

CA ARCserve® Central 仮想スタ ンバイ

ユーザ ガイド

r16.5



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

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複写、譲渡、開示、変更、複本することはできません。本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、

(i) 本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

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

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

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

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

本ドキュメントの制作者は CA です。

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

Copyright © 2013 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

CA Technologies 製品リファレンス

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

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

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト (<http://www.ca.com/jp/support/>) 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 仮想スタンバイ 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。
- 「[リモート仮想スタンバイの CA ARCserve Replication/High Availability シナリオの作成](#) (P. 20)」が追加されました。このトピックでは、リモート仮想スタンバイ ポリシーを作成する場合に、CA ARCserve Replication/High Availability から CA ARCserve D2D および CA ARCserve Central Host-Based VM Backup シナリオを作成する方法について説明します。
- 「[CA ARCserve Replication からのノードのインポート](#) (P. 46)」が追加されました。このトピックでは、CA ARCserve Replication から複数ノードをインポートする方法について説明します。
- 「[リモート コンバータの設定](#) (P. 47)」が追加されました。このトピックでは、CA ARCserve D2D 復旧ポイントを変換して、Microsoft Hyper-V、VMware vCenter、または ESXi のいずれかに自動登録する方法について説明します。
- 「[CA ARCserve Central 仮想スタンバイ ポリシーの作成](#) (P. 47)」が更新されました。このトピックには、作成可能な 2 種類のポリシー、ローカル仮想スタンバイ ポリシーとリモート仮想スタンバイ ポリシーが追加されました。
- 「[ノード管理タスク](#) (P. 74)」が更新されました。このトピックには、[CA ARCserve Replication からのノードのインポート] オプションが追加されました。
- 「[1 つ以上の CA ARCserve D2D ノードのバックアップパスワードの設定](#) (P. 77)」が追加されました。このトピックでは、1 つ以上の CA ARCserve D2D バックアップパスワードを設定し、MSP サイト上のコンバータに転送する方法について説明します。
- 「[ポリシーの編集またはコピー](#) (P. 90)」が更新されました。このトピックには、編集またはコピーするために選択できる 2 種類のポリシーが追加されました。

- 「[ログの表示](#) (P. 100)」が更新されました。このトピックには、以下のモジュール オプションが追加されました：[ハートビートの一時停止/再開]、[仮想スタンバイの一時停止/再開]、[複数ノードの更新]、[スタンバイ VM]、および[CA ARCserve Replication からのノードのインポート]。
- 「[仮想スタンバイ VM の電源オン](#) (P. 133)」が追加されました。このセクションでは、[ローカル](#) (P. 133) または [リモート](#) (P. 141) で仮想スタンバイ VM の電源をオンにする機能について説明します。
- 「[BMR 操作メニューの管理](#) (P. 175)」が追加されました。このセクションでは、3 種類の BMR 操作について説明します。
- 「[IP/名前によるノードの追加時にアクセス拒否エラーが発生する](#) (P. 226)」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。
- 「[アンチウイルス スキャンからのファイルの除外](#) (P. 255)」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。

目次

第 1 章: CA ARCserve Central 仮想スタンバイ の概要	11
概要.....	12
CA ARCserve Central 仮想スタンバイ の動作.....	13
CA ARCserve Central Applications マニュアル選択メニュー	15
 第 2 章: CA ARCserve Central 仮想スタンバイ のインストール	 17
インストール タスクの前提条件	17
リモート仮想スタンバイの前提条件となるインストール タスク	19
インストールに関する考慮事項.....	28
CA ARCserve Central 仮想スタンバイ のインストール	30
CA ARCserve Central 仮想スタンバイ のアンインストール	33
CA ARCserve Central 仮想スタンバイ のサイレント インストール	34
CA ARCserve Central 仮想スタンバイ のサイレント アンインストール	37
 第 3 章: 仮想スタンバイ ポリシーの設定	 39
ノードのディスカバリ	39
IP アドレスまたはノード名によるノードの追加	40
ファイルからのノードのインポート	41
CA ARCserve Central Host-Based VM Backup サーバからのノードの追加	43
CA ARCserve Replication からのノードのインポート	46
CA ARCserve Central 仮想スタンバイ ポリシーの作成	47
ローカル仮想スタンバイ ポリシーの作成	48
リモート仮想スタンバイ ポリシーの作成	56
ノードのポリシーへの割り当て/割り当て解除.....	62
ポリシーの展開.....	65
 第 4 章: CA ARCserve Central 仮想スタンバイ の紹介	 67
CA ARCserve Central 仮想スタンバイ へのログイン	68
VMware ベース ノードの ESX Server または vCenter Server システムの指定	69
 第 5 章: CA ARCserve Central 仮想スタンバイ の使い方	 71
CA ARCserve D2D ノードへのログイン	71

モニタ サーバへのログイン	72
ノード メンテナンス タスク	74
ノードの更新.....	75
1 つ以上の CA ARCserve D2D ノードのバックアップ パスワードの設定	77
ノードの削除.....	80
ノードからのライセンスの解放.....	80
モニタ サーバからノードのモニタを停止	82
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	83
ノード グループ管理タスク	84
ノード グループの追加	84
ノード グループの変更	86
ノード グループの削除	87
ノード グループのフィルタ	88
Virtual Standby のポリシー管理タスク	89
ポリシーの編集またはコピー	90
ポリシーの削除.....	91
アプリケーション環境設定タスク	91
電子メール設定の環境設定	92
自動更新の設定.....	93
ソーシャル ネットワーキングの環境設定	97
管理者アカウントの変更	98
ログの表示.....	100
ナビゲーション バーへのリンクの追加	102
Virtual Standby ホーム画面	103
Virtual Standby ホーム画面の使用方法.....	103
サーバリストの使用方法.....	105
最新の仮想スタンバイ ジョブに関するサマリ情報の表示	105
仮想変換ジョブのステータスのモニタ	107
ソース サーバの仮想スタンバイ設定の表示	108
復旧ポイント スナップショットのリストの表示	109
CA ARCserve Central 仮想スタンバイ モニタリング タスク	109
ジョブに関するアクティビティ ログ データの表示	110
Virtual Standby サーバからの仮想スタンバイ ジョブに関するステータス情報の表示	114
CA ARCserve D2D ノードに割り当てられたポリシーに関する情報の表示	118
Virtual Standby サーバからの仮想スタンバイ ジョブの一時停止および再開.....	123
Virtual Standby サーバからのハートビートの一時停止および再開	126
サーバの通信プロトコルの変更	130

第 6 章: 仮想スタンバイ VM の電源オン 133

ローカル仮想スタンバイ VM の電源をオンにする方法	133
復旧ポイント スナップショットからの仮想スタンバイ VM の電源投入	134
電源がオンになった後の仮想スタンバイ VM の保護	140
リモート仮想スタンバイ VM の電源をオンにする方法	141
復旧ポイント スナップショットからのリモート仮想スタンバイ VM の電源投入	142
電源がオンになった後のリモート仮想スタンバイ VM の保護	149
電源をオンにする NIC の数をアプリケーションが決定する方法	150
電源がオンになった仮想スタンバイ VM の保護方法	152

第 7 章: データのリストア 155

CA ARCserve D2D 復旧ポイントからのデータのリストア	156
CA ARCserve D2D ファイル コピーからのデータのリストア	161
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	167
ベア メタル復旧を使用したソース サーバの復旧	173
BMR 操作メニューの管理	175
Hyper-V 仮想スタンバイ VM からのデータを使用したソース サーバの復旧	180
VMware 仮想スタンバイ VM からのデータを使用したソース サーバの復旧	187
Microsoft Exchange 電子メール メッセージのリストア	194

第 8 章: CA ARCserve Central 仮想スタンバイ のトラブルシューティング 205

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	206
空の Web ページが表示される、または、JavaScript エラーが発生する	209
ページのロード問題のトラブルシューティング方法	212
CA ARCserve D2D ノードおよびモニタ サーバへのログイン時に Web ページが正しくロードされない	213
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	215
CA ARCserve D2D Web サービスが CA ARCserve D2D ノード上で失敗する	216
CA ARCserve D2D Web サービスの実行が遅い	219
CA ARCserve Central 仮想スタンバイ 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	221
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	222
ノードの追加時に無効な認証情報メッセージが表示される	224
Windows XP での無効な認証情報メッセージ	225
IP/名前によるノードの追加時にアクセス拒否エラーが発生する	226
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	228

オペレーティング システムが見つからないエラー	229
Hyper-V システムへの仮想スタンバイ ジョブが失敗する	230
仮想スタンバイ ジョブが内部エラーのために失敗する	231
ホット追加転送モードを使用した仮想スタンバイ ジョブが失敗する	234
仮想スタンバイ ジョブがセッションなしの警告メッセージで終わる	237
バックアップ/復旧ジョブが SAN 転送モードを使用しない	238
ホット追加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ディスクがマウントできない	239
トラブルシューティングのエラー番号	240
Internet Explorer 8、9、Chrome で追加した新しいタブのリンクが正しく起動しない	241
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	245
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	246
仮想マシンの電源が自動的にオンにならない	247
CA ARCserve Central 仮想スタンバイ がノードと通信できない	247
リモート変換の準備エラー。VSS スクリプト作成の失敗	248

第 9 章: ベスト プラクティスの適用 249

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	249
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	251
埋め込みマニフェストを含まないバイナリ ファイル	252
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	253
アンチウイルス スキャンからのファイルの除外	255
CA ARCserve Central 仮想スタンバイ のライセンス方法	258

用語集 261

第 1 章: CA ARCserve Central 仮想スタンバイ 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. 12)

[CA ARCserve Central 仮想スタンバイ の動作](#) (P. 13)

[CA ARCserve Central Applications マニュアル選択メニュー](#) (P. 15)

概要

CA ARCserve Central Applications は、コア データ保護および管理テクノロジーと、併せて動作するターゲット アプリケーションのエコシステムとを組み合わせ、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 Applications によって提供されるアプリケーションの 1 つに CA ARCserve Central 仮想スタンバイ があります。CA ARCserve Central 仮想スタンバイ は CA ARCserve D2D と統合され、CA ARCserve D2D バックアップセッションから仮想マシンをプロビジョニングすることができます。このアプリケーションを使用して、以下を行うことができます。

- スケジュールに基づいて、CA ARCserve D2D デスティネーションデバイス上に保存されている CA ARCserve D2D 復旧ポイントを、VMware Virtual Disk (VMDK) または Microsoft 仮想ハードディスク (VHD) フォーマットに変換します。ソース サーバが失敗した場合に、復旧ポイントスナップショットから、仮想マシンが CA ARCserve D2D ソース サーバとして機能するように設定することができます。
- 変換ポリシーを CA ARCserve D2D ソース サーバにプッシュします。
- 復旧ポイント スナップショットを VMware ESX Server ベースまたは Windows Hyper-V ベースの仮想マシンに保存します。
- 緊急事態が発生した場合、手動または自動で仮想マシンの電源を投入します。
- 復旧ポイント スナップショットからデータを元のまたは別のソースサーバ (V2P 復旧) に回復します。

CA ARCserve Central 仮想スタンバイの動作

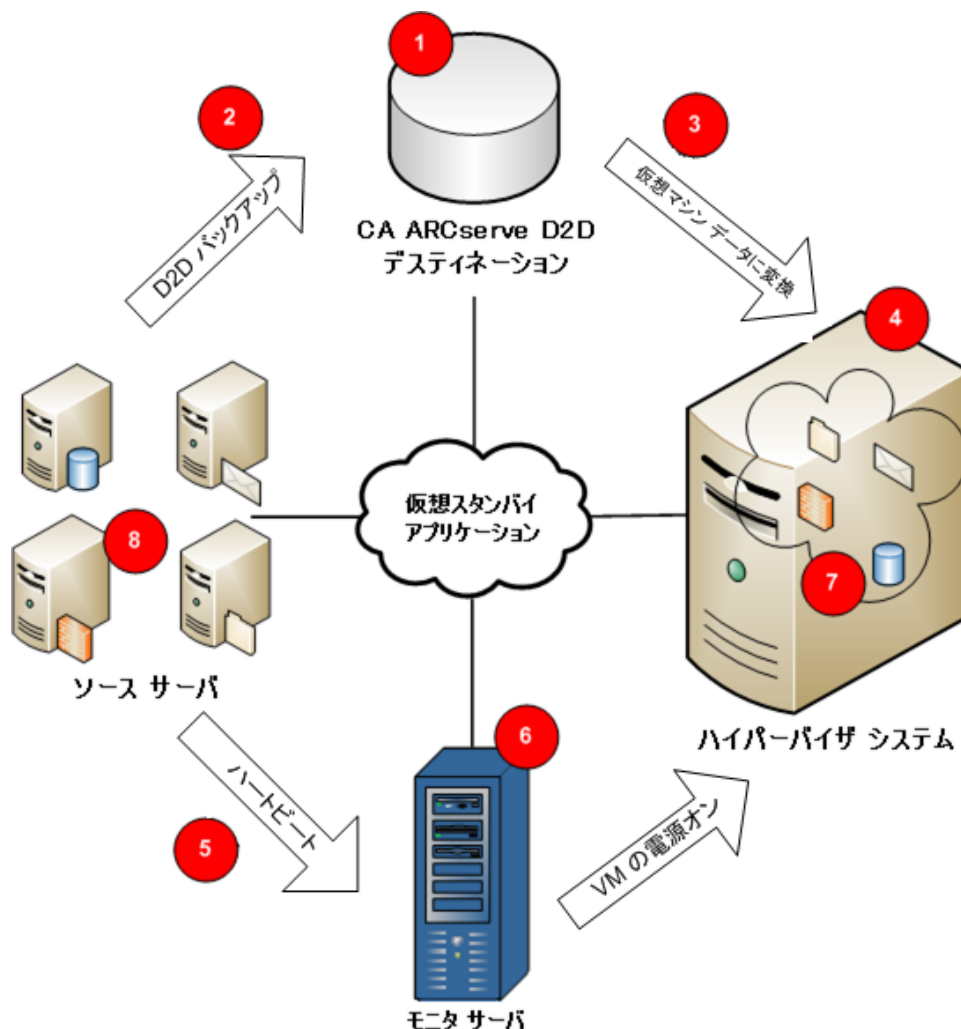
Virtual Standby では、以下により、環境内で動作する CA ARCserve D2D ソース サーバを保護できます。

- スケジュールに基づいて、CA ARCserve D2D デスティネーションデバイス上に保存されている CA ARCserve D2D 復旧ポイントを、VMware Virtual Disk (VMDK) または Microsoft 仮想ハードディスク (VHD) フォーマットに変換します。
- 変換データをハイパーバイザー システムへコピーします。
- 仮想マシンの VMDK または VHD データから復旧ポイント スナップショットを作成します。
- ソース サーバの状態をモニタします。
- 緊急事態が検出された場合に、復旧ポイント スナップショットから自動的に仮想マシンの電源を投入します。

注: Virtual Standby では問題が発生した場合に、復旧ポイント スナップショットを自動的にあるいは手動で電源を投入するように設定できます。

- ソース サーバの問題を修正後、仮想マシンからソース サーバへデータを復旧します。

以下の図は、このプロセスを表しています。



CA ARCserve D2D (1)はソース サーバの CA ARCserve D2D デスティネーション デバイス (2) に復旧ポイントを作成します。Virtual Standby は復旧ポイントを仮想マシンフォーマット (3) に変換し、ハイパーバイザー システム (4) 上に復旧ポイント スナップショットとしてデータを保存します。

モニタ サーバ (6) は、ソース サーバの状態をモニタします。モニタ サーバがソース サーバ (8) からのハートビート (5) を検出できない場合、モニタ サーバは、最新の復旧ポイント スナップショットのデータを使用して、ハイパーバイザー システム (4) 上のシンプロビジョニングされた仮想マシン (7) の電源を投入し、ソース サーバとして機能させます。CA ARCserve Central 仮想スタンバイは、ソース サーバと同じサイズの仮想マシンパーティションを作成します。

ソース サーバ上の問題を修正後、ハイパーバイザー システム上の VM に保存されるデータ (7) を使用して、最新の状態へソース サーバ (8) を復旧できます。

注: 仮想マシンの電源がオンになった後にバックアップするには、CA ARCserve Central Protection Manager を使用して CA ARCserve D2D バックアップ ポリシーを仮想マシンに展開できます。

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 仮想スタンバイのインストール

このセクションには、以下のトピックが含まれています。

[インストール タスクの前提条件 \(P. 17\)](#)

[インストールに関する考慮事項 \(P. 28\)](#)

[CA ARCserve Central 仮想スタンバイ のインストール \(P. 30\)](#)

[CA ARCserve Central 仮想スタンバイ のアンインストール \(P. 33\)](#)

[CA ARCserve Central 仮想スタンバイ のサイレントインストール \(P. 34\)](#)

[CA ARCserve Central 仮想スタンバイ のサイレントアンインストール \(P. 37\)](#)

インストール タスクの前提条件

CA ARCserve Central 仮想スタンバイ をインストールする前に、以下の前提条件タスクを完了する必要があります。

- CA ARCserve D2D のサポートされた最新リリースが以下にインストールされていることを確認します。

- 保護するソース サーバ
- 復旧ポイント スナップショットを保存するためのサーバ

注: この要件が適用されるのは、ノード（物理的または仮想マシン）の状態をモニタし、それらのノードの復旧ポイント スナップショットを格納するように設定されている HYper-V サーバに対してのみです。

- ソース サーバをモニタするためのサーバ

注: CA ARCserve Central Protection Manager を実稼働環境にインストールした場合、D2D 展開を使用してリモート ノードに CA ARCserve D2D をインストールできます。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。

- Hyper-V 環境の場合、CA ARCserve D2D が Hyper-V ホスト システムにインストールされていることを確認します。Hyper-V 環境では、Hyper-V ホスト システムが、復旧ポイント スナップショットの格納場所として、およびモニタ サーバとして機能します。

- VMware 環境の場合、CA ARCserve D2D がプロキシ システムにインストールされていることを確認します。

注: VMware 環境では、ターゲット ESX Server データ ストアは復旧ポイント スナップショットのストレージ場所として機能します。プロキシシステムは、オプションでモニタ サーバとして機能させることができます。

- リリース ノート ファイルを確認します。リリース ノート ファイルには、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、およびこのリリースで存在する既存の問題のリストが含まれています。
- お使いのシステムが、CA ARCserve Central 仮想スタンバイ のインストールに必要なハードウェアおよびソフトウェアの最小要件を満たしていることを確認します。
- お使いの Windows アカウントが、CA ARCserve Central 仮想スタンバイ をインストールするコンピュータに対する管理者権限、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の権限を持っていることを確認します。
- お使いのアカウントが、VMware vCenter または ESX Server の管理者権限、および Windows 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ためには、vCenter Server システムまたは ESX Server システムでアカウントに Global License の役割が必要です。
- CA ARCserve Central 仮想スタンバイ 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。
- 環境内のソース コンピュータをモニタするコンピュータのホスト名または IP アドレスを把握していることを確認します。
- 環境内の復旧ポイント スナップショットを保存するコンピュータのホスト名または IP アドレスを把握していることを確認します。
- CA ARCserve Central 仮想スタンバイ をインストールするために必要なライセンスがすべて利用可能であることを確認します。

- CA ARCserve D2D リリース番号が CA ARCserve Central 仮想スタンバイと同じリリース番号であ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。

リモート仮想スタンバイの前提条件となるインストール タスク

リモート仮想スタンバイでは、レプリケートされた CA ARCserve D2D および CA ARCserve Central Host-Based VM Backup セッションから仮想スタンバイ VM を作成できます。

仮想スタンバイを使用して、レプリケートされた CA ARCserve D2D セッションの仮想スタンバイ VM を作成する前に、前提条件となるタスクを以下の順序で完了します。

1. CA ARCserve Replication/High Availability をインストールします。詳細については、「CA ARCserve Replication/High Availability ユーザ ガイド」を参照してください。

重要: リモート仮想スタンバイを行う際、CA ARCserve Replication/High Availability を実行するにはライセンスが必要です。

2. 復旧ポイントを作成するために CA ARCserve D2D または CA ARCserve Central Host-Based VM Backup のいずれか、または両方を設定します。詳細については、「CA ARCserve D2D ユーザ ガイド」または「CA ARCserve Central Host-Based VM Backup ユーザ ガイド」を参照してください。
3. 復旧ポイントをリモート ロケーションにコピーするレプリケーション シナリオを作成します。詳細については、「[リモート仮想スタンバイの CA ARCserve Replication/High Availability シナリオの作成](#) (P. 20)」を参照してください。

リモート仮想スタンプの CA ARCserve Replication/High Availability シナリオの作成

仮想スタンプでは、リモート ロケーションに復旧ポイントをコピーする CA ARCserve Replication/High Availability シナリオを作成できます。

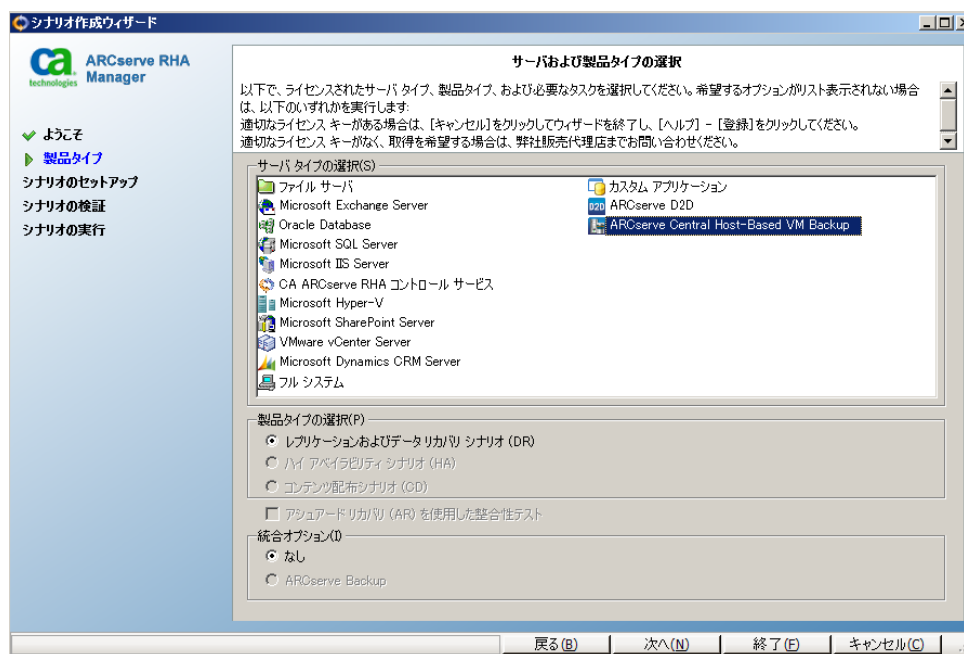
次の手順に従ってください:

1. CA ARCserve Replication/High Availability マネージャを開きます。[シナリオ] メニューから [新規] をクリックするか、または [標準] ツールバー上の [新規] ボタンをクリックします。

シナリオ作成ウィザードの「ようこそ」画面が表示されます。

2. [新規シナリオの作成] を選択します。

[サーバおよび製品タイプの選択] 画面が表示されます。



3. 以下のオプションを選択して、[次へ] ボタンをクリックします。

- a. サーバタイプ: ARCserve Central Host-Based VM Backup

注: 以下のプロセスは、ARCserve D2D にも適用されます。

- b. 製品タイプ: レプリケーションおよびデータ リカバリ シナリオ (DR)
- c. 統合オプション: なし

「ARCserve Central Host-Based VM Backup サーバ認証情報」ダイアログボックスが表示されます。

ARCserve Central Host-Based VM Backup サーバ

ARCserve Central Host-Based VM Backup サーバ設定およびユーザ認証情報:

ホスト名/IP:

ドメイン/ユーザ名:

パスワード:

プロトコル: ☒ HTTP ☐ HTTPS

ポート:

OK(O) キャンセル(C)

4. Central Host-Based VM Backup サーバ認証情報を入力し、[OK]をクリックします。手順3で指定した内容に基づいて、サーバ名が自動入力されます。

「ARCserve Central Host-Based VM Backup 宛先ホストおよび仮想マシン選択」画面が表示されます。

注: この画面は、CA ARCserve Central Host-Based VM Backup シナリオでのみ表示され、CA ARCserve D2D シナリオでは表示されません。

シナリオ作成ウィザード

ARCserve RHA Manager

ARCserve Central Host-Based VM Backup 宛先ホストおよび仮想マシン選択

検出された仮想マシンに従って、対象のマスタサーバに対する ARCserve Central Host-Based VM バックアップ先ホストを選択します。

仮想マシン名	ポリシー名	プロキシ名	vCenter/ESX
<input type="checkbox"/> <VM1>	<ポリシー1>	<IPアドレス>	<IPアドレス>
<input type="checkbox"/> <VM2>	<ポリシー2>	<IPアドレス>	<IPアドレス>
<input type="checkbox"/> <VM3>	<ポリシー3>	<IPアドレス>	<IPアドレス>
<input type="checkbox"/> <VM4>	<ポリシー4>	<IPアドレス>	<IPアドレス>

すべて選択 すべて選択解除

戻る(B) 次へ(N) 終了(F) キャンセル(C)

CA ARCserve Replication/High Availability は CA ARCserve Central Host-Based VM Backup サーバに接続して、ポリシーを取得し、バックアップ先ホストおよびその仮想マシンを表示します。

5. ホスト名を選択し、保護する仮想マシンを選択します。

新規作成された仮想マシンを含める： このシナリオの実行時に、メイン ホスト バックアップ フォルダ内のすべてのサブフォルダがレプリケートされるように指定します。新しく作成された **VM** バックアップ フォルダもレプリケートされます。選択されていない **VM** のフォルダのみが除外されます。それらのフォルダは、除外フォルダとしてマークされます。このオプションを選択しない場合、選択されたバックアップ フォルダのみがレプリケートされます。

このシナリオの実行時に、選択された仮想マシンのバックアップ ファイルがレプリケートされます。これらは **CA ARCserve D2D** によって作成されたバックアップ ファイルです。

6. 以下のマスタおよびレプリカの詳細を入力します。

シナリオ名： デフォルト名を使用するか、一意の名前を入力します。

マスタ ホスト名/IP： ユーザが選択したホスト名に従って、自動入力されます。

レプリカ ホスト名/IP： レプリカ サーバのホスト名または IP アドレスを入力します。このサーバはターゲット サーバです。[参照] ボタンを使用して、レプリカ サーバを検索します。

ポート： マスタおよびレプリカのデフォルトのポート番号 (25000) を使用するか、または新しいポート番号を入力します。

(オプション) ホスト上の CA ARCserve RHA エンジンを検証： 指定されたマスタおよびレプリカ ホスト上にエンジンがインストールされ実行されているかどうかを検証する場合にこのオプションを選択します。

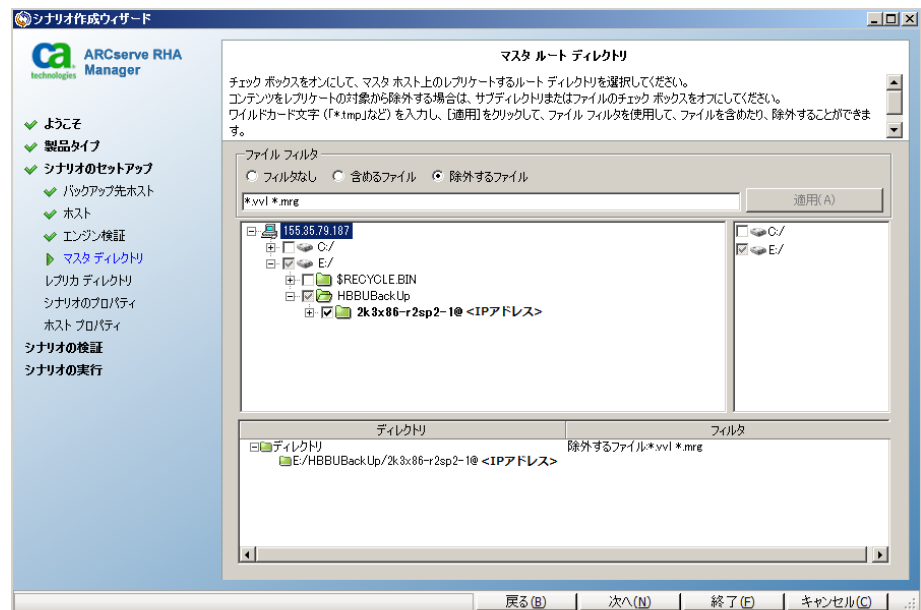
7. [次へ] をクリックします。

[エンジンの検証] 画面が表示されます。

[ホスト上の CA ARCserve RHA エンジンを検証] オプションを有効にした場合は、[エンジン検証] 画面が開きます。前の画面で指定されたマスタ ホストとレプリカ ホストの存在および接続性が確認されます。

8. [次へ] をクリックします。

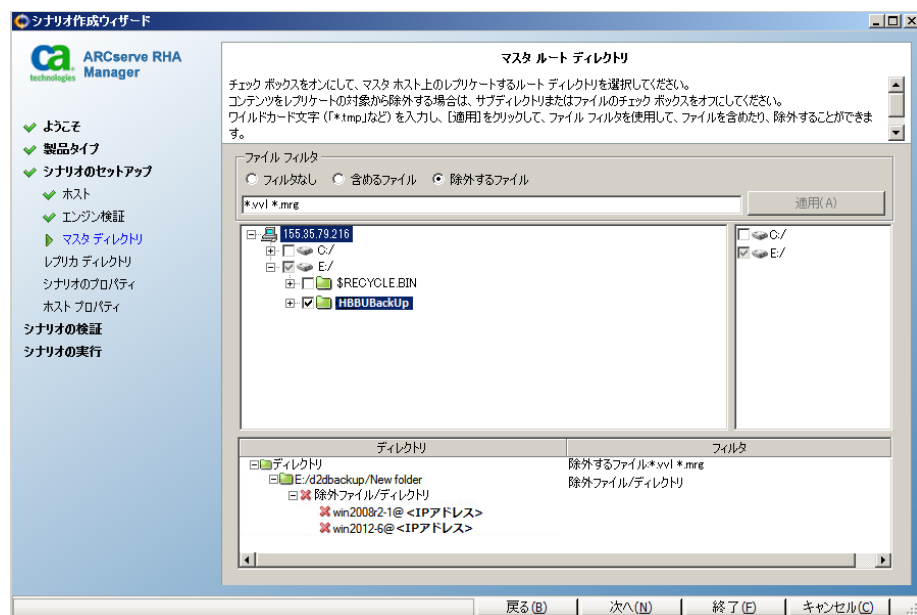
[マスタ ルート ディレクトリ] 画面が表示されます。



RHA エンジンは、選択された仮想マシンのバックアップ フォルダを検出します。これらのバックアップ フォルダは自動的に選択されています。

注: これらのフォルダは CA ARCserve D2D によって作成されるバックアップ フォルダです。

「ARCserve Central Host-Based VM Backup 宛先ホストおよび仮想マシン選択」画面で「新規作成された仮想マシンを含める」を選択した場合、メインバックアップフォルダがレプリケーション対象として選択され、除外されたフォルダはフィルタ ペインに表示されます。



9. 「次へ」をクリックします。

「レプリカルートディレクトリ」画面が表示されます。

10. デフォルト状態のまま「次へ」をクリックします。

「シナリオのプロパティ」画面が表示されます。

11. シナリオ全体に影響するプロパティを設定します。この例では、デフォルト設定を使用します。これらのプロパティは、ウィザードを使用せずに設定することもできます。シナリオプロパティの設定の詳細については、「シナリオのプロパティの設定」を参照してください。
12. [次へ] をクリックします。

[マスタとレプリカのプロパティ] 画面が開きます。

マスタとレプリカのプロパティ

マスタとレプリカのプロパティはここで設定されます。これらのプロパティは、ウィザードの手順終了後に設定することもできます。推奨されているデフォルト値はすでにリスト内にあります。値を変更する前に、「CA ARCserve RHA 管理者ガイド」を参照してください。

マスタ プロパティ	値	レプリカ プロパティ	値
⊕ ホスト接続		⊕ ホスト接続	
⊕ レプリケーション		⊕ レプリケーション	
⊖ スプール		⊕ スプール	
⊕ 最大スプール サイズ (MB)	制限なし	⊕ リカバリ	
⊕ 最小空きディスク容量 (MB)	1024	⊕ ボリューム スナップショット管理プロ...	
⊕ スプール ディレクトリ	[インストール ディレ...	⊕ スケジュール タスク	
⊕ イベント通知		⊕ イベント通知	
⊕ レポート		⊕ レポート	

13. マスタまたはレプリカのいずれかのホストに関連するプロパティを設定します。この例では、デフォルト設定を使用します。マスタおよびレプリカのプロパティの設定方法の詳細については、「マスタまたはレプリカ サーバのプロパティの設定」を参照してください。

注: デフォルトのスプール場所 (C:) がいっぱいにならないように、マスタ プロパティでのスプーリングには別のドライブを選択してください。(推奨)

14. [次へ] をクリックします。

[シナリオの検証] 画面が表示されます。

レプリケーションが失敗することのないよう、新しいシナリオが検証され、パラメータが確認されます。検証が完了すると、画面が開き、問題および警告があれば表示されます。警告が表示されても、操作の続行が可能です。必要に応じて、警告を解決します。

15. すべてのエラーおよび警告が解決されたら、[次へ] をクリックします。

[シナリオ実行] 画面が表示されます。

16. [完了] を選択します。

CA ARCserve Replication/High Availability シナリオは正常に作成されました。これで、このシナリオを実行し、CA ARCserve D2D によって作成された仮想マシン ファイルをバックアップできます。

重要: イベント コンソールを参照して、最初のデータ同期が完了しているかを検証することをお勧めします。完了していない場合、バックアップジョブが失敗します。

インストールに関する考慮事項

CA ARCserve Central 仮想スタンバイ 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ある場合、パッチは製品コンポーネントを更新する前にモジュールを更新します。

- CA ARCserve 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。Virtual Standby 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

- CA ARCserve Central 仮想スタンバイ は、圧縮したボリューム、およびファイルシステムによって暗号化されたボリューム上で仮想ディスク イメージ (VHD ファイル) を作成することをサポートしません。

注: この制限は Hyper-V ハイパーバイザのみに適用されます。

- CA ARCserve Central 仮想スタンバイ は、JIS2004 Unicode 文字を使用して名前が付けられた VMware 仮想マシンの保護をサポートしません。
- CA ARCserve Central 仮想スタンバイ は、ディスク サイズが 2 テラバイトを超える仮想マシンの保護はサポートしていません。

CA ARCserve Central 仮想スタンバイ 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 仮想スタンバイ 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が実行されます。

インストールプロセスの完了後、[インストール レポート] ダイアログ ボックスが表示されます。

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 仮想スタンバイ 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。

次の手順に従ってください:

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 仮想スタンバイ のサイレント インストール

CA ARCserve Central Applications では、CA ARCserve Central 仮想スタンバイのサイレント 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 仮想スタンバイ 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 仮想スタンバイのサイレントアンインストール

CA ARCserve Central Applications では、CA ARCserve Central 仮想スタンバイ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。

次の手順に従ってください:

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: 以下の構文では、CA ARCserve Central 仮想スタンバイ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 {CAED4835-964B-484B-A395-E2DF12E6F73D}
```

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。

第 3 章：仮想スタンバイ ポリシーの設定

このセクションには、以下のトピックが含まれています。

[ノードのディスカバリ](#) (P. 39)

[CA ARCserve Central 仮想スタンバイ ポリシーの作成](#) (P. 47)

[ノードのポリシーへの割り当て/割り当て解除](#) (P. 62)

ノードのディスカバリ

CA ARCserve Central 仮想スタンバイ では、以下の方法を使用してノードを検出または追加できます。

ローカル ポリシー：

- [IP アドレスまたはノード名によるノードの追加](#) (P. 40)
- [ファイルからノードをインポート](#) (P. 41)
- [CA ARCserve Central Host-Based VM Backup サーバからノードを追加](#) (P. 43)

リモート ポリシー：

- [CA ARCserve Replication/High Availability からのノードのインポート](#) (P. 46)

IP アドレスまたはノード名によるノードの追加

Virtual Standby では、IP アドレスまたはノード名に基づいてノードを追加することができます。保護する CA ARCserve D2D ソース ノードを追加します。

注: このオプションはローカルの仮想スタンバイ ポリシーにのみ適用されます。

IP アドレスまたはノード名によってノードを追加する方法

1. ホーム画面から、ナビゲーションバーの [ノード] を選択します。
[ノード] 画面が表示されます。
2. [ノード] ツールバーから [追加] をクリックし、コンテキストメニューの [IP/名前によるノードの追加] をクリックします。
[IP/名前によるノードの追加] ダイアログ ボックスが開きます。
3. [IP/名前によるノードの追加] ダイアログ ボックスの以下のフィールドに入力します。
 - **IP/ノード名** -- ノードの IP アドレスまたは名前を指定できます。
 - **説明** -- ノードの説明を指定できます。
 - **ユーザ名** -- ノードへのログインに必要なユーザ名を指定できます。
 - **パスワード** -- ノードへのログインに必要なパスワードを指定できます。
[OK] をクリックします。
4. (オプション) 新しく追加されたノードがノードリストに表示されない場合は、[ノード] ツールバー上で [更新] をクリックします。

[IP/名前によるノードの追加] ダイアログ ボックスが閉じて、ノードが追加されます。

ファイルからのノードのインポート

CA ARCserve Central 仮想スタンバイ では、ファイルからの複数のノードをインポートすることができます。ノードは、カンマ区切り値のテキストファイル（.txt）またはスプレッドシート（.CSV）からインポートできます。

ファイルから最大 100 までのノードをインポートすることができます。ファイルに 100 を超えるノードが含まれている場合は最初の 100 のノードのみがインポートされます。100 以上のノードを追加する必要がある場合は、ファイルを使用して 100 のノードをインポートし、残りのノードを手動で追加します。

注: このオプションはローカルの仮想スタンバイ ポリシーにのみ適用されます。ノードを手動で追加する方法の詳細については、「[IP アドレスまたはノード名によるノードの追加](#) (P. 40)」を参照してください。

ファイルからノードをインポートする方法

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. [ノード] ツールバーから [追加] をクリックし、コンテキストメニューの [ファイルからのノードのインポート] をクリックします。

[ノードの選択] ダイアログ ボックスが表示されます。

3. [参照] をクリックして、インポートするノードが含まれるファイルを指定します。

注: カンマ区切り（CSV）ファイル、またはカンマ区切り値が含まれたテキスト ファイルを指定できます。

[アップロード] をクリックします。

ノード名および対応するユーザ名がダイアログ ボックスに表示されます。

4. [次へ] をクリックします。

[ノード認証情報] ダイアログ ボックスが表示されます。

指定されたユーザ名とパスワードが正しい場合、緑のチェック マークが [検証済み] フィールドに表示されます。指定されたユーザ名とパスワードが正しくない場合、赤い感嘆符が [検証済み] フィールドに表示されます。

5. 以下のいずれかを行います。

- ノードを追加するには、ユーザ名およびパスワードがすべて正しいことを確認します。特定のノードの認証情報を変更するには、[ノード名] フィールドをクリックします。

[認証情報の検証] ダイアログ ボックスが表示されます。

[認証情報の検証] ダイアログ ボックスで必須フィールドに入力し、[OK] をクリックします。

- すべてのノードにグローバル ユーザ名およびパスワードを適用するには、[ユーザ名] と [パスワード] フィールドに入力し、[選択対象に適用] をクリックします。

グローバル ユーザ名とパスワードがすべてのノードに適用されます。

[完了] ボタンをクリックします。

ノードが追加されます。

CA ARCserve Central Host-Based VM Backup サーバからのノードの追加

CA ARCserve Central Host-Based VM Backup は、バックアッププロキシサーバにインストールされている CA ARCserve D2D の 1 つのインスタンスを使用して、仮想マシンをバックアップするためのアプリケーションです。CA ARCserve Central 仮想スタンバイ では、ノードの復旧ポイント スナップショットを作成できるようにするため、CA ARCserve Central Host-Based VM Backup サーバが保護しているノードを追加できます。仮想マシンには CA ARCserve D2D ポリシーが割り当てられている必要があり、ポリシーは CA ARCserve Central Host-Based VM Backup を使用して割り当てられます。

以下の点に注意してください。

- このオプションはローカルの仮想スタンバイ ポリシーにのみ適用されます。
- CA ARCserve Central 仮想スタンバイ では、以下の方法を使用してノードを追加できます。
 - ノードを手動で追加
 - テキスト ファイルからノードを追加
 - CA ARCserve Central Host-Based VM Backup サーバからノードを追加

CA ARCserve Central 仮想スタンバイ では、ポリシーを直接ノードに適用しますが、CA ARCserve Central Host-Based VM Backup では、ポリシーをバックアッププロキシサーバに適用します。この動作は、CA ARCserve Central Host-Based VM Backup サーバからのノードを追加した後も続行します。

注: 仮想マシンへの CA ARCserve D2D ポリシーの割り当ての詳細については、「CA ARCserve Central Host-Based VM Backup ユーザ ガイド」を参照してください。

- Virtual Standby では、CA ARCserve Central Host-Based VM Backup サーバから自動で追加されたノード用の復旧ポイント スナップショットの電源をオンにすることができません。ただし、CA ARCserve Central Host-Based VM Backup サーバから手動で追加されたノード用の復旧ポイント スナップショットの電源をオンにすることはできます。

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. [ノード] カテゴリから [追加] をクリックし、ポップアップ メニューの [CA ARCserve Central Host-Based VM Backup サーバからの仮想マシンの追加] をクリックします。

[CA ARCserve Central Host-Based VM Backup サーバからの仮想マシンの追加] ダイアログ ボックスが表示されます。

3. [CA ARCserve Central Host-Based VM Backup サーバからの仮想マシンの追加] ダイアログ ボックスの以下のフィールドに入力します。
 - **マシン名** -- CA ARCserve Central Host-Based VM Backup サーバの IP アドレスまたは名前を指定します。
 - **ユーザ名** -- CA ARCserve Central Host-Based VM Backup サーバへのログインに必要なユーザ名を指定します。
 - **パスワード** -- CA ARCserve Central Host-Based VM Backup サーバへのログインに必要なパスワードを指定します。
 - **ポート** -- アプリケーションで CA ARCserve Central Host-Based VM Backup サーバとの通信に使用するポート番号を指定します。
 - **HTTPS を使用** -- 安全な HTTPS 通信を使用するように指定できます。

[OK] をクリックします。

次のいずれかが実行されます。

- 初めてこの ESX Server システムからノードをインポートしている場合、Virtual Standby では CA ARCserve Central Host-Based VM Backup ポリシー割り当てが含まれる仮想マシンすべてをインポートします。インポートプロセスが完了した後、[ノード] 画面上でノードを確認できます。
- この ESX Server システムからノードをインポートするのが初めてではない場合、[CA ARCserve Central Host-Based VM Backup サーバからの仮想マシンの追加] ダイアログ ボックスには、それまでにインポートされたノードのリストが表示されます。さらに、それまでにインポートされたノードの情報を上書きするかどうかを確認されます。
- 新規ノードが検出されない場合、[CA ARCserve Central Host-Based VM Backup サーバからの仮想マシンの追加] ダイアログ ボックスは閉じます。その場合はノードがインポートされなかったことを示すメッセージが表示されます。

4. 以下のいずれかの操作を実行します。

- **新しく検出されたノードを追加し、検出済みのノードを上書きする場合：** インポート済みとして検出されたノードの横のチェックボックスをオンにして [OK] をクリックします。

新しく検出されたノードが追加され、検出済みのノードが上書きされます。上書きされるのは、ステータスと、検出済みのノードに適用された認証情報のみです。

- **新しく検出されたノードのみを追加する（検出済みのノードをインポート/上書きしない）場合：** インポート済みとして検出されたノードの横のチェックボックスをオンにしないで、[OK] をクリックします。

新しく検出されたノードのみが追加されます。検出済みのノードは上書きされません。

- **新しく検出されたノードおよび検出済みのノードを追加せずに終了する場合：** [キャンセル] をクリックします。

ノードは追加されません。

5. （オプション） ツールバー上の [更新] アイコンをクリックし、新しく検出されたすべてのノードがノードリストに表示されていることを確認します。

ノードが追加されます。

注： CA ARCserve D2D 情報が CA ARCserve Central Host-Based VM Backup サーバ上で更新されると、サーバは、CA ARCserve Central Host-Based VM Backup から仮想マシンをインポートしてポリシーを再展開するように自動的に CA ARCserve Central 仮想スタンバイ に伝えます。CA ARCserve Central 仮想スタンバイ が利用可能でない場合は、CA ARCserve Central Host-Based VM Backup から手動で仮想マシンをインポートできます。

CA ARCserve Replication からのノードのインポート

CA ARCserve Central 仮想スタンバイ では、1 つ以上のノードを CA ARCserve Replication/High Availability からインポートできます。ノードをインポートするには、インポート先の Replication マネージャの情報を指定します。

注: このオプションは [リモート仮想スタンバイ ポリシー \(P. 56\)](#) にのみ適用されます。ノードをインポートする前に、[リモート仮想スタンバイ ポリシーの CA ARCserve Replication/High Availability シナリオを作成 \(P. 20\)](#) する必要があります。

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. [ノード] ツールバーから [追加] をクリックし、ポップアップメニューの [CA ARCserve Replication からのノードのインポート] をクリックします。
[CA ARCserve Replication からのノードのインポート] ダイアログ ボックスが表示されます。
3. インポートするノードが含まれる Replication マネージャのホスト名、ポート、プロトコル、ユーザ名、およびパスワードを指定します。
[接続] をクリックします。
ノード名、シナリオ名、コンバータ、バックアップ場所、および環境設定のステータスが、ダイアログ ボックスに表示されます。
4. [インポート] をクリックします。

ノードが正常にインポートされ、[ノード] 画面に表示されます。

リモートコンバータの設定

CA ARCserve Central 仮想スタンバイ では、CA ARCserve Replication/High Availability が保護する CA ARCserve D2D 復旧ポイントを変換し、Microsoft Hyper-V、VMware vCenter、または ESXi に自動登録することができます。

ノードが CA ARCserve Replication/High Availability から CA ARCserve Central Applications にインポートされる場合、ノードはその後に変換できます。CA ARCserve Replication/High Availability のレプリカ フォルダが、ノードの変換元になります。

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、あるいは変換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. [コンバータ] 列から設定するコンバータをクリックします。
[リモート コンバータの設定] ダイアログ ボックスが表示されます。
4. 選択されたコンバータのポート、プロトコル、ユーザ名、およびパスワードを指定し、[更新] をクリックして情報を保存します。

コンバータが設定されました。

CA ARCserve Central 仮想スタンバイ ポリシーの作成

Virtual Standby では、CA ARCserve D2D ノードに割り当てるカスタム変換ポリシーを定義するために、2 種類のポリシーを作成できます。以下の 2 つのポリシーです。

- [ローカル仮想スタンバイ ポリシー](#) (P. 48)
- [リモート仮想スタンバイ ポリシー](#) (P. 56)

注: ポリシーを作成するには、モニタ サーバ上に CA ARCserve D2D をインストールする必要があります。

ローカル仮想スタンバイ ポリシーの作成

Virtual Standby では、CA ARCserve D2D ノードに割り当てるカスタム変換ポリシーを定義するために、ローカル仮想スタンバイ ポリシーを作成できます。

注: ポリシーを作成するには、モニタ サーバ上に CA ARCserve D2D をインストールする必要があります。

次の手順に従ってください:

1. Virtual Standby サーバにログインし、Virtual Standby を開始します。
ホーム画面上のナビゲーションバーから、[ポリシー] をクリックします。
[ポリシー] ウィンドウが開きます。
2. [新規] をクリックし、ポップアップメニューの [新規ローカル仮想スタンバイ ポリシー] をクリックします。
[ローカル仮想スタンバイ ポリシーの作成] ダイアログ ボックスが表示されます。
3. [ポリシー名] フィールドにポリシーの名前を入力します。
[Virtual Standby] タブをクリックします。
[仮想化サーバ]、[仮想マシン]、[代理設定] オプションが表示されます。

4. [仮想化サーバ] をクリックします。
仮想化サーバ オプションが表示されます。
5. 以下の仮想化サーバ オプションを入力します。

VMware システム :

- **仮想化の種類** -- [VMware] をクリックします。
- **ESX ホスト/vCenter** -- ESX または vCenter Server システムのホスト名を指定します。
- **ユーザ名** -- VMware システムへのログインに必要なユーザ名を指定します。

注: 指定するアカウントは、ESX/vCenter Server システム上の管理者アカウントまたは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** -- VMware システムへのログインに必要なユーザ名のパスワードを指定します。
- **プロトコル** -- ソースの CA ARCserve D2D ノードとモニタ サーバ間の通信に使用するプロトコルとして、HTTP または HTTPS を指定します。
- **ポート** -- ソース サーバとモニタ サーバとの間のデータ転送に使用するポートを指定します。
- **ESX ノード** -- このフィールドの値は、[ESX ホスト/vCenter] フィールドで指定した値によって異なります。
 - **ESX Server システム** -- [ESX ホスト/vCenter] フィールドで ESX Server システムを指定すると、このフィールドには ESX Server システムのホスト名が表示されます。
 - **vCenter Server システム** -- [ESX ホスト/vCenter] フィールドで vCenter Server システムを指定すると、このフィールドでこのポリシーに関連付ける ESX Server システムを（ドロップダウン リストから）選択できます。
- **モニタ サーバ** -- ソース サーバのステータスをモニタするサーバのホスト名を指定します。

注: モニタ サーバとしては、どの物理コンピュータまたは仮想マシンでも使用できますが、サーバが CA ARCserve Central Host-Based VM Backup 環境用のプロキシ サーバとして機能していないことが条件です。

- **ユーザ名** -- モニタ システムへのログインに必要なユーザ名を指定します。
- **パスワード** -- モニタ システムへのログインに必要なユーザ名のパスワードを指定します。
- **プロトコル** -- CA ARCserve Central 仮想スタンバイ サーバと ESX Server システム (モニタ サーバ) 間の通信に使用するプロトコルとして、HTTP または HTTPS を指定します。
- **ポート** -- CA ARCserve Central 仮想スタンバイ サーバと ESX Server (モニタ サーバ) 間のデータ転送に使用するポートを指定します。
- **データ転送にプロキシとしてモニタ サーバを使用** -- モニタ サーバによって CA ARCserve D2D ソース ノードから ESX Server データストアに変換データをコピーする場合は、このオプションを指定します。このオプションを有効にすると、Virtual Standby は、LAN によるデータ通信よりも高速なファイバチャネル通信を使用して、ソース ノードから ESX Server データ ストアに変換データを転送します。

注: [データ転送にプロキシとしてモニタ サーバを使用] オプションはデフォルトで有効になっています。 このオプションを無効にすると、CA ARCserve D2D ソース サーバが ESX Server システムに変換データを直接コピーできるようになります。

Hyper-V システム :

- **仮想化の種類** -- [Hyper-V] をクリックします。
- **Hyper-V ホスト名** -- Hyper-V システムのホスト名を指定します。
- **ユーザ名** -- Hyper-V システムへのログインに必要なユーザ名を指定します。

注: 指定するアカウントは、Hyper-V システム上の管理者アカウントまたは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** -- Hyper-V システムへのログインに必要なユーザ名のパスワードを指定します。
- **ポート** -- ソース サーバとモニタ サーバとの間のデータ転送に使用するポートを指定します。
- **ユーザ名** -- モニタ システムへのログインに必要なユーザ名を指定します。
- **パスワード** -- モニタ システムへのログインに必要なユーザ名のパスワードを指定します。
- **プロトコル** -- CA ARCserve Central 仮想スタンバイ サーバと Hyper-V Server システム (モニタ サーバ) 間の通信に使用するプロトコルとして、HTTP または HTTPS を指定します。
- **ポート** -- CA ARCserve Central 仮想スタンバイ サーバと Hyper-V Server (モニタ サーバ) 間のデータ転送に使用するポートを指定します。

[仮想マシン] をクリックします。

[仮想マシン] オプションが表示されます。

6. 以下の「仮想マシン」オプションに入力します。

VMware システム :

VMware システムに以下の仮想マシン オプションを適用します。

- **VM 名プレフィックス** -- ESX Server システム上の仮想マシンの表示名に追加するプレフィックスを指定します。

デフォルト値 : CAVM_

- **VM リソース プール** -- スタンバイ仮想マシンがグループ化されるリソース プールの名前を指定します。
- **CPU 数** -- スタンバイ仮想マシンによってサポートされる最小および最大の CPU 数を指定します。
- **メモリ** -- スタンバイ仮想マシンに割り当てられる RAM の総量を MB で指定します。

注: 指定する RAM の量は 2 の倍数である必要があります。

- **VM データ ストア** -- 変換データを格納する場所を指定します。
 - すべての仮想ディスク用に 1 つのデータ ストアを指定します -- 仮想マシンに関連するディスクをすべて 1 つのデータ ストアにコピーします。
 - 各仮想ディスクのデータ ストアを指定します -- 仮想マシンのディスク関連情報を対応するデータ ストアにコピーします。
- **VM ネットワーク** -- 仮想マシンと通信するために ESX Server システムが使用する NIC、仮想ネットワーク、およびバスを定義します。
 - 各 NIC のネットワーク アダプタの種類を指定し、そのネットワーク アダプタを以下の仮想ネットワークに接続します。 -- 仮想 NIC を仮想ネットワークにマップする方法を定義します。仮想マシンに仮想 NIC および仮想ネットワークが含まれる場合は、このオプションを指定します。
 - 各 NIC のネットワーク アダプタの種類および仮想ネットワークを指定します -- NIC が通信に使用する仮想ネットワークの名前を定義します。

Hyper-V システム :

Hyper-V システムに以下の仮想マシン オプションを適用します。

- **VM ベーシック設定** -- 以下の VM ベーシック設定を指定します。
 - **VM 名プレフィックス** -- Hyper-V システム上の仮想マシンの表示名に追加するプレフィックスを指定します。
デフォルト値 : CAVM_
CPU 数 -- スタンバイ仮想システムによってサポートされる最小および最大の CPU 数を指定します。
 - **メモリ** -- スタンバイ仮想マシンに割り当てられる RAM の総量を MB で指定します。
注: 指定する RAM の量は 4 の倍数である必要があります。
- **VM パス** -- 以下の VM パス オプションのうちの 1 つを指定します。
 - **すべての仮想ディスク用に 1 つのパスを指定します** -- 変換データを格納する Hyper-v サーバ上の場所を指定します。
 - **各仮想ディスクのパスを指定します** -- 各仮想ディスクの変換データを格納する Hyper-V サーバ上の場所を指定します。

注: CA ARCserve Central 仮想スタンバイ は圧縮したボリューム、およびファイルシステムによって暗号化されたボリューム上で仮想ディスク イメージ (VHD ファイル) を作成することをサポートしません。指定されたパスが圧縮または暗号化された Hyper-V ボリューム上に存在する場合、Virtual Standby ではポリシーの作成が禁止されます。

- **VM ネットワーク** -- 仮想マシンと通信するために Hyper-V サーバが使用する NIC、仮想ネットワーク、およびパスを定義します。以下のオプションのうちの 1 つを指定し、必要なフィールドに入力します。
 - **各 NIC のネットワーク アダプタの種類を指定し、そのネットワーク アダプタを以下のネットワークに接続します** -- 仮想 NIC を仮想ネットワークにマップする方法を定義します。仮想マシンに仮想 NIC および仮想ネットワークが含まれる場合は、このオプションを指定します。
 - **各 NIC のネットワーク アダプタの種類および仮想ネットワークを指定します** -- NIC が通信に使用する仮想ネットワークの名前を定義します。

[代理設定] をクリックします。

[代理設定] オプションが表示されます。

7. 以下の [代理設定] オプションに入力します。

復旧:

以下の方式のいずれかを選択します。

- **手動で仮想マシンを開始します** -- ソース サーバが失敗、または通信を停止した場合、手動で仮想マシンの電源の投入およびプロビジョニングを行います。仮想マシンをプロビジョニングし、ソース サーバとしてサーバが機能することを許可する前に、失敗の原因を分析する場合、このオプションを指定します。
- **自動的に仮想マシンを開始します** -- ソース サーバが失敗、または通信を停止した場合、自動で仮想マシンの電源の投入およびプロビジョニングを行います。ソース サーバが失敗、または通信を停止した直後、仮想マシンがソース サーバとして機能するようにするには、このオプションを指定します。

注: [手動で仮想マシンを開始します] はデフォルトのオプションです。

ハートビートプロパティ:

- **タイムアウト** -- 復旧ポイント スナップショットの電源がオンになる前に、モニタ サーバでハートビートを待機する必要がある時間を指定します。
- **周期** -- ソース サーバがハートビートをモニタ サーバに伝える周期を指定します。

例: 指定されたタイムアウト値は **60** です。指定された周期の値は **10** です。ソース サーバは、**10** 秒の間隔でハートビートを通信します。モニタ サーバで、最後にハートビートが検出されてから **60** 秒以内に次のハートビートを検出しない場合、モニタ サーバは最新の復旧ポイント スナップショットを使用して仮想マシンの電源をオンにします。

[環境設定] タブをクリックします。

電子メール スキャン オプションが表示されます。

8. 以下の電子メール アラート オプションに入力します。

- **ソース マシンのハートビートがありません** -- モニタ サーバがソース サーバからのハートビートを検出しない場合、Virtual Standby はアラート通知を送信します。
- **自動電源オンが設定されたソース マシンに対して VM の電源がオンになりました** -- ハートビートが検出されない場合に自動的に電源がオンになるよう設定された仮想マシンの電源をオンにした場合、Virtual Standby はアラート通知を送信します。
- **手動電源オンが設定されたソース マシンのハートビートがありません** -- 自動的に電源がオンになるよう設定されていないソースサーバからハートビートを検出しない場合、Virtual Standby はアラート通知を送信します。
- **VM ストレージ空き容量が次の値より少ない** -- 定義されたハイパーバイザパス上のディスク空き容量が十分でないことが検出された場合、Virtual Standby はアラート通知を送信します。これが検出されるのは、ディスク空き容量がユーザ定義のしきい値を下回った場合です。しきい値は、ボリュームの絶対値 (MB) またはその容量の割合として定義できます。
- **仮想スタンバイ エラー/失敗/クラッシュ** -- 変換処理中に発生したエラーを検出した場合、Virtual Standby はアラート通知を送信します。
- **仮想スタンバイが成功** -- 仮想マシンで正常に電源がオンになったことを検出した場合、Virtual Standby はアラート通知を送信します。
- **ハイパーバイザがアクセス不可能** -- ESX Server システムまたは Hyper-V システムと通信できないことを検出した場合、Virtual Standby はアラート通知を送信します。
- **ライセンス エラー** -- Virtual Standby サーバ、ソース サーバ、およびモニタ サーバ上でライセンスの問題を検出した場合、Virtual Standby はアラート通知を送信します。
- **仮想スタンバイは、復旧ポイント スナップショットから正常に開始しませんでした** -- 仮想マシンの電源が自動的にオンにならず、[自動的に仮想マシンを開始します] オプションが指定されていることを検出した場合、Virtual Standby はアラート通知を送信します。

[保存] をクリックします。

ポリシーが保存されます。

リモート仮想スタンバイ ポリシーの作成

Virtual Standby では、CA ARCserve Replication/High Availability からノードに割り当てるカスタム変換ポリシーを定義するために、リモート仮想スタンバイ ポリシーを作成できます。

次の手順に従ってください:

1. Virtual Standby サーバにログインし、Virtual Standby を開始します。
ホーム画面上のナビゲーションバーから、[ポリシー] をクリックします。
[ポリシー] ウィンドウが開きます。
2. [新規] をクリックし、ポップアップメニューの [新規リモート仮想スタンバイ ポリシー] をクリックします。
[リモート仮想スタンバイ ポリシーの作成] ダイアログ ボックスが表示されます。
3. [ポリシー名] フィールドにポリシーの名前を入力します。
[Virtual Standby] タブをクリックします。
[仮想化サーバ] および [仮想マシン] オプションが表示されます。

4. [仮想化サーバ] をクリックします。
仮想化サーバ オプションが表示されます。
5. 以下の仮想化サーバ オプションを入力します。

VMware システム :

- **仮想化の種類** -- [VMware] をクリックします。
- **ESX ホスト/vCenter** -- ESX または vCenter Server システムのホスト名を指定します。
- **ユーザ名** -- VMware システムへのログインに必要なユーザ名を指定します。

注: 指定するアカウントは、ESX/vCenter Server システム上の管理者アカウントまたは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** -- VMware システムへのログインに必要なユーザ名のパスワードを指定します。
- **プロトコル** -- ソースの CA ARCserve D2D ノードとモニタ サーバ間の通信に使用するプロトコルとして、HTTP または HTTPS を指定します。
- **ポート** -- ソース サーバとモニタ サーバとの間のデータ転送に使用するポートを指定します。
- **ESX ノード** -- このフィールドの値は、[ESX ホスト/vCenter] フィールドで指定した値によって異なります。
 - **ESX Server システム** -- [ESX ホスト/vCenter] フィールドで ESX Server システムを指定すると、このフィールドには ESX Server システムのホスト名が表示されます。
 - **vCenter Server システム** -- [ESX ホスト/vCenter] フィールドで vCenter Server システムを指定すると、このフィールドでこのポリシーに関連付ける ESX Server システムを（ドロップダウン リストから）選択できます。

Hyper-V システム :

- **仮想化の種類** -- [Hyper-V] をクリックします。
- **Hyper-V ホスト名** -- Hyper-V システムのホスト名を指定します。
- **ユーザ名** -- Hyper-V システムへのログインに必要なユーザ名を指定します。

注: 指定するアカウントは、Hyper-V システム上の管理者アカウントまたは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** -- Hyper-V システムへのログインに必要なユーザ名のパスワードを指定します。
- **プロトコル** -- ソースの CA ARCserve D2D ノードとモニタ サーバ間の通信に使用するプロトコルとして、HTTP または HTTPS を指定します。
- **ポート** -- ソース サーバとモニタ サーバとの間のデータ転送に使用するポートを指定します。

[仮想マシン] をクリックします。

[仮想マシン] オプションが表示されます。

6. 以下の「仮想マシン」オプションに入力します。

VMware システム :

VMware システムに以下の仮想マシン オプションを適用します。

- **VM 名プレフィックス** -- ESX Server システム上の仮想マシンの表示名に追加するプレフィックスを指定します。

デフォルト値 : CAVM_

- **VM リソース プール** -- スタンバイ仮想マシンがグループ化されるリソース プールの名前を指定します。
- **CPU 数** -- スタンバイ仮想マシンによってサポートされる最小および最大の CPU 数を指定します。
- **メモリ** -- スタンバイ仮想マシンに割り当てられる RAM の総量を MB で指定します。

注: 指定する RAM の量は 2 の倍数である必要があります。

- **VM データ ストア** -- 変換データを格納する場所を指定します。
 - すべての仮想ディスク用に 1 つのデータ ストアを指定します -- 仮想マシンに関連するディスクをすべて 1 つのデータ ストアにコピーします。
 - 各仮想ディスクのデータ ストアを指定します -- 仮想マシンのディスク関連情報を対応するデータ ストアにコピーします。
- **VM ネットワーク** -- 仮想マシンと通信するために ESX Server システムが使用する NIC、仮想ネットワーク、およびパスを定義します。
 - 各 NIC のネットワーク アダプタの種類を指定し、そのネットワーク アダプタを以下の仮想ネットワークに接続します。 -- 仮想 NIC を仮想ネットワークにマップする方法を定義します。仮想マシンに仮想 NIC および仮想ネットワークが含まれる場合は、このオプションを指定します。
 - 各 NIC のネットワーク アダプタの種類および仮想ネットワークを指定します -- NIC が通信に使用する仮想ネットワークの名前を定義します。

Hyper-V システム :

Hyper-V システムに以下の仮想マシン オプションを適用します。

- **VM ベーシック設定** -- 以下の VM ベーシック設定を指定します。
 - **VM 名プレフィックス** -- Hyper-V システム上の仮想マシンの表示名に追加するプレフィックスを指定します。
デフォルト値 : CAVM_
CPU 数 -- スタンバイ仮想システムによってサポートされる最小および最大の CPU 数を指定します。
 - **メモリ** -- スタンバイ仮想マシンに割り当てられる RAM の総量を MB で指定します。
注: 指定する RAM の量は 4 の倍数である必要があります。
- **VM パス** -- 以下の VM パス オプションのうちの 1 つを指定します。
 - **すべての仮想ディスク用に 1 つのパスを指定します** -- 変換データを格納する Hyper-v サーバ上の場所を指定します。
 - **各仮想ディスクのパスを指定します** -- 各仮想ディスクの変換データを格納する Hyper-V サーバ上の場所を指定します。

注: CA ARCserve Central 仮想スタンバイ は圧縮したボリューム、およびファイルシステムによって暗号化されたボリューム上で仮想ディスク イメージ (VHD ファイル) を作成することをサポートしません。指定されたパスが圧縮または暗号化された Hyper-V ボリューム上に存在する場合、Virtual Standby ではポリシーの作成が禁止されます。

- **VM ネットワーク** -- 仮想マシンと通信するために Hyper-V サーバが使用する NIC、仮想ネットワーク、およびパスを定義します。以下のオプションのうちの 1 つを指定し、必要なフィールドに入力します。
 - **各 NIC のネットワーク アダプタの種類を指定し、そのネットワーク アダプタを以下のネットワークに接続します** -- 仮想 NIC を仮想ネットワークにマップする方法を定義します。仮想マシンに仮想 NIC および仮想ネットワークが含まれる場合は、このオプションを指定します。
 - **各 NIC のネットワーク アダプタの種類および仮想ネットワークを指定します** -- NIC が通信に使用する仮想ネットワークの名前を定義します。

[環境設定] タブをクリックします。

電子メール スキャン オプションが表示されます。

7. 以下の電子メール アラート オプションに入力します。

- **VM ストレージ空き容量が次の値より少ない** -- 定義されたハイパーバイザパス上のディスク空き容量が十分でないことが検出された場合、Virtual Standby はアラート通知を送信します。これが検出されるのは、ディスク空き容量がユーザ定義のしきい値を下回った場合です。しきい値は、ボリュームの絶対値 (MB) またはその容量の割合として定義できます。
- **仮想スタンバイ エラー/失敗/クラッシュ** -- 変換処理中に発生したエラーを検出した場合、Virtual Standby はアラート通知を送信します。
- **仮想スタンバイが成功** -- 仮想マシンで正常に電源がオンになったことを検出した場合、Virtual Standby はアラート通知を送信します。
- **ハイパーバイザがアクセス不可能** -- ESX Server システムまたは Hyper-V システムと通信できないことを検出した場合、Virtual Standby はアラート通知を送信します。
- **ライセンス エラー** -- Virtual Standby サーバ、ソース サーバ、およびモニタ サーバ上でライセンスの問題を検出した場合、Virtual Standby はアラート通知を送信します。
- **仮想スタンバイは、復旧ポイント スナップショットから正常に開始しませんでした。** -- 仮想マシンの電源が自動的にオンにならず、[自動的に仮想マシンを開始します] オプションが指定されていることを検出した場合、Virtual Standby はアラート通知を送信します。

[保存] をクリックします。

ポリシーが保存されます。

ノードのポリシーへの割り当て/割り当て解除

復旧ポイント スナップショットを作成するには、保護する CA ARCserve D2D ノードに仮想スタンバイ変換ポリシーを割り当てます。

Virtual Standby では、ポリシーからノードの割り当てを解除できます。Virtual Standby ではノードに複数のポリシーを割り当てることはできません。ノードを新規ポリシーに割り当てる場合、ノードに新規ポリシーを割り当てる前に、そのノードから現在のポリシーの割り当てを解除します。

次の手順に従ってください:

1. Virtual Standby サーバにログインし、Virtual Standby を開始します。
ホーム画面上のナビゲーションバーから [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 リストから、ノードに割り当てる、または、割り当て解除するポリシーを選択します。
指定されたポリシーに関する詳細情報が [ポリシー詳細] タブおよび [ポリシーの割り当て] タブに表示されます。
3. [ポリシー詳細] タブをクリックし、ポリシーに関する詳細情報を表示します。
(オプション) ツールバーの [編集] ボタンをクリックし、ポリシーの現在の設定を編集します。
注: 詳細については、「ポリシーの編集」を参照してください。
4. [ポリシーの割り当て] タブをクリックします。
[ポリシーの割り当て] タブで [割り当てと割り当て解除] をクリックします。
[ポリシーの割り当て/割り当て解除] ダイアログ ボックスが表示されます。

5. [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ポリシー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: [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。

例:

- **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。
- ***.123** は、IP アドレスに「.123」があるノードをすべてフィルタ処理できます。

注: 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。

6. 以下のいずれかの操作を実行します。

- **ノードの割り当て（単一ノード）** -- [利用可能なノード] リストから、ポリシーに割り当てるノードを選択します。

一重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。

- **ノードの割り当て（複数ノード）** -- [利用可能なノード] リストから二重右矢印をクリックします。

すべてのノードが [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。

- **ノードの割り当て解除（単一ノード）** -- [選択されたノード] リストで、ポリシーから割り当て解除するノードを選択します。

一重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。

- **ノードの割り当て解除（複数ノード）** -- [選択されたノード] リストで、二重左矢印をクリックします。

すべてのノードが [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。

[OK] をクリックします。

ノードがポリシーに割り当て/割り当て解除されます。

ポリシーの展開

ポリシーを作成したら、[ノードをポリシーに割り当てて](#) (P. 62)、ポリシーを展開します。

以下の動作はポリシー展開プロセスに適用されます。

- 以下の条件では、ポリシー展開プロセスは失敗します。
 - CA ARCserve D2D ソース サーバ（ノード）に Windows Server 2008 Hyper-V の役割がインストールされている。
 - CA ARCserve D2D ノードが CA ARCserve Central Host-Based VM Backup からインポートされた。Host-based VM バックアップ プロキシシステム上で Windows Server 2008 Hyper-V の役割が有効になっていて、そのバックアッププロキシシステムが Virtual Standby のデスティネーションとして指定されている場合。
- CA ARCserve Central 仮想スタンバイは、CA ARCserve Central Host-Based VM Backup サーバから追加された仮想マシンの電源を自動的にオンにできません。そのため、リカバリ方法が「自動的に仮想マシンを開始します」に定義されているポリシーを Host-Based VM Backup で保護されているノードに展開する際に、Virtual Standby は復旧方法の値を「手動で仮想マシンを開始します」に変更します。

次の手順に従ってください:

1. Virtual Standby サーバにログインし、Virtual Standby を開始します。
ホーム画面上のナビゲーションバーから「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 リストから、展開するポリシーをクリックします。
指定されたポリシーに関する詳細情報が「ポリシー詳細」タブおよび「ポリシーの割り当て」タブに表示されます。
3. 「ポリシー詳細」タブをクリックし、ポリシーに関する詳細情報を表示します。
(オプション) ツールバーの「編集」をクリックし、現在のポリシー設定を編集します。
注: 詳細については、「ポリシーの編集」を参照してください。

4. [ポリシーの割り当て] タブをクリックします。

ポリシーに割り当てられたノードに関する詳細情報が表示されます。

(オプション) ツールバーの [割り当てと割り当て解除] をクリックし、ノードをポリシーに割り当てたり、または割り当てを解除したりします。

注: 詳細については、「[ポリシーへのノードの割り当て \(P. 62\)](#)」または「[ポリシーからのノードの割り当て解除](#)」を参照してください。

5. ツールバーの [今すぐ展開] をクリックします。

[今すぐ展開] 確認メッセージが表示されます。

6. [OK] をクリックします。

ポリシーが展開されます。

注: [ノード] 画面上の [ポリシー] 列で、特定ノードのポリシー展開ステータスを確認することもできます。

第 4 章: CA ARCserve Central 仮想スタンバイ の紹介

以下のセクションでは、CA ARCserve D2D ノードを保護するために CA ARCserve Central 仮想スタンバイ を設定する方法について説明します。

注: このセクションで説明する環境設定を完了する前に、[インストールタスクの前提条件](#) (P. 17) がすべて完了していることを確認してください。

このセクションには、以下のトピックが含まれています。

[CA ARCserve Central 仮想スタンバイ へのログイン](#) (P. 68)

[VMware ベース ノードの ESX Server または vCenter Server システムの指定](#) (P. 69)

CA ARCserve Central 仮想スタンバイ へのログイン

CA ARCserve Central 仮想スタンバイ へのログインは、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から直接、または、サポートされているブラウザを使用してリモート コンピュータから行うことができます。サポートされているブラウザの一覧については、「*CA ARCserve Central 仮想スタンバイ リリース ノート*」をご覧ください。

CA ARCserve Central 仮想スタンバイ へのログイン方法

1. 以下のいずれかのオプションを実行します。

- CA ARCserve Central 仮想スタンバイ がインストールされているサーバにログインしている場合、プログラム ファイルからアプリケーションを起動します。

ブラウザのウィンドウが開き CA ARCserve Central 仮想スタンバイ のログイン画面が表示されます。

ログイン画面で以下のフィールドを入力します。

- ユーザ名
- パスワード

[ログイン] をクリックします。

- CA ARCserve Central 仮想スタンバイ がインストールされているサーバにログインしていない場合は、ブラウザ ウィンドウを開いて、アドレス バーに以下の URL を入力してください。

`http://<CA ARCserve Central Application サーバ名>:<ポート番号>/virtualstandby/`

注: CA ARCserve Central 仮想スタンバイ がインストールされている場合、サーバのホスト名または IP アドレスを指定できます。デフォルト ポートは 8015 です。

Enter キーを押します。

ブラウザのウィンドウが開き CA ARCserve Central 仮想スタンバイ のログイン画面が表示されます。

ログイン画面で以下のフィールドを入力します。

- ユーザ名
- パスワード

[ログイン] をクリックします。

CA ARCserve Central 仮想スタンバイ にログインし、ホーム ページが開きます。

VMware ベース ノードの ESX Server または vCenter Server システムの指定

注: 以下の手順は、VMware ベースの仮想マシン ソース ノードにのみ適用されます。

さまざまな VMware ベースの環境では、Virtual Standby が、ESX Server および vCenter Server システム上に存在する仮想マシンとして設定されたソース ノードを検出できない場合があります。そのため、Virtual Standby がノードに正しいライセンスを適用できず、ノードにポリシーを展開したり変換ジョブを実行したりできなくなります。

それ以降の手順では、ノードが存在する ESX Server または 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ができます。手順を完了したら、Virtual Standby によって、保護するノードに対する検出、ライセンスの適用、ポリシーの展開、変換ジョブの実行などが可能になります。1 つのソース ノードとして動作する 1 つの ESX Server または vCenter Server システム上に複数の仮想マシンが存在する場合、ノードのすべてに 1 つのライセンスを適用できるため、ソース ノードを保護するための全体的なコストを削減することができます。

VMware ベースのノードに ESX Server または vCenter Server システムを指定する方法

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. 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。

グループと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、ポップアップメニューから「ESX Server の指定」をクリックします。

「ESX Server の指定」ダイアログ ボックスが表示されます。

注: ESX Server または vCenter Server システムによって管理される仮想マシン上に、VMware Tools がインストールされていないことが検出された場合、仮想マシンは Hyper-V システム上に存在するか、または検出されたノードは仮想マシンではありません。エラー メッセージが表示されます。

4. 「ESX Server の指定」ダイアログ ボックスの以下のフィールドに入力します。

- ESX/vCenter ホスト

注: ESX Server/vCenter 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
- パスワード
- ポート

注: デフォルトの通信ポートは 443 です。ノードが別のポート番号を使用して ESX Server または vCenter Server システムと通信する場合は、使用されるポート番号を指定します。

- プロトコル

注: デフォルトの通信プロトコルは HTTPS です。ノードが HTTP を使用して ESX Server または vCenter Server システムと通信する場合は、HTTP をクリックします。

[OK] をクリックします。

ESX Server または vCenter Server システムがノードに割り当てられます。

第 5 章: CA ARCserve Central 仮想スタンバイの使い方

このセクションには、以下のトピックが含まれています。

- [CA ARCserve D2D ノードへのログイン](#) (P. 71)
- [モニタ サーバへのログイン](#) (P. 72)
- [ノード メンテナンス タスク](#) (P. 74)
- [ノード グループ管理タスク](#) (P. 84)
- [Virtual Standby のポリシー管理タスク](#) (P. 89)
- [アプリケーション環境設定タスク](#) (P. 91)
- [ログの表示](#) (P. 100)
- [ナビゲーションバーへのリンクの追加](#) (P. 102)
- [Virtual Standby ホーム画面](#) (P. 103)
- [CA ARCserve Central 仮想スタンバイ モニタリング タスク](#) (P. 109)
- [サーバの通信プロトコルの変更](#) (P. 130)

CA ARCserve D2D ノードへのログイン

Virtual Standby 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。

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。

モニタサーバへのログイン

Virtual Standby では、CA ARCserve D2D ソース ノードをモニタしているサーバに直接ログインすることができます。モニタサーバから、メンテナンスタスクを実行し、モニタサーバがモニタしているソースサーバの状態に関する情報を表示できます。以下のアイコンによって、モニタサーバから CA ARCserve D2D ノードを識別することができます。

モニタサーバアイコン



CA ARCserve D2D ノードアイコン



モニタサーバにログインする方法

1. Virtual Standby サーバにログインし、Virtual Standby を開始します。
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. 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. 以下のいずれかを行います。

- モニタサーバの IP アドレスまたはホスト名がわかっている場合、ログインするモニタサーバを参照してクリックし、次に、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。
- モニタサーバの IP アドレスまたはホスト名が不明な場合は、ログインするモニタサーバの CA ARCserve D2D ノードを参照してクリックし、次に、ポップアップメニューから [モニタサーバへのログイン] をクリックします。

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。

モニタサーバにログインされます。

ノード メンテナンス タスク

Virtual Standby では、ノードを追加するためにいくつかの方法が提供されています。

- [IP アドレスまたはノード名によるノードの追加](#) (P. 40)
- [ファイルからノードをインポート](#) (P. 41)

注: この方法では、カンマ区切りファイル内のノードのリストから複数のノードをインポートできます。

- [CA ARCserve Central Host-Based VM Backup サーバからノードを追加](#) (P. 43)

注: この方法では、CA ARCserve Central Host-Based VM Backup アプリケーションによって保護される仮想マシン ノードをインポートすることができます。

- [CA ARCserve Replication/High Availability からのノードのインポート](#) (P. 46)

さらに、以下のノード管理タスクを実行できます。

- [ノードの更新](#) (P. 75)
- [1 つ以上の CA ARCserve D2D ノードのバックアップ パスワードの設定](#) (P. 77)
- [ノードの削除](#) (P. 80)
- [ノードからのライセンスの解放](#) (P. 80)
- [モニタ サーバからノードのモニタを停止](#) (P. 82)
- [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. 83)

ノードの更新

Virtual Standby では、以前に追加されたノードに関する情報を更新できません。

注: CA ARCserve Central Host-Based VM Backup サーバからインポートされたノードを更新することはできません。

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

注: 変更が CA ARCserve D2D ノードに対して行われた場合、[ノードの更新] ダイアログ ボックスが開き、詳細を指定することができます。

ノードの更新

IP/ノード名:

説明:

ユーザ名:

パスワード:

ユーザ名の形式は、(1) <コンピュータ名またはドメイン名>¥<ユーザ名> または (2) <ユーザ名> です。

インストール済み CA ARCserve Backup 製品

☒ CA ARCserve D2D (16.0)

ポート:

HTTPS を使用: ☐

OK キャンセル ヘルプ

6. (オプション) 更新された情報がノードリストに表示されない場合は、ツールバー上の [更新] をクリックします。

ノードが更新されます。

1 つ以上の CA ARCserve D2D ノードのバックアップ パスワードの設定

D2D バックアップをサブミットすると、バックアップのパスワードは保護している D2D ノードに保存されます。次に、CA ARCserve Replication/High Availability は、D2D 復旧ポイントを MSP（マネージド サービス プロバイダ）のサイトに レプリケートします。次に、MSP サイトのコンバータはレプリケートされたデータを仮想マシン データに変換し、MSP サイト上にそのデータを保存します。ただし、バックアップ パスワードは D2D ノード上に存在するため、コンバータはレプリケートされた復旧ポイント スナップショットを変換できません。

コンバータがレプリケートされた復旧ポイント スナップショットを確実に変換できるようにするために、仮想スタンバイでは、コンバータがデータの変換に使用できる D2D データのバックアップ パスワードを指定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、あるいはバックアップ パスワードを設定するノードを含む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. バックアップ パスワードを設定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 [バックアップ パスワードの設定] を選択します。

[ノードのバックアップ パスワードを設定] ダイアログ ボックスが開きます。

ノード <ノード名> のバックアップ パスワードを設定

1つ以上のバックアップ信号化/パスワードを入力します。変換処理中には、セッションの信号化を続行するためにすべてのパスワードが連続して使用されます。

注: すべてのパスワードが有効でない場合、変換ジョブは失敗します。

+ 追加 | 削除

<input checked="" type="checkbox"/> パスワード	パスワードの複製	コメント	作成時刻
パスワードなし			

保存 キャンセル ヘルプ

1つ以上のノードに対して、[バックアップパスワードの設定] ダイアログボックスで以下のタスクを行うことができます。

- **追加** -- [追加] をクリックすると、1つ以上のバックアップパスワードを選択したノードに追加します。
- **削除** -- [削除] をクリックすると、1つ以上のバックアップパスワードを選択したノードから削除します。

注: [選択したノードの現在のバックアップパスワードを上書きします。] チェックボックスをオンにすると、複数のノードの現在のバックアップパスワードを上書きできます。

複数ノードのバックアップ パスワードを設定

1つ以上のバックアップ暗号化/パスワードを入力します。変換処理中には、セッションの暗号化を並行するためにすべてのパスワードが連続して使用されます。
注: すべてのパスワードが有効でない場合、変換ジョブは失敗します。

+ 追加 | - 削除

パスワード	パスワードの確認	コメント	作成時刻
強調表示されたノードにはユーザ定義のパスワードが含まれます。指定したパスワードはそれらのノードに適用されます。			

☐ 選択したノードの現在のバックアップ パスワードを上書きします。

保存 | キャンセル | ヘルプ

4. [保存] をクリックします。

ダイアログボックスが閉じ、選択したリモート ノードにバックアップパスワードが設定されます。

ノードの削除

Virtual Standby では、使用している環境から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。

ノードからのライセンスの解放

CA ARCserve Central 仮想スタンバイ のライセンスはカウントベース方式で機能します。カウントベースのライセンス管理では、1つの包括的なライセンスがノードに付与され、ライセンス プール内でアクティブなライセンス権限の数が事前に定義されます。ライセンスを使用する各ノードには、使用可能なライセンス数の上限に達するまで、先着順にプールからアクティブ ライセンスが供与されます。アクティブなライセンス権限がすべて適用された後、別のノードにライセンスを追加する場合は、ノードからライセンス権限を解放して使用可能なライセンス数を増やすことにより、ほかのノードでライセンス使用できるようにする必要があります。

ノードからライセンスを解放する方法

1. アプリケーションにログインします。
2. ホーム画面から、[ヘルプ] の [ライセンスの管理] をクリックして [ライセンス管理] ダイアログ ボックスを開きます。

[ライセンス管理] ダイアログ ボックスが以下のように表示され、物理コンピュータ、VMware ベースの仮想マシン、Hyper-V ベースの仮想マシンに適用されているライセンスのリストが表示されます。

ライセンス管理

マシンからライセンスを解放するには、ライセンスをクリックしてから目的のマシンをクリアしてください。

ライセンス ステータス		ライセンス			
コンポーネント名	バージョン	アクティブ	利用可能	合計	必要 (最小)
CA ARCserve Central Host-Based VM Backup r16.0 for Windows	16.0	0	1	1	0

ライセンスされたマシン

すべて選択 すべてクリア 適用 更新

ライセンス キー 追加

キーの形式: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

閉じる ヘルプ

3. [ライセンス ステータス] セクションで、ノードから解放するライセンスを選択します。

そのライセンスを使用しているノードは、[ライセンス管理] ダイアログ ボックスの [ライセンスされたマシン] セクションに表示されます。

4. ライセンスを解放するノードの横にあるチェック ボックスをオンにします。

注: [ライセンス管理] ダイアログ ボックスの [ライセンスされたマシン] セクションに表示されるすべてのノードのチェック ボックスをオフにする場合は、[すべてクリア] をクリックします。

5. [適用] をクリックします。

指定したノードからライセンスが解放されます。

6. (オプション) [更新] をクリックし、指定されたライセンスを使用するノードのリストを更新します。

モニタ サーバからノードのモニタを停止

CA ARCserve Central 仮想スタンバイ では、モニタ サーバの [Virtual Standby] タブからノードのモニタを停止することができます。

重要: ノードのモニタを停止した場合、仮想マシンの電源投入に必要な最新の復旧ポイント スナップショットが、仮想スタンバイ VM に含まれていない可能性があります。また、(手動で) モニタを停止したノードの仮想マシンの電源投入は、ハイパーバイザ システムからのみ行うことができます。

モニタ サーバからノードのモニタを停止する方法

1. モニタ サーバにログインします。

注: 詳細については、「[モニタ サーバへのログイン](#) (P. 72)」を参照してください。

2. モニタ サーバにログインしたら、[Virtual Standby] タブをクリックします。

[Virtual Standby] 画面が表示されます。

3. [ソース] ツリーですべてを展開し、[ソース実行中] - [要アクション] - [VM 実行中] を選択して、モニタを停止するソース ノードを探します。

4. モニタを停止するノードを右クリックし、ポップアップメニューで [モニタの停止] をクリックします。
警告メッセージが表示されます。
5. 指定したノードのモニタを停止してもよいことを確認したら、[はい] をクリックします。

ノードは、[ソース] ツリーから削除され、モニタ サーバはそのノードのモニタを停止します。

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 仮想スタンバイ 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、CA ARCserve Central 仮想スタンバイ サーバと CA ARCserve Central 仮想スタンバイ 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行います。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 仮想スタンバイ 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。	何も行う必要はありません。
ノードを追加した後で CA ARCserve Central 仮想スタンバイ 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. 75) 」を参照してください。
ノードを追加した後で CA ARCserve Central 仮想スタンバイ 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。注: 詳細については、「 ポリシーの展開 (P. 65) 」を参照してください。

ノードグループ管理タスク

Virtual Standby では、保護している CA ARCserve D2D ノードグループを管理することができます。

このセクションには、以下のトピックが含まれます。

[ノードグループの追加](#) (P. 84)

[ノードグループの変更](#) (P. 86)

[ノードグループの削除](#) (P. 87)

[ノードグループのフィルタ](#) (P. 88)

ノードグループの追加

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。

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。

ノード グループの削除

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。

ノードグループのフィルタ

Virtual Standby では、フィルタを使用して、特定のアプリケーションがインストールされたグループ内の **CA ARCserve D2D** ノードを表示できます。Virtual Standby は、以下のアプリケーションがインストールされたノードをフィルタできます。

- CA ARCserve Backup
- CA ARCserve D2D
- Microsoft SQL Server
- Microsoft Exchange Server

ノード グループをフィルタする方法

1. Virtual Standby サーバにログインし、Virtual Standby を開始します。

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 リストから、フィルタするグループを選択します。

注: すべてのデフォルト グループ (すべてのノード、未割り当て、SQL Server、Exchange) およびすべてのカスタム グループをフィルタできます。

[フィルタ] ツールバーから、フィルタするアプリケーションの横のチェック ボックスをオンにします。

ノード グループがフィルタされます。

Virtual Standby のポリシー管理タスク

Virtual Standby では、CA ARCserve D2D ノードを保護するために使用する変換ポリシーを管理できます。

- [CA ARCserve Central 仮想スタンバイ ポリシーの作成](#) (P. 47)
- [ノードのポリシーへの割り当て/割り当て解除](#) (P. 62)
 - [ポリシーの展開](#) (P. 65)
- [ポリシーの編集またはコピー](#) (P. 90)
- [ポリシーの削除](#) (P. 91)

ポリシーの編集またはコピー

Virtual Standby では、ポリシーを作成された後に編集またはコピーすることができます。

ポリシーを編集する方法

1. Virtual Standby サーバにログインし、Virtual Standby を開始します。

ホーム画面上のナビゲーションバーから、[ポリシー] をクリックします。

[ポリシー] ウィンドウが開きます。

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] フィールドに名前を指定します。
4. 選択したポリシーのタイプに基づいて、[Virtual Standby] タブと [環境設定] タブに変更を適用します。
 - [ローカル仮想スタンバイ ポリシー](#) (P. 48)
 - [リモート仮想スタンバイ ポリシー](#) (P. 56)

ポリシーが編集されます。

ポリシーの削除

Virtual Standby では、作成済みのポリシーを削除することができます。

注: Virtual Standby では、ノードに割り当てられているポリシーを削除することはできません。ノードに割り当てられたポリシーを削除するには、ポリシーからノードの割り当てを解除し、その後ポリシーを削除する必要があります。ポリシーからノードの割り当てを解除する方法については、「ポリシーからのノードの割り当て解除」を参照してください。

ポリシーを削除する方法

1. Virtual Standby サーバにログインし、Virtual Standby を開始します。
ホーム画面上のナビゲーションバーから、[VCM ポリシー] をクリックします。
[ポリシー] ウィンドウが開きます。
2. ポリシー リストから、削除するポリシーを選択します。
3. [ポリシー] ツールバーの [削除] をクリックします。
削除の確認メッセージが表示されます。
4. [はい] をクリックしてポリシーを削除します。

注: エラーのあるポリシーを削除した場合、ポリシーを再作成する必要があります。ノードを削除しない場合は [いいえ] をクリックします。

ポリシーが削除されます。

アプリケーション環境設定タスク

Virtual Standby では、電子メールアラート設定を指定し、Virtual Standby インストール環境を更新する方法を設定することができます。

このセクションには、以下のトピックが含まれます。

[電子メール設定の環境設定](#) (P. 92)

[自動更新の設定](#) (P. 93)

[ソーシャルネットワーキングの環境設定](#) (P. 97)

[管理者アカウントの変更](#) (P. 98)

電子メール設定の環境設定

アプリケーションで使用するための電子メール設定を指定して、指定した条件下でアラートを自動的に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] パネルで、[電子メール環境設定]をクリックすると、[電子メール環境設定] オプションが表示されます。
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. [保存] をクリックします。

注: [リセット] をクリックすると、事前に保存されていた値に戻ります。

電子メール環境設定が適用されます。

自動更新の設定

CA ARCserve Central 仮想スタンバイ では、製品の更新を確認する時期と、Virtual Standby インストール環境を更新する頻度を定義できます。

自動更新を設定する方法

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。

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。

ソーシャル ネットワーキング環境設定を設定する方法

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、[環境設定の設定] をクリックします。
[環境設定] オプションが表示されます。



ニュース フィード

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

ソーシャル ネットワーキング

☒ Facebook および Twitter へのリンクをメイン ページに表示

ビデオ

☐ CA サポート ビデオの使用 ☒ YouTube ビデオの使用

3. 必要なオプションを指定します。

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

[保存] ボタンをクリックします。

[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。

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。
 - **ファイルからのノードのインポート** -- ファイルからアプリケーションへの CA ARCserve D2D ノードのインポートに関する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。
 - **ハートビートの一時停止/再開** -- ハートビートを一時停止したか再開した仮想スタンバイ VM のログのみを表示します。

- ハートビートの一時停止/再開 -- 仮想スタンバイを一時停止または再開した仮想スタンバイ VM の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。
 - スタンバイ VM -- 電源がオンの仮想マシンのログのみを表示します。
 - CA ARCserve Replication からのノードのインポート -- CA ARCserve Replication からインポートされたノード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。

[更新] をクリックします。 

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。

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

Virtual Standby ホーム画面

モニタ サーバ上の [Virtual Standby] タブには、保護している CA ARCserve D2D サーバのすべてに関する情報を表示することができます。ただし、ソース サーバ上の [Virtual Standby] タブには、ユーザがログインしている特定のソース サーバに関する情報のみが表示されます。

このセクションには、以下のトピックが含まれます。

[Virtual Standby ホーム画面の使用方法](#) (P. 103)

[サーバリストの使用方法](#) (P. 105)

[最新の仮想スタンバイ ジョブに関するサマリ情報の表示](#) (P. 105)

[仮想変換ジョブのステータスのモニタ](#) (P. 107)

[ソース サーバの仮想スタンバイ設定の表示](#) (P. 108)

[復旧ポイントスナップショットのリストの表示](#) (P. 109)

Virtual Standby ホーム画面の使用方法

「仮想スタンバイ サマリ」画面には、現在のステータスを視覚的に伝えるアイコンが示され、緊急にアクションを必要とする場合の指示が表示されます。

ホーム画面には、以下のアイコンが表示されます。



成功
(アクションは必要はありません)



注意 - 潜在的な問題あり
(すぐにアクションが必要な場合があります)



危険/失敗 - 問題あり
(すぐにアクションが必要です)

[仮想スタンバイ サマリ] 画面には、以下の情報が表示されます。

- **サーバリスト** -- このモニタ サーバが保護しているソース サーバのリストが表示されます。リストではサーバがその現在のステータスによって並べ替えられます。（例：すべて、要アクション、ソース実行中）

注：サーバリストは、モニタ サーバにログインしている場合のみ表示されます。詳細については、「[サーバリストの使い方](#) (P. 105)」を参照してください。
- **仮想スタンバイ サマリ** -- 選択したソース サーバのサマリ情報が表示されます。詳細については、「[仮想変換ジョブのステータスのモニタ](#) (P. 107)」を参照してください。
- **仮想スタンバイ設定** -- 選択したソース サーバの仮想変換設定に関するサマリ情報が表示されます。詳細については、「[ソース サーバの仮想スタンバイ設定の表示](#) (P. 108)」を参照してください。
- **復旧ポイント スナップショット** -- 選択したソース サーバで使用可能な復旧ポイント スナップショットのリストが表示されます。詳細については、「[復旧ポイント スナップショットのリストの表示](#) (P. 109)」を参照してください。
- **タスク** -- 選択したソース サーバに対して実行可能なタスクのリストが表示されます。詳細については、「[仮想スタンバイ モニタ タスク](#) (P. 109)」を参照してください。
- **サポートおよびコミュニティへのアクセス** -- さまざまなサポート関連の機能を開始できるメカニズムを提供します。

注：サポートおよびコミュニティへのアクセスの詳細については、CA ARCserve D2D のマニュアルを参照してください。

サーバリストの使用方法

〔仮想スタンバイ サマリ〕画面上のサーバリストは、モニタ サーバが保護しているソース サーバのリストを表示します。リストではサーバがその現在のステータスによって並べ替えられます。たとえば、〔すべて〕、〔要アクション〕、〔ソース実行中〕などです。

メンテナンス タスクを実行する、または CA ARCserve D2D ノードに関する情報を表示するには、〔Virtual Standby〕タブをクリックし、以下の画面によって示されるようにサーバをクリックします。



最新の仮想スタンバイ ジョブに関するサマリ情報の表示

〔ノード〕画面では、ノードの最新の仮想スタンバイ（変換）ジョブに関するサマリ情報を表示できます。正常に完了または完了しなかった仮想スタンバイ ジョブに関する情報を表示できます。

次の手順に従ってください：

1. Virtual Standby サーバにログインします。

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。

2. [ステータス] 列で、以下に表示されているアイコンのいずれかにマウスのポインタを合わせます。



成功



警告



エラー/失敗

[ノードステータス サマリ] メッセージ ボックスが表示され、成功した最新の仮想スタンバイ ジョブの以下の結果が提供されます。

最新の仮想スタンバイ

最新の仮想スタンバイ ジョブが正常に完了したまたはしなかった日時。

復旧ポイント スナップショット

最新の仮想スタンバイの時点でノードに対して変換されている復旧ポイントの数を表示します。

デスティネーション ステータス

仮想スタンバイ デスティネーション上で利用可能な空きディスク容量を表示します。デスティネーションには以下を指定できます。

- ESX Server システムへの変換に使用される ESX Server データ ストア。
- Hyper-V サーバが復旧ポイント スナップショットを保存するボリューム上のディスク空き容量。

3. マウス ポインタを[ステータス]アイコンから離して、[ノードステータス サマリ] メッセージ ボックスを閉じます。
4. 成功したまたはしなかった最新の仮想スタンバイ ジョブの詳細情報は、以下のフィールドで確認できます。

最新の変換結果

正常に完了したまたはしなかった最新の仮想スタンバイ ジョブの結果。[完了]、[キャンセル]、[失敗] などがあります。

前回の変換時刻

成功したまたはしなかった最新の仮想スタンバイ ジョブが完了した日時。

仮想変換ジョブのステータスのモニタ

Virtual Standby では、進行中の仮想変換ジョブのステータスをモニタできます。また、Virtual Standby では、仮想変換データ、および CA ARCserve D2D ソース サーバを保護している仮想マシンに関するサマリ情報を表示できます。

仮想変換ジョブのステータスをモニタする方法

1. Virtual Standby を開き、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. [Virtual Standby] タブをクリックします。

(オプション) CA ARCserve D2D サーバがモニタ サーバである場合は、サーバリストをクリックし、[すべて]、[ソース実行]、または [要アクション] を展開し、モニタするサーバを選択します。

Virtual Standby に、進行中の仮想変換ジョブに関する情報、および仮想変換ジョブとサーバを保護している仮想マシンに関するサマリ情報が表示されます。



ソース サーバの仮想スタンバイ設定の表示

「仮想スタンバイ サマリ」画面には、ソース サーバを保護している仮想マシンに関する情報が表示されます。

仮想マシン情報	
タイプ:	VMware ESX
ESX ホスト名:	10.134.17.65
バージョン:	4.1.0
仮想マシン名:	reena-phy
プロセッサ:	1
メモリ:	1024 MB
データ ストア:	datastore1
ネットワーク アダプタ:	
▼ Broadcom BCM5708C NetXtreme II GigE (NDIS VBD クライアント)	
アダプタ タイプ:	E1000
ネットワーク接続:	VM Network
▼ Broadcom BCM5708C NetXtreme II GigE (NDIS VBD クライアント)	
アダプタ タイプ:	E1000
ネットワーク接続:	VM Network

復旧ポイント スナップショットのリストの表示

Virtual Standby 画面には、最新の復旧ポイント スナップショットのリストが表示されます。

リスト ボックスには、CA ARCserve D2D サーバのバックアップが完了した日付および時刻が表示されます。

復旧ポイント スナップショットのリストから、仮想マシンの電源をオンにすることができます。詳細については、「復旧ポイント スナップショットの電源投入」を参照してください。

復旧ポイント スナップショット - 電源オンの準備完了	
バックアップ時間	アクション
2011/06/13 15:33	 このスナップショットから VM の電源をオンにする
2011/06/13 15:33	 このスナップショットから VM の電源をオンにする
2011/06/13 15:45	 このスナップショットから VM の電源をオンにする
2011/06/13 15:55	 このスナップショットから VM の電源をオンにする
2011/06/13 16:05	 このスナップショットから VM の電源をオンにする
2011/06/13 17:30	 このスナップショットから VM の電源をオンにする
2011/06/13 18:35	 このスナップショットから VM の電源をオンにする
2011/06/13 18:45	 このスナップショットから VM の電源をオンにする

注：[仮想スタンバイ] デスティネーションが VMware ESX サーバである場合、表示される復旧ポイント スナップショットの最大数は 29 です。[仮想スタンバイ] デスティネーションが Microsoft Hyper-V サーバである場合、表示される復旧ポイント スナップショットの最大数は 24 です。

CA ARCserve Central 仮想スタンバイ モニタリング タスク

Virtual Standby では、以下の CA ARCserve D2D モニタ タスクを実行できます。

- ハートビートの一時停止および再開
- 仮想変換ジョブの一時停止および再開
- [仮想変換および復旧ポイント スナップショットに関するアクティビティ ログ データの表 \(P. 110\)](#) 示
- 復旧ポイント スナップショットの電源投入

ジョブに関するアクティビティ ログ データの表示

Virtual Standby では、仮想変換ジョブに関するアクティビティ ログ 情報の表示ができます。アクティビティ ログには、保護対象の CA ARCserve D2D ソース サーバの仮想変換ジョブ レコードが含まれます。

注: アクティビティ ログ (activity.log) は CA ARCserve D2D がインストールされているサーバの以下のディレクトリに保存されます。

C:\Program Files\CA\ARCserve D2D\Logs

ジョブに関するアクティビティ ログ データを表示する方法

1. Virtual Standby を開き、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。

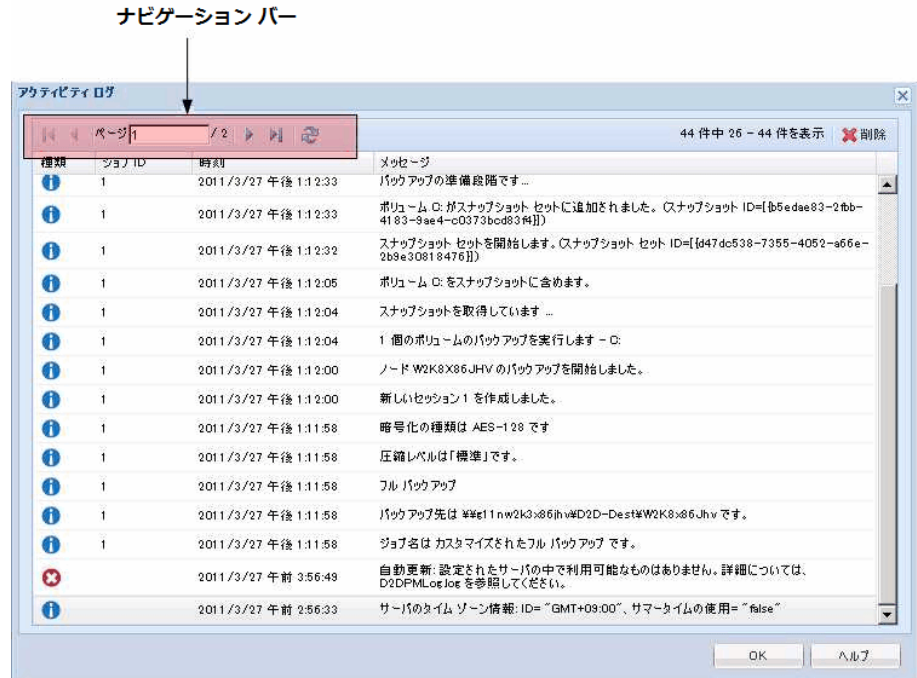
注: 新しいブラウザ ウィンドウが表示されない場合は、ブラウザのポップアップ オプションですべてのポップアップ、あるいはこの Web サイトのポップアップのみ許可されていることを確認します。

4. [Virtual Standby] タブをクリックします。
[仮想スタンバイ サマリ] 画面が表示されます。

5. (オプション) モニタ サーバにログインし、サーバリストから [すべて] または [ソース実行中] を展開して、アクティビティ ログ データを表示するノードをクリックします。

[仮想スタンバイ サマリ] 画面の右側にある仮想変換タスク リストから、[ログの表示] をクリックします。

[アクティビティ ログ] ウィンドウが表示されます。



ナビゲーション バーを使用してアクティビティ ログ レコードを検索および表示します。以下のアイコンがアクティビティ ログに表示されます。



注: アクティビティ ログ レコードの削除に関する情報については、「[アクティビティ ログ レコードの削除 \(P. 112\)](#)」を参照してください。

アクティビティ ログ レコードの削除

Virtual Standby では、アクティビティ ログ データの全体的なサイズを管理できます。アクティビティ ログには、保護対象の CA ARCserve D2D ソース ノードのジョブ レコードが含まれます。大量のソース サーバを保護している場合、頻繁なバックアップを実行している場合、またはその両方が当てはまる場合は、アクティビティ ログが CA ARCserve D2D ノード上のディスク容量を大量に消費する可能性があります。

指定した日付より古いアクティビティ ログ レコード、またはすべてのアクティビティ ログ レコードを削除できます。

注: アクティビティ ログ (activity.log) は CA ARCserve D2D がインストールされているサーバの以下のディレクトリに保存されます。

C:\Program Files\CA\ARCserve D2D\Logs

アクティビティ ログ レコードを削除する方法

1. Virtual Standby を開き、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. [Virtual Standby] タブをクリックします。
[仮想スタンバイ サマリ] 画面が表示されます。
5. (オプション) モニタ サーバにログインし、サーバ リストから [すべて] または [ソース 実行中] を展開して、アクティビティ ログ データを削除するノードをクリックします。

6. [仮想スタンバイ サマリ] 画面の右側にある仮想変換タスク リストから、[ログの表示] をクリックします。
[アクティビティ ログ] ウィンドウが表示されます。
 7. ツールバーの [削除] をクリックします。
[アクティビティ ログの削除] ダイアログ ボックスが表示されます。
 8. 以下のいずれかのオプションをクリックします。
 - **ログ レコードをすべて削除** -- アクティビティ ログ内のすべてのジョブレコードを削除します。
注: このオプションは慎重に使用してください。削除したアクティビティ ログ レコードは復旧できません。
 - **次の日付より前のログ レコードをすべて削除** -- 指定する日付より古い、アクティビティ ログ 内のジョブレコードをすべて削除します。
- [OK] をクリックします。

レコードがアクティビティ ログから削除されます。

Virtual Standby サーバからの仮想スタンバイ ジョブに関する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。進行中のスタンバイ ジョブに関するステータス情報を表示できます。

オプションで、Virtual Standby サーバまたは直接ノードからステータス情報にアクセスできます。ノードからステータス情報にアクセスする方法の詳細については、「[ノードからの仮想スタンバイ ジョブに関するステータス情報の表示](#) (P. 115)」を参照してください。

次の手順に従ってください:

1. Virtual Standby サーバにログインします。

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。

2. 進行中の仮想スタンバイ 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。

ノード名	ポリシー	仮想マシン名	vCenter/ESX	ジョブ
 **** *				
 <ノード名>	新規ポリシー	<仮想マシン名>	**** *	 **** * 接続中

3. フェーズをクリックして、[仮想スタンバイ ステータス モニタ] ダイアログ ボックスを開きます。

注: [仮想スタンバイ 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、「[仮想スタンバイ ステータス モニタ](#) (P. 116)」を参照してください。

4. [閉じる] をクリックし、[仮想スタンバイ ステータス モニタ] ダイアログ ボックスを閉じます。

ノードからの仮想スタンバイ ジョブに関する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。進行中の変換ジョブに関するステータス情報を表示することができます。

オプションで、Virtual Standby サーバまたは直接ノードからステータス情報にアクセスできます。Virtual Standby サーバからステータス情報にアクセスする方法の詳細については、「[Virtual Standby サーバからの仮想スタンバイ ジョブに関するステータス情報の表示 \(P. 114\)](#)」を参照してください。

次の手順に従ってください:

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 ノードにログインしました。

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. [Virtual Standby] タブをクリックします。

[仮想スタンバイ サマリ] 画面が表示されます。

進行中の仮想スタンバイ ジョブがある場合、以下に示すように、[ジョブ モニタ] フィールドにステータスのダイアログ ボックスが表示されます。



5. [詳細] をクリックして、仮想スタンバイ ステータス モニタを開きます。

注: [仮想スタンバイ 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、「[仮想スタンバイ ステータス モニタ \(P. 116\)](#)」を参照してください。

6. [閉じる] をクリックし、[仮想スタンバイ ステータス モニタ] ダイアログ ボックスを閉じます。

仮想スタンバイ ステータス モニタ

[仮想スタンバイ ステータス モニタ] が表示され、仮想スタンバイ ジョブに関する以下のリアルタイム情報が示されます。

フェーズ

変換処理の現在の段階を表示します。

ジョブのキャンセル

変換ジョブを終了します。

処理中

変換ジョブの全体的な進捗状況、およびアプリケーションが変換している復旧ポイントのセッション番号を表示します。

現在のプロビジョニング ポイント

アプリケーションが変換しているセッションに関するステータス情報を表示します。

ソース セッション

アプリケーションが変換しているセッション番号を指定します。

開始時刻

アプリケーションがセッションの変換を開始した日時を表示します。

経過時間

アプリケーションが現在のセッションの変換を開始してから経過した時間の長さを表示します。

スループット

アプリケーションがセッションを変換している速度を表示します。

推定残り時間

現在のソース セッションを変換するための推定残り時間を表示します。

すべてのセッション

アプリケーションが変換している、復旧ポイント内のすべてのセッションに関するステータス情報を表示します。

変換されたセッション数

プロビジョニング ポイントでの変換されたセッションの合計数を表示します。

経過時間

アプリケーションが復旧ポイントに含まれるすべてのセッションの変換を開始してから経過した時間を表示します。

推定残り時間

復旧ポイントに含まれるセッションをすべて変換するための推定残り時間を表示します。

保留中のセッション数

変換が保留されているセッションの数を表示します。

CA ARCserve D2D ノードに割り当てられたポリシーに関する情報の表示

アプリケーションでは、CA ARCserve D2D ノードに割り当てられた変換ポリシーに関する情報を表示することができます。

CA ARCserve D2D ノードに割り当てられたポリシーに関する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 ノードにログインしました。

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. [Virtual Standby] タブをクリックします。

[仮想スタンバイ サマリ] 画面が表示されます。

5. [仮想スタンバイ タスク] リストから、[仮想スタンバイ設定] をクリックします。

[仮想スタンバイ設定] ダイアログ ボックスが表示されます。

[仮想スタンバイ設定] ダイアログ ボックスでは、CA ARCserve D2D ノードに割り当てられたポリシーに定義されている仮想化サーバ、仮想マシン、代理サーバ、環境設定に関する情報を表示できます。[仮想スタンバイ設定] ダイアログ ボックスで、CA ARCserve D2D に割り当てられたポリシーを編集することはできません。

注: ポリシーを編集する方法の詳細については、「ポリシーの編集」を参照してください。

6. [キャンセル] をクリックして [仮想スタンバイ設定] ダイアログ ボックスを閉じます。

仮想スタンバイ設定

[仮想スタンバイ設定] ダイアログ ボックスには、ノードに割り当てられたポリシーに関する情報が含まれます。このダイアログ ボックスからポリシーを編集することはできません。**注:** 詳細については、「ポリシーの編集」を参照してください。

[Virtual Standby] タブには、以下のオプションが表示されます。

仮想化サーバオプション

■ VMware システム :

VMware システムに以下のオプションを適用します。

- 仮想化の種類 -- VMware
- ESX ホスト/vCenter -- ESX または vCenter Server システムのホスト名を指定します。
- ユーザ名 -- VMware システムへのログインに必要なユーザ名を特定します。
- パスワード -- VMware システムへのログインに必要なユーザのパスワードを特定します。
- プロトコル -- ソース CA ARCserve D2D ノードとモニタ サーバの間で使用される通信プロトコルを表示します。
- ポート -- ソース サーバとモニタ サーバの間でデータ転送に使用されるポートを指定します。

■ モニタリング :

VMware システムに以下のオプションを適用します。

- モニタ サーバ -- ソース サーバをモニタするサーバのホスト名を特定します。
- ユーザ名 -- モニタ サーバへのログインに必要なユーザ名を特定します。
- パスワード -- モニタ サーバへのログインに必要なユーザのパスワードを特定します。

- プロトコル -- CA ARCserve Central 仮想スタンバイ サーバと ESX Server システム（モニタ サーバ）の間で使用される通信プロトコルを特定します。
- ポート -- CA ARCserve Central 仮想スタンバイ サーバと ESX Server システム（モニタ サーバ）の間でデータ転送に使用されるポートを特定します。
- データ転送にプロキシとしてモニタ サーバを使用 -- モニタ サーバによって CA ARCserve D2D ソース サーバから ESX Server データストアに変換データをコピーする場合は、このオプションを特定します。

注: [データ転送にプロキシとしてモニタ サーバを使用] オプションはデフォルトで有効になっています。このオプションを無効にすると、CA ARCserve D2D ソース サーバが ESX Server データストアに変換データを直接コピーできるようになります。

■ **Hyper-V システム :**

Hyper-V システムに以下のオプションを適用します。

- 仮想化の種類 -- Hyper-V
- Hyper-V ホスト名 -- Hyper-V システムのホスト名を特定します。
- ユーザ名 -- Hyper-V システムへのログインに必要なユーザ名を特定します。
- パスワード -- Hyper-V システムへのログインに必要なユーザのパスワードを特定します。
- ポート -- ソース サーバとモニタ サーバの間でデータ転送に使用されるポートを指定します。

仮想マシン オプション

■ **VMware システム :**

- VM 名プレフィックス --ESX Server システム上の仮想マシンの表示名に追加されるプレフィックスを特定します。
デフォルト値: CAVM_
- VM リソース プール -- スタンバイ仮想マシンがグループ化されているリソース プールの名前を特定します。

- データ ストア -- 変換データを格納する場所を特定します。
 - すべての仮想マシン ソース ディスクに1つデータ ストアを使用します -- 仮想マシンに関連するディスクをすべて1つのデータ ストアにコピーするよう指定します。
 - 各 VM ソース ディスクのデータ ストアを選択します -- 仮想マシンのディスク関連情報を対応するデータ ストアにコピーするよう指定します。
- ネットワーク -- 仮想マシンと通信するために ESX Server システムが使用する NIC、仮想ネットワーク、およびパスを特定します。
 - 仮想 NIC をすべて以下の仮想ネットワークに接続します -- 仮想ネットワークにマップされる仮想 NIC を特定します。仮想マシンに仮想 NIC および仮想ネットワークが含まれる場合は、このオプションを指定します。
 - 各仮想 NIC の仮想ネットワークを選択します -- NIC が通信に使用する仮想ネットワークの名前を特定します。
- CPU 数 -- スタンバイ仮想マシンによってサポートされる最小および最大の CPU 数を特定します。
- メモリ -- スタンバイ仮想マシンに割り当てられる RAM の総量を MB で特定します。
- Hyper-V システム :
 - VM 名プレフィックス --Hyper-V システム上の仮想マシンの表示名に追加されるプレフィックスを特定します。
デフォルト値: CAVM_
 - パス -- 変換データが保存される Hyper-v Server 上の場所を特定します。
 - ネットワーク -- 仮想マシンと通信するために Hyper-V サーバが使用する NIC、仮想ネットワーク、およびパスを特定します。
 - CPU 数 -- スタンバイ仮想マシンによってサポートされる最小および最大の CPU 数を特定します。
 - メモリ -- スタンバイ仮想マシンに割り当てられる RAM の総量を MB で特定します。

代理設定

■ 復旧:

- 手動で仮想マシンを開始します -- ソース サーバが失敗するか通信を停止した場合に、手動で仮想マシンの電源をオンにしてプロビジョニングを行います。
- 自動的に仮想マシンを開始します -- ソース サーバが失敗するか通信を停止した場合に、自動的に仮想マシンの電源をオンにしてプロビジョニングを行います。

■ ハートビートプロパティ:

- タイムアウト -- 復旧ポイント スナップショットの電源がオンになる前に、モニタ サーバでハートビートを待機する必要がある時間を特定します。
- 周期 -- ソース サーバがハートビートをモニタ サーバに伝える周期を特定します。

[環境設定] タブには、以下のオプションが表示されます。

■ 電子メールアラート:

- ソース マシンのハートビートがありません -- モニタ サーバがソース サーバからのハートビートを検出しない場合、Virtual Standby がアラート通知を送信することを示します。
- 自動電源オンが設定されたソース マシンに対して VM の電源がオンになりました -- ハートビートが検出されない場合に自動的に電源がオンになるよう設定された仮想マシンの電源をオンにした場合、Virtual Standby がアラート通知を送信することを示します。
- 手動電源オンが設定されたソース マシンのハートビートがありません -- 自動的に電源がオンになるよう設定されていないソース サーバからハートビートを検出しない場合、Virtual Standby がアラート通知を送信することを示します。
- VM ストレージ空き容量が次の値より少ない -- 定義されたハイパーバイザ パス上のディスク空き容量が十分でないことが検出された場合、Virtual Standby がアラート通知を送信することを示します。これが検出されるのは、ディスク空き容量がユーザ定義のしきい値を下回った場合です。しきい値は、ボリュームの絶対値 (MB) またはその容量の割合として定義できます。

- **仮想スタンバイ エラー/失敗/クラッシュ** -- 変換処理中に発生したエラーを検出した場合、Virtual Standby がアラート通知を送信することを示します。
- **仮想スタンバイが成功** -- 仮想スタンバイ VM の作成プロセスが正常に完了したことを示します。
- **ハイパーバイザーがアクセス可能ではありません** -- ESX Server システムまたは Hyper-V システムと通信できないことを検出した場合、Virtual Standby がアラート通知を送信することを示します。
- **ライセンス エラー** -- Virtual Standby サーバ、ソース サーバ、およびモニタ サーバ上でライセンスの問題を検出した場合、Virtual Standby がアラート通知を送信することを示します。
- **仮想スタンバイは、復旧ポイント スナップショットから正常に開始しませんでした** -- 復旧ポイント スナップショットから仮想スタンバイ VM の作成プロセスが正常に完了しなかったことを示します。

Virtual Standby サーバからの仮想スタンバイ ジョブの一時停止および再開

仮想変換は、Virtual Standby が CA ARCserve D2D 復旧ポイントをソース ノードから仮想マシンデータ ファイル(復旧ポイント スナップショット)に変換するプロセスです。ソース ノードが失敗した場合、Virtual Standby は、復旧ポイント スナップショットを使用して、ソース ノードの仮想マシンの電源をオンにします。

ベストプラクティスとして、仮想変換プロセスが連続的に動作することを許可します。ただし、ローカルおよびリモートの Virtual Standby サーバ上の仮想変換プロセスを一時停止する場合、その操作を Virtual Standby サーバから実行できます。ソース サーバ上の問題を解決した後、仮想変換プロセスを再開できます。

仮想スタンバイ ジョブ (変換ジョブ) を一時停止しても、現在進行中の変換ジョブが一時停止することはありません。一時停止の操作は、次の CA ARCserve D2D バックアップ ジョブの最後に実行されるジョブのみに適用されます。その結果、(一時停止した) 変換ジョブを明示的に再開するまで、次の変換ジョブは開始しません。

注: オプションで、ノードから直接、仮想スタンバイ ジョブを一時停止および再開できます。詳細については、「ノードからの仮想スタンバイ ジョブの一時停止および再開」を参照してください。

次の手順に従ってください:

1. **Virtual Standby** サーバにログインし、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. 以下のいずれかのアクションを実行して、仮想スタンバイ ジョブを一時停止または再開するノードを指定します。
 - **ノード レベル**: 一時停止または再開するノードが含まれるグループをクリックし、次に一時停止または再開するノードの横のチェック ボックスをクリックします。
 - **グループ レベル**: 一時停止または再開するノードが含まれるグループをクリックします。
3. 以下のいずれかを行います。
 - ツールバー上の [仮想スタンバイ] をクリックし、ポップアップメニューの [一時停止] または [再開] をクリックして、変換ジョブを一時停止します。

選択したグループをクリックするか、ノードをクリックし、ポップアップメニューの [仮想スタンバイの一時停止] または [仮想スタンバイの再開] をクリックして、変換ジョブを再開します。

ノードからの仮想スタンバイ ジョブの一時停止および再開

仮想変換は、**Virtual Standby** が **CA ARCserve D2D** 復旧ポイントをソース ノードから仮想マシンデータ ファイル(復旧ポイント スナップショット)に変換するプロセスです。ソース ノードが失敗した場合、**Virtual Standby** は、復旧ポイント スナップショットを使用して、ソース ノードの仮想マシンの電源をオンにします。

ベストプラクティスとして、仮想変換プロセスが連続的に動作することを許可します。ただし、ローカルおよびリモートの **Virtual Standby** サーバ上の仮想変換プロセスを一時停止する場合、その操作を **Virtual Standby** サーバから実行できます。ソース サーバ上の問題を解決した後、仮想変換プロセスを再開できます。

仮想スタンバイ ジョブ(変換ジョブ)を一時停止しても、現在進行中の変換ジョブが一時停止することはありません。一時停止の操作は、次の **CA ARCserve D2D** バックアップ ジョブの最後に実行されるジョブのみに適用されます。その結果、(一時停止した)変換ジョブを明示的に再開するまで、次の変換ジョブは開始しません。

注: オプションで、**Virtual Standby** サーバから仮想スタンバイ ジョブを一時停止および再開できます。詳細については、「**Virtual Standby** サーバからの仮想スタンバイ ジョブの一時停止および再開」を参照してください。

次の手順に従ってください:

1. [仮想スタンバイ]を開き、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。
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て、指定したグループに関連付けられたすべてのノードを表示します。
3. 一時停止または再開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]をクリックして **CA ARCserve D2D**を開きます。
4. [Virtual Standby] タブをクリックして、[仮想スタンバイ サマリ]画面を開きます。

5. (オプション) モニタ サーバにログインしている場合、[サーバ] リストから [すべて] または [ソース実行中] を展開して、仮想スタンバイ ジョブを一時停止または再開するノードをクリックします。

注: 仮想スタンバイ変換ジョブが実行中の場合、[仮想スタンバイの一時停止] が仮想スタンバイ タスク リストに表示されます。仮想スタンバイ変換ジョブが実行中でない場合、[仮想スタンバイの再開] が仮想スタンバイ タスク リストに表示されます。

6. 以下のいずれかを行います。
 - [仮想スタンバイの一時停止] をクリックして、変換ジョブを一時停止します。

[仮想スタンバイの再開] をクリックして、変換ジョブを再開します。

Virtual Standby サーバからのハートビートの一時停止および再開

Virtual Standby では、モニタ サーバによって検出されたハートビートの一時停止および再開を行うことができます。ハートビートは、ソースサーバとモニタサーバがソースサーバの状態に関して通信するプロセスです。指定時間経過後もモニタサーバでハートビートが検出されない場合、**Virtual Standby** では、ソースノードとして機能するように仮想マシンをプロビジョニングします。

例: ハートビートを一時停止または再開するタイミング

以下の例では、ハートビートを一時停止および再開するタイミングについて説明します。

- ノード (ソースサーバ) をオフラインにしてメンテナンスする場合に、ハートビートを一時停止します。
- メンテナンスタスクが完了し、ノード (ソースサーバ) がオンラインになったら、ハートビートを再開します。

以下の動作に注意してください。

- グループ レベルまたは個別のノード レベルで、ハートビートを一時停止し再開できます。
- 1つの手順で1つ以上のノード用のハートビートを一時停止および再開できます。
- CA ARCserve Central 仮想スタンバイ では、ハートビートが一時停止状態である間は、復旧ポイント スナップショットの電源をオンにしません。
- ソース ノード上で CA ARCserve D2D インストールをアップグレードする場合、CA ARCserve Central 仮想スタンバイ はノードのハートビートを一時停止します。モニタ サーバがアップグレードされたノードを確実にモニタするようにするには、それらのノードでアップグレードが完了した後、ノードのハートビートを再開します。

注: オプションで、ノード上の [仮想スタンバイ サマリ] 画面から、ハートビートを一時停止および再開できます。詳細については、「ノードからのハートビートの一時停止および再開」を参照してください。

次の手順に従ってください:

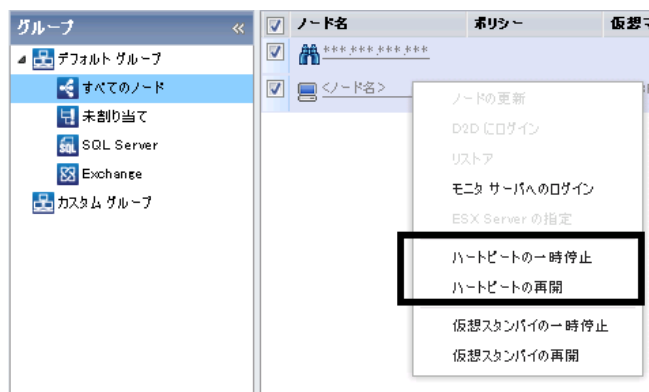
1. Virtual Standby サーバにログインします。
ナビゲーションバー上で [ノード] をクリックして、[ノード] 画面を開きます。
2. 以下のいずれかのアクションを実行して、一時停止または再開するノードを指定します。
 - **ノード レベル:** 一時停止または再開するノードが含まれるグループをクリックし、次に一時停止または再開するノードの横のチェック ボックスをクリックします。
 - **グループ レベル:** 一時停止または再開するノードが含まれるグループをクリックします。

3. 次に、以下のいずれかのアクションを実行して、ハートビートを一時停止または再開します。

- 以下の画面に示すように、ツールバー上の「ハートビート」をクリックし、ポップアップメニューの「一時停止」または「再開」をクリックします。



- 以下の画面に示すように、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、ポップアップメニューの「ハートビートの一時停止」または「ハートビートの再開」をクリックします。



ノードからのハートビートの一時停止および再開

Virtual Standby では、モニタ サーバによって検出されたハートビートの一時停止および再開を行うことができます。ハートビートは、ソース サーバとモニタ サーバがソース サーバの状態に関して通信するプロセスです。指定時間経過後もモニタ サーバでハートビートが検出されない場合、**Virtual Standby** では、ソース ノードとして機能するように仮想マシンをプロビジョニングします。

例: ハートビートを一時停止または再開するタイミング

以下の例では、ハートビートを一時停止および再開するタイミングについて説明します。

- ノード (ソース サーバ) をオフラインにしてメンテナンスする場合に、ハートビートを一時停止します。
- メンテナンス タスクが完了し、ノード (ソース サーバ) がオンラインになったら、ハートビートを再開します。

注: オプションで、**Virtual Standby** サーバ上の[ノード]画面からハートビートを一時停止および再開できます。詳細については、「**Virtual Standby** サーバからのハートビートの一時停止および再開」を参照してください。

次の手順に従ってください:

1. **Virtual Standby** サーバにログインします。

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。

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. ハートビートを一時停止または再開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 が開きます。

4. [Virtual Standby] タブをクリックします。

[仮想スタンバイ サマリ] 画面が表示されます。

5. (オプション) モニタ サーバにログインしたら、サーバリストから[すべて] または [ソース実行中] を展開し、ハートビートを一時停止または再開するノードをクリックします。

注: ハートビートが実行中の場合、[ハートビートの一時停止] が仮想変換タスク リストに表示されます。ハートビートが実行中でない場合は、[ハートビートの再開] が仮想変換タスク リストに表示されます。

6. 以下のいずれかを行います。

- ハートビートが実行中の場合は、[ハートビートの一時停止] をクリックしてハートビートを一時停止します。

例: メンテナンス タスクを実行するためにサーバをオフラインにする場合などです。

- ハートビートが実行中でない場合は、[ハートビートの再開] をクリックしてハートビートを再開します。

例: メンテナンス タスクが完了し、サーバをオンラインにする場合などです。

ハートビートが一時停止または再開されます。

サーバの通信プロトコルの変更

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

次の手順に従ってください:

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

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

2. Windows のコマンドラインを開きます。

3. 以下のいずれかを行います。

■ プロトコルを HTTP から HTTPS に変更：

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

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

プロトコルが正常に変更されると、以下のようなメッセージが表示されます。

通信プロトコルは HTTPS に変更されました。

■ プロトコルを HTTPS から HTTP に変更：

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

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

プロトコルが正常に変更されると、以下のようなメッセージが表示されます。

通信プロトコルは HTTP に変更されました。

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

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

第 6 章：仮想スタンバイ VM の電源オン

このセクションには、以下のトピックが含まれています。

[ローカル仮想スタンバイ VM の電源をオンにする方法](#) (P. 133)

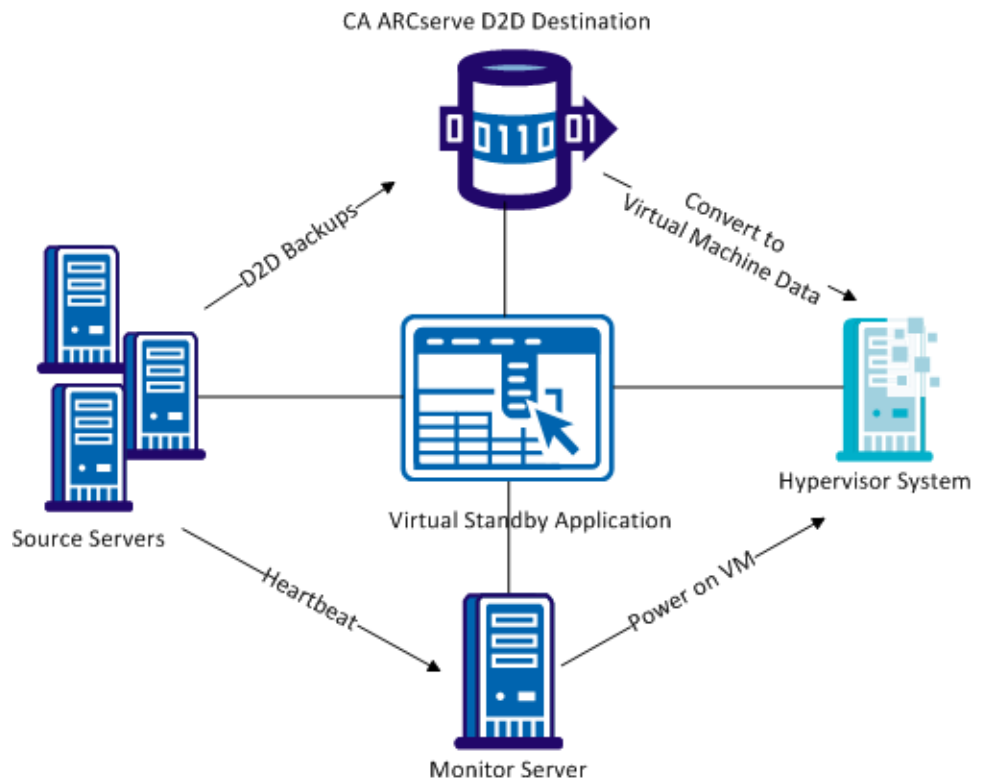
[リモート仮想スタンバイ VM の電源をオンにする方法](#) (P. 141)

[電源をオンにする NIC の数をアプリケーションが決定する方法](#) (P. 150)

[電源がオンになった仮想スタンバイ VM の保護方法](#) (P. 152)

ローカル仮想スタンバイ VM の電源をオンにする方法

このシナリオでは、ストレージ管理者が Virtual Standby サーバからのハートビートを一時停止および再開する方法、Virtual Standby サーバからの仮想変換処理を一時停止および再開する方法、仮想スタンバイ マシンの電源を自動的にオンにする方法、およびマシンの電源がオンになった後に仮想マシンを保護する方法について説明します。



以下の表に、仮想スタンバイ マシンの電源をオンにするタスクについて説明したトピックのリストを示します。

タスク	参照トピック
モニタ サーバがソース サーバからのハートビートを検出できないときに、自動的に復旧ポイント スナップショットから仮想スタンバイ VM の電源をオンにします。	復旧ポイント スナップショットからの仮想スタンバイ VM の電源投入 (P. 134)
仮想マシンの電源がオンになった後に仮想スタンバイ VM を保護します。	電源がオンになった後の仮想スタンバイ VM の保護 (P. 140)

復旧ポイント スナップショットからの仮想スタンバイ VM の電源投入

Virtual Standby では、モニタ サーバがソース サーバからのハートビートを検出しない場合に、復旧ポイント スナップショットから仮想スタンバイ VM の電源を自動的にオンにするように設定できます。さらに、ソース サーバの失敗、緊急事態の発生、またはメンテナンスのためにソース ノードをオフラインにする場合に、復旧ポイント スナップショットから仮想スタンバイ VM の電源を手動でオンにできます。

注: 以下の手順は、復旧ポイント スナップショットから仮想スタンバイ VM の電源を手動でオンにする方法について説明します。Virtual Standby で自動的に復旧ポイント スナップショットの電源を投入できるようにする方法については、「[CA ARCserve Central 仮想スタンバイ ポリシーの作成](#) (P. 47)」を参照してください。

次の手順に従ってください:

1. [仮想スタンバイ] を開き、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。
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、指定したグループに関連付けられているノードがすべて表示されます。

3. 復旧ポイント スナップショットから電源をオンにするノードを参照してクリックし、[アクション] ツールバーから [スタンバイ VM] をクリックします。

[復旧ポイント スナップショット] ダイアログ ボックスが表示されます。

4. [復旧ポイント スナップショット] ダイアログ ボックスで、以下のいずれかのオプションを実行します。

- 仮想マシンの電源をオンにする復旧ポイント スナップショットの日時範囲を選択します。

または

- [カスタマイズされたネットワーク設定でスタンバイ VM の電源をオンにする] チェック ボックスを選択して、[スタンバイ VM ネットワーク環境設定] ダイアログ ボックスを開きます。

注: スタンバイ VM がまだ設定されていない場合、[スタンバイ仮想マシン ネットワークが設定されていません] というリンクが表示されます。このリンクをクリックして、ネットワークを設定してください。

[保存] をクリックします。仮想スタンバイ VM の設定が保存されます。

[閉じる] をクリックすると、[復旧ポイント スナップショット] ダイアログ ボックスが表示されます。

[VM の電源をオンにする] をクリックします。

復旧ポイント スナップショットに含まれているデータを使用して仮想マシンの電源がオンになります。

注: 仮想マシンの電源がオンになった後、コンピュータの再起動を要求される場合があります。この動作は、VMware が仮想マシンに VMware Tools をインストールするか、または、Windows Hyper-V が仮想マシンに Integration Services をインストールするために発生します。

復旧ポイント スナップショットから仮想スタンバイ VM の電源を投入した後で、以下のタスクを完了する必要がある場合があります。

- 仮想マシンで実行する Windows オペレーティング システムをアクティブにします。
- 仮想マシン上の CA ARCserve D2D バックアップを開始します。

注: CA ARCserve Central Protection Manager を使用して、CA ARCserve D2D バックアップ ポリシーを作成および割り当てる方法の詳細については、「*CA ARCserve Central Protection Manager ユーザガイド*」を参照してください。

- 仮想マシンのホスト名、IP アドレスおよびログイン認証情報で CA ARCserve Central 仮想スタンバイ を更新します。
- ノードをポリシーに割り当てます。

注: このタスクは、電源投入した仮想マシンの復旧ポイント スナップショットを作成する場合にのみ必要です。詳細については、「[ポリシーへのノードの割り当て \(P. 62\)](#)」を参照してください。

Hyper-V マネージャからの仮想スタンバイ VM の電源投入

仮想スタンバイ VM の電源を手動でオンにする場合、CA ARCserve D2D サーバ上の仮想スタンバイ画面から仮想マシンの電源をオンにするのが最適な方法です。詳細については、「復旧ポイント スナップショットからの仮想スタンバイ VM の電源投入」を参照してください。ただし、Hyper-V サーバから仮想スタンバイ VM を開始する必要がある場合、Hyper-V マネージャを使用して行うことが可能です。

注: Hyper-V マネージャでは、ノードを保護するために CA ARCserve Central 仮想スタンバイ が作成した復旧ポイント スナップショットにアクセスできません。スナップショットを削除することはしないでください。スナップショットを削除すると、次回仮想スタンバイが実行された場合に、スナップショット内に含まれているデータの関係の整合性が失われます。データの整合性がないと、仮想スタンバイ VM の電源を適切にオンにすることができません。

Hyper-V マネージャから仮想スタンバイ VM の電源をオンにする方法

1. 保護しているノードをモニタしている Hyper-V サーバにログインします。
2. 以下の手順に従って Hyper-V マネージャを開始します。

[スタート] - [すべてのプログラム] - [管理ツール] をクリックし、Hyper-V マネージャをクリックします。

Hyper-V マネージャが開きます。

3. Hyper-V マネージャのディレクトリ ツリーから、Hyper-V マネージャを展開し、電源をオンにする仮想マシンが含まれる Hyper-V サーバをクリックします。

指定された hyper-V サーバに関連付けられた仮想マシンが、中央ペインの仮想マシン リストに表示されます。

4. 以下のいずれかを行います。
 - 最新のスナップショットを使用して仮想マシンの電源をオンにする：仮想マシン リストで、電源をオンにする仮想マシンを右クリックし、ポップアップメニューの [開始] をクリックします。
 - より古いスナップショットを使用して仮想マシンの電源をオンにする：
 - a. 仮想マシン リストで、電源をオンにする仮想マシンをクリックします。

仮想マシンに関連付けられたスナップショットが、スナップショット リストに表示されます。
 - b. 仮想マシンの電源をオンにするのに使用するスナップショットを右クリックし、ポップアップメニュー上の [適用] をクリックします。

スナップショットの適用ダイアログ ボックスが表示されます。
 - c. [適用] をクリックします。
 - d. 仮想マシン リストで、電源をオンにする仮想マシンを右クリックし、ポップアップメニューの [開始] をクリックします。

仮想スタンバイ VM の電源がオンになります。

必要に応じて、仮想マシンの電源をオンにした後、仮想マシンをバックアップして、復旧ポイント スナップショットを作成することができます。詳細については、「仮想スタンバイ VM の電源投入後に実行するタスク」を参照してください。

VMware vSphere Client からの仮想スタンバイ VM の電源投入

仮想スタンバイ VM の電源を手動でオンにする場合、CA ARCserve D2D サーバ上の仮想スタンバイ画面から仮想マシンの電源をオンにするのが最適な方法です。詳細については、「復旧ポイント スナップショットからの仮想スタンバイ VM の電源投入」を参照してください。ただし、ESX Server または vCenter Server システムから仮想スタンバイ VM を開始する必要がある場合、VMware vSphere Client を使用して行うことができます。

注: VMware vSphere Client では、ノードを保護するために CA ARCserve Central 仮想スタンバイ が作成した復旧ポイント スナップショットにアクセスできます。スナップショットを削除することはしないでください。スナップショットを削除すると、次回仮想スタンバイが実行された場合に、スナップショット内に含まれているデータの関係の整合性が失われます。データの整合性がないと、仮想スタンバイ VM の電源を適切にオンにすることができません。

VMware vSphere Client から仮想スタンバイ VM の電源をオンにする方法

1. VMware vSphere Client を開き、保護しているノードをモニタしている ESX Server または vCenter Server システムにログインします。

ディレクトリ ツリーから、ESX Server システムまたは vCenter Server システムを展開し、電源をオンにする仮想マシンを特定してクリックします。

2. 以下のいずれかを行います。
 - 最新のスナップショットを使用して仮想マシンの電源をオンにする： [使用方法] タブをクリックし、画面下部の [仮想マシンの電源をオンにする] をクリックします。
 - より古いスナップショットを使用して仮想マシンの電源をオンにする：
 - a. ツールバーのスナップショット マネージャ ボタンをクリックします。



該当する仮想マシンのスナップショット ダイアログ ボックスが開き、仮想マシンに対して利用可能なスナップショットのリストが表示されます。

- b. スナップショットのリストから、仮想マシンの電源をオンにするのに使用するスナップショットをクリックし、[選択] をクリックします。

仮想スタンバイ VM の電源がオンになります。

必要に応じて、仮想マシンの電源をオンにした後、仮想マシンをバックアップして、復旧ポイント スナップショットを作成することができます。詳細については、「仮想スタンバイ VM の電源投入後に実行するタスク」を参照してください。

電源がオンになった後の仮想スタンバイ VM の保護

仮想スタンバイ VM の電源が（手動でまたは自動で）投入されると、CA ARCserve D2D バックアップ ジョブおよび仮想スタンバイ ジョブはスケジュールしたとおりに実行されません。仮想スタンバイ VM の電源投入後にジョブを再開するには、以下を行います。

1. 仮想スタンバイ ポリシーの VM 名プレフィックスを変更します。

CA ARCserve Central 仮想スタンバイ が仮想スタンバイ VM の電源を投入すると、電源投入された仮想マシンの仮想マシン名は、仮想スタンバイ ポリシーで指定した VM 名プレフィックス オプションと、ソースノードのホスト名とが連結されたものになります。

例：

- VM 名プレフィックス：AA_
- ソース ノードのホスト名：Server1
- 仮想スタンバイ VM の仮想マシン名：AA_Server1

仮想スタンバイ VM の電源投入後、仮想スタンバイ ポリシーで VM 名プレフィックスを変更しないと、仮想マシン名の競合が発生する場合があります。このタイプの問題は、ソース ノードと仮想スタンバイ VM とが同じハイパーバイザ上にある場合に発生します。

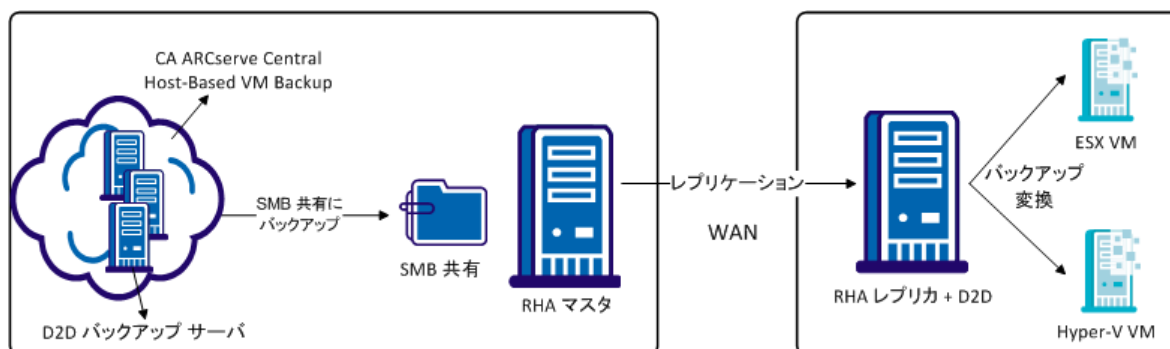
仮想スタンバイ ポリシーでの VM 名プレフィックス変更の詳細については、「[ポリシーの編集 \(P. 90\)](#)」を参照してください。必要に応じて、他の仮想スタンバイ ポリシー設定を更新できます。オプションで、新しい仮想スタンバイ ポリシーを作成して、仮想スタンバイ VM を保護できます。新規ポリシー作成の詳細については、「[CA ARCserve Central 仮想スタンバイ ポリシーの作成 \(P. 47\)](#)」を参照してください。

2. ポリシーの更新または新規ポリシーの作成後に、仮想スタンバイ VM にポリシーを展開します。注：詳細については、「[ポリシーの展開 \(P. 65\)](#)」を参照してください。
3. 仮想スタンバイ VM にポリシーを展開した後で、仮想スタンバイ ジョブを再開します。詳細については、「仮想スタンバイ ジョブの一時停止および再開」を参照してください。
4. ポリシーを展開した後で、仮想スタンバイ VM 上で CA ARCserve D2D にログインし、CA ARCserve D2D バックアップ ジョブの繰り返し方法をスケジュールします。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。

注: CA ARCserve Central Protection Manager および CA ARCserve Central 仮想スタンバイ には、管理対象の CA ARCserve D2D ノードに対して週次でポリシーを自動的に再同期する仕組みが備わっています。この仕組みでは、CA ARCserve D2D ノード上で有効だったポリシーを 仮想スタンバイ VM に再展開することにより、仮想スタンバイ VM 上で CA ARCserve Central Protection Manager にバックアップジョブを再起動させることができます。ポリシーの展開プロセスがこのように動作するのは、ソース ノードと仮想スタンバイ VM が同じホスト名を持つために、CA ARCserve Central Protection Manager によるポリシーの再同期が可能になるからです。この動作のただ一つの制限事項は、CA ARCserve Central Protection Manager サーバと仮想スタンバイ VM がネットワークを介して互いに通信可能であることです。CA ARCserve Central Protection Manager が仮想スタンバイ VM とポリシーを再同期および展開したら、仮想スタンバイ VM 上で仮想スタンバイ ジョブを再開します。詳細については、「仮想スタンバイ ジョブの一時停止および再開」を参照してください。

リモート仮想スタンバイ VM の電源をオンにする方法

このシナリオでは、ストレージ管理者が CA ARCserve Replication ですでに利用可能な機能を活用および統合して、CA ARCserve D2D および CA ARCserve Central Host-Based VM Backup 復旧ポイントをオフサイトの場所に移動する方法について説明します。この機能では、レプリケートされた復旧ポイントを CA ARCserve Central 仮想スタンバイ で変換し、Microsoft Hyper-V、VMWare vCenter、または ESXi のいずれかに自動登録できます。



以下の表に、仮想スタンバイ マシンの電源をオンにするタスクについて説明したトピックのリストを示します。

タスク	参照トピック
ソース サーバがダウンした場合に、レプリケートされた復旧ポイント スナップショットからリモート仮想スタンバイ VM の電源をオンにします。	復旧ポイント スナップショットからのリモート仮想スタンバイ VM の電源投入 (P. 142)
仮想マシンの電源がオンになった後に仮想スタンバイ VM を保護します。	電源がオンになった後の仮想スタンバイ VM の保護 (P. 149)

復旧ポイント スナップショットからのリモート仮想スタンバイ VM の電源投入

Virtual Standby では、ソース サーバのダウン、緊急事態の発生、またはメンテナンスのためにソース ノードをオフラインにする場合に、レプリケートされた復旧ポイント スナップショットからリモート仮想スタンバイ VM の電源をオンにするように設定できます。

注: 以下の手順で、レプリケートされた復旧ポイント スナップショットからリモート仮想スタンバイ VM の電源をオンにする方法について説明します。

次の手順に従ってください:

1. [仮想スタンバイ] を開き、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。
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 または CA ARCserve Central Host-Based VM Backup 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. レプリケートされた復旧ポイントから作成されたスタンバイ VM を持つノードを参照してクリックし、電源をオンにします。ポップアップメニューから以下のいずれかのオプションをクリックします。

- **スタンバイ VM ネットワーク環境設定 :**

- [ネットワーク アダプタ設定] タブで、仮想ネットワーク、NIC (ネットワーク インターフェース カード) 、および各ネットワーク アダプタの TCP/IP 設定を指定します。

または

- [DNS 更新設定] タブで、TCP/IP 設定に基づいてソース コンピュータから仮想スタンバイ VM にクライアントをリダイレクトする DNS サーバを更新します。

- **スタンバイ VM :**

- 仮想マシンの電源をオンにする復旧ポイント スナップショットの日時範囲を選択します。

または

- [カスタマイズされたネットワーク設定でスタンバイ VM の電源をオンにする] チェック ボックスを選択して、[スタンバイ VM ネットワーク環境設定] ダイアログ ボックスを開きます。

注: スタンバイ VM がまだ設定されていない場合、[スタンバイ仮想マシン ネットワークが設定されていません]というリンクが表示されます。このリンクをクリックして、ネットワークを設定してください。

[保存] をクリックします。

リモート仮想スタンバイ VM の設定が保存されます。

注: 仮想マシンの電源がオンになった後、コンピュータの再起動を要求される場合があります。この動作は、VMware が仮想マシンに VMware Tools をインストールするか、または、Windows Hyper-V が仮想マシンに Integration Services をインストールするために発生します。

復旧ポイント スナップショットからリモート仮想スタンバイ VM の電源をオンにした後に、以下のタスクの完了が必要になる場合があります。

- 仮想マシンで実行する Windows オペレーティング システムをアクティブにします。
- 仮想マシン上の CA ARCserve D2D バックアップを開始します。

注: CA ARCserve Central Protection Manager を使用して、CA ARCserve D2D バックアップ ポリシーを作成および割り当てる方法の詳細については、「*CA ARCserve Central Protection Manager ユーザガイド*」を参照してください。

- 仮想マシンのホスト名、IP アドレスおよびログイン認証情報で CA ARCserve Central 仮想スタンバイ を更新します。
- ノードをポリシーに割り当てます。

注: このタスクは、電源投入した仮想マシンの復旧ポイント スナップショットを作成する場合にのみ必要です。詳細については、「[ポリシーへのノードの割り当て \(P. 62\)](#)」を参照してください。

Hyper-V マネージャからのリモート仮想スタンバイ VM の電源投入

Hyper-V サーバからリモート仮想スタンバイ VM の電源をオンにする場合、Hyper-V マネージャを使用することができます。

注: Hyper-V マネージャを使用すると、ノードを保護するために CA ARCserve Replication/High Availability によってレプリケートされて CA ARCserve Central 仮想スタンバイ によって変換された復旧ポイント スナップショットにアクセスできます。スナップショットを削除することはしないでください。スナップショットを削除すると、次回仮想スタンバイ が実行された場合に、スナップショット内に含まれているデータの関係の整合性が失われます。データの整合性がないと、仮想スタンバイ VM の電源を適切にオンにすることができません。

次の手順に従ってください:

1. 保護しているノードをモニタしている **Hyper-V** サーバにログインします。
2. 以下の手順に従って **Hyper-V** マネージャを開始します。
[スタート] - [すべてのプログラム] - [管理ツール] をクリックし、次に [Hyper-V マネージャ] をクリックして **Hyper-V** マネージャを開きます。
3. **Hyper-V** マネージャのディレクトリ ツリーから、**Hyper-V** マネージャを展開し、電源をオンにする仮想マシンが含まれる **Hyper-V** サーバをクリックします。

指定された **hyper-V** サーバに関連付けられた仮想マシンが、中央ページの仮想マシン リストに表示されます。

4. 以下のいずれかを行います。

- **最新のスナップショットを使用してリモート仮想マシンの電源をオンにする：** 仮想マシン リストで、電源をオンにする仮想マシンを右クリックし、ポップアップメニューの「開始」をクリックします。
- **古いスナップショットを使用してリモート仮想マシンの電源をオンにする：**
 - a. 仮想マシン リストで、電源をオンにする仮想マシンをクリックします。

仮想マシンに関連付けられたスナップショットが、スナップショット リストに表示されます。
 - b. リモート仮想マシンの電源をオンにするために使用するスナップショットを右クリックし、ポップアップメニューの「適用」をクリックして、「スナップショットの適用」ダイアログボックスを開きます。
 - c. 「適用」をクリックします。
 - d. 仮想マシン リストで、電源をオンにする仮想マシンを右クリックし、ポップアップメニューの「開始」をクリックします。

リモート仮想スタンバイ VM の電源がオンになります。

必要に応じて、リモート仮想マシンの電源をオンにした後、リモート仮想マシンをバックアップして、復旧ポイント スナップショットを作成できます。詳細については、「仮想スタンバイ VM の電源投入後に実行するタスク」を参照してください。

VMware vSphere Client からのリモート仮想スタンバイ VM の電源投入

ESX Server または vCenter Server システムからリモート仮想スタンバイ VM の電源をオンにする場合、VMware vSphere Client を使用することができます。

注: VMware vSphere Client を使用すると、ノードを保護するために CA ARCserve Replication/High Availability によってレプリケートされて CA ARCserve Central 仮想スタンバイ によって変換された復旧ポイント スナップショットにアクセスできます。スナップショットを削除することはしないでください。スナップショットを削除すると、次回仮想スタンバイが実行された場合に、スナップショット内に含まれているデータの関係の整合性が失われます。データの整合性がないと、仮想スタンバイ VM の電源を適切にオンにすることができません。

次の手順に従ってください:

1. VMware vSphere Client を開き、保護しているノードをモニタしている ESX Server または vCenter Server システムにログインします。

ディレクトリ ツリーから、ESX Server システムまたは vCenter Server システムを展開し、電源をオンにする仮想マシンを特定してクリックします。

2. 以下のいずれかを行います。

- **最新のスナップショットを使用してリモート仮想マシンの電源をオンにする：** [使用方法] タブをクリックし、画面下部の [リモート仮想マシンの電源をオンにする] をクリックします。
- **古いスナップショットを使用してリモート仮想マシンの電源をオンにする：**
 - a. VMware vSphere Client から、スナップショットが必要な仮想マシン名を右クリックし、**Snapshot Manager** を選択します。 [<仮想マシン名> のスナップショット] ダイアログ ボックスが開き、リモート仮想マシンで利用可能なスナップショットのリストが表示されます。
 - b. スナップショットのリストから、リモート仮想マシンの電源をオンにするために使用するスナップショットをクリックし、[選択] をクリックします。

リモート仮想スタンバイ VM の電源がオンになります。

必要に応じて、リモート仮想マシンの電源をオンにした後、仮想マシンをバックアップして復旧ポイント スナップショットを作成できます。詳細については、「仮想スタンバイ VM の電源投入後に実行するタスク」を参照してください。

電源がオンになった後のリモート仮想スタンバイ VM の保護

リモート仮想スタンバイ VM の電源をオンにした後は、CA ARCserve D2D バックアップ ジョブおよび仮想スタンバイ ジョブはスケジュールどおりに実行されません。リモート仮想スタンバイ VM の電源投入後にジョブを再開するには、以下の操作を行います。

1. 仮想スタンバイ ポリシーの VM 名プレフィックスを変更します。

CA ARCserve Central 仮想スタンバイ がリモート仮想スタンバイ VM の電源を投入すると、電源投入されたリモート仮想マシンの仮想マシン名は、仮想スタンバイ ポリシーで指定した VM 名プレフィックス オプションと、ソース ノードのホスト名とが連結されたものになります。

例：

- VM 名プレフィックス：AA_
- ソース ノードのホスト名：Server1
- 仮想スタンバイ VM の仮想マシン名：AA_Server1

リモート仮想スタンバイ VM の電源投入後、仮想スタンバイ ポリシーで VM 名プレフィックスを変更しない場合、仮想マシン名の競合が発生することがあります。この問題は、ソース ノードとリモート仮想スタンバイ VM が同じハイパーバイザ上にある場合に発生します。

仮想スタンバイ ポリシーでの VM 名プレフィックス変更の詳細については、「ポリシーの編集」を参照してください。必要に応じて、他の仮想スタンバイ ポリシー設定を更新できます。オプションで、新しい仮想スタンバイ ポリシーを作成して、リモート仮想スタンバイ VM を保護できます。新規ポリシー作成の詳細については、「[CA ARCserve Central 仮想スタンバイ ポリシーの作成 \(P. 47\)](#)」を参照してください。

2. ポリシーの更新または新規ポリシーの作成後に、リモート仮想スタンバイ VM にポリシーを展開します。注：詳細については、「[ポリシーの展開 \(P. 65\)](#)」を参照してください。
3. リモート仮想スタンバイ VM にポリシーを展開した後に、仮想スタンバイ ジョブを再開します。詳細については、「[仮想スタンバイ ジョブの一時停止および再開 \(P. 123\)](#)」を参照してください。
4. ポリシーを展開した後に、リモート仮想スタンバイ VM 上で CA ARCserve D2D にログインし、CA ARCserve D2D バックアップ ジョブの繰り返し方法をスケジュールします。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。

注: CA ARCserve Central Protection Manager および CA ARCserve Central 仮想スタンバイ には、管理対象の CA ARCserve D2D ノードに対して週次でポリシーを自動的に再同期する仕組みが備わっています。この仕組みでは、CA ARCserve D2D ノード上で有効だったポリシーをリモート仮想スタンバイ VM に再展開することにより、CA ARCserve Central Protection Manager はリモート仮想スタンバイ VM 上でバックアップジョブを再起動することができます。ポリシーの展開プロセスがこのように動作するのは、ソースノードとリモート仮想スタンバイ VM が同じホスト名を持つために、CA ARCserve Central Protection Manager によるポリシーの再同期が可能になるからです。この動作のただ一つの制限事項は、CA ARCserve Central Protection Manager サーバとリモート仮想スタンバイ VM がネットワークを介して互いに通信可能でなければならないことです。CA ARCserve Central Protection Manager がリモート仮想スタンバイ VM にポリシーを再同期および展開したら、リモート仮想スタンバイ VM 上で仮想スタンバイジョブを再開します。詳細については、「[仮想スタンバイ ジョブの一時停止および再開 \(P. 123\)](#)」を参照してください。

電源をオンにする NIC の数をアプリケーションが決定する方法

仮想マシンの電源をオンにすると、Virtual Standby は、スタンバイ VM ネットワークが設定されているかどうかに基づいて、電源をオンにする NIC（ネットワーク インターフェース カード）の数を決定します。以下の表では、スタンバイ VM の電源をオンにするために必要な NIC の数を Virtual Standby がどのように決定するかを説明します

VM ネットワークのポリシーで定義された値	[カスタマイズされたネットワーク設定でスタンバイ VM の電源をオンにする]オプションが指定されていない	[カスタマイズされたネットワーク設定でスタンバイ VM の電源をオンにする]オプションが指定されている
定義された値がソース マシンと同一。	Virtual Standby は最後のバックアップジョブの時点でソース マシンに定義された数の NIC の電源をオンにします。	Virtual Standby は以下のうち、より大きな値に基づいた数の NIC の電源をオンにします。 <ul style="list-style-type: none">■ カスタム ネットワーク設定で定義された数。■ 最後のバックアップジョブの時点でソース マシンに定義された NIC の数。

VM ネットワークのポリシーで定義された値

[カスタマイズされたネットワーク設定でスタンバイ VM の電源をオンにする]オプションが指定されていない

[カスタマイズされたネットワーク設定でスタンバイ VM の電源をオンにする]オプションが指定されている

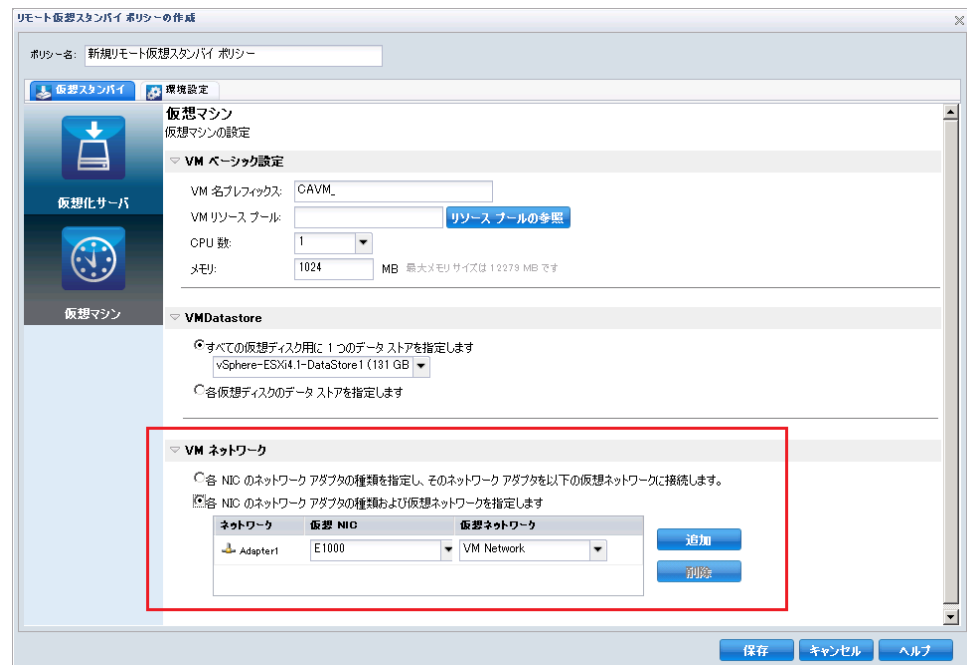
定義された値がカスタム値。

Virtual Standby はポリシーで定義されている数のカスタムネットワークの電源をオンにします。

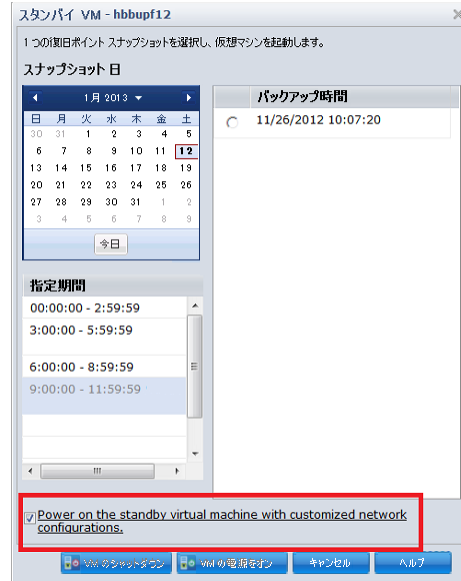
Virtual Standby は以下のうち、より大きな値に基づいた数の NIC の電源をオンにします。

- カスタム ネットワーク設定で定義された数。
- カスタム ポリシーで定義された NIC の数。

以下のダイアログ（ローカル仮想スタンバイ ポリシーの編集）では、電源をオンにする NIC のカスタム設定が含まれるポリシーの定義場所を示しています。



以下のダイアログ（スタンバイ VM - <ホスト名>）では、[カスタマイズされたネットワーク設定でスタンバイ VM の電源をオンにする] オプションを指定する場所を示しています。



電源がオンになった仮想スタンバイ VM の保護方法

仮想スタンバイ VM の電源が（手動でまたは自動で）投入されると、CA ARCserve D2D バックアップ ジョブおよび仮想スタンバイ ジョブはスケジュールしたとおりに実行されません。仮想スタンバイ VM の電源投入後にジョブを再開するには、以下を行います。

1. 仮想スタンバイ ポリシーの VM 名プレフィックスを変更します。

CA ARCserve Central 仮想スタンバイ が仮想スタンバイ VM の電源を投入すると、電源投入された仮想マシンの仮想マシン名は、仮想スタンバイ ポリシーで指定した VM 名プレフィックス オプションと、ソースノードのホスト名とが連結されたものになります。

例：

- VM 名プレフィックス：AA_
- ソース ノードのホスト名：Server1
- 仮想スタンバイ VM の仮想マシン名：AA_Server1

仮想スタンバイ VM の電源投入後、仮想スタンバイ ポリシーで VM 名プレフィックスを変更しないと、仮想マシン名の競合が発生する場合があります。このタイプの問題は、ソース ノードと仮想スタンバイ VM とが同じハイパーバイザ上にある場合に発生します。

仮想スタンバイ ポリシーでの VM 名プレフィックス変更の詳細については、「[ポリシーの編集 \(P. 90\)](#)」を参照してください。必要に応じて、他の仮想スタンバイ ポリシー設定を更新できます。オプションで、新しい仮想スタンバイ ポリシーを作成して、仮想スタンバイ VM を保護できます。新規ポリシー作成の詳細については、「[CA ARCserve Central 仮想スタンバイ ポリシーの作成 \(P. 47\)](#)」を参照してください。

2. ポリシーの更新または新規ポリシーの作成後に、仮想スタンバイ VM にポリシーを展開します。注：詳細については、「[ポリシーの展開 \(P. 65\)](#)」を参照してください。
3. 仮想スタンバイ VM にポリシーを展開した後で、仮想スタンバイ ジョブを再開します。詳細については、「仮想スタンバイ ジョブの一時停止および再開」を参照してください。
4. ポリシーを展開した後で、仮想スタンバイ VM 上で CA ARCserve D2D にログインし、CA ARCserve D2D バックアップジョブの繰り返し方法をスケジュールします。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。

注: CA ARCserve Central Protection Manager および CA ARCserve Central 仮想スタンバイ には、管理対象の CA ARCserve D2D ノードに対して週次でポリシーを自動的に再同期する仕組みが備わっています。この仕組みでは、CA ARCserve D2D ノード上で有効だったポリシーを 仮想スタンバイ VM に再展開することにより、仮想スタンバイ VM 上で CA ARCserve Central Protection Manager にバックアップ ジョブを再起動させることができます。ポリシーの展開プロセスがこのように動作するのは、ソース ノードと仮想スタンバイ VM が同じホスト名を持つために、CA ARCserve Central Protection Manager によるポリシーの再同期が可能になるからです。この動作のただ一つの制限事項は、CA ARCserve Central Protection Manager サーバと仮想スタンバイ VM がネットワークを介して互いに通信可能であることです。CA ARCserve Central Protection Manager が仮想スタンバイ VM とポリシーを再同期および展開したら、仮想スタンバイ VM 上で仮想スタンバイ ジョブを再開します。詳細については、「仮想スタンバイ ジョブの一時停止および再開」を参照してください。

第 7 章：データのリストア

このセクションには、以下のトピックが含まれています。

[CA ARCserve D2D 復旧ポイントからのデータのリストア \(P. 156\)](#)

[CA ARCserve D2D ファイル コピーからのデータのリストア \(P. 161\)](#)

[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 \(P. 167\)](#)

[ベア メタル復旧を使用したソース サーバの復旧 \(P. 173\)](#)

[Microsoft Exchange 電子メール メッセージのリストア \(P. 194\)](#)

CA ARCserve D2D 復旧ポイントからのデータのリストア

Virtual Standby では、利用可能な復旧ポイントからデータを回復することができます。復旧ポイントは、CA ARCserve D2D ソース ノード上に存在するデータのある時点でのスナップショットです。復旧ポイントから、回復するデータを指定できます。

CA ARCserve D2D の復旧ポイントからデータをリストアする方法

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、次に、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。

[復旧ポイントの参照] ダイアログ ボックスが表示されます。



3. 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。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。緑色の矢印で表示される検証アイコンをクリックすると、ソースの場所に正常にアクセスできるかどうかを検証します。
カレンダー表示では、表示期間にバックアップ ソースの復旧ポイントを含むすべての日付が（緑色で）強調表示されます。
4. リストアするデータを指定します。
 - a. カレンダーで、リストアするバックアップ 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。
 - b. リストア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。
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となる可能性があることを示します。
 - c. リストアするコンテンツを選択します。
 - ボリューム レベルのリストアの場合、ボリューム全体をリストアするか、ボリューム内のファイル/フォルダを選択してリストアするかを指定できます。
 - アプリケーション レベルのリストアの場合、アプリケーション全体をリストアするか、アプリケーション内のコンポーネント、データベース、インスタンスなどを選択してリストアするかを指定できます。
5. リストアするデータを指定したら [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。

6. [リストア オプション] ダイアログ ボックスで以下のオプションを入力します。

■ **デスティネーション** -- 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データをリストアします。
- 別の場所にリストアする -- バックアップ イメージをリストアする場所を指定するか、参照して選択します。[別の場所にリストアする] フィールドの横の矢印をクリックし、指定された場所への接続を確認します。

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。

■ **競合の解決** -- リストア処理中に競合が発生した場合、CA ARCserve D2D でどのように解決するかを指定します。

- 既存ファイルを上書きする -- リストア先に存在する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バックアップ ファイルからリストアされます。その際、マシン上に存在しているかどうかは考慮されません。
- アクティブ ファイルを置換する -- 再起動時にアクティブな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であることが CA ARCserve D2D によって検出された場合、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 -- ファイル名がすでに存在する場合に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、ファイル名は変えず、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。そのコンピュータ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。

- **ディレクトリ構造** -- リストア処理中に CA ARCserve D2D でディレクトリ構造に対して何を実行するかを指定します。
 - ルートディレクトリを作成する -- キャプチャされたバックアップイメージ内にルートディレクトリ構造が存在する場合、CA ARCserve D2D によって、リストア先のパス上に同じルートディレクトリ構造が再作成されます。

[ルートディレクトリを作成する]オプションが選択されない場合（チェックボックスをオフにした場合）、リストアされるファイル/フォルダはリストア先のフォルダに直接リストアされます。

例：

バックアップ時に、ファイル「C:¥Folder1¥SubFolder2¥A.txt」および「C:¥Folder1¥SubFolder2¥B.txt」をキャプチャし、リストア時にリストア先として「D:¥Restore」を指定したとします。

ファイル「A.txt」および「B.txt」を個々にリストアする場合、リストアされるファイルのリストア先は

「D:¥Restore¥A.txt」および「D:¥Restore¥B.txt」になります（指定されたファイルレベルより上のルートディレクトリは再作成されません）。

「SubFolder2」レベルからリストアする場合、リストアされるファイルのリストア先は

「D:¥Restore¥SubFolder2¥A.txt」および

「D:¥Restore¥SubFolder2¥B.txt」になります（指定されたファイルレベルより上のルートディレクトリは再作成されません）。

[ルートディレクトリを作成する]オプションが選択された場合（チェックボックスをオンにした場合）、ファイル/フォルダのルートディレクトリパス全体（ボリューム名を含む）が、リストア先のフォルダに再作成されます。リストア対象のファイル/フォルダが、同一ボリューム名からリストアされる場合は、リストア先のルートディレクトリパスにそのボリューム名は含まれません。ただし、リストア対象のファイル/フォルダが、異なるボリューム名からリストアされる場合は、リストア先のルートディレクトリパスにボリューム名が含まれます。

例：

バックアップ時に、ファイル「C:¥Folder1¥SubFolder2¥A.txt」、
「C:¥Folder1¥SubFolder2¥B.txt」、および

「E:¥Folder3¥SubFolder4¥C.txt」をキャプチャし、リストア時にリストア先として「D:¥Restore」を指定したとします。

「A.txt」ファイルのみをリストアするよう選択した場合、リストアされるファイルのリストア先は

「D:¥Restore¥ Folder1¥SubFolder2¥A.txt」になります（ルートディレクトリ構造が、ボリューム名なしで再作成されます）。

「A.txt」と「C.txt」の両方のファイルをリストアするよう選択した場合、リストアされるファイルのリストア先は

「D:¥Restore¥C¥Folder1¥SubFolder2¥A.txt」および

「D:¥Restore¥E¥Folder3¥SubFolder4¥C.txt」になります（ルートディレクトリ構造が、ボリューム名付きで再作成されます）。

- **暗号化パスワード** -- リストアしようとしている復旧ポイントデータが暗号化されている場合、暗号化パスワードを提供する必要があります。

暗号化されたバックアップが実行されたマシンと同じマシンにリストアする場合、パスワードは必要とされません。しかし、別のマシンへのリストアを試行する場合は、パスワードが必要になります。

注: 以下のアイコンは、復旧ポイントに暗号化された情報が含まれていてリストアにパスワードが必要かどうかを示します。

暗号化されていない復旧ポイント



暗号化された復旧ポイント



[次へ] をクリックします。

[リストア サマリ] ダイアログ ボックスが表示されます。

7. [リストア サマリ] ダイアログ ボックスの情報が正しいことを確認します。

注: 指定したリストア オプションを変更する場合は、[前へ] をクリックし、該当するダイアログ ボックスに戻って値を変更します。

[完了] ボタンをクリックします。

リストア オプションが適用され、データが回復されます。

CA ARCserve D2D ファイル コピーからのデータのリストア

Virtual Standby では、CA ARCserve D2D ファイル コピーからデータを回復することができます。ファイル コピーは、ディスクやクラウドなどのオフラインストレージにコピーされた CA ARCserve D2D 復旧ポイントのコピーです。ファイル コピーから、回復するデータを指定できます。

CA ARCserve D2D ファイル コピーからデータをリストアする方法

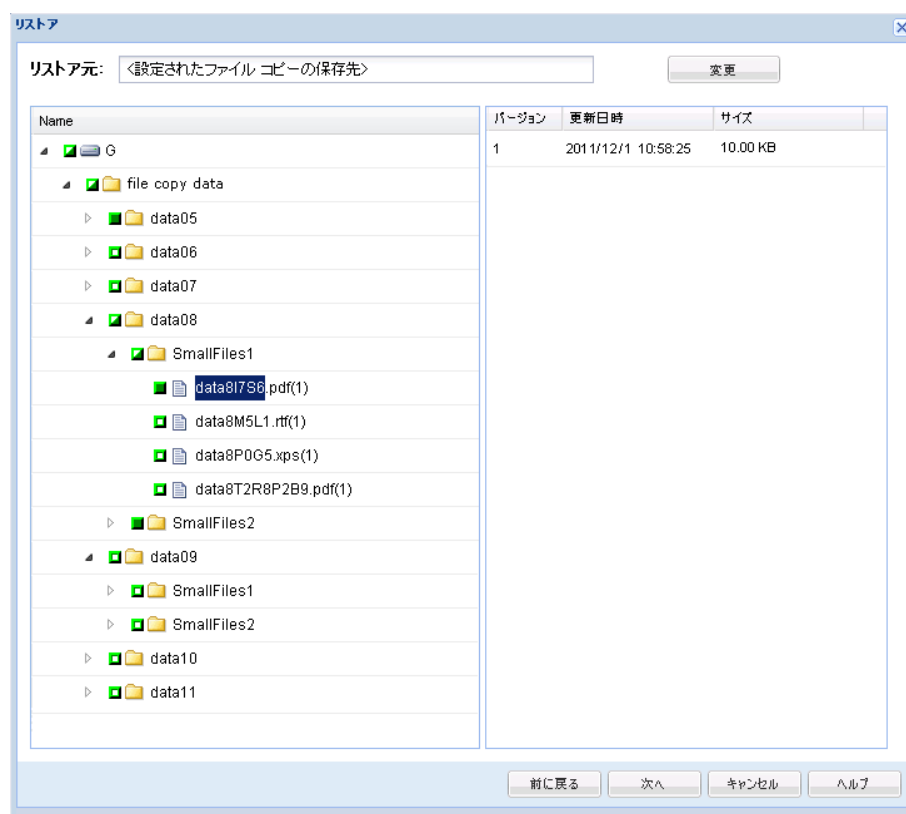
1. アプリケーションにログインし、ナビゲーションバー上の [ノード] をクリックします。

[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、次に、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、[ファイル コピーの参照] をクリックします。

以下のように、[ファイル コピーの参照] ダイアログ ボックスが表示されます。

注: 右ペインに表示されているデスティネーションはデフォルトのデスティネーションです。

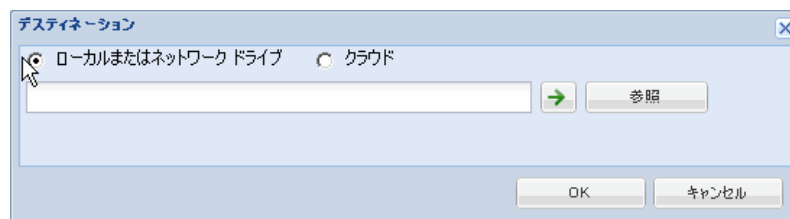


3. [名前] ペインから、回復するファイル コピー データを指定します。ファイルとフォルダ、またはボリュームの組み合わせを自由に指定できます。

個別のファイルを選択する場合、そのファイルのコピーされたバージョンがすべて右ペインに表示されます。複数のバージョンが利用可能な場合は、回復する対象のファイル コピー バージョンを選択します。

- **デスティネーションの変更** -- ファイル コピー イメージが保存されている別の場所を参照できます。

利用可能な他のデスティネーション オプションを示すダイアログボックスが表示されます。



- ローカルまたはネットワーク ドライブ -- [バックアップ場所の選択] ダイアログ ボックスが表示され、別の場所としてローカルまたはネットワーク ドライブを参照して選択することができます。
 - クラウド -- [クラウド環境設定] ダイアログ ボックスが表示され、別のクラウド場所にアクセスして選択できるようになります。
4. [次へ] をクリックします。
- [リストア オプション] ダイアログ ボックスが表示されます。
5. [リストア オプション] ダイアログ ボックスで以下のオプションを入力します。
- デスティネーション -- 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データをリストアします。
 - 別の場所にリストアする -- バックアップ イメージをリストアする場所を指定するか、参照して選択します。[別の場所にリストアする] フィールドの横の矢印をクリックし、指定された場所への接続を確認します。
- 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。

■ **競合の解決** -- リストア処理中に競合が発生した場合、CA ARCserve D2D でどのように解決するかを指定します。

- 既存ファイルを上書きする -- リストア先に存在する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バックアップファイルからリストアされます。その際、マシン上に存在しているかどうかは考慮されません。
- アクティブ ファイルを置換する -- 再起動時にアクティブな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であることが **CA ARCserve D2D** によって検出された場合、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 -- ファイル名がすでに存在する場合に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、ファイル名は変えず、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。そのコンピュータ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。

- **ディレクトリ構造** -- リストア処理中に CA ARCserve D2D でディレクトリ構造に対して何を実行するかを指定します。
 - ルートディレクトリを作成する -- キャプチャされたバックアップイメージ内にルートディレクトリ構造が存在する場合、CA ARCserve D2D によって、リストア先のパス上に同じルートディレクトリ構造が再作成されます。

[ルートディレクトリを作成する]オプションが選択されない場合（チェックボックスをオフにした場合）、リストアされるファイル/フォルダはリストア先のフォルダに直接リストアされます。

例：

バックアップ時に、ファイル「C:¥Folder1¥SubFolder2¥A.txt」および「C:¥Folder1¥SubFolder2¥B.txt」をキャプチャし、リストア時にリストア先として「D:¥Restore」を指定したとします。

ファイル「A.txt」および「B.txt」を個々にリストアする場合、リストアされるファイルのリストア先は

「D:¥Restore¥A.txt」および「D:¥Restore¥B.txt」になります（指定されたファイルレベルより上のルートディレクトリは再作成されません）。

「SubFolder2」レベルからリストアする場合、リストアされるファイルのリストア先は

「D:¥Restore¥SubFolder2¥A.txt」および「D:¥Restore¥SubFolder2¥B.txt」になります（指定されたファイルレベルより上のルートディレクトリは再作成されません）。

[ルートディレクトリを作成する]オプションが選択された場合（チェックボックスをオンにした場合）、ファイル/フォルダのルートディレクトリパス全体（ボリューム名を含む）が、リストア先のフォルダに再作成されます。リストア対象のファイル/フォルダが、同一ボリューム名からリストアされる場合は、リストア先のルートディレクトリパスにそのボリューム名は含まれません。ただし、リストア対象のファイル/フォルダが、異なるボリューム名からリストアされる場合は、リストア先のルートディレクトリパスにボリューム名が含まれます。

例：

バックアップ時に、ファイル「C:¥Folder1¥SubFolder2¥A.txt」、
「C:¥Folder1¥SubFolder2¥B.txt」、および
「E:¥Folder3¥SubFolder4¥C.txt」をキャプチャし、リストア時にリストア先として「D:¥Restore」を指定したとします。

「A.txt」ファイルのみをリストアするよう選択した場合、リストアされるファイルのリストア先は

「D:¥Restore¥ Folder1¥SubFolder2¥A.txt」になります（ルートディレクトリ構造が、ボリューム名なしで再作成されます）。

「A.txt」と「C.txt」の両方のファイルをリストアするよう選択した場合、リストアされるファイルのリストア先は

「D:¥Restore¥C¥Folder1¥SubFolder2¥A.txt」および

「D:¥Restore¥E¥Folder3¥SubFolder4¥C.txt」になります（ルートディレクトリ構造が、ボリューム名付きで再作成されます）。

- **暗号化パスワード** -- リストアしようとしている復旧ポイントデータが暗号化されている場合、暗号化パスワードを提供する必要があります。

暗号化されたバックアップが実行されたマシンと同じマシンにリストアする場合、パスワードは必要とされません。しかし、別のマシンへのリストアを試行する場合は、パスワードが必要になります。

注: 以下のアイコンは、復旧ポイントに暗号化された情報が含まれていてリストアにパスワードが必要かどうかを示します。

暗号化されていない復旧ポイント



暗号化された復旧ポイント



[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. [リストア サマリ] ダイアログ ボックスの情報が正しいことを確認します。

注: 指定したリストア オプションを変更する場合は、[前へ] をクリックし、該当するダイアログ ボックスに戻って値を変更します。

[完了] ボタンをクリックします。

リストア オプションが適用され、データが回復されます。

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

Virtual Standby では、リストアする特定のファイルまたはフォルダの CA ARCserve D2D 復旧ポイントおよびファイル コピーを検索することができます。

リストアするファイル/フォルダの検索を使用してデータをリストアする方法

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、次に、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。
[リストアするファイル/フォルダの検索] ダイアログ ボックスが表示されます。

リストア

リストアするファイル/フォルダの検索

検索場所

☒ バックアップ場所 <バックアップ場所> 参照

☐ ファイル コピーの場所 変更

検索対象

ファイル/フォルダ名 *.txt

検索パス

☒ サブディレクトリを含める

検索

リストアするバージョンの選択

名前	サイズ	更新日	ファイル コピー/バックアップ
C:\AMD\FireGL_Win2kXP_40334\ScanVirus_040334_PostWHQL.txt			
ScanVirus_040334_PostWHQL.txt	892 バイト	2006/12/20 午後 5:32:38	バックアップ
C:\D2DPMConfig.txt			
D2DPMConfig.txt	842 バイト	2011/4/22 午後 8:32:22	バックアップ
C:\D2DPMUninstall.txt			
D2DPMUninstall.txt	692 バイト	2011/4/22 午後 7:52:34	バックアップ
C:\Documents and Settings\Administrator\Cookies\administrator@de11[1].txt			
administrator@de11[1].txt	652 バイト	2011/4/5 午後 8:11:08	バックアップ

次へ キャンセル ヘルプ

3. 検索する場所（バックアップ/アーカイブ ソース）を指定します。

バックアップ/アーカイブ イメージが保存されている場所を指定するか、参照して選択します。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。緑色の矢印で表示される検証アイコンをクリックすると、ソースの場所に正常にアクセスできるかどうかを検証します。

4. 検索対象（リストアするファイルまたはフォルダ名）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、ファイル名またはディレクトリ名の 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。

注： 必要に応じて、パスを指定して検索をさらにフィルタしたり、サブディレクトリを含めるかどうかを選択したりできます。

5. [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（最も最近のものがリストの最初に）表示されます。 また、検索されたファイルがバックアップされたものかアーカイブされたものかを示します。

6. リストアするファイル/フォルダのバージョン（インスタンス）を選択して [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。

7. [リストア オプション] ダイアログ ボックスで以下のオプションを入力します。

- **デスティネーション** -- 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データをリストアします。
 - 別の場所にリストアする -- バックアップ イメージをリストアする場所を指定するか、参照して選択します。 [別の場所にリストアする] フィールドの横の矢印をクリックし、指定された場所への接続を確認します。

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。

■ **競合の解決** -- リストア処理中に競合が発生した場合、CA ARCserve D2D でどのように解決するかを指定します。

- 既存ファイルを上書きする -- リストア先に存在する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バックアップファイルからリストアされます。その際、マシン上に存在しているかどうかは考慮されません。
- アクティブ ファイルを置換する -- 再起動時にアクティブな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であることが **CA ARCserve D2D** によって検出された場合、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（リストアはすぐには実行されますが、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 -- ファイル名がすでに存在する場合に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、ファイル名は変えず、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。そのコンピュータ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。

- ディレクトリ構造 -- リストア処理中に CA ARCserve D2D でディレクトリ構造に対して何を実行するかを指定します。
 - ルートディレクトリを作成する -- キャプチャされたバックアップイメージ内にルートディレクトリ構造が存在する場合、CA ARCserve D2D によって、リストア先のパス上に同じルートディレクトリ構造が再作成されます。

[ルートディレクトリを作成する]オプションが選択されない場合（チェックボックスをオフにした場合）、リストアされるファイル/フォルダはリストア先のフォルダに直接リストアされます。

例：

バックアップ時に、ファイル「C:¥Folder1¥SubFolder2¥A.txt」および「C:¥Folder1¥SubFolder2¥B.txt」をキャプチャし、リストア時にリストア先として「D:¥Restore」を指定したとします。

ファイル「A.txt」および「B.txt」を個々にリストアする場合、リストアされるファイルのリストア先は

「D:¥Restore¥A.txt」および「D:¥Restore¥B.txt」になります（指定されたファイルレベルより上のルートディレクトリは再作成されません）。

「SubFolder2」レベルからリストアする場合、リストアされるファイルのリストア先は

「D:¥Restore¥SubFolder2¥A.txt」および「D:¥Restore¥SubFolder2¥B.txt」になります（指定されたファイルレベルより上のルートディレクトリは再作成されません）。

[ルートディレクトリを作成する]オプションが選択された場合（チェックボックスをオンにした場合）、ファイル/フォルダのルートディレクトリパス全体（ボリューム名を含む）が、リストア先のフォルダに再作成されます。リストア対象のファイル/フォルダが、同一ボリューム名からリストアされる場合は、リストア先のルートディレクトリパスにそのボリューム名は含まれません。ただし、リストア対象のファイル/フォルダが、異なるボリューム名からリストアされる場合は、リストア先のルートディレクトリパスにボリューム名が含まれます。

例：

バックアップ時に、ファイル「C:¥Folder1¥SubFolder2¥A.txt」、
「C:¥Folder1¥SubFolder2¥B.txt」、および
「E:¥Folder3¥SubFolder4¥C.txt」をキャプチャし、リストア時にリストア先として「D:¥Restore」を指定したとします。

「A.txt」ファイルのみをリストアするよう選択した場合、リストアされるファイルのリストア先は

「D:¥Restore¥ Folder1¥SubFolder2¥A.txt」になります（ルートディレクトリ構造が、ボリューム名なしで再作成されます）。

「A.txt」と「C.txt」の両方のファイルをリストアするよう選択した場合、リストアされるファイルのリストア先は

「D:¥Restore¥C¥Folder1¥SubFolder2¥A.txt」および

「D:¥Restore¥E¥Folder3¥SubFolder4¥C.txt」になります（ルートディレクトリ構造が、ボリューム名付きで再作成されます）。

- **暗号化パスワード** -- リストアしようとしている復旧ポイントデータが暗号化されている場合、暗号化パスワードを提供する必要があります。

暗号化されたバックアップが実行されたマシンと同じマシンにリストアする場合、パスワードは必要とされません。しかし、別のマシンへのリストアを試行する場合は、パスワードが必要になります。

注: 以下のアイコンは、復旧ポイントに暗号化された情報が含まれていてリストアにパスワードが必要かどうかを示します。

暗号化されていない復旧ポイント



暗号化された復旧ポイント



[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。

8. [リストア サマリ] ダイアログ ボックスの情報が正しいことを確認します。

注: 指定したリストア オプションを変更する場合は、[前へ] をクリックし、該当するダイアログ ボックスに戻って値を変更します。

[完了] ボタンをクリックします。

リストア オプションが適用され、データが回復されます。

ベア メタル復旧を使用したソース サーバの復旧

ユーザによる問題の修正後またはソース サーバのメンテナンス実行後、**Virtual Standby** では、ソース サーバを最後の正常な状態に復旧し、復旧ポイント スナップショットの電源がオンだった間の増分を含めることができます。

この復旧プロセスは、**V2P**（仮想 - 物理）復旧と呼ばれます。

V2P 復旧プロセスは、**CA ARCserve D2D** ベア メタル復旧（**BMR**）プロセスを利用して仮想マシンから物理マシンにデータをリストアします。**BMR** 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リストアの再インストール、およびその後のデータと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 を実行する前に、以下を準備する必要があります。

- 利用可能なフル バックアップが少なくとも 1 つ。
- 復旧する仮想マシンおよびソース サーバ上にインストールされた少なくとも **1GB** の **RAM**。
- **VMware** 仮想マシンを、物理サーバとして動作するよう設定された **VMware** 仮想マシンに復旧するには、**VMware Tools** アプリケーションがデスティネーション仮想マシンにインストールされていることを確認します。

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

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

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

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

ISO または BMR USB メモリの作成方法の詳細については、「CA ARCserve D2D ユーザ ガイド」の「ブート キットの作成方法」を参照してください。

データの回復は、以下の表に示されている方法を使用して行うことができます。

復旧方法	詳細情報
Hyper-V ベースの仮想スタンバイ VM に変換されたデータからソース サーバを復旧します。	Hyper-V 仮想スタンバイ VM からのデータを使用したソース サーバの復旧 (P. 180)。
VMware ベースの仮想スタンバイ VM に変換されたデータからソース サーバを復旧します。	VMware 仮想スタンバイ VM からのデータを使用したソース サーバの復旧 (P. 187)。

BMR 操作メニューの管理

BMR 操作メニューは、以下の 3 種類の操作で構成されます。

- ディスク固有の操作
- Volume/Partition 固有の操作
- BMR 固有の操作

ディスク固有の操作:

ディスク固有の操作を実行するには、ディスク ヘッドを選択し、[操作] をクリックします。

ディスクの消去

この操作ではディスクのすべてのパーティションの消去、および以下を行うことができます。

- ディスクのすべてのボリュームを削除する代替方法として使用できます。ディスクの消去操作では、ボリュームを 1 つずつ削除する必要はありません。
- Windows 以外のパーティションを削除できます。VDS の制限事項により、Windows 以外のパーティションは UI から削除できませんが、この操作を使用すれば、すべて削除できます。

注: BMR 中、デスティネーションディスクに Windows 以外のパーティションまたは OEM パーティションがある場合、そのパーティションを BMR UI から選択して削除することはできません。このような事態が発生するのは、デスティネーションディスク上に Linux/Unix をインストールしていた場合です。この問題を解決するには、以下のいずれかのタスクを実行します。

- BMR UI 上のディスク ヘッドを選択し、[操作] をクリックし、[ディスクの消去] 操作を使用して、ディスク上のパーティションをすべて消去します。
- コマンドプロンプトを開いて「Diskpart」と入力し、Diskpart コマンドコンソールを開きます。次に、「select disk x」、「clean」と入力し、ディスク上のすべてのパーティションを消去します。「x」はディスク番号を表します。

MBR に変換

この操作は、ディスクを **MBR**（マスタ ブート レコード）に変換するために使用します。この操作は、選択したディスクが **GPT**（GUID パーティション テーブル）ディスクで、このディスク上にボリュームがない場合にのみ利用できます。

GPT に変換

この操作はディスクを **GPT** に変換するために使用します。この操作は、選択したディスクが **MBR** ディスクで、このディスク上にボリュームがない場合にのみ利用できます。

ベーシックに変換

この操作はディスクをベーシックに変換するために使用します。この操作は、選択したディスクがダイナミック ディスクで、このディスク上にボリュームがない場合にのみ利用できます。

ダイナミックに変換

この操作はディスクをダイナミック ディスクに変換するために使用します。選択したディスクがベーシック ディスクの場合にのみ利用できます。

オンライン ディスク

この操作はディスクをオンラインにするために使用します。選択したディスクがオフライン ステータスの場合にのみ利用できます。

ディスクのプロパティ

この操作は、ディスク プロパティの詳細を表示するために使用します。この操作は、いつでも利用することができます。この操作を選択すると、[ディスク プロパティ] ダイアログ ボックスが表示されます。

Volume/Partition 固有の操作:

ボリューム/パーティションの操作を実行するには、ディスクのボディ領域を選択し、[操作] をクリックします。このメニューから、ソース ボリューム上のディスク パーティションに対応する新しいパーティションを作成することができます。

プライマリ パーティションの作成

この操作はベーシック ディスク上でパーティションを作成するために使用します。選択した領域が未割り当てのディスク領域である場合にのみ利用できます。

論理パーティションの作成

この操作はベーシック MBR ディスク上に論理パーティションを作成するために使用します。選択した領域が拡張パーティションである場合にのみ利用できます。

拡張パーティションの作成

この操作は、ベーシック MBR ディスク上に拡張パーティションを作成するために使用します。ディスクが MBR ディスクで、選択した領域が未割り当てのディスク領域である場合にのみ利用できます。

システム予約済みパーティションの作成

この操作は、BIOS ファームウェア システム上でシステム予約済みパーティションを作成し、ソースの EFI パーティションとのマッピング関係を作成するために使用します。UEFI システムを BIOS システム上にリストアする場合にのみ利用できます。

注: 過去に UEFI から BIOS 互換のシステムに切り替えている場合は、[システム予約済みパーティションの作成] 操作を使用してデステネーション ディスクのサイズを変更してください。

EFI システム パーティションの作成

この操作はベーシック GPT ディスク上に EFI システム パーティションを作成するために使用します。ターゲット マシンのファームウェアが UEFI で、選択したディスクがベーシック GPT ディスクである場合にのみ利用できます。

注: 過去に BIOS から UEFI 互換のシステムに切り替えている場合は、[EFI システム パーティションの作成] 操作を使用してデステネーション ディスクのサイズを変更してください。

注: UEFI をサポートするシステムでは、ブートパーティションが GPT (GUID パーティションテーブル) ディスクに存在している必要があります。MBR (マスタブートレコード) ディスクを使用している場合は、このディスクを GPT ディスクに変換してから、[EFI システムパーティションの作成] 操作を使用してデスティネーションディスクのサイズを変更する必要があります。

ボリューム サイズの変更

この操作はボリューム サイズを変更するために使用します。
Windows の「ボリュームの拡張/ボリュームの圧縮」の代わりに使用できます。選択した領域が、有効なディスク パーティションである場合にのみ利用できます。

ボリュームの削除

この操作はボリュームを削除するために使用します。選択した領域が、有効なボリュームである場合にのみ利用できます。

拡張パーティションの削除

この操作は拡張パーティションを削除するために使用します。選択した領域が拡張パーティションである場合にのみ利用できます。

ボリューム プロパティ

この操作は、ボリューム プロパティの詳細を表示するために使用します。この操作を選択すると、[ボリューム プロパティ] ダイアログ ボックスが表示されます。

BMR 固有の操作:

これらの操作は BMR に固有の操作です。BMR 操作を実行するには、ディスク ヘッダまたはディスク ボディ領域を選択し、[操作] をクリックします。

ディスクのマップ元

この操作はソースとターゲットのダイナミック ディスク間のマッピング関係を作成するために使用します。選択したディスクがダイナミック ディスクの場合にのみ利用できます。

注: 別のディスクにマップする場合、マップされた各ターゲット ボリュームの容量は同じサイズか、対応するソース ボリュームより大きくする必要があります。

ボリュームのマップ元

この操作はソースとターゲットのベーシック ボリューム間のマッピング関係を作成するために使用します。選択したボリュームがベーシック ボリュームの場合にのみ利用できます。

注: 別のディスクにマップする場合、マップされた各ターゲット ボリュームの容量は同じサイズか、対応するソース ボリュームより大きくする必要があります。

コミット

この操作はいつでも利用することができます。すべての操作はメモリにキャッシュされ、[コミット] 操作を選択するまで、ターゲット ディスクは変更されません。

リセット

この操作はいつでも利用することができます。[リセット] 操作は、操作を破棄し、ディスク レイアウトをデフォルト ステータスにリストアするために使用します。この操作はキャッシュされた操作をすべて消去します。「リセット」とは、環境設定ファイルおよび現在の OS からソースとターゲットのディスク レイアウト情報を再ロードし、ユーザによって変更されたすべてのディスク レイアウト情報を破棄することを意味します。

Hyper-V 仮想スタンバイ VM からのデータを使用したソース サーバの復旧

Hyper-V 仮想スタンバイ VM に変換された CA ARCserve D2D データを使用して、ソース サーバを復旧することができます。

注: アプリケーションでは、Hyper-V 仮想マシンからソース サーバを復旧するためにベア メタル復旧プロセスを使用します。詳細については、「[ベア メタル復旧を使用したソース サーバの復旧 \(P. 173\)](#)」を参照してください。

CA ARCserve D2D は、V2P (Virtual-to-Physical) マシンに対してベア メタル復旧を実行する機能を提供します。この機能を使用して、スタンバイ仮想マシンの最新の状態から V2P 復旧を実行し、本稼働マシンの損失を減らすのに役立てることができます。

「Hyper-V 仮想スタンバイ VM を使用して回復する」オプションを選択した場合、ベア メタル復旧手順に戻ってプロセスを完了する前に、以下の手順に従います。

次の手順に従ってください:

1. ベア メタル復旧 (BMR) のタイプを選択するウィザード画面から、
「Hyper-V Virtual Standby VM を使用して回復する」オプションを選択します。

ARCserve D2D Bare Metal Recovery

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

回復の種類を指定してください:

☐ CA ARCserve D2D を使用してバックアップされたデータを回復する
(CA ARCserve D2D または CA ARCserve Host-Level Virtual Machine Backup アプリケーションを使用するバックアップ セッション)

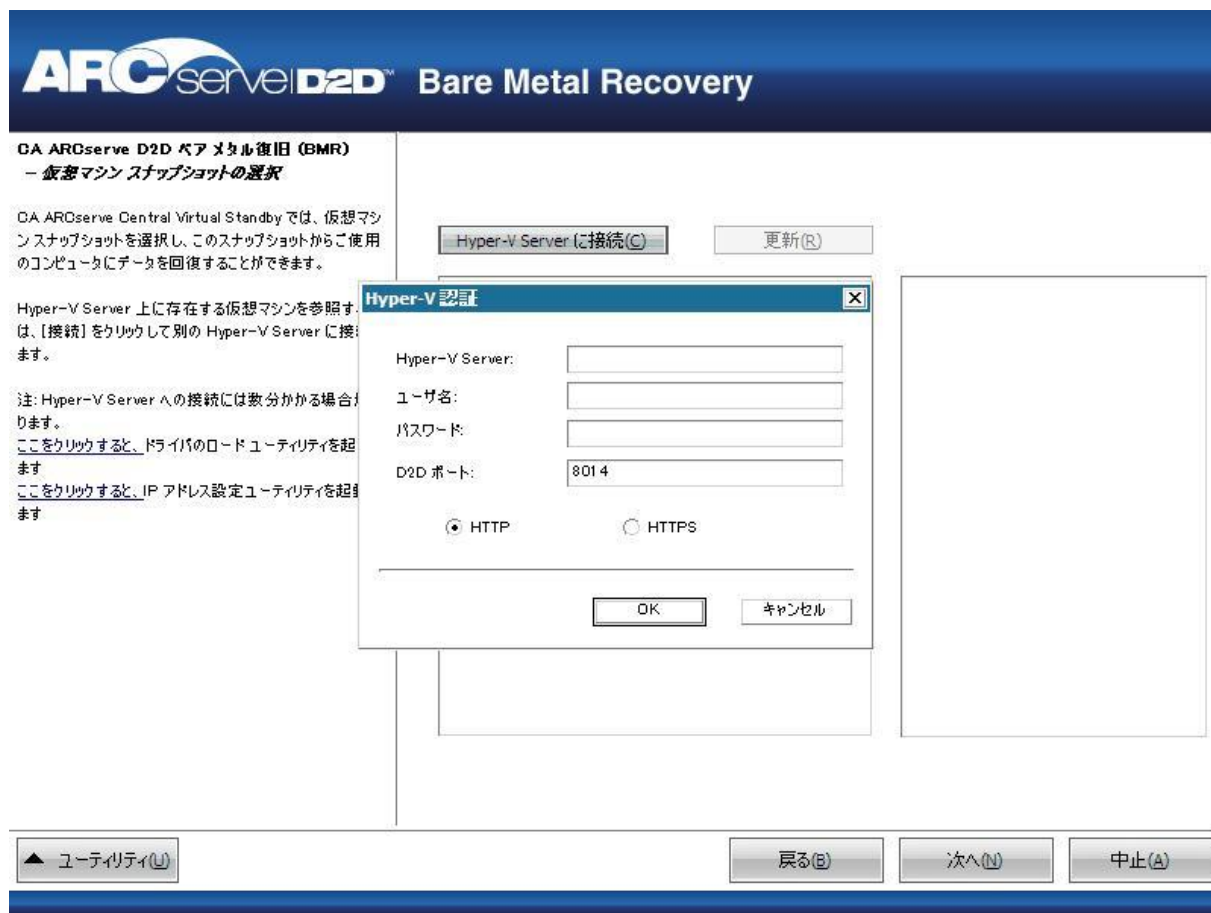
☒ Hyper-V Virtual Standby VM を使用して回復する
(CA ARCserve Central Virtual Standby を使用して仮想変換が実行された場合にのみ、データを回復できます)

☐ VMware Virtual Standby VM を使用して回復する
(CA ARCserve Central Virtual Standby を使用して仮想変換が実行された場合にのみ、データを回復できます)

▲ ユーティリティ(U) 戻る(B) 次へ(N) 中止(A)

2. 「次へ」をクリックします。

「仮想マシンスナップショットの選択」画面が「Hyper-V 認証」ダイアログボックスと共に表示され、Hyper-V サーバの詳細を入力するよう要求します。



3. 認証情報を入力して「OK」をクリックします。

CA ARCserve D2D は Hyper-V サーバを検出し、CA ARCserve Central 仮想スタンバイを使用して、指定された Hyper-V サーバに変換されるすべての仮想マシンのリストと共に表示します。



4. バックアップ イメージの復旧ポイント スナップショットを含む仮想マシンを選択します。

選択した仮想マシンのバックアップ セッション (復旧ポイント スナップショット) が表示されます。



5. 復旧する仮想マシンバックアップセッション（復旧ポイント スナップショット）を選択します。

選択した復旧ポイント スナップショットの詳細（仮想マシン名、バックアップセッション名、バックアップ ボリューム）が、右側ペインに表示されます。

リスト表示された復旧ポイントのうちの1つを選択し、さらに、「現在の状態」または「最新の状態」を選択することができます。

- 復旧元の仮想マシンの電源がオンである場合、「現在の状態」の復旧ポイントが表示されます。
- 復旧元の仮想マシンの電源がオフである場合、「最新の状態」の復旧ポイントが表示されます。

「最新の状態」復旧ポイントを選択すると、エラー メッセージが表示されます。復旧元の復旧ポイントは（現在ではなく）最新の状態であり、復旧処理を続行する前に仮想マシンを起動させるよう要求します。

- リストア対象の復旧ポイントであることを確認した後、[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。

この手順の残りについては、「ベア メタル復旧の実行」を参照し、復旧モードが選択された時点の対応する手順から続行してください。



ARCserve D2D Bare Metal Recovery

CA ARCserve D2D ベア メタル復旧 (BMR)

復旧モードの選択

どちらの復旧モードを使用しますか?

☒ 高速モード (H)

高速モードでは、マシンのデフォルト設定を使用し、ユーザの操作を最小限に抑えてシステムを自動的に復旧できます。

☐ 拡張モード (D)

拡張モードではリストア処理をカスタマイズできます。このモードを使用すると、以下を実行できます：
パーティション ボリュームまたはダイナミック ディスク上のデータ リストア先を選択する。
再起動する前に、ドライバをインストールする。

! 注：[次へ] をクリックすると、BMR ウィザードは、ソース マシン上に存在するパーティションと一致する、新しいパーティションをデスティネーション上に作成します。そのため、デスティネーション マシン上の既存のパーティションが破壊され、新しいパーティションが作成される場合があります。

▲ ユーティリティ (U) 戻る (B) 次へ (N) 中止 (A)

VMware 仮想スタンバイ VM からのデータを使用したソース サーバの復旧

VMware 仮想スタンバイ VM に変換された CA ARCserve D2D データを使用して、ソース サーバを復旧することができます。

注: アプリケーションでは、VMware 仮想マシンからソース サーバを復旧するためにベア メタル復旧プロセスを使用します。詳細については、「[ベア メタル復旧を使用したソース サーバの復旧 \(P. 173\)](#)」を参照してください。

CA ARCserve D2D は、V2P (Virtual-to-Physical) マシンに対してベア メタル復旧を実行する機能を提供します。この機能を使用して、スタンバイ仮想マシンの最新の状態から V2P 復旧を実行し、本稼働マシンの損失を減らすのに役立てることができます。

〔VMware 仮想スタンバイ VM を使用して回復する〕 オプションを選択した場合、ベア メタル復旧手順に戻ってプロセスを完了する前に、以下の手順に従います。

次の手順に従ってください:

1. ベア メタル復旧 (BMR) のタイプを選択するウィザード画面から、
〔VMware Virtual Standby VM を使用して回復する〕 オプションを選択します。



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

回復の種類を指定してください:

- ☐ CA ARCserve D2D を使用してバックアップされたデータを回復する

(CA ARCserve D2D または CA ARCserve Host-Level Virtual Machine Backup アプリケーションを使用するバックアップ セッション)

- ☐ Hyper-V Virtual Standby VM を使用して回復する

(CA ARCserve Central Virtual Standby を使用して仮想変換が実行された場合にのみ、データを回復できます)

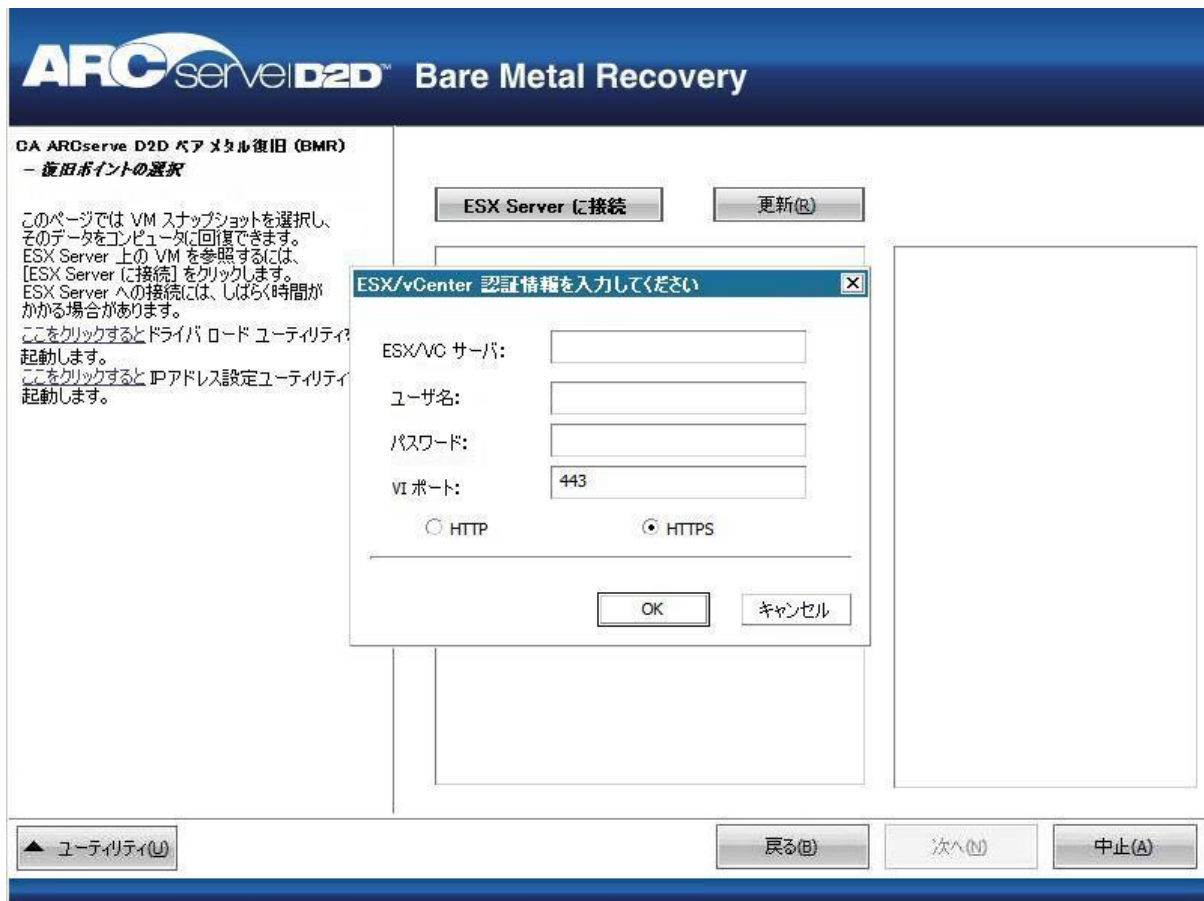
- ☒ VMware Virtual Standby VM を使用して回復する

(CA ARCserve Central Virtual Standby を使用して仮想変換が実行された場合にのみ、データを回復できます)



2. 「次へ」 をクリックします。

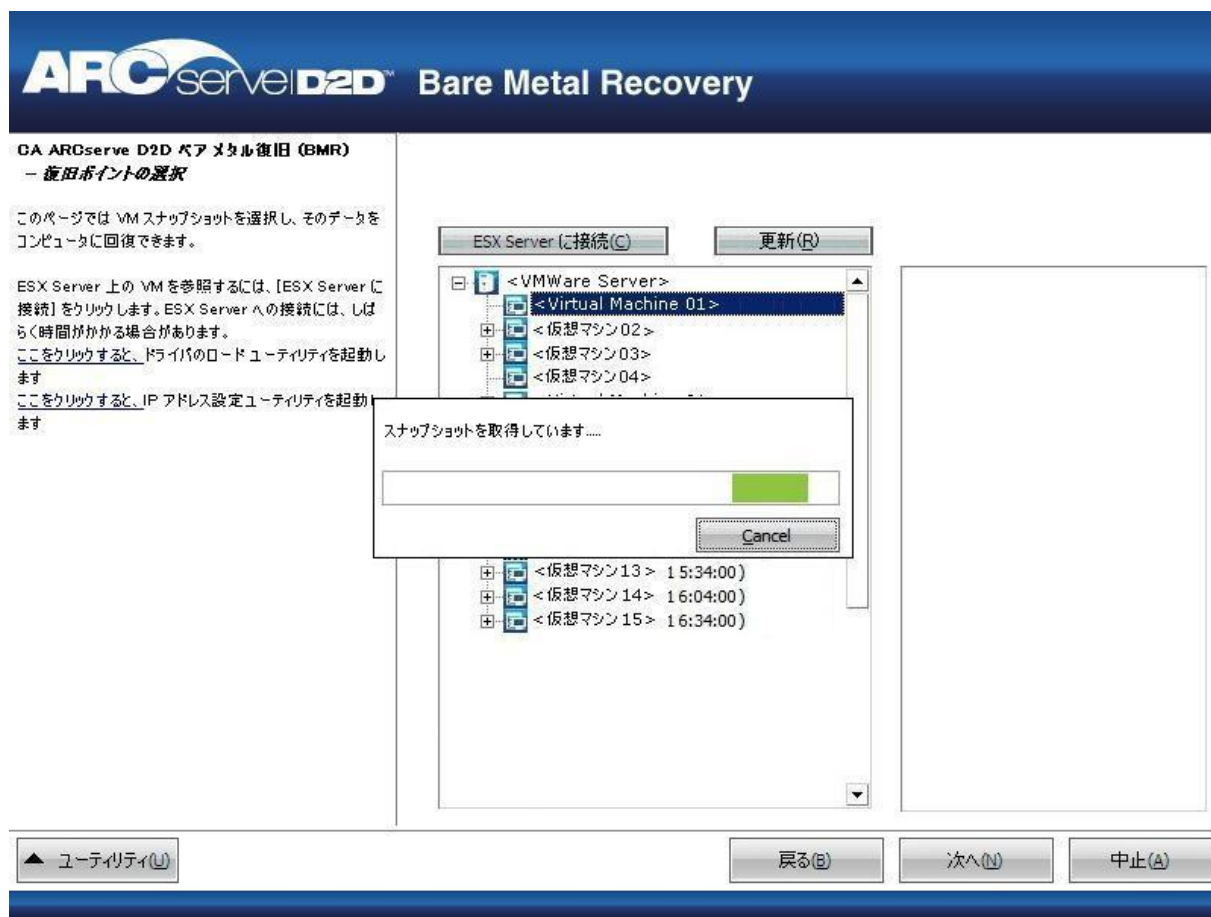
「復旧ポイントの選択」画面が ESX/VC の認証ダイアログ ボックスとともに表示されます。



3. 認証情報を入力して [OK] をクリックします。

[復旧ポイントの選択] 画面が表示されます。

次に CA ARCserve D2D は、選択されている VMware サーバのすべての復旧ポイント スナップショットを取得し、その VMware サーバ上にホストされているすべての仮想マシンのリストとともに、左側ペインに VMware サーバを表示します。



4. バックアップイメージの復旧ポイントを含む仮想マシンを選択します。

選択した仮想マシンのバックアップセッション（復旧ポイントスナップショット）が表示されます。



5. 復旧する仮想マシンバックアップセッション（復旧ポイント スナップショット）を選択します。

選択した復旧ポイント スナップショットの詳細（仮想マシン名、バックアップセッション名、バックアップ ボリューム、バックアップされたダイナミック ディスク）が、右側ペインに表示されます。

リスト表示された復旧ポイントのうちの1つを選択し、さらに、「現在の状態」または「最新の状態」を選択することができます。

- 復旧元の仮想マシンの電源がオンである場合、「現在の状態」の復旧ポイントが表示されます。
- 復旧元の仮想マシンの電源がオフである場合、「最新の状態」の復旧ポイントが表示されます。

「最新の状態」復旧ポイントを選択すると、エラー メッセージが表示されます。復旧元の復旧ポイントは（現在ではなく）最新の状態であり、復旧処理を続行する前に仮想マシンを起動させるよう要求します。

- リストア対象の復旧ポイントであることを確認した後、[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。

この手順の残りについては、「ベア メタル復旧の実行」を参照し、復旧モードが選択された時点の対応する手順から続行してください。



Microsoft Exchange 電子メール メッセージのリストア

Virtual Standby では、CA ARCserve D2D 復旧ポイントから Microsoft Exchange データをリストアすることができます。復旧ポイントから、メールボックス、メールボックス フォルダ、および個別の電子メール メッセージを回復またはリストアできます。

注: Exchange サーバデータの詳細リストアを実行するには、使用するアカウントに必要なアクセス権限が備わっている必要があります。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。

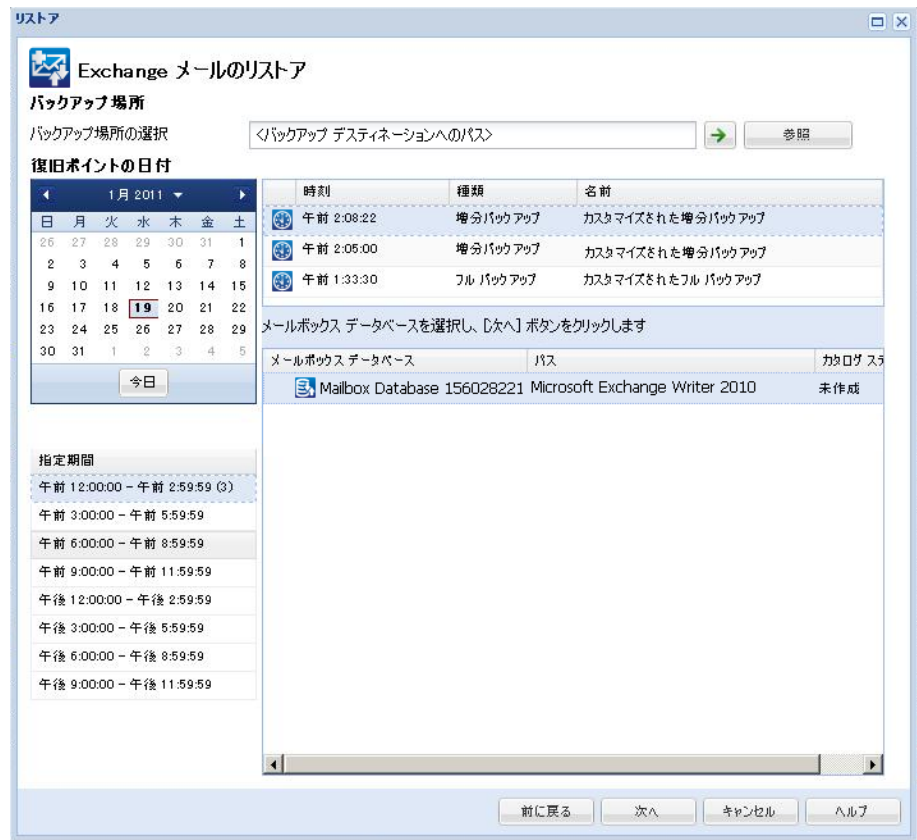
Microsoft Exchange 電子メール メッセージをリストアする方法

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、次に、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、[Exchange メール] のリストア] をクリックします。

[Exchange メール] のリストア] ダイアログ ボックスが表示されます。



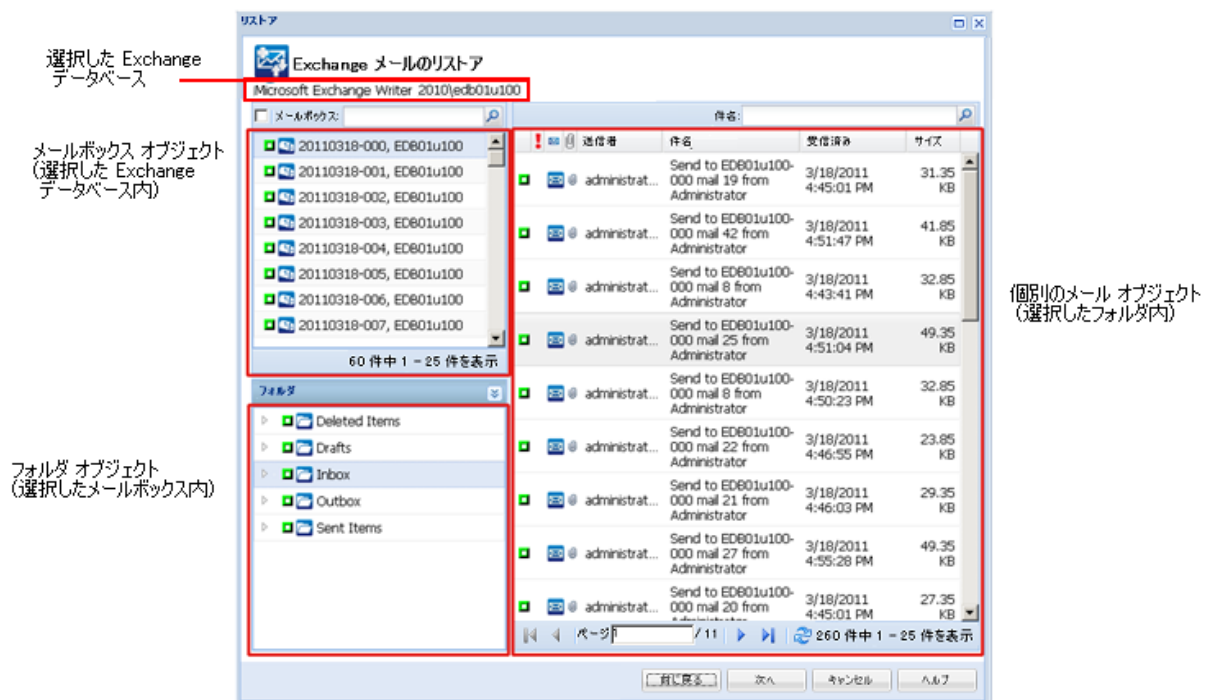
3. バックアップの場所を指定します。バックアップ イメージが保存されている場所を指定するか、参照して指定します。必要に応じて、その場所にアクセスするための [ユーザ名] および [パスワード] 認証情報を入力します。緑色の矢印で表示される検証アイコンをクリックすると、ソースの場所に正常にアクセスできるかどうかを検証します。
 カレンダ表示では、表示期間にバックアップ ソースの復旧ポイントを含むすべての日付が（緑色で）強調表示されます。
4. カレンダで、リストアするバックアップ イメージの日付を選択します。
 その日付に対応する **Exchange** メールボックス データベースが、バックアップの時刻、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。

5. リストアする Exchange メールボックス データベースを選択し、[次へ] をクリックします。

注: バックアップ時に Exchange 詳細リストア オプションを有効にしていない（カタログが生成されていない）場合、通知メッセージが表示され、Exchange 詳細リストア カatalogをこの時点で生成するかどうかユーザに確認されます。カタログの生成に対して [いいえ] を選択した場合、詳細復旧ポイントを参照または選択することはできません。その場合、[復旧ポイントの参照] ダイアログ ボックスから実行できるのは、フルデータベース リストアのみになります。

[Exchange メールのリストア] ダイアログ ボックスが更新され、選択したデータベースのメールボックスの内容がリスト表示されます。

注: Exchange 詳細リストアでは電子メールのリストアのみをサポートします。予定表、連絡先、メモ、タスクのリストアはサポートされていません。



6. リストアする Exchange オブジェクトのレベル（メールボックス、フォルダ、個々のメール）を選択します。

リストアする Exchange オブジェクトの全コンテンツまたは一部のコンテンツを選択できます。複数の Exchange オブジェクトを選択できます。

注: CA ARCserve D2D は、Exchange パブリック フォルダ オブジェクトの詳細復旧をサポートしていません。アプリケーションのリストアを使用してパブリック フォルダ データベース全体を回復してから、必要な特定の Exchange オブジェクトを抽出する必要があります。

注: Exchange メールボックス データベースからの個別のメールボックス/メール オブジェクトをリストアするために CA ARCserve D2D を使用する場合、リストアに使用されるオペレーティング システムは、バックアップ時に使用されたものと同じである必要があります。

（Windows バージョン番号とサービス パック レベル、およびそのサポートに必須の Visual C++ 再頒布可能パッケージの関連バージョンを含む）。

注: Exchange Server へ以前にログ記録されたことがないメールボックスの場合、CA ARCserve D2D UI からの電子メールの照会およびリストア中に、UI にメッセージの [送信者] フィールドプロパティが表示されません。ただし、これが発生した場合でも、電子メールは正しくリストアされます。

- a. メールボックス データベースを選択できます。

メールボックス データベースを選択した場合、そのデータベース内のすべてのメールボックスがリストアされます。

- b. メールボックス（複数可）を選択できます。

メールボックス レベルを選択した場合、そのメールボックス内の対応するコンテンツ（フォルダおよび個別のメール）がすべてリストアされます。

- c. 選択されたメールボックス内のフォルダを選択してリストアすることができます。

メールボックス フォルダ レベルを選択した場合、そのフォルダ内の対応するメール コンテンツがすべてリストアされます。

- d. 個別のメールを選択してリストアできます。

個別のメール レベルを選択した場合、選択されたメール オブジェクトのみがリストアされます。

注: Exchange 2003 の場合のみ、リストアされる個々の電子メールが Outlook 以外のメール クライアントを使用して送信され、バックアップ時にそのメールに何らかのフラグ ステータス マーカが添付されていた場合、メール自体はリストアされますが、添付のマーカは、リストアされたメールには含まれません。

7. リストアする Exchange オブジェクトを指定したら、[次へ] をクリックします。

8. リストア先を選択します。

使用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。

注: Exchange 2010 の場合、アーカイブされたメールボックス アイテムは元の場所にリストアできません。アーカイブされたメールボックス アイテムは、別の場所またはローカル ディスクにのみリストアできます。また、標準のメールボックス アイテムはアーカイブ メールボックスにはリストアできません。

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電子メールをリストアします。メールの階層は保持され、元のメールボックスおよび元のフォルダにリストアされます。

- 現在のマシンがアクティブな Exchange サーバでない場合、CA ARCserve D2D はアクティブなサーバの場所を検出し、そのアクティブなサーバへメールをリストアします。
- メールボックスが別の Exchange サーバに移動され、組織はそのままの場合、CA ARCserve D2D は、元のメールボックスが存在する新しい Exchange サーバを検出し、その新しいサーバへリストアします。
- メールボックスの表示名が変更されていると、CA ARCserve D2D では変更後の名前を見つけることができないので、元の場所にメールボックスをリストアしようとしても（それ以前のバックアップセッションから）失敗します。この問題を解決するには、このメールボックスを別の場所にリストアするよう指定します。

注: メールボックスまたはメールを元の場所にリストアする場合、デスティネーション メールボックスが利用可能であることを必ず確認してください。そうしないと、リストアは失敗します。CA ARCserve D2D では、リストア ジョブがサブミットされた場合のみリストア先を検証します。

ダンプ ファイルのみ

メールをディスクにリストアします。このディスクはローカルマシンまたはリモート マシンのいずれのものでもかまいません。リストアされるメールの階層は、Exchange メールボックスの階層と同じものになります。ファイル名がメールの件名になります。

注: メールの件名、フォルダ名、メールボックス名に次の文字のいずれかが含まれている場合、ファイル名ではハイフン (-) に置き換えられます: ¥/:*?"<>|

このオプションではまた、競合が発生した場合に CA ARCserve D2D が行う処理を指定する必要があります。Exchange では、同じフォルダに同じ名前の複数のメール オブジェクトを保存することができます。ただし、ファイル システムでは、同じフォルダに同じ名前のファイルを保存することはできません。

この競合状況の解決には、2つのオプションを利用できます。

- **名前の変更** - ディスク上にメールの件名と同じ名前のファイルがある場合、CA ARCserve D2D はメールの件名を使用しますが、件名の最後に番号を追加します。
- **上書き** - ディスク上にメールの件名と同じ名前のファイルがある場合、CA ARCserve D2D はそのファイルを上書きします。

注: 個別のメール オブジェクトをディスク（ダンプ）にリストアすることを選択した場合、デフォルトでは、リストアされたメール オブジェクトの形式は、**Personal Storage Table (.PST)** ファイルではなく、**Outlook Message (.MSG)** ファイルになります。

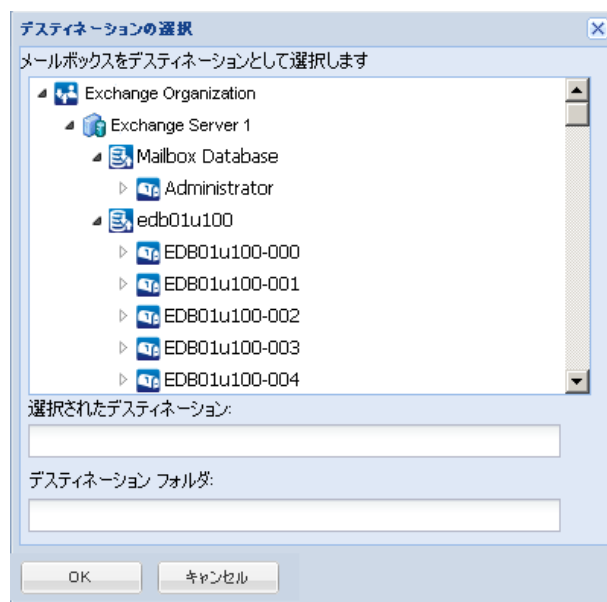
別の場所にリストアする

指定された場所にメールをリストアするか、またはバックアップ イメージがリストアされる場所を参照して選択します。 リストア 先は同じ **Exchange** 組織内のメールボックスである必要があり、新規フォルダ名が必要になります（メールを別の場所にリストアする場合、リストア先をパブリック フォルダにすることはできません）。

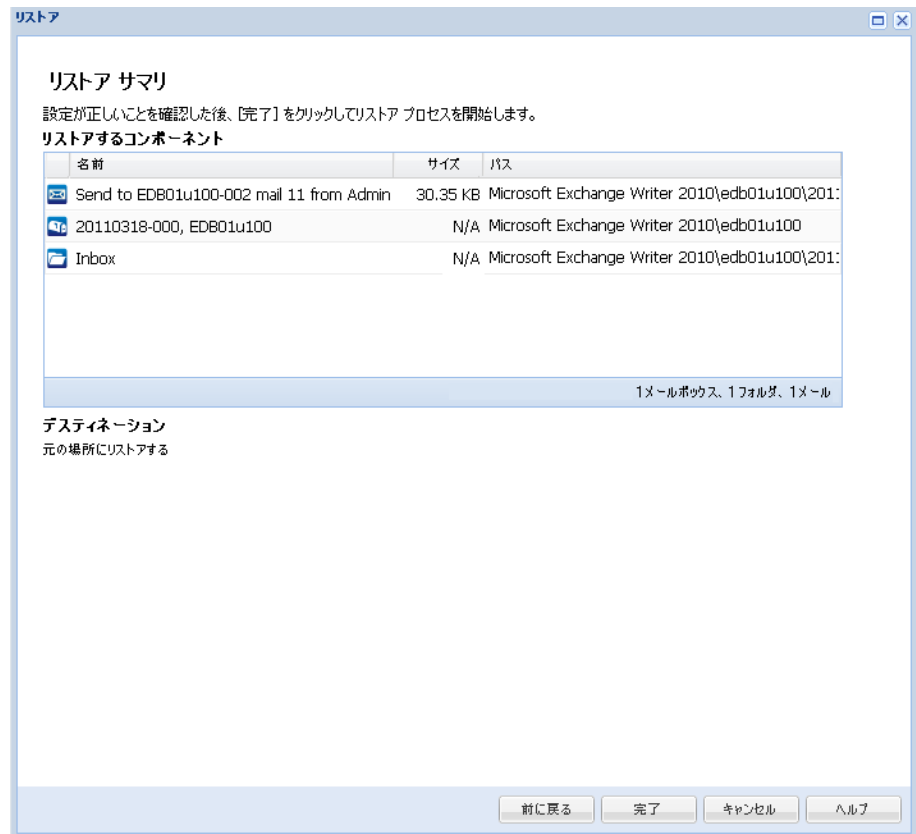
注: メールを別の場所にリストアする場合、指定されたデスティネーションフォルダがすでに存在すれば、リストアは続行します。しかし、指定されたフォルダが存在しない場合は、CA ARCserve D2D はまずフォルダを作成してから、リストアを続行します。

ユーザ名とパスワードを入力して [参照] ボタンをクリックすると、現在の組織内のすべての **Exchange Server**、ストレージグループ、**Exchange** データベース、メールボックスのリストを参照できます。

リストア先としてメールボックスを選択します。



9. リストア オプションを選択したら、[次へ] ボタンをクリックします。
[リストア サマリ] ダイアログ ボックスが表示されます。



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。

注: Exchange 詳細リストア用のカタログ化とリストアのジョブが進行中である場合、バックアップセッションはマウントされた状態になります。このマウントされたボリューム上で操作（フォーマット、ドライブ文字の変更、パーティションの削除など）は一切実行しないでください。

第 8 章: CA ARCserve Central 仮想スタンバイのトラブルシューティング

このセクションでは、CA ARCserve Central 仮想スタンバイ 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 \(P. 206\)](#)

[空の Web ページが表示される、または、JavaScript エラーが発生する \(P. 209\)](#)

[ページのロード問題のトラブルシューティング方法 \(P. 212\)](#)

[CA ARCserve D2D ノードおよびモニタ サーバへのログイン時に Web ページが正しくロードされない \(P. 213\)](#)

[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 \(P. 215\)](#)

[CA ARCserve D2D Web サービスが CA ARCserve D2D ノード上で失敗する \(P. 216\)](#)

[CA ARCserve D2D Web サービスの実行が遅い \(P. 219\)](#)

[CA ARCserve Central 仮想スタンバイ 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 \(P. 221\)](#)

[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 \(P. 222\)](#)

[ノードの追加時に無効な認証情報メッセージが表示される \(P. 224\)](#)

[Windows XP での無効な認証情報メッセージ \(P. 225\)](#)

[IP/名前によるノードの追加時にアクセス拒否エラーが発生する \(P. 226\)](#)

[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 \(P. 228\)](#)

[オペレーティング システムが見つからないエラー \(P. 229\)](#)

[Hyper-V システムへの仮想スタンバイ ジョブが失敗する \(P. 230\)](#)

[仮想スタンバイ ジョブが内部エラーのために失敗する \(P. 231\)](#)

[ホット追加転送モードを使用した仮想スタンバイ ジョブが失敗する \(P. 234\)](#)

[仮想スタンバイ ジョブがセッションなしの警告メッセージで終わる \(P. 237\)](#)

[バックアップ/復旧ジョブが SAN 転送モードを使用しない \(P. 238\)](#)

[ホット追加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ディスクがマウントできない \(P. 239\)](#)

[トラブルシューティングのエラー番号 \(P. 240\)](#)

[Internet Explorer 8、9、Chrome で追加した新しいタブのリンクが正しく起動しない \(P. 241\)](#)

[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 \(P. 245\)](#)

[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 \(P. 246\)](#)

[仮想マシンの電源が自動的にオンにならない \(P. 247\)](#)

[CA ARCserve Central 仮想スタンバイ がノードと通信できない \(P. 247\)](#)

[リモート変換の準備エラー。VSS スクリプト作成の失敗 \(P. 248\)](#)

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 仮想スタンバイ 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 仮想スタンバイ 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 仮想スタンバイ 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 仮想スタンバイ 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 仮想スタンバイ 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 仮想スタンバイ 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:

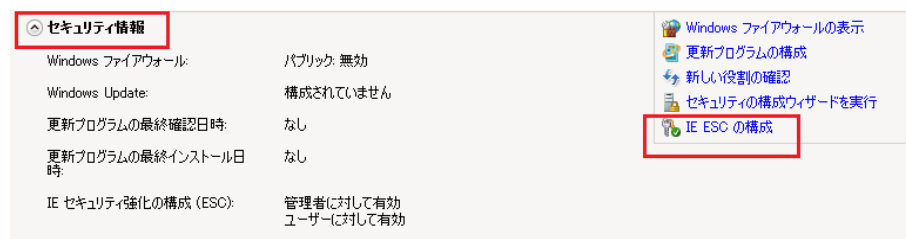
この問題を修正するには、アプリケーションの表示に使用しているコンピュータ上の Internet Explorer のセキュリティ強化の構成を無効にします。

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。

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 D2D ノードおよびモニタ サーバへのログイン時に 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 ノードおよびモニタ サーバ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。

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

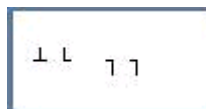
すべての Windows オペレーティング システムで有効。すべてのブラウザに該当します。

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。

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。

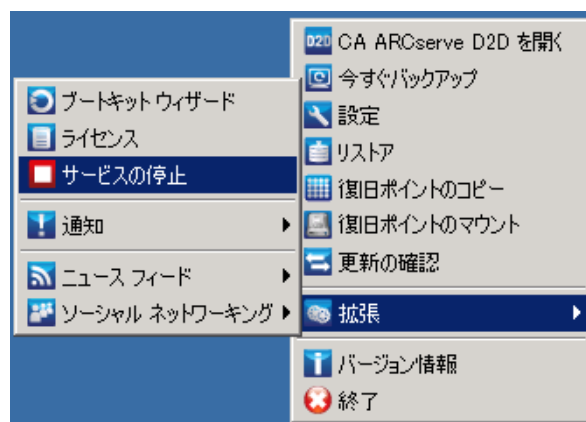
解決方法:

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。

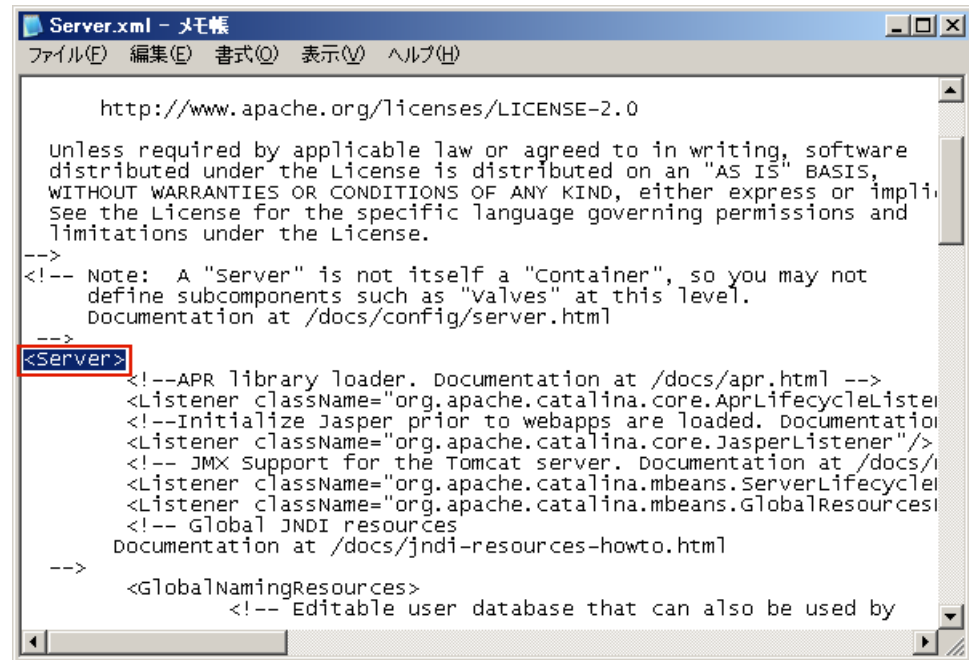


2. Tomcat の server.xml ファイルを開いて、Tomcat の動作を変更/設定します。

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。



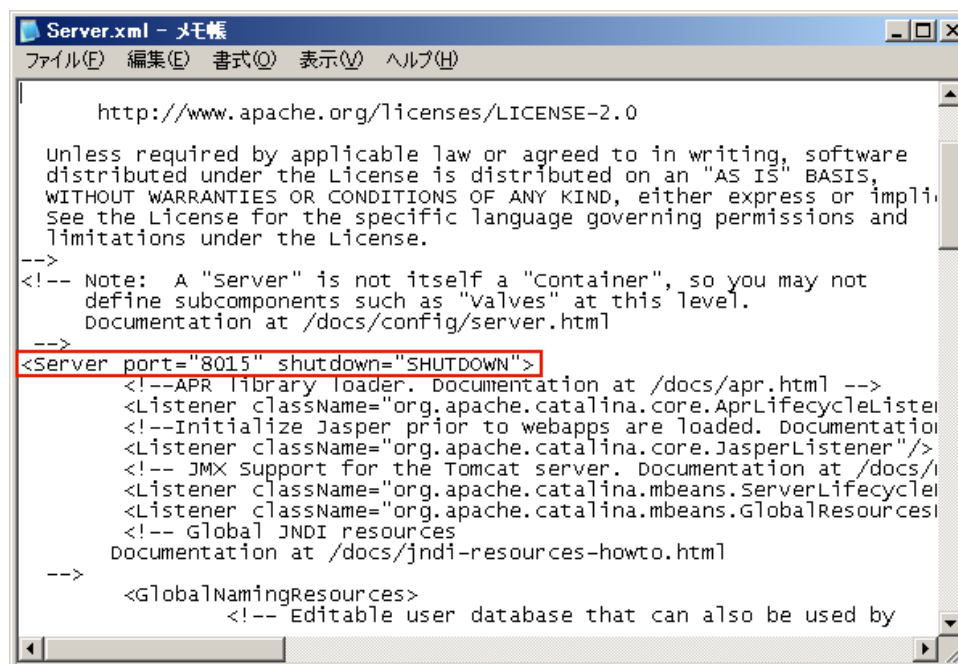
4. <Server> タグを以下のように編集します。

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 D2D Web サービスの実行が遅い

Windows オペレーティング システムで該当

症状 1:

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

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

解決策 1:

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

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

以下のメッセージを探します。

```
java.lang.OutOfMemoryError
```

この問題を修正するには、割り当てられるメモリの量を増加させます。

この値を増やすには、以下の手順に従います。

1. レジストリ エディタを開いて、以下のキーを選択します。

- x86 オペレーティング システムの場合

```
HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun
2.0\CASAD2DWebSvc\Parameters\Java
```

- x64 オペレーティング システムの場合

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun
2.0\CASAD2DWebSvc\Parameters\Java
```

2. 以下のいずれかを行います。

- ログ ファイル内のメッセージが以下の場合：

`java.lang.OutOfMemoryError: PermGen space`

Options の値に以下を追加します。

`-XX:PermSize=128M -XX:MaxPermSize=128M`

注： 使用している環境に合わせて「XX:MaxPermSize」の値を増加する必要がある場合があります。

- ログ ファイル内のメッセージが以下のいずれかの場合：

`java.lang.OutOfMemoryError: Java heap space`

`java.lang.OutOfMemoryError: GC overhead limit exceeded`

以下の DWORD の値を増加させます。

JvmMx

3. CA ARCserve D2D Web サービスを再起動します。

症状 2

スケジュールされたバックアップがスキップされ、実行を停止します。

解決策 2

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

1. 以下の DWORD の値を増加させます。

JvmMx=256

注： この DWORD は解決策 1 で参照されています。

2. Options の値に以下を追加します。

`-XX:MaxPermSize=128M`

注： この DWORD は解決策 1 で参照されています。

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

1. 以下の DWORD の値を増加させます。

JvmMx=512

注: この DWORD は解決策 1 で参照されています。

2. Options の値に以下を追加します。

-XX:MaxPermSize=256M

注: この DWORD は解決策 1 で参照されています。

CA ARCserve Central 仮想スタンバイ 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 仮想スタンバイ 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 仮想スタンバイ がリモートノード上の CA ARCserve D2D Web サービスと通信できない理由、および対応する是正処置を示したものです。

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

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

ノードの追加時に無効な認証情報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:

ノード画面でノードを追加しようとする、以下の内容のメッセージが表示されます。

認証情報が無効です。

解決方法:

この問題は、以下の状況で発生します。

- [ノードの追加] ダイアログ ボックスで指定された認証情報が正しくありません。
- ノード上の時間がアプリケーション サーバ上の時間と同じではありません。

この問題を解決するには、以下の手順に従います。

1. アプリケーション サーバにログインし、次にアプリケーションにログインします。
2. ホーム画面から、ナビゲーション バーの [ノード] を選択します。
[ノード] 画面が表示されます。
3. [ノード] ツールバーから [追加] をクリックし、コンテキスト メニューの [IP/名前によるノードの追加] をクリックします。
[IP/名前によるノードの追加] ダイアログ ボックスが開きます。

4. [IP/名前によるノードの追加] ダイアログ ボックスの以下のフィールドに入力します。
 - **IP/ノード名** -- ノードの IP アドレスまたは名前を指定できます。
 - **説明** -- ノードの説明を指定できます。
 - **ユーザ名** -- ノードへのログインに必要なユーザ名を指定できます。
 - **パスワード** -- ノードへのログインに必要なパスワードを指定できます。

[検証] をクリックします。

5. 無効な認証情報のメッセージが表示された場合は、以下の手順に従います。
 - a. [ノードの追加] ダイアログ ボックスで正しい認証情報が指定されたことを確認し、次に [検証] をクリックします。
 - b. 無効な認証情報のメッセージが表示された場合は、アプリケーション サーバ上のオペレーティング システムの時間がノード上のオペレーティング システムの時間と同じであることを確認します。

注: オペレーティング システム時間が別のタイム ゾーンに存在していても問題ありません。ただし、オペレーティング システム時間を異なる日付にすることはできません。ノード上のオペレーティング システム日付が、アプリケーション サーバ上のオペレーティング システム日付と比較して 1 日以上離れていないことを確認してください。

Windows XP での無効な認証情報メッセージ

Windows XP 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

症状:

[ノード] 画面から Windows XP ベースのノードを追加すると、以下のメッセージが表示されます。

ユーザ認証情報が無効です。

解決方法:

さまざまな状況において、CA ARCserve Central 仮想スタンバイ では、Windows の [フォルダ オプション] の [簡易ファイルの共有を使用する] が指定されている Windows XP ベースのノードを追加できません。この問題を解決するには、以下の手順に従います。

1. Windows XP ノードにログインし、Windows エクスプローラを開きます。
2. [ツール] メニューで、[フォルダ オプション] をクリックします。
[フォルダ オプション] ダイアログ ボックスが表示されます。
3. [表示] をクリックし、[簡易ファイルの共有を使用する (推奨)] までスクロールします。
4. [簡易ファイルの共有を使用する (推奨)] の横にあるチェックボックスをオフにして [OK] をクリックします。
簡易ファイルの共有が無効になりました。
5. CA ARCserve Central 仮想スタンバイ サーバにログインし、ノードを追加します。

IP/名前によるノードの追加時にアクセス拒否エラーが発生する

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。

症状:

[IP/名前によるノードの追加] ダイアログ ボックスからノードを追加するときに使用する 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ーである場合、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、ノードを追加できません。

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。

リモート UAC の無効化

1. [スタート] メニューをクリックし、[プログラムとファイルの検索] フィールドに「regedit」と入力して Enter キーを押します。Windows レジストリ エディタが開きます。

注: Windows レジストリ エディタを開くには、管理者の認証情報の指定が必要になる場合があります。

2. 以下のレジストリ キーを検索してクリックします。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System

3. [編集] メニューの [新規] をクリックし、[DWORD (32 ビット) 値] をクリックします。
4. 新規エントリに「LocalAccountTokenFilterPolicy」という名前を付けて、Enter キーを押します。
5. [LocalAccountTokenFilterPolicy] を右クリックし、[修正] をクリックします。
6. [値] データ フィールドに「1」を入力して、[OK] をクリックします。
7. レジストリ エディタを終了します。

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。

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 仮想スタンバイ 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、Virtual Standby 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. 80) します。
3. 新しい名前を使用して、[ノードを追加](#) (P. 40) します。

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:

仮想スタンバイ VM の電源投入操作に失敗すると、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。

解決方法:

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ます。

注: 最初の IDE ディスクを表すには (0:1) を使用します。

Hyper-V システムへの仮想スタンバイジョブが失敗する

Windows オペレーティング システムで有効

症状:

Hyper-V システムへの仮想スタンバイ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。

仮想スタンバイジョブで、Hyper-V VM の取得に失敗しました。

解決方法:

仮想スタンバイジョブは以下の状況で失敗します。

- 仮想スタンバイ Web サービスが、Hyper-V システムから仮想マシンに関する情報を取得できない場合。必要な Hyper-V サービスが Hyper-V システム上で実行されていないと、CA ARCserve Central 仮想スタンバイサーバと Hyper-V システム間で通信の問題が発生します。

解決策: 必要な Hyper-V サービスがすべて Hyper-V システム上で実行されていることを確認します。

- Hyper-V システムに、仮想スタンバイ VM を作成するか、または仮想スタンバイ VM のスナップショットを作成するために必要とされる十分なディスク空き容量が含まれていない場合。

解決策: システム ボリューム内のディスク空き容量を増やすために Hyper-V システムの再設定を検討します。

注: 他に原因が考えられる場合は、CA サポートにお問い合わせください。

仮想スタンバイ ジョブが内部エラーのために失敗する

Windows オペレーティング システムで該当

症状 1:

仮想スタンバイ ジョブが失敗します。以下のメッセージの 1 つがアクティビティ ログに示されます。

仮想ディスクの変換に失敗しました。
内部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。

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。

- 仮想スタンバイ ポリシーで指定されたデータ ストア上に十分なディスク空き容量がないと、変換操作に失敗する場合があります。VDDK API は（現在）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。この問題を修正するには、元のデータ ストア上で処理を完了するのに必要なディスク空き容量を解放し、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、変換処理が失敗する場合があります。この問題を修正するには、ソース ノードと、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。

この問題は VMware VDDK 接続の制限の結果です。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
- ESXi 5：すべての NFC 接続の転送バッファによって制限され、ホストによって適用されます。ESXi ホストに対するすべての NFC 接続バッファの合計は、32MB を超えることができません。vCenter Server を介した接続数 52。ホストごとの制限が含まれます。

注：接続がディスク間で共有されることはありません。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。

- 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。

症状 2:

仮想スタンバイ ジョブが失敗します。以下のメッセージの 1 つがアクティビティ ログに示されます。

仮想ディスクの変換に失敗しました。
内部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。

さらに、VDDK は以下のエラー メッセージをレポートします。

VMDK ファイルを開くことに失敗しました。ファイルが見つかりません。

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。

症状 3:

仮想スタンバイジョブが失敗します。以下のメッセージの 1 つがアクティビティ ログに示されます。

仮想ディスクの変換に失敗しました。
内部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。

さらに、VDDK は以下のエラー メッセージをレポートします。

VMDK ファイルを開くことに失敗しました。サーバで接続が拒否されました。

解決策 3:

この問題は VMware VDDK 接続の制限の結果です。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

注: 接続がディスク間で共有されることはありません。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。

ホット追加転送モードを使用した仮想スタンバイジョブが失敗する

Windows プラットフォームで有効

症状:

ホット追加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。

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。

解決方法:

ディスクが正しく設定されていない状態でホット追加モードを使用すると、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。

Windows のコマンドラインを開きます。

2. 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。

`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。

3. 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。

4. 特定の SAN ディスクの読み取り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。

5. 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、ホット追加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。

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。

2. 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。

3. [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。

4. 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。

仮想スタンバイ ジョブがセッションなしの警告メッセージで終わる

Windows プラットフォームで有効

症状:

仮想スタンバイ ジョブが終了し、以下のいずれかのメッセージがアクティビティ ログに表示されます。

仮想スタンバイ ジョブを終了します (セッションなし)。

Virtual Standby では、復旧ポイント スナップショットを作成するためのバックアップ セッションを CA ARCserve D2D サーバ上に検出できませんでした。 変換できるバックアップ セッションが CA ARCserve D2D サーバ上にない可能性があります。

解決方法:

この問題は、以下の状況で発生する可能性があります。

- CA ARCserve D2D バックアップ ポリシーを適用するために CA ARCserve Central Protection Manager を使用し、以下のいずれかに当てはまる場合。
 - CA ARCserve D2D バックアップ ソース設定のオプションが、[バックアップする個々のボリュームを選択する] から [マシン全体をバックアップする] に変更され、仮想スタンバイ ポリシーがノードに展開された後に、更新されたバックアップ設定を使用してフルバックアップがサブミットされていないか完了していない。

解決策: CA ARCserve D2D ノードのフルバックアップをサブミットします。

- 仮想スタンバイ ポリシーがノードに展開された後に、CA ARCserve D2D バックアップ ソース設定のオプションが、[マシン全体をバックアップする] から [バックアップする個々のボリュームを選択する] に変更された。

解決策: CA ARCserve D2D バックアップ ソース設定のオプションを [バックアップする個々のボリュームを選択する] から [マシン全体をバックアップする] に変更し、CA ARCserve D2D ノードのフルバックアップをサブミットします。

バックアップ/復旧ジョブが SAN 転送モードを使用しない

Windows プラットフォームで有効

症状:

バックアップジョブと復旧ジョブが [SAN 転送モード](#) (P. 261)を使用しません。ジョブは [NBD 転送モード](#) (P. 261)または [NBDSSL 転送モード](#) (P. 261)に戻ります。[バックアップステータスマニタ]ダイアログボックスの[転送モード]フィールドには、使用されるモードが表示されます。

解決方法:

上記の問題は、SAN LUN がバックアッププロキシシステム上で正しく設定されていない場合に発生します。ただし、Windows ディスク管理で SAN LUN が検出され、問題が継続する場合は、ディスクがオフラインであるか、またはディスクの読み取り属性が正しくない可能性があります。この動作が発生するのを防ぐには、ディスクを再設定します。

ディスクを設定するには、以下の手順に従います。

1. 管理者権限を持つアカウントを使用してソースノードまたはモニタサーバにログインします。
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。

ホット追加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:

ホット追加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、ソース ノードまたはモニタ サーバにディスクをマウントできません。さらに、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 %1!s! を開くことに失敗しました。詳細については、デバッグ ログ AFBBackend.Log を参照してください。テクニカル サポートにお問い合わせください。

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. hotadd ディスクが変換ジョブ中に接続された場合は、プロキシシステムからディスクを外します。
4. ジョブを再サブミットします。

トラブルシューティングのエラー番号

以下の表では、CA ARCserve Central 仮想スタンバイ を使用してノードを追加または更新したときにポップアップ メッセージとして表示されるエラー番号について説明します。

エラー番号	説明	考えられる解決策
12884901933	*** 上の CA ARCserve D2D サービスに接続できません。エラー番号は 12884901933 です。目的のノードの全エントリが正しいこと、および CA ARCserve D2D サービスが実行されていることを確認してください。	以下を確認します。 <ul style="list-style-type: none">■ CA ARCserve D2D サービスがノード上で実行されている。■ ノードに指定されたホスト名、IP アドレス、通信プロトコルが正しい。■ ノード上で CA ARCserve D2D Web サービスが実行されており、ノードの IP アドレスを DNS が解決できないことによるブロックは発生していない。■ ノード上で CA ARCserve D2D Web サービスが実行されており、Windows ファイアウォールまたは他のファイアウォールが通信をブロックしていない。■ ノードに接続されるネットワーク ケーブルが正しく機能する。■ ノードにログインしているユーザは、ワイヤレスネットワークを使用した通信に必要な権限を取得している。

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

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

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。

仮想マシンの電源が自動的にオンにならない

Windows で該当。

症状：

仮想マシンの電源が自動的にオンになりません。 [リカバリ] - [代理設定] が [自動的に仮想マシンを開始します] に定義されます。

解決方法：

これは正常な動作です。 アプリケーションは、CA ARCserve Central Host-Based VM Backup サーバから追加された仮想マシンの電源を自動的にオンにできません。 その結果、リカバリ方法が [自動的に仮想マシンを開始します] に定義されているポリシーを Host-Based VM Backup で保護されているノードに展開する際に、Virtual Standby は復旧方法の値を [手動で仮想マシンを開始します] に変更します。

この動作の解決策は、CA ARCserve D2D または CA ARCserve Central Protection Manager を使用して、仮想マシンを保護します。

CA ARCserve Central 仮想スタンバイ がノードと通信できない

Windows オペレーティングシステムで該当

症状：

CA ARCserve Central 仮想スタンバイ がノードと通信できません。

解決方法：

CA ARCserve Central 仮想スタンバイ がノードにポリシーを展開してノードを確実に保護できるようにするには、Virtual Standby サーバ、および保護するノード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 仮想スタンバイ サーバから、ノードのホスト名を使用して、保護するノードに ping を実行します。
2. 保護するノードから、サーバのホスト名を使用して CA ARCserve Central 仮想スタンバイ サーバに ping を実行します。

リモート変換の準備エラー。VSS スクリプト作成の失敗

すべての Windows オペレーティング システムが該当

症状:

vssadmin ユーティリティで手動で VSS スナップショットを作成すると、以下のようなエラー メッセージが表示されます。

「別のシャドウ コピーの作成が進行中です。しばらく待ってから再試行してください。」

解決方法:

ボリューム シャドウ コピー サービスを再起動します。

第 9 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。

[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 \(P. 249\)](#)

[アンチウイルス スキャンからのファイルの除外 \(P. 255\)](#)

[CA ARCserve Central 仮想スタンバイ のライセンス方法 \(P. 258\)](#)

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、アンインストールを行うカスタム 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 のインストールおよびアン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。
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。

コンポーネント	説明
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

アンチウイルス 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

CA ARCserve Central 仮想スタンバイ とリモート仮想スタンバイが正しく動作するようにするには、Hyper-V 仮想マシンと Hyper-V プロセスをターゲットとする以下のファイルを除外してください。

1. 仮想マシンの環境設定ファイル ディレクトリ :

- (デフォルト) C:¥ProgramData¥Microsoft¥Windows¥Hyper-V
- CA ARCserve Central 仮想スタンバイ 仮想マシンの環境設定ファイル ディレクトリ

2. 仮想マシンの仮想ハードディスク ファイル ディレクトリ :

- (デフォルト) C:¥Users¥Public¥Documents¥Hyper-V¥Virtual Hard Disks
- CA ARCserve Central 仮想スタンバイ 仮想マシンの仮想ハードディスク ファイル ディレクトリ

3. スナップショットのファイル ディレクトリ :

- (デフォルト) %systemdrive%¥ProgramData¥Microsoft¥Windows¥Hyper-V¥Snapshots
- CA ARCserve Central 仮想スタンバイ 仮想マシンのスナップショット ファイル ディレクトリ

4. Hyper-V プロセス :

- %windows%¥system32¥Vmms.exe
- %windows%¥system32¥Vmwpx.exe

CA ARCserve Central 仮想スタンバイ のライセンス方法

CA ARCserve Central 仮想スタンバイ には以下のライセンスが含まれます。

- CA ARCserve Central 仮想スタンバイ -Physical
- CA ARCserve Central 仮想スタンバイ VMware
- CA ARCserve Central 仮想スタンバイ -Hyper-V

ライセンスはすべて数ベースです。CA ARCserve Central 仮想スタンバイ は以下の条件に基づいて CA ARCserve D2D ノードにライセンスを付与および確認します。

- CA ARCserve Central 仮想スタンバイ は、名前/IP アドレスまたはファイルからのインポートによって追加したすべての CA ARCserve D2D ノードに CA ARCserve Central 仮想スタンバイ -Physical ライセンスを適用します。CA ARCserve Central 仮想スタンバイ は、ユーザがノードにポリシーを適用し、仮想変換プロセスを開始した後に、CA ARCserve Central 仮想スタンバイ -Physical ライセンスをノードに付与します。

注: これは CA ARCserve Central 仮想スタンバイ によるライセンスのデフォルトの動作です。

- CA ARCserve Central 仮想スタンバイ は、名前/IP アドレスまたはファイルからのインポートによって追加したすべての CA ARCserve D2D ノード、および ESX Server システムまたは vCenter Server システム上にある VMware 仮想マシンであるノードに、CA ARCserve Central 仮想スタンバイ -VMware ライセンスを適用します。ただし、CA ARCserve Central 仮想スタンバイ がノードに CA ARCserve Central 仮想スタンバイ -VMware ライセンスを適用できるようにするには、ノードを特定の ESX Server システムまたは vCenter Server システムに関連付ける必要があります。

注: 詳細については、「[VMware ベース ノードの ESX Server または vCenter Server システムの指定](#) (P. 69)」を参照してください。

CA ARCserve Central 仮想スタンバイ は、ユーザがノードにポリシーを適用し、仮想変換プロセスを開始した後に、CA ARCserve Central 仮想スタンバイ -VMware ライセンスを各 ESX Server システムに付与します。

- CA ARCserve Central 仮想スタンバイ は、ユーザが CA ARCserve Central Host-Based VM Backup システムからインポートしたすべての仮想マシンノードに CA ARCserve Central 仮想スタンバイ-VMware ライセンスを適用します。CA ARCserve Central 仮想スタンバイ は、ユーザがノードにポリシーを適用し、仮想変換プロセスを開始した後に、CA ARCserve Central 仮想スタンバイ-VMware ライセンスを仮想マシンノードに付与します。
- CA ARCserve Central 仮想スタンバイ は、名前/IP アドレスまたはファイルからのインポートによって追加したすべての CA ARCserve D2D ノード、および Hyper-V ハイパーバイザ上にあるすべての CA ARCserve D2D ノードに CA ARCserve Central 仮想スタンバイ-Hyper-V ライセンスを適用します。ユーザが名前/IP アドレスまたはファイルからのインポートによってノードを追加すると、CA ARCserve Central 仮想スタンバイは Hyper-V サーバの存在を検出します。CA ARCserve Central 仮想スタンバイ は、ユーザが名前/IP アドレスまたはファイルからのインポートによってノードを追加すると、CA ARCserve Central 仮想スタンバイ-Hyper-V ライセンスを CA ARCserve D2D ノードに付与します。

カウントの仕組み

以下の表では、必要となる CA ARCserve Central 仮想スタンバイ ライセンス数をシナリオ別に説明します。

D2D ノードの種類	必要なライセンス	カウントの仕組み
物理ノード	CA ARCserve Central 仮想スタンバイ-Physical	各ノードに 1 ライセンス
VMware 仮想マシン	CA ARCserve Central 仮想スタンバイ-VMware	各 ESX/vCenter Server システムに 1 ライセンス
Hyper-V 仮想マシン	CA ARCserve Central 仮想スタンバイ-Hyper-V	各 Hyper-V システムに 1 ライセンス

例

- CA ARCserve Central 仮想スタンバイ は 5 個の物理 CA ARCserve D2D ノードを保護しています。5 個の CA ARCserve Central 仮想スタンバイ-Physical ライセンスが必要です。
- CA ARCserve Central 仮想スタンバイ は、1 個の ESX Server システム上にある 3 個の VMware 仮想マシンを保護しています。1 個の CA ARCserve Central 仮想スタンバイ-VMware ライセンスが必要です。
- CA ARCserve Central 仮想スタンバイ は、10 個の ESX Server システム上に分散した 100 個の VMware 仮想マシンを保護しています。10 個の CA ARCserve Central 仮想スタンバイ-VMware ライセンスが必要です。
- CA ARCserve Central 仮想スタンバイ は、5 個の Hyper-V システム上に分散した 20 個の Hyper-V 仮想マシンを保護しています。5 個の CA ARCserve Central 仮想スタンバイ-Hyper-V ライセンスが必要です。
- CA ARCserve Central 仮想スタンバイは、1 個の Hyper-V システム上に存在する 3 個の Hyper-V 仮想マシンと、1 個の ESX Server システム上に存在する 3 個の VMware 仮想マシンを保護しています。1 個の CA ARCserve Central 仮想スタンバイ-VMware ライセンスと 1 個の CA ARCserve Central 仮想スタンバイ-Hyper-V ライセンスが必要です。
- CA ARCserve Central 仮想スタンバイ は、CA ARCserve Central Host-Based VM Backup からインポートされ、1 個の ESX Server システム上に存在する 5 個の VMware 仮想マシンを保護しています。1 個の CA ARCserve Central 仮想スタンバイ-VMware ライセンスが必要です。

用語集

HOTADD 転送モード

HOTADD 転送モードは、SCSI ディスクで設定された仮想マシンをバックアップするためのデータ転送方式です。詳細については、VMware Web サイトの [Virtual Disk API Programming Guide](#) を参照してください。

NBDSSL 転送モード

NBDSSL (Network Block Device Secure Sockets Layer) 転送モードは、通信に NFC (Network File Copy) プロトコルを使用します。NBDSSL は TCP/IP 通信ネットワークを使用して、暗号化されたデータを転送します。

NBD 転送モード

NBD (ネットワーク ブロック デバイス) 転送モード (別名、LAN 転送モード) は、通信に NFC (ネットワーク ファイル コピー) プロトコルを使用します。各種の VDDK および VCB 操作は、NBD を使用するとき、各 ESX/ESXi Server ホストでアクセスする仮想ディスクごとに 1 つの接続を使用します。

SAN 転送モード

SAN (Storage Area Network) 転送モードは、ファイバチャネル通信を使用して、SAN に接続されたプロキシシステムからストレージデバイスにバックアップデータを転送できます。

仮想変換

仮想変換は、CA ARCserve Central 仮想スタンバイ が CA ARCserve D2D 復旧ポイントをソース ノードから仮想マシンデータ ファイル (復旧ポイントスナップショット) に変換するプロセスです。

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。

ハートビート

ハートビートは、ソース ノードがノードのステータスを特定するために モニタ サーバに送信する電子信号です。

復旧ポイント スナップショット

復旧ポイント スナップショットは、CA ARCserve Central 仮想スタンバイ が CA ARCserve D2D 復旧ポイントから作成する VMware Virtual Disk (VMDK) または Microsoft 仮想ハードディスク (VHD) フォーマットのファイルです。CA ARCserve Central 仮想スタンバイ では、実稼働環境で CA ARCserve D2D を実行しているソース サーバに障害が発生した場合に復旧ポイント スナップショットを使用して仮想マシンの電源をオンにできます。

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。

モニタ サーバ

モニタ サーバは、CA ARCserve Central 仮想スタンバイ 環境内のソース サーバのステータスを確認するサーバです。

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。