CA ARCserve® Central Protection Manager

ユーザ ガイド

r16.5

ca technologies

CA Technologies 製品リファレンス

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

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

CA への連絡先

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

CA ARCserve Central Applications のサポート リンク

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

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

  http://www.ca.com/jp/support/

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

  http://www.casupport.jp/support/supportonline/

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

  http://www.casupport.jp/resources/storagesupp/

マニュアルの変更点

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

- 製品およびドキュメント自体の利便性と理解の向上に役立つことを目的として、ユーザのフィードバック、拡張機能、修正、その他小規模な変更を反映するために更新されました。
- 「バックアップ拡張設定の指定（P. 115）」が更新されました。 このトピックには、各バックアップ後の検索速度を向上させるためにファイル システム カタログの生成に使用するオプションが追加されました。
- 「CA ARCserve Central Protection Manager ログの表示（P. 190）」が更新されました。このトピックには、新しい 2 つのモジュール オプション、［複数ノードの更新］と［CA ARCserve D2D マージ ジョブ］が追加されました。 ［プレフライト チェック］と［VM バックアップ ジョブのサブミット］は削除されました。
- 「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. 225）」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。

目次

第 4 章: CA ARCserve Central Protection Manager の使用 55

第 5 章: CA ARCserve Central Protection Manager と IT 管理サーバ ツールの統合 197

第 1 章: CA ARCserve Central Protection Manager 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

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

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

CA ARCserve Central Applications によって提供されるアプリケーションの 1 つが CA ARCserve Central Protection Manager です。 CA ARCserve Central Protection Manager では、CA ARCserve D2D および CA ARCserve Backup の環境を 1 つの場所から管理することができます。個別のアプリケーションによってある程度のノード管理は提供されますが、CA ARCserve Central Protection Manager を使用すると以下が可能になります。

- 1 つまたは複数のノードの追加
- Active Directory サーバからのノードの検出
- ハイパーバイザによって管理される仮想マシンの検出と追加
- 追加されたサーバ上のアプリケーションの検出
- CA ARCserve D2D ポリシーの作成と割り当て
- 管理対象の CA ARCserve D2D に対するリストア ジョブのサブミット
- 管理対象の CA ARCserve Backup および CA ARCserve D2D サーバからのデータの同期
- CA ARCserve D2D の展開

アプリケーションの動作の仕組み

CA ARCserve Central Protection Manager では、保護されているノードを中央の場所から表示および管理することができます。

CA ARCserve Central Protection Manager を開始するには、［スタート］メニュー -［すべてのプログラム］-［CA］-［ARCserve Central Applications］-［CA ARCserve Central Protection Manager］を選択します。 CA ARCserve Central Protection Manager ホーム画面が表示され、以下のナビゲーション機能を使用して、さまざまな CA ARCserve Central Protection Manager 機能にアクセスできます。

- **ノード** -- さまざまなツールを使用して、ノードとノード グループの管理、ノードのディスカバリ、CA ARCserve D2D のノードへの 展開、データの同期を実行できます。
- **ポリシー** -- CA ARCserve D2D ポリシーの追加、編集、削除、コピー、割り当てを行うことができます。 この機能では、ポリシー詳細が表示され、その対応する CA ARCserve D2D ポリシーに対してノードを割り当てまたは割り当て解除できます。
- **環境設定** -- データベース、CA ARCserve Backup データ同期、SRM、ディスカバリ、電子メール環境設定、更新環境設定、環境設定、管理者アカウント、D2D 展開、IT 管理サーバの環境設定を行います。
- **ログの表示** -- 個別のノードについてアクティビティ ログを表示します。 CA ARCserve Central Protection Manager には、そのノードと関連付けられているログ メッセージがすべて表示されます。以下のオプションを指定してリストをフィルタできます。
  - 重大度（すべて、情報、エラー、警告、エラーと警告）
  - モジュール（すべて、共通、ディスカバリからのノードのインポート、ハイパーバイザからのノードのインポート、ファイルからのノードのインポート、ポリシー管理、CA ARCserve Backup 同期、CA ARCserve D2D 同期、CA ARCserve D2D の更新、更新、CA ARCserve D2D バックアップ ジョブのサブミット、複数ノードの更新、および CA ARCserve D2D マージ ジョブ）
  - ノード名

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 Protection Manager 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

アプリケーションをインストールする前に、以下の必須のタスクを完了します。

- 「リリース ノート」を確認します。「リリース ノート」には、システム要件の説明、サポートされるオペレーティング システム、および CA ARCserve Central Protection Manager のこのリリースで存在する既存の問題のリストが含まれます。
- お使いのシステムがアプリケーションをインストールするためのハードウェア要件とソフトウェア要件を満たしていることを確認します。
- 使用している Windows アカウントが、CA ARCserve Central Protection Manager をインストールするコンピュータに対して、管理者権限またはソフトウェアをインストールするのに必要な管理者相当権限を持っていることを確認します。
- アプリケーションをインストールするコンピュータのユーザ名およびパスワードを所有していることを確認します。

- CA ARCserve Central Protection Manager をインストールするサーバおよびポリシーを展開するノードが、ホスト名を使用して互いに通信できることを確認します。 CA ARCserve Central Protection Manager サーバとノードが互いに通信できることを確認するには、以下の手順に従います。
  - CA ARCserve Central Protection Manager サーバから、ノードのホスト名を使用してノードに ping を実行します。
  - 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 Protection Manager サーバに ping を実行します。
- 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。
- CA ARCserve Central Protection Manager インストール メディアには Microsoft SQL Server 2008 R2 Express Edition が含まれています。これは、CA ARCserve Central Protection Manager データベースをサポートするために必要とされる最小限のデータベース アプリケーションです。 CA ARCserve Central Protection Manager データベースをサポートするために Microsoft SQL Server を使用する場合は、CA ARCserve Central Protection Manager をインストールする前に、CA ARCserve Central Protection Manager サーバまたはリモート サーバ上に Microsoft SQL Server をインストールします。 インストール ルーチンによって、サポートされていない Microsoft SQL Server のバージョンが検出された場合、インストール ルーチンは失敗します。 Microsoft SQL Server のサポートされているバージョンの詳細については、「リリース ノート」を参照してください。

インストールに関する考慮事項

CA ARCserve Central Protection Manager をインストールする前に、以下のインストールに関する考慮事項を確認します。

- CA ARCserve Central Applications インストール パッケージは、CA ARCserve Central Applications Server という名前のモジュールをインストールします。 このサーバは、すべてのアプリケーションに共通のモジュールです。 このモジュールには、アプリケーションが互いに通信するために使用される Web サービス、バイナリ、および設定が含まれています。

  アプリケーションをインストールする場合、インストール パッケージは製品コンポーネントをインストールする前に CA ARCserve Central Applications Server モジュールをインストールします。アプリケーションにパッチを適用する必要が生じた場合、パッチは製品コンポーネントを更新する前にモジュールを更新します。

- CA ARCserve D2D をリモート ノードに展開する場合、CA ARCserve Central Protection Manager は VMware Virtual Disk Development Kit （VDDK） 1.2.1 をターゲット ノードにインストールします。 CA ARCserve Central Protection Manager インストール メディアには、VMware Virtual Disk Development キット（VDDK） 1.2.1 を CA ARCserve Central Protection Manager サーバおよびターゲット ノード上にインストールするのに必要なセットアップ ファイルが含まれています。そのため、CA ARCserve D2D をリモート ノードに展開するために VMware Web サイトから VDDK セットアップ ファイルをダウンロードする必要はありません。

CA ARCserve Central Protection Manager 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 Protection Manager 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。

［データベースの設定］ダイアログ ボックスが表示されます。

5. ［データベースの設定］ダイアログ ボックスで、［データベースの種類を選択してください］の横のドロップダウン リストをクリックし、以下のいずれかを指定します。

   - ARCserve Central Applications デフォルト データベース
   - Microsoft SQL Server

   データベースの種類を指定したら、指定されたデータベースに必須のオプションが［データベースの設定］ダイアログ ボックス上に表示されます。

6. 以下のいずれかを行います。

   - **ARCserve Central Applications デフォルト データベース** -- ［データベースの設定］ダイアログ ボックスで以下の情報を入力します。

     - **インストール パスの指定** -- CA ARCserve Central Applications デフォルト データベースをインストールする場所を指定します。デフォルト パスを使用するか、または別のパスを指定できます。
     - **データ ファイル パスの指定** -- CA ARCserve Central Applications デフォルト データベース用のデータ ファイルをインストールする場所を指定します。 デフォルト パスを使用するか、または別のパスを指定できます。

     注: CA ARCserve Central Applications デフォルト データベースはリモート通信をサポートしません。 そのため、デフォルト データベースとデータ ファイルは、アプリケーションをインストールしているコンピュータにインストールします。

- **Microsoft SQL Server データベース** -- ［データベースの設定］ダイアログ ボックスで以下の情報を入力します。
  - **SQL Server の種類** -- アプリケーションが SQL Server データベースとの通信に使用する通信の種類を指定します。

    ローカル: アプリケーションと SQL Server が同じコンピュータにインストールされる場合は［ローカル］を指定します。

    リモート: アプリケーションと SQL Server が異なるコンピュータにインストールされる場合は［リモート］を指定します。
  - **SQL Server 名** -- 指定された SQL Server の種類がリモートである場合は、リモート SQL Server 名を指定します。SQL Server をローカルで使用する場合は、ドロップダウン リストから該当するサーバを選択します。
  - **セキュリティ** --SQL Server との認証に使用する認証情報の種類を指定します。

    Windows セキュリティを使用 -- Windows 認証情報を使用して認証する場合は［Windows セキュリティを使用］を指定します。

    SQL Server セキュリティを使用 -- SQL Server 認証情報を使用して認証する場合は［SQL Server セキュリティを使用］を指定します。その場合は、SQL Server アカウントのログイン ID およびパスワードを指定します。
  - **既存のデータベースに上書き** -- 既存の CA ARCserve Central Applications データベースを検出して上書きすることを許可する場合は、既存のデータベースの上書きを指定します。

［インストール］をクリックします。

インストール処理が完了すると、［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。

7. ［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 Protection Manager のサイレント インストール

CA ARCserve Central Applications では、CA ARCserve Central Protection Manager 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サイレント インストールする方法を説明しています。

CA ARCserve Central Protection Manager 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 Protection Manager をアンインストールする方法

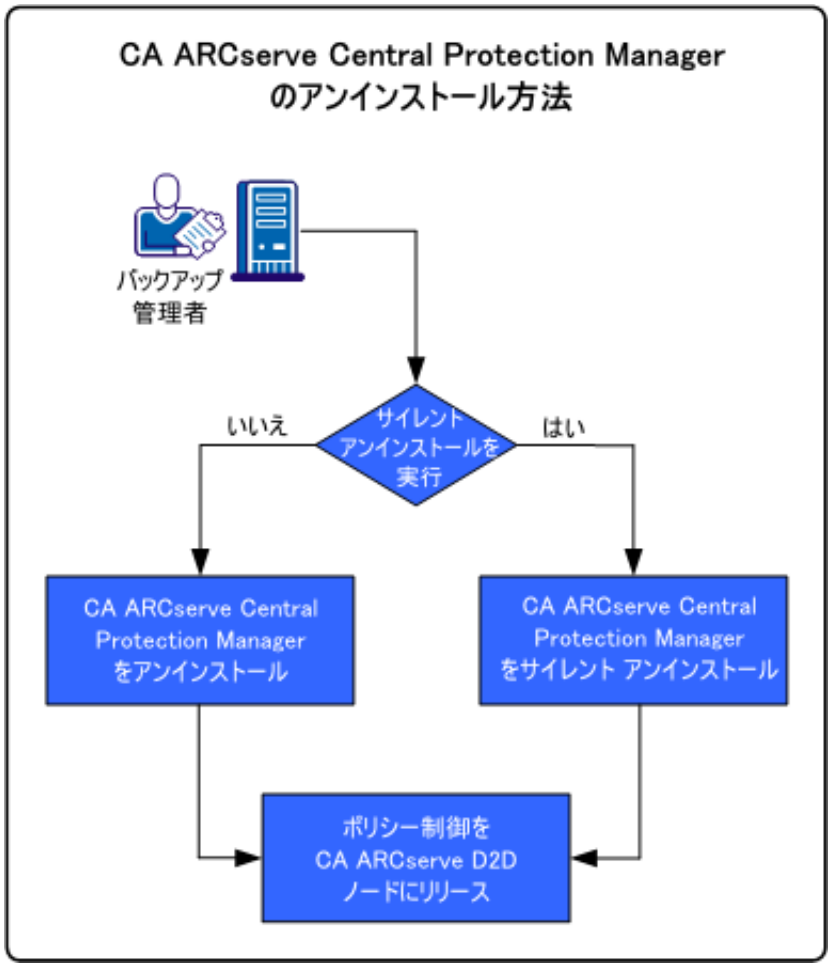
CA ARCserve Central Protection Manager は以下の方法を使用してアンインストールできます。

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

ポリシーの割り当て解除

ベスト プラクティスとして、アプリケーションをアンインストールする前に、ポリシーが割り当てられているノードからすべてのポリシーの割り当てを解除します。 CA ARCserve Central Protection Manager ポリシーがノードに割り当てられる間は、ノードに CA ARCserve D2D バックアップ設定を指定できないため、この方法が推奨されます。 また、アプリケーションをアンインストールした後にノードからポリシーの割り当てを解除することはできません。 CA ARCserve D2D では、提供されたコマンド ライン ユーティリティを使用することにより、アプリケーションをアンインストールした後にノードからポリシーの割り当てを解除することができます。

以下の図は、アプリケーションをアンインストールする方法を示しています。



タスク	参照トピック
Windows コントロール パネルを使用して、標準的なアンインストールを実行します。	CA ARCserve Central Protection Manager をアンインストール (P. 27) します。
Windows コマンド ラインを使用して、サイレント アンインストールを実行します。	CA ARCserve Central Protection Manager をサイレント アンインストール (P. 28) します。
CA ARCserve Central Protection Manager をアンインストールした後にノードからポリシーの割り当てを解除します。	ポリシー制御を CA ARCserve D2D ノードにリリース (P. 29) します。

CA ARCserve Central Protection Manager 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 CA ARCserve Central Protection Manager 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. 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します。

2. Windows［スタート］メニューから、［コントロール パネル］をクリックして Windows コントロール パネルを開きます。

3. ［プログラムと機能］をクリックして、プログラムのアンインストールまたは変更用のウィンドウを開きます。

4. CA ARCserve Central Protection Manager を選択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 Protection Manager のサイレント アンインストール

CA ARCserve Central Applications では、CA ARCserve Central Protection Manager 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サイレント 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します。

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 : 以下の構文は、アプリケーションのサイレント 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
   {CAED05FE-D895-4FD5-B964-001928BD2D62}
   ```

   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。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 Protection Manager

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

   CA ARCserve Central Host-Based VM Backup

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

CA ARCserve Central Reporting

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

CA ARCserve Central 仮想スタンバイ

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

アプリケーションがサイレント アンインストールされます。

CA ARCserve D2D ノードへのポリシー制御のリリース

CA ARCserve Central Protection Manager をアンインストールするプロセスでは、CA ARCserve D2D ノードからバックアップ ポリシーの割り当てが解除されません。そのため、Protection Manager をアンインストールした後、CA ARCserve D2D ノードにバックアップ設定を直接指定することができなくなります。 ベスト プラクティスとして、アプリケーションをアンインストールする前にポリシーが割り当てられているノードからすべてのポリシーの割り当てを解除します。 この手順を実行しない場合、専用に設計されたユーティリティを使用して、ポリシー制御をノードにリリースすることができます。

次の手順に従ってください:

1. CA ARCserve D2D ノードにログインします。
2. Windows コマンド ラインを開き、以下のディレクトリに移動します。

   C:¥Program Files¥CA¥ARCserve D2D¥BIN

3. 以下の構文を使用して ARCCentralAppMgrUtility.exe を実行します。

```
ARCCentralAppMgrUtility.exe -clean pm|hbvb|vs [-debug]
```

pm|hbvb|vs

CA ARCserve D2D ノードの制御からリリースするアプリケーションを定義します。 以下のいずれかの引数を指定します。

pm

CA ARCserve Central Protection Manager

hbvb

CA ARCserve Central Host-Based VM Backup

vs

CA ARCserve Central 仮想スタンバイ

-debug

-debug オプションは必須ではありません。 このオプションを指定したまま、ユーティリティは、以下のディレクトリに保存されるデバッグ ログ ファイルを生成します。

```
<D2D_Home>¥Log¥ARCCentralAppMgrUtility.log
```

例： 以下の例は、ノードにポリシー制御をリリースするための構文を表しています。

```
ARCCentralAppMgrUtility.exe -clean pm
```

ポリシー制御がノードにリリースされます。

インストール処理のオペレーティング システムに対する影響

CA ARCserve Central Applications インストール処理は、Microsoft Installer Package （MSI）というインストール エンジンを使用して、さまざまな Windows オペレーティング システムのコンポーネントを更新します。 CA ARCserve Central Applications では、MSI に含まれるコンポーネントによって、CA ARCserve Central Applications のインストール、アップグレード、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。
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。

コンポーネント	説明
ShowMsiLog	［SetupCompleteSuccess］、［SetupCompleteError］、または［SetupInterrupted］ダイアログ ボックスの［Windows Installer のログを表示］チェック ボックスがオンの場合に［完了］をクリックすると、Windows Installer ログ ファイルをメモ帳で表示することができます。（これは Windows Installer 4.0 でのみ機能します。）
ISPrint	ScrollableText コントロールの内容をダイアログ ボックス上に出力します。 これは、Windows Installer .dll カスタム アクションです。 .dll ファイルの名前は SetAllUsers.dll で、エントリ ポイントは PrintScrollableText です。
CheckForProductUpdates	FLEXnet Connect を使用して製品アップデートを確認します。 このカスタム アクションは、Agent.exe という名前の実行可能ファイルを起動し、以下に移動します。 /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	再起動の際に FLEXnet Connect を使用して製品アップデートを確認します。 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
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

第 3 章: CA ARCserve Central Protection Manager 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 Protection Manager を設定する方法について説明します。

このセクションには、以下のトピックが含まれています。

CA ARCserve Central Protection Manager サーバとノード間の通信の確認

注: これは、ノードを保護するために CA ARCserve Central Protection Manager を設定する任意の手順です。

CA ARCserve Central Protection Manager 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、Protection Manager 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。

CA ARCserve Central Protection Manager サーバがノードと通信できることを確認する方法

1. CA ARCserve Central Protection Manager 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 Protection Manager サーバに ping を実行します。

CA ARCserve Backup データ同期スケジュールの環境設定

CA ARCserve Backup データ同期によって、CA ARCserve Central Protection Manager データベースと CA ARCserve Backup データベースとを同期するためのスケジュールおよび繰り返し方法（何日間、曜日、または日付）をシステムに設定できます。

次の手順に従ってください:

1. アプリケーションにログインします。
2. ナビゲーション バーの［環境設定］をクリックして、［環境設定］画面を開きます。
3. ［環境設定］パネルで、［CA ARCserve Backup データ同期スケジュール］オプションをクリックすると、［CA ARCserve Backup データ同期］オプションが表示されます。
4. ［有効］をクリックして、CA ARCserve Backup データ同期を有効にします。

   注: デフォルトでは、CA ARCserve Backup データ同期環境設定は有効になっています。

5. 以下のパラメータを指定し、CA ARCserve Backup データ同期をスケジュール設定します。
   - 繰り返し方法
   - スケジュールされた時刻
6. ［保存］をクリックして CA ARCserve Backup データ同期スケジュールを適用します。
7. （オプション）［今すぐ実行］をクリックし、CA ARCserve Backup データ同期プロセスをすぐに開始します。

SRM スケジュールの環境設定

バックアップ管理者は、CA ARCserve Central Protection Manager を使用して、CA ARCserve D2D ノードのスケジュールを設定し、SRM データを収集する時間および頻度を定義します。 SRM （Storage Resource Management）は以下のような情報を収集する機能です。

- ハードウェア、ソフトウェア、Microsoft SQL Server や Microsoft Exchange Server 実装のアプリケーション データ。
- CA ARCserve Central Applications サーバによって管理されている CA ARCserve D2D サーバからの PKI （Performance Key Indicator）データ。

  注: CA ARCserve Backup ノードについて、CA ARCserve Backup は、CA ARCserve Backup データ同期プロセス中に PKI データを収集し、そのデータと CA ARCserve Central Protection Manager とを同期します。

次の手順に従ってください:

1. アプリケーションにログインします。
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］パネルで、［SRM 環境設定］をクリックすると、SRM 環境設定オプションが表示されます。
4. ［有効］をクリックして SRM を有効にします。

   注: デフォルトでは、SRM 環境設定は有効になっています。
5. 以下のパラメータを指定して、SRM をスケジュール設定します。
   - 繰り返し方法
   - スケジュールされた時刻

6. ［保存］をクリックして、SRM スケジュールを適用します。
7. （オプション）［今すぐ実行］をクリックし、SRM データ収集プロセスをすぐに開始します。

ディスカバリ スケジュールの設定

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

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

ノード ディスカバリのスケジュール設定時に Active Directory リストが表示されます。

電子メールとアラートの設定の指定

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

次の手順に従ってください:

1. アプリケーションにログインします。

   ホーム画面上のナビゲーション バーから［環境設定］をクリックして、［環境設定］画面を開きます。

2. ［環境設定］パネルから、［電子メールとアラートの環境設定］をクリックし、［電子メールとアラートの環境設定］オプションを開きます。

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

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

電子メール環境設定が適用されます。

IT 管理サーバの設定

CA ARCserve Central Protection Manager では IT 管理サーバにアラート メッセージを送信できます。 アラート情報を送信するには、アプリケーション サーバが IT 管理サーバと通信できるよう設定します。

IT 管理サーバの設定方法

1. CA ARCserve Central Protection Manager にログインし、［ナビゲーション］で［環境設定］をクリックします。
2. ［環境設定］画面の［環境設定］リストで［IT 管理サーバ環境設定］をクリックします。
3. 以下の IT 管理サーバ環境設定オプションの入力を完了します。
   - ［有効］をクリックします。
   - ［Nimsoft］または［Kasaya］をクリックします。
   - ［繰り返し方法］を指定します。 繰り返し方法は、最初の送信プロセスが失敗した場合に、アラート通知を IT 管理サーバに再送信する日を定義します。 IT 管理サーバが利用可能でないかオフラインでない場合は、アラートを送信するプロセスが失敗する可能性があります。
   - スケジュールを指定します。 スケジュールは、アラート通知を Nimsoft サーバに再送信する時間を定義します。
4. ［保存］をクリックします。

CA ARCserve Central Protection Manager サーバは IT 管理サーバと通信するように設定されました。

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。

CA ARCserve Central Applications 更新スケジュールの環境設定

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

CA ARCserve Central Applications 更新スケジュールを設定する方法

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。

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。

D2D 展開設定の環境設定

CA ARCserve Central Protection Manager では、CA ARCserve D2D を展開する先の場所に対して D2D 展開設定を指定できます。

注: Windows XP を実行するコンピュータに CA ARCserve D2D を展開するには、リモート Windows XP コンピュータ上で［簡易ファイルの共有を使用する］オプションを無効にします。

D2D 展開設定の方法

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］画面で、［D2D 展開環境設定］をクリックします。

   ［D2D 展開環境設定］オプションが表示されます。

3. 環境設定画面で以下の情報を入力します。
   - **ポート** -- このポート番号は、Web ベースの UI に接続する際に使用されます。 デフォルトでは、ポート番号は 8014 です。
   - **インストール パス** -- CA ARCserve D2D のリモート サーバ上のインストール パスです。 デフォルトでは、この場所は %Program Files% になります。
   - **セットアップによるドライバのインストールを許可します**（デフォルトでオン） -- ドライバを自動的にインストールするかどうかを指定します。
   - **再起動**（デフォルトでオン） -- 展開プロセスが完了したときに必要な再起動を自動的に実行するか、後で手動で再起動するかを指定します。
   - **HTTPS を使用**（デフォルトでオフ）-- HTTPS（安全）を使用すると、HTTP 通信より高いレベルのセキュリティが提供されます。 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。
4. ［保存］をクリックします。

D2D 展開環境設定が適用されます。

データベースの設定

CA ARCserve Central Protection Manager をインストールした後、以下を実行できます。

- CA ARCserve Central Protection Manager データベースの設定を更新します。たとえば、インスタンスの名前、ポート値、などを更新できます。
- CA ARCserve Central Protection Manager データベース アプリケーションを Microsoft SQL Server に変更します。
- CA ARCserve Central Protection Manager データベース アプリケーションを Microsoft SQL Server Express Edition に変更します。

CA ARCserve Central Protection Manager **データベースの設定方法**

1. ナビゲーション バーから、［環境設定］をクリックします。
2. ［環境設定］パネルで、［データベース環境設定］をクリックします。
3. 環境設定画面で以下の情報を入力します。
   - **SQL Server マシン名** -- SQL Server インスタンスをホストするサーバの名前を指定します。
   - **SQL サーバ インスタンス** -- SQL Server インスタンスの名前を指定します。
   - **SQL Server ポート** -- このインスタンスのポート番号を指定するか、または［自動検出］オプションを有効にします。
   - **認証モードの選択** -- デフォルトは［Windows 認証モード］です。

     注:［SQL Server および Windows 認証モード］を選択すると、［ユーザ名］および［パスワード］のフィールドが有効になります。
   - （オプション）**テスト** -- アプリケーションが Microsoft SQL Server インスタンスと通信できることを確認します。
   - **データベース接続プール値の指定** -- 最大と最小の接続数について 1 から 99 までの値を入力します。
4. ［保存］ボタンをクリックします。

   注: 指定した値をすべてクリアし、元のデータをロードするには［リセット］をクリックします。
5. （オプション）アプリケーションが CA ARCserve Central Reporting にデータを提供している場合、Windows Server Manager を開き、以下のサービスを再起動します。

   `CA ARCserve Central Applications` サービス

   データベース サーバ環境設定が適用されます。

CA ARCserve Central Protection Manager データベースの再作成

さまざまな理由で、CA ARCserve Central Protection Manager データベースを再作成する場合があります。 たとえば、現在のデータベースが 10GB 以上のデータを消費している場合などです。以下の手順で、CA ARCserve Central Protection Manager データベースを再作成する方法について説明します。この手順は、Microsoft SQL Server および Microsoft SQL Server Express Edition データベースに適用されます。

重要: CA ARCserve Central Protection Manager データベースを削除すると、現在のデータがすべて失われます。

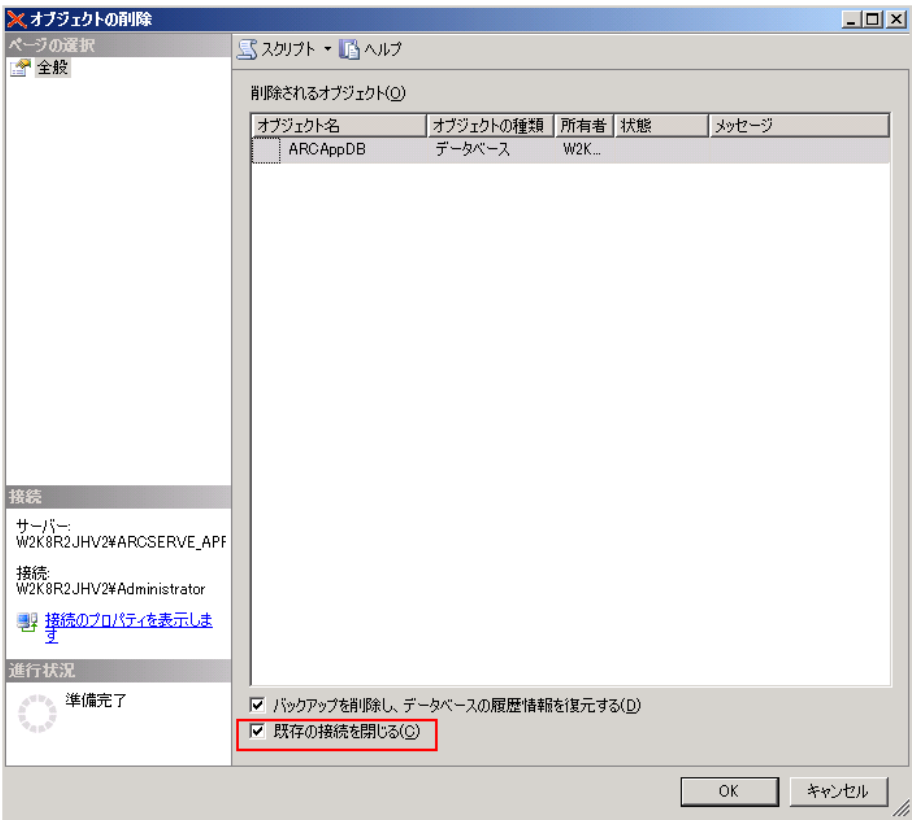
CA ARCserve Central Protection Manager データベースを再作成する方法

1. Microsoft SQL Server Management Studio Express を開き、ARCserve_APP インスタンスにログインします。

   注: CA ARCserve Central Protection Manager サーバに Microsoft SQL Server Management Studio Express がインストールされていない場合、Microsoft ダウンロード センターからユーティリティをダウンロードできます。

2. ARCAppDB を右クリックして、コンテキスト メニューの［削除］をクリックします。

   ［オブジェクトの削除］ダイアログ ボックスが開きます。



3. ［オブジェクトの削除］ダイアログ ボックスで、［既存の接続を閉じる］オプションをクリックして［OK］をクリックします。

   ［オブジェクトの削除］ダイアログ ボックスが閉じ、CA ARCserve Central Protection Manager データベースが削除されます。

4. CA ARCserve Central Protection Manager を開き、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。

5. ［データベース環境設定］をクリックします。

   データベース オプションが表示されます。

6. 以下のフィールドに指定された値が正しいことを確認します。

   - **SQL Server マシン名** -- SQL Server インスタンスをホストするサーバの名前を指定します。
   - **SQL サーバ インスタンス** -- SQL Server インスタンスの名前を指定します。

7. （オプション）以下のフィールドに入力します。

   - **SQL Server ポート** -- このインスタンスのポート番号を指定するか、または［自動検出］オプションを有効にします。
   - **認証モードの選択** -- デフォルトは［Windows 認証モード］です。

     注:［SQL Server および Windows 認証モード］を選択すると、［ユーザ名］および［パスワード］のフィールドが有効になります。

   - **データベース接続プール値の指定** -- 最大と最小の接続数について 1 から 99 までの値を入力します。

8. ［テスト］をクリックして、データベースへの接続を確立します。

9. ［保存］ボタンをクリックします。

CA ARCserve Central Protection Manager で、データベースが再作成されます。データベース インスタンスの名前は ARCAppDB です。

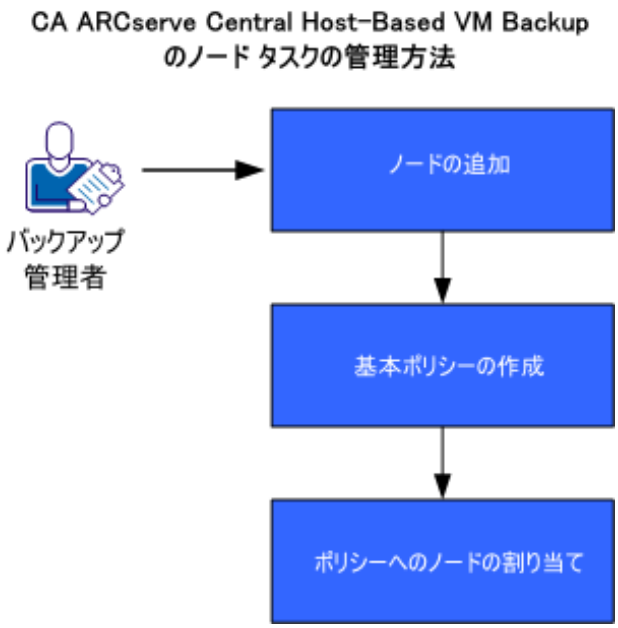
第 4 章: CA ARCserve Central Protection Manager の使用

このセクションには、以下のトピックが含まれています。

CA ARCserve Central Protection Manager を使用した CA ARCserve D2D ノードのバックアップ

CA ARCserve Central Protection Manager を使用すると、CA ARCserve D2D ノード上に存在するデータをバックアップおよび保存する方法と時期を定義するポリシーを作成できます。 以下のトピックでは、基本ポリシーを使用して CA ARCserve D2D バックアップ ジョブをサブミットする方法について説明します。 基本ポリシーは、実稼働環境で機能するほぼすべての CA ARCserve D2D ノードを保護することができます。

以下の図は、CA ARCserve Central Protection Manager を使用して、基本的なバックアップ ポリシーを作成し、CA ARCserve D2D ノードをバックアップするプロセスを表しています。



CA ARCserve Central Protection Manager を使用して、基本ポリシーを作成し CA ARCserve D2D ノードをバックアップするには以下の手順に従います。

1. ノードを追加 (P. 57) します。
2. 基本ポリシーを作成 (P. 58) します。
3. ノードをポリシーに割り当て (P. 63) ます。

ノードの追加

ポリシーを使用して CA ARCserve D2D ノードをバックアップするには、まずバックアップするノードを定義します。

注: ディスカバリを使用してこのタスクを自動化できます。ただし、ディスカバリでは、Active Directory サーバ上で Active Directory に表示されるノードのみが検出されます。

次の手順に従ってください:

1. CA ARCserve Central Protection Manager にログインし、ナビゲーションバーの［ノード］をクリックします。
2. ［ノード］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。
3. ［IP/名前によるノードの追加］ダイアログ ボックスで、すべてのフィールドに入力して［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。

   注: さらにノードを追加するには、手順 2、3、4 を繰り返します。

ノードが追加されたら、デフォルト グループ内に表示されます。

基本ポリシーの作成

ポリシーは、CA ARCserve D2D ノード上に存在するデータをバックアップおよび保存する方法と時期を定義します。 CA ARCserve Central Protection Manager にはデフォルト ポリシーが含まれません。 ポリシーを作成することは、ノード上に存在するデータをバックアップするための前提条件タスクです。

基本ポリシーを作成するには、保護設定を指定し、スケジュールを作成します。 保護設定は、バックアップするデータ、データを保存する場所、データを保存する方法を定義します。 スケジュールは、ノードをバックアップする時間および頻度を定義します。

次の手順に従ってください:

1. CA ARCserve Central Protection Manager ホーム画面で、ナビゲーションバーの［ポリシー］をクリックして［ポリシー］画面を開きます。
2. ［新規］をクリックして、新しいポリシーを作成します。
3. ［新規ポリシー］ダイアログ ボックスの［ポリシー名］フィールドで、ポリシーの名前を指定します。
4. ［バックアップ設定］タブをクリックし、［保護設定］をクリックすると、保護設定オプションが表示されます。

5. バックアップ先を指定します。

   バックアップ場所としてローカル パス（ボリュームやフォルダ）、またはリモート共有フォルダ（またはマップされたドライブ） を指定できます。

   - ローカル パス（ボリュームまたはフォルダ）にバックアップするように指定する場合、ソースと同じ場所をバックアップ先に指定することはできません。 バックアップ先にソースが含まれている場合、ジョブではソースのこの部分を無視するため、バックアップには含まれません。

     重要: 指定したデスティネーション ボリュームにシステム情報が含まれていないことを確認してください。 CA ARCserve D2D は、システム情報が含まれるデスティネーション ボリュームをバックアップしません。 ベア メタル復旧（BMR）を使用してコンピュータを復旧しようとすると、復旧に失敗する場合があります。

     注: ダイナミック ディスクをディスク レベルでリストアすることはできません。 ダイナミック ディスク上のボリュームにデータがバックアップされた場合、このダイナミック ディスクを BMR 実行中にリストアすることはできません。

   - リモート共有される場所にデータをバックアップする場合は、リモート コンピュータにアクセスするのに必要な認証情報およびパスを指定します。

6. バックアップ ソースを指定します。

   ノード全体またはノード上の個別のボリュームをバックアップ対象として指定できます。

   以下の点に注意してください。

   - マシン全体のバックアップが選択された場合、CA ARCserve D2D は現在のマシンに接続されているすべてのディスク/ボリュームを自動的に検出し、それらをバックアップ対象に追加します。

   - システム/ブート ボリュームがバックアップ対象に選択されない場合、警告メッセージが表示されます。 このメッセージは、バックアップを BMR に使用できないことを示します。

7. 復旧ポイントを指定します。

   保持されるバックアップ イメージの数量を指定します。デフォルトは 31 で、最大は 1344 です。この数量を変更する場合、デスティネーションにおける空き容量を考慮する必要があります。

   指定した復旧ポイントの数を超過すると CA ARCserve D2D は最も古い子の増分バックアップを親バックアップにマージし、ベースライン イメージを再作成します。新しいベースライン イメージは「親 + 最も古い子」のブロックから構成されます。 最も古い子バックアップを親バックアップにマージするサイクルは、後続の各バックアップに対して繰り返されます。 このプロセスにより、バックアップの保持数を一定に保ちながら、増分バックアップを無限に実行することができます。

8. バックアップに使用する圧縮の種類を指定します。

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

   利用できる圧縮オプションは以下のとおりです。

   圧縮なし

   圧縮は実行されません。 このオプションを使用すると、CPU 使用率は最も低くなります （最も高速で動作します）。ただし、バックアップ イメージのディスク容量の使用率は最大になります。

   標準圧縮

   一般的な圧縮が実行されます。このオプションを使用すると、CPU 使用率とディスク容量使用率のバランスを適度に調節します。 標準圧縮はデフォルトの設定です。

   最大圧縮

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

   以下の点に注意してください。

   - バックアップ イメージに圧縮できないデータ（JPG イメージや ZIP ファイルなど）が含まれている場合は、それらのデータを扱うためにストレージ容量を割り当てます。
   - デスティネーションの空き容量が足りない場合、バックアップの圧縮設定を高くすることを検討してください。

9. セキュリティの強化に使用する暗号化設定を指定します。

   a. バックアップに使用する暗号化アルゴリズムの種類を選択します。

      データの暗号化とは、解読メカニズムがなければ理解できない形式にデータを変換することです。 CA ARCserve D2D のデータ保護では、安全な AES （Advanced Encryption Standard）暗号化アルゴリズムを使用し、指定したデータに対して最大限のセキュリティおよびプライバシーを確保します。

      利用可能なオプションは、暗号化なし、AES-128、AES-192、および AES-256 です（暗号化を無効にするには、［暗号化なし］を選択します）。

      - フル バックアップと関連するすべての増分/検証バックアップで同じ暗号化アルゴリズムを使用する必要があります。
      - 増分/検証バックアップの暗号化アルゴリズムを変更した場合は、フル バックアップを実行します。 つまり、暗号化アルゴリズムが変更されたら、元のバックアップの種類にかかわらず、最初のバックアップはフル バックアップになります。

        たとえば、アルゴリズム形式を変更し、カスタマイズされた増分または検証バックアップを手動でサブミットすると、自動的にフル バックアップに変換されます。

   b. 暗号化アルゴリズムを指定したら、暗号化パスワードを提供（および確認）します。

      - 暗号化パスワードは最大 23 文字に制限されています。
      - フル バックアップと関連するすべての増分/検証バックアップでは、データの暗号化に同じパスワードを使用する必要があります。
      - 増分/検証バックアップの暗号化パスワードを変更した場合は、フル バックアップを実行します。 つまり、暗号化パスワードが変更されたら、元のバックアップの種類にかかわらず、最初のバックアップは常にフル バックアップになります。

        たとえば、暗号化パスワードを変更し、カスタマイズされた増分/検証バックアップを手動でサブミットすると、自動的にフル バックアップに変換されます。

   暗号化が有効になると、アクティビティ ログが更新され、すべてのバックアップに使用される暗号化が記述されます。

10. スロットル バックアップを指定します。

    バックアップが書き込まれる最高速度（MB/分）を指定できます。CPU またはネットワークの使用率を削減するためにバックアップ速度のスロットル制御を実行できます。 しかし、バックアップ速度を制限すると、バックアップ ウィンドウに悪影響を及ぼします。

11. ［スケジュール］タブをクリックすると、スケジュール オプションが表示されます。

12. バックアップ スケジュールの指定

    開始日時の設定

    バックアップ スケジュールの開始日および開始時刻を指定します。

    増分バックアップ

    増分バックアップのバックアップ スケジュールを指定します。

    使用可能なオプションは［繰り返し実行する］と［実行しない］です。 ［繰り返し実行する］オプションを選択した場合、バックアップの実行間隔（分単位、時間単位、または日単位）を指定します。 増分バックアップの最小設定は 15 分ごとです。

    デフォルトでは、増分バックアップのスケジュールは 1 日ごとに繰り返すよう設定されています。

    フル バックアップ

    フル バックアップのバックアップ スケジュールを指定します。

    CA ARCserve D2D は、スケジュールされたとおりに、ソース マシンから、使用されているすべてのブロックのフル バックアップを実行します。 使用可能なオプションは［繰り返し実行する］と［実行しない］です。 ［繰り返し実行する］オプションを選択した場合、バックアップの実行間隔（分単位、時間単位、または日単位）を指定します。 フル バックアップの最小設定は 15 分ごとです。

    デフォルトでは、フル バックアップのスケジュールは［実行しない］（スケジュールされている繰り返しはない）です。

検証バックアップ

検証バックアップのバックアップ スケジュールを指定します。

使用可能なオプションは［繰り返し実行する］と［実行しない］です。 ［繰り返し実行する］オプションを選択した場合、バックアップの実行間隔（分単位、時間単位、または日単位）を指定します。 検証バックアップの最小設定は 15 分ごとです。

デフォルトでは、検証バックアップのスケジュールは［実行しない］（スケジュールされている繰り返しはない）です。

13. ［保存］をクリックします。

基本的なバックアップ ポリシーが作成されます。 ［ポリシー］画面のポリシー リストに、手順 3 で指定した名前でポリシーが表示されます。

注: 同時に実行するようスケジュールされたバックアップの種類が複数ある場合、実行されるバックアップの種類は、以下の優先度に基づきます。

- 優先度 1 - フル バックアップ
- 優先度 2 - 検証バックアップ
- 優先度 3 - 増分バックアップ

例: バックアップの 3 つの種類がすべて同時に実行されるようスケジュールされた場合、CA ARCserve D2D はフル バックアップを実行します。 検証バックアップと増分バックアップが同時に実行されるようスケジュールされ、フル バックアップがスケジュールされていない場合、CA ARCserve D2D は検証バックアップを実行します。 スケジュールされた増分バックアップは、他の種類のバックアップとの競合がない場合のみ実行されます。

ポリシーへのノードの割り当て

基本ポリシーを作成したら、そのポリシーに使用してバックアップする CA ARCserve D2D ノードを割り当てます。

次の手順に従ってください:

1. CA ARCserve Central Protection Manager ホーム画面で、ナビゲーション バーの［ポリシー］をクリックして［ポリシー］画面を開きます。
2. ［ポリシー］画面でポリシーのリストから、作成したポリシーをクリックします。

3. ［ポリシーの割り当て］タブをクリックすると、ポリシーの割り当て（リスト）が表示されます。
4. ［割り当てと割り当て解除］をクリックし、［ポリシーの割り当て/割り当て解除］ダイアログ ボックスを開きます。
5. 追加するノードの横のチェックボックスをオンにして、右向き矢印をクリックします。

   ［使用許諾契約］ダイアログ ボックスが表示されます。
6. 使用許諾契約の内容を確認して同意し、［完了］をクリックします。

   作成したポリシーにノードが割り当てられ、すぐに展開されます。バックアップは、［スケジュール］タブで定義されたスケジュールに基づいて開始します。
7. ポリシーへのノードの割り当てが完了したら、［OK］をクリックしてポリシーの割り当てを保存し、［割り当てと割り当て解除］ダイアログ ボックスを閉じます。

ノードが割り当てられた後、CA ARCserve Central Protection Manager はポリシーをノードに直ちに展開します。 バックアップ処理は、選択した保護設定に基づいて開始され、ポリシーで定義されたスケジュールに従って実行されます。

CA ARCserve Central Protection Manager でノードを管理する方法

CA ARCserve Central Protection Manager では、ノードおよびノード グループの管理に使用できるさまざまなツールやオプションが用意されています。このセクションでは、ノードおよびノード グループについて追加、削除、変更、データ同期を実行する方法について説明します。CA ARCserve D2D を検出してノードに展開することもできます。

このセクションには、以下のトピックが含まれます。

ノード管理画面について

ノード管理は、CA ARCserve Central Applications で最初に使用するコンポーネントです。CA ARCserve Central Protection Manager アプリケーションの左パネルのナビゲーション バーからアクセスできます。

ノード管理には、画面で作業を開始するための 4 つのカテゴリが含まれています。

- **ノード** -- 特定のノードを管理します。 ノード管理の詳細については、「ノードに対して実行できること (P. 67)」を参照してください。
- **ノード グループ** -- 特定のノード グループを管理します。 詳細については、「ノード グループに対して実行できること (P. 87)」を参照してください。
- **アクション** -- データのバックアップ (P. 163)、データのリストア (P. 167)、データの展開 (P. 94) を実行できます。
- **フィルタ** -- 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ノードを表示します。 詳細については、「ノード グループのフィルタ (P. 98)」を参照してください。

［製品］列にある各ノードのステータスは、CA ARCserve Backup および CA ARCserve D2D アイコンを識別します。 以下の表で、製品列に示される各製品のステータスについて説明します。

アイコン	説明
	'M' という文字を含むこのステータスは、ノードが、CA ARCserve Central Applications によって管理されたプライマリまたはスタンドアロンの CA ARCserve Backup サーバであることを示します。
	'M' という文字と右下に感嘆符を含むこのステータスは、ノードが、CA ARCserve Central Applications によって管理されたプライマリまたはスタンドアロンの CA ARCserve Backup サーバで、過去 'xx' 時間に同期が成功していないことを示します。（'xx' のデフォルトは 48 時間）。または同期がまだ実行されていなかったことを示します。
	'M' という文字のないこのステータスは、ノードが、CA ARCserve Central Applications によって管理されないプライマリ、スタンドアロン またはメンバのいずれかの CA ARCserve Backup サーバであることを示します。
	このステータスは、このノードに CA ARCserve Backup の古いバージョンが含まれることを示します。
	このステータスは、ノードが CA ARCserve Central Applications によって管理されておらず、CA ARCserve D2D に接続できないことを示します。
	このステータスは、ノードに CA ARCserve D2D の古いバージョンが含まれることを示します。
	'M' という文字を含むこのステータスは、ノードが CA ARCserve Central Applications によって管理され、CA ARCserve D2D に接続されていることを示します。
	'M' という文字を含むこのステータスは、ノードが CA ARCserve Central Applications によって管理され、CA ARCserve D2D に接続できないことを示します。
	'M' という文字を含むこのステータスは、ノードが CA ARCserve Central Applications によって管理され、警告付きで CA ARCserve D2D に接続されていることを示します。
	'M' という文字と右下に感嘆符を含むこのステータスは、ノードが、CA ARCserve Central Applications によって管理された CA ARCserve D2D サーバで、過去 'xx' 時間に同期が成功していないことを示します （'xx' のデフォルトは 48 時間）。または同期がまだ実行されていなかったことを示します。

ノードに対して実行可能な操作

CA ARCserve Central Protection Manager では、ノードの追加、変更、削除、データの同期、ノード設定の指定、ノードのディスカバリ、CSV へのノード情報のエクスポート、およびノードのステータスを判断を行うことができます。

注: 一致する CA ARCserve Backup および CA ARCserve D2D サーバと共にノードを CA ARCserve Central Protection Manager に追加し、各ノード上で同期を実行した場合、その特定のノードのデータが生成され、CA ARCserve Central Reporting で表示することができます。同期の詳細については、「同期データと同期オプション (P. 82)」を参照してください。

ディスカバリを使用したノードの追加

CA ARCserve Central Protection Manager では、ディスカバリ プロセスから複数のノードを追加することができます。

ディスカバリを使用してノードを追加する方法

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. ［ノード］ツールバーの［ディスカバリ］をクリックします。

   ［Active Directory によるノードのディスカバリ］ダイアログ ボックスが表示されます。

3. 以下のフィールドに入力します。

   - ユーザ名（ドメイン）
   - パスワード（ドメイン）
   - コンピュータ名フィルタ

   ［追加］をクリックし、［ディスカバリの開始］をクリックします。

   ディスカバリ (P. 69)が実行されます。

4. ノードのディスカバリが完了すると、以下の確認メッセージが表示されます。

   ディスカバリの結果からのノードの追加を続行してもよろしいですか?

   ［はい］をクリックし、ディスカバリ結果からノードを追加します。

   注: ノードを追加せずにメッセージを閉じるには、［いいえ］をクリックします。

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

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

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

6. （オプション）1 つ以上のノードを選択して［選択したノードを非表示にする］をクリックし、バックアップ対象外のノードを非表示にします。

7. （オプション）［非表示のノードを表示］オプションをオンにすると、非表示になっていたノードが［検出された］ノードリストに戻ります。ノードを再度非表示にするには、このオプションをオフにします。

8. ［ノード認証情報］画面で、追加するノードのユーザ名およびパスワードを指定します。 グローバル認証情報を指定するか、または選択したノードに認証情報を適用できます。

9. ［完了］ボタンをクリックします。

ノードが追加されます。

［ディスカバリ モニタ］ダイアログ ボックス

［ディスカバリ モニタ］ダイアログ ボックスには、ユーザの環境内で検出されたノードの全体的なステータスが表示されます。

［ディスカバリ モニタ］ダイアログ ボックスには、以下の情報が表示されます。

フェーズ

ノード ディスカバリの 3 つのフェーズ（［ノードのディスカバリを実行しています］、［データを更新しています］、［ディスカバリが完了しました］）が表示されます。

ステータス

ディスカバリ プロセス中は、ステータスとして［アクティブ］、ディスカバリが完了すると［完了］が表示されます。

経過時間

ノードのディスカバリに費やした時間を表示します。

処理されたノード数

データベースでログ記録され更新される、処理されたノード数を表示します。

IP アドレスまたはノード名によるノードの追加

CA ARCserve Central Protection Manager では、ノードの IP アドレスまたはホスト名の参照により、CA ARCserve D2D ノードおよび CA ARCserve Backup ノードをノード グループに追加することができます。

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。
5. （オプション）CA ARCserve Backup がノード上にインストールされ、CA ARCserve Central Protection Manager 認証情報に CA ARCserve Backup 管理者権限がない場合、以下のメッセージが表示されます。

   ARCserve Backup 管理者権限が必要です。

   続行するには、CA ARCserve Backup 管理者アカウント用のログイン認証情報を指定し、［OK］をクリックします。

   注: CA ARCserve Central Protection Manager は、CA ARCserve Backup プライマリ サーバおよびスタンド アロン サーバ上でのみデータ同期を実行できます。 プライマリ サーバがブランチ サーバである場合、CA ARCserve Central Protection Manager は Global Dashboard サーバで CA ARCserve Backup データのみを同期できます。

ノードが追加されます。

ディスカバリ結果からのノードの追加

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

次の手順に従ってください:

1. アプリケーションにログインします。

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

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

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

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

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

4. （オプション）1 つ以上のノードを選択して［選択したノードを非表示にする］をクリックし、バックアップ対象外のノードを非表示にします。

5. （オプション）［非表示のノードを表示］オプションをオンにすると、非表示になっていたノードが［検出された］ノードリストに戻ります。ノードを再度非表示にするには、このオプションをオフにします。

6. ［ノード認証情報］画面で、追加するノードのユーザ名およびパスワードを指定します。 グローバル認証情報を指定するか、または選択したノードに認証情報を適用できます。

7. ［完了］ボタンをクリックします。

ノードが追加されます。

ESX/VC からの仮想マシンのインポートによるノードの追加

ノードの追加のこのオプションを使用すると、指定した ESX または vCenter Server ホスト上のすべての仮想マシンを検索および追加できます。

注: 検出可能な仮想マシンは、VMware ツールがインストールされたマシンのみです。

ESX/VC から仮想マシンをインポートしてノードを追加する方法

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. ［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［ESX/VC から仮想マシンをインポート］をクリックします。

   ［ノードのディスカバリ］ダイアログ ボックスが表示されます。

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

   - ESX/vCenter Server ホスト -- スキャンするハイパーバイザを指定します。
   - ユーザ名
   - パスワード
   - ポート
   - プロトコル

   ［接続］をクリックします。

   指定したハイパーバイザがアプリケーションによってスキャンされます。

4. スキャンが完了したら、［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。

5. ［ノード認証情報］画面で、検出されたすべての仮想マシン用のグローバル ユーザ名およびパスワードを指定し、［選択対象に適用］をクリックします。

6. （オプション）仮想マシンをクリックし、その仮想マシン用の特定の認証情報を入力します。

7. ［完了］ボタンをクリックします。

選択された仮想マシンが、指定したノード グループに追加されます。

ファイルからのノードのインポート

CA ARCserve Central Protection Manager では、ファイルから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。

ノードの更新

CA ARCserve Central Protection Manager では、以前に追加されたノードに関する情報を更新することができます。 以下の条件が満たされた場合にノードを更新します。

- すべてのノード：
  - ノードを CA ARCserve Central Protection Manager に登録した後に、新製品がそのノードにインストールされた。
  - ノードを CA ARCserve Central Protection Manager に登録した後に、ノードのユーザ名またはパスワードが更新された。
- **CA ARCserve Backup ノード：**
  - CA ARCserve Backup ブランチ サーバは CA ARCserve Backup プライマリ サーバに更新された。
  - セントラル プライマリ サーバを CA ARCserve Central Protection Manager に登録した後に、CA ARCserve Backup セントラル プライマリ サーバが CA ARCserve Backup プライマリ サーバに更新された。

  注: セントラル プライマリ サーバに関連付けられた CA ARCserve Backup ブランチ サーバとして機能するノードを追加または更新する場合、セントラル プライマリ サーバのホスト名が［ノード］画面上の 2 つの場所に表示されます。 ［ノード］画面上の最初の場所は、［すべてのノード］グループです。 サーバのフル ネームは、サーバのホスト名に含まれる文字数に関係なく、［すべてのノード］グループに表示されます。 ［ノード］画面上の 2 番目の場所は、［グローバル Dashboard グループ］です。サーバのホスト名が 15 文字を超える場合、サーバのホスト名は［グローバル Dashboard グループ］内で 15 文字に切り詰められます。

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。

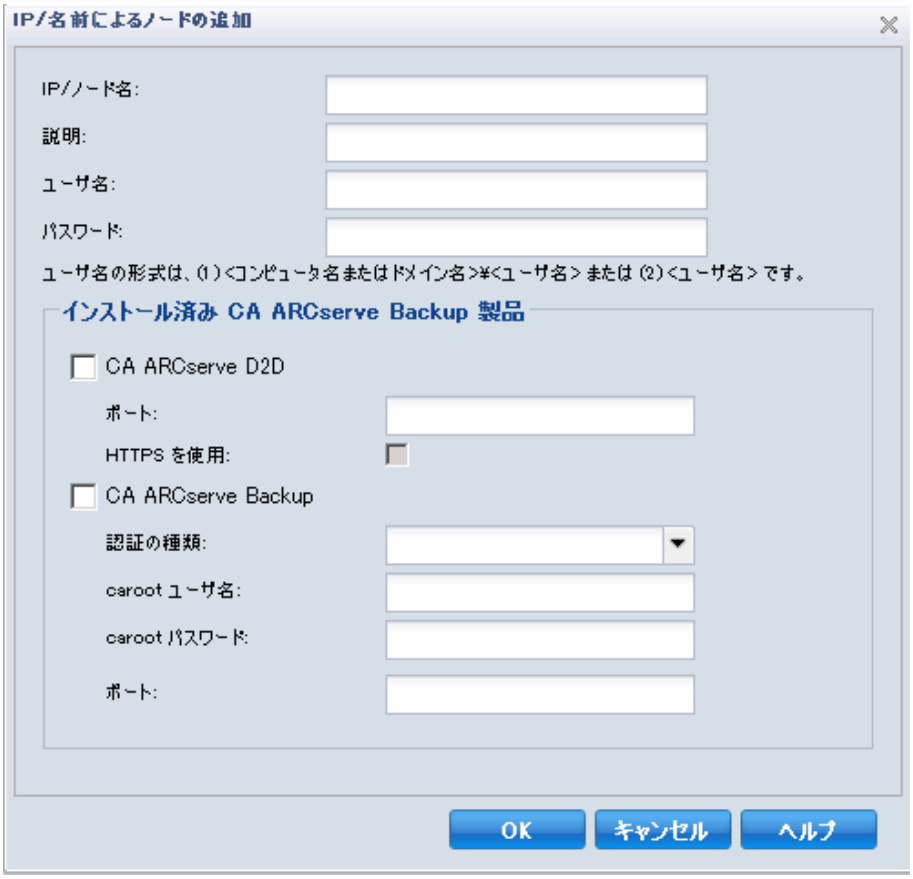
4. 必要に応じてノードの詳細を更新します。

   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: 前述の手順で述べたフィールドの少なくとも 1 つを更新した場合、［ノードの更新］ダイアログ ボックスが開き、より詳細を指定することができます。



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。

ノードの削除

CA ARCserve Central Protection Manager では、お使いの環境からノードを削除することができます。

次の手順に従ってください:

1. アプリケーションにログインします。

   ナビゲーション バーの［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。

ファイルへのノードのエクスポート

CA ARCserve Central Protection Manager では、選択されたノード グループからノードを認証情報情報と共に CSV ファイルにエクスポートすることができます。

ファイルにノードをエクスポートする方法

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. エクスポートするノード グループを選択します。

   選択されたノード グループのノードが表示されます。

3. ［ノード］ツールバーから［エクスポート］をクリックします。

   メッセージが表示され、プレーン テキストで表示されるパスワードが CSV ファイルに含まれることが通知されます。

   ［はい］をクリックして CSV ファイルを開くまたは保存するか、［いいえ］をクリックしてキャンセルします。

ノードが CSV ファイルにエクスポートされます。

CA ARCserve D2D ノードへのログイン

CA ARCserve Central Protection Manager のホーム画面から、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。

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

シナリオ	対処法
CA ARCserve Central Protection Manager 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 Protection Manager 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 Protection Manager 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. 161)」を参照してください。

マージ ジョブ オプション

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

ノード上のマージ ジョブの一時停止

CA ARCserve Central Protection Manager では、特定ノードのマージ ジョブを一時停止できます。

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

次の手順に従ってください:

1. CA ARCserve Central Protection Manager ホーム画面で、ナビゲーション バーの［ノード］をクリックして［ノード］画面を開きます。
2. マージ ジョブを一時停止するノードが含まれるノード グループを選択します。

   選択されたノード グループのノードのリストが表示されます。
3. マージ ジョブを一時停止するノードをクリックします。 次に、選択したノードを右クリックし、ポップアップ メニューからの［マージ ジョブの一時停止］をクリックします。

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

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

ノード上のマージ ジョブの再開

CA ARCserve Central Protection Manager では、一時停止した特定のノードのマージ ジョブを再開できます。

次の手順に従ってください:

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

   選択されたノード グループのノードのリストが表示されます。
3. 一時停止されたマージ ジョブを再開するノードをクリックします。次に、選択したノードを右クリックし、ポップアップ メニューからの［マージ ジョブの再開］をクリックします。

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

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

同期データと同期オプション

CA ARCserve Central Protection Manager では、各ノードに対してデータを同期する機能が提供されています。そのためには、CA ARCserve Backup プライマリ サーバ（asdb）、CA ARCserve D2D、または Global Dashboard セントラル プライマリ データベース（central_asdb）から CA ARCserve Central Protection Manager データベース（ARCAppDB）にデータを転送します。

データを同期することによって、複数のデータベースにあるデータが、整合性の取れた最新の状態に保たれ、登録済みの各ブランチ サイトのデータベースと同じ情報がセントラル サイトのデータベースに格納されます。

このセクションには、以下のトピックが含まれます。

特定のノードまたはノード グループに対する CA ARCserve Backup データのフル同期の実行

CA ARCserve Central Protection Manager では、特定のノードまたはノード グループ上で、CA ARCserve Backup データのフル同期を実行することができます。

CA ARCserve Backup のフル同期プロセスの実行中は、CA ARCserve Backup データベース エンジンが数分間停止します。 これにより、データベース同期プロセスが完了するまで、CA ARCserve Backup ジョブ情報が記録されるのを防ぐことができます。

特定のノードまたはノード グループに対して CA ARCserve Backup データのフル同期を実行する方法

1. CA ARCserve Central Protection Manager ホーム画面から、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. 同期するノードが含まれるノード グループを選択します。

   選択されたノード グループのノードのリストが表示されます。

3. 以下のいずれかを行います。

   - 特定のノードについては、グループの右側から CA ARCserve Backup ノードを選択し、ポップアップ メニューまたは［ノード］ツールバーの［データの同期］ボタンから［CA ARCserve Backup のフル同期］をクリックします。
   - ノードのグループの場合、ノード グループを右クリックし、コンテキスト メニューの［CA ARCserve Backup のフル同期］をクリックします。

CA ARCserve Central Protection Manager は、選択したノードまたはノード グループについて CA ARCserve Backup データのフル同期をサブミットします。

特定のノードまたはノード グループに対する CA ARCserve Backup データの増分同期の実行

CA ARCserve Central Protection Manager では、特定のノード上で CA ARCserve Backup データの増分同期を実行することができます。

CA ARCserve Backup の増分同期は、前回の同期が実行されてから変更、削除、追加されたデータが同期されます。 同期されたデータは、最小サイズに圧縮されてから送信されます。

特定のノードまたはノード グループに対して CA ARCserve Backup データの増分同期を実行する方法

1. CA ARCserve Central Protection Manager ホーム画面から、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. 同期するノードが含まれるノード グループを選択します。

   選択されたノード グループのノードのリストが表示されます。

3. 以下のいずれかを行います。

   - 特定のノードについては、グループの右側から CA ARCserve Backup ノードを選択し、ポップアップ メニューまたは［ノード］ツールバーの［データの同期］ボタンから［CA ARCserve Backup の増分同期］をクリックします。
   - ノードのグループの場合、ノード グループを右クリックし、コンテキスト メニューの［CA ARCserve Backup の増分同期］をクリックします。

CA ARCserve Central Protection Manager は、選択したノードまたはノード グループについて CA ARCserve Backup データの増分同期をサブミットします。

特定のノードまたはノード グループに対する CA ARCserve D2D データのフル同期の実行

CA ARCserve Central Protection Manager では、特定のノードまたはノード グループ上で、CA ARCserve D2D データのフル同期を実行することができます。

特定のノードまたはノード グループに対して CA ARCserve D2D データのフル同期を実行する方法

1. CA ARCserve Central Protection Manager ホーム画面から、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. 同期するノードが含まれるノード グループを選択します。

   選択されたノード グループのノードのリストが表示されます。

3. 以下のいずれかを行います。

   - 特定のノードについては、グループの右側から CA ARCserve D2D ノードを選択し、ポップアップ メニューまたは［ノード］ツールバーの［データの同期］ボタンから［CA ARCserve D2D のフル同期］をクリックします。
   - ノードのグループの場合、ノード グループを右クリックし、コンテキスト メニューの［フル同期 CA ARCserve D2D］をクリックします。

CA ARCserve Central Protection Manager は、選択したノードまたはノード グループについて CA ARCserve D2D データのフル同期をサブミットします。

ノード設定

CA ARCserve Central Protection Manager では、増分同期を実行するために、各 CA ARCserve Backup または Global Dashboard セントラル プライマリ ノードのローカル スケジュールを設定することができます。

CA ARCserve Backup データ同期スケジュールの適用

CA ARCserve Backup 設定では、各 CA ARCserve Backup ノードに対してカスタマイズされたスケジュールを設定できます。

CA ARCserve Backup データ同期スケジュールを適用する方法

1. CA ARCserve Central Protection Manager ホーム画面から、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. CA ARCserve Backup 設定を適用するノードを含むノード グループを［グループ］リストから選択します。

   選択されたノード グループのノードのリストが表示されます。

3. 設定を適用するノードを選択し、次に、ポップアップ メニューから［CA ARCserve Backup データ同期スケジュール］をクリックします。

   ［CA ARCserve Backup データ同期スケジュール］ダイアログ ボックスが表示されます。

4. 以下のオプションから 1 つを選択します。

   - **有効** -- ［繰り返し方法］および［スケジュールされた時刻］を入力することにより、スケジュール オプションを指定できます。
     - 指定の日数ごと
     - 指定の曜日ごと
     - 月の指定の日付ごと
   - **無効** -- このオプションの場合、設定は適用されません。
   - **グローバル設定を使用** -- CA ARCserve Backup 環境設定モジュールで設定されたグローバル設定を適用します。詳細については、「CA ARCserve Backup データ同期スケジュール」を参照してください。

5. ［OK］をクリックします。

CA ARCserve Backup 設定が適用されます。

ノード グループに対して実行可能な操作

CA ARCserve Central Protection Manager では、ノード グループを作成し、個別のノードを各グループに割り当てたり、ノード グループを変更および削除したりすることができます。

注: 変更および削除できるのは、自分で作成したノード グループのみです。

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。
- **vCenter/ESX グループ** -- ［vCenter/ESX から仮想マシンをインポート］オプションを使用してノードを追加した場合、vCenter/ESX Server の名前がこのグループに追加されます。
- **Global Dashboard グループ** -- セントラル プライマリ サーバと関連付けら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。

注: CA ARCserve Backup Global Dashboard ノードをノード グループに割り当てると、すべての CA ARCserve Backup ブランチがそのノード グループに属するわけではない場合でも、すべてのブランチが CA ARCserve Backup Global Dashboard ノードに表示されます。 そのため、CA ARCserve Central Reporting アプリケーションで CA ARCserve Backup Global Dashboard ノードが含まれるノード グループを選択すると、Global Dashboard ノードからのすべてのブランチのデータがレポートに表示されません。

ノード グループの削除

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

作成したノード グループを削除できます。

以下のノード グループは削除できません。

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

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

次の手順に従ってください:

1. アプリケーションにログインします。

   ホーム画面上のナビゲーション バーから［ノード］をクリックして［ノード］画面を開きます。

2. 削除するノード グループをクリックし、［ノード グループ］ツールバーの［削除］をクリックします。

   確認メッセージのダイアログ ボックスが表示されます。

3. ノード グループを削除する場合は、［はい］をクリックします。

   注: ノード グループを削除しない場合は、［いいえ］をクリックします。

ノード グループが削除されます。

ディスカバリを使用したノードの検索

CA ARCserve Central Protection Manager では、ディスカバリを使用してノードを検索することができます。 Protection Manager は、サーバの Active Directory 内に保持された情報に基づいてノードを検索します。 Active Directory は以下の情報を提供します。

- マシン名
- オペレーティング システム情報（名前、バージョン、パッチ）
- Microsoft Exchange Server がマシン上に存在するかどうか
- Microsoft SQL Server がマシン上に存在するかどうか

ディスカバリを使用してノードを検索する方法

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. ［ノード］カテゴリから［ディスカバリ］をクリックして、［Active Directory によるノードのディスカバリ］ダイアログ ボックスを開きます。

3. ［Active Directory によるノードのディスカバリ］ダイアログ ボックスで以下のフィールドに入力し、［追加］をクリックします。
   - （ドメイン）ユーザ名
   - （ドメイン）パスワード
   - コンピュータ名フィルタ

   ［ディスカバリ］をクリックします。

   ディスカバリ プロセス (P. 69)が開始されます。
4. ディスカバリが完了すると、以下の確認メッセージが表示されます。

   ディスカバリの結果からのノードの追加を続行してもよろしいですか?

   以下のいずれかを行います。
   - ［はい］をクリックし、［ディスカバリ結果からのノードの追加］に移動します。
   - ［いいえ］をクリックし、メッセージを閉じます。

   注: ［はい］を選択した場合、詳細については、「ディスカバリを使用したノードの追加 (P. 67)」を参照してください。

CA ARCserve D2D 展開タスク

CA ARCserve Central Protection Manager では、1 つ以上のノードをリモートまたはローカルで同時にターゲット システムに展開できます。 また、展開用のノードを追加または編集したり、展開からノードを削除したりできます。

このセクションには、以下のトピックが含まれます。

ノードへの CA ARCserve D2D の展開

CA ARCserve Central Protection Manager では、1 つ以上の新規または既存のノードに対して、CA ARCserve D2D の最新のバージョンのディスカバリおよび展開を行うことができます。

注: Windows XP を実行するコンピュータに CA ARCserve D2D を展開するには、リモート Windows XP コンピュータ上で［簡易ファイルの共有を使用する］オプションを無効にします。

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［ノード］をクリックします。
2. ［ノード］画面で、ツールバー上の［展開］をクリックします。

   使用許諾契約のダイアログ ボックスが表示されます。
3. 使用許諾契約の条件を確認して同意し、［次へ］をクリックすると［D2D 展開］ダイアログ ボックスが開きます。
4. ［D2D 展開］ダイアログ ボックスから、共通の基準に基づいた利用可能なノードのグループ名およびノード名フィルタを指定します。

   各ノードの［名前］、［バージョン］、および［ステータス］が表示されます。

   注:［バージョン］列には、ノードを実行している現在の D2D バージョンが表示されます。
5. D2D を展開するノードの隣のチェック ボックス、または、リストされているすべてのノードが対象の場合は［すべて選択］をクリックします。

   注: ［すべて選択］をクリックすると、ユーザが簡単に操作できるように［すべて選択解除］に変更されます。 さらに、［ノード］リストからノードを選択した場合は、［ノード情報］タブからノード フィールドを編集できます。
6. ［今すぐ展開］をクリックすると、最新の D2D バージョンがノードに展開され、タイトル バーに表示されます。

   注: 特定のノードの情報および展開ステータスを参照するには、ノードを強調表示し、右側のペインで該当するタブを選択します。

注: CA ARCserve Central Protection Manager で D2D 展開ユーティリティを使用すると、古いバージョンがインストールされている、または、CA ARCserve D2D がインストールされていないノードに、CA ARCserve D2D の最新バージョンをインストール、アップグレード、および展開できます。

展開用のノードの追加

CA ARCserve Central Protection Manager では、複数のノードを展開用に追加することができます。

展開用にノードを追加する方法

1. アプリケーションにログインし、ナビゲーション バーの［ノード］をクリックします。
2. ［ノード］画面で、ツールバー上の［展開］をクリックします。

   使用許諾契約のダイアログ ボックスが表示されます。
3. 使用許諾契約の内容を確認して同意し、［次へ］をクリックします。

   ［D2D 展開］ダイアログ ボックスが表示されます。

4. ［D2D 展開］ダイアログ ボックスで、［追加］をクリックして以下のフィールドに入力します。
   - サーバ名
   - ユーザ名
   - パスワード
   - ポート
   - インストール パス
   - セットアップでドライバをインストールするかどうか（デフォルトでは選択）
   - 再起動（デフォルトではオン）

     再起動が成功した時点でノードが展開される場合（オン）、ノードは CA ARCserve Central Applications によって管理されるノード リストに追加されます。

     再起動オプションなしでノードが展開される場合（オフ）、ノードは CA ARCserve Central Applications によって管理されないノード グループに追加されます。
   - HTTPS を使用（デフォルトではオフ）

     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。

   注: 追加したノードは、［すべてのノード］および[グループ化解除済みグループ]フィルタ以下で表示できます。
5. ［OK］ボタンをクリックするとノードが追加されます。

展開用のノードの編集

CA ARCserve Central Protection Manager では、展開用にノードを編集することができます。

展開用にノードを編集する方法

1. アプリケーションにログインし、ナビゲーション バーの［ノード］をクリックします。
2. ［ノード］画面で、ツールバー上の［展開］をクリックします。

   使用許諾契約のダイアログ ボックスが表示されます。

3. 使用許諾契約の内容を確認して同意し、［次へ］をクリックします。

   ［D2D 展開］画面が表示されます。

4. 展開に対して編集するノードを選択し、［編集］をクリックすると［編集］ダイアログ ボックスが開きます。

5. ［編集］ダイアログ ボックスで、変更するデータを編集し、［OK］をクリックします。

展開からのノードの削除

CA ARCserve Central Protection Manager では、1 つ以上のノードを展開から削除することができます。

展開からノードを削除する方法

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

2. ［ノード］画面で、ツールバー上の［展開］をクリックします。

   使用許諾契約のダイアログ ボックスが表示されます。

3. 使用許諾契約の内容を確認して同意し、［次へ］をクリックします。

   ［D2D 展開］画面が表示されます。

4. 展開から削除するノード（複数可）を選択します。

5. ［削除］をクリックすると、D2D 展開からノードが削除されます。

ノード グループのフィルタ

CA ARCserve Central Protection Manager 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ノードを表示します。CA ARCserve Central Protection Manager では以下のアプリケーション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. CA ARCserve Central Protection Manager 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 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。

CA ARCserve D2D ポリシーの管理方法

CA ARCserve Central Protection Manager には、CA ARCserve D2D ポリシーの管理に使用できるさまざまなツールやオプションが用意されています。このセクションでは、リモート サーバでのポリシーの追加、削除、変更、D2D 展開、コピーの方法について説明します。一元化されたバックアップ ポリシーを作成し、複数の管理対象ノードに同時に配布することができます。

一元化されるバックアップ ポリシーの一般的な例として以下が挙げられます。

- スケジュール
- ジョブ
- デスティネーション
- イベント
- 設定

このセクションには、以下のトピックが含まれます。

ポリシーの作成

CA ARCserve Central Protection Manager では、D2D ノードに割り当てるポリシーを作成することができます。

次の手順に従ってください:

1. CA ARCserve Central Protection Manager ホーム画面で、ナビゲーションバーの［ポリシー］をクリックして［ポリシー］画面を開きます。
2. ［新規］をクリックして、［新規ポリシー］ダイアログ ボックスを開きます。
3. ポリシー名を入力し、［バックアップ設定 (P. 100)］、［ファイル コピー設定 (P. 121)］、［復旧ポイントのコピー (P. 139)］、［環境設定 (P. 144)］の各タブ内のフィールドに入力します。
4. ［保存］をクリックします。

新規ポリシーが保存され、ポリシーを今すぐノードに割り当てるかどうかを確認するメッセージが表示されます。［いいえ］をクリックすると、［ポリシー］画面上に新規ポリシーが表示されます。［はい］をクリックすると、［ポリシーの割り当て/割り当て解除］ (P. 162)画面が表示されます。

バックアップ設定の管理

バックアップ設定では、バックアップのソース、バックアップ先、バックアップの種類別のスケジュール、バックアップ ジョブの設定や拡張設定などの動作を定義することができます。これらの設定は、［ポリシー］画面でいつでも変更できます。

バックアップ設定を管理するには、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、［新規］をクリックします。

このセクションには、以下のトピックが含まれます。

保護設定の指定

CA ARCserve Central Protection Manager では、バックアップするデータの保護設定を指定することができます。

保護設定を指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。

2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開き、［バックアップ設定］タブに［保護設定］オプションが表示されます。

3. **バックアップ先**を指定します。

   バックアップ場所としてローカル パス（ボリュームやフォルダ）、またはリモート共有フォルダ（またはマップされたドライブ） を指定できます。

   a. ローカル パス（ボリュームまたはフォルダ）にバックアップするように指定する場合、バックアップ ソースと同じ場所をバックアップ先に指定することはできません。 バックアップ先にソースが含まれている場合、バックアップ ジョブではソースのこの部分を無視するため、バックアップには含まれません。

      たとえば、ローカル コンピュータ全体（ボリューム C、D、および E で構成）をバックアップする際に、バックアップ先としてボリューム E を指定した場合は、CA ARCserve D2D ではボリューム C および D のみがボリューム E にバックアップされます。 ボリューム E のデータはバックアップに含まれません。 ローカル ボリュームをすべてバックアップする場合は、バックアップ先としてリモート ロケーションを指定する必要があります。

      重要: 指定したバックアップ先ボリュームにシステム情報が含まれていないことを確認してください。システム情報が含まれていると、そのボリュームは保護（バックアップ）されず、必要が生じてベア メタル復旧（BMR）を実施したときにシステムの復旧に失敗します。

      注: ダイナミック ディスクをディスク レベルでリストアすることはできません。 ダイナミック ディスク上のボリュームにデータがバックアップされた場合、このダイナミック ディスクを BMR 実行中にリストアすることはできません。

b. リモート共有場所にバックアップすることを選択した場合、パスを指定するか、場所を参照して選択し、リモート コンピュータにアクセスするためのユーザ認証情報（ユーザ名とパスワード）を指定する必要があります。

c. 前回のバックアップが実行された後、指定したバックアップ先が変更されている場合、バックアップの種類を選択する必要があります。 このオプションは、バックアップ先を変更した場合に有効になります。 利用可能なオプションは、「フル バックアップ」と「増分バックアップ」です。

- **フル バックアップ** -- 次に実行されるバックアップがフル バックアップであることを指定します。新しいバックアップ先には、古いバックアップ先との依存関係はありません。 フル バックアップを続行する場合、バックアップを続行するために前の場所を指定する必要はありません。前回のバックアップ先からリストアを実行しない場合、リストア用に古いバックアップを保持するか、削除するかを選択できます。この選択は、今後のバックアップには影響を与えることはありません。

- **増分バックアップ** -- 次に実行されるバックアップが増分バックアップであることを指定します。次の増分バックアップを新しいバックアップ先に対して実行する場合は、前回のバックアップ先にあるバックアップをすべてコピーすることはありません。ただし、変更には増分データのみが含まれているため（フル バックアップ データではない）、新しいバックアップ先は前回のバックアップ先に依存することになります。前回のバックアップ先からデータを削除しないでください。 バックアップ先を別のフォルダに変更し、増分バックアップの実行時に前回のバックアップ先が存在しない場合、バックアップは失敗します。

4. **バックアップ ソース**を指定します。

   コンピュータ全体またはコンピュータの個別のボリュームをバックアップ対象として指定できます。

   - **マシン全体をバックアップする** -- マシン全体をバックアップするように指定します。 マシン上のすべてのボリュームがバックアップされます。

     注: マシン全体のバックアップが選択された場合、CA ARCserve D2D は現在のマシンに接続されているすべてのディスク/ボリュームを自動的に検出し、それらをバックアップ対象に追加します。

     たとえば、バックアップ設定の実行後に新しいディスクがマシンに接続された場合でもバックアップ設定を変更する必要はなく、新しいディスク上のデータは自動的に保護されます。

   - **バックアップする個々のボリュームを選択する** -- このボリュームフィルタ機能を使用すると、選択されたボリュームのみをバックアップするよう指定できます。 ただし、ユーザがリモート CA ARCserve D2D サーバに存在しないボリュームを指定すると、バックアップ中、ボリュームは自動的にスキップされます。たとえば、ボリューム C、D、および E をバックアップするよう指定し、ボリューム C および D のみを含む CA ARCserve D2D サーバに割り当てます。ポリシーは CA ARCserve D2D サーバのボリューム C および D に割り当てられますが、ボリューム E はスキップされ、アクティビティ ログに警告メッセージが保存されます。

     また、リスト内のすべてのボリュームを選択または選択解除することもできます。

     注: 一部のボリュームがバックアップ対象として明示的に選択されている場合は、選択されたボリュームのみがバックアップされます。

     通知メッセージは以下の条件で表示されます。

     - **BMR 関連** -- システム/ブート ボリュームがバックアップ対象に選択されていない場合、バックアップが BMR に使用できないことを通知する警告メッセージが表示されます。

5. ［**保存設定**］を指定します。

   保存する復旧ポイントの数（セッションをマージ）または保存する復旧セットの数（復旧セットを削除し、無限増分バックアップを無効化）に基く保存ポリシーを設定できます。

   - 復旧ポイント - これが推奨オプションです。 このオプションを選択すると、無限増分バックアップの機能をフルに活用してストレージ容量を節約できます。
   - 復旧セット - このオプションは、通常、規模の大きいストレージ環境で使用します。 このオプションを選択すると、大量のデータを保護している場合、バックアップ ウィンドウ時間を効率的に管理できるバックアップ セットを作成および管理できます。 このオプションは、バックアップの容量よりもバックアップ時間を優先する場合に使用します。

   デフォルト： 復旧ポイントの保持

復旧ポイントの保持

保持する復旧ポイント（フル、増分および検証バックアップ イメージ）の数を指定する場合、このオプションを選択します。

- **保持する復旧ポイント数の指定**

  指定した制限数を超えると、CA ARCserve D2D によって、最も早い（最も古い）増分/子バックアップが親バックアップにマージされ、「親と最も古い子」のブロックを含むベースライン イメージが作成されます。 最も古い子バックアップを親バックアップにマージするサイクルは、それ以降のバックアップごとに繰り返されます。これによって、同じ保持数を維持しながら、継続的に増分バックアップを実行できます。

  注: デスティネーションの空き容量が不足している場合、保持する復旧ポイントの数を減らすことを検討してください。

  デフォルト： 31

  最小： 1

  最大： 1344

- **マージ ジョブの実行** -- マージ ジョブを実行するタイミングについて、以下のいずれかのオプションを選択してください。

  - **至急** -- 任意の時点でマージ ジョブを実行する場合にこのオプションを選択します。
  - **以下の時間範囲のすべての日** -- 指定した時間帯にマージ ジョブを実行する場合、このオプションを選択します。時間帯を指定すると、マージ ジョブの実行が長時間におよぶ場合でも、マージ ジョブにより実稼働サーバ上で過剰な I/O 処理が発生するのを防ぐことができます。

    注: マージ ジョブを実行する時間範囲を設定するときは、関連するバックアップ ジョブがマージの開始前に完了できるように時間範囲を指定します。

復旧セットの保持

保持する復旧セットの数を指定する場合、このオプションを選択します。 この設定では、無限増分バックアップを無期限に無効化し、セッションのマージは行いません。 復旧セットを使用すると、マージ ジョブが完了するまでの時間を減らすことができます。

– 保持する復旧セット数の指定

保持する復旧セットの数を指定する場合、このオプションを選択します。 復旧セットは、フル バックアップから始まり、そのあとに複数の増分、検証、またはフル バックアップが続く、一連のバックアップです。

例 - セット **1** :

- フル
- 増分
- 増分
- 検証
- 増分

例 - セット **2** :

- フル
- 増分
- フル
- 増分

新しい復旧セットを開始するには、フル バックアップが必要です。 指定された時間に実行するよう設定またはスケジュールされたフル バックアップがない場合でも、セットを開始するバックアップは自動的にフル バックアップに変換されます。

注: 既存の復旧セット数を計算する際、未完了の復旧セットは無視されます。 復旧セットが完了しているとみなされるのは、次の復旧セットの開始バックアップが作成されたときです。

デフォルト： 2

最小： 1

最大： 100

注: 復旧セットを削除して、バックアップ用のストレージ容量を節約したい場合は、保持するセット数を減らします。CA ARCserve D2D が最も古い復旧セットを自動的に削除します。 復旧セットは手動で削除しないようにしてください。

例 1 - 復旧セット:

- バックアップの開始時刻は 2012 年 8 月 20 日午前 6:00 です。
- 12 時間ごとに増分バックアップを実行します。
- 新しい復旧セットは、金曜日の最終バックアップから開始します。
- 3 個の復旧セットを保持します。

この例では、増分バックアップは毎日午前 6:00 および午後 6:00 に実行されます。 最初のバックアップ（フル バックアップである必要があります）を取る際、最初の復旧セットが作成されます。 最初のフル バックアップは復旧セットの開始バックアップとしてマークされます。 金曜日の午後 6:00 にスケジュールされたバックアップは、実行と同時にフル バックアップに変換され、復旧セットの開始バックアップとしてマークされます。

例 2 - 復旧セット:

- 保持する復旧セット数を 1 に指定します。

注: CA ARCserve D2D は、完了したセットを 1 つ保持するため、次の復旧セットの開始まで、常に 2 つのセットを保持します。

例 3 - 復旧セット:

- 保持する復旧セット数を 2 に指定します。

注: 4 番目の復旧セットを開始する際、CA ARCserve D2D は、最初の復旧セットを削除します。 これにより、最初のバックアップが削除され、かつ、4 番目のバックアップが開始された時点で、ディスク上には 2 個の復旧セットが存在します（復旧セット 2 および 3）。

保持する復旧セットの数を 1 つに指定した場合でも、少なくともフル バックアップ 2 個分の容量が必要になります。

- 新しい復旧セットを開始する間隔：
  - **週の選択された曜日** -- 新しい復旧セットを開始する曜日を指定します。
  - **月の選択された日付** -- 新しい復旧セットを開始する月の日付を指定します。 1 ～ 30 の日付を指定します。また、月の日数は異なった値を取るため（28、29、30、または 31 日）、月の最終日を復旧セットの作成日として指定することができます。
- 新しい復旧セットを開始する対象：
  - **選択された日の最初のバックアップ** -- 新しい復旧セットを開始する曜日を指定します。
  - **選択された日の最後のバックアップ** -- 新しい復旧セットを、指定した日の最後にスケジュールされたバックアップで開始する場合に指定します。最後のバックアップでセットを開始することを選択し、何らかの理由で最後のバックアップが実行されなかった場合、その次にスケジュールされたバックアップがフル バックアップに変換されてセットを開始します。 次のバックアップが（緊急事態により、即座に増分バックアップを実行したなどの理由により）アドホックに実行された場合は、フルバックアップを実行して復旧セットを開始するか、または、増分バックアップを実行して次のバックアップで復旧セットを開始するかを決定できます。

    注: アドホック バックアップを実行した場合、最終バックアップはその日の最後のバックアップではない場合があります。

6. **圧縮**の種類を指定します。

   バックアップに使用する圧縮の種類を指定するためにこのオプションを選択します。

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

利用できる圧縮オプションは以下のとおりです。

- **圧縮なし**

  圧縮は実行されません。 このオプションを使用すると、CPU 使用率は最も低くなります （最も高速で動作します）。ただし、バックアップ イメージのディスク容量の使用率は最大になります。

- **標準圧縮**

  一般的な圧縮が実行されます。このオプションを使用すると、CPU 使用率とディスク容量使用率のバランスを適度に調節します。 これはデフォルトの設定です。

- **最大圧縮**

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

以下のシナリオに注意してください。

- バックアップ イメージに圧縮できないデータ（JPG イメージや ZIP ファイルなど）が含まれている場合、それらのデータを処理するために、追加のストレージ領域を割り当てる必要が生じることがあります。 圧縮オプションを指定し、バックアップ ソースに圧縮できないデータが含まれている場合、ディスク容量の使用量が全体的に増加する可能性があります。
- 圧縮レベルを［圧縮なし］から［標準圧縮］または［最大圧縮］に変更した場合、または、［標準圧縮］や［最大圧縮］から［圧縮なし］に変更した場合、圧縮レベルの変更後に実行される最初のバックアップは自動的にフル バックアップとなります。 フル バックアップを実行した後、それ以降のすべてのバックアップ（フル、増分、検証）はスケジュールどおりに実行されます。
- デスティネーションの空き容量が足りない場合、バックアップの圧縮設定を高くすることを検討してください。

7. **暗号化**設定を指定します。

   a. バックアップに使用する暗号化アルゴリズムの種類を選択します。

      データの暗号化とは、解読メカニズムがなければ理解できない形式にデータを変換することです。 CA ARCserve D2D のデータ保護では、安全な AES （Advanced Encryption Standard）暗号化アルゴリズムを使用し、指定したデータに対して最大限のセキュリティおよびプライバシーを確保します。

利用可能なオプションは、暗号化なし、AES-128、AES-192、および AES-256 です（暗号化を無効にするには、［暗号化なし］を選択します）。

- フル バックアップと関連するすべての増分/検証バックアップで同じ暗号化アルゴリズムを使用する必要があります。
- 増分または検証バックアップの暗号化アルゴリズムが変更された場合、フル バックアップが実行される必要があります。つまり、暗号化アルゴリズムが変更されたら、元のバックアップの種類にかかわらず、最初のバックアップはフル バックアップになります。

  たとえば、アルゴリズム形式を変更し、カスタマイズされた増分または検証バックアップを手動でサブミットすると、自動的にフル バックアップに変換されます。

b. 暗号化アルゴリズムを選択した場合は、暗号化パスワードを指定（および確認）します。

- 暗号化パスワードは最大 23 文字に制限されています。
- フル バックアップと関連するすべての増分/検証バックアップでは、データの暗号化に同じパスワードを使用する必要があります。
- 増分/検証バックアップの暗号化パスワードが変更された場合、フル バックアップを実行する必要があります。 つまり、暗号化パスワードが変更されたら、元のバックアップの種類にかかわらず、最初のバックアップは常にフル バックアップになります。

  たとえば、暗号化パスワードを変更し、カスタマイズされた増分/検証バックアップを手動でサブミットすると、自動的にフル バックアップに変換されます。

c. CA ARCserve D2D では暗号化パスワード管理が提供されるため、ユーザが暗号化パスワードを記憶している必要がありません。

- パスワードも暗号化されます。
- 同じマシンにリストアする場合は、パスワードが記憶されているため必要ありません。
- 別のマシンにリストアする場合、パスワードは必須です。
- 暗号化されたデータが含まれる復旧ポイントのエクスポートを試行し、その復旧ポイントが現在のマシンで実行されたバックアップに含まれている場合、パスワードは必要ありません。
- 暗号化されたデータの回復を、エクスポートされた復旧ポイントから実行する場合は常にパスワードが必要です。
- 暗号化された復旧ポイントを参照するのにパスワードは必要ありません。
- BMR を実行するためにはパスワードが必須です。

d. 暗号化が有効になると、アクティビティ ログが更新されます。

- メッセージがアクティビティ ログに記録され、バックアップごとに選択された暗号化アルゴリズムについて記述されます。
- メッセージがアクティビティ ログに記録され、増分/検証バックアップがフル バックアップに変換された理由（パスワード変更またはアルゴリズム変更）について示されます。

注: バックアップに対して暗号化設定を同じままにする必要はありません。 同じデータを複数回バックアップした後でも、これらの設定はいつでも変更できます。

8. **スロットル バックアップ**を指定します。

バックアップが書き込まれる最高速度（MB/分）を指定できます。CPU またはネットワークの使用率を削減するためにバックアップ速度のスロットル制御を実行できます。 ただし、バックアップ速度を制限すると、バックアップ ウィンドウに悪影響を及ぼします。バックアップの最高速度を抑えるれば抑えるほど、バックアップの実行にかかる時間は増大します。

注: デフォルトでは、［スロットル バックアップ］オプションは有効ではなく、バックアップ速度は制御されません。

9. ［保存］をクリックします。

保護設定が保存されます。

バックアップ スケジュールの指定

CA ARCserve Central Protection Manager では、バックアップのスケジュールを指定できます。

バックアップ スケジュールを指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。

2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開きます。

3. ［スケジュール］タブをクリックします。

   スケジュール オプションを表示するダイアログ ボックスが表示されます。

4. バックアップ スケジュール オプションを指定します。

   - **開始日時の設定** -- スケジュールされたバックアップの開始日および開始時刻を指定します。

     注: バックアップ ジョブの繰り返し間隔を設定するときは、以前のジョブおよび関連するすべてのマージ ジョブが、次回のバックアップ ジョブが開始する前に完了できるように十分な時間を確保してください。 この時間は、ユーザ固有のバックアップ環境および履歴に基づいて概算することができます。

   - **増分バックアップ** -- 増分バックアップのバックアップ スケジュールを指定します。

     スケジュールされたとおりに、前回の成功したバックアップ以降に変更されたブロックのみの増分バックアップが CA ARCserve D2D によって実行されます。 増分バックアップのメリットは、バックアップを高速で実行できること、また作成されるバックアップ イメージのサイズが小さいということです。 これは、バックアップを実行する場合に最も適した方法です。そのため、デフォルトではこのオプションを使用します。

     利用可能なオプションは「繰り返し実行する」と「実行しない」です。 ［繰り返し実行する］オプションを選択した場合、バックアップの実行間隔（分単位、時間単位、または日単位）を指定する必要があります。増分バックアップの最小設定は 15 分ごとです。

     デフォルトでは、増分バックアップのスケジュールは 1 日ごとに繰り返すよう設定されています。

   - **フル バックアップ** -- フル バックアップのバックアップ スケジュールを指定します。

     CA ARCserve D2D は、スケジュールされたとおりに、ソース マシンから、使用されているすべてのブロックのフル バックアップを実行します。 利用可能なオプションは「繰り返し実行する」と「実行しない」です。 ［繰り返し実行する］オプションを選択した場合、バックアップの実行間隔（分単位、時間単位、または日単位）を指定する必要があります。フル バックアップの最小設定は 15 分ごとです。

     デフォルトでは、フル バックアップのスケジュールは［実行しない］（スケジュールされている繰り返しはない）です。

   - **検証バックアップ** -- 検証バックアップのバックアップ スケジュールを指定します。

CA ARCserve D2D は、スケジュールされたとおりに、保護されたデータが有効で完全であることを検証します。保存されたバックアップ イメージの信頼性チェックを元のバックアップ ソースに対して実行し、必要に応じてイメージを再同期します。 検証タイプのバックアップは、個別のブロックの最新バックアップを参照し、そのコンテンツおよび情報をソースと比較します。 この比較によって、前回バックアップされたブロックが、ソースの対応する情報を表しているかどうかを検証します。 ブロックのバックアップ イメージがソースと一致しない場合（多くは、最後のバックアップ以降にシステムに変更が加えられていることが原因）、CA ARCserve D2D によって、一致していないブロックのバックアップが更新（再同期）されます。また、検証バックアップは、フル バックアップほどの容量を使用せずに、フル バックアップの信頼性を確認するためにも使用できます。

検証バックアップのメリットは、変更されたブロック（前回のバックアップと一致しないブロック）のみをバックアップするため、フル バックアップと比較するとバックアップ サイズが小さくなることです。 検証バックアップのデメリットは、CA ARCserve D2D がソース ディスク のすべてのブロックを前回バックアップしたブロックと比較する必要があるため、バックアップに時間がかかることです。

利用可能なオプションは「繰り返し実行する」と「実行しない」です。 ［繰り返し実行する］オプションを選択した場合、バックアップの実行間隔（分単位、時間単位、または日単位）を指定する必要があります。検証バックアップの最小設定は 15 分ごとです。

デフォルトでは、検証バックアップのスケジュールは［実行しない］（スケジュールされている繰り返しはない）です。

5. ［保存］をクリックします。

バックアップ スケジュール設定が保存されます。

注: ある時点に同時に実行するようスケジュールされたバックアップの種類が複数ある場合、実行されるバックアップの種類は、以下の優先度に基づきます。

- 優先度 1 - フル バックアップ
- 優先度 2 - 検証バックアップ
- 優先度 3 - 増分バックアップ

たとえば、3 種類のバックアップすべてを同時に実行するようスケジュールされている場合、CA ARCserve D2D ではフル バックアップを実行します。フル バックアップがスケジュールされておらず、検証バックアップと増分バックアップが同時に実行するようスケジュールされている場合、CA ARCserve D2D は検証バックアップを実行します。 他の種類のバックアップとの競合がなければ、スケジュールされた増分バックアップのみが実行されます。

バックアップ拡張設定の指定

CA ARCserve Central Protection Manager では、バックアップの拡張設定を指定できます。

バックアップ拡張設定を指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。

2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開きます。

3. ［拡張］タブをクリックします。

   拡張設定オプションを表示するダイアログ ボックスが表示されます。

4. 拡張アクション設定オプションを指定します。

   - **ログの切り捨て** -- 次回の成功したバックアップ後に、選択したアプリケーションの累積トランザクション ログ ファイルを切り捨てるように指定します。

     CA ARCserve D2D バックアップは、スナップショット イメージと、そのイメージ用に作成されたトランザクション ログ ファイルで構成されます。 ある時点で古い（コミット済み）トランザクション ログ ファイルは必要ではなくなるため、新しいログ ファイルのスペースを作るためにパージできます。 これらのログ ファイルをパージするプロセスを、ログの切り捨てと呼びます。このオプションを選択すると、コミット済みのトランザクション ログ ファイルの切り捨てが有効になり、ディスク容量を節約できます。

     利用可能なオプションは、「SQL Server」および「Exchange Server」です。 これらのアプリケーションのどちらか、または両方を選択でき、どちらも選択しないことも可能です。 これらのアプリケーションのいずれかを選択した場合、自動的なログ切り捨てのスケジュール（［毎日］、［毎週］、［毎月］）を指定できます。

     注: バックアップが正常に完了しないと、トランザクション ログ ファイルの切り捨ては実行されません。

     - **毎日** -- 毎日のバックアップが正常に完了した直後に、コミット済みのトランザクション ログがパージされます。
     - **毎週** -- 7 日間のバックアップが正常に完了した直後に、コミット済みのトランザクション ログがパージされます。
     - **毎週** -- 30 日間のバックアップが正常に完了した直後に、コミット済みのトランザクション ログがパージされます。

     パージの実行がスケジュールされた時刻にバックアップ ジョブがすでに実行中である場合、パージ処理は次のスケジュール ジョブに移動します。

     たとえば、以下のようになります。

     増分バックアップが毎日午後 5 時に自動的に実行されるようにスケジュールされている場合に、午後 4 時 55 分にフル バックアップを手動で開始し、5 時 10 分に正常に完了したとします。

この場合、アドホックのフル バックアップが進行中なので、午後 5 時にスケジュールされていた増分バックアップは実行されません。 コミット済みのトランザクション ログは、次回、バックアップ ジョブが正常に完了した後でパージされます。この例では、翌日の午後 5 時にスケジュールされた増分バックアップが正常に完了した後で実行されます。

- デスティネーション上の予約容量

  この値は、バックアップを実行するのに必要な計算された容量の割合を示します。 この継続的な容量はバックアップがデータの書き込みを開始する前にデスティネーション上で直ちに予約され、バックアップ速度の改善に役立ちます。

  デフォルト： 10%。

  例： 値は 10% に設定され、現在のバックアップにはバックアップするデータが 50GB あります。バックアップがデータの書き込みを開始する前に、5 GB のディスク容量が予約されます。 5 GB のディスク容量が使い果たされると、さらに 5 GB のディスク容量が予約されます。 バックアップの残りデータが 5 GB 未満（あと 2 GB のバックアップが必要だと仮定します）である場合、残りの GB 数（この例では 2 GB）が予約されます。

- カタログ

  Exchange 詳細リストア カタログ

  このオプションが選択されている場合、各バックアップの後に Exchange 詳細リストア カタログの自動生成が有効になります。このオプションはデフォルトでは有効になっています。

  Exchange 詳細リストア バックアップでは、電子メール メッセージ、メール フォルダ、Exchange のメールボックス レベルに関する情報を、Exchange データベースを通じた 1 回のバックアップでキャプチャします。 このオプションを有効にすると、Exchange データベースの詳細復旧を実行できます。その場合は、Exchange データベースをまず別の場所に回復またはダンプしなくても、Exchange 内のオブジェクトのリストを選択し、回復する対象を厳密に指定することができます。

  メリット： Exchange 詳細リストア カタログを使用すると、リストアの参照を実行するのに長時間待機する必要がありません。

  デメリット： バックアップごとに Exchange 詳細リストア カタログを生成すると、バックアップ ウィンドウの拡大（バックアップ ジョブの完了までにかかる時間の増加）および作業負荷の増大につながります。CA ARCserve D2D では、それぞれのメールボックスを確認し、詳細情報を認証および構築する必要があります。メールボックスの数およびデータのサイズを考えると、これは非常に時間のかかる作業となります。

  注: このオプションを無効にすると、CA ARCserve D2D では Exchange の一般情報のみが保存されます。 リストアの前には、その時点で Exchange 詳細リストア カタログを生成することができます。

ファイル システム カタログ

このオプションを選択すると、ファイル システム カタログの生成が有効になります。 参照に長時間かかる場合（特に CA ARCserve D2D のデスティネーションが WAN 上にあるとき）、または検索によってリストアに長時間かかる場合、このオプションは待機時間の短縮に役立ちます。このオプションを選択すると、このカタログ ジョブはスケジュール済みの各バックアップ ジョブに対して実行されます。

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

注: 各バックアップ ジョブのファイル システム カタログを生成する場合、メタデータ ファイルとカタログ ファイルを格納するために必要なディスク ストレージの容量と、CPU 使用率が増加します。 さらに、バックアップ ソースに多数のファイルが含まれる場合、カタログを生成するプロセスに長時間かかることがあります。

- **管理者アカウント** -- バックアップを実行するためのアクセス権があるユーザ名およびパスワードを指定します。 CA ARCserve D2D によって、名前とパスワードが有効で、ユーザが管理者グループに属していることが確認されます。

  以下の点に注意してください。

  - ドメイン アカウントを指定する場合、ユーザ名の形式は、完全修飾ドメイン ユーザ名「<ドメイン名>¥<ユーザ名>」の形式で指定します。
  - CA ARCserve D2D サーバの管理者アカウントの情報を変更する場合（ユーザ名/パスワード）、このダイアログ ボックスでも管理者アカウント情報を再設定することをお勧めします。
  - 管理者アカウントの認証情報を指定しない場合、CA ARCserve D2D はポリシーの展開先のアカウント情報を自動的に入力します。

5. ［保存］をクリックします。

バックアップ拡張設定が保存されます。

バックアップの実行前/後の設定の指定

CA ARCserve Central Protection Manager では、バックアップの設定を指定できます。

バックアップ実行前/後の設定を指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。

2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開きます。

3. ［バックアップ実行前/後の設定］タブをクリックします。

   ［バックアップ実行前/後の設定］オプション ダイアログ ボックスが表示されます。

4. バックアップ設定オプションを指定します。

   - **アクション** -- バックアップの開始前、スナップショット イメージのキャプチャ後、またはバックアップの完了時、あるいはそれらを組み合わせたタイミングで、スクリプト コマンドを実行するよう指定します。 また、特定の終了コードに基づいてスクリプト コマンドをトリガしたり、その終了コードが返されたときに処理するアクション（ジョブを続行またはジョブを中止）を選択できます。

     - 「ジョブを続行」アクションでは、指定した終了コードが返された場合、CA ARCserve D2D がジョブを続行するように指定します。

     - 「ジョブを中止」アクションでは、指定した終了コードが返された場合、CA ARCserve D2D がジョブをキャンセルするように指定します。

5. ［保存］をクリックします。

バックアップ実行前/後の設定が保存されます。

ファイル コピー設定の管理

最初のファイル コピー ジョブを実行する前に、ファイル コピーの設定およびポリシーを指定する必要があります。 これらの設定により、ファイル コピー ジョブの動作が決まります。たとえば、ファイル コピー データのソース、ファイルのコピー先、各ファイル コピー ジョブのスケジュール、ファイル コピー ジョブに適用される設定とフィルタなどを指定します。 これらの設定は、［ポリシー］画面でいつでも変更できます。

ファイル コピー ソースの指定

CA ARCserve Central Protection Manager では、特定のデスティネーションにファイル コピーされるソース ファイルを指定することができます。

ファイル コピーのソースを指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。

2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開きます。

3. ［ファイル コピー設定］タブを選択します。

   ［ファイル コピー設定］の［ソース］ダイアログ ボックスが表示されます。

4. ［ファイル コピーの有効化］オプションを選択すると、ファイル コピー設定に対するすべての変更が検証およびコピーされます。 このオプションは、デフォルトで無効になっています。

5. ファイル コピーのソース設定を指定します。

ファイル コピー ソース

ファイル コピー ソースと、対応するポリシー（フィルタ）、CA ARCserve D2D バックアップが成功するたびに実行されるファイル コピーの種類（元のファイルを保持するかまたは移動するか）を手動で指定できます。 これらのファイル コピー ソースは、追加、削除、変更することができます。

注: CA ARCserve D2D では、アプリケーション ファイル、システム属性を含むファイル、一時属性を含むファイルはコピーされません。

- **ソースの追加**

  クリックすると、［ポリシーの種類］ダイアログ ボックスが表示され、実行されるファイル コピー ジョブの種類（元のファイルを保持するかまたは移動するか）を選択できます。 ポリシーの種類を選択すると、対応する［ファイル コピー ポリシー］ダイアログ ボックスが表示され、コピーするソースを追加して、そのソースの対応するポリシーを指定することができます。 詳細については、「ファイル コピー ポリシーの指定 (P. 123)」を参照してください。

  注: 現在のバックアップ ソースのみが、コピーの対象となります。 CA ARCserve D2D によってあらかじめバックアップされていないボリュームからソースを追加することはできません。

- **削除**

  クリックすると、選択したソースを表示されているリストから削除します。

- **修正**

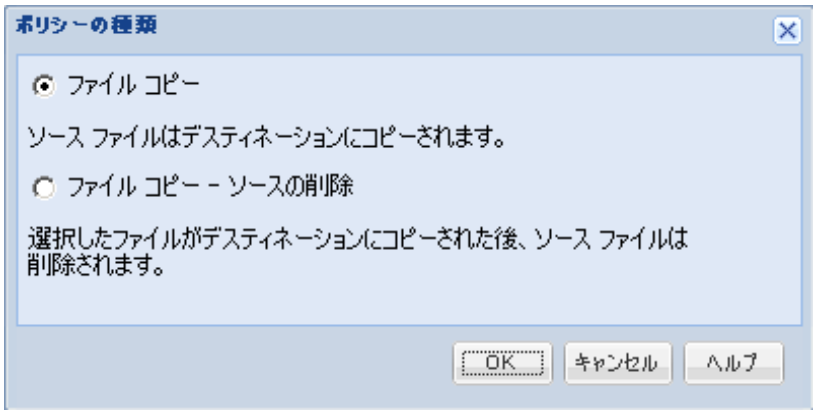
  クリックすると、［ファイル コピー ポリシー］ダイアログ ボックスが表示され、選択したソースのポリシー設定を変更することができます。 詳細については、「ファイル コピー ポリシーの指定 (P. 123)」を参照してください。

6. ［設定の保存］をクリックします。

ファイル コピーの設定が保存されます。

ファイル コピー ポリシーの指定

ファイル コピーに対してソースの追加オプションをクリックすると、［ポリシーの種類］ダイアログ ボックスが表示され、実行するファイル コピー ジョブの種類を選択することができます。



利用可能な種類は、［ファイル コピー］および［ファイル コピー - ソースの削除］です。

ファイル コピー

データがソースからデスティネーションにコピーされ（ソースのデータは削除されない）、複数のバージョンが保存された状態になります。

ファイル コピー - ソースの削除

データがソースからデスティネーションに移動され（ソース場所から削除される）、ソースの空き容量を増加させます。

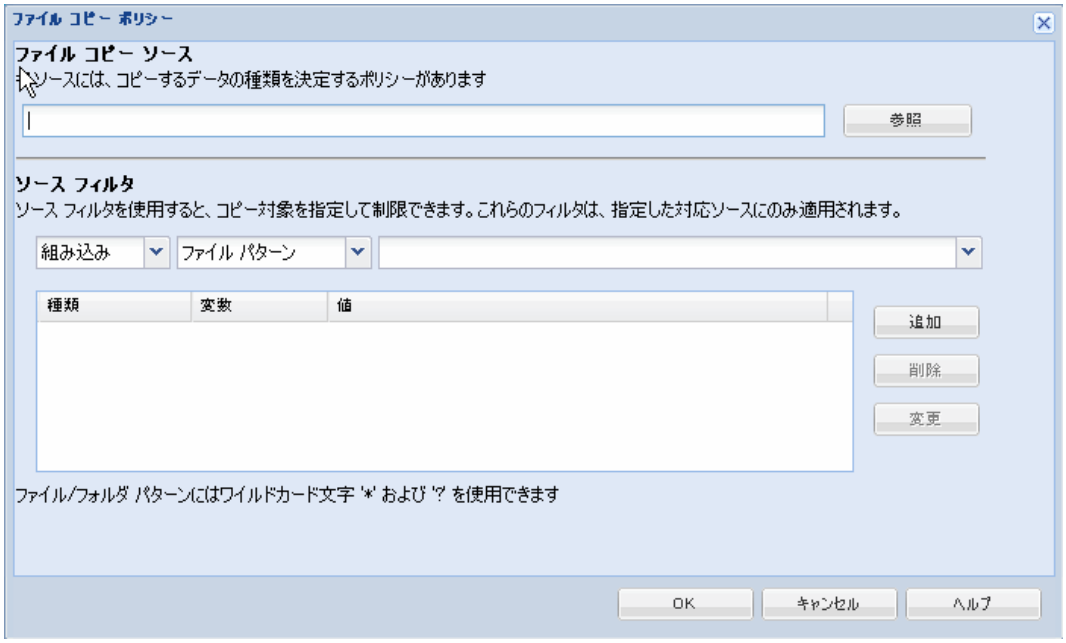
［ファイル コピー - ソースの削除］を選択すると、警告メッセージがすぐに表示され、指定されたファイル コピー データが元のソース場所からは削除され使用できなくなることが警告されます。［OK］をクリックすると、［ファイル コピー ポリシー］ダイアログ ボックスが続行されます。

重要: ［ファイル コピー - ソースの削除］オプションを使用したファイル コピーの場合、CA ARCserve D2D では "D2DARC" 拡張子の付いたスタブ ファイルを保持します。 スタブ ファイルには、デスティネーションおよびファイルが移動された時間に関する情報が含まれます。

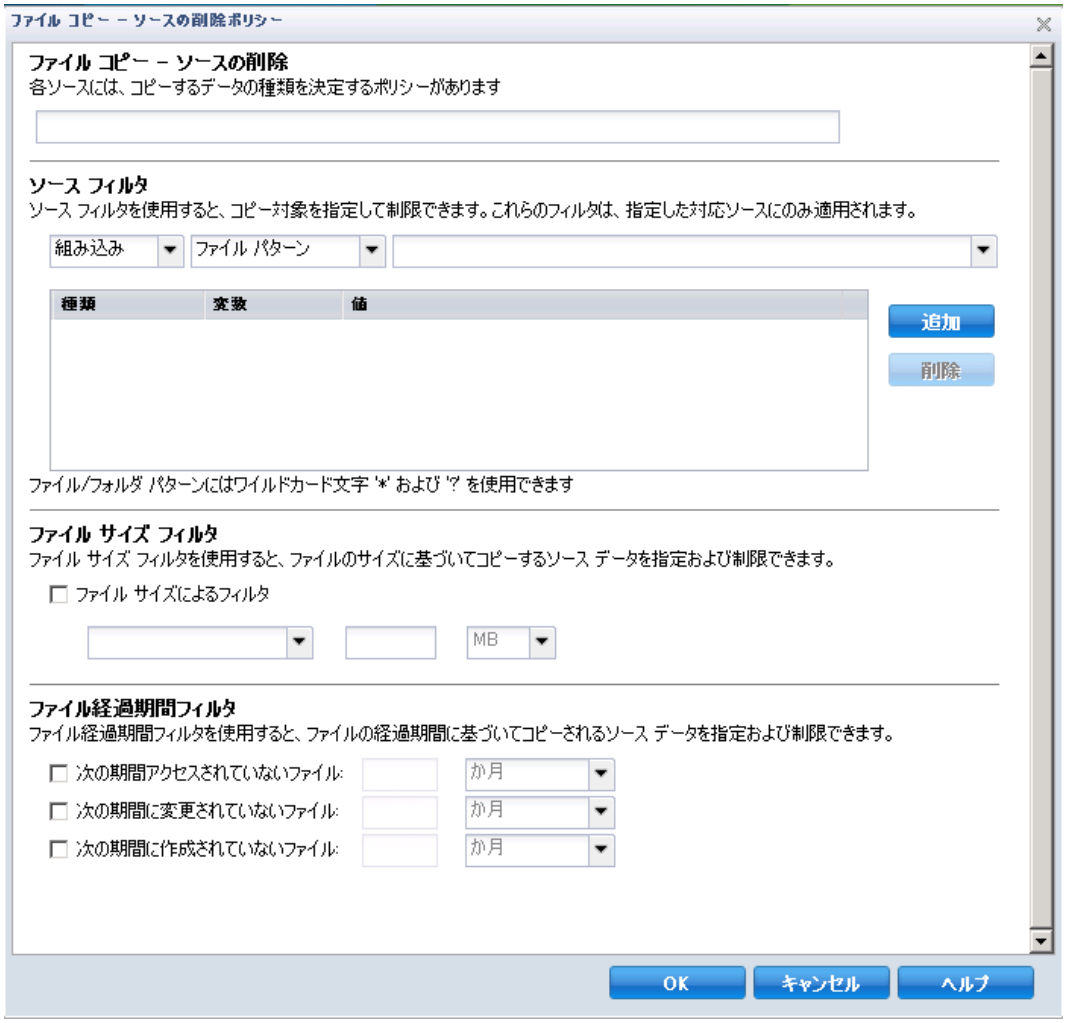
バックアップされたデータのソースを削除するためのポリシーの種類を指定する場合、関連するポリシーも併せて指定する必要があります。［ファイル コピー設定］ダイアログ ボックスで、新しくファイル コピー ソースを追加するか、既存のファイル コピー ソースを変更する場合、［ファイル コピー ポリシー］ダイアログ ボックスでポリシーを指定することができます。

選択したポリシーの種類に応じて、別の［ファイル コピー ポリシー］ダイアログ ボックスが表示されますが、選択する内容は似ています。

ファイル コピーが選択された場合



ファイル コピー - ソースの削除が選択された場合

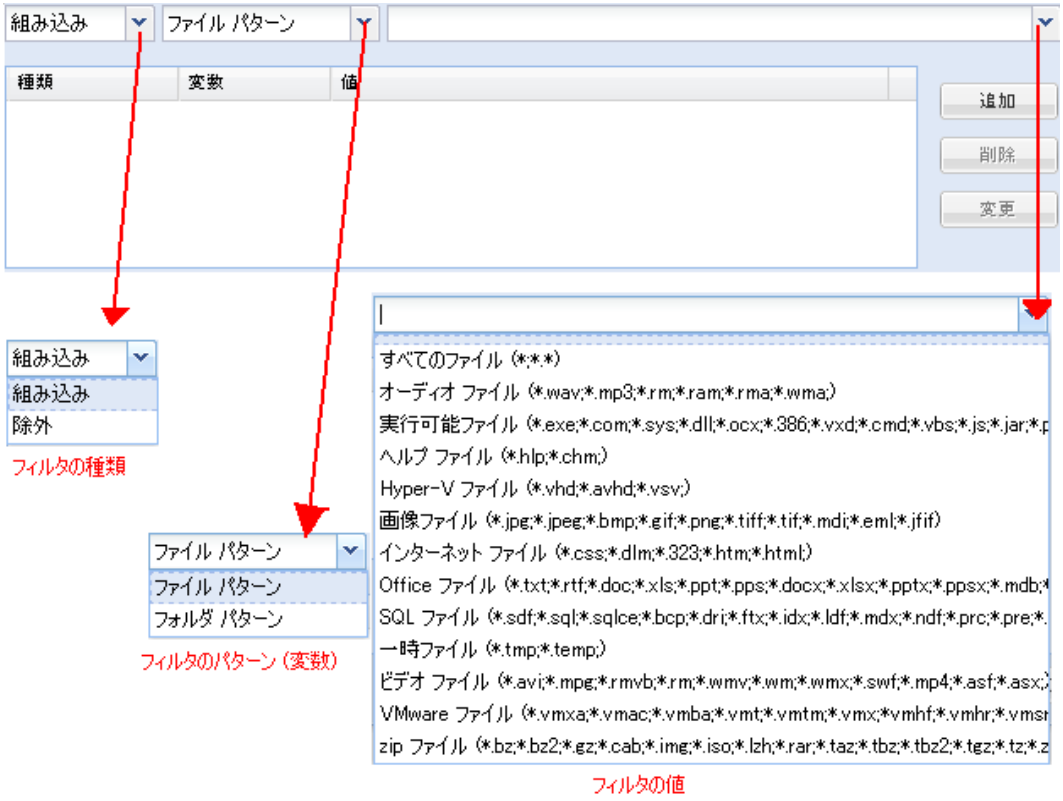


ファイル コピー - ソースの削除

ファイル コピー ソースを指定し、対応するポリシーおよび実行するファイル コピーの種類を設定します。ソース場所は参照して選択できます。

ソース フィルタ

フィルタを使用して、指定した種類および値によってファイル コピーが実行される対象のオブジェクトを制限できます。



フィルタの種類

フィルタには、「組み込み」と「除外」の 2 つの種類があります。

［組み込み］フィルタは、指定された値と一致するオブジェクトのみをファイル コピー ソースからファイル コピーします。

［除外］フィルタは、指定された値と一致するもの以外のすべてのオブジェクトをファイル コピー ソースからファイル コピーします。

同じファイル コピー リクエスト内に複数のフィルタを指定できます。その場合は、フィルタの値をカンマで区切ります。

- 複数の［組み込み］フィルタを指定した場合、それらのフィルタのいずれか 1 つに一致すれば、データがファイル コピーに含まれます。
- 複数の［除外］フィルタを指定した場合、それらのフィルタのいずれかの 1 つに一致すれば、データがファイル コピーから除外されます。
- 同じファイル コピー リクエストで［組み込み］および［除外］フィルタの両方を混在させることができます。

注: ［組み込み］および［除外］フィルタの指定されたパラメータが矛盾する場合は、常に［除外］フィルタが優先され適用されます。［除外］フィルタに一致するオブジェクトが［組み込み］フィルタによって含まれることはありません。

フィルタ変数（パターン）

変数パターン フィルタには、ファイル パターンとフォルダ パターンの 2 種類があります。

ファイル パターン フィルタまたはフォルダ パターン フィルタを使用して、特定のオブジェクトをファイル コピーに含めるかまたは除外することができます。

フィルタの値

フィルタの値を使用することにより、指定するパラメータ情報のみを選択してファイル コピーされる情報を制限することができます（.txt ファイルなど）。

CA ARCserve D2D では、ワイルドカード文字の使用がサポートされており、1 つのリクエストで複数のオブジェクトをファイル コピーの対象に選択することができます。 ワイルドカード文字は、1 任意の文字または文字列を表すための代用として使用できる特別な文字です。

［値］フィールドでは、ワイルドカード文字としてアスタリスク（*）と疑問符 (?) がサポートされています。完全なファイル/フォルダ パターン名が不明な場合は、ワイルドカード文字を指定することによって、フィルタの結果を簡略化することができます。

- "*" -- アスタリスクは、0 個以上の文字を表します。
- "?" -- 疑問符は、1 つの文字を表します。

たとえば、特定のファイル名がわからない場合に、.txt 拡張子を持つすべてのファイルを除外するには、「*.txt」を入力します。 わかっているファイル名をすべて指定してから、残りを埋めるためにワイルドカードを使用することもできます。

注: フィルタの種類として［ファイル パターン］を選択した場合、あらかじめ定義されたフィルタのドロップダウン リストが提供され、多くの一般的に使用されているファイルを選択することができます（MS Office ファイル、イメージ ファイル、実行ファイル、一時ファイルなど）。

ファイル サイズ フィルタ（ファイル コピー - ソースの削除ジョブのみ）

このフィルタは、ファイル コピー - ソースの削除ジョブにのみ適用されます（ファイル コピー ジョブには適用されません）。

ファイル サイズ フィルタを使用すると、ファイルのサイズに基づいて、ファイル コピーのソース オブジェクトを制限することができます。 ファイル サイズ フィルタを有効にした場合、指定したパラメータに基づいて、オブジェクトがファイル コピーに含まれるかどうかが判断されます。 範囲（等しい、次より大きい、次より小さい、範囲内）を選択し、サイズの値を入力します。

たとえば、10 MB と等しいかそれより大きいことを指定した場合、CA ARCserve D2D は、この基準を満たすオブジェクトのみをファイル コピーします。このファイル サイズ基準を満たさない他のすべてのオブジェクトはファイル コピーされません。

ファイル経過期間フィルタ（ファイル コピー - ソースの削除ジョブのみ）

このフィルタは、ファイル コピー - ソースの削除ジョブにのみ適用されます（ファイル コピー ジョブには適用されません）。

ファイル経過期間フィルタを使用すると、ファイルの特定の日数に基づいて、ファイル コピーに含まれるソース オブジェクトが自動的に決まります。パラメータ（[次の期間にアクセスされていないファイル]、[次の期間に変更されていないファイル]、[次の期間に作成されていないファイル]）を選択し、ファイル経過期間フィルタの日数、月数、または年数を入力します。自動ファイル コピー用に複数のファイル経過期間フィルタを選択できます。

たとえば、[次の期間に変更されていないファイル]を選択して 180 日を指定した場合、CA ARCserve D2D はこの基準を満たすすべてのファイル（過去 180 日以内に変更されていない）をすべて自動的にファイル コピーします。

重要: ファイル サイズ フィルタとファイル経過期間フィルタの両方（または複数のファイル経過期間フィルタ）を指定した場合、指定されたフィルタ パラメータをすべて満たすファイルのみがファイル コピーされます。指定されたパラメータのうち 1 つでも適合しないファイルはファイル コピーされません。

ファイル コピー デスティネーションの指定

CA ARCserve Central Protection Manager では、ファイル コピーされる情報に対してデスティネーション設定を指定できます。

ファイル コピー デスティネーションを指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。

2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開きます。

3. ［ファイル コピー設定］タブを選択し、［デスティネーション］を選択すると、［ファイル コピー設定］の［デスティネーション］ダイアログ ボックスが開きます。

4. デスティネーション設定を指定します。

   - **デスティネーション** -- ファイル コピー ジョブのデスティネーション場所を指定します。 選択できるデスティネーションは 1 つだけです。

     CA ARCserve D2D では、バックアップされたファイルのファイル コピー設定としてディスクまたはクラウドへのコピーを指定できます。 ファイル コピーの種類として、バックアップされたデータをコピーして元のデータを保持するのか、コピーして元のデータを移動するのかを指定できます。 2 つのプロセスは似ていますが、コピー＆移動の場合、データがソースからデスティネーションに移動される（ソースからは削除される）点が異なります。この方法の場合、ソース場所の空き容量を増やすことができます。コピー＆保持を実行すると、データはソースからデスティネーションにコピーされ（ソースには残る）、複数のバージョンが保存された状態になります。

     - **ローカルまたはネットワーク ドライブへのファイル コピー** -- このオプションを選択した場合は、ソース ファイル/フォルダを移動またはコピーする先の場所をフル パスで指定します。この場所は参照して選択できます。緑の矢印アイコンをクリックすると、指定したデスティネーションへの接続を確認することができます。

     - **クラウドへのファイル コピー** -- このオプションを選択した場合は、ソース ファイル/フォルダを移動またはコピーする先のクラウドを指定します。 CA ARCserve D2D では、現在複数のクラウド ベンダへのファイルのコピーがサポートされています。たとえば、Amazon S3（Simple Storage Service）、Windows Azure、Fujitsu Cloud （Windows Azure）、Eucalyptus-Walrus などがあります。これらのクラウド ベンダは、一般に公開されている Web サービスで、任意の量のデータをいつでも、Web 上のどこからでも安全かつ確実に保存および取得することができます。

       ［設定］ボタンをクリックすると、［クラウド環境設定］ダイアログ ボックスが表示されます。 詳細については、「ファイル コピー用のクラウド環境設定詳細の指定 (P. 133)」を参照してください。

注: クラウドへの接続試行においてクロック スキュー エラーの可能性を排除するには、マシンに正しいタイム ゾーンが設定されており、クロックがグローバル時間と同期されていることを確認します。 お使いのマシンの時間は常に GMT 時間と照合しておく必要があります。 マシンの時間が正しいグローバルクロック時間と同期（5 分から 10 分以内）されていない場合、Amazon S3 は機能しません。 必要に応じて、マシンの時間をリセットし、アーカイブ ジョブを再実行します。

いずれのデスティネーション オプションでも、指定されたデスティネーションへの接続が失われたか切断された場合、CA ARCserve D2D はファイル コピー ジョブの続行を何度か試行します。 これらの再試行が成功しなければ、問題が発生したポイントからメークアップ ジョブが実行されます。 また、アクティビティ ログが対応するエラー メッセージで更新され、電子メール通知が送信されます（設定されている場合）。

- **圧縮** -- ファイル コピー ジョブに使用される圧縮の種類を指定します。

  圧縮は、通常ストレージ容量を減らすために実行されますが、CPU 使用率が増加するため、ファイル コピー速度が低下するという影響があります。

  使用可能なオプションは、以下のとおりです。

  - **圧縮なし** -- 圧縮は実行されません。このオプションを使用すると、CPU 使用率は最も低くなります（最も高速で動作）。ただし、ファイル コピーに必要なストレージ空き容量は最も大きくなります。
  - **標準圧縮** -- 標準圧縮が実行されます。このオプションを使用すると、CPU 使用率と必要なストレージ容量のバランスを適度に調節します。 これはデフォルトの設定です。
  - **最大圧縮** -- 最大圧縮が実行されます。このオプションを使用すると、CPU 使用率が最も高くなります（最も低速で動作）。ただし、ファイル コピーに必要なストレージ空き容量は最も小さくなります。

- **暗号化** -- ファイル コピーの暗号化パスワードを有効にします。

- **保存期間** -- この設定は、元のデータを移動する（ソースには保持されない）ファイル コピーが実行されたデータにのみ適用されます。

  保存されるデータがデスティネーション場所で保持される期間（年数、月数、週数、日数）を指定します。 指定された保存期間が経過すると、保存されているデータはデスティネーションからパージされます。

  保持期間は、1 か月が 30 日あり、1 年間が 365 日あるという前提で計算されます。 例： 保存期間を 2 年 2 か月と 5 日間として指定した場合、ファイル コピー データの保持期間の合計は、795 日（365 + 365 + 30 + 30 + 5）になります。

  重要: この保存期間の設定は、ソースからデスティネーションにコピーおよび移動されたデータ（元のデータは保持されない）にのみ適用されます。指定された保存期間が経過し、データがデスティネーションからパージされたら、この移動されたデータは一切保存されなくなることに注意してください。

- **ファイル バージョン** -- この設定は、コピーおよび保持されたデータ（元のデータは移動されない）にのみ適用されます。

  デスティネーション（クラウドまたはディスク）に保持されるコピーの数を指定します。 この数を超過したら、最も初期の（最も古い）バージョンが破棄されます。この破棄の手順は、新しいバージョンがデスティネーションに追加されるたびに繰り返され、保存されるバージョン数を指定された数に常に保つことができます。

  たとえば、ファイル バージョンの保存数に 5 を指定し、ファイル コピーを 5 回（t1、t2、t3、t4、t5）実行した場合、これらの 5 つのファイル コピー バージョンが保持され回復に使用できるようになります。 6 番目のファイル コピーが実行されたら（新バージョンが保存される）、CA ARCserve D2D は t1 コピーを削除します。回復可能な 5 つのバージョンは、t2、t3、t4、t5、および t6 になります。

  デフォルトでは、デスティネーションで破棄されずに保持できるコピーの数は 15 です。

5. ［設定の保存］をクリックします。

ファイル コピーのデスティネーション設定が保存されます。

ファイル コピー用のクラウド環境設定詳細の指定

このダイアログ ボックスのドロップダウン メニューを使用して、ファイル コピーのストレージに利用するクラウド ベンダ タイプを選択できます。利用可能なオプションは、［Amazon S3］、［Windows Azure］、［富士通クラウド（Windows Azure）］および［Eucalyptus-Walrus］です。（Amazon S3 がデフォルト ベンダです）。富士通クラウド（Windows Azure）の詳細については、概要および登録を参照してください。

注: ファイル コピー クラウド ベンダとして Eucalyptus-Walrus を使用している場合、そのパス全体の長さが 170 文字を超えるファイルをコピーすることができません。

各クラウド ベンダの環境設定オプションは類似していますが、使用されている用語が若干異なっており、その相違点についても説明します。

1. 接続設定の指定

   ベンダ URL

   クラウド プロバイダの URL アドレスを指定します。

   （［Amazon S3］、［Windows Azure］および［富士通クラウド（Windows Azure）］の場合、［ベンダ URL］はあらかじめ自動的に入力されています。Eucalyptus-Walrus の場合は、指定された形式で［ベンダ URL］を手動で入力する必要があります）。

   アクセス キー ID/アカウント名/照会 ID

   この場所へのアクセスを要求しているユーザを指定します。

   （このフィールドについては、Amazon S3 では、アクセス キー ID を使用します。Windows Azure と富士通クラウド（Windows Azure）ではアカウント名を使用します。また、Eucalyptus-Walrus では照会 ID を使用します）。

シークレット アクセス キー/シークレット キー

アクセス キーは暗号化されないため、このシークレット アクセス キーは、この場所にアクセスするためのリクエストの信頼性を確認するのに使用されるパスワードになります。

重要: このシークレット アクセス キーは、ユーザのアカウントのセキュリティを管理するのに重要です。 このキーおよびアカウント認証情報は安全な場所に保管しておく必要があります。 シークレット アクセス キーを Web ページや他の一般にアクセス可能なソース コード内に埋め込んだり、安全が確保されていないチャネルを介して転送しないようにしてください。

（このフィールドについては、Amazon S3 はシークレット アクセス キーを使用します。 Windows Azure、富士通クラウド（Windows Azure）および Eucalyptus-Walrus は、シークレット キーを使用します）。

プロキシの有効化

このオプションを選択すると、プロキシ サーバの IP アドレス（またはマシン名）およびプロキシ サーバがインターネット接続する際に使用される、対応するポート番号も指定する必要があります。このオプションを選択して、プロキシ サーバでの認証が必要なように設定することもできます。 該当する場合は、プロキシ サーバを使用するのに必要とされる対応する認証情報（ユーザ名とパスワード）を指定する必要があります。

（プロキシ機能は Eucalyptus-Walrus では利用できません）。

2. 拡張設定の指定

バケット名/コンテナ名

クラウド ベンダに移動またはコピーされたファイル/フォルダはすべて、ユーザのバケット（またはコンテナ）内に保存および整理されます。 バケットは、ファイルのコンテナのようなもので、オブジェクトをグループ化して整理するために使用されます。クラウド ベンダで保存されたすべてのオブジェクトは、バケット内に格納されます

（このフィールドは、Amazon S3 および Eucalyptus-Walrus では、［Bucket Name］を使用します。 Windows Azure および Fujitsu Cloud（Windows Azure）では［Container］を使用します）。

注: この手順では、特に指定のない限り、「バケット」として言及されるものはすべて「コンテナ」にも当てはまります。

新しいバケット名を指定する方法

a. 新しいバケット名を指定します。

注: CA ARCserve Central Protection Manager はバケット名を作成しませんが、CA ARCserve Central Protection Manager ポリシーが正常に割り当てられると、各 CA ARCserve D2D ノードに生成されます。各 CA ARCserve D2D ノードのバケット名には、「d2dfilecopy-<hostname>-<user given name>」というプレフィックスが自動的に付けられます。

バケット名は一意で、容易に識別可能かつインターネット ドメインの命名規則に準拠しています。 複数のバケットが同じ名前を持つことができません。 バケット名の有効な構文を理解しておくことは重要です。

Amazon S3 および Eucalyptus-Walrus の場合、バケット命名要件の詳細については、Amazon S3 のドキュメントを参照してください。

Windows Azure および Fujitsu Cloud （Windows Azure）の場合、コンテナ命名要件の詳細については、Microsoft のドキュメントを参照してください。

b. Amazon S3 の場合のみ、ドロップダウン メニューから利用可能な地域を選択します。 デフォルトでは、選択可能な地域がすべてドロップダウン メニューに含まれ、新規バケットが作成される地域を選択することができます。

地域を指定することにより、作成したバケットが Amazon S3 で保存される地理的な場所を選択できます。地域を選択する際は、データへの最速アクセス、遅延の最小化、コストの削減、または規制要件への対応を考慮して地域を選択します。

（Windows Azure、Fujitsu Cloud （Windows Azure）および Eucalyptus-Walrus の場合、地域は選択できません）

c. 値を指定したら［OK］をクリックします。 バケット名が検証されクラウドに作成されます。

d. バケットが作成されたら、［クラウド環境設定］ダイアログ ボックスが再度表示され、［拡張設定］フィールドに新しいバケット情報（名前と地域）が示されます。

低冗長化ストレージを有効にする

Amazon S3 でのみ、このオプションを使用して、低冗長化ストレージ（RRS）を有効にすることができます。 RRS は、Amazon S3 のストレージ オプションで、クリティカルでない再生可能なデータを Amazon S3 の標準ストレージより低いレベルの冗長性で保存することによりコストを削減することができます。 標準ストレージも RRS オプションも、複数の設備および複数のデバイスにデータを保存しますが、RRS ではデータのレプリケート回数が少なくなるため、コストが低く抑えられます。Amazon S3 の標準ストレージまたは RRS のいずれを使用しても、同じ遅延およびスループットが期待できます。 デフォルトでは、このオプションは選択されていません（Amazon S3 は標準ストレージ オプションを使用します）。

3. ［接続テスト］をクリックして、指定されたクラウド場所への接続を確認します。

4. ［OK］をクリックし、［クラウド環境設定］ダイアログ ボックスを終了します。

ファイル コピー スケジュールの指定

CA ARCserve Central Protection Manager では、ファイル コピーされる情報に対してスケジュール設定を指定できます。

ファイル コピー スケジュールを指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

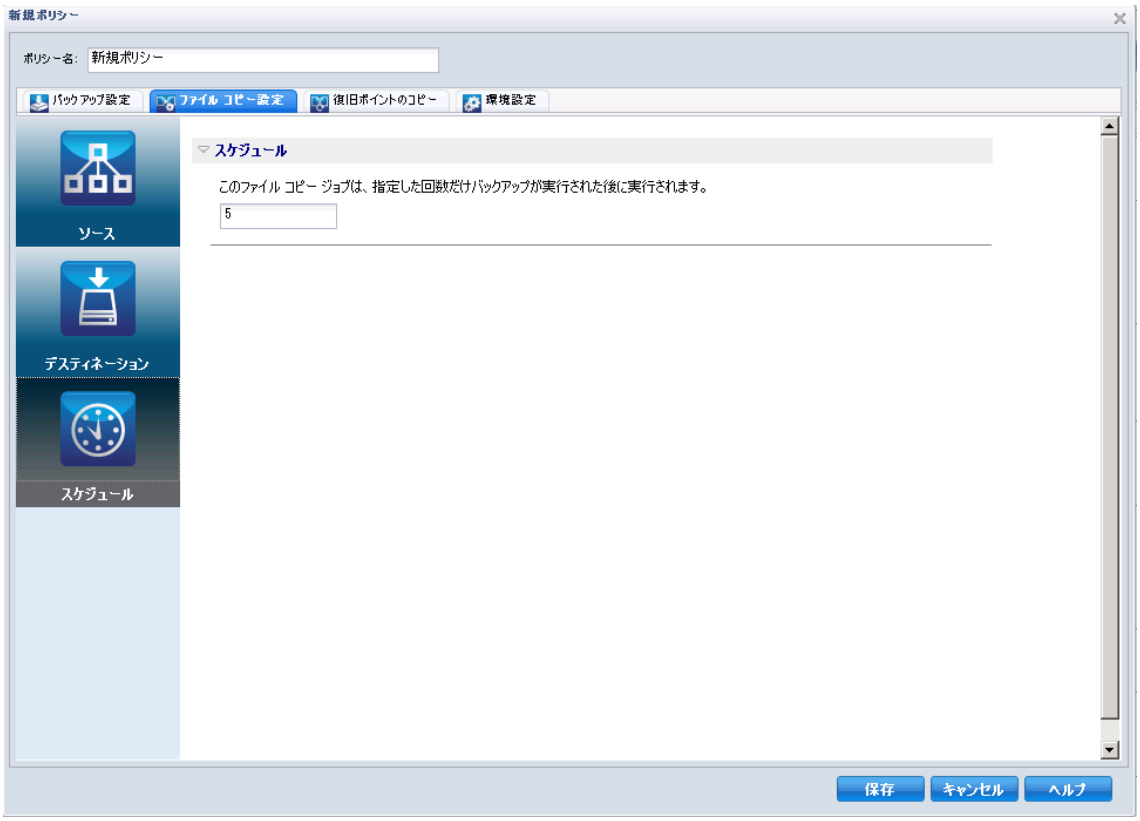
   ［ポリシー］画面が開きます。

2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開きます。

3. ［ファイル コピー設定］タブを選択し、次に［スケジュール］を選択します。

   ［ファイル コピー設定］の［スケジュール］ダイアログ ボックスが表示されます。



4. ファイル コピーのスケジュール設定を指定します。

   - **スケジュール** — 指定された数のバックアップが実行された後にデータのファイル コピーを有効にします。

     指定された数のバックアップが正常に実行されたら、選択したファイル コピー ポリシーに基づいて、ファイル コピー プロセスが自動的に開始されます。

     この設定を使用して、ファイル コピー ジョブが 1 日にトリガされる回数を制御することができます。 たとえば、バックアップ ジョブが 15 分おきに実行されるよう指定し、バックアップが 4 回実行されるたびにファイル コピー ジョブが 1 回実行されるよう指定した場合、1 日に実行されるファイル コピー ジョブの回数は 24 になります（1 時間に 1 回）。

デフォルトでは、バックアップが 5 回正常に完了するたびにファイル コピーが実行されるようスケジュールされます （指定できるバックアップの最大数は 700 です）。

5. ［設定の保存］をクリックします。

ファイル コピーのスケジュール設定が保存されます。

復旧ポイントのコピー設定の指定

CA ARCserve D2D では、コピー（および必要に応じてエクスポート）する復旧ポイントに対して、スケジュール設定を指定することができます。このダイアログ ボックス上のオプションを使用して復旧ポイントのコピー スケジュールを設定する方法については、「復旧ポイントのコピー - シナリオ例」を参照してください。

注: 復旧ポイントのコピー プロセスは、コピー＆貼り付けの操作のみで、切り取り＆貼り付け操作はありません。 そのため、スケジュールされた復旧ポイントのコピー ジョブが実行された場合は常に、CA ARCserve D2D では、指定されたコピー先に復旧ポイントの追加のコピーを作成しますが、バックアップ設定で指定されたバックアップ先には元のコピーを保持します。

復旧ポイントのコピー設定を指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。

2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開きます。

3. ［復旧ポイントのコピー］タブを選択します。

   ［復旧ポイントのコピー］ダイアログ ボックスが表示されます。

4. 復旧ポイントのコピー スケジュール設定を指定します。

   復旧ポイントのコピーを有効にする

   指定された回数のバックアップが実行された後、スケジュールされた復旧ポイントのコピーを有効にします。 このオプションが選択されていない場合、スケジュールされた復旧ポイントのコピーは実行されません。

デスティネーション

復旧ポイントのコピーの場所（デスティネーション）を指定するか、またはコピー場所を参照します。 緑色の矢印アイコン ボタンをクリックすると、指定した場所への接続を検証できます。

指定された数のバックアップが実行された後、復旧ポイントのコピー ジョブが実行されます。

スケジュールされた復旧ポイントのコピー プロセスが自動的に起動されるタイミングを指定します。

指定された数のバックアップが正常に実行されたら、選択したコピー ファイル ポリシーに基づいて、復旧ポイントのコピー プロセスが自動的に開始されます。

この設定を使用して、復旧ポイントのコピープロセスが 1 日にトリガされる回数を制御することができます。たとえば、バックアップ ジョブが 15 分おきに実行されるよう指定し、バックアップが 4 回実行されるたびに復旧ポイントのコピーが 1 回実行されるよう指定した場合、1 日に実行される復旧ポイントのコピー ジョブの回数は 24 になります（1 時間に 1 回）。

デフォルトでは、バックアップが 8 回正常に完了するたびに復旧ポイントのコピーが実行されるようスケジュールされます

重要: バックアップおよびコピー ジョブが定期的に実行されるようスケジュールされていて、バックアップ ジョブの実行がスケジュールされている時間がきてもコピー ジョブが実行中（アクティブな状態）である場合、バックアップ ジョブは失敗します（次回のバックアップ ジョブはスケジュールどおりに実行され、別のコピー ジョブと競合しなければ正常に完了します）。 コピー操作にはフル バックアップの実行とほぼ同じ時間がかかるため、復旧ポイント コピー ジョブのスケジュールはそれほど頻繁に設定しないことをお勧めします。

保存する復旧ポイントのコピー数を指定します。

指定したコピー先に保持される復旧ポイントの数を指定します。この数を超過したら、最も初期の（最も古い）復旧ポイントが破棄されます。 この破棄の手順は、新しい復旧ポイントがデスティネーションに追加されるたびに繰り返され、保存される復旧ポイントの数を指定された数に常に保つことができます。

注: デスティネーションの空き容量が不足している場合、保存する復旧ポイントの数を減らすことを検討してください。

デフォルトでは、復旧ポイント保存数は 31 個に設定されます。

注: 復旧ポイントの最大数は 1344 です。

圧縮

復旧ポイントのコピーに使用される圧縮の種類を指定します。

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

使用可能なオプションは、以下のとおりです。

- 圧縮なし - 圧縮は実行されません。ファイルは純粋な VHD です。このオプションを使用すると、CPU 使用率は最も低くなります（最も高速で動作します）。ただし、バックアップ イメージのディスク容量の使用率は最大になります。
- 圧縮なし - **VHD** - 圧縮は実行されません。 ファイルは .vhd 形式に直接変換されます。手動操作は必要ありません。 このオプションを使用すると、CPU 使用率は最も低くなります（最も高速で動作します）。ただし、バックアップ イメージのディスク容量の使用率は最大になります。
- 標準圧縮 - 標準圧縮が実行されます。 このオプションを使用すると、CPU 使用率とディスク容量使用率のバランスを適度に調節します。 これはデフォルトの設定です。
- 最大圧縮 - 最大圧縮が実行されます。 このオプションを使用すると、CPU 使用率が最も高くなります（最も低速で動作します）。ただし、ディスク容量の使用率は、最小になります。

注: バックアップ イメージに圧縮可能でないデータ（JPG イメージ、ZIP ファイルなど）が含まれている場合、それらのデータを処理するために、追加のストレージ スペースを割り当てることができます。 そのため、圧縮オプションを選択していて、バックアップに圧縮可能でないデータがある場合、実際にはディスク容量の使用率が増大する場合があります。

暗号化アルゴリズム

復旧ポイントのコピーに使用される暗号化アルゴリズムの種類を指定します。

データの暗号化とは、解読メカニズムがなければ理解できない形式にデータを変換することです。 CA ARCserve D2D のデータ保護では、安全な AES （Encryption Standard を進めた）暗号化アルゴリズムを使用し、指定したデータに対して最大限のセキュリティおよびプライバシーを確保します。

利用可能なオプションは、暗号化なし、AES-128、AES-192、および AES-256 です（暗号化を無効にするには、［暗号化なし］を選択します）。

暗号化パスワード

コピーする復旧ポイントが暗号化されていれば、パスワードを提供（および確認）する必要があります。

- 復旧ポイントが同じマシン上の場所にコピーされている場合は、暗号化パスワードが記憶されているため、このフィールドには自動的に入力されます。
- 復旧ポイントが別のマシンにコピーされている場合は、暗号化パスワードを入力する必要があります。

5. ［設定の保存］をクリックします。

復旧ポイントのコピー設定が保存されます。

環境設定の管理

CA ARCserve Central Protection Manager では、ポリシーの一般的な要件を管理することができます。 ニュース フィードの生成、電子メール アラート通知の作成、またはサーバや接続の更新を実行できます。

このセクションには、以下のトピックが含まれます。

一般的な環境設定の指定

CA ARCserve Central Protection Manager では、ポリシーの一般的な環境設定を指定することができます。

一般的な環境設定を指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

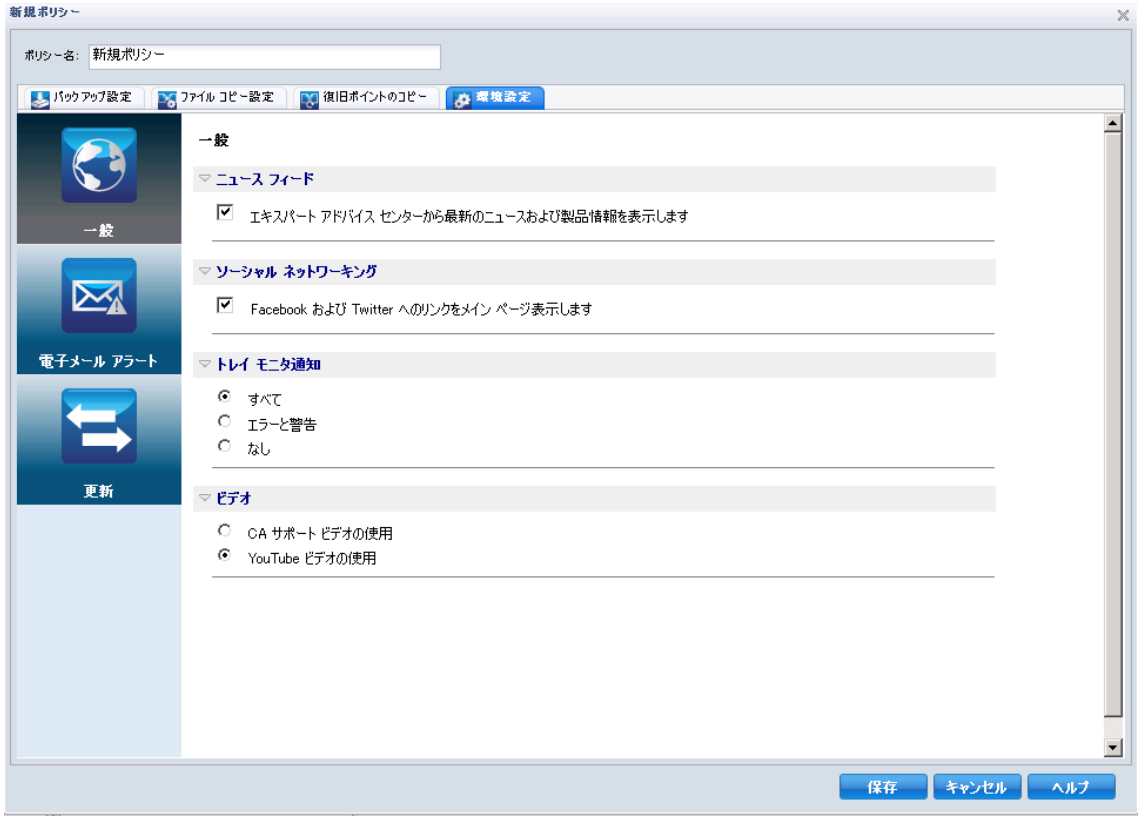
   ［ポリシー］画面が開きます。

2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開きます。

3. ［環境設定］タブを選択します。

   ［環境設定］の［一般］ダイアログ ボックスが開きます。



4. 使用する環境設定を指定します。
   - **ニュース フィード** -- このオプションを有効にすると、エキスパート アドバイス センターからの最新ニュースおよび製品情報が表示されます。
   - **ソーシャル ネットワーキング** -- このオプションを有効にすると、メイン ページから Facebook および Twitter へのリンクが表示されます。
   - **トレイ通知** — 以下のいずれかを選択できます。
     - ［すべて］ - すべての通知をシステム トレイに表示します。
     - ［エラーと警告］ - エラーと警告のみをシステム トレイに表示します。
     - ［なし］ - 通知を一切表示しません。
   - **ビデオ** -- D2D ポリシーで使用するビデオの種類を 1 つ選択します。
     - CA サポート ビデオの使用
     - YouTube ビデオの使用（デフォルト）
5. ［保存］ボタンをクリックします。

一般的な環境設定が保存されます。

電子メール アラートの指定

CA ARCserve Central Protection Manager では、電子メール アラートの環境設定を指定できます。

電子メール アラートを指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。
2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開きます。

3. ［環境設定］タブを選択し、次に［電子メール アラート］を選択します。

   ［環境設定］の［電子メール アラート］ダイアログ ボックスが表示されます。

4. 電子メール アラートを指定します。

   - **電子メール アラートの有効化** — このオプションを選択すると、この画面上で環境設定が有効になります。
   - **電子メールの設定** -- このボタンをクリックすると、［電子メールの設定 (P. 151)］ダイアログ ボックスが表示されます。
   - **通知** — 選択したイベントが完了したときに、自動的に電子メール アラート通知を送信するよう指定します。 以下のオプションのいずれかまたはすべてを選択できます。

     以下のイベント通知を送信するオプションが利用可能です。

     バックアップ ジョブ アラート

     - **ジョブが失敗した場合** -- 失敗したすべてのジョブに対して電子メール アラート通知を送信します。 失敗したジョブとは、スケジュールが設定されているが、スケジュール時刻に実行されなかったジョブのことです。 これは、他のジョブが実行中の場合、または先に開始したジョブがまだ完了していない場合に発生します。 たとえば、バックアップ ジョブのスケジュール時刻にエクスポートまたは復旧ジョブが実行中の場合、バックアップ ジョブは失敗します。
     - **バックアップ、カタログ、ファイル コピー、リストア、または復旧ポイント コピー ジョブが失敗またはクラッシュした場合** -- バックアップ、カタログ、ファイル コピー、リストア、または復旧ポイント コピー ジョブの試行が失敗した場合に電子メール アラート通知を送信します。このカテゴリには、失敗、未完了、キャンセル、スケジュール ジョブの未実行、およびクラッシュのすべてが含まれます。
     - **バックアップ、カタログ、ファイル コピー、リストア、または復旧ポイント コピー ジョブが成功した場合** -- バックアップ、カタログ、ファイル コピー、リストア、または復旧ポイント コピー ジョブの試行が成功した場合に電子メール アラート通知を送信します。

- **マージ ジョブが停止、スキップ、失敗、またはクラッシュした場合** -- 停止、スキップ、失敗、またはクラッシュしたすべてのマージ ジョブについて、アラート通知を送信します。 このアラートを有効にすると、マージ ジョブが失敗した際に通知が送られます。マージは、セッションがマウントされていたり、セッションがカタログ ジョブによってロックされていたり、セッションがその他の理由によりロックされていると、失敗する場合があります。
- **マージ ジョブが成功した場合** -- 成功したすべてのマージ ジョブについて電子メール アラートを送信します。

ディスク容量アラート

- **バックアップ先の空き容量が次の値を下回った場合** - バックアップ先の空き容量が指定した値を下回った場合に電子メール アラート通知を送信します。 このオプションでは、アラート通知を送信するしきい値として、全容量の割合または特定の値（単位 - MB）のどちらで指定するかを選択することができます。

更新アラート

- **新しい更新がある場合** - CA ARCserve D2D 用の新しい更新が利用可能な場合に電子メール通知を送信します。 また、更新の確認中またはダウンロード中に問題が発生した場合も、電子メール通知が送信されます。

リソース アラート

- **リソース アラートを有効にする** -- 指定されたパフォーマンス キー インジケータ（PKI）のしきい値レベルに到達した場合に電子メール通知を送信します。サーバの効率性と信頼性を保証するには、常にパフォーマンスをモニタして潜在的な問題を特定し、ボトルネックとなる状況を迅速に解消する必要があります。

  これらのパフォーマンス インジケータのしきい値レベルを定義することは、サーバに関するユーザの知識に基づいて、完全にユーザの裁量において行われます。正しい設定や誤った設定というのもはありません。アラート通知は「正常」で許容可能なパフォーマンスに基づいて送られる必要があります。たとえば、システムが通常は 80% の CPU 負荷で実行される場合、CPU 使用率のしきい値に 75% を設定することは効率的かつ有用とは言えません。

  これらの各 PKI パラメータは、対応するしきい値レベルに達するとそれぞれ個別にアラート通知を送信するように設定できます。 送信される PKI アラート電子メールの最大数は 1 日あたり 5 件までです。

- **CPU 使用率** -- 指定される CPU 使用率アラートしきい値は、CA ARCserve D2D によって保護されたサーバの CPU 使用率を示します。 このアラート通知を使用して、サーバが頻繁に過負荷状態になり過ぎることがないか確認できます。

  CPU 使用率が高すぎると、サーバの応答時間が非常に遅くなるか、反応しなくなる場合があります。この場合、負荷の分散（バランシング）を検討する必要があります。

- **ディスク スループット** -- 指定されるディスク スループット アラートしきい値は、CA ARCserve D2D によって保護されたサーバのディスク スループット（MB/秒）を示します。 このアラート通知を使用して、お使いのディスクの機能が最大化されていることを確認できます。

  ディスク スループットがディスクの最大処理能力に近い場合、ニーズと一致させるためにディスクのアップグレードを検討する必要があります。 通常、高速なディスクほどパフォーマンスは高くなります。

- **メモリ使用率** -- 指定されるメモリ使用率アラートしきい値は、CA ARCserve D2D によって保護されたサーバのメモリ使用率を示します。使用率は、メモリ容量のどれくらいが使用されているかを表します。使用率が高くなるほど、サーバのパフォーマンスは低くなります。

  メモリ使用率が頻繁に高くなりすぎる場合、原因となっているプロセスを特定する必要があります。このインジケータ設定を使用して、アプリケーションまたはサーバのアップグレードが必要となった場合に警告されるようにすることができます。

- **ネットワーク I/O** -- 指定されるネットワーク I/O アラートしきい値は、CA ARCserve D2D によって保護されたサーバで現在使用されている NIC 帯域幅率を示します。使用率は、ネットワーク インターフェース カード（NIC）がどの程度使用されているかを表します。 使用率が高くなるほど、ネットワークのパフォーマンスは低くなります。

  ネットワーク使用率が頻繁に高くなりすぎる場合、原因となっているプロセスを特定して問題を解決する必要があります。また、特定のネットワーク容量に基づいて、バックアップ中のネットワーク使用率が高すぎる場合、NIC カードをアップグレードして高いスループット要件に対応する必要があります。

5. ［保存］をクリックします。

電子メール アラート オプションが保存されます。

電子メール設定の指定

［電子メールの設定］ダイアログ ボックスでは、電子メール サーバおよびポリシー電子メール環境設定から新規ポリシーに自動的に値が読み込まれます。 これらの設定は、すべての電子メール アラート通知に適用されます。また、設定はいつでも変更できます。

サービス

アラート通知の送信に使用する電子メール プロバイダ サービス。 利用可能なオプションは、Google メール、Yahoo メール、Live メールおよびその他です。

- ［その他］を選択した場合、デフォルト設定として使用されるメール サーバおよび対応するポート番号を特定する必要があります。
- ［Google メール］、［Yahoo メール］、［Live メール］を選択する場合、メール サーバとポート番号は自動的に入力されます。

メール サーバ

CA ARCserve D2D で電子メール アラートの送信に使用できる SMTP メール サーバのホスト名。

ポート

メール サーバの出力ポート番号。

認証が必要

インターネット経由で電子メールを送信する際、このメール サーバが認証を必要とするかどうかを指定します。 このオプションを選択する場合、対応するユーザ アカウント名とパスワードを指定する必要があります。

件名

CA ARCserve D2D が送信する電子メール アラート通知の件名。 デフォルトは、CA ARCserve D2D アラートです。

送信者

CA ARCserve D2D で電子メール アラート通知の送信に使用する電子メール アドレス。

受信者

電子メール アラート通知を受信する受信者の電子メール アドレス。

注: 複数の電子メール アドレスを入力するには、各アドレスをセミコロンで区切る必要があります。

SSL の使用

インターネット経由でデータを安全に転送するために、電子メール サーバで SSL （Secure Sockets Layer）接続を必要とすることを指定します。

STARTTLS の送信

サーバ間で安全な SMTP 接続を開始するために、発行された STARTTLS （Start TLS extension） コマンドを電子メール サーバで必要とすることを指定します。

HTML 形式を使用

電子メール アラート通知が HTML 形式で送信されます。このオプションを選択しない場合、アラートはプレーン テキストで送信されます。デフォルトでは、このオプションが選択されています。

プロキシ設定を有効にする

電子メール アラート通知を送信する際に、プロキシ サーバに接続するかどうかを指定します。 このオプションを選択する場合、対応するプロキシ サーバ名とポート番号を指定する必要があります。

テスト メール

メールの環境設定が正しいことを確認します。

更新の環境設定の指定

CA ARCserve Central Protection Manager では、更新の環境設定を指定できます。

更新の環境設定を指定する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。

2. ［新規］をクリックして、新しいポリシーを作成します。

   ［新規ポリシー］ダイアログ ボックスが開きます。

3. ［環境設定］タブを選択し、次に［更新］を選択します。

［環境設定］の［更新］ダイアログ ボックスが表示されます。

4. 更新の環境設定を指定します。

   - **ダウンロード サーバ** -- CA ARCserve D2D サーバが利用可能な更新をダウンロードするために接続するソース サーバを指定します。

     - **CA Technologies サーバ** -- このオプションを使用すると、CA ARCserve D2D 更新が CA Technologies サーバからローカル サーバに直接ダウンロードされます。

     - **ステージング サーバ** -- ステージング サーバとして使用するサーバを指定します。

       複数のステージング サーバを指定した場合、リストの最初のサーバがプライマリ ステージング サーバとして指定されます。CA ARCserve D2D は、まずプライマリ ステージング サーバへの接続を試行します。何らかの理由で最初のサーバが利用可能でない場合は、リストの次のサーバがプライマリ ステージング サーバになります。 リストの最後のサーバがプライマリ ステージング サーバになるまで、この手順が続行されます （ステージング サーバ リストには最大で 5 つのサーバを含めることができます）。

     - ［上に移動］および［下に移動］ボタンを使用してステージング サーバの順序を変更できます。

     - ［削除］ボタンを使用して、このリストからサーバを削除できます。

     - 新しいサーバをこのリストに追加するには［サーバの追加］ボタンを使用します。［サーバの追加］ボタンをクリックすると、［ステージング サーバ］ダイアログ ボックスが開き、追加するステージング サーバの名前を指定できます。

       これはデフォルトの設定です。

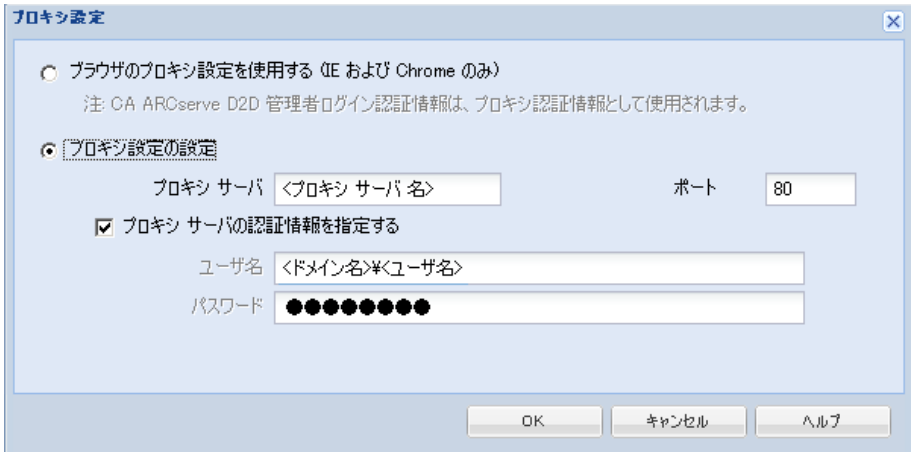
       注: D2D ポリシーの場合、デフォルトのステージング サーバはローカルの CA ARCserve Central Applications コンピュータです。

       CA ARCserve D2D 更新は、CA Technologies サーバから指定されたステージング サーバ場所へ直接ダウンロードされます。 更新がステージング サーバにダウンロードされたら、その更新をステージング サーバからクライアント サーバにダウンロードできます。 ステージング サーバを選択した場合、ステージング サーバのホスト名または IP アドレスと、対応するポート番号も指定します。

- **プロキシ設定** -- このオプションは、ダウンロード サーバとして CA サーバを選択した場合のみ使用できます。

  CA ARCserve D2D 更新をプロキシ サーバ経由でダウンロードする場合は［プロキシ設定］をクリックします。 これは、ダウンロード サーバが更新を入手する先の CA サーバへの接続になります。

  このボタンをクリックすると、［プロキシ設定］ダイアログ ボックスが表示されます。



  - **ブラウザのプロキシ設定を使用する（IE および Chrome のみ）** -- CA ARCserve D2D プロキシに提供された認証情報を使用します。
  - **プロキシを設定する** — プロキシ サーバは、ダウンロード サーバ（ステージングまたはクライアント）と CA サーバとの間の中継として機能します。目的は、セキュリティ、パフォーマンス、管理制御を向上させることです。デフォルトでは、この機能はオフになっています。

    CA ARCserve D2D 更新情報を取得するために CA サーバへの接続にプロキシ サーバを使用する場合は、このオプションを選択します。 プロキシ サーバは、直接 CA サーバに接続して更新情報を取得します。このオプションを有効にした場合、プロキシ サーバの IP アドレス（またはホスト名）と、プロキシ サーバがインターネット接続の際に使用するポート番号も指定します。

    このオプションを選択しない場合は、プロキシ サーバを介さずにダウンロード サーバが直接 CA サーバに接続します。

    また、プロキシ サーバで認証が必要かどうかも指定できます。指定すると、プロキシ サーバを使用する際に認証情報（ユーザ ID とパスワード）が必要となります。

- **接続テスト** -- 以下の接続をテストし、完了時にステータス メッセージを表示します。
  - ダウンロード サーバとして CA Technologies サーバを選択した場合、指定されたプロキシ サーバを介したコンピュータと CA Technologies サーバ間の接続をテストします。
  - ダウンロード サーバとしてステージング サーバを選択した場合、指定されたステージング サーバとコンピュータ間の接続をテストします。

    ［接続テスト］ボタンを使用して、リストに含まれているステージング サーバの可用性をテストできます。また、対応するステータスが［接続状態］フィールドに表示されます。

  注: 新規ポリシーの作成時に、［環境設定 - 自動更新］ダイアログ ボックスを開くと、接続テストが自動的に実行されます。

- **更新スケジュール** — 新しい CA ARCserve D2D 更新をチェックしてダウンロードするタイミングを指定します。

  このオプションを選択して、利用可能な新しい CA ARCserve D2D 更新を自動的にチェックするかどうかを指定します。 このオプションを選択すると、ドロップダウン メニューを使用して、この機能を実行する日（毎日、毎週、または指定した曜日）と時刻を指定できます。

  このオプションを選択して日時を指定しない場合、デフォルトのスケジュールでは、毎週日曜日の午前 4 時に自動チェックが実行されます。

  このチェックによって新しい更新が利用可能であることが判断された場合、デフォルトでは、CA ARCserve D2D によって自動的に更新がダウンロードされます。 更新を自動的にダウンロードしない場合、D2DPMSettings.INI ファイルでこの機能を無効にすることができます。 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。

  このオプションが選択されていない場合、自動チェックとダウンロードの機能はすべて無効になります（ホーム画面のステータス サマリ セクションにそのステータスが表示されます）。

  このオプションが選択されていなければ、これらの更新機能は手動でのみ開始できます。

  注: スケジュールされた更新チェックで新しい更新が利用可能であることがわかった場合に、電子メール通知が送信されるよう設定することができます。 また、更新の確認中またはダウンロード中に問題が発生した場合も、電子メール通知が送信されます。

5. ［保存］をクリックします。

更新環境設定が保存されます。

ポリシーの編集またはコピー

CA ARCserve Central Protection Manager では、ポリシーを作成し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. アプリケーションにログインします。

   ナビゲーション バー上の［ポリシー］をクリックして、［ポリシー］画面を開きます。

2. ［ポリシー］画面でポリシーの隣のチェック ボックスをオンにし、以下のいずれかを実行します。

   - ツールバー上の［編集］をクリックし、選択したポリシーを編集します。
   - ツールバー上の［コピー］をクリックし、選択したポリシーから新規ポリシーをコピーして作成します。

     注: ポリシーをコピーする際、［ポリシーのコピー］ダイアログ ボックスが表示されます。新しいポリシーの名前を指定し、［OK］ボタンをクリックします。

   ［ポリシーの編集］ダイアログ ボックスが開きます。

3. ポリシー名を変更する場合は、［ポリシー名］フィールドで名前を指定します。

4. 必要な値を指定して、［保存］をクリックします。

ポリシーが編集またはコピーされます。

ポリシーの削除

CA ARCserve Central Protection Manager では、作成済みのポリシーを削除することができます。

注: CA ARCserve Central Protection Manager 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、「ポリシーのノードの割り当て/割り当て解除 (P. 162)」を参照してください。

ポリシーを削除する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。

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。

ポリシーの展開

CA ARCserve Central Protection Manager では、リモート サーバに複数回展開されたか、展開できなかったかに関わらず、ポリシーを展開することができます。

ポリシーを展開する方法

1. CA ARCserve Central Protection Manager ホーム画面から、ナビゲーション バーの［ポリシー］をクリックします。

   ［ポリシー］画面が開きます。

2. ポリシー リストからポリシーを選択し、［今すぐ展開］をクリックします。

   ポリシーがすぐに展開されます。

注: ポリシーが CA ARCserve D2D ノードに正常に展開された場合、CA ARCserve D2D ノード上のすべての設定は変更できません。［接続の更新］ボタンが有効である場合を除き、CA ARCserve D2D では、アクセス認証情報がリモート サーバ上で変更されている場合、バックアップ デスティネーションへの接続情報を再同期させることができます。さらに、［ノード リスト］画面の［ポリシー］列でポリシーの展開ステータスを表示できます。

ポリシーのノードの割り当て/割り当て解除

CA ARCserve Central Protection Manager では、既存の D2D ポリシーから、ノードの割り当てまたは割り当て解除を行うことができます。

次の手順に従ってください:

1. CA ARCserve Central Protection Manager ホーム画面で、ナビゲーションバーの［ポリシー］をクリックして［ポリシー］画面を開きます。
2. ポリシー リストからポリシーを選択し、［ポリシーの割り当て］タブをクリックします。

   選択したポリシーに割り当てられているノードのリストが表示され、以下のいずれかの展開アクションおよびステータスが示されます（形式： [アクション] 展開ステータス）。

   - [割り当て] 保留中
   - [割り当て解除] 展開
   - [再同期] 処理済み
   - [更新] 失敗
   - [再展開] D2D 展開は正常に完了しました
   - [再展開] D2D の展開に失敗しました
   - [再展開] D2D の展開を再開しています
3. ［割り当てと割り当て解除］ボタンをクリックします。

   ［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。
4. ［ポリシーの割り当て/割り当て解除］ダイアログ ボックスから以下のフィールドを指定します。

   - **グループ** -- 割り当てるノードが含まれているグループの名前を選択できます。
   - **ノード名フィルタ** -- 共通の条件に基づいて利用可能なノードをフィルタ処理できます。

     注: ［ノード名］フィールドでは、ワイルドカード文字を使用してノードのフィルタリングを行えます。

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

5. 以下のいずれかの操作を実行します。

   - **ポリシーへのノードの割り当て** -- 追加するノードを選択して、右矢印をクリックします。

     ノードが［利用可能なノード］リストから［選択されたノード］リストに移動します。

     注: ノードをすべて選択し移動させるには、二重右矢印をクリックします。

   - **ポリシーからのノードの割り当て解除** -- 割り当てを解除するノードを選択して左矢印をクリックします。

     ノードが［選択されたノード］リストから［利用可能なノード］リストに移動します。

     注: ノードをすべて選択し移動させるには、二重左矢印をクリックします。

   ［OK］をクリックします。

   注: ポリシーの割り当てを解除すると、以下のメッセージが表示されます。

   ノードからポリシーを割り当て解除しようとしています。 現在の設定を保持して、ノードがバックアップ処理を継続できるようにできます。 設定を維持しますか? 現在の CA ARCserve D2D 設定を維持するには［はい］をクリックし、現在の CA ARCserve D2D 設定を削除するには［いいえ］をクリックします。または、［ポリシーの割り当て/割り当て解除］画面に戻る場合は［キャンセル］をクリックします。

   ［いいえ］をクリックした場合、リモート CA ARCserve D2D 設定は失われ、CA ARCserve D2D サーバは保護されません。

ノードが指定されたポリシーに適用されます。

今すぐバックアップを実行

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

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

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

次の手順に従ってください:

1. アプリケーションにログインします。
2. ホーム画面上のナビゲーション バーから［ノード］をクリックして［ノード］画面を開きます。
3. バックアップするノードを指定するために、以下のいずれかのアクションを実行します。
   - **ノード レベル**： バックアップするノードが含まれるグループをクリックし、バックアップするノードの横のチェック ボックスをオンにします。
   - **グループ レベル**： バックアップするノードが含まれるグループをクリックします。
4. 次に、ノードをバックアップするために以下のいずれかのアクションを実行します。
   - ツールバーの［バックアップ］をクリックします。
   - 選択したグループを右クリックするか、またはノードを右クリックし、コンテキスト メニューの［今すぐバックアップ］をクリックします。

5. ［今すぐバックアップを実行］ダイアログ ボックスで、以下のいずれかの種類をクリックしてバックアップの種類を指定します。

   - **フル バックアップ** -- マシン全体または選択されたボリュームのフル バックアップを開始します。
   - **増分バックアップ** -- マシンの増分バックアップを開始します。 増分バックアップは、前回のバックアップ以降に変更されたブロックのみをバックアップします。

     注: 増分バックアップのメリットは、バックアップを高速で実行できること、また作成されるバックアップ イメージのサイズが小さいことです。 これは、バックアップを実行する場合に最も適した方法です。
   - **検証バックアップ** -- マシンの検証バックアップを開始します。個別のブロックの最新のバックアップを確認し、中身および情報を元のソースと比較します。 この比較によって、前回バックアップされたブロックが、ソースの対応する情報を表しているかどうかを検証します。 ブロックのバックアップ イメージがソースと一致しない場合、CA ARCserve D2D によって、一致していないブロックのバックアップが更新（再同期）されます。 検証バックアップの実行には、以下のようなメリットとデメリットがあることに注意してください。

     - メリット -- フル バックアップに比べて作成されるバックアップ イメージは極めて小さくなります。これは、変更されたブロック（最新のブロックに一致しないブロック）のみがバックアップされるためです。
     - デメリット -- すべてのソース ディスク ブロックが前回のバックアップのブロックと比較されるため、バックアップ時間は遅くなります。

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

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

確認の画面が表示され、選択した種類のバックアップがただちに開始されます。

以下の動作に注意してください。

- ［ポリシー］ダイアログ ボックスで指定された値はすべてジョブに適用されます。
- カスタム（アドホック）バックアップ ジョブが失敗してもメークアップ ジョブは作成されません。 メークアップ ジョブが作成されるのは、スケジュールされたジョブが失敗したときのみです。

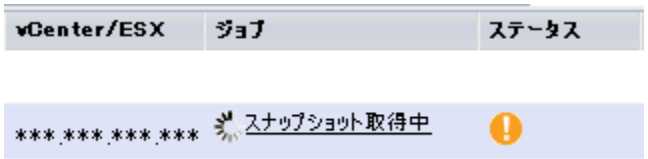
ジョブ ステータス情報の表示

ジョブが実行されている場合、ジョブに関する詳細情報を表示できます。進行中のジョブを必要に応じて停止することもできます。

次の手順に従ってください:

1. アプリケーションにログインします。
2. ホーム画面上のナビゲーション バーから［ノード］をクリックして［ノード］画面を開きます。
3. ［グループ］ツリーで、ジョブのステータスを表示するノードが含まれるグループをクリックします。

   ジョブが進行中である場合、ジョブのフェーズが［ジョブ］列に表示されます。



4. ［ジョブ］列のフェーズをクリックすると、［バックアップ ステータス モニタ］ダイアログ ボックスが開きます。
5. ［バックアップ ステータス モニタ］ダイアログ ボックスで、以下のいずれかを実行できます。
   - ［閉じる］をクリックし、［バックアップ ステータス モニタ］ダイアログ ボックスを閉じます。
   - ［キャンセル］をクリックし、現在のジョブを停止します。

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

CA ARCserve Central Protection Manager でノードをリストアする方法

CA ARCserve Central Protection Manager では、ノードのリストアに使用できるさまざまなツールやオプションが提供されています。 このセクションでは、データを安全かつ効率的にリストアするための方法について説明します。

このセクションには以下のトピックが含まれます。

復旧ポイントからのデータのリストア

［復旧ポイントの参照］を使用して、利用可能な復旧ポイント（成功したバックアップ）をカレンダ表示から選択することにより、すべてのアプリケーションをリストアできます。

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 バーの［ノード］をクリックします。
2. ［ノード］画面で、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、ツールバー上の［リストア］をクリックします。
3. ［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。

4. ［バックアップ場所］を指定するか、またはバックアップ イメージが保存されている場所を参照して選択します。

   注: 指定されたバックアップ先への接続を検証するために、［参照］ボタンの横の緑の矢印をクリックできます。 リモート ネットワーク共有に接続するには、ユーザ名およびパスワードの認証情報を入力する必要がある場合があります。

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

5. リストアする情報を指定します。

   a. 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、バックアップの名前、カタログ ステータス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。

   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。

   ［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。

   元の場所にリストアする

   バックアップ イメージがキャプチャされた元の場所にリストアします。

   注: CA ARCserve D2D のログ フォルダを元の場所にリストアする場合、ログ フォルダにあるファイルはスキップされます。 CA ARCserve Central Host-Based VM Backup では、このオプションはデフォルトで無効になっています。このオプションを使用するには、ゲスト OS 内に CA ARCserve D2D をインストールしてからリストアします。

   別の場所にリストアする

   場所を指定するか、バックアップ イメージをリストアする場所を参照して選択します。 緑色の矢印アイコン ボタンをクリックすると、指定した場所への接続を検証できます。

   必要に応じて、その場所にアクセスするための［ユーザ名］および［パスワード］認証情報を入力します。

7. リストア プロセスで競合が発生した場合に、CA ARCserve D2D でどのように解決するかを選択します。

   使用可能なオプションは、以下のとおりです。

   既存ファイルを上書きする

   リストア先で検出された既存ファイルを上書き（置換）します。すべてのオブジェクトがバックアップ 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

   再起動の際にアクティブ ファイルを置換します。 リストア試行時に、既存ファイルが使用中またはアクセス中であることが 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、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

   リストア先で検出された既存ファイルを上書き（置き換え）せず、スキップします。 そのコンピュータに現在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。

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

   これにより、CA ARCserve D2D では、リストア デスティネーション パス上に同じルート ディレクトリ構造を作成できます。

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

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

   ［リストア サマリ］ダイアログ ボックスが表示されます。

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。

ファイル コピーからのデータのリストア

［ファイル コピーの参照］オプションを使用すると、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。

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 バーの［ノード］をクリックします。

2. ［ノード］画面で、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、ツールバー上の［リストア］をクリックします。

3. ［リストア］ダイアログ ボックスで、［ファイル コピーの参照］をクリックします。

   ［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。

4. ［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。

   - **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。

     ダイアログ ボックスが表示され、利用可能な別のデスティネーション オプションが示されます。

     - **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。

5. ［次へ］をクリックします。

   ［リストア オプション］ダイアログ ボックスが表示されます。

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¥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¥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る場合があります。

  暗号化されたバックアップが実行されたコンピュータ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、別のコンピュータ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（時計アイコン）

  暗号化された復旧ポイント（鍵の付いた時計アイコン）

［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。

ファイル/フォルダからのデータのリストア

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

ファイル/フォルダ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 バーの［ノード］をクリックします。

   ［ノード］画面で、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、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、［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。

3. ［バックアップ場所］および［ファイル コピーの場所］を指定するか、またはバックアップ イメージが保存される場所を参照して選択します。

   以下の点に注意してください。

   - バックアップ場所については、指定されたバックアップ先への接続を検証するために［参照］ボタンの横の緑の矢印をクリックできます。 リモート ネットワーク共有に接続するには、ユーザ名およびパスワードの認証情報を入力する必要がある場合があります。
   - [［ファイル コピーの場所］は、［変更］をクリックして、ローカル/ネットワーク ドライブまたはクラウドに切り替えることができます。 ファイル コピーの場所の詳細については、「ファイル コピーからのデータのリストア (P. 171)」を参照してください。

4. リストアするファイル名またはフォルダ名を指定します。

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

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

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

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

5. （オプション）検索をさらに絞り込むにはパスを指定し、サブディレクトリまたはファイル/フォルダを含めるかどうかを選択します。

6. ［検索］ボタンをクリックして、検索を開始します。

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

7. 回復するバージョンをリストから選択して[次へ]をクリックします。

   ［リストア オプション］ダイアログ ボックスが表示されます。

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。

   元の場所にリストアする

   バックアップ イメージがキャプチャされた元の場所にリストアします。

   注: CA ARCserve D2D のログ フォルダを元の場所にリストアする場合、ログ フォルダにあるファイルはスキップされます。

   別の場所にリストアする

   場所を指定するか、バックアップ イメージをリストアする場所を参照して選択します。 緑色の矢印アイコン ボタンをクリックすると、指定した場所への接続を検証できます。

   必要に応じて、その場所にアクセスするための［ユーザ名］および［パスワード］認証情報を入力します。

9. リストア プロセスで競合が発生した場合に、CA ARCserve D2D でどのように解決するかを選択します。

   使用可能なオプションは、以下のとおりです。

   既存ファイルを上書きする

   リストア先で検出された既存ファイルを上書き（置換）します。すべてのオブジェクトがバックアップ 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

   再起動の際にアクティブ ファイルを置換します。 リストア試行時に、既存ファイルが使用中またはアクセス中であることが 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、新規ファイルを作成します。このオプションを選択すると、ファイル名は変更せず、拡張子を変更してソース ファイルをデスティネーションにコピーします。 その後、データは新規ファイルにリストアされます。

   既存ファイルをスキップする

   リストア先で検出された既存ファイルを上書き（置き換え）せず、スキップします。 現在マシン上に存在しないオブジェクトのみがバックアップ ファイルからリストアされます。

   デフォルトでは、このオプションが選択されています。

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

    これにより、CA ARCserve D2D では、リストア デスティネーション パス上に同じルート ディレクトリ構造を作成できます。

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

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

    ［リストア サマリ］ダイアログ ボックスが表示されます。

12. 表示された情報に目を通し、リストア オプションおよび設定がすべて正しいことを確認します。

    - サマリ情報が正しくない場合は、［前に戻る］をクリックし、該当するダイアログ ボックスに戻って、正しくない設定を変更します。

サマリ情報が正しい場合は、［完了］ボタンをクリックし、リストア プロセスを開始します。

仮想マシンからのデータのリストア

VM （仮想マシン）の復旧オプションを使用して、バックアップ済みの仮想マシンをリストアすることができます。

仮想マシン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 バーの［ノード］をクリックします。

   ［ノード］画面から、リストアするノードが含まれるグループを展開します。

   リストアするノードの横のチェック ボックスをオンにしてから、ツールバー上の［リストア］をクリックします。 CA ARCserve D2D にログインします。

2. ［リストア］ダイアログ ボックスから、［VM の復旧］をクリックします。

   ［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（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. リストアする仮想マシンを指定します。

   ドロップダウン メニューには、指定されたバックアップ場所にあるすべての仮想マシンが含まれます。

5. カレンダで、リストアする仮想マシン 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。

6. 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）が参照のため表示されます。 仮想マシンのリストアでは、マシン全体がリストアされます。 そのため、選択された仮想マシン内の個別のボリューム、フォルダ、またはファイルを参照はできますが、選択することはできません。

   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。

7. リストアするバックアップ情報を指定したら、［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。

8. リストア デスティネーションを選択します。

   元の場所にリストアする

   バックアップ イメージがキャプチャされた元の場所に仮想マシンをリストアします。 デフォルトでは、このオプションが選択されています。

   詳細については、「元の場所への VM のリストア (P. 183)」を参照してください。

   別の場所にリストアする

   バックアップ イメージがキャプチャされた場所とは別の場所へ仮想マシンをリストアします。

   詳細については、「別の場所への VM のリストア (P. 184)」を参照してください。

9. リストア処理中に競合が発生した場合に CA ARCserve D2D によって競合を解決する方法を指定します。

   既存の仮想マシンに上書きするかどうかを選択できます。 上書きオプションはデフォルトでは選択されていません。

   - このオプションを選択した場合、リストア プロセスでは、指定されたリストア デスティネーションにこの仮想マシンの既存イメージが存在すると、上書き（置換）します。仮想マシン イメージは、現在リストア デスティネーションに存在しているかどうかにかかわらず、バックアップ ファイルからリストアされます。
   - このオプションを選択しない場合、リストア プロセスでは、指定されたリストア デスティネーションにこの仮想マシンの既存イメージが存在すると、別のイメージを作成します（既存イメージを上書きしません）。

10. ［復旧後の処理］オプションを指定します。

    リストア プロセスの最後に仮想マシンの電源をオンにするかどうかを選択します。 このオプションは、デフォルトでは選択されていません。

仮想マシンの元の場所へのリストア

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

元の場所への VM のリストアを選択した場合は、以下の手順に従います。

次の手順に従ってください:

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

   注: ［競合の解決］および［復旧後の処理］オプションの詳細については、「仮想マシンからのデータのリストア (P. 180)」を参照してください。

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

2. 仮想マシンにアクセスするための認証情報を指定します。

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

3. 認証情報を指定したら、［OK］をクリックします。

   ［リストア サマリ］ダイアログ ボックスが表示されます。

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

仮想マシンの別の場所へのリストア

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

仮想マシンを別の場所にリストアする場合は、以下の手順に従います。

次の手順に従ってください:

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

   注: ［競合の解決］および［復旧後の処理］オプションの詳細については、「仮想マシンからのデータのリストア (P. 180)」を参照してください。

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

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

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

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

4. 以下の情報を指定します。

   - **VM 名** -- リストアする仮想マシンのホスト名を指定します。
   - **ESX Server** -- デスティネーションの ESX Server を指定します。 ドロップダウン メニューには、指定された仮想マシンに関連付けられているすべての ESX Server のリストが含まれます。
   - **VM データ ストア** -- デスティネーション VM データ ストアを指定します。

5. その他の情報が指定されたら、［次へ］をクリックします。

   ［リストア サマリ］ダイアログ ボックスが表示されます。

6. 表示された情報に目を通し、リストア オプションおよび設定がすべて正しいことを確認します。

   - サマリ情報が正しくない場合は、［前に戻る］をクリックし、該当するダイアログ ボックスに戻って、正しくない設定を変更します。
   - サマリ情報が正しい場合は、［完了］ボタンをクリックし、リストア プロセスを開始します。

Microsoft Exchange 電子メール データのリストア

CA ARCserve D2D によってバックアップが正常に実行されるたびに、バックアップの Point-in-Time スナップショット イメージも作成されます。 この復旧ポイントの集合体によって、リストアする必要があるバックアップ イメージを正確に特定して指定できます。 Microsoft Exchange Server の場合は、これらの復旧ポイントを参照し、回復する個々のオブジェクト（メールボックス、メールボックス フォルダ、電子メールなど）を特定することができます。 Exchange 詳細リストアを実行するには、アカウントに権限が必要です。 詳細については、「Exchange アカウントのリストア権限」を参照してください。

注: Microsoft Exchange Server 2007 以降の場合、Messaging API （MAPI）が Exchange 詳細リストアの前提条件になります。 MAPI が Exchange Server にインストールされていなければ、メールボックスまたはメール レベルの詳細リストアは失敗する場合があります。 Exchange Server に MAPI をインストールする詳細については、Microsoft Download Center を参照してください。

Microsoft Exchange 電子メール 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 バーの［ノード］をクリックします。

   ［ノード］画面から、リストアするノードが含まれるグループを展開します。

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

2. ［リストア］ダイアログ ボックスから、［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確認できます。

   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: 通知メッセージが表示され、Exchange 詳細リストア カタログをこの時点で生成するかどうかをユーザに確認します。 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。

   ［リストア オプション］ダイアログ ボックスが表示され、選択したデータベースの対応するメールボックス コンテンツのリストが示されます。

   注: 電子メール リストアのみがサポートされています。 カレンダ、連絡先、メモ、および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。

   注: リストアする対象として、コンテンツ全体、部分的コンテンツ、または複数の Exchange オブジェクトを選択できます。

   a. 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 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. 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 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. ［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:

   - メールボックスまたはメールをリストアする場合（元の場所または別の場所に）、リストア先が利用可能であることを確認する必要があります。利用可能でないとリストアに失敗します。 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。
   - 電子メールをマシンにリストアしようとして、それらのメール内の電子メール アドレスがそのマシンで有効ではない（ドメインに存在しない）場合、またはユーザがメールボックスにログインしていない場合は、一部のフィールドがバックアップと同じように表示されないことがあります。
   - 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に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。

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。 このディスクの場所はローカル パスである必要があります。 リストアされたメールは、対応する Exchange メールボックスにおける階層と同じ階層を維持します。 ファイル名は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： ¥ / : * ? " < > |

ファイル システムの競合状態を解決するには 2 つのオプションがあります。 Exchange メールでは 2 つのファイルが同じフォルダに存在しても問題ありませんが、ファイル システムの場合は同じフォルダには存在できません。

- **名前を変更する** -- メールの件名と同じ名前のファイルがディスク上に存在する場合、CA ARCserve D2D ではメールの件名の最後に数字を追加します。
- **上書きする** -- メールの件名と同じ名前のファイルがディスク上に存在する場合、CA ARCserve D2D ではそのファイルを上書きします。

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）。

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. ［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。

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。

CA ARCserve Central Protection Manager ログの表示

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

次の手順に従ってください:

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

   ［ログの表示］画面が表示されます。

2. ドロップダウン リストから、表示するログ情報を指定します。

   - **重大度** -- 表示するログの重大度を指定します。 以下の重大度オプションを指定できます。
     - **すべて** -- 重大度にかかわらず、すべてのログを表示します。
     - **情報** -- 一般的な情報を説明するログのみを表示します。
     - **エラー** -- 発生したエラーを説明するログのみを表示します。
     - **警告** -- 発生した警告を説明するログのみを表示します。
     - **エラーと警告** -- 発生したエラーおよび警告のみを表示します。

- **モジュール** -- ログを表示するモジュールを指定します。 以下のモジュール オプションを指定できます。
  - **すべて** -- すべてのアプリケーション コンポーネントに関するログを表示します。
  - **共通** -- 共通のプロセスに関するログを表示します。
  - **ディスカバリからのノードのインポート** -- ディスカバリからインポートされたノードのログのみを表示します。
  - **ハイパーバイザからのノードのインポート** -- ハイパーバイザからインポートされたノードのログのみを表示します。
  - **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。
  - **CA ARCserve Backup 同期** --CA ARCserve Backup データの同期に関するログのみを表示します。
  - **CA ARCserve D2D 同期** --CA ARCserve D2D データの同期に関するログのみを表示します。
  - **CA ARCserve D2D の更新** --CA ARCserve D2D の変更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。
  - **CA ARCserve D2D バックアップ ジョブのサブミット** -- サブミットした CA ARCserve D2D バックアップ ジョブに関するログのみを表示します。
  - **複数ノードの更新** -- 複数ノードの同時更新に関するログのみを表示します。
  - **CA ARCserve D2D マージ ジョブ** -- CA ARCserve D2D マージ ジョブのログのみを表示します。
- **ノード名** -- 特定のノードのログのみを表示します。

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

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

［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、CA ARCserve Central Protection Manager サーバがある場所のタイム 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。

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

ベスト プラクティスの適用

CA ARCserve Central Protection Manager アプリケーションでは、以下のベストプラクティスを検討してください。

- CA ARCserve Central Applications は、CA ARCserve Central Applications ローカル コンピュータとリモート コンピュータの間の通信によって、リモート コンピュータから特定のノードのデータを取得できます。

  リモート アクセスが常に正常に機能するようにするには、以下の制限が必要です。

  - **ネットワークの制限** -- リモート コンピュータ上の 'admin$' というリモート管理者共有を有効にする必要があります。 リモート コンピュータ上の 'admin$' を有効にするには、以下のリンクをクリックして指示に従ってください。

    http://support.microsoft.com/kb/947232

  - **ユーザ アカウントの制限** -- CA ARCserve Central Applications にログインするには、CA ARCserve Central Applications ローカル コンピュータからの管理者アカウントを使用するか、CA ARCserve Central Applications ローカル コンピュータおよびリモート コンピュータに管理者権限を追加する必要があります。

  注: ノードを追加するには、リモート コンピュータからの管理者権限を持っていることが必要になります。

- Windows Server 2008 R2 コンピュータ上でノード名または IP アドレスによってノードを追加するには、以下の要件のいずれかに基づいてアカウントを使用します。

  - CA ARCserve Central Applications へのログインに、CA ARCserve Central Applications コンピュータおよびリモート コンピュータから管理者グループ アカウントを使用する場合、同じアカウントを使用してノードを追加できます。

  - CA ARCserve Central Applications へのログインに、CA ARCserve Central Applications コンピュータから Bulletin Administrator アカウントを使用する場合、リモート コンピュータから管理者アカウントを使用してノードを追加します。

- Active Directory からノードを検出するには、以下のオプションのいずれかを実行します。

- Windows ドメインに接続されたノードに CA ARCserve Central Applications をインストールする場合、CA ARCserve Central Applications はドメイン コントローラ上に存在する Active Directory 情報にアクセスできます。
- ワークグループに接続されたノードに CA ARCserve Central Applications をインストールする場合、コマンド ウィンドウで以下のコマンド ラインを実行し、CA ARCserve Central Applications が関連するドメイン コントローラにアクセスできることを確認する必要があります。

  ```
  nltest /dsgetdc:%domain_name%
  ```

  注: このオプションが ERROR_NO_SUCH_DOMAIN （1355）ステータスで失敗した場合、ネットワーク設定を調整する必要があります。

サーバの通信プロトコルの変更

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

次の手順に従ってください:

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

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

2. Windows のコマンド ラインを開きます。

3. 以下のいずれかを行います。

   - **プロトコルを HTTP から HTTPS に変更：**

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

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

     プロトコルが正常に変更されると、以下のようなメッセージが表示されます。

     通信プロトコルは HTTPS に変更されました。

   - **プロトコルを HTTPS から HTTP に変更：**

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

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

     プロトコルが正常に変更されると、以下のようなメッセージが表示されます。

     通信プロトコルは HTTP に変更されました。

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

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

第 5 章: CA ARCserve Central Protection Manager と IT 管理サーバ ツールの統合

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 Protection Manager と Nimsoft/Kaseya との統合方法

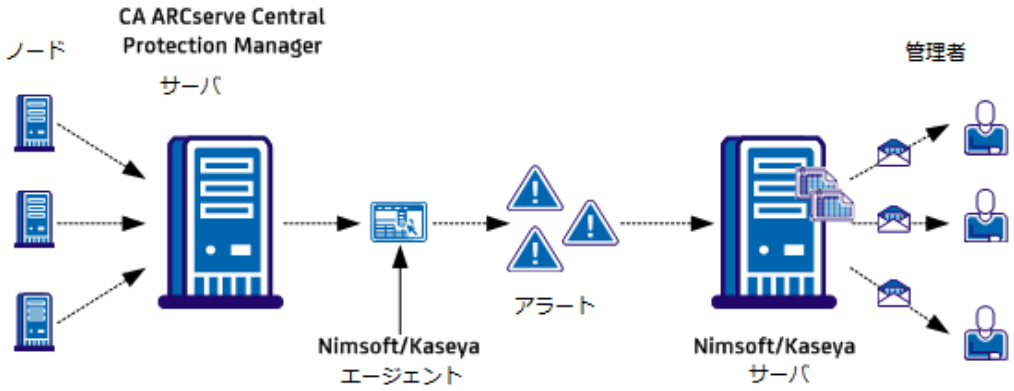
CA ARCserve Central Protection Manager を設定して、アラート メッセージに関する情報が IT 管理サーバ インフラストラクチャの管理ツールにリアルタイムで発行されるようにできます。この機能によって、IT サーバ管理の管理者は適切な方式で CA ARCserve Central Protection Manager アラートに対応できます。

CA ARCserve Central Protection Manager は、以下の IT 管理サーバ インフラストラクチャの管理ツールと統合します。

- Nimsoft
  - Server： 5.11
  - Robot: 5.32
  - Unified Monitoring Portal: 2.1.2
- Kaseya
  - Server： 6.1.0.0
  - Agent： 6.1.0.6

以下の図は、CA ARCserve Central Protection Manager が Nimsoft および Kaseya と統合される方法の例を示しています。

CA ARCserve Central Protection Manager と Nimsoft/Kaseya との統合方法



CA ARCserve Central Protection Manager サーバは、CA ARCserve D2D がインストールされているノードをモニタします。CA ARCserve Central Protection Manager サーバでアラート状態を検出すると、CA ARCserve Central Protection Manager サーバにインストールされている Nimsoft または Kaseya エージェントにそのアラートが送信されます。 エージェントは、受信したアラートを Nimsoft または Kaseya サーバにすぐに送信します。

CA ARCserve Central Protection Manager は、以下のアプリケーションから発生するアラートをモニタします。

- CA ARCserve D2D
- CA ARCserve Central 仮想スタンバイ
- CA ARCserve Central Host-Based VM Backup
- CA ARCserve Central Protection Manager

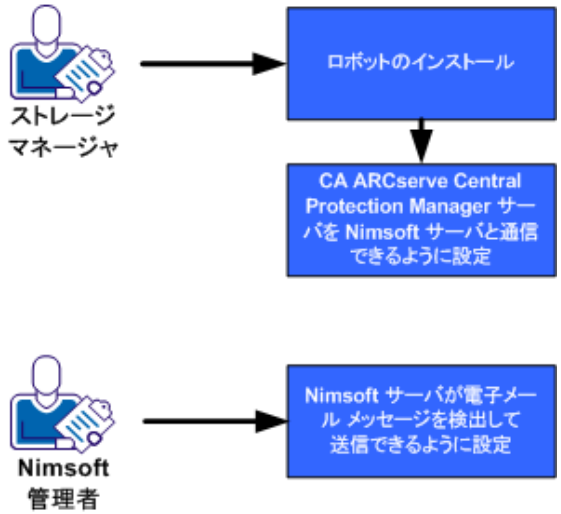
Nimsoft または Kaseya サーバは、これらのアプリケーションを実行しているノードに関するレポートを生成し、管理者は Nimsoft および Kaseya の管理ツールを使用して参照できます。 Nimsoft/Kaseya サーバは、事前に定義された条件に基づいて管理者に電子メール メッセージを送信するように設定できます。

CA ARCserve Central Protection Manager と Nimsoft との統合方法

ストレージ マネージャは、Nimsoft サーバにアラート メッセージを送信するよう CA ARCserve Central Protection Manager を設定できます。 Nimsoft 管理者は、Nimsoft IT インフラストラクチャ管理ツールを設定し、CA ARCserve Central Protection Manager アラートの検出、アラート レポートの生成、電子メール メッセージの送信が行われるようにします。 管理者は、レポートを使用して CA ARCserve D2D ノードの健全性を管理できます。

以下の図は、ストレージ マネージャが CA ARCserve Central Protection Manager と Nimsoft IT インフラストラクチャ管理ツールをどのように統合するかを示しています。

CA ARCserve Central Protection Manager と Nimsoft の統合方法



CA ARCserve Central Protection Manager と Nimsoft を統合するには、以下の手順に従います。

1. ロボットをインストール (P. 200) します。
2. CA ARCserve Central Protection Manager サーバが Nimsoft サーバと通信するよう設定 (P. 202) します。
3. Nimsoft サーバが電子メール メッセージを検出して送信するよう設定 (P. 202) します。

注: CA ARCserve Central Protection Manager サーバが、ローカライズされた文字が含まれるアラート メッセージを Nimsoft サーバに送信した場合、ローカライズされた文字が Nimsoft Unified Monitoring Portal（UMP）アラーム コンソール内では文字化けしたテキストとして表示されます。 この動作が発生するのを防ぐには、Nimsoft サーバで UTF-8 エンコーディングを使用するよう設定します。 詳細については、「CA ARCserve Central Protection Manager ユーザ ガイド」の「ローカライズされたサーバからの文字が Nimsoft UMP アラーム コンソールで文字化けして表示される」を参照してください。

ロボットのインストール

ロボットは CA ARCserve Central Protection Manager サーバにインストールします。 ロボットによって CA ARCserve Central Protection Manager サーバが Nimsoft サーバと通信し、アラート メッセージをリアルタイムで送信することができます。

注: セットアップ プログラムを実行する前に、有効なライセンスが使用可能であることを確認します。

次の手順に従ってください:

1. ロボットのセットアップ ファイルをコンピュータにダウンロードまたはコピーします。

   NimBUS Robot.exe をダブルクリックして、インストールを開始します。

   使用許諾契約のダイアログ ボックスが表示されます。

2. ライセンスのダイアログ ボックスで［Yes］をクリックしてインストールを開始します。

   ［Choose Destination Location］ダイアログ ボックスが表示されます。

3. ロボットをインストール場所を指定するか、デフォルト ディレクトリを使用する場合は［Next］をクリックします。

   ［Choose Setup Type］ダイアログ ボックスが表示されます。

4. 標準のインストールを選択して［Next］をクリックします。

   ［Nimsoft Domain］ダイアログ ボックスが表示され、検出されたドメインのリストが示されます。

5. ［Choose to connect to the network interface through IP address］の横のチェック ボックスをオンにして［Next］をクリックします。

   ［Specify Nimsoft Hub IP Address］ダイアログ ボックスが表示されます。

6. ［Hub IP］フィールドで、CA ARCserve Central Protection Manager サーバがアラート メッセージを送信する Nimsoft ハブの IP アドレスを指定します。

   ［次へ］をクリックします。

   ［Options］ダイアログ ボックスが開きます。

7. ［Options］ダイアログ ボックスで、以下のフィールドに入力します。

   （オプション）First probe port

   プローブの開始時に使用する最初のポート番号を指定できます。

   注: オペレーティング システムでランダムなポートを生成できるようにするため、ポートは指定しないでください。

   Passive mode

   このモードは、ロボットが Nimsoft ハブと通信できない場合のみ指定します。 Nimsoft ハブが CA ARCserve Central Protection Manager サーバと通信できる場合は、［Passive mode］の横のチェック ボックスをオンにします。

   注: このオプションを指定し、パッシブ ロボットをハブ環境設定に手動で追加します。

   ［次へ］をクリックします。

   ［Start Copying Files］ダイアログ ボックスが表示されます。

8. ［次へ］をクリックします。

   ロボットのインストールが開始されます。

9. インストールが完了したら、［Finish］ボタンをクリックします。

ロボットがインストールされます。

CA ARCserve Central Protection Manager サーバと Nimsoft サーバとの通信の設定

CA ARCserve Central Protection Manager では Nimsoft IT 管理サーバにアラート メッセージを送信できます。アラート情報を送信するには、CA ARCserve Central Protection Manager サーバが Nimsoft サーバと通信できるよう設定します。

次の手順に従ってください:

1. CA ARCserve Central Protection Manager 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. ［環境設定］リストで IT 管理サーバの環境設定をクリックします。

   IT 管理サーバの環境設定オプションが表示されます。

3. 以下のオプションに入力します。

   a. ［有効］をクリックします。

   b. ［Nimsoft］をクリックします。

   c. ［繰り返し方法］を指定します。 繰り返し方法は、最初の送信プロセスが失敗した場合に、アラート通知を Nimsoft サーバに再送信する日を定義します。Nimsoft サーバが利用可能でないかオフラインでない場合は、アラートを送信するプロセスが失敗する可能性があります。

   d. スケジュールを指定します。 スケジュールは、アラート通知を Nimsoft サーバに再送信する時間を定義します。

   ［保存］をクリックします。

CA ARCserve Central Protection Manager サーバは Nimsoft サーバと通信するように設定されました。

Nimsoft サーバでの電子メール メッセージの検出および送信の設定

Nimsoft 管理者は、アラーム サブコンソールを設定して、CA ARCserve Central Protection Manager サーバからアラート メッセージを検出した時点で、指定の受信者に電子メール メッセージが送信されるようにすることができます。 詳細については、Nimsoft のドキュメントを参照してください。

Nimsoft アラーム サブコンソールでのアラート情報の表示

Nimsoft アラーム サブコンソールでは、Nimsoft 管理者が CA ARCserve Central Protection Manager アラートに関する情報を参照できます。Nimsoft アラーム サブコンソールは、CA ARCserve Central Protection Manager アラートに関して以下の情報を提供します。

ホスト名

Nimsoft サーバへアラートを送信した CA ARCserve Central Protection Manager サーバのホスト名を指定します。

ソース

Nimsoft サーバへアラートを送信した CA ARCserve Central Protection Manager サーバの IP アドレスを指定します。

Severity

Nimsoft サーバに送信されたアラートの重大度を指定します。

サブシステム

アラート状態が発生したサーバのホスト名を指定します。

例： アラート状態が CA ARCserve D2D サーバ上で発生しました。 システム フィールドは CA ARCserve D2D サーバのホスト名を指定します。

サブシステム ID

アラート状態が発生したサーバの IP アドレスを指定します。

アラーム サブコンソールでは、Nimsoft 管理者がさまざまなタスクを実行できます。たとえば以下のタスクがあります。

- アラーム サブコンソールを設定し、アラートを検出した時点で指定の受信者へ電子メール メッセージを送信
- アラートの履歴を表示
- アラートを確認
- 各担当者にアラートを割り当て

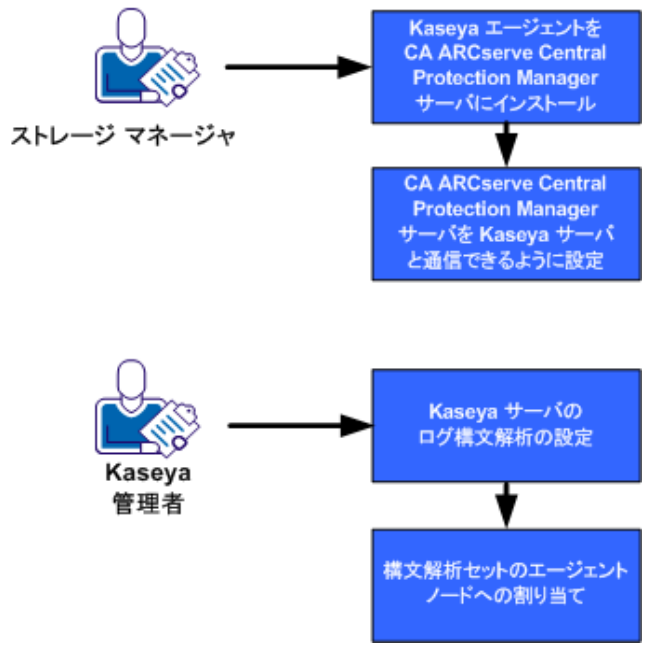
注: Nimsoft アラーム サブコンソールを使用する方法の詳細については、Nimsoft のドキュメントを参照してください。

CA ARCserve Central Protection Manager と Kaseya との統合方法

ストレージ マネージャは、Kaseya サーバにアラート メッセージを送信するよう CA ARCserve Central Protection Manager を設定できます。 Kaseya 管理者は、Kaseya IT 管理ツールを設定し、CA ARCserve Central Protection Manager アラートの検出、アラート レポートの生成、電子メール メッセージの送信などが行われるようにします。管理者は、レポートを使用して CA ARCserve D2D ノードの健全性を管理できます。

以下の図は、ストレージ マネージャが CA ARCserve Central Protection Manager と Kaseya IT インフラストラクチャ管理ツールをどのように統合するかを示しています。

CA ARCserve Central Protection Manager と Kaseya の統合方法



CA ARCserve Central Protection Manager と Kaseya を統合するには、以下の手順に従います。

1. Kaseya エージェントを CA ARCserve Central Protection Manager サーバにインストール (P. 205) します。
2. CA ARCserve Central Protection Manager サーバが Kaseya サーバと通信するよう設定 (P. 206) します。
3. Kaseya サーバのログ構文解析を設定 (P. 207) します。

4. 構文解析セットをエージェント ノードに割り当て (P. 210) ます。

Kaseya エージェントのインストール

Kaseya エージェントを CA ARCserve Central Protection Manager サーバにインストールし、Kaseya サーバと通信できるようにします。 エージェントをインストールするには、Kaseya IT 管理コンソールから展開します。

次の手順に従ってください:

1. ブラウザ ウィンドウを開き、Kaseya IT 管理コンソールにログインします。

   ウィンドウの左側のナビゲーション バーで［Agent］をクリックします。

   エージェント オプションが表示されます。

2. ［Install Agents］を展開し、［Deploy Agents］をクリックします。

   エージェントの展開オプションが表示されます。

3. 以下のいずれかのオプションをクリックします。

   Click to download default Agent

   インストール ファイルをターゲット コンピュータ上にダウンロードして保存します。

   ダウンロードが完了した後、エージェント インストール ファイルをターゲット コンピュータ上で直接実行します。

   Create Package

   コンピュータにエージェントをインストールするためにインストール パッケージ ユーティリティを作成します。画面の指示に従い、インストール パッケージを作成します。 詳細については、Kaseya のドキュメントを参照してください。

エージェントがインストールされます。

CA ARCserve Central Protection Manager サーバと Kaseya サーバとの通信の設定

CA ARCserve Central Protection Manager では Kaseya IT マネジメント サーバにアラート メッセージを送信できます。 アラート情報を送信するには、CA ARCserve Central Protection Manager サーバが Kaseya サーバと通信できるよう設定します。

次の手順に従ってください:

1. CA ARCserve Central Protection Manager 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. ［環境設定］リストで IT 管理サーバの環境設定をクリックします。

   IT 管理サーバの環境設定オプションが表示されます。

3. 以下のオプションに入力します。

   a. ［有効］をクリックします。

   b. ［Kaseya］をクリックします。

   c. ［繰り返し方法］を指定します。 繰り返し方法は、最初の送信プロセスが失敗した場合に、アラート通知を Kaseya サーバに再送信する日を定義します。 Kaseya サーバが利用可能でないかオフラインでない場合は、アラートを送信するプロセスが失敗する可能性があります。

   d. スケジュールを指定します。 スケジュールは、アラート通知を Kaseya サーバに再送信する時間を定義します。

   ［保存］をクリックします。

CA ARCserve Central Protection Manager サーバは Kaseya サーバと通信するように設定されました。

Kaseya サーバのログ構文解析の設定

CA ARCserve Central Protection Manager アラートに関する情報を表示するには、CA ARCserve Central Protection Manager アラート ログ ファイル内のデータを読み取るよう Kaseya サーバを設定します。

次の手順に従ってください:

1. ブラウザ ウィンドウを開き、Kaseya IT 管理コンソールにログインします。
2. ウィンドウの左側のナビゲーション バーで［Monitor］をクリックします。

   モニタ オプションが表示されます。
3. ［Log Monitoring］を展開し、［Log Parser］をクリックします。

   ログ解析構文の設定オプションが表示されます。
4. ［Machine.Group ID］リストで、CA ARCserve Central Protection Manager サーバの横のチェック ボックスをオンにします。

   ［Log File Parser］ドロップダウン リストから、［<Select Log Parser>］をクリックします。

   ［New］をクリックします。

   ［Log File Parser Definition］ダイアログ ボックスが表示されます。
5. ［Log File Parser Definition］ダイアログ ボックスで、以下のフィールドに入力します。

   Parser Name

   ログ ファイル構文解析ファイルの名前を定義します。

Log File Path

CA ARCserve Central Protection Manager サーバ上のログ ファイルへのパスを定義します。 ログ ファイルのパスは以下のとおりです。

```
<HOME_CA ARCserve Central Applications>¥ITMgmtIntegration¥<log_fle_name>
```

CA ARCserve Central Protection Manager は、Unicode 文字および非 Unicode 文字をサポートするログ ファイルを生成します。 この場合、ログ ファイルの名前は、以下のようになります。

非 Unicode の場合

```
CentralAppAlertsForKaseyaANSI.log
```

Unicode の場合

```
CentralAppAlertsForKaseyaUTF8.log
```

重要: Kaseya IT 管理コンソールは Unicode 文字をサポートしません。 したがって、CentralAppAlertsForKaseyaANSI.log という名前のログ ファイルを使用します。

Log Archive Path

CA ARCserve Central Protection Manager サーバ上のアーカイブ ログ ファイルへのパスを定義します。 デフォルトでは、ログ ファイルが 10MB 超えると、Protection Manager がログ ファイルをアーカイブします。

注: Protection Manager がログ ファイルをアーカイブする場合の値を変更するには、以下のファイルで MaxLogFileSize の値（MB）を変更します。

```
<HOME_CA ARCserve Central
Applications>¥ITMgmtIntegration¥Configuration¥Edge-ITMgmtIntegration.INI
```

説明

ログ ファイル構文解析のファイルの説明を定義します。

Template

CA ARCserve Central Protection Manager サーバ上のログ ファイルに含まれるデータの形式を定義します。 構文は以下のとおりです。

```
$CACentral Protection Manager Machine Name$ [$Alert Generated Product$]
$Alert Generated Machine Name$ $Severity$ $Send Time From Origin
Product$ $Alert Message$
```

Output Template

Kaseya サーバ上の出力データの形式を定義します。 構文は以下のとおりです。

```
$Protection Manager Server$ $Generated by$ $Host
Name$ $Severity$ $Sent$ $Message$
```

Log File Parameters

以下のログ ファイル パラメータを作成します。

注: パラメータのタイプを指定した後、［Apply］をクリックしてパラメータを保存します。

CA ARCserve Central Protection Manager Machine Name

タイプ： String

Alert Generated Product

タイプ： String

Alert Generated Machine Name

タイプ： String

Severity

タイプ： String

Send Time From Origin Product

タイプ： DateTime

形式： YYYY-MM-DD hh:mm:ss

Alert Message

タイプ： String

［保存］をクリックします。

ログ構文解析定義が保存されます。

6. ［Close］をクリックします。

［Log Parser Definition］ダイアログ ボックスが閉じます。ログ構文解析定義ファイルが作成され、CA ARCserve Central Protection Manager サーバに適用されます。

Kaseya サーバでの構文解析セットの割り当て

構文解析セットを設定することにより、Kaseya 管理コンソールで CA ARCserve Central Protection Manager アラートに関する情報をフィルタすることができます。構文解析セットは、フィルタする条件を定義します。たとえば、重大度レベル、バックアップの失敗、などに基づいてアラートをフィルタできます。

次の手順に従ってください:

1. ブラウザ ウィンドウを開き、Kaseya IT 管理コンソールにログインします。
2. ウィンドウの左側のナビゲーション バーで［Monitor］をクリックします。

   モニタ オプションが表示されます。
3. ［Log Monitoring］を展開し、［Assign Log Parser］をクリックします。

   ログ構文解析セットの割り当てオプションが表示されます。
4. ［Assign log parser sets to selected machines］セクションで、必要なアラート オプションを指定します。
5. ［Select log parser］ドロップダウン リストで、構文解析セットを割り当てるログ構文解析をクリックします。

   ［Define parser sets］ドロップダウン リストで、［<New Parser Set>］をクリックします。

   ［Edit Parser Set］ダイアログ ボックスが表示されます。
6. ［Parser Set Name］フィールドで、構文解析セットの名前を指定し、［New］をクリックします。

   解析オプションが表示されます。

7. 以下の値を指定します。

   Parser Column

   フィルタするパラメータを定義します。

   Operator

   パラメータに含まれているデータをどのようにフィルタするかを定義します。

   Parameter File

   フィルタするパラメータの値を定義します。

   ［Add］をクリックし、［Close］をクリックします。

   フィルタが構文解析セットに適用され、［Edit Parser Set］ダイアログボックスが閉じます。

   注: 構文解析セット フィルタを指定する方法の例については、「構文解析セット フィルタの例」を参照してください。

8. ［Select log parser］ドロップダウン リストで、適用するログ構文解析をクリックします。

   ［Define parser sets］ドロップダウン リストで、作成した構文解析セットをクリックします。

   ［Machine ID］列で、構文解析セットを適用するサーバの横のチェックボックスをクリックします。

   ［Apply］をクリックします。

ログ構文解析および構文解析セットが割り当てられます。

構文解析セット フィルタの例

エラーが含まれるアラートのみをフィルタする構文解析セットを作成するには、以下の値を指定します。

Parser Column

Severity

Operator

Equal

Parameter Filter

error

重大度レベルにかかわらず、すべてのアラートを表示する構文解析セットを作成するには、以下の値を指定します。

Parser Column

Severity

Operator

Contains

Parameter Filter

error, warning, information

失敗したバックアップに関するアラートのみを表示する構文解析セットを作成するには、以下の値を指定します。

Parser Column

Alert Message

Operator

Contains

Parameter Filter

backup, failed

Kaseya サーバでの電子メール メッセージの検出および送信の設定

Kaseya 管理者は、管理コンソールを設定して、CA ARCserve Central Protection Manager サーバからアラート メッセージを検出した時点で、指定の受信者に電子メール メッセージが送信されるようにすることができます。 詳細については、Kaseya のドキュメントを参照してください。

Kaseya エージェント ログ モニタでのアラートに関する情報の表示

Kaseya エージェント ログ モニタでは、ログ構文解析と構文解析セットに定義された条件に基づいて、アラート ログを表示することができます。このログによって、アラート状態を是正するために必要なアクションを特定して実行できます。

Kaseya エージェント ログ モニタでアラートに関する情報を表示する方法

1. ブラウザ ウィンドウを開き、Kaseya IT 管理コンソールにログインします。

   ウィンドウの左側のナビゲーション バーで［Agent］をクリックします。

   エージェント オプションが表示されます。

2. ［Machine Status］を展開し、［Agent Logs］をクリックします。

   ウィンドウの右側に、エージェント ログが表示されます。

3. サーバのリストから、情報を参照するサーバをクリックします。

   ［Refresh］をクリックします。

指定されたサーバについてアラート メッセージが表示されます。

第 6 章: CA ARCserve Central Protection Manager のトラブルシューティング

このセクションでは、CA ARCserve Central Protection Manager 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

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 Protection Manager 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 Protection Manager 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 Protection Manager 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 Protection Manager 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 Protection Manager 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 Protection Manager サーバにログインし、コマンド プロンプトを開きます。

     以下のコマンドを実行します。

     ```
     secpol.msc
     ```

     ［ローカル セキュリティ設定］ダイアログ ボックスが表示されます。

  2. ローカル ポリシーを選択し、［セキュリティ オプション］をクリックします。

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

     このオプションをダブルクリックします。

     プロパティのダイアログ ボックスが開きます。

3. 以下のオプションを選択して、［OK］ボタンをクリックします。

   LM と NTLM を送信する – ネゴシエーションの場合、NTLMv2 セッション セキュリティを使う

4. コマンド プロンプトで以下のコマンドを入力します。

   ```
   gpupdate
   ```

値が適用されます。

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

Windows Server 2008 および Windows Server 2003 OS で有効

症状:

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

この問題は以下の状況で発生します。

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

解決方法:

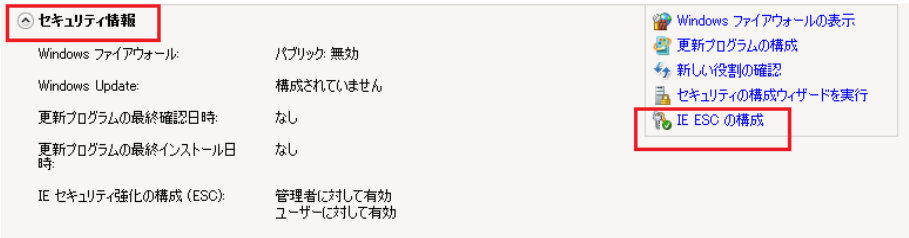
この問題を修正するには、アプリケーションの表示に使用しているコンピュータ上の Internet Explorer のセキュリティ強化の構成を無効にします。

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

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

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

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



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

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

   - 管理者 -- オフ
   - ユーザー -- オフ

   ［OK］をクリックします。

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

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

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

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

   ［次へ］をクリックします。

   引き続き画面の指示に従って手順を完了し、［完了］をクリックします。

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

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

Windows プラットフォームで有効

症状:

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

解決方法:

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

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

1. Internet Explorer を起動します。

   ［ツール］メニューで、［インターネット オプション］をクリックします。

   ［インターネットオプション］ダイアログ ボックスが表示されます。

2. ［セキュリティ］タブをクリックします。

   ［セキュリティ］オプションが表示されます。

3. ［インターネット］ゾーンをクリックします。

   インターネット ゾーン オプションが表示されます。

4. ［レベルのカスタマイズ］をクリックします。

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

5. ［スクリプト］カテゴリにスクロールします。

   ［アクティブ スクリプト］を確認します。

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

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

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

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

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

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

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と、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 Protection Manager 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 Protection Manager 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。

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

CA ARCserve Backup 同期プロセスが失敗する

Windows プラットフォームで有効

症状:

CA ARCserve Backup 同期プロセスが失敗し、［ログの表示］に表示されます。

解決方法:

一時同期データ（ダンプ ファイル）を保存するのに十分なディスク空き容量がないと、CA ARCserve Backup 同期プロセスは失敗する場合があります。 デフォルトでは、アプリケーションはダンプ ファイルを ARCserve_Central_Applications_Home¥ASBUSync ディレクトリに保存します。

C:¥Program Files 内のディスク空き容量に制限があり、ASBUSync に含まれているファイルがそれ以上の容量を必要とする場合、アプリケーションでは、同期プロセスを完了するのに必要とされる CA ARCserve Backup データベース ダンプ データを取得できません。その結果、CA ARCserve Backup 同期処理は失敗します。

必要に応じて、CA ARCserve Backup 同期データを保存するための代替場所を指定することができます。 この問題を解決する、または発生を防ぐには、以下の手順に従います。

1. CA ARCserve Central Protection Manager サーバにログインします。
2. Windows レジストリ エディタを開き、以下を選択します。

   HKEY_LOCAL_MACHINE¥SOFTWARE¥CA¥CA ARCserve Central Application¥CM

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

   以下のようにキーに名前を付けます。

   ARCserveSyncPath

4. ARCserveSyncPath を右クリックして、コンテキスト メニューの［変更］をクリックします。

   ［文字列の編集］ダイアログ ボックスが開きます。

5. ［値のデータ］フィールドで、CA ARCserve Backup 同期データを保存する代替場所を指定します。

   ［OK］をクリックします。

代替場所が指定されました。

CA ARCserve D2D 再展開が失敗する

Windows プラットフォームで有効

症状:

CA ARCserve D2D をノードに再展開した場合、展開プロセスが正常に完了しません。 この症状は、以下のイベントのいずれかが発生した場合に顕著になります。

- 以下のいずれかのメッセージが［D2D 展開］ダイアログ ボックスの［展開ステータス］に表示される。

  ユーザは正常にログインしませんでした。

  同じバージョン、新しいバージョン、またはサポートされていないこの製品のバージョンがターゲット コンピュータにインストールされています。 この製品の現在のバージョンをインストールする前に、ターゲット コンピュータからの旧バージョンをアンインストールする必要があります。

  セットアップはリモート コンピュータにファイルをコピーできません。

- ノードが［ノード］画面に表示されない。
- ノードが［ノード］画面に正しくないステータスで表示される。 たとえば、 アイコンが［ノード］画面上に表示されるか、または アイコンが［ノード］画面上に表示されない場合です。

解決方法:

これらのイベントは、以下の状態で発生します。

- CA ARCserve Central Applications Web サービスが展開プロセス中に停止または再起動し、CA ARCserve D2D がインストールされた後にデスティネーション サーバが再起動されなかった場合。
- CA ARCserve Central Applications サーバは展開プロセス中に再起動し、CA ARCserve D2D がインストールされた後にデスティネーション サーバが再起動されなかった場合。

解決するには、以下の手順に従います。

1. D2D サーバにログインし、サーバを再起動します。
2. Central Protection Manager にログインし、以下のいずれかのタスクを完了します。
   - ノードが［ノード］画面のノード リストに表示され、そのステータスが正しくない場合は、ノードを更新します。

     ノードを更新するには、ノードをクリックし、コンテキスト メニューの［更新］をクリックします。
   - ノードが［ノード］画面のノード リストに表示されない場合は、ノードを手動で追加します。

     ノードを手動で追加するには、ツールバーの［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。

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。

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

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

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

症状:

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

解決方法:

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

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

ノード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 Protection Manager では、ノード画面で追加されたノード名を保持します。 ノード名を変更した場合、アプリケーションはノードを検出できません。 そのため、ノードがノード画面に表示されません。

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

1. ノードの名前を変更します。
2. ［ノード］画面を開き、名前が変更されたノードを削除 (P. 78) します。
3. 新しい名前を使用して、ノードを追加 (P. 69) します。

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

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

D2D 展開後にノードが管理されない

Windows プラットフォームで有効

症状:

ローカルまたはリモートのサーバ上でノードに CA ARCserve D2D を展開すると、ノードがノード グループに追加されますが、ステータスは「管理されていない」になります。

この問題は、以下の状況のいずれかで発生します。

- CA ARCserve D2D が再起動なしでリモートノードに展開された。
- CA ARCserve D2D が再起動あり/なしでローカルの CA ARCserve Central Applications サーバに展開された。

解決方法:

この問題を修正するには、CA ARCserve D2D サーバを再起動し、CA ARCserve Central Protection Manager で CA ARCserve D2D ノード情報を更新します。ステータスは「管理済み」になります。

ノード データ削除スケジュールを設定する方法

Windows プラットフォームで有効

症状:

デフォルトでは、ノード データ削除スケジュールによって、削除されたノードのデータが毎日午前 2 時に消去されるよう設定されています。このスケジュールをさまざまなデータ削除用にカスタマイズする必要があります。

解決方法:

ノード データ削除用にカスタマイズされたスケジュールを作成するには、レジストリ キー CA ARCserve Central Applications¥CM¥ShowDeleteNodeConfigurationUI の値を 1 に設定します。このレジストリ キーを 1 に設定すると、CA ARCserve Central Protection Manager アプリケーション内の［環境設定］画面に［ノード データ削除環境設定］タブが追加され、スケジュールを変更できるようになります。

注: レジストリにアクセスするには、CA ARCserve Central Protection Manager サーバに直接ログインし、［スタート］-［名前を指定して実行］を選択して「Regedit」を入力します。

CA ARCserve Central Applications データベース サービスが開始されない

Windows プラットフォーム、Microsoft SQL Server、および Microsoft SQL Server Express Edition データベースで有効です。

症状:

CA ARCserve Central Protection Manager サーバを開始または再起動、または、CA ARCserve Central Applications データベースがインストールされているサーバを開始または再起動すると、CA ARCserve Central Applications データベース サービスが開始されない。

解決方法:

コンピュータを起動すると、サービスはオペレーティング システムに起動ステータスをレポートします。 事前に定義された時間（またはタイムアウト時間）内にサービスがオペレーティング システムにステータスをレポートしない場合、Windows はサービスを停止します。 デフォルトでは、CA ARCserve Central Applications サービスが起動後 30 秒以内に Windows にステータスをレポートしないと、 Windows は CA ARCserve Central Applications データベース サービスを停止します。 十分な空き容量がないサーバにデータベースをインストールすると、このタイプの問題が発生する可能性が高くなります。 ただし、起動のタイムアウト時間を増加させることによりこの問題の発生を防ぐことができます。 タイムアウト時間を増やすには、以下の手順に従います。

1. Windows レジストリ エディタ を開き、以下のキーを探します。
   `HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control`
2. Control を右クリックし、ポップアップ メニューから［新規］-［キー］をポイントします。

   「新しいキー #1」という名前のキーが作成されます。
3. 「新しいキー #1」を「ServicesPipeTimeout」に変更します。
4. ServicesPipeTimeout を右クリックして、コンテキスト メニューの［変更］をクリックします。

   ［DWORD 値の編集］ダイアログ ボックスが表示されます。
5. ［値データ］フィールドに、タイムアウト時間として設定する値を指定します。値の単位はミリ秒です。たとえば、タイムアウト時間を 60 秒に設定する場合は、［値データ］フィールドに「60000」と指定します。

   注: 1 秒は 1000 ミリ秒です。

   ［OK］をクリックします。

   タイムアウト時間が適用されます。
6. Windows に変更を適用するには、コンピュータを再起動します。

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

すべての Windows プラットフォームで有効。

症状:

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

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

解決方法:

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

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

    ```
    net session ¥¥machinename /delete
    ```

  - 以下のディレクトリに移動して、セッションを切断します。

    ```
    Compmgmt.msc > System Tools > Shared Folders > Sessions > Disconnect session
    ```

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

データ同期およびポリシー展開操作が失敗する

Windows プラットフォームで有効

症状:

CA ARCserve D2D データ同期操作が開始した後、以下のメッセージがアクティビティ ログに表示されます。

アプリケーションは CA ARCserve D2D サービスにログインできません。

ポリシーをノードに展開すると、以下のメッセージ ボックスが表示されます。

ポリシーの展開に失敗しました（ノードに接続できませんでした）。

解決方法:

この動作は、CA ARCserve Central Protection Manager サーバに登録された後でノードから CA ARCserve D2D をアンインストールし、その後 CA ARCserve D2D をノード上に手動で再インストールすると発生します。 CA ARCserve Central Protection Manager 展開ユーティリティを使用して CA ARCserve D2D をノードに再インストールする場合、この動作は発生しません。

この動作を解決するには、［ノード］画面でノードを更新します。 ノードを更新するには、ノードをクリックし、コンテキスト メニューの［更新］をクリックします。［ノードの更新］ダイアログ ボックスで必須フィールドに入力します。

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 Protection Manager 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。 ■ 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。
12884901935	*** 上の CA ARCserve Backup サービスに接続できません。エラー番号は 12884901935 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 Backup サービスが実行されていることを確認してください。	CA ARCserve Communication Foundation サービスがノード上で実行されていることを確認してください。

エラー番号	説明	考えられる解決策
12884901936	*** 上の CA ARCserve Backup サービスに接続できません。エラー番号は 12884901936 です。CA ARCserve Central Applications で、ノードにインストールされているバージョンの CA ARCserve Backup がサポートされていることを確認してください。	以下を確認します。 ■ CA ARCserve Central Applications で、ノードにインストールされているバージョンの CA ARCserve Backup がサポートされている。 ■ CA ARCserve Communication サービスがノード上で実行されている。

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。

ローカライズされたサーバからの文字が Nimsoft UMP アラーム コンソールで文字化けして表示される

Windows で有効。

症状:

ローカライズされたサーバから受信したアラート メッセージの文字が Nimsoft Unified Monitoring Portal （UMP） アラーム コンソール内で文字化けしたテキストとして表示されます。

解決方法:

この動作は、アラートを送信しているサーバ上で実行されている文字セットが、Nimsoft サーバ上で実行されている文字セットとは異なる場合に発生します。 これを解決するには、Nimsoft サーバで UTF-8 エンコーディングを使用するよう設定します。 UTF-8 エンコーディングを使用するよう Nimsoft サーバを設定するには、以下の手順に従います。

1. ダッシュボード エンジンでスタートアップ パラメータとして -Dfile.encoding=utf-8 を使用するよう設定されていることを確認します。
2. wasp Extra Java VM 引数オプションが –Dfile.encoding=utf-8 として設定されていることを確認します。

注: 詳細については、Nimsoft のドキュメントを参照してください。