



Data Protector

ソフトウェアバージョン: 10.00

トラブルシューティングガイド

ドキュメントリリース日: 2017年6月
ソフトウェアリリース日: 2017年6月

ご注意

保証

Micro Focus or one of its affiliates製品に関する保証は、製品およびサービスに付属する保証規定に明示されている内容に限定されます。本書のいかなる記述も、追加の保証を構成するものではありません。Micro Focusは、本書の技術的内容や編集に関する誤りや欠落に関して責任を負いません。

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

機密コンピューターソフトウェア。保持、使用、またはコピーには、Micro Focusからの有効なライセンスが必要です。FAR 12.211および12.212に従って、商用コンピューターソフトウェア、コンピューターソフトウェアドキュメント、および商用品目の技術データは、米国政府に対して、ベンダーの標準商用ライセンスに基づいてライセンスされます。

著作権について

© Copyright 2017 Micro Focus or one of its affiliates

商標について

Adobe™はAdobe Systems Incorporatedの商標です。

Microsoft®およびWindows®は、米国におけるMicrosoft Corporationの登録商標です。

UNIX®は、The Open Groupの登録商標です。

この製品には、'zlib' 汎用圧縮ライブラリのインターフェースが含まれています。Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアバージョンの番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに更新されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

最新のソフトウェア更新をチェックするには、次のサイトを参照してください。

<https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=patches?keyword=>

更新状況、およびご使用のドキュメントが最新版かどうかは、次のサイトで確認できます。

<https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=>

このサイトを利用するには、Passportへの登録とサインインが必要です。Passport IDの登録は、次のWebサイトから行なうことができます。<https://cf.passport.softwaregrp.com/hppcf/login.do>.

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、の営業担当にお問い合わせください。

サポート

ソフトウェアサポートオンラインWebサイトを参照してください。<https://softwaresupport.softwaregrp.com/>

このサイトでは、お客様窓口のほか、ソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

ソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HPソフトウェアサポートのWebサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング
- ソフトウェアパッチのダウンロード
- 製品ドキュメントへのアクセス

- サポート契約の管理
- カスタマーサポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部のサポートを除き、サポートのご利用には、Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。

Passport IDを登録するには、次のWebサイトにアクセスしてください。

<https://cf.passport.softwaregrp.com/hppcf/login.do>

アクセスレベルの詳細については、次のWebサイトをご覧ください。<https://softwaresupport.softwaregrp.com/>

目次

第1章：Data Protectorのトラブルシューティングについて	11
トラブルシューティングの方法	11
全般的なチェック	11
Data Protectorログファイルについて	12
ログファイルの保存場所	12
ログファイルの形式	12
ログファイルの内容	12
Data Protectorのテレメトリファイルについて	14
Data Protectorエラーメッセージについて	15
Data Protector GUIでのエラーメッセージ	15
Data Protector CLIでのエラーメッセージ	16
Data Protectorのカスタマイズについて	16
グローバルオプション	16
最も頻繁に使用されるグローバルオプション	16
Omnircオプション	18
omnircオプションの使用法	18
最も頻繁に使用されるomnircオプション	19
Data Protectorのグローバルオプションをカスタマイズする	22
前提条件	22
GUI使用によるグローバルオプション設定	22
手順	22
グローバルファイルの編集によるオプションのカスタマイズ	23
手順	23
第2章：ネットワークおよび通信のトラブルシューティング	24
ホスト名の解決に関する問題	24
TCP/IP設定をチェックする	24
DNSの名前解決のテスト	24
接続したシステムがそれ自体の名前としてクライアントXを返す	24
クライアントAがクライアントBへの接続に失敗する	25
クライアントXに接続できない	25
セル内の時刻設定のチェック	25
停電からの復旧	26
システムリカバリ後にIDBが到達不可能	26
Data Protector セッションが実際には実行中でないにもかかわらず、セッションステータスが[実行中]と表示される	26
hdpd-idb-cpサービスが開始しない	26
Novell Open Enterprise Server (OES)の問題	27
TSAログインが拒否される	27

その他の問題	27
「接続はピアによってリセットされました」メッセージによるクライアントの障害	27
「このクライアントは、どのセルのメンバーでもありません」メッセージによるクライアントの障害	28
inet.logファイルに大量のログが記録される	28
「StoreOnceデバイスはオフラインです」メッセージによるStoreonceSoftwareデバイスの障害	29
暗号制御通信	29
MoM Cell ManagerにインストールされているMedia Agentの使用に失敗する	29
MoMでの暗号化通信の有効化に失敗する	30
セルでの暗号化通信の無効化に失敗する	30
Microsoft以外のクラスターでの暗号化通信の無効化に失敗する	31
暗号化通信が機能しない	31
インストールセッションが失敗し、エラーメッセージが表示される場合がある	32
クライアント上で暗号制御通信を有効にした後にクライアントに接続できない	32
Cell Managerで暗号化通信を有効にすると、CRS接続に失敗する	33
第3章：Data Protectorのサービスおよびデーモンのトラブルシューティング	35
概要	35
Data Protectorプロセス一覧	35
Data ProtectorのサービスをWindowsで起動する際の問題	36
サービスを起動するためのパーミッションがない	36
変更されたサービスアカウントのプロパティ	36
指定したサービスが見つからない	36
CRSサービスを起動するとMMDが異常終了する	37
Data ProtectorのデーモンをUNIXで起動する際の問題	37
Data ProtectorのCell Managerデーモンを起動できない	38
hpd-idbサービスが起動に失敗し、共有メモリの問題をレポートする	38
CRSサービスを起動するとMMDが異常終了する	38
Data Protectorプロセスの他の問題	39
Name Server Cachingが無効になると、UNIX上のData Protectorのパフォーマンスに影響を及ぼす	39
バックアップの実行中、一定時間経過後にバックアップセッションが停止し、BSMが応答しなくなる	39
第4章：ユーザーインターフェイスのトラブルシューティング	41
グラフィカルユーザーインターフェイスの問題	41
接続性とアクセシビリティの問題	41
Cell Managerにアクセスするパーミッションがない	41
リモートシステムへの接続が拒否される	41
Cell Manager上でinetが応答しない	42
ファイルシステムのブラウザエージェントを起動できない	42
コマンドラインインターフェイスの問題	42
Data Protectorコマンドを実行できない	42

第5章: バックアップと復元のセッションのトラブルシューティング	44
増分バックアップの代わりにフルバックアップが実行される	44
前回 のフルバックアップがない	44
説明を変更した	44
ツリーを変更した	44
バックアップオーナーが違う	45
アップグレード後に拡張増分が実行されない	45
拡張増分バックアップでZDBファイルシステムバックアップを実行すると、フルバックアップが実行される	46
Data Protectorがセッションを開始できない	46
対話型セッションを開始できない	46
スケジュール設定されたセッションが実行されない	46
セッションが正常に行われず、「使用可能なライセンスがありません」というステータスメッセージが表示される	47
スケジュール設定したバックアップが開始されない(UNIXシステムの場合のみ)	47
デバイスにメディアが入っているのにマウント要求が発行される	47
デバイス内のメディアが所属するメディアプールのポリシーが[追加不可能]である	47
デバイス内のメディアがまだフォーマットされていない	48
デバイス内のメディアが事前割り当てリストで指定されているメディアと違っている	48
ファイルライブラリに対してマウント要求が発行される	49
ファイルライブラリデバイスのディスクに空き領域がない	49
ファイル名に関する問題	49
ファイル名またはセッションメッセージがData Protector GUI上に正常に表示されない	49
クラスターに関する問題	49
IDBサービスが同期しない	49
Windows NTFS Change Log Providerを使用した共有クラスターボリュームの増分ファイルシステムのバックアップが、クラスターのフェイルオーバー後にフルバックアップにフォールバックする	50
Cell Managerがクラスター内に構成されている場合の復元の問題	50
Microsoft Cluster ServerノードのCONFIGURATIONオブジェクトのバックアップが失敗する	51
HP-UXおよびLinuxのCell ManagerでのIDBの復元	51
別のCell ManagerでのIDBの復元は失敗する可能性がある	52
復元プロセスの終了時にIDBの復元に失敗する	52
復元操作の実行後、Data Protector GUIからCell Managerへの接続が失敗する	53
その他の問題	53
Storage Optimizerのスタブの復元でエラーがレポートされる	53
バックアップの保護期限が終了した	54
ファイルが大量であるために拡張増分バックアップが失敗する	54
接続拒否エラーが断続的に発生する	55
ディスクイメージ復元時に予想外のマウント済みファイルシステムが検出される	55
アプリケーションデータベースの復元に関する問題	56
HP-UX上でバックアップが失敗する	56
非同期の読み込みによりバックアップパフォーマンスが改善されない	56
WindowsシステムでIIS構成オブジェクトのバックアップが失敗する	57
ハードリンクがあるボリュームからのサブツリーの復元が失敗する	57

Mac OS X上で、共有メモリの容量が不十分であるためにバックアップセッションが失敗する	58
ミラー化されているシステム予約パーティションのバックアップが失敗した可能性がある	58
中断されたファイルバックアップまたはファイルが見つからない	58
バックアップのスケジュールを試みたときにスケジューラーが失敗する	59
データ重複排除機能がないWindowsの重複排除ボリュームでZDBファイルシステムバックアップが失敗する	59
実行前および実行後スクリプトが失敗し、エラーメッセージが表示される	60
OB2OEXECOFFが設定されている場合、実行前および実行後スクリプトが失敗する	60
実行前スクリプトが失敗した場合に実行後スクリプトが実行されない	61
第6章：デバイスとメディアのトラブルシューティング	62
デバイスおよびメディアに関する全般的な問題	62
データフォーマットに互換性がないと、フリープールメディアが自動的に再フォーマットされない	62
Media Agentクライアント上のStoreOnceファイバーチャネルデバイスが不足している	62
Windows上でエクステンジャー制御デバイスにアクセスできない	63
SCSIデバイスのロックが解除されずにセッションが失敗する	63
デバイスのオープンに関する問題	64
Windows上でサポートされていないSCSI HBA/FC HBAの使用	64
ライブラリ再構成の失敗	64
暗号化されたメディアが読み込みまたは書き込み操作の後に不良とマークされる	65
Data Protector GUIとCLIを使用したNULLデバイスの作成	65
メディアに関するさまざまな問題	68
DLT/SDLTデバイス	68
LTOデバイス	69
DDSデバイス	69
メディアヘッダーのサニティチェックエラー	69
デバイスのシリアル番号に関する問題	70
破損したデータを復元またはコピーできない	70
よく発生するハードウェア関連の問題	71
ADIC/GRAU DASライブラリとSTK ACSライブラリに関する問題	71
ADIC/GRAU DASライブラリのインストール失敗	71
ドライブが1つも表示されない	72
GRAU CAPが正しく構成されていない	72
ライブラリ操作が失敗する	73
クラウドデバイスに関する問題	73
クラウド(Helion)とクラウド(Azure)での通信エラー	73
Data Protector 9.00を使用してクラウド(Helion)デバイスを構成できない	73
10.00以前のバージョンのData Protectorを使用してクラウド(Azure)デバイスを構成できない	74
第7章：オブジェクト操作セッションのトラブルシューティング	75
オブジェクトコピーに関する問題	75
コピーされたオブジェクトの数が想定された数より少ない	75
選択したライブラリ内の一部のオブジェクトしかコピーされない	75
追加のメディアに対するマウント要求が発行される	75

オブジェクトコピーを作成したときに、保護の終了時間が延長される	76
複数のオブジェクトを含むセッションを複製すると、応答が停止する	76
データメインブーストデバイス上の複製セッションが再試行期間中に中止操作に応答できない	77
オブジェクト集約に関する問題	77
多くの時点のオブジェクト集約を行うと、上限を超える数のファイルが開かれる	77
B2Dデバイスへのオブジェクト集約が2回目の試行で失敗した	78
第8章：Data Protector内部データベースのトラブルシューティング	79
ディレクトリが見つからないことによる問題	79
データベース/ファイルを開けない、またはデータベースのネットワーク通信エラーが発生する	79
Cell Managerにアクセスできない	79
バックアップ時またはインポート時の問題	80
IDBバックアップが失敗してアーカイブログファイル名形式が正しくないことを報告する	80
バックアップ中にファイル名がIDBに記録されない	80
IDBのバックアップまたはインポート中に、BSMまたはRSMが強制終了する	81
IDBバックアップまたはインポート中に、MMDが強制終了する	81
DCバイナリファイルが破損または見つからない	82
内部データベースのバックアップが失敗する	82
パフォーマンスに関する問題	83
復元時のブラウズに時間がかかる	83
IDBのサイズ増加による問題	83
IDBのスペースが不足している場合	83
IDBのDCBF部分が急激に増加する	84
その他の問題	84
データベースセッションマネージャーが稼働していないことによるプロセス間通信エラー	84
MMDBとCDBが同期しない	84
IDBが破損している	85
MMDBのCMMDBへのマージが失敗する	85
IDBの復元中にセッションがエラーを出して完了する	86
DCバイナリファイルがDCBFセグメントのエラーを報告する	86
PDB OracleのPoint-in-Timeリカバリが失敗してエラーが表示される	86
復元を手動で中止した後に3PAR Oracle ASM IR復元が失敗する	87
ブラガブルデータベースのバックアップが失敗して「ブラガブルデータベースが存在しません」というエラーが表示される	87
第9章：レポートおよび通知のトラブルシューティング	88
レポートと通知に関する問題	88
Data Protector Windows上で送信方法として電子メールを使用したときにData Protector GUIが応答しなくなる	88
SNMPによる送信が失敗する	88
第10章：Data Protectorヘルプのトラブルシューティング	89

概要	89
オンラインヘルプのトラブルシューティング	89
Data Protectorの画面を別の画面に切り替えても、その画面の説明がヘルプナビゲーターに 表示されない	89
第11章：サポートサービスへご連絡いただく前に	91
当社サポートサービスへご連絡いただく前に	91
デバッグについて	91
デバッグの有効化	91
Data Protector GUIを使用する	92
OB2DBG変数を使用する	92
OB2OPTS変数を使用する	92
デバッグ構文	92
ログファイルの圧縮	93
デバッグオプション	93
必要なデバッグファイル	93
デバッグの最大サイズの制限	95
デバッグファイルの名前と保存場所	95
Inetのデバッグ	96
CRSのデバッグ	96
AppServerのデバッグ	97
スケジューラーおよび実行されなかったジョブ実行のデバッグ	98
カスタマーサポートサービスに送付するための生成データの準備	98
omnidlcコマンドについて	98
制限事項	99
CLIからomnidlcコマンドを使用することによるデバッグファイルの処理	99
収集データの範囲限定	99
データのセグメント化	100
収集データの圧縮の無効化	100
パックしたデータの保存	100
パックされていないデータの保存	100
必要なスペースの推定	101
クライアント上のデバッグファイルの削除	101
デバッグファイルについての情報の削除	101
問題と回避策	101
その他の操作	102
Data Protector GUIを使用したデバッグファイルの処理	102
デバッグファイル操作の実行	103
デバッグファイルの収集	103
デバッグファイル領域の計算	104
デバッグファイルの削除	105
omnidlcコマンドの使用例	106
Data Protector GUIを使用することによるデバッグファイルの処理	107
デバッグファイル操作の実行	107

デバッグファイルの収集	108
デバッグファイル領域の計算	109
デバッグファイルの削除	109
カスタマーサポートサービスに送付するデータ収集の例	110
フィードバックを送信	112

第1章: Data Protectorのトラブルシューティングについて

Data Protectorの使用に際して問題が発生した場合でも、多くの場合はユーザー自身が問題を解決することができます。そのような場合には、このガイドを手引きとしてお役立てください。

トラブルシューティングの方法

問題を短時間で効率的に解決するために、以下の事項に留意してください。

1. 一般的なトラブルシューティング情報を把握します。
2. 問題がData Protectorヘルプファイルに記載されているか、該当するガイドのトラブルシューティングのセクションに記載されているかを確認します。
 - インストールとアップグレードのトラブルシューティングについては、『Data Protectorインストールガイド』を参照してください。
 - アプリケーション統合セッションのトラブルシューティングについては、『Data Protectorインテグレーションガイド』を参照してください。
 - ゼロダウンタイムバックアップおよびインスタントリカバリのトラブルシューティングについては、『Data Protectorゼロダウンタイムバックアップ管理者ガイド』と『Data Protectorゼロダウンタイムバックアップインテグレーションガイド』を参照してください。
 - ディザスタリカバリのトラブルシューティングについては、『Data Protectorディザスタリカバリガイド』を参照してください。
3. 問題の解決方法が見つからない場合は、その問題をカスタマーサポートサービスにご連絡ください。

ヒント:

Data Protectorのパフォーマンスに関する概要やヒントについては、『Data Protectorヘルプ』のキーワード「パフォーマンス」で表示される内容を参照してください。

全般的なチェック

最初に、以下の事項を確認してください。

- 現段階では克服できない既知の制限事項に触れていないかどうか。Data Protectorの制限事項と推奨事項、Data ProtectorおよびData Protector以外における既知の問題点の詳細については、『Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。
- サードパーティ製のハードウェアやソフトウェアに関連した問題ではないこと。その場合には、各ベンダーにサポートの問い合わせを行ってください。
- 最新のData Protectorパッチがインストールされていること。パッチは、以下のサイトから入手可能です。
<https://softwaresupport.softwaregrp.com/>

どのData Protectorパッチがシステムにインストールされているかをチェックする方法については、Data Protectorヘルプのキーワード「パッチ」で表示される内容を参照してください。

- 適切なオペレーティングシステムパッチがインストールされていること。
必要なオペレーティングシステムパッチのリストについては、『Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。
- アプリケーションバックアップの場合、バックアップ失敗の原因がアプリケーションのダウンではないこと。
- デバッグログまたはREDOログを格納しているファイルシステムが満杯になっていないこと。
- アプリケーションデータを格納しているファイルシステムが満杯になっていないこと。
- システムのメモリが不足していないこと。

Data Protectorログファイルについて

Data Protectorの使用に際して問題が発生した場合は、ログファイル内の情報を問題の特定に役立てることができます。

ログファイルの保存場所

ほとんどのData Protectorログファイルは、以下の場所にあります。

Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2012の場合 :`Data_Protector_program_data\log`

その他のWindowsシステムの場合 :`Data_Protector_home\log`

HP-UXシステム、Solarisシステム、Linuxシステムの場合 :`/var/opt/omni/log`および
`/var/opt/omni/server/log`(後者はHP-UXおよびLinuxシステムのみ)

その他のUNIXシステムおよびMac OS Xシステムの場合 :`/usr/omni/log`

ログファイルの形式

ほとんどのData Protectorログファイルのエントリは以下の形式になっています。

```
time_stamp process.PID.Thread_ID source_file_info Data Protector_version Log_entry_message
```

例

```
03/16/2013 8:47:00 AM INET.3048.3036 ["inetnt/allow_deny.c /main/dp61/6":467] 10.00
b330 A request 0 (BDF) came from host computer.company.com (10.17.xx.xxx) which is
not in AllowList: not proceeding with this request!
```

ログファイルの内容

Data Protectorログファイルに記録される情報は、下の表に示すとおりです。

Data Protectorログファイル

ログファイル	説明
debug.log	予期しない状況が記録されます。ユーザーにとって役立つものもありますが、主に当社サポートサービスが使用します。
inet.log	要求拒否など、クライアントのローカルセキュリティに関するイベントが記録されます。UNIXシステムでは、Data ProtectorInetサービスに対して発行されたすべての要求も記録されます。
enhincr.log	拡張増分バックアップの動作に関する情報が記録されます。たとえば、拡張増分バックアップレポジトリで起こった問題のエラー情報の詳細などがこれに含まれます。
Ob2EventLog.txt	Data Protectorのイベントと通知が記録されます。イベントログには、Data Protectorイベントが一括して保存されます。
media.log	バックアップ、初期化、インポートのためにメディアが使用されるたびに、このログファイルに新しいエントリが作成されます。IDBの復旧では、このファイルを使って、IDBをバックアップしたテープや、前回のIDBバックアップ以降に使用されているメディアを特定できます。
omnisv.log	Data Protectorサービスが開始および停止された日時に関する情報が記録されます。
security.log	Cell Manager上でのセキュリティ関連のイベントが記録されます。イベントには、通常の動作の結果であり、単に特定のユーザーによって禁止されている動作が試行されたことを示すものもあります。これに対し、意図的な侵入行為が進行中である可能性を示すイベントもあります。
purge.log	IDBのバックグラウンドでの削除動作のトレースを記録します。
PostgreSQLログ	IDBのログが記録されます。 このファイルはCell Manager上の以下の場所に格納されます。 Windowsシステムの場合 :Data_Protector_program_data\server\db80\pg\pg_log UNIXシステムの場合 :/var/opt/omni/server/db80/pg/pg_log
pgbouncer.log	pgBouncerのログが記録されます。
アプリケーションサーバーのログ	スケジューラーや失敗したジョブ実行などのコンポーネントのアプリケーションサーバーログが格納されます。 このファイルは以下の場所に格納されます。 Windowsシステムの場合 :Data_Protector_program_data\log\AppServer UNIXシステムの場合 :/var/opt/omni/log/AppServer
sanconf.log	sanconfコマンドにより生成されたセッションレポートが保存されています。
sm.log	バックアップセッションや復元セッションで発生した内部エラーの詳細(バックアップ仕様の解析エラーなど)が記録されます。

stats-HPeCloud-year-month.log	<p>クラウド (Helion) コピーセッション中にクラウドゲートウェイから生成された利用状況ログレポートが格納されています。これらのファイルには、セッションID、デバイス名、日付と時刻、要求数に関する詳細情報が含まれています。</p> <p>このファイルは以下の場所に格納されます。</p> <p>Windowsシステムの場合 :Data_Protector_program_data\log\Server</p> <p>UNIXシステムの場合 :/var/opt/omni/log/Server</p>
stats-Azure-year-month.log	<p>クラウド (Azure) コピーセッション中にクラウドゲートウェイから生成された利用状況ログレポートが格納されています。これらのファイルには、セッションID、デバイス名、日付と時刻、要求数に関する詳細情報が含まれています。</p> <p>このファイルは以下の場所に格納されます。</p> <p>Windowsシステムの場合 :Data_Protector_program_data\log\Server</p> <p>UNIXシステムの場合 :/var/opt/omni/log/Server</p>
upgrade.log	<p>このログは、アップグレード処理中に作成されます。UCP (アップグレードコアパート) とUDP (アップグレード詳細パート) のメッセージが記録されます。</p>
DPIDBsetup_PID.log (UNIXの場合のみ)	<p>このログは、アップグレード処理中に作成されます。アップグレード処理のトレース情報が記録されます。</p>
IS_install.log	<p>リモートインストールのトレース情報が記録されます。このファイルは、インストールサーバー上に置かれます。</p>
sap.log, oracle8.log, informix.log, sybase.log, db2.log	<p>アプリケーション固有のログファイルです。アプリケーションとData Protector間の統合ソフトウェア呼び出しに関するトレース結果が記録されます。このファイルは、アプリケーションシステムに保存されます。</p>

Data Protectorのテレメトリファイルについて

Data Protectorは以下のテレメトリクスの上位レベルの情報を収集します。

- ホストのOSバージョン
- Data Protectorのコンポーネントとそのバージョン
- デバイスまたはメディアサーバー - Cell Manager内のクライアントに関連付けられています。デバイスが接続されているホスト名の詳細、デバイス名、ライブラリ名、メディアが配置されているプール名、およびデバイスの種類が含まれます。
- デバイス使用状況 - デバイスの使用状況。
- スケジュール - スケジュールテレメトリは、バックアップとセッションのタイプ別にグループ化された情報を公開します。バックアップとセッションのタイプ別に毎年スケジュールされるフルバックアッププロセスの数と増分バックアッププロセスの数を示します。

- 容量ベースのライセンス (CBL) - CBLは容量に関する情報の収集に活用されます。詳細は、『Data Protectorインストールガイド』を参照してください。
- ライセンスのカテゴリ - Data Protectorで使用可能なライセンス数を一覧します。
- クライアント使用状況 - 情報が、クライアントごとに収集されます。ホスト名、アプリケーション名、バックアップ済みデータの合計サイズなどの情報があります。
- ストレージ使用状況 - デバイスにバックアップされているデータの合計です。

注:

お客様関連の内部情報は収集されますが、ホスト情報はマスクされるか、文字数値フォーマットに置換されます。

注:

テレメトリデータの収集中に、Cell Managerのパフォーマンスに大きな影響を及ぼすことはありません。

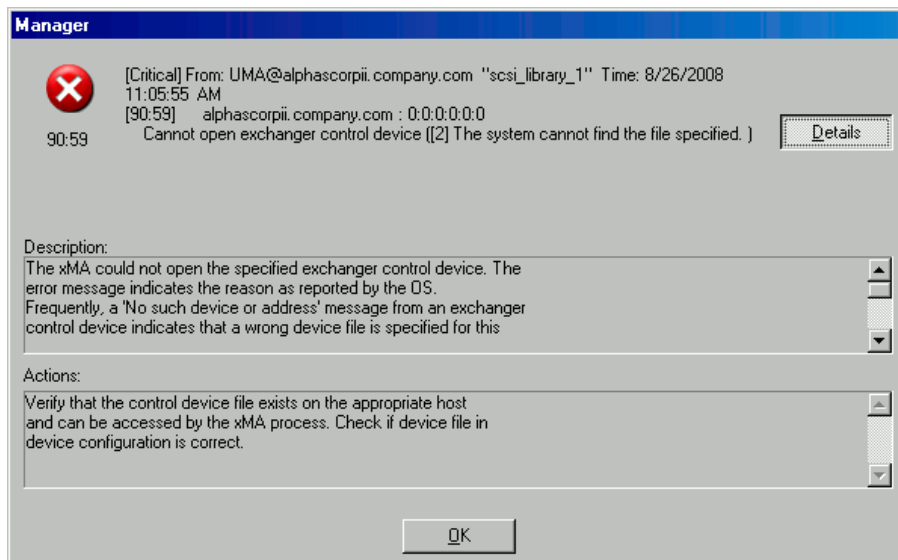
Data Protectorエラーメッセージについて

Data Protectorの多くのエラーメッセージにはトラブルシューティング情報が関連付けられており、ここからはエラーの詳細情報や問題解決に対する示唆を得ることができます。このようなメッセージには、情報にアクセスするためのエラー番号が含まれています。

Data Protector GUIでのエラーメッセージ

セッション出力内の一部のエラーメッセージには、クリック可能なリンクでエラー番号が示されています。このリンクをクリックすると、エラーメッセージダイアログにエラーに関する詳細情報が表示されます。エラーの詳細な説明と解決のヒントを表示するには、**[詳細]**をクリックします。

エラーメッセージダイアログのサンプル



Data Protector CLIでのエラーメッセージ

Data Protector CLI内でエラー番号を含むエラーが返された場合は、トラブルシューティングファイルでエラーの詳細を探ることができます。このテキストファイルには、すべてのData Protectorエラーメッセージが記録され、メッセージごとに説明と対処方法が示されます。

トラブルシューティングファイルは、Cell Manager上の以下の場所にあります。

Windowsシステムの場合: `Data_Protector_home\help\enu\Trouble.txt`

UNIXシステムの場合: `/opt/omni/gui/help/C/Trouble.txt`

例

メッセージ:

[12:1051]クライアントのセキュリティ侵害。アクセスが拒否されました。

説明:

ターゲットホストはセキュリティ保護されており、Cell権限のリストに存在しないホストによってアクセスされました。

対処方法:

- * クライアントのCell権限のリストを確認して更新してください。
- * クライアントがロックアウトされている場合は、allow_hostsファイルを手動で編集します。

Data Protectorのカスタマイズについて

グローバルまたはomnircオプションをカスタマイズすることで、Data Protectorの問題を解決できる場合があります。

グローバルオプション

グローバルオプションは、タイムアウトや制限値などの、Data Protectorセル全体の挙動を定義するパラメーターのセットです。Cell Managerで設定できます。

注:

ほとんどの場合は、グローバルオプションを変更しなくても、Data Protectorを操作できます。

グローバルオプションは、次の2つの方法で設定できます。

- [Data Protectorのグローバルオプションをカスタマイズする、ページ 22](#)
- [グローバルファイルの編集によるオプションのカスタマイズ、ページ 23](#)

最も頻繁に使用されるグローバルオプション

最も頻繁に使用されるグローバルオプションを以下に示します。詳細な説明については、グローバルオプションファイルを参照してください。

グローバルオプション	説明
------------	----

MaxSessions	セル内で同時に実行可能なData Protectorセッション(任意の種類)の最大数を指定します。デフォルト: 1000。
MaxBSessions	セル内で同時に実行可能なData Protectorバックアップセッション(任意の種類)の最大数を指定します。デフォルト: 100。
MaxMAperSM	1つのバックアップ、オブジェクトコピー、オブジェクト集約、または復元セッションで同時に使用可能なData Protectorバックアップデバイスの最大数を指定します。デフォルト: 100。
MaxDAperMA	Data Protectorバックアップ、オブジェクトコピー、オブジェクト集約の各セッションの、Disk Agentの最大同時使用数(デバイスの最大同時使用数)を指定します。デフォルト: 32。
DCDirAllocation	新しいDC(詳細カタログ)バイナリファイルを格納するDCディレクトリの選択に使用するアルゴリズムを指定します。Fill in sequence、Balance size(デフォルト)、Balance number。 DCディレクトリ選択アルゴリズムの詳細については、『Data Protectorヘルプ』のキーワード「DCBFの保守」で表示される内容を参照してください。
MediaView	[メディア管理]コンテキストに表示されるフィールドとその順番を変更します。
InitOnLoosePolicy	メディアポリシーが[緩和]の場合に、空のメディアまたは認識されないメディアをData Protectorが自動的に初期化できるようにします。
DailyMaintenanceTime	日常の保守作業を開始可能な時刻を指定します。デフォルト: 12:00(正午)。 日常の保守作業の一覧は、『Data Protectorヘルプ』のキーワード「Data Protectorが実行するチェック」で表示される内容を参照してください。
DailyCheckTime	日常のチェック作業を開始可能な時刻を指定します。デフォルト: 12:30 P.M.。日常のチェック作業を無効にすることもできます。 日常のチェック作業の一覧は、『Data Protectorヘルプ』のキーワード「Data Protectorが実行するチェック」で表示される内容を参照してください。
SessionStatusWhenNoObjectToCopyおよび SessionStatusWhenNoObjectToConsolidate	コピーまたは集約対象のオブジェクトがない場合は、オブジェクトコピーとオブジェクト集約セッションのセッションステータスを制御できます。 値が次のように設定されている場合は次のような結

	<p>果になります。</p> <ul style="list-style-type: none">• 0 (デフォルト) にすると、セッションが失敗とマークされ、重大なエラーが表示されます。• 1 にすると、セッションが成功とマークされ、警告が表示されます。• 2 にすると、セッションが成功とマークされ、通常メッセージが表示されます。
SetInitialMediumProtection	<p>新しいメディアが保護されていることを確認します。保護されていないメディアのバックアップまたはコピーセッション中にデータ損失が発生しないように、値を1に設定する必要があります。</p>

Omnircオプション

omnircオプションは、トラブルシューティングを行う場合や、他の設定値を無効にしたい場合に非常に便利で、Data Protectorクライアントの動作にのみ影響します。ただし、動作環境で本当に必要になった場合にのみ使用してください。これらのオプションの値は、Disk AgentやMedia Agentによって使用されません。

omnircオプションは、各クライアント上の以下のファイル内に設定できます。

Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2012の場合:

`Data_Protector_program_data\omnirc`

その他のWindowsシステムの場合: `Data_Protector_home\omnirc`

HP-UXシステム、Solarisシステム、Linuxシステムの場合: `/opt/omni/.omnirc`

その他のUNIXシステムおよびMac OS Xシステムの場合: `/usr/omni/.omnirc`

omnircオプションの使用方法

omnircオプションを設定するには、以下の手順を実行してください。

1. プラットフォームに応じて、テンプレートomnirc.tplまたはomnirc.TMPLを、それぞれomnircまたはomnircIにコピーします。
2. ファイルomnircまたはomnircIを編集します。目的のオプションから#記号を削除してコメント行の指定を解除し、適切な値を設定します。
3. オプションの設定が終了したら、以下の操作を行います。
 - ファイルをコピーするかまたはエディターを使用してomnircファイルを作成するときは、ファイルのパーミッションを確認してください。UNIXシステムの場合、ファイルのパーミッションはユーザーのumask設定値に応じて設定されるため、一部のプロセスでファイルを読み取れない設定になることがあります。
ファイルのパーミッションを手動で644に設定してください。
 - omnircファイルを変更したときは、omnircファイルを変更したData Protectorクライアント上で、Data Protectorのサービスデーモンを再起動してください。UNIXシステム上のcrsデーモンについてはこの操作が必須です。必ず再起動してください。また、Windowsシステム上のData Protector

CRSサービスとinetサービスも再起動することをお勧めします。Windowsの場合に限り、エントリを追加または変更した場合や、エントリを削除(またはファイル名を変更)しただけの場合は、再起動は必要ありません。

注:
omnircファイル内のオプション名に特殊な文字を使用する場合は、環境変数の設定に使用できる文字に関するオペレーティングシステム固有の制限事項にも注意が必要です。たとえばUNIXシステムの場合であれば、変数内にSpace Tab / : * " < > |。

ディザスタリカバリ中にomnircオプションを設定する方法については、『Data Protectorディザスタリカバリガイド』を参照してください。

最も頻繁に使用されるomnircオプション

最も頻繁に使用されるomnircオプションを以下に示します。詳細な説明については、omnircファイルを参照してください。

Omnircオプション	説明
OB2_SHOW_BTRFS_MOUNTS	明示的にマウントしたボリュームをバックアップするには、inetがすべてのボリュームを返すようにomnirc変数(OB2_SHOW_BTRFS_MOUNTS)をエクスポートする必要があります。OB2_SHOW_BTRFS_MOUNTS変数は、1に設定する必要があります。
OB2_ENCRYPT_PVT_KEY	保護されたリモートインストールに暗号化された秘密鍵を使用するには、インストールサーバーでこのオプションを1に設定します。デフォルト値は0(オフ)です。
OB2_ENCRYPT_MEDIUM_STRICT	バックアップ、オブジェクト集約、オブジェクトコピー、および自動メディアコピーセッションでドライブベースの暗号化を使用するかどうかを制御できます。オプションは、現在のセッションに対してGUIオプションのDrive-based encryptionが選択されている場合にのみ考慮します。 値が1に設定されている場合、次のような結果になります。 <ul style="list-style-type: none">• 選択されたテープドライブで暗号化がサポートされていない場合、デフォルトでセッションが中止されます。• 選択されたテープドライブで暗号化がサポートされているが、そのドライブ内のメディアで暗号化がサポートされていない場合、マウント要求が発行されるか(スタンドアロンテープドライブの場合)、まず暗号化をサポートするために使用可能な次のメディアが確認されてから、暗号化がサポートされるメディアが見つからない場合は最終的にマウント要求が発行されます(テープライブラリの場合)。• 選択されたテープドライブおよびそのドライブ内のメディアの両方で暗号化がサポートされている場合、データ書き込み操作が暗号化モードで実行されます。 値が0に設定されている場合、次のような結果になります。 <ul style="list-style-type: none">• 選択されたテープドライブで暗号化がサポートされていない場合、データ書き込み操作が非暗号化モードで実行されます。

	<ul style="list-style-type: none"> • 選択されたテープドライブで暗号化がサポートされているが、そのドライブ内のメディアで暗号化がサポートされていない場合、データ書き込み操作が非暗号化モードで実行されます。 • 選択されたテープドライブおよびそのドライブ内のメディアの両方で暗号化がサポートされている場合、データ書き込み操作が暗号化モードで実行されます。
OB2_ENCRYPT_FORCE_FORMAT	<p>Data Protectorドライブベースの暗号化を使用する場合、フォーマットの動作を制御できます。</p> <p>値が次のように設定されている場合は次のような結果になります。</p> <ul style="list-style-type: none"> • 0(デフォルト)の場合、フォーマット操作は中止されます。 • 1の場合、フォーマット操作は強制実行されます。
OB2_AES_COMPATIBILITY_MODE	<p>Data Protectorバージョン(DP 7.03_108、8.14、8.14_209、8.14_210、9.03、9.04)で作成したAES暗号化バックアップからデータを復元しても役に立ちません。この状態を修正するには、手動による操作が必要です。</p> <p>Data Protectorバージョン(DP 7.03_108、8.14、8.14_209、8.14_210、9.03、9.04)で作成した、AES-256ソフトウェアによる暗号化バックアップを復元するには、復元するクライアントのomnircファイルにあるこのオプションを1に設定します。</p> <p>他のData Protectorバージョンで作成した、AES-256ソフトウェアによる暗号化バックアップを復元するには、このオプションを0に設定するか、omnircファイルからこのオプションを削除し、そのクライアントのinetデーモンを再起動します。</p>
OB2FORCEPOSTEXEC	<p>実行後スクリプトを強制的に実行することができます。</p> <p>値が次のように設定されている場合は次のような結果になります。</p> <ul style="list-style-type: none"> • 0(デフォルト)の場合、実行後スクリプトの実行は強制されません。 • 1の場合、実行前スクリプトが失敗した場合でも、実行後スクリプトは常に実行されます。
OB2BLKPADDDING_n	<p>初期化時にメディアに書き込まれる空のブロック数を指定します。これにより、メディアのコピー時に、すべてのデータのコピーが完了する前にターゲットメディアがスペース不足になるのを防ぎます。</p>
OB2DEVSLEEP	<p>デバイスのロード中、再試行後に次の再試行が行われるまでのスリープ時間を変更します。</p>
OB2ENCODE	<p>バックアップ仕様でのバックアップオプションの設定に関わらず、データエンコーディングの使用を常に可能にします。</p>
OB2OEXECOFF	<p>特定のクライアントに対するバックアップ仕様で定義されているオブジェクトのpre-/post-execスクリプトを、制限または無効化できるようにします。</p>
OB2REXECOFF	<p>特定のクライアントに対するリモートセッションのpre-/post-execスクリプトを無効化できるようにします。</p>
OB2CHECKCHANGETIME	<p>増分バックアップで「前回inode変更日時」をいつ使用するかを制御しま</p>

(UNIXの場合のみ)	す。
OB2INCRDIFFTIME (UNIXの場合のみ)	増分バックアップに対する「前回inode変更日時」のチェック時に適用される「増分待ち」時間を指定します。このオプションは、OB2CHECKCHANGETIMEオプションが2に設定されている場合にのみ有効です。
OB2RECONNECT_ACK	Data ProtectorがAckメッセージを待つ時間を定義します(デフォルトは1200秒です)。エージェントがこの時間内にAckを受け取らなかった場合、ソケット接続が有効でなくなったとみなされます。
OB2RECONNECT_RETRY	接続の失敗後、Data Protector Disk AgentまたはMedia Agentが再接続を試行する時間を定義します。デフォルト: 600秒。
OB2SHMEM_IPCGLOBAL	Disk AgentとMediaAgentの両方がインストールされているHP-UXクライアントでは、バックアップ中に以下のエラーが発生した場合に備えて、このオプションを1に設定しておく必要があります。 Cannot allocate/attach shared memory (IPC Cannot Allocate Shared Memory Segment) System error: [13] Permission denied) => aborting
OB2VXDIRECT	拡張VxFSファイルシステムでの直接読み取り(キャッシュ不使用)によるパフォーマンスの向上を可能にします。
OB2_CLP_MAX_ENTRIES (Windowsシステムのみ)	Windows NTFS Change Log Providerがメモリ内に保持できるエントリ数を設定します。Change Log Providerが使用するメモリの容量は、すべてのエントリのファイル名の長さによって異なります。最小値: 15 000エントリ(約25MBのRAM)です。デフォルト: 100 000エントリ(約120 MBのRAM)です。この数値が小さな値に変更されたため、すべてのエントリをメモリに保持できない場合は、バックアップ時間が長くなることがあります。
OB2_CLP_CREATE_EI_REPOSITORY (Windowsシステムのみ)	Windows NTFS Change Log Providerを初めて実行する際に、拡張インクリメンタルリポジトリを作成するかどうかを指定します。拡張インクリメンタルリポジトリを作成する場合は1に設定します。デフォルト: 0です(作成しません)。このオプションセットでは、拡張増分レポジトリが常に更新されるため、バックアップ時間が長くなります。ただし、従来の拡張増分バックアップへのフォールバックは可能です。
OB2_ENHINC_SQLITE_MAX_ROWS	内部メモリキャッシュに格納できる拡張増分バックアップデータベース(Windows、HP-UX、およびLinuxシステムのSQLite)で、行の最大数を指定します。バックアップが膨大な数(数百万)のディレクトリで構成されている場合、このオプションを使用すると、キャッシュに格納できる行の最大数を増やすことができるため、Disk Agentのパフォーマンスが向上します。
OB2SANCONFSCSITIMEOUT (Windowsシステムのみ)	sanconf関連の操作にタイムアウトを設定します。sanconfコマンドを実行する前に、このコマンドの影響を受けるすべてのクライアント上にこの変数を設定する必要があります。デフォルト: 20秒。
OB2PORTRANGE	Data Protectorがリスポートを動的に割り当てる際に使用するポート番号の範囲を限定します。通常このオプションは、ファイアウォール越しのセル管理を可能にする場合に設定します。ファイアウォールは、この変数と

	別に構成する必要があります。指定した範囲は、Inetリスポートに影響を与えません。
OB2PORTRANGESPEC	<p>特定のData Protectorプロセスが使用するポート番号の範囲を限定します。ファイアウォールは、この変数と別に構成する必要があります。指定した範囲は、Inetリスポートに影響を与えません。</p> <p>ポート範囲の構成例については、Data Protectorヘルプのキーワード「ファイアウォールのサポート」で表示される内容を参照してください。</p>
OB2HSMBACKUPALL	<p>オフライン属性が指定されたファイルをバックアップするには、このオプションを1に設定します。デフォルト値は0(設定なし)です。この場合、オフライン属性が指定されたファイルはすべて、バックアッププロセスでスキップされます。</p> <p>このオプションを1に設定すると、Disk AgentがStorage Optimizerですべてのファイルのオフライン属性をチェックし、バックアップ操作を実行します。再解析ポイント付きのファイルの場合、Windowsオペレーティングシステムでは、スタブのバックアップのみが行われます。Linuxオペレーティングシステムの場合、Storage Optimizerはソフトリンクを作成します。</p> <p>オフライン属性があり、再解析ポイントのないファイルの場合、バックアップの前にデータの再呼び出しとリハイドレートが行われるかどうかは、階層ストレージ管理(HSM)製品に基づきます。この処理が行われる場合、I/Oトラフィックが大きくなり、システムが過負荷の状態になることがあります。詳細については、HSM製品のドキュメントを参照してください。</p> <p>注: 再解析ポイントとは、そこから外部ファイルと見なされる場所を指します。</p>

Data Protectorのグローバルオプションをカスタマイズする

Data Protectorグローバルオプションファイルでは、グローバルオプションの値を変更したり、新しいオプションを追加できます。

前提条件

- ユーザーアカウントはData Protector Adminユーザーグループに所属する必要があります。


GUI使用によるグローバルオプション設定

手順

GUIを使用してグローバルオプションを設定するには、以下の手順を実行してください。

1. コンテキストリストで**[内部データベース]**をクリックします。
2. Scopingペインで**[内部データベース]**の**[グローバルオプション]**をクリックします。

[結果エリア]に**Data Protectorグローバルオプション**テーブルが表示されます。このテーブルには、次の6つの列があります。

- [グループ]- オプションが属するコンテキストセクションを表します。
 - [使用中]- オプションのステータスを示します。オンになっているオプションはアクティブです。チェックボックスが空白の場合は、グローバルオプションファイルでコメントアウトされている非アクティブなオプションです。
 - 名前
 - [元]- オプションのロード元のファイルを示します。
 - [値]- オプションに現在設定されている値を示します。
 - [説明]- オプションの使用方法が示されます。
3. オプションを変更するには、[結果エリア]の[値]列で、変更する値をクリックし、[編集]アイコン  をクリックして新しい値を入力します。[保存]をクリックして変更内容を適用します。

オプションを追加するには、[追加]アイコン  をクリックし、ダイアログボックスにオプションパラメーターを入力して[追加]をクリックします。

4. [結果エリア]の一番上にある[保存]アイコン  をクリックします。

保存する前に複数の行を変更することもできます。

テーブルの表示を変更するには、テーブル見出しのフィルターを使用します。

保存プロセスでエラーが発生した場合は、元のグローバルオプションファイルのコピーがglobal.oldという名前で、グローバルオプションフォルダーに作成されます。

グローバルファイルの編集によるオプションのカスタマイズ

GUIの使用以外にも、テキストエディターでglobalファイルを編集して、Data Protectorグローバルオプションを設定することができます。

注意:

Micro Focusでは、GUIを使用してグローバルオプションを設定することを推奨します。保存時に変更内容が検証されるため、範囲外または無効な設定、誤った削除、タイポまたはスペルミスが原因の問題が発生する可能性を減らせるためです。

手順

1. テキストエディターを開きます
2. テキストエディターで、デフォルトのData Protectorサーバー構成ディレクトリのoptionsサブディレクトリにあるglobalファイルを開きます。
3. オプションをアクティブにするには、名前前の#記号を削除して、目的の値に設定します。
4. ファイルをUnicode形式で保存します。

第2章: ネットワークおよび通信のトラブルシューティング

ホスト名の解決に関する問題

TCP/IPプロトコルは、ホスト名を正しく解決できるようにセットアップする必要があります。

通信を成功させるには、ホストAが、ホストBの完全修復ドメイン名 (FQDN)を解決できなくてはなりません。ホスト名の解決とは、ホストAがホストBのFQDNを解釈してIPアドレスを判別することです。

ホスト名の解決では、少なくとも以下の要件を満たす必要があります。

- 各クライアントで、Cell ManagerのアドレスおよびMedia Agentがインストールされているクライアントのアドレスを解決できること。
- Cell Managerがセル内のすべてのクライアントの名前を解決できること。
- MoM Server (使用されている場合)がMoM環境内のすべてのCell Managerの名前を解決できること。

TCP/IP設定をチェックする

TCP/IPプロトコルのインストール後、pingおよびipconfig (Windowsシステム)またはifconfig (UNIXシステム)ユーティリティを使ってTCP/IP構成を検証できます。

一部のシステムでは、pingコマンドをIPv6のアドレスに対して使用することができないので、代わりにping6コマンドを使用してください。

DNSの名前解決のテスト

次のコマンドを実行して、ホスト間のDNSの名前解決をテストします。

```
omnicheck -dns
```

このコマンドは、通常のData Protector操作に必要なすべてのDNS接続を確認します。

このコマンドの詳細については、omnicheck manページまたは『*Data Protector Command Line Interface Reference*』を参照してください。

接続したシステムがそれ自体の名前としてクライアントXを返す

問題

omnicheckコマンドを実行すると、以下のような応答が返されることがあります。

```
client_1 connects to client_2, but connected system presents itself as client_3  
client_1のhostsファイルが正しく構成されていないか、client_2のホスト名がDNS名と一致していません。
```

対処方法

ネットワーク管理者に問い合わせてください。この問題は、ユーザーの環境が名前解決の実行に対してどのように構成されているかに応じて、お使いのDNS構成を変更するか、または影響を受けるクライアント上の以下のディレクトリにあるhostsを変更するか、どちらかの方法で解決する必要があります。

Windowsシステムの場合 :%SystemRoot%\system32\drivers\etc

UNIXシステムの場合 :/etc

クライアントAがクライアントBへの接続に失敗する

問題

omnicheckコマンドを実行すると、以下のような応答が返されることがあります。

```
client_1 failed to connect to client_2
```

client_1のhostsファイルが正しく構成されていないか、client_2にアクセスできません(接続されていないなど)。

対処方法

hostsファイルを正しく構成するか、または切断されたシステムを接続します。

クライアントXに接続できない

問題

omnicheckコマンドを実行すると、以下のような応答が返されることがあります。

```
client_1 cannot connect to client_2
```

このメッセージは、送信されたパケットがタイムアウトのため受信されなかったことを意味します。

対処方法

リモートホスト上でネットワークの問題が発生していないかをチェックして解決します。

セル内の時刻設定のチェック

問題

Data Protectorでは、さまざまなセルコンポーネント(Cell Manager、クライアント)間の通信に、タイムスタンプが広範に使用されます。Cell Managerとクライアント上のシステムクロックが数週間や数ヶ月単位で大幅に異なる場合(テスト用に設定を変更した場合や、仮想マシンの復元後にシステムクロックを更新しなかった場合など)、通信エラー、バックアップの検索や復元の失敗などの予期しない結果が発生する場合があります。

対処方法

システム時刻設定をチェックして、システムクロックが大幅に異ならないようにしてください。

クライアント上のクロックがCell Manager上のクロックと同期されていないと、証明書が無効となり、認証が失敗する可能性があります。たとえば、Cell Manager上のクロックがクライアント上のクロックより進んでいる場合、インストール時に作成された証明書は、クライアントが証明書への接続を試みた時点で有効になっていません。

停電からの復旧

システムリカバリ後にIDBが到達不可能

問題
データベースは、停電、深刻なオペレーティングシステムまたはハードウェアの障害などの予期しないイベントの後に、整合した状態に復旧することができます。ただし、データベースへの(システムリカバリ後の)最初のアクセスが、内部エラーにより失敗する場合があります。これは一時的な問題であり、一度のみ発生します。
対処方法
データベースに再度アクセスします。

Data Protector セッションが実際には実行中でないにもかかわらず、セッションステータスが[実行中]と表示される

問題
Data Protector GUIの[内部データベース]コンテキストで、実際には実行中ではない1つまたは複数のData Protectorセッションのセッションステータスが[In Progress]と表示されます。
対処方法
<ol style="list-style-type: none">1. Data Protector GUIを閉じます。2. <code>omnidbutil -clear</code>コマンドを実行し、実際には実行中でないが[In Progress]と表示されているすべてのセッションのステータスを、[Failed]に設定します。3. Data Protector GUIを再起動します。

hpd-idb-cpサービスが開始しない

問題
hpd-idb-cpサービスが開始しません。
対処方法

1. Data Protectorサービスを停止します。
2. 以下のファイルを削除します。
Windowsシステムの場合: `Data_Protector_program_data\log\hpdp-idb-cp.pid`
UNIXシステムの場合: `/var/opt/omni/log/pgbouncer.pid`
3. Data Protectorサービスを再起動します。

Novell Open Enterprise Server (OES)の問題

TSAログインが拒否される

問題

以下のメッセージが表示されます。

From: VRDA@computer.company.com

"/media/nss/NSS_VOLUME_5"

TSA: Cannot connect to Target Service (login denied).

対処方法

正しいユーザーの証明書でHPLOGINユーティリティ/`usr/omni/bin/hplogin`を実行します。

その他の問題

「接続はピアによってリセットされました」メッセージによるクライアントの障害

問題

Windowsシステムでは、TCP/IPプロトコルのデフォルトの構成パラメーターにより接続の問題が発生する場合があります。このような状態の原因としては、ネットワークまたはコンピューターの負荷が高いこと、ネットワークの信頼性が低いことが考えられ、特に異なるオペレーティングシステムに接続する場合に発生しがちです。以下のエラーが報告されます。

[10054] Connection reset by peer.

対処方法

TCP/IPプロトコルの構成で、デフォルトは5である再送信回数を8に設定できます。1増加するごとにタイムアウトが2倍になるため、これ以上高い値を使用することはお勧めできません。ここでの設定は、Data Protectorによって使用される接続だけでなく、すべてのネットワーク接続に適用されます。

Cell ManagerがWindowsシステムで動作している場合、Cell Managerシステムでまず変更を適用しま

す。それでも問題が解決しない場合、またはCell ManagerがUNIXシステムで動作している場合は、問題のあるWindowsクライアントに変更を適用します。

1. 以下のレジストリキーの下に、DWORDパラメーターTcpMaxDataRetransmissionsを追加して、値を0x00000008(8)に設定します。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

2. システムを再起動します。

注意:

レジストリを誤って編集すると、システムが不安定になったり、使用できなくなったりする場合があります。

「このクライアントは、どのセルのメンバーでもありません」 メッセージによるクライアントの障害

問題

クライアント上でData Protector操作を実行したときに、Cell Manager情報がクライアント上に見つかりません。次のエラーが表示され、操作が失敗します。

The Client is not a member of any cell.

対処方法

- 問題のクライアントがData Protector GUIの[クライアント]コンテキストに一覧表示されている場合は、以下の操作を行います。
 1. [クライアント]コンテキスト内で[クライアント]を展開して問題のクライアントを右クリックし、[削除]を選択します。
 2. クライアントからData Protectorもアンインストールするかどうかを確認するダイアログが表示されます。[いいえ]をクリックします。
 3. [クライアント]を右クリックし、[クライアントのインポート]を選択します。
 4. クライアントを指定して[完了]をクリックします。
- 問題のクライアントが[クライアント]コンテキストに一覧表示されていない場合は、以下の操作を実行します。
 1. [クライアント]コンテキスト内で[クライアント]を右クリックし、[クライアントのインポート]を選択します。
 2. クライアントを指定して[完了]をクリックします。

inet.logファイルに大量のログが記録される

問題

クライアントが保護されておらず、Cell ManagerがServiceguard環境に構成されているか、複数の名前またはIPアドレスを持っている場合、inet.logファイルに以下のようなエントリが大量に記録される可能性があります。

A request 3 (vbda.exe) came from host computer.company.com which is not a cell

manager of this client.

これは、保護されていないクライアントがCell Managerのプライマリホスト名しか認識しないために発生します。その他のクライアントからの要求もすべて許可されますが、要求はinet.logファイルに記録されます。

対処方法

クライアントを保護します。allow_hostsファイルにリストされているクライアントからの要求は、inet.logには記録されなくなります。他のクライアントからの要求は拒否されます。

何らかの理由でユーザー環境でこの対処方法を使用できない場合は、クライアントを保護し、アクセスを許可するシステムのIPアドレスの範囲として*を指定します。これは、クライアントがすべてのシステム(任意のIPアドレス)からの要求を受け付け、クライアントが事実上保護されないことを意味しますが、大量のログが記録される問題は解決します。

重要:

Cell Managerノード用に使用可能なすべてのホスト名を、保護する各クライアントのallow_hostsファイルに記述する必要があります。これによってフェイルオーバー時もクライアントへのアクセスが可能になります。誤って、アクセスできないクライアントが生じた場合は、そのクライアントに関するallow_hostsファイルを手作業で編集できます。

「StoreOnceデバイスはオフラインです」メッセージによるStoreonceSoftwareデバイスの障害

問題

StoreOnceSoftware (SOS)サービスで暗号制御通信を有効にしている、デフォルトのhpdpcert.pemを使用する場合に、Data Protector 9.05以降のバージョンにアップグレードすると、SOSが以降の接続を承認しなくなります。

対処方法

Data Protector 9.05以降にアップグレードした後にSOSが接続を必ず承認するようにするには、『9.08 Data Protector インストールガイド』(第6章: インストールの保守 > セキュリティの留意事項 > 暗号制御通信の管理)を参照してください。

暗号制御通信

MoM Cell ManagerにインストールされているMedia Agentの使用に失敗する

問題

CMMDBを構成し暗号制御通信を有効にしているMoM環境で、異なるセルからクライアントをバックアップするためにいずれか1つのCell Manager上にインストールしたMedia Agentを使用すると、処理が

失敗して次のエラーメッセージが表示されます。

```
[Major] From: BSM@cmcomputer.company.com "BackupSpec" Time: 14.04.2015 08:39:36  
[61:4006] Could not connect to inet in order to start BMA@macomputer.company.com  
"Device".[Critical] From: BSM@cmcomputer.company.com "BackupSpec" Time:  
14.04.2015 08:39:36 None of the Disk Agents completed successfully. Session has  
failed.
```

対処方法

Cell Managerホスト上にインストールしていないMedia Agentを使用します。

または

Media Agentホストを使用しているCell Managerについて、問題が発生しているCell ManagerまたはMedia Agentホスト上の暗号制御通信例外を削除します。

MoMでの暗号化通信の有効化に失敗する

問題

MOM環境全体の暗号制御通信を有効にすると、一部のセルで暗号制御通信がCell Manager上でのみ有効になり、対応するクライアント上では有効になりません。

この問題は、問題のCell Manager上の協定標準時(UST)がMoMサーバー上のUSTと同一でない場合に発生します。これにより、新しく生成した証明書は有効にならず、残りのクライアントに対して証明書を生成することができなくなります。

対処方法

1. USTはMoM環境内のすべてのCell Managerとクライアント上で必ず同一にします。
2. 問題のCell Manager上の暗号制御通信を削除します。『Data Protectorインストールガイド』の「暗号制御通信を手動で無効にする方法」を参照してください。
3. MOM環境内で暗号化通信をもう一度有効にします。

セルでの暗号化通信の無効化に失敗する

問題

セル全体で暗号化通信を無効にしたにもかかわらず、一部のクライアントおよびCell Managerで暗号制御通信が有効であり続けます。

暗号化通信がまだ使用可能になっているセル内にクライアントが存在する場合、Cell Managerで暗号制御通信を無効にすることはできません。暗号化通信がクライアント上で無効にならないのは、以下の原因が考えられます。

- クライアントがオフラインになっている。
- クライアントがData Protector 9.03以降のバージョンにアップグレードされていない。
- Cell Managerとクライアント間の暗号制御通信が切断されている(クライアント上の証明書の期限

が切れているなど)。

対処方法

次の2つの解決策があります。

1. 標準機能を使用して、問題のクライアントをセルから削除し、Cell Manager上の暗号化通信を無効にします。
2. 『Data Protector インストールガイド』の「暗号制御通信を手動で無効にする方法」に記載されている説明に従って、問題のクライアントとCell Manager上の暗号化通信を無効にします。

Microsoft以外のクラスターでの暗号化通信の無効化に失敗する

問題

Microsoft以外のクラスター(Cell ManagerをServiceguardクラスターで構成しているなど)で構成されたセルで暗号制御通信を無効にすると、一部のノードでは暗号化通信が有効なままになり、一部のノードでは無効になります。

暗号化通信がまだ使用可能になっているセル内にクライアントが存在する場合、Cell Managerで暗号制御通信を無効にすることはできません。Cell Managerがクラスター内に構成されている場合に発生する問題です。Data ProtectorはMicrosoft以外のクラスターに含まれるシステムを正確に検出できないため、暗号化通信はノックアウトノード上では無効になりますが、アクティブノード(現在のCell Manager)上では有効なままになります。

クラスターノードの1つが停止した場合も同じ問題が発生することがあります。

対処方法

1. クラスター仮想サーバーを含む、クラスターに含まれるすべてのノード上で暗号化通信を有効にして、整合性のある状態にします。
2. 『Data Protector インストールガイド』の「Cell Managerがクラスター対応の場合に暗号化通信を無効にする方法」の項に記載される手順を実行します。
3. または『Data Protectorインストールガイド』の「暗号制御通信を手動で無効にする方法」の項を参照してください。

暗号化通信が機能しない

問題

セル内で暗号制御通信を有効にした後にCell Managerとクライアント間の通信が正しく機能しなくなります。この問題はさまざまな形で現れます。たとえば、バックアップ仕様を作成するときにクライアント上でファイルをブラウザできない場合があります。

原因として考えられるのは、Cell Manager上の協定標準時(UST)とクライアント上のUSTとの不一致です。2分の誤差でも問題が生じます。このため、新しく生成された証明書が有効になっていない可能性があります。

対処方法

1. Cell ManagerとクライアントのUSTを同一にします。
2. 数分間待ちます。何分間待つかは、時間のずれによって異なります。
3. 問題が解決されない場合は、『Data Protector インストールガイド』の「暗号制御通信を手動で無効にする方法」に記載される説明に従って暗号化通信を無効にします。
4. もう一度暗号化通信を有効にします。

インストールセッションが失敗し、エラーメッセージが表示される場合がある

問題

暗号制御通信を有効にして、インストールサーバーを2つのセルで共有するとインストールセッションが失敗します。以下のエラーメッセージが表示されます。

```
Cannot start session
```

```
ErrorNo <3069>
```

```
Error Text <[12:3069] Certificate verification has failed. The certificate is signed by an untrusted certificate authority (CA).>
```

対処方法

インストールセッションを正常に完了させるには、次のいずれかを実行する必要があります。

- インストールで使用するインストールサーバーが現在のセルに属するようにします。
- セル内のクライアントとインストールサーバー間の信頼を確立するように暗号制御通信を構成します。

クライアント上で暗号制御通信を有効にした後にクライアントに接続できない

問題

クライアント上で暗号制御通信を有効にした後に、クライアントに接続できなくなり、-omnirsh client.company.com INFOを実行すると次のエラーメッセージが表示されます。

```
[Critical] From: OMNIRSH@cellserver.company.com "cli" Time: 4/9/2015 4:18:25 PM  
Cannot connect to host: Secure communication protocol negotiation error when trying to establish a connection. Check the validity of certificates and their configuration.
```

対処方法

アプリケーションシステム上でクライアントシステムの整合性をチェックします。証明書を生成した直後でも、クライアント上の時間が正しく設定されていないと、証明書が有効にならない可能性があります。

重要:

証明書の有効性と有効期限を管理する必要があります。有効でなくなった(またはまだ有効になっていない)証明書は機能しません。

opensslを使用すると、証明書の使用期限をチェックできます。例:

```
ProgramData\OmniBack\Config\Server\certificates> openssl x509 -in <hostname>_cert.pem -subject -dates -noout
```

```
subject= /C=US/ST=CA/O=HEWLETT-PACKARD/CN=<hostname>  
notBefore=Apr 8 10:55:13 2015 GMT  
notAfter=Apr 5 10:55:13 2025 GMT
```

opensslを使用して、証明書の期限が近いかどうかをチェックすることもできます。たとえば、opensslでは、証明書が後1日で期限切れとなるかどうかを示すことができます。

```
ProgramData\OmniBack\Config\Server\certificates> openssl x509 -in <hostname>_cert.pem -checkend 86400
```

```
The certificate will not expire.
```

Cell Managerで暗号化通信を有効にすると、CRS接続に失敗する

問題

Cell Manager上で暗号制御通信を有効にした後にCRS接続が失敗します。Cell Managerサービスは実行されていますがCRS接続が失敗します。

対処方法

OpenSSLを使用して証明書の信頼が有効であるかどうかをチェックします。

Cell Managerホスト上の証明書が正しいことを確認する

1. Cell Managerホスト上の暗号化を有効にした後にホストからの接続が機能しない場合、Cell Managerホスト上の証明書が正しいことを確認します。以下の順に選択します。

- **Windowsの場合:** <Data_Protector_program_data>\Config\client\certificates
- **UNIX:** /etc/opt/omni/client/certificates

2. openssl verify -verbose -CAfile CM1_cacert.pem <host Cell Manager>_cert.pemを実行します。

3. 証明書に問題がある場合は、ProgramData\OmniBack\Config\client\configファイルを削除して暗号化を無効にし、証明書を再生成して、もう一度暗号化を有効にします。この処理を行うには、omnicc -encryption -enable <host Cell Manager> -recreate_certを実行します。

同じCell Managerに属する2つのホスト間の適切な接続について証明書の信頼が確立していることを確認する

同じCell Managerに属していない2つのホストが適切に接続するように、証明書の信頼を正しく設定する必要があります。この処理を行うには、openssl verify -verbose -CAfile trusted_

cert.pem host_cert.pemを実行します。適切な信頼が有効であることを確認するには、両方のホストの証明書を相互に検証する必要があります。

異なるCell Managerに属する2つのホスト間の適切な接続について証明書の信頼が確立していることを確認する

適切な信頼が有効であることを確認するには、次のコマンドを実行します。

- openssl verify -verbose -CAfile <Cell Manager 1>_cacert.pem host1_cert.pem
- openssl verify -verbose -CAfile <Cell Manager 2>_cacert.pem host1_cert.pem
- openssl verify -verbose -CAfile <Cell Manager 2>_cacert.pem host2_cert.pem
- openssl verify -verbose -CAfile <Cell Manager 1>_cacert.pem host2_cert.pem

第3章: Data Protectorのサービスおよびデーモンのトラブルシューティング

概要

Data Protectorのサービス(Windowsシステム)およびデーモン(UNIXシステム)はCell Manager上で動作します。サービス/デーモンが実行されているかどうかを確認するには、`omnisv -status`コマンドを実行します。

Data Protectorサービス/デーモンが停止しているか、Data Protectorターゲットクライアント上にインストールされていないと思われる場合は、名前解決に関する問題が発生していないかを確認します。

Data Protectorプロセス一覧

以下の表は、Data Protectorの待機中や、バックアップ、復元、メディア管理セッションなどの基本処理が行われるときに、どのプロセスが実行されるかを示しています。

		常時	バックアップ	復元	メディア管理
Cell Manager	Windows	Omnilnet.exe mmd.exe crs.exe kms.exe hpdp-idb hpdp-idb-cp hpdp-as	bsm.exe	rsm.exe	msm.exe
	UNIX	mmd crs kms hpdp-idb (postgres) hpdp-idb-cp (pgbouncer) hpdp-as (standalone.sh)	bsm	rsm	msm
Disk Agentクライアント	Windows	Omnilnet.exe	vbda.exe	vrda.exe	
	UNIX		vbda	vrda	

Media Agent クライアント	Windows	Omninet.exe	bma.exe	ma.exe	mma.exe
	UNIX		bma	ma	mma

Data ProtectorのサービスをWindowsで起動する際の問題

サービスを起動するためのパーミッションがない

問題

以下のエラーが表示されます。

Could not start the *ServiceName* on *SystemName*.

Access is denied.

対処方法

システム管理者が、管理対象のシステム上で、このユーザーに対してサービスを起動、終了、変更するパーミッションを設定する必要があります。

変更されたサービスアカウントのプロパティ

問題

サービスアカウントにサービスを起動するためのパーミッションがない場合、またはサービスアカウントのプロパティ(パスワードなど)が変更されている場合、以下のエラーが表示されます。

The Data Protector Inet service failed to start due to the following error:

The service did not start due to a logon failure.

対処方法

[コントロールパネル]で[管理ツール]をクリックし、[サービス]をダブルクリックして、サービスのパラメーターを変更します。

上記を行っても問題が解決しない場合は、システム管理者に連絡して、適切なパーミッションを持つアカウントを設定するよう依頼してください。Adminグループのメンバーで、[Log on as a service]というユーザー権限を持つアカウントを作成する必要があります。

指定したサービスが見つからない

問題

サービスの場所は、ImagePathレジストリキーに登録されています。このキーで指定された場所を実行

可能ファイルが存在しない場合は、次のエラーが表示されます。

Could not start the *ServiceName* on *SystemName*. The system can not find the file specified!

対処方法

IDBを保持したまま、Cell ManagerにData Protectorを再インストールします。

CRSサービスを起動するとMMDが異常終了する

問題

Data Protector CRSサービスが起動に失敗し、mmd.exeにより診断ツール[Dr. Watson]が起動された場合は、データベースログファイルが破損していることが考えられます。

対処方法

1. デフォルトのData Protector内部データベースディレクトリからmmd.ctxファイルを削除します。
2. omnisv -stopコマンドとomnisv -startコマンドを使用してサービスを再起動します。

Data ProtectorのデーモンをUNIXで起動する際の問題

UNIX Cell Managerでは以下のデーモンが実行されます。

- /opt/omni/sbinディレクトリ内:
 - Data Protector CRSデーモン: crs
 - Data Protector IDBデーモン: hdp-idb (postgres)、hdp-idb-cp (pgbouncer)、hdp-as (standalone.sh)
 - Data Protectorメディア管理デーモン: mmd

通常、これらのデーモンはシステムの起動時に自動的に起動します。

Data Protector Inetプロセス(/opt/omni/sbin/inet)は、アプリケーションがData Protectorポート(デフォルトのポートは5565)へ接続しようとした場合にシステムのinetデーモンによって起動されます。

Data Protectorの各デーモンに対して、手動による開始と停止およびステータスのチェックを行うには、rootとしてCell Managerにログインし、/opt/omni/sbinディレクトリから次のコマンドを実行します。

- omnisv -stop
- omnisv -start
- omnisv -status

Data ProtectorのCell Managerデーモンを起動できない

問題

omnisv -startコマンドの出力は次のようになります。

```
Could not start the Cell Manager daemon.
```

対処方法

詳細についてはomni_start.logファイルを参照してください。このファイルはデフォルトのData Protector一時ファイルディレクトリに置かれています。

以下の構成ファイルが存在することを確認します。

- /etc/opt/omni/server/options/global
- /etc/opt/omni/server/options/users/UserList
- /etc/opt/omni/server/options/ClassSpec

hpd-idbサービスが起動に失敗し、共有メモリの問題をレポートする

問題

HP-UXシステムでは、hpd-idbサービスが起動に失敗し、以下のエラーがPostgreSQLログファイル(/var/opt/omni/server/db80/pg/pg_log)に記録されます。

```
FATAL: could not create shared memory segment: Not enough space
```

```
DETAIL: Failed system call was shmget(key=7112001, size=2473459712, 03600)
```

この問題は、hpd-idbサービスが、システムのメモリが断片化されているため要求された量の共有メモリを取得できないときに発生します。

対処方法

システムを再起動してメモリをデフラグします。

CRSサービスを起動するとMMDが異常終了する

問題

Data Protector CRSサービスが起動に失敗し、以下のエラーが表示されます。

```
[Critical] From: CRS@computer.company.com "" Time: 03/04/13 11:47:24 Unable to start MMD: Unknown internal error..
```

データベースログファイルが破損していることが考えられます。

対処方法

1. デフォルトのData Protector内部データベースディレクトリからmmd.ctxファイルを削除します。
2. omniv -stopコマンドとomniv -startコマンドを使用してサービスを再起動します。

Data Protectorプロセスの他の問題

Name Server Cachingが無効になると、UNIX上のData Protectorのパフォーマンスに影響を及ぼす

問題

Name Server Caching(nscd)デーモンが無効になると、UNIX上のData Protectorのパフォーマンスに悪影響を及ぼすことがあります。

UNIXおよびWindowsシステムにはデフォルトの名前サーバーキャッシュがありません。Name Server Caching(nscd)デーモンが無効になると、Data Protector操作によって大量のDNS要求が作成され、パフォーマンスが低下することがあります。

対処方法

1. Name Server Caching(nscd)デーモンが有効になっており、構成されていることを確認します。
nscdの構成はプラットフォームごとに異なります。詳細は、お使いのプラットフォームのマニュアルを参照してください。
2. DNS設定をチェックして、etc/resolv.confファイル内の最初のローカルドメインでDNS検索順序が正しく構成されていることを確認します。
3. omniv -stopコマンドとomniv -startコマンドを使用してサービスを再起動します。

バックアップの実行中、一定時間経過後にバックアップセッションが停止し、BSMが応答しなくなる

問題

この問題は、ファイアウォールがアクティブではない接続を閉じたことにより発生する場合があります。

対処方法

接続をアクティブに保ち、ファイアウォールがその接続を閉じないようにします。以下のomnircオプションを設定します。

```
OB2IPCKEERALIVE=1
OB2IPCKEERALIVETIME=number_of_seconds
OB2IPCKEERALIVEINTERVAL=number_of_seconds
```

OB2IPCKEERALIVETIMEには、非アクティブな接続の猶予時間を指定します。この時間を超過すると、

最初のkeep-aliveパケットが送信されます。OB2IPCKEERALIVEINTERVALには、ACKを受信しない場合に次のkeep-aliveパケットを送信するまでの間隔を指定します。このオプションはCell Managerシステムで設定する必要があります。

第4章: ユーザーインターフェイスのトラブルシューティング

グラフィカルユーザーインターフェイスの問題

Data Protectorグラフィカルユーザーインターフェイスの問題が発生する原因は、通常、サービスが実行されていない、サービスがインストールされていない、または、ネットワーク通信の問題が発生しているの、いずれかです。

接続性とアクセシビリティの問題

Cell Managerにアクセスするパーミッションがない

問題
以下のメッセージが表示されます。 Your Data Protector administrator set your user rights so that you do not have access to any Data Protector functionality. Contact your Data Protector administrator for details.
対処方法
Data Protector管理者に、ユーザーとして追加することと、セル内での適切なユーザー権限の付与を要請します。 ユーザーグループの設定方法については、『Data Protectorヘルプ』のキーワード「ユーザーグループ」で表示される内容を参照してください。

リモートシステムへの接続が拒否される

問題
Windows上で、telnet <i>hostname</i> 5565コマンドを実行すると、Connection refusedが返されます。
対処方法
<ul style="list-style-type: none">• Data Protector Inetサービスがリモートシステム上で実行されていない場合は、omnisv -startコマンドを実行して、サービスを起動します。• Data Protectorがリモートシステム上にインストールされていない場合は、インストールします。

Cell Manager上でinetが応答しない

問題

以下のメッセージが表示されます。

```
Cannot access the system (inet is not responding). The Cell Manager host is not reachable, is not up and running, or has no Data Protector software installed and configured on it.
```

対処方法

システム間の通信に問題がない場合は、telnetを使ってソフトウェアがインストールされているかチェックしてください。

一部のコンポーネントが正しくインストールされていないことが考えられます。『Data Protectorインストールガイド』を参照し、インストール手順を確認してください。

インストールに問題がない場合は、`omnisv -status`コマンドを実行して、Cell Manager上でサービスが正常に実行されているかチェックしてください。

ファイルシステムのブラウザエージェントを起動できない

問題

十分な権限を持つData Protectorユーザーがバックアップ仕様を保存してバックアップを開始しようとしたときに、次のエラーが発生します。

```
Unable to start filesystem browse agent
```

対処方法

Data Protectorユーザーは、inet内に適切に構成された偽装の詳細情報が必要です。

コマンドラインインターフェイスの問題

Data Protectorコマンドを実行できない

問題

Data Protectorコマンドをコマンドプロンプトまたはターミナルウィンドウで実行しようとした後、コマンドラインインタープリターで、コマンドが見つからないことがレポートされます。

対処方法

オペレーティングシステム設定のPATH環境変数の値を、コマンドの場所までのパスを使用して拡張します。この対処方法により、どのディレクトリからでもData Protectorコマンドを実行できます。この値を拡

張しない場合、コマンドは、『*Data Protector Command Line Interface Reference*』のomniintroリファレンスページまたはomniintroのmanページに記載されている場所からのみ実行できます。

第5章: バックアップと復元のセッションのトラブルシューティング

Storage Optimizerのスタブの復元でエラーがレポートされる

増分バックアップの代わりにフルバックアップが実行される

増分バックアップを指定したにもかかわらず、フルバックアップが実行されます。これには、以下の理由が考えられます。

前回のフルバックアップがない

問題
オブジェクトの増分バックアップを実行する前に、フルバックアップを実行する必要があります。Data Protectorは、どのファイルが変更され、増分バックアップに含める必要があるかを比較するベースとしてフルバックアップを使用します。保護されたフルバックアップがない場合は、フルバックアップが実行されます。
対処方法
そのオブジェクトのフルバックアップが存在し、保護設定されているかどうかを確認します。

説明を変更した

問題
バックアップオブジェクトは、クライアント、マウントポイント、および説明によって定義されます。これらの3つの値のいずれかが変更された場合、Data Protectorはそのオブジェクトを新しいバックアップオブジェクトとみなし、増分バックアップの代わりにフルバックアップを実行します。
対処方法
フルバックアップと増分バックアップの両方に同じ説明を使用します。

ツリーを変更した

問題
保護されたフルバックアップがすでに存在しますが、増分バックアップとは異なるツリーが含まれています。以下の2つの理由が考えられます。
<ul style="list-style-type: none">保護設定されたフルバックアップに関するバックアップ仕様のツリーを変更した。

- 同じバックアップオブジェクトを含んでいるが、バックアップオブジェクトに異なるツリーが指定されている複数のバックアップ仕様を作成した。

対処方法

同じバックアップオブジェクトを含んだ複数のバックアップ仕様がある場合は、(自動的に生成される)バックアップオブジェクトのユニバーサルな説明を変更します。Data Protectorでは、それらは新しいオブジェクトとみなされ、フルバックアップが実行されます。フルバックアップの実行後は、増分バックアップが可能になります。

バックアップオーナーが違う

問題

バックアップをプライベートとして実行するように設定した場合は、バックアップを開始したユーザーがそのデータのオーナーになります。たとえば、ユーザーAがフルバックアップを実行し、ユーザーBが増分バックアップを開始しようとすると、増分バックアップはフルバックアップとして実行されます。これは、ユーザーAのデータがプライベートであり、ユーザーBの増分バックアップのベースとしては使用できないためです。

対処方法

[バックアップ仕様オプション]の[拡張]でバックアップセッションの[所有権]を指定します。バックアップオーナーはAdminユーザーグループに所属している必要があります。このユーザーは、バックアップセッションを実際に開始したユーザーに関係なく、このバックアップ仕様に基づいてすべてのバックアップのオーナーとなります。

手順については、『Data Protectorヘルプ』のキーワード「バックアップオプションの設定」で表示される内容を参照してください。

アップグレード後に拡張増分が実行されない

問題

この問題は、Windows、HP-UX、およびLinuxシステムで発生する場合があります。A.06.11のバージョンからData Protectorにアップグレードした場合、古い拡張増分バックアップのレポジトリを新バージョンの製品で使用できなくなります。そのため、フルバックアップを実行します。フルバックアップ中、拡張増分バックアップのレポジトリが以下の場所に新規作成されます。

Windowsシステムの場合: `Data_Protector_home\enhincrd`

UNIXシステムの場合: `/var/opt/omni/enhincrd`

対処方法

フルバックアップを実行します。拡張増分バックアップのレポジトリが新規作成され、拡張増分バックアップを実行できます。

拡張増分バックアップでZDBファイルシステム/バックアップを実行すると、フルバックアップが実行される

問題

マウントパスにセッションIDディレクトリを追加するようにZDBを構成している場合、[拡張増分バックアップ]オプションを有効にしてZDBファイルシステム/バックアップを実行すると、フルバックアップが実行されません。

対処方法

[バックアップシステム]オプションセクションの下のマウントパスに追加されるディレクトリに[ホスト名]オプションを使用します。[ファイルシステムを目的のマウントポイントで自動的にアンマウントする]オプションを使用して次のセッションの前にマウントパスがフリーになるようにするか、または[バックアップシステムを使用可能にしておく]が選択されていないことを確認します。

Data Protectorがセッションを開始できない

対話型セッションを開始できない

問題

バックアップが開始されるたびに、バックアップセッションを開始するためのパーミッションが必要となり、Data Protectorを現在実行しているユーザーについてパーミッションの有無がチェックされます。ユーザーがこのパーミッションを持っていない場合は、セッションを開始できません。

対処方法

ユーザーが適切な権限のあるユーザーグループに所属していることを確認してください。

ユーザーグループの設定方法については、『Data Protectorヘルプ』のキーワード「ユーザーグループ」で表示される内容を参照してください。

スケジュール設定されたセッションが実行されない

問題

スケジュール設定されていたセッションを開始するData ProtectorシステムアカウントがCell ManagerのAdminユーザーグループに含まれていないため、スケジュール設定されていたセッションは実行されません。

このアカウントは、インストール時にCell ManagerでData ProtectorのAdminグループに追加されます。このアカウントを変更してそのパーミッションが削除された場合、またはサービスアカウントが変更された場合は、スケジュール設定されていたセッションは実行されません。

対処方法

Data ProtectorアカウントをCell ManagerのAdminユーザーグループに追加します。

セッションが正常に行われず、「使用可能なライセンスがありません」というステータスメッセージが表示される

問題

バックアップセッションを開始するには、使用可能なライセンスがData Protectorですでにチェックされている必要があります。ライセンスが使用可能でない場合は、バックアップセッションは正常に行われず、Data Protectorからセッションステータスを示すメッセージ「No licenses available」が表示されます。

対処方法

使用可能なライセンスの情報を取得するには、次のコマンドを実行します。

```
omnicc -check_licenses -detail
```

新しいライセンスを請求し、これを適用します。ライセンスの詳細については、『Data Protectorインストールガイド』を参照してください。

スケジュール設定したバックアップが開始されない (UNIXシステムの場合のみ)

問題

UNIXシステムで、スケジュール設定したバックアップが開始されない。

対処方法

omnisv -stopおよびomnisv -startを実行して、Data Protectorデーモンを停止または起動します。

デバイスにメディアが入っているのにマウント要求が発行される

バックアップセッション中に、バックアップデバイス内に使用可能なメディアがあるにもかかわらず、Data Protectorからマウントが要求される場合があります。これには、以下の理由が考えられます。

デバイス内のメディアが所属するメディアプールのポリシーが[追加不可能]である

問題

メディアに使用可能なスペースが残っていても、メディアプールのポリシーが[Non Appendable]に設定されていると、そのメディアは使用されません。

対処方法

メディアプールのポリシーを[Appendable]に変更して、メディアがいっぱいになるまでバックアップを追加できるようにしてください。

デバイス内のメディアがまだフォーマットされていない

問題

デフォルトでは、メディアは自動的にフォーマットされません。使用可能なフォーマット済みメディアがない場合は、マウント要求が発行されます。

対処方法

メディアをフォーマットします。

手順については、『Data Protectorヘルプ』のキーワード「メディアのフォーマット」で表示される内容を参照してください。

デバイス内のメディアが事前割り当てリストで指定されているメディアと違っている

問題

デバイス内のメディアはフォーマットされていますが、バックアップ仕様の事前割り当てリストで指定されているメディアと違っています。また、指定されているメディアプールのポリシーが[Strict]になっています。

メディアの事前割り当てリストと[Strict]ポリシーを併用している場合は、事前割り当てリストで指定されているメディアがバックアップの開始時にデバイス内で使用可能になっている必要があります。

対処方法

- 事前割り当てリストを併用しながら、デバイス内にある使用可能なメディアを使用するには、メディアプールポリシーを[Loose]に変更します。
- デバイス内にある使用可能なメディアのいずれかを使用するには、バックアップ仕様から事前割り当てリストを削除します。削除するには、バックアップ仕様でバックアップデバイスのオプションを変更します。

ファイルライブラリに対してマウント要求が発行される ファイルライブラリデバイスのディスクに空き領域がない

問題

ファイルライブラリデバイスの使用中に、以下のメッセージとともにマウント要求が発行されることがあります。

There is no disk space available for file library File Library Device. Add some new disk space to this library.

対処方法

ファイルライブラリが置かれているディスクの空き領域を増やす。

- ファイルのバックアップ先となるディスク上の空き領域を増やす。
- ファイルライブラリデバイスが存在するシステムにディスクを追加する。

ファイル名に関する問題

ファイル名またはセッションメッセージがData Protector GUI上に正常に表示されない

問題

非ASCII文字を含むファイル名やセッションメッセージは正しく表示されないことがあります。これは、Data Protector GUIでファイル名やセッションメッセージを表示するのに、不正な文字エンコードが使用されているためです。

対処方法

適切なエンコードを指定します。[表示]メニューから[エンコード]を選択し、適切な文字コードセットを選択します。

クラスターに関する問題

IDBサービスが同期しない

問題

UNIXシステムでは、Serviceguard環境内の別の場所にIDBを復元する場合で、1つまたは複数のクラ

スターノードがオフラインの時に、IDBサービスがセッション完了後に全ノードで同期されません。

対処方法

クラスター環境で全ノードのIDBデータファイルの場所を同期するには、アクティブなクラスターノードで `omnidbutil -sync_srv` コマンドを実行します。

Windows NTFS Change Log Providerを使用した共有クラスターボリュームの増分ファイルシステムのバックアップが、クラスターのフェイルオーバー後にフルバックアップにフォールバックする

問題

バックアップ仕様で[可能な場合は、標準で用意されているファイルシステムのChange Log Providerを使用]オプションを使用してクラスター共有ボリュームの増分ファイルシステムバックアップを実行すると、代わりにフルバックアップが実行され、以下のエラーメッセージが表示されます。

```
[Major] From: VBDA@Host Name "F:" Time: Date Time
```

```
The Change Log Provider could not use the Directory Database. This session will use the normal file system traversal.
```

対処方法

増分バックアップが正しく実行されたことを確認するため、Change Log Providerデータベースから個々のクラスター共有ボリュームへのシンボリックリンクを以下のように作成します。

1. 共有ボリュームのChange Log Providerデータベースにダイレクト可能な共有ディスクを選択します。Data Protectorクラスター対応のCell Managerの場合、Data Protector共有ディスクを選択できません。
2. 以下の例のように共有ディスクにディレクトリを作成します: `E:\Omniback\clp`
3. ディレクトリ `Data_Protector_home\clp` に移動し、作成したディレクトリへのシンボリックリンクを作成します。

たとえば、共有ディスクJをバックアップするには、

```
mklink /D J E:\Omniback\clp\J
```

ここで、`E:\Omniback\clp\J` は共有ディスクJについて作成されたシンボリックリンクでEはその他のクラスターノードからアクセス可能なクラスター共有ボリュームです。

クラスターのフェイルオーバー後に増分バックアップが行われたすべてのクラスターノード上の共有ボリュームに対するChange Log Providerデータベースリンクを作成します。

Cell Managerがクラスター内に構成されている場合の復元の問題

問題

[Restart backup of all objects]バックアップオプションを有効にして、クラスター対応 Data Protector Cell Managerを使用したバックアップが実行されました。バックアップ中にフェイルオーバーが発生し、他のクラスターノードでバックアップセッションが再開され、正常に終了しました。最後のバックアップから復元を行うと、セッションは正常に終了しますが、次のエラーが報告されます。

You have selected a version that was not successfully completed. If you restore from such a backup, some or all the files may not be restored correctly.

Cell Managerクラスターノード上のシステム時刻が同期化されていない場合、失敗したバックアップに、再開されたバックアップよりも新しいタイムスタンプが付くことがあります。復元用のデータを選択したときに、最後のバックアップバージョンがデフォルトで選択され、失敗したバックアップからの復元が行われず。

対処方法

最後の正常なバックアップから復元を行うには、正しいバックアップバージョンを復元対象として選択します。

このようなエラーを防止するには、ネットワーク上にタイムサーバーを構成することをお勧めします。これにより、Cell Managerクラスターノード上でシステム時刻が自動的に同期化されます。

Microsoft Cluster ServerノードのCONFIGURATIONオブジェクトのバックアップが失敗する

問題

Windows Server 2008またはWindows Server 2012システムでは、クラスターノード上の CONFIGURATIONオブジェクトのバックアップが次のエラーで失敗します。

```
[Minor] From: VBDA@computer.company.com "CONFIGURATION:" Time: Date Time
```

```
[81:141] \Registry\0.Cluster
```

```
Cannot export configuration object: (Details unknown.) = backup incomplete
```

対処方法

Cluster Serviceの実行に使用されるユーザーアカウントでData Protector Inetサービスを再開して、バックアップを再開します。

HP-UXおよびLinuxのCell ManagerでのIDBの復元

HP-UXおよびLinuxのCell ManagerでIDBの復元に失敗することがあります。この項では、この復元の失敗についてのいくつかの考えられる原因について簡単に説明します。

別のCell ManagerでのIDBの復元は失敗する可能性がある

問題

別のCell ManagerでのIDBの復元が失敗して次のメッセージが表示される場合があります。

```
Recovery of the Internal Database failed.
```

対処方法

復元が失敗したCell ManagerのオペレーティングシステムユーザーのユーザーIDとグループIDを変更して、IDBのバックアップを作成したCell ManagerのオペレーティングシステムユーザーのユーザーIDとグループIDに一致させます。

復元プロセスの終了時にIDBの復元に失敗する

問題

復元プロセスの終了時にIDBの復元が失敗して次のメッセージが表示されます。

```
cannot execute omnidbutil -clear command
```

対処方法

これは、HP-UX Cell Managerでは、別のCell Managerに復元しようとしている場合、あるいは同じCell Manager上であるが、バックアップセッションの復元後または新しいCell Managerをインストールした後にpostgresパスワードを変更した場合に発生する可能性があります。

注: Linux環境では、復元は正常に完了します。これは、Linuxは、HP-UXとは対照的に、データベース上で主にオペレーティングシステム認証を使用しているためです。HP-UXはパスワード認証を使用しており、この場合パスワードファイルが正しく復元されません。ただし、Linux環境でも、正しいパスワードファイルを保持するためにこの対処方法を適用する必要があります。

手順

1. IDB全体を復元する特定の時点まで、構成ファイルのみを別の場所<restore-conf>に復元します。
2. DCBFを除くIDB全体を復元するか、またはDCBF全体を元の場所に復元します。
3. /etc/opt/omni/server/idb/idb.configのバックアップを次の場所に保存します:
idb.config.bkp
4. 場所<restore-conf>から元の場所にファイルのコピーを実行します。
 - a. `cp <restore-conf>/etc/opt/omni/server/idb/idb.config /etc/opt/omni/server/idb/idb.config`
 - b. `cp <restore-conf>/etc/opt/omni/server/idb/ulist /etc/opt/omni/server/idb/ulist`
 - c. `cp <restore-conf>/etc/opt/omni/server/AppServer/standalone.xml`

問題

/etc/opt/omni/server/AppServer/standalone.xml

5. 正しい場所をポイントするようにidb.config内の以下のフィールドを修正します(正しい場所はidb.config.bkpに保存されます)。
 - a. PGDATA_PG='/space/restore1/pg';
 - b. PGDATA_IDB='/space/restore1/idb';
 - c. PGDATA_JCE='/space/restore1/jce';
 - d. PGWALPATH='/space/restore1/pg/pg_xlog_archive' ;
6. Data Protectorサービスを停止してから、開始します。
 - a. omniv stopを実行します(これには時間がかかる場合があります)。
 - b. run omniv start
 - c. run omnidbutil -clear

復元操作の実行後、Data Protector GUIからCell Managerへの接続が失敗する

問題

復元操作の完了後、および次の問題に対する対処方法の適用後に

別のCell ManagerでIDBの復元に失敗する可能性があり、その結果復元プロセスの終了時にIDBの復元に失敗し、

これによりGUIからCell Managerへの接続が失敗して次のエラーが表示されます。

A server error has occurred. Reported error message: couldn't connect to host.

対処方法

1. /etc/opt/omni/server/AppServer/standalone.xmlファイルのバックアップを作成する
2. /etc/opt/omni/server/AppServer/standalone.xml 内のすべてのキーストアと信頼ストアのパスワードを次の場所に保存されているパスワードに置き換える:
/etc/opt/omni/client/components/webservice.properties

その他の問題

Storage Optimizerのスタブの復元でエラーがレポートされる

問題

ターゲットファイルがシステム上に既に存在している場合でも、Data ProtectorはStorage Optimizerのスタブの復元に失敗し、次のエラーが報告される:

「ファイルを置換できません」

対処方法

この問題は、既存のファイルが最近開かれた場合に発生する可能性があります。以下のいずれかの対処方法を実行できます。

- a) ファイルを別の場所に復元する
- b) Storage Optimizerがファイルをリリースするまで待機し、再試行する
- c) 既存のファイルの名前を変更する

バックアップの保護期限が終了した

問題

バックアップのスケジュール設定時にフルバックアップと増分バックアップの両方に対して同じ保護期間を設定すると、増分バックアップがその基準となるフルバックアップと同じ期間保護されることとなります。つまり、フルバックアップの期限が切れた時点で、増分バックアップの期限も切れることとなります。期限切れのフルバックアップをベースにする増分バックアップは、復元できません。

対処方法

増分バックアップよりもフルバックアップの方が保護期間が長くなるように構成します。

フルバックアップと増分バックアップの保護期間の差が、フルバックアップから次のフルバックアップ前の最後の増分バックアップまでの期間になるように設定する必要があります。

たとえば、増分バックアップを月曜日から金曜日まで実行し、フルバックアップを土曜日に行う場合は、フルバックアップの保護期間を増分バックアップよりも6日以上長く設定する必要があります。これにより、最後の増分バックアップの期限が切れるまで、フルバックアップが保護されて使用可能になります。

ファイルが大量であるために拡張増分バックアップが失敗する

問題

HP-UXシステムでは、バックアップ対象のファイルが多すぎると、拡張増分バックアップが失敗します。

対処方法

拡張増分バックアップでDisk Agentがより多くのメモリにアクセスできるようにするには、調整可能カーネルパラメーターmaxdsizを次のように設定します。

HP-UX 11.11システムの場合:

```
kmtune set maxdsiz=2147483648
```

```
kmtune set maxdsiz_64bit=2147483648
```

HP-UX 11.23/11.31システムの場合:

```
kctune set maxdsiz=2147483648
```

```
kctune set maxdsiz_64bit=2147483648
```

接続拒否エラーが断続的に発生する

問題

次の重大なエラーが表示されて、バックアップセッションが中止されます。

```
Cannot connect to Media Agent on system computer.company.com, port 40005 (IPC  
Cannot Connect System error: [10061] Connection refused)
```

この問題は、Media AgentがServer Edition以外のWindows上で実行されており、Disk Agentの同時処理数が5より大きな値に設定されている場合に発生します。Server Edition以外のWindowsオペレーティングシステム上のTCP/IPの実装により、Server Edition以外のWindowsオペレーティングシステムでは同時に5つの着信接続しか受け付けることができません。

対処方法

Disk Agentの同時処理数に5以下の値を設定してください。

バックアップ処理 (Cell Manager、Media Agentクライアント、Application Agentクライアント、ファイルサーバーなど)に頻繁に使用されるシステムには、サーバー版のWindowsを使用することをお勧めします。

ディスクイメージ復元時に予想外のマウント済みファイルシステムが検出される

問題

ディスクイメージの復元時に、復元対象のディスクイメージはマウントされたファイルシステムであるため復元されないというメッセージが表示されることがあります。

```
Object is a mounted filesystem = not restored.
```

これは、ディスクイメージ上のアプリケーションが特定のパターンをディスクイメージに保存しているためです。ディスクイメージ上のファイルシステムがマウント済みかどうかを確認するシステムコールでこのパターンが誤って解釈され、ディスクイメージ上にマウント済みのファイルシステムがあると表示されます。

対処方法

復元を開始する前に、復元対象のディスクイメージがあるData Protectorクライアント上で、以下のコマンドを入力してディスクイメージを消去します。

```
prealloc null_file 65536
```

```
dd if=null_file of=device_file
```

ここで、*device_file*は、復元対象のディスクイメージ用のデバイスファイルです。

アプリケーションデータベースの復元に関する問題

問題

データベースを復元しようとする、復元に失敗し、以下のいずれかのメッセージが表示されます。

- Cannot connect to target database
- Cannot create restore set

DNS環境の構成に問題があると、データベースアプリケーションに問題が発生することがあります。問題は以下のようなものです。

データベースのバックアップ時には、データベースが置かれているクライアントで起動したエージェントがクライアント名を `computer.company.com` としてデータベースに記録します。

復元時には、復元セッションマネージャーが `computer.company.com` への復元を試行しますが、このクライアントを `computer` としてしか認識していないため復元に失敗します。これは、DNSが正しく構成されていないため、クライアント名をフルネームに展開できないことが原因です。

また、DNSがCell Manager上では構成されているがアプリケーションクライアント上では構成されていない場合には、ロングネームをシステム名に変換できないという逆の問題が発生することがあります。

対処方法

TCP/IPプロトコルを設定し、DNSを正しく構成します。詳細については、『Data Protectorインストールガイド』の付録Bを参照してください。

HP-UX上でバックアップが失敗する

問題

バックアップ中に以下のエラーが発生することがあります。

Cannot allocate/attach shared memory (IPC Cannot Allocate Shared Memory Segment)
System error: [13] Permission denied) = aborting

対処方法

Disk AgentとMedia Agentの両方がインストールされているか、またはサポートされている統合ソフトウェアのいずれかとMedia AgentがインストールされているHP-UXクライアント上では、OB2SHMEM_IPCGLOBAL omnircオプションを1に設定します。

非同期の読み込みによりバックアップパフォーマンスが改善されない

問題

バックアップ仕様で選択された[非同期の読み込み] (Windows固有)オプションを使用しても、バックアッ

パフォーマンスが改善されないか、パフォーマンスが低下することさえあります。

対処方法

OB2DAASYNCが0に設定されていないか確認します。オプションを1に設定して非同期読み込みを常に使用するか、オプションをコメントアウトしてバックアップ仕様で**Asynchronous reading**オプションを使用します。

2. 非同期の読み込みがバックアップ環境に適しているかどうかを考慮します。通常、非同期読み込みは1 MBを超えるファイルに適しています。さらに、omnircオプションOB2DAASYNC_SECTORSの微調整を試みることもできます。原則として、ファイルのサイズ(バイト数)がオプションの値の2~3倍の大きさでなければなりません。

WindowsシステムでIIS構成オブジェクトのバックアップが失敗する

問題

Windows Vista、Windows 7、Windows 8、Windows Server 2008、またはWindows Server 2012システムで、IIS構成オブジェクトのバックアップ中に、Data Protectorから次のエラーが出力されます。

[Minor]

From: VBDA@computer.company.com "CONFIGURATION:" Time: Date & Time [81:141]

\IISDatabase Cannot export configuration object: (Details unknown.) = backup incomplete.

対処方法

IIS 6 Management Compatibilityの下にある**IIS 6 Metabase Compatibility**コンポーネントをインストールしてバックアップを再開します。

ハードリンクがあるボリュームからのサブツリーの復元が失敗する

問題

ハードリンクがあるボリュームからのサブツリーの復元が失敗し、次のメッセージが表示されます。

Lost connection to Filesystem restore DA named ""

incomplete.

対処方法

ハードリンクがあるツリーを復元する場合は、グローバルオプションのRepositionWithinRestoredObjectを0に設定します。

このオプションを0に設定すると、復元処理が少し遅くなることがありますが、ハードリンクを復元する場合は必ず必要です。このオプションは、デフォルトでは1に設定されています。

Mac OS X上で、共有メモリの容量が不十分であるためにバックアップセッションが失敗する

問題

Mac OS X上でデバイスブロックサイズを増やすと、以下のエラーメッセージが表示されバックアップセッションが失敗する場合があります。

```
[80:1003] Cannot allocate/attach shared memory (IPC Cannot Create Shared Memory Segment System error: [12] Cannot allocate memory ) => aborting.
```

対処方法

カーネルパラメーターkern.sysv.shmmax(共有メモリセグメントの最大サイズをより大きな値に設定します。パラメーターを32MBに設定することをお勧めします。

ミラー化されているシステム予約パーティションのバックアップが失敗した可能性がある

問題

システム予約済みパーティションと複数のフルボリュームオブジェクトをバックアップしようとしたときに、バックアップが失敗して次のいずれかのエラーメッセージが表示されます。

```
Fallback to legacy filesystem backup was not allowed. Aborting the backup.
```

```
Not a valid mount point => aborting.
```

注:

この問題は、VSSオプションを有効にしており、システム予約済みパーティションがミラー化される場合にのみ発生します。

対処方法

omnirc変数OB2_DISABLE_REGLIST_FOR_FULL_VOLUMEを1に設定して、バックアップを再開します。

中断されたファイルバックアップまたはファイルが見つからない

問題

システム予約済みパーティションと複数のフルボリュームオブジェクトをバックアップしようとしたときに、バックアップが失敗して次のいずれかのエラーメッセージが表示されます。

```
- Cannot read <number> bytes at offset <number>(:1): ([21] The device is not ready. ).
```

問題

- Cannot open: ([2] The system cannot find the file specified.) => not backed up.

注:

この問題は、VSSオプションを有効にしており、システム予約済みパーティションに複数のスナップショットを保持するだけの十分な空き容量がない場合にのみ発生します。

対処方法

omnirc変数OB2_DISABLE_REGLIST_FOR_FULL_VOLUMEを1に設定して、バックアップを再開します。問題が解決しない場合は、次のMicrosoft Webページにあるこの問題の解決方法を参照してください。

<http://support.microsoft.com/kb/2930294>

バックアップのスケジュールを試みたときにスケジューラーが失敗する

問題

複数のタイミングでバックアップのスケジュールを試みたときにスケジューラーが失敗する

対処方法

これはJavaサービスが原因で発生する可能性があります。この場合、以下の手順を実行します。

1. Data Protector GUIを閉じます。
2. omniv stopを実行します。
3. タスクマネージャーからJavaサービスを終了します。
4. omniv startを実行します。
5. Data Protector GUIを開きます。

データ重複排除機能がなしWindowsの重複排除ボリュームでZDBファイルシステムバックアップが失敗する

問題

データ重複排除機能をインストールせずに、Windowsバックアップホスト上でWindows重複排除ボリュームのZDBファイルシステムバックアップを実行すると、バックアップが失敗して次のエラーメッセージが表示されます。

[Warning] From: VBDA@computer.company.com "<volume label>" Time: <Date Time>

[81:77] <Path name>

Cannot open: ([1920] The file cannot be accessed by the system.) => not backed up.

問題

対処方法

1. バックアップホストにWindowsデータ重複排除機能をインストールします。
2. ZDB/バックアップ中にデータ重複排除ジョブが存在しないように、以下を実行します。
 - ZDB/バックアッププロセスの前または後に、データ重複排除ジョブをスケジュールします。
 - バックアップ前にデータ重複排除ジョブを停止する実行前スクリプトと、バックアップ後にこれらのジョブを開始する実行後スクリプトを実装します。

実行前および実行後スクリプトが失敗し、エラーメッセージが表示される

問題

pre-スクリプトとpost-execスクリプトは、次のエラーメッセージで失敗します:

```
[Major] From: OB2BAR_SQLBAR@hostname.com "(<Instance>)" Time: <DATE><TIME>
..\script.bat
Illegal command format. Command not executed.
[Major] From: OB2BAR_SQLBAR@hostname.com "(<Instance>)" Time: <DATE><TIME>
[131:104] Script returned error. (Return value: -1).
```

対処方法

エラーメッセージに、pre-スクリプトとpost-execスクリプトを正しい場所がないことが示されます。pre-スクリプトとpost-execスクリプトが次のディレクトリにあることを確認します:

- Windowsシステムの場合: *Data_Protector_home*\binディレクトリ、またはサブディレクトリ。
- Unixシステムの場合: /opt/omni/lbinディレクトリ、またはサブディレクトリ。

ここに表示される問題の記述で、SQLエージェントのエラーメッセージがリスト表示されます。pre-スクリプトとpost-execスクリプトに失敗したときに、すべての統合ソフトウェアとZDBモジュールに対して同様のエラーメッセージが表示されます。

OB2OEXECOFFが設定されている場合、実行前および実行後スクリプトが失敗する

問題

pre-スクリプトとpost-execスクリプトの実行が、次のエラーメッセージで失敗する:

```
[Major] From: OB2BAR_SQLBAR@hostname.com "(<Instance>)" Time: <DATE><TIME>
OB2OEXECOFF変数の値によって、このホストに対する実行前および実行後スクリプトが妨げられる。
```

問題

対処方法

エラーメッセージに、このクライアントに対してomnircファイルのOB2OEXECOFF変数が有効になっていることが示されています。この変数を設定すると、pre-スクリプトとpost-execスクリプトの実行が無効になります。OB2OEXECOFF変数を無効にするには、値を0に設定します。

実行前スクリプトが失敗した場合に実行後スクリプトが実行されない

問題

クライアントに対してpre-execスクリプトが失敗した場合、post-execスクリプトがスキップされ、次のメッセージが表示される:

```
[Major] From: OB2BAR_SQLBAR@hostname.com "<Instance>" Time:<DATE><TIME>
..\script.bat
Illegal command format. Command not executed.
[Major] From: OB2BAR_SQLBAR@hostname.com "<Instance>" Time:<DATE><TIME>
[131:104] Script returned error. (Return value: -1).
[Warning] From: OB2BAR_SQLBAR@hostname.com "1" Time:<DATE><TIME>
Pre-exec script failed. Skipping Post-exec !
```

対処方法

omnircファイルのOB2FORCEPOSTEXEC変数を1に設定して、クライアントに対してpre-execスクリプトが失敗した場合でも、post-execスクリプトが常に実行されるようにします。

OB2FORCEPOSTEXEC変数を有効にした後で、バックアップ仕様を実行すると、次のメッセージが表示されます:

```
[Normal] From: OB2BAR_SQLBAR@hostname.com "<Instance>" Time:<DATE><TIME>
Starting post-exec script 'script.bat'...
[Normal] From: OB2BAR_SQLBAR@hostname.com "<Instance>" Time:<DATE><TIME>
Script executed successfully.
```

このメッセージは、クライアントに対してpre-execスクリプトは失敗したものの、post-execスクリプトが正常に実行されたことを示しています。

第6章: デバイスとメディアのトラブルシューティング

バックアップデバイスには、専用のData Protectorライセンスが必要です。詳細は、『Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。

デバイスのSCSIアドレスに関する問題の説明については、『Data Protectorインストールガイド』の付録Bを参照してください。

デバイスおよびメディアに関する全般的な問題

データフォーマットに互換性がないと、フリープールメディアが自動的に再フォーマットされない

問題
<p>バックアップまたは復元セッションが中止して、次の警告が表示されます。</p> <pre>[Warning] From: BSM@cell_manager.com "xtest" Time: 4.4.2014 11:45:41 [60:1023] Medium "200011ac:533e6a06:0134:0001" labeled "[MTV341L4] MTV341L4" of data format NDMP - Hitachi is not compatible with device "EML-Tape1" of dataformat OB2 - Generic.</pre>
対処方法
<p>ユーザーに標準ファイルシステムのバックアップ用のメディアプールとNDMPバックアップ用の独立したプールがあり、これらのプールが共通のフリープールを共有している場合に、バックアップまたは復元セッションが中止する場合があります。</p> <p>CheckNDMPDataFormatTypeグローバルパラメーターを1に設定します。</p>

Media Agentクライアント上のStoreOnceファイバーチャネルデバイスが不足している

問題
<p>Media AgentでStoreOnceファイバーチャネル(FC)が不足していると、多数のオブジェクトのバックアップ中、または複数の同時実行セッションの実行中に次のエラーメッセージが表示されます。</p> <pre>[Major] From: BMA@abc.com "DEV_FC_gw2 [GW 23117:0:6931224894398172655]" Time: <DATE> <TIME> 90:54 \\abcd\FC\75232e10_5322f96a_445f_01b1 Cannot open device (StoreOnce error: StoreOnce device offline, network error occurred or secure communication failed while contacting the StoreOnce device)</pre>
対処方法
<p>Media Agentクライアント上で使用可能なFCデバイスの数を増やします。たとえば、FCに接続されている</p>

Media Agentに使用可能なStoreOnce FCデバイスが16個のみで、200のオブジェクトを同時にバックアップする必要がある場合、Data Protectorには200の接続が必要になるため、使用可能なFCデバイスを200以上に増やす必要があります。

Media Agentクライアント上で使用可能なFCデバイスを増やすには、次の操作を実行します。

1. B6200 StoreOnceバックアップシステムアプリケーションを開きます。
2. **[StoreOnce]**、**[StoreOnce Catalyst]**を順に展開します。
3. **[Fibre Channel Settings]**タブで、下方向にスクロールして**[Devices]**セクションを表示して**[Edit]**をクリックします。
4. (各ポートの)**[Devices per Initiator Port]**フィールドに必要な値を設定します。

Windowsでは、デバイスマネージャーウィンドウで使用可能なStoreOnce FCデバイス数を確認できます。Media Agent上に表示可能なデバイス数は、すべてのFCポートのイニシエーターポートごとのデバイスの合計になるので注意してください。

Windows上でエクステンジャー制御デバイスにアクセスできない

問題

Data ProtectorはSCSIミニポートドライバーを使って、バックアップドライブとライブラリを制御します。他のデバイスのドライバーが同一のシステムに読み込まれている場合に、Data Protectorがデバイスを管理できないことがあります。この場合、メディアのフォーマットやスキャンなどのデバイス操作の開始時に、以下のエラーメッセージが表示されます。

Cannot access exchanger control device

対処方法

デバイスが置かれているシステム上で次のコマンドを実行して、システム上で構成されているすべての物理デバイスのリストを表示します。

```
Data_Protector_home\bin\devbra -dev
```

SCSIアドレスのいずれかのステータスがCLAIMEDの場合、そのSCSIアドレスは別のデバイスドライバーが使用中です。

Windowsのロボティクスドライバーを無効にします。

手順については、『Data Protectorヘルプ』のキーワード「ロボティクスドライバー」で表示される内容を参照してください。

SCSIデバイスのロックが解除されずにセッションが失敗する

問題

SCSIの予約または解放操作が不完全なので、SCSIドライブまたはロボティクス制御のロックが解除されません。

以下のメッセージが表示されます。

Cannot open device

Media Agentに障害が発生した場合、予約されたデバイスを再度解放することはできません。Data ProtectorでSCSIドライブまたはロボティクス制御のアンロックに失敗し、後続のセッションで使用できない可能性があります。

対処方法

他のアプリケーションがこのデバイスを使用していないことを確認します。SCSIドライブまたはSCSIロボティクス制御のロックを解除するには、デバイスの電源をいったん切ってから入れ直す必要があります。

デバイスのオープンに関する問題

問題

DDSデバイスを使おうとすると、次のエラーメッセージが表示されます。

Cannot open device (not owner)

対処方法

メディア認識システムと互換性がないメディアを使用していないかどうか確認します。DDSドライブでは、メディア認識システムと互換性のあるメディアを使用する必要があります。

Windows上でサポートされていないSCSI HBA/FC HBAの使用

問題

バックアップデバイスで、サポートされていないSCSI HBA/FC HBAを使用すると、システムエラーが発生します。

問題が発生するのは、主に複数のMedia Agentが同時にSCSIデバイスにアクセスした場合、またはデバイスのブロックサイズによって定義されている転送データの長さがSCSI HBA/FC HBAのサポートするデータ長を上回った場合です。

対処方法

デバイスのブロックサイズは変更できます。

その手順については、『Data Protectorヘルプ』の「デバイスとメディアの拡張オプションの設定」で表示される内容を参照してください。

サポート対象のSCSI HBA/FC HBAについては、『Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。

ライブラリ再構成の失敗

問題

デバイスリストの変更後、sanconfコマンドで既存のライブラリ構成を変更しようとする、構成エラーが報告されます。ライブラリ構成は一部しか作成されません。

対処方法

SAN環境内のホストのリストを再利用し、sanconfコマンドで再度ホストをスキャンすることで、従来のライブラリ構成を復旧できます。復旧後、以下の手順に従ってください。

1. 次のコマンドを実行して、セル内のホストをスキャンします。

```
sanconf -list_devices mySAN.txt -hostsfile hosts.txt
```

2. 保存した構成ファイルを使用してライブラリを構成します。次のコマンドを実行してください。

```
sanconf -configure mySAN.txt -library LibrarySerialNumberLibraryName  
[RoboticControlHostName] [DeviceTypeNumber] -hostsfile hosts.txt
```

正常動作していた従来のライブラリ構成が自動的に復旧されます。

後でライブラリを追加、削除、変更する際にsanconfコマンドによるライブラリ構成を失敗した場合は、上記の手順を実行すれば正常に動作する構成を復旧することができます。

暗号化されたメディアが読み込みまたは書き込み操作の後に不良とマークされる

問題

ドライブベースの暗号化を使用して書き込まれたメディアで読み取りまたは書き込み操作を行っているとき、セッションが失敗してメディアが自動的に不良とマークされます。

以下のエラーが表示されます。

```
Cannot read from device ([5] I/O error)
```

このエラーは、ドライブベースの暗号化をサポートしていないプラットフォームで読み込み操作または書き込み操作が実行された場合に発生します。メディア品質には影響しません。サポートされるプラットフォームの最新リストについては、<https://softwaresupport.softwaregrp.com/>にある最新サポート一覧を参照してください。

対処方法

メディア状態ステータスを修正するには、omnimm -reset_poor_mediumオプションを使用してメディア状態をリセットします。

詳細については、omnimmのmanページまたは『Data Protector Command Line Interface Reference』を参照してください。

Data Protector GUIとCLIを使用したNULLデバイスの作成

問題

UNIXのようなオペレーティングシステムでは、NULLデバイスは特殊ファイルで、書き込まれたすべてのデータを削除します。したがって、このファイルから読み込んだようなプロセスでもデータは使用できず、直ちにEOFになります。ただし、この書き込み操作のレポートには、処理は正常に終了したことが示されます。

トラブルシューティングを行うために、実際のデータ出力が必要なければ、ソフトウェアサポートからの要

求に応じてNULLデバイスを作成できます。このドキュメントでは、Data Protector GUIとCLIを使用したNULLデバイスの作成について説明します。

対処方法

注意: NULLデバイスは一時的な解決策として作成して使用するものであり、トラブルシューティングが正常に完了したら、削除する必要があります。NULLデバイスを削除しないで、プロダクションバックアップに間違って使用すると、このプロセスにより即座にデータが失われます。

Data Protector GUIで次の手順を実行してください。

1. コンテキストリストで**[デバイスメディア]**をクリックします。
2. Scopingペインで、**[デバイス]**を右クリックし、**[デバイスの追加]**をクリックして、ウィザードを起動します。
3. **[デバイス名]**テキストボックスにデバイスの名前を入力します。
4. **[説明]**テキストボックスに必要なに応じて説明を入力します。
5. **[デバイスの種類]**リストで、デバイスの種類として**[スタンドアロン]**を選択します。
6. **[次へ]**をクリックします。
7. 名前に「null」を指定して、**[追加]**をクリックします。
8. **[次へ]**をクリックします。
9. **[メディアの種類]**リストでは、デフォルト値をそのまま使用します。
10. **[デフォルトメディアプール]**では、デフォルト値をそのまま使用します。
11. **[完了]**をクリックしてウィザードを終了します。

デバイス名が構成済みデバイスのリストに表示されます。デバイスをスキャンすると、構成を確認できます。

12. Data Protector GUIを使用してNULLデバイスを作成したら、指定したバックアップデバイスの構成をASCIIファイルにエクスポートします。次のCLIコマンドを使用して、構成をエクスポートします。

```
omnidownload -device BackupDevice [-file FileName]
```

例: omnidownload -device ThisIsNULLDevice -file NULL.dev。

CLIを使用したNULLデバイスの作成

Data Protector GUIを使用して作成したNULLデバイスは、CLIを使用して別のシステムに複製できません。

omnidownload コマンドを使用すると、バックアップデバイスについての情報を表示したり、指定したバックアップデバイスの構成をASCIIファイルにダウンロードしたりすることができます。このコマンドにより、Data Protector内部データベース(IDB)から、バックアップデバイスとライブラリについての情報がダウンロードされます。このコマンドは、Data Protectorユーザーインターフェイスコンポーネントがインストールされたシステム上で使用できます。

このコマンドをomniupload ユーティリティと併せて使用すると、コマンドラインインターフェイスを使用してバックアップを作成および維持できます。

omniupload ユーティリティは、バックアップデバイスファイルをData Protector内部データベース(IDB)にアップロードします。Data Protectorバックアップデバイス上の情報はIDB内に保存されます。バックアップデバイスを構成するには、このデバイス上の情報をファイルにダウンロードする必要があります。この操作は、omnidownload コマンドを使用して実行します。その後このファイルを修正し、再びIDBにアップロードします。

詳細は、『*Data Protector Command Line Interface Reference*』を参照してください。

以下の手順を実行します。

1. Data Protector GUIを使用してファイルデバイスを作成したら、次のコマンドを使用して使用可能なデバイスのリストを表示します。

```
omnidownload -list_devices
```

このコマンドにより、Data Protectorバックアップデバイスに関する情報が表示されます。レポートには、各デバイスのデバイス名、クライアント、デバイスの種類、プールに関する情報が含まれます。

2. 次のCLIコマンドを使用して、作成したバックアップデバイスの構成をダウンロードするか、ASCIIファイルにエクスポートします。

```
omnidownload -device BackupDevice [-file FileName]
```

例:omnidownload -device ThisIsNULLDevice -file NULL.dev

このコマンドにより、ASCIIファイルまたはテキストファイルが、すべてのバックアップデバイス構成の詳細で更新されます。

例:

```
NAME "ThisIsNULLDevice"
DESCRIPTION " "
HOST dppvt5140.company.com
POLICY Standalone
TYPE File
POOL "Default File"
ENCRAPABLE
DRIVES
>null"
DEVSERIAL ""
RESTOREDEVICEPOOL NO
COPYDEVICEPOOL NO
```

注: HOSTに指定した値がCell Manager内の通常のクライアントであることを確認してください。あるCell Manager上のデバイスをエクスポートし、そのデバイスを新しいCell Managerまたは別のell Managerにインポートする場合、HOSTの名前を、新しいCell Managerの一部である新しいメディアエージェントホストに変更する必要があります。

3. 新しいCell Managerまたは別のCell Managerを使用する場合、次のコマンドを使用して、ASCIIファイルまたはテキストファイル内のホスト名を変更し、ASCIIファイルをシステムにアップロードします。

```
omniupload -create_device FileName
```

例:omniupload -create_device NULL.dev

メディアに関するさまざまな問題

問題

メディアに関するさまざまな問題が発生します。

対処方法

メディア品質統計機能を使うと、メディアに関する問題を早期の段階で検出できます。

各メディアがドライブから取り出される前に、Data ProtectorはSCSI log senseコマンドを発行してメディアの読み込み/書き込みに関する統計情報を照会します。この情報はmedia.logファイルに書き込まれます。

メディア品質統計機能は、デフォルトでは無効になっています。有効にするには、グローバルオプションOb2TapeStatisticsを1に設定します。

その手順については、[グローバルオプション](#)、[ページ 16](#)を参照してください。

書き込み操作中にメディア関連のエラーが表示された場合、またはメディアが「不良」とマークされた場合は、media.logファイルでメディアのエラー統計を確認できます。

Media.logファイルには以下のエラー統計が書き込まれます。ここで、nはエラー数です。

エラー統計	説明
errsubdel=n	大幅な遅延後に修正されたエラーの数
errposdel=n	ある程度の遅延をもって修正されたエラーの数
total=n	再書き込みの合計回数
toterrcorr=n	書き込み中に修正および回復されたエラーの合計数
totcorralgproc=n	修正アルゴリズムの処理時間の合計
totb=n	書き込み処理したバイト数の合計
totuncorrerr=n	未修正のエラー(書き込み)の合計数

パラメーターの値が-1の場合は、デバイスがその統計パラメーターをサポートしていないことを示しています。すべてのパラメーターの値が-1になっている場合は、テープ品質の統計情報の処理中にエラーが発生したか、デバイスがメディア品質の統計情報をまったくサポートしていないかのどちらかです。

テープの統計結果は、ほとんどのデバイスの場合、[total bytes processed]にバイト数でレポートされます。ただし、LTOデバイスとDDSデバイスについてはバイト単位ではなく、それぞれデータセット単位、グループ単位でレポートされます。

例

ここでは、さまざまなデバイスの種類ごとに、media.logmedia.logファイルの内容の例を示します。

DLT/SDLTデバイス

DLT/SDLTデバイスに関するLog sense書き込みレポート — 処理されたバイト数の合計

Media ID from tape= 0fa003bd:3e00dbb4:2310:0001; Medium Label= DLT10; Logical drive= dlt1; Errors corrected no delay= 0; Errors corrected delay= 0; Total= 13639; Total errors corrected= 13639; Total correction algorithm processed= 0; Total bytes processed= 46774780560; Total uncorrected errors= 0

46774780560バイト(圧縮後)のネイティブデータが処理されました(DLT8000テープ全体)。

LTOデバイス

LTOデバイスに関するLog sense書き込みレポート — 処理されたデータセット数の合計

Media ID from tape=0fa003bd:3e0057e6:05b7:0001; Medium Label= ULT2; Logical drive=ultrium1; Errors corrected no delay= 0; Errors corrected delay= 0; Total= 0; Total errors corrected= 0; Total correction algorithm processed= 0; Total bytes processed= 47246; Total uncorrected errors= 0

1つのデータセットのサイズは404352バイトです。処理されたバイト数の合計を計算するには、以下の公式を使用します。

$47246 \text{ data sets} * 404352 \text{ bytes} = 19104014592 \text{ bytes after compression (a full tape)}$

DDSデバイス

DDSデバイスに関するLog sense書き込みレポート — 処理されたグループ数の合計

Media ID from tape= 0fa0049f:3df881e9:41f3:0001; Medium Label= Default DDS_5; Logical drive= DDS; Errors corrected no delay= -1; Errors corrected delay= -1; Total= -1; Total errors corrected= 0; Total correction algorithm processed= 154; Total bytes processed= 2244; Total uncorrected errors= 0

DDS1/2: 1グループは126632バイトです。

DDS3/4: 1グループは384296バイトです。

処理されたバイト数の合計を計算するには、以下の公式を使用します。

$2244 \text{ groups} * 126632 \text{ bytes} = 284162208 \text{ bytes after compression (a 359 MB backup on DDS2)}$

359MBのデータがバックアップされ、テープ上に271MBのネイティブデータが書き込まれました。

メディアヘッダーのサニティチェックエラー

問題

Data Protectorのデフォルト動作では、メディアがドライブから取り出される前にメディアヘッダーのサニティチェックが実行されます。

メディアヘッダーのサニティチェックでメディアヘッダーの整合性エラーが検出された場合は、エラーメッセージが表示されます。このメディア上のすべてのオブジェクトに失敗のマークが付けられ、さらにこのメディア

のオブジェクトを含むセッションの状態も変更されます。

メディアヘッダーが破損していた場合、そのメディア上のすべてのオブジェクトに失敗のマークが付けられ、メディアには不良のマークが付けられます。

対処方法

IDBセッションからメディアをエクスポートし、別のメディアを使って失敗したセッションを再開します。

デバイスのシリアル番号に関する問題

問題

問題があるバックアップデバイスやロボティクスに対して何らかの操作(バックアップ、復元、フォーマット、スキャンなど)を実行すると、以下のエラーが表示されます。

Device DeviceName could not be opened (Serial number has changed).

このエラーは、デバイスパスで指定しているデバイスのシリアル番号がIDBに格納されている番号とは異なる場合に報告されます。この問題は、以下の場合に発生することがあります。

- デバイスを誤って構成した(たとえば、omniuploadコマンドを使用したり、構成したデバイスファイルが正しくない場合)。
- 物理デバイスを交換したときに、対応する論理デバイスの更新(新しいシリアル番号の再読み込み)をしなかった場合。
- SCSIライブラリ内にあるSCSIテープドライブを物理的に交換します。**[変更されたSCSIアドレスの自動検出]**オプションが有効になっていないか、omnircオプションOB2MADETECTDRIVESWAPが0になっています。
- マルチパスデバイス内のパスを正しく構成していない場合。

対処方法

1. Data Protector GUIで、[デバイス/メディア]コンテキストを選択します。
2. Scopingペインで**[デバイス]**を展開して問題のデバイスを右クリックし、**[プロパティ]**をクリックします。
3. [コントロール]タブをクリックし、**[変更されたSCSIアドレスの自動検出]**オプションを有効にします。
4. **[再読み込み]**をクリックしてIDB内のデバイスシリアル番号を更新します。
SCSIライブラリにあるSCSIテープドライブを物理的に置き換えた場合は、omnircオプションOB2MADETECTDRIVESWAPが1(デフォルト)になっていることを確認してください。デバイスシリアル番号をリロードする必要はありません。

破損したデータを復元またはコピーできない

問題

デフォルトでは、テープ上でCRC値が使用可能な場合はCRC値が必ずチェックされ、CRCの不一致によって破損が検出されたデータは復元もコピーもされません。ただし、状況によっては、そのようなデータの復元やコピーが必要な場合があります。

対処方法

Media Agentホスト上のomnircオプション0B2CRCHECKを一時的に0に設定します。破損オブジェクト(データ)の復旧後、設定をデフォルト値(1)に戻します。

よく発生するハードウェア関連の問題

問題

ハードウェアに関する一般的な問題が発生します。

対処方法

システムとデバイス間のSCSI接続(SCSIケーブルとその長さ、SCSIアダプターなど)を確認します。OSで提供されているtarなどのコマンドを実行し、システムとデバイスが通信していることを確認します。

ADIC/GRAU DASライブラリとSTK ACSライブラリに関する問題

ADIC/GRAU DASライブラリのインストール失敗

問題

ADIC/GRAU DASライブラリのインストールが失敗します。

対処方法

1. GRAUロボティクス(PC/ロボット)を制御するクライアントにMedia Agentをインストールします。
2. ドライブが接続されているクライアント(PC/ドライブ)にMedia Agentをインストールします。
3. aci.dll + winrpc.dll + ezrpcw32.dllを%SystemRoot%\system32およびData_Protector_home\binディレクトリにコピーします。
4. PC/ロボット上にディレクトリaciを作成します。
5. dasadmin.exe、portmapper、portinstをaciディレクトリにコピーします。
6. portinstを起動して、portmapperをインストールします(PC/ロボットに対してのみ)。
7. mmdノッチをCell Managerにインストールします。
8. システムを再起動します。
9. Windowsの[コントロールパネル]ウィンドウで[管理ツール]をクリックし、[サービス]をダブルクリックして、portmapperサービスと両方のrpcサービスがともに稼働しているかどうかをチェックします。
10. GRAUライブラリ内のOS/2システムで、ファイル/das/etc/configを編集します。PC/ロボットのIPアドレスを含むOMNIBACKという名前のクライアントを追加します。

ドライブが1つも表示されない

問題
ドライブが1つも表示されません。
対処方法
<p>PC/ロボットから次のコマンドを実行します。</p> <ol style="list-style-type: none"> 1. <code>dasadmin listd</code> 2. <code>dasadmin all DLT7000 UP AMUCLIENT</code> 3. <code>dasadmin mount VOLSER</code>(次にドライブ上のUNLOADボタンを押します) 4. <code>dasadmin dismount VOLSER</code>または<code>dasadmin dismount -d DRIVENAME</code> <p>ここで:</p> <ul style="list-style-type: none"> • <code>AMUCLIENT = OMNIBACK</code> • <code>VOLSER</code>、例: 001565 • <code>DRIVENAME</code>、例: DLT7001 • <code>all</code>は"allocate"を意味します。 <p>上記のコマンド(DAS Server (OS/2)への通信)が正しく実行されなかった場合は、OS/2システム上で <code>/das/bin/</code> directoryからコマンドをもう一度実行してみてください。</p> <p>OS/2システムから上記のコマンドを実行する場合は、<code>AMUCLIENT = AMUCLIENT</code>を使用してください。</p> <ol style="list-style-type: none"> 1. AMUクライアントにログインします。一般的なログイン情報は以下のとおりです。 <ul style="list-style-type: none"> <code>user: Administrator pwd: administrator</code> <code>user: Supervisor pwd: supervisor</code> 2. メディアの種類を必要に応じて設定します。 <ul style="list-style-type: none"> <code>ACI_MEDIA_TYPE</code>の設定 <code>ACI_MEDIA_TYPE=DECDLT</code>の設定 3. ライブラリを再起動します。 <ol style="list-style-type: none"> a. OS/2をシャットダウンして、ロボティクスの電源をオフにします。 b. OS/2を再起動します。OS/2が起動すると、ロボティクスの使用準備ができていないことを示すAMUログが表示されます。次にロボティクスの電源をオンにします。

GRAU CAPが正しく構成されていない

問題
GRAU CAPが適切に構成されていません。
対処方法
<p>メディアをCAPからスロットへ移動した後、ドライブに移動するには、デバイスのロボティクスを使用しなければなりません。以下の例のようにimportコマンドとexportコマンドを使います。</p>


```
import CAP: I01
import CAP range: I01-I03
export CAP: E01
export CAP range: E01-E03
```

ライブラリ操作が失敗する

問題

ライブラリ操作が失敗します。

対処方法

Data Protectorのumaユーティリティを使ってGRAUおよびSTKライブラリドライブを管理するには、以下の構文を使用します。

```
uma -pol POLNUMBER -ioctl LIBRARYNAME -type MEDIATYPE
```

ここで、*POLNUMBER*には、GRAUの場合は8、STKの場合は9を指定します。

例:uma -pol 8 -ioctl grauamu

デフォルトのメディアの種類はDLTです。

クラウドデバイスに関する問題

クラウド(Helion)とクラウド(Azure)での通信エラー

問題

クラウド(Helion)デバイスとクラウド(Azure)デバイスで、クラウドオブジェクトストアとの通信中にエラーが発生します。エラーが発生すると、クラウド(Helion)デバイスとクラウド(Azure)デバイスは操作を再試行します。

通信エラーが発生すると、次のエラーが表示されます。

クラウド[ERROR]との通信中にエラーが発生しました。再試行しています。

対処方法

クラウドのデフォルトの再試行回数は5回です。

Media Agentホスト上のomnircオプションOB2_CLOUDDEV_MAXRETRIESを6以上に設定します。

Data Protector 9.00を使用してクラウド(Helion)デバイスを構成できない

問題

Data Protector 9.00以前のバージョンでクラウド (Helion) デバイスを構成しているときに、クラウド (Helion) デバイスで問題が発生します。

対処方法

Data Protectorの以前のバージョンではクラウド (Helion) デバイスはサポートされていません。

Cell Manager、GUIサーバー、インストールサーバー、およびMedia Agentがすべて一般リリースパッチ以降に更新されていることを確認してください。

10.00以前のバージョンのData Protectorを使用してクラウド (Azure) デバイスを構成できない

問題

Data Protector 9.08以前のバージョンでクラウド (Azure) デバイスを構成しているときに、クラウド (Azure) デバイスで問題が発生します。

対処方法

Data Protectorの以前のバージョンではクラウド (Azure) デバイスはサポートされていません。

Cell Manager、GUIサーバー、インストールサーバー、およびMedia Agentがすべて一般リリースパッチ以降に更新されていることを確認してください。

第7章: オブジェクト操作セッションのトラブルシューティング

オブジェクトコピーに関する問題

コピーされたオブジェクトの数が想定された数より少ない

問題
ポストバックアップのオブジェクトコピーまたはスケジュール済みのオブジェクトコピーでは、選択したフィルターに一致するオブジェクトの数が実際にコピーされるオブジェクトの数よりも多くなります。 以下のメッセージが表示されます。 Too many objects match specified filters.
対処方法
<ul style="list-style-type: none">オブジェクトバージョンの選択条件を絞り込みます。グローバルオプションファイル内のCopyAutomatedMaxObjects変数の値を大きくして、同一セッション内でコピーされるオブジェクトの最大数を増やします。

選択したライブラリ内の一部のオブジェクトしかコピーされない

問題
ポストバックアップのオブジェクトコピーまたはスケジュール済みのオブジェクトコピーで、選択したライブラリ内のメディアに格納されている一部のオブジェクトがコピーされません。この問題は、選択したライブラリにオブジェクトの完全なメディアセットが存在しない場合に発生します。
対処方法
選択したライブラリに不足しているメディアを挿入するか、これらのオブジェクトの完全なメディアセットが存在するライブラリを選択します。

追加のメディアに対するマウント要求が発行される

問題
[メディア]開始ポイントからの対話型オブジェクトコピーセッションで、特定のメディアを選択しました。これにより、追加メディアのマウント要求が発行されます。この現象は、メディア上のオブジェクトが他のメディアにまたがっている場合に発生します。

対処方法

必要なメディアをデバイスに挿入し、マウント要求を確認します。

オブジェクトコピーを作成したときに、保護の終了時間が延長される

問題

オブジェクトコピーを作成したときに、元のオブジェクトから保護の終了時間が継承されません。保護期間はコピーされますが、開始時間が、オブジェクトの作成時間ではなく、オブジェクトコピーの作成時間に設定されます。その結果、元のオブジェクトより保護期間が延長されます。元のバックアップが作成されてからオブジェクトコピーセッションを行うまでの時間が長いほど、保護終了時間の差は大きくなります。

たとえば、オブジェクトを9月5日に作成し、保護期間を14日間に設定した場合、保護期間は9月19日に期限切れとなります。オブジェクトコピーセッションを9月10日に開始した場合、オブジェクトコピー保護期間は9月24日に期限切れとなります。

場合によっては、このような動作は望ましくなく、保護の終了時間を維持しなければならないこともあります。

対処方法

グローバルオプションCopyDataProtectionEndtimeEqualToBackupを1に設定すると、オブジェクトコピー保護の終了時間がバックアップのオブジェクト保護の終了時間に等しくなります。このオプションは、デフォルトでは0に設定されています。許容されるファイルの最大数を増やします。

複数のオブジェクトを含むセッションを複製すると、応答が停止する

問題

別のデバイスにセッションを複製しようとする時、セッションが応答を停止します。セッションの出力には、以下の情報が含まれます。

```
[Normal] From: BMA@company.com "d2d1_1_gw1 [GW 26177:1:15198446278003495809]"  
Time: 3/21/2013 9:13:06 AM
```

```
COMPLETED Media Agent "d2d1_1_gw1 [GW 26177:1:15198446278003495809]"
```

問題は、デュアルIPスタックネットワーク構成でHP-UX Media Agentを使用する場合に発生します。

対処方法

デュアルIPスタックネットワークで、Media Agentクライアント上の/etc/hostsファイルに、IPv6 localhostアドレスの独立したエントリを追加します。

たとえば、hostsファイルに以下のエントリが存在する場合を考えます。

```
:::1 localhost loopback
```

問題を解決するには、IPv6アドレス用に以下の行を追加します。

```
:::1 ipv6-localhost ipv6-loopback
```

データドメインブースト デバイス上の複製セッションが再試行期間中に中止操作に 응답できない

問題

あるデータドメインブーストバックアップデバイスから別のデバイスにセッションを複製しているときに、デバイスに利用可能なストリームが十分ないと、複製セッションが再試行期間中に中止操作に 응답できません。

対処方法

この問題は、omnirc DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMITが0(サポートされていません)に設定されている場合に発生することがわかっています。

この変数は、データドメインブーストデバイスに利用可能なストリームが十分でない場合、複製セッションが再試行を開始するまでに待機する間隔を定義します。この間隔が大きすぎたり、0に設定されたりしている場合、セッションが中止操作に 응답できません。

DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMITのデフォルト値は60秒です。

DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMITの詳細な説明については、omnircファイルを参照してください。

オブジェクト集約に関する問題

多くの時点のオブジェクト集約を行うと、上限を超える数のファイルが開かれる

問題

多くの時点のオブジェクト集約操作を開始した場合、Data Protectorは操作を実行するために必要なすべてのメディアを読み取ります。この場合、すべてのファイルが同時に開かれます。Data Protectorが開いたファイルの数が、オペレーティングシステムで許容される上限を超えた場合、次のようなメッセージが表示されます。

```
|Major| From: RMA@computer.company.com "AFL1_ConsolidateConc2_bs128" Time: time /omni/temp/Cons_Media/AFL1/
```

```
0a1109ab54417fab351d15500c6.fd
```

```
Cannot open device ([24] Too many open files)
```

対処方法

許容されるファイルの最大数を増やします。

HP-UXシステムの場合:

1. System Administration Manager (SAM)を使用して、開けるファイルの最大数を設定します:
 - a. [カーネル構成]→[構成可能パラメーター]を選択し、次に、[アクション]→[構成可能パラメーターの変更]を選択します。
 - b. **formula/value**フィールドに**maxfiles_lim**と**maxfiles**の新しい値を入力します。
2. 新しい値を適用した後、コンピューターを再起動します。

Solarisシステムの場合:

1. /etc/systemファイルを編集して、開けるファイルの最大数を設定します: 以下の行を追加します。

```
set rlim_fd_cur=value  
set rlim_fd_max=value
```
2. 新しい値を適用した後、コンピューターを再起動します。

B2Dデバイスへのオブジェクト集約が2回目の試行で失敗した

問題

最初のオブジェクトの集約後に増分バックアップを実行し、2回目のオブジェクト集約を実行すると、操作が失敗します。

対処方法

2回目の集約を正常に完了させるには、最初のオブジェクト集約を実行した後にフルバックアップを実行します。その後、増分バックアップを実行して、後で集約できるようにします。

第8章: Data Protector内部データベースのトラブルシューティング

IDBディレクトリのリストについては、『Data Protector Command Line Interface Reference』のomniintroリファレンスページを参照してください。

ディレクトリが見つからないことによる問題

データベース/ファイルを開けない、またはデータベースのネットワーク通信エラーが発生する

問題
Data ProtectorがIDBにアクセスしようとしたときに、1つまたは複数のIDBデータファイルまたはディレクトリが見つからない場合、以下のエラーが表示されます。 <ul style="list-style-type: none">• Cannot open database/file• Database network communication error
対処方法
IDBデータファイルおよびディレクトリを再インストールします。 <ol style="list-style-type: none">1. Data Protectorを再インストールします。2. Cell Managerを再起動します。

Cell Managerにアクセスできない

問題
Data Protector GUIがCell Managerに接続しようとしたときに、Data Protectorの一時ディレクトリが見つからない場合、以下のエラーメッセージが表示されます。 Cannot access the Cell Manager system. (inet is not responding) The Cell Manager host is not reachable or is not up and running or has no Data Protector software installed and configured on it.
対処方法
<ol style="list-style-type: none">1. Cell Managerで、Data Protector GUIを閉じます。2. 以下を実行して保守モードを開始します。 <code>omnisv -maintenance</code>3. 以下の場所に、ディレクトリtmpを手動で作成します。

Windowsシステムの場合 :Data_Protector_program_data

UNIXシステムの場合 :/var/opt/omni

4. 以下を実行して保守モードを終了します。

```
omnisv -maintenance -stop
```

5. Data Protector GUIを再起動します。

バックアップ時またはインポート時の問題

IDBバックアップが失敗してアーカイブログファイル名形式が正しくないことを報告する

問題

Data Protector 9.00パッチにアップグレードした後にIDBバックアップが失敗して、次のメッセージが表示されます。"The archive log filename format is incorrect."

対処方法

この場合、以下の手順を実行します。

1. omnisv stopを実行します。
2. アップグレード後にレジストリ内のパスが古いIDBの場所を指し示しているため、新しく復元されたIDBの場所を指し示すようにHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\hdpd-idb\ImagePathレジストリキー内のIDBの場所のパスを手動で変更します。
3. omnisv startを実行します。
4. omnidbutil -set_schema_crcを実行します。

注: すべてのIDBスキーマには関連付けられたCRCファイルがあります。IDBの場所を(手順2の説明に従って)変更した後に、新しいIDBの場所のスキーマに一致するようにCRCファイルを変更する必要があります。最後に、新しいIDBスキーマに一致するCRCファイルを作成します。

バックアップ中にファイル名がIDBに記録されない

問題

以下に該当する場合は、Data Protectorを使用してバックアップを実行したときにファイル名がIDBに記録されません。

- バックアップオプションとして[No Log]を選択した場合。
- IDBのDCBF部分のスペースが不足している場合、またはIDBのあるディスクのディスクスペースが不足している場合。これは、セッション出力内のエラーにより通知されます。

対処方法

- バックアップオプションとして、[No Log]を選択していないかどうかを確認してください。
- バックアップセッションのセッションメッセージに警告 およびエラーが含まれていないかどうかをチェックします。

IDBのバックアップまたはインポート中に、BSMまたはRSMが強制終了する

問題

IDBのバックアップまたはインポートセッション中に、BSMまたはRSMが強制終了する場合、以下のエラーが表示されます。

IPC Read Error System Error: [10054] Connection reset by peer

Data Protector GUIの[内部 データベース]コンテキストで、セッションが実際には実行中でないにもかかわらず、セッションステータスが[In Progress]と表示されます。

対処方法

1. Data Protector GUIを閉じます。
2. omnidbutil -clearコマンドを実行し、実際には実行中でないが[]と表示されているすべてのセッションのステータスを、[In Progress to Failed]に設定します。
3. omnidbutil -show_locked_devsコマンドを実行して、Data Protector[]によってロックされているデバイスやメディアがないかどうか確認します。
4. ロックされているものがあつた場合、omnidbutil -free_locked_devsを実行してロックを解除します。
5. Data Protector GUIを再起動します。

IDBバックアップまたはインポート中に、MMDが強制終了する

問題

IDBバックアップまたはインポートセッション中に、メディア管理デーモン(MMD)が強制終了する場合、以下のエラーが表示されます。

- Lost connection to MMD
- IPC Read Error System Error: [10054] Connection reset by peer

MMDサービス/プロセスが稼動していない場合:

- omniv -statusコマンドを実行すると、MMDサービス/プロセスが動作していないことが通知されます。
- 以下に注意してください。

Windowsシステム: Data Protector MMDプロセス(mmd.exe)はWindowsタスクマネージャー内のプロ

セスとして表示されません。

UNIXシステム: `ps -ef | grep omni`コマンドを使用してData Protectorプロセスを一覧している場合はData ProtectorMMDプロセス(`/opt/omni/lbin/mmd`)は表示されません。

対処方法

1. Data Protector GUIを閉じます。
2. `omnisv -stop`コマンドを実行してData Protectorサービス/プロセスを停止します。
3. `omnisv -start`コマンドを実行してData Protectorサービス/プロセスを開始します。
4. `omnisv -status`コマンドを実行して、サービス/プロセスがすべて実行中かどうかチェックします。

DCバイナリファイルが破損または見つからない

問題

Data Protector GUIの[復元]コンテキストでバックアップオブジェクトをブラウズすると、以下のエラーが表示されます。

Open of Detail Catalog Binary File failed

- `omnidbcheck -bf`コマンドを実行すると、1つまたは複数のDCバイナリファイルが見つからないか、サイズが不適切であることが通知されます。`omnidbcheck -dc`コマンドを実行すると、1つまたは複数のDCバイナリファイルが破損していることが通知されます。
- Cell Manager上の`debug.log`ファイルには、Data ProtectorがDCバイナリファイルを開くのに失敗したことを示すエントリが1つ以上含まれています。

対処方法

メディアからカタログをインポートして、DCバイナリファイルを再作成します。

手順については、『Data Protectorヘルプ』のキーワード「IDBのDCBF部分の[警戒域]レベルの破損」で表示される内容を参照してください。

内部データベースのバックアップが失敗する

問題

Data Protector内部 データベースをバックアップするセッションが、以下のエラーで失敗します。

```
[Critical] From: OB2BAR_POSTGRES_BAR@computer.company.com "DPIDB" Time: 4/2/2013 4:05:20 PM
```

```
Error while running the PSQL script
```

```
[Normal] From: BSM@computer.company.com "idb" Time: 4/2/2013 4:05:20 PM
```

```
OB2BAR application on "computer.company.com" disconnected.
```

```
[Critical] From: BSM@computer.company.com "idb" Time: 4/2/2013 4:05:20 PM
```

```
None of the Disk Agents completed successfully. Session has
```

failed.

Data Protector Inetサービスがドメインユーザーアカウントのコンテキストで実行中の場合、そのアカウントのセキュリティポリシー権限が不十分であることが問題の最も考えられる原因です。

対処方法

Data Protector Inetサービスに使用されるWindowsドメインユーザーアカウントに以下のWindowsオペレーティングシステムセキュリティポリシー権限を与え、セッションを再開します。

- 認証後にクライアントを偽装
- プロセスレベルトークンの置き換え

詳細については、『Data Protectorヘルプ』のキーワード「Inetユーザーの偽装」で表示される内容を参照してください。

パフォーマンスに関する問題

復元時のブラウズに時間がかかる

問題

Data Protector GUIで復元対象のオブジェクトバージョンおよび個々のファイルをブラウズするとき、IDBから情報が読み込まれて表示されるまでに時間がかかります。これは、IDB内で選択されたオブジェクトのオブジェクトバージョン数が大きすぎる場合に発生します。

対処方法

復元対象のオブジェクトバージョンをブラウズする際の時間間隔を設定します。

- 特定の復元に対して時間間隔を指定するには、[ソース]ページの**[検索インターバル]**オプションを設定します。
- これ以降ブラウズするすべての復元に対してグローバルに時間間隔を設定するには、以下の手順に従ってください。
 1. [ファイル]メニューの**[選択値]**をクリックします。
 2. **[復元]**タブをクリックします。
 3. **[検索インターバル]**オプションを設定し、**[OK]**をクリックします。

IDBのサイズ増加による問題

IDBのスペースが不足している場合

問題

一部のIDBのスペースが不足しています。[IDBのスペース不足]通知が表示されます。

対処方法

IDBのサイズを拡張します。

IDBのDCBF部分が急激に増加する

問題

[Client Statistics]のレポートで、いくつかのシステムの[書き込まれたデータ[GB]または[ファイル数]の数字がconsiderably大きくなる。

対処方法

IDBのDCBF部分のサイズを縮小するには、Cell Manager上でomnidbutil -purge -dcbfコマンドを実行して、IDBにあるカタログ保護のついたすべてのメディアについてDCBFを削除します。削除セッションの間はData Protectorセッションが何も実行されないようにします。

IDBのDCBF部分の増大を抑えるには、[ロギングレベル]を[ディレクトリレベルまでログに記録]に変更します。

その他の問題

データベースセッションマネージャーが稼動していないことによるプロセス間通信エラー

問題

Data Protector GUIがIDBにアクセスしているときにCell Managerでデータベースセッションマネージャプロセスが動作を停止するか、または終了すると、以下のエラーが表示されます。

Interprocess communication problem

Cell Managerで、以下に注意してください。

Windowsシステム: Data Protectorのプロセス(dbsm.exe)はWindowsタスクマネージャー内のプロセスとして表示されません。

UNIXシステム: ps -ef | grep omniコマンドを使用してData Protectorプロセスを一覧しているときには/opt/omni/lbin/dbsmは表示されません。

対処方法

Data Protector GUIを再起動します。

MMDBとCDBが同期しない

問題

CMMDB復元の結果、MoM環境でMMDBとCDBが非同期になることがあります。

対処方法

CMMDBをインストールしているシステムで、以下を実行します。

```
omnidbutil -cdbsync CellManagerHostname
```

CMMDBを変更した場合、MoMセルのそれぞれのCell ManagerでCellManagerHostname引数を指定して、このセルのそれぞれのCell Managerでコマンドを実行します。

IDBが破損している

問題

以下のいずれかのメッセージが表示されることがあります。

- Database is corrupted.
- Interprocess communication problem.
- Cannot open Database/File.
- Error - Details Unknown.

対処方法

IDBを回復します。

MMDBのCMMDBへのマージが失敗する

問題

omnidbutil -mergemmdbコマンドを実行した後、MMDBのCMMDBへのマージが、
Could not establish connection.

対処方法

omnidbutil -mergemmdbを使う前に、リモートデータベース接続を有効にする必要があります。接続を確立できるようにするには、以下のように構成ファイルを変更してサービスを再起動します。

1. Momクライアント上で、デフォルトのData Protector内部 データベースディレクトリのpgサブディレクトリに移動します。
2. テキストエディターでpg_hba.confを開き、以下の行を追加します。
host hdpidb hdpidb_app MoM_Server_IP_Address/32 trust
3. MoMクライアントでサービスを再起動します。
omnisv -stop
omnisv -start

IDBの復元中にセッションがエラーを出して完了する

問題

IDBをスタンドアロンデバイスにバックアップします。IDBの復元を実行するとセッションがエラーを出して完了します。

アップグレードが完了すると、パッチ用のファイルが次の場所に追加されます。

C:\ProgramData\OmniBack\Config\Server\install

例: patch_CC

このファイルはIDBのバックアップによってバックアップされます。しかし、このファイル(上書き)を復元しようとしたときに、「Access denied」 というエラーが表示されます。

対処方法

Data Protectorの構成ファイルを元の場所に復元する場合、次の操作を実行します。

1. <dp_data>\Config\Server\install\に移動して次のファイルを特定します。
patch_CC, patch_CORE, patch_CS, patch_DA, patch_DOC, patch_MA, patch_NETAPP, patch_SMISA, patch_VEPA
2. これらのすべてのファイルについて、非表示フラグを解除します。
3. IDBの復元を実行します。
4. 前述のファイルの非表示フラグを再設定します。

注: この問題はWindows CMでしか発生しないため、対処方法はWindowsにしか適用できません。ファイルを別の場所に復元し、これらのファイルがその場所にすでに存在する場合、同じ対処方法を適用できます。

DCバイナリファイルがDCBFセグメントのエラーを報告する

問題

復元したデータベースを新しい内部データベースとして使用してIDB復元を実行した後に、omnidbcheck -dcがエラーを報告します。

対処方法

IDBバックアップオブジェクトが置かれているメディアのエクスポートと再インポートを実行します。

PDB OracleのPoint-in-Timeリカバリが失敗してエラーが表示される

問題

PDB OracleのPoint-in-Timeリカバリの実行中、次のエラーを表示します。

PLS-00306: wrong number or types of arguments in call to 'GETCNCTSTR'

PDBのPoint-in-Timeリカバリを実行する場合、問題はOracle Bundle Patchに存在します。

対処方法

この問題を解決するには、より新しいOracleパッチバンドルを見つけるか、ソフトウェアサポートに問い合わせてください。

復元を手動で中止した後に3PAR Oracle ASM IR復元が失敗する

問題

IR ASM Oracleデータベースの復元と復旧を手動で中止した場合に、セッションの再起動が失敗しエラーが表示されます。

対処方法

処理が失敗した後に、ASMディスクグループをマウントして、RMANから手動による復旧を実行します。

プラガブルデータベースのバックアップが失敗して「プラガブルデータベースが存在しません」というエラーが表示される

問題

PDBがCDBからドロップした場合、次のエラーが表示されます。

ORA-65011: プラガブルデータベースが存在しません。

対処方法

このバグはOracle固有のバグです。

[Oracleサポート](#) ページにログインし、バグID **18967466**を検索します。

Bug 18967466 : ALTER DATABASE BEGIN BACKUP" COMMAND FAILS DUE TO ORA-65011 IF PDB HAS BEEN DROPED

第9章: レポートおよび通知のトラブルシューティング

レポートと通知に関する問題

Data Protector Windows上で送信方法として電子メールを使用したときにData Protector GUIが応答しなくなる

問題
<p>最新のセキュリティパッチをインストールしたMicrosoft Outlook XPを使用している場合、送信方法として電子メールを指定してレポートグループにレポートを追加した後、レポートグループを開始しようとすると、GUIがハングするという問題が発生します。通知を構成し、電子メールを送信方法として選択したときにも、同じ問題が発生します。</p> <p>Outlookでは、電子メール通知を送信する前にユーザー操作を要求するようになっているため、この問題が発生します。この機能は、Outlookセキュリティポリシーの一部なので無効化できません。</p>
対処方法
<ul style="list-style-type: none">ネットワーク上でSMTPサーバーを使用できる場合は、送信方法としてE-mail (SMTP)を選択します。電子メールの送信方法としては、この方法が推奨されます。以下のData Protector CLIを使用してレポートを開始します。 <pre>omnirpt -report licensing -email email_address</pre>電子メールの自動送信を許可するかどうかを確認する警告メッセージが表示されたら、[はい]をクリックして、レポートを受信します。 セキュリティ設定のカスタマイズ方法の詳細については、『Data Protector製品案内、ソフトウェアノート、およびリファレンス』を参照してください。

SNMPによる送信が失敗する

問題
レポートをSNMPトラップとして送信する際、レポートがあて先に到達しません。
対処方法
SNMPトラップによる送信方法は、構成されたSNMPトラップの最大サイズを超えないレポートにのみ使用します。

第10章: Data Protectorヘルプのトラブルシューティング

概要

Data Protectorヘルプは、以下の2つのパートで構成されています。

- ヘルプトピック: 概念、手順、例などが含まれます。
- 状況依存のヘルプ: コンテキストに依存する、ヘルプの動的な構成要素です。Data Protector GUIに表示される画面やオプションの説明を表示します。状況依存型ヘルプは、ヘルプナビゲーターというData Protector GUIコンポーネントによって表示されます。

このオンラインヘルプは、Microsoft HTML HelpとWebHelpの2種類の形式が用意されています。どちらの形式を使用するかは、Data Protector GUIのヘルプビューアーの現在の設定で決定します。

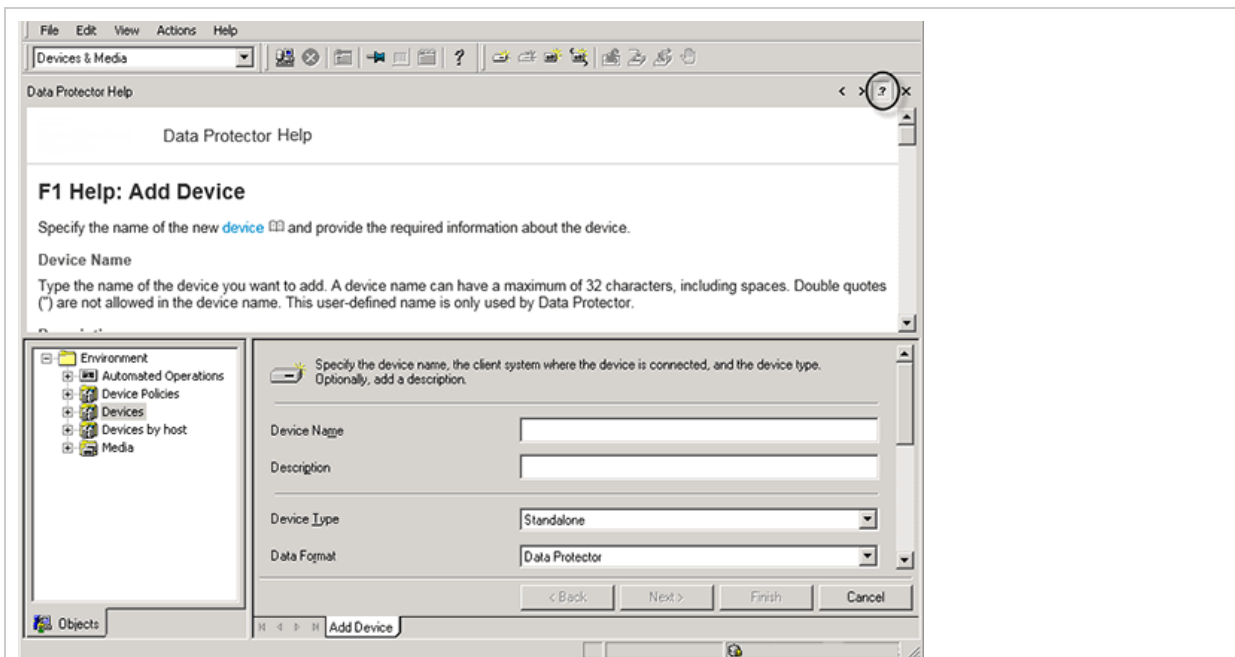
オンラインヘルプのトラブルシューティング

Data Protectorの画面を別の画面に切り替えても、その画面の説明がヘルプナビゲーターに表示されない

問題

Data Protectorの画面を別の画面に切り替えても、その画面の説明がヘルプナビゲーターに表示されません。

ヘルプナビゲーターの内容が切り替わらない



対処方法

- Microsoft HTMLヘルプビューアーを使用してHTMLヘルプ形式のData Protectorヘルプを表示する場合 (デフォルト選択)、Data Protectorヘルプのトラブルシューティング、前のページの図のようにボタンが選択されていることを確認してください。
- システムデフォルトのWebブラウザを使用してWebHelp形式のData Protectorヘルプを表示する場合、[ファイル]メニューから[選択値]をクリックし、[状況依存のヘルプナビゲーターを使用可能にする]オプションを選択します。その後、ヘルプナビゲーターを再起動します。

第11章: サポート サービスへご連絡いただく前に

当社サポート サービスへご連絡いただく前に

問題を解決できない場合は、HPカスタマーサポート サービスへご連絡ください。ただし、カスタマーサポート サービスへご連絡いただく前に、以下のことを確認してください。

- 一般的なチェックをすでに済ませていること。
([一般的なチェック](#)、[ページ 11](#)を参照)。
- また、その問題に関する情報が、該当するユーザーガイドのトラブルシューティングセクションに記載されているかどうかをチェックし終えていること。
- カスタマーサポート サービスに送付するデータとして、発生している問題の説明、セッションの出力(問題の種類によってそれに相当する出力)、および実際の環境の説明などの情報をすでに収集し終えていること。

その後の手順については、カスタマーサポート サービスよりご説明させていただきます。たとえば、以下のような作業をお願いすることがあります。

1. Data Protectorをデバッグモードで実行する。
2. カスタマーサポート サービスに送付するための生成データを準備する。

これらの手順について、以降の項で説明します。これらの手順が必要になるのは、カスタマーサポート サービスから依頼があった場合のみです。

デバッグについて

当社サポート担当者が技術的な問題を解決するために情報が必要となった場合にのみ、デバッグ情報の収集をお願いいたします。Data Protectorをデバッグモードで実行すると、デバッグ情報が作成され、大量のディスクスペースを消費します。デバッグの際に必要な詳細レベルおよび環境条件については、当社サポートサービスにお問い合わせください。

デバッグの有効化

Data Protectorをデバッグモードで起動するには、数通りの方法があります。デバッグオプションについては、「[デバッグ構文](#)、[次のページ](#)」を参照してください。

重要:

Data Protectorがデバッグモードで実行されている場合、すべての動作についてデバッグ情報が生成されます。バックアップセッションをデバッグモードで開始した場合、このバックアップ仕様でバックアップされた各クライアント上にDisk Agentから出力が送信されます。

注:

Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2012システムでネットワーク共有によるバックアップや復元セッションのデバッグを有効にするには、そのセッションが実行されているオペレーティングシステムのアカウントに対して、`Data_Protector_program_data\tmp`フォルダー

への書き込み権限が割り当てられている必要があります。

Data Protector GUIを使用する

[ファイル]メニューで[選択値]を選択し、[デバッグ]タブをクリックします。デバッグオプションを指定しGUIを再起動します。GUIはデバッグモードで再起動されます。

OB2DBG変数を使用する

Cell Serverのomnircファイル

Cell Serverまたは特定のクライアントでデバッグを実行する

```
OB2DBG=1-200 MA.txt "BMA@computer1.company.com,UMA@computer2.company.com"
```

クライアントのomnircファイル

プログラムの起動時に、omnirc変数がローカルで設定されていることが常に確認されます。ローカルのクライアントのみでデバッグを実行します。

```
OB2DBG=1-200 bma.txt "BMA,UMA"
```

OB2OPTS変数を使用する

Data Protector統合ソフトウェア用のデバッグパラメーターは、OB2OPTS環境変数を使用して設定します。この変数の設定方法については、当社サポート担当にお問い合わせください。

デバッグファイルのデフォルトの保存場所をシステムごとに変更するには、omnircオプションのOB2DBGDIRを使います。

デバッグ構文

ほとんどすべてのData Protectorコマンドは、-debug パラメーターを指定して起動できます。以下のような構文になります。

```
-debug 1-200[,C:n][,T:s][,U] XYZ Progname[@hostname]
```

ここで、

- 1-200は、デバッグ範囲を示します。特に指示のない限り、1-200と指定してください。省略可能なパラメーターは、この範囲パラメーターの一部として、カンマ区切りで指定してください。
 - C:nは、デバッグファイルのサイズをnキロバイトに制限します。最小値は4(4KB)で、デフォルト値は1024(1MB)です。詳細は、「[デバッグの最大サイズの制限、ページ 95](#)」を参照してください。
 - T:sは、タイムスタンプの分解能です。デフォルト値は1000です。一部のプラットフォームでは、ミリ秒の分解能を使用できません。
 - Uは、Unicodeフラグです。指定すると、Windows上のデバッグファイルがUnicode形式で書き込まれます。
- XYZは、デバッグの接尾辞です(DBG_01.txtなど)。
- hostは、デバッグモードが起動されているクライアントのリストです。

このオプションを使うと、指定したクライアント上でのみデバッグを実行することができます。複数のクライアントを指定する場合は、スペースで区切ります。リストは引用符で囲みます。

例:"computer1.company.com computer2.company.com"。

ログファイルの圧縮

範囲 (1-200,gz) の後に gz オプションを指定して、デバッグログファイルを圧縮することを選択できます。これは、ログをプレーンテキスト形式ではなく圧縮形式で作成します。ログは .gz 拡張子が付いて作成され、作成されたログファイルを展開するにはどのような市販ツールでも使用できます。

制限事項

- この機能は CM プラットフォームでのみサポートされています。
- Windows VEPA セッションで、CDpSessionLoggerSingleton および Lotus コンポーネントが gz フラグを無視し、圧縮されたログが作成されません。
- この機能は、循環デバッグと組み合わせて動作させることはできません。
- デバッグログのアーカイブは、異常終了時には使用できません。

デバッグオプション

- **範囲:** 1-200 は、デバッグ範囲を示します。指示された場合は、拡張範囲を指定します。省略可能なパラメーターは、この範囲パラメーターの一部として、カンマ区切りで指定してください。広い範囲を設定する場合、デバッグファイルのサイズが大きくなります。デバッグファイルリポジトリに十分な空き容量があることを確認してください。範囲は分割できます。区切り文字は、二重引用符で囲まれた「,」または「スペース」です。たとえば、-debug "1-99 104-140" debug.txt を使用できます。
- **循環デバッグ:** C:n は、デバッグファイルのサイズを n キロバイトに制限します。最小値は 4(4KB) で、デフォルト値は 1024(1MB) です。
- **秒単位およびミリ秒単位のタイムスタンプ:** T:s は、タイムスタンプの分解能で、使用できる値は 0、1 および 1000 です。デフォルトは 1 で、1000 が分解能 1 ミリ秒、0 がタイムスタンプを使用しないことを意味します。
- **Unicode 形式のデバッグファイル:** U は、Unicode フラグです。指定すると、Windows 上のデバッグファイルが Unicode 形式で書き込まれます。
- **接尾辞:** XYZ は、デバッグの接尾辞です (My_debug.txt など)。

注: 接尾辞はデバッグファイルを別のディレクトリにリダイレクトするために使用できます。保存先ディレクトリが存在していて、デバッグの書き込みプロセスに対してフルパスへの権限が正しいことが必要です。例: <DirPath>/My_debug.txt。

- **プログラムとホスト名:** select は、デバッグモードが起動されているクライアントのリストです。このオプションを使うと、指定したクライアント上でのみデバッグを実行することができます。複数のクライアントを指定する場合は、スペースで区切ります。リストは引用符で囲みます。例: progname[@hostname] [;progname[@hostname]]。

必要なデバッグファイル

一般的なデバッグ

ほとんどの場合、一般的なデバッグの範囲は1~200です。特にDAとMAのデバッグファイルの場合、フルデバッグはサイズが大きくなる可能性があります。

VEAgentデバッグログファイル

問題がVEAgentバックアップホストに関連している場合、次の一般的な設定をお勧めします。GUIの [Preferences Debug] タブで、-debug 1-199を実行します。

問題がVEAgent内で発生している場合、不要なBMAデバッグのサイズが非常に大きくなります。デバッグのサイズを制限するには、以下をお勧めします。

VEAgentバックアップホストのomnircファイルを作成するか、または以下の行を追加します:

```
OB2DBG=1-199,240 VM.txt "VEPA_BAR,VEPALIB_VMWARE_EXECUTION_THREAD,VEPALIB_VMWARE,VEPALIB_VMWARE_THREAD"
```

範囲1~199は不十分です。範囲240でvepa_bar debugファイルにomni_cellの内容が追加されます。ネットワークの詳細が必要な場合、範囲0~199、240~270を使用します。

VMware VDDKのログファイル

バージョン6.21、7.01、8.0の場合、vmware統合ソフトウェアで問題が発生すると、vddkログファイルに根本原因についての詳細情報が記録される可能性があります。有効にするには、VEAgentバックアップホストで、次の場所に移動します

C:\ProgramData\OmniBack\Config\client。Linuxの場合は、/etc/opt/omni/clientに移動します。ファイルvepa_vddk.configを編集して、ログレベルを6に上げます。

Vmware Triviaトランスポートログ

TRIVIAデバッグを有効にするには、vepa_vddk.configファイルを更新する必要があります。このファイルは/etc/opt/omni/clientの下、またはVepaバックアップホストの

C:\ProgramData\OmniBack\Config\client上にあります。このファイルを編集して、ログレベルを6にします。VMwareからTriviaの出力を収集するには、VEAgentに対してデバッグを有効にする必要があります。トランスポートログは、VEPALIB_VMWARE_EXECUTION_THREADファイル内の実行されたコマンドで操作します。

VMwareのログファイル

Managementエージェント(hostd)、VirtualCenter Agent Service (vpxa)、VirtualCenter (vpxd) のログは自動的にローテーションされ、その増加を管理するために維持されます。ログのローテーションが早すぎる場合、ログ内の情報が失われる可能性があります。詳細については、<http://kb.vmware.com/kb/1001457>を参照してください。

VMware ESX(i)のログファイル

esx(i)ホストには、たとえば、スナップショットの作成、削除など、実行されたすべてのアクティビティのログファイルが含まれます。ログファイルは、hostdで始まり、一度にすべてが圧縮されるテキストファイルです。hostd.logはアクティブなログファイルです。このファイルはデータストアに物理的に保存されます(たとえば、/var/log ->/scratch/log->/vmfs/volumes/4e265cdb-6b91f4b2-bc38-e4115b13545a/log)。

vCenter ServerのTriviaのログファイル

Triviaレベルのロギングを有効にするには、一般的には[管理] > [vCenter Server Settings] > [Logging Options] > [Trivia]に移動します。

Windowsでクラッシュした場合のVepa_bar localdump

<http://msdn.microsoft.com/en-us/library/windows/desktop/bb787181%28v=vs.85%29.aspx>を参照してください。レジストリを編集し、[LocalDumps]の下にvepa_bar.exeを追加します。

Media Agentのデバッグ

Media Agentに固有の問題については、次の一般的なガイダンスが適用されます:

- 一般的なほとんどの場合、1~200
- 19
- SHMIPCの場合、1~300
- 集約の場合、1~350
- メモリの追跡の場合、1~505

デバッグの最大サイズの制限

Data Protectorを循環デバッグと呼ばれる特殊なデバッグモードで実行することができます。このモードでは、デバッグファイルのサイズが事前設定されたサイズ(n)に達するまで、デバッグメッセージが追加されません。事前設定されたサイズに達すると、カウンターがリセットされ、最も古いデバッグメッセージが上書きされます。これにより、最新レコードに影響を与えることなく、トレースファイルのサイズを制限できます。

このモードは、セッションの終わり近くで問題が発生する場合、または問題発生後すぐにData Protectorが中止または終了する場合にのみ使用することをお勧めします。

循環デバッグを使用する場合、必要なディスクスペースの推定値は以下ようになります。

システム	必要となるディスクスペースの最大量
Media Agentクライアント	$2*n$ [kB] - バックアップまたは復元セッションで実行されるMedia Agentごとに必要
Disk Agentクライアント	$2*n$ [kB] - バックアップまたは復元セッションのマウントポイントごとに必要
Cell Manager	$2*n$ [kB]
統合ソフトウェアクライアント	$2*n$ [kB] * 並列処理

InetおよびCRSのデバッグでは、それぞれの動作に対して個別にデバッグファイルが作成されるため、正確な上限値を計算することはできません。

デバッグファイルの名前と保存場所

デバッグの接尾辞オプションを使って、デバッグファイルをデフォルトのData Protector一時ファイルディレクトリに作成します。

Windowsシステムの場合: `Data_Protector_program_data\tmp`

Windows 2003システムの場合: `Data_Protector_home\tmp`

UNIXシステムの場合: `/tmp`

ファイル名は以下ようになります。

`OB2DBG_DID__Program_Host_PID_XYZ`

ここで、

- *DID*(デバッグID)は、デバッグパラメーターを受け付ける最初のプロセスのプロセスIDです。このIDがデバッグセッションのIDとして使用されます。後続のプロセスもこのIDを使用します。
- *Program*は、デバッグファイルの書き込みを行うData Protectorプログラムのコード名です。
- *Host*は、デバッグファイルが作成されるクライアントの名前です。
- *PID*は、プロセスIDです。
- *XYZ*は、-debugパラメーターで指定された接尾辞です。

バックアップまたは復元セッションのID(*SID*)が決まると、そのIDがファイル名に付加されます。

OB2DBG_*DID*_*SID*_*Program*_*Host*_*PID*_*XYZ*

*SID*を付加するプロセスは、BMA/RMA、xBDA/xRDA、およびセッションにより起動された他のプロセスであり、BSM/RSM自体によっては付加されません。

注:

セッションIDは、デバッグファイルの識別に役立ちます。他のデバッグファイルも同じセッションに属している場合、それらにも付加する必要があります。

ctrace.logファイルはCell Manager上に作成され、デバッグファイルがどこに(どのクライアントに)作成されたか、どのようなデバッグ接頭辞が使われたかという情報が保存されます。このファイルには、生成されたすべてのファイルのリストが含まれているわけではないことに注意してください。

デバッグファイルのデフォルトの保存場所をシステムごとに変更するには、omnircオプションのOB2DBGDIRを使います。

Inetのデバッグ

注:

InetはWindowsプラットフォーム上のサービスで、omnircエントリを有効にするには、再起動する必要があります:

(sc stop OmniInet && sc start OmniInet)。

Inetのデバッグのみを有効にするには、inet クライアントの.omnirc ファイルを変更します

a) inet のデバッグのみを有効にするには: OB2DBG=1-200 inet.txt INET,INET-THREAD

b) すべてのデバッグを有効にするには: OB2DBG=1-200 all.txt

CRSのデバッグ

Windowsシステムの場合:

<Data Protector bin>\crs -redebug <range> <postfix> <select>

UNIXシステムの場合:

<Data Protector lbin>/crs -redebug <range> <postfix> <select>

注意:

Data Protectorクラスターグループがフェイルオーバーする原因となるため、Windows Service Control ManagerからCRSを終了しないでください。

Serviceguard/Symantec Veritas Cluster Server環境の場合:

1. デバッグを開始するには: CRSを開始する前に、`crs -debug <ranges> <postfix> [<select>]`を指定するか、またはOB2DBGをomnircファイルに入力します。
2. デバッグを停止するには: `/opt/omni/sbin/crs -redebug`
3. デバッグを再開するには: `crs -redebug <ranges> <postfix> [<select>]`

AppServerのデバッグ

デフォルトでは、AppServerログは、warnレベルのメッセージを表示します。詳細なAppServerログを確認するには、以下のコードのように、standalone.xmlファイルでlevel nameパラメーターを変更します。

```
<size-rotating-file-handler name="DP_LOGGER" autoflush="true">
  <level name="ALL"/>
  <formatter>
    <pattern-formatter pattern="%d{HH:mm:ss,SSS} %-5p [%C{1}:%L:%t]
    %s%E%n"/>
  </formatter>
  <file relative-to="jboss.server.log.dir" path="DPServer.log"/>
  <rotate-size value="10M"/>
  <max-backup-index value="5"/>
  <append value="true"/>
</size-rotating-file-handler>
```

standalone.xmlファイルで変更を行ったら、AppServerを再起動します。

詳細なWildFlyログを確認するには、<root logger>タグの前に<level name>パラメーターをstandalone.xmlファイルに追加します。パラメーターの追加後、standalone.xmlのコードは通常、以下のように表示されます。

```
<logger category="org.jboss.as">
  <level name="ALL" />
</logger>
<root-logger>
  <handlers>
    <handler name="CONSOLE"/>
    <handler name="FILE"/>
  </handlers>
</root-logger>
```

standalone.xmlファイルで変更を行ったら、AppServerを再起動します。

スケジューラーおよび実行されなかったジョブ実行のデバッグ

スケジューラーおよび実行されなかったジョブ実行をデバッグするには、アプリケーションサーバーのログを参照してください。

server.logを開き、詳細情報、エラーコード、エラーメッセージについて出力を確認します。

詳細については、「[ログファイルの保存場所](#)」を参照してください。

カスタマーサポートサービスに送付するための生成データの準備

カスタマーサポートサービスが技術上の問題を解決するために何らかのデータが必要な場合は、それらのデータを収集して送付するようにお客様にお願いすることがあります。Data Protectorは大規模なネットワーク環境で動作するため、データの収集が難しい場合があります。Data Protectorのomnidlcコマンドは、ログファイル、デバッグファイル、getinfoファイルの収集やパッキングを行うためのツールとして用意されています。このコマンドは、カスタマーサポートサービスから依頼があった場合に使用してください。

omnidlcコマンドは、Data Protector CLIまたはData Protector GUIから実行できます。この項では、両方の方法を説明します。

注:

omnidlcコマンドでは、Data Protectorインストール実行トレースの収集はできません。これらのトレースの作成と収集の方法の詳細については、『Data Protectorインストールガイド』を参照してください。

omnidlcコマンドについて

Data Protectorデバッグデータの生成後、omnidlcコマンドを使用すると、Data Protectorセル(デフォルトでは、すべてのクライアントから)から、Data Protectorデバッグファイル、ログファイル、getinfoファイルを収集できます。このコマンドでは、選択したクライアントからCell Managerにデータが転送され、そこでデータがパックされます。

このコマンドでは、特定のデータを選別して収集することができます。たとえば、あるクライアントのログファイルのみを収集したり、ある特定のData Protectorセッション中に作成されたデバッグファイルのみを収集したりすることができます。

注:

オブジェクト集約がポストバックアップセッションの一部としてスケジュールされている場合、バックアップセッションと集約セッションのセッションIDは異なります。ただし、デバッグIDはバックアップと集約の両方で同じになります。この場合、-sessionパラメーターを使用してomnidlcコマンドを実行し、集約セッションIDを指定すると、デバッグがバックアップと集約の両方に対して収集されます。

制限事項

- このコマンドはCell Managerでのみ実行できます。
- MoM環境では、個々のCell Managerからコマンドを実行することにより、各Data Protectorセルごとのデータのみを収集できます。
- デバッグファイルをデフォルトディレクトリから移動した場合は、`-debug_loc Directory1`オプションを使用して新しい場所を指定します。指定しない場合は、デバッグファイルが収集されなくなります。
- HP OpenVMSでデバッグおよびログファイルコレクターを使用する場合、以下の制限事項が適用されます。
 - OpenVMS ODS-2ディスク構造のファイル名には、最大で39文字まで使用できます。
 - OpenVMSシステムには`get_info`ユーティリティがないため、`get_info.out`ファイルは空白となり、収集されません。
 - `-session`オプションを指定して`omnidlc`コマンドを実行すると、指定されたセッション中に生成されたデバッグファイルは収集されません。これは、セッション名がOpenVMSデバッグファイル名の一部ではないためです。代わりに、すべての利用可能なログが収集されます。

CLIからomnidlcコマンドを使用することによるデバッグファイルの処理

収集データの範囲限定

収集データの範囲を限定するには、`omnidlc`コマンドを以下のオプションと共に使用します。

```
{-session SessionID | -did DebugID | -postfix String | -no_filter} [-hosts List] [-no_getinfo] [-no_config] [-no_logs] [-no_debugs] [-debug_loc Directory1 [Directory2]...]
```

以下の機能は、組み合わせて使用することができます。

- 選択したクライアントからのみデータを収集するには、`-hosts List`オプションを使用します。クライアントの名前をスペース区切りで指定します。
クラスター環境では、`-hosts`オプションを使用してクラスターノードを指定します。このオプションが指定されていない場合、データはアクティブなノードからのみ収集されます。
- 収集データから`getinfo`ファイル、構成情報、ログファイル、デバッグファイルを除外するには、`-no_getinfo`、`-no_config`、`-no_logs`、または`-no_debugs`オプションを使用します。`-no_getinfo`は、HP OpenVMSシステムには適用できないことに留意してください。
- 特定のセッションだけからデバッグファイルを収集するには、`-session SessionID`オプションを使用します。OpenVMSでは、利用可能なすべてのログが収集されます。
- 特定のデバッグIDに一致するデバッグファイルだけを収集するには、`-did DebugID`オプションを使用します。
- 指定した接尾辞に一致するデバッグファイルだけを収集するには、`-postfix String`オプションを使用します。
- すべてのデバッグファイルを収集するには、`-no_filter`オプションを使用します。

- デフォルトのデバッグファイルディレクトリだけではなく、他のディレクトリからもデバッグファイルを収集するには、`-debug_loc Directory1[Directory2]...` オプションを使用します。サブディレクトリは検索対象に含まれません。指定したディレクトリがクライアントに存在しない場合、そのディレクトリは無視されます。

データのセグメント化

Cell Manager に送信するファイルのサイズが 2 Gb を超えている場合、そのファイルは 2 GB サイズのチャンクに分割されます。各チャンクには、s001～s999 の範囲内の拡張子が付加されます。ファイルが圧縮されている場合は、2 番目の拡張子として .gz が付加されます。

一方、Cell Manager 側では、圧縮済みまたは未圧縮の収集ファイルのサイズがすべて 2 Gb を超えている場合、収集ファイルは 2 GB サイズのパッケージにパックされ、ファイル名には s001～s999 の範囲内の拡張子が付加されます。

収集データの圧縮の無効化

デフォルトでは、収集データは Cell Manager への送信前に圧縮されます。圧縮を無効にするには、`-no_compress` オプションを使用します。

パックしたデータの保存

デフォルトでは、ネットワークを経由して Cell Manager にデータが送信され、そこでデータがパックされて、カレントディレクトリに dlc.pck ファイルとして保存されます。

パックされたファイルには、関連するクライアントのホスト名、パス、収集ファイルを含むディレクトリ構造が含まれています。

制限事項

- 最終的なパック済みファイルのサイズは 2 GB 以内に制限されます。この制限を超える場合はデータをパックしないでください。

データをパックして保存するには、`-pack Filename` オプションを使用します。

- 異なるファイル名を使用する場合は、ファイル名として *Filename* を指定します。
- 異なるディレクトリに異なるファイル名で保存する場合は、フルパス名として *Filename* を指定します。

パックされていないデータの保存

データをパックせずに保存するには、`-depot [Directory]` オプションを使用します。ファイルは、dlc サブディレクトリ内に収集されます。*Directory* を指定しない場合、ファイルは Cell Manager 上のデフォルトの Data Protector 一時ファイルディレクトリの dlc ディレクトリに保存されます。

パックされた、またはパックされていないファイルのディレクトリは、以下のように生成されます。

```
./dlc/client_1/tmp/debug_files
./dlc/client_1/log/log_files
./dlc/client_1/getinfo/get_info.txt
./dlc/client_2/tmp/debug_files
./dlc/client_2/log/log_files
```

```
./dlc/client_2/getinfo/get_info.txt
```

...

必要なスペースの推定

データの収集に必要なとなるCell Manager上のディスクスペースを表示するには、-spaceオプションを使用します。

クライアント上のデバッグファイルの削除

収集データをクライアントから削除するには、-delete_dbgオプションを使用します。デバッグファイルだけが削除されることに注意してください。getinfoファイルとログファイルは削除されません。HP OpenVMSで、-sessionオプションを指定してomnidlcコマンドを実行した場合、いずれのデバッグファイルもデバッグファイルディレクトリから削除されません。

デバッグファイルについての情報の削除

デバッグログの生成場所(どのクライアント上か)、および使用されるデバッグ接頭辞の情報が格納されているctrace.logファイルを削除するには、-del_ctrace_logオプションを使います。-hosts Listオプションと一緒に使用すると、特定のクライアント上だけでctrace.logファイルが削除されます。それ以外の場合は、セル内のすべてのクライアントでctrace.logファイルが削除されます。

注:

このオプションは、ctrace.logファイルのクリーンアップに使用します。このファイルを削除すると、デバッグログコレクターはデフォルトのData Protector一時ファイルディレクトリに存在するデフォルトのdlcからのみデバッグを取得し、ユーザーが指定した他のデバッグディレクトリからは取得しません。

問題と回避策

デバッグログの収集に失敗する

問題

デバッグログの収集処理の際に、omnidlcがクライアントに接続できない。以下のエラーが表示される。

```
Collection from client1.company.com started.
```

```
Error: Data retrieval from client1.company.com failed.
```

```
Warning: Collection from client1.company.com incomplete.
```

この問題は、クライアントの構成ファイルで指定されているCell Managerの名前と、デバッグログの収集で必要とするCell Managerの名前が一致しない場合に発生します。

対処方法

Cell Managerホスト名を、デフォルトのData Protectorクライアント構成ディレクトリにあるomnidlc_hostsファイルに追加します。

その他の操作

- 圧縮データか未圧縮データかにかかわらず、パックされていないデータをCell Managerに送信 (-depot オプションを使用した後でパックするには、-localpack [Filename] オプションを使用します。
このオプションでは、カレントディレクトリのディレクトリ構造がパックされます(カレントディレクトリは、-depot オプションで生成されたdlcディレクトリが含まれるディレクトリでなくてはなりません)。Filename 引数を省略すると、カレントディレクトリ内にdlc.pckファイルが生成されます。
このオプションの機能は-pack オプションの機能と同等ですが、-depot オプションを使用してデータを収集した場合にのみ使用してください。
- クライアントの特定のディレクトリから追加情報(スクリーンショットやピクチャーなど)を取得するには、-add_info [-any | Host] Path オプションを使用します。
-any オプションは、すべてのクライアントでディレクトリパスが同じ場合に使用されます。
- データをアンパックするには、-unpack [Filename] オプションを使用します。
Filename 引数を省略すると、カレントディレクトリ内のdlc.pckファイルがアンパックされます。カレントディレクトリ内のdlcディレクトリが常にデータのアンパック先となります。
このオプションは、-pack オプションまたは-localpack オプションのいずれかを使用して収集データをCell Manager上でパックした場合に使用してください。
- 単一の圧縮ファイルを展開するには、-uncompress Filename オプションを使用します。パックされているデータの場合は、先にアンパックしておく必要があります。
- 詳細出力を有効にするには、-verbose オプションを使用します。

Data Protector GUIを使用したデバッグファイルの処理

デバッグセッション中に生成できるファイルの種類は、デバッグ、ログ、およびgetinfoです。

Data Protector GUIでは、以下のデバッグファイルの操作を実行できます。

- [デバッグファイル操作の実行、次のページ](#)
デバッグファイル操作は、Data Protector GUI内のさまざまな場所から開始できます。
- [デバッグファイルの収集、次のページ](#)
デバッグファイルがクライアントシステムから収集され、Cell Manager上に格納されます。
- [デバッグファイル領域の計算、ページ 104](#)
収集ファイル用としてCell Manager上に必要なスペースが計算されます。
- [デバッグファイルの削除、ページ 105](#)
デバッグファイルがクライアントシステムから削除されます。

これらは、**内部データベース**または**クライアント**のコンテキストで実行できます。

GUI操作では、omnidlcコマンドのさまざまなオプションを使用します。コマンドラインインターフェイスでomnidlcコマンドを直接使用すると、収集したファイルに対して他の操作も実行できます。詳細は、[CLIからomnidlcコマンドを使用することによるデバッグファイルの処理、ページ 99](#)または『*Data Protector Command Line Interface Reference*』を参照してください。

以下の項の操作を実行すると、使用されたomnidlc構文が**[結果]**ウィンドウに表示されます。

デバッグファイル操作の実行

クライアントのコンテキストからデバッグファイル操作にアクセスするには:

1. Scoping ペインで、**[クライアント]** フォルダを展開してから、デバッグファイル操作が必要なクライアントを選択します。
2. 実行する操作を選択します。
 - 選択項目を右クリックし、必要な操作を選択します。**デバッグファイルの収集**、**デバッグファイル領域の計算**または**デバッグファイルの削除**。
または
 - メニューバーで**[アクション]**→**[デバッグファイル]**を選択してから、**[収集]**、**[スペースのチェック]**、または**[削除]**を選択します。

内部データベースのコンテキストからデバッグファイル操作にアクセスするには:

1. Scoping ペインで、**[セッション]** フォルダを展開してから、デバッグファイル操作が必要なセッションを選択します。
2. 実行する操作を選択します。
 - 選択項目を右クリックし、必要な操作を選択します。**デバッグファイルの収集**、**デバッグファイル領域の計算**または**デバッグファイルの削除**。
または
 - メニューバーで**[アクション]**→**[デバッグファイル]**を選択してから、**[収集]**、**[スペースのチェック]**、または**[削除]**を選択します。

どちらの場合も、操作を選択するとウィザードが開始され、必要な手順を画面に従って実行できます。

サービスを再起動しないでMMDのデバッグを開始/停止する

1. MMDのデバッグを開始するには、MMDの実行中に、以下のコマンドを実行します。

```
mmd.exe -redebug [ranges] [postfix] [select]
```
2. MMDのデバッグを停止するには、MMDの実行中に、以下のコマンドを実行します。

```
mmd.exe -stopdebug
```

デバッグファイルの収集

デバッグファイルを収集するには:

1. **デバッグファイル操作の実行**、**上**の説明に従って、デバッグファイルコレクターウィザードを起動します。

セッションを選択して**[内部データベース]**コンテキストから開始した場合は、そのセッションがウィザードの**[クライアント]**ページの**[フィルター]**セクションであらかじめ選択され、セッションに関係するクライアントが選択されます。

[クライアント]コンテキストから開始した場合は、そこで選択したクライアントがウィザードの**[クライアント]**ページであらかじめ選択されます。
2. **[クライアント]**ページで、対象とするクライアントを限定するために、以下の手順を実行します。

- a. ファイルを収集するクライアントのみを選択します。クライアントが事前に選択されている場合、それらの選択を解除できます。
- b. **[次へ]**をクリックします。
3. [ディレクトリ]ページで、以下の手順を実行します。
 - a. デバッグファイルの有無をチェックするディレクトリが、デフォルトのデバッグファイルディレクトリの他にあればそのディレクトリを入力し、**[追加]**をクリックします。
 - b. 内容を収集するディレクトリが他にある場合は、ディレクトリツリーでそのディレクトリを選択します (そのサブディレクトリの内容は収集されません)。
 - c. **[次へ]**をクリックします。
4. [オプションと操作]ページで、以下の手順を実行します。
 - a. 使用しないデバッグ収集オプションがあれば、選択を解除します。omnidlcオプションに関する一般情報は、『Data Protector Command Line Interface Reference』を参照してください。
 - b. デバッグログの収集時に、複数のフィルターオプションを指定できます。以下のフィルターオプションを使用できます。
 - セッションID: デバッグファイルが生成されたバックアップセッションです。
 - デバッグID: デバッグファイルが生成されたデバッグセッションです。
 - 接尾辞: デバッグファイル名です。
 - モジュール: デバッグログを必要とするモジュールです。複数のモジュールをカンマで区切って入力できます。例: BSM,BDSM,VBDA
 - c. デバッグファイルをCell Managerに格納する際の手順を選択します。
 - **[デポの作成]**は、(バックされていない)ファイルをデフォルトのData Protector一時ファイルディレクトリのdlcサブディレクトリに保存します。
別の場所を指定するには、既存のディレクトリを**[ターゲットパス]**に入力します。デフォルトの場所を使用する場合は、テキストボックスが空白になっていることを確認してください。
このオプションを使用すると、サポート窓口に情報を送付する前に、収集したファイルを確認し任意のファイルを削除できます。以降は、CLIコマンド `omnidlc -localpack [Filename]` を使用してバックファイルを作成できます (詳細については、『Data Protector Command Line Interface Reference』を参照してください)。
 - **[バックファイルの作成]**を使用すると、収集したファイルを含むバックファイルを作成できます。**[ターゲットパス]**で、ファイルのフルパスを指定します。
 - d. **[完了]**をクリックします。

デバッグファイル領域の計算

実際に収集を行う前に、デバッグファイル収集用としてCell Manager上に必要な合計スペースを計算できます。それには、必要なすべての収集情報を「デバッグファイル領域計算」ウィザードに入力します。計算が完了したら、指定条件に基づいて収集を開始することができます。

デバッグファイル収集用としてCell Managerに必要な合計スペースを計算するには:

1. **デバッグファイル操作の実行、前のページ**の説明に従って、デバッグファイル領域計算ウィザードを起動します。
2. [クライアント]ページで、対象とするクライアントを限定するために、以下の手順を実行します。

- a. ファイルを収集するクライアントのみを選択します。クライアントが事前に選択されている場合、それらの選択を解除できます。
 - b. **[フィルター]**で、フィルター条件 (**[セッションID]**、**[デバッグID]**、**[Postfix]**、または**[フィルターなし]**)を選択し、必要な識別子を入力します。**[フィルターなし]**を選択すると、選択したクライアント上のすべてのデバッグファイルが収集されます。セッションが事前に選択されている場合、そのセッションを変更できません。
 - c. **[次へ]**をクリックします。
3. **[ディレクトリ]**ページで、以下の手順を実行します。
 - a. デバッグファイルの有無をチェックするディレクトリが、デフォルトのデバッグファイルディレクトリの他にあればそのディレクトリを入力し、**[追加]**をクリックします。
 - b. 内容を収集するディレクトリが他にある場合は、ディレクトリツリーでそのディレクトリを選択します (そのサブディレクトリの内容は収集されません)。
 - c. **[次へ]**をクリックします。
 4. **[オプション]**ページで、以下の手順を実行します。
 - a. 使用しないデバッグ収集オプションがあれば、選択を解除します。omnidlcオプションに関する一般情報は、『Data Protector Command Line Interface Reference』を参照してください。
 - b. **[次へ]**をクリックします。

チェックの結果は**[結果]**タブに表示されます。

計算が終了すると、ダイアログボックスが表示され、デバッグファイルの収集を開始するかどうか尋ねられます。

スペース計算に対して選択したオプションを使用して、デバッグファイルの収集を開始するには:

- **[はい]**をクリックします。
デフォルトの操作動作 (バックアップファイルの作成) が Cell Manager で使用されます。「[デバッグファイルの収集、ページ 103](#)」を参照してください。

デバッグファイルの削除

デバッグファイルをクライアントから削除するには:

1. [デバッグファイル操作の実行、ページ 103](#)の説明に従って、デバッグファイルの削除ウィザードを起動します。
2. **[クライアント]**ページで、削除するファイルを制限するには:
 - a. ファイルを削除するクライアントのみを選択します。
 - b. **[フィルター]**で、フィルター条件 (**[セッションID]**、**[デバッグID]**、**[Postfix]**、または**[フィルターなし]**)を選択し、必要な識別子を入力します。
[フィルターなし]を選択すると、選択したクライアント上のすべてのデバッグファイルが削除されます。
 - c. **[次へ]**をクリックします。
3. **[ディレクトリ]**ページで、以下の手順を実行します。
 - a. デバッグファイルを削除するディレクトリが、デフォルトのデバッグファイルディレクトリの他にあればそのディレクトリを入力し、**[追加]**をクリックします。
 - b. **[完了]**をクリックします。

omnidlcコマンドの使用例

1. 詳細出力を有効にして、セル内のすべてのデバッグファイル、ログファイル、getinfoファイルを収集して圧縮し、それらをCell Manager上のカレントディレクトリにd1c.pckファイルとしてパックするには、次のコマンドを実行します。

```
omnidlc -no_filter -verbose
```

2. client1.company.comおよびclient2.company.comというクライアントからログファイルとデバッグファイルのみをCell Managerのc:\depotディレクトリに収集し、圧縮もパックも行わないようにするには、次のコマンドを実行します。

```
omnidlc -no_filter -hosts client1.company.com client2.company.com -depot c:\depot -no_getinfo -no_compress
```

3. client1.company.comというクライアントからログファイル、デバッグファイル、getinfoファイルを収集し、それらをCell Manager上のc:\pack\pack.pckというファイルに圧縮およびパックするには、次のコマンドを実行します。

```
omnidlc -hosts client1.company.com -pack c:\pack\pack.pck
```

4. クライアントclient1.company.comおよびclient2.company.com上で、デフォルトの保存場所からログファイル、デバッグファイル、getinfoファイルを収集するとともに、追加のディレクトリC:\tmpおよび/tmp/debugsからデバッグファイルを収集して、Cell Manager上で圧縮およびパックするには、次のコマンドを実行します。

```
omnidlc -hosts client1.company.com client2.company.com -debug_loc C:\tmp /tmp/debugs
```

5. ID 2012/02/16-11に一致するセッションのすべてのデバッグファイルを削除するには、次のコマンドを実行します。

```
omnidlc -session 2012/02/16-11 -delete_dbg
```

6. クライアントclient.company.com上で、デバッグID 2351に一致する未圧縮デバッグファイルに関して、Cell Manager上で必要となるディスクスペースを表示させるには、次のコマンドを実行します。

```
omnidlc -did 2351 -hosts client.company.com -space -no_getinfo -no_logs -no_compress
```

7. クライアントclient1.company.comのC:\debugディレクトリにある他のファイルを、ID 2012/02/12-24のセッションのデバッグログファイルとともにパックするには、次のコマンドを実行します。

```
omnidlc -session 2012/02/12-24 -add_info -host client1.company.com C:\debug
```

8. カレントディレクトリのディレクトリ構造を同じディレクトリ内のd1c.pckファイルにパックするには、次のコマンドを実行します(カレントディレクトリは、-depotオプションで生成したd1cディレクトリが格納されているディレクトリでなければなりません)。

```
omnidlc -localpack
```

9. d1c.pckファイルをカレントディレクトリのd1cディレクトリにアンパックするには、次のコマンドを実行します。

```
omnidlc -unpack
```

Data Protector GUIを使用することによるデバッグファイルの処理

デバッグセッション中に生成できるファイルの種類は、デバッグ、ログ、およびgetinfoです。

Data Protector GUIでは、以下のデバッグファイルの操作を実行できます。

- [デバッグファイル操作の実行、下](#)
デバッグファイル操作は、Data Protector GUI内のさまざまな場所から開始できます。
- [デバッグファイルの収集、次のページ](#)
デバッグファイルがクライアントシステムから収集され、Cell Manager上に格納されます。
- [デバッグファイル領域の計算、ページ 109](#)
収集ファイル用としてCell Manager上に必要なスペースが計算されます。
- [デバッグファイルの削除、ページ 109](#)
デバッグファイルがクライアントシステムから削除されます。

これらは、**内部データベース**または**クライアント**のコンテキストで実行できます。

GUI操作では、omnidlcコマンドのさまざまなオプションを使用します。コマンドラインインターフェイスでomnidlcコマンドを直接使用すると、収集したファイルに対して他の操作も実行できます。詳細は、[CLIからomnidlcコマンドを使用することによるデバッグファイルの処理、ページ 99](#)または『Data Protector Command Line Interface Reference』を参照してください。

以下の項の操作を実行すると、使用されたomnidlc構文が**[結果]**ウィンドウに表示されます。

デバッグファイル操作の実行

内部データベースのコンテキストからデバッグファイル操作にアクセスするには:

1. Scopingペインで、**[セッション]**フォルダーを展開してから、デバッグファイル操作が必要なセッションを選択します。
2. 実行する操作を選択します。
 - 選択したアイテムを右クリックし、**[デバッグファイルの収集]**、**[デバッグファイル領域の計算]**、**[デバッグファイルの削除]**の中から必要な操作を選択します。
または
 - メニューバーで**[アクション]**→**[デバッグファイル]**を選択してから、**[収集]**、**[スペースのチェック]**、または**[削除]**を選択します。

クライアントのコンテキストからデバッグファイル操作にアクセスするには:

1. Scopingペインで、**[クライアント]**フォルダーを展開してから、デバッグファイル操作が必要なクライアントを選択します。
2. 実行する操作を選択します。
 - 選択したアイテムを右クリックし、**[デバッグファイルの収集]**、**[デバッグファイル領域の計算]**、**[デバッグファイルの削除]**の中から必要な操作を選択します。

または

- メニューバーで[アクション]→[デバッグファイル]を選択してから、[収集]、[スペースのチェック]、または[削除]を選択します。

どちらの場合も、操作を選択するとウィザードが開始され、必要な手順を画面に従って実行できます。

デバッグファイルの収集

1. **デバッグファイル操作の実行、前のページ**の説明に従って、デバッグファイルコレクターウィザードを起動します。
セッションを選択して[内部データベース]コンテキストから開始した場合は、そのセッションがウィザードの[クライアント]ページの[フィルター]セクションであらかじめ選択され、セッションに関係するクライアントが選択されます。
[クライアント]コンテキストから開始した場合、選択したクライアントは、ウィザードの[クライアント]パネルで事前に選択されます。
2. [クライアント]ページで、対象とするクライアントを限定するために、以下の手順を実行します。
 - a. ファイルを収集するクライアントのみを選択します。クライアントが事前に選択されている場合、それらの選択を解除できます。
 - b. [フィルター]で、フィルター条件 ([セッションID]、[デバッグID]、[Postfix]、または[フィルターなし])を選択し、必要な識別子を入力します。[フィルターなし]を選択すると、選択したクライアント上のすべてのデバッグファイルが収集されます。セッションIDが事前に選択されている場合、そのセッションIDを変更できません。
 - c. [次へ]をクリックします。
3. [ディレクトリ]ページで、以下の手順を実行します。
 - a. デバッグファイルの有無をチェックするディレクトリが、デフォルトのデバッグファイルディレクトリの他にあればそのディレクトリを入力し、[追加]をクリックします。
 - b. 内容を収集するディレクトリが他にある場合は、ディレクトリツリーでそのディレクトリを選択します (そのサブディレクトリの内容は収集されません)。
 - c. [次へ]をクリックします。
4. [オプションと操作]ページで、以下の手順を実行します。
 - a. 使用しないデバッグ収集オプションがあれば、選択を解除します。最初に開いたときは、omnidlcコマンドで使用する標準のデフォルトに一致するように選択されています。この詳細については、『*Data Protector Command Line Interface Reference*』を参照してください。
 - b. デバッグファイルをCell Managerに格納する際の操作を選択します。
 - [デポの作成]は、(バックされていない)ファイルをデフォルトのData Protector一時ファイルディレクトリのdlcサブディレクトリに保存します。
別の場所を指定するには、既存のディレクトリを[ターゲットパス]に入力します。デフォルトの場所を使用する場合は、テキストボックスが空白になっていることを確認してください。
このオプションを使用すると、サポート窓口に情報を送付する前に、収集したファイルを確認し任意のファイルを削除できます。以降は、CLIコマンド `omnidlc -localpack [filename]` を使用してバックファイルを作成できます (詳細については、『*Data Protector Command Line Interface Reference*』を参照してください)。

- **[パックファイルの作成]**を使用すると、収集したファイルを含むパックファイルを作成できます。
[ターゲットパス]で、ファイルのフルパスを指定します。
- c. **[完了]**をクリックします。

デバッグファイル領域の計算

実際に収集を行う前に、デバッグファイル収集用としてCell Manager上に必要な合計スペースを計算できます。それには、必要なすべての収集情報を「デバッグファイル領域計算」ウィザードに入力します。計算が完了したら、指定条件に基づいて収集を開始することができます。

デバッグファイル収集用としてCell Managerに必要な合計スペースを計算するには:

1. **デバッグファイル操作の実行、ページ 107**の説明に従って、デバッグファイル領域計算ウィザードを起動します。
2. **[クライアント]**ページで、対象とするクライアントを限定するために、以下の手順を実行します。
 - a. ファイルを収集するクライアントのみを選択します。クライアントが事前に選択されている場合、それらの選択を解除できます。
 - b. **[フィルター]**で、フィルター条件 (**[セッションID]**、**[デバッグID]**、**[Postfix]**、または**[フィルターなし]**)を選択し、必要な識別子を入力します。**[フィルターなし]**を選択すると、選択したクライアント上のすべてのデバッグファイルが収集されます。セッションが事前に選択されている場合、そのセッションを変更できません。
 - c. **[次へ]**をクリックします。
3. **[ディレクトリ]**ページで、以下の手順を実行します。
 - a. デバッグファイルの有無をチェックするディレクトリが、デフォルトのデバッグファイルディレクトリの他にあればそのディレクトリを入力し、**[追加]**をクリックします。
 - b. 内容を収集するディレクトリが他にある場合は、ディレクトリツリーでそのディレクトリを選択します (そのサブディレクトリの内容は収集されません)。
 - c. **[次へ]**をクリックします。
4. **[オプション]**ページで、以下の手順を実行します。
 - a. 使用しないデバッグ収集オプションがあれば、選択を解除します。最初に開いたときは、omnidlcコマンドで使用する標準のデフォルトに一致するように選択されています。この詳細については、『*Data Protector Command Line Interface Reference*』を参照してください。
 - b. **[次へ]**をクリックします。

チェックの結果は**[結果]**タブに表示されます。

計算が終了すると、ダイアログボックスが表示され、デバッグファイルの収集を開始するかどうか尋ねられます。

スペース計算に対して選択したオプションを使用して、デバッグファイルの収集を開始するには:

- **[はい]**をクリックします。
デフォルトの操作動作 (**[パックファイルの作成]**)がCell Managerで使用されます。**デバッグファイルの収集、前のページ**を参照してください。

デバッグファイルの削除

デバッグファイルをクライアントから削除するには:

1. **デバッグファイル操作の実行、ページ 107**の説明に従って、デバッグファイルの削除ウィザードを起動します。
2. [クライアント]ページで、削除するファイルを制限するには:
 - a. ファイルを削除するクライアントのみを選択します。
 - b. **[フィルター]**で、フィルター条件 (**[セッションID]**、**[デバッグID]**、**[Postfix]**、または**[フィルターなし]**)を選択し、必要な識別子を入力します。
[フィルターなし]を選択すると、選択したクライアント上のすべてのデバッグファイルが削除されます。
 - c. **[次へ]**をクリックします。
3. [ディレクトリ]ページで、以下の手順を実行します。
 - a. デバッグファイルを削除するディレクトリが、デフォルトのデバッグファイルディレクトリの他にあればそのディレクトリを入力し、**[追加]**をクリックします。
 - b. **[完了]**をクリックします。

カスタマーサポート サービスに送付するデータ収集の例

あるクライアントとCell Managerにおいてバックアップセッション中に発生した問題について、デバッグファイル、ログファイル、getinfoファイルを収集する場合は、次の操作を実行します。

1. 以下のことを行って、エラー環境の規模をできる限り縮小します。
 - 1つまたは少数のファイルやディレクトリだけを含むバックアップ仕様を作成します。
 - デバッグでは、問題のあるクライアントだけを実行します。
2. info用のテキストファイルを作成して、以下の情報を入力します。
 - Cell Manager、Media Agent、Disk Agentのクライアントのハードウェア識別情報 例: HPE-9000 T-600 Series、Vectra XA
 - SCSIコントローラーの名前(たとえば、onboard_type/Adaptec xxx/... (Windows Media Agent クライアントの場合))
 - omniceilinginfo -cellコマンドの出力結果に含まれるトポロジ情報
 - devbra -devコマンドの出力(バックアップデバイスに問題がある場合)
3. 技術的な問題について当社サポート窓口にお問い合わせの上、以下の情報を照会します。
 - デバッグレベル(例: 1-200)。これは後で必要になるコマンドオプションです。
 - デバッグ範囲(クライアントのみ、Cell Managerのみ、すべてのシステムなど)
4. すべてのユーザーインターフェイスを終了して、セル内の他のすべてのバックアップ動作を中止します。
5. InetデバッグまたはCRSデバッグも同時に収集するには、Cell ManagerのInetサービスまたはCRSサービスをデバッグモードで再起動します。
6. Cell Manager上で以下のコマンドを実行すると、GUIがデバッグモードで起動します。

```
manager -debug 1-200 error_run.txt
```

作成されるデバッグファイルの名前の末尾には、error_run文字列の代わりに、ユーザーが希望する名前を定義できます。

7. Data Protectorを使って問題を再現します。
8. すべてのユーザーインターフェイスを終了して、デバッグモードを終了します。

InetおよびCRSのデバッグ情報も収集した場合は、Cell Manager上のData Protectorサービスをデバッグオプションなしで再起動する必要があります。

9. Cell Managerで、次のコマンドを実行します。

```
omnidlc -postfix error_run.txt
```

このコマンドを実行すると、クライアント上でerror_run.txt接尾辞を持つログファイル、getinfoファイル、およびデバッグファイルが圧縮されて、ネットワーク経由でCell Managerに送信されます。これらのファイルはCell Managerで1つにまとめられて、カレントディレクトリにdlc.pckファイルとして保存されません。

10. このdlc.pckファイルを当社サポート窓口に電子メールで送信します。
11. Cell Manager上で次のコマンドを実行し、クライアント上に作成されたデバッグファイル(末尾がerror_run.txtという名前のファイル)を削除します。

```
omnidlc -postfix error_run.txt -delete_dbg
```

フィードバックを送信

このドキュメントに関するご意見は、[ドキュメンテーションチーム](#)まで電子メールでお送りください。お使いのシステムに電子メールクライアントが設定されている場合は、上のリンクをクリックすると、電子メールウィンドウが開き、件名行に次の情報が入力されます。

トラブルシューティングガイド (Data Protector 10.00)に関するフィードバック

本文にご意見、ご感想を記入の上、**[送信]**をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーしてWebメールクライアントの新規メッセージに貼り付け、docs.feedback@microfocus.com宛にお送りください。

お客様からのご意見、ご感想をお待ちしています。