Hitachi Command Suite のインストールディレクトリ > /Base64/uCPSB/httpsd/conf/user_httpsd.conf

user_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。

user_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 user_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。

関連タスク

- [9.1.2 Hitachi Command Suite のサービスの起動](#)
- [9.1.3 Hitachi Command Suite のサービスの停止](#)

関連参照

- [付録 A.8.1 server.http.security.clientIP](#)
- [付録 A.8.2 server.http.security.clientIPv6](#)

コピーペア定義の移行

ここでは、構成定義ファイルで管理されるコピーペア定義をストレージシステム上のデバイスグループ定義に移行する方法について説明します。

- F.1 コピーペア定義の移行とは
- F.2 コピーペア定義を移行するための前提条件
- F.3 コピーペア定義をデバイスグループ定義に移行する
- F.4 ペア定義移行コマンドで使用するプロパティ

F.1 コピーペア定義の移行とは

構成定義ファイルで管理されているコピーペア定義を、ストレージシステム上のデバイスグループ定義に移行します。

構成定義ファイルを利用してコピーペアを管理している場合、ペア管理サーバ上にある構成定義ファイルの情報が消失したり、ペア管理サーバが使用できなくなったりして、コピーペアを管理できなくなるおそれがあります。この状況を回避するには、構成定義ファイルにコピーペアを定義するのではなく、ストレージシステム上でコピーペアの実体と定義とを一元管理することが必要です。デバイスグループを用いたコピーペア定義により、ストレージシステム上にコピーペア定義を持たせられます。

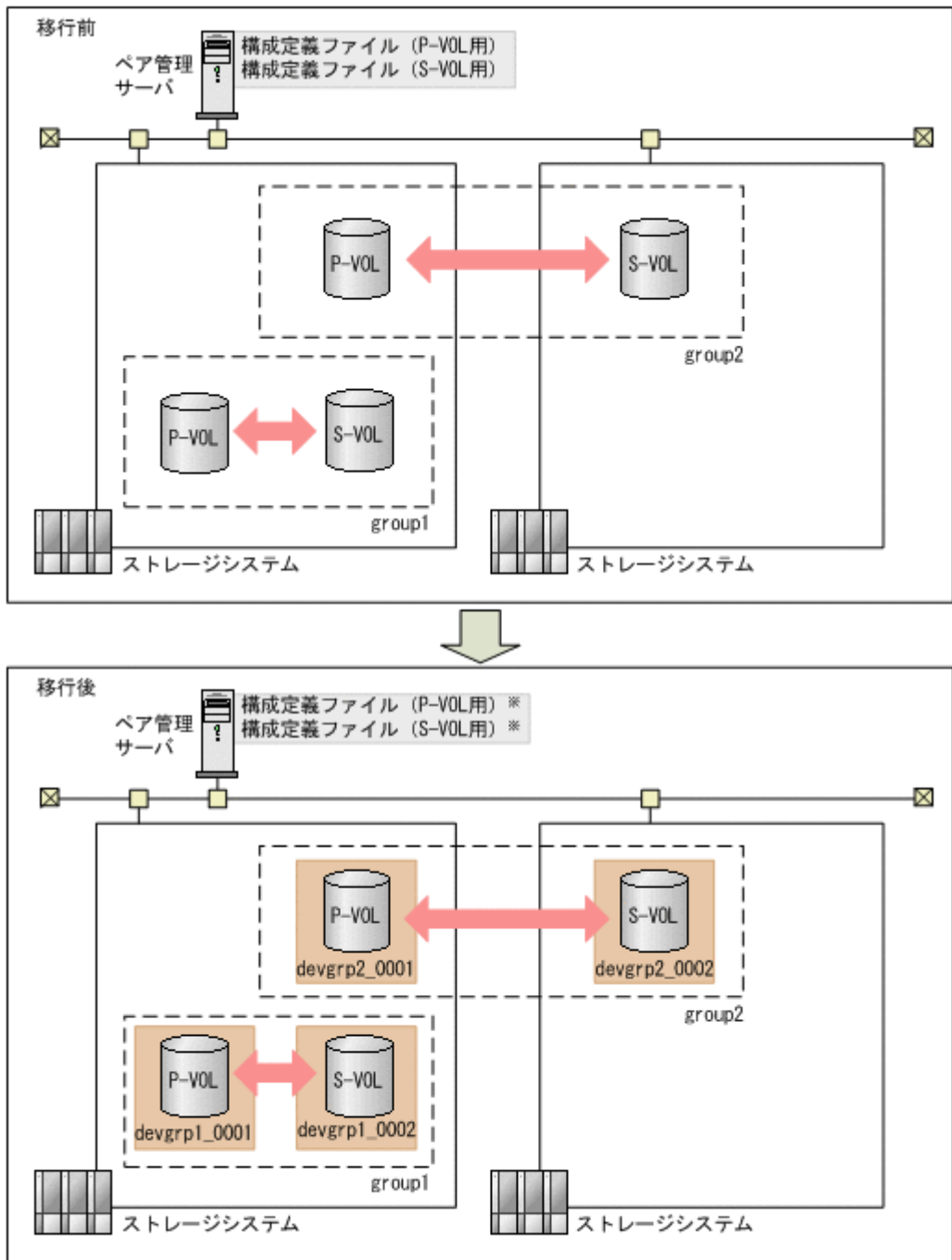
Device Manager , Replication Manager または RAID Manager を利用していたユーザーが、デバイスグループを用いてコピーペアを管理している Hitachi Command Suite REST API を利用したい場合、コピーペア定義をデバイスグループ定義に移行する必要があります。

コピーペア定義をデバイスグループ定義に移行するには、構成定義ファイルが格納されているペア管理サーバでペア定義移行コマンド (PairCfgMigration) を実行します。ペア定義移行コマンドを実行すると、移行元の構成定義ファイルからコピーペア情報を取得し、ストレージシステム上にデバイスグループおよびコピーグループを作成します。

移行後のデバイスグループ定義のコピーグループを操作するために、HORCM_LDEVG を記載した構成定義ファイルも作成できます。

ペア定義を移行する場合のシステム構成例を次に示します。

図 63 ペア定義を移行する場合のシステム構成例



デバイスグループ名は、ペア定義移行コマンドの実行時に指定したプレフィックスによって決まります。移行後のコピーグループ名は、移行前の構成定義ファイルで定義されたコピーグループ名と同じです。

移行後の構成を次に示します。

表 148 デバイスグループ定義への移行後の構成

移行対象のコピーペア種別	移行後の構成
ShadowImage	<p>デバイスグループ</p> <p>ペア管理サーバ上に P-VOL 用, S-VOL 用両方の構成定義ファイルがある場合, P-VOL 用, S-VOL 用のデバイスグループが 1 つずつ作成されます。</p> <p>ペア管理サーバ上に P-VOL 用の構成定義ファイルだけがある場合, P-VOL 用, S-VOL 用のデバイスグループが 1 つずつ作成されます。</p> <p>S-VOL 用の構成定義ファイルがある別のペア管理サーバでペア定義移行コマンドを実行する必要はありません。</p> <p>コピーグループ</p> <p>1 つのコピーグループ定義に対して, 1 つのコピーグループが作成されます。</p>
TrueCopy Universal Replicator High Availability Manager global-active device	<p>デバイスグループ</p> <p>ペア管理サーバ上に P-VOL 用, S-VOL 用両方の構成定義ファイルがある場合, 正側のストレージシステムに P-VOL 用のデバイスグループが 1 つ, 副側のストレージシステムに S-VOL 用のデバイスグループが 1 つ作成されます。</p> <p>ペア管理サーバ上に P-VOL 用 (または S-VOL 用) の構成定義ファイルだけがある場合, 正側 (または副側) のストレージシステムに P-VOL 用 (または S-VOL 用) のデバイスグループが 1 つ作成されます。</p> <p>S-VOL 用 (または P-VOL 用) の構成定義ファイルがある別のペア管理サーバでも, ペア定義移行コマンドを実行してください。</p> <p>コピーグループ</p> <p>1 つのコピーグループ定義に対して, 正側のストレージシステムに P-VOL 用のコピーグループが 1 つ, 副側のストレージシステムに S-VOL 用のコピーグループが 1 つ作成されます。</p>



注意

コピーペア定義をデバイスグループ定義へ移行する場合, 次の点に注意してください。

- Replication Manager では, ペア定義移行コマンドの実行時に再作成したデバイスグループによる構成定義ファイルを利用してコピーペアを操作または参照できますが, コピーペアを作成できなくなります。
- [レプリケーション] タブまたは Device Manager CLI では, コピーペアを管理できなくなります。

F.2 コピーペア定義を移行するための前提条件

コピーペア定義を移行するために必要な条件について説明します。

ストレージシステム

デバイスグループを利用できる次のストレージシステムを対象としています。

- VSP 5000 シリーズ
- VSP G1000
- VSP G1500
- VSP F1500
- VSP Gx00 モデル
- VSP Fx00 モデル
- Virtual Storage Platform

- HUS VM

ペア管理サーバ

次の条件を満たす必要があります。

- ペア定義移行コマンドを実行するペア管理サーバに、JDK または JRE (1.5.0_22 以上) がインストールされていること
環境変数 PATH または paircfgmigration.properties ファイルに、Java の実行環境のインストール先が指定されている必要があります。
- ペア定義移行コマンドを実行するペア管理サーバに、RAID Manager または RAID Manager XP がインストールされていること
VSP 5000 シリーズの場合は、RAID Manager 01-50-03/XX 以降をインストールしてください。
VSP G1000, G1500, VSP F1500, VSP G100, G200, G400, G600, G800, VSP F400, F600, または VSP F800 の場合は、RAID Manager 01-32-03/01 以降、または XP7 RAID Manager 01.32.01 以降をインストールしてください。
VSP G150, G350, G370, G700, G900, VSP F350, F370, F700, または VSP F900 の場合は、RAID Manager 01-45-03/XX 以降をインストールしてください。
VSP G130 の場合は、RAID Manager 01-47-03/XX 以降をインストールしてください。

移行対象のコピーペア種別

移行対象のコピーペア種別は次のとおりです。

- ShadowImage
- TrueCopy
- Universal Replicator
- High Availability Manager
- global-active device

コピーペア種別が Copy-on-Write Snapshot および Thin Image の場合は、デバイスグループにコピーペア定義を移行できません。

移行対象の構成定義ファイル

移行対象の構成定義ファイルは、次の条件を満たす必要があります。

- paircfgmigration.properties ファイルの paircfgmigration.horcmFilePath プロパティで指定したディレクトリにあること
- 構成定義ファイルのファイル名が、horcmXX.conf であること
XX (インスタンス番号) は 0~4094 が対象になります。数値の先頭に 0 が付いている場合 (01, 001 など) は対象外になります。
- コピーペア定義 (HORCM_LDEV または HORCM_DEV) を含む構成定義情報が記載されていること
- RAID Manager のインスタンスが起動できること
- 構成定義ファイルに記載されているコピーペアが作成済みであること
- ShadowImage を定義した構成定義ファイルの場合、P-VOL 用の構成定義ファイルが存在すること
- ShadowImage を定義した構成定義ファイルの場合、1 つの構成定義ファイルに P-VOL と S-VOL の定義が混在していないこと
- MU 番号がコピーグループ内で一意であること

- MU 番号が 0 の場合、構成定義ファイルの MU# は次のように指定されていること
ShadowImage の場合 : 0
TrueCopy, Universal Replicator, High Availability Manager または global-active device の場合 : 指定なし
- ジャーナル ID がコピーグループ内で一意であること
- コピーペア定義が物理 ID で定義されていること

F.3 コピーペア定義をデバイスグループ定義に移行する

コピーペア定義をデバイスグループ定義に移行するには、ペア定義移行コマンド (PairCfgMigration) を実行します。

前提条件

- コマンドデバイスの認証モードが有効であること
- Administrator 権限 (Windows の場合) または root (UNIX の場合) でのログイン
- ストレージシステムに対してユーザー認証が完了していること
ペア管理サーバの OS が Windows の場合は、ペア定義移行コマンドの実行ユーザーでユーザー認証を行ってください。このユーザーにはストレージ管理者 (プロビジョニング) のロールが必要です。
- 移行対象の構成定義ファイルの RAID Manager インスタンスが停止状態であること

操作手順

1. 統合インストールメディアからペア定義移行コマンドのアーカイブファイルを取得して、ペア管理サーバの任意の場所に展開します。
アーカイブファイルは次の場所に格納されています。

Windows の場合 :

```
<DVD-ROM ドライブ>%AGENTS%MigCmd%Windows%PairCfgMigration.zip
```

UNIX の場合 :

```
<DVD-ROM のマウントディレクトリ>/AGENTS/MigCmd/Unix/  
PairCfgMigration.tar
```

2. 構成定義ファイルの格納先やデバイスグループ名のプレフィックスなどを、プロパティファイル (paircfgmigration.properties) に設定します。

プロパティファイルは、次の場所に格納されています。

Windows の場合 :

```
<アーカイブファイルの展開先フォルダ>%PairCfgMigration  
%paircfgmigration.properties
```

UNIX の場合 :

```
<アーカイブファイルの展開先ディレクトリ>/PairCfgMigration/  
paircfgmigration.properties
```

3. 次のコマンドを実行して、コピーペア定義を移行します。

Windows の場合 :

```
<アーカイブファイルの展開先フォルダ>%PairCfgMigration  
%PairCfgMigration.bat [/s]
```

UNIX の場合 :

<アーカイブファイルの展開先ディレクトリ>/PairCfgMigration/
PairCfgMigration.sh [-s]

オプション

s

ユーザーの応答を省略してコマンドを実行します。

s オプションを省略してコマンドを実行すると、対話形式で移行対象となる構成定義ファイルの一覧の表示や、移行処理の実行を指定できます。



メモ

- ペア定義移行コマンドの実行中は、操作対象のストレージシステムのリソースをほかのユーザーにロックされないようにしてください。
- ペア定義移行コマンドを使用して、構成定義ファイルに HORCM_VCMD 定義を記載した仮想 ID のコピーペア定義をデバイスグループ定義に移行した場合、その構成定義ファイル内のコピーペアの運用をするには、次のどちらかをする必要があります。
 - コピーペアを解除し、再度コピーペアを作成する。
移行後のデバイスグループによる構成定義ファイルと RAID Manager のコマンドを使用して、コピーペアを解除したあと、再度、同コピーペアを作成する。
 - コピーペアを解除しないで、ペア定義移行コマンドで移行する前の構成定義ファイルを再利用する。
ペア定義移行コマンドで作成したデバイスグループを RAID Manager のコマンドを使用して削除してから、ペア定義移行コマンドの実行時に保存された移行前の構成定義ファイル（拡張子が .old）の拡張子を取り除いたファイル名にリネームする。



ヒント

コピーペア定義の移行時に障害が発生した場合は、次のログファイルを取得してください。

ペア定義移行コマンドのログファイル

<アーカイブファイルの展開先ディレクトリ>/PairCfgMigration/log

RAID Manager のログファイル

<RAID Manager のインストール先>/HORCM/logXX

構成定義ファイル

構成定義ファイル配置先の horcmXX.conf

XX はインスタンス番号です。

関連参照

- [付録 F.4 ペア定義移行コマンドで使用するプロパティ](#)

F.4 ペア定義移行コマンドで使用するプロパティ

移行対象となる構成定義ファイルの格納先やデバイスグループ名のプレフィックスなどをプロパティファイル（paircfgmigration.properties）で設定します。

paircfgmigration.properties ファイルで設定するプロパティを次に示します。

表 149 paircfgmigration.properties ファイルのプロパティ

プロパティ名	説明
paircfgmigration.horcmFilePath	<p>移行対象の構成定義ファイルを格納しているディレクトリを絶対パスで指定します。プロパティは、半角文字で指定してください。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。</p> <p>このプロパティを指定していない場合は、次に示す格納場所が指定されたものとして動作します。</p> <p>Windows の場合 :</p> <p style="padding-left: 40px;">システムフォルダ (環境変数"%windir%"で表されるフォルダ)</p> <p>UNIX の場合 :</p> <p style="padding-left: 40px;">/etc ディレクトリ</p> <p>デフォルト : なし</p>
paircfgmigration.ignoreInstanceNumber	<p>paircfgmigration.horcmFilePath プロパティで指定したディレクトリにある構成定義ファイルのうち、移行対象外と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。プロパティは、半角文字で指定してください。複数指定する場合は、コンマ (,) で区切ります。</p> <p>例えば、ペア定義移行コマンドを複数回連続して実行する場合、すでに移行した構成定義ファイルを移行対象外として指定できます。移行が成功したインスタンス番号の一覧がペア定義移行コマンドのログファイルに出力されるので、その番号をこのプロパティにコピーして使用できます。</p> <p>(例)</p> <pre style="background-color: #f0f0f0; padding: 5px;">paircfgmigration.ignoreInstanceNumber=101,102,103</pre> <p>このプロパティで指定した構成定義ファイルは、ペア定義移行コマンドを対話形式で実行したときに表示される構成定義ファイルの一覧には表示されません。</p> <p>このプロパティを指定していない場合は、すべての構成定義ファイルが移行対象になります。</p> <p>デフォルト : なし</p>
paircfgmigration.rm.location	<p>RAID Manager または RAID Manager XP 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絶対パスで指定します。プロパティは、半角文字で指定してください。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。</p> <p>このプロパティを指定していない場合は、次のドライブまたはディレクトリが指定されたものとして動作します。</p> <p>Windows の場合 :</p> <p style="padding-left: 40px;"><PairCfgMigration コマンドの格納されているドライブ>/HORCM</p> <p>UNIX の場合 :</p> <p style="padding-left: 40px;">/HORCM</p> <p>デフォルト : なし</p>
paircfgmigration.deviceGroupPrefix	<p>新規に作成するデバイスグループ名のプレフィックスを 26 文字以内で指定します。ハイフン (-) で始まる文字列は指定できません。</p> <p>使用できる文字は次のとおりです。</p> <p>A~Z a~z 0~9 . @ _ : , -</p> <p>デバイスグループ名は、<プレフィックス>_xxxx (xxxx : 0001~9999 の 4 桁の番号) の形式で作成されます。</p> <p>このプロパティを指定していない場合は、プレフィックスに devgrp が指定されたものとして動作します。</p> <p>デフォルト : なし</p>

プロパティ名	説明
paircfgmigration.updateHorcmFile	<p>移行元の構成定義ファイルのペア定義情報をすべて移行した際、新たに作成したデバイスグループによる構成定義ファイルを再作成するかどうかを指定します。</p> <p>disable</p> <p>デバイスグループによる構成定義ファイルを再作成しません。</p> <p>enable</p> <p>デバイスグループによる構成定義ファイルを再作成します。移行元の構成定義ファイルの HORCM_DEV, HORCM_LDEV 定義を, HORCM_LDEVG 定義に書き換えます。そのほかの定義は変更されません。移行後の構成定義ファイルの名称は, 移行元の構成定義ファイルと同じです。移行元の構成定義ファイルには, .old の拡張子が付与されます。</p> <p>デフォルト: disable</p>
paircfgmigration.java.location	<p>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。プロパティは, 半角文字で指定してください。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。</p> <p>このプロパティを指定していない場合は, 環境変数 PATH に指定されている Java の実行環境のインストール先が使用されます。</p> <p>デフォルト: なし</p>



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。

- [G.1 関連マニュアル](#)
- [G.2 このマニュアルでの表記](#)
- [G.3 このマニュアルで使用している略語](#)
- [G.4 KB \(キロバイト\) などの単位表記について](#)

G.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 ユーザーズガイド* (3021-9-003)
- *Hitachi Command Suite CLI リファレンスガイド* (3021-9-004)
- *Hitachi Command Suite Tiered Storage Manager CLI リファレンスガイド* (3021-9-005)
- *Hitachi Command Suite インストールガイド* (3021-9-006)
- *Hitachi Command Suite メッセージ* (3021-9-011)
- *Hitachi Command Suite Mainframe Agent ユーザーズガイド* (3021-9-012)
- *Hitachi Command Suite Tuning Manager 運用管理ガイド* (3021-9-037)
- *Hitachi Command Suite Tuning Manager インストールガイド* (3021-9-038)
- *Hitachi Command Suite Tuning Manager ユーザーズガイド* (3021-9-039)
- *Hitachi Command Suite Tuning Manager - Agents* (3021-9-040)
- *Hitachi Command Suite Replication Manager ユーザーズガイド* (3021-9-064)
- *Hitachi Command Suite Replication Manager システム構成ガイド* (3021-9-065)
- *JP1 Version 10 JP1/Performance Management リファレンス* (3021-3-043)

G.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
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

表記	製品名
	<ul style="list-style-type: none"> Copy-on-Write Snapshot Copy-on-write SnapShot Snapshot XP
Device Manager	Hitachi Device Manager
Dynamic Link 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 Dynamic Link Manager Hitachi Dynamic Link Manager EX
Dynamic Provisioning	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 Dynamic Provisioning Software Dynamic Provisioning Thin Provisioning
Global Link Manager	Hitachi Global Link Manager
H10000	Hitachi Universal Storage Platform H10000
H12000	Hitachi Universal Storage Platform H12000
H20000	Hitachi Universal Storage Platform H20000
H24000	Hitachi Universal Storage Platform H24000
H10000/H12000	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 H10000 Hitachi Universal Storage Platform H12000
H20000/H24000	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 H20000 Hitachi Universal Storage Platform H24000
HAM	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 High Availability Manager Hitachi High Availability Manager Software
HDP	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 Dynamic Provisioning Thin Provisioning
HDT	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 Dynamic Tiering Software XP7 Smart Tiers
Hitachi AMS	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 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	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 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
Hitachi AMS 200	Hitachi Adaptable Modular Storage 200
Hitachi AMS 500	Hitachi Adaptable Modular Storage 500

表記	製品名
Hitachi AMS 1000	Hitachi Adaptable Modular Storage 1000
Hitachi AMS2000	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 AMS2010	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 AMS2100	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 AMS2300	Hitachi Adaptable Modular Storage 2300
Hitachi AMS2500	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

表記	製品名
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 Hitachi Universal Storage Platform H12000 Hitachi Universal Storage Platform H10000
J2EE	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"> J2EE Java 2 Platform, Enterprise Edition
JDK	Java Development Kit
JP1/AJS2 - Scenario Operation	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"> JP1/Automatic Job Management System 2 - Scenario Operation Manager JP1/Automatic Job Management System 2 - Scenario Operation View
JP1/IM	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"> 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	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"> JP1/Integrated Management - Manager JP1/Integrated Manager - Central Console
JP1/IM - View	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"> JP1/Integrated Management - View JP1/Integrated Manager - Console View JP1/Integrated Manager - View
JRE	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"> Java Runtime Environment Java 2 Runtime Environment
Linux	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"> Red Hat Enterprise Linux[®] SUSE Linux[®] Enterprise Server Oracle Linux[®]
Mainframe Agent	Hitachi Device Manager Mainframe Agent
NAS Platform	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 NAS Platform NAS Platform
PFM - Base	JP1/Performance Management - Base
PFM - Manager	JP1/Performance Management - Manager
Performance Monitor	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"> Performance Management - Base Monitor Performance Monitor
Protection Manager	Hitachi Protection Manager
RAID 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"> RAID Manager RAID Manager XP XP7 RAID Manager
RAID Manager XP	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"> RAID Manager XP P9000 RAID Manager XP7 RAID Manager
Replication Manager	Hitachi Replication Manager
Replication Monitor	JP1/HiCommand Replication Monitor
ShadowImage	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"> 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	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"> Storage Navigator Hitachi Device Manager - Storage Navigator Remote Web Console
Storage Navigator Modular 2	Hitachi Storage Navigator Modular 2
SUSE Linux Enterprise Server	SUSE Linux [®] Enterprise Server
Thin Image	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"> Fast Snap Hitachi Thin Image
Tiered Storage Manager	Hitachi Tiered Storage Manager
TrueCopy	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"> Continuous Access XP Asynchronous Continuous Access XP Synchronous Continuous Access Synchronous Continuous Access Synchronous for Mainframe Hitachi Open Remote Copy

表記	製品名
	<ul style="list-style-type: none"> • Hitachi Open Remote Copy Asynchronous • Hitachi TrueCopy • Hitachi TrueCopy Asynchronous • Hitachi TrueCopy Asynchronous for Mainframe • 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 • Continuous Access Synchronous for Mainframe • Hitachi Open Remote Copy • Hitachi TrueCopy • 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

表記	製品名
Universal Storage Platform V/VM	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 V Hitachi Universal Storage Platform VM Hitachi Universal Storage Platform H24000 Hitachi Universal Storage Platform H20000
Universal Storage Platform VM	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 VM Hitachi Universal Storage Platform H20000
Universal Volume 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"> Universal Volume Manager External Storage XP
UNIX	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"> Solaris AIX Linux[®] HP-UX
Virtual Partition 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"> Virtual Partition Manager Hitachi Virtual Partition Manager Software Disk/Cache Partition
Virtual Storage Platform	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 Hitachi Virtual Storage Platform VP9500
VMware	VMware [®]
VMware ESXi	VMware vSphere [®] ESXi [™]
VMware Tools	VMware Tools [™]
VMware vCenter Server	VMware vCenter Server [™]
VMware vSphere	VMware vSphere [®]
VP9500	Hitachi Virtual Storage Platform VP9500
VSP 5000 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 5100 Hitachi Virtual Storage Platform 5500 Hitachi Virtual Storage Platform 5100H Hitachi Virtual Storage Platform 5500H
VSP E990	Hitachi Virtual Storage Platform E990
VSP F1500	Hitachi Virtual Storage Platform F1500
VSP Fx00 モデル	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 F350 Hitachi Virtual Storage Platform F370 Hitachi Virtual Storage Platform F400 Hitachi Virtual Storage Platform F600

表記	製品名
	<ul style="list-style-type: none"> Hitachi Virtual Storage Platform F700 Hitachi Virtual Storage Platform F800 Hitachi Virtual Storage Platform F900
VSP G1000	<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 G1000 Hitachi Virtual Storage Platform VX7
VSP G1500	Hitachi Virtual Storage Platform G1500
VSP Gx00 モデル	<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 G100 Hitachi Virtual Storage Platform G130 Hitachi Virtual Storage Platform G150 Hitachi Virtual Storage Platform G200 Hitachi Virtual Storage Platform G350 Hitachi Virtual Storage Platform G370 Hitachi Virtual Storage Platform G400 Hitachi Virtual Storage Platform G600 Hitachi Virtual Storage Platform G700 Hitachi Virtual Storage Platform G800 Hitachi Virtual Storage Platform G900
VxVM	Veritas Volume Manager
XP7 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 XP7 RAID 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"> VSP 5000 シリーズ VSP G1000 VSP G1500 VSP F1500 Virtual Storage Platform Universal Storage Platform V/VM Hitachi USP
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

G.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

略語	正式名称
ALUA	Asymmetric Logical Unit Access
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
DMTF	Distributed Management Task Force
DN	Distinguished Name
DNS	Domain Name System
DoS	Denial of Services
ECC	Elliptic Curve Cryptography
EVS	Enterprise Virtual Server
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

略語	正式名称
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
MPIO	Multipath I/O
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
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
REST	Representational State Transfer
RFC	Request For Comments
RMI	Remote Method Invocation
S-VOL	Secondary VOLume

略語	正式名称
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
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

G.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1KiB（キビバイト）、1MiB（メビバイト）、1GiB（ギビバイト）、1TiB（テビバイト）と読み替えてください。

1KiB、1MiB、1GiB、1TiBは、それぞれ1,024バイト、1,024KiB、1,024MiB、1,024GiBです。

索引

記号

.truststore 222

A

account.lock.num 146
agent.logger.loglevel 611
agent.logger.MaxBackupIndex 611
agent.logger.MaxFileSize 612
agent.properties ファイル 609
agent.rm.everytimeShutdown 609
agent.rm.horcmInstance 610
agent.rm.horcmRange 611
agent.rm.horcmService 610
agent.rm.lunPathCheck 612
agent.rm.shutdownWait 609
agent.rm.TimeOut 609
agent.util.hpux.displayDsf 613
auditlog.conf ファイル 473

B

BaseDN 158

C

C/T デルタ
分析 302
CIM/WBEM 350
CIM/WBEM 機能
Device Manager 350
設定 352
ユーザーアカウント設定 352
cimxmlcpa.properties ファイル 578
cimxmlsca.properties ファイル 558, 578
Ciphers 561
client.externaltask.sn.fetch.enable 557
client.externaltask.sn.fetch.pollinginterval 557
client.launch.em.secure 557
client.properties ファイル 556
client.rmi.port 556
com.wbem solutions.jsrserver.bindto 578
Compute Systems Manager 56

config.xml ファイル 300
configforclient.xml ファイル 300
customizedsnmptrap.customizedSNMPTrapEnable
563
customizedsnmptrap.customizelist 563
customizedsnmptrap.properties ファイル 562

D

database.properties ファイル 546, 587
dbm.startingCheck.retryCount 546
dbm.startingCheck.retryPeriod 547
dbm.traceSQL 546, 587
Device Manager CLI 29
SSL/TLS の有効化 253
Device Manager エージェント 29
環境設定 416
常駐プロセス 425
前提バージョン 76
ファイアウォール 418
プロパティファイル 608
ポート 104
保守情報の取得 [ホスト] 529
Device Manager エージェントのサービス
稼働状態の確認 426
起動 426
停止 426
Device Manager サーバ 29
自己署名証明書のエクスポート 250
プロパティファイル 535
ポート 101
devicemanager.properties ファイル 588
dispatcher.properties ファイル 549
dsquery コマンド 184
dvmcacerts 222
Dynamic Link Manager 56

E

Element Manager
設定 285
設定の解除 287
exauth.properties ファイル
Kerberos サーバ 176
LDAP ディレクトリサーバ 163

- RADIUS サーバ 170
- E メール通知
 - アラート 327
 - イベント 334, 338
 - 受信ユーザーの設定 328
 - テンプレートのカスタマイズ [イベント] 336, 341
 - テンプレートのカスタマイズ [アラート] 330
- F**
 - firewall_setup コマンド 418
- G**
 - Global Link Manager 56
 - global-active device 84
 - GUI 29
- H**
 - hbsa_modinfo コマンド 427
 - hbsa_util コマンド 429
 - hbsasrv コマンド 426
 - hcnds64banner コマンド 630, 632
 - hcnds64getlogs コマンド 525
 - hcnds64unlockaccount コマンド 147
 - hdc.adapter.adapterProcessNum 597
 - hdc.adapter.esx.timeout 600
 - hdc.adapter.localport 597
 - hdc.classloader 568
 - hdc.common.allowIPAddressList 602
 - hdc.common.bindServerIPAddress 602
 - hdc.common.http.serverPort 598
 - hdc.common.https.serverPort 599
 - hdc.common.rmi.registryPort 597
 - hdc.common.rmi.serverPort 598
 - hdc.common.rmi.ssl.registryPort 599
 - hdc.common.rmi.ssl.serverPort 599
 - hdc.request.timeout 567
 - hdc.rmiregistry 567
 - hdc.rmiserver 568
 - hdc.service.fileCleanup.startTime 600
 - hdc.service.localport 597
 - hdc.service.rmi.registryIPAddress 600
 - hdc.ssl.ciphers 605
 - hdc.ssl.esx.certCheck 601
 - hdc.ssl.esx.enabledTLSv1 606
 - hdc.ssl.secure 601
 - hdc.usessl 569
 - hdcbase.properties ファイル 596, 605
 - hdccacerts 222
 - hdvm_info コマンド 429
 - hdvm.analytics.disabled 573
 - hdvm.analytics.healthcheck.excludeMainframe 573
 - hdvm.analytics.healthcheck.notification.exportreport.locale 573
 - hdvm.analytics.report.pdf.showLogo 573
 - hdvm.port 588
 - hdvm.protocol 588
 - hdvm.replication.disabled 577
 - hdvm.rmi.port 588
 - hdvm.timeout 588
 - hdvmagt_setting コマンド 430
 - hdvmcacerts 222
 - hdvmmodmailuser コマンド
 - アラート通知 329
 - イベント通知 335
 - hdvmmodpolluser コマンド 361
 - hdvmsnmpuser コマンド 325
 - HiScan.log ファイル 430
 - HiScan.msg ファイル 521
 - HiScan コマンド 433
 - Hitachi Command Suite 共通トレースログ設定 320
 - Hitachi Command Suite 共通コンポーネント 29
 - ポート 100
 - ポートの変更 107
 - ログ出力 320
 - Hitachi File Services Manager 56
 - hldutil.properties ファイル 612
 - hldutil コマンド 435
 - HORCM_CMD 444
 - HORCM_DEV 446
 - HORCM_INST 450
 - HORCM_INSTP 452
 - HORCM_LDEV 448
 - HORCM_MON 442
 - HORCM_VCMD 446
 - Host Data Collector 29
 - ファイアウォール 130
 - 複数の IP アドレスがある場合の設定 133
 - プロパティファイル 596
 - ポート 103
 - 保守情報の取得 528
 - 保守情報の取得 [ホスト] 528
 - Host Data Collector のサービス稼働状態の確認 373
 - 起動 372
 - 停止 373
 - 例外登録 130, 131
 - host.agent.access.timeoutForRpm 566
 - host.mf.agent.connection.timeout 566
 - host.properties ファイル 566
 - hostdatacollectors.properties ファイル 566
 - htmsetup コマンド 299
 - 非クラスタ環境 297
 - クラスタ環境 298
 - htnm.agent.use.cipher.type 574
 - htnm.flashMode 572
 - htnm.infoAcquirePeriod 571
 - htnm.server.n.host 572
 - htnm.server.n.port 572
 - htnm.server.n.protocol 572
 - htnm.servers 571
 - HtsmgetTI.properties ファイル 527
 - htsmmodmailuser コマンド 340
 - HTTPPort 579
 - HTTPSPort 579

I

IETF 350
indruststore 222
IPv6
 グローバルアドレス 133
 グローバルユニークローカルアドレス 133
 サイトローカルアドレス 133
 ストレージシステムとの連携 135
 リンクローカルアドレス 133
IP アドレス
 変更 137

J

Java
 変更 [Device Manager エージェント] 416
 変更 [Host Data Collector] 36
javaconfig.properties ファイル 604
javapath_setup コマンド 416
javapathlocation 605
JDK
 変更 35
JP1/IM 56, 346
 Hitachi Command Suite 製品の GUI のラウンチ
 315
JP1/NETM/DM 56
 配布指令 458, 459
 パッケージング 457
jsserver.properties ファイル 578
jssecacerts 222

K

Kerberos サーバ
 exauth.properties ファイル 176

L

launchapp.elementmanager.role.mode 565
launchapp.elementmanager.usehostname 566
launchapp.properties ファイル 564
launchapp.snm2.rmi.port 565
launchapp.snm2.url 565
ldapcacerts 222
LDAP ディレクトリサーバ
 exauth.properties ファイル 163
 サーバ証明書の条件 258
Linux
 ファイアウォールの例外登録 113
logger.guiMessageFileCount 591
logger.guiMessageMaxFileSize 592
logger.guiTraceFileCount 591
logger.guiTraceMaxFileSize 592
logger.hicommandbase.loglevel 548
logger.hicommandbase.MaxBackupIndex 548
logger.hicommandbase.MaxFileSize 549
logger.hicommandbase.sysloglevel 548

logger.iotrace.maxFileSize 604
logger.iotrace.numOfFiles 604
logger.loglevel 547, 614
logger.MaxBackupIndex 547, 614
logger.MaxFileSize 548, 614
logger.messageLogLevel 589
logger.properties ファイル 547, 589, 603, 613
logger.serverMessageFileCount 590
logger.serverMessageMaxFileSize 592
logger.serverTraceFileCount 591
logger.serverTraceMaxFileSize 592
logger.syslogLevel 590
logger.trace.level 603
logger.trace.maxFileSize 603
logger.trace.numOfFiles 604
logger.tracelogLevel 590

M

migration.dataErase.defaultValue 570
migration.multiExecution 570
migration.plan.candidateCapacityGroupDisplayMa
xCount 570
migration.plan.candidateVolumeCountLimit 570
migration.properties ファイル 569
migration.volumeDelete.defaultValue 571
mime.properties ファイル 556
MOF ファイル
 編集 [インディケーション通知] 275
 編集 [オブジェクト操作] 270

N

NIC
 複数の NIC のネットワーク設定 132

O

OutOfMemory エラー 521

P

paircfgmigration.properties ファイル 641
PairCfgMigration コマンド 640
password.check.userID 144
password.min.length 144
password.min.lowercase 144
password.min.numeric 144
password.min.symbol 144
password.min.uppercase 144
perf_cmddev.properties ファイル 359
perf_findcmddev コマンド 357
PFM - Manager
 ホスト名の設定 307
programproductinfo.properties ファイル 615

R

RADIUS サーバ
 exauth.properties ファイル 170
RAID Manager 29
Replication Manager 56
Replication Manager サーバ 29
replication.properties ファイル 574
rgcmddev.properties ファイル 627
RMI 通信
 Device Manager 306, 314
rpmlib.properties ファイル 577
rpmlib.rpm.port 578

S

server.agent.differentialrefresh.manual.enabled 545
server.agent.differentialrefresh.periodical.enabled 545
server.agent.evtwait.timeout 626
server.agent.JRE.location 618
server.agent.maxMemorySize 618
server.agent.port 616
server.agent.rm.centralizePairConfiguration 620
server.agent.rm.cuLdevForm 620
server.agent.rm.exclusion.instance 621
server.agent.rm.horcm.poll 622
server.agent.rm.horcmSource 625
server.agent.rm.ignorePairStatus 624
server.agent.rm.location 621
server.agent.rm.moduleTimeOut 625
server.agent.rm.optimization.userHorcmFile 621
server.agent.rm.pairDefinitionForm 622
server.agent.rm.temporaryInstance 622
server.agent.rm.temporaryPort 622
server.agent.rm.userAuthentication 624
server.agent.rmxp.location 626
server.agent.shutdownTime 618
server.agent.snapshotEvtwait.timeout 626
server.base.home 539
server.base.initialsynchro 540, 584
server.checkOutVolumeRange 586
server.cim.agent 540
server.cim.http.port 541
server.cim.https.port 541
server.cim.support 540
server.cim.support.job 540
server.cim.support.protocol 541
server.configchange.enabled 542
server.dispatcher.configchange.pollingPeriod 550
server.dispatcher.daemon.autoSynchro.dayOfWeek 553
server.dispatcher.daemon.autoSynchro.doRefresh 552
server.dispatcher.daemon.autoSynchro.interval 553
server.dispatcher.daemon.autoSynchro.logicalGroup.doRefresh 555
server.dispatcher.daemon.autoSynchro.performance.doRefresh 554
server.dispatcher.daemon.autoSynchro.performance.startTime 555

server.dispatcher.daemon.autoSynchro.startTime 553
server.dispatcher.daemon.autoSynchro.type 552
server.dispatcher.daemon.configUpdate.detection.interval 551
server.dispatcher.daemon.configUpdate.detection.variable.enabled 553
server.dispatcher.daemon.logicalGroupMappingUpdate.startTime 556
server.dispatcher.daemon.pollingPeriod 549
server.dispatcher.daemon.receiveTrap 550
server.dispatcher.daemon.replication.config.doUpdate 574
server.dispatcher.daemon.replication.config.minute 576
server.dispatcher.daemon.replication.config.offset 575
server.dispatcher.daemon.replication.config.updateInterval 575
server.dispatcher.daemon.replication.performance.rpm.updateInterval 576
server.dispatcher.daemon.replication.performance.tnm.minute 577
server.dispatcher.daemon.replication.performance.tnm.offset 576
server.dispatcher.daemon.replication.performance.tnm.updateInterval 576
server.dispatcher.message.timeout 549
server.dispatcher.message.timeout.in.processing 549
server.dispatcher.snm2.configchange.pollingPeriod 550
server.dispatcher.traps.purgePeriod 550
server.eventMonitoringIntervalInMinute 585
server.eventNotification.mail.to 544, 585
server.horcmconfigfile.hostname 540
server.http.entity.maxLength 539, 619
server.http.host 537, 616
server.http.localPort 616
server.http.port 537, 616
server.http.security.clientIP 558, 619
server.http.security.clientIPv6 559
server.http.security.unprotected 560
server.http.server.timeOut 626
server.http.socket.agentAddress 617
server.http.socket.bindAddress 617
server.https.enabledCipherSuites 560
server.https.port 538
server.https.protocols 561
server.https.security.keystore 559
server.https.security.truststore 560
server.logicalGroupMapping.updateInterval 546
server.logicalview.initialsynchro 542
server.mail.alert.status 545
server.mail.alert.type.storagesystem 544
server.mail.enabled.fileserver 543
server.mail.enabled.storagesystem 542
server.mail.errorsTo 544, 585
server.mail.from 543, 585
server.mail.smtp.auth 544, 585
server.mail.smtp.host 543, 584
server.mail.smtp.port 543, 585
server.migration.dataErase.defaultValue 586
server.migration.maxRetryCount 587

server.migration.multiExecution 586
 server.migrationPlan.candidateCapacityGroupDisplayMaxCount 587
 server.migrationPlan.candidateVolumeCountLimit 586
 server.properties ファイル
 Device Manager エージェント 615
 Device Manager サーバ 537, 558
 Tiered Storage Manager サーバ 583, 592
 server.rmi.port 539, 583
 server.rmi.secure 593
 server.rmi.security.enabledCipherSuites 593
 server.rmi.security.port 584
 server.rmi.security.protocols 594
 server.server.authorization 619
 server.server.serverIPAddress 619
 server.server.serverPort 620
 server.server.ssl.hdvm 625
 server.subsystem.ssid.availableValues 545
 server.util.processTimeOut 626
 SLP サービス
 解除 363
 起動 362
 制御 361
 停止 362
 SLP デモン
 解除 364
 起動 363
 停止 363
 SMTP サーバ 328
 SMTP 認証ユーザー 329, 335, 340
 SNMP トラップ
 アラート 323
 ログファイル出力 332
 SNMP トラップ受信ユーザー 325
 SSL/TLS
 有効 [Device Manager CLI] 253
 有効 [Device Manager サーバ] 235
 有効 [Tiered Storage Manager CLI] 255
 Storage Navigator Modular 2
 前提条件 284
 連携 284
 SVP 32
 System アカウント
 ロックに関する設定 147

T

TIC コマンド 529
 Tiered Storage Manager CLI 29
 SSL/TLS の有効化 255
 ログファイル 527
 Tiered Storage Manager サーバ 29
 プロパティファイル 582
 ポート 102
 Tuning Manager 56
 プロパティ設定 308
 リモート接続 [Windows のクラスタ環境] 298
 リモート接続 [非クラスタ環境] 297
 Tuning Manager - Agent for RAID
 インスタンスの起動 307

tuningmanager.properties ファイル 571

U

URL
 変更 140
 user_httpsd.conf ファイル 227

V

veritas.volume.manager.version 615

W

Windows
 ファイアウォールの例外登録 113

あ

アカウント
 条件 157
 アラート 321
 E メール通知 327
 SNMP トラップ 323
 アラート通知
 SMTP サーバ 328
 暗号タイプ
 Kerberos 認証 190

い

移行
 IPv6 133
 データベース 395
 デバイスグループ 640
 一括管理構成 620
 イベント通知
 SMTP 認証ユーザーの設定 335, 340
 テンプレートのカスタマイズ 336, 341
 プロパティの設定 335, 339
 インスタンス環境の構築 306
 インスタンスの起動 [Tuning Manager - Agent for RAID] 307
 インストール
 リモートインストール 455
 インディケーション通知
 CIM クライアントのサーバ証明書のインポート 277
 CIM クライアントのサーバ証明書のエクスポート 281
 CIM クライアントの自己署名証明書の作成 280
 Device Manager サーバのクライアント証明書のインポート 281
 Device Manager サーバのクライアント証明書のエクスポート 276

MOF ファイルの編集 275
キーストアーファイルの作成 274
相互認証の無効化 279
相互認証の有効化 277
インポート
CIM クライアントのクライアント証明書〔オブジェクト操作〕 273
CIM クライアントのサーバ証明書〔インディケーション通知〕 277
Device Manager サーバのクライアント証明書〔インディケーション通知〕 281
Device Manager サーバのサーバ証明書 238
Device Manager サーバのサーバ証明書〔オブジェクト操作〕 281
Host Data Collector のサーバ証明書 248
サーバ証明書〔Device Manager エージェント〕 265
証明書 242, 251, 252, 260
証明書〔Hitachi Command Suite 共通コンポーネント〕 256
証明書〔Host Data Collector〕 262
データベース 402, 404, 407

え

エクスポート
CIM クライアントのクライアント証明書〔オブジェクト操作〕 281
CIM クライアントのサーバ証明書〔インディケーション通知〕 281
Device Manager サーバのクライアント証明書〔インディケーション通知〕 276
Device Manager サーバの自己署名証明書 250
Device Manager サーバのサーバ証明書〔オブジェクト操作〕 271
データベース 396, 398, 400

お

オープンホスト 37
オブジェクト操作
CIM クライアントのクライアント証明書のインポート 273
CIM クライアントのクライアント証明書のエクスポート 281
CIM クライアントの自己署名証明書の作成 280
Device Manager サーバのサーバ証明書のインポート 281
Device Manager サーバのサーバ証明書のエクスポート 271
MOF ファイルの編集 270
キーストアーファイルの作成 269
相互認証の無効化 279
相互認証の有効化 272
デフォルトの自己署名証明書 279

か

階層構造モデル 158
外部認可サーバ 150
接続確認 188
登録 162
外部認証サーバ 150
接続確認 188
登録 162
仮想化サーバ 37
前提環境 48
登録情報の変更 264
仮想コマンドデバイスサーバ 62
仮想マシン 37
構成変更時に必要な作業 47
前提環境〔Device Manager エージェント〕 413
前提環境〔Host Data Collector〕 42
環境設定
Device Manager エージェント 416
監査ログ
Device Manager GUI 479
Device Manager サーバ 478
Device Manager サーバ〔CIM 経由〕 481
Hitachi Command Suite 共通コンポーネント 478
syslog ファイル 464
イベントログファイル 464
確認 476
環境設定ファイルの編集 473
監査事象 465
関連製品 479
詳細メッセージ 487
設定 464
メッセージテキスト 478
メッセージ部 478, 487
管理クライアント 29
制限 632
管理サーバ 29
保守情報の取得 525
ホスト名の変更 135

き

キーストアー
キーペアの削除〔Device Manager サーバ〕 240
サーバ証明書のインポート〔Device Manager サーバ〕 238
サーバ証明書のインポート〔Host Data Collector〕 248
パスワードの変更〔Device Manager サーバ〕 241
キーストアーファイル
作成〔インディケーション通知〕 274
作成〔オブジェクト操作〕 269
キーペア
作成〔CIM クライアント〕 280
作成〔Device Manager サーバ〕 232
作成〔Host Data Collector〕 246
参照〔Device Manager サーバ〕 239
パスワードの変更〔Device Manager サーバ〕 241
共有秘密鍵
確認 187

削除 187
登録 186

く

クライアント証明書
インポート [CIM クライアント] 281
インポート [オブジェクト操作] 273
エクスポート [CIM クライアント] 281
エクスポート [インディケーション通知] 276

け

警告バナー 630
メッセージの削除 632
メッセージの作成と登録 630
メッセージの条件 630

こ

構成定義ファイル 419
格納場所の変更 454
記述規則 441
サポートしているパラメーター 441
前提環境 439
注意事項 454
編集 440
コピーペア
Device Manager エージェントの前提バージョン
76
ストレージシステムの要件 75
設定 [Device Manager エージェント] 419

さ

サーバ証明書
LDAP ディレクトリサーバ 258
インポート [CIM クライアント] 281
インポート [インディケーション通知] 277
インポート [Device Manager エージェント] 265
エクスポート [CIM クライアント] 281
エクスポート [オブジェクト操作] 271
確認 [Device Manager エージェント] 266
キーストアーへのインポート [Device Manager サ
ーバ] 238
キーストアーへのインポート [Host Data
Collector] 248
申請 [Device Manager サーバ] 237
申請 [Hitachi Command Suite 共通コンポーネン
ト] 227
申請 [Host Data Collector] 247
トラストストアからの削除 [Device Manager エ
ージェント] 268
トラストストアからの削除 [Device Manager サ
ーバ] 244

サービス
Hitachi Command Suite 製品 365
実行ユーザーの変更 [Device Manager エージェン
ト] 427

し

資源登録システム 456
自己署名証明書
エクスポート [Device Manager サーバ] 250
オブジェクト操作 279
確認 [インディケーション通知] 278
確認 [オブジェクト操作] 278
作成 [CIM クライアント] 280
作成 [Device Manager サーバ] 232
作成 [Hitachi Command Suite 共通コンポーネン
ト] 224
システム構成 29
SVP 構成 70, 73
一括管理構成 58
仮想コマンドデバイス構成 66
性能情報 355
条件
アカウント 157
情報検索用のユーザーアカウント 182
メッセージ [警告バナー] 630
詳細メッセージ
監査ログ 487
常駐プロセス 366
Device Manager エージェント 425
冗長構成 160
情報検索用のユーザーアカウント 182
確認 186
削除 185
条件 182
登録 184
証明書
インポート 251, 252
インポート [Device Manager サーバ] 242, 260
インポート [Hitachi Command Suite 共通コンポ
ーネント] 256
インポート [Host Data Collector] 262
確認 [Host Data Collector] 263
削除 259
確認 258, 261
トラストストアへのインポート [Device
Manager サーバ] 242, 260
証明書発行要求
作成 [Device Manager サーバ] 236
作成 [Hitachi Command Suite 共通コンポーネン
ト] 224
作成 [Host Data Collector] 246
申請
サーバ証明書 [Device Manager サーバ] 237
サーバ証明書 [Hitachi Command Suite 共通コン
ポーネント] 227
サーバ証明書 [Host Data Collector] 247

す

- ストレージシステム 29
 - インスタンス環境の構築 306
 - コピーペアを管理する場合の要件 75
- 性能情報の収集 288
- 性能情報の取得〔CIM/WBEM 機能〕 354
- 登録情報の変更 269
- ポート 104

せ

- 性能情報
 - システム構成 355
 - ストレージシステム 288
 - ストレージシステム〔CIM/WBEM 機能〕 354
 - 設定 356, 360
- セキュリティ通信
 - 通信路 194
- 接続確認
 - 外部認可サーバ 188
 - 外部認証サーバ 188
- 前提環境
 - 仮想化サーバ 48
 - 仮想マシン〔Device Manager エージェント〕 413
 - 仮想マシン〔Host Data Collector〕 42
 - 構成定義ファイルの利用 439
 - 通常ホスト〔Device Manager エージェント〕 412
 - 通常ホスト〔Host Data Collector〕 39
- 前提条件
 - Storage Navigator Modular 2 284

そ

- 相互認証
 - 無効化〔インディケーション通知〕 279
 - 無効化〔オブジェクト操作〕 279
 - 有効化〔インディケーション通知〕 277
 - 有効化〔オブジェクト操作〕 272

た

- ダウンロード
 - トラストストアファイル〔Device Manager サーバ〕 249
 - トラストストアファイル〔Tiered Storage Manager サーバ〕 254

つ

- 通常ホスト 37
 - 前提環境〔Device Manager エージェント〕 412
 - 前提環境〔Host Data Collector〕 39
- 通信
 - セキュリティ通信路 194

- 通信プロトコル
- 変更 260

て

- データベース
 - 移行 395
 - インポート 402, 404, 407
 - エクスポート 396, 398, 400
 - バックアップ 378
 - 復元 383
- デバイスグループ
 - 移行 640

と

- トラストストア 222
 - サーバ証明書の削除〔Device Manager エージェント〕 268
 - サーバ証明書の削除〔Device Manager サーバ〕 244
 - 参照〔Device Manager サーバ〕 242, 243
 - 証明書のインポート〔Device Manager サーバ〕 242, 260
 - パスワードの変更〔Device Manager エージェント〕 267
 - パスワードの変更〔Device Manager サーバ〕 245
 - パスワードの変更〔Host Data Collector〕 263
- トラストストアファイル
 - ダウンロード〔Device Manager サーバ〕 249
 - ダウンロード〔Tiered Storage Manager サーバ〕 254
- トラストストアファイルの作成
 - Device Manager CLI 250

に

- 認可グループ 150

ね

- ネームスペース 351
- ネットワーク
 - ブリッジ 132

は

- 配布管理システム 456
- 配布先システム 456
- パスワード
 - トラストストア〔Device Manager エージェント〕 267
 - トラストストア〔Device Manager サーバ〕 245
 - トラストストア〔Host Data Collector〕 263

バックアップ
データベース 378
パラメーター
構成定義ファイル 441

ひ

秘密鍵
作成 [Hitachi Command Suite 共通コンポーネン
ト] 224

ふ

ファイアウォール
Device Manager エージェント 418
Host Data Collector 130
設定 113
例外登録 113
例外登録 [Linux] 113
例外登録 [Windows] 113
ファイルサーバ 37
復元
データベース 383
フラットモデル 159
ブリッジ
ネットワークの設定 132
プロパティ
変更 [Device Manager エージェント] 608
変更 [Tiered Storage Manager サーバ] 582
変更 [Device Manager サーバ] 536
プロパティファイル
Device Manager エージェント 608
Device Manager サーバ 535
Host Data Collector 596
Tiered Storage Manager サーバ 582
記述規則 536, 583

へ

ペア管理サーバ 29
ペア定義マイグレーション 636

ほ

ポート
Device Manager エージェント 104
Device Manager サーバ 101
Hitachi Command Suite 共通コンポーネント 100
Host Data Collector 103
Tiered Storage Manager サーバ 102
ストレージシステム 104
変更 107
変更 [CIM/WBEM 機能] 354
例外登録 113

保守情報
Device Manager エージェントの管理対象ホスト
529
Host Data Collector 528
Host Data Collector の管理対象ホスト 528
管理サーバ 525
ホスト 29, 37
バージョンアップ 415
ホスト管理ソフトウェア 38
ホスト名
PFM - Manager 307
変更 135
ポップアップブロック
変更 253

ま

マルチドメイン構成 160

む

無効化
相互認証 [インディケーション通知] 279
相互認証 [オブジェクト操作] 279

め

メインフレームホスト 37
メインフレームボリューム 50
ヘルスチェック 573
メッセージテキスト
監査ログ 478
メモリーヒープサイズ
変更 34

ゆ

有効化
SSL/TLS [Device Manager CLI の実行マシン]
253
SSL/TLS [Device Manager サーバ] 235
SSL/TLS [Tiered Storage Manager CLI の実行マ
シン] 255
相互認証 [インディケーション通知] 277
相互認証 [オブジェクト操作] 272
ユーザーアカウント
アカウントロック 145
アカウントロックの解除 147
アカウントロックポリシー 146
アカウントロックポリシーの設定 146
パスワードポリシー 144
パスワードポリシーの設定 144

り

- リモートインストール 455
 - 実行結果の戻り値 460
 - 配布指令 458, 459
 - パッケージング 457
- リモート接続
 - Tuning Manager [Windows のクラスタ環境] 298
 - Tuning Manager [非クラスタ環境] 297

れ

- 例外登録
 - Host Data Collector のサービス 130, 131
- [レプリケーション] タブ 302
 - システム構成 302, 311
 - レプリケーション管理 310

ろ

- ログ
 - 参照 346
- ログファイル
 - SNMP トラップ 332
 - Tiered Storage Manager CLI 527
- ロック
 - System アカウント 147
 - アカウントロックの解除 147
 - ユーザーアカウント 146