

CA ARCserve® Central Host-Based VM Backup

ユーザガイド

r16



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複製、譲渡、開示、変更、複製することはできません。本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、
(i) 本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負いません。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者は CA です。

「制限された権利」のもとの提供: アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2012 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication/High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

CA への連絡先

テクニカルサポートの詳細については、弊社テクニカルサポートの Web サイト (<http://www.ca.com/jp/support/> (<http://www.ca.com/jp/support/>)) をご覧ください。

CA ARCserve Central Applications のサポート リンク

CA サポート オンラインでは、技術的な問題を解決するのに役立つ豊富なリソースのセットが提供され、重要な製品情報にも容易にアクセスできます。CA サポートを使用して、信頼できるアドバイスをいつでも簡単に利用できます。以下のリンクを使用すると、さまざまな CA サポートサイトにアクセスできます。

- **サポートの紹介** -- 以下のリンクでは、契約条件、請求、サービスレベル目標 (SLO)、サービス時間など、メンテナンスプログラムおよびサポート サービスに関する情報が提供されます。

<http://www.ca.com/jp/support/> (<http://www.ca.com/jp/support/>)

- **サポートへの登録** -- 以下は、CA サポート オンライン登録フォームへのリンクです。製品サポートを有効にするために使用します。

<http://www.casupport.jp/support/supportonline/>
(<http://www.casupport.jp/support/supportonline/>)

- **テクニカルサポートへのアクセス** -- 以下は、CA ARCserve Central Applications のワンストップ サポート ページへのリンクです。

<http://www.casupport.jp/resources/storagesupp>
(<http://www.casupport.jp/resources/storagesupp/>)

マニュアルの変更点

このドキュメントには、製品およびドキュメント自体の利便性と理解の向上に役立つことを目的として、ユーザのフィードバック、拡張機能、修正、その他小規模な変更が含まれています。

本マニュアルでは、GA リリース以降に以下の点を更新しています。

Update 7

- 「[バックアップポリシーの作成](#) (P. 87)」が更新されました。このトピックには、新しい保存設定機能が含まれています。この機能では、保持する復旧ポイントの数または保持する復旧セットの数に基づいて保存ポリシーを設定できます。
- 「[バックアップポリシーの編集またはコピー](#) (P. 91)」が更新されました。このトピックには、新しい保存設定機能が含まれています。この機能では、保持する復旧ポイントの数または保持する復旧セットの数に基づいて保存ポリシーを設定できます。
- 「[マージジョブ オプション](#) (P. 60)」が追加されました。このトピックには、[ノード] 画面上の 2 つの新しいオプション、[[マージジョブの一時停止](#) (P. 60)] および [[マージジョブの再開](#) (P. 61)] が含まれています。これらのトピックでは、特定のノード用のマージジョブを一時停止または再開する方法について説明しています。
- 「[増分バックアップジョブが検証バックアップジョブとして処理される](#) (P. 165)」が更新されました。このトピックでは、VMware ナレッジベース記事に説明されている手順に基づいて、検証バックアップジョブとして実行される増分バックアップジョブを修正する方法について説明します。
- 「[仮想マシンの復旧で指定とは異なる転送モードが使用される](#) (P. 176)」が追加されました。このトラブルシューティングトピックでは、レジストリ キーでの指定とは異なる転送モードが使用される場合の仮想マシン復旧の動作を指定します。

Update 6

- 「[CA ARCserve Central Protection Manager サーバを設定する方法 \(P. 34\)](#)」が追加されました。この環境設定では、CA ARCserve Central Host-Based VM Backup の現在の設定を CA ARCserve Central Protection Manager サーバ設定に変更できます。設定を指定すると、Host-Based VM Backup 検出ノード用電子メールアラート情報を CA ARCserve Central Reporting から表示できます。
- 「[ディスクバリ スケジュールの設定 \(P. 36\)](#)」が更新されました。このトピックには、ノードディスクバリのスケジュール設定時に表示される vCenter/ESX ホストリストが含まれるようになりました。
- 「[電子メールとアラートの設定の指定 \(P. 36\)](#)」が更新されました。トピックのタイトルを変更し、検出されたノード用のアラートを含めるように更新しました。保存した設定を削除できる、新しい [削除] ボタンがこの画面に追加されました。保存した設定を削除すると、電子メールアラートメッセージを受信しなくなります。
- 「[CA ARCserve Central Host-Based VM Backup 用のノードタスクを管理する方法 \(P. 49\)](#)」が更新されました。[ノードリスト] に、削除済み、および、サーバから検出できない、利用不可能なノードが表示されるようになりました。[ノードリスト] の [ポリシー] 列に、ポリシーの展開ステータスが表示されるようになりました。
- 「[ノードの更新 \(P. 58\)](#)」が更新されました。このトピックでは、既存の認証情報の使用または新しい認証情報の指定により、複数ノードを同時に更新する方法が説明されています。ノードを選択して、サーバに管理させることができます。
- 「[ノードグループの追加 \(P. 63\)](#)」が更新されました。このトピックでは「未割り当て」ノードグループが、「ポリシーがないノード」に、「グループ化解除済み」ノードグループが「グループがないノード」にそれぞれ置き換えられました。

- 「[今すぐバックアップを実行 \(P. 74\)](#)」が更新されました。このトピックでは、キュー内に待機中の別のバックアップジョブがあるときにサブミットしたバックアップジョブの優先度レベルについて説明しています。
- 「[使用済みブロックデータのみを含むフルディスクバックアップの実行 \(P. 83\)](#)」が追加されました。このトピックでは、フルディスクバックアップジョブをサブミットした後に使用済みブロックデータを取得する方法について説明します。
- 「[バックアップポリシーの作成 \(P. 87\)](#)」が更新されました。このトピックには、失敗および成功したカタログジョブの電子メールアラートが含まれるようになりました。このトピックにはまた、ジョブキュー内で待機しているバックアップジョブ、スキップされるバックアップジョブ、および別のジョブに置き換えられるバックアップジョブの電子メールアラートも含まれています。
- 「[バックアップの転送モードの定義 \(P. 103\)](#)」が追加されました。CA ARCserve Central Host-Based VM Backup で、Host-Based VM Backup を使用して実行する D2D バックアップジョブの転送モードを定義できるようになりました。
- 「[変更ブロックのトラッキングバックアップに失敗する \(P. 160\)](#)」が更新されました。バックアップジョブが失敗したときの、変更ブロックトラッキング (CBT) のリセットに関する説明を削除しました。CA ARCserve Central Host-Based VM Backup は、仮想マシン上で自動的に CBT を有効化できます。

Update 5

- [ノードグループの追加 \(P. 63\)](#)。このトピックが更新され、[グループ名] および [ノード名] のフィルタが含められました。
- [バックアップポリシーのノードの割り当てと割り当て解除 \(P. 94\)](#)。このトピックが更新され、[グループ名] および [ノード名] のフィルタが含められました。

Update 4

- CA ARCserve Central Host-Based VM Backup のサイレント インストール。サブトピック「サイレント インストール用製品コード」を削除し、ここに含めました。
- CA ARCserve Central Host-Based VM Backup のサイレント アンインストール。サブトピック「サイレント アンインストール用製品コード」を削除し、ここに含めました。
- [CA ARCserve Central Host-Based VM Backup ホーム画面の使用方法](#) (P. 47)。ナビゲーションバーから [リストア] を削除しました。
- 「[CA ARCserve Central Host-Based VM Backup 用のノードタスクの管理](#) (P. 49)」を追加しました。ノード管理について、シナリオベースのコンテンツと図を作成しました。
- 「[CA ARCserve Central Host-Based VM Backup 用のノードグループタスクの管理](#) (P. 62)」を追加しました。ノードグループ管理について、シナリオベースのコンテンツと図を作成しました。
- 「[仮想マシン環境のバックアップ](#) (P. 68)」を追加しました。ユーザ環境内のすべての仮想マシンのバックアップに関して、シナリオベースのコンテンツと図を作成しました。
- 「[バックアップジョブのプレフライトチェックの実行](#) (P. 69)」を追加しました。このトピックでは、[プレフライトチェック] (PFC) のサブミット方法について説明します。
- 「[プレフライトチェック項目のソリューション](#) (P. 71)」を追加しました。このトピックでは、PFC の実行時に受信可能なエラーおよび警告メッセージ、およびそれらを解決するソリューションについて説明します。
- 「[今すぐバックアップを実行](#) (P. 74)」を追加しました。タイトルを「バックアップジョブのサブミット」から「今すぐバックアップを実行」に変更しました。
- 「[ジョブステータス情報の表示](#) (P. 83)」が追加されました。このトピックでは、進行中のバックアップジョブについてリアルタイム情報を表示する方法について説明します。
- [Host-Based VM Backup モニタリングタスク](#) (P. 84)。CA ARCserve Central Host-Based VM Backup アプリケーションの更新済み画面をエミュレートするために、このトピックを更新しました。

- 「[CA ARCserve Central Host-Based VM Backup 用ポリシーの管理方法](#) (P. 86)」を追加しました。バックアップポリシーの作成、編集、割り当て、割り当て解除に関して、シナリオベースのコンテンツと図を作成しました。
- [仮想マシンのリストアおよび復旧](#) (P. 105)。画面上の [リストア] ボタンの新しい場所に関して、リストア関連のすべてのトピックを修正しました。

目次

第 1 章: CA ARCserve Central Host-Based VM Backup の概要	15
概要.....	15
CA ARCserve Central Host-Based VM Backup について	16
CA ARCserve Central Host-Based VM Backup の仕組み	17
CA ARCserve Central Applications マニュアル選択メニュー	18
第 2 章: CA ARCserve Central Host-Based VM Backup のインストールおよび設定	19
CA ARCserve Central Host-Based VM Backup をインストールする方法	19
インストール タスクの前提条件	21
CA ARCserve Central Host-Based VM Backup のインストール	24
CA ARCserve Central Host-Based VM Backup のサイレント インストール	26
CA ARCserve Central Host-Based VM Backup をアンインストールする方法.....	29
CA ARCserve Central Host-Based VM Backup のアンインストール	30
CA ARCserve Central Host-Based VM Backup のサイレント アンインストール.....	31
CA ARCserve D2D ノードを保護するように CA ARCserve Central Host-Based VM Backup を設定する方 法.....	33
CA ARCserve Central Protection Manager サーバの設定	34
ディスクバリエーションのスケジュールの設定	36
電子メールおよびアラート設定の指定	36
更新スケジュールの設定.....	38
ソーシャル ネットワーキングの環境設定	41
管理者アカウントの変更.....	42
第 3 章: CA ARCserve Central Host-Based VM Backup の使用	45
実稼働環境の設定方法.....	46
CA ARCserve Central Host-Based VM Backup ホーム画面の使用方法	47
CA ARCserve D2D ノードへのログイン.....	48
CA ARCserve Central Host-Based VM Backup 用のノードタスクを管理する方法.....	49
CA ARCserve Central Host-Based VM Backup からのノードのディスクバリエーション	52
ノードの追加.....	53
ノードの更新.....	58
ノードの削除.....	59

マージジョブ オプション	60
CA ARCserve Central Host-Based VM Backup 用のノードグループ タスクを管理する方法	62
ノードグループの追加	63
ノードグループの削除	65
ノードグループの変更	66
仮想マシン環境のバックアップ方法	68
バックアップジョブのプレフライトチェックの実行	69
今すぐバックアップを実行	74
アプリケーション レベルバックアップの実行	82
使用済みブロック データのみを含むフルディスク バックアップの実行	83
ジョブ ステータス情報の参照	83
CA ARCserve Central Host-Based VM Backup 用ポリシーの管理方法	86
バックアップ ポリシーの作成	87
バックアップ ポリシーの編集またはコピー	91
バックアップ ポリシーのノードの割り当てと割り当て解除	94
CA ARCserve Central Host-Based VM Backup ログの表示	96
特定ノードのアクティビティ ログ情報の表示	98
ナビゲーションバーへのリンクの追加	100
CA ARCserve Central Host-Based VM Backup と CA ARCserve Central Applications との統合	100
raw デバイス マッピング保護のための考慮事項	101
サーバの通信プロトコルの変更	102
バックアップの転送モードの定義	103

第 4 章: 仮想マシンのリストアおよび復旧 105

リストア方式	106
復旧ポイントからのリストア	107
復旧ポイントのマウントによるリストア	111
リストアするファイル/フォルダの検索を使用したデータのリストア	112
仮想マシン全体の復旧	115
リストアの考慮事項	118
アプリケーション レベル リストア	119
Exchange Server のデータのリストア	120
SQL Server のデータのリストア	126

第 5 章: CA ARCserve Central Host-Based VM Backup のトラブルシューティング 131

ノードの追加を試行すると、指定されたサーバにアクセスできないというメッセージが表示される	133
--	-----

空の Web ページが表示される、または、JavaScript エラーが発生する	136
CA ARCserve D2D ノードへのログイン時に Web ページが正しくロードされない	138
ページのロード問題のトラブルシューティング方法	140
CA ARCserve Central Applications にアクセスすると、文字化けがブラウザ ウィンドウ内に表示される	141
ノード更新時のアクセス拒否エラー発生	142
アプリケーションへのログイン時に証明書エラーが表示される	144
バックアップがスナップショット作成エラーで失敗する	145
VM の復旧が不明なエラーで失敗する	147
hotadd 転送モードを使用したバックアップおよび復旧操作でディスクがマウントできない	149
HOTADD または SAN 転送モードを使用してデータを復旧すると復旧に失敗する	149
オペレーティング システムが見つからないエラー	152
MAC アドレスの変更が VM 復旧後に保持されない	153
CA ARCserve D2D Web サービスが CA ARCserve D2D ノード上で失敗する	154
CA ARCserve Central Host-Based VM Backup がリモート ノード上の CA ARCserve D2D Web サービスと通信できない	157
CA ARCserve D2D Web サービスの実行が遅い	158
変更ブロックのトラッキングに失敗する	160
ESXi ライセンスのためにバックアップが失敗する	161
VM にスナップショットがあるためバックアップが失敗する	162
バックアップが失敗し、バックアッププロキシシステムのイベント ログにイベント 1530 がログ記録される	163
ホット追加転送モードを指定したのに NBD 転送モードでバックアップが完了する	164
増分バックアップ ジョブが検証バックアップ ジョブとして処理される	165
ブロックを識別できないため、バックアップ ジョブに失敗する	166
VMDK ファイルを開けない	167
ノード名を変更した後にノードがノード画面に表示されない	168
ポリシーを CA ARCserve D2D サーバに保存または割り当てる際に複数の接続エラーが発生する	169
ESX Server にアクセスできないために仮想マシンのバックアップが失敗する	170
Internet Explorer 8、9、Chrome で追加した新しいタブのリンクが正常に起動しない	171
Internet Explorer 8 および 9 で、新しいタブの追加リンク、RSS フィード、および ソーシャル ネットワーキング フィードバックが正常に起動しない	175
日本語キーボードを使用して [フィルタ] フィールドのワイルドカードとしてアスタリスクまたはアンダースコアを指定できない	176
仮想マシンの復旧で指定とは異なる転送モードが使用される	176

第 6 章: ベストプラクティスの適用 179

仮想マシンのベア メタル復旧の実行	179
ブートキットの作成	198
同時バックアップ数の制限の定義	202

VMVixMgr ログ ファイルに保持されるメッセージ容量を増加させる	203
CA ARCserve D2D バックアップ プロキシの保護	204
インストール処理のオペレーティング システムに対する影響	205
無効なファイル バージョン情報が含まれるバイナリ ファイル	207
埋め込みマニフェストを含まないバイナリ ファイル	208
マニフェストで管理者に必要な権限を持つバイナリ ファイル	209

付録 A: CA ARCserve D2D の操作手順 **211**

CA ARCserve D2D のインストール	211
バックアップ設定の管理	214
保護設定の指定	215
バックアップ スケジュールの指定	233
バックアップ拡張設定の指定	236
バックアップの実行前/後の設定の指定	241
環境設定の指定	243
アプリケーションのリストア	259
アプリケーションのリストア - MS Exchange Server	259
アプリケーションのリストア - MS SQL Server	268
復旧ポイントのコピー方法	274
前提条件の確認	276
復旧ポイントのコピー設定の指定	276
復旧ポイントのコピー	283
コピーされた復旧ポイントの確認	288

第 7 章: 用語集 **291**

索引 **293**

第 1 章: CA ARCserve Central Host-Based VM Backup の概要

このセクションには、以下のトピックが含まれています。

[概要](#) (P. 15)

[CA ARCserve Central Host-Based VM Backup について](#) (P. 16)

[CA ARCserve Central Host-Based VM Backup の仕組み](#) (P. 17)

[CA ARCserve Central Applications マニュアル選択メニュー](#) (P. 18)

概要

CA ARCserve Central Applications は、コア データ保護および管理テクノロジーと、併せて動作するターゲット アプリケーションのエコシステムとを組み合わせて、グローバル環境全体におけるデータの社内外での保護、コピー、移動、および変換を容易にします。

CA ARCserve Central Applications は使い易く、管理およびインストールも簡単に行うことができます。組織は、組織の情報に対する制御を自動化し、データのアクセス、可用性、セキュリティに関して、全体的なビジネス価値に基づいて適切な意思決定を下すことができます。

CA ARCserve Central Host-Based VM Backup について

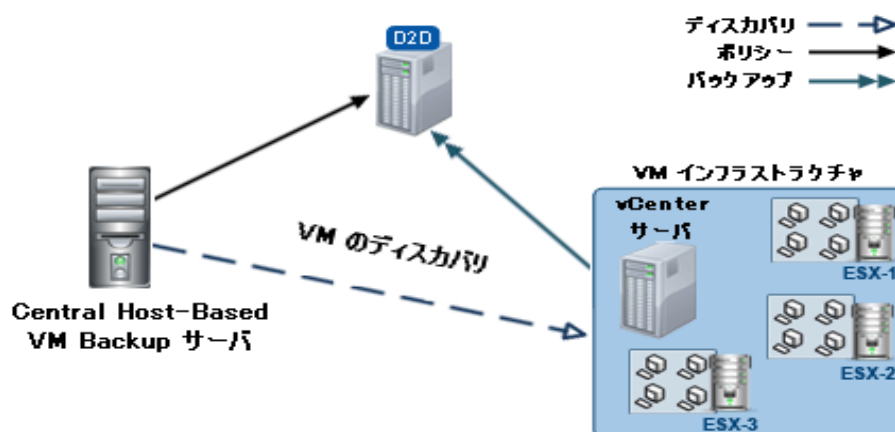
CA ARCserve Central Applications の 1 つが CA ARCserve Central Host-Based VM Backup アプリケーションです。このアプリケーションは、軽量のバックアップソリューションである CA ARCserve D2D と共に動作して、個別の仮想マシンにソフトウェアまたはエージェントをインストールする必要なしに、複数の仮想マシンを保護することができます。この機能によって、同一の物理サーバ上で複数のバックアップ処理を実行する際の悪影響を最小限にし、仮想マシンのバックアップからファイルレベル、アプリケーションレベルの復旧あるいはベアメタル復旧（BMR）を実行することができます。

CA ARCserve Central Host-Based VM Backup はスケーラビリティに優れ、必要に応じて仮想マシンを追加できます。そのために追加のライセンスを購入したり、環境内のすべての仮想マシンにソフトウェアをインストールしたりする必要はありません。

CA ARCserve Central Host-Based VM Backup の仕組み

CA ARCserve Central Host-Based VM Backup では、プロキシにインストールされた CA ARCserve D2D の 1 つのインスタンスを使用して、単一パスで ESX または vCenter Server 上で実行される仮想マシンを保護することができます。まず最初に以下のチェックリストを使用します。

1. 環境内でバックアッププロキシとして動作する 1 台のマシン（物理または仮想）に CA ARCserve D2D をインストールします。インストール手順については、「CA ARCserve D2D ユーザガイド」の「[CA ARCserve D2D のインストール](#) (P. 211)」を参照してください。プロキシが正しく設定されていることを確認します。
2. 管理するノードを追加します。ESX Server を指定すると、アプリケーションは、そこで実行中の仮想マシンで要件を満たすものを検出します。
3. バックアップポリシーを作成します。各ポリシーについて、CA ARCserve D2D をインストールするバックアッププロキシを指定します。
4. バックアップポリシーを各 VM に割り当てて、バックアッププロキシ上で実行される CA ARCserve D2D のシングルインスタンスですべての VM を保護できるようにします。
5. ノードグループを作成し、仮想マシン環境を管理しやすくします。たとえば、部門やインストールされたアプリケーションなどによってノードをグループ化し、設定されたポリシーを割り当てて、特定の部門に関連するノードまたは特定のアプリケーションを実行するノードが保護されるようにします。



CA ARCserve Central Applications マニュアル選択メニュー

CA ARCserve Central Applications ヘルプ システムに含まれているトピックは、PDF 形式の「ユーザ ガイド」でも提供されています。このガイドおよびヘルプ システムの最新の PDF バージョンは CA ARCserve Central Applications マニュアル選択メニュー

(<https://support.ca.com/cadocs/0/CA%20ARCserve%20Central%20Applications%20Enterprise%20Support%2016%200-ENU/Bookshelf.html>)からアクセスできます。

CA ARCserve Central Applications リリース ノートには、この製品をインストールする前に理解しておく必要があるさまざまな情報が含まれています。たとえば、システム要件、オペレーティング システムのサポート、アプリケーション回復サポートなどがあります。さらに、CA ARCserve Central Applications を使用する前に確認する必要がある既知の問題のリストが含まれています。リリース ノートの最新バージョンは CA ARCserve Central Applications マニュアル選択メニュー

(<https://support.ca.com/cadocs/0/CA%20ARCserve%20Central%20Applications%20Enterprise%20Support%2016%200-ENU/Bookshelf.html>)から入手できます。

第 2 章: CA ARCserve Central Host-Based VM Backup のインストールおよび設定

このセクションには、以下のトピックが含まれています。

[CA ARCserve Central Host-Based VM Backup をインストールする方法 \(P. 19\)](#)

[CA ARCserve Central Host-Based VM Backup をアンインストールする方法 \(P. 29\)](#)

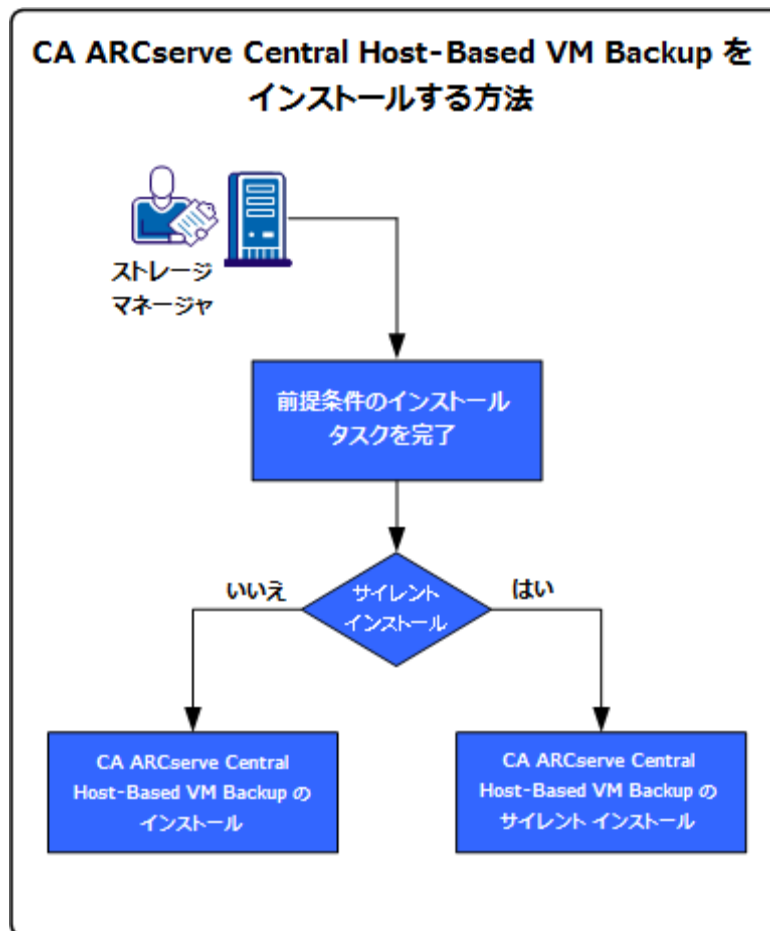
[CA ARCserve D2D ノードを保護するように CA ARCserve Central Host-Based VM Backup を設定する方法 \(P. 33\)](#)

CA ARCserve Central Host-Based VM Backup をインストールする方法

このシナリオでは、以下の方法を使用したストレージマネージャによる CA ARCserve Central Host-Based VM Backup のインストールについて説明します。

- 標準インストール -- この方法は、アプリケーションのインストールにインストール ウィザードを使用します。
- サイレントインストール -- この方法は、Windows コマンドラインを使用して無人インストールを実行します。

以下の図は、アプリケーションをインストールする方法を示しています。



以下の表は、CA ARCserve Central Host-Based VM Backup をインストールするタスクが説明されているトピックを示しています。

タスク	参照トピック
アプリケーションをインストールする前に、インストールの前提条件となるタスクを実行し、インストール考慮事項を確認します。	インストールタスクの前提条件 (P. 21)
インストールウィザードを使用して、標準インストールを実行します。	CA ARCserve Central Host-Based VM Backup のインストール (P. 24)
Windows コマンドラインを使用して、サイレントインストールを実行します。	CA ARCserve Central Host-Based VM Backup のサイレントインストール (P. 26)

アプリケーションのインストール後の Windows OS コンポーネントの更新については、「CA ARCserve Central Host-Based VM Backup ユーザ ガイド」の「ベストプラクティスの適用」セクションを参照してください。

インストール タスクの前提条件

アプリケーションをインストールする前に、以下の前提条件タスクを完了し、インストール考慮事項を確認してください。

前提条件タスク

- 「リリース ノート」を確認します。「リリース ノート」には、システム要件の説明、サポートされるオペレーティング システム、およびアプリケーションのこのリリースで存在する既存の問題のリストが含まれます。
- お使いのシステムがアプリケーションをインストールするためのハードウェア要件とソフトウェア要件を満たしていることを確認します。
- 変更されたブロック トラッキングを有効にでき、保護している仮想マシン上で有効になっていることを確認します。

注: 変更されたブロック トラッキングの詳細については、VMware Web サイト上の以下の Knowledge Base ドキュメントを参照してください。

<http://kb.vmware.com/kb/1020128> (<http://kb.vmware.com/kb/1020128>)

- 使用している Windows アカウントが、CA ARCserve Central Host-Based VM Backup をインストールするコンピュータに対して、管理者権限またはソフトウェアをインストールするのに必要な管理者相当権限を持っていることを確認します。
- vCenter Server または ESX Server アカウントが VMware および Windows の管理者権限を持っていることを確認します。VDDK の処理が正常に完了するように、vCenter Server システムまたは ESX Server システムでアカウントに Global License の役割を割り当てます。

- アプリケーションをインストールするコンピュータのユーザ名およびパスワードを所有していることを確認します。
- 実稼働環境内の仮想マシンを保護するバックアップ プロキシシステム上に CA ARCserve D2D がインストールされていることを確認します。
- VM バックアップからの詳細リストア機能を使用する場合は、以下の項目を確認します。
 - 管理者権限を持った任意のユーザからの管理者認証情報が、仮想マシンゲスト オペレーティング システムにログインするために提供されています。
 - ユーザアカウント制御 (UAC) が無効になっています。

インストールに関する考慮事項

CA ARCserve Central Host-Based VM Backup をインストールする前に、以下の考慮事項を確認します。

- CA ARCserve Central Applications インストールパッケージは、CA ARCserve Central Applications Server という名前のモジュールをインストールします。CA ARCserve Central Applications Server は、すべての CA ARCserve Central Applications に共通のモジュールです。このモジュールには、CA ARCserve Central Applications が互いに通信するために使用される Web サービス、バイナリ、および環境設定が含まれています。
CA ARCserve Central Applications をインストールすると、インストールパッケージは製品コンポーネントをインストールする前に CA ARCserve Central Applications Server モジュールをインストールします。CA ARCserve Central Applications にパッチを適用する必要がある場合、パッチは製品コンポーネントを更新する前にモジュールを更新します。
- CA ARCserve Central Applications のインストール後、ファイル レベル バックアップ サポート用に、VMware VIX API バージョン 1.10.1 以降をバックアップ プロキシシステム上にダウンロードしインストールします。
- CA ARCserve Central Host-Based VM Backup のインストール後、同じコンピュータ上に VMware VIX API バージョン 1.10.1 以降をダウンロードしインストールします。これは、後でプレフライトチェックに使用されます。
- CA ARCserve D2D は、VMware Virtual Disk Development Kit (VDDK) を CA ARCserve D2D をインストールするすべてのコンピュータにインストールします。バックアップ プロキシシステムに VDDK をダウンロードしてインストールする必要はありません。

VDDK の新しいバージョンを使用する場合は、VDDK をダウンロードおよびインストールし、HKEY_LOCAL_MACHINE¥SOFTWARE¥CA¥CA ARCSERVE D2D にある VDDKDirectory レジストリの値を、新しいバージョンの VDDK がインストールされているフォルダに変更します。

VDDK のデフォルトの場所は以下のとおりです。

- **X64 オペレーティング システム**

c:¥Program Files (x86)¥VMware¥VMware Virtual Disk Development Kit

注: VDDK64.zip ファイルを VDDK インストールディレクトリから VDDK64 フォルダに解凍します。

例: c:¥Program Files (x86)¥VMware¥VMware Virtual Disk Development Kit¥VDDK64

- **X86 オペレーティング システム**

c:¥Program Files¥VMware¥VMware Virtual Disk Development Kit

- 特定のリストア処理を実行するには、CA ARCserve D2D のローカルインストールが必要となります。詳細については、「[リストアに関する考慮事項](#) (P. 118)」を参照してください。CA ARCserve D2D のライセンスは CA ARCserve Central Host-Based VM Backup に含まれています。製品インストールファイルを取得するには、CA サポートサイトにアクセスします。
- raw デバイス マッピングに対して仮想互換性はサポートされていますが、物理互換性はサポートされていません。

CA ARCserve Central Host-Based VM Backup のインストール

インストール ウィザードを使用すると、示される手順に従って CA ARCserve Central Applications をインストールすることができます。

注: アプリケーションをインストールする前に、「リリース ノート」を参照し、「必須タスク」に説明されているタスクがすべて完了していることを確認してください。

CA ARCserve Central Host-Based VM Backup をインストールする方法

1. アプリケーションをインストールするコンピュータに CA ARCserve Central Applications インストールパッケージをダウンロードし、次に、セットアップファイルをダブルクリックします。

インストールパッケージにより、そのコンテンツがコンピュータへ展開されます。次に、[前提条件コンポーネント] ダイアログ ボックスが表示されます。

2. [前提条件コンポーネント] ダイアログ ボックスで [インストール] をクリックします。

注: [前提条件コンポーネント] ダイアログ ボックスは、必要な前提条件コンポーネントがコンピュータにインストールされていることを検出できなかった場合にのみ表示されます。

セットアップで前提条件コンポーネントをインストールした後、[使用許諾契約] ダイアログ ボックスが表示されます。

3. [使用許諾契約] ダイアログ ボックスで必要なオプションを入力して、[次へ] をクリックします。

[環境設定] ダイアログ ボックスが表示されます。

4. [環境設定] ダイアログ ボックスで、以下を入力します。

- **コンポーネント** -- インストールするアプリケーションを指定します。

注: スイートインストールパッケージを使用してこのアプリケーションをインストールしている場合、複数のアプリケーションをインストールできます。

- **場所** -- デフォルトのインストール場所を使用するか、あるいは [参照] をクリックして別のインストール場所を指定します。デフォルトの場所は以下のとおりです。

C:\Program Files\CA\ARCserve Central Applications

- **ディスク情報** -- ハードドライブに、アプリケーションをインストールするために十分なディスク空き容量があることを確認します。
- **Windows 管理者の名前** -- 以下の構文を使用して、Windows 管理者アカウントのユーザ名を指定します。

<ドメイン名>\<ユーザ名>

- **パスワード** -- ユーザアカウントのパスワードを指定します。
- **ポート番号の選択** -- Web ベースのユーザ インターフェースとの通信に使用するポート番号を指定します。ベストプラクティスとして、デフォルトポート番号を使用することをお勧めします。デフォルトポート番号は以下のとおりです。

8015

注: 別のポート番号を指定する場合、利用可能なポート番号は 1024 ~ 65535 です。別のポート番号を指定する前に、指定するポート番号が未使用で利用可能であることを確認してください。セットアップでは、利用可能でないポートを使用して、アプリケーションをインストールすることはできません。

- **Web 通信に https を使用する** -- データ転送に HTTPS 通信を使用するように指定します。このオプションは、デフォルトでは選択されていません。

注: 安全な HTTPS 通信は、HTTP 通信より高いレベルのセキュリティを提供します。ネットワーク内で機密情報を転送する場合は、HTTPS 通信プロトコルが推奨されます。

- **Windows ファイアウォールの例外として CA ARCserve Central Applications サービス/プログラムを登録することを許可する** -- このオプションの横のチェック ボックスが選択されていることを確認します。CA ARCserve Central Applications の設定や管理をリモート コンピュータから実行する場合、ファイアウォールの例外に登録する必要があります。

注: ローカルユーザの場合、ファイアウォールの例外に登録する必要はありません。

[次へ] をクリックします。

インストールプロセスの完了後、[インストール レポート] が開きます。

5. [インストール レポート] ダイアログ ボックスにはインストール サマリが表示されます。アプリケーションの更新をすぐに確認する場合は、[更新の確認] をクリックし、次に [完了] をクリックします。

アプリケーションがインストールされます。

CA ARCserve Central Host-Based VM Backup のサイレント インストール

CA ARCserve Central Applications では、CA ARCserve Central Host-Based VM Backup のサイレント インストールを実行できます。サイレント インストールでは、ユーザによる操作が不要になります。以下の手順は、Windows コマンドラインを使用してアプリケーションをインストールする方法を説明しています。

CA ARCserve Central Host-Based VM Backup をサイレント インストールする方法

1. サイレント インストール処理を開始するコンピュータ上で Windows コマンドラインを開きます。
2. CA ARCserve Central Applications の自己解凍インストールパッケージを対象のコンピュータにダウンロードします。

以下のコマンドライン構文を使用して、サイレント インストール処理を開始します。

```
"CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<INSTALLDIR>  
-Port:<PORT> -U:<UserName> -P:<Password> -Products:<ProductList>"
```

使用法:

s

実行ファイルパッケージをサイレント モードで実行します。

v

追加のコマンドライン オプションを指定します。

q

アプリケーションをサイレント モードでインストールします。

-Path:<INSTALLDIR>

(オプション) インストールパスを指定します。

例:

```
-Path:"%C:%Program Files%CA%ARCserve Central Applications%"
```

注: INSTALLDIR の値にスペースが含まれる場合は、パスを円記号と引用符で囲みます。また、パスの末尾を円記号にすることはできません。

-Port:<PORT>

(オプション) 通信用のポート番号を指定します。

例:

```
-Port:8015
```

-U:<UserName>

アプリケーションのインストールおよび起動に使用するユーザ名を指定します。

注: このユーザは、管理者アカウントか、または管理者権限のあるアカウントである必要があります。

-P:<Password>

ユーザのパスワードを指定します。

-Products:<ProductList>

(オプション) CA ARCserve Central Applications のサイレントインストールを指定します。この引数に値を指定しない場合、サイレントインストール処理は CA ARCserve Central Applications のすべてのコンポーネントをインストールします。

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

CA ARCserve Central Applications すべて

ALL

注: 以下の例は、それぞれ 1 つ、2 つ、3 つ、またはすべての CA ARCserve Central Applications をサイレントインストールするために必要な構文です。

-Products:CMX64

-Products:CMX64,VCMX64

-Products:CMX64,VCMX64,REPORTINGX64

-Products:ALL

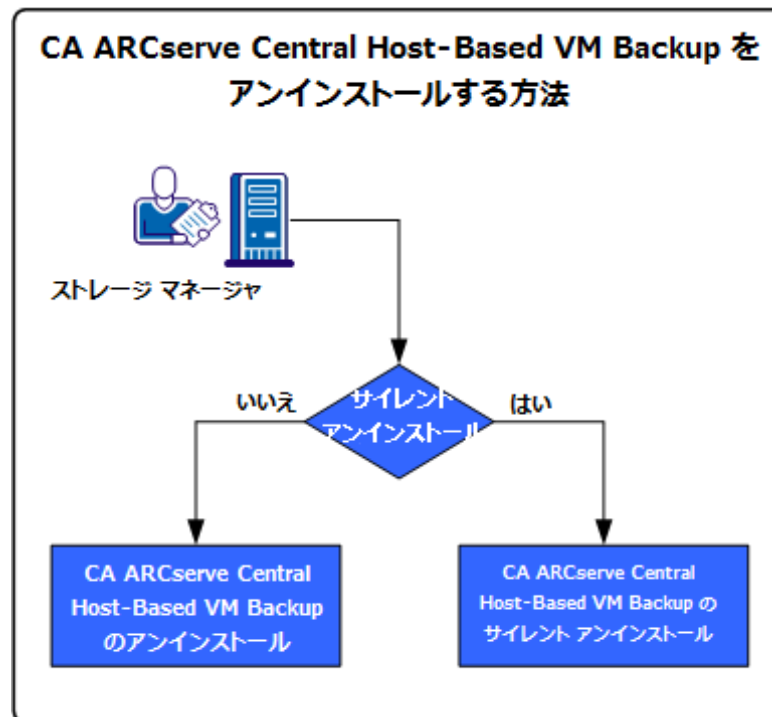
アプリケーションがサイレントインストールされます。

CA ARCserve Central Host-Based VM Backup をアンインストールする方法

CA ARCserve Central Host-Based VM Backup は以下の方法を使用してアンインストールできます。

- 標準アンインストール -- この方法は、Windows コントロールパネルを使用してアプリケーションをアンインストールします。
- サイレントアンインストール -- この方法は、Windows コマンドラインを使用して無人アンインストールを実行します。

以下の図は、アプリケーションをアンインストールする方法を示しています。



タスク

Windows コントロールパネルを使用して、標準的なアンインストールを実行します。

Windows コマンドラインを使用して、サイレントアンインストールを実行します。

参照トピック

[CA ARCserve Central Host-Based VM Backup のアンインストール](#) (P. 30)

[CA ARCserve Central Host-Based VM Backup のサイレントアンインストール](#) (P. 31)

アプリケーションのアンインストール後の Windows OS コンポーネントの更新については、「CA ARCserve Central Host-Based VM Backup ユーザ ガイド」の「ベストプラクティスの適用」セクションを参照してください。

CA ARCserve Central Host-Based VM Backup のアンインストール

Windows コントロールパネルの [プログラムと機能] を使用してアプリケーションをアンインストールできます。

CA ARCserve Central Host-Based VM Backup をアンインストールする方法

1. Windows の [スタート] メニューから、[スタート] をクリックして [コントロールパネル] をクリックします。

Windows の [コントロールパネル] が開きます。

2. Windows の [コントロールパネル] から、[表示] の横のドロップダウンリストをクリックし、次に [大きいアイコン] または [小さいアイコン] をクリックします。

Windows の [コントロールパネル] アプリケーションのアイコンがグリッドレイアウトで表示されます。

3. [プログラムと機能] をクリックします。

[プログラムのアンインストールまたは変更] ウィンドウが表示されます。

4. アンインストールするアプリケーションを検索してクリックします。

アプリケーションを右クリックし、コンテキストメニューから [アンインストール] を選択します。

画面の指示に従い、アプリケーションをアンインストールします。

アプリケーションがアンインストールされます。

CA ARCserve Central Host-Based VM Backup のサイレントアンインストール

CA ARCserve Central Applications では、CA ARCserve Central Host-Based VM Backup のサイレントアンインストールを実行できます。サイレントアンインストールでは、ユーザによる操作が不要になります。以下の手順は、Windows コマンドラインを使用してアプリケーションをアンインストールする方法を説明しています。

CA ARCserve Central Host-Based VM Backup をサイレントアンインストールする方法

1. アプリケーションをアンインストールするコンピュータにログインします。

注: 管理者アカウント、または管理者権限のあるアカウントを使用してログインする必要があります。

2. Windows コマンドラインを開き、以下のコマンドを実行してサイレントアンインストール処理を開始します。

```
<INSTALLDIR>%Setup%uninstall.exe /q /p <ProductCode>
```

または

```
<INSTALLDIR>%Setup%uninstall.exe /q /ALL
```

例: 以下の構文で、CA ARCserve Central Host-Based VM Backup のサイレントアンインストールを実行できます。

```
"%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}
```

使用法:

<INSTALLDIR>

アプリケーションがインストールされているディレクトリを指定します。

注: コンピュータのオペレーティングシステムのアーキテクチャに対応する構文を実行してください。

<ProductCode>

サイレント アンインストールするアプリケーションを指定します。

注: サイレント アンインストールでは、1 つ以上の CA ARCserve Central Applications をアンインストールできます。 CA ARCserve Central Applications のサイレント アンインストールを行うには、以下の製品コードを使用します。

CA ARCserve Central Host-Based VM Backup

{CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

CA ARCserve Central Protection Manager

{CAED05FE-D895-4FD5-B964-001928BD2D62}

CA ARCserve Central Reporting

{CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

CA ARCserve Central Virtual Standby

{CAED4835-964B-484B-A395-E2DF12E6F73D}

アプリケーションがサイレント アンインストールされます。

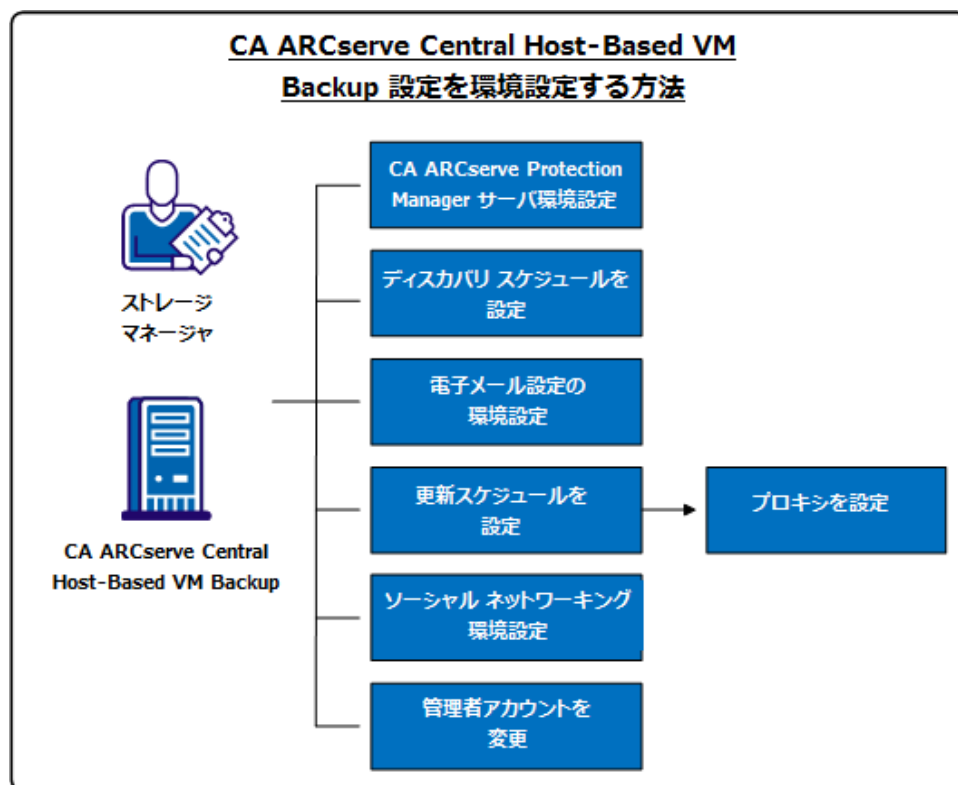
CA ARCserve D2D ノードを保護するように CA ARCserve Central Host-Based VM Backup を設定する方法

電子メールアラートおよびスケジュールの環境設定、および CA ARCserve Central Host-Based VM Backup インストールの更新方法を指定できます。

ユーザが環境設定を指定する前に、バックアップジョブを実行するサーバに CA ARCserve D2D をインストールする必要があります。このピア（すなわちプロキシサーバ）は、必要に応じて、単一または複数のコンピュータである場合があります。手順については、「CA ARCserve D2D ユーザガイド」の「[CA ARCserve D2D のインストール \(P. 211\)](#)」を参照してください。

同じあるいは別のコンピュータに CA ARCserve Central Host-Based VM Backup をインストールできます。インストール手順は、ウィザードで簡単に行うことができます。詳細については、「CA ARCserve Central Host-Based VM Backup のインストール」を参照してください。

以下の図は、アプリケーションに設定できる環境設定のタイプを示しています。



このシナリオでは、以下のトピックについて説明します。

- [CA ARCserve Central Protection Manager サーバの設定](#) (P. 34)
- [ディスカバリ スケジュールの設定](#) (P. 36)
- [電子メール設定の環境設定](#) (P. 36)
- [更新スケジュールの設定](#) (P. 38)
 - [プロキシ設定の環境設定](#) (P. 39)
- [ソーシャル ネットワーキングの環境設定](#) (P. 41)
- [管理者アカウントの変更](#) (P. 42)

CA ARCserve Central Protection Manager サーバの設定

CA ARCserve Central Protection Manager サーバの設定では、CA ARCserve Central Host-Based VM Backup の現在の設定を CA ARCserve Central Protection Manager サーバ設定に変更することができます。設定を指定すると、Host-Based VM Backup 検出ノード用電子メールアラート情報を CA ARCserve Central Reporting から表示できます。

次の手順に従ってください:

1. CA ARCserve Central Host-Based VM Backup サーバにログインし、ナビゲーションバーの [環境設定] をクリックします。
[環境設定] 画面が表示されます。
2. [環境設定] パネルから、[CA ARCserve Central Protection Manager 環境設定] をクリックします。
3. 以下のフィールドに入力します。
 - **CA ARCserve Central Protection Manager サーバ**
注: CA ARCserve Central Protection Manager および CA ARCserve Central Host-Based VM Backup がインストールされている場合、以下のフィールドにはデフォルトでローカルの CA ARCserve Central Protection Manager サーバが設定されます。CA ARCserve Central Protection Manager がインストールされていない場合、フィールドは空白のままになり、手動での設定が必要です。CA ARCserve Central Reporting から検出されたノードのアラート情報を表示できます。

- **マシン名** -- CA ARCserve Central Protection Manager がインストールされているコンピュータのホスト名。
- **ユーザ名** -- CA ARCserve Central Protection Manager アプリケーションがインストールされているコンピュータにログインするために必要なユーザ名。
- **パスワード** -- ユーザのパスワード。
- **ポート** -- CA ARCserve Central Protection Manager Web サービスと通信するために使用するポート番号。
- **HTTPS** -- このオプションは、CA ARCserve Central Protection Manager サーバで設定されている接続に基づいて、オンまたはオフになります。
- **ポートとプロトコルの自動検出** -- Protection Manager データベースの CA ARCserve Central Protection Manager ポートおよびプロトコルを取得し、前述のフィールドにロードします。

注: CA ARCserve Central Protection Manager サーバのリモートレジストリ アクセスが許可される場合のみ、このオプションは有効です。

リモート レジストリが許可されているかどうか確認するには、以下の手順に従います。

1. CA ARCserve Central Protection Manager がインストールされている CA ARCserve Central Protection Manager サーバに移動します。
2. services.msc に移動し、「Remote Registry」サービスが開始されていることを確認します。
3. [自動] に設定します。

- **テスト** -- CA ARCserve Central Protection Manager 用のアクセス情報が正しいことを確認します。
4. [保存] をクリックします。

ディスクバリ スケジュールの設定

ノードに対してディスクバリのスケジュールを設定し、予定された時間に繰り返されるようにすることができます。デフォルトでは、ディスクバリの環境設定は無効になっています。この環境設定を有効にするには、[有効] オプションをクリックし、ディスクバリが開始される時刻と繰り返しの方法を指定します。ディスクバリ スケジュールの設定には以下のパラメータを指定できます。

- **指定の日数ごと** -- 指定された日数ごとにこの方法を繰り返します。
(デフォルト)
- **指定の曜日ごと** -- 指定した 1 つまたは複数の曜日にこの方法を繰り返します。月曜日、火曜日、水曜日、木曜日、および金曜日がデフォルトの曜日です。
- **月の指定の日付ごと** -- その月の指定された日付にこの方法を繰り返します。1 は月の指定の日付のデフォルト オプションです。

ノードディスクバリのスケジュールをセットアップする際、[vCenter/ESX ホストリスト] が表示されます。

電子メールおよびアラート設定の指定

アプリケーションで使用するために電子メールとアラート設定を指定し、指定条件でアラートを自動送信することができます。

次の手順に従ってください:

1. アプリケーションにログインします。
ホーム画面上のナビゲーションバーから [環境設定] をクリックして、[環境設定] 画面を開きます。
2. [環境設定] パネルから、[電子メールとアラートの環境設定] をクリックし、[電子メールとアラートの環境設定] オプションを開きます。

3. 以下のフィールドに入力します。
 - **サービス** -- 電子メールサービスの種類をドロップダウンから指定します。（[Google メール]、[Yahoo メール]、[Live メール]、[その他]）
 - **メール サーバ** -- CA ARCserve Central Applications 電子メールの送信に使用される SMTP サーバのホスト名を指定します。
 - **認証が必要** -- 指定したメールサーバで認証が必要な場合は、このオプションを選択します。アカウント名とパスワードは必須です。
 - **件名** -- デフォルトの電子メールの件名を指定します。
 - **送信者** -- 電子メールが送信される電子メールアドレスを指定します。
 - **受信者** -- 電子メールの送信先アドレスを指定します。複数の場合はセミコロン (;) で区切ります。
 - **SSL を使用** -- 指定したメールサーバでセキュアな接続 (SSL) が必要な場合、このオプションを選択します、
 - **STARTTLS の送信** -- 指定したメールサーバで STARTTLS コマンドが必要な場合は、このオプションを選択します。
 - **HTML 形式を使用** -- HTML 形式で電子メールメッセージを送信します。（デフォルトで選択されています）
 - **プロキシ設定を有効にする** -- プロキシサーバがある場合は、このオプションを選択してプロキシサーバ設定を指定します。
4. [テスト電子メール] をクリックして、メールの環境設定が正しいことを確認します。
5. (オプション) [電子メールアラートの送信] セクションから、[検出されたノード] をクリックし、新しいノードが検出された場合にアプリケーションに電子メールアラートを送信させることができます。
6. [保存] をクリックします。

注: [リセット] をクリックすると、保存済みの値に戻ります。[削除] をクリックすると、保存した設定が削除されます。電子メールとアラートの設定を削除すると、電子メールアラートメッセージを受信しなくなります。

電子メール環境設定が適用されます。

更新スケジュールの設定

CA サーバまたはローカルのソフトウェア ステージング サーバから自動的に製品の更新をダウンロードするスケジュールを設定できます。

次の手順に従ってください:

1. アプリケーションにログインします。
2. ナビゲーションバーの [環境設定] をクリックして、[環境設定] 画面を開きます。
3. [環境設定] パネルから、[更新環境設定] をクリックします。
更新の環境設定オプションが表示されます。
4. ダウンロードサーバを選択します。
 - **CA サーバ** -- [プロキシ設定] をクリックして以下のオプションを設定します。
 - **ブラウザのプロキシ設定を使用する** -- ブラウザのプロキシ設定に提供された認証情報を使用します。
注: [ブラウザのプロキシ設定を使用する] オプションは、Internet Explorer と Chrome に影響します。
 - **プロキシ設定の環境設定** -- プロキシサーバの IP アドレスまたはホスト名、およびポート番号を指定します。指定したサーバで認証が必要な場合、[プロキシサーバには認証が必要です] オプションをクリックし、認証情報を指定します。
[OK] をクリックして、更新環境設定に戻ります。
 - **ステージングサーバ** -- このオプションを選択する場合は、[サーバの追加] をクリックして、ステージングサーバをリストに追加します。ホスト名とポート番号を入力して、[OK] をクリックします。
複数のステージングサーバを指定した場合、アプリケーションではリストの最初のサーバを使用しようとします。接続に成功した場合、リスト内の残りのサーバはステージングに使用されません。
5. (オプション) [接続テスト] をクリックして、サーバ接続を確認し、テストが完了するまで待機します。

6. (オプション) [更新の自動確認] をクリックし、スケジュールを指定します。日単位または週単位でスケジュールを指定できます。

[保存] をクリックして更新環境設定を適用します。

プロキシ設定の環境設定

CA ARCserve Central Applications では、ダウンロード可能な更新を確認するために CA サポートとの通信に使用するプロキシサーバを指定できます。この機能を有効にするには、CA ARCserve Central Applications サーバに代わって通信するプロキシサーバを指定します。

次の手順に従ってください:

1. アプリケーションにログインし、ナビゲーションバーの [環境設定] をクリックします。
環境設定オプションが表示されます。
2. [更新環境設定] をクリックします。
更新の環境設定オプションが表示されます。
3. [プロキシ設定] をクリックします。
[プロキシ設定] ダイアログ ボックスが表示されます。

4. 以下のいずれかのオプションをクリックします。

- **ブラウザのプロキシ設定を使用する** -- 更新情報を取得するための CA Technologies サーバとの通信で、ブラウザに適用されているのと同じプロキシ設定を検出して使用します。

注: この動作は Internet Explorer および Chrome ブラウザにのみ適用されます。

- **プロキシを設定する** -- 更新をチェックするための CA サポートとの通信で、アプリケーションが使用する代替サーバを定義します。代替サーバ (プロキシ) を使用すると、セキュリティの強化、パフォーマンスの向上、管理制御などに役立ちます。

以下のフィールドに入力します。

- **プロキシサーバ** -- プロキシサーバのホスト名または IP アドレスを指定します。
- **ポート** -- CA サポート Web サイトと通信するためにプロキシサーバが使用するポート番号を指定します。
- **(オプション) プロキシサーバには認証が必要です** -- プロキシサーバ用のログイン認証情報が CA ARCserve Central Applications サーバ用の認証情報と同じでない場合は、[プロキシサーバには認証が必要です] チェック ボックスをオンにし、プロキシサーバへのログインに必要とされるユーザ名およびパスワードを指定します。

注: ユーザ名を指定する際は、「<ドメイン名>/<ユーザ名>」の形式を使用してください。

[OK] をクリックします。

プロキシ設定が指定されました。

注: CA ARCserve Central Host-Based VM Backup がノードにポリシーを展開でき CA ARCserve D2D ノードを保護できるようにするには、Host-Based VM Backup サーバおよびプロキシサーバがそれらのホスト名を使用して、互いに通信できることを確認します。以下の操作を行ってください。

1. CA ARCserve Central Host-Based VM Backup サーバから、サーバのホスト名を使用してプロキシサーバに ping を実行します。
2. プロキシサーバから、サーバのホスト名を使用して CA ARCserve Central Host-Based VM Backup サーバに ping を実行します。

ソーシャル ネットワーキングの環境設定

CA ARCserve Central Applications では、各アプリケーションを管理するのに役立つソーシャル ネットワーキング ツールを管理することができます。ニュース フィードの生成、よく使用されるソーシャル ネットワーキング Web サイトへのリンク指定、ビデオ ソース Web サイトの選択を行うことができます。

次の手順に従ってください:

1. アプリケーションにログインします。
ホーム画面上のナビゲーション バーから [環境設定] をクリックして、[環境設定] 画面を開きます。
2. [環境設定] パネルから [プリファレンス環境設定] をクリックし、[環境設定] オプションを開きます。

ニュース フィード

エキスパート アドバイス センターからの最新のニュースおよび製品情報を表示します

ソーシャル ネットワーキング

Facebook および Twitter へのリンクをメイン ページに表示

ビデオ

CA サポート ビデオの使用 YouTube ビデオの使用

3. 必要なオプションを指定します。
 - ニュース フィード -- アプリケーションに、CA ARCserve Central Applications および CA ARCserve D2D に関連するニュースおよび製品情報に対する RSS フィードを表示させます（[エキスパート アドバイスセンター] から）。このフィードはホーム画面に表示されます。
 - ソーシャル ネットワーキング -- アプリケーションのホーム画面に、ツイッターおよび Facebook へのアイコンを表示させ、CA ARCserve Central Applications および CA ARCserve D2D に関連するソーシャル ネットワーキング Web サイトにアクセスできるようにします。
 - ビデオ -- CA ARCserve Central Applications および CA ARCserve D2D 製品を表示するためにビデオの種類を選択します。（デフォルトのビデオは [YouTube ビデオの使用] です。）

[保存] をクリックします。

[ソーシャル ネットワーキング] オプションが適用されます。
4. ナビゲーションバーから [ホーム] をクリックします。

ホーム画面が表示されます。

5. ブラウザ画面を更新します。

[ソーシャル ネットワーキング] オプションが適用されます。

管理者アカウントの変更

CA ARCserve Central Applications では、アプリケーションをインストールした後、管理者アカウントのユーザ名、パスワード、またはその両方を変更できます。この管理者アカウントは、ログイン画面で、デフォルトの表示ユーザ名としてのみ使用されます。

注: 指定するユーザ名は、Windows 管理者アカウントか、Windows 管理者権限のあるアカウントである必要があります。

次の手順に従ってください:

1. アプリケーションにログインし、ナビゲーションバーの [環境設定] をクリックします。

環境設定オプションが表示されます。

2. [管理者アカウント] をクリックします

3. 管理者アカウント設定が表示されます。
4. 必要に応じて、以下のフィールドを更新します。
 - ユーザ名
 - パスワード[保存] をクリックします。

管理者アカウントが変更されます。

第 3 章: CA ARCserve Central Host-Based VM Backup の使用

このセクションには、以下のトピックが含まれています。

[実稼働環境の設定方法 \(P. 46\)](#)

[CA ARCserve Central Host-Based VM Backup ホーム画面の使用法 \(P. 47\)](#)

[CA ARCserve D2D ノードへのログイン \(P. 48\)](#)

[CA ARCserve Central Host-Based VM Backup 用のノードタスクを管理する方法 \(P. 49\)](#)

[CA ARCserve Central Host-Based VM Backup 用のノードグループタスクを管理する方法 \(P. 62\)](#)

[仮想マシン環境のバックアップ方法 \(P. 68\)](#)

[CA ARCserve Central Host-Based VM Backup 用ポリシーの管理方法 \(P. 86\)](#)

[CA ARCserve Central Host-Based VM Backup ログの表示 \(P. 96\)](#)

[特定ノードのアクティビティログ情報の表示 \(P. 98\)](#)

[ナビゲーションバーへのリンクの追加 \(P. 100\)](#)

[CA ARCserve Central Host-Based VM Backup と CA ARCserve Central Applications との統合 \(P. 100\)](#)

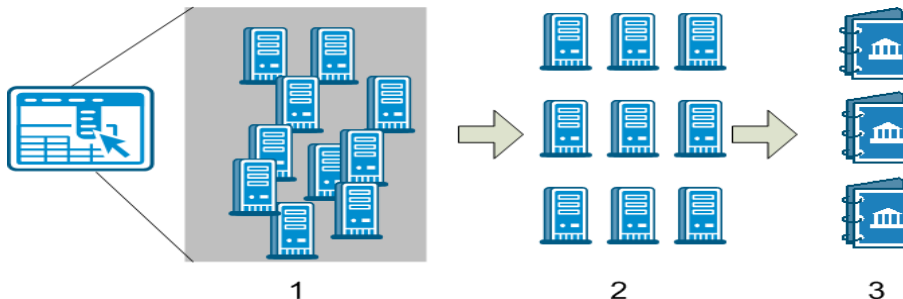
[raw デバイスマッピング保護のための考慮事項 \(P. 101\)](#)

[サーバの通信プロトコルの変更 \(P. 102\)](#)

[バックアップの転送モードの定義 \(P. 103\)](#)

実稼働環境の設定方法

仮想マシン環境を保護するには、以下に示すいくつかの基本アクティビティが必要です。



1. CA ARCserve Central Host-Based VM Backup にノードを追加します。ESX Server または vCenter Server によってホストされるすべての仮想マシンをインポートできます。
2. ノードをグループ化して、管理が容易になるようにします。たとえば、部門別またはインストールされたアプリケーション別などでノードをグループ化できます。
3. バックアップポリシーを作成してノードに割り当てます。すべてのノードは、設定したポリシーに基づいてバックアップされます。

CA ARCserve Central Host-Based VM Backup ホーム画面の使用法

CA ARCserve Central Host-Based VM Backup を起動すると、Web ブラウザでホーム画面が開きます。ホーム画面から、以下のタスクを実行できます。

- **左側ナビゲーション：**
 - **ノード** -- [ノード] 画面では、ノードグループ、インストール済みのアプリケーション、および割り当てられた vSphere ポリシーに基づいて仮想マシン環境を表示できます。
 - **ポリシー** -- [vSphere ポリシー] 画面では、環境内のすべてのノードに対してバックアップポリシーの作成、編集、および割り当てを行うことができます。
 - **環境設定** -- [環境設定] 画面では、電子メールアラートおよび自動更新スケジュールを指定できます。
 - **ログの表示** -- [ログの表示] 画面では、特定の問題（情報、エラー、警告など）を検索できます。
 - **新しいタブの追加** -- モニタする任意の Web サイトの名前および URL を手動で追加できます。
 - **CA サポート** -- さまざまなサポート サイトおよび Facebook や Twitter などのソーシャル ネットワーキング サイトへのアクセスを提供します。

CA ARCserve D2D ノードへのログイン

Host-Based VM Backup ホーム画面から、CA ARCserve D2D ノードにログインできます。

CA ARCserve D2D ノードにログインする方法

1. アプリケーションを開いて、ナビゲーションバーの[ノード]をクリックします。

[ノード] 画面が表示されます。

2. グループリストから [すべてのノード] をクリックするか、またはログインする CA ARCserve D2D ノードが含まれるグループをクリックします。

ノードリストに、指定したグループと関連付けられているノードがすべて表示されます。

3. ログインするノードを探してクリックし、ポップアップメニューから [D2D にログイン] をクリックします。

CA ARCserve D2D の CA ARCserve Central Host-Based VM Backup バージョンが開きます。

注: 新しいブラウザウィンドウが表示されない場合は、ブラウザのポップアップオプションですべてのポップアップ、あるいはこの Web サイトのポップアップのみ許可されていることを確認します。


CA ARCserve D2D ノードにログインしました。




注: 初めて CA ARCserve D2D ノードにログインする場合、警告メッセージを表示する HTML ページが開く場合があります。これは、Internet Explorer を使用する場合に発生する可能性があります。この動作を修正するには、Internet Explorer を閉じて手順 3 を繰り返します。その後、CA ARCserve D2D ノードに正常にログインできるようになります。

CA ARCserve Central Host-Based VM Backup 用のノードタスクを管理する方法

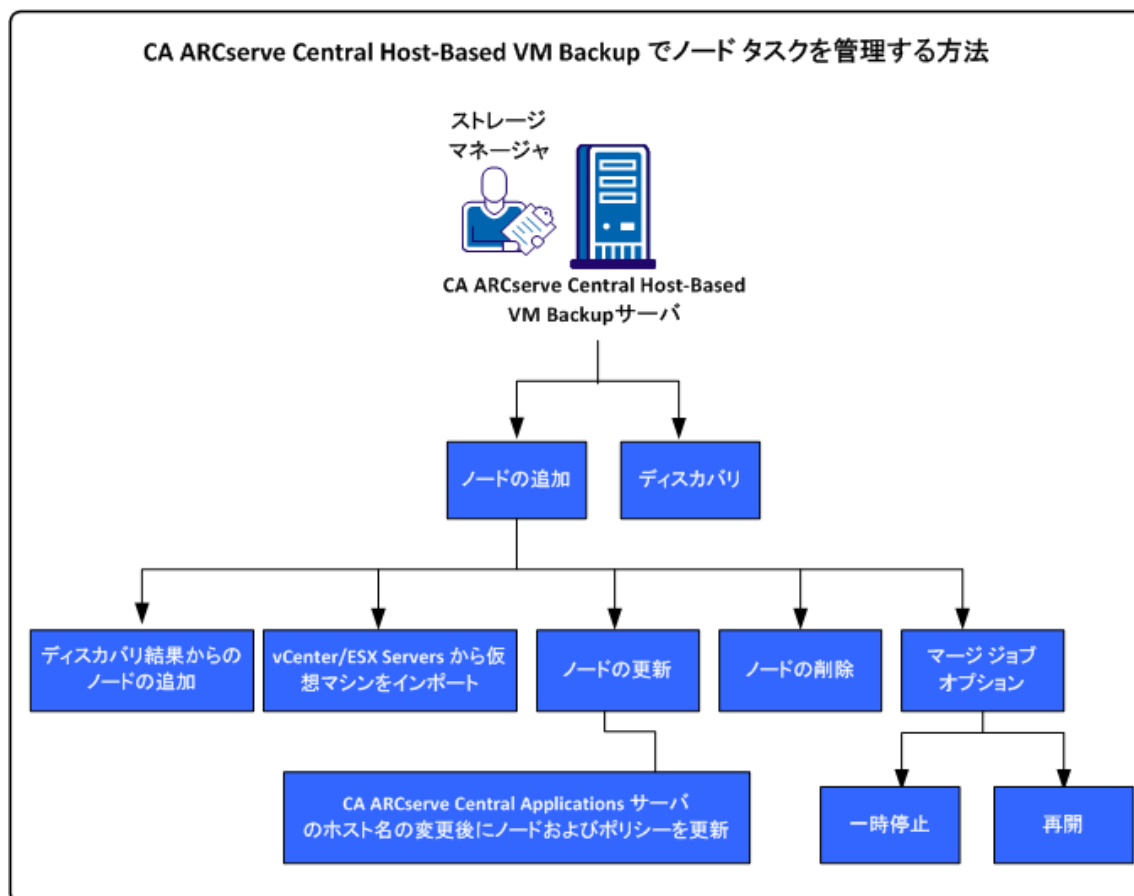
このシナリオでは、ストレージマネージャがどのようにノードを管理できるかについて説明します。たとえば、ノードの追加やディスカバリの実行、ノードのノードグループへの追加、および [ノード] 画面からのノードの更新または削除を行います。

以下の表では、[ノード] 画面に表示される項目について説明します。

列名	説明
ノード名	ノードの名前を表示します。 注: リスト表示されるノードの中には、選択できないものが含まれている場合があります。それは、サーバによって検出できないノードであるためです。たとえば、そのノードがサーバから削除されている場合などが考えられます。
ポリシー	ポリシーおよびポリシー展開ステータスの名前を表示します。
仮想マシン名	仮想マシンの名前を表示します。
vCenter/ESX	サーバの詳細を表示します。これは、仮想マシンの検出に役立ちます。
ジョブ (P. 83)	バックアップジョブのステータスを表示し、詳細については、ユーザを [バックアップステータスマニタ (P. 84)] にリンクします。
ステータス	ノードのステータスを表示します。 <ul style="list-style-type: none"> ■  = エラー/失敗 ■  = 警告 ■  = 成功 アイコンにマウスを合わせると、[ノードステータスマリ] ポップアップテーブルが表示されます。ここに、以下のカテゴリの結果が表示されます。 <ul style="list-style-type: none"> ■ 前回のバックアップ - バックアップの種類、日時、およびステータスを表示します。 ■ 復旧ポイント - モニタされているサーバの復旧ポイントの数を表示します ■ バックアップ先の容量 - バックアップ先で利用可能な空き容量を表示します。

列名	説明
前回のバックアップ結果	前回のバックアップジョブのステータスを表示します。
前回のバックアップ時刻	前回のバックアップの日時を表示します。
PFC ステータス	<p>ユーザのバックアップジョブのプレフライトチェックのステータスを表示します。</p> <ul style="list-style-type: none"> ■  = エラー/失敗 ■  = 警告 ■  = 成功 <p>アイコンは、特定のノードに対してバックアップジョブを実行できるかどうかを示します。</p> <p>アイコンにマウスを合わせると、[検証] ポップアップテーブルが表示されます。ここに、以下のカテゴリの結果が表示されます。</p> <ul style="list-style-type: none"> ■ 変更ブロックのトラッキング (CBT) - バックアップ用の CBT 結果を表示します。 ■ VMware Tools - VMware ツールがインストールされているかどうかが表示されます。 ■ ディスク - ディスクのステータスを表示します。 ■ 電力状態 - 仮想マシンの電源がオンになっているかオフかが表示されます。 ■ 認証情報 - ユーザ認証情報のステータスを表示します。 ■ アプリケーション - ノード上のアプリケーションのインストールステータスを表示します。 <p>詳細については、トピック「バックアップジョブのプレフライトチェックの実行 (P. 69)」を参照してください。</p>
アプリケーション	ノードが関連付けられているアプリケーションを表示します。
OS	ノードが関連付けられているオペレーティングシステムを表示します。
説明	ノードの説明を表示します。

以下の図は、ノード上で実行できるタスクを示しています。



このシナリオでは、ノードの追加または更新時に使用可能なオプションについて説明します。

- [ディスカバリ](#) (P. 52)
- [ノードの追加](#) (P. 53)
 - [オート ディスカバリの結果からのノードの自動追加](#) (P. 54)
 - [vCenter/ESX Server からの仮想マシンのインポート](#) (P. 56)
- [ノードの更新](#) (P. 58)
 - [CA ARCserve Central Applications サーバのホスト名変更後のノードおよびポリシーの更新](#) (P. 59)
- [ノードの削除](#) (P. 59)
- [マージジョブ オプション](#) (P. 60)
 - [ノード上のマージジョブの一時停止](#) (P. 60)

- [ノード上のマージジョブの再開 \(P. 61\)](#)

CA ARCserve Central Host-Based VM Backup からのノードのディスカバリ

CA ARCserve Central Host-Based VM Backup では、vCenter Server および ESX Server システムをユーザの環境に追加して、ノードの自動ディスカバリを実行できます。これらのサーバを追加することで、アプリケーションはホストする仮想マシンを自動的に検出できます。

重要: ノードのディスカバリ プロセスでは、vCenter Server または ESX Server システムのホスト名または IP アドレスを指定する必要があります。この情報によって、ディスカバリ プロセスは vCenter Server および ESX Server システムに接続されている仮想マシンを検出できます。vCenter Server または ESX Server システムのホスト名または IP アドレスの変更が必要であることが分かったら、このトピックの手順を繰り返し、バックアップ ポリシーを再度展開して、更新されたホスト名または IP アドレスで設定された新規バックアップを作成します。

次の手順に従ってください:

1. アプリケーションにログインし、ナビゲーションバー上の [ノード] をクリックして、[ノード] 画面を開きます。
2. ツールバー上の [ディスカバリ] をクリックして、[vCenter/ESX サーバによるノードのディスカバリ] ダイアログ ボックスを開きます。
3. [vCenter/ESX サーバによるノードのディスカバリ] ダイアログ ボックスで、以下のフィールドに入力します。

- vCenter/ESX ホスト
- ユーザ名

注: 指定するアカウントは、ESX Server または vCenter Server システムの管理者権限を持つアカウントである必要があります。

- パスワード
- ポート

[追加] をクリックします。

注: この手順を繰り返して、vCenter/ESX Server システムを追加します。

4. [ディスカバリ] をクリックして、ディスカバリ処理を開始します。
[ディスカバリ モニタ] が開き、ディスカバリの進捗状況が示されます。

5. ディスカバリ処理が完了すると、次の確認メッセージが表示されます。オート ディスカバリの結果からのノードの追加を続行してもよろしいですか?

[はい] をクリックすると、[ディスカバリの結果からのノードの追加] 画面が表示されます。追加するハイパーバイザがある場合は、[いいえ] をクリックします。

注: ノードを自動検出し [ノード名] リストに追加する場合の詳細については、トピック「ディスカバリ スケジュールの設定」を参照してください。

6. [検出されたノード] リストで、追加するノードをクリックし右方向矢印をクリックします。ノードは [保護するノード] リストに追加されます。
7. [次へ] をクリックして、[ノード認証情報] 画面を開きます。
8. 追加する各ノードのユーザ名およびパスワードを指定するか、または適切なグローバル認証情報を指定します。

[完了] ボタンをクリックします。

選択したノードが、選択したノードグループの [ノード画面] の [ノード名] リストに追加されます。

9. (オプション) [更新] をクリックします。追加したサーバが [ノード] 画面上の [グループ] リストに表示されます。
10. (オプション) [ディスカバリ] をクリックし、サーバがすべて追加されるまで、前の手順を繰り返します。

ノードの追加

環境が拡大するのに伴い、[ノード] 画面でノードを追加し、ノードをグループに割り当ててアプリケーション内で管理されるようにすることができます。アプリケーションは、以下の条件を満たす場合のみ仮想マシンを追加します。

- ゲスト OS が Windows
- VMware ハードウェア バージョンが 7 以上

以下プロセスを使用して、ノードを追加できます。

- [ディスカバリの結果からのノードの追加 \(P. 54\)](#) -- ディスカバリを使用すると、ESX/vCenter Server の詳細の入力、各サーバ上で実行される仮想マシンの検出、検出されたノードの管理および保護可能なアプリケーションへの手動または自動追加を実行できます。

ディスカバリ リストに追加されたサーバは、[環境設定] 画面で指定したスケジュールに基づいてスキャンされます。これは、サーバがリストから削除されるまで続きます。サーバ詳細を繰り返し入力する必要はありません。ディスカバリ リストには、前回のスキャン以降サーバに追加された新しい仮想マシンのみが表示されます。アプリケーションですでに管理されている VM は表示されません。また、次のスケジュール スキャンを待たずに、ディスカバリを実行することもできます。

- [v Center/ESX からの仮想マシンのインポート \(P. 56\)](#)

このオプションは手動のプロセスです。このプロセスでは、プロセスを起動するたびに ESX または vCenter サーバ詳細を指定する必要があります。サーバ詳細を繰り返し入力する手間を省くには、ディスカバリ リストにサーバを追加します。このオプションでは、指定されたサーバ上で検出された仮想マシンがすべてリスト表示されます。これには、すでにアプリケーションで管理されている仮想マシンも含まれます。

ディスカバリの結果からのノードの追加

このオプションを使用すると、[ディスカバリ環境設定] パネルで指定した設定に基づいて自動検出されたノードを選択できます。

次の手順に従ってください:

1. アプリケーションにログインします。

ナビゲーションバーの [ノード] をクリックして [ノード] 画面を開きます。

2. [ノード] カテゴリから、[追加] をクリックし、コンテキストメニューの [ディスカバリ結果からのノードの追加] をクリックします。

[ディスカバリ結果からのノードの追加] 画面が開き、検出されたノードのリストが表示されます。

3. [検出されたノード] リストから、追加するノードを選択し、矢印をクリックして[保護するノード] リストに追加します。終了したら[次へ] をクリックします。

注: ノード名またはドメインでリストをフィルタし、リストを最小化することができます。

4. (オプション) 1つ以上のノードを選択して [選択したノードを非表示にする] をクリックし、バックアップ対象外のノードを非表示にします。
5. (オプション) [非表示のノードを表示] オプションをオンにすると、非表示になっていたノードが[検出された] ノードリストに戻ります。ノードを再度非表示にするには、このオプションをオフにします。
6. [ノード認証情報] 画面で、追加するノードのユーザ名およびパスワードを指定します。グローバル認証情報を指定するか、または選択したノードに認証情報を適用できます。
7. [完了] ボタンをクリックします。

ノードが追加されます。

vCenter/ESX からの仮想マシンのインポート

[vCenter/ESX から仮想マシンをインポート] オプションを使用して、ノードを追加することもできます。このタスクでは、アプリケーションによって指定されたホスト上で実行されている仮想マシンがすべてディスカバリされますが、定期的な自動的なスキャンは実行されません。仮想マシンを後で追加した場合は、この手順を繰り返します。そうしないと、新しい仮想マシンは認識されません。

このオプションとディスカバリ オプションの以下の相違点について考慮する必要があります。

- このオプションを起動するたびに、ESX/vCenter Server 詳細を指定する必要があります。
- 指定したサーバをディスカバリ リストに追加するオプションを使用すると、認証情報を毎回入力する必要がなくなります。
- このオプションを使用するたびに、利用可能な仮想マシンがすべてリスト表示されます。アプリケーションによって管理される仮想マシンもリスト表示されます。

次の手順に従ってください:

1. アプリケーションにログインします。
ナビゲーションバー上の [ノード] をクリックして、[ノード] 画面を開きます。
2. ツールバー上で [追加] をクリックし、ポップアップメニュー上の [vCenter/ESX から仮想マシンをインポート] をクリックします。
[ノードのディスカバリ] ダイアログ ボックスが表示されます。

3. [ノードのディスカバリ] ダイアログ ボックスで、以下のフィールドに入力します。
 - vCenter/ESX ホスト

注: お使いの環境で VMware Distributed Resource Scheduler (DRS) を実行している場合、vCenter Server システムのホスト名を指定することをお勧めします。この方法により、お使いの環境で実行されている仮想マシンを CA ARCserve Central Host-Based VM Backup が検出し、DRS が有効な仮想マシンのバックアップを正常に完了することができます。Distributed Resource Scheduling の詳細については、VMware の Web サイトを参照してください。

 - ユーザ名
 - パスワード
 - ポート
 - プロトコル

[接続] をクリックし、スキャンが完了するまで待ちます。
4. (オプション) オプション [オート ディスカバリ リストに vCenter/ESX サーバを自動的に追加します] オプションを有効にします。
5. [次へ] をクリックして、[ノード認証情報] ダイアログ ボックスを開きます。
6. [ノード認証情報] 画面で、検出されたすべての仮想マシンのグローバル ユーザ名およびパスワードを指定し、[選択対象に適用] オプションをクリックします。あるいは、1 つの VM をクリックして、特定の認証情報を入力します。
7. [完了] ボタンをクリックします。

選択した仮想マシンは、指定したノードグループに追加されます。

注: CA ARCserve Central Host-Based VM Backup は、電源が投入されていない状態の仮想マシンおよび VMware Tools がインストールされていない仮想マシンのホスト名を検出できません。このような場合、ノードをインポートすると、[ノード] 画面の [ホスト名] フィールドには「不明」と表示されます。さらに、（[ノード] 画面の）ノード名フィルタは、「不明」が付されているノードをフィルタできません。

ノードの更新

CA ARCserve Central Host-Based VM Backup では、以前に追加されたノードに関する情報を更新することができます。

次の手順に従ってください:

1. アプリケーションにログインします。
ホーム画面上のナビゲーションバーで [ノード] を選択します。
[ノード] 画面が表示されます。
2. グループバーから、[すべてのノード] グループをクリックするか、あるいは更新するノードが含まれるグループ名をクリックします。
グループに関連付けられたノードが、ノードリストに表示されます。
3. 更新するノードをクリックし、右クリックしてポップアップメニューから [ノードの更新] をクリックします。
[ノードの更新] ダイアログ ボックスが開きます。

注: ノードグループ内のノードをすべて更新するには [ノードグループ] 名を右クリックし、ポップアップメニューから [ノードの更新] をクリックします。

4. 必要に応じてノードの詳細を更新します。
注: ノードリストで複数のノードを更新するには、ノードを選択し、右クリックしてポップアップメニューから [ノードの更新] をクリックします。ユーザ名とパスワードはすべての選択したノードに対して同じです。デフォルトでは、[新しい認証情報を指定] オプションおよび [管理対象ノード] チェック ボックスがオンになっています。選択したノードに新しいユーザ名とパスワードを指定することができます。また、このサーバにノードを管理させることができます。さらに、[既存の認証情報を使用] を選択し、現在のユーザ名とパスワードを適用することができます。フィールドは無効になります。
5. [OK] をクリックします。
[ノードの更新] ダイアログ ボックスが閉じ、ノードが更新されます。

CA ARCserve Central Applications サーバのホスト名変更後のノードおよびポリシーの更新

CA ARCserve Central Host-Based VM Backup サーバのホスト名を変更した後で、ノードおよびノードに適用されているポリシーを更新します。これらのタスクは、サーバとサーバが保護しているノードとの関係を保持するために実行します。以下の表では考えられるシナリオと各シナリオの対処法について説明します。

シナリオ	対処法
CA ARCserve Central Host-Based VM Backup サーバのホスト名が変更された後で、ノードが追加された。	特に対処は必要ありません。
ノードを追加した後で CA ARCserve Central Host-Based VM Backup サーバのホスト名を変更した。ポリシーはノードに適用されていない。	ノードを更新します。詳細については、「 ノードの更新 (P. 58) 」を参照してください。
ノードを追加した後で CA ARCserve Central Host-Based VM Backup サーバのホスト名を変更した。ポリシーはノードに適用されている。	ポリシーを再適用します。詳細については、「 仮想マシンへのポリシーの割り当て 」を参照してください。

ノードの削除

必要に応じてノードを削除できます。

次の手順に従ってください:

1. アプリケーションにログインします。
ナビゲーションバーの [ノード] をクリックし、[ノード] 画面を開きます。
2. グループ バーから、[すべてのノード] グループをクリックするか、あるいは削除するノードが含まれるグループ名をクリックします。
グループに関連付けられたノードが、ノードリストに表示されます。

3. 削除するノード（複数可）をオンにして、ツールバー上の [削除] をクリックします。
確認メッセージが表示されます。
4. 以下のいずれかを行います。
 - ノードを削除する場合は、 [はい] をクリックします。
 - ノードグループを削除しない場合は、 [いいえ] をクリックします。

マージジョブオプション

CA ARCserve Central Host-Based VM Backup では、各ノードのマージジョブをいつでも一時停止/再開できます。マージジョブを一時停止/再開しても、進行中のジョブには影響しません。

ノード上のマージジョブの一時停止

CA ARCserve Central Host-Based VM Backup では、特定ノードのマージジョブを一時停止できます。

たとえば、マージジョブがシステムリソースを消費して、バックアップジョブの進行が遅くなる場合があります。一時停止オプションを使用すると、進行中のバックアップジョブが効率よく完了するように、進行中のマージジョブを停止できます。バックアップが完了した後で、マージジョブを再開することができます。

次の手順に従ってください:

1. CA ARCserve Central Host-Based VM Backup ホーム画面で、ナビゲーションバーの [ノード] をクリックして [ノード] 画面を開きます。
2. マージジョブを一時停止するノードが含まれるノードグループを選択します。
選択されたノードグループのノードのリストが表示されます。

3. マージジョブを一時停止するノードをクリックします。次に、選択したノードを右クリックし、ポップアップメニューからの [マージジョブの一時停止] をクリックします。

注: [マージジョブの一時停止] オプションはデフォルトでは無効です。ノードがマージジョブを実行しているとき、[ジョブ] 列に示されるように、[マージジョブの一時停止] オプションは有効になります。

選択したノードのマージジョブは一時停止され、CA ARCserve D2D ホームページ上で確認できます。

ノード上のマージジョブの再開

CA ARCserve Central Host-Based VM Backup では、一時停止した特定のノードのマージジョブを再開できます。

次の手順に従ってください:

1. CA ARCserve Central Host-Based VM Backup ホーム画面で、ナビゲーションバーの [ノード] をクリックして [ノード] 画面を開きます。
2. マージジョブを再開するノードが含まれるノードグループを選択します。

選択されたノードグループのノードのリストが表示されます。

3. 一時停止されたマージジョブを再開するノードをクリックします。次に、選択したノードを右クリックし、ポップアップメニューからの [マージジョブの再開] をクリックします。

注: 実行中のバックアップジョブがなく、マージジョブが一時停止されている場合に、[マージジョブの再開] オプションは有効になります。

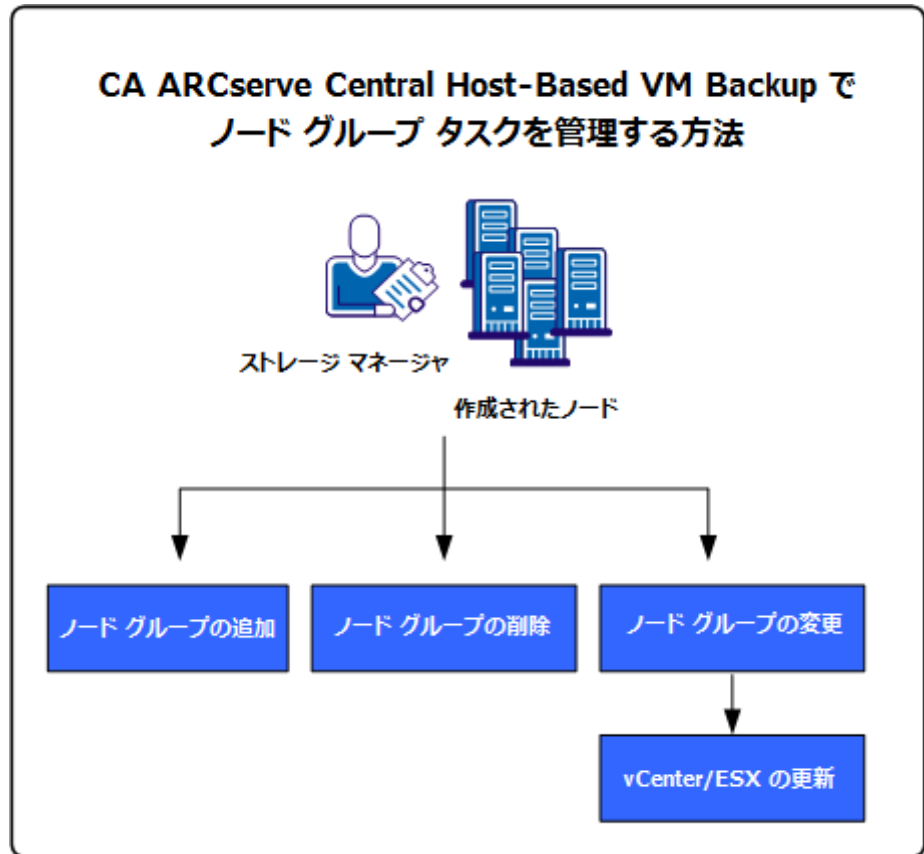
選択したノードのマージジョブは再開され、CA ARCserve D2D ホームページ上で確認できます。

CA ARCserve Central Host-Based VM Backup 用のノードグループ タスクを管理する方法

CA ARCserve Central Host-Based VM Backup を使用することで、ストレージマネージャは多数の仮想マシンを1つのマシンを保護すると同じくらい容易に保護できます。

まずはノードを追加します。ノードをアプリケーション別、または目的別にグループ化できます。ノードグループを作成すると、仮想マシン環境を容易に視覚化できます。バックアップポリシーを作成し、ポリシーをノードに割り当てることで、簡単に仮想環境を保護できます。詳細については、「[CA ARCserve Central Host-Based VM Backup 用ポリシーの管理方法](#) (P. 86)」を参照してください。

以下の図では、ノードグループに対して実行できるタスクについて説明します。



このシナリオでは、以下のトピックについて説明します。

- [ノード グループの追加](#) (P. 63)
- [ノード グループの削除](#) (P. 65)
- [ノード グループの変更](#) (P. 66)

ノード グループの追加

ESX/vCenter Server ホストから仮想マシンを最初にインポートする場合は、新規ノード グループが自動的に追加されます。

ノード グループを使用すると、共通の特性に基づいて CA ARCserve D2D ソース コンピュータの集合を管理することができます。たとえば、サポートする部門別に分類されたノード グループを定義できます（例：会計、マーケティング、開発など）。

アプリケーションには以下のノード グループが含まれます。

- **デフォルト グループ**：
 - **すべてのノード** -- アプリケーションに関連付けられたすべてのノードが含まれます。
 - **グループがないノード** -- アプリケーションに関連付けられ、ノード グループに割り当てられていないすべてのノードが含まれます。
 - **ポリシーがないノード** -- アプリケーションに関連付けられ、ポリシーが割り当てられていないすべてのノードが含まれます。
 - **SQL Server** -- ノードにインストールされている、アプリケーションおよび Microsoft SQL Server に関連付けられるノードがすべて含まれます。
 - **Exchange** -- ノードにインストールされている、アプリケーションおよび Microsoft Exchange Server に関連付けられるノードがすべて含まれます。

注: デフォルト ノード グループの変更または削除はできません。

- **カスタム グループ** -- カスタマイズされたノード グループが含まれます。
- **vCenter/ESX グループ** -- [vCenter/ESX から仮想マシンをインポート] オプションを使用してノードを追加した場合、vCenter/ESX Server の名前がこのグループに追加されます。

次の手順に従ってください:

1. アプリケーションにログインします。
ホーム画面上のナビゲーションバーから [ノード] をクリックして [ノード] 画面を開きます。
2. [ノードグループ] ツールバーで [追加] をクリックします。
[グループの追加] ダイアログ ボックスが表示され、[利用可能なノード] リストにノードが表示されます。
3. ノードグループの [グループ名] を指定します。
4. [グループの追加] ダイアログ ボックスから以下のフィールドを指定します。
 - **グループ** -- 割り当てるノードが含まれているグループの名前を選択します。
 - **ノード名フィルタ** -- 共通の条件に基づいて利用可能なノードをフィルタ処理できます。
注: [ノード名フィルタ] フィールドでは、ワイルドカード文字を使用サポートします。
たとえば、**Acc*** は、ノード名が「Acc」で始まるすべてのノードをフィルタ処理できます。フィルタ結果をクリアするには、[フィルタ] フィールドで **X** をクリックします。
5. ノードグループにノードを追加するには、追加するノードを選択して、右矢印をクリックします。
ノードが [利用可能なノード] リストから [選択されたノード] リストへ移動され、ノードグループに割り当てられます。
注: 現在のグループからノードをすべて選択し移動するには、二重右矢印をクリックします。
6. (オプション) [選択されたノード] リストからノードを [利用可能なノード] リストに移動するには、左矢印をクリックします。
注: 現在のグループのノードをすべて選択し移動するには、二重左矢印をクリックします。
7. [OK] をクリックします。
ノードグループが追加されます。

ノードグループの削除

必要に応じてノードグループを削除できます。手動で追加されたグループを削除しても、仮想マシンはアプリケーションから削除されません。ただし、ESX/vCenter Server のディスカバリから自動的に作成されたグループを削除すると、そのグループおよびすべての仮想マシンがアプリケーションから削除されます。

作成したノードグループを削除できます。

以下のノードグループは削除できません。

- **すべてのノード** -- アプリケーションに関連付けられたすべてのノードが含まれます。
- **グループがないノード** -- アプリケーションに関連付けられ、ノードグループに割り当てられていないすべてのノードが含まれます。
- **ポリシーがないノード** -- アプリケーションに関連付けられ、ポリシーが割り当てられていないすべてのノードが含まれます。
- **SQL Server** -- ノードにインストールされている、アプリケーションおよび Microsoft SQL Server に関連付けられるノードがすべて含まれます。
- **Exchange** -- ノードにインストールされている、アプリケーションおよび Microsoft Exchange Server に関連付けられるノードがすべて含まれます。

注: ノードグループを削除しても、個々のノードがアプリケーションから削除されるわけではありません。

次の手順に従ってください:

1. アプリケーションにログインします。
ホーム画面上のナビゲーションバーから [ノード] をクリックして [ノード] 画面を開きます。
2. 削除するノードグループをクリックし、[ノードグループ] ツールバーの [削除] をクリックします。
確認メッセージのダイアログボックスが表示されます。
3. ノードグループを削除する場合は、[はい] をクリックします。

注: ノードグループを削除しない場合は、[いいえ] をクリックします。

ノードグループが削除されます。

ノードグループの変更

作成したノードグループを変更できます。ノードグループでのノードの追加と削除、およびノードグループの名前を変更できます。

注: 以下のノードグループは変更できません。

- **すべてのノード** -- アプリケーションに関連付けられたすべてのノードが含まれます。
- **グループがないノード** -- アプリケーションに関連付けられ、ノードグループに割り当てられていないすべてのノードが含まれます。
- **ポリシーがないノード** -- アプリケーションに関連付けられ、ポリシーが割り当てられていないすべてのノードが含まれます。
- **SQL Server** -- アプリケーションに関連付けられ、Microsoft SQL Server がインストールされたすべてのノードが含まれます。
- **Exchange** -- アプリケーションに関連付けられ、Microsoft Exchange Server がインストールされたすべてのノードが含まれます。

次の手順に従ってください:

1. アプリケーションにログインします。
ホーム画面上のナビゲーションバーから、[ノード] をクリックします。
[ノード] 画面が表示されます。
2. 変更するノードグループをクリックし、[ノードグループ] ツールバーで [変更] をクリックします。
[グループの変更] ダイアログボックスが表示されます。
3. グループ名を変更するには、[グループ名] フィールドに新しい名前を指定します。
4. ノードグループにノードを追加するには、ノードグループに追加するノードを選択して、右矢印をクリックします。
ノードが [利用可能なノード] リストから [選択されたノード] リストへ移動され、ノードグループに割り当てられます。
注: [利用可能なノード] リストからすべてのノードを [選択されたノード] リストに移動するには、二重右矢印をクリックします。

5. ノードグループからノードを削除するには、左矢印か二重左矢印をクリックし、1つずつまたはすべてのノードを削除します。
6. (オプション) 共通の条件に基づいて利用可能なノードをフィルタ処理するには、[ノード名フィルタ] フィールドにフィルタ値を指定します。

注: [フィルタ] フィールドでは、ワイルドカード文字を使用サポートします。

たとえば、**Acc*** は、ノード名が「**Acc**」で始まるすべてのノードをフィルタ処理できます。フィルタ結果をクリアするには、[フィルタ] フィールドで **X** をクリックします。

7. [OK] をクリックします。

ノードグループが変更されます。

vCenter/ESX Server の詳細を更新します。

CA ARCserve Central Host-Based VM Backup では、以前に追加された vCenter/ESX Server の詳細を更新できます。

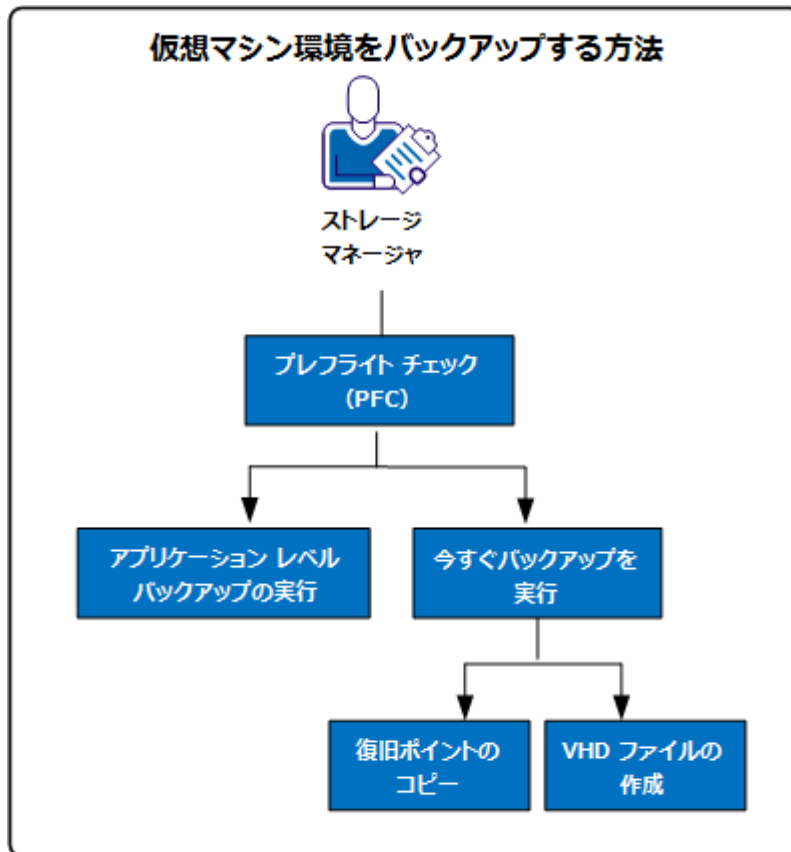
次の手順に従ってください:

1. [ノード] 画面で、[グループ] バーからの [vCenter/ESX グループ] を展開します。
2. サーバの詳細を更新する vCenter/ESX グループを選択し、右クリックして、[vCenter/ESX の更新] をクリックします。
[vCenter/ESX の更新] ダイアログ ボックスが表示されます。
3. vCenter/ESX Server の詳細をそれに応じて更新します。
4. [OK] をクリックします。
[vCenter/ESX の更新] ダイアログ ボックスが閉じ、ノードグループが更新されます

仮想マシン環境のバックアップ方法

このシナリオでは、ストレージマネージャがユーザの環境内のすべての仮想マシンをどのようにバックアップおよび保護できるかについて説明します。

以下の図は、仮想マシン環境をバックアップする方法を示しています。



以下のリストでは、図に示されているプロセスについて説明します。

- [バックアップジョブのプレフライト チェックの実行](#) (P. 69)
- [今すぐバックアップを実行](#) (P. 74)
 - [バックアップ復旧ポイントのコピー](#) (P. 77)
 - [VHD ファイルの作成](#) (P. 81)
- [アプリケーション レベル バックアップの実行](#) (P. 82)

バックアップ ジョブのプレフライト チェックの実行

CA ARCserve Central Host-Based VM Backup の主要な機能として、「プレフライト チェック (PFC)」というユーティリティがあります。これによって、ユーザは特定のノードに対して重要なチェックを実行し、バックアップ ジョブの失敗につながる条件を検出できます。ユーザが以下のアクションを実行すると、PFC は自動的に実行されます。

- vCenter Server/ESX Server システムからの仮想マシンのインポート
- ディスカバリ結果からのノードの追加
- ノードの更新

さらに、プレフライト チェックを手動で実行することもできます。

次の手順に従ってください:

1. アプリケーションにログインします。
ナビゲーションバー上の [ノード] をクリックして、[ノード] 画面を開きます。
2. 以下のアクションのいずれかを実行して、プレフライト チェックの実行元となるノードを指定します。
 - **ノード レベル:** プレフライト チェックの実行対象ノードが含まれるグループをクリックしてから、ノードの横のチェック ボックスをクリックします。次に、ノードを右クリックし、コンテキストメニューから [プレフライト チェック] をクリックします。
 - **グループ レベル:** ノードが含まれるグループを右クリックし、[プレフライト チェック] をクリックします。

「仮想マシンのプレフライト チェックを開始しています」というメッセージが表示されます。
3. [PFC ステータス] 列へスクロールし、プレフライト チェックのステータスを表示します。

以下の表では、PFCによって実行されるチェックについて説明します。

項目	説明
変更ブロックのトラッキング (CBT)	(CBT) は、仮想マシン上に存在する、変更されたディスクセクタのトラッキングを行う機能です。これは、バックアップのサイズを最小化するのに役立ちます。 この項目は、CBT が有効であることを確認します。
VMware Tools	この項目は、VMware Tools が各仮想マシンにインストールされていることを確認します。
ディスク	この項目は、仮想マシンに、バスを共有するように設定されているコントローラに接続されているハードディスクがあることを確認します。
電源状態	この項目は、仮想マシンの電源がオンになっていることを確認します。
認証情報	この項目は、ユーザの認証情報が有効であることを確認します。
アプリケーション	この項目は、Microsoft SQL Server と Microsoft Exchange Server がインストールされているかどうかを確認します。

プレフライトチェックの結果のエラーおよび警告を解決する方法の詳細については、トピック「[プレフライトチェック項目のソリューション \(P. 71\)](#)」を参照してください。

プレフライトチェック項目のソリューション

以下の表では、プレフライトチェックの結果としてのエラーおよび警告を解決するのに役立つソリューションについて説明します。

変更ブロックのトラッキング (CBT)

ステータス	メッセージ	ソリューション
警告	変更ブロックのトラッキングが、スナップショットが存在する状態で有効になっています。ディスクのフルバックアップが適用されます。	<p>使用済みブロック バックアップを適用するには、以下の手順に従います。</p> <ol style="list-style-type: none"> 1. 仮想マシンと関連付けられたスナップショットをすべて削除します。 2. Host-Based VM プロキシサーバにログインします。 3. レジストリ エディタ を開き、以下のキーを探します。 HKEY_LOCAL_MACHINE¥SOFTWARE¥CA¥CA ARCserve D2D¥AFBackupDll¥VM_InstanceUUID¥<UUID> 4. レジストリキーを「"full disk backupForFullBackup"=0」に設定します。 5. 「ResetCBT=1」というレジストリを作成/設定します。 5. バックアップ ジョブをサブミットします。

VMware Tools

ステータス	メッセージ	ソリューション
警告	期限切れです。	VMware Tools の最新バージョンをインストールしてください。
警告	インストールされていないか実行されていません。	VMware Tools の最新のバージョンをインストールし、ツールが実行されていることを確認します。

ディスク

ステータス	メッセージ	ソリューション
エラー	VM スナップショットは VM ではサポートされていません。これは VM では SCSI コントローラがバスを共有するように設定されているためです。	CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、VM をバックアップします。
警告	物理 Raw デバイス マッピング (RDM) ディスクはバックアップされません。	CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、VM をバックアップします。
警告	仮想 Raw デバイス マッピング (RDM) ディスクはフルディスクとしてバックアップされます。	CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、VM をバックアップします。
警告	独立したディスクはバックアップされません。	CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、VM をバックアップします。
警告	アプリケーションは、NFS データストア上のディスクをフルディスクとしてバックアップします。	CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、VM をバックアップします。

電源状態

ステータス	メッセージ	ソリューション
警告	電源がオフにされました。	仮想マシンの電源をオンにします。
警告	一時停止中です。	仮想マシンの電源をオンにします。

認証情報

ステータス	メッセージ	ソリューション
警告	認証情報が正しくありません。	有効なユーザ認証情報を提供します。
警告	提供されていません。	有効なユーザ認証情報を提供します。

アプリケーション

ステータス	メッセージ	ソリューション
警告	VM に IDE ディスクがあるので、アプリケーション レベル リストアはサポートされていません。	CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、Microsoft SQL Server および Exchange Server データをバックアップします。
警告	VMware VIX がホスト サーバにインストールされていません。	VIX を VMware Web サイトからダウンロードし、それを CA ARCserve Central Applications ホスト サーバにインストールします。
警告	CA ARCserve Central Host-Based VM Backup サーバ上の VMware VIX は期限切れです。	VIX を VMware Web サイトからダウンロードし、それを CA ARCserve Central Applications ホスト サーバにインストールします。
警告	ESX Server はサポートされていないので、アプリケーション レベル リストアはサポートされていません。	ESX Server を 4.1 以上にアップグレードするか、CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、Microsoft SQL Server および Exchange Server データをバックアップします。
警告	利用可能な SCSI スロットが不足しているため、アプリケーション レベル リストアはサポートされていません。	CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、Microsoft SQL Server および Exchange Server データをバックアップします。
警告	ソースがダイナミック ディスクに存在します。アプリケーション レベル リストアはサポートされていません。	CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、Microsoft SQL Server および Exchange Server データをバックアップします。 注: VMware は、ESX Server 4.1 以降で実行されるダイナミック ディスクを備えた Windows 2008 以降の仮想マシンに対して、アプリケーション レベルの静止 (quiescing) をサポートしません。
警告	アプリケーションに関する情報を取得できません。そのため、アプリケーション レベルバックアップが正常に完了できません。	仮想マシンの Windows オペレーティングシステム内の UAC を無効にします。

今すぐバックアップを実行

通常、バックアップは自動的に実行され、スケジュール設定によって制御されます。ただし、スケジュールされていない時間にアドホック バックアップ（フル、増分、検証）をただちに実行する必要がある場合があります。

アドホック バックアップは、バックアップ計画の一部としてあらかじめスケジュールされるのではなく、必要に応じて実行されます。たとえば、フル、増分、検証バックアップを繰り返し実行するスケジュールが設定されている状況でマシンに大幅な変更を加える場合、次にスケジュールされたバックアップを待つ代わりに、すぐにアドホック バックアップを実行する必要があります。

アドホック バックアップでは、カスタマイズされた（スケジュールされていない）復旧ポイントを追加することにより、必要に応じてその時点までロールバックすることができます。たとえば、パッチまたはサービスパックをインストールした後、マシンのパフォーマンスに悪影響を及ぼすことが判明した場合、そのパッチやサービスパックが含まれていないアドホックのバックアップセッションまでロールバックすることができます。

次の手順に従ってください:

1. アプリケーションにログインします。
2. ホーム画面上のナビゲーションバーから [ノード] をクリックして [ノード] 画面を開きます。
3. バックアップするノードを指定するために、以下のいずれかのアクションを実行します。
 - **ノード レベル**：バックアップするノードが含まれるグループをクリックし、バックアップするノードの横のチェック ボックスをオンにします。
 - **グループ レベル**：バックアップするノードが含まれるグループをクリックします。

4. 次に、ノードをバックアップするために以下のいずれかのアクションを実行します。
 - ツールバーの [バックアップ] をクリックします。
 - 選択したグループを右クリックするか、またはノードを右クリックし、コンテキストメニューの [今すぐバックアップ] をクリックします。

5. [今すぐバックアップを実行] ダイアログボックスで、以下のいずれかの種類をクリックしてバックアップの種類を指定します。
 - **フルバックアップ** -- マシン全体または選択されたボリュームのフルバックアップを開始します。
 - **増分バックアップ** -- マシンの増分バックアップを開始します。増分バックアップは、前回のバックアップ以降に変更されたブロックのみをバックアップします。

注: 増分バックアップのメリットは、バックアップを高速で実行できること、また作成されるバックアップイメージのサイズが小さいことです。これは、バックアップを実行する場合に最も適した方法です。

- **検証バックアップ** -- マシンの検証バックアップを開始します。個別のブロックの最新のバックアップを確認し、中身および情報を元のソースと比較します。この比較によって、前回バックアップされたブロックが、ソースの対応する情報を表しているかどうかを検証します。ブロックのバックアップイメージがソースと一致しない場合、CA ARCserve D2D によって、一致していないブロックのバックアップが更新（再同期）されます。検証バックアップの実行には、以下のようなメリットとデメリットがあることに注意してください。
 - **メリット** -- フルバックアップに比べて作成されるバックアップイメージは極めて小さくなります。これは、変更されたブロック（最新のブロックに一致しないブロック）のみがバックアップされるためです。
 - **デメリット** -- すべてのソース ディスク ブロックが前回のバックアップのブロックと比較されるため、バックアップ時間は遅くなります。

注: バックアップソースに新しいボリュームを追加した場合、全体でどのバックアップ方式を選択した場合でも、新しく追加されたボリュームにはフルバックアップが実行されます。

6. (オプション) バックアップ名を指定して [OK] をクリックします。名前を指定しない場合、デフォルトでは、「カスタマイズされた/フル/増分/検証バックアップ」という名前になります。

確認の画面が表示され、選択した種類のバックアップがただちに開始されます。

以下の動作に注意してください。

- [ポリシー] ダイアログボックスで指定された値はすべてジョブに適用されます。
- カスタム (アドホック) バックアップジョブが失敗してもメイクアップジョブは作成されません。メイクアップジョブが作成されるのは、スケジュールされたジョブが失敗したときのみです。
- CA ARCserve Central Host-Based VM Backup は、優先度に従い、以下のバックアップジョブを適用します。
 - フル
 - 検証
 - 増分

[今すぐバックアップ] がサブミットされたときにキュー内に待機ジョブがある場合、以下のように処理されます。

- [フルバックアップ]ジョブがサブミットされたときに[検証バックアップ]ジョブがキュー内で待機していると、[フルバックアップ]ジョブがキュー内のジョブを上書きします。
- [フルバックアップ]ジョブがサブミットされたときに[増分バックアップ]ジョブがキュー内で待機していると、[フルバックアップ]ジョブがキュー内のジョブを上書きします。
- [検証バックアップ]ジョブがサブミットされたときに[増分バックアップ]ジョブがキュー内で待機していると、[検証バックアップ]ジョブがキュー内のジョブを上書きします。

- [検証バックアップ]ジョブがサブミットされたときに[フルバックアップ]ジョブがキュー内で待機していると、[検証バックアップ]ジョブはスキップされます。
- [増分バックアップ]ジョブがサブミットされたときに[フルバックアップ]ジョブがキュー内で待機していると、[増分バックアップ]ジョブはスキップされます。
- [増分バックアップ]ジョブがサブミットされたときに[検証バックアップ]ジョブがキュー内で待機していると、[増分バックアップ]ジョブはスキップされます。

復旧ポイントのコピー

CA ARCserve D2D によってバックアップが正常に実行されるたびに、バックアップの Point-in-Time スナップショット イメージも作成されます。この復旧ポイントの集合体によって、コピーするバックアップイメージを特定して指定できます。以下の手順を実行して、バックアップを保護できます。

- 障害発生時に、復旧ポイント情報をコピー/エクスポートして、それをオフサイトに安全に格納します。
- 復旧ポイントを複数の場所へ保存します。
- バックアップ先がいっぱいになったが、すべての復旧ポイントを保存したい場合、バックアップを統合します。

コピーする復旧ポイントの選択時に、フルかつ最新のバックアップイメージを再作成するために必要な以前のバックアップをすべてキャプチャします。

次の手順に従ってください:

1. アプリケーションにログインします。
ナビゲーションバー上の [ノード] をクリックして、[ノード] 画面を開きます。
2. グループリストから [すべてのノード] をクリックするか、またはコピーする復旧ポイントを含む CA ARCserve D2D ノードが含まれるグループをクリックします。
ノードリストに、指定したグループに関連付けられているノードがすべて表示されます。

- ログインするノードを探してクリックし、ポップアップメニューから [D2Dにログイン] をクリックします。

CA ARCserve D2D が開き、CA ARCserve D2D ノードのホーム画面にログインします。

注: ブラウザ ウィンドウでポップアップ オプションが有効になっていることを確認します。

- CA ARCserve D2D ホーム画面で、[復旧ポイントのコピー] を選択します。

[復旧ポイントのコピー] ダイアログ ボックスが表示されます。

- [バックアップ場所] フィールドでバックアップ ソースを指定します。バックアップ イメージが保存されている場所を指定するか、参照して指定します。緑色の矢印アイコン ボタンをクリックすると、指定した場所への接続を検証できます。必要に応じて、その場所にアクセスするための [ユーザ名] および [パスワード] 認証情報を入力します。

- [仮想マシン] フィールドで、[仮想マシンの選択] ドロップダウン リストをクリックし、コピーする復旧ポイントが含まれる仮想マシンを指定します。

カレンダー表示では、表示期間にそのバックアップ ソースの復旧ポイントを含むすべての日付が強調表示されます。

- コピーする復旧ポイントを指定します。

- カレンダーで、コピーするバックアップ イメージの日付を選択します。

その日付に対応する復旧ポイントが、バックアップの時刻、実行されたバックアップの種類、およびバックアップの名前と共に表示されます。

注: ロック記号の付いた時計のアイコンは、復旧ポイントに暗号化された情報が含まれており、リストアするにはパスワードが必要であることを示します。

- コピーする復旧ポイントを選択します。

その復旧ポイントに対応するバックアップ コンテンツ (すべてのアプリケーションを含む) が表示されます。

- [次へ] をクリックします。

[コピー オプション] ダイアログ ボックスが表示されます。

注: このダイアログボックスには2つのパスワードフィールドがあります。[パスワード]フィールドは、ソースセッションを復号化するパスワード用に、[暗号化パスワード]フィールドはデスティネーションセッションを暗号化するために使用します。

- a. エクスポートされた復旧ポイントが以前に暗号化された場合、パスワードが必要です。
 - エクスポートされた復旧ポイントが復旧ポイント コピー ジョブを実行する同じマシンのバックアップセッションである場合、暗号化パスワードは保存され自動的に入力されています。
 - エクスポートされた復旧ポイントが別のマシンのバックアップセッションである場合、暗号化パスワードが必要です。
- b. デスティネーションを選択します。

選択した復旧ポイントのコピーを格納する場所を指定するか、参照して指定できます。緑色の矢印アイコンボタンをクリックすると、指定した場所への接続を検証できます。必要に応じて、[ユーザ名] および [パスワード] を入力します。

- c. 実行する圧縮のレベルを選択します。

注: 指定されたバックアップ圧縮レベルとコピー圧縮レベルに関係はありません。たとえば、バックアップ先で圧縮レベルを[標準]に設定できます。しかし、コピージョブのサブミット時に、圧縮を[圧縮なし]または[最大圧縮]に変更することができます。

圧縮は、通常、ディスク容量の使用率を減らすために実行されますが、CPU使用率が増加するため、バックアップ速度が低下するという影響があります。

使用可能なオプションは、以下のとおりです。

- **圧縮なし** - 圧縮は実行されません。ファイルは純粹な VHD です。このオプションを使用すると、CPU 使用率は最も低くなります（最も高速で動作します）。ただし、バックアップイメージのディスク容量の使用率は最大になります。
- **標準圧縮** - 標準圧縮が実行されます。このオプションを使用すると、CPU 使用率とディスク容量使用率のバランスを適度に調節します。このオプションはデフォルトの設定です。

- **最大圧縮** - 最大圧縮が実行されます。このオプションを使用すると、CPU 使用率が最も高くなります (最も低速で動作します)。ただし、ディスク容量の使用率は、最小になります。

以下のような点を考慮する必要があります。

- ユーザのバックアップイメージに圧縮できないデータ (JPG イメージ、ZIP ファイルなど) が含まれている場合、そのようなデータを処理するために追加のストレージ容量が使用されます。その結果、圧縮オプションを選択していて、バックアップに圧縮できないデータがある場合、実際にはディスク容量の使用率が増大する場合があります。
 - 圧縮レベルを [圧縮なし] から [標準圧縮] または [最大圧縮] のいずれかに変更するか、[標準圧縮] または [最大圧縮] のいずれかから [圧縮なし] に変更した場合、圧縮レベルの変更後に実行される最初のバックアップは自動的にフルバックアップになります。フルバックアップを実行した後、それ以降のすべてのバックアップ (フル、増分、検証) はスケジュールどおりに実行されます。
- d. コピーされる復旧ポイントも暗号化するには、以下の情報を入力します。
- 復旧ポイントのコピー用の暗号は変更、追加、削除することができます。
- コピーに使用される暗号化アルゴリズムの種類を選択します。
利用可能なオプションは、暗号化なし、AES-128、AES-192、および AES-256 です
 - 暗号化パスワードを提供 (および確認) します。
9. [コピーの作成] をクリックします。

ステータスの通知画面が表示され、選択した種類の復旧ポイントのコピー処理がすぐに開始されます。

注: CA ARCserve D2D では、同時に実行できる復旧ポイントのコピージョブは 1 つだけです。

復旧ポイントイメージが、バックアップソースからコピー先にコピーされます。

CA ARCserve Central Host-Based VM Backup からの VHD ファイルの作成

この CA ARCserve D2D 手順では、バックアップが成功するたびに作成される復旧ポイントから仮想ハードディスク (VHD) ファイルを作成できます。詳細については、付録の CA ARCserve D2D の項目を参照してください。

次の手順に従ってください:

1. [復旧ポイントのコピー](#) (P. 77) 手順を実行します。
2. コピーが完了したら、指定したデスティネーションを参照し、CA ARCserve D2D ホストに移動します。
3. フォルダ VStore¥\$0000000001 を開きます。
4. 拡張子が「D2D」のファイルをすべて確認し、それぞれ「VHD」に変更します。すべてのファイル名を変更したら、標準の VHD ファイルとして使用できます。

アプリケーションレベルバックアップの実行

通常、Microsoft Exchange または SQL Server システムを保護するの必要な手順は特にありません。しかし、障害発生時のリストア方法によっては、いくつかのオプションを有効にします。

たとえば、[バックアップ設定/拡張] 画面上で [Exchange 詳細カタログ] オプションを有効にすると、後で特定のメールボックスまたは個別の電子メールメッセージを復旧できます。また、Windows エクスプローラからフォルダまたは電子メールメッセージを直接リストアできます。

フルアプリケーションバックアップを実行するには、以下のポイントが確認されている必要があります。

- すべてのアプリケーションライタが安定した状態にある。ライタのステータスを参照するには *vssadmin* を使用します。
- バックアップされるすべてのデータベースに問題がない。たとえば SQL Server の場合、データベースステータスが「リストア中」ではないことを確認します。

また、SQL Server と Exchange Server 用のトランザクションログを別々に切り捨てることもできます。

注: ESX Server にアップグレードする場合、「期限切れ」エラーを回避するために、ゲストオペレーティングシステムで VMware Tools をアップグレードしてから、アプリケーションレベルのバックアップを実行する必要があります。

使用済みブロックデータのみを含むフル ディスク バックアップの実行

フルディスク バックアップを実行した後に使用済みブロック データを取得すると、バックアップ ウィンドウが短縮され、バックアップ先の空き容量の要件を削減することができます。

注: VMware の制限のため、復旧ポイント スナップショットが存在する場合、使用済みブロックは仮想マシンから取得できません。そのような場合、仮想マシン上でフルディスク バックアップが実行されます。

フル ディスク バックアップがサブミットされた後、以下の手順に従って使用済みブロック データを取得します。

1. 仮想マシンに関連付けられているスナップショットをすべて削除します。
2. CA ARCserve Central Host-Based VM Backup 仮想マシンにログインします。
3. レジストリ エディタ を開き、以下のキーを探します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve  
D2D\AFBackupDll\VM_InstanceUUID<UUID>
```

4. レジストリ キー "full disk backupForFullBackup" を 0 に設定します。
5. レジストリ "ResetCBT" (存在しない場合は作成) を 1 に設定します。
6. バックアップ ジョブをサブミットします。

ジョブ ステータス情報の参照

CA ARCserve Central Virtual Standby は CA ARCserve D2D 復旧ポイントを復旧ポイント スナップショットに変換します。進行中の Host-Based VM Backup ジョブに関するステータス情報を表示できます。

ジョブの実行時に、そのジョブに関する詳細情報を表示できます。また、現在のジョブを停止できます。

次の手順に従ってください:

1. アプリケーションにログインします。
2. ナビゲーションバー上の [ノード] をクリックして、[ノード] 画面を開きます。

3. 進行中の Host-Based VM Backup ジョブがある場合、ジョブのフェーズが以下の画面に示されるように、[ジョブ] フィールドに表示されます。

<input type="checkbox"/>	ノード名	ポリシー	仮想マシン名	vCenter/ESX	ジョブ
<input checked="" type="checkbox"/>	<ノード名>	新規ポリシー	<仮想マシン名>	*****	 バックアップ開始中

4. フェーズをクリックして、[バックアップ ステータス モニタ] ダイアログ ボックスを開きます。

注: バックアップ ステータス モニタに表示されるフィールドの詳細については、「[バックアップ ステータス モニタ](#)」を参照してください。
(P. 84)

5. 以下のいずれかのオプションを実行します。
 - [閉じる] をクリックして、[バックアップ ステータス モニタ] ダイアログ ボックスを閉じます。
 - [キャンセル] をクリックして、現在のジョブを停止します。

注: [キャンセル] をクリックするとすぐに、[バックアップ ステータス モニタ] ダイアログ ボックスが閉じます。

詳細情報:

[ジョブ ステータス情報の参照](#) (P. 83)

Host-Based VM Backup モニタリング タスク

仮想マシンバックアップのステータスを [ノード] 画面から参照することができます。 [ジョブ] フィールドからの進行中のジョブがあるノードを検索し、そのリンクをクリックします。すると、このダイアログ ボックスが開きます。

仮想マシンバックアップは2つのフェーズで実行されます。まず、仮想ハードディスクがバックアップされます。操作が正常に終了すると、カタログが生成されます。このカタログによって、ファイルおよびフォルダ、仮想マシン全体をリストアできます。

モニタに、バックアップ ステータス ジョブに関する以下のリアルタイム情報が表示されます。

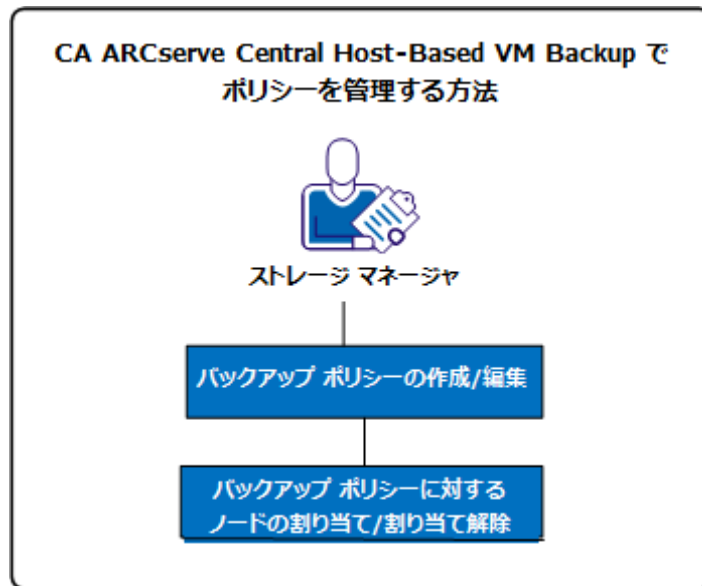
- **フェーズ** -- (バックアップおよびカタログ モニタ) プロセスにおける現在の段階が、プログレスバーの塗りつぶされた部分で示されます。
- **開始時刻** -- (バックアップおよびカタログ モニタ) ポリシー設定に基づいて処理が開始された日時を表示します。
- **経過時間** -- (バックアップおよびカタログ モニタ) 開始時間と現在の時間との差を表示します。
- **推定残り時間** -- (バックアップ モニタのみ) ジョブの完了に必要と予測される時間を表示します。
- **処理中** -- (カタログ モニタのみ) 現在カタログを生成しているボリュームのドライブ文字またはアプリケーションを表示します。
- **圧縮による削減容量** -- (バックアップ モニタのみ) バックアップ処理ポリシーで圧縮が指定されている場合、節約されるディスク容量を表示します。
- **圧縮レベル** -- (バックアップ モニタのみ) バックアップに使用される圧縮の種類を表示します。オプションは [圧縮なし]、[標準圧縮] (デフォルト) または [最大圧縮] です。
- **暗号化** -- (バックアップ モニタのみ) バックアップジョブの設定時に選択された暗号化方式を表示します。
- **書き込み速度制限** -- (バックアップ モニタのみ) バックアップポリシーの [保護設定] 画面でスロットルバックアップが設定された場合の値を表示します。
- **書き込み速度** -- (バックアップ モニタのみ) 実際の書き込み速度を分あたりの MB 数で表示します。
- **読み取り速度** -- (バックアップ モニタのみ) 実際の読み取り速度を分あたりの MB 数で表示します。

CA ARCserve Central Host-Based VM Backup 用ポリシーの管理方法

バックアップポリシーは、vCenter/ESX Server からインポートされるノードをバックアップする方法およびタイミングを定義します。ストレージマネージャはバックアップポリシーを作成および編集し、次に、ノードに割り当て、または割り当て解除します。

注: 1つのポリシーを1つ以上のノードへ割り当てることができます。ただし、1つ以上のポリシーを1つのノードに割り当ててはできません。

以下の図は、バックアップポリシーの管理プロセスを示しています。



以下のリストでは、図に示されているプロセスについて説明します。

- [バックアップポリシーの作成](#) (P. 87)
- [バックアップポリシーの編集](#) (P. 91)
- [バックアップポリシーのノードの割り当てと割り当て解除](#) (P. 94)

バックアップポリシーの作成

バックアップポリシーの作成プロセスでは、バックアップ設定用の CA ARCserve D2D インターフェースを使用しますが、若干の違いがあります。同様のバックアップニーズに基づいてポリシーを作成できます。たとえば、インストール済みのアプリケーション別、あるいはスケジュール別などです。

以下のプロセスは、単純な CA ARCserve D2D バックアップジョブポリシーの作成に必要な手順の概要を示しています。CA ARCserve D2D バックアップポリシーの作成に関する詳細については、付録の該当する CA ARCserve D2D トピックを参照してください。

注: 転送モードとして「ホット追加」を使用している場合は、ホストベースのバックアップ中に以下の内容のメッセージが表示されます。

ドライブ <ドライブ文字> を使用するには、ディスクをフォーマットする必要があります。フォーマットしますか?

[キャンセル] をクリックしてこのメッセージを無視します。仮想ハードディスクがバックアッププロキシサーバに追加されたことをオペレーティングシステムが検出すると、メッセージが発生します。オペレーティングシステムは、仮想ハードディスクがフォーマットを必要とする新しいデバイスであるとみなします。該当する [ディスクのフォーマット] をクリックしても、仮想ハードディスクは読み取り専用であるため問題は発生しません。

次の手順に従ってください:

1. アプリケーションにログインします。
ナビゲーションバーの [ポリシー] をクリックして、[ポリシー] 画面を開きます。
2. ツールバー上の [新規] をクリックして、[新規ポリシー] ダイアログボックスを開きます。
3. ポリシーを適切に説明する [ポリシー名] を入力します。

4. [バックアップ設定] タブで、[保護設定] をクリックし、以下の情報を指定します。
 - **バックアップ先** -- バックアップセッションが保存されるローカルボリュームまたはリモート共有フォルダを指定します。
 - **CA ARCserve D2D VM バックアップ プロキシ** -- CA ARCserve D2D がインストールされているサーバのホスト名または IP アドレスを指定します。CA ARCserve D2D がすでにインストールされていない場合、展開に CA ARCserve Central Protection Manager を使用できます。このサーバの適切な認証情報を提供します。ポート番号のデフォルトは 8014 です。CA ARCserve D2D インストール時にこのデフォルトを変更した場合は、正しいポート番号を指定します。
 - **保存設定** -- 保存する復旧ポイントの数（セッションをマージ）または保存する復旧セットの数（復旧セットを削除し、無限増分バックアップを無効化）に基く保存ポリシーを設定できます。デフォルトのオプションは [復旧ポイントの保持] です。詳細については、「CA ARCserve Central Protection Manager ユーザガイド」の「保護設定の指定」を参照してください。
 - **圧縮** -- 圧縮レベルを選択します。デフォルト値は「標準圧縮」です。[圧縮なし] や [最大圧縮] を選択することはできません。
 - **暗号化** -- 暗号化レベルを指定します。デフォルト値は「暗号化なし」です。暗号化レベルを指定する場合、暗号化データのリストアに使用される暗号化パスワードを提供します。
 - **スロットルバックアップ** -- バックアップがディスクに書き込まれる速度を入力します。CPU またはネットワークの負荷を軽減するにはこの値を低くしますが、そうするとバックアップ時間は増加します。このオプションは、デフォルトで無効になっています。

5. [スケジュール] をクリックし、以下の情報を入力します。
 - **開始日時** -- バックアップ ジョブを開始する日付および時間を指定します。
 - **増分バックアップ** -- 増分バックアップ ジョブ用の繰り返しスケジュールを定義します。デフォルトでは、増分バックアップを1日に1回繰り返します。
 - **フルバックアップ** -- フルバックアップ ジョブ用の繰り返しスケジュールを定義します。デフォルトでは、この値は繰り返さないように設定されています。
 - **検証バックアップ** -- 検証バックアップ ジョブ用の繰り返しスケジュールを定義します。デフォルトでは、この値は繰り返さないように設定されています。
6. [拡張] をクリックし、アプリケーション ログ ファイルを切り捨てる場合は、以下のオプションを有効にします。
 - **SQL Server** -- 毎日、毎週、毎月の切り捨てスケジュールを指定します。
 - **Exchange Server** -- 毎日、毎週、毎月の切り捨てスケジュールを指定します。
7. [バックアップの実行前/後の設定] をクリックし、必要な実行前/後のバックアップ コマンドを指定します。必要に応じて適切な認証情報を提供します。
 - **バックアップ開始前にコマンドを実行する** -- バックアップ ジョブを開始する前に実行するスクリプト コマンドを入力します。
 - **終了コード** -- 特定の終了コードでスクリプト コマンドをトリガする場合は、このオプションを有効にします。
 - **ジョブを続行** -- 選択された場合、指定された終了コードが返されるとジョブの実行が続行されます。
 - **ジョブを中止** -- 選択された場合、指定された終了コードが返されるとバックアップ ジョブの実行が中止されます。
 - **スナップショット取得後にコマンドを実行する** -- スナップショットの取得後に実行するスクリプト コマンドを入力します。
 - **バックアップ完了後にコマンドを実行する** -- バックアップの完了後に実行するスクリプト コマンドを入力します。

8. (オプション) [環境設定] タブをクリックします。必要に応じて、以下の電子メールアラートを設定します。

- ジョブが失敗
- vCenter/ESX にアクセスできない (バックアップ前)
- ライセンスエラー
- ジョブのバックアップ、カタログ、リストアまたはコピーの失敗/クラッシュ/キャンセル
- ジョブのバックアップ、カタログ、リストアまたはコピーの成功
- デスティネーションの空き容量が次の値を下回った場合
- マージエラー

注: マージ失敗は、以下の理由で発生する場合があります。

- セッションがマウントされている。
この問題を解決するには、セッションをマウント解除します。
- カタログジョブがセッションをロックしている。
このセッションは、次のバックアップジョブによって自動的にマージされます。
- セッションが他の理由でロックされている。

- ジョブキュー内の待機ジョブのスキップ/マージ

これらのオプションを有効にする場合、[電子メールの設定]をクリックし、電子メールサーバを設定します。サービスの種類、メールサーバ、およびポートを指定します。認証が必要な場合は、オプションを有効にして認証情報を指定します。

- 電子メールに表示される件名を指定します (例: CA ARCserve Central Host-Based VM Backup アラート)。
- 送信者の値を指定します (例: CA ARCserve Central Host-Based VM Backup)。
- すべての受信者の電子メールアドレスを指定します。各アドレスは、セミコロン (;) で区切ります。

プロキシサーバ名、ポートおよび必要な認証情報指定することで、[プロキシ設定] を有効にできます。

[OK] をクリックします。

9. [保存] をクリックします。

バックアップポリシーの編集またはコピー

CA ARCserve Central Host-Based VM Backup では、CA ARCserve D2D バックアップポリシーを作成後に編集またはコピーすることができます。

次の手順に従ってください:

1. アプリケーションにログインします。
ナビゲーションバーの [ポリシー] をクリックして、[ポリシー] 画面を開きます。
2. [ポリシー] 画面でポリシーの隣のチェックボックスをオンにし、以下のいずれかを実行します。
 - ツールバー上の [編集] をクリックし、選択したポリシーを編集します。
 - ツールバー上の [コピー] をクリックし、選択したポリシーから新規ポリシーをコピーして作成します。
注: ポリシーをコピーする際、[ポリシーのコピー] ダイアログボックスが表示されます。新しいポリシーの名前を指定し、[OK] ボタンをクリックします。
[ポリシーの編集] ダイアログボックスが開きます。
3. ポリシー名を変更する場合は、[ポリシー名] フィールドで名前を指定します。

4. [バックアップ設定] タブで、[保護設定] をクリックし、以下の情報を指定します。
 - **バックアップ先** -- バックアップセッションが保存されるリモート共有フォルダを指定します。
 - **CA ARCserve D2D VM バックアップ プロキシ** -- CA ARCserve D2D がインストールされているサーバのホスト名または IP アドレスを指定します。CA ARCserve D2D がすでにインストールされていない場合、展開に CA ARCserve Central Protection Manager を使用できます。このサーバの適切な認証情報を提供します。ポート番号のデフォルトは 8014 です。CA ARCserve D2D インストール時にこのデフォルトを変更した場合は、正しいポート番号を指定します。
 - **保存設定** -- 保存する復旧ポイントの数（セッションをマージ）または保存する復旧セットの数（復旧セットを削除し、無限増分バックアップを無効化）に基く保存ポリシーを設定できます。デフォルトのオプションは [復旧ポイントの保持] です。詳細については、「CA ARCserve Central Protection Manager ユーザガイド」の「保護設定の指定」を参照してください。
 - **圧縮** -- 圧縮レベルを選択します。デフォルト値は「標準圧縮」です。[圧縮なし] や [最大圧縮] を選択することはできません。
 - **暗号化** -- 暗号化レベルを指定します。デフォルト値は「暗号化なし」です。暗号化レベルを指定する場合、暗号化データのリストアに使用される暗号化パスワードを提供します。
 - **スロットルバックアップ** -- バックアップがディスクに書き込まれる速度を入力します。CPU またはネットワークの負荷を軽減するにはこの値を低くしますが、そうするとバックアップ時間は増加します。このオプションは、デフォルトで無効になっています。

5. [スケジュール] をクリックし、以下の情報を入力します。
 - **開始日時** -- バックアップ ジョブを開始する日付および時間を指定します。
 - **増分バックアップ** -- 増分バックアップ ジョブ用の繰り返しスケジュールを定義します。デフォルトでは、増分バックアップを1日に1回繰り返します。
 - **フルバックアップ** -- フルバックアップ ジョブ用の繰り返しスケジュールを定義します。デフォルトでは、この値は繰り返さないように設定されています。
 - **検証バックアップ** -- 検証バックアップ ジョブ用の繰り返しスケジュールを定義します。デフォルトでは、この値は繰り返さないように設定されています。
6. [拡張] をクリックし、アプリケーション ログ ファイルを切り捨てる場合は、以下のオプションを有効にします。
 - **SQL Server** -- 毎日、毎週、毎月の切り捨てスケジュールを指定します。
 - **Exchange Server** -- 毎日、毎週、毎月の切り捨てスケジュールを指定します。

7. [バックアップの実行前/後の設定] をクリックし、必要な実行前/後のバックアップ コマンドを指定します。必要に応じて適切な認証情報を提供します。
 - **バックアップ開始前にコマンドを実行する** --バックアップ ジョブを開始する前に実行するスクリプト コマンドを入力します。
 - **終了コード** -- 特定の終了コードでスクリプト コマンドをトリガする場合は、このオプションを有効にします。
 - **ジョブを続行** -- 選択された場合、指定された終了コードが返されるとジョブの実行が続行されます。
 - **ジョブを中止** -- 選択された場合、指定された終了コードが返されるとバックアップ ジョブの実行が中止されます。
 - **スナップショット取得後にコマンドを実行する** -- スナップショットの取得後に実行するスクリプト コマンドを入力します。
 - **バックアップ完了後にコマンドを実行する** --バックアップの完了後に実行するスクリプト コマンドを入力します。
8. (オプション) [環境設定] タブをクリックします。必要に応じて、電子メールアラートを設定します。これらのオプションを有効にする場合、[電子メールの設定] をクリックし、電子メールサーバを設定します。
9. [保存] をクリックします。

ポリシーが編集またはコピーされます。

バックアップ ポリシーのノードの割り当てと割り当て解除

複数の仮想マシンを保護するには、使用するポリシーを選択し、それを1つ以上のノードに割り当てます。

次の手順に従ってください:

1. アプリケーションにログインします。

ナビゲーションバーの [ポリシー] をクリックして、[ポリシー] 画面を開きます。
2. [ポリシー] 画面で [ポリシーの割り当て] タブをクリックします。

3. [ポリシー] リストから、割り当てるポリシーを選択します。
[割り当てと割り当て解除] をクリックし、[ポリシーの割り当て/割り当て解除] ダイアログ ボックスを開きます。
 4. [ポリシーの割り当て/割り当て解除] ダイアログ ボックスから以下のフィールドを指定します。
 - **グループ** -- 割り当てるノードが含まれているグループの名前を選択できます。
 - **ノード名フィルタ** -- 共通の条件に基づいて利用可能なノードをフィルタ処理できます。
注: [ノード名] フィールドでは、ワイルドカード文字を使用してノードのフィルタリングを行えます。
たとえば、**Acc*** は、ノード名が「Acc」で始まるすべてのノードをフィルタ処理できます。フィルタ結果をクリアするには、[フィルタ] フィールドで **X** をクリックします。
 5. 以下のいずれかの操作を実行します。
 - **ポリシーへのノードの割り当て** -- 追加するノードを選択して、右矢印をクリックします。
ノードが [利用可能なノード] リストから [選択されたノード] リストに移動します。
注: ノードをすべて選択し移動させるには、二重右矢印をクリックします。
 - **ポリシーからのノードの割り当て解除** -- 割り当てを解除するノードを選択して左矢印をクリックします。
ノードが [選択されたノード] リストから [利用可能なノード] リストに移動します。
注: ノードをすべて選択し移動させるには、二重左矢印をクリックします。
- [OK] をクリックします。

- 必要に応じて、グローバルユーザ名およびパスワードを提供し、選択したノードに適用します。

[OK] をクリックします。

選択したノードが [ポリシーの割り当て] リストに追加され、展開ステータスは [割り当て済み] / [保留中] になります。

注: [ノード] 画面上で展開ステータスを表示することもできます。

- [今すぐ展開] をクリックすると、割り当てられたポリシーが指定されたノードにすぐに適用されます。 [更新] ボタンを使用してステータスを更新します。

[ノード] 画面では、 [ポリシーの割り当て] リストで指定したノードのステータスが、 [ポリシー] 列の割り当てられたポリシーに表示されます。

[ノード名] をクリックし、 [D2D にログイン] をクリックしてバックアップジョブのステータスを確認します。

CA ARCserve Central Host-Based VM Backup ログの表示

ログには、アプリケーションによって実行されたすべての処理の包括的な情報が記録されます。このログは、実行されたすべてのジョブの監査記録になります（最も最近のアクティビティがリストの最初に表示されません）。発生した問題をトラブルシューティングする際に役立ちます。

CA ARCserve Central Host-Based VM Backup ログを表示する方法

- ホーム画面から、ナビゲーションバーの [ログの表示] をクリックします。

[ログの表示] 画面が表示されます。

- ドロップダウンリストから、表示するログ情報を指定します。

- **重大度** -- 表示するログの重大度を指定します。以下の重大度オプションを指定できます。

- **すべて** -- 重大度にかかわらず、すべてのログを表示します。

- **情報** -- 一般的な情報を説明するログのみを表示します。

- **エラー** -- 発生したエラーを説明するログのみを表示します。

- **警告** -- 発生した警告を説明するログのみを表示します。

- **エラーと警告** -- 発生したエラーおよび警告のみを表示します。

- **モジュール** -- ログを表示するモジュールを指定します。以下のモジュール オプションを指定できます。
 - **すべて** -- すべてのアプリケーション コンポーネントに関するログを表示します。
 - **共通** -- 共通のプロセスに関するログを表示します。
 - **オート ディスカバリからのノードのインポート** -- オート ディスカバリからインポートされたノードのログのみを表示します。
 - **ハイパーバイザからのノードのインポート** -- ハイパーバイザからインポートされたノードのログのみを表示します。
 - **ポリシー管理** -- ポリシーの管理に関するログのみを表示します。
 - **更新** -- アプリケーションの更新に関するログのみを表示します。
 - **プレフライトチェック** -- 各ノードのプレフライトチェック ステータスを実行したログのみを表示します。
 - **VM バックアップ ジョブのサブミット** -- ノードが仮想マシン バックアップ ジョブに対してサブミットされたログのみを表示します。
- **ノード名** -- 特定のノードのログのみを表示します。

注: このフィールドではワイルドカード ('*' および '?') がサポートされます。たとえば、「lod*」と入力すると、'lod' で始まるマシン名のすべてのアクティビティ ログが返されます。

注: 重大度、モジュール、ノード名のオプションはまとめて適用できます。たとえば、「ノード X」（ノード名）の「更新」（モジュール）に関連する「エラー」（重大度）を表示するよう指定できます。

指定された表示オプションに基づいてログが表示されます。

注: ログに表記される時刻は、アプリケーションのデータベース サーバのタイムゾーンに従います。

特定ノードのアクティビティ ログ情報の表示

CA ARCserve Central Host-Based VM Backup では、特定の CA ARCserve D2D ノード用のアクティビティ ログ情報を表示することができます。アクティビティ ログは、実行されたすべてのジョブの監査記録になります（最も最近のアクティビティがリストの最初に表示されます）。発生した問題をトラブルシューティングする際に役立ちます。

特定ノードのアクティビティ ログ情報を表示する方法

1. アプリケーションを開いて、ナビゲーションバーの [ノード] をクリックします。

[ノード] 画面が表示されます。

2. グループリストから [すべてのノード] をクリックするか、またはログインする CA ARCserve D2D ノードが含まれるグループをクリックします。

ノードリストに、指定したグループと関連付けられているノードがすべて表示されます。

3. ログインするノードを探してクリックし、ポップアップメニューから [D2D にログイン] をクリックします。

CA ARCserve D2D が開き、CA ARCserve D2D ノードのホーム画面にログインします。

注: 新しいブラウザ ウィンドウが表示されない場合は、ブラウザのポップアップ オプションですべてのポップアップ、あるいはこの Web サイトのポップアップのみ許可されていることを確認します。

4. [タスク] リスト上の [ログの表示] をクリックします。
以下に示すように、アクティビティログが開きます。



アクティビティログは以下の情報を提供します。

- **種類** -- アクティビティの重大度を指定します。情報、警告、エラーが含まれます。
 - **ジョブ ID** -- アクティビティが適用されるジョブを指定します。
 - **時刻** -- アクティビティが適用される日付および時刻を指定します。
 - **メッセージ** -- アクティビティを説明します。
5. [OK] をクリックしてアクティビティログを閉じます。

ナビゲーションバーへのリンクの追加

CA ARCserve Central Applications には、ナビゲーションバーに [新しいタブの追加] リンクがあります。管理する Web ベース アプリケーションを追加した場合などは、この機能を使用してナビゲーションバーにエントリーを追加できます。ただし、インストールされたすべてのアプリケーションについては、ナビゲーションバーに新しいリンクが自動的に追加されます。たとえば、CA ARCserve Central Reporting および CA ARCserve Central Virtual Standby をコンピュータ A にインストールし、CA ARCserve Central Reporting を起動した場合、CA ARCserve Central Virtual Standby が自動的にナビゲーションバーに追加されます。

注: 他の CA ARCserve Central Applications が同じコンピュータ上にある場合のみ、インストールされたすべてのアプリケーションが検出されます。

次の手順に従ってください:

1. アプリケーションのナビゲーションバーで [新しいタブの追加] リンクをクリックします。
2. 追加するアプリケーションまたは Web サイトの名前および URL を指定します。たとえば www.google.com などです。
必要に応じてアイコンの場所を指定します。
3. [OK] をクリックします。
新しいタブはナビゲーションバーの下部に追加されます。

以下の点に注意してください。

- CA サポート リンクは、ユーザの便宜のためにデフォルトで追加されています。

新しいタグを削除するには、タブをハイライトして [削除] リンクをクリックします。

CA ARCserve Central Host-Based VM Backup と CA ARCserve Central Applications との統合

CA ARCserve Central Protection Manager および CA ARCserve Central Reporting をインストールした場合、ホストベースのバックアップのステータスを一元的にモニタできます。

raw デバイス マッピング保護のための考慮事項

raw デバイス マッピング (RDM) を保護する場合は以下の動作を考慮する必要があります。

- アプリケーションでは物理互換モードの raw デバイス マッピングの保護をサポートしません(この種類のディスクは物理デバイスです)。アプリケーションではバックアップ処理中にバックアップソースから物理互換モードの raw デバイス マッピングを省略します。この動作に対する解決策は、ゲストオペレーティングシステム内に CA ARCserve D2D をインストールし、物理ディスクをバックアップするのと同じ方法でバックアップを実行することです。
- アプリケーションでは仮想互換モードの raw デバイス マッピングの保護をサポートします。ただし、以下の点に留意してください。
 - フルバックアップの場合、完全な仮想互換モードの RDM ディスクをバックアップできます。ただし、データ圧縮を使用しないと、バックアップデータセットがソースディスクと同じサイズになる場合があります。
 - CA ARCserve Central Host-Based VM Backup は仮想互換モード RDM ディスクを通常の仮想ディスクとしてリストアします。復旧処理が完了した後、ディスクは仮想 RDM としての設定も動作も行われなくなります。
 - 仮想互換モードの RDM をバックアップする別の方法としては、ゲストオペレーティングシステム内に CA ARCserve D2D をインストールし、物理マシンをバックアップするのと同じ方法で RDM をバックアップします。

サーバの通信プロトコルの変更

デフォルトでは、CA ARCserve Central Applications は、すべてのコンポーネント間の通信に Hypertext Transfer Protocol (HTTP) を使用します。コンポーネント間でやり取りされるパスワードのセキュリティを強化したい場合は、使用するプロトコルを Hypertext Transfer Protocol Secure (HTTPS) に変更することもできます。それほどレベルのセキュリティが必要でない場合は、使用するプロトコルを簡単に HTTP に戻すことができます。

次の手順に従ってください:

1. 管理者アカウントまたは管理者権限のあるアカウントを使用して、アプリケーションがインストールされているコンピュータにログインします。

注: 管理者アカウントまたは管理者権限を持つアカウントを使用してログインしない場合、コマンドラインが [管理者として実行] 権限で実行されるよう設定します。

2. Windows のコマンドラインを開きます。
3. 以下のいずれかを行います。

- **プロトコルを HTTP から HTTPS に変更:**

以下のデフォルトの場所から `changeToHttps.bat` ユーティリティツールを起動します (BIN フォルダの場所は、アプリケーションをインストールした場所に応じて異なります)。

`C:\Program Files\CA\ARCserve Central Applications\BIN`

プロトコルが正常に変更されると、以下のようなメッセージが表示されます。

通信プロトコルは HTTPS に変更されました。

- **プロトコルを HTTPS から HTTP に変更:**

以下のデフォルトの場所から `changeToHttp.bat` ユーティリティツールを起動します (BIN フォルダの場所は、アプリケーションをインストールした場所に応じて異なります)。

C:\Program Files\CA\ARCserve Central Applications\BIN

プロトコルが正常に変更されると、以下のようなメッセージが表示されます。

通信プロトコルは HTTP に変更されました。

4. ブラウザを再起動し、CA ARCserve Central Applications に再接続します。

注: プロトコルを HTTPS に変更した場合、Web ブラウザに警告が表示されます。この動作は、自己署名されたセキュリティ証明書が原因で発生します。警告を無視して続行するか、その証明書をブラウザに追加して今後同じ警告が発生しないようにします。

バックアップの転送モードの定義

Host-Based VM Backup を使用して実行する D2D バックアップジョブの転送モード（データ転送）を定義できます。Host-Based VM backup がデフォルトで使用するモードでは、バックアップ処理のパフォーマンスが最適化（速度を増加）されます。ただし、バックアップ処理用に特定の転送モードを指定する場合は、このトピックに述べられているようにレジストリキーを設定する必要があります。

Host-Based VM Backup は、以下の転送モードを使用して、バックアップを実行できます。

- [HOTADD 転送モード](#) (P. 291)
- [NBD 転送モード](#) (P. 291)
- [NBDSSL 転送モード](#) (P. 291)
- [SAN 転送モード](#) (P. 291)

以下の点に注意してください。

- この環境設定タスクは省略可能です。デフォルトでは、Host-Based VM Backup は、バックアップ処理のパフォーマンスを最適化する転送モードを使用して、バックアップを実行します。
- 特定の転送モードを使用するためにこのレジストリキーを設定しても、そのモードが利用可能でない場合は、Host-Based VM Backup は、利用可能なデフォルトの転送モードでバックアップ処理を行います。

次の手順に従ってください:

1. 仮想マシン用の CA ARCserve D2D バックアッププロキシシステムにログインします。

Windows レジストリ エディタ を開き、以下のキーを探します。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA_ARCSERVE  
D2D\AFBackupDll\{VM-InstanceUUID}]
```

2. VM-InstanceUUID を右クリックし、コンテキストメニューで [新規] - [文字列値] をクリックします。

新しい文字列値は以下に設定します。

EnforceTransport

3. 「EnforceTransport」を右クリックし、コンテキストメニューメニューで [変更] をクリックし、[文字列の編集] ダイアログボックスを開きます。
4. [値データ] フィールドで、バックアップジョブで使用する転送モードを指定します。以下のいずれかの値を指定します。

hotadd

[HOTADD 転送モード](#) (P. 291)

nbd

[NBD 転送モード](#) (P. 291)

nbdssl

[NBDSSL 転送モード](#) (P. 291)

san

[SAN 転送モード](#) (P. 291)

5. [OK] をクリックして値を適用し、[文字列の編集] ダイアログボックスを閉じます。

転送モードが定義され、次回のジョブ実行時に使用されます。

第 4 章: 仮想マシンのリストアおよび復旧

使用可能なリストアと復旧のオプションは、システムのバックアップ方法に応じて変わります。たとえば、CA ARCserve Central Host-Based VM Backup で作成されたバックアップセッションを使用してアプリケーションレベルまたは Microsoft Exchange の詳細リストア操作を実行することはできませんが、CA ARCserve Central Protection Manager または CA ARCserve D2D で作成されたセッションを使用してそれを行うことは可能です。CA ARCserve D2D で利用できるリストア オプションの中には、このアプリケーションで利用できないものがあります。たとえば、[元の場所にリストアする] はこのアプリケーションのバックアップで利用できません。これは、プロキシサーバの場所がバックアップソースの仮想マシンの場所と異なるからです。

詳細については、「[リストアの考慮事項 \(P. 118\)](#)」を参照し、ニーズに適した[リストア方式 \(P. 106\)](#)を選択するのに役立ててください。

このセクションには、以下のトピックが含まれています。

[リストア方式 \(P. 106\)](#)

[リストアの考慮事項 \(P. 118\)](#)

[アプリケーションレベルリストア \(P. 119\)](#)

リストア方式

バックアップセッションがどのように作成されたかによって、使用可能なリストア方式が決まります。たとえば、一部のリストア方式は、ローカルにインストールされた CA ARCserve D2D のバージョンで実行される場合にのみ使用可能です。一部の方式では、バックアップ時に仮想マシンの電源がオンになっている必要があります。

復旧ポイントの参照

利用可能な復旧ポイント（正常に完了したバックアップ）をカレンダー表示から検索できます。この方式を使用して、ファイルやフォルダをリストアするか、またはアプリケーション レベル リストア プロセスを実行します。

CA ARCserve D2D、CA ARCserve Central Host-Based VM Backup、または CA ARCserve Central Protection Manager で作成されたバックアップは、この方式でリストアできます。

リストアするファイル/フォルダの検索

リストアする特定のファイルまたはフォルダを検索します。

CA ARCserve D2D で作成されたバックアップはこの方式でリストアできます。また、バックアップ時に仮想マシンの電源がオンになっていた場合は、CA ARCserve Central Host-Based VM Backup および CA ARCserve Central Protection Manager で作成されたバックアップをリストアすることもできます。

VM の復旧

利用可能なすべての仮想マシン復旧ポイント（正常に完了したバックアップ）をカレンダー表示から参照できます。次に、回復する仮想マシンを指定できます。

この方式は、CA ARCserve Central Host-Based VM Backup で作成されたバックアップのリストアに使用可能です。最初に仮想マシンのプロビジョニングを行い、指定した復旧ポイントから OS、アプリケーション、データをリストアします。

アプリケーションのリストア

Microsoft Exchange または SQL Server を再構築する必要なしに完全に回復するには、CA ARCserve D2D のローカルにインストールされたバージョンからの [復旧ポイントの参照] 方式をクリックします。

ベアメタル復旧

ベアメタル復旧 (BMR) は、ベアメタルからコンピュータを回復するプロセスです。これには、そのオペレーティングシステム、ソフトウェアアプリケーション、設定、およびデータが含まれます。BMR では、Windows イメージまたはブートキットと、少なくとも 1 つのフルバックアップが必要です。CA ARCserve D2D、CA ARCserve Central Host-Based VM Backup、CA ARCserve Central Virtual Standby、および CA ARCserve Central Protection Manager で作成されたバックアップは、この方式でリストアできます。ただし、バックアップ時に仮想マシンの電源がオフになっていた場合、BMR を実行することはできません。

復旧ポイントからのリストア

復旧ポイントの参照方式では、成功したバックアップ (保存された復旧ポイント) をカレンダー表示で検索することができます。次に、リストアするコンテンツをアプリケーションも含めて参照および選択できます。復旧ポイントの参照方式によるリストアでは、CA ARCserve D2D を使用するのと同じように処理されますが、1 つだけ例外があります。仮想マシン復旧ポイントのリストアで、元の場所にリストアするオプションを使用することができません。

次の手順に従ってください:

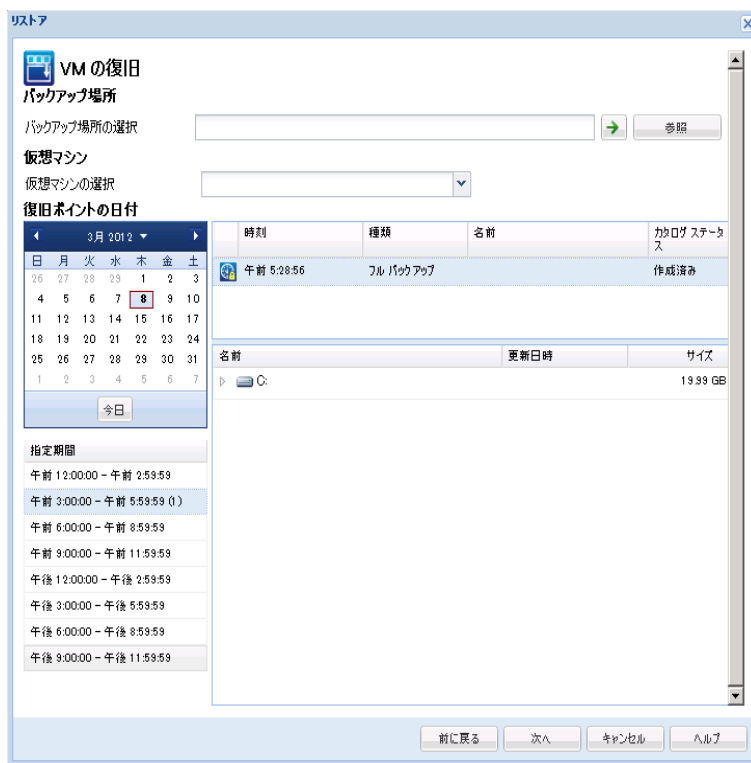
1. アプリケーションにログインし、ナビゲーションバーの [ノード] をクリックします。

[ノード] 画面から、リストアするノードが含まれるグループを展開します。

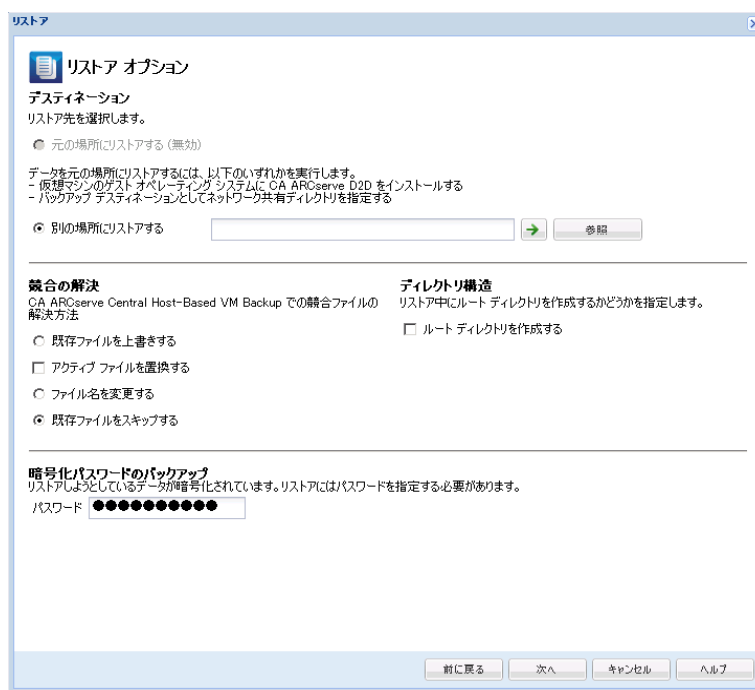
リストアするノードの横のチェックボックスをオンにしてから、ツールバー上の [リストア] をクリックします。

2. [リストア] ダイアログボックスで、[復旧ポイントの参照] をクリックします。

[リストア] ダイアログボックスが開き、選択したノードに基づいて、バックアップ場所が自動的に読み込まれます。必要に応じて別のバックアップ先に変更し、ユーザ認証情報を提供します。



3. 復旧ポイントの日付をクリックし、次に復旧ポイントの時刻をクリックします。リストアする内容を選択します。ボリューム全体、またはファイル、フォルダ、データベース、アプリケーションを選択します。選択したアイテムの横の緑色のボックスは、それがリストア対象として選択されていることを示します。終了したら、[次へ] をクリックします。



4. [リストア オプション] ダイアログ ボックスで、リストア先を指定します。
 - **元の場所にリストアする（無効）** -- CA ARCserve Central Host-Based VM Backup のセッションでは、元の場所にリストアすることはできません。ファイルまたはフォルダを VM のゲスト OS 内の元の場所にリストアするには、VM のゲスト OS に CA ARCserve D2D をインストールするか、VM 上でネットワークの共有フォルダにリストアする必要があります。
 - **別の場所にリストアする** -- リストア先の場所を指定します。
 - **既存ファイルを上書きする** -- デスティネーションにあるファイルを置換します。
 - **アクティブ ファイルを置換する** -- 再起動時に使用中またはアクセス中のファイルを置換します。
 - **ファイル名を変更する** -- ファイル名がすでに存在する場合、新規ファイルを作成します。このオプションを選択すると、ファイル名は変更せず、拡張子を変更してソース ファイルをデスティネーションにコピーします。データは新しい拡張のファイルにリストアされます。
 - **既存ファイルをスキップする** -- デスティネーションに存在する既存ファイルをスキップし、置換しません。これはデフォルトの設定です。
 - **ルート ディレクトリを作成する** -- バックアップ イメージに存在するルート ディレクトリ構造と同じものをデスティネーションに再作成します。
5. [次へ] をクリックします。[リストア サマリ] 画面で、オプションがすべて正しいことを確認します。問題があれば、[前に戻る] をクリックして修正します。問題がなければ、[完了] をクリックしてリストア プロセスを起動します。

復旧ポイントのマウントによるリストア

復旧ポイントのマウント リストア方式では、復旧ポイントをバックアッププロキシシステムへマウントできます。復旧ポイントをマウントするには、CA ARCserve D2D ユーザ インターフェースにログインする必要があります。

次の手順に従ってください:

1. CA ARCserve Central Host-Based VM Backup にログインし、ナビゲーションバーの [ノード] をクリックします。
2. [ノード] 画面から、リストアするノードが含まれるグループを展開します。

リストアするノードの横のチェック ボックスをオンにしてから、ツールバー上の [リストア] をクリックします。

CA ARCserve D2D の CA ARCserve Central Host-Based VM Backup バージョンが開きます。

注: 使用するブラウザのポップアップ オプションで、すべてのポップアップまたはこの Web サイトのポップアップのみが許可されていて、新規ウィンドウがオープンできることを確認します。

[復旧ポイントのマウント] ダイアログ ボックスの詳細については、CA ARCserve D2D ホーム ページからダイアログ ボックス画面上の [ヘルプ] をクリックしてください。

リストアするファイル/フォルダの検索を使用したデータのリストア

アプリケーションによってバックアップが正常に実行されるたびに、バックアップされたすべてのファイル/フォルダがバックアップのスナップショットイメージに含まれます。このリストア方式を使用すると、リストアするファイル/フォルダを厳密に指定できます。

次の手順に従ってください:

1. アプリケーションにログインし、ナビゲーションバーの [ノード] をクリックします。

[ノード] 画面から、リストアするノードが含まれるグループを展開します。

リストアするノードの横のチェック ボックスをオンにしてから、ツールバー上の [リストア] をクリックします。

2. [リストア] ダイアログ ボックスから、[リストアするファイル/フォルダの検索] をクリックします。

3. [リストアするファイル/フォルダの検索] ダイアログ ボックスで、バックアップ場所を指定するか、または参照して選択します。CA ARCserve Central Host-Based VM Backup セッションからリストアしている場合、[ファイル コピーの場所] を指定することはできません。ファイル コピー リストアは、CA ARCserve Central Protection Manager または CA ARCserve D2D バックアップセッションからリストアしている場合のみ許可されます。

4. リストアするファイル名またはフォルダ名を指定します。

注: [ファイル名] フィールドは、完全一致検索およびワイルドカード検索をサポートしています。完全なファイル名がわからない場合、ワイルドカード文字「*」や「?」を [ファイル名] フィールドに入力して、検索結果を簡単にすることができます。

ファイル名やフォルダ名向けにサポートされているワイルドカード文字は以下のとおりです。

- "*" -- アスタリスクは、ファイル名またはフォルダ名の 0 個以上の文字を表します。
- "?" -- 疑問符は、ファイル名またはフォルダ名の 1 個の文字を表します。

たとえば、「*.txt」と入力すると、.txt ファイル拡張子が付いたすべてのファイルが検索結果に表示されます。

5. (オプション) 検索をさらに絞り込むにはパスを指定し、サブディレクトリまたはファイル/フォルダを含めるかどうかを選択します。
6. [検索] ボタンをクリックして、検索を開始します。

検索結果が表示されます。検索によって、同一ファイルが複数存在する(復旧ポイントが複数ある)ことが検出された場合は、すべての存在が日付順に並べ替えられて(最も最近のものから)表示されます。

7. 回復するバージョンをリストから選択して[次へ]をクリックします。

[リストア オプション] ダイアログ ボックスが表示されます。別の場所へのリストアのみ実行できます。バックアップ イメージを保存する場所を指定するか、または参照して選択します。緑の矢印をクリックして接続の検証を行います。必要に応じてユーザ認証情報を提供します。

8. 競合の解消オプションを選択します。

既存ファイルを上書きする

リストア先で検出された既存ファイルを上書き(置換)します。すべてのオブジェクトが、コンピュータ上に存在しているかどうかに関わらずバックアップ ファイルからリストアされます。

アクティブ ファイルを置換する

再起動の際にアクティブ ファイルを置換します。リストア試行時に、既存ファイルが使用中またはアクセス中であることが検出された場合、ファイルはすぐには置換されません。問題の発生を避けるために、次回マシンが再起動されるまで、アクティブ ファイルの置換は延期されます(リストアはすぐに実行されますが、アクティブ ファイルの置換は次の再起動中に完了します)。

注: このオプションが選択されていない場合、アクティブ ファイルはリストアからスキップされます。

ファイル名を変更する

ファイル名が存在する場合、新規ファイルを作成します。このオプションを選択すると、ファイル名は変更せず、拡張子を変更してソース ファイルをデスティネーションにコピーします。その後、データは新規ファイルにリストアされます。

既存ファイルをスキップする

リストア先に存在する既存ファイルをスキップし、上書き（置換）はしません。現在ユーザのコンピュータ上に存在しないオブジェクトのみがバックアップファイルからリストアされます。

デフォルトでは、このオプションが選択されています。

9. （オプション）ディレクトリ構造から [ルートディレクトリを作成する] を選択します。

このオプションは、リストアデスティネーションパス上に同じルートディレクトリ構造を再作成します。

注: このオプションが選択されていない場合、ファイルまたはフォルダはデスティネーションフォルダに直接リストアされます。

10. 暗号化されたデータをリストアするためのバックアップ暗号化パスワードを入力し、[次へ] をクリックします。

[リストア サマリ] ダイアログ ボックスが表示されます。

11. 表示された情報に目を通し、リストア オプションおよび設定がすべて正しいことを確認します。
 - サマリ情報が正しくない場合は、[前に戻る] をクリックし、該当するダイアログ ボックスに戻って、正しくない設定を変更します。
 - サマリ情報が正しい場合は、[完了] ボタンをクリックし、リストア プロセスを開始します。

仮想マシン全体の復旧

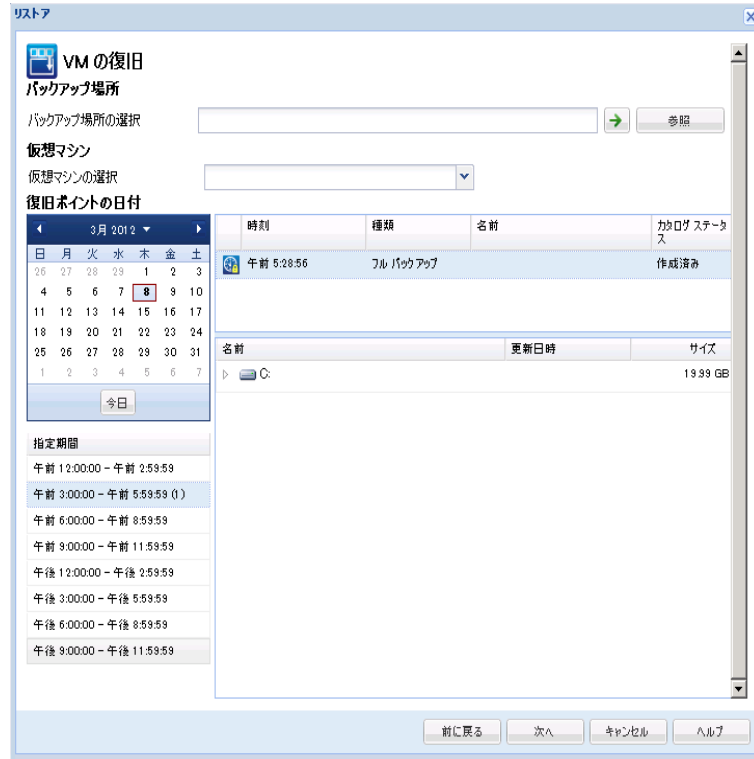
仮想マシン全体を CA ARCserve Central Host-Based VM Backup セッションから復旧します。

このバックアップ方式は BMR の実行に似ています。この方式で、Windows ゲストオペレーティングシステム、アプリケーションおよびデータを回復できます。

次の手順に従ってください:

1. アプリケーションにログインし、ナビゲーションバーの [ノード] をクリックします。
[ノード] 画面から、リストアするノードが含まれるグループを展開します。
リストアするノードの横のチェックボックスをオンにしてから、ツールバー上の [リストア] をクリックします。
2. [リストア] ダイアログボックスから、[VM の復旧] をクリックします。

3. [リストア] ダイアログボックスが表示されます。[バックアップ場所] および [仮想マシン] フィールドには、[ノード] 画面で選択した VM に基づいて値が読み込まれます。必要に応じてこれらの値を変更します。



仮想マシンバックアップセッションが保存されているソースを指定します。プロンプトが表示されたらユーザ認証情報を入力します。

ドロップダウンメニューには、[バックアップ場所] フィールドの場所にある仮想マシンがすべてリスト表示されます。

4. カレンダーから、回復する仮想マシンイメージの日付をクリックします。[指定期間] リストから、回復するバックアップイメージをクリックします。選択した内容に一致するコンテンツが参照用に表示されます。個別のボリューム、フォルダ、ファイルを選択することはできません。仮想マシン全体がリストアされます。

5. [次へ] をクリックします。[リストア オプション] ダイアログ ボックスで、デスティネーションを指定します。
 - 元の場所にリストアする -- 仮想マシンをバックアップイメージがキャプチャされた vCenter/ESX Server にリストアします。
 - 別の場所にリストアする -- 新しい場所に仮想マシンをリストアします。
6. 競合の解消および復旧後のオプションを指定します。デフォルトでは、これらのオプションは選択されていません。
 - 既存の仮想マシンに上書きする -- vCenter/ESX Server 上にある既存の仮想マシンイメージを置換します。
 - 仮想マシンの電源をオンにする -- リストア プロセスが完了した後、仮想マシンを起動します。
7. [次へ] をクリックします。プロンプトが表示されたら、バックアップソース用の vCenter/ESX Server 認証情報を入力し、[OK] をクリックします。
8. [リストア サマリ] ダイアログ ボックスで、すべてのオプションが正しいことを確認します。問題があれば、[前に戻る] をクリックして修正します。問題がなければ、[完了] をクリックして復旧プロセスを開始します。

リストアの考慮事項

以下の表は、特定の状況においてどのリストア方式を使用すべきかを判断するのに役立ちます。

リストア方式	目的	考慮事項:
復旧ポイントの参照 (アプリケーションレベルリストアを実行する場合はこの方法を使用します。) リストアするファイル/フォルダの検索	破損したファイル、フォルダ、データベース、またはアプリケーションをリストアします。	<ul style="list-style-type: none"> ■ CA ARCserve Central Host-Based VM Backup: ファイルまたはフォルダをリストアするには、バックアップ時に VM の電源がオンになっている必要があります。[元の場所にリストアする] オプションは使用できません。ネットワークドライブを元の場所にマップするか、または元の場所に共有としてアクセスし、その場所にリストアします。CA ARCserve D2D を新しい VM のゲスト OS にインストールし、アプリケーションデータベースをリストアします。詳細については、「アプリケーションレベルリストアの実行」を参照してください。 ■ CA ARCserve D2D または CA ARCserve Central Protection Manager: それぞれのアプリケーションユーザガイドを参照してください。
VM の復旧	新しい VM、OS、アプリケーション、データのプロビジョニングを行います	<ul style="list-style-type: none"> ■ CA ARCserve Central Host-Based VM Backup: 推奨されます ■ CA ARCserve D2D または CA ARCserve Central Protection Manager: サポートされていません

BMR およびアプリケーションレベルリストアのプロセスを使用して回復することもできます。詳細については、「[リストア方式](#) (P. 106)」を参照してください。

アプリケーションレベルリストア

CA ARCserve Central Applications では、データの保護および回復が可能だけでなく、そのデータを使用するアプリケーションをバックアップおよび実行することができます。アプリケーションレベルリストアは、リストア方式として復旧ポイントの参照を使用します。アプリケーションレベルリストアのプロセスでは、完全な惨事復旧を実行する必要なしに、Microsoft Exchange または SQL Servers を復旧できます。

アプリケーションレベルリストアプロセスを開始する前に、以下のタスクの実行が必要な場合があります。

- Windows ゲスト OS を備えた新しい仮想マシンをプロビジョニングします。
- CA ARCserve D2D をゲスト OS にインストールします。
- Exchange Server アプリケーションのリストアの場合
 - アカウントが、Exchange 管理者 (完全) 役割の権限 (Exchange Server 2003 用)、または Exchange の組織管理者または、サーバ管理者役割の権限 (Exchange Server 2007/2010 用) を持っていることを確認します。
 - Exchange Server 2007 データベースの回復用ストレージグループへのリストア時に、保護されているサーバ上で回復用ストレージグループを作成します。同様に、Exchange Server 2010 データベースの回復用データベースへのリストア時に、保護されているサーバ上で回復用データベースを作成します。
 - アプリケーションレベルリストアの完全な手順については、「CA ARCserve D2D ユーザガイド」にも記載されており、「[CA ARCserve D2D 手順 \(P. 211\)](#)」に抜粋が掲載されています。

Exchange Server のデータのリストア

Microsoft Exchange Server データのアプリケーション レベルのリストアの実行は、以下で可能です。

- Exchange Server 2003 - シングル サーバ環境。 クラスタ環境はサポートされていません。
- Exchange Server 2007 - シングル サーバ環境、 ローカル連続レプリケーション (LCR) 環境、 クラスタ連続レプリケーション (CCR) 環境。 Exchange Server 2007 CCR の場合、 アクティブおよびパッシブの両方のノードに CA ARCserve D2D をローカルにインストールします。 アクティブまたはパッシブのどちらのノードでもバックアップを実行できますが、 リストア処理はアクティブ ノードに対してのみ実行できます。 シングル コピー クラスタ (SCC) はサポートされていません。
- Exchange Server 2010 - シングル サーバ環境およびデータベース可用性グループ (DAG) 環境。 DAG 環境の場合、 CA ARCserve D2D が DAG 内のすべてのサーバにインストールされていることを確認します。 バックアップは、アクティブおよびパッシブの両方のデータベース コピーから実行できますが、 リストアはアクティブなデータベース コピーに対してのみ実行できます。

Microsoft Exchange Server データのリストアは、以下のレベルで実行できます。

- Microsoft Exchange ライタ レベル -- すべての Exchange Server データをリストアします。
- ストレージグループ レベル -- 特定のストレージグループをリストアします (Microsoft Exchange Server 2010 には適用されません)。
- メールボックス ストア レベル -- 特定のメールボックス ストアをリストアします (Microsoft Exchange Server 2003 にのみ適用されます)。
- メールボックス データベース レベル -- 特定のメールボックス データベースをリストアします (Exchange Server 2007 および 2010 に適用されます)。

注: 作業を開始する前に、「[アプリケーション レベル リストア \(P. 119\)](#)」の必要な前提条件を実行してください。

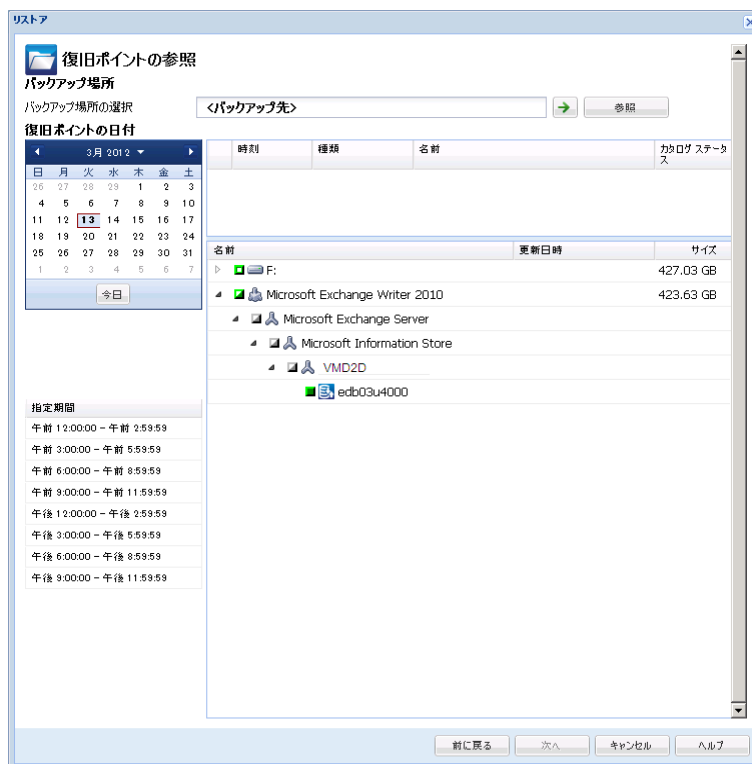
重要: CA ARCserve Central Host-Based VM Backup バックアップセッションからの Microsoft Exchange Server の詳細リストアはサポートされていません。詳細レベルで Microsoft Exchange Server データをリストアするには、CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、Exchange Server データをバックアップします。

Exchange Server のデータのリストア方法

1. CA ARCserve D2D がゲスト オペレーティング システムにインストールされていることを確認します。
2. Exchange Server データをリストアする仮想マシン上のゲスト オペレーティング システムにログインします。
3. CA ARCserve D2D を開始してから、CA ARCserve D2D [ナビゲーション] パネル上で [リストア] をクリックして、[リストア] ダイアログ ボックスを開きます。
4. [復旧ポイントの参照] をクリックして、[復旧ポイントの参照] ダイアログ ボックスを開きます。
5. [復旧ポイントの参照] ダイアログ ボックスの [バックアップ場所の指定] フィールドで、Exchange Server データのリストア元の Host-Based VM Backup 仮想マシン上のバックアップセッションのパスを指定します。以下のパスは、Host-Based VM Backup 仮想マシン上のバックアップセッションのパスの例です。

`https://<サーバ名>/<共有名>/vm@<ESX Server システムのホスト名または IP アドレス>`

6. カレンダーで、復旧ポイントの日付と時刻をクリックします。



7. [次へ] ボタンをクリックすると、[リストア オプション] ダイアログボックスが開きます。
8. リストア先を選択します。

利用可能なオプションは、[元の場所にリストアする]、[ダンプファイルのみ]、[回復用ストレージグループにリストアする]、[回復用メールボックス データベースにリストアする] です。

元の場所にリストアする

バックアップ イメージがキャプチャされた元の場所にリストアします。

ダンプファイルのみ

ダンプファイルのみをリストアします。

このオプションの場合、CA ARCserve D2D は Microsoft Exchange データベース ファイルを指定のフォルダにリストアし、回復が完了するまでデータベースをオンラインにしません。このファイルを別のサーバに移動し、Exchange サーバに手動でマウントして、ファイル内に含まれているデータを表示できます。

注: 回復用メールボックス データベースが存在する場合、「ダンプファイルのみ」オプションを使用したリストアは失敗します。

データベース上のログを再生

データベース ファイルをデスティネーションフォルダにダンプする際に、すべての Microsoft Exchange トランザクション ログ ファイルの再生および適用を行い、それらをデータベースにコミットするように指定できます。次回データベースを起動すると、データベースが利用可能になる前に、データベースにまだ書き込まれていないログ ファイルが適用されます。

注: このオプションは Microsoft Exchange Server 2003 では適用されません。

回復用ストレージグループにリストアする(Exchange 2007)

回復用ストレージグループ (RSG) にデータベースをリストアします。

RSG は、回復用に使用できるストレージグループです。Microsoft Exchange メールボックス データベースを、回復用ストレージグループ内のバックアップからリストアし、そこからデータを抽出することができます。その場合、ユーザがアクセスしている実稼働データベースに影響を及ぼすことはありません。

- 1つのストレージグループ、または同じストレージグループのデータベース (パブリック フォルダ データベース以外) がリストアに選択された場合、デフォルトのリストア デスティネーションは、[回復用ストレージグループにリストアする] (または [回復用データベースにリストアする]) です。
- 複数のストレージグループ、または複数のストレージグループのデータベースがリストアに選択された場合、Exchange は元の場所にリストアするか、または [ダンプファイルのみ] オプションでリストアする必要があります。デフォルトのリストア デスティネーションは [元の場所にリストアする] です。

Exchange 2007 データベースを回復用ストレージグループにリストアするには、回復用ストレージグループ、および同じ名前のメールボックス データベースを作成しておく必要があります。

たとえば、第 1 ストレージグループから MailboxDatabase1 を回復用ストレージグループにリストアする場合、回復用ストレージグループを作成し、データベース「MailboxDatabase1」をその回復用ストレージグループに追加する必要があります。

注: このオプションは Microsoft Exchange Server 2003 では適用されません。

リストア前にデータベースのマウントを解除し、リストア後にデータベースをマウントする

通常、Microsoft Exchange は、リストアの前にいくつかのチェックを実行して以下を確認します。

- リストアされるデータベースが「マウント解除済み」ステータスにある。
- データベースが予期せずリストアされないことがない。

Microsoft Exchange 実稼働データベースが予期せずリストアされるのを防ぐため、リストア処理中にデータベースへの上書きを許可するためのスイッチが追加されています。このスイッチが設定されていないと、Microsoft Exchange ではデータベースのリストアを拒否します。

CA ARCserve D2D では、これらの 2 つの動作は、[リストア前にデータベースのマウントを解除し、リストア後にデータベースをマウントする] オプションによって制御されます。このオプションを使用することで、CA ARCserve D2D では、手動操作なしでリストアプロセスを自動的に起動できます（データベースを手動でマウント解除/マウントするよう指定することもできます）。

- オンに設定した場合、回復処理によってリストアの実行前に自動的に Exchange データベースがマウント解除され、リストアが完了した後マウントされます。また、このオプションをオンにすると、リストア中の Exchange データベースへの上書きが可能になります。
- オフに設定した場合、回復処理で Exchange データベースを回復前に自動的にマウント解除することはなく、回復後にマウントすることはありません。

その場合、Exchange 管理者は手動で一部の操作を実行する必要があります。たとえば、Exchange データベースのマウント解除、データベース上での「上書きを許可」フラグの設定、Exchange データベースのマウントなどです。（回復手順は、データベースのマウント中に Exchange によって実行されます。）

また、このオプションをオフにすると、リストア中の Exchange データベースへの上書きはできなくなります。

回復用ストレージ データベースにリストアする(Exchange 2010)

回復用データベースにデータベースをリストアします。回復用データベースとは、回復目的に使用できるデータベースです。

Microsoft Exchange メールボックス データベースを、バックアップから回復用データベースにリストアし、そこからデータを抽出することができます。その場合、ユーザがアクセスしている実稼働データベースに影響を及ぼすことはありません。

Exchange 2010 データベースを回復用データベースにリストアするには、まず回復用データベースを作成する必要があります。

注: このオプションは Microsoft Exchange Server 2003 および 2007 には適用されません。

9. [次へ]ボタンをクリックすると、[リストア サマリ]ダイアログ ボックスが開きます。
10. 表示された情報に目を通し、リストア オプションおよび設定がすべて正しいことを確認します。
 - サマリ情報が正しくない場合は、[前に戻る] をクリックし、該当するダイアログ ボックスに戻って、正しくない設定を変更します。
 - サマリ情報が正しい場合は、[完了] ボタンをクリックし、リストア プロセスを開始します。

SQL Server のデータのリストア

Microsoft SQL Server データのアプリケーション レベルのリストアの実行は、以下で可能です。

- Microsoft SQL Server 2005 Express/Standard/Workgroup/Enterprise
- Microsoft SQL Server 2008、SQL Server 2008 R2 Express/Web/Standard/Workgroup/Enterprise

注: 作業を開始する前に、「[アプリケーションレベル リストア \(P. 119\)](#)」で前提条件を確認してください。

重要: CA ARCserve Central Host-Based VM Backup バックアップセッションからの Microsoft SQL Server の詳細リストアはサポートされていません。詳細レベルで Microsoft SQL Server データをリストアするには、CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、SQL Server データをバックアップします。

SQL Server のデータのリストア方法

1. CA ARCserve D2D がゲスト オペレーティング システムにインストールされていることを確認します。
2. Exchange Server データをリストアする仮想マシンのゲスト オペレーティング システムにログインします。
3. CA ARCserve D2D を開始してから、CA ARCserve D2D [ナビゲーション] パネル上で [リストア] をクリックして、[リストア] ダイアログ ボックスを開きます。
4. [復旧ポイントの参照] をクリックして、[復旧ポイントの参照] ダイアログ ボックスを開きます。

5. [復旧ポイントの参照] ダイアログボックスの [バックアップ場所の指定] フィールドで、Exchange Server データのリストア元の Host-Based VM Backup 仮想マシン上のバックアップセッションのパスを指定します。以下のパスは、Host-Based VM Backup 仮想マシン上のバックアップセッションのパスの例です。

https://<サーバ名>/<共有名>/vm@<ESX Server システムのホスト名または IP アドレス>

6. 復旧ポイント（日付と時間）を選択した後、リストアする Microsoft SQL Server データベースを選択します。



7. [次へ] ボタンをクリックすると、[リストア オプション] ダイアログ ボックスが開きます。

リストア先を選択します。利用可能なオプションは、[元の場所にリストアする]、[ダンプ ファイルのみ]、[別の場所にリストアする]です。

元の場所にリストアする

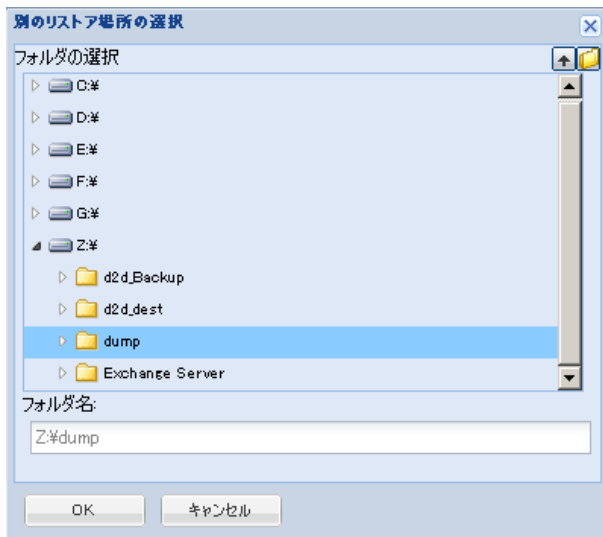
バックアップ イメージがキャプチャされた元の場所にリストアします。

ダンプ ファイルのみ

ダンプ ファイルのみをリストアします。

ダンプ ファイルは、アプリケーションがクラッシュした場合に作成されます。このファイルには、問題の原因をトラブルシューティングのために使用できる追加情報（タイム スタンプ付き）が含まれます。

このオプションを選択すると、ダンプ ファイルのリストア先となるフォルダを指定するか、参照して選択できます。

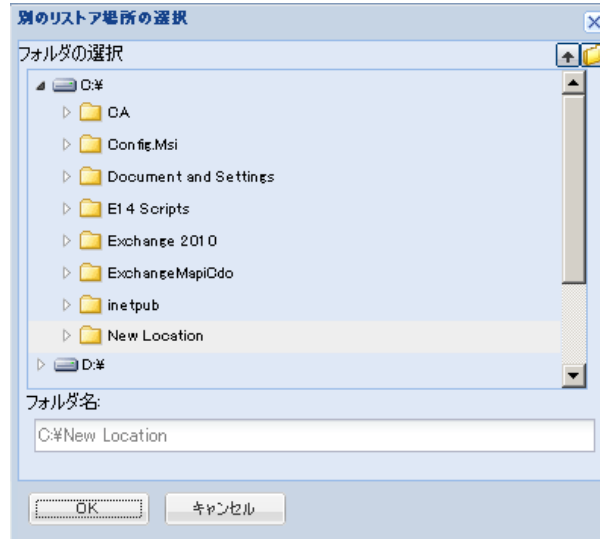


別の場所にリストアする

元の場所以外の別の場所にリストアします。

インスタンス名	データベース名	新しいデータベース名	ファイルの別の場所
MSSQLSERVER	LogShippingDatabase	LogShippingDatabase	<input type="button" value="参照"/>
MSSQLSERVER	MirrorDatabase001	<新規データベース名>	C:\NewDBLocation <input type="button" value="参照"/>

バックアップはネットワーク上の場所にコピーできるので、複数の SQL サーバインスタンスでバックアップを使用できます。複数のデータベースのリストアは、インスタンスレベルで（同時に）実行できます。このリストからデータベースインスタンスを選択し、新しいデータベース名およびデータベースのリストア先となる別の場所を指定できます。また、データベースのリストア先となる別の場所を参照することもできます。



8. [次へ] ボタンをクリックすると、[リストア サマリ] ダイアログ ボックスが開きます。
9. 表示された情報に目を通し、リストア オプションおよび設定がすべて正しいことを確認します。
 - サマリ情報が正しくない場合は、[前に戻る] をクリックし、該当するダイアログ ボックスに戻って、正しくない設定を変更します。
 - サマリ情報が正しい場合は、[完了] ボタンをクリックし、リストア プロセスを開始します。

第 5 章: CA ARCserve Central Host-Based VM Backup のトラブルシューティング

このセクションでは、CA ARCserve Central Host-Based VM Backup の使用中に発生する可能性がある問題について、問題の特定と解決に役立つトラブルシューティング情報を提供します。

このセクションには、以下のトピックが含まれています。

[ノードの追加を試行すると、指定されたサーバにアクセスできないというメッセージが表示される \(P. 133\)](#)

[空の Web ページが表示される、または、JavaScript エラーが発生する \(P. 136\)](#)

[CA ARCserve D2D ノードへのログイン時に Web ページが正しくロードされない \(P. 138\)](#)

[ページのロード問題のトラブルシューティング方法 \(P. 140\)](#)

[CA ARCserve Central Applications にアクセスすると、文字化けがブラウザウィンドウ内に表示される \(P. 141\)](#)

[ノード更新時のアクセス拒否エラー発生 \(P. 142\)](#)

[アプリケーションへのログイン時に証明書エラーが表示される \(P. 144\)](#)

[バックアップがスナップショット作成エラーで失敗する \(P. 145\)](#)

[VM の復旧が不明なエラーで失敗する \(P. 147\)](#)

[hotadd 転送モードを使用したバックアップおよび復旧操作でディスクがマウントできない \(P. 149\)](#)

[HOTADD または SAN 転送モードを使用してデータを復旧すると復旧に失敗する \(P. 149\)](#)

[オペレーティング システムが見つからないエラー \(P. 152\)](#)

[MAC アドレスの変更が VM 復旧後に保持されない \(P. 153\)](#)

[CA ARCserve D2D Web サービスが CA ARCserve D2D ノード上で失敗する \(P. 154\)](#)

[CA ARCserve Central Host-Based VM Backup がリモート ノード上の CA ARCserve D2D Web サービスと通信できない \(P. 157\)](#)

[CA ARCserve D2D Web サービスの実行が遅い \(P. 158\)](#)

[変更ブロックのトラッキングに失敗する \(P. 160\)](#)

[ESXi ライセンスのためにバックアップが失敗する \(P. 161\)](#)

[VM にスナップショットがあるためバックアップが失敗する \(P. 162\)](#)

[バックアップが失敗し、バックアッププロキシシステムのイベント ログにイベント 1530 がログ記録される \(P. 163\)](#)

[ホット追加転送モードを指定したのに NBD 転送モードでバックアップが完了する \(P. 164\)](#)

[増分バックアップ ジョブが検証バックアップ ジョブとして処理される \(P. 165\)](#)

[ブロックを識別できないため、バックアップ ジョブに失敗する \(P. 166\)](#)

[VMDK ファイルを開けない \(P. 167\)](#)

[ノード名を変更した後にノードがノード画面に表示されない \(P. 168\)](#)

[ポリシーを CA ARCserve D2D サーバに保存または割り当てる際に複数の接続エラーが発生する \(P. 169\)](#)

[ESX Server にアクセスできないために仮想マシンのバックアップが失敗する \(P. 170\)](#)

[Internet Explorer 8、9、Chrome で追加した新しいタブのリンクが正常に起動しない \(P. 171\)](#)

[Internet Explorer 8 および 9 で、新しいタブの追加リンク、RSS フィード、およびソーシャル ネットワーキング フィードバックが正常に起動しない \(P. 175\)](#)

[日本語キーボードを使用して \[フィルタ\] フィールドのワイルドカードとしてアスタリスクまたはアンダースコアを指定できない \(P. 176\)](#)

[仮想マシンの復旧で指定とは異なる転送モードが使用される \(P. 176\)](#)

ノードの追加を試行すると、指定されたサーバにアクセスできないというメッセージが表示される

Windows プラットフォームで有効

症状:

[ノード] 画面からノードの追加または接続を試行すると、以下のメッセージが表示されます。

指定したサーバに接続できません。

解決方法:

[ノード] 画面からノードを追加しようとして上記のメッセージが表示された場合、以下を実行することによって問題を解決できることがあります。

- CA ARCserve Central Host-Based VM Backup サーバおよびソース仮想マシン (ノード) 上で Windows Server サービスが実行されていることを確認します。
- CA ARCserve Central Host-Based VM Backup サーバおよびソース仮想マシン (ノード) 上で、Windows ファイアウォールの例外が「ファイルとプリンタの共有」に適用されていることを確認します。
- ノードがドメインのメンバでない場合のみ、Windows ファイアウォールの例外が「Netlogon サービス」に適用されていることを確認します。CA ARCserve Central Host-Based VM Backup サーバおよびソース仮想マシン (ノード) 上でこのタスクを実行します。

- ローカルアカウントの共有とセキュリティ モデルが「クラシック」であることを確認します。クラシック値を適用するには、以下の手順に従います。

注: CA ARCserve Central Host-Based VM Backup サーバおよびソース仮想マシン（ノード）上で以下の手順に従います。

1. CA ARCserve Central Host-Based VM Backup サーバにログインし、コントロールパネルを開きます。
2. [コントロールパネル] の [管理ツール] を開きます。
3. [ローカルセキュリティ ポリシー] をダブルクリックします。
[ローカルセキュリティ ポリシー] ウィンドウが表示されます。
4. [ローカルセキュリティ ポリシー] ウィンドウで、[ローカルポリシー] を展開し、[セキュリティ オプション] を展開します。
セキュリティ ポリシーが表示されます。
5. [ネットワーク アクセス：ローカルアカウントの共有とセキュリティ モデル] を右クリックし、コンテキストメニューの [プロパティ] をクリックします。
[ネットワーク アクセス：ローカルアカウントの共有とセキュリティ モデル] ダイアログ ボックスが表示されます。
6. [ローカルセキュリティの設定] をクリックします。
ドロップダウンリストから [クラシック - ローカルユーザがローカルユーザとして認証する] を選択します。
[OK] をクリックします。

- LAN Manager 認証レベルのローカル ポリシーの値が、[LM と NTLM を送信する – ネゴシエーションの場合、NTLMv2 セッションセキュリティを使う] に設定されていることを確認します。この値を適用するには、以下の手順に従います。
 1. CA ARCserve Central Host-Based VM Backup サーバにログインし、コマンドプロンプトを開きます。

以下のコマンドを実行します。

```
secpol.msc
```

[ローカルセキュリティ設定] ダイアログ ボックスが表示されます。
 2. ローカルポリシーを選択し、[セキュリティオプション] をクリックします。

[ネットワークセキュリティ：LAN Manager 認証レベル] を確認します。

このオプションをダブルクリックします。

プロパティのダイアログ ボックスが開きます。
 3. 以下のオプションを選択して、[OK] ボタンをクリックします。

LM と NTLM を送信する – ネゴシエーションの場合、NTLMv2 セッション セキュリティを使う
 4. コマンドプロンプトで以下のコマンドを入力します。

```
gpupdate
```

値が適用されます。

空の Web ページが表示される、または、JavaScript エラーが発生する

Windows Server 2008 および Windows Server 2003 OS で有効

症状:

CA ARCserve Central Applications Web サイトを Internet Explorer を使用して開くと、空の Web ページが表示されるか、または Javascript エラーが発生します。この問題は、Windows Server 2008 および Windows Server 2003 のオペレーティングシステム上で Internet Explorer を使用した場合に発生します。

この問題は以下の状況で発生します。

- Internet Explorer 8 または Internet Explorer 9 を使用してアプリケーションを表示していて、ブラウザがこの URL を信頼済みサイトとして認識しない。
- アプリケーションを表示するために Internet Explorer 9 を使用していて、通信プロトコルとして HTTPS を使用している。

解決方法:

この問題を修正するには、アプリケーションの表示に使用しているコンピュータ上の Internet Explorer のセキュリティ強化の構成を無効にします。

Windows Server 2008 システム上で Internet Explorer セキュリティ強化の構成を無効にするには、以下の手順に従います。

1. 管理者アカウントまたは管理者権限があるアカウントを使用して、レポートを表示するために使用する Windows Server 2008 コンピュータにログオンします。
2. デスクトップ上で [コンピュータ] を右クリックし、[管理] をクリックして [サーバー マネージャー] ウィンドウを開きます。

3. [サーバー マネージャー] ウィンドウで、[サーバー マネージャー (サーバ名)] をクリックします。

[サーバーの概要] セクションで、以下のとおり [セキュリティ情報] を開いて [IE ESC の構成] をクリックします。

セキュリティ情報	
Windows ファイアウォール:	パブリック 無効
Windows Update:	構成されていません
更新プログラムの最終確認日時:	なし
更新プログラムの最終インストール日時:	なし
IE セキュリティ強化の構成 (ESC):	管理者に対して有効 ユーザーに対して有効

- Windows ファイアウォールの表示
- 更新プログラムの構成
- 新しい役割の確認
- セキュリティの構成ウィザードを実行
- IE ESC の構成

[Internet Explorer セキュリティ強化の構成] ダイアログ ボックスが表示されます。

4. [Internet Explorer セキュリティ強化の構成] ダイアログ ボックスで、以下を設定します。

- 管理者 -- オフ
- ユーザー -- オフ

[OK] をクリックします。

[Internet Explorer セキュリティ強化の構成] ダイアログ ボックスが閉じ、Internet Explorer セキュリティ強化の構成が無効になります。

Windows Server 2003 システム上で Internet Explorer セキュリティ強化の構成を無効にするには、以下の手順に従います。

1. 管理者アカウントまたは管理者権限があるアカウントを使用して、レポートを表示するために使用する Windows Server 2003 コンピュータにログオンします。
2. Windows コントロールパネルから [プログラムの追加と削除] を開きます。
3. [プログラムの追加と削除] ダイアログ ボックスで、[Windows コンポーネントの追加と削除] オプションをクリックし、[Windows コンポーネント ウィザード] にアクセスします。

[Internet Explorer セキュリティ強化の構成] の横のチェック マークをクリアします。

[次へ] をクリックします。

引き続き画面の指示に従って手順を完了し、[完了] をクリックします。

Internet Explorer セキュリティ強化の構成が無効になります。

CA ARCserve D2D ノードへのログイン時に Web ページが正しくロードされない

Windows プラットフォームで有効

症状:

[ノード] 画面から CA ARCserve D2D ノードにログインした場合、ブラウザ ウィンドウで Web ページが正しくロードされないか、エラーメッセージが表示されるか、またはその両方が発生します。

解決方法:

この動作は、主に Internet Explorer ブラウザに影響します。アクティブ スクリプト、ActiveX コントロール、Java プログラムがコンピュータ上で無効になるか、ネットワーク上でブロックされた場合、Web ページが正しくロードしないことがあります。

ブラウザ ウィンドウを更新すると、この問題を解決できます。しかし、ブラウザ ウィンドウを更新しても問題が解決されない場合は、以下の手順に従います。

1. Internet Explorer を起動します。

[ツール] メニューで、[インターネット オプション] をクリックします。

[インターネットオプション] ダイアログ ボックスが表示されます。

2. [セキュリティ] タブをクリックします。

[セキュリティ] オプションが表示されます。

3. [インターネット] ゾーンをクリックします。

インターネットゾーン オプションが表示されます。

4. [レベルのカスタマイズ] をクリックします。

インターネットゾーンの [セキュリティの設定] ダイアログ ボックスが表示されます。

5. [スクリプト] カテゴリにスクロールします。

[アクティブ スクリプト] を確認します。

[有効にする] または [ダイアログを表示する] オプションをクリックします。

6. [セキュリティの設定] ダイアログ ボックスで [OK] をクリックします。

インターネットゾーンの [セキュリティの設定] ダイアログ ボックスが閉じます。

7. [インターネット オプション] ダイアログ ボックスで [OK] をクリックします。

[インターネット オプション] ダイアログ ボックスが閉じます。また、アクティブ スクリプト オプションが適用されます。

注: このソリューションによって問題が解決されない場合は、アンチウイルスやファイアウォールなどの他のプログラムがアクティブ スクリプト、ActiveX コントロール、Java プログラムをブロックしている可能性がないかどうか、システム管理者に問い合わせてください。

ページのロード問題のトラブルシューティング方法

Windows プラットフォームで有効

症状:

CA ARCserve Central Applications、CA ARCserve D2D ノード、モニタ サーバにログインすると、以下のエラーメッセージがブラウザ ウィンドウに表示されます。

メッセージ 1

この web ページのエラーにより、正しく機能しない場合があります

メッセージ 2

!

解決方法:

Web ページが正しくロードされない場合はいくつかの原因が考えられます。以下の表は、よく見られる原因および対応する対処法について説明したものです。

原因	対処法
基になる HTML ソース コードに問題がある。	Web ページを更新して再度試行します。
ネットワークでアクティブ スクリプト、ActiveX、または Java プログラムがブロックされている。	ブラウザでアクティブ スクリプト、ActiveX、または Java プログラムの使用を許可します。
アンチウイルス アプリケーションが一時インターネット ファイルおよびダウンロードされたプログラムをスキャンするよう設定されている。	アンチウイルス アプリケーションをフィルタし、CA ARCserve Central Applications Web ページと関連付けられたインターネット関連ファイルが許可されるようにします。
コンピュータにインストールされた、スクリプティング エンジンが破損しているかまたは古い。	スクリプティング エンジンを更新します。
コンピュータにインストールされたビデオカード ドライバが破損しているかまたは古い。	ビデオカード ドライバを更新します。

原因	対処法
----	-----

コンピュータにインストールされた、DirectX コ	DirectX コンポーネントを更新します。 ンポーネントが破損しているかまたは古い。
----------------------------	--

CA ARCserve Central Applications にアクセスすると、文字化けがブラウザ ウィンドウ内に表示される

すべての Windows オペレーティング システムで有効。すべてのブラウザに該当します。

症状:

CA ARCserve Central Applications にログインすると、文字化けした文字がブラウザ ウィンドウのコンテンツ領域に表示されます。

解決方法:

この問題が発生するのは、HTTPS 通信を使用して CA ARCserve Central Applications をインストールし、次に HTTP 通信を使用して CA ARCserve Central Applications にアクセスしようとした場合です。基盤となる CA ARCserve Central Applications Web サービス コンポーネントでは、HTTP URL から HTTPS URL に変換する機能をサポートしません。そのため、文字化けした文字がブラウザ ウィンドウに表示されます。例:



この問題を解決するには、HTTPS を使用して CA ARCserve Central Applications をインストールまたは設定した場合は、HTTPS を使用してアプリケーションにアクセスします。

ノード更新時のアクセス拒否エラー発生

ユーザアカウント制御(UAC)をサポートするすべての Windows オペレーティングシステムに該当します。

注: Windows Vista、Windows Server 2008、Windows Server 2008 R2、および Windows 7 は UAC をサポートしています。

症状 1:

管理者グループのメンバである Windows ユーザアカウントを提供する場合、[vCenter/ESX から仮想マシンをインポート] ダイアログボックスの [ノード認証情報] ダイアログボックスでパスワードを適用すると、以下のメッセージが表示されます。

管理者権限が必要です。

このため、ノード認証情報を適用できません。

症状 2:

インポート操作中に、ノードはインポートするがノード認証情報は提供しない場合、管理者グループのメンバである Windows ユーザアカウントを使用してノードの更新操作を実行すると、以下のメッセージが表示されます。

アクセスが拒否されました。ユーザに管理者権限があること、および追加されたマシンのローカルセキュリティポリシーによってリモートレジストリアクセスが制限されていないことを確認してください。

このため、ノードを更新できません。

解決方法:

こうした結果が予測されるのは、UAC が UAC をサポートする Windows オペレーティングシステムを実行するコンピュータ上で有効である場合です。UAC は、管理者アカウントにのみリモートロケーションからのコンピュータへのログインを許可する Windows の機能です。この問題の解決策として、以下の手順を完了します。

次の手順に従ってください:

1. 管理者アカウントを使用して、コンピュータにログインします。
2. Windows のコントロールパネルを開きます。
3. [ユーザーアカウント] を開きます。

4. [ユーザー アカウントの変更] 画面で [ユーザー アカウント制御設定の変更] をクリックし、以下のいずれかの操作を実行します。
 - **Windows Vista および Windows Server 2008** : [ユーザー アカウントの変更] 画面で [ユーザーアカウント制御の有効化または無効化] をクリックします。次に、 [ユーザー アカウント制御 (UAC) を有効にして、お使いのコンピュータをより安全にします] 画面で、 [ユーザー アカウント制御 (UAC) を使ってコンピュータの保護に役立たせる] の横のチェック ボックスをオフにして、 [OK] をクリックします。

コンピュータを再起動して、UAC への変更を適用します。
 - **Windows Server 2008 r2 および Windows 7** : [コンピューターへの変更の通知を受け取るタイミングの選択] で、スライダを [常に通知する] から [通知しない] へ移動します。 [OK] をクリックし、Windows のコントロールパネルを閉じます。

コンピュータを再起動して、UAC への変更を適用します。
5. コンピュータの再起動後、仮想マシン上のゲスト オペレーティング システムに以下の環境設定が適用されていることを確認します。
 - Windows Server サービスが実行されている。
 - [ファイルとプリンタの共有] サービスが Windows ファイアウォールを通じて通信を行うことを許可されている。
 - ドメイン参加にノードが必要ではない場合、 [Netlogon] サービスが Windows ファイアウォールを通じて通信を行うことを許可されている。
 - ローカルセキュリティ ポリシー、ローカル ポリシー、セキュリティ オプション、ネットワーク アクセスの値 : ローカルアカウントの共有およびセキュリティ モデルが [クラシック] である。
6. 以下の環境設定が Host-Based VM Backup サーバに適用されていることを確認します。
 - ローカルセキュリティ ポリシー、ローカル ポリシー、セキュリティ オプション、ネットワーク セキュリティの値 : LAN Manager 認証レベルは [LM と NTLM を送信する - ネゴシエーションの場合、NTLMv2 セッションセキュリティを使う] です。

アプリケーションへのログイン時に証明書エラーが表示される

Windows プラットフォームで有効

症状:

アプリケーションにログインすると、以下の内容のメッセージがブラウザウィンドウに表示されます。

- Internet Explorer

この web サイトのセキュリティ証明書には問題があります

- Firefox

この接続は信頼されていません

- Chrome

このサイトのセキュリティ証明書は信頼されていません

Web サイトへ続行するオプションを指定した場合、アプリケーションに正常にログインできます。ただし、アプリケーションにログインするたびにこの動作が発生します。

解決方法:

この動作は、通信プロトコルとして HTTPS を使用するよう指定されている場合に発生します。この問題を一時的に解決するには、ブラウザウィンドウで Web サイトへ続行するためのリンクをクリックします。ただし、次回アプリケーションにログインした場合、再度このメッセージが表示されます。

HTTPS 通信プロトコルは、HTTP 通信プロトコルより高いレベルのセキュリティを提供します。HTTPS 通信プロトコルを使用して通信を続ける必要がある場合は、VeriSign からセキュリティ証明書を購入し、アプリケーションサーバに証明書をインストールできます。可能であれば、アプリケーションによって使用される通信プロトコルを HTTP に変更することもできます。通信プロトコルを HTTP に変更するには、以下の手順に従います。

1. アプリケーションがインストールされたサーバにログインします。
2. 以下のディレクトリを参照します。

`C:\Program Files\CA\ARCserve Central Applications\BIN`

3. 以下のバッチ ファイルを実行します。

`ChangeToHttp.bat`

4. バッチ ファイルが実行されたら、Windows サーバ マネージャを開きます。

以下のサービスを再起動します。

CA ARCserve Central Applications サービス

バックアップがスナップショット作成エラーで失敗する

Windows プラットフォームで有効

VMware ベースの仮想マシンのバックアップをサブミットすると、以下の症状が発生します。

症状 1

バックアップ ジョブが失敗し、以下のメッセージがアクティビティ ログに表示されます。

スナップショットの取得に失敗しました。 ESX/vCenter レポート エラー。 一般システム エラーが発生しました。 VMX からのプロトコル エラー。

解決策 1

このエラーは VMware の問題です。この問題を修正するには、ゲストオペレーティング システム内の VMware Tools をアンインストールして再インストールし、ジョブを再度サブミットします。

症状 2

バックアップジョブが失敗し、以下のメッセージがアクティビティログに表示されます。

仮想マシンのスナップショットを作成できませんでした。ESX Server/vCenter Server から次のエラーがレポートされました: スナップショット作成処理が、停止した仮想コンピュータの I/O 解放の制限時間を超えたため、静止スナップショットを作成できません。

解決策 2

スナップショットの作成中に VSS がエラーに遭遇すると、このエラーが発生します。VSS は、以下の条件下でエラーに遭遇する場合があります。

VSS ライタが不安定な状態にある。

この動作の原因を特定し、修正するには、以下の是正アクションを行います。

1. 仮想マシンのゲストオペレーティングシステムのコマンドラインからコマンド "vssadmin list writers" を実行します。
2. すべての VSS ライタが正常な状態であることを確認します。
3. 以下の状態のライタのエラーを修正する方法の詳細については、Microsoft またはライタのベンダにエラーの修正方法を問い合わせます。

```
state=Stable  
Last Error=No Error
```

注: 通常、ライタを再起動すると問題が解決します。

スナップショットの作成時に、VSS がエラーに遭遇します。

この動作の原因を特定し、修正するには、以下の是正アクションを行います。

1. ゲスト オペレーティング システムの Windows イベント ログを確認します。バックアップ開始時刻の近辺で発生した、VSS コンポーネント関連エラーをチェックします。
2. VSS がディスクの容量不足エラーをレポートしている場合、エラー関連ボリュームのディスク容量を解放します。
3. VSS または Windows Volsnap ドライバによってタイムアウトエラーが生成されている場合、仮想マシン内で実行されるアプリケーションは非常にアクティブな状態にあります。非常にアクティブな状況においては、VSS による一貫したスナップショットの作成が妨げられます。この状況を改善するには、該当ボリュームに対するアプリケーションの入出力処理が少ない時間帯にバックアップをスケジュールします。
4. Windows イベント ログが VolSnap ドライバでのエラー発生を示している場合は、Microsoft Technet ライブラリの「Volume Snapshot Driver Integrity ([http://technet.microsoft.com/en-us/library/cc734554\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc734554(v=ws.10).aspx))」で、VolSnap ドライバエラーの修正方法を確認してください。

VM の復旧が不明なエラーで失敗する

Windows オペレーティング システムで有効

症状:

VM の復旧ジョブが失敗します。VM の復旧ジョブをサブミットすることはできますが、以下のメッセージがアクティビティ ログに表示されます。

仮想ディスクの復旧に失敗しました。

さらに、VDDK は以下のエラー メッセージをレポートします。

不明なエラーです。

解決策 1:

この問題を修正するには、以下の解決策を検討してください。

- 元のデータストア上に十分なディスク空き容量がないと、VM の復旧ジョブは失敗する場合があります。VDDK API は（現在のところ）元のデータストア上のディスク空き容量を検出する機能をサポートしないため、VDDK はエラーメッセージを返します。（データストアは仮想マシンの復旧用に指定した場所です。）この問題を修正するには、操作を完了するために必要な元のデータストア上のディスク容量を解放してから、ジョブを再サブミットします。
- ネットワーク障害および高いネットワークトラフィックにより、VM の復旧ジョブが失敗する場合があります。この問題を修正するには、プロキシサーバと、ESX Server システムまたは vCenter Server システムがネットワークを介して通信できているかどうかを確認し、ジョブを再サブミットします。
- ESX Server システムまたは vCenter Server システムへの VM のバックアップまたは復旧ジョブから構成される複数の同時接続は、VMware vSphere Client を通じた vSphere SDK 接続を含む場合に、失敗することがあります。この問題を修正するには、不要な接続をすべて閉じてから、ジョブを再サブミットします。許可される同時接続の最大数の詳細については、「[VMDK ファイルを開けない \(P. 167\)](#)」を参照してください。
- 個別の仮想マシンの内部エラーを特定するには、VMware vSphere Client ログの「Examine the Tasks and Events」のセクションを確認してください。内部エラーを修正してから、ジョブを再サブミットします。
例：他のアプリケーションまたは操作が VMDK ファイルを使用しています。この問題を修正するには、ファイルを解放してジョブを再サブミットします。

解決策 2:

この問題は、以下の状況で発生する可能性があります。

- VDDK がスナップショットを正しく処理しなかった。
- VDDK がスナップショットを手動または仮想マシンの内部で削除しなかった。

この問題を修正するには、ジョブを再サブミットします。ジョブが再度失敗する場合は、復旧した仮想マシンを削除して、ジョブを再サブミットします。

hotadd 転送モードを使用したバックアップおよび復旧操作でディスクがマウントできない

Windows プラットフォームで有効

症状:

hotadd 転送モードを使用したバックアップおよび復旧ジョブでは、プロキシシステムにディスクをマウントできません。

解決方法:

この問題を解決するには、以下の手順に従います。

1. VMware vSphere Client を開きます。
管理者の認証情報を使用して ESX Server システムまたは vCenter Server システムにログインします。
2. プロキシ仮想マシンを選択し、そのプロキシ仮想マシン用の設定を編集します。
3. ソース仮想マシンまたはプロキシ仮想マシンに接続している hotadd ディスクを取り外します。
4. ジョブを再サブミットします。

HOTADD または SAN 転送モードを使用してデータを復旧すると復旧に失敗する

Windows プラットフォームで有効

症状:

HOTADD または SAN 転送モードを使用してデータを復旧すると復旧に失敗します。以下のようなメッセージがアクティビティログに表示されます。

不明なエラーが発生しました。テクニカル サポートにお問い合わせください。

解決方法:

ディスクが正しく設定されていない状態で [HOTADD 転送モード \(P. 291\)](#) または [SAN 転送モード \(P. 291\)](#) を使用すると、復旧処理が失敗します。

ディスクを設定するには、以下の手順に従います。

1. 管理者権限のあるアカウントを使用してバックアップ プロキシ システムにログインします。
2. Windows のコマンドラインを開きます。
3. コマンドラインから以下のコマンドを入力します。

```
diskpart
```

Enter キーを押します。

4. SAN と入力し、Enter キーを押します。

現在の SAN ポリシーが表示されます。

5. 以下のコマンドを入力します。

```
SAN POLICY = OnlineAll
```

Enter キーを押します。

SAN にホストされたボリュームが自動的にマウントされないように SAN ポリシーが設定されます。

6. 特定の SAN ディスクの読み取り専用属性をクリアするには、ディスクの一覧からディスクを選択し、以下のコマンドを入力します。

```
attribute disk clear readonly
```

Enter キーを押します。

7. exit と入力し、Enter キーを押します。

ディスクが設定され、ジョブを再サブミットできます。

ジョブが再度失敗する場合は、プロキシシステム上でディスク管理を使用して、HOTADD ディスクを手動でマウントします。

ディスクを手動でマウントするには、以下の手順に従います。

1. 管理者権限のあるアカウントを使用してバックアッププロキシシステムにログインします。
2. Windows のコントロールパネルを開き、[管理ツール] をダブルクリックします。
[管理ツール] ウィンドウが開きます。
3. お気に入りリストから、[コンピュータの管理] をダブルクリックします。
[コンピュータの管理] ダイアログ ボックスが表示されます。
4. [記憶域] を展開し、[ディスクの管理] をクリックします。
ディスクが表示されます。
5. マウントするディスクを右クリックし、[オンライン] をクリックします。

ディスクがマウントされ、ジョブを再サブミットできます。

オペレーティング システムが見つからないエラー

Windows プラットフォームで有効

症状 1

[別の場所にリストアする] オプションを使用して仮想マシンを復旧した後、仮想マシン上のゲスト オペレーティング システムを開始しようとすると、以下のメッセージが表示されます。

オペレーティング システムが見つかりません。

解決策 1

上記の動作は、SCSI および IDE デバイスが含まれる仮想マシン上で発生する可能性があります。この問題が発生した場合は、仮想マシン上でディスクがどのように設定されているかを調査し、復旧した仮想マシンのブート シーケンスがソース仮想マシンと同じであることを確認します。ブート シーケンスが異なる場合、復旧した仮想マシン上の BIOS を更新し、ソースのものと一致させる必要があります。

注: 最初の IDE ディスクは (0 : 1) を使用する必要があります。

症状 2

仮想マシンを復旧した後、仮想マシン上のゲスト オペレーティング システムを開始しようとすると、以下のメッセージが表示されます。

オペレーティング システムが見つかりません。

解決策 2

この問題が発生した場合は、仮想マシン上でディスクがどのように設定されているかを調査し、レプリカ仮想マシンのブート シーケンスがソース仮想マシンと同じであることを確認します。

MAC アドレスの変更が VM 復旧後に保持されない

Windows プラットフォームで有効

症状:

仮想マシンの MAC アドレスが仮想マシン復旧後に保持されません。

解決方法:

MAC アドレスは、重複を防ぐため復旧中は保持されません。MAC アドレス情報を保持するには、プロキシサーバ上で以下のレジストリ キーを設定します。

場所: SOFTWARE\CA\CA ARCSERVE D2D

キー名: RetainMACForVDDK

値タイプ: 文字列

キー値: 1

2 つの NIC カードを持つ仮想マシンで、必要に応じて RetainMACForVDDK レジストリ キーを設定し、1 つを「Manual」に設定します。そうしないと、すべてのカードは復旧後に「Automatic」に設定されます。

CA ARCserve D2D Web サービスが CA ARCserve D2D ノード上で失敗する

Windows プラットフォームで有効

症状:

CA ARCserve D2D ノード上で実行される Web サービスが開始後に失敗するか、または開始できません。

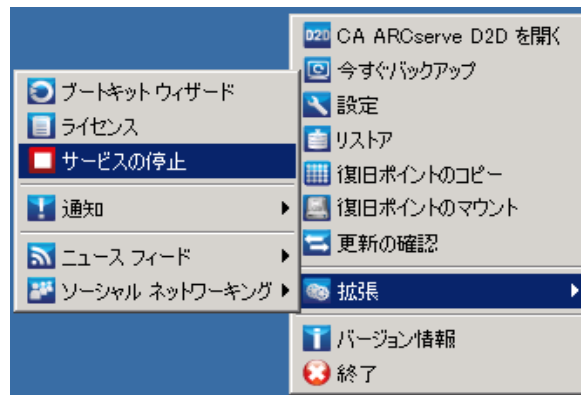
解決方法:

この問題は、CA ARCserve D2D Web サービスによって使用されるポートが VMware vCenter Web サービス (Tomcat) によって使用されるポートと同じである場合に発生します。

CA ARCserve D2D が使用するポートは、Tomcat が使用するデフォルトポートと競合する場合があります。この競合により、Tomcat の前に CA ARCserve D2D が起動した場合は Tomcat が失敗します。この問題を解決するため、以下のように Tomcat のデフォルトポートを変更することができます。

1. CA ARCserve D2D モニタにアクセスし、[拡張] オプションをクリックして、[サービスの停止] を選択します。

CA ARCserve D2D Web サービスが停止されます。



2. Tomcat の server.xml ファイルを開いて、Tomcat の動作を変更/設定します。

Tomcat の server.xml ファイルは、以下のフォルダ内にあります。

C:\Program Files\CA\ARCserve Central Applications\TOMCAT\conf

3. server.xml ファイル内で <Server> タグを見つけます。



```
Server.xml - メモ帳
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<!-- Note: A "server" is not itself a "Container", so you may not
define subcomponents such as "valves" at this level.
Documentation at /docs/config/server.html
-->
<Server>
  <!--APR library loader. Documentation at /docs/apr.html -->
  <Listener className="org.apache.catalina.core.AprLifecycleListener"/>
  <!--Initialize Jasper prior to webapps are loaded. Documentation at /docs/jasper-howto.html -->
  <Listener className="org.apache.catalina.core.JasperListener"/>
  <!-- JMX Support for the Tomcat server. Documentation at /docs/jmx-remote.html -->
  <Listener className="org.apache.catalina.mbeans.ServerLifecycleListener"/>
  <!-- Global JNDI resources
Documentation at /docs/jndi-resources-howto.html
-->
  <GlobalNamingResources>
    <!-- Editable user database that can also be used by
```

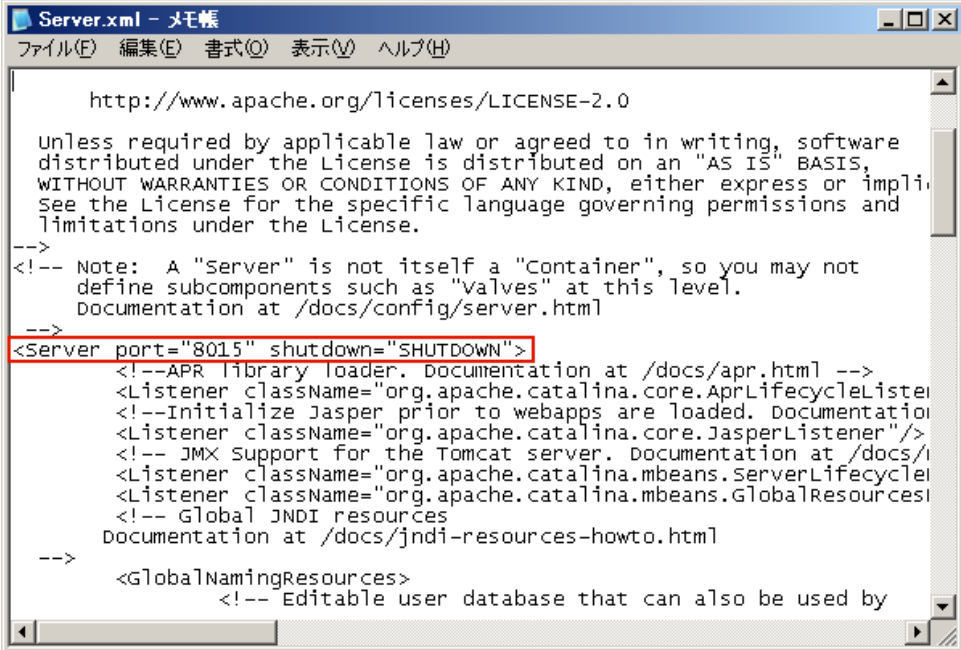
4. <Server> タグを以下のように編集します。

変更前 :

```
<Server>
```

変更後 :

```
<Server port="8015" shutdown="SHUTDOWN">
```



```
Server.xml - メモ帳
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<!-- Note: A "server" is not itself a "Container", so you may not
define subcomponents such as "valves" at this level.
Documentation at /docs/config/server.html
-->
<Server port="8015" shutdown="SHUTDOWN">
  <!--APR library loader. Documentation at /docs/apr.html -->
  <Listener className="org.apache.catalina.core.AprLifecycleLister
  <!--Initialize Jasper prior to webapps are loaded. Documentation
  <Listener className="org.apache.catalina.core.JasperListener"/>
  <!-- JMX Support for the Tomcat server. Documentation at /docs/
  <Listener className="org.apache.catalina.mbeans.ServerLifecycle
  <Listener className="org.apache.catalina.mbeans.GlobalResources
  <!-- Global JNDI resources
  Documentation at /docs/jndi-resources-howto.html
-->
  <GlobalNamingResources>
    <!-- Editable user database that can also be used by
```

5. server.xml ファイルを保存して閉じます。

Tomcat をシャットダウンするコマンドが設定され、指定されたポート (8015) でサーバによって受信されるようになりました。

6. CA ARCserve D2D モニタにアクセスし、[拡張] オプションをクリックして、[サービスの開始] を選択します。

CA ARCserve D2D Web サービスが開始されます。

CA ARCserve Central Host-Based VM Backup がリモート ノード上の CA ARCserve D2D Web サービスと通信できない

Windows オペレーティング システムで有効

症状:

CA ARCserve Central Host-Based VM Backup が、リモート ノード上の CA ARCserve D2D Web サービスと通信できません。

解決方法:

以下の表は、CA ARCserve Central Host-Based VM Backup がリモートノード上の CA ARCserve D2D Web サービスと通信できない理由、および対応する是正処置を示したものです。

原因	対処法
ポリシーを適用するときに、ネットワークが利用できないか安定していなかった。	ネットワークが利用できて安定していることを確認し、再試行します。
アプリケーションがノードとの通信を試行したときに、CA ARCserve D2D コンピュータで負荷に対応できなかった。	リモート CA ARCserve D2D ノード上の CPU が通常の状態にあることを確認し、再試行します。
ポリシーを適用するときに、リモートノード上の CA ARCserve D2D サービスが実行されていない。	リモートノード上の CA ARCserve D2D が実行されていることを確認し、再試行します。
CA ARCserve D2D サービスが正しく通信していなかった。	リモートノード上の CA ARCserve D2D サービスを再起動し、再試行します。

CA ARCserve D2D Web サービスの実行が遅い

Windows オペレーティング システムで該当

症状 1:

CA ARCserve D2D システム上の CA ARCserve D2D Web サービスの実行が遅くなります。以下のような症状が検出されます。

- CA ARCserve D2D Web サービスが応答を停止するか、または CPU リソースの 100 パーセントを消費している。
- CA ARCserve D2D ノードのパフォーマンスが低下するか、または Web サービスと通信できない。

解決策 1:

さまざまな環境上の環境設定では、CA ARCserve D2D Web サービスが著しく CPU 時間を占有していたり、応答が遅いことを検出する場合があります。デフォルトでは、Tomcat は一定のメモリ量をノードに割り当てるように設定されていますが、お使いの環境には適していない場合があります。この問題を検証するには、以下のログ ファイルを確認します。

```
<D2D_home>%TOMCAT%logs%casad2dwebsvc-stdout.*.log  
<D2D_home>%TOMCAT%logs%casad2dwebsvc-stderr.*.log  
<D2D_home>%TOMCAT%logs%catalina.*.log  
<D2D_home>%TOMCAT%logs%localhost.*.log
```

以下のメッセージを探します。

```
java.lang.OutOfMemoryError
```

この問題を修正するには、割り当てられるメモリの量を増加させます。

この値を増やすには、以下の手順に従います。

1. レジストリ エディタを開いて、以下のキーを選択します。
 - x86 オペレーティング システムの場合
HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun
2.0\CASAD2DWebSvc\Parameters\Java
 - x64 オペレーティング システムの場合
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun
2.0\CASAD2DWebSvc\Parameters\Java

2. 以下のいずれかを行います。
 - ログ ファイル内のメッセージが以下の場合：
java.lang.OutOfMemoryError: PermGen space
Options の値に以下を追加します。
-XX:PermSize=128M -XX:MaxPermSize=128M
注: 使用している環境に合わせて「XX:MaxPermSize」の値を増加する必要がある場合があります。
 - ログ ファイル内のメッセージが以下のいずれかの場合：
java.lang.OutOfMemoryError: Java heap space
java.lang.OutOfMemoryError: GC overhead limit exceeded
以下の DWORD の値を増加させます。
JvmMx
3. CA ARCserve D2D Web サービスを再起動します。

症状 2

スケジュールされたバックアップがスキップされ、実行を停止します。

解決策 2

同時バックアップの MAX 値を 20 以下に設定している場合、以下の手順に従います。

1. 以下の DWORD の値を増加させます。
JvmMx=256
注: この DWORD は解決策 1 で参照されています。
2. Options の値に以下を追加します。
-XX:MaxPermSize=128M
注: この DWORD は解決策 1 で参照されています。

同時バックアップの MAX 値を 20 より大きく 50 より小さい値に設定している場合、以下の手順に従います。

1. 以下の DWORD の値を増加させます。

```
JvmMx=512
```

注: この DWORD は解決策 1 で参照されています。

2. Options の値に以下を追加します。

```
-XX:MaxPermSize=256M
```

注: この DWORD は解決策 1 で参照されています。

変更ブロックのトラッキングに失敗する

Windows で該当。

症状:

仮想マシンバックアップが失敗し、変更ブロックのトラッキングが仮想マシンで有効です。

解決方法:

以下の表では、変更ブロックのトラッキングが有効な仮想マシンバックアップの失敗につながる環境条件について説明します。

条件	ソリューション
ユーザが生成したスナップショットが仮想マシン上に存在し、変更ブロックのトラッキングが無効です。	フルバックアップジョブが続行されるように、変更ブロックのトラッキングを有効化またはリセットします。 注: フルバックアップジョブは、VMDK ファイルからのデータ使用/未使用ブロックに対して実行されます。
正しくないバージョンの VMware ハードウェアが仮想マシンにインストールされています。	VMware ハードウェアバージョン 7.0 以降が仮想マシンにインストールされていることを確認します。
正しくないバージョンの ESX Server が仮想マシンにインストールされています。	ESX Server バージョン 4.0 以降が仮想マシンにインストールされていることを確認します。

条件	ソリューション
ESX Server システムでハードシャットダウンが発生しました。ハードシャットダウンは変更ブロックのトラッキングバックアップの失敗につながる場合があります。	CA ARCserve Central Host-Based VM Backup は、仮想マシンの変更ブロックのトラッキングを自動的に有効化します。
仮想マシンの電源がオンの状態で ESX Server システムの (クリーン) 再起動が発生しました。	CA ARCserve Central Host-Based VM Backup は、仮想マシンの変更ブロックのトラッキングを自動的に有効化します。
仮想マシンが Storage vMotion を使用して移動されました。	CA ARCserve Central Host-Based VM Backup は、仮想マシンの変更ブロックのトラッキングを自動的に有効化します。

ESXi ライセンスのためにバックアップが失敗する

Windows プラットフォームで有効

症状:

CA ARCserve D2D のフル、増分、検証のバックアップジョブが失敗します。以下のようなメッセージが CA ARCserve D2D アクティビティ ログに表示されます。

VM サーバ <server_name> には、購入済み ESX ライセンスがありません

解決方法:

VMware の制約により、無償ライセンスによる ESXi サーバ上で実行される仮想マシンはバックアップできません。これらの VM を保護するには、購入したライセンスを適用する必要があります。

VM にスナップショットがあるためバックアップが失敗する

Windows プラットフォームで有効

症状:

CA ARCserve D2D のフル、増分、検証のバックアップ ジョブが失敗します。以下のようなメッセージが CA ARCserve D2D アクティビティ ログに表示されます。

仮想マシン上にスナップショットが存在するため、アプリケーションは、仮想マシン上の変更されたブロックのトラッキングを有効にできません。この問題を修正するには、スナップショットを削除してから、バックアップを再サブミットしてください。

解決方法:

変更されたブロックのトラッキング (CBT) 機能を無効にしている場合、vCenter Server から直接状態をテストするなどの目的でスナップショットを手動で作成すると、次回スケジュールされたバックアップ ジョブが失敗します。これは、変更されたブロックのトラッキング (CBT) 機能が無効であるために、手動で作成されたスナップショットがアプリケーションで認識されないためです。スナップショットを削除し、バックアップ ジョブを再サブミットしてください。CA ARCserve Central Host-Based VM Backup は自動的に CBT を有効にします。CBT が有効な状態でスナップショットを手動作成した場合、バックアップは失敗しません。

注: CBT 機能は、vSphere クライアントから手動で有効にすることができません。

バックアップが失敗し、バックアップ プロキシ システムのイベント ログにイベント 1530 がログ記録される

Windows プラットフォームで有効

症状:

CA ARCserve Central Host-Based VM Backup ジョブが失敗します。バックアップ プロキシ システムのアプリケーション イベント ログにイベント 1530 がログ記録されます。

再現に必要な環境と手順:

- 仮想マシンに Microsoft SQL Server または Microsoft Exchange Server がインストールされている。
- 管理者アカウントまたは管理者グループのメンバーであるアカウントを使用して、ユーザが CA ARCserve Central Host-Based VM Backup プロキシ サーバにログインする、または、すでにログインしている。
- バックアップ ジョブが開始されたら、プロキシ サーバからログアウトする。
- バックアップ ジョブが失敗し、アプリケーション イベント ログにイベント 1530 がログ記録される。

警告 ... Microsoft-Windows-User プロファイル サービス 1530 なし レジストリ ファイルは他のアプリケーションまたはサービスで使用されています。 ファイルはすぐにアンロードされます。 レジストリ ファイルを保持しているアプリケーションまたはサービスはこれ以降正しく機能しない可能性があります。

原因:

Windows Server 2008 には、コンピュータからログアウトするとユーザのプロファイルをアンロードするユーザ プロファイル サービスが含まれています。 その結果、COM オブジェクトが作成されない場合があります。 これにより Host-Based VM Backup は COM モジュールを呼び出すことができません。

解決方法:

バックアップ ジョブの失敗を防ぐには、以下の手順に従います。

注: この方法によって問題が解決されるのは、上記のすべての症状が発生している場合です。

1. 管理者アカウントまたは管理者グループのメンバであるアカウントを使用して、Host-Based VM Backup プロキシサーバにログインします。
2. [ファイル名を指定して実行] ダイアログ ボックスで「gpedit.msc」と入力し、ローカルグループ ポリシー エディタを開始します。
3. ローカルグループ ポリシー エディタで、[コンピュータの構成] - [管理用テンプレート] - [システム] - [ユーザー プロファイル] を展開します。
4. [ユーザー プロファイル] ディレクトリにある、[ユーザーのログオフ時に強制的にユーザー レジストリをアンロードしない] をダブルクリックし、[ユーザーのログオフ時に強制的にユーザー レジストリをアンロードしない] ダイアログ ボックスを開きます。
5. [ユーザーのログオフ時に強制的にユーザー レジストリをアンロードしない] ダイアログ ボックスで [有効] をクリックし、次に、[OK] をクリックします。

注: レジストリに DisableForceUnload という値が追加されています。

6. Host-Based VM Backup サーバを再起動します。

ホット追加転送モードを指定したのに NBD 転送モードでバックアップが完了する

Windows プラットフォームで有効

症状:

仮想マシンのバックアップに[ホット追加転送モード](#) (P. 291)を指定した場合に、[NBD 転送モード](#) (P. 291)でバックアップが完了します。

解決方法:

CA ARCserve Central Host-Based VM Backup では、ESX Server システム上にある仮想マシンをバックアップできます。ホット追加転送モードを使用して、仮想マシンをバックアップするとき、CA ARCserve D2D 仮想マシンプロキシサーバ上で各 SCSI コントローラに最大 15 の仮想ディスクを接続できます。15 を超える仮想ディスクを含むバックアップをサブミットし、CA ARCserve D2D 仮想マシンプロキシサーバ上に 1 つの SCSI コントローラしかない場合、すべての仮想マシンをその 1 つの SCSI コントローラに接続することはできません。結果として、CA ARCserve Central Host-Based VM Backup は NBD 転送モードのデータをバックアップします。

この動作を防ぐには、CA ARCserve D2D 仮想マシンプロキシサーバ上に、バックアップジョブですべての仮想マシンに接続できる数の SCSI コントローラがあることを確認してください。

増分バックアップ ジョブが検証バックアップ ジョブとして処理される

Windows で該当。

症状:

Htadd 転送モードを使用して処理する増分バックアップジョブをサブミットまたはスケジュールすると、以下のように動作します。

- 増分ジョブが検証バックアップジョブに切り替わります。増分バックアップジョブが検証バックアップジョブに変換されたことがジョブのアクティビティログエントリによって示されます。
- バックアップされた仮想マシンの VI クライアント内のスナップショットマネージャには、統合されたヘルパー スナップショットが含まれています。
- 影響を受けた仮想マシンの VI クライアント内の [設定の編集] ダイアログボックスに、バックアッププロキシシステムにエラーディスクが接続されていることが示されます。エラーディスクと関連付けられた VMDK URL は、バックアッププロキシシステムと関連付けられた VMDK URL と同じ URL ではありません。

解決方法:

この動作を修正するには、VMware ナレッジ ベース記事 1003302 (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003302) に説明されているガイドラインを使用して、エラーのある VMDK ファイル (ディスク) をバックアップ プロキシ システムから削除します。さらに、VMware では、データ ストア上の空き容量を仮想マシンの累積ファイル サイズの 2 倍に設定することを推奨します。

ブロックを識別できないため、バックアップ ジョブに失敗する

Windows で該当。

症状:

特定の仮想マシンで、すべてのバックアップ ジョブが失敗し、以下のメッセージがアクティビティ ログに表示されます。

本アプリケーションでは、仮想マシン上で使用または変更されたブロックを識別できませんでした。この問題が発生するのは、仮想マシンの実行中に ESX Server システムが再起動する場合です。次回バックアップ ジョブを実行すると、アプリケーションは変更ブロックのトラッキングをリセットし、検証バックアップ操作を実行します。

解決方法:

この動作を解決するには、仮想マシン上でディスク統合操作を実行します。ディスク統合を実行するには、以下の手順に従います。

1. VMware VI クライアントを開きます。
2. 影響を受けた仮想マシンの ESX Server システムを展開します。
3. 影響を受けた仮想マシンを右クリックして [スナップショット] を選択し、次にポップアップ メニューの [統合] をクリックしてディスクを統合します。
4. バックアップ ジョブを再サブミットします。

VMDK ファイルを開けない

Windows プラットフォームで有効

症状:

NBD（または LAN）転送モードで複数の同時バックアップジョブが失敗します。以下のようなメッセージがアクティビティログに表示されます。

VMDK ファイルを開けません。

解決方法:

これは、VMware 接続の制限事項です。以下の NFC（ネットワーク ファイル コピー）プロトコルの制限が適用されます。

- ESX 4：直接接続の最大数 9
- vCenter Server を介した ESX 4：接続の最大数 27
- ESXi 4：直接接続の最大数 11
- vCenter Server を介した ESXi 4：接続の最大数 23

ディスク間で接続を共有することはできません。最大接続数の制限は、SAN およびホット追加接続には適用されません。NFC クライアントが正しくシャットダウンしない場合、接続は 10 分間有効なままにできます。

ノード名を変更した後にノードがノード画面に表示されない

Windows プラットフォームで有効

症状:

ノードが [ノード] 画面に追加された後、ホスト名が変更されました。ノードが [ノード] 画面に表示されなくなりました。

解決方法:

これは予期された動作です。CA ARCserve Central Host-Based VM Backup では、ノード画面で追加されたノード名を保持します。ノード名を変更した場合、アプリケーションはノードを検出できません。そのため、ノードがノード画面に表示されません。

名前が変更されたノードがノード画面に表示されるようにするには、以下の手順に従います。

1. ノードの名前を変更します。
2. [ノード] 画面を開き、名前が変更された [ノードを削除](#) (P. 59) します。
3. 新しい名前を使用して、ノードを追加します。

ポリシーを CA ARCserve D2D サーバに保存または割り当てる際に複数の接続エラーが発生する

すべての Windows プラットフォームで有効。

症状:

ポリシーを CA ARCserve D2D サーバに保存または割り当てようとする、以下のエラー メッセージが表示されます。

バックアップ先を検証できませんでした。同一ユーザによる複数のユーザ名を使用した、サーバまたは共有リソースへの複数の接続は許可されません。サーバまたは共有リソースへのこれまでの接続をすべて解除した後、再度試行してください。

解決方法:

ポリシーを CA ARCserve D2D サーバに保存または割り当てようとして上記のメッセージが表示された場合、以下を実行することによって問題を解決できることがあります。

- ユーザ名フィールドに、「マシン (またはドメイン) 名¥ユーザ名」と指定します。
- 共有フォルダがホストされているリモートサーバに移動し、CA ARCserve Central Applications サーバまたは CA ARCserve D2D サーバからセッションをすべて削除します。セッションを削除するには、以下のいずれかを実行してください。
 - 以下のコマンドラインを実行します。

```
net session ¥machinename /delete
```
 - 以下のディレクトリに移動して、セッションを切断します。

```
Compmgmt.msc > System Tools > Shared Folders > Sessions > Disconnect session
```
- リモート共有フォルダにアクセスするために同じユーザ名を使用していることを確認します。
- 保存してポリシーを再度展開します。

ESX Server にアクセスできないために仮想マシンのバックアップが失敗する

Windows プラットフォームで有効

症状:

仮想マシン バックアップが失敗します。以下のようなメッセージがアクティビティ ログに表示されます。

仮想マシン スナップショットの作成に失敗しました。

解決方法:

1 つの ESX Server システム上で複数のバックアップを同時に実行すると、仮想マシンのバックアップが失敗する場合があります。複数のバックアップを複数の ESX Server システム上で同時に実行すると、この問題は発生しません。仮想マシンをバックアップするために、CA ARCserve Central Host-Based VM Backup は、仮想マシン上に存在するデータのスナップショットを作成します。複数のスナップショット処理が 1 つのシステム上で同時に実行されると、ESX Server システムが応答を停止する場合があります。ESX Server システムによる応答の停止は一時的なものです。バックアップ処理は中断され、バックアップ処理は失敗します。

バックアップの失敗を防ぐには、ユーザの環境に適したソリューションを使用します。

- 同時にバックアップする仮想マシンの数を減らします。たとえば、8 つの仮想マシンを同時にバックアップしている場合は、7 つの仮想マシンに減らし、バックアップを再サブミットして、結果を分析します。必要に応じて、バックアップが失敗しなくなるか、前述のメッセージがアクティビティ ログに表示されなくなるまでバックアップする仮想マシンの数を減らします。

バックアップの仮想マシン数を減らすには、ポリシーから仮想マシンを割り当て解除します。詳細については、「仮想マシンからのポリシーの割り当て解除」を参照してください。

- 同時バックアップ数に制限を定義します。この方法では、環境内で同時に実行できるバックアップ ジョブの数を制御できます。詳細については、「[同時バックアップ数の制限の定義 \(P. 202\)](#)」を参照してください。

Internet Explorer 8、9、Chrome で追加した新しいタブのリンクが正常に起動しない

Windows で有効

症状:

新しいタブのリンクをナビゲーションバーに追加し、HTTPS URL を指定した場合、新しいタブをクリックすると以下のエラーメッセージが表示されます。

- Internet Explorer 8 および 9

コンテンツは、有効なセキュリティ証明書により署名されていないため、ブロックされました。

- Chrome

このウェブサイトはご利用いただけません。

解決方法:

Internet Explorer でこの問題を修正するには、以下の手順に従います。

- Internet Explorer 8

メッセージバーをクリックし、ブロックされたコンテンツの表示を選択します。

- Internet Explorer 9

ページ下部のメッセージバーからコンテンツの表示ボタンをクリックします。ページが更新され、追加されたタブリンクが正常に開きます。

Chrome でこの問題を修正するには、以下の手順に従います。

手順 1 - 証明書のエクスポート

1. Chrome で新しいタブを開き、HTTPS URL を入力します。
サイトのセキュリティ証明書が信頼されたものでないことを示す警告メッセージが表示されます。
2. アドレスバーから、'X' の付いたロックをクリックします。
ポップアップ ウィンドウが開き、証明書情報のリンクが表示されます。
3. 証明書情報リンクをクリックします。
[証明書] ダイアログ ボックスが表示されます。
4. [証明書] タブをクリックし、[ファイルにコピー] をクリックして
証明書をローカル コンピュータに保存します。
証明書のエクスポート ウィザード ダイアログ ボックスが表示されま
す。

5. [次へ] をクリックし、ファイルをエクスポートするために使用する形式を選択します。

注: デフォルトでは DER encoded binary X.509 (.CER) が選択されています。

6. [次へ] をクリックし、証明書を保存する場所を選択します。
7. [次へ] をクリックして証明書のエクスポート ウィザードを完了し、[完了] をクリックします。

証明書が正常にエクスポートされます。

手順 2 - 証明書のインポート

1. Chrome で [ツール] - [オプション] を開きます。
[オプション] 画面が開きます。
2. [高度な設定] オプションを選択し、[証明書の管理] をクリックします。
[証明書] ダイアログ ボックスが開きます。
3. [インポート] をクリックします。
証明書のインポート ウィザードが開きます。
4. [次へ] をクリックし、ローカル コンピュータに保存した証明書を参照します。

5. [次へ] をクリックし、証明書ストアを開きます。
[証明書ストア] ダイアログ ボックスが表示されます。
6. [参照] をクリックし、[証明書ストアの選択] ダイアログ ボックスを開きます。
[証明書ストアの選択] ダイアログ ボックスが表示されます。
7. ファイルリストから [信頼されたルート証明機関] を選択して [OK] をクリックします。
[証明書ストア] ダイアログ ボックスが表示されます。
8. [次へ] をクリックして証明書のインポート ウィザードを完了し、[完了] をクリックします。
セキュリティの警告ダイアログ ボックスが表示され、証明書をインストールすることが通知されます。
[はい] をクリックして条件に同意します。

証明書が正常にインポートされます。

Internet Explorer 8 および 9 で、新しいタブの追加リンク、RSS フィード、およびソーシャル ネットワーキング フィードバックが正常に起動しない

Windows で有効

症状:

HTTPS CA ARCserve Central Applications URL の場合 :

新しいタブのリンクをナビゲーションバーに追加し、HTTP URL を指定した場合、新しいタブおよび [フィードバック] リンクをクリックすると以下のエラー メッセージが表示されます。

Web ページへのナビゲーションは取り消されました。

また、RSS フィードが表示されません。

注: 新しく追加されたタブのリンクを選択しなくても、[フィードバック] リンクをクリックした場合にもエラー メッセージが表示されます。

解決方法:

この問題を解決するには、以下の手順に従います。

■ Internet Explorer 8

ログインし、ポップアップセキュリティ警告メッセージの「セキュリティで保護された Web ページ コンテンツのみ表示しますか」に対して [いいえ] をクリックします。これにより、保護されていないコンテンツが Web ページに表示できるようになります。

■ Internet Explorer 9

ページ下部に表示されるメッセージバー上で「コンテンツをすべて表示」ボタンをクリックします。ページが更新され、追加されたタブリンクが正常に開きます。

日本語キーボードを使用して[フィルタ]フィールドのワイルドカードとしてアスタリスクまたはアンダースコアを指定できない

Windows で有効

症状:

米国と日本のキーボードではキーコードが異なるため、日本のキーボードでは、以下のフィルタ フィールドに対して、ワイルドカード文字 "*" と、アンダースコア文字 "_" などの特殊文字を入力することができません。

■ Firefox 上でのみ発生:

- [ノード] - [グループの追加] - [ノード名フィルタ] フィールド
- [ポリシー] - [ポリシーの割り当て] タブ - [割り当てと割り当て解除] - [ノード名フィルタ] フィールド
- [リストア] - [ノードエクスプローラ] - [ノード名] フィールド
- [ノード] - [オート ディスカバリの結果からのノードの追加] - [保護するノード] - [ノード名] フィールド

解決方法:

この問題が発生するのを防ぐには、メモ帳などのテキスト エディタ アプリケーションを開きます。テキスト エディタで、"*" や "_" などの特殊文字を入力します。テキスト エディタから該当フィールドにその文字をコピーします。

仮想マシンの復旧で指定とは異なる転送モードが使用される

Windows プラットフォームで有効

症状:

仮想マシンの復旧で、レジストリ キーでの指定とは異なる転送モードが使用されます。

解決方法:

この動作はシンディスクに影響します。この問題を修正するには、以下の手順に従います。

1. CA ARCserve Central Host-Based VM Backup 仮想マシンにログインします。
2. レジストリ エディタ を開き、以下のキーを探します。
HKEY_LOCAL_MACHINE¥SOFTWARE¥CA¥CA ARCserve D2D¥AFRestoreDll
3. レジストリ キー "EnforceTransportForRecovery" を以下のいずれかの転送モードに設定します。
 - NBD
 - NBDSSL
4. 仮想マシンの復旧をサブミットします。

第 6 章: ベストプラクティスの適用

このセクションには、以下のトピックが含まれています。

[仮想マシンのベア メタル復旧の実行 \(P. 179\)](#)

[同時バックアップ数の制限の定義 \(P. 202\)](#)

[VMVixMgr ログ ファイルに保持されるメッセージ容量を増加させる \(P. 203\)](#)

[CA ARCserve D2D バックアップ プロキシの保護 \(P. 204\)](#)

[インストール処理のオペレーティング システムに対する影響 \(P. 205\)](#)

仮想マシンのベア メタル復旧の実行

バックアップ ジョブの実行時に仮想マシンの電源がオンにされている場合は、ベア メタル復旧がサポートされます。

ベア メタル復旧 (BMR) とは、オペレーティング システムとソフトウェア アプリケーションの再インストール、およびその後のデータや設定のリストアといった、「ベア メタル」からコンピュータ システムをリストアするプロセスです。BMR プロセスでは、ハードウェアが異なる場合でも、わずかな作業でコンピュータ全体をリストアすることができます。BMR を実行できるのは、ブロック レベルのバックアップ プロセス中に、CA ARCserve D2D がデータだけではなく、以下に関連する情報も取得しているためです。

- オペレーティング システム
- インストールされたアプリケーション
- 環境設定
- 必要なドライバ

ベアメタルからコンピュータシステムを再構築するのに必要なすべての関連情報は、連続するブロックにバックアップされ、バックアップ場所に格納されます。



ビデオ

CA サポート :

ベアメタル復旧を実行する方法

http://www.arcserve.com/arcserve2d/r16/redirect.php?item=video_bmr_support

YouTube :

ベアメタル復旧を実行する方法

http://www.arcserve.com/arcserve2d/r16/redirect.php?item=video_bmr_youtube

BMR を実行する前に、以下を準備する必要があります。

- 以下のいずれか 1 つ。
 - CA ARCserve D2D 製品と共にリリースされたカスタマイズ済み Windows PE イメージ (D2DBMR.ISO)。
 - ブートキットウィザードから作成された BMR USB メモリおよび、Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 のインストールメディア (CD/DVD)。(必要に応じて、インストールメディアの代わりに Windows PE イメージを USB メモリと共に使用して、BMR 中に必要なドライバをロードできます)。

注: USB メモリを使用している場合、Windows PE イメージで使用できないドライバを追加できます。
- 利用可能なフルバックアップが少なくとも 1 つ。
- 復旧する仮想マシンおよびソースサーバ上にインストールされた少なくとも 1GB の RAM。
- VMware 仮想マシンを、物理サーバとして動作するよう設定された VMware 仮想マシンに復旧するには、VMware Tools アプリケーションがデスティネーション仮想マシンにインストールされていることを確認します。

ダイナミックディスクのリストアは、ディスクレベルでのみ実行できます。ダイナミックディスク上のローカルボリュームにデータがバックアップされた場合、このダイナミックディスクを BMR 実行中にリストアすることはできません。このシナリオでは、BMR 実行中にリストアするには、以下のいずれかのタスクを実行し、次に、コピーした復旧ポイントから BMR を実行する必要があります。

- 別のドライブ上のボリュームにバックアップする。
- リモート共有にバックアップする。
- 復旧ポイントを別の場所にコピーする。

注: ダイナミックディスクへ BMR を実行する場合、BMR 前のディスク操作（ボリュームの削除やクリーニングなど）を実行しないでください。実行した場合、ディスクの存在が認識されない可能性があります。

ブートキットイメージを作成する際にどの方法を選択しても、BMR プロセスは基本的に同じです。

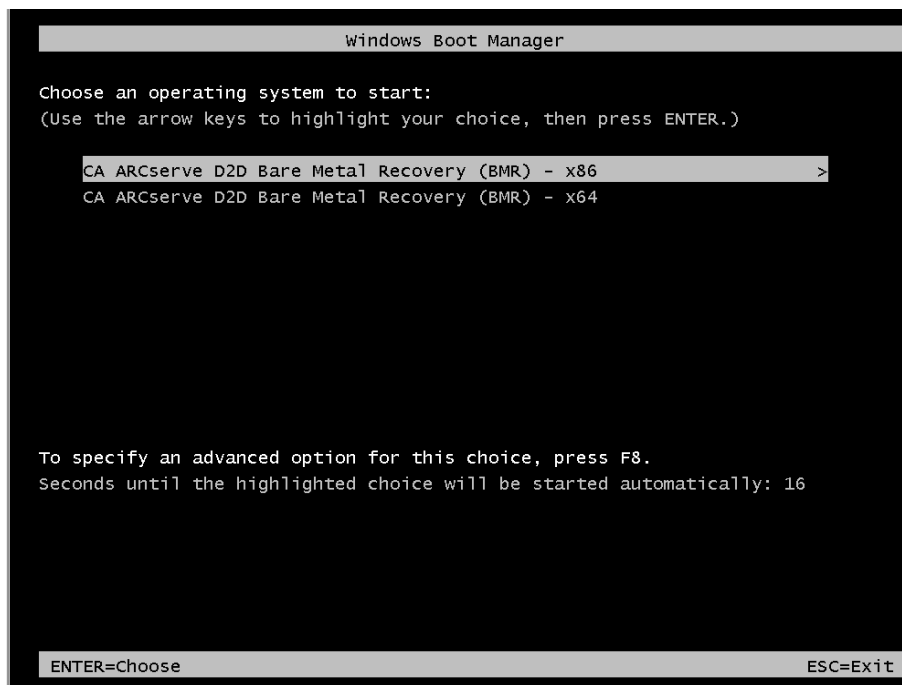
ベアメタル復旧を使用してデータをリストアする方法

1. 保存したブートキットイメージメディアを挿入し、コンピュータを起動します。
 - 保存した Windows PE イメージを使用している場合は、ブートキットイメージ CD/DVD を挿入します。
 - USB メモリを使用している場合は、Windows Server インストール CD/DVD を挿入し、保存したブートキットイメージが含まれる USB メモリを接続します。

BIOS セットアップユーティリティ画面が表示されます。

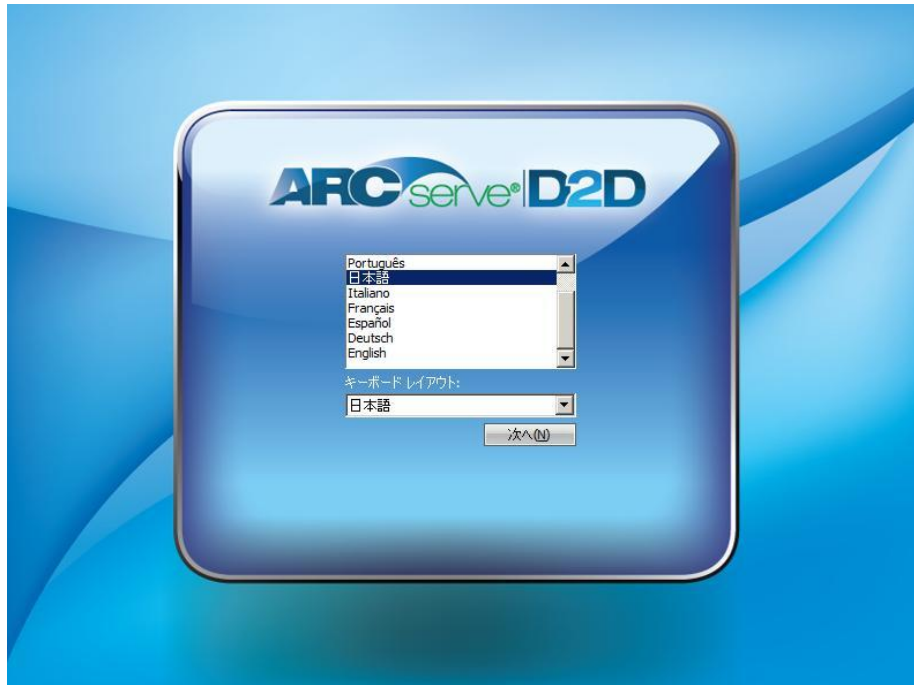
2. BIOS セットアップユーティリティ画面から、ブートプロセスを起動する CD-ROM ドライブのオプションを選択します。

注: Windows PE イメージを使用して BMR を実行する場合は、アーキテクチャ (x86/x64) を選択し、Enter キーを押して続行する必要があります。



3. CA ARCserve D2D の言語選択画面が表示されます。言語を選択し、[次へ] をクリックして続行します。

注：BMR USB メモリ、および Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 インストールメディア（CD/DVD）を使用して BMR を実行する場合、Multilingual User Interface（MUI）がサポートされていないならば、この言語選択画面は表示されません。



ベアメタル復旧プロセスが開始され、最初の BMR ウィザード画面が表示されます。

ARCserve D2D™ Bare Metal Recovery

CA ARCserve D2D ベアメタル復旧 (BMR)
- BMR の種類を選択してください

回復の種類を指定してください:

- CA ARCserve D2D を使用してバックアップされたデータを回復する**
(CA ARCserve D2D または CA ARCserve Host-Level Virtual Machine Backup アプリケーションを使用するバックアップセッション)
- Hyper-V Virtual Standby VM を使用して回復する**
(CA ARCserve Central Virtual Standby を使用して仮想変換が実行された場合にのみ、データを回復できます)
- VMware Virtual Standby VM を使用して回復する**
(CA ARCserve Central Virtual Standby を使用して仮想変換が実行された場合にのみ、データを回復できます)

▲ ユーティリティ(U) 戻る(B) 次へ(N) 中止(A)

4. BMR ウィザード画面で、実行する BMR の種類を選択します。

■ **CA ARCserve D2D を使用してバックアップされたデータを回復する**

CA ARCserve D2D を使用してバックアップされたデータを回復します。このオプションは、CA ARCserve D2D または CA ARCserve Central Host-Based VM Backup アプリケーションで実行されたバックアップセッションに関して使用されます。

このオプションを選択した場合は、これ以降の手順を続行します。

■ **Hyper-V 仮想スタンバイ VM を使用して回復する**

Hyper-V 仮想マシンに対して仮想変換が実行されたマシンのデータを回復します。このオプションは CA ARCserve Central Virtual Standby アプリケーションに関して使用されます。

注: このオプションを使用する場合、VHD ファイル (Hyper-V 用) への仮想変換が CA ARCserve Central Virtual Standby によって実行された場合のみデータを回復できます。

このオプションを選択した場合は、「Hyper-V 仮想スタンバイ VM を使用した回復」を参照してこの手順を続行してください。

■ **VMware 仮想スタンバイ VM を使用して回復する**

VMware 仮想マシンに対して仮想変換が実行されたマシンのデータを回復します。このオプションは CA ARCserve Central Virtual Standby アプリケーションに関して使用されます。

注: このオプションを使用する場合、VMDK ファイル (VMware 用) への仮想変換が CA ARCserve Central Virtual Standby によって実行された場合のみデータを回復できます。

このオプションを選択した場合は、「VMware 仮想スタンバイ VM を使用した回復」を参照してこの手順を続行してください。

5. [次へ] をクリックします。

[復旧ポイントの選択] ウィザード画面が表示されます。



6. [復旧ポイントの選択] ウィザード画面で、バックアップイメージ用の復旧ポイントが含まれるマシン(またはボリューム)を選択します。

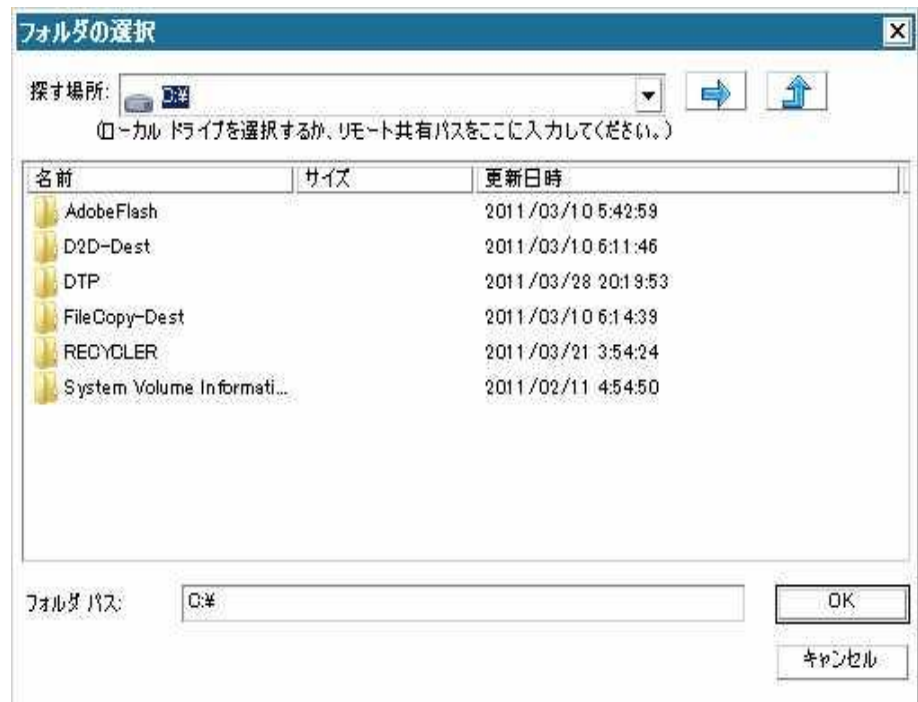
CA ARCserve D2D を使用すると、任意のローカルドライブまたはネットワーク共有から復旧を実行できます。

- ローカルバックアップから復旧を実行する場合、BMR ウィザードは、復旧ポイントが含まれるすべてのボリュームを自動的に検出して表示します。
- リモート共有から復旧を実行する場合、復旧ポイントが格納されているリモートロケーションを参照します。復旧ポイントを含むマシンが複数ある場合、すべてのマシンが表示されます。

また、リモートマシンのアクセス情報(ユーザ名およびパスワード)が必要な場合があります。

注: リモートの復旧ポイント参照する場合、ネットワークが稼働中である必要があります。必要な場合は、ネットワーク設定情報を確認/更新したり、必要なドライバを[ユーティリティ]メニューからロードすることができます。

7. BMR モジュールがローカルデスティネーションボリュームを検出できない場合、[フォルダの選択] ダイアログボックスが自動的に表示されます。バックアップが存在するリモート共有を指定します。



8. バックアップの復旧ポイントが保存されているフォルダを選択し、[OK] をクリックします。（矢印アイコンをクリックすると、選択した場所への接続を検証できます）。

BMR ウィザード画面には、以下の情報が表示されます。

- マシン名（左上のペイン）
- 関連するバックアップ情報（右上のペイン）
- 対応するすべての復旧ポイント（左下のペイン）。

注: UEFI システムに対して BMR を実行するには、UEFI モードでコンピュータを起動する必要があります。BMR は、別のファームウェアを持つコンピュータのリストをサポートしていません。ブートファームウェアが BIOS ではなく UEFI であることを確認するには、[ユーティリティ] - [バージョン情報] をクリックします。



9. リストアする復旧ポイントを選択します。

選択した復旧ポイントの関連情報が表示されます(右下のペイン)。表示される情報には、実行した(保存した)バックアップの種類、バックアップ先、バックアップされたボリュームなどが含まれます。

復旧ポイントに暗号化されたセッション(復旧ポイントの時計アイコンにロックがかけられます)が含まれる場合、パスワードを要求する画面が表示されます。セッションパスワードを入力して、[OK]をクリックします。



暗号化パスワードの入力

現在のパスワード長: 0 文字
最大のパスワード長: 23 文字

OK

キャンセル

注: ご使用のマシンがドメインコントローラの場合、CA ARCserve D2D は BMR 実行中に Active Directory (AD) データベースファイルの「権限のないリストア」(Non-Authoritative Restore) をサポートします (CA ARCserve D2D は MSCS クラスタのリストアをサポートしません)。

10. リストア対象の復旧ポイントを選択したことを確認し、[次へ] をクリックします。

BMR ウィザード画面には、利用可能な復旧モードのオプションが表示されます。



11. 復旧モードを選択します。

利用可能なオプションは、[拡張モード] と [高速モード] です。

- 復旧処理をカスタマイズする場合は、[拡張モード] を選択します。
- 復旧処理中にユーザの介入を最小限に抑えるには、[高速モード] を選択します。

デフォルト：高速モード

注: 残りの手順は、[拡張モード] を選択した場合のみ適用されます。この手順では、BMR 処理を実行するための情報が示されます。

12. [次へ] をクリックします。

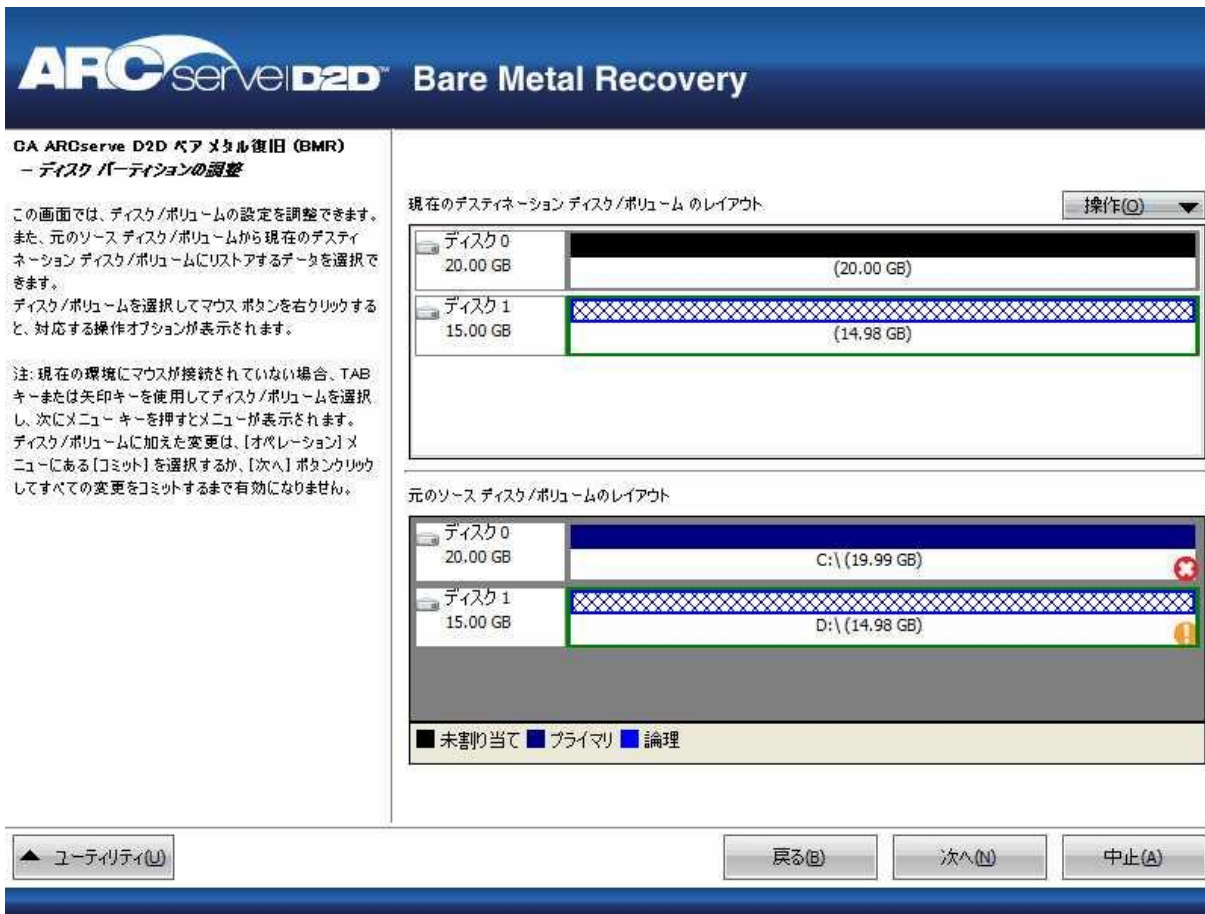
BMR ユーティリティによって復旧するマシンの検索が開始され、対応するディスクパーティション情報が表示されます。

上部ペインには、現在のマシン（ターゲットマシン）上のディスク設定が表示されます。下部ペインには、元のマシン（ソースマシン）上のディスクパーティション情報が表示されます。

重要: 下部ペインで、ソース ボリュームに赤いXアイコンが表示されている場合、このボリュームにはシステム情報が含まれており、ターゲット ボリュームに割り当てられていない (マップされていない) ことを示しています。ソース ディスクにあるこのシステム情報ボリュームは、**BMR** 実行中にターゲット ディスクに割り当て、リストアする必要があります。これらを実行しない場合、リブートできません。

注: ユーザが **BMR** を実行し、ブートディスクとして設定されていないディスクにシステム ボリュームをリストアした場合、**BMR** の完了後にマシンを起動できません。正しく設定されたブートディスクにシステム ボリュームをリストアしていることを確認してください。

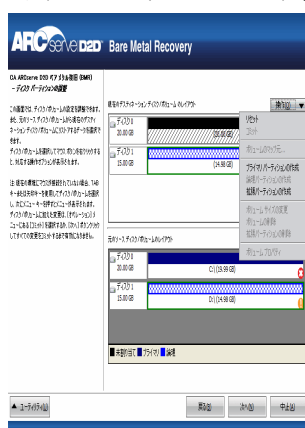
注: 別のディスク/ボリュームにリストアする場合、新しいディスク/ボリュームの容量は同じサイズか、元のディスク/ボリュームより大きいサイズにする必要があります。また、ディスク サイズの変更はベーシックディスクのみに対応しています。ダイナミック ディスクには対応していません。



- 表示されている現在のディスク情報が正しくない場合、[ユーティリティ] メニューにアクセスし、必要なドライバを確認することができます。
- 必要に応じて、ターゲット ボリューム ペインで [操作] ドロップダウンメニューをクリックすると、利用可能なオプションを表示できます。

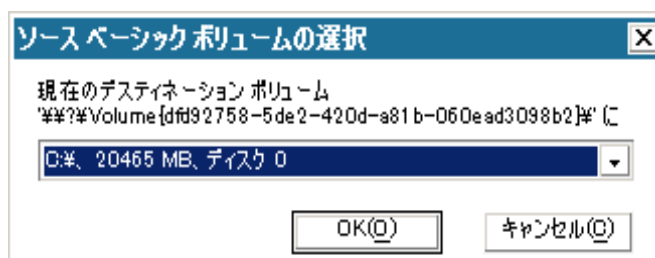
このメニューから、既存のパーティションをリセットしたり、ソースボリューム上のディスクパーティションに対応する新しいパーティションを作成することができます。（「リセット」とは、環境設定ファイルおよび現在の OS からソースとターゲットのディスクレイアウト情報を再ロードし、ユーザによって変更されたすべてのディスクレイアウト情報を破棄することを意味します。）

注: 別のディスクにマップする場合、マップされた各ターゲット ボリュームの容量は同じサイズか、対応するソース ボリュームより大きくする必要があります。



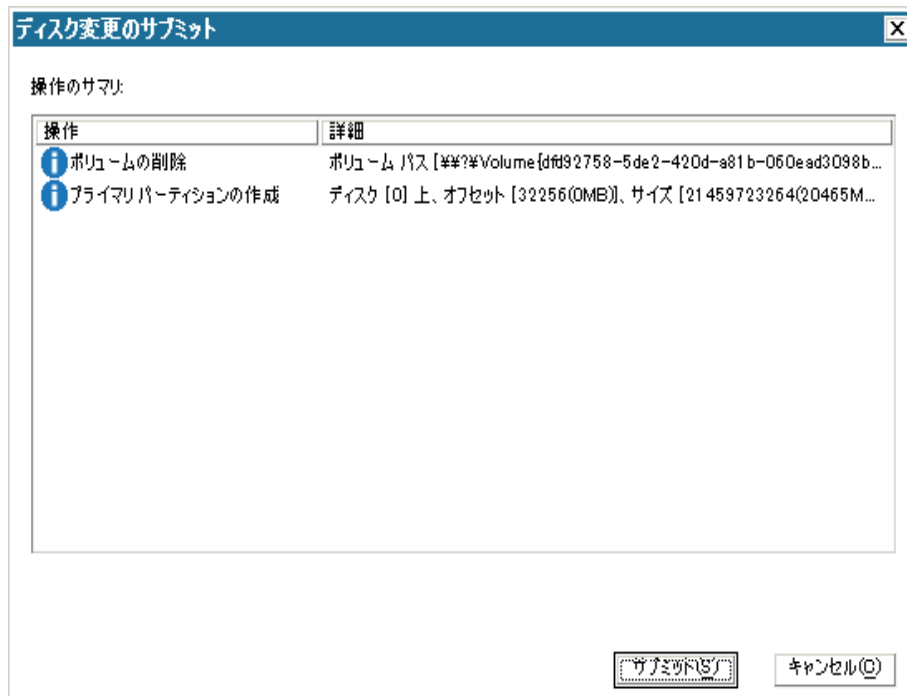
- それぞれのターゲット ボリュームをクリックし、コンテキストメニューから [ボリュームのマップ元] オプションを選択すると、このターゲット ボリュームにソース ボリュームを割り当てることができます。

[ソース ベーシック ボリュームの選択] ダイアログ ボックスが開きます。



16. [ソースベーシックボリュームの選択] ダイアログボックスから、ドロップダウンメニューをクリックして利用可能なソースボリュームを選択し、選択したターゲットボリュームに割り当てます。[OK]をクリックします。
- ターゲットボリューム上に表示されるチェックマークアイコンは、このターゲットボリュームがマップされたことを示しています。
 - ソースボリューム上の赤いXアイコンが緑色のアイコンに変化すると、このソースボリュームがターゲットボリュームに割り当てられたことを示します。
17. リストアするすべてのボリューム、およびシステム情報を含むすべてのボリュームがターゲットボリュームに割り当てられていることを確認した後、[次へ] をクリックします。

[ディスク変更のサブミット] 画面が開き、選択した操作のサマリが表示されます。作成中の個々の新しいボリュームについては、対応する情報が表示されます。



18. サマリ情報が正しいことを確認した後、[サブミット] をクリックします。(情報が正しくない場合は、[キャンセル] をクリックします)。

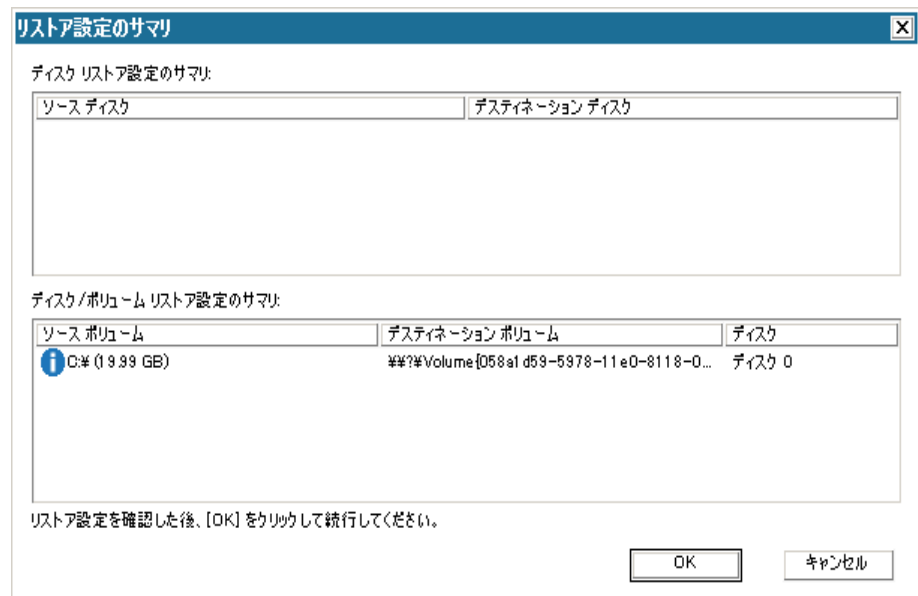
注: ハードドライブへのすべての操作は、サブミットするまで適用されません。

ターゲットマシン上に新しいボリュームが作成され、対応するソースマシンにマップされます。

19. 変更が完了した後、[OK] をクリックします。

[リストア設定のサマリ] 画面が開き、リストアするボリュームのサマリが表示されます。

注: リストアサマリウィンドウの下部にある「デスティネーションボリューム」列に表示されるドライブ文字は、Windows プレインストール環境 (WinPE) から自動的に生成されます。これらのドライブ文字は、「ソースボリューム」列に表示されるドライブ文字とは異なる場合があります。ただし、ドライブ文字が異なっている場合でも、データは適切なボリュームにリストアされます。



20. サマリ情報が正しいことを確認したら、[OK] をクリックします。

リストア処理が開始されます。BMR ウィザード画面には、各ボリュームのリストアステータスが表示されます。

- リストア中のボリュームサイズによっては、この操作に時間かかる場合があります。
- このプロセスを実行中、復旧ポイント用にバックアップしたすべてのものをブロック単位でリストアし、ターゲットマシン上にソースマシンのレプリカを作成します。
- デフォルトでは、[復旧後にシステムを自動的に再起動する] オプションが選択されています。必要に応じて、このオプションの選択を解除し、後から手動で再起動することができます。
- 必要な場合には、いつでも操作のキャンセルまたは中止を実行できます。



21. [ユーティリティ] メニューから、BMR アクティビティ ログにアクセスすることができます。また、保存オプションを使用して、アクティビティ ログを保存することができます。

デフォルトでは、アクティビティ ログは以下の場所に保存されます。

`C:\windows\system32\drlog`

注: Windows で生成されるエラーを回避するため、BMR アクティビティ ログ ウィンドウで [名前をつけて保存] オプションを使用して、アクティビティ ログをデスクトップ上に保存したり、デスクトップ上に新しいフォルダを作成することはしないでください。

22. 異なる種類のハードウェアにリストアする場合 (以前、ハードドライブを接続していた SCSI/FC アダプタが変更されている場合など)、元のシステムで互換性のあるドライバが検出されなければ、ドライバの挿入ページが表示され、これらのデバイス用のドライバを指定できます。

復旧されたシステムに挿入するドライバを参照して選択できます。そのため、異なるハードウェアのマシンを復旧する場合でも、BMR 実行後にマシンを元の状態に戻すことができます。

23. BMR プロセスが完了すると、確認の通知が表示されます。

注: BMR の完了後に以下を行ってください。

- 実行される最初のバックアップは [検証バックアップ] です。
- ブート ボリュームのリストア先のディスクから起動するように BIOS が設定されていることを確認してください。
- 異なるハードウェアにリストアした場合は、マシンが再起動した後で、ネットワーク アダプタを手動で設定する必要がある場合があります。
- ダイナミック ディスクの場合、ディスクのステータスがオフラインのときはディスクの管理 UI (Diskmgmt.msc コントロールユーティリティを実行してアクセス可能) から手動でオンラインに変更できます。
- ダイナミック ディスクの場合、ダイナミック ボリュームが「冗長化に失敗」ステータスのとき、ディスクの管理 UI (Diskmgmt.msc コントロールユーティリティを実行してアクセス可能) からボリュームを手動で再同期することができます。

ブートキットの作成

ブートキットの作成は、必要な CA ARCserve D2D ファイルを USB メモリへコピーすることから成り、作成後これを、Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 インストールメディアあるいは Windows PE イメージのいずれかと共に使用できます。

注: 作成された USB メモリを使用してコンピュータを起動することはできません。実際の BMR を実行するには、USB メモリを Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 のインストールメディア (CD/DVD) と併せて使用する必要があります。



CA サポート :

ブートキットを作成する方法

http://www.arcserve.com/arcserve2d/r16/redirect.php?item=video_bootkit_support

YouTube :

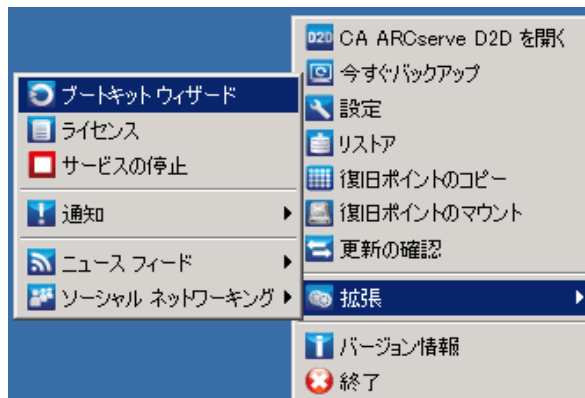
ブートキットを作成する方法

http://www.arcserve.com/arcserve2d/r16/redirect.php?item=video_bootkit_youtube

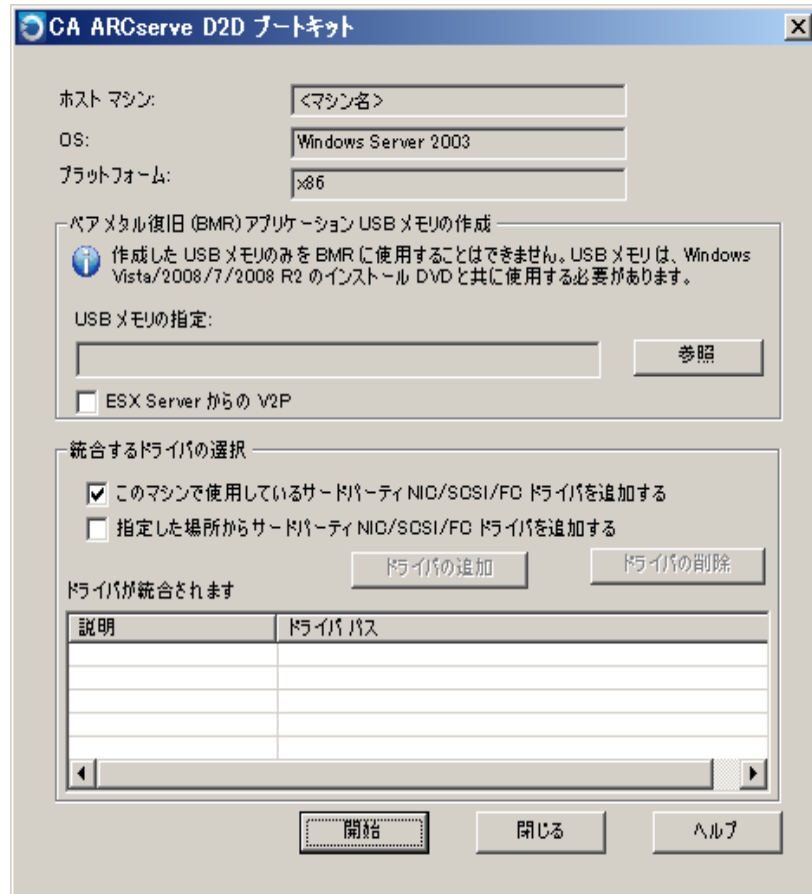
ブートキットを作成する方法

1. CA ARCserve D2D モニタから、[拡張] オプションをクリックし、[ブートキットウィザード] を選択します。

CA ARCserve D2D ブートキットウィザードが起動し、[ようこそ] 画面が表示されます。



2. [OK] をクリックして、[ようこそ] メッセージを閉じます。
[CA ARCserve D2D ブートキット] ダイアログボックスが表示されます。



3. 接続された USB メモリを指定するか、その場所を参照します。
利用可能な USB メモリがない場合、または USB メモリにブートイメージを作成しない場合は、ブートキットのデータを一時的に他の場所に保存し、後で USB メモリにコピーすることができます。
4. 必要に応じて、ドライバを統合するオプションを選択します。
 - このコンピュータで使用しているサードパーティ NIC/SCSI/FC ドライバを追加する
サーバにサードパーティ ドライバがインストールされている場合、このドライバのコピーがバックアップ中に作成されます。サードパーティ ドライバがインストールされていない場合、このチェックボックスは選択可能ではありません。

- 指定した場所からサードパーティ NIC/SCSI/FC ドライバを追加する
必要な NIC (ネットワーク)、SCSI (Small Computer System Interface)、FC (ファイバチャネル) の各ドライバがブートキット作成プロセスに含まれます。また、表示されたリストからドライバの追加または削除を実行できます。

注: [指定した場所からサードパーティ NIC/SCSI/FC ドライバを追加する] オプションを選択しない場合、USB メモリには特定のマシンのデータは含まれません。

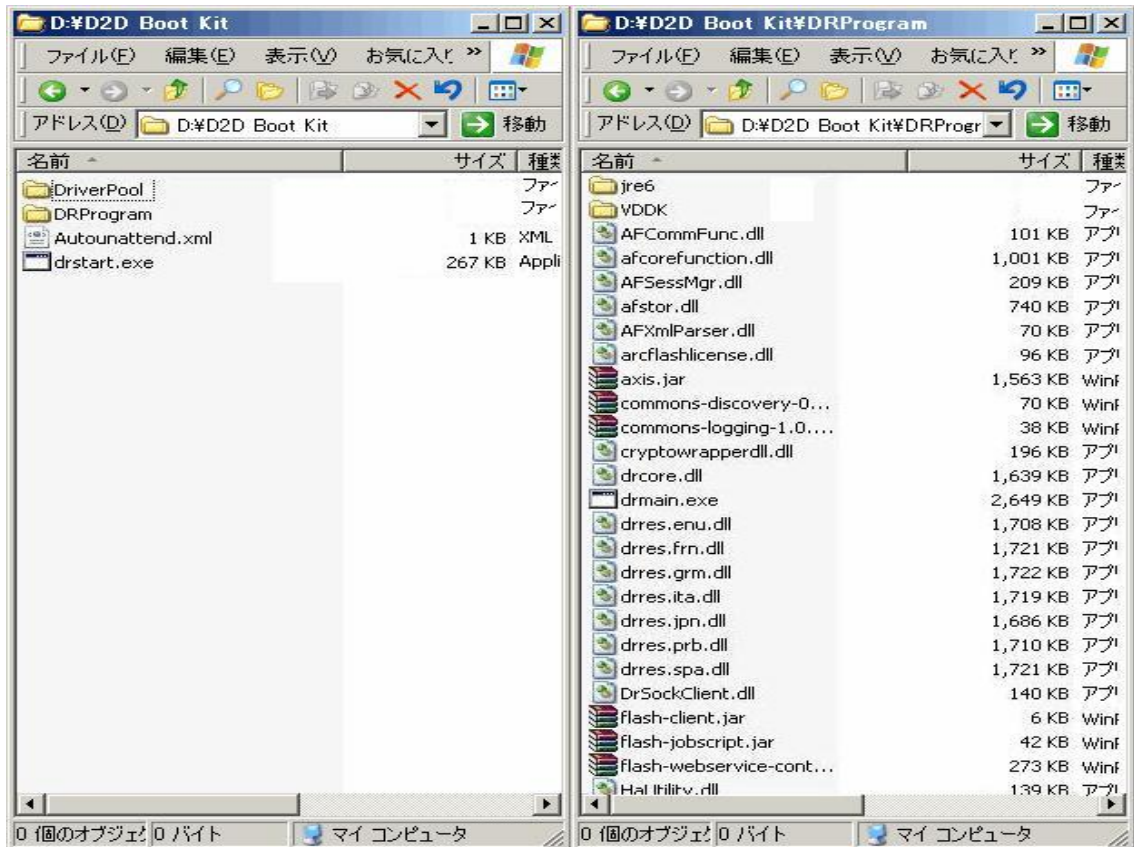
選択されたドライバは、回復処理中にロードされます。

5. [開始] をクリックします。

ブートキットを作成する進捗状況が表示されます。また、USB メモリが正常に作成された場合、確認メッセージが表示されます。

- ブートキットの作成が正常に完了した後、CA ARCserve D2D ブートキットファイルは USB メモリにあります。

注: 作成された USB メモリは、その他の同種のコンピュータに使用できません。32 ビットプラットフォームから作成された USB メモリは、32 ビットサーバをリストアする場合のみ使用できます。64 ビットプラットフォームから作成された USB メモリは、64 ビットサーバをリストアする場合のみ使用できます。



同時バックアップ数の制限の定義

同時に実行される CA ARCserve D2D バックアップジョブ数の制限を定義することができます。この機能を使用することにより、お使いのバックアップ環境内の CA ARCserve D2D 仮想マシンプロキシサーバのパフォーマンスを最適化できます。デフォルトでは、Host-Based VM Backup は、最大 10 までの D2D バックアップジョブを同時に実行できます。CA ARCserve D2D 仮想マシンプロキシシステムに関連付けられた仮想マシンが多く存在する環境では、同時に多くのバックアップが実行されると、ネットワークおよびバックアップのパフォーマンスに悪影響を及ぼす可能性があります。

注: 同時に実行されるジョブの数が定義された制限を超えた場合、制限を超えたジョブはジョブキューに入ります。

次の手順に従ってください:

1. CA ARCserve D2D 仮想マシンプロキシシステムにログインします。
2. Windows レジストリ エディタ を開き、以下のキーを探します。

`HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D`

3. CA ARCserve D2D を右クリックし、コンテキストメニューで [新規] - [文字列値] をクリックします。

以下のようにキーに名前を付けます。

`VsphereMaxJobNum`

4. `VsphereMaxJobNum` を右クリックして、コンテキストメニューの [変更] をクリックします。

[文字列の編集] ダイアログ ボックスが開きます。

5. [値のデータ] フィールドで、同時に実行可能な CA ARCserve D2D バックアップジョブの数を指定します。

- 最小 -- 1
- 最大 -- なし

6. [OK] をクリックします。

制限が定義されます。

VMVixMgr ログ ファイルに保持されるメッセージ容量を増加させる

VMVixMgr ログ ファイルには、VMware VIX の処理に関するメッセージが保持されます。VMware VIX API の詳細については、VMware の Web サイトを参照してください。

VMVixMgr ログ ファイル (VMVixMgr.log) は、バックアップ プロキシ システム上の以下のディレクトリに保存されます。

```
C:\Program Files\CA\ARCserve D2D\Log
```

デフォルトでは、このログ ファイルは 500 KB を超えることができません。ログ ファイルが 500 KB を超えると、ログ ファイルのメッセージが上書きされます。この動作により、ログ ファイルが 500 KB を超えることはありません。

15 分間隔でデータをバックアップするようスケジュールを定義すると、500 KB の超過によるログ ファイルの上書きが発生する可能性があります。ログ ファイルのサイズを増加させると、ログ ファイルにより多くのメッセージを保持させることができます。

ベストプラクティスとして、15 分ごとにデータをバックアップするようスケジュールする場合に限り、ログ ファイルのサイズを増加させることを推奨します。

次の手順に従ってください:

1. バックアップ プロキシ システムにログインします。
2. Windows レジストリ エディタ を開き、以下のキーを探します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D
```

3. CA ARCserve D2D を右クリックし、コンテキストメニューで [新規] を選択し、[DWORD] をクリックします。

DWORD に以下の名前を設定します。

```
VixMgrLogSize
```

注: この DWORD が存在しない場合、ログ ファイルのデフォルト値である 500 KB が有効です。

4. DWORD を作成したら、VixMgrLogSize を右クリックし、コンテキストメニューから [変更] をクリックして DWORD を編集するためのダイアログ ボックスを開きます。
5. DWORD の編集ダイアログ ボックスの [値データ] フィールドで、ログ ファイルの値 (KB) を指定します。たとえば 750、1000 などの値を指定します。
6. [OK] をクリックして値を適用し、DWORD の編集ダイアログ ボックスを閉じます。

CA ARCserve D2D バックアップ プロキシの保護

CA ARCserve Central Host-Based VM Backup で作成されたバックアップセッションは、バックアップ プロキシに保存されます。環境設定に応じて、バックアップ プロキシの保護にはいくつかの方法があります。

- CA ARCserve Central Protection Manager を実行している場合、保護対象のノードとしてバックアップ プロキシを追加できます。詳細については、「CA ARCserve Central Protection Manager ユーザ ガイド」を参照してください。
- バックアップ プロキシ上でローカルに実行される CA ARCserve D2D インスタンスを起動し、バックアップ設定の環境設定を行います。バックアップ ソースとして [マシン全体] を選択します。詳細については、「CA ARCserve D2D ユーザ ガイド」を参照してください。
- CA ARCserve Backup を実行している場合、プロキシを保護するようバックアップ ジョブを設定できます。

インストール処理のオペレーティング システムに対する影響

CA ARCserve Central Applications インストール処理は、Microsoft Installer Package (MSI) というインストール エンジンを使用して、さまざまな Windows オペレーティング システムのコンポーネントを更新します。CA ARCserve Central Applications では、MSI に含まれるコンポーネントによって、CA ARCserve Central Applications のインストール、アップグレードを行うカスタム アクションを実行できます。

以下の表では、カスタム アクションと影響を受けるコンポーネントについて説明します。

注: CA ARCserve Central Applications のインストールを行う場合、すべての CA ARCserve Central Applications MSI パッケージは、この表にリストされたコンポーネントを呼び出します。

コンポーネント	説明
CallAllowInstall	インストール処理で現在の CA ARCserve Central Applications インストールに関する状態を確認できます。
CallPreInstall	インストール処理で MSI プロパティの読み取りと書き込みが可能になります。たとえば、MSI から CA ARCserve Central Applications インストールパスを読み取ります。
CallPostInstall	インストール処理でインストールに関するさまざまなタスクを実行できます。たとえば、CA ARCserve Central Applications を Windows レジストリに登録します。
CallAllowUninstall	アンインストール処理で現在の CA ARCserve Central Applications インストールに関する状態を確認できます。
CallPreUninstall	アンインストール処理でアンインストールに関するさまざまなタスクを実行できます。たとえば、Windows レジストリから CA ARCserve Central Applications の登録を削除します。
CallPostUninstall	アンインストール処理で、インストール済みファイルがアンインストールされた後、さまざまなタスクを実行できます。たとえば、残ったファイルを削除することができます。

コンポーネント	説明
ShowMsiLog	[SetupCompleteSuccess]、[SetupCompleteError]、または [SetupInterrupted] ダイアログ ボックスの [Windows Installer のログを表示] チェック ボックスがオンの場合に [完了] をクリックすると、Windows Installer ログ ファイルをメモ帳で表示することができます。（これは Windows Installer 4.0 でのみ機能します。）
ISPrint	ScrollableText コントロールの内容をダイアログ ボックス 上に出力します。 これは、Windows Installer .dll カスタム アクションで す。 .dll ファイルの名前は SetAllUsers.dll で、エントリ ポ イントは PrintScrollableText です。
CheckForProductUpdates	FLEXnet Connect を使用して製品アップデートを確認しま す。 このカスタム アクションは、Agent.exe という名前の実行 可能ファイルを起動し、以下に移動します。 /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	再起動の際に FLEXnet Connect を使用して製品アップ データを確認します。 このカスタム アクションは、Agent.exe という名前の実行 可能ファイルを起動し、以下に移動します。 /au[ProductCode] /EndOfInstall /Reboot

- **更新されるディレクトリ** -- インストール処理では、デフォルトで以下のディレクトリに、CA ARCserve Central Applications ファイルのインストールと更新が行われます。

C:\Program Files\CA\ARCserve Central Applications

CA ARCserve Central Applications は、デフォルトのインストールディレクトリ、または別のディレクトリにインストールすることができます。インストール処理では、さまざまなシステム ファイルが以下のディレクトリにコピーされます。

C:\WINDOWS\SYSTEM32

- **更新される Windows レジストリ キー** -- インストール処理は以下の Windows レジストリ キーを更新します。

デフォルトのレジストリ キー

HKLM\SOFTWARE\CA\CA ARCserve Central Applications

インストール処理では、システムの現在の設定に基づき、新しいレジストリ キーが作成され、その他のさまざまなレジストリ キーが変更されます。

- **インストールされるアプリケーション** -- インストール処理では、以下のアプリケーションがコンピュータにインストールされます。
 - CA ライセンス
 - Microsoft Visual C++ 2005 SP1 Redistributable
 - Microsoft Windows Installer 3.1 Redistributable (v2) パッケージ
 - Java Runtime Environment (JRE) 1.6.0_16
 - Tomcat 6.0.32

無効なファイル バージョン情報が含まれるバイナリファイル

CA ARCserve Central Applications は、サードパーティ、他の CA 製品、CA ARCserve Central Applications によって開発され、正しくないバージョン情報を含むバイナリ ファイルをインストールします。以下の表は、これらのバイナリ ファイルについての説明です。

バイナリ名	ソース
UpdateData.exe	CA ライセンス
zlib1.dll	Zlib 圧縮ライブラリ

埋め込みマニフェストを含まないバイナリファイル

CA ARCserve Central Applications は、サードパーティ、他の CA Technologies 製品、CA ARCserve Central Applications によって開発され、埋め込みマニフェストおよびテキスト マニフェストを含まないバイナリ ファイルをインストールします。以下の表は、これらのバイナリ ファイルについての説明です。

バイナリ名	ソース
BaseLicInst.exe	CA ライセンス
UpdateData.exe	CA ライセンス
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
tomcat6.exe	Tomcat

マニフェストで管理者に必要な権限を持つバイナリファイル

CA ARCserve Central Applications はサードパーティ、他の CA Technologies 製品、CA ARCserve Central Applications によって開発され、管理者レベルまたは利用可能な最上位レベルの権限を持つバイナリ ファイルをインストールします。さまざまな CA ARCserve Central Applications サービス、コンポーネントおよびアプリケーションを実行するには、管理者アカウントまたは最上位の権限を持つアカウントを使用してログインする必要があります。これらのサービス、コンポーネントおよびアプリケーションに関係しているバイナリは CA ARCserve Central Applications 固有の機能を含み、基本ユーザアカウントには利用が許可されていません。このため、Windows はパスワードの指定または管理者権限を持つアカウントの使用を促し、権限を確認した後で作業を完了します。

- **管理者権限** - 管理者プロファイルまたは管理者権限を持つアカウントには、すべての Windows リソースおよびシステム リソースに対する読み取り権限、書き込み権限、および実行権限が付与されています。管理者権限を持っていない場合、続行するには管理者ユーザのユーザ名/パスワードを入力するように促されます。
- **最上位の権限** - 最上位の権限を持つアカウントは、管理者としての実行権限を持つ基本ユーザアカウントとパワーユーザアカウントです。

以下の表は、これらのバイナリ ファイルについての説明です。

バイナリ名	ソース
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIconfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications

バイナリ名	ソース
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

付録 A: CA ARCserve D2D の操作手順

このセクションには、「CA ARCserve D2D ユーザガイド」から役立つ情報が抜粋されています。

注: CA ARCserve D2D 設定には CA ARCserve Central Host-Based VM Backup に適用されないものがあります。

このセクションには、以下のトピックが含まれています。

[CA ARCserve D2D のインストール](#) (P. 211)

[バックアップ設定の管理](#) (P. 214)

[アプリケーションのリストア](#) (P. 259)

[復旧ポイントのコピー方法](#) (P. 274)

CA ARCserve D2D のインストール

このセクションは、InstallShield ウィザードを使用して、ローカルシステム上に CA ARCserve D2D をインストールする方法を説明します。InstallShield ウィザードは、インストールプロセスの手順を指示する対話型アプリケーションです。



ビデオ

CA サポート :

CA ARCserve D2D のインストール方法

(http://www.arcserve.com/arcserve2d/r16/redirect.php?item=video_install_support)

YouTube :

CA ARCserve D2D のインストール方法

(http://www.arcserve.com/arcserve2d/r16/redirect.php?item=video_install_youtube)

CA ARCserve D2D をインストールする方法

1. CA Web サイトまたは製品 CD のいずれかから CA ARCserve D2D インストールパッケージにアクセスします。CA Web サイトからダウンロードされたインストールパッケージを使用している場合は、CA ARCserve D2D Setup.exe を選択します。製品 CD を使用している場合は、setup.exe を選択します。

注: Web サイトからダウンロードしたインストールパッケージを使用してインストールを実行する場合、パッケージのコンテンツはユーザのローカルシステムに抽出されます。

使用許諾契約のダイアログ ボックスが表示されます。

2. [使用許諾契約] ダイアログ ボックスで、使用許諾契約の条件を読んで同意した後、[次へ] をクリックします。

[環境設定] ダイアログ ボックスが表示されます。

3. [環境設定] ダイアログ ボックスに、以下の情報を入力します。

- a. ユーザ名およびパスワード。

- b. CA ARCserve D2D をインストールする予定の場所を指定または参照します。

デフォルトの場所は、C:\Program Files\CA\ARCserve Central Applications です。

注: CA ARCserve D2D インストール時に、一部のファイルはデフォルトの場所にインストールされません。これらのファイルの完全なリストについては、「デフォルト以外の場所にインストールされるファイル」を参照してください。

- c. ポート番号。このポート番号は、Web ベースの UI に接続する際に使用されます。

デフォルトのポート番号は 8014 です。

注: CA ARCserve D2D のインストールで利用可能なポート番号は 1024 ~ 65535 です。指定したポート番号が空いていて利用可能であることを確認してください。セットアップでは、利用可能でないポートでは CA ARCserve D2D をインストールできません。

- d. Web 通信プロトコルとして https を使用する場合は指定します。

デフォルトでは、CA ARCserve D2D は、すべてのコンポーネント間の通信に Hypertext Transfer Protocol (HTTP) を使用します。コンポーネント間でやり取りされるパスワードのセキュリティを考慮する必要がある場合は、このオプションを選択して使用するプロトコルを Hypertext Transfer Protocol Secure (HTTPS) に変更できます。

注: 通信プロトコルはインストール後にいつでも変更することができます。詳細については、「サーバの通信プロトコルの変更」を参照してください。

- e. CA ARCserve D2D 変更トラッキング ドライバをインストールする場合は指定します。

デフォルトでは、このオプションが選択されています。

- このドライバがインストールされていないと、CA ARCserve D2D はローカルバックアップを実行できません。
- ローカルバックアップを実行するには、このドライバがインストールされた状態で、有効な CA ARCserve D2D ライセンスが存在している必要があります。

注: このドライバはインストールの完了後にいつでもインストールできます。そのためには、次の場所から 'InstallDriver.bat' ユーティリティを実行します: "<ARCserve Central Applications install folder>%BIN%DRIVER"

- f. セットアップで CA ARCserve D2D のサービスおよびプログラムが Windows ファイアウォールの例外として登録されるようにする場合は指定します。

注: CA ARCserve D2D の設定や管理をリモートマシンから実行する場合、ファイアウォールの例外に登録する必要があります。(ローカルユーザの場合、ファイアウォールの例外に登録する必要はありません。)

4. [インストール] をクリックして、インストールプロセスを開始します。

[インストールの進捗状況] 画面が開き、インストールのステータスが表示されます。

5. インストールが完了すると、[インストール レポート] のサマリ画面が表示され、自動的に製品の環境設定が実行されます。[完了] ボタンをクリックします。

システムの再起動が必要であることを伝え、再起動を今すぐ実行するか後で実行するかを尋ねるアラートメッセージが表示されます。

再起動が完了すると、CA ARCserve D2D はローカル システムにインストールされています。

6. インストール後は、CA ARCserve D2D には [スタート] メニューまたは CA ARCserve D2D モニタからアクセスできます。
7. USB メモリを Windows 7/2008/2008 R2 インストール メディア (CD/DVD) と共に使用するのであれば、インストールが完了した後、CA ARCserve D2D ブートキットユーティリティを使用して BMR アプリケーション USB メモリを作成することができます。

BMR を実行する際、Windows PE イメージ (CA ARCserve D2D 製品と共に提供) を使用するか、作成した USB メモリを Windows 7/2008/2008 R2 インストール メディアと共に使用するかを選択できます。また、ブートキットユーティリティを使用すると、BMR アプリケーションとサードパーティの NIC/SCSI/FC ドライバを USB メモリに統合することもできます。

ブートキットユーティリティの詳細については、「[ブートキットの作成 \(P. 198\)](#)」を参照してください。

バックアップ設定の管理

最初のバックアップを実行する前に、各バックアップ ジョブに適用されるバックアップ設定を指定します。これらの設定では、以下のような動作を指定します。

- バックアップのソースおよびデスティネーション
- バックアップの種類ごとのスケジュール
- バックアップ ジョブの詳細設定
- バックアップ前または後の処理

これらの設定は、CA ARCserve D2D ホーム画面からいつでも変更できます。



ビデオ

CA サポート : 自動バックアップを実行する方法-バックアップ設定を指定する (http://www.arcservedocs.com/arcserved2d/r16/redirect.php?item=video_autobackup_support)。

YouTube : 自動バックアップを実行する方法-バックアップ設定を指定する (http://www.arcservedocs.com/arcserved2d/r16/redirect.php?item=video_autobackup_youtube)。

バックアップ設定を管理するには、CA ARCserve D2D ホーム画面上で [設定] リンクをクリックし、[バックアップ設定] ダイアログボックスおよびそこに含まれる以下のタブを表示します。

- [保護設定](#) (P. 215)
- [スケジュール設定](#) (P. 233)
- [拡張設定](#) (P. 236)
- [バックアップ実行前/後の設定](#) (P. 241)

保護設定の指定

バックアップされる情報の保護設定により、バックアップデータがあらゆる形のデータ損失から確実に保護（コピーおよび保存）されます。

注: バックアップ設定に関連するビデオを閲覧するには、「[バックアップ設定の管理](#) (P. 214)」を参照してください。

保護設定の指定

1. CA ARCserve D2D ホーム画面（または CA ARCserve D2D モニタ）で、タスクバーから [設定] を選択し、[バックアップ設定] タブを選択します。[バックアップ設定] ダイアログボックスが開いたら、[保護設定] を選択します。

[バックアップ設定] の [保護設定] ダイアログボックスが表示されます。



2. バックアップ先を指定します。

バックアップ場所としてローカルパス（ボリュームまたはフォルダ）、またはリモート共有フォルダ（またはマップされたドライブ）を指定できます。また、バックアップ先を参照して指定することもできます。

緑色の矢印アイコン ボタンをクリックすると、指定した場所への接続を検証できます。

- バックアップ先にローカルパスを入力した場合、このボタンは無効になります。
 - ネットワークパスを入力してこのボタンをクリックした場合は、ユーザ名とパスワードの指定が要求されます。
 - すでにこのパスに正常に接続されている場合は、この矢印ボタンをクリックして接続に使用するユーザ名とパスワードを変更できます。
 - 矢印ボタンをクリックしない場合は、デスティネーションパスが検証されます。必要な場合、ユーザ名とパスワードが要求されます。
- a. ローカルパス（ボリュームまたはフォルダ）にバックアップする場合、バックアップソースと同じ場所をバックアップ先に指定することはできません。バックアップ先にバックアップソースが含まれている場合、バックアップジョブではそのソースが無視され、バックアップには含まれません。

例： ボリューム C、D および E で構成されるローカルマシン全体をバックアップしようとし、デスティネーションとしてボリューム E を指定したとします。この場合、CA ARCserve D2D はボリューム C および D のみをボリューム E にバックアップします。ボリューム E のデータはバックアップに含まれません。ローカルボリュームをすべてバックアップする場合は、バックアップ先としてリモートロケーションを指定する必要があります。

重要： 指定したデスティネーションボリュームにシステム情報が含まれていないことを確認してください。システム情報が含まれていると、そのボリュームは保護（バックアップ）されず、必要が生じてベアメタル復旧（BMR）を実施したときにシステムの復旧が失敗します。

注： ダイナミックディスクのリストアはディスクレベルでのみ実行できます。ダイナミックディスク上のボリュームにデータがバックアップされた場合、このダイナミックディスクを BMR 実行中にリストアすることはできません。

- b. リモートの共有場所にバックアップする場合は、その場所へのパスを入力するか、その場所を参照して選択します。また、リモートマシンにアクセスする際に、ユーザ認証情報（ユーザ名とパスワード）を入力する必要があります。
- c. 前回のバックアップの実行後にバックアップ先が変更された場合、バックアップの種類としてフルバックアップまたは増分バックアップを選択します。これらのオプションは、バックアップ先を変更した場合にのみ有効になります。デフォルト オプションは [フルバックアップ] です。

フルバックアップ

実行される次のバックアップはフルバックアップになります。新しいバックアップ先には、古いバックアップ先との依存関係はありません。フルバックアップを続行する場合、バックアップを続行するために前の場所を指定する必要はありません。古いバックアップをリストア用として保持することも、そこからリストアを実行しない場合は削除することもできます。古いバックアップは将来のバックアップに影響しません。

増分バックアップ

実行される次のバックアップは増分バックアップになります。次の増分バックアップを新しいバックアップ先に対して実行する場合は、前回のバックアップ先にあるバックアップをすべてコピーすることはありません。ただし、このオプションでは、変更を増分データのみが含まれるため（フルバックアップデータではない）、新しいバックアップ先には前回のバックアップ先との依存関係があります。前回のバックアップ先からデータを削除しないでください。バックアップ先を別のフォルダに変更し、増分バックアップの実行時に前回のバックアップ先が存在しない場合、バックアップは失敗します。

3. バックアップソースを指定します。

マシン全体または選択されたボリュームをバックアップできます。

マシン全体をバックアップする

マシン全体をバックアップします。マシン上のすべてのボリュームがバックアップされます。

注: マシン全体のバックアップが選択された場合、CA ARCserve D2Dは現在のマシンに接続されているすべてのディスク/ボリュームを自動的に検出し、それらをバックアップ対象に追加します。

例: バックアップ設定の実行後に新しいディスクがマシンに接続された場合でも、バックアップ設定を変更する必要はなく、新しいディスク上のデータは自動的に保護されます。

バックアップする個々のボリュームを選択する

このボリュームフィルタ機能を使用すると、選択したボリュームのみをバックアップできます。また、リスト内のすべてのボリュームを選択または選択解除することもできます。

注: 一部のボリュームがバックアップ対象として明示的に選択されている場合は、選択されたボリュームのみがバックアップされます。新しいディスク/ボリュームがマシンに接続された場合、そのディスク/ボリューム上のデータを保護するにはボリューム選択リストを手動で変更します。

このオプションを選択すると、利用可能なすべてのボリュームが表示され、対応するボリューム情報および通知メッセージが表示されます。

注: Extensible Firmware Interface (EFI) に準拠するコンピュータは、EFI システムパーティション (データストレージデバイス上のパーティション) を使用します。EFI システムパーティションは、ベアメタル復旧 (BMR) に不可欠です。そのため、UEFI システム上のブートボリューム「C」を選択すると、EFI システムパーティションが BMR 用のバックアップソースとして自動的に選択され、情報メッセージが表示されます。

名前	レイアウト	種類	ファイルシステム	コンテンツ	合計サイズ	使用容量
E:	シンプル	ベーシック	NTFS		49.90 GB	15.25 GB
F:	シンプル	ベーシック	NTFS		30.00 GB	29.06 GB
システムで予約済み	シンプル	ベーシック	NTFS	システム	100.00 MB	28.19 MB

選択したボリュームのサイズ: 15.25 GB

通知 (2 個の警告)

- ローカル バックアップ デスティネーション ボリューム F:¥ は、バックアップ ソースの選択から除外されます。
- システム ボリューム (通常 システムで予約済み ドライブ) がバックアップ ソース ボリューム リストに含まれていない場合、このバックアップは BMR には使用できません。

- **名前** - ボリューム ドライブ文字、マウント ポイント、ボリューム GUID (Globally Unique Identifier) 名。
- **レイアウト** - シンプル、スパン、ミラー、ストライプ、RAID5 (Microsoft ダイナミック ディスク上での RAID 5 ボリュームのバックアップはサポートされていませんが、ハードウェア RAID のバックアップはサポートされています)。
- **種類** - ベーシック、ダイナミック
- **ファイルシステム** - NTFS、FAT、FAT32 (FAT と FAT32 のバックアップはサポートされていません)
- **コンテンツ** - アプリケーション (SQL/Exchange)、システム、ブート、ページファイル、アクティブ、リムーバブルデバイス、VHD、2-TB ディスク
- **合計サイズ** - ボリュームの容量
- **使用容量** - ファイル/フォルダおよびボリュームデータによって使用されている容量

以下のいずれかの条件では、通知メッセージが表示されます。

- ローカルボリューム関連

指定されたバックアップ先がローカルボリュームにある場合、そのボリュームがバックアップされていないことを通知する警告メッセージが表示されます。

- BMR 関連

システム/ブート ボリュームがバックアップ用に選択されていない場合、バックアップをベア メタル復旧 (BMR) に使用できないことを通知する警告メッセージが表示されます。

UEFI システム上のブート ボリューム「C」を選択すると、EFI システムパーティションが BMR 用のバックアップソースとして自動的に選択され、情報メッセージが表示されます。

- アプリケーション関連

バックアップ対象として選択されていないボリュームにアプリケーションデータ ファイルが存在する場合、そのアプリケーション名とデータベース名が参照用に表示されます。

4. [保存設定] を指定します。

保存設定は、保存する復旧ポイントの数 (セッションをマージ) または保存する復旧セットの数 (復旧セットを削除し、無限増分バックアップを無効化) に基づいて設定できます。

- 復旧ポイント - これが推奨オプションです。このオプションを選択すると、無限増分バックアップの機能をフルに活用してストレージ容量を節約できます。
- 復旧セット - このオプションは、通常、規模の大きいストレージ環境で使用します。このオプションを選択すると、大量のデータを保護している場合、バックアップ ウィンドウ時間を効率的に管理できるバックアップセットを作成および管理できます。このオプションは、バックアップの容量よりもバックアップ時間を優先する場合に使用します。

デフォルト：復旧ポイントの保持

復旧ポイントの保持

このオプションは、保持する復旧セットの数ではなく、保持する復旧ポイントの数に基づいて保存設定を指定する場合に選択します。

▼ 保存設定

復旧ポイントの保持
 復旧セットの保持

! 保存設定が変更されました。新しい保存設定でバックアップを開始するには、新しいバックアップ デスティネーションを使用してください。

保存する復旧ポイントの数を指定します。

マージ ジョブの実行:

至急

以下の時間範囲のすべての日

開始 :
終了 :

保持する復旧ポイント数の指定

保持する復旧ポイント（フル、増分および検証バックアップ イメージ）の数を指定します。デスティネーションにある復旧ポイント数が指定した上限を超えると、最も古い増分バックアップから、上限を超えた数だけ親バックアップにマージされ、「親 + 最古の子」ブロックで構成される新しいベースラインイメージが生成されます。バックアップが圧縮され、マージできる複数のセッションがある場合、最も古い子バックアップから単一パスで親バックアップにマージされます。バックアップが圧縮されない場合、最も古い単一の子バックアップのみが親バックアップにマージされ、以降にマージされる各子バックアップについてもこのサイクルが繰り返されます。

保持する復旧ポイント数を指定すると、保持数を一定に保ちながら無限増分バックアップを行うことができます。詳細については、「マージジョブの管理」を参照してください。

注: デスティネーションの空き容量が不足している場合、保存する復旧ポイントの数を減らすことを検討してください。

デフォルト : 31

最小 : 1

最大 : 1344

注: CA ARCserve D2D のホームページの [サマリ] セクションは、指定された数からどれだけの復旧ポイントが保持されるかを示します。詳細については、「ステータス サマリ概要」を参照してください。

マージジョブの実行:

至急

任意の時点でマージジョブを実行する場合にこのオプションを選択します。

以下の時間範囲のすべての日

毎日、指定した時間帯にのみマージジョブを実行する場合、このオプションを選択します。時間帯を指定すると、マージジョブの実行が長時間におよぶ場合でも、マージジョブにより実稼働サーバ上で過剰な I/O 処理が発生するのを防ぐことができます。

注: マージジョブを実行する時間帯を設定する際に、マージの開始前に、関連するバックアップジョブが完了するように時間帯を設定します。

復旧セットの保持

このオプションは、保持する復旧ポイント数ではなく、保持する復旧セット数に基づいて保存設定を指定する場合に選択します。この設定では、無限増分バックアップを無効化し、セッションのマージは行いません。復旧セットを使用すると、マージジョブが完了するまでの合計時間を減らすことができます。

▼ 保存設定

復旧ポイントの保持

復旧セットの保持

! 注: 多数の復旧セットを保持するよう指定する場合は、指定した数 + 2 のフル バックアップで利用できる十分な空き容量があることを確認してください。

保存する復旧セットの数を指定します。

新しい復旧セットを開始する間隔:

週の選択された曜日

月の選択された日付

新しい復旧セットを開始する対象:

選択された日の最初のバックアップ

選択された日の最後のバックアップ

保持する復旧セット数の指定

保持する復旧セット数を指定します。復旧セットは、フルバックアップから始まり、そのあとに複数の増分、検証、またはフルバックアップが続く、一連のバックアップです。

例-セット 1:

- フル
- 増分
- 増分
- 検証
- 増分

例-セット 2:

- フル
- 増分
- フル
- 増分

新しい復旧セットを開始するには、フルバックアップが必要です。指定された時間に実行するよう設定またはスケジュールされたフルバックアップがない場合でも、セットを開始するバックアップは自動的にフルバックアップに変換されます。CA ARCserve D2D ホーム ページ上の [最新のイベント] セクションにあるステータス列のフラグは、フルバックアップが復旧セットを開始するバックアップであることを示します。復旧セットの設定を変更（たとえば、復旧セットの開始ポイントを月曜日の最初のバックアップから木曜日の最初のバックアップに変更、など）した場合、既存の復旧セットの開始ポイントは変更されません。

注: 既存の復旧セット数を計算する際、未完了の復旧セットは無視されます。復旧セットが完了しているとみなされるのは、次の復旧セットの開始バックアップが作成されたときです。

指定した制限を超過すると、最も古い復旧セットは（マージされるのではなく）削除されます。

デフォルト: 2

最小: 1

最大: 100

注: 復旧セットを削除して、バックアップ用のストレージ容量を節約したい場合は、保持するセット数を減らします。CA ARCserve D2D が最も古い復旧セットを自動的に削除します。復旧セットは手動で削除しないようにしてください。

例 1 - 復旧セットを 1 個保持 :

- 保持する復旧セット数を 1 に指定します。

CA ARCserve D2D は、完了したセットを 1 つ保持するため、次の復旧セットの開始まで、常に 2 つのセットを保持します。

例 2 - 復旧セットを 2 個保持 :

- 保持する復旧セット数を 2 に指定します。

4 番目の復旧セットを開始する際、CA ARCserve D2D は、最初の復旧セットを削除します。これにより、最初のバックアップが削除され、かつ、4 番目のバックアップが開始された時点で、ディスク上には 2 個の復旧セットが存在します（復旧セット 2 および 3）。

注: 保持する復旧セットの数を 1 つに指定した場合でも、少なくともフルバックアップ 2 個分の容量が必要になります。

例 3 - 復旧セットを 3 個保持 :

- バックアップの開始時間は 2012 年 8 月 20 日、午前 6:00 です。
- 12 時間ごとに増分バックアップを実行します。
- 新しい復旧セットは、金曜日の最終バックアップから開始します。
- 3 個の復旧セットを保持します。

上記の条件では、増分バックアップは毎日午前 6:00 および午後 6:00 に実行されます。最初のバックアップ（フルバックアップである必要があります）を取る際、最初の復旧セットが作成されます。最初のフルバックアップは復旧セットの開始バックアップとしてマークされます。金曜日の午後 6:00 にスケジュールされたバックアップは、実行と同時にフルバックアップに変換され、復旧セットの開始バックアップとしてマークされます。

新しい復旧セットを開始する間隔:

週の選択された曜日

新しい復旧セットを開始する曜日を指定します。

月の選択された日付

新しい復旧セットを開始する月の日付を指定します。1～30を指定します。また、月の日数は異なった値を取るため（28、29、30、または31日）、月の最終日を復旧セットの作成日として指定することができます。

新しい復旧セットを開始する対象

選択された日の最初のバックアップ

新しい復旧セットを、指定した日の最初にスケジュールされたバックアップで開始する場合に指定します。

選択された日の最後のバックアップ

新しい復旧セットを、指定した日の最後にスケジュールされたバックアップで開始する場合に指定します。最後のバックアップでセットを開始することを選択し、何らかの理由で最後のバックアップが実行されなかった場合、その次にスケジュールされたバックアップがフルバックアップに変換されてセットを開始します。次のバックアップが（緊急事態により、即座に増分バックアップを実行したなどの理由により）アドホックに実行された場合は、フルバックアップを実行して復旧セットを開始するか、または、増分バックアップを実行して次のバックアップで復旧セットを開始するかを決定できます。

注: アドホック バックアップを実行した場合、最終バックアップはその日の最後のバックアップではない場合があります。

CA ARCserve D2D のホームページの [サマリ] セクションは、指定された数からどれだけの復旧セットが保持（または進行中）されるかを示します。[復旧セット] の下のリンクをクリックすると、[復旧セットの詳細] ダイアログ ボックスが表示されます。このダイアログ ボックスには、復旧セットの内容に関する詳細情報が含まれます。このダイアログ ボックスの詳細については、「ステータス サマリ概要」を参照してください。

5. 圧縮の種類を指定します。

バックアップに使用される圧縮の種類を指定します。

圧縮は、通常ディスク容量の使用率を減らすために実行されますが、CPU 使用率が増加するため、バックアップ速度が低下するという影響があります。

使用可能なオプションは、以下のとおりです。

■ 圧縮なし

圧縮は実行されません。このオプションを使用すると、CPU 使用率は最も低くなります（最も高速で動作します）。ただし、バックアップイメージのディスク容量の使用率は最大になります。

■ 標準圧縮

一般的な圧縮が実行されます。このオプションを使用すると、CPU 使用率とディスク容量使用率のバランスを適度に調節します。標準圧縮はデフォルトの設定です。

■ 最大圧縮

最大圧縮が実行されます。このオプションを使用すると、CPU 使用率が最も高くなります（最も低速で動作します）。ただし、ディスク容量の使用率は、最小になります。

注:

- バックアップイメージに圧縮可能でないデータ (JPG イメージ、ZIP ファイルなど) が含まれている場合、それらのデータを処理するために、追加のストレージスペースを割り当てることができます。そのため、圧縮オプションを選択していて、バックアップに圧縮可能でないデータがある場合、ディスク容量の使用率が增大する場合があります。
- 圧縮レベルを「圧縮なし」から「標準圧縮」または「最大圧縮」にした場合、あるいは、「標準圧縮」または「最大圧縮」から「圧縮なし」に変更した場合、圧縮レベルの変更後に実行される最初のバックアップは自動的に「フルバックアップ」となります。フルバックアップを実行した後、それ以降のすべてのバックアップ（フル、増分、検証）はスケジュールどおりに実行されます。
- デスティネーションの空き容量が足りない場合、バックアップの圧縮設定を高くすることを検討してください。

6. 暗号化設定を指定します。

- a. バックアップに使用される暗号化アルゴリズムの種類を選択します。

データの暗号化とは、解読メカニズムがなければ理解できない形式にデータを変換することです。CA ARCserve D2D のデータ保護では、安全な AES (Advanced Encryption Standard) 暗号化アルゴリズムを使用し、指定したデータに対して最大限のセキュリティおよびプライバシーを確保します。

利用可能なオプションは、暗号化なし、AES-128、AES-192、および AES-256 です（暗号化を無効にするには、[暗号化なし] を選択します）。

- フルバックアップと関連するすべての増分/検証バックアップで同じ暗号化アルゴリズムを使用する必要があります。
- 増分または検証バックアップの暗号化アルゴリズムが変更された場合、フルバックアップが実行される必要があります。つまり、暗号化アルゴリズムが変更されたら、元のバックアップの種類にかかわらず、最初のバックアップはフルバックアップになります。

たとえば、アルゴリズム形式を変更し、カスタマイズされた増分/検証バックアップを手動でサブミットした場合は、自動的にフルバックアップに変換されます。

- b. 暗号化アルゴリズムを選択した場合は、暗号化パスワードを指定（および確認）します。

- 暗号化パスワードは最大 23 文字に制限されています。
- フルバックアップと関連するすべての増分/検証バックアップでは、データの暗号化に同じパスワードを使用する必要があります。
- 増分/検証バックアップの暗号化パスワードが変更された場合、フルバックアップを実行する必要があります。つまり、暗号化パスワードが変更されたら、元のバックアップの種類にかかわらず、最初のバックアップは常にフルバックアップになります。

たとえば、暗号化パスワードを変更し、カスタマイズされた増分/検証バックアップを手動でサブミットした場合は、自動的にフルバックアップに変換されます。

- c. CA ARCserve D2D では暗号化パスワード管理が提供されるため、ユーザが暗号化パスワードを記憶している必要がありません。
- パスワードも暗号化されます。
 - 同じマシンにリストアする場合は、パスワードは記憶されているため必要ありません。
 - 別のマシンにリストアする場合、パスワードは必須です。
 - 暗号化されたデータが含まれる復旧ポイントのエクスポートを試行し、その復旧ポイントが現在のマシンで実行されたバックアップに含まれている場合、パスワードは必要ありません。
 - 暗号化されたデータの回復を、エクスポートされた復旧ポイントから実行する場合は常にパスワードが必要です。
 - 暗号化された復旧ポイントを参照するのにパスワードは必要ありません。
 - BMR を実行するためにはパスワードが必須です。
- d. 暗号化が有効になると、アクティビティログが更新されます。
- メッセージがアクティビティログに記録され、バックアップごとに選択された暗号化アルゴリズムについて記述されます。
 - メッセージがアクティビティログに記録され、増分/検証バックアップがフルバックアップに変換された理由(パスワード変更またはアルゴリズム変更) が示されます。

注: バックアップに対して暗号化設定を同じままにする必要はありません。同じデータを複数回バックアップした後でも、これらの設定はいつでも変更できます。

7. スロットルバックアップを指定します。

バックアップが書き込まれる最高速度 (MB/分) を指定できます。バックアップ速度のスロットル制御を実行すると、CPU またはネットワークの使用率を低減できます。ただし、バックアップ速度の制限は、バックアップウィンドウに悪影響を及ぼします。バックアップの最高速度を抑えるほど、バックアップの実行時間が増加します。バックアップジョブの場合、CA ARCserve D2D ホーム画面上の [ジョブ モニタ] に、進行中ジョブの平均読み取り/書き込み速度が表示され、設定されたスロットルスピード制限も示されます。

注: デフォルトでは、[スロットルバックアップ] オプションは有効ではなく、バックアップ速度は制御されません。

8. 推定バックアップサイズを計算します。

デスティネーションボリュームの推定使用量を表示します。

推定バックアップ計算の使い方の詳細については、「[将来のバックアップスペース要件の推定 \(P. 230\)](#)」を参照してください。

9. [設定の保存] をクリックします。

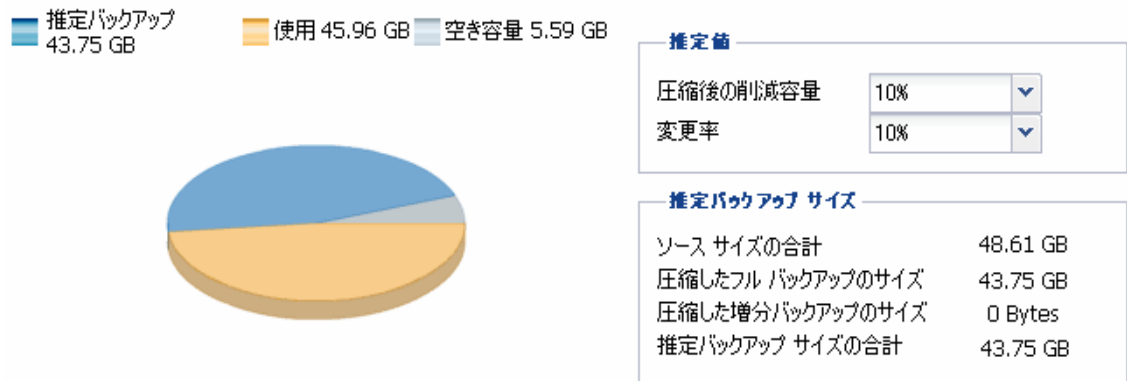
バックアップ保護設定が保存されます。

将来のバックアップスペース要件の推定

CA ARCserve D2D には、バックアップに必要な空き容量の推定値を計算するためのツールが用意されています。この計算は、将来のデータ変更の予測と過去のバックアップで使用された容量に基づいています。

推定バックアップ サイズ

以下のグラフは、バックアップ先ボリュームの推定使用量を示しています。[圧縮後の削減容量] または [変更率] を変更すると、推定バックアップ サイズへの影響を確認することができます。



i 現在のバックアップで使用される実際のディスク容量: 38.89 GB。

このツールの使用方法

1. バックアップソースを選択します。これは、マシン全体か、またはマシン内の選択したボリュームのいずれかです。

選択されたバックアップソースの実サイズが [ソース サイズの合計] フィールドに表示されます。

2. 将来のバックアップの予想変更率を見積もります。

この推定は、合計バックアップサイズが以後の各増分バックアップでどのくらい変化したかに関する過去のパフォーマンスに基づいて行います。

推定値が定義されている場合、CA ARCserve D2D はバックアップ先の設定と復旧ポイントに基づいて必要な推定バックアップサイズを計算して表示します。また、円グラフには、使用容量および空き容量も表示されます。

3. 圧縮後の削減容量をパーセンテージで見積もります。

推定値

推定値を使用すると、復旧ポイントの数に基づいて総バックアップサイズの概算値を計算できます。この推定は、異なる圧縮設定を適用した過去のバックアップのパフォーマンスに基づいて行います。この値を変更すると、それに応じたバックアップサイズへの影響を確認できます。

注: 必要な場合、異なる圧縮設定（圧縮なし、標準圧縮、および最大圧縮）でフルバックアップを何度か実行して過去のパフォーマンス値を定義しておく、各設定によって実現される容量の削減率をより正確に計算できます。

■ 圧縮後の削減容量

この値は、圧縮後に節約されたディスク容量を示します。

例: ボリュームのデータサイズが **1000 MB** で、バックアップ後の圧縮データサイズが **800 MB** である場合、圧縮後の削減容量の推定値は **200 MB (20%)** です。

■ 変更率

この値は、増分バックアップの一般的なデータサイズを示します。

例: 増分バックアップのデータサイズが **100 MB** で、フルバックアップのデータサイズが **1000 MB** である場合、推定変更率は **10%** です。

推定バックアップサイズ

ソースサイズの合計、圧縮したフルバックアップのサイズ、圧縮した増分バックアップのサイズ、および推定バックアップサイズの合計の推定値が表示されます。

- [圧縮したフルバックアップのサイズ] フィールドには、以下に基づく計算値が表示されます。
 - バックアップソースのサイズ
 - 指定した圧縮率
- [圧縮した増分バックアップのサイズ] フィールドには、以下に基づく計算値が表示されます。
 - 推定変更率
 - 保存される復旧ポイントの数
 - 指定した圧縮率
- [推定バックアップサイズの合計] フィールドには、将来のバックアップに必要な予想スペースが表示されます。この値は、以下に基づきます。
 - 1回のフルバックアップに必要な容量
 - 指定した数の復旧ポイントを保存するために必要な増分バックアップの容量

4. この [推定バックアップサイズの合計] 値に基づいて、バックアップ先にバックアップを保存するための十分なスペースがあるかどうかを調べることができます。

バックアップ先に十分な空き容量が存在しない場合は、以下の修正処置を検討してください。

- 保存する復旧ポイントの数を減らす。
- バックアップ先の利用可能な空き容量を増やす。
- より大容量のバックアップ先に変更する。
- バックアップソースのサイズを減らす (バックアップから不要なボリュームを除外する)。
- バックアップの圧縮率を大きくする。

バックアップ スケジュールの指定

CA ARCserve D2D では、バックアップのスケジュールを指定できます。

注: バックアップ設定に関連するビデオを閲覧するには、「[バックアップ設定の管理](#) (P. 214)」を参照してください。

バックアップ スケジュールの指定

1. CA ARCserve D2D ホーム画面（または CA ARCserve D2D モニタ）で、タスクバーから [設定] を選択し、[バックアップ設定] タブを選択します。[バックアップ設定] ダイアログボックスが開いたら、[スケジュール] を選択します。

[バックアップ設定] の [スケジュール] ダイアログボックスが表示されます。

The screenshot shows the 'Backup Settings' dialog box with the 'Schedule' tab selected. The dialog has a sidebar on the left with icons for Backup Settings, Security Settings, Schedule, Expansion, and Backup/Restore Settings. The main area is titled 'スケジュール' (Schedule) and contains the following sections:

- 開始日時の設定** (Start Date/Time Settings):
 - フル バックアップ、増分バックアップ、検証バックアップのスケジュール開始日と開始時刻を指定してください。
 - 開始日: 11/04/25
 - 開始時刻: 3:04 午後
- 増分バックアップ** (Incremental Backup):
 - CA ARCserve D2D は、最後に正常に完了したバックアップ後に変更されたデータのみを増分バックアップします。
 - 繰り返し実行する (一定間隔: 1 日)
 - 実行しない
- フル バックアップ** (Full Backup):
 - CA ARCserve D2D は、選択したデータをマシンからすべてバックアップします。
 - 繰り返し実行する (一定間隔: 1 日)
 - 実行しない
- 検証バックアップ** (Verify Backup):
 - CA ARCserve D2D は最後に正常に完了したバックアップ データとソース データを比較し、信頼性チェックを実行します。次に差分のみを増分バックアップ (再同期) します。最終的なバックアップ サイズは増分バックアップよりも小さいか同程度ですが、すべてのデータを比較するため増分バックアップよりも時間がかかる場合があります。
 - 繰り返し実行する (一定間隔: 1 日)
 - 実行しない

At the bottom of the dialog are buttons for '設定の保存' (Save Settings), 'キャンセル' (Cancel), and 'ヘルプ' (Help).

2. バックアップ スケジュール オプションを指定します。

開始日時の設定

スケジュールされたバックアップの開始日および開始時刻を指定します。

注: 繰り返しバックアップ ジョブの間隔を設定する際に、次のバックアップ ジョブが始まる前に前のジョブおよび関連するマーレジョブが完了するのに十分な時間を設定します。この時間の見積もりは、ユーザ自身の特定のバックアップ環境および履歴に基づいて行うことができます。

増分バックアップ

増分バックアップのバックアップ スケジュールを指定します。

スケジュールされたとおりに、前回の成功したバックアップ以降に変更されたブロックのみの増分バックアップが CA ARCserve D2D によって実行されます。増分バックアップのメリットは、バックアップを高速で実行できること、また作成されるバックアップイメージのサイズが小さいことです。これは、バックアップを実行する場合に最も適した方法です。そのため、デフォルトではこのバックアップを使用します。

利用可能なオプションは「繰り返し実行する」と「実行しない」です。[繰り返し実行する] オプションを選択した場合、バックアップの実行間隔（分単位、時間単位、または日単位）を指定する必要があります。増分バックアップの最小設定は 15 分ごとです。

デフォルトでは、増分バックアップのスケジュールは 1 日ごとに繰り返すよう設定されています。

フルバックアップ

フルバックアップのバックアップ スケジュールを指定します。

CA ARCserve D2D は、スケジュールされたとおりに、ソースマシンから、使用されているすべてのブロックのフルバックアップを実行します。利用可能なオプションは「繰り返し実行する」と「実行しない」です。[繰り返し実行する] オプションを選択した場合、バックアップの実行間隔（分単位、時間単位、または日単位）を指定する必要があります。フルバックアップの最小設定は 15 分ごとです。

デフォルトでは、フルバックアップのスケジュールは [実行しない]（スケジュールされている繰り返しはない）です。

検証バックアップ

検証バックアップのバックアップ スケジュールを指定します。

CA ARCserve D2D は、スケジュールされたとおりに、保護されたデータが有効かつ完全であることを検証します。そのためには、保存されたバックアップイメージの信頼性チェックを元のバックアップソースに対して実行します。必要に応じてイメージが再同期されます。検証バックアップは、個別のブロックの最新バックアップを参照し、そのコンテンツおよび情報をソースと比較します。この比較によって、前回バックアップされたブロックが、ソースの対応する情報を表しているかどうかを検証します。ブロックのバックアップイメージがソースと一致しない場合（多くは、前回のバックアップ以降にシステムに変更が加えられていることが原因）、CA ARCserve D2D では、一致していないブロックのバックアップが更新（再同期）されます。また、検証バックアップを使用して、フルバックアップに必要な容量を消費せずにフルバックアップと同じ保証を得ることができます（実行の頻度は低い）。

メリット：変更されたブロック（前回のバックアップと一致しないブロック）のみがバックアップされるため、フルバックアップと比べて作成されるバックアップイメージが小さくなります。

デメリット：すべてのソースブロックが前回のバックアップのブロックと比較されるため、バックアップ時間が長くなります。

利用可能なオプションは「繰り返し実行する」と「実行しない」です。[繰り返し実行する] オプションを選択した場合、バックアップの実行間隔（分単位、時間単位、または日単位）を指定する必要があります。検証バックアップの最小設定は 15 分ごとです。

デフォルトでは、検証バックアップのスケジュールは [実行しない]（スケジュールされている繰り返しはない）です。

3. [設定の保存] をクリックします。

バックアップ スケジュール設定が保存されます。

注: ある時点に同時に実行するようスケジュールされたバックアップの種類が複数ある場合、実行されるバックアップの種類は、以下の優先度に基づきます。

- 優先度 1 - フルバックアップ
- 優先度 2 - 検証バックアップ
- 優先度 3 - 増分バックアップ
- たとえば、3 種類のバックアップすべてを同時に実行するようスケジュールされている場合、CA ARCserve D2D ではフルバックアップを実行します。フルバックアップがスケジュールされておらず、検証バックアップと増分バックアップを同時に実行するようスケジュールされている場合、CA ARCserve D2D では検証バックアップを実行します。スケジュールされた増分バックアップは、他の種類のバックアップとの競合がない場合のみ実行されます。

バックアップ拡張設定の指定

CA ARCserve D2D では、バックアップの拡張設定を指定できます。

注: バックアップ設定に関連するビデオを閲覧するには、「[バックアップ設定の管理](#) (P. 214)」を参照してください。

次の手順に従ってください:

1. CA ARCserve D2D ホーム画面（または CA ARCserve D2D モニタ）で、タスクバーから [設定] を選択し、[バックアップ設定] タブを選択します。[バックアップ設定] ダイアログボックスが開いたら [拡張] を選択します。

[拡張] ダイアログボックスが表示されます。



- バックアップ拡張設定オプションを指定します。

ログの切り捨て

選択したアプリケーションに対して蓄積されたトランザクションログ ファイルを、次に正常にバックアップが完了した後に切り捨てます。

CA ARCserve D2D バックアップは、スナップショット イメージと、そのイメージ用に作成されたトランザクション ログ ファイルで構成されます。ある時点で古い（コミット済み）トランザクション ログ ファイルは必要ではなくなるため、新しいログ ファイルのスペースを作るためにパージできます。これらのログ ファイルをパージするプロセスを、ログの切り捨てと呼びます。このオプションを選択すると、コミット済みのトランザクション ログ ファイルの切り捨てが有効になり、ディスク容量を節約できます。

利用可能なオプションは、「SQL Server」および「Exchange Server」です。これらのアプリケーションのどちらか、または両方を選択でき、どちらも選択しないことも可能です。これらのアプリケーションのいずれかを選択した場合、自動的なログ切り捨てのスケジュール（[毎日]、[毎週]、[毎月]）を指定できます。

注: バックアップが正常に完了しないと、トランザクション ログ ファイルの切り捨ては実行されません。

- [毎日] - 毎日のバックアップが正常に完了した直後に、コミット済みのトランザクション ログがパージされます。
- [毎週] - 7 日後のバックアップが正常に完了した直後に、コミット済みのトランザクション ログがパージされます。
- [毎月] - 30 日後のバックアップが正常に完了した直後に、コミット済みのトランザクション ログがパージされます。

ページの実行がスケジュールされた時刻にバックアップジョブがすでに実行中である場合、ページ処理は次のスケジュールジョブに移動します。

例：

増分バックアップが毎日午後 5 時に自動的に実行されるようにスケジュールされており、午後 4 時 55 分にフルバックアップを手動で開始した場合を考えてみます。バックアップは午後 5 時 10 分に正常に完了するとします。

この場合、アドホックなフルバックアップが進行中なので、午後 5 時にスケジュールされている増分バックアップはスキップされます。コミットされたトランザクションログファイルは、次のバックアップジョブが成功した後にページされ、スケジュールされた増分バックアップが翌日の午後 5 時に正常に完了した後に実行されます。

デスティネーション上の予約容量

この値は、バックアップを実行するのに必要な計算された容量の割合を示します。この継続的な容量はバックアップがデータの書き込みを開始する前にデスティネーション上で直ちに予約され、バックアップ速度の改善に役立ちます。

デフォルト： 10%。

例： 値は 10% に設定され、現在のバックアップにはバックアップするデータが 50GB あります。バックアップがデータの書き込みを開始する前に、5 GB のディスク容量が予約されます。5 GB のディスク容量が使い果たされると、さらに 5 GB のディスク容量が予約されます。バックアップの残りデータが 5 GB 未満（あと 2 GB のバックアップが必要だと仮定します）である場合、残りの GB 数（この例では 2 GB）が予約されます。

Exchange 詳細リストア カタログ

各バックアップ後の Exchange 詳細リストア カタログの自動生成を有効にします。

Exchange 詳細リストア バックアップでは、電子メール メッセージ、メールフォルダ、Exchange のメールボックス レベルに関する情報を、Exchange データベースを通じた 1 回のバックアップでキャプチャします。このオプションを有効にすると、Exchange データベースの詳細復旧を実行できます。その場合は、Exchange データベースをまず別の場所に回復またはダンプしなくても、Exchange 内のオブジェクトのリストを選択し、回復する対象を厳密に指定することができます。

- メリット： Exchange 詳細リストア カタログを使用すると、リストアの参照を実行するのに長時間待機する必要がありません。
- デメリット： バックアップごとに Exchange 詳細リストア カタログを生成すると、バックアップ ウィンドウの拡大（バックアップ ジョブの完了までにかかる時間の増加）および作業負荷の増大につながります。CA ARCserve D2D では、それぞれのメールボックスを確認し、詳細情報を認証および構築する必要があります。メールボックスの数およびデータのサイズを考えると、これは非常に時間のかかる作業となります。
- このオプションを無効にすると、CA ARCserve D2D では Exchange の一般情報のみが保存されます。リストアの前には、その時点で Exchange 詳細リストア カタログを生成することができます。

管理者アカウント

バックアップを実行するためのアクセス権がある [ユーザ名] および [パスワード] を指定します。CA ARCserve D2D によって、名前とパスワードが有効で、ユーザが管理者グループに属していることが確認されます。

重要： CA ARCserve D2D サーバの管理者アカウントの認証情報が変更されている場合（ユーザ名/パスワード）、このダイアログ ボックスでも管理者アカウント情報を再設定/更新する必要があります。

注： ドメインアカウントを指定する場合、ユーザ名の形式は、完全修飾ドメイン ユーザ名「<ドメイン名>\<ユーザ名>」の形式で指定します。

バックアップ デスティネーション接続の回復

バックアップ デスティネーションへの接続情報を更新（再同期）します。

リモート共有コンピュータへの定期的なバックアップを実行しており、そのリモート コンピュータ用のアクセス認証情報（ユーザ名/パスワード）を変更できる場合、このオプションを使用できます。その場合、ローカル コンピュータで設定されたアクセス認証情報がリモート コンピュータの新しい認証情報と一致しないので、次のバックアップは通常であれば失敗します。

注: [接続の更新] ボタンをクリックし、再同期プロセスが開始したら、キャンセルすることはできません。

この [更新] ボタンをクリックする前に、以下のタスクを実行します。

- リモート デスティネーション コンピュータにログインし、以下の `net session` コマンドを実行して、ローカル CA ARCserve D2D コンピュータとリモート コンピュータ間の接続を切断します。

```
net session ¥¥<コンピュータ名または IP アドレス> /d
```

- CA ARCserve D2D コンピュータに戻り、[接続の更新] ボタンをクリックします。
- デスティネーション用の新しいパスワードを入力します。
- CA ARCserve D2D は、設定されている認証情報を更新し、リモート共有デスティネーションの新しい認証情報と一致するようにします。ポップアップ確認画面が表示され、認証情報が更新されたことをユーザに通知します。

3. [設定の保存] をクリックします。

バックアップの拡張設定が保存されます。

バックアップの実行前/後の設定の指定

CA ARCserve D2D では、バックアップの実行前/後の設定を指定することができます。

注: バックアップ設定に関連するビデオを閲覧するには、「[バックアップ設定の管理 \(P. 214\)](#)」を参照してください。

3. [設定の保存] をクリックします。
バックアップ実行前/後の設定が保存されます。

環境設定の指定

[環境設定] ダイアログ ボックスでは、CA ARCserve D2D の動作に関する各種オプションを迅速かつ容易に指定するための方法が提供されます。クリックすると [環境設定] ダイアログ ボックスが開き、以下のタブが表示されます。

- [一般](#) (P. 244)
- [電子メールアラート](#) (P. 246)
- [更新](#) (P. 254)

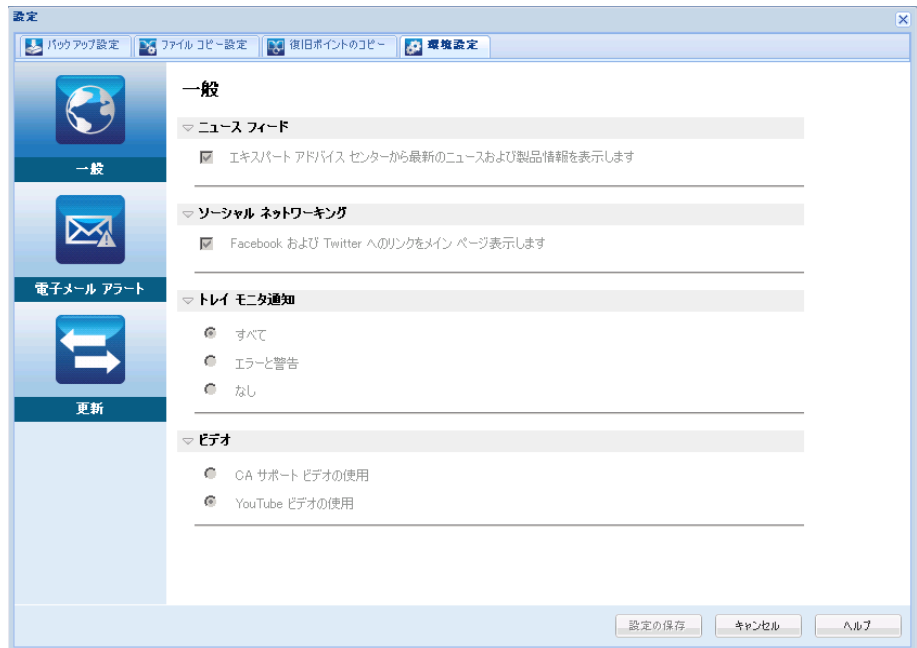
一般的な環境設定の指定

CA ARCserve D2D では、以下の一般的な環境設定を指定できます。

一般的な環境設定の指定

1. CA ARCserve D2D ホーム画面（または CA ARCserve D2D モニタ）で、タスクバーから [設定] を選択し、[環境設定] タブを選択します。[環境設定] ダイアログボックスが開いたら、[一般] を選択します。

[環境設定] の [一般] ダイアログボックスが開きます。



2. 一般の環境設定を指定します。

ニュースフィード

選択した場合、RSS フィードが有効になり、最新の CA ARCserve D2D 関連のニュースと製品情報（エキスパート アドバイス センターから）がホーム画面に表示されます。

ソーシャル ネットワーキング

選択した場合、Twitter と Facebook で CA ARCserve D2D 関連のソーシャル ネットワーキングにアクセスするためのアイコンがホーム画面上に表示されます。これらの選択は、ホーム画面を更新しないと有効になりません。

トレイ通知

表示するアラート通知の種類を選択します。有効なオプションは [なし]、[すべて]、[エラーと警告] です。

ビデオ

CA ARCserve D2D のビデオに [使用方法] 画面または [サポートおよびコミュニティへのアクセス] タスクバーのいずれかからアクセスした場合に、ビデオを参照するためのソースを選択します。これらの「手順」ビデオを参照するために選択できるオプションは、[CA サポート ビデオの使用] と [YouTube ビデオの使用] です（ビデオの内容はどちらのソースでも同じです）。

注: この選択は、関連するヘルプ トピックで提供されているビデオ表示オプションには影響しません。

3. [設定の保存] をクリックします。
一般の環境設定が保存されます。

電子メール環境設定の指定

CA ARCserve D2D では、以下の電子メールアラート環境設定を指定できます。

電子メールアラートの環境設定の指定

1. CA ARCserve D2D ホーム画面（または CA ARCserve D2D モニタ）で、タスクバーから [設定] を選択し、[環境設定] タブを選択します。[環境設定] ダイアログボックスが開いたら、[電子メールアラート] を選択します。

[環境設定] の [電子メールアラート] ダイアログボックスが表示されます。



2. 電子メールアラート通知設定を指定します。

選択したイベントが完了したときに、自動的に電子メールアラート通知が送信されます。以下のオプションのいずれかまたはすべてを選択できます。

注: 成功したジョブについて特に通知を必要としない場合、失敗したジョブまたは実行されなかったジョブについてのみ電子メールアラートが送信されるよう **CA ARCserve D2D** を設定できます。この設定により、電子メール通知の量を減らすことができるだけでなく、失敗をモニタしやすくなります。

以下のイベント通知を送信するオプションが利用可能です。

ジョブが失敗した場合

失敗したすべてのジョブについて電子メールアラート通知を送信します。失敗したジョブとは、スケジュールが設定されているが、スケジュール時刻に実行されなかったジョブのことです。失敗したジョブは、同じ種類の他のジョブが実行中の場合、または先に開始したジョブがまだ完了していない場合に発生します。

CA ARCserve D2D では、異なる種類のジョブを同時に実行することは可能ですが、同じ種類のジョブは一度に1つしか実行できません。たとえば、コピージョブがスケジュールされた時間に、別のコピージョブがまだ実行されている場合、スケジュールされたコピージョブは実行されませんが、別のバックアップジョブは予定どおり実行することができます。

バックアップ、カタログ、ファイルコピー、リストア、復旧ポイントのコピージョブが失敗またはクラッシュした場合

バックアップ、カタログ、ファイルコピー、リストア、復旧ポイントのコピーのジョブ試行が失敗すると、アラート通知を送信します。このカテゴリには、失敗、未完了、およびキャンセルされたジョブと、クラッシュしたジョブ試行のすべてが含まれます。

注: これらの電子メールアラートは高い重要度で送信されます。高い重要度レベルに設定された電子メールアラートには、受信トレイ内で感嘆符の視覚的インジケータが表示されます。

バックアップ、カタログ、ファイルコピー、リストア、または復旧ポイントのコピージョブが成功した場合

バックアップ、カタログ、ファイルコピー、リストア、復旧ポイントのコピーのジョブ試行が成功すると、アラート通知を送信します。

マージジョブが停止、スキップ、失敗、またはクラッシュした場合

停止、スキップ、失敗、またはクラッシュしたすべてのマージジョブについて、アラート通知を送信します。このアラートを有効にすると、マージジョブが失敗した場合に通知が送られます。

マージ失敗は、以下の理由で発生する場合があります。

- セッションがマウントされている。
この問題を解決するために、セッションをマウント解除できます。
- セッションがカタログジョブによってロックされている。
このセッションは、次のバックアップジョブによって自動的にマージされます。
- セッションが他の理由でロックされている。

このアラートを無効にすると、トレイモニタのバルーンメッセージ、または CA ARCserve D2D ホームページ上の復旧ポイントのサマリーで、マージがいつ失敗したかしかわからなくなります。

マージジョブが成功した場合

成功したすべてのマージジョブについて電子メールアラート通知を送信します。

バックアップ先の空き容量が次の値を下回った場合

バックアップ先の未使用容量が指定した値を下回った場合、電子メールアラート通知を送信します。このオプションでは、アラート通知を送信するしきい値として、全容量の割合または特定の値（単位 - MB）のどちらかで指定するかを選択することができます。

新しい更新がある場合

CA ARCserve D2D 用の新しい更新が利用可能な場合に電子メール通知を送信します。更新の確認中またはダウンロード中に問題が発生した場合も、電子メール通知が送信されます。

リソースアラートの有効化

指定されたリソースのしきい値レベルに到達した場合に電子メール通知を送信します。サーバの効率性と信頼性を確保するには、常にパフォーマンスをモニタして潜在的な問題を特定し、ボトルネックとなる状況を迅速に解消する必要があります。

これらのリソース インジケータのしきい値レベルを定義することは、サーバに関するユーザの知識に基づいて、完全にユーザの裁量において行われます。正しい設定や誤った設定を指定することはできません。これらのアラート通知は「正常」で許容可能なパフォーマンスに基づいて設定します。たとえば、システムが通常は 80% の CPU 負荷で実行される場合、CPU 使用率のしきい値に 75% を設定することは効率的かつ有用とは言えません。

これらの各リソース パラメータは、対応するしきい値レベルに達するとそれぞれ個別にアラート通知を送信するように設定できます。送信される各リソース アラート電子メールの最大数は 1 日あたり 5 通までです。

- CPU 使用率

指定された CPU 使用率のアラートしきい値は、CA ARCserve D2D によって保護されているサーバの CPU 使用率を示します。このアラート通知を使用すると、サーバが頻繁に過負荷状態になることがないかを確認できます。

CPU 使用率が高すぎると、サーバの応答時間が遅くなるか、反応しなくなる場合があります。そのため、負荷の分散（バランシング）を検討する必要があります。

- ディスク スループット

指定されたディスク スループットのアラートしきい値は、CA ARCserve D2D によって保護されたサーバのディスク スループット (MB/秒) を示します。このアラート通知を使用すると、ディスクの処理能力が最大限に利用されていることを確認できます。

ディスク スループットがディスクの最大処理能力に近い場合、ニーズと一致させるためにディスクのアップグレードを検討してください。通常、高速なディスクほどパフォーマンスは高くなります。

- **メモリ使用率**

指定されたメモリ使用率のアラートしきい値は、CA ARCserve D2D によって保護されたサーバのメモリ使用率を示します。使用率は、メモリ容量のどれくらいが使用されているかを表します。使用率が高くなるほど、サーバのパフォーマンスは低くなります。

メモリ使用率が頻繁に高くなりすぎる場合、原因となっているプロセスを特定する必要があります。このインジケータ設定を使用して、アプリケーションまたはサーバのアップグレードが必要となった場合に警告されるようにすることができます。

- **ネットワーク I/O**

指定されたネットワーク I/O のアラートしきい値は、CA ARCserve D2D によって保護されたサーバでの現在の NIC 帯域幅使用率を示します。使用率は、ネットワーク インターフェース カード (NIC) がどの程度使用されているかを表します。使用率が高くなるほど、ネットワークのパフォーマンスは低くなります。

ネットワーク使用率が頻繁に高くなりすぎる場合、原因となっているプロセスを特定して問題を解決する必要があります。また、特定のネットワーク容量に基づいて、バックアップ中のネットワーク使用率が高すぎる場合、NIC カードをアップグレードして高いスループット要件に対応することができます。

3. [設定の保存] をクリックします。

電子メール アラートの環境設定が保存されます。

電子メール通知を送信するよう選択したら、[電子メールの設定] をクリックし、関連するダイアログ ボックスを表示します。

電子メール設定の指定

[電子メールの設定] ダイアログ ボックスから、以下のような電子メール設定を指定できます。

- メール サーバ
- 件名
- 電子メールの送信者
- 電子メールの受信者

プロキシ設定を有効にして定義することもできます。これらの設定は、すべての電子メールアラート通知に適用されます。また、設定はいつでも変更できます。

電子メール設定の完了後、[テスト電子メール] ボタンを使用して設定をテストできます。ジョブが正常に実行されたか失敗した後に、誤った設定に対する電子メールアラートを受信しても手遅れです。そのため、電子メール情報のテストでは、設定を検証し、指定された設定で電子メールの送信を試行します。電子メール設定が有効な場合、そのようなメッセージを含む電子メールを受信します。電子メール設定が無効な場合、失敗メッセージを受信します。

電子メールの設定

電子メールの設定

サービス

電子メール サーバ ポート

認証が必要

アカウント名

パスワード

件名

送信者

受信者

SSL を使用 STARTTLS の送信 HTML 形式を使用

プロキシ設定を有効にする

プロキシ サーバ ポート

認証が必要

プロキシ ユーザ名

プロキシ パスワード

テスト電子メール OK キャンセル ヘルプ

サービス

アラート通知の送信に使用する電子メールプロバイダサービス。利用可能なオプションは、Google メール、Yahoo メール、Live メールおよびその他です。

- [その他] を選択する場合、使用されるメールサーバおよび対応するポート番号を特定する必要があります。
- [Google メール]、[Yahoo メール]、[Live メール] を選択する場合、メールサーバとポート番号は自動的に入力されます。

デフォルト：その他

メールサーバ

CA ARCserve D2D で電子メールアラートの送信に使用できる SMTP メールサーバのホスト名。

ポート

メールサーバの出力ポート番号。

認証が必要

インターネット経由で電子メールを送信する際、このメールサーバが認証を必要とするかどうかを指定します。このオプションを選択する場合、対応するユーザアカウント名とパスワードを指定する必要があります。

件名

CA ARCserve D2D が送信する電子メールアラート通知の件名。

デフォルト：「CA ARCserve D2D アラート」

送信者

CA ARCserve D2D で電子メールアラート通知の送信に使用する電子メールアドレス。

受信者

送信された電子メールアラート通知の受信者の電子メールアドレス。

注：複数の電子メールアドレスを入力するには、各アドレスをセミコロンで区切る必要があります。

SSL の使用

インターネット経由でデータを安全に転送するために、電子メールサーバで SSL (Secure Sockets Layer) 接続を必要とすることを指定します。

STARTTLS の送信

サーバ間で安全な SMTP 接続を開始するために、発行される STARTTLS (Start TLS extension) コマンドを電子メールサーバで必要とすることを指定します。

HTML 形式を使用

電子メールアラート通知が HTML 形式で送信されます。このオプションを選択しない場合、アラートはプレーンテキストで送信されます。デフォルトでは、このオプションが選択されています。

プロキシ設定を有効にする

電子メールアラート通知を送信する際に、プロキシサーバに接続するかどうかを指定します。このオプションを選択する場合、対応するプロキシサーバ名とポート番号を指定する必要があります。

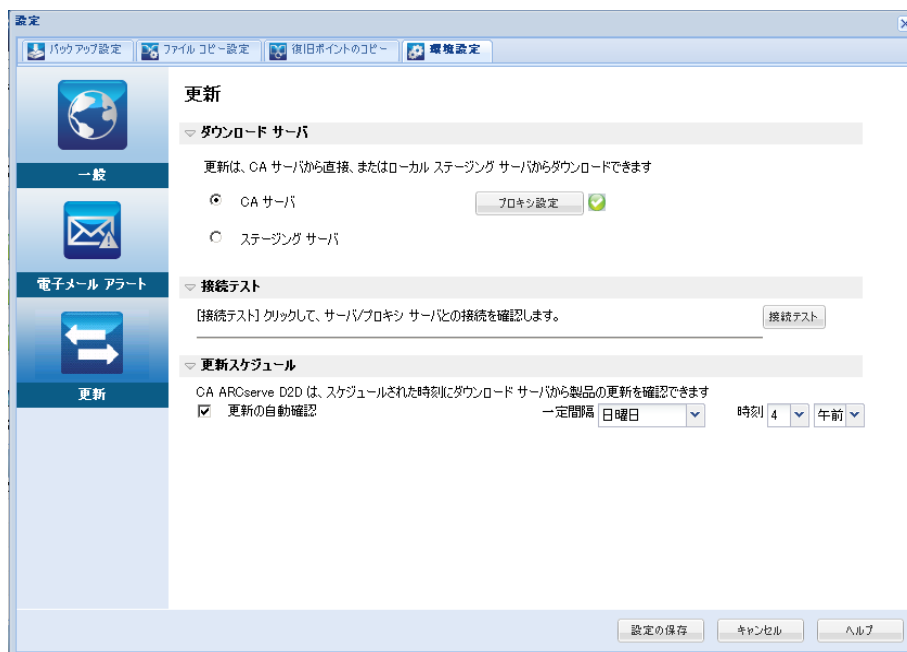
更新の環境設定の指定

CA ARCserve D2D では、以下の更新環境設定を指定できます。

更新環境設定の指定

1. CA ARCserve D2D ホーム画面（または CA ARCserve D2D モニタ）で、タスクバーから [設定] を選択し、[環境設定] タブを選択します。[環境設定] ダイアログボックスが開いたら、[更新] を選択します。

[環境設定] の [更新] ダイアログボックスが開きます。



2. 更新の環境設定を指定します。

ダウンロードサーバ

CA ARCserve D2D サーバが利用可能な更新をダウンロードするために接続するソースサーバを指定します。

■ CA サーバ

このオプションを使用すると、CA ARCserve D2D 更新が CA Technologies サーバからローカルサーバに直接ダウンロードされます。

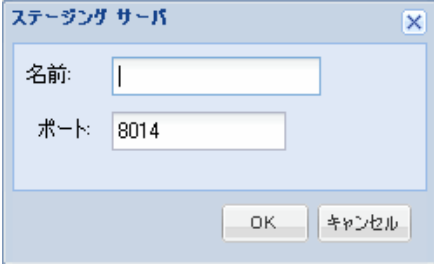
これはデフォルトの設定です。

■ ステージング サーバ

このオプションを使用すると、ステージング サーバとして使用されるサーバを指定できます。

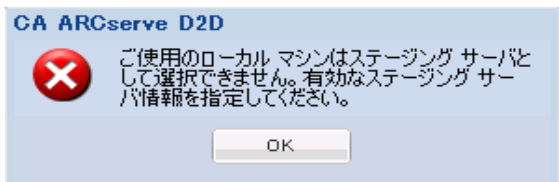
複数のステージング サーバを指定した場合、リストの最初のサーバがプライマリ ステージング サーバとして指定されます。CA ARCserve D2D は、まずプライマリ ステージング サーバへの接続を試行します。何らかの理由で最初のサーバが利用可能でない場合は、リストの次のサーバがプライマリ ステージング サーバになります。リストの最後のサーバがプライマリ ステージング サーバになるまで、この手順が続行されます（ステージング サーバリストには最大で5つのサーバを含めることができます）。

- [上に移動] および [下に移動] ボタンを使用してステージング サーバの順序を変更できます。
- [削除] ボタンを使用して、このリストからサーバを削除できます。
- 新しいサーバをこのリストに追加するには [サーバの追加] ボタンを使用します。[サーバの追加] ボタンをクリックすると、[ステージング サーバ] ダイアログ ボックスが開き、追加するステージング サーバの名前を指定できます。



CA ARCserve D2D 更新は、CA Technologies サーバから指定されたステージング サーバ場所へ直接ダウンロードされます。更新がステージング サーバにダウンロードされたら、その更新をステージング サーバからクライアント サーバにダウンロードできます。ステージング サーバを選択した場合、ステージング サーバのホスト名または IP アドレスと、対応するポート番号も指定する必要があります。

使用しているローカルクライアントサーバをステージングサーバとして指定することはできません。更新をダウンロードするためにステージングサーバが自身に接続することはできないため、これは無効な設定です。ステージングサーバとしてローカルクライアントサーバを使用しようとすると、エラーメッセージが表示されます。



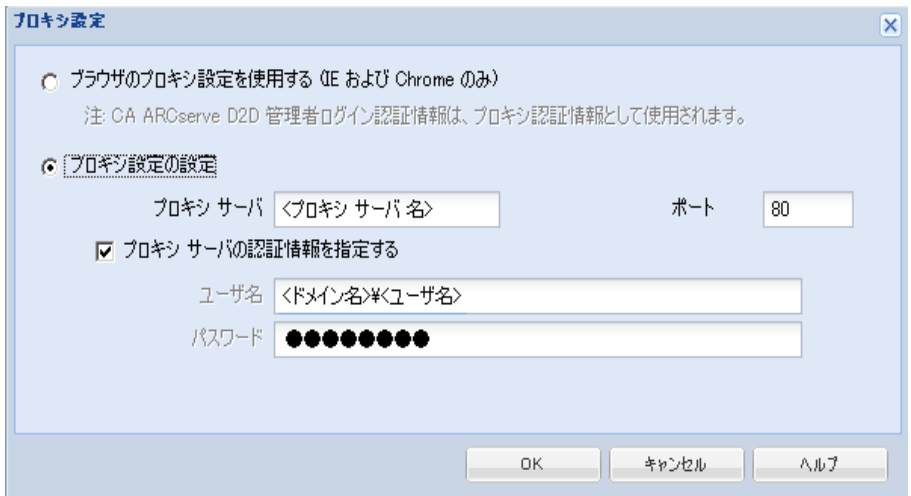
注: Web 通信に対してステージングサーバ上で HTTPS が有効になっている場合、そのサーバから CA ARCserve D2D 更新をダウンロードすることはできません。

■ プロキシ設定

注: このプロキシサーバオプションは、ダウンロードサーバとして CA Technologies サーバを選択した場合のみ使用できます。

CA ARCserve D2D 更新をプロキシサーバ経由でダウンロードする場合はプロキシ設定を選択します。プロキシサーバは、ダウンロードサーバ（ステージングまたはクライアント）と CA Technologies サーバとの間の中継として機能します。目的は、セキュリティ、パフォーマンス、管理制御を向上させることです。これは、ダウンロードサーバが更新を入手する先の CA Technologies サーバへの接続になります。

このオプションを選択すると、[プロキシ設定] ダイアログボックスが表示されます。



- ブラウザのプロキシ設定を使用する

このオプションは、Windows Internet Explorer (IE) および Google Chrome にのみ適用されます。

選択された場合、CA ARCserve D2D では、ブラウザに適用されたプロキシ設定を自動的に検出し、同じ設定を使用して、CA ARCserve D2D の更新情報の取得のために CA Technologies サーバに接続します。

- プロキシ設定の設定

選択された場合、指定されたプロキシサーバが有効になり、CA ARCserve D2D の更新情報の取得のために CA Technologies サーバに接続します。このオプションを選択すると、プロキシサーバの IP アドレス（またはマシン名）およびプロキシサーバがインターネット接続する際に使用される、対応するポート番号も指定する必要があります。

また、プロキシサーバで認証が必要かどうかも指定できます。指定すると、プロキシサーバを使用する際に認証情報（ユーザ ID とパスワード）が必要となります。

注: ユーザ名の形式は、「<ドメイン名>¥<ユーザ名>」の形式で完全修飾ドメインユーザ名を指定する必要があります。

接続テスト

以下の接続をテストして、完了時にステータス メッセージを表示させることができます。

- ダウンロードサーバとして CA Technologies サーバを選択した場合、指定されたプロキシサーバを介したマシンと CA Technologies サーバ間の接続をテストします。
- ダウンロードサーバとしてステージングサーバを選択した場合、指定されたステージングサーバとマシン間の接続をテストします。[接続テスト] ボタンを使用して、リストに含まれているステージングサーバの可用性をテストできます。また、対応するステータスが [接続状態] フィールドに表示されます。設定されたステージングサーバがどれも利用可能でない場合は、赤いアイコンがホーム画面のステータス サマリ セクションに表示され、この状態について視覚的に警告します。

注: ホーム画面から [環境設定 - 更新] ダイアログ ボックスを開くと、接続テストが自動的に実行されます。この自動テストが実行された場合、以前に設定されたダウンロードサーバ (CA Technologies サーバまたはステージング サーバのいずれか選択された方) の最新の接続ステータスが確認されます。以前に複数のステージング サーバが設定されていた場合、この自動テストは、すべてのステージング サーバに対して実行され、最新の接続ステータスが取得されます。

更新スケジュール

新しい CA ARCserve D2D 更新をチェックしてダウンロードするタイミングを指定します。

- このオプションを選択して、利用可能な新しい CA ARCserve D2D 更新を自動的にチェックするかどうかを指定します。このオプションを選択すると、ドロップダウンメニューを使用して、この機能を実行する日 (毎日、毎週、または指定した曜日) と時刻を指定できます。

注: インストール時に CA ARCserve D2D によって、これらの確認する曜日または時刻のデフォルト設定は自動で実行され、無作為に割り当てられます。インストール後、この [更新スケジュール] 設定を使用して、これらの確認する曜日および時刻を変更できます。

このチェックによって新しい更新が利用可能であることが判断された場合、デフォルトでは、CA ARCserve D2D によって自動的に更新がダウンロードされます。この自動ダウンロードが実行されないようにするには、D2DPMSettings.INI ファイルでこの機能を無効にします。詳細については、付録 B 「D2DPMSettings.INI ファイル」を参照してください。

- このオプションが選択されていない場合、自動チェックとダウンロードの機能はすべて無効になります (ホーム画面のステータス サマリ セクションにそのステータスが表示されます)。このオプションが選択されていないければ、これらの更新機能は手動でのみ開始できます。

注: スケジュールされた更新チェックで新しい更新が利用可能であることがわかった場合に、電子メール通知が送信されるよう設定することができます。また、更新の確認中またはダウンロード中に問題が発生した場合も、電子メール通知が送信されます。

3. [設定の保存] をクリックします。

更新の環境設定が保存されます。

アプリケーションのリストア

CA ARCserve D2D では、データの保護や回復を行うだけでなく、そのデータを使用するアプリケーションのバックアップや実行をサポートします。すべてのアプリケーションの回復は、復旧ポイントによるリストア方式を使用して実行されます。アプリケーションの回復の際、CA ARCserve D2D は Windows ボリューム シャドウ コピー サービス (VSS) を利用して、VSS に対応したアプリケーションのデータ整合性を保ちます。CA ARCserve D2D を使用すると、完全な惨事復旧を実行せずに、以下のアプリケーションを回復できます。

- [Microsoft Exchange Server](#) (P. 259)
- [Microsoft SQL Server](#) (P. 268)

アプリケーションのリストア - MS Exchange Server

CA ARCserve D2D では、データの保護や回復を行うだけでなく、そのデータを使用する Microsoft Exchange Server アプリケーションのバックアップや実行をサポートします。Microsoft Exchange Server を復旧するには、「復旧ポイントによるリストア」方式を使用する必要があります。



ビデオ

CA サポート :

MS Exchange アプリケーションのリストア方法
(http://www.arcserve.com/arcserve2d/r16/redirect.php?item=video_restore_application_exchange_support)

YouTube :

MS Exchange アプリケーションのリストア方法
(http://www.arcserve.com/arcserve2d/r16/redirect.php?item=video_restore_application_exchange_youtube)

CA ARCserve D2D は、Microsoft Exchange Server の以下のバージョンをサポートしています。

- **Exchange 2003** - シングル サーバ環境。
- **Exchange 2007** - シングル サーバ環境、ローカル連続レプリケーション (LCR) 、クラスタ連続レプリケーション (CCR) 環境。

Exchange 2007 CCR 環境の場合、CA ARCserve D2D は、Microsoft クラスターのアクティブ ノードおよびパッシブ ノードの両方にインストールされる必要があります。バックアップはアクティブ ノードおよびパッシブ ノードから実行できますが、リストアはアクティブ ノードに対してのみ実行できます。

- **Exchange 2010** - シングル サーバ環境およびデータベース可用性グループ (DAG) 環境。

Exchange 2010 DAG 環境の場合、CA ARCserve D2D は DAG グループ内のすべてのメンバサーバにインストールされる必要があります。バックアップジョブは、アクティブおよびパッシブの両方のデータベース コピーに対して、すべてのメンバサーバから実行できます。しかし、リストアはアクティブなデータベース コピーに対してのみ実行できます。

注: Microsoft Exchange Server 2003 クラスタ環境および Microsoft Exchange Server 2007 シングル コピー クラスタ (SCC) 環境は、CA ARCserve D2D ではサポートされていません。

Microsoft Exchange Server は以下のレベルでリストアできます。

Microsoft Exchange ライタ レベル

Microsoft Exchange Server データをすべてリストアする場合、Microsoft Exchange ライタ レベルでリストアを実行できます。

ストレージグループレベル

特定のストレージグループをリストアする場合、Microsoft Exchange ストレージグループ レベルでリストアを実行できます。

(Microsoft Exchange Server 2010 には適用されません。)

メールボックス ストア レベル (Exchange 2003)

特定のメールボックス ストアをリストアする場合、メールボックス ストア レベルでリストアを実行できます。

メールボックス データベース レベル (Exchange 2007/2010)

特定のメールボックス データベースをリストアする場合、メールボックス データベース レベルでリストアを実行できます。

Microsoft Exchange Server アプリケーションのリストア

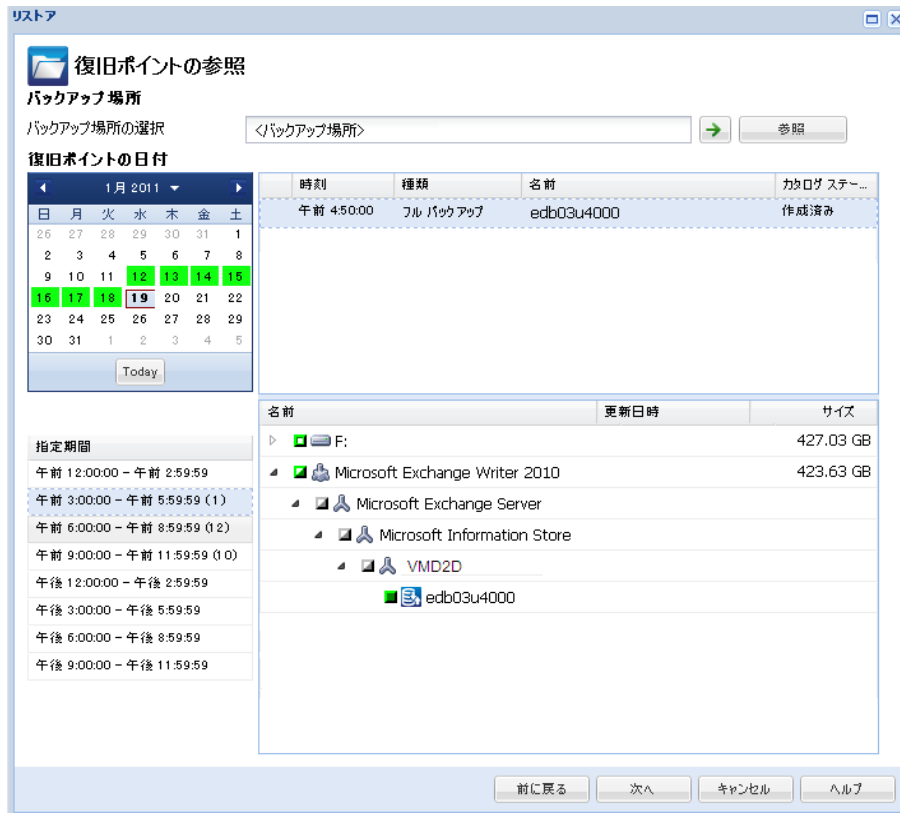
注: Microsoft Exchange Server データベース リストアを実行する場合 (元の場所または回復用ストレージ グループ/回復用データベースのいずれかに対して)、アカウントが以下の管理者権限も持っていることを確認する必要があります。

- Exchange 2003 - Exchange 管理者 (完全) の役割
 - Exchange 2007/2010 - Exchange 組織管理者、または Exchange Server 管理者の役割
1. CA ARCserve D2D ホーム画面 (または CA ARCserve D2D モニタ) から、
[リストア] を選択します。
リストア方式を選択するダイアログ ボックスが表示されます。
 2. [復旧ポイントの参照] オプションをクリックします。
[復旧ポイントの参照] ダイアログ ボックスが表示されます。

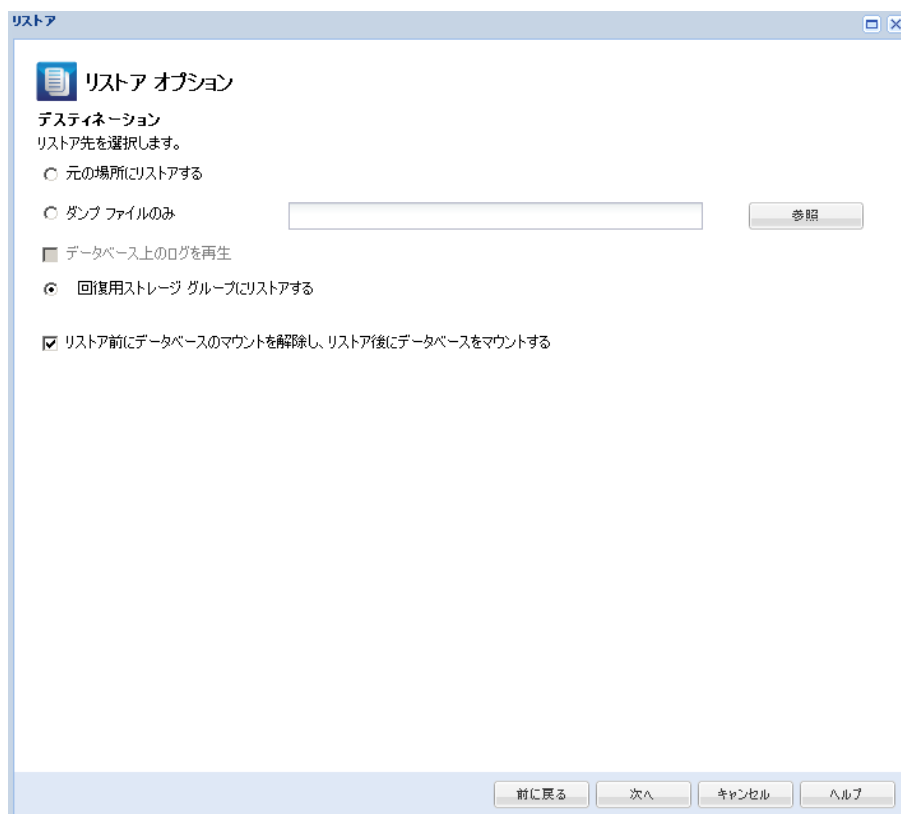
3. 復旧ポイント（日付と時間）を選択した後、リストアする Microsoft Exchange データベースを選択します。

対応するボックスが緑色に塗りつぶされます。これは、データベースがリストア対象として選択されたことを示しています。

注: リストア後にトランザクションログファイルが適用されないようにする場合は、リストアが実行される前に手動で削除する必要があります。トランザクションログファイルの手動での削除の詳細については、Microsoft Exchange Server のドキュメントを参照してください。



4. [次へ] をクリックします。
[リストア オプション] ダイアログ ボックスが表示されます。



5. リストア先を選択します。

利用可能なオプションは、[元の場所にリストアする]、[ダンプ ファイルのみ]、[回復用ストレージグループにリストアする]、[回復用メールボックス データベースにリストアする] です。

元の場所にリストアする

バックアップ イメージがキャプチャされた元の場所にリストアします。

ダンプファイルのみ

ダンプファイルのみをリストアします。

このオプションの場合、CA ARCserve D2D は Microsoft Exchange データベース ファイルを指定のフォルダにリストアし、回復が完了するまでデータベースをオンラインにしません。このファイルを別のサーバに移動し、Exchange サーバに手動でマウントして、ファイル内に含まれているデータを表示できます。

注: 回復用メールボックス データベースが存在する場合、「ダンプファイルのみ」オプションを使用したリストアは失敗します。

データベース上のログを再生

データベース ファイルをデスティネーションフォルダにダンプする際に、すべての Microsoft Exchange トランザクション ログ ファイルの再生および適用を行い、それらをデータベースにコミットするように指定できます。次回データベースを起動すると、データベースが利用可能になる前に、データベースにまだ書き込まれていないログ ファイルが適用されます。

注: このオプションは Microsoft Exchange Server 2003 では適用されません。

回復用ストレージグループにリストアする(Exchange 2007)

回復用ストレージグループ (RSG) にデータベースをリストアします。

RSG は、回復用に使用できるストレージグループです。Microsoft Exchange メールボックス データベースを、回復用ストレージグループ内のバックアップからリストアし、そこからデータを抽出することができます。その場合、ユーザがアクセスしている実稼働データベースに影響を及ぼすことはありません。

- 1つのストレージグループ、または同じストレージグループのデータベース (パブリック フォルダ データベース以外) がリストアに選択された場合、デフォルトのリストア デスティネーションは、[回復用ストレージグループにリストアする] (または [回復用データベースにリストアする]) です。
- 複数のストレージグループ、または複数のストレージグループのデータベースがリストアに選択された場合、Exchange は元の場所にリストアするか、または [ダンプファイルのみ] オプションでリストアする必要があります。デフォルトのリストア デスティネーションは [元の場所にリストアする] です。

Exchange 2007 データベースを回復用ストレージグループにリストアするには、回復用ストレージグループ、および同じ名前のメールボックス データベースを作成しておく必要があります。

たとえば、第 1 ストレージグループから MailboxDatabase1 を回復用ストレージグループにリストアする場合、回復用ストレージグループを作成し、データベース「MailboxDatabase1」をその回復用ストレージグループに追加する必要があります。

注: このオプションは Microsoft Exchange Server 2003 では適用されません。

リストア前にデータベースのマウントを解除し、リストア後にデータベースをマウントする

通常、Microsoft Exchange は、リストアの前にいくつかのチェックを実行して以下を確認します。

- リストアされるデータベースが「マウント解除済み」ステータスにある。
- データベースが予期せずリストアされないことがない。

Microsoft Exchange 実稼働データベースが予期せずリストアされるのを防ぐため、リストア処理中にデータベースへの上書きを許可するためのスイッチが追加されています。このスイッチが設定されていないと、Microsoft Exchange ではデータベースのリストアを拒否します。

CA ARCserve D2D では、これらの 2 つの動作は、[リストア前にデータベースのマウントを解除し、リストア後にデータベースをマウントする] オプションによって制御されます。このオプションを使用することで、CA ARCserve D2D では、手動操作なしでリストアプロセスを自動的に起動できます（データベースを手動でマウント解除/マウントするよう指定することもできます）。

- オンに設定した場合、回復処理によってリストアの実行前に自動的に Exchange データベースがマウント解除され、リストアが完了した後マウントされます。また、このオプションをオンにすると、リストア中の Exchange データベースへの上書きが可能になります。
- オフに設定した場合、回復処理で Exchange データベースを回復前に自動的にマウント解除することはなく、回復後にマウントすることはありません。

その場合、Exchange 管理者は手動で一部の操作を実行する必要があります。たとえば、Exchange データベースのマウント解除、データベース上での「上書きを許可」フラグの設定、Exchange データベースのマウントなどです。（回復手順は、データベースのマウント中に Exchange によって実行されます。）

また、このオプションをオフにすると、リストア中の Exchange データベースへの上書きはできなくなります。

回復用ストレージ データベースにリストアする(Exchange 2010)

回復用データベースにデータベースをリストアします。回復用データベースとは、回復目的に使用できるデータベースです。

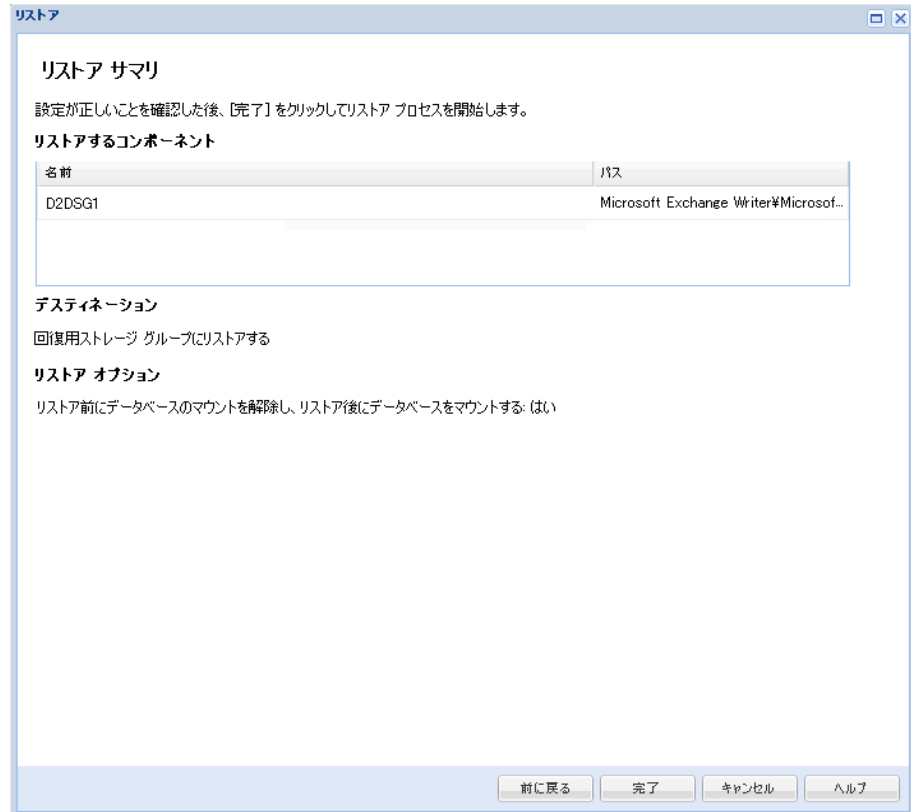
Microsoft Exchange メールボックス データベースを、バックアップから回復用データベースにリストアし、そこからデータを抽出することができます。その場合、ユーザがアクセスしている実稼働データベースに影響を及ぼすことはありません。

Exchange 2010 データベースを回復用データベースにリストアするには、まず回復用データベースを作成する必要があります。

注: このオプションは Microsoft Exchange Server 2003 および 2007 には適用されません。

6. [次へ] をクリックします。

[リストア サマリ] ダイアログ ボックスが表示されます。



7. 表示された情報に目を通し、リストア オプションおよび設定がすべて正しいことを確認します。
- サマリ情報が正しくない場合は、[前に戻る] をクリックし、該当するダイアログ ボックスに戻って、正しくない設定を変更します。
 - サマリ情報が正しい場合は、[完了] ボタンをクリックし、リストア プロセスを開始します。

アプリケーションのリストア - MS SQL Server

CA ARCserve D2D では、データの保護や回復を行うだけでなく、そのデータを使用する Microsoft SQL Server アプリケーションのバックアップや実行をサポートします。Microsoft SQL Server を回復するには、「復旧ポイントによるリストア」方式を使用する必要があります。



ビデオ

CA サポート :

MS SQL Server アプリケーションをリストアする方法

http://www.arcservedocs.com/arcserved2d/r16/redirect.php?item=video_restore_application_sql_support

YouTube :

MS SQL Server アプリケーションをリストアする方法

http://www.arcservedocs.com/arcserved2d/r16/redirect.php?item=video_restore_application_sql_youtube

Microsoft SQL Server アプリケーションのリストア

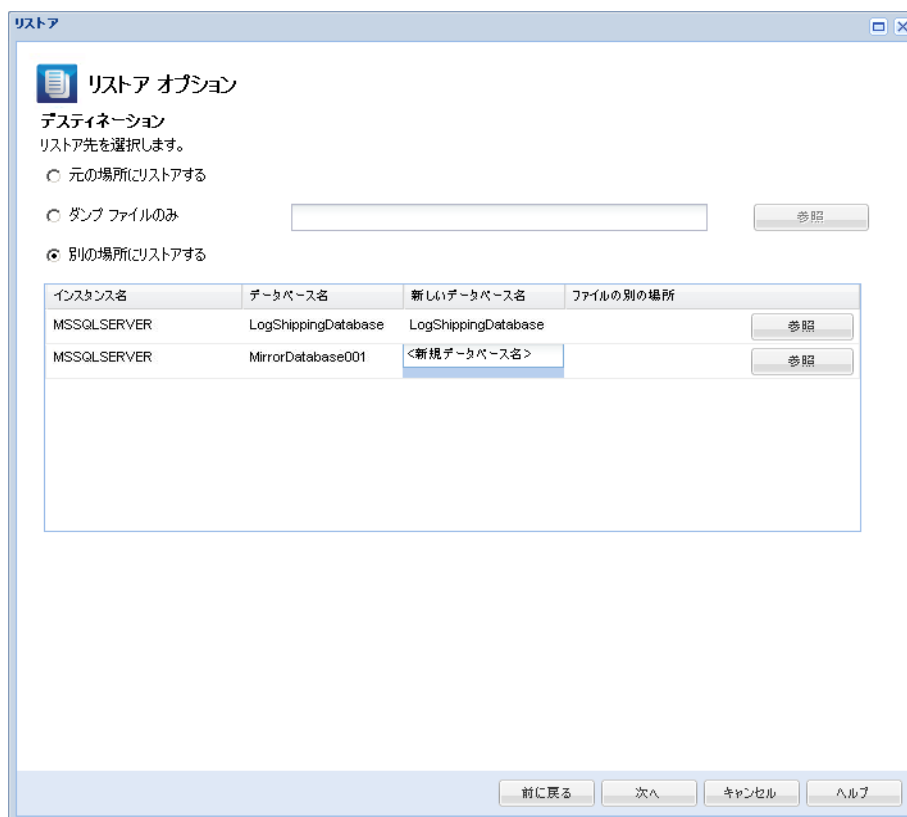
1. CA ARCserve D2D ホーム画面（または CA ARCserve D2D モニタ）から、
[リストア] を選択します。
リストア方式を選択するダイアログ ボックスが表示されます。
2. [復旧ポイントの参照] オプションをクリックします。
[復旧ポイントの参照] ダイアログ ボックスが表示されます。

3. 復旧ポイント（日付と時間）を選択した後、リストアする Microsoft SQL Server データベースを選択します。

対応するボックスが緑色に塗りつぶされます。これは、データベースがリストア対象として選択されたことを示しています。リストア対象として、1つまたは複数のデータベースを選択できます。



4. [次へ] をクリックします。
[リストア オプション] ダイアログ ボックスが表示されます。



5. リストア先を選択します。

利用可能なオプションは、[元の場所に戻す]、[ダンプ ファイルのみ]、[別の場所に戻す] です。

注: AlwaysOn Availability Group (AAG) の一部である Microsoft SQL Server 2012 データベースをリストアする際に、認識しておくべきいくつかの考慮事項があります。詳細については、「Microsoft SQL Server 2012 AAG のリストアに関する考慮事項」を参照してください。

元の場所に戻す

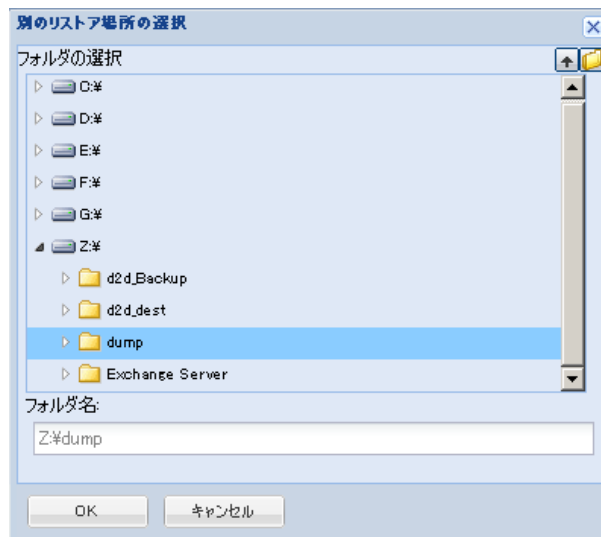
バックアップ イメージがキャプチャされた元の場所にリストアします。

ダンプファイルのみ

ダンプファイルのみをリストアします。

ダンプファイルは、アプリケーションがクラッシュした場合に作成されます。このファイルには、問題の原因をトラブルシューティングのために使用できる追加情報（タイムスタンプ付き）が含まれます。

このオプションを選択すると、ダンプファイルのリストア先となるフォルダを指定するか、参照して選択できます。



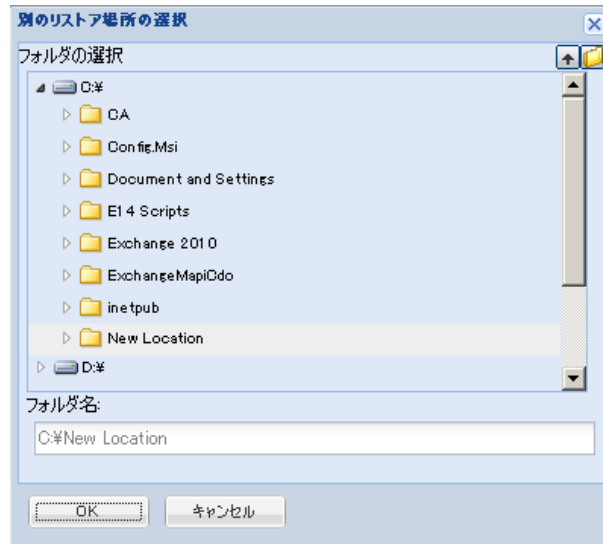
別の場所にリストアする

元の場所以外の別の場所にリストアします。

インスタンス名	データベース名	新しいデータベース名	ファイルの別の場所
MSSQLSERVER	LogShippingDatabase	LogShippingDatabase	<input type="button" value="参照"/>
MSSQLSERVER	MirrorDatabase001	<新規データベース名>	C:\NewDBLocation <input type="button" value="参照"/>

バックアップはネットワーク上の場所にコピーできるので、複数のSQLサーバインスタンスでバックアップを使用できます。複数のデータベースのリストアは、インスタンスレベルで（同時に）実行できます。このリストからデータベースインスタンスを選択し、新しいデータベース名およびデータベースのリストア先となる別の場所を指定できます。また、データベースのリストア先となる別の場所を参照することもできます。

Microsoft SQL Server アプリケーションを別の場所にリストアする場合、いくつかの考慮事項に注意する必要があります。詳細については、「[MS SQL Server を別の場所にリストアする際の考慮事項 \(P. 272\)](#)」を参照してください。



6. [次へ] をクリックします。
[リストア サマリ] ダイアログ ボックスが表示されます。
7. 表示された情報に目を通し、リストア オプションおよび設定がすべて正しいことを確認します。
 - サマリ情報が正しくない場合は、[前に戻る] をクリックし、該当するダイアログ ボックスに戻って、正しくない設定を変更します。
 - サマリ情報が正しい場合は、[完了] ボタンをクリックし、リストア プロセスを開始します。

MS SQL Server を別の場所にリストアする際の考慮事項

Microsoft SQL Server アプリケーションを別の場所にリストアすることを指定した場合は、リストア先として同じマシンの別の場所、または別のマシンの別の場所のいずれかを選択できます。

CA ARCserve D2D で Microsoft SQL Server アプリケーションを別の場所にリストアする前に、以下のことを考慮する必要があります。

別の場所が同じマシンにある場合

このオプションでは、データベースを新しい場所に（同じ名前でも）リストアするか、または新しい名前でも（同じ場所に）リストアできます。

■ 同じ名前 - 新しい場所

たとえば、現在の SQL Server にデータベース A (C:¥DB_A) がインストールされ、バックアップされているとします。この場合、このオプションを選択して別のファイルの場所を指定して、データベース A を別の場所 (D:¥Alternate_A など) にリストアできます。

データベースがリストアされた後は、新しい場所「D:¥Alternate_A」にあるデータベース ファイルが使用されます。

別の場所へのリストア中は、[インスタンス名] セクションは利用できません。インスタンス名は常に同じである必要があります。そのため、同じ MS SQL Server 上に存在する別のインスタンスへはデータベースをリストアできません。

■ 同じ場所 - 新しい名前

たとえば、現在の SQL Server に 2 つのデータベース (データベース A およびデータベース B) がインストールされており、その両方がバックアップされているとします。この場合、このオプションを選択して新しいデータベース名を指定して、データベース A をデータベース A_New として同じ場所にリストアできます。

データベースのリストア後、この場所には 3 つのデータベース (データベース A、データベース B、およびデータベース A_New) が存在します。

別の場所が別のマシンにある場合

- SQL Server のインストールパスは、バックアップが実行されたときに存在したパスと同じである必要があります。

たとえば、SQL Server のバックアップが「C:¥SQLServer」にインストールされている場合、新しい CA ARCserve D2D サーバ上の SQL Server も C:¥SQLServer にインストールされる必要があります。

- バックアップが実行されたときに存在したデータベース用の同じインスタンス名が CA ARCserve D2D サーバにインストールされる必要があります。それ以外の場合、そのインスタンスと関連付けられているデータベースはリストアからスキップされます。

たとえば、SQL Server のバックアップにデータベース A およびデータベースに関連付けられた「Instance_1」と、データベース C に関連付けられた「Instance_2」が含まれているのに対して、CA ARCserve D2D サーバには「Instance_1」しか存在しないとします。この場合、リストアが完了すると、データベース A およびデータベース B はリストアされますが、データベース C はリストアされません。

- CA ARCserve D2D サーバの SQL Server バージョンは、バックアップセッション中に使用される SQL Server のバージョンと後方互換性がある必要があります。

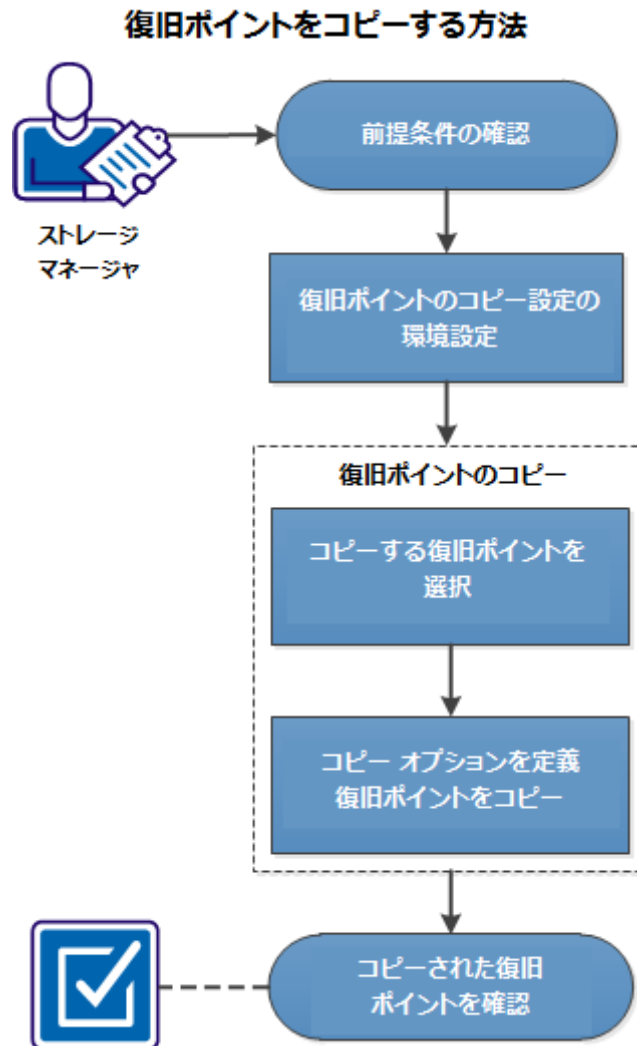
たとえば、SQL Server 2005 マシンを SQL Server 2008 マシンにリストアできますが、SQL Server 2008 マシンを SQL Server 2005 マシンにリストアできません。

- 64 ビット インスタンスのデータベースを 32 ビット インスタンスにリストアする操作はサポートされていません。

復旧ポイントのコピー方法

CA ARCserve D2D によってバックアップが正常に実行されるたびに、バックアップの Point-in-Time スナップショットイメージも作成されます。この復旧ポイントの集合体によって、コピーするバックアップイメージを正確に特定して指定できます。

以下の図は、復旧ポイントをコピーするプロセスを示しています。



復旧ポイントをコピーするには、以下のタスクを実行します。

1. [前提条件の確認](#) (P. 276)
2. [復旧ポイントのコピー設定の指定](#) (P. 276)
3. [復旧ポイントのコピー](#) (P. 283)
 - a. [コピーする復旧ポイントの選択](#) (P. 283)
 - b. [コピー オプションの定義と復旧ポイントのコピー](#) (P. 285)
4. [コピーされた復旧ポイントの確認](#) (P. 288)

チュートリアル ビデオ

この手順には操作説明用のチュートリアル ビデオが含まれています。ビデオの表示媒体として CA サポート または YouTube のいずれかを選択してください。CA サポート と YouTube のビデオは、表示媒体が異なるのみで、バージョンは同一です。



ビデオ

CA サポート :

復旧ポイントのコピー方法

http://www.arcserve.com/arcserve2d/r16/redirect.php?item=video_copy_recoverypoints_support

YouTube :

復旧ポイントのコピー方法

http://www.arcserve.com/arcserve2d/r16/redirect.php?item=video_copy_recoverypoints_youtube

前提条件の確認

復旧ポイントをコピーする前に以下の前提条件について確認します。

- コピーに利用可能なフルバックアップが 1 つ以上ある。
- 復旧ポイントをコピーするための有効なデスティネーションが必要。

復旧ポイントのコピー設定の指定

CA ARCserve D2D では、復旧ポイントのコピー設定を指定できます。復旧ポイントのコピーする前に、復旧ポイントのコピー設定を指定します。このダイアログ ボックス上のオプションを使用して復旧ポイントのコピースケジュールを設定する方法については、「[復旧ポイントのコピー - シナリオ例 \(P. 280\)](#)」を参照してください。

注: 復旧ポイントのコピー プロセスは、コピー&貼り付けの操作のみで、切り取り&貼り付け操作はありません。そのため、スケジュールされた復旧ポイントのコピージョブが実行された場合は常に、CA ARCserve D2D では、指定されたコピー先に復旧ポイントの追加のコピーを作成しますが、バックアップ設定で指定されたバックアップ先には元のコピーを保持します。

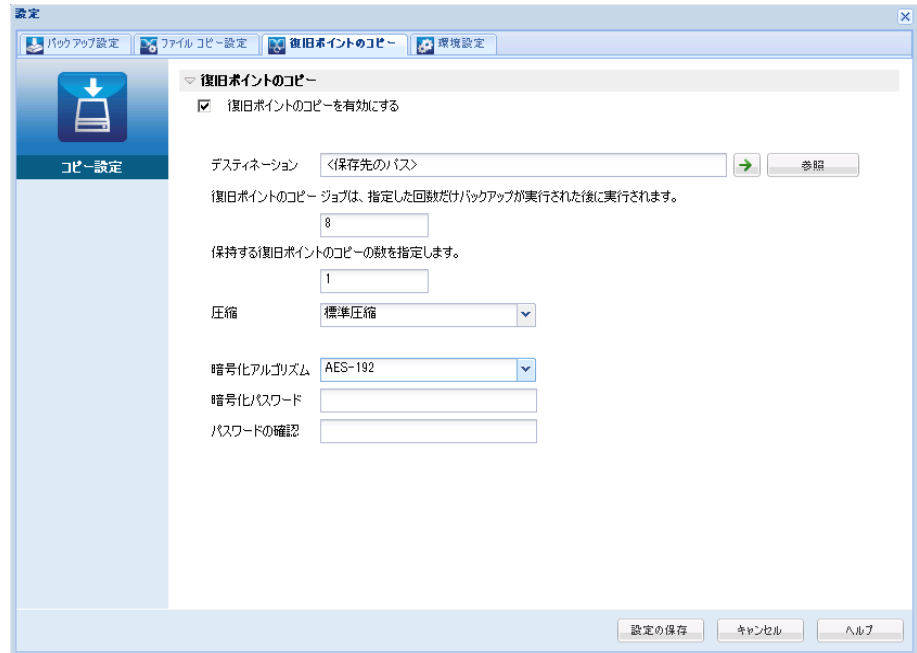
次の手順に従ってください:

1. CA ARCserve D2D ホーム ページで、タスク バーから [設定] を選択します。

[設定] ダイアログ ボックスが表示されます。

2. [復旧ポイントのコピー] タブをクリックします。

[復旧ポイントのコピー] ダイアログ ボックスが表示されます。



3. [復旧ポイントのコピーを有効にする] を選択します。

選択すると、復旧ポイントのコピーが有効になります。

注: このオプションを選択しないと、スケジュールされた復旧ポイントのコピーは実行されません。

4. 以下の復旧ポイントのコピー スケジュール設定を指定します。

デスティネーション

選択した復旧ポイントのコピーの格納場所を指定します。（オプション）緑色の矢印ボタンをクリックすると、指定した場所への接続を検証できます。

注: 指定されたデスティネーションパスの最大長は 158 文字です。

指定された数のバックアップが実行された後、復旧ポイントのコピー ジョブが実行されます。

スケジュールされた復旧ポイントのコピー プロセスが自動的に起動されるタイミングを指定します。このプロセスは、選択したコピー ポリシーおよび指定した成功バックアップ数（フル、増分、検証）に基づいて開始されます。

この設定を使用して、復旧ポイントのコピー プロセスが 1 日にトリガされる回数を制御することができます。たとえば、15 分ごとにバックアップ ジョブを実行し、4 バックアップごとにコピー ジョブを実行する場合、復旧ポイントのコピー ジョブは毎日 24 回（1 時間ごと）実行されます。

デフォルト：8

最小：1

最大：1344

重要：バックアップおよびコピー ジョブが定期的に行われるようスケジュールされていて、バックアップ ジョブの実行がスケジュールされている時間がきてもコピー ジョブが実行中（アクティブな状態）である場合、バックアップ ジョブは失敗します（次のバックアップ ジョブはスケジュールどおりに実行され、別のコピー ジョブと競合しなければ正常に完了します）。コピー操作にはフルバックアップの実行とほぼ同じ時間がかかるため、復旧ポイント コピー ジョブのスケジュールはそれほど頻繁に設定しないことをお勧めします。

保存する復旧ポイントの数の指定

指定したコピー デスティネーションに保持および保存される復旧ポイントの数を指定します。この数を超過すると、最も古い復旧ポイントを破棄します。

注：ターゲット デスティネーションで十分な空き容量がない場合は、保存する復旧ポイント数を減らします。

デフォルト：1

最大：1344

5. 圧縮レベルを選択します。

圧縮は、通常、ディスク容量の使用率を減らすために実行されますが、CPU 使用率が増加するため、バックアップ速度が低下するという影響があります。

使用可能なオプションは、以下のとおりです。

- **圧縮なし** - 圧縮は実行されません。ファイルは純粹な VHD です。このオプションを使用すると、CPU 使用率は最も低くなります（最も高速で動作します）。ただし、バックアップイメージのディスク容量の使用率は最大になります。
- **圧縮なし - VHD** - 圧縮は実行されません。ファイルは .vhd 形式に直接変換されます。手動操作は必要ありません。このオプションを使用すると、CPU 使用率は最も低くなります（最も高速で動作します）。ただし、バックアップイメージのディスク容量の使用率は最大になります。
- **標準圧縮** - 標準圧縮が実行されます。このオプションを使用すると、CPU 使用率とディスク容量使用率のバランスを適度に調節します。これはデフォルトの設定です。
- **最大圧縮** - 最大圧縮が実行されます。このオプションを使用すると、CPU 使用率が最も高くなります（最も低速で動作します）。ただし、ディスク容量の使用率は、最小になります。

注: バックアップイメージに圧縮可能でないデータ (JPG イメージ、ZIP ファイルなど) が含まれている場合、それらのデータを処理するために、追加のストレージスペースを割り当てることができます。そのため、圧縮オプションを選択して、バックアップに圧縮可能でないデータがある場合、実際にはディスク容量の使用率が增大する場合があります。

6. コピーする復旧ポイントを暗号化するには、以下の情報を入力します。

暗号化アルゴリズム

復旧ポイントのコピーに使用される暗号化アルゴリズムの種類を指定します。

利用可能なオプションは、暗号化なし、AES-128、AES-192、および AES-256 です

暗号化パスワード

デスティネーションセッションの暗号化に使用される暗号化パスワードを指定および確認します。

7. [設定の保存] をクリックします。

復旧ポイント コピー設定が保存されます。

復旧ポイントのコピー設定が正しく指定されました。

復旧ポイントのコピー - シナリオ例

以下のシナリオ例は、各種オプションの設定によって復旧ポイントのコピーのスケジュールにどのような影響があるかについて説明しています。

この例では、CA ARCserve D2D バックアップ スケジュールが以下のように設定されていると仮定します。

- フルバックアップ - 7 日ごと
- 増分バックアップ - 1 時間ごと
- 検証バックアップ - 3 日ごと

および以下の状況であるとします。

- 最初のバックアップは、1 日目の午後 5 時に実行されます（デフォルトでは、最初のバックアップは常にフルバックアップになります）
- 最初の増分バックアップは、1 日目の午後 6 時に実行されます（その後は 1 時間ごとに実行）
- 復旧ポイントの保存数は 31（デフォルト）に設定されています
- コピー先としてデスティネーション "D" が設定されています

シナリオ #1

このシナリオでは、復旧ポイントのコピーが以下のように設定されています。

- コピー実行までのバックアップ数：4
- 保持する復旧ポイント数：1

結果

- 午後8時(4回目のバックアップ後)に、スケジュールされたコピージョブが実行されます。4つの復旧ポイントはすべて1つの復旧ポイントに統合され、デスティネーションDに保存されます。
- 夜中の12時(8回目のバックアップ後)に、次にスケジュールされたコピージョブが実行されます。8つの復旧ポイントはすべて1つの復旧ポイントに統合され、デスティネーションDに保存されます。

デスティネーションでは1つの復旧ポイントのみを保持するように設定されているため、前の復旧ポイントはデスティネーションDから削除されます。

シナリオ #2

このシナリオでは、復旧ポイントのコピーが以下のように設定されています。

- コピー実行までのバックアップ数：4
- 保持する復旧ポイント数：4

結果

- 午後8時(4回目のバックアップ後)に、スケジュールされたコピージョブが実行されます。4つの復旧ポイントはすべて1つの復旧ポイント(復旧ポイント#1)に統合され、デスティネーションDに保存されます。
- 午前0時(8回目のバックアップ後)に、次にスケジュールされたコピージョブが実行されます。復旧ポイント#2が作成され、デスティネーションDに保存されます。
- 2日目の午前4時(12回目のバックアップ後)に、次にスケジュールされたコピージョブが実行されます。復旧ポイント#3が作成され、デスティネーションDに保存されます。

- 2日目の午前8時（16回目のバックアップ後）に、次にスケジュールされたコピージョブが実行されます。復旧ポイント #4 が作成され、デスティネーション D に保存されます。
- 2日目の午後12時（20回目のバックアップ後）に、次にスケジュールされたコピージョブが実行されます。デスティネーションでは4つの復旧ポイントまで保持するよう設定されているため、新しい復旧ポイントが作成されたら、最初の復旧ポイントはデスティネーション D から削除されます。

シナリオ #3

このシナリオでは、復旧ポイントのコピーが以下のように設定されています。

- コピー実行までのバックアップ数：1
- 保持する復旧ポイント数：4

結果

- 午後5時（最初のバックアップ後）に、スケジュールされたコピージョブが実行されます。1つの復旧ポイント（復旧ポイント #1）が作成され、デスティネーション D に保存されます。
- 午後6時（2回目のバックアップ後）に、次にスケジュールされたコピージョブが実行されます。復旧ポイント #2 が作成され、デスティネーション D に保存されます。
- 午後7時（3回目のバックアップ後）に、次にスケジュールされたコピージョブが実行されます。復旧ポイント #3 が作成され、デスティネーション D に保存されます。
- 午後8時（4回目のバックアップ後）に、次にスケジュールされたコピージョブが実行されます。復旧ポイント #4 が作成され、デスティネーション D に保存されます。
- 午後9時（5回目のバックアップ後）に、次にスケジュールされたコピージョブが実行されます。デスティネーションで4つの復旧ポイントまで保持するよう設定されているため、新しい復旧ポイントが作成されたら、最初の復旧ポイント（午後5時のバックアップ後に作成されたもの）はデスティネーション D から削除されます。

復旧ポイントのコピー

コピーする復旧ポイントを選択すると、それ以前のすべてのバックアップブロック（フルおよび増分）は、完全で最新のバックアップイメージを再作成するために、すべて統合およびキャプチャされます。

以下のタスクを実行して、バックアップを保護できます。

- 障害発生時に、復旧ポイント情報をコピー/エクスポートして、それをオフサイトに安全に格納します。
- 復旧ポイントを複数の場所へ保存します。
- すべての復旧ポイントを保持するためにバックアップを統合します。

復旧ポイントのコピーには、以下のプロセスが含まれます。

1. [コピーする復旧ポイントの選択](#) (P. 283)。
2. [コピーオプションの定義と復旧ポイントのコピー](#) (P. 285)。

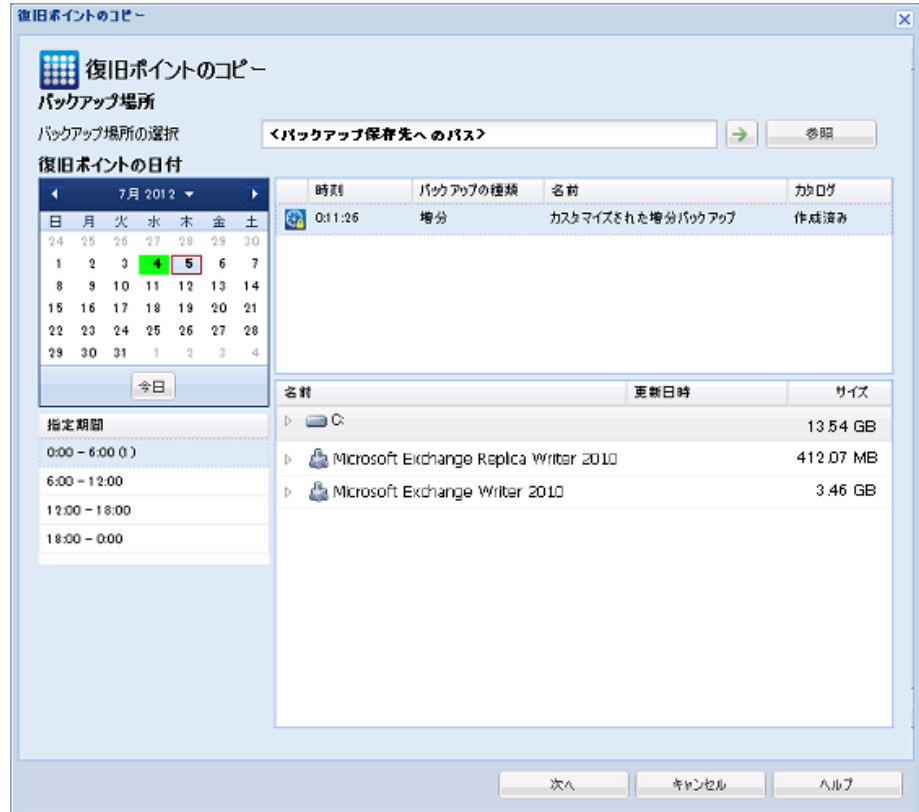
コピーする復旧ポイントの選択

CA ARCserve D2D は利用可能な復旧ポイントのリストを提供し、ユーザはコピーを作成する復旧ポイントを選択できます。復旧ポイントをコピーするためのデスティネーション、および復旧ポイントの日付と時間の範囲を指定できます。

次の手順に従ってください:

1. CA ARCserve D2D ホーム画面で、[復旧ポイントのコピー] を選択します。

[復旧ポイントのコピー] ダイアログ ボックスが表示されます。



2. バックアップ イメージが保存されている場所を指定または参照し、適切なバックアップ ソースを選択します。

緑色の矢印ボタンをクリックすると、指定した場所への接続を検証できます。必要に応じて、その場所にアクセスするための [ユーザ名] および [パスワード] 認証情報を入力します。

カレンダー ビューが表示されます。

注: 指定された場所用の復旧ポイントが含まれる日付はすべて、緑で強調表示されます。

3. カレンダーで、コピーするバックアップイメージの日付を選択します。
その日付に対応する復旧ポイントが、バックアップの時刻、実行されたバックアップの種類、およびバックアップの名前と共に表示されます。

注: ロック記号の付いた時計のアイコンは、復旧ポイントに暗号化された情報が含まれており、リストアするにはパスワードが必要な場合があることを示します。

4. コピーする復旧ポイントを選択します。
選択した復旧ポイントのバックアップ コンテンツ（任意のアプリケーションを含む）が表示されます。

5. [次へ] をクリックします。
[コピー オプション] ダイアログ ボックスが表示されます。

コピーする復旧ポイントが指定されます。

コピー オプションの定義と復旧ポイントのコピー

コピーする復旧ポイントを指定したら、選択した復旧ポイントのそれ以前のフルバックアップと増分バックアップとが組み合わせられた、コピー作成用のコピー オプションを定義します。

次の手順に従ってください:

1. [コピー オプション] ダイアログ ボックスから、以下のコピー オプションを指定します。

パスワード

バックアップの暗号化パスワードを指定します。

注: このダイアログ ボックスには 2 つのパスワード フィールドが含まれます。上のフィールドは、ソース セッションを復号化するパスワード、下のフィールドはデスティネーション セッションを暗号化するために使用します。

コピー用に選択する復旧ポイントが以前暗号化されている場合は、パスワードを指定します。

- コピーされる復旧ポイントが、復旧ポイントのコピー ジョブを実行しているのと同じコンピュータのバックアップセッションである場合、暗号化パスワードが記憶されており、このフィールドに自動的に入力されます。
- コピーされる復旧ポイントが別のコンピュータのバックアップセッションである場合、暗号化パスワードを入力します。

デスティネーション

選択した復旧ポイントの格納場所を指定(または参照)します。(オプション) 緑色の矢印ボタンをクリックすると、指定した場所への接続を検証できます。

必要に応じて、[ユーザ名] および [パスワード] を入力します。

2. 圧縮レベルを選択します。

注: 指定されたバックアップ圧縮レベルとコピー圧縮レベルに関係はありません。たとえば、バックアップ先で圧縮レベルを [標準] に設定できます。しかし、コピージョブのサブミット時に、圧縮を [圧縮なし] または [最大圧縮] に変更することができます。

圧縮は、通常、ディスク容量の使用率を減らすために実行されますが、CPU 使用率が増加するため、バックアップ速度が低下するという影響があります。

使用可能なオプションは、以下のとおりです。

- **圧縮なし** - 圧縮は実行されません。ファイルは純粋な VHD です。このオプションを使用すると、CPU 使用率は最も低くなります (最も高速で動作します)。ただし、バックアップイメージのディスク容量の使用率は最大になります。
- **圧縮なし - VHD** - 圧縮は実行されません。ファイルは .vhd 形式に直接変換されます。手動操作は必要ありません。このオプションを使用すると、CPU 使用率は最も低くなります (最も高速で動作します)。ただし、バックアップイメージのディスク容量の使用率は最大になります。
- **標準圧縮** - 標準圧縮が実行されます。このオプションを使用すると、CPU 使用率とディスク容量使用率のバランスを適度に調節します。これはデフォルトの設定です。
- **最大圧縮** - 最大圧縮が実行されます。このオプションを使用すると、CPU 使用率が最も高くなります (最も低速で動作します)。ただし、ディスク容量の使用率は、最小になります。

注: バックアップイメージに圧縮可能でないデータ (JPG イメージ、ZIP ファイルなど) が含まれている場合、それらのデータを処理するために、追加のストレージスペースを割り当てることができます。そのため、圧縮オプションを選択していて、バックアップに圧縮可能でないデータがある場合、実際にはディスク容量の使用率が增大する場合があります。

注: 圧縮レベルを「圧縮なし」から「標準圧縮」または「最大圧縮」にした場合、あるいは、「標準圧縮」または「最大圧縮」から「圧縮なし」に変更した場合、圧縮レベルの変更後に実行される最初のバックアップは自動的に「フルバックアップ」となります。フルバックアップを実行した後、それ以降のすべてのバックアップ（フル、増分、検証）はスケジュールどおりに実行されます。

3. コピーする復旧ポイントを暗号化するには、以下の情報を入力します。

暗号化アルゴリズム

復旧ポイントのコピーに使用される暗号化アルゴリズムの種類を指定します。

利用可能なオプションは、暗号化なし、AES-128、AES-192、および AES-256 です

暗号化パスワード

デスティネーションセッションの暗号化に使用される暗号化パスワードを指定および確認します。

注: 暗号化を有効化する際、新しいパスワードを指定します。このパスワードは、コピーした復旧ポイントをリストアする際に必要となります。

4. [コピーの作成] をクリックします。

ステータスの通知画面が表示され、選択した種類の復旧ポイントのコピー処理がすぐに開始されます。

注: CA ARCserve D2D では、同時に実行できる復旧ポイントのコピージョブは1つのみです。別のスケジュールされたコピージョブの実行中に、手動で復旧ポイントのコピージョブを開始しようとすると、アラートメッセージが表示されます。メッセージは、別のジョブが実行中であるため、後で実行するよう通知します。

復旧ポイントが、バックアップソースからコピーターゲットデスティネーションにコピーされます。

コピーされた復旧ポイントの確認

復旧ポイントをコピーしたら、コピーした復旧ポイントが指定したデスティネーションで利用可能であることを確認します。

次の手順に従ってください:

1. 指定した CA ARCserve D2D のデスティネーションに移動します。
フォルダのリストが表示されます。
2. ホスト名のフォルダを開き、以下の下位フォルダに移動します。
ホスト名¥VStore
3. VStore フォルダを開き、以下のセッション フォルダに移動します。
VStore¥S0000000001
4. 指定された場所で、D2D の拡張子を持つファイルをすべて見つけ、コピーした復旧ポイントを確認します。
たとえば、ユーザのコンピュータ名が「Department_A」で、復旧ポイント（バックアップ）を「E:¥copied_vhd¥」にコピーした場合は、以下の場所に移動します。
E:¥copied_vhd¥Department_A¥VStore¥S0000000001

復旧ポイントのコピーが正常に確認されました。

第 7 章: 用語集

HOTADD 転送モード

HOTADD 転送モードは、SCSI ディスクで設定された仮想マシンをバックアップするためのデータ転送方式です。詳細については、VMware Web サイトの [Virtual Disk API Programming Guide](#) を参照してください。

NBDSSL 転送モード

NBDSSL (Network Block Device Secure Sockets Layer) 転送モードは、通信に NFC (Network File Copy) プロトコルを使用します。NBDSSL は TCP/IP 通信ネットワークを使用して、暗号化されたデータを転送します。

NBD 転送モード

NBD (ネットワーク ブロック デバイス) 転送モード (別名、LAN 転送モード) は、通信に NFC (ネットワーク ファイル コピー) プロトコルを使用します。各種の VDDK および VCB 操作は、NBD を使用するとき、各 ESX/ESXi Server ホストでアクセスする仮想ディスクごとに 1 つの接続を使用します。

SAN 転送モード

SAN (Storage Area Network) 転送モードは、ファイバチャネル通信を使用して、SAN に接続されたプロキシシステムからストレージデバイスにバックアップデータを転送できます。

SRM

SRM (Storage Resource Management) は、環境の効果的な管理のため、情報を収集する機能です。たとえば、アプリケーションデータ、ハードウェアおよびソフトウェアのデータ、パフォーマンス キー インジケータなどが収集されます。

オート ディスカバリ

オート ディスカバリは、ノードが検出され、一元管理のために CA ARCserve Central Applications に追加されるプロセスです。

カタログ ファイル

カタログ ファイルは、CA ARCserve D2D データベースに含まれているバックアップデータに関する情報のディレクトリです。CA ARCserve D2D カタログ ファイルの詳細については、「[CA ARCserve D2D ユーザガイド](#)」を参照してください。

同期

同期は、異なるデータベース内のデータを最新の状態に保つためのプロセスです。これにより、セントラルデータベースと登録済みのブランチ、ノード、またはサイトとの整合性が保たれます。

ノード

ノードは、CA ARCserve Central Applications によって管理される物理マシンまたは仮想マシンです。

ノードグループ

ノードグループは、CA ARCserve Central Applications によって管理されるすべてのノードを整理する方法で、たとえば目的、OS、インストールされたアプリケーション別などでグループ化します。

バックアッププロキシ

バックアッププロキシは、CA ARCserve D2D が実行されるホスト コンピュータです。プロキシは CA ARCserve Central Host-Based VM Backup に設定されたバックアップを実行します。

復旧ポイント

復旧ポイントは、親ブロックと最も古い子ブロックで構成されるバックアップイメージです。子バックアップは親バックアップとマージされ、新しい復旧ポイントイメージが作成されます。これにより指定された値が常に保持されます。

プレフライトチェック

プレフライトチェック (PFC) は、ノードに対してバイタルチェックを実行して、バックアップジョブの失敗につながる可能性のある条件を検出できるユーティリティです。[ノード] 画面で [PFC ステータス] 列内のアイコンをクリックして、ノードに対する PFC の結果を表示できます。

ポリシー

ポリシーは、CA ARCserve Central Applications 内のノードを保護するための仕様のセットです。

索引

C

- CA ARCserve Central Applications サーバのホスト名変更後のノードおよびポリシーの更新 - 59
- CA ARCserve Central Applications にアクセスすると、文字化けがブラウザ ウィンドウ内に表示される - 141
- CA ARCserve Central Applications マニュアル 選択メニュー - 18
- CA ARCserve Central Host-Based VM Backup からの VHD ファイルの作成 - 81
- CA ARCserve Central Host-Based VM Backup からのノードのディスクバリ - 52
- CA ARCserve Central Host-Based VM Backup がリモートノード上の CA ARCserve D2D Web サービスと通信できない - 157
- CA ARCserve Central Host-Based VM Backup と CA ARCserve Central Applications との統合 - 100
- CA ARCserve Central Host-Based VM Backup について - 16
- CA ARCserve Central Host-Based VM Backup のアンインストール - 30
- CA ARCserve Central Host-Based VM Backup のインストール - 24
- CA ARCserve Central Host-Based VM Backup のインストールおよび設定 - 19
- CA ARCserve Central Host-Based VM Backup のサイレントアンインストール - 31
- CA ARCserve Central Host-Based VM Backup のサイレントインストール - 26
- CA ARCserve Central Host-Based VM Backup のトラブルシューティング - 131
- CA ARCserve Central Host-Based VM Backup の概要 - 15
- CA ARCserve Central Host-Based VM Backup の仕組み - 17
- CA ARCserve Central Host-Based VM Backup の使用 - 45
- CA ARCserve Central Host-Based VM Backup ホーム画面の使用法 - 47
- CA ARCserve Central Host-Based VM Backup ログの表示 - 96
- CA ARCserve Central Host-Based VM Backup をアンインストールする方法 - 29
- CA ARCserve Central Host-Based VM Backup をインストールする方法 - 19
- CA ARCserve Central Host-Based VM Backup 用のノードグループタスクを管理する方法 - 62
- CA ARCserve Central Host-Based VM Backup 用のノードタスクを管理する方法 - 49
- CA ARCserve Central Host-Based VM Backup 用ポリシーの管理方法 - 86
- CA ARCserve Central Protection Manager サーバの設定 - 34
- CA ARCserve D2D Web サービスが CA ARCserve D2D ノード上で失敗する - 154
- CA ARCserve D2D Web サービスの実行が遅い - 158
- CA ARCserve D2D のインストール - 211
- CA ARCserve D2D ノードへのログイン - 48
- CA ARCserve D2D ノードへのログイン時に Web ページが正しくロードされない - 138
- CA ARCserve D2D ノードを保護するように CA ARCserve Central Host-Based VM Backup を設定する方法 - 33
- CA ARCserve D2D の操作手順 - 211
- CA ARCserve D2D バックアッププロキシの保護 - 204
- CA Technologies 製品リファレンス - 3
- CA への連絡先 - 3

E

- ESX Server にアクセスできないために仮想マシンのバックアップが失敗する - 170
- ESXi ライセンスのためにバックアップが失敗する - 161
- Exchange Server - 120
- Exchange Server のデータのリストア - 120

H

- Host-Based VM Backup モニタリング タスク - 84
- HOTADD 転送モード - 291
- hotadd 転送モードを使用したバックアップおよび復旧操作でディスクがマウントできない - 149
- HOTADD または SAN 転送モードを使用してデータを復旧すると復旧に失敗する - 149

I

- Internet Explorer 8、9、Chrome で追加した新しいタブのリンクが正常に起動しない - 171
- Internet Explorer 8 および 9 で、新しいタブの追加リンク、RSS フィード、およびソーシャル ネットワーキング フィードバックが正常に起動しない - 175

M

- MAC アドレスの変更が VM 復旧後に保持されない - 153
- MS SQL Server を別の場所にリストアする際の考慮事項 - 272

N

- NBDSSL 転送モード - 291
- NBD 転送モード - 291

R

- raw デバイス マッピング保護のための考慮事項 - 101

S

- SAN 転送モード - 291
- SQL Server - 126
- SQL Server のデータのリストア - 126
- SRM - 291

V

- vCenter/ESX Server の詳細を更新します。 - 67
- v Center/ESX からの仮想マシンのインポート - 56
- VMDK ファイルを開けない - 167
- VMVixMgr ログ ファイルに保持されるメッセージ容量を増加させる - 203
- VM にスナップショットがあるためバックアップが失敗する - 162
- VM の復旧が不明なエラーで失敗する - 147

あ

- 圧縮 - 215
- アプリケーションのリストア - 259
- アプリケーションのリストア - MS Exchange Server - 259
- アプリケーションのリストア - MS SQL Server - 268
- アプリケーションへのログイン時に証明書エラーが表示される - 144
- アプリケーション レベル バックアップの実行 - 82
- アプリケーション レベル リストア - 119
- 暗号化 - 215
- 一般的な環境設定の指定 - 244
- 今すぐバックアップを実行 - 74
- インストール処理のオペレーティング システムに対する影響 - 205
- インストール タスクの前提条件 - 21
- 埋め込みマニフェストを含まないバイナリ ファイル - 208
- オート ディスカバリ - 291
- オペレーティング システムが見つからないエラー - 152

か

- 概要 - 15
- 仮想マシン環境のバックアップ方法 - 68
- 仮想マシン全体の復旧 - 115
- 仮想マシンの復旧で指定とは異なる転送モードが使用される - 176
- 仮想マシンのベア メタル復旧の実行 - 179
- 仮想マシンのリストアおよび復旧 - 105
- カタログ ファイル - 291
- 環境設定の指定 - 243
- 管理者アカウントの変更 - 42
- グループ - 63, 65
 - グループ、ノードグループの削除 - 65
 - グループ、ノードグループの追加 - 63
- 更新スケジュールの設定 - 38
- 更新の環境設定の指定 - 254
- コピー オプションの定義と復旧ポイントのコピー - 285
- コピーされた復旧ポイントの確認 - 288
- コピーする復旧ポイントの選択 - 283

さ

- サーバの通信プロトコルの変更 - 102
- 実稼働環境の設定方法 - 46
- 自動更新スケジュール - 254
- 使用済みブロック データのみを含むフル ディスク バックアップの実行 - 83
- 将来のバックアップ スペース要件の推定 - 230
- ジョブ ステータス情報の参照 - 83
- 設定
 - 設定、拡張バックアップ設定 - 241
 - 設定、環境設定 - 243
 - 設定、自動更新環境設定 - 254
 - 設定、電子メール環境設定 - 246
 - 設定、バックアップ設定 - 236
 - 設定、バックアップ設定の管理 - 214
 - 設定、保護設定 - 215
- 前提条件の確認 - 276
- 増分バックアップ ジョブが検証バックアップ ジョブとして処理される - 165

- ソーシャル ネットワーキングの環境設定 - 41
- 空の Web ページが表示される、または、JavaScript エラーが発生する - 136

た

- ディスカバリ スケジュールの設定 - 36
- ディスカバリの結果からのノードの追加 - 54
- 電子メールおよびアラート設定の指定 - 36
- 電子メール環境設定の指定 - 246
- 電子メール設定の指定 - 250
- 同期 - 292
- 同時バックアップ数の制限の定義 - 202
- 特定ノードのアクティビティ ログ情報の表示 - 98

な

- ナビゲーション バーへのリンクの追加 - 100
- 日本語キーボードを使用して [フィルタ] フィールドのワイルドカードとしてアスタリスクまたはアンダースコアを指定できない - 176
- ノード - 292
 - ノード、ノードの削除 - 59
 - ノードグループ - 292
 - ノードグループの削除 - 65
 - ノードグループの追加 - 63
 - ノードグループの変更 - 66
 - ノード更新時のアクセス拒否エラー発生 - 142
 - ノード上のマージ ジョブの一時停止 - 60
 - ノード上のマージ ジョブの再開 - 61
 - ノードの更新 - 58
 - ノードの削除 - 59
 - ノードの追加 - 53
 - ノードの追加を試行すると、指定されたサーバにアクセスできないというメッセージが表示される - 133
 - ノード名を変更した後にノードがノード画面に表示されない - 168

は

- バックアップ拡張設定の指定 - 236
- バックアップが失敗し、バックアッププロキシシステムのイベントログにイベント 1530 がログ記録される - 163
- バックアップがスナップショット作成エラーで失敗する - 145
- バックアップジョブのプレフライトチェックの実行 - 69
- バックアップスケジュールの指定 - 233
- バックアップ設定の管理 - 214
- バックアップの実行前/後の設定の指定 - 241
- バックアップの転送モードの定義 - 103
- バックアッププロキシ - 17, 292
- バックアップポリシーの作成 - 87
- バックアップポリシーのノードの割り当てと割り当て解除 - 94
- バックアップポリシーの編集またはコピー - 91
- ブートキット - 198
- ブートキットの作成 - 198
- 復旧ポイント - 292
 - 復旧ポイント、設定 - 215
 - 復旧ポイント、リストア - 107
- 復旧ポイントからのリストア - 107
- 復旧ポイントのコピー - 77, 283
- 復旧ポイントのコピー - シナリオ例 - 280
- 復旧ポイントのコピー設定の指定 - 276
- 復旧ポイントのコピー方法 - 274
- 復旧ポイントのマウントによるリストア - 111
- プレフライトチェック - 292
- プレフライトチェック項目のソリューション - 71
- プロキシ設定の環境設定 - 39
- ブロックを識別できないため、バックアップジョブに失敗する - 166
- ベアメタル復旧 - 179
- ページのロード問題のトラブルシューティング方法 - 140

- ベストプラクティスの適用 - 179
- 変更ブロックのトラッキングに失敗する - 160
- 保護設定の指定 - 215
- ホット追加転送モードを指定したのに NBD 転送モードでバックアップが完了する - 164
- ポリシー - 292
- ポリシーを CA ARCserve D2D サーバに保存または割り当てる際に複数の接続エラーが発生する - 169

ま

- マージジョブオプション - 60
- マニフェストで管理者に必要な権限を持つバイナリファイル - 209
- マニュアルの変更点 - 5
- 無効なファイルバージョン情報が含まれるバイナリファイル - 207

ら

- リストア
 - リストア、Exchange Server - 120
 - リストア、SQL Server - 126
 - リストア、仮想マシンの復旧 - 105
 - リストア、ファイル/フォルダ - 112
 - リストア、復旧ポイントから - 107
- リストアするファイル/フォルダの検索を使用したデータのリストア - 112
- リストアの考慮事項 - 118
- リストア方式 - 106