CA ARCserve® Central Host-Based VM Backup

ユーザ ガイド

r16.5

ca technologies

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/）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/

- **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/

- **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/

マニュアルの変更点

本マニュアルでは、CA ARCserve Central Host-Based VM Backup の前回のリリース以降に、以下の点を更新しています。

- 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を反映するために更新されました。
- 「バックアップ ポリシーの作成 (P. 84)」が更新されました。 このトピックには、［バックアップ設定］/［拡張］タブの［デスティネーション上の予約容量］および［カタログ］という 2 つの新しいオプションが追加されました。また、［環境設定］/［電子メール アラート］タブの 2 つの新しいマージ ジョブ アラートが追加され、マージ エラーは削除されました。
- 「バックアップ ポリシーの編集またはコピー (P. 89)」が更新されました。 このトピックには、［バックアップ設定］/［拡張］タブの［デスティネーション上の予約容量］および［カタログ］という 2 つの新しいオプションが追加されました。
- 「CA ARCserve Central Host-Based VM Backup ログの表示 (P. 97)」が更新されました。 このトピックには、［モジュール］ドロップダウン メニューの［複数ノードの更新］および［CA ARCserve D2D マージ ジョブ］という 2 つの新しいオプションが追加されました。
- 「仮想マシン全体の復旧 (P. 115)」が更新されました。 このトピックは、ダイアログ ボックスの最新のデザインを反映するように更新されました。
- 「ノード更新時のアクセス拒否エラー発生 (P. 144)」が更新されました。 このトピックには、ユーザー アカウント制御（UAC）を無効にする 2 つの解決策が追加されました。
- 「ベア メタル復旧の実行 (P. 181)」が更新されました。 このトピックには、BMR を実行するための WinPE ISO を作成する新しいユーティリティ（ベア メタル復旧用のブート キットの作成）が追加されました。ISO ファイルは提供されなくなりました。さらに、このトピックには、UEFI マシン上で取得されたバックアップから BIOS マシンへ、および BIOS マシンから UEFI マシンへの BMR のサポートも追加されました。
- 「ブート キットの作成方法 (P. 201)」が追加されました。 このトピックでは、BMR を実行するための WinPE ISO イメージを作成する新しいユーティリティの新機能を説明します。

注: 「ブートキットの作成」は削除され、このトピックに置き換えられました。

- 「アプリケーションのリストア - MS Exchange Server」が、「MS Exchange アプリケーションのリストア方法」の新しいシナリオ トピックで更新されました。このトピックには、Exchange 2013 のサポートが追加されました。「リストアの前提条件と考慮事項の確認」を参照してください。
- 「仮想マシンを代替の ESX サーバまたは Hyper-V サーバに復旧するときに、CA ARCserve Central Host-Based VM Backup がダイナミック ディスク上のボリュームを認識できない (P. 178)」が追加されました。 このトピックでは、ダイナミック ディスク上のボリュームを取得するための解決策を説明します。
- 「アンチウイルス スキャンからのファイルの除外 (P. 225)」が追加されました。このトピックでは、アンチウイルス スキャンを実行する前に対象から除外するファイル、フォルダおよびプロセスについて説明します。
- ビルトイン認証情報またはドメイン管理者認証情報を指定して、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、以下のトピックが更新されました。
  - インストール タスクの前提条件 (P. 17)
  - プレフライト チェック項目のソリューション (P. 67)
  - ノード更新時のアクセス拒否エラー発生 (P. 144)

目次

第 1 章: CA ARCserve Central Host-Based VM Backup の概要 11

概要 11
CA ARCserve Central Host-Based VM Backup について 12
CA ARCserve Central Host-Based VM Backup の仕組み 13
CA ARCserve Central Applications マニュアル選択メニュー 14

第 2 章: CA ARCserve Central Host-Based VM Backup のインストールおよび設定 15

CA ARCserve Central Host-Based VM Backup をインストールする方法 15
インストール タスクの前提条件 17
CA ARCserve Central Host-Based VM Backup のインストール 20
CA ARCserve Central Host-Based VM Backup のサイレント インストール 22
CA ARCserve Central Host-Based VM Backup をアンインストールする方法 25
CA ARCserve Central Host-Based VM Backup のアンインストール 26
CA ARCserve Central Host-Based VM Backup のサイレント アンインストール 27
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 29
CA ARCserve Central Protection Manager サーバの設定 30
ディスカバリ スケジュールの設定 32
電子メールおよびアラート設定の指定 32
更新スケジュールの設定 34
ソーシャル ネットワーキングの環境設定 37
管理者アカウントの変更 38

第 3 章: CA ARCserve Central Host-Based VM Backup の使用 41

実稼働環境の設定方法 42
CA ARCserve Central Host-Based VM Backup ホーム画面の使用方法 43
CA ARCserve D2D ノードへのログイン 44
CA ARCserve Central Host-Based VM Backup 用のノード タスクを管理する方法 45
CA ARCserve Central Host-Based VM Backup からのノードのディスカバリ 48
ノードの追加 49
ノードの更新 54
ノードの削除 56

マージ ジョブ オプション 56
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 58
ノード グループの追加 59
ノード グループの削除 61
ノード グループの変更 62
仮想マシン環境のバックアップ方法 64
バックアップ ジョブのプレフライト チェックの実行 65
今すぐバックアップを実行 70
アプリケーション レベル バックアップの実行 79
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 80
ジョブ ステータス情報の表示 80
CA ARCserve Central Host-Based VM Backup 用ポリシーの管理方法 83
バックアップ ポリシーの作成 84
バックアップ ポリシーの編集またはコピー 89
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 93
CA ARCserve Central Host-Based VM Backup ログの表示 95
特定ノードのアクティビティ ログ情報の表示 97
CA ARCserve Central Host-Based VM Backup のステータスをレポートに表示 98
ナビゲーション バーへのリンクの追加 99
raw デバイス マッピング保護のための考慮事項 100
サーバの通信プロトコルの変更 101
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
リストアに関する考慮事項 121
アプリケーション レベル リストア 122
Exchange Server のデータのリストア 123
SQL Server のデータのリストア 129

第 5 章: CA ARCserve Central Host-Based VM Backup のトラブルシューティング 133

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 135

空の Web ページが表示される、または、JavaScript エラーが発生する 138
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 140
ページのロード問題のトラブルシューティング方法 142
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 143
ノード更新時のアクセス拒否エラー発生 144
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 146
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 147
VM の復旧が不明なエラーで失敗する 149
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 151
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 151
オペレーティング システムが見つからないエラー 154
MAC アドレスの変更が VM 復旧後に保持されない 155
CA ARCserve D2D Web サービスが CA ARCserve D2D ノード上で失敗する 156
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 159
CA ARCserve D2D Web サービスの実行が遅い 160
変更ブロックのトラッキングに失敗する 162
ESXi ライセンスのためにバックアップが失敗する 163
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 164
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 165
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 166
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 167
VMDK ファイルを開けない 168
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 169
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 170
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 171
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 172
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 176
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 177
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 177
仮想マシンを代替の ESX サーバまたは Hyper-V サーバに復旧するときに、CA ARCserve Central Host-Based VM Backup がダイナミック ディスク上のボリュームを認識できない 178
容量が 2 TB より大きいディスクに［ホット追加トランスポート］（HotAdd Transport）モードを使用してデータをバックアップした場合のデータ リストアの問題 179

第 6 章: ベストプラクティスの適用 181

仮想マシンのベア メタル復旧の実行 181
ブート キットの作成方法 201
同時バックアップ数の制限の定義 216
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 217
CA ARCserve D2D バックアップ プロキシの保護 219
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 219
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 221
埋め込みマニフェストを含まないバイナリ ファイル 222
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 223
アンチウイルス スキャンからのファイルの除外 225

用語集 229

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. 11)
CA ARCserve Central Host-Based VM Backup について (P. 12)
CA ARCserve Central Host-Based VM Backup の仕組み (P. 13)
CA ARCserve Central Applications マニュアル選択メニュー (P. 14)

概要

CA ARCserve Central Applications は、コア データ保護および管理テクノロジと、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

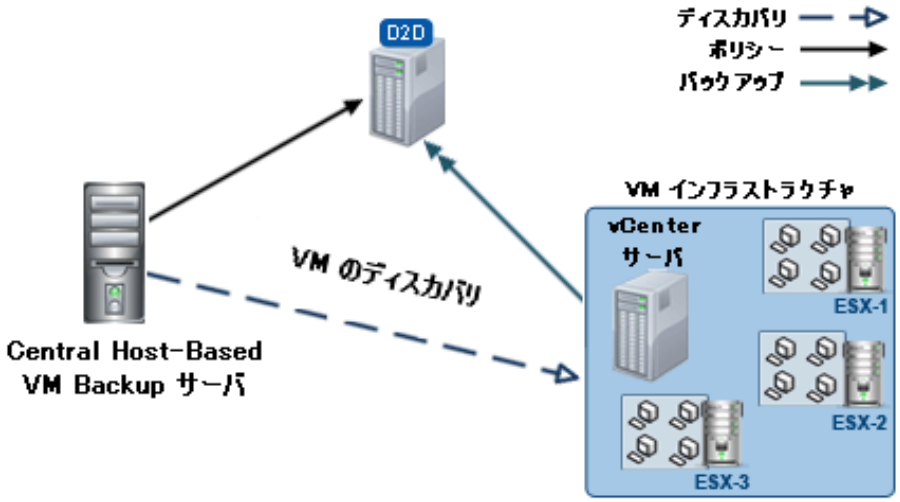
CA ARCserve Central Applications の 1 つが CA ARCserve Central Host-Based VM Backup アプリケーションです。 このアプリケーションは、軽量のバックアップ ソリューションである CA ARCserve D2D と共に動作して、個別の仮想マシンにソフトウェアまたはエージェントをインストールする必要なしに、複数の仮想マシンを保護することができます。 この機能によって、同一の物理サーバ上で複数のバックアップ処理を実行する際の悪影響を最小限にし、仮想マシンのバックアップからファイル レベル、アプリケーション レベルの復旧あるいは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

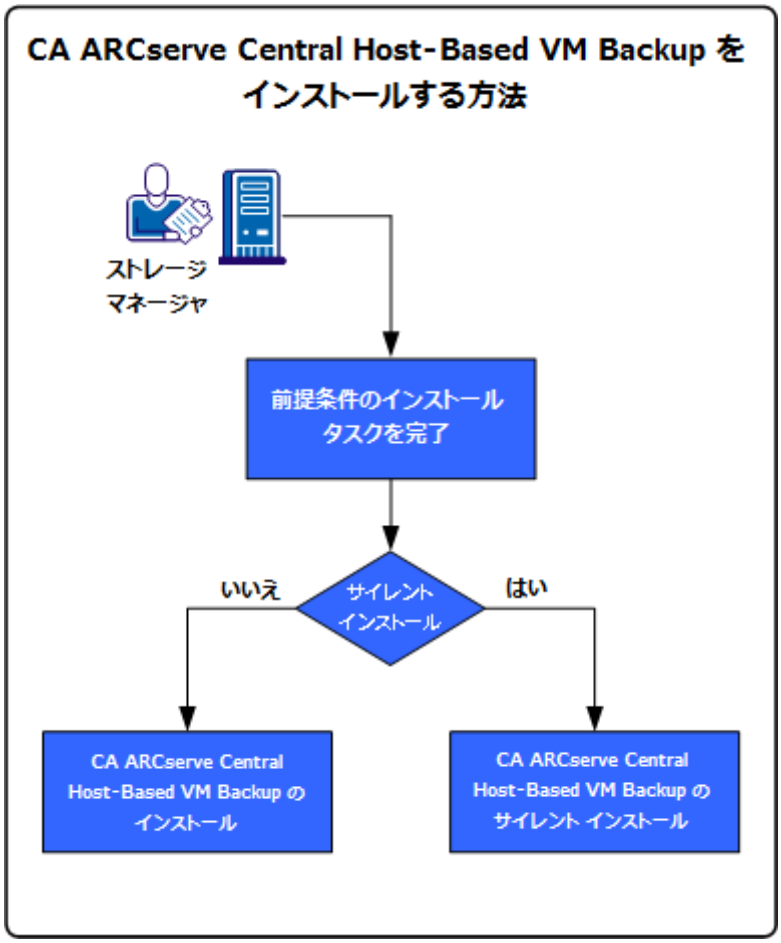
CA ARCserve Central Host-Based VM Backup をインストールする方法 (P. 15)
CA ARCserve Central Host-Based VM Backup をアンインストールする方法 (P. 25)
CA ARCserve D2D ノードを保護するように CA ARCserve Central Host-Based VM Backup を設定する方法 (P. 29)

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. 17)
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. 20)
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. 22)

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
- 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 バックアップから詳細リストア機能を使用する場合は、管理者権限を持った任意のユーザのビルトイン認証情報またはドメイン管理者認証情報が、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ることを確認します。
- CA ARCserve Central Applications では、展開ユーティリティを使用して、リモート ノード上に CA ARCserve D2D をインストールし、旧バージョンを最新バージョンにアップグレードできます。最新バージョンの CA ARCserve D2D を使用して、リモート ノード上のデータをバックアップするには、最新バージョンの CA ARCserve D2D ライセンスを取得し、ノード上でライセンスを適用する必要があります。 ノード上にインストールまたはアップグレードした日付から 31 日以内にライセンスを適用しない場合、CA ARCserve D2D は動作を停止します。

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。 このサーバは、すべてのアプリケーションに共通のモジュールです。 このモジュールには、アプリケーション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、および設定が含まれています。

  アプリケーションをインストールする場合、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。アプリケーションにパッチを適用する必要が生じた場合、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 Host-Based VM Backup のインストール後に、バックアップ プロキシ システム、およびプレフライト チェックの実行に使用されるコンピュータに VMware VIX API バージョン 1.11 をダウンロードおよびインストールします。 VMware VIX は、バックアップからファイル レベルおよびアプリケーション レベルのリストアを実行するために使用されます。

注: VIX API 1.11 では、すべての仮想マシンが最新の VMware Tools で更新されている必要があります。

- 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。

  異なるバージョンの VDDK 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. 121)」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 仮想スタンバイ

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
```

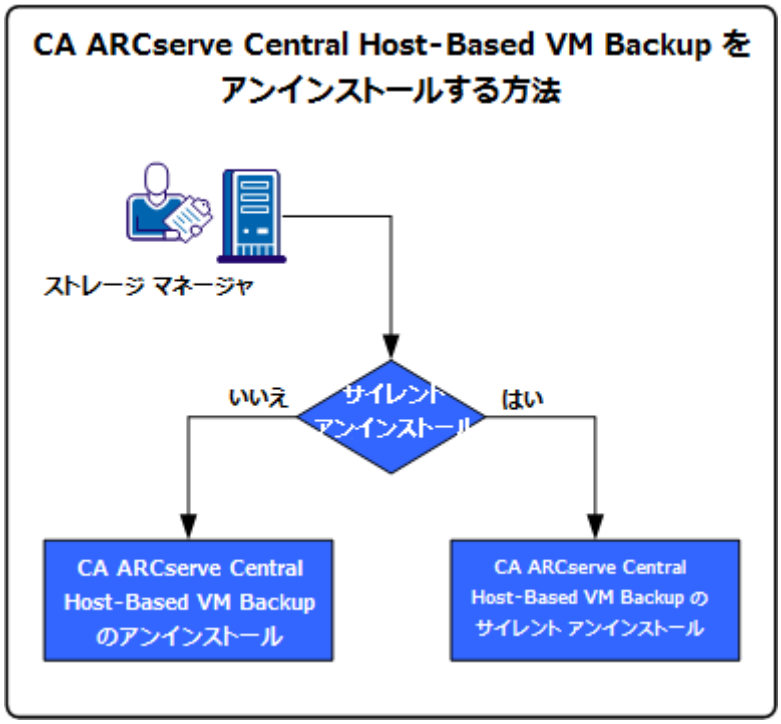
アプリケーションがサイレント インストールされます。

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	参照トピック
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。	CA ARCserve Central Host-Based VM Backup のアンインストール (P. 26)
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。	CA ARCserve Central Host-Based VM Backup のサイレント アンインストール (P. 27)

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 仮想スタンバイ

{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。

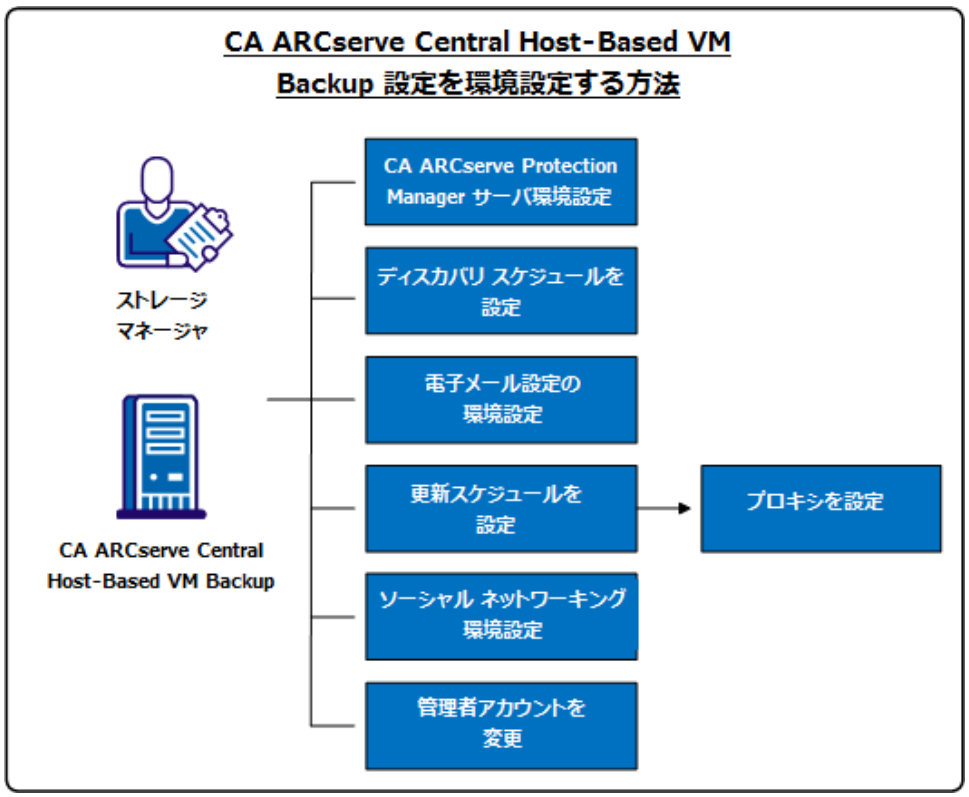
CA ARCserve D2D ノードを保護するように CA ARCserve Central Host-Based VM Backup を設定する方法

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」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. 30)
- ディスカバリ スケジュールの設定 (P. 32)
- 電子メール設定の環境設定 (P. 32)
- 更新スケジュールの設定 (P. 34)
  - プロキシ設定の環境設定 (P. 35)
- ソーシャル ネットワーキングの環境設定 (P. 37)
- 管理者アカウントの変更 (P. 38)

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。

ディスカバリ スケジュールの設定

ノードに対してディスカ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、ディスカ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、ディスカバリが開始される時刻と繰り返しの方法を指定します。 ディスカバリ 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 ディスカ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。

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。

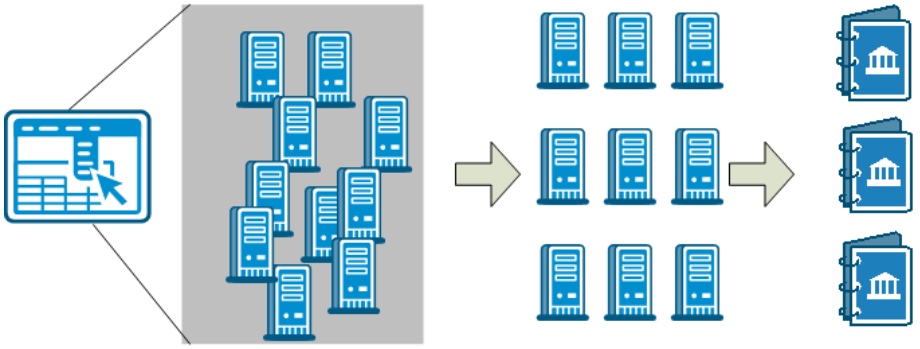
第 3 章: CA ARCserve Central Host-Based VM Backup の使用

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. 42)
CA ARCserve Central Host-Based VM Backup ホーム画面の使用方法 (P. 43)
CA ARCserve D2D ノードへのログイン (P. 44)
CA ARCserve Central Host-Based VM Backup 用のノード タスクを管理する方法 (P. 45)
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. 58)
仮想マシン環境のバックアップ方法 (P. 64)
CA ARCserve Central Host-Based VM Backup 用ポリシーの管理方法 (P. 83)
CA ARCserve Central Host-Based VM Backup ログの表示 (P. 95)
特定ノードのアクティビティ ログ情報の表示 (P. 97)
CA ARCserve Central Host-Based VM Backup のステータスをレポートに表示 (P. 98)
ナビゲーション バーへのリンクの追加 (P. 99)
raw デバイス マッピング保護のための考慮事項 (P. 100)
サーバの通信プロトコルの変更 (P. 101)
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 ホーム画面の使用方法

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

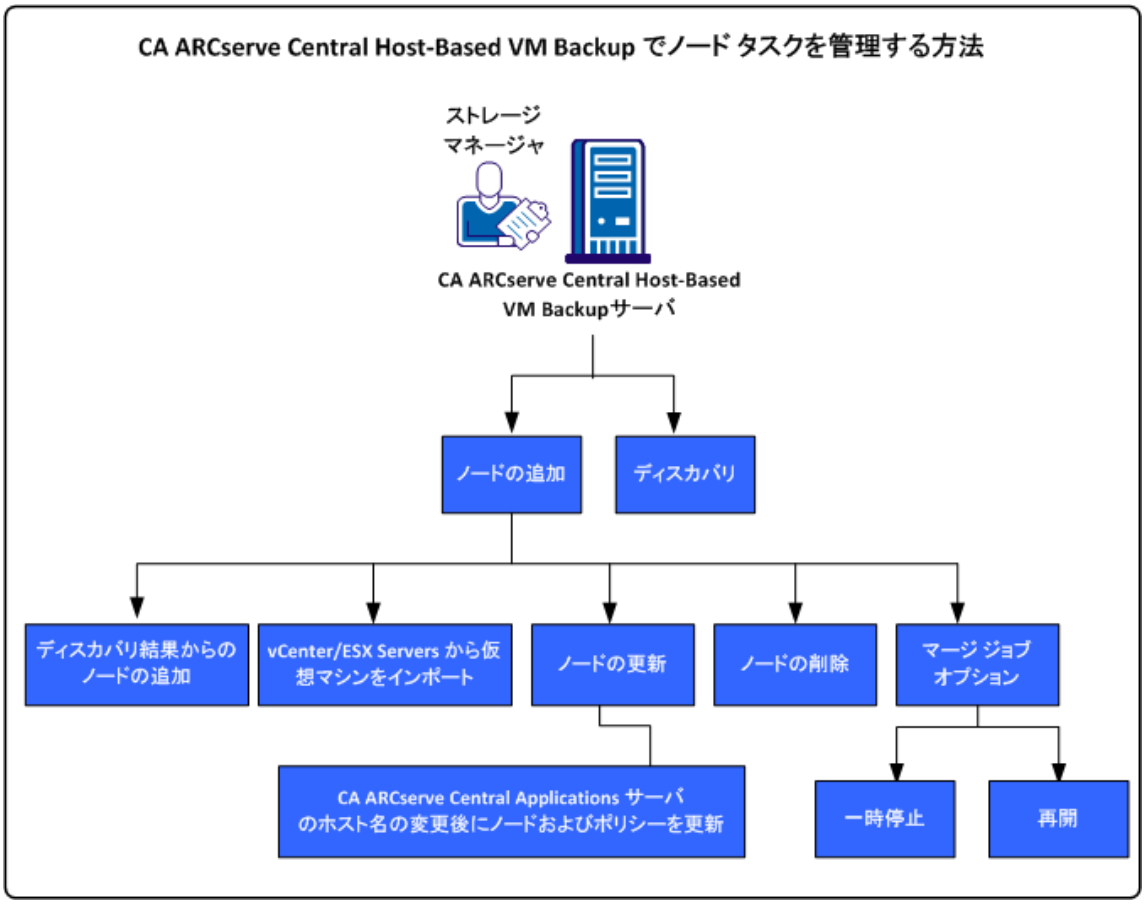
このシナリオでは、ストレージ マネージャがどのようにノードを管理できるかについて説明します。 たとえば、ノードの追加やディスカバリの実行、ノードのノード グループへの追加、および［ノード］画面からのノードの更新または削除を行います。

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. 80)	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 モニタ (P. 81)］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。 ■ = 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 サマリ］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。 ■ 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	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。 ■ = エラー/失敗 ■ = 警告 ■ = 成功 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。 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。 ■ 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。 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. 65)」を参照してください。
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. 48)
- ノードの追加 (P. 49)
  - オート ディスカバリの結果からのノードの自動追加 (P. 50)
  - vCenter/ESX Server からの仮想マシンのインポート (P. 52)
- ノードの更新 (P. 54)
  - 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. 55)
- ノードの削除 (P. 56)
- マージ ジョブ オプション (P. 56)
  - ノード上のマージ ジョブの一時停止 (P. 56)

- ノード上のマージ ジョブの再開 (P. 57)

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. 50) -- 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、次回のスケジュール 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. 52)

  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 Scheduling （DRS）を実行している場合に仮想マシンをインポートする際は、vCenter Server システムのホスト名または IP アドレス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。 仮想マシンが ESX サーバ間を移動するときにバックアップが失敗しないように、仮想マシンのインポート中には、ESX サーバのホスト名や IP アドレスを指定しないことを推奨します。

     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. 54)」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。

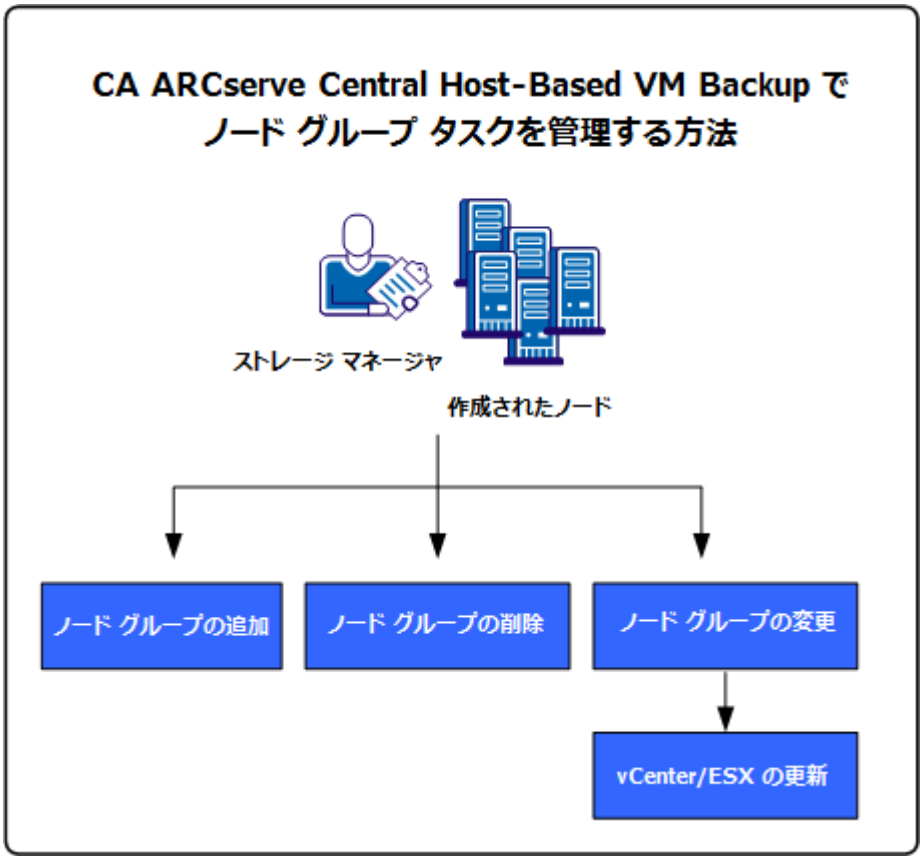
選択したノードのマージ ジョブは再開され、CA ARCserve D2D ホーム ページ上で確認できます。

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. 83)」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. 59)
- ノード グループの削除 (P. 61)
- ノード グループの変更 (P. 62)

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。

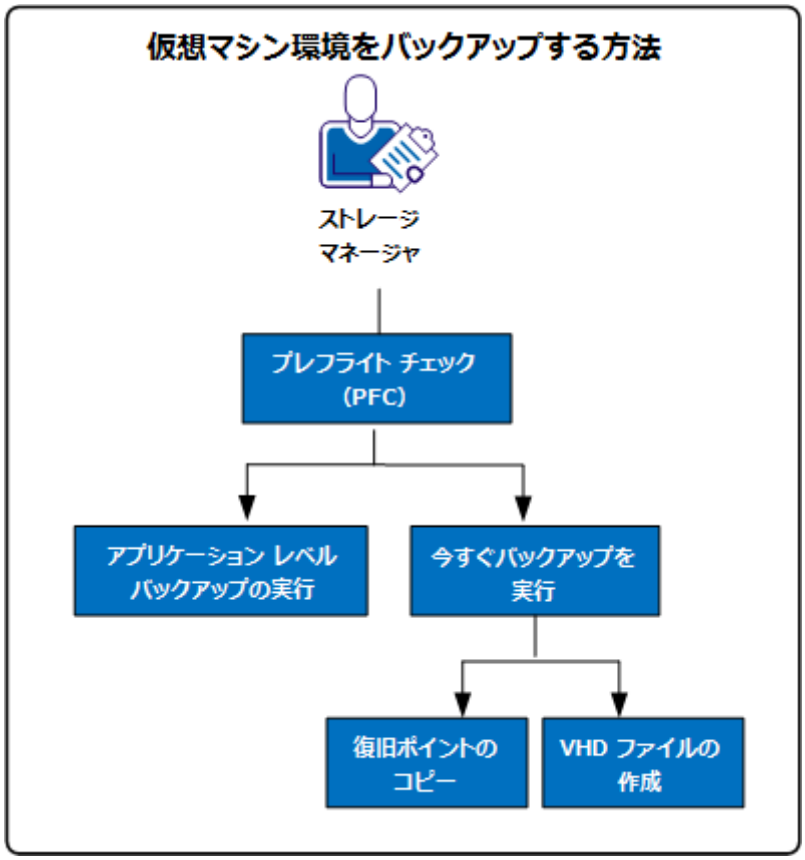
   ［vCenter/ESX の更新］ダイアログ ボックスが表示されます。
3. vCenter/ESX Server の詳細をそれに応じて更新します。
4. ［OK］をクリックします。

   ［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. 65)
- 今すぐバックアップを実行 (P. 70)
  - バックアップ復旧ポイントのコピー (P. 74)
  - VHD ファイルの作成 (P. 78)
- アプリケーション レベル バックアップの実行 (P. 79)

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、仮想マシンのディスクを確認します。
電力状態	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. 67)」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	解決策
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。	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。 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> **注**: <VM-InstanceUUID> を、CBT が失敗している仮想マシンの UUID 値に置き換えます。この値は、CA ARCserve D2D に接続したときに使用される仮想マシンの URL 内で見つけることができます。 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。 6. 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	解決策
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。

ステータス	メッセージ	解決策
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	解決策
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。

電力状態

ステータス	メッセージ	解決策
警告	電源がオフになりました。	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	解決策
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	解決策
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。

ステータス	メッセージ	解決策
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。	ビルトイン認証情報またはドメイン管理者認証情報を指定して、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します。 VMware 制限により、バックアップは、購入済みライセンスがある ESX Server 上で実行される VM でのみサポートされています。バックアップは無償ライセンスがある ESXi Server ではサポートされていません。
警告	アプリケーション レベル復旧は、記憶域が有効になっているシステムではサポートされていません。仮想マシン全体のみを復旧できます。	CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、Microsoft SQL Server および Microsoft Exchange Server のデータをバックアップします。

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生じる場合があります。

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ークアップ ジョブは作成されません。 メークアップ 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。

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: 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。

4. 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。

5. ［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。

6. ［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。

7. コピーする復旧ポイントを指定します。

   a. カレンダで、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。

   b. 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。

8. ［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。
- **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. 74) 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¥S0000000001 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。

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
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 ステータス情報の表示

CA ARCserve Central 仮想スタンバイ 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。

ジョブが実行されている場合、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 バー上で［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。

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 (P. 81)」を参照してください。

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、［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、現在のジョブを停止します。

     注: ［キャンセル］をクリックした場合、［バックアップ ステータス モニタ］ダイアログ ボックスは閉じます。

詳細情報:

ジョブ ステータス情報の表示 (P. 80)

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。

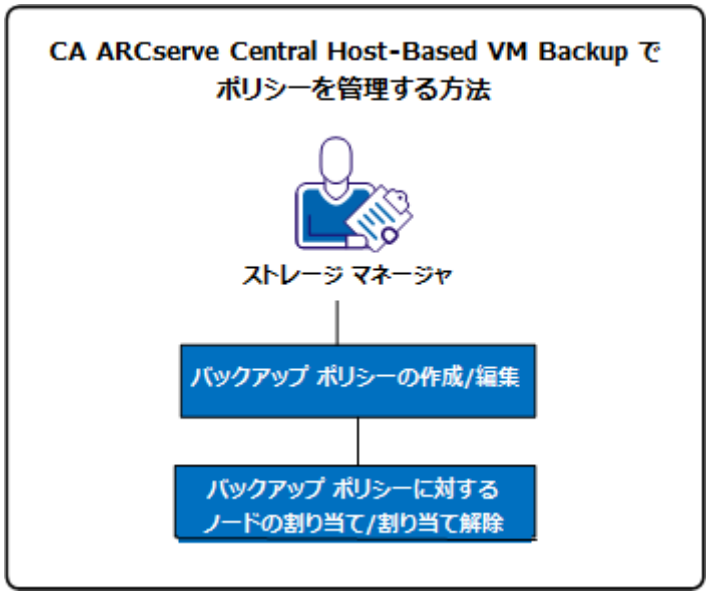
- **フェーズ -- （バックアップおよびカタログ モニタ）**プロセスにおける現在の段階が、プログレス バーの塗りつぶされた部分で示されます。
- **開始時刻 -- （バックアップおよびカタログ モニタ）**ポリシー設定に基づいて処理が開始された日時を表示します。
- **経過時間 -- （バックアップおよびカタログ モニタ）**開始時間と現在の時間との差を表示します。
- **推定残り時間 -- （バックアップ モニタのみ）**ジョブの完了に必要と予測される時間を表示します。
- **処理中 -- （カタログ モニタのみ）** 現在カタログを生成しているボリュームのドライブ文字またはア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ることはできません。

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. 84)
- バックアップ ポリシーの編集 (P. 89)
- 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. 93)

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、以下の情報を入力します。

   - **ログの切り捨て** -- 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。
   - **デスティネーション上の予約容量** --1 つのバックアップを実行するために予約する容量パーセントを指定します。 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。
   - **カタログ** -- ブラウザ検索の待機時間を短縮するには、［各バックアップ後に、検索速度を上げるためのファイル システム カタログを生成］オプションを選択します。

     このオプションが選択されていない場合は、カタログ ジョブの完了を待たずに、バックアップの直後にリストアを実行することができます。 このオプションは、デフォルトでは有効化されていません。 以下の点に注意してください。
     - 各バックアップ ジョブのファイル システム カタログを生成すると、メタデータ ファイルとカタログ ファイルを格納するディスク ストレージの容量と、CPU 使用率が増加します。 さらに、バックアップ ソースに多数のファイルが含まれる場合、カタログ生成のプロセスは時間のかかるタスクとなる場合があります。
     - バックアップ ソースとして ReFS ボリュームを選択すると、カタログを生成できません。警告メッセージが表示され、この状況が通知されます。

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 ジョブが停止、スキップ、失敗、またはクラッシュした場合
   - マージ ジョブが成功した場合
   - 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、以下の情報を入力します。

   - **ログの切り捨て** -- 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。
   - **デスティネーション上の予約容量** --1 つのバックアップを実行するために予約する容量パーセントを指定します。 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。
   - **カタログ** -- ブラウザ検索の待機時間を短縮するには、［各バックアップ後に、検索速度を上げるためのファイル システム カタログを生成］オプションを選択します。

     このオプションを選択しない場合、リストアはバックアップ直後に実行され、カタログ ジョブの完了を待機することはありません。このオプションは、デフォルトでは無効になっています。

     注: 各バックアップ ジョブのファイル システム カタログを生成すると、メタデータ ファイルとカタログ ファイルを格納するディスク ストレージの容量と、CPU 使用率が増加します。 さらに、バックアップ ソースに多数のファイルが含まれる場合、カタログ生成のプロセスは時間のかかるタスクとなる場合があります。

     注: バックアップ ソースとして ReFS またはデデュプリケーション NTFS ボリュームを選択した場合、カタログは生成されずに警告メッセージが表示されます。

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。

6. 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。

7. ［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。

次の手順に従ってください:

1. 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。

2. 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。
  - **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。
  - **複数ノードの更新** -- 複数ノードの同時更新に関するログのみを表示します。
  - **CA ARCserve D2D マージ ジョブ** -- CA ARCserve D2D マージ ジョブの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' で始まるコンピュータ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 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。

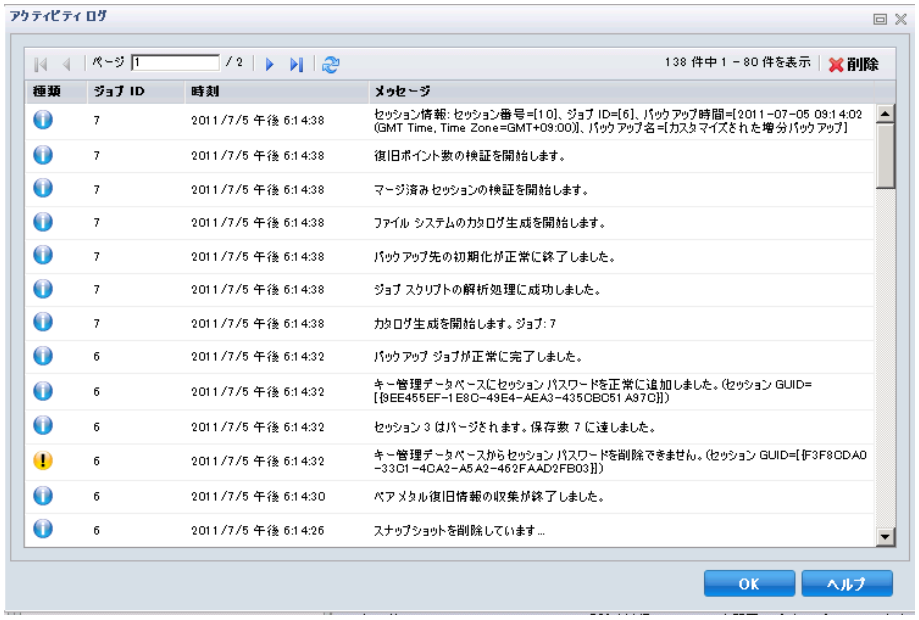
3. ログインするノードを探してクリックし、ポップアップ メニューから [D2D にログイン] をクリックします。

   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。

CA ARCserve Central Host-Based VM Backup のステータスをレポートに表示

CA ARCserve Central Protection Manager および CA ARCserve Central Reporting をインストールした場合、Host-Based VM Backup プロキシ サーバを CA ARCserve Central Protection Manager に追加して仮想化保護ステータス レポートを生成し、Host-Based VM Backup プロキシのステータスを表示できます。

仮想化保護ステータス レポートの詳細については、「CA ARCserve Central Reporting ユーザ ガイド」を参照してください。

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 仮想スタンバイ 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 仮想スタンバイ 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。

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。 それほどの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. 229）
- NBD 転送モード（P. 229）
- NBDSSL 転送モード（P. 229）
- SAN 転送モード（P. 229）

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. 229)

   nbd

   NBD 転送モード (P. 229)

   nbdssl

   NBDSSL 転送モード (P. 229)

   san

   SAN 転送モード (P. 229)
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. 121)」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)
リストアに関する考慮事項 (P. 121)
アプリケーション レベル リストア (P. 122)

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 (P. 107)

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 (P. 112)

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 (P. 115)

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 (P. 122)

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 (P. 181)

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 仮想スタンバイ、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:

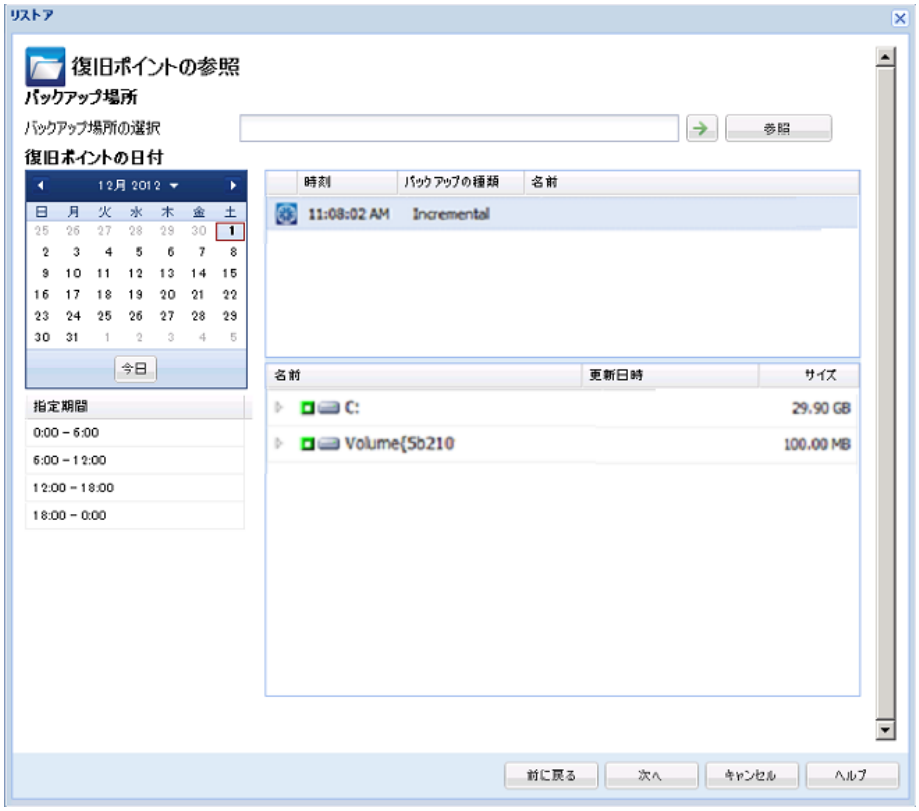
1. アプリケーションにログインし、ナビゲーション バーの［ノード］をクリックします。

   ［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。

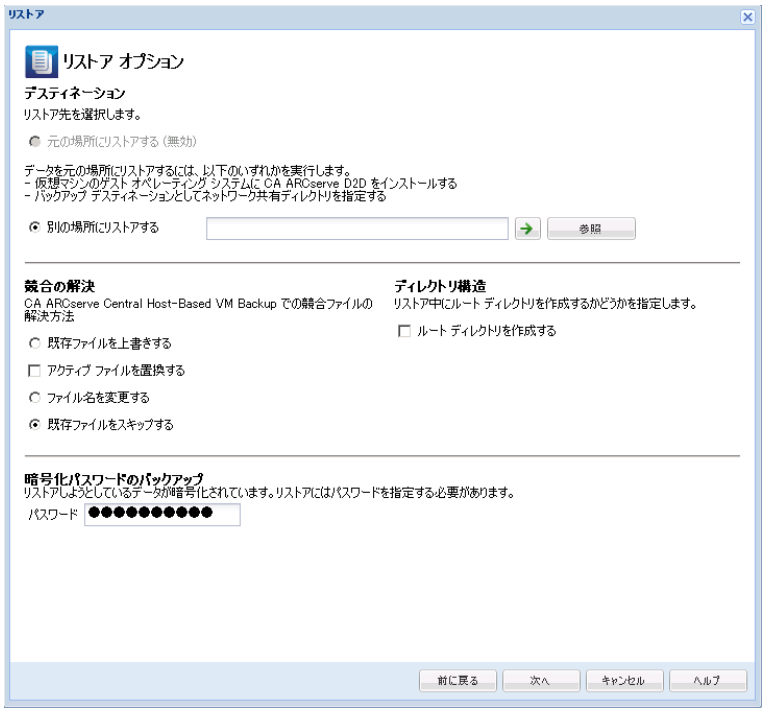
   リストアするノードの横のチェック ボックスをオンにしてから、ツールバー上の［リストア］をクリックします。

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 イメージに含められます。 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:

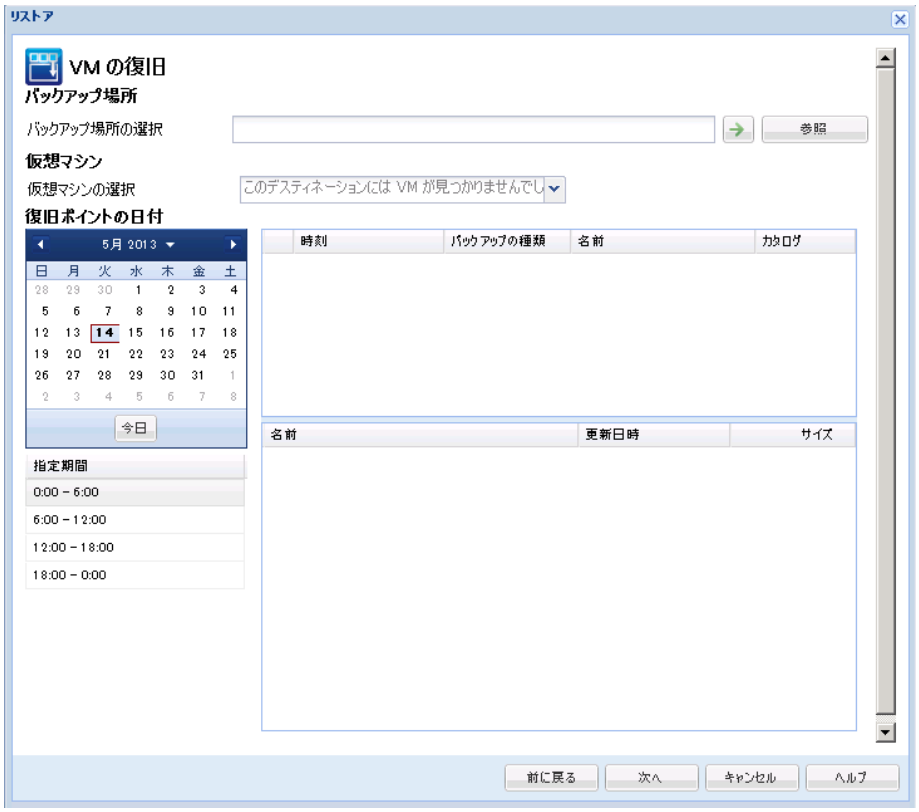
1. アプリケーションにログインし、ナビゲーション バーの［ノード］をクリックします。

   ［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。 CA ARCserve D2D にログインします。

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、リストア先を選択します。

   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仮想マシンをリストアします。 デフォルトでは、このオプションが選択されています。

   詳細については、「元の場所への VM のリストア (P. 117)」を参照してください。

   別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場所とは別の場所へ仮想マシンをリストアします。

   詳細については、「別の場所への VM のリストア (P. 119)」を参照してください。

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 Serve 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。

仮想マシンの元の場所へのリストア

VM （仮想マシン）のリストアの環境設定では、仮想マシンをリストアする場所を選択する必要があります 選択可能なオプションは、［元の場所にリストアする］または［別の場所にリストアする］です。

元の場所への VM のリストアを選択した場合は、以下の手順に従います。

次の手順に従ってください:

1. ［リストア オプション］ダイアログ ボックスで、［競合の解決］および［復旧後の処理］オプションを指定した後、［元の場所にリストアする］を選択して［次へ］をクリックします。

   注: ［競合の解決］および［復旧後の処理］オプションの詳細については、「仮想マシンからのデータのリストア」を参照してください。

   ［ソース vCenter/ESX Server の認証情報の設定］ダイアログ ボックスが表示されます。

2. 仮想マシンにアクセスするための認証情報を指定します。

   - **Center/ESX Server** -- デスティネーションの vCenter/ESX Server システムのホスト名または IP アドレスを指定します。
   - **VM 名** -- リストアする仮想マシンのホスト名を指定します。
   - **プロトコル** -- デスティネーション サーバとの通信に使用するプロトコルを指定します。 選択肢は HTTP と HTTPS です。
   - **ポート番号** -- ソース サーバとデスティネーションとの間のデータ転送に使用するポートを指定します。 デフォルトのポート番号は 443 です。
   - **ユーザ名** -- リストアしている仮想マシンにログインするためのアクセス権限があるユーザ名を指定します。
   - **パスワード** -- リストアする仮想マシンへのログインに必要な、［ユーザ名］に対応するパスワードを指定します。

3. 認証情報を指定したら、［OK］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。

4. 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。

仮想マシンの別の場所へのリストア

VM （仮想マシン）のリストアの環境設定では、仮想マシンをリストアする場所を選択する必要があります 選択可能なオプションは、［元の場所にリストアする］または［別の場所にリストアする］です。

仮想マシンを別の場所にリストアする場合は、以下の手順に従います。

次の手順に従ってください:

1. ［リストア オプション］ダイアログ ボックスで、［競合の解決］および［復旧後の処理］オプションを指定した後、［別の場所にリストアする］を選択します。

   注: ［競合の解決］および［復旧後の処理］オプションの詳細については、「仮想マシンからのデータのリストア」を参照してください。

   ［リストア オプション］ダイアログ ボックスが展開され、別の場所にリストアするための追加のオプションが表示されます。

2. vCenter/ESX Server 情報を指定します。

   - **Center/ESX Server** -- デスティネーションの vCenter/ESX Server システムのホスト名または IP アドレスを指定します。
   - **ユーザ名** -- リストアしている仮想マシンにログインするためのアクセス権限があるユーザ名を指定します。
   - **パスワード** -- リストアする仮想マシンへのログインに必要な、［ユーザ名］に対応するパスワードを指定します。
   - **プロトコル** -- デスティネーション サーバとの通信に使用するプロトコルを指定します。 選択肢は HTTP と HTTPS です。
   - **ポート番号** -- ソース サーバとデスティネーションとの間のデータ転送に使用するポートを指定します。 デフォルトのポート番号は 44 です。

3. vCenter/ESX Server 情報が指定されたら、［この vCenter/ESX Server に接続］ボタンをクリックします。

   別のサーバへのアクセス認証情報情報が正しい場合、［その他の情報］フィールドが有効になります。

4. 以下の情報を指定します。

   - **VM 名** -- リストアする仮想マシンのホスト名を指定します。
   - **ESX Server** -- デスティネーションの ESX Server を指定します。 ドロップダウン メニューには、指定された仮想マシンに関連付けられているすべての ESX Server のリストが含まれます。
   - **リソース プール** -- 仮想マシン復旧に使用するリソース プールまたは vApp プールを指定します。 ［リソース プールの参照］ボタンをクリックすると、［リソース プールの選択］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、デスティネーション ESX サーバで利用可能なすべてのリソース プールおよび vApp プールのリストが含まれます。仮想マシンの復旧に使用するプールを選択します。 この仮想マシン復旧にリソース プールまたは vApp プールを割り当てない場合は、このフィールドを空白のままにできます。

     注: リソース プールは、CPU およびメモリ リソースの設定済みコレクションです。 vApp プールは、1 つのオブジェクトとして管理可能な仮想マシンのコレクションです。
   - **VM データ ストア** -- 仮想マシン復旧または仮想マシン内の各仮想ディスクのデスティネーション VM データストアを指定します。

     仮想マシンは複数の仮想ディスクを持つことができ、各仮想ディスクに異なるデータ ストアを指定できます。

     例：

     - Disk0 を Datastore1 にリストアできます。
     - Disk1 を Datastore1 にリストアできます。
     - Disk2 を Datastore2 にリストアできます。

     重要: VM データ ストアについては、このフィールドに値が入力されるのは、ユーザに完全な VMware System 管理者権限がある場合のみです。 ユーザに適切な管理者権限がない場合、vCenter/ESX Server に接続した後、CA ARCserve Central Host-Based VM Backup はリストア プロセスを続行しません。

5. その他の情報が指定されたら、［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。

6. 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。

リストアに関する考慮事項

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。	■ **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」トピック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。

リストア方式	目的	考慮事項:
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	■ **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なだけでなく、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）、あるいは Exchange の組織管理者またはサーバ管理者役割の権限（Exchange Server 2007/2010/2013 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 または 2013 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。
  - リストアを実行する方法の完全な手順については、「CA ARCserve D2D ユーザ ガイド」を参照してください。

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。
- Exchange Server 2013 - Microsoft ボリューム シャドウ コピー サービス（VSS）のバックアップおよびリストアがサポートされています。 Granular Recovery Technology （GRT）はサポートされていません。

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. 122)」の必要な前提条件を実行してください。

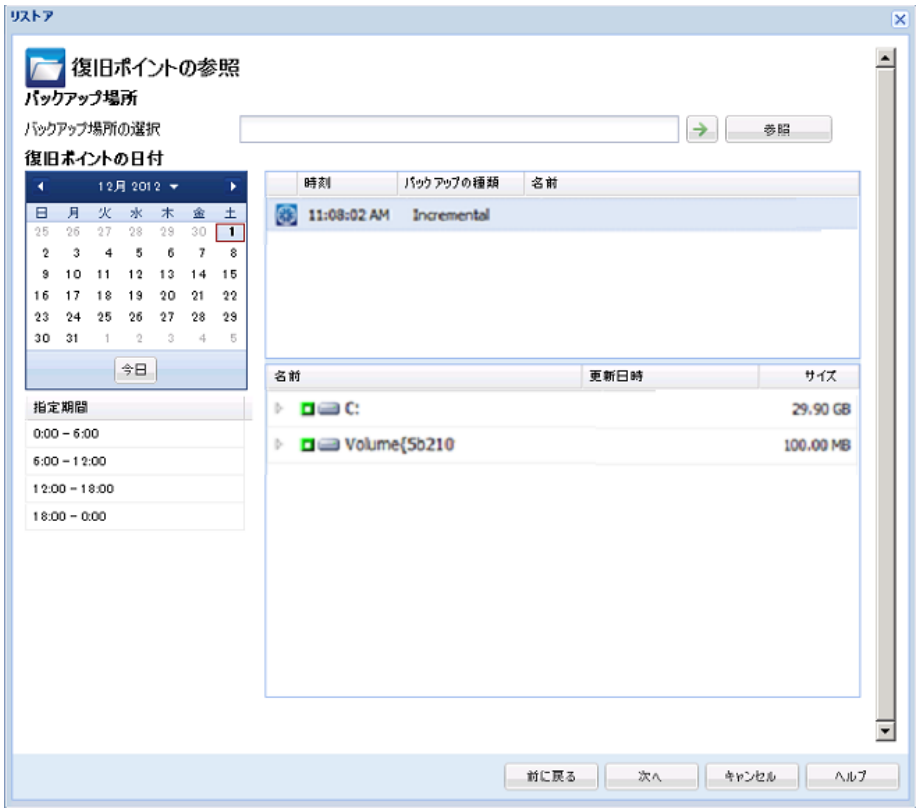
重要: Microsoft Exchange Server のユーザ メールボックス アイテムのリストアは、CA ARCserve Central Host-Based VM Backup セッションからはサポートされていません。 詳細レベルで Microsoft Exchange Server データをリストアするには、CA ARCserve Central Protection Manager または CA ARCserve D2D を使用して、Exchange Server データをバックアップします。

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選択］フィールドで、Exchange Server データのリストア元である 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、回復の完了後も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ることがない。

  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もありません。

  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. 122)」で前提条件を確認してください。

重要: Microsoft SQL Server の詳細リストアは、CA ARCserve Central Host-Based VM Backup コンソールでは実行できません。 Microsoft SQL Server データをリストアするには、ゲスト仮想マシンに CA ARCserve D2D をインストールします。

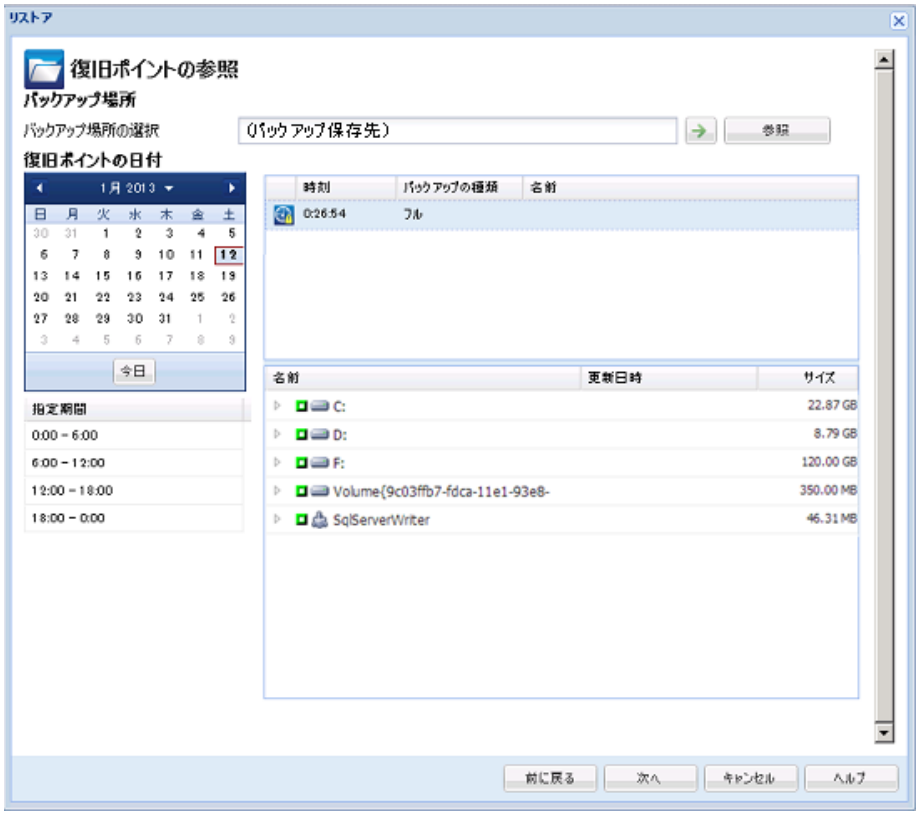
次の手順に従ってください:

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. SQL 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選択］フィールドで、SQL Server データのリストア元である 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

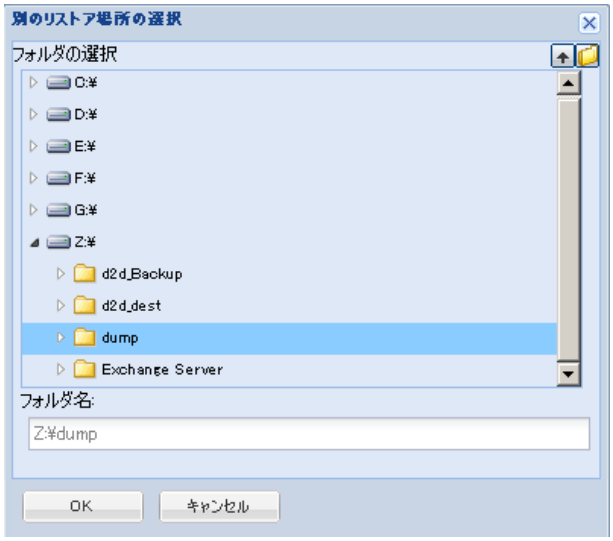
   バックアップ イメージがキャプチャされた元の場所にリストアします。

   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。

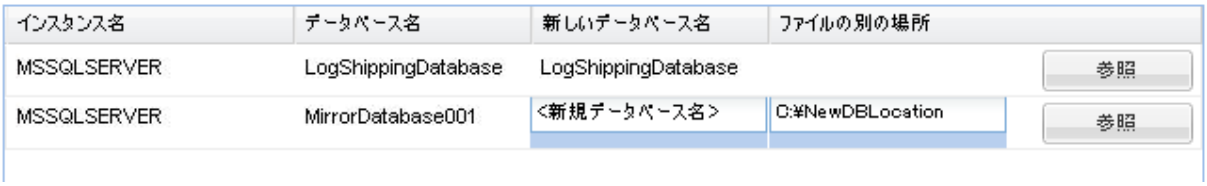
   ダンプ ファイルは、アプリケーションがクラッシュした場合に作成されます。このファイルには、問題の原因をトラブルシュートするために使用できる追加情報（タイム スタンプ付き）が含まれます。

   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。

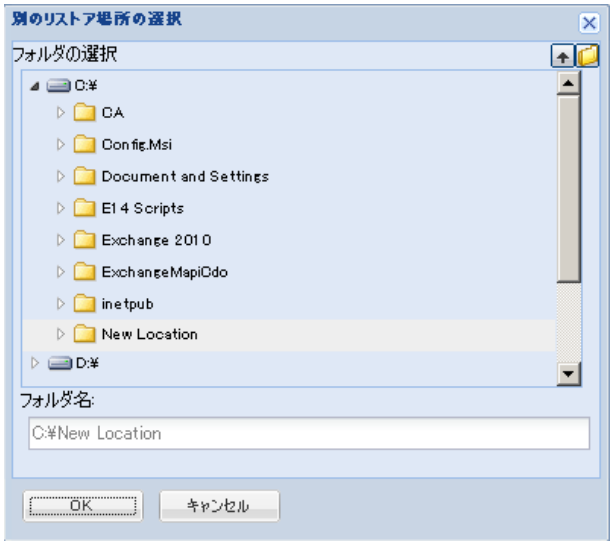


   別の場所にリストアする

   元の場所以外の別の場所にリストアします。



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. 135)
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. 138)
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. 140)
ページのロード問題のトラブルシューティング方法 (P. 142)
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. 143)
ノード更新時のアクセス拒否エラー発生 (P. 144)
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. 146)
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. 147)
VM の復旧が不明なエラーで失敗する (P. 149)
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. 151)
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. 151)
オペレーティング システムが見つからないエラー (P. 154)
MAC アドレスの変更が VM 復旧後に保持されない (P. 155)
CA ARCserve D2D Web サービスが CA ARCserve D2D ノード上で失敗する (P. 156)
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. 159)
CA ARCserve D2D Web サービスの実行が遅い (P. 160)
変更ブロックのトラッキングに失敗する (P. 162)
ESXi ライセンスのためにバックアップが失敗する (P. 163)
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. 164)
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. 165)
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. 166)
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. 167)
VMDK ファイルを開けない (P. 168)
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. 169)
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. 170)
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. 171)

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. 172)
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. 176)
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. 177)
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. 177)
仮想マシンを代替の ESX サーバまたは Hyper-V サーバに復旧するときに、CA ARCserve Central Host-Based VM Backup がダイナミック ディスク上のボリュームを認識できない (P. 178)
容量が 2 TB より大きいディスクに［ホット追加トランスポート］（HotAdd Transport）モードを使用してデータをバックアップした場合のデータ リストアの問題 (P. 179)

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:

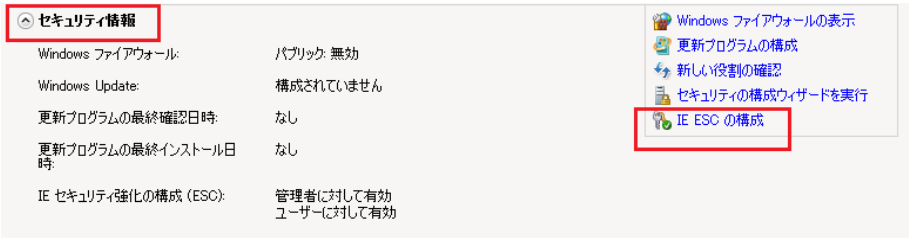
この問題を修正するには、アプリケーションの表示に使用しているコンピュータ上の Internet Explorer のセキュリティ強化の構成を無効にします。

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。



   ［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 コンポーネントが破損しているかまたは古い。	DirectX コンポーネントを更新します。

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 以降のバージョンです。

現象 1:

指定する Windows ユーザ アカウントが、組み込みの管理者またはドメイン ユーザ アカウントではなく、管理者グループのメンバである場合、［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。

現象 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指定しない場合、［ノードの更新］操作を実行する Windows ユーザ アカウントが組み込みの管理者またはドメイン ユーザ アカウントではなく、管理者グループのメンバである場合、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。

この問題を解決するには、以下のいずれかの方法を使用します。

- ビルトイン認証情報またはドメイン管理者認証情報を指定します。
- UAC の無効化
  1. 管理者アカウントを使用して、ノードにログインします。
  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. ［アカウントの変更］画面から、［ユーザ アカウント制御設定の変更］をクリックし、次に、以下のいずれかを実行します。
     - **Windows Vista および Windows Server 2008：** ［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、変更内容を UAC へ適用します。
     - **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］画面で、スライダを［常に通知する］から［通知しない］に移動します。 ［OK］をクリックし、Windows 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、変更内容を UAC へ適用します。

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=Failed
   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」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. 168)」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. 229)または SAN 転送モード (P. 229)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。

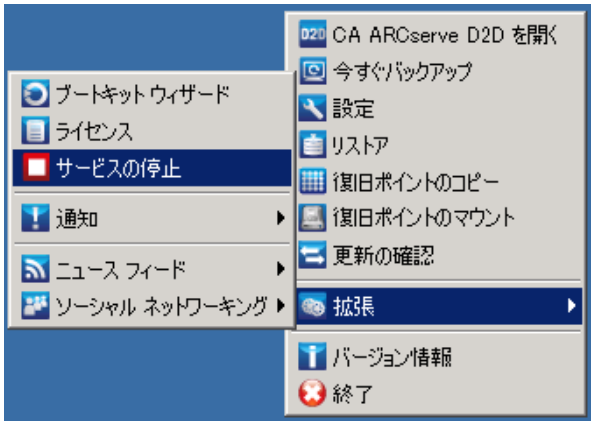
解決方法:

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。

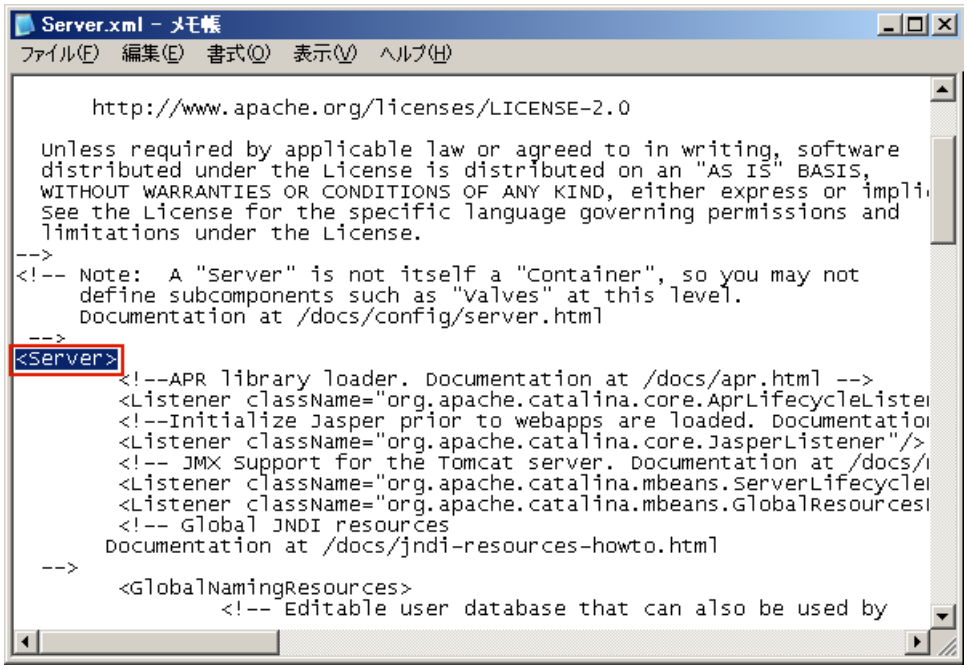
   

2. Tomcat の server.xml ファイルを開いて、Tomcat の動作を変更/設定します。

   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。



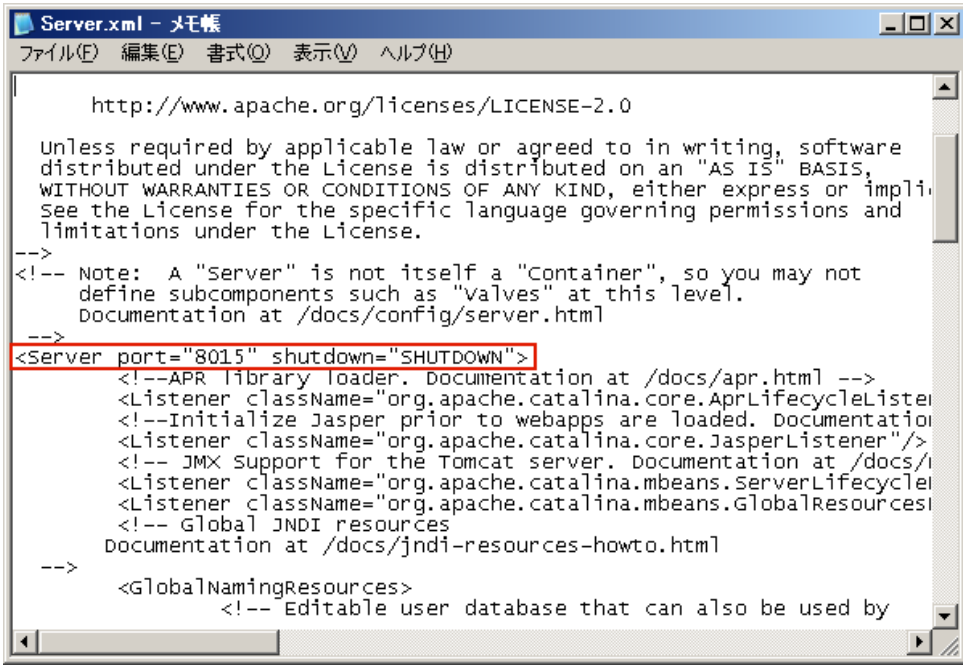
4. <Server> タグを以下のように編集します。

   変更前：

   <Server>

   変更後：

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



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かった。	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-stder.*.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。

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. 229)を指定した場合に、NBD 転送モード (P. 229)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 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. 56)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と、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が、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. 216)」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. 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。
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。

仮想マシンを代替の ESX サーバまたは Hyper-V サーバに復旧するときに、CA ARCserve Central Host-Based VM Backup がダイナミック ディスク上のボリュームを認識できない

Windows プラットフォームで有効

症状:

仮想マシンを代替の ESX サーバまたは Hyper-V サーバに復旧するときに、アプリケーションがダイナミック ディスク上のボリュームを認識できません。

一部のディスクはオフラインになり、仮想マシンが開始するときに対応するボリュームは利用不可になります。

解決方法:

ボリュームを取得するには、スタンバイ仮想マシンにログインして diskmgmt.msc から手動でディスクをオンラインに設定します。

容量が 2 TB より大きいディスクに[ホット追加トランスポート](HotAdd Transport)モードを使用してデータをバックアップした場合のデータ リストアの問題

症状:

2 TB より大きい VMDK (仮想マシンディスク) ファイルを VMware の[ホット追加トランスポート] (HotAdd Transport) モードを使用してバックアップすると、バックアップは成功しますが復元されたデータが壊れています。

解決方法:

VMware VDDK (Virtual Disk Development Kit) の既知の問題により、バックアップ ジョブは成功しますが、復元されたデータは壊れています。 この問題を解決するには、以下のいずれかの手順を実行します。

- バックアップ プランを再設定して、異なるバックアップ プロキシで実行されるバックアップ ジョブが[ホット追加トランスポート] (HotAdd Transport) モードを使用して実行されないようにする。
- レジストリ設定を使用して、バックアップ中にはホット追加モードが使用されないように設定する。 SAN または NBD/NBDSSL のいずれかを使用できます。

この VMware 問題の詳細については、VMware のドキュメント http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2068424を参照してください。

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. 181)
同時バックアップ数の制限の定義 (P. 216)
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. 217)
CA ARCserve D2D バックアップ プロキシの保護 (P. 219)
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. 219)
アンチウイルス スキャンからのファイルの除外 (P. 225)

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

YouTube： ベア メタル復旧を実行する方法

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。
  - CD/DVD 上に作成された BMR ISO イメージ
  - ポータブル USB メモリ上に作成された BMR ISO イメージ

  注: CA ARCserve D2D では、ブート キット ユーティリティを利用して WinPE イメージと CA ARCserve D2D イメージを組み合わせて BMR ISO イメージを作成します。 この ISO イメージがブート可能メディアに書き込まれます。 その後、これらのブート可能メディア（CD/DVD または USB メモリ）のいずれかを使用して、新しいコンピュータ システムを初期化し、ベア メタル復旧プロセスを開始できるようにします。保存されたイメージが常に最新のバージョンであるようにしておくために、CA ARCserve D2D を更新する度に新しい ISO イメージを作成することをお勧めします。
- 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: 複数のダイナミック ディスクで BMR を実行する場合、BMR は起動の失敗や認識できないダイナミック ボリュームなどの予期しないエラーで失敗する場合があります。 これが発生する場合は、システム ディスクのみを BMR を使用してリストアし、その後マシンを再起動してから他のダイナミック ボリュームを通常の環境でリストアするようにしてください。

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。

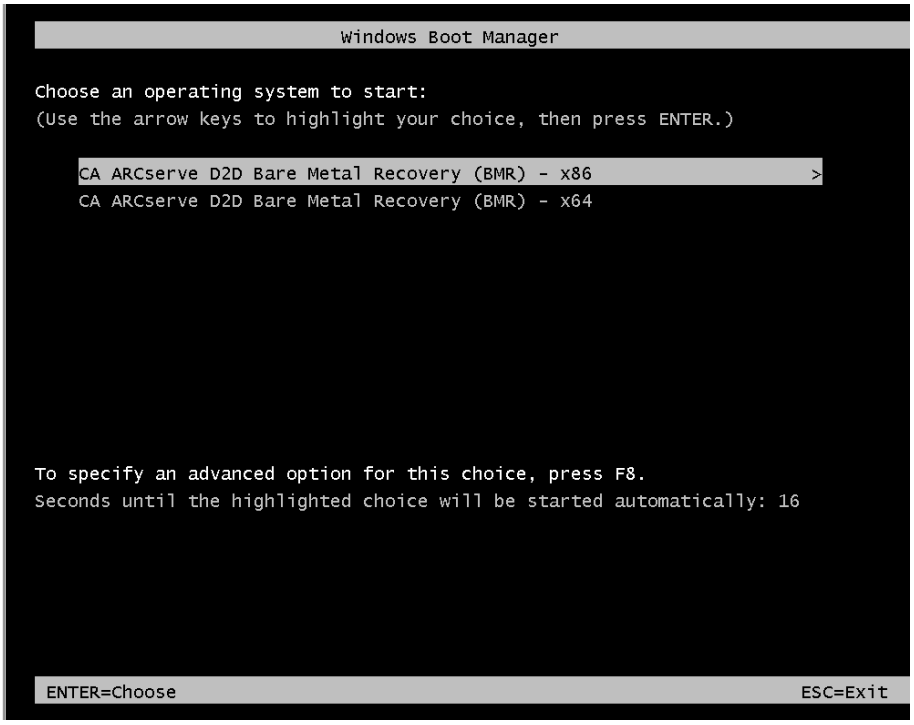
注: BMR プロセスではストレージ領域を作成できません。 ソース マシンにストレージ領域がある場合、BMR の実行中にデスティネーション マシンでストレージ領域を作成することはできません。 ユーザは、それらのボリュームを標準のディスク/ボリュームにリストアするか、BMR を実行する前にストレージ領域を作成してから、作成されたストレージ領域にデータをリストアすることができます。

ベア メタル復旧を使用してデータをリストアする方法

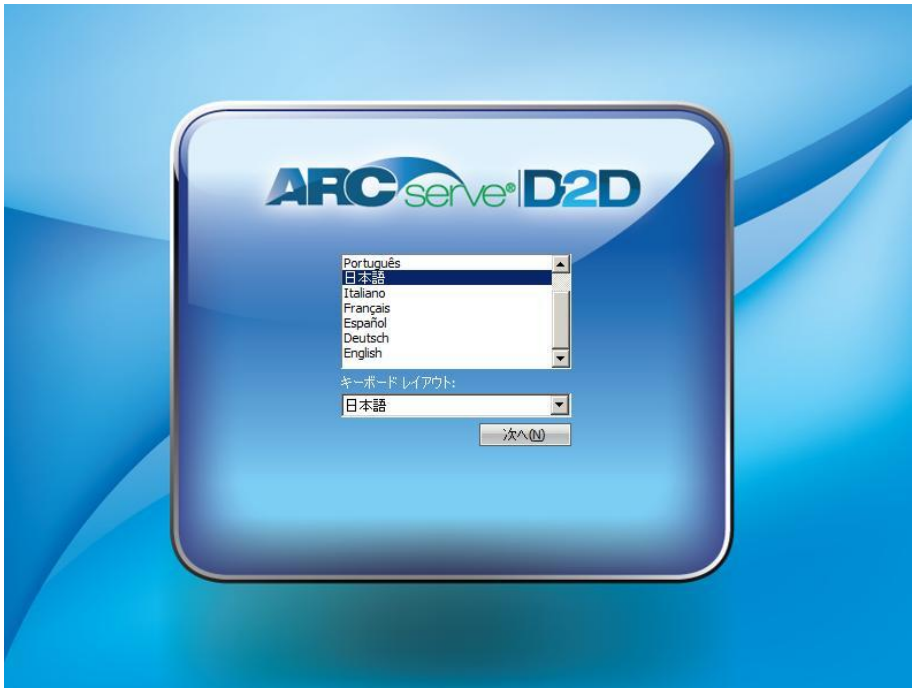
1. 保存したブートキット イメージ メディアを挿入し、コンピュータを起動します。
   - CD/DVD に書き込まれた BMR ISO イメージを使用する場合は、保存された CD/DVD を挿入します。
   - USB メモリに書き込まれた BMR ISO イメージを使用する場合は、保存された USB メモリを挿入します。

   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で、CD-ROM ドライブのオプションか USB のオプションを選択してブート プロセスを起動します。アーキテクチャ（x86/x64）を選択し、Enter キーを押して続行します。



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。



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。

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 を使用した回復**

     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 仮想スタンバイ 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 仮想スタンバイ 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 を使用した回復**

     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 仮想スタンバイ 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 仮想スタンバイ 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。

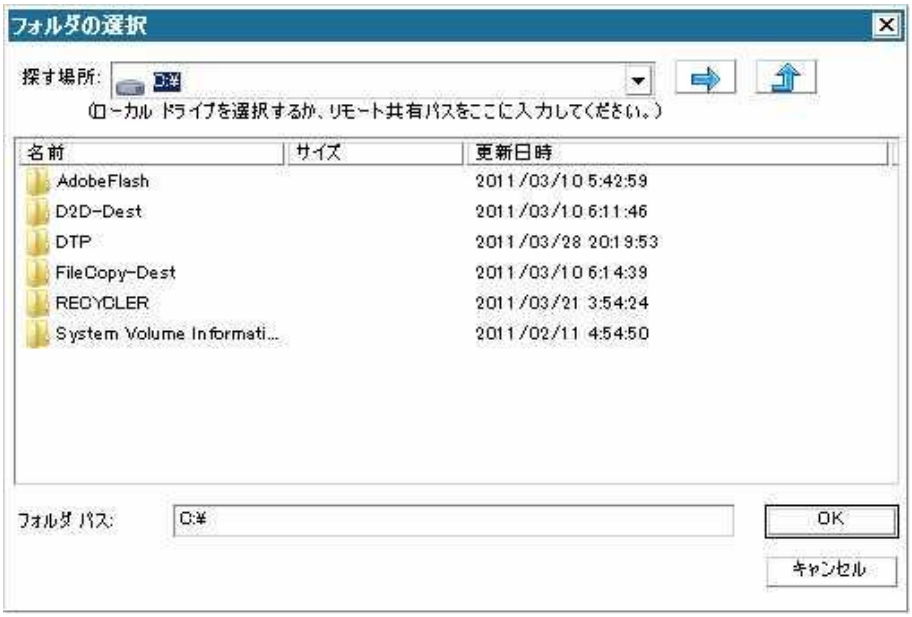
   CA ARCserve D2D を使用すると、任意のローカル ドライブまたはネットワーク共有から復旧を実行できます。

   - 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: サポート対象のオペレーティング システムであれば、UEFI マシンで取得したバックアップから BIOS 互換マシンへ、また BIOS マシンから UEFI 互換マシンへの BMR の実行が可能です。 ファームウェア変換がサポートされるシステムの完全なリストについては、「UEFI/BIOS 変換をサポートするオペレーティング システム」を参照してください。

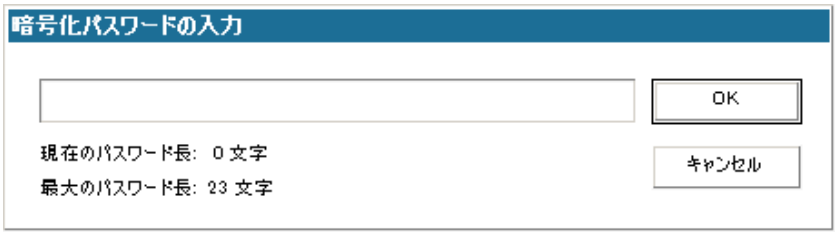
   - ファームウェア変換をサポートしないオペレーティング システムで UEFI システムでの BMR を実行するには、コンピュータを UEFI モードで起動する必要があります。 BMR は、異なるファームウェアを持つコンピュータのリストアをサポートしていません。ブート ファームウェアが BIOS ではなく UEFI であることを確認するには、［ユーティリティ］-［バージョン情報］をクリックします。
   - ファームウェア変換をサポートするオペレーティング システムでは、リカバリ ポイントの選択後に、ソース マシンのファームウェアがユーザのシステムと同一でないことが検出されると、UEFI を BIOS 互換のシステムに変換するか、または BIOS を UEFI 互換のシステムに変換するかを確認されます。


ARCserve D2D
Bare Metal Recovery
CA ARCserve D2D ベア メタル復旧 (BMR)
- 復旧ポイントを選択します
上部ペインには、すべてのバックアップ済みマシンとバックアップ先が表示されます。マシンをクリックすると、下部ペインに関連する復旧ポイントが表示されます。続行するには、復旧ポイントを選択してください。
注: デフォルトでは、ローカル ボリュームから検出されたバックアップ済みマシンのみがここにリストされます。新しいリムーバブル ディスクを接続または接続解除した後、[更新] をクリックするとマシン リストを更新することができます。
また、[参照]をクリックすると、リモート共有フォルダからバックアップ済みマシンを追加することもできます。
リモート共有フォルダを参照できない場合、NIC ドライバがインストールされていないか、IP アドレスが間違っている可能性があります。必要な場合には、以下を実行できます:
1 個のネットワーク アダプタが検出されました
Intel(R) PRO/1000 MT Network Connection
- IP アドレス: 155.35.128.63
- ステータス: 接続済み
以下のバックアップ済みマシンが検出されました:
<マシン名>
バックアップ情報
ホスト名:
<マシン 名>
OS:
Windows Server 2008 R2
プラットフォーム:
X64
更新(R)
参照(W)
指定したマシンに以下の復旧ポイントが検出されました。復旧ポイントを 1 つ選択した後、続行してください:
2012/04/17
0:48:34
2012/04/16
バックアップの種類:
- フル バックアップ
バックアップ先 (現在のシステムから検出):
-
バックアップの説明:
-
ブート ファームウェア:
- UEFI
ユーティリティ(U)
戻る(B)
次へ(N)
中止(A)

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。



   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。

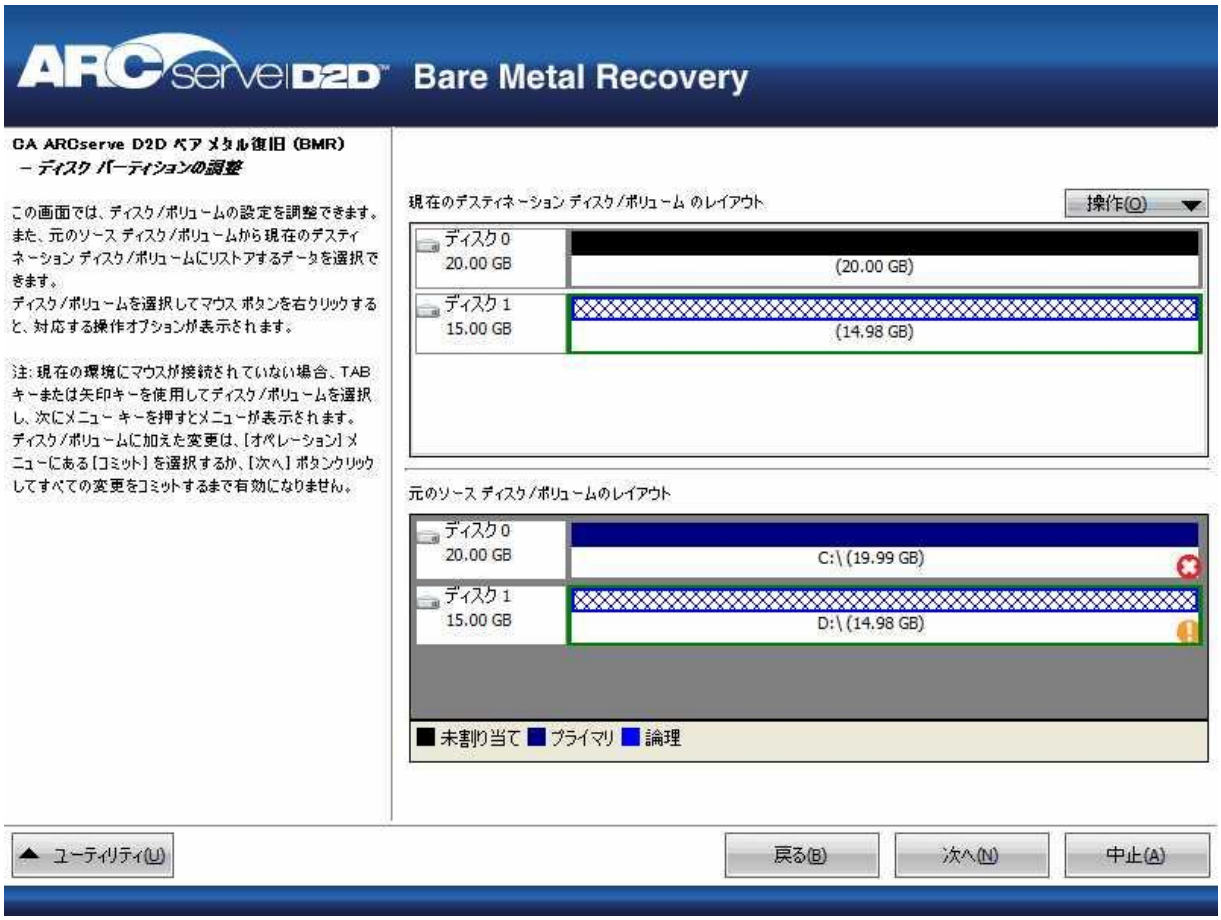
    BMR ユーティリティによって復旧するマシンの検索が開始され、対応するディスク パーティション情報が表示されます。

    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。

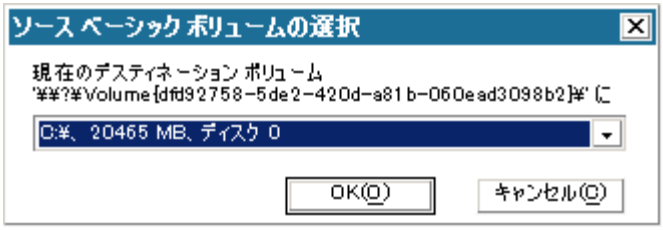


13. 表示されている現在のディスク情報が正しくない場合、［ユーティリティ］メニューにアクセスし、必要なドライバを確認することができます。

14. 必要に応じて、ターゲット ディスク/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。 これらのオプションの詳細については、「BMR 操作メニューの管理」を参照してください。

15. 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。

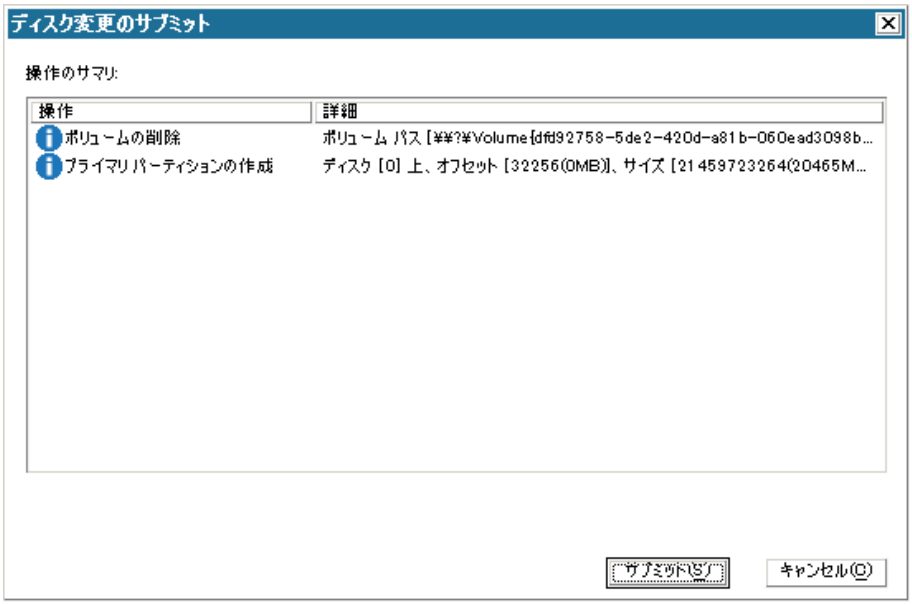


16. ［ソース ベーシック ボリュームの選択］ダイアログ ボックスから、ドロップダウン メニューをクリックして利用可能なソース ボリュームを選択し、選択したターゲット ボリュームに割り当てます。 ［OK］をクリックします。

    - 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)。

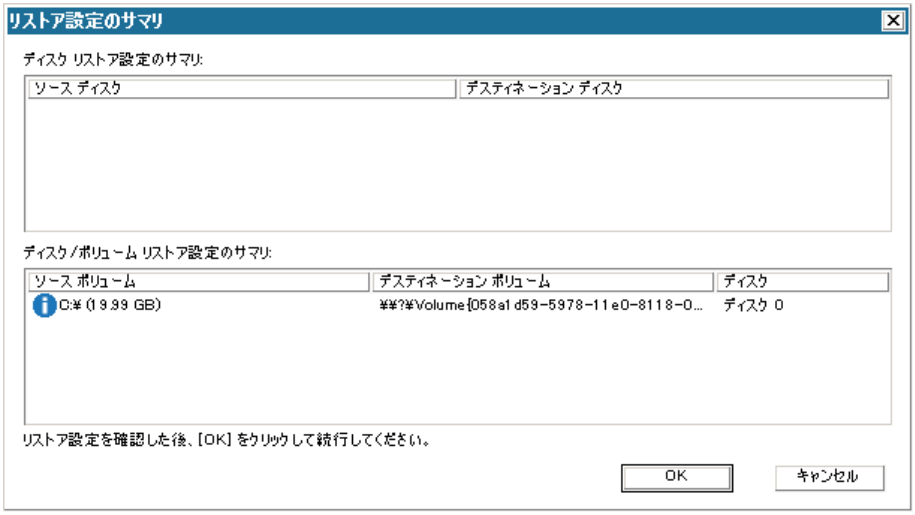
    注: ハード ドライブへのすべての操作は、サブミットするまで適用されません。

    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。

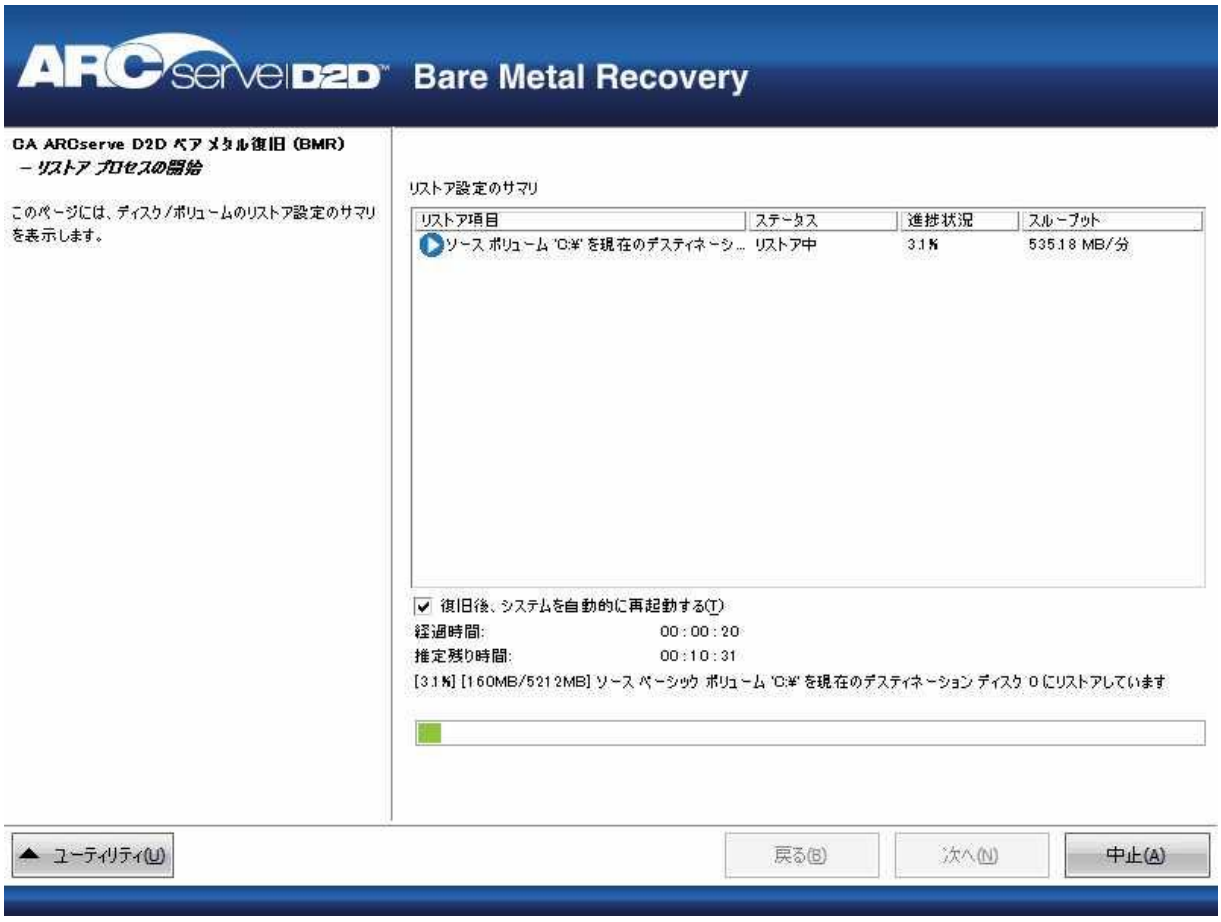
    注: リストア サマリ ウィンドウの下部にある「デスティネーション ボリューム」列に表示されるドライブ文字は、WinPE （Windows Preinstallation Environment）から自動的に生成されます。 これらのドライブ文字は、「ソース ボリューム」列に表示されるドライブ文字とは異なる場合があります。 ただし、ドライブ文字が異なっている場合でも、データは適切なボリュームにリストアされます。



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¥dr¥log

    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。

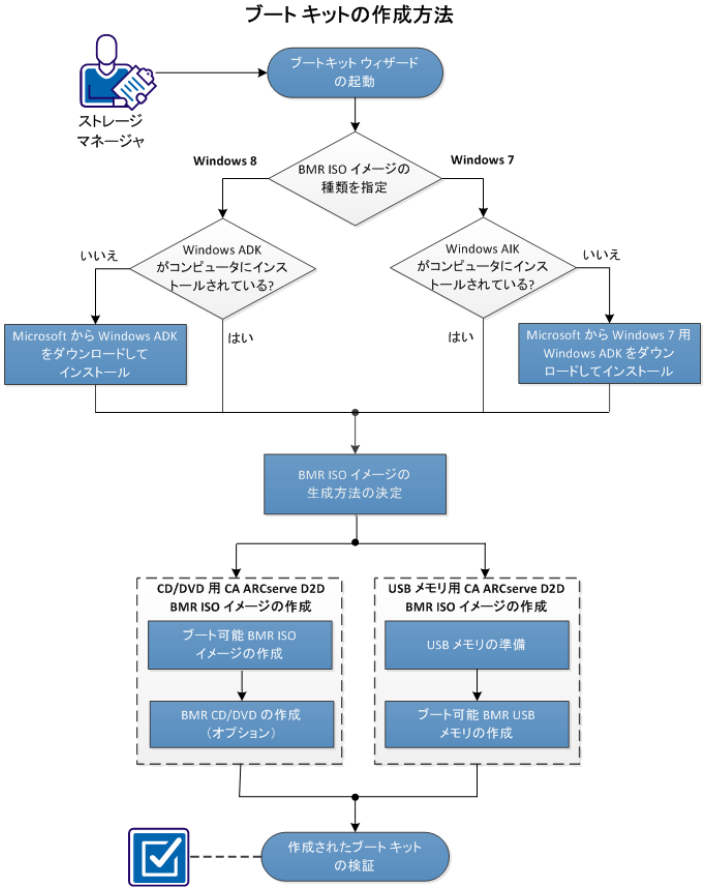
注: BMR の完了後に以下を行ってください。

- 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。
- マシンの再起動中、［Windows エラー回復処理］画面が表示され、Windows が正常にシャットダウンされなかったことが通知される場合があります。これが発生しても、警告を無視して続行すれば、Windows を通常どおり起動できます。
- 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 キットの作成方法

CA ARCserve D2D では、ブート キット ユーティリティを利用して WinPE（Windows Preinstallation Environment）イメージと CA ARCserve D2D イメージを組み合わせて BMR ISO イメージを作成します。 この ISO イメージがブート可能メディアに書き込まれます。ベア メタル復旧を実行する場合、CA ARCserve D2D ブート可能メディア（CD/DVD または USB メモリ）を使用して新しいコンピュータ システムを初期化し、ベア メタル復旧プロセスを開始できるようにします。

以下の図に、ブート キットの作成プロセスを示します。



ブート キットを作成するには以下の作業を実行します。

1. ブートキット ウィザードの起動 (P. 203)
2. BMR ISO イメージの生成方法の決定 (P. 206)
3. CD/DVD 用 CA ARCserve D2D BMR ISO イメージの作成 (P. 207)
   a. ブート可能 BMR ISO イメージの作成 (P. 207)
   b. （オプション）BMR CD/DVD の作成 (P. 210)
4. USB メモリ用 CA ARCserve D2D BMR ISO イメージの作成 (P. 210)
   a. USB メモリの準備 (P. 211)
   b. ブート可能 BMR USB メモリの作成 (P. 214)
5. 作成されたブート キットの検証 (P. 216)

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。

CA サポート： ブート キットの作成方法

YouTube： ブート キットの作成方法

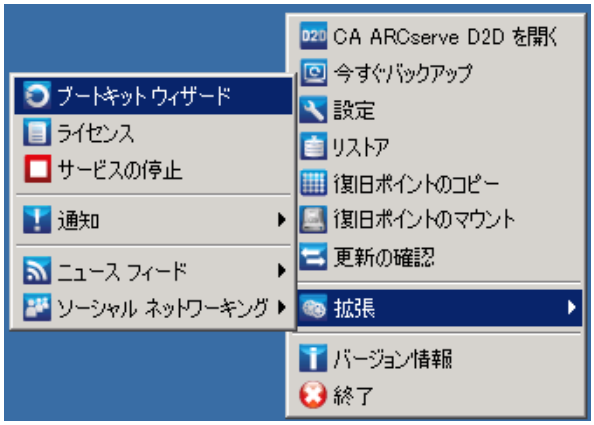
ブートキット ウィザードの起動

CA ARCserve D2D では、「ベア メタル復旧用のブート キットの作成」ユーティリティを使用して、WinPE-based ISO イメージを生成できます。 この ISO イメージには、ベア メタル復旧（BMR）の実行に必要な情報がすべて含まれています。

次の手順に従ってください:

1. ［ブートキット ウィザード］ユーティリティは、［システム トレイ モニタ］の［拡張］オプション、または［スタート］メニューから起動できます。

   ［ブートキット ウィザード］ユーティリティが起動し、［BMR ISO イメージの種類を指定］画面が表示されます。



2. 作成する BMR ISO イメージの種類（Windows 8 または Windows 7）を指定し、［次へ］をクリックします。

   注: Windows XP、Windows Vista および Windows Server 2003 については、BMR ISO イメージの作成はサポートされていません。 これらのオペレーティング システムについては、Windows Vista SP1、Windows 2003 SP2 または Windows の以降のバージョンを使用して BMR ISO イメージを作成できます。

   - **Windows 8**

     ユーティリティは、起動するとすぐにコンピュータをチェックし、Windows アセスメント & デプロイメント キット（ADK）がすでにインストールされているかどうかを調べます。 Windows ADK は、Windows オペレーティング システムをコンピュータに展開するための Microsoft ツールです。

     注: Windows ADK は、以下のオペレーティング システムを実行しているコンピュータにインストールできます。

     - Windows 7
     - Windows Server 2008
     - Windows Server 2008 R2
     - Windows 8
     - Windows Server 2012

- **Windows 7**

  ユーティリティは、起動するとすぐにコンピュータをチェックし、Windows 自動インストール キット（AIK）がすでにインストールされているかどうかを調べます。Windows AIK は、Windows オペレーティング システムをコンピュータに展開するための Microsoft ツールです。

  注: Windows 7 用の Windows AIK は、以下のオペレーティング システムを実行しているコンピュータにインストールできます。

  - Windows 2003 SP2
  - Windows Vista SP1
  - Windows 7
  - Windows Server 2008
  - Windows Server 2008 R2

3. ブート可能 ISO イメージを作成するには、コンピュータに Windows ADK または Windows AIK （該当する場合）がインストールされている必要があります。

   a. Windows ADK（または AIK）がインストールされている場合、［ブートキット方式の選択］画面が表示され、ブートキットを作成できます。

   b. Windows ADK （または AIK）がインストールされていない場合、該当する Windows 情報画面が表示されます。Microsoft ダウンロード センターから Windows ADK （または AIK）をダウンロードし、インストールする必要があります。

      注: Windows ADK（または AIK）のインストールの詳細については、以下の Web サイトを参照してください。

      - Windows ADK のインストール
      - Windows 7 用 Windows AIK のインストール

      Windows ADK（または AIK）は、以下のいずれかの方法でインストールできます。

      - インストール メディアを Microsoft の Web サイトから直接ダウンロードし、Windows ADK （または AIK）をコンピュータにインストールします。
      - 情報画面のリンクをクリックして Microsoft の Web サイトを開き、Windows ADK（または AIK）をダウンロードしてコンピュータにインストールします。

Windows ADK（または AIK）のインストールが完了したら、［次へ］をクリックします。［ブートキット方式の選択］画面が表示され、ブートキットを作成することができます。

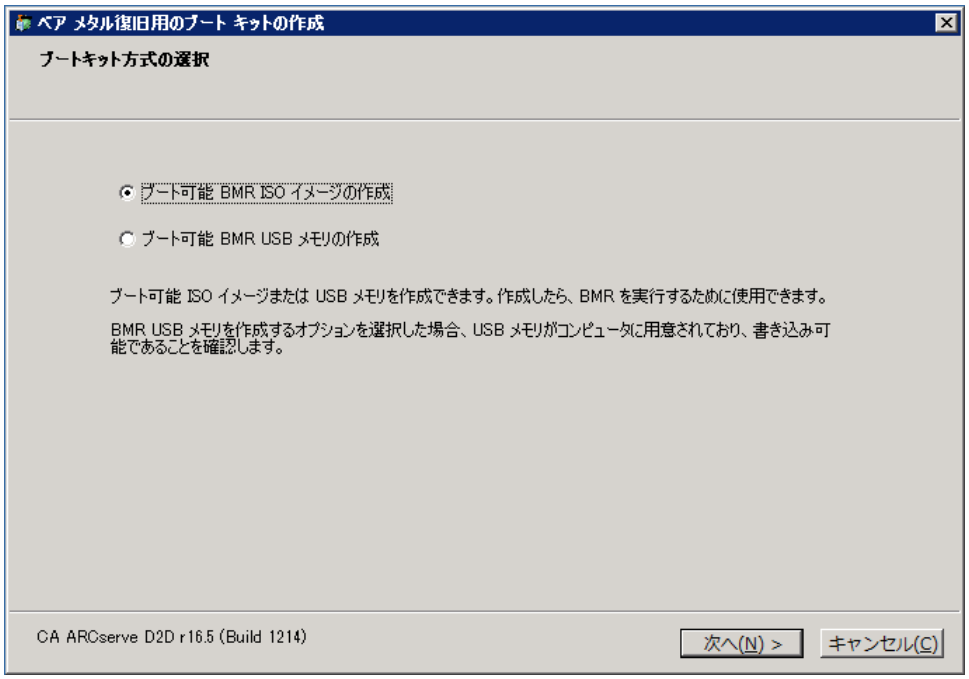
注: Windows ADK をインストールする場合、ブートキットの作成をサポートする以下の機能が必要です。

- Deployment Tools
- Windows PE （Windows Preinstallation Environment）

注: Windows AIK インストールについては、Windows AIK のセットアップを選択します。

BMR ISO イメージの生成方法の決定

ブートキット ウィザード ユーティリティでは、2 つの方法で ISO イメージを生成できます。



- ブート可能 BMR ISO イメージの作成 (P. 207)

  この方法では、ISO イメージを作成し、保存用の CD/DVD に書き込みます。デフォルトでは、このオプションが選択されています。詳細については、「CD/DVD 用 CA ARCserve D2D BMR ISO イメージの作成 (P. 207)」を参照してください。

- ブート可能 BMR USB メモリの作成 (P. 214)

  この方法では、ISO イメージを作成し、携帯可能な保存用 USB メモリに直接書き込みます。詳細については、「USB メモリ用 CA ARCserve D2D BMR ISO イメージの作成 (P. 210)」を参照してください。

次に、いずれかのブート可能メディアを使用して、新しいコンピュータ システムを初期化し、ベア メタル リカバリ プロセスを開始できるようにします。保存されたイメージが常に最新のバージョンであるようにしておくために、CA ARCserve D2D を更新する度に新しい ISO イメージを作成することをお勧めします。

注: 仮想マシン (VM) 上で BMR を実行する場合、ISO イメージを CD/DVD に書き込まずに、直接 VM に接続し、BMR プロセスを開始することも可能です。

CD/DVD 用 CA ARCserve D2D BMR ISO イメージの作成

CA ARCserve D2D BMR ISO イメージは、以下の手順で作成します。

- ブート可能 BMR ISO イメージの作成 (P. 207)
- BMR CD/DVD の作成 (P. 210)

ブート可能 BMR ISO イメージの作成

BMR ISO イメージの作成を選択した場合は、このイメージをブート可能メディア (CD または DVD) に書き込んで新しいコンピュータ システムを初期化し、ベア メタル復旧プロセスを開始できるようにします。

次の手順に従ってください:

1. [ブートキット方式の選択] 画面で [ブート可能 BMR ISO イメージの作成] を選択し、[次へ] をクリックします。

   [プラットフォームとデスティネーションの選択] ダイアログ ボックスが表示されます。

2. ISO イメージのプラットフォームを選択します。

   2 つのうちのいずれか、または両方を選択できます。 両方のプラットフォームを選択すると、イメージの作成に要する時間が長くなります。

   注: 32 ビット プラットフォームから作成された ISO イメージは、32 ビット サーバをリストアする場合にのみ使用します。 64 ビット プラットフォームから作成された ISO イメージは、64 ビット サーバをリストアする場合にのみ使用します。UEFI ファームウェア システムを起動する場合は、x64 プラットフォーム オプションを選択してください。

   使用可能なオプションは、以下のとおりです。

   - x86 プラットフォーム用 BMR ISO イメージ（のみ）。
   - x64 プラットフォーム用 BMR ISO イメージ（のみ）。
   - x86 および x64 の両方のプラットフォーム用 BMR ISO イメージ。

3. デスティネーションを指定します。

   BMR ISO イメージ ファイルを作成および保存する場所を指定または参照します。

4. 生成する BMR ISO イメージ ファイルの名前を指定します。

5. プラットフォームと場所を指定したら、［次へ］をクリックします。

   ［言語の選択］ダイアログ ボックスが表示されます。

6. 生成した BMR ISO イメージで使用する言語を選択します。BMR の作業中、ユーザ インターフェースとキーボードには選択した言語が適用されます。

   BMR ISO イメージでは、1 つ以上の言語を選択できます。 ただし、選択する言語が 1 つ増えるごとに、イメージの作成にかかる時間もそれだけ長くなります。 選択した言語が増えると、完了までの時間も長くなります。 そのため、本当に必要な言語のみを選択することを推奨します。

7. ［次へ］をクリックします。

   ［ドライバの指定］ダイアログ ボックスが表示されます。

8. ドライバを指定します。指定したドライバは、BMR ISO イメージに統合するドライバ用のドライバ リストに表示されます。

   有効化されたドライバ ペインで、任意のドライバを追加、または BMR ISO イメージから削除できます。

   注: VirtualBox Host-Only Ethernet Adapter ドライバを BMR ISO イメージに統合する場合、Windows ADK コンポーネントとの間に競合が発生する場合があります。 競合を回避するため、BMR ISO イメージにこのドライバを統合しないことをお勧めします。

   a. ローカル ドライバを含む : ローカルのクリティカルなデバイス ドライバ（NIC、FC または SCSI 用 OEM ドライバのみ）をドライバ リストにロードします。クリックすると、このコンピュータ用の BMR ISO イメージに追加する必要があるクリティカル デバイス ドライバがあるかどうかを確認します。クリティカル デバイス ドライバが見つかった場合、自動的にリストに追加されます。

   b. ドライバの追加 : ドライバ リストに追加するドライバを参照します。

   c. ドライバの削除 : BMR ISO イメージに追加したくないドライバを、リストから選択して削除します。

9. ［作成］をクリックしてプロセスを起動し、ブート可能 BMR ISO イメージを作成します。

   処理中は、ステータスが表示されます。

10. 処理が完了すると確認画面が表示され、BMR ISO イメージが正常に生成されたことが示されます。 この画面では、イメージの場所とプラットフォームが表示されます。また、リンクをクリックすると、イメージの場所が参照されます。

BMR CD/DVD の作成

ISO イメージを作成し、場所を指定して保存したら、ブート可能 CD または DVD にイメージを書き込む必要があります。 このブート可能メディアを使用して、新しいコンピュータ システムを初期化し、ベア メタル復旧（BMR）プロセスを開始できるようにします。

保存した ISO イメージが常に最新のバージョンであるようにしておくために、以下を行う必要があります。

- CA ARCserve D2D を更新するたびに、ISO イメージを新規作成する必要があります。
- ISO イメージをリモートの場所に保存した場合は、BMR を実行する必要がある場合にのみ、CD/DVD に書き込みます。
- 複数のコンピュータに CA ARCserve D2D をインストールしている場合は、イメージに最新の CA ARCserve D2D の更新が含まれるように、更新状態が最新のコンピュータから ISO イメージ（および CD/DVD）を新規作成し、BMR を実行します。

USB メモリ用 CA ARCserve D2D BMR ISO イメージの作成

CA ARCserve D2D BMR USB メモリは、以下の手順で作成します。

USB メモリの準備 (P. 211)

ブート可能 BMR USB メモリの作成 (P. 214)

USB メモリの準備

BMR ISO イメージを USB メモリに書き込む前に、USB メモリの準備が必要です。 ブート可能 USB BMR メモリを作成するには、USB メモリがシステムを起動できるよう、アクティブ化されている必要があります。 DiskPart コマンドを使用して、USB メモリをアクティブにすることができます。

重要: USB メモリをフォーマットする必要がある場合、フォーマットにより、USB メモリに保存されているすべてのデータは消去されます。この処理を行う前に、USB メモリ上に重要なデータが存在しないことを確認してください。USB メモリがすでにフォーマットされている場合は、この処理により、同じ名前のファイルはすべて上書きされます。

次の手順に従ってください:

1. コマンド プロンプトを開きます(OS によって要求される場合は管理者権限のアカウントで開きます)。
2. 「**Diskpart**」と入力し、Enter キーを押します。
3. 「**List Disk**」と入力し、Enter キーを押します。

   検出されたすべてのディスクが一覧表示されます。 表示されたディスクの中から、USB ディスクを決定します。
4. 「**Select Disk <n>**」(「n」は USB ディスクのディスク番号)と入力して USB ディスクを選択し、Enter キーを押します。
5. 「**Clean**」と入力し、Enter キーを押します。

   「DiskPart はディスクを正常にクリーンな状態にしました。」というメッセージが表示されます。
6. 「**create partition primary**」と入力し、Enter キーを押します。

   「DiskPart は指定したパーティションの作成に成功しました。」というメッセージが表示されます。
7. 「**select partition 1**」と入力し、Enter キーを押します。

   「パーティション 1 が選択されました。」というメッセージが表示されます。
8. 「**active**」と入力し、Enter キーを押します。

   「DiskPart は現在のパーティションをアクティブとしてマークしました。」というメッセージが表示されます。
9. 必要に応じて、USB メモリを FAT32 または NTFS ファイル システムでフォーマットします。

「**format fs=fat32 quick**」または「**format fs=ntfs quick**」と入力します。

USB メモリは使用できる状態になりました。

```
C:\Windows\System32>diskpart

Microsoft DiskPart version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: <computer name>

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          465 GB  1024 KB   *
  Disk 1    Online         3745 MB      0 B

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART> create partition primary

DiskPart succeeded in creating the specified partition.

DISKPART> select partition 1

Partition 1 is now the selected partition.

DISKPART> active

DiskPart marked the current partition as active.

DISKPART> format fs=fat32 quick

  100 percent completed

DiskPart successfully formatted the volume.

DISKPART> exit_
```

ブート可能 BMR USB メモリの作成

ブート可能 BMR（ベア メタル復旧）USB メモリの作成を選択した場合は、ISO イメージを USB メモリに直接書き込み、新しいコンピュータ システムを初期化し、ベア メタル復旧プロセスを開始できるようにします。

次の手順に従ってください:

1. 必要に応じて、USB メモリを準備します。 詳細については、「USB メモリの準備 (P. 211)」を参照してください。
2. ［ブートキット方式の選択］画面で［ブート可能 BMR USB メモリの作成］を選択し、［次へ］をクリックします。

   ［プラットフォームとデスティネーションの選択］ダイアログ ボックスが表示されます。
3. ISO イメージのプラットフォームを選択します。

   2 つのうちのいずれか、または両方を選択できます。 両方のプラットフォームを選択すると、イメージの作成に要する時間が長くなります。

   注: 32 ビット プラットフォームから作成された ISO イメージは、32 ビット サーバをリストアする場合にのみ使用します。 64 ビット プラットフォームから作成された ISO イメージは、64 ビット サーバをリストアする場合にのみ使用します。UEFI ファームウェア システムを起動する場合は、x64 プラットフォーム オプションを選択してください。

   使用可能なオプションは、以下のとおりです。

   - x86 プラットフォーム用 BMR ISO イメージ（のみ）。
   - x64 プラットフォーム用 BMR ISO イメージ（のみ）。
   - x86 および x64 の両方のプラットフォーム用 BMR ISO イメージ。

4. USB ドライブを指定します。

   BMR ISO イメージ ファイルを作成し、USB メモリに書き込むためのドライブを指定または参照します。

   注: USB ドライブを使用して UEFI ファームウェア システムを起動する場合、USB ドライブは、FAT32 ファイル システムでフォーマットする必要があります。

5. 準備の整った USB メモリが指定したドライブに挿入されていることを確認してください。

6. プラットフォームと場所を指定したら、［次へ］をクリックします。

   ［言語の選択］ダイアログ ボックスが表示されます。

7. 生成した BMR ISO イメージで使用する言語を選択します。BMR の作業中、ユーザ インターフェースとキーボードには選択した言語が適用されます。

   BMR ISO イメージでは、1 つ以上の言語を選択できます。 ただし、選択する言語が 1 つ増えるごとに、イメージの作成にかかる時間もそれだけ長くなります。 選択した言語が増えると、完了までの時間も長くなります。 そのため、本当に必要な言語のみを選択することを推奨します。

8. ［次へ］をクリックします。

   ［ドライバの指定］ダイアログ ボックスが表示されます。

9. 必要に応じて、追加で統合するドライバ オプションを選択します。

   有効化されたドライバ ペインで、任意のドライバを追加、または BMR ISO イメージから削除できます。

10. ［作成］をクリックしてプロセスを起動し、ブート可能 BMR ISO イメージを作成します。

    処理中は、ステータスが表示されます。

11. 処理が完了すると確認画面が表示され、BMR ISO イメージが正常に生成され、USB メモリに書き込まれたことが示されます。この画面では、イメージの場所とプラットフォームが表示されます。また、リンクをクリックすると、イメージの場所が参照されます。

作成されたブート キットの検証

BMR ISO イメージが正常に作成されると、ブートキット ウィザード ユーティリティは、イメージが保存されている場所へのリンクを表示します。BMR ISO イメージがその場所に保存されていることを確認します。デフォルトでは、イメージは、以下のデフォルトのイメージ名フォーマットで Libraries/Documents フォルダに保存されます。

<PRODUCT>_BMR_<Platform>_<OS Kernel>_<version>(Build xxx).ISO

例:

D2D_BMR_x86x64_w8_r16.5 (Build 1234).ISO

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。

7. CA ARCserve D2D Web サービスを再起動します。

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¥Logs
```

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アプリケーションの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 からアプリケーションのインストール パスを読み取ります。

コンポーネント	説明
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、アプリケーションを 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アプリケーションの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 レジストリからアプリケーションの登録を解除します。
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。
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 /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対してアプリケーション ファイルのインストールと更新を行います。

  C:¥Program Files¥CA¥<アプリケーション名> （たとえば、ARCserve Central Applications または ARCserve D2D）

  アプリケーションは、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** -- インストール処理では、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¥<*アプリケーション名*> *（たとえば、ARCserve Central Applications または ARCserve D2D）*

  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++ 2010 SP1 Redistributable
  - JRE（Java Runtime Environment）1.7.0_06
  - Tomcat 7.0.29

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

バイナリ名	ソース
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 License
UpdateData.exe	CA License
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
tomcat7.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

アンチウイルス スキャンからのファイルの除外

アンチウィルス ソフトウェアによる、ファイル アクセスの一時的な妨害や、疑わしい、または危険であると識別されたファイルの検疫または削除によって、アプリケーションの円滑な処理が妨げられることがあります。ほとんどのアンチウイルス ソフトウェアでは、保護の不要なデータをスキャンしないように、特定のプロセス、ファイルまたはフォルダを対象から除外するように設定できます。 バックアップとリストアや、他の処理が妨害されないように、アンチウイルス ソフトウェアを設定することは重要です。

以下のプロセス、フォルダおよびファイルは、アンチウイルスによるスキャンから除外する必要があります。

- プロセス リスト
  - C:¥Program Files¥CA¥ARCserve Central Applications¥BIN¥CCIConfigSettings.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥BIN¥CfgUpdateUtil.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥BIN¥DBConfig.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥BIN¥GetApplicationDetails.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥BIN¥GetApplicationDetails64.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥BIN¥GetVolumeDetails.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥BIN¥VixGetApplicationDetails.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥BIN¥VixGetVolumeDetails.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥BIN¥GetApplicationDetails64.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥Deployment¥Asremsvc.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥Deployment¥CheckProdInfo.exe
  - C:¥Program Files¥CA¥ARCserve Central Applications¥Deployment¥DeleteMe.exe

- C:¥Program Files¥CA¥ARCserve Central Applications¥Deployment¥SetupComm.exe
- C:¥Program Files¥CA¥ARCserve Central Applications¥Deployment¥RestartHost.exe
- C:¥Program Files¥CA¥ARCserve Central Applications¥Update Manager¥D2DAutoUpdateUninstallUtility.exe
- C:¥Program Files¥CA¥ARCserve Central Applications¥Update Manager¥D2DPMConfigSettings.exe
- C:¥Program Files¥CA¥ARCserve Central Applications¥Update Manager¥D2DUpdateManager.exe
- C:¥Program Files¥CA¥ARCserve Central Applications¥Update Manager¥UpgradeDataSyncupUtility.exe
- C:¥Program Files¥CA¥ARCserve Central Applications¥TOMCAT¥BIN¥tomcat7.exe
- C:¥Program Files¥CA¥ARCserve D2D¥TOMCAT¥JRE¥jre7¥bin
  - java.exe
  - Java-rmi.exe
  - javaw.exe
  - keytool.exe
  - rmid.exe
  - rmiregistry.exe
- C:¥Program Files (x86)¥CA¥SharedComponents¥CA_LIC
  - CALicnse.exe
  - CAminfo.exe
  - CAregit.exe
  - ErrBox.exe
  - lic98log.exe
  - lic98Service.exe
  - lic98version.exe
  - LicDebug.exe
  - LicRCmd.exe
  - LogWatNT.exe
  - mergecalic.exe

- mergeolf.exe

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 を使用するときに、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。

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。

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。