Veritas NetBackup™ 管理者ガイド (高可用性環境)

Windows、UNIX および Linux

リリース 8.2

VERITAS™

Veritas NetBackup™ 管理者ガイド (高可用性環境)

法的通知と登録商標

Veritas、Veritas ロゴ、NetBackup は Veritas Technologies LLC または同社の米国とその他の国における関連会社の商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

この製品には、サードパーティの所有物であることをベリタスが示す必要のあるサードパーティソフトウェア (「サードパーティプログラム」) が含まれている場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このベリタス製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

https://www.veritas.com/about/legal/license-agreements

本書に記載されている製品は、その使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されます。Veritas Technologies LLC からの書面による許可なく本書を複製することはできません。

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC は、本書の提供、内容の実施、また本書の利用によって偶発的あるいは必然的に生じる損害については責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商業用コンピュータソフトウェアと見なされ、場合に応じて、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202、「Commercial Computer Software and Commercial Computer Software Documentation」、その後継規制の規定により制限された権利の対象となります。業務用またはホスト対象サービスとしてベリタスによって提供されている場合でも同様です。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

テクニカルサポートは世界中にサポートセンターを設けています。すべてのサポートサービスは、お客様のサポート契約およびその時点でのエンタープライズテクニカルサポートポリシーに従って提供されます。サポートサービスとテクニカルサポートへの問い合わせ方法については、次の弊社の Web サイトにアクセスしてください。

https://www.veritas.com/support/ja_JP.html

次の URL で Veritas Account の情報を管理できます。

https://my.veritas.com

既存のサポート契約に関する質問については、次に示す地域のサポート契約管理チームに電子メールでお問い合わせください。

世界全域 (日本を除く)	CustomerCare@veritas.com
Japan (日本)	CustomerCare_Japan@veritas.com

マニュアル

マニュアルの最新バージョンがあることを確認してください。各マニュアルには、2 ページに最終更新日付が記載されています。最新のマニュアルは、次のベリタス Web サイトで入手できます。

https://sort.veritas.com/documents

マニュアルに対するご意見

お客様のご意見は弊社の財産です。改善点のご指摘やマニュアルの誤謬脱漏などの報告をお願いします。その際には、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。ご意見は次のアドレスに送信してください。

NB.docs@veritas.com

次のベリタスコミュニティサイトでマニュアルの情報を参照したり、質問することもできます。

http://www.veritas.com/community/ja

ベリタスの Service and Operations Readiness Tools (SORT) の表示

ベリタスの Service and Operations Readiness Tools (SORT) は、時間がかかる管理タスクを自動化および簡素化するための情報とツールを提供する Web サイトです。製品によって異なりますが、SORT はインストールとアップグレードの準備、データセンターにおけるリスクの識別、および運用効率の向上を支援します。SORT がお客様の製品に提供できるサービスとツールについては、次のデータシートを参照してください。

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目次

1

単一障害点に対する NetBackup の保護

この章では以下の項目について説明しています。

コンポーネントのエラーからの保護について

NetBackup はいくつかの異なるコンポーネントで構成されています。それぞれにバックアップ処理かリストア処理を失敗または中断する可能性があります。

表 1-1 に、コンポーネントレベルの障害点と、関連する保護方式を示します。

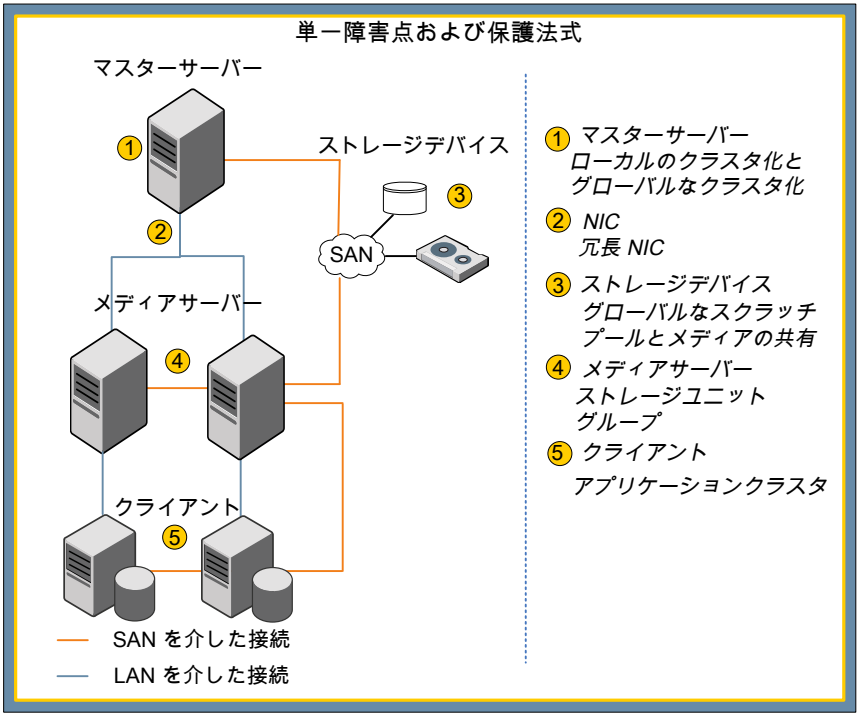
表 1-1　コンポーネントのエラーに対する NetBackup の保護

障害点	保護方式
ネットワークリンク	p.8 の「ネットワークリンクエラーからの保護について」を参照してください。
ストレージデバイスの接続	p.8 の「ストレージデバイスの接続エラーからの保護について」を参照してください。
ストレージデバイス	p.9 の「ストレージデバイスのエラーからの保護について」を参照してください。
メディアの可用性	p.9 の「メディアの可用性エラーからの保護について」を参照してください。

障害点	保護方式
マスターサーバー	p.10 の「マスターサーバーのエラーからの保護について」を参照してください。
メディアサーバー	p.11 の「メディアサーバーのエラーからの保護について」を参照してください。
LAN クライアント	p.14 の「LAN クライアントのエラーからの保護について」を参照してください。
SAN クライアント	p.15 の「SAN クライアントのエラーからの保護について」を参照してください。

図 1-1 は各種 NetBackup コンポーネントと単一障害点を示しています。単一障害点は、コンポーネントの可用性を高くするか、または冗長性を確保するために複数のコンポーネントを配備することによって各コンポーネントレベルで回避できます。

図 1-1　　単一障害点と保護方式



ネットワークリンクエラーからの保護について

バックアップ通信の大半は、それぞれ約 8 MB/秒と 65 MB/秒の転送速度を提供する 100 MB と 1 GB の速度のネットワーク接続を介して転送されます。ネットワークリンクの可用性を高くするには、冗長ネットワークのチーミングを配備します。コストを考慮する必要があるため、多くの場合ネットワークのチーミングはバックアップサーバーとミッションクリティカルなクライアントにのみ制限されます。ミッションクリティカルでないクライアントには単一のネットワーク接続があり、接続エラー (とそれに続くバックアップエラー) のリスクは受け入れられます。

ストレージデバイスの接続エラーからの保護について

ストレージデバイスとそのコントローラへの接続も単一障害点となります。接続エラーの場合、デバイスは使うことができません。

p.8 の「SAN 接続エラーからの保護について」を参照してください。

p.8 の「ロボット制御接続エラーからの保護について」を参照してください。

SAN 接続エラーからの保護について

NetBackup の SAN クライアントはクライアントからメディアサーバーへの SAN 接続もサポートしますが、一般に SAN 接続はバックアップサーバーとバックアップストレージの間に存在します。いずれの場合も、SAN 接続エラーから NetBackup を保護するには、ソースとターゲットのコンポーネント間に冗長な接続を提供するように SAN を構成する必要があります。

ほとんどの SAN 接続されたディスクアレイは冗長な SAN 接続を持ち、動的マルチパス (DMP) ソフトウェアをサポートします。この冗長性によって 1 つのパスが失敗してもストレージへの接続が保持されます。多くの場合、DMP ソフトウェアはまたディスクストレージ間のデータ転送速度を改善するために SAN 接続を介した通信の負荷を分散します。

多くの SAN 接続されたテープデバイスはまた冗長性を確保するために 2 つの接続を提供することによって、2 つの別々のデバイスとしてサーバーに表示されます。マルチパスの選択は動的ではないです。NetBackup は最初に検出した利用可能なパスを選択し、常にそのパスを使います。2 つ目のデバイスパスは最初のパスが壊れている場合にのみ使われます。

ロボット制御接続エラーからの保護について

テープベースのバックアップ環境では、ロボット制御接続は単一障害点となる可能性があります。テープライブラリに指示を送信できない場合は、テープドライブが利用可能でも、バックアップとリストアの操作を行うことはできません。

Sun STK ACSLS、Quantum ATM のようなテープライブラリは、ライブラリから独立しているサーバーで動作する専用の制御ソフトウェアを使います。そのような制御サーバーは

クラスタ化できます。メディアサーバーはライブラリのスロットとドライブ間のテープの移動を処理する制御サーバーに要求を送信します。

他のテープライブラリは制御指示用の NetBackup マスターサーバーからライブラリへのデバイスの直接接続に依存します。このデバイスの接続が失われると、テープライブラリを使うことはできません。SAN 接続されたテープライブラリは、冗長性を確保するためにロボット制御への複数の接続をサポートします。サーバーエラーから保護するようにこれらの接続を構成できます。たとえば、クラスタ化されたマスターサーバーの各ノードに 1 つのパスを構成できます。パスが同時にはアクティブになっていないことを確認してください。パスが両方ともアクティブな場合は、競合する指示が発行され、バックアップエラーかデータ損失という結果になる可能性があります。

ストレージデバイスのエラーからの保護について

テープであろうとディスクであろうと、ストレージデバイスが失敗すると単一障害点であるとみなされます。ストレージデバイスのエラーから保護するには、バックアップターゲットとして複数のデバイスが必要です。

1 つのテープドライブのみにアクセスするメディアサーバーはそのテープドライブが停止するとテープへのバックアップを完了できません。そのようなエラーから NetBackup を保護するには、少なくとも 2 つのテープドライブにアクセスするようにメディアサーバーを構成します。メディアサーバーの間で共有できる SAN 接続されたテープドライブを使います。この共有によって、テープドライブは多数の冗長なデバイスを必要とせずにアクセス可能になります。通常、1 つか 2 つの冗長なドライブは耐性を提供し、バックアップが進行中の間にリストア操作を可能にします。たとえば、5 つのテープドライブを共有するように 4 つのメディアサーバーを構成すると、1 つのドライブが停止してもバックアップはまだ実行できます。バックアップは時間がかかる場合がありますが、完了し、データは安全なままです。メディアサーバーが異なるタイミングでバックアップを実行すると、サーバーに対するテープドライブの比率はバックアップエラーの危険を冒さずにさらに低くなる場合があります。

AdvancedDisk ディスクプールは、単一のディスクデバイスのエラーから保護するために個々のメディアサーバーに作成できます。

メディアの可用性エラーからの保護について

テープベースのバックアップソリューションでは、適切なテープメディアがバックアップジョブに利用可能でなければエラーが発生する場合があります。NetBackup を使うと、グローバルなスクラッチプールとメディア共有によってそのようなエラーのリスクを減らすことができます。

表 1-2 はメディアの可用性エラーに対する保護方式を説明しています。

表 1-2 メディアの可用性エラーに対する NetBackup の保護

保護方式	説明
グローバルなスクラッチプール	テープに書き込まれるすべてのバックアップジョブと複製ジョブでは、バックアップデータと同じ保持基準の特定のメディアプールにあるテープを使います。適切なテープが利用可能でなければ、バックアップは失敗します。 グローバルなスクラッチプールは、オンデマンドで特定のメディアプールに自動的に再割り当てできる未割り当てのテープを保持する NetBackup メディアプールです。たとえば、バックアップジョブまたは複製ジョブが実行され、ジョブによって指定済みのメディアプールで適切なテープが利用可能でないとします。その場合、未割り当てのテープはグローバルなスクラッチプールから指定済みのメディアプールに転送され、バックアップジョブのために使われます。このテープは、期限切れになると、再利用のためにグローバルなスクラッチプールに自動的に戻されます。 グローバルなスクラッチプールを使うと、ジョブによって指定済みのメディアプールに関係なく、すべての未割り当てのテープが任意のバックアップジョブで利用可能になります。
メディアの共有	メディアの共有は部分的に使用されているテープを空きがなくなるまで複数のメディアサーバーで使うことを可能にします。テープを最も効率的に使用します。一度に 1 つのメディアサーバーのみテープに書き込むことができます。そのテープが使用中でないとき、そのメディアプールからのテープを必要とする別のメディアサーバーがそれを使うことができます。 メディア共有を有効にするには、[部分的に使用されているメディアの最大数 (Maximum number of partially full media)]プロパティを使うように[ボリュームプール (Volume Pool)]プロパティを設定してください。このプロパティはメディアプール内の部分的に使用されているテープの数を制限します。すべてのテープの空きがなくなるまで、空きテープをプールに割り当てることはできません。1 つのテープの空きがなくなるまで、別の空きテープをプールに割り当てることはできません。

マスターサーバーのエラーからの保護について

各 NetBackup ドメインの単一のマスターサーバーがドメイン内のすべてのバックアップ処理を制御します。したがって、マスターサーバーはデータ保護環境の最も明らかな単一障害点となります。マスターサーバーなしで、バックアップとリストアを行うことはできません。このようなエラーから NetBackup を保護するには、マスターサーバーの高可用性が必要です。

これらのクラスタテクノロジでの NetBackup のインストールと構成について詳しくは、『NetBackup マスターサーバーのクラスタ化 管理者ガイド』を参照してください。

https://www.veritas.com/support/en_US/article.DOC5332

仮想マシンで動作しているマスターサーバーはハイパーバイザの高可用性ツールを使って保護できます。詳しくは、https://www.veritas.com/support/ja_JP/article.000006177 を参照してください。

メディアサーバーのエラーからの保護について

メディアサーバーは冗長ネットワークとSAN接続で構成できますが、サーバー自身は単一障害点のままとなります。メディアサーバーのエラーに対して NetBackup を保護する方式は使うメディアサーバーの種類によって変わることがあります。

表 1-3 は各種メディアサーバーと保護方式をリストしています。

表 1-3　メディアサーバーの種類と保護方式

メディアサーバーの種類	説明
専用のメディアサーバー	メディアサーバーのソフトウェアのみ実行し、他のシステムから排他的なバックアップを行います。 p.11 の「専用のメディアサーバーのエラーからの保護について」を参照してください。
非専用のメディアサーバー	バックアップを必要する他のアプリケーションも実行します。また他のシステムからのデータもバックアップします。 p.12 の「非専用のメディアサーバーのエラーからの保護について」を参照してください。
SAN メディアサーバー	バックアップを必要する他のアプリケーションも実行します。他のシステムからのデータはバックアップしません。 p.13 の「SAN メディアサーバーのエラーからの保護について」を参照してください。

専用のメディアサーバーのエラーからの保護について

ストレージユニットグループは単一のメディアサーバーのエラーから NetBackup を保護するために使うことができます。ストレージユニットグループはまた複数のメディアサーバーに負荷を分散してバックアップとリストアの最適なパフォーマンスを実現するために使うことができます。

表 1-4 はストレージユニットグループを構成できる各種モードを説明しています。

表 1-4 ストレージユニットグループを構成するためのモード

モード	説明
フェールオーバー	フェールオーバーモードでは、メディアサーバーが停止していないかぎり、最初のストレージユニットが常に使われます。余分なジョブは次のストレージユニットに送信されるのではなく、キューに投入されます。フェールオーバーモードは 2 つのメディアサーバーがアクティブクラスタかパッシブクラスタとして構成されている場合と同様に機能します。
優先	優先モードでは、リストの最初の利用可能なストレージユニットが使われます。このモードでは、ストレージユニットで処理可能な合計数を超えるジョブはリストの次のストレージユニットに送信されます。メディアサーバーが停止している場合は、すべてのバックアップが次のストレージユニットに送信されます。
ラウンドロビン	ラウンドロビンモードでは、各ジョブに対してリストから異なるストレージユニットが周期的に使われます。各ストレージユニットが異なるメディアサーバーにある場合、これは負荷分散のしくみとして機能します。
負荷分散	負荷分散モードは Flexible Disk と Media Manager のストレージユニット形式でのみ動作します。負荷分散モードでは、NetBackup は各メディアで利用可能なアクティビティとリソースの確認を実行します。確認は負荷が最も軽いメディアにバックアップが送信される前に実行されます。

ベストプラクティスとして、優先グループとフェールオーバーグループを使って 2 つのストレージユニットグループを構成するときは 2 つのメディアサーバーを次の通り使います。

- 単一のストレージユニットを持つように各メディアサーバーを構成します。従って、たとえば、ノード A は STU A を持ち、ノード B は STU B を持ちます。
- ストレージユニットを持つ 2 つのストレージユニットグループをそれぞれに固有の順序で構成します。この例では、SUG AB は STU A、その後に STU B を含んでいます。SUG BA は STU B、その後に STU A を含んでいます。
- それから、バックアップポリシーは SUG AB と SUG BA の間で均等に共有されます。

操作の間、バックアップ通信は通常 2 つのノードの間で共有されますが、一方のノードが失敗すると、すべてのバックアップが自動的に他方のノードに移動します。

非専用のメディアサーバーのエラーからの保護について

ストレージユニットグループは非専用のメディアサーバーのエラーから保護するために使うこともできます。ただし、そのような使用法では、特定のメディアサーバーで実行される他のアプリケーションはそのメディアサーバーのエラーから保護されません。非専用のメディアサーバーは、他のアプリケーションをサポートしているクラスタの一部である場合があります。これらのアプリケーションは仮想ストレージユニットを使って保護できます。

SAN メディアサーバーのエラーからの保護について

通常のメディアサーバーとは違って、SAN メディアサーバーは自身のみを保護します。SAN メディアサーバーは通常のメディアサーバーと同様にバックアップストレージに直接接続します。ただし、ネットワークリンクまたは SAN リンクを介して他のクライアントシステムからデータは受信しません。

通常、SAN メディアサーバーは、多くの場合にクラスタ化されている大規模のミッションクリティカルなアプリケーションをサポートするサーバーに配備されます。アプリケーションはクラスタ化されていることがありますが、SAN メディアサーバー自体をクラスタ化する必要はありません。その代わり、クラスタの各メンバーノードに SAN メディアサーバーソフトウェアをインストールし、クラスタで使われる仮想名ごとに NetBackup EMM にアプリケーションクラスタ定義を作成します。その後、メディアサーバーとしてクラスタの仮想名を使ってストレージユニットを作成します。特定の仮想名に関連付けられているアプリケーションは、バックアップ用に同じ仮想名に関連付けられているストレージユニットを使います。

代替メディアサーバーを使ったテープバックアップのリストア

通常、ファイルをリストアするとき、NetBackup では元のバックアップに使ったのと同じメディアサーバーとクライアントを使うことが想定されます。しかし、ディザスタリカバリの場合、別のクライアントにバックアップをリストアするために別のメディアサーバーを使います。ディザスタリカバリサイトのメディアサーバーとクライアントはプライマリサイトのメディアサーバーとクライアントとは異なる名前である可能性が高いです。

NetBackup は、元のメディアサーバーを利用できない場合にリストアを処理するようにリストア用のフェールオーバーメディアサーバーを構成することを可能にします。

リストア用のフェールオーバーメディアサーバーを設定する方法:

- Windows マスターサーバーでは、NetBackup 管理コンソールを使ってリストア用のフェールオーバーメディアサーバーを構成できます。
  [ホストプロパティ (Host Properties)]>[マスターサーバー (Master Server)]>[リストアのフェールオーバー (Restore Failover)]に移動します。
- UNIX と Linux のマスターサーバーでは、`bp.conf` ファイルに FAILOVER_RESTORE_MEDIA_SERVER エントリを作成する必要があります。

代替メディアサーバーを使ったディスクバックアップのリストア

NetBackup は複数のメディアサーバー間でディスクストレージプールを共有できます。デフォルトではリストアの間 NetBackup はジョブの負荷を分散し、バックアップを作成したメディアサーバーではなく、最もビジー状態でないメディアサーバーにリストアを自動的に指示します。ただし、リストアを実行するように選択されたメディアサーバーが SAN メディアサーバーとしてライセンスを取得済みであるか、またはリストアを必要とするクライアントへのネットワークアクセスを持っていない場合は、この処理によって問題が発生する可能性があります。

この問題が発生した場合に利用可能なオプションが 3 つあります。

- 強制リストア用のメディアサーバー設定を次のように構成します。
  - UNIX と Linux のマスターサーバーでは、bp.conf ファイルに FORCE_RESTORE_MEDIA_SERVER エントリを作成します。
  - Windows マスターサーバーでは、NetBackup 管理コンソールでこの設定を定義できます。
    [ホストプロパティ (Host Properties)]>[マスターサーバー (Master Server)]に移動します。
    この設定はサーバーごとに機能します。バックアップを作るために使われるメディアサーバーに基づいて、リストア操作のためにメディアサーバーを指定することを可能にします。バックアップとリストアを行うために同じメディアサーバーが使われるようにするには、バックアップサーバーとリストアサーバーに同じ名前を指定します。
- 次の通り、タッチファイル USE_BACKUP_MEDIA_SERVER_FOR_RESTORE を作成します。
  - UNIX と Linux マスターサーバーでは、/usr/openv/netbackup/db/config にファイルを作成します
  - Windows マスターサーバーでは、<install path>¥veritas¥netbackup¥db¥config にファイルを作成します。
    USE_BACKUP_MEDIA_SERVER_FOR_RESTORE はグローバル設定であり、バックアップをしたサーバーに常に強制的にリストアします。

  メモ: USE_BACKUP_MEDIA_SERVER_FOR_RESTORE タッチファイルが作成されると、すべての FAILOVER_RESTORE_MEDIA_SERVER と FORCE_RESTORE_MEDIA_SERVER の設定は無視されます。

- bprestore -disk_media_server コマンドを使ってコマンドラインからリストアを実行します。この設定はジョブごとに機能します。また特定のリストアジョブに必要となるメディアサーバーを指定することも可能にします。他の 2 つのオプションとは違って、この設定は動的であり、必要に応じて適用できます。

LAN クライアントのエラーからの保護について

NetBackup クライアントパッケージ (アプリケーションエージェントを含む) はクラスタ対応ではないため、NetBackup クライアントとして保護されているクラスタの各ノードで個別にインストールする必要があります。クラスタ化されたアプリケーションをバックアップするときに、バックアップポリシーでクライアント名としてアプリケーションに関連付けられている仮想サーバー名を指定します。これにより、バックアップ操作中にクラスタの正しいノードが確実に選択されます。

SAN クライアントのエラーからの保護について

SAN メディアサーバーと同様に、SAN クライアントもネットワークを介してメディアサーバーにバックアップ通信を送信しません。ただし、ストレージデバイスにバックアップデータを直接送信する SAN メディアサーバーとは異なり、SAN クライアントは SAN 接続を介してリモートメディアサーバーにバックアップデータを送信します。

SAN クライアントは多くの場合クラスタ化されたアプリケーションを保護するために使われます。このように使われた場合に SAN クライアントのエラーから NetBackup を保護するには、SAN クライアントを EMM のアプリケーションクラスタとして構成してください。また、この構成によって、バックアップが開始されるときに、バックアップを制御するメディアサーバーがクラスタのアクティブノードへのファイバートランスポート接続を常に開くようにもなります。

サイトのエラーからの保護について

ローカルのクラスタ化は各サイトにローカルのフェールオーバーを提供します。ただし、これらの構成は地域全体の機能停止を引き起こす大洪水、台風、地震のような大規模な障害に対しての保護は提供しません。クラスタ全体がそのような停止によって影響を受ける可能性があります。そのような状況で、グローバルなクラスタ化か広域のクラスタ化は、かなり離れて位置するリモートクラスタにアプリケーションをマイグレートすることによってデータの可用性を確保します。

グローバルクラスタアーキテクチャは、遠く離れている 2 つ以上のデータセンター、クラスタ、サブネットの配備をサポートします。レプリケートされたマスターサーバークラスタを含んでいるグローバルクラスタは、各サイトでレプリケーションジョブとクラスタを監視し、管理できます。サイトの停止の場合には、レプリケーションロールのセカンダリサイトへのシフトを制御します。重要なアプリケーションを起動し、1 つのクラスタから他にクライアントの通信をリダイレクトします。

自動イメージレプリケーションは NetBackup のドメインの間でレプリケートされるべき個々のディスクベースのバックアップを可能にする NetBackup 機能です。バックアップがターゲットのドメインの NetBackup カタログに自動的に記録されるので、自動イメージレプリケーションを使うとき、複合のカタログリカバリの手順のカタログレプリケーションの必要がありません。詳細については、『NetBackup 管理者ガイド Vol.1』を参照してください。

https://www.veritas.com/support/en_US/article.DOC5332

高可用性環境でのカタログの保護について

NetBackup カタログは、既存のバックアップとバックアップポリシーの両方についての情報 (バックアップ対象、バックアップのタイミング、バックアップ先、バックアップの保持期間など) を含んでいます。したがって、カタログは単一障害点であり、保護する必要があります。RAID ストレージを使うと、ストレージのエラーに対して保護が提供されます。また、

レプリケーションを使ってストレージのエラーとサイトの損失から保護することもできます。カタログの通常のバックアップでは破損と予想外のデータ損失から保護できます。

p.16 の 表 1-5 を参照してください。は NetBackup カタログを保護するための各種の方式を説明しています。

表 1-5　　高可用性環境での NetBackup カタログの保護

保護方式	説明
カタログバックアップ	カタログバックアップはハードウェア障害とデータ破損の両方からマスターサーバーの NetBackup カタログを保護するもので、カタログバックアップは定期的に (理想的には 1 日 1 回以上) 作成する必要があります。カタログバックアップでは、ポリシーに基づくバックアップが行われます。そのため、通常のバックアップポリシーと同様に柔軟にスケジュールを設定できます。ポリシーが増分バックアップを可能にするので、大きいカタログのカタログバックアップ時間をかなり減らすことができます。ただし、リストアの必要があるため、増分バックアップからのリカバリには時間がかかる可能性があります。 テープに書き込まれるカタログバックアップは、カタログバックアップポリュームプールのメディアのみを使います。 詳細については、『NetBackup 管理者ガイド Vol.1』を参照してください。
カタログレプリケーション	カタログレプリケーションはカタログデータベースの複製バージョンを作成し、管理する処理です。カタログレプリケーションはデータベースをコピーし、1 つのレプリカに行われた変更が他のすべてに反映されるように一連のレプリカの同期化を行います。 カタログをディザスタリカバリサイトかセカンダリサイトのスタンバイマスターサーバーにレプリケートすると、ディザスタリカバリサイトでの迅速なカタログリカバリが実現します。継続的なレプリケーションによって、カタログはレプリケーションリンクで可能な最新の状態になります。 **メモ:** レプリケーションはカタログの破損、誤った削除、イメージの期限切れに対しては保護しません。通常のスケジュールカタログバックアップを行ってください。 p.28 の「NetBackup カタログレプリケーションについて」を参照してください。 p.18 の「カタログリカバリについて」を参照してください。

2

カタログバックアップとリカバリを使用したサイトディザスタリカバリについて

この章では以下の項目について説明しています。

ディザスタリカバリパッケージ

セキュリティ向上のため、各カタログがバックアップされる際にディザスタリカバリパッケージが作成されます。ディザスタリカバリパッケージファイルの拡張子は `.drpkg` です。

ディザスタリカバリパッケージには、マスターサーバーホストの識別情報が保存されます。このパッケージは、災害発生後にマスターサーバーの識別情報を NetBackup に再取得させるために必要です。ホストの識別情報をリカバリすると、カタログリカバリを実行できます。

ディザスタリカバリパッケージには、次の情報が含まれます。

- マスターサーバー証明書と NetBackup 認証局 (CA) 証明書の、NetBackup CA が署名した証明書と秘密鍵
- ドメイン内のホストについての情報
- セキュリティ設定
- 外部 CA が署名した証明書
  外部 CA が署名した Windows 証明書ストアからの証明書 (該当する場合)

- 外部 CA が署名した証明書に固有の NetBackup 構成オプション

メモ: カタログバックアップが成功するようにディザスタリカバリパッケージのパスフレーズを設定する必要があります。

カタログリカバリについて

サイトのディザスタリカバリの間に発生する重要な問題は、ディザスタリカバリ (DR) サイトが本番サイトのミラーイメージではないことです。DR 操作を実行するには、本番マスターサーバーからの NetBackup カタログのコピーを必要とします。NetBackup カタログのバックアップとリカバリ処理は、サイトの損失よりもむしろカタログストレージかマスターサーバーのエラーからのリカバリのために主に使用されます。デフォルトの状況では、NetBackup は EMM データベースを含む完全なカタログをリストアします。EMM データベースはメディアサーバー、バックアップデバイス、ストレージユニットの詳細を含んでいます。マスターサーバーはバックアップとリストアを指示するためにこの情報を使います。マスターサーバーはまたバックアップデバイスの状態を設定するためにメディアサーバーに問い合わせる場合にこの情報を使います。これらのメディアサーバーを含んでいない DR 環境では、マスターサーバーのパフォーマンスに影響が及ぶ可能性があります。また、ポーリング操作が接続に失敗し、タイムアウトになるため、リストア操作を実行する機能に影響が及ぶ可能性もあります。

メモ: クラスタの設定で、ホストとの通信に外部 CA が署名した証明書を使用する場合、仮想名とクラスタノードで認証局 (CA) の使用状況が同じであることを確認します。たとえば、ノードで外部 CA が署名した証明書のみを使用している場合、仮想名でも外部 CA が署名した証明書を使用していることを確認します。仮想名とクラスタノードの CA の使用方法に不一致がある場合は、カタログバックアップとカタログリカバリが失敗する可能性があります。

メディアサーバーとクライアントの配置が主要本番サイトと異なる DR サイトで NetBackup 環境をリカバリするには、次の方法を使ってください。両方の方法に利点と欠点があります。

- 完全カタログリカバリの方法では、カタログ全体がリカバリされます。その後、不要な構成要素を削除するか、または無効にできます。
  p.19 の「完全カタログリカバリについて」を参照してください。
- 部分的なカタログリカバリでは、EMM データベースと BMR データベースはリストアされません。
  p.23 の「部分的なカタログリカバリについて」を参照してください。

リカバリの最も適切な方法は DR 機能の性質と本番機能との類似程度によって判断できます。

ディザスタリカバリ計画を作成する場合は、次のセクションで説明する方法に沿っていることを確認してください。

- p.35 の「クロスドメインレプリケーションのディザスタリカバリドメインの計画」を参照してください。
- p.20 の「完全カタログリストアの実行」を参照してください。
- p.24 の「部分的なカタログリストアの実行」を参照してください。

完全カタログリカバリについて

完全カタログリカバリは、本番サイトでデータの破損またはストレージの損失が発生した場合にカタログをリカバリするために主に使われます。完全カタログリカバリは単一ドメイン構成に推奨されます。完全カタログリカバリは本番サイトで使われる名前と同じ名前のメディアサーバーが DR サイトに同じ数ある場合に使われます。

完全カタログリカバリには部分的なカタログリカバリと比較して次の利点があります。

- ストレージユニット定義、メディアの割り当て、履歴を含んでいるリレーショナルデータベースのコンポーネントをリストアします。
- メディアプールと他の割り当て情報を含むプライマリサイトからのテープ情報を保有します。
- BMR データをリストアします。
- 本番サイトで使われるのと同じポリシーとテープを使って DR サイトでのバックアップの実行を可能にします。

完全カタログリカバリには、次の制限事項があります。

- カタログリカバリではホスト証明書はリカバリされません。NetBackup マスターサーバー ID またはホスト証明書とその他の情報をリカバリするには、ディザスタリカバリパッケージをリカバリする必要があります。
  p.17 の「ディザスタリカバリパッケージ」を参照してください。
- リレーショナルデータベースのコンポーネントをリカバリすると、リカバリ前に DR サイトで設定されたデバイス構成とサーバー構成が失われます。リカバリ後に再度設定してください。リレーショナルデータベースに存在する、本番サーバーとデバイスについての情報は DR サイトに存在しないことがあります。DR 環境で円滑に操作を行うには、これらのサーバーエントリを無効にし、それらと関連付けられているデバイスを削除する必要があります。
- 完全カタログリカバリはリレーショナルデータベースのデバイス構成とサーバー構成を上書きします。カタログがリストアされた後、DR のドメインサーバーとデバイスの構成を再検出してください。

完全カタログリストアの実行

完全カタログリカバリでは、カタログバックアップ全体が DR マスターサーバーにリカバリされます。DR 環境に存在しないメディアサーバーは不必要なプールを避けるために無効にされます。DR サイトのデバイス構成が本番サイトと異なる可能性があるため、すべてのデバイスレコードが削除されます。EMM データベースを更新するためにデバイスの検出が実行されます。リストアを開始する前に次の手順を実行してください。また、DR 計画の手順を文書化してください。

完全カタログリストアを準備する方法

1. UNIX と Linux マスターサーバーで、`bp.conf` と `vm.conf` ファイルのコピーを作成します。
2. カタログ全体をリカバリする `bprecover` コマンドを実行します。

メモ: DR マスターサーバーには本番マスターサーバーと同じ名前とトポロジーがなければなりません。本番マスターサーバーがクラスタの場合は、DR マスターサーバーもクラスタである必要があります。メンバーノードの数とノードの名前は異なる可能性があります。

メモ: 別のメディアサーバーで作成されたカタログバックアップが使われる場合は、同じ名前のメディアサーバーがカタログリカバリに必要になります。

---

3. `bprecover` コマンドを実行した後、後続のカタログバックアップが成功するように、ディザスタリカバリパッケージのパスフレーズを設定します。

   p.17 の「ディザスタリカバリパッケージ」を参照してください。

4. カタログリカバリ時に、クラスタノードのセキュリティ証明書はリカバリされません。仮想名の証明書のみがリカバリされます。

ホストの通信に NetBackup 証明書を使用する場合	ホストで正常に通信するには、災害後にすべてのクラスタノードに NetBackup 証明書 (ホスト名ベースの証明書とホスト ID ベースの証明書) を配備する必要があります。 詳しくは、『NetBackup セキュリティおよび暗号化ガイド』で「ディザスタリカバリインストール後にクラスタマスターサーバーで証明書を生成する」の章を参照してください。
ホストの通信に外部証明書を使用する場合	ホストと正常に通信するには、災害後に外部証明書を使用するようにすべてのクラスタノードを構成する必要があります。 詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

5 ドメイン内のすべてのホストでホワイトリストのキャッシュをクリアし、サービスを再起動します。

6 バックアップが自動的に開始されないようにすべてのバックアップポリシーを無効にします。

- NetBackup 管理コンソールを使ってこれを手動でできます。
- または、`bpplinfo <policy> -modify -inactive` CLI を実行します。

7 NetBackup を停止します。

8 UNIX と Linux のマスターサーバーで、カタログバックアップからリストアされた `bp.conf` と `vm.conf` ファイルを手順 1 で作成したコピーと置き換えます。

9 新しいマスターサーバーで NetBackup Relational Database Manager、NetBackup PBX、EMM サービスを起動します。

- UNIX と Linux マスターサーバーで、次のコマンドを実行します。
  - `/usr/openv/netbackup/bin/nbdbms_start_stop start`
  - `start /opt/VRTSpbx/bin/pbx_exchange`
  - `/usr/openv/netbackup/bin/nbemm`
- Windows マスターサーバーで、次の Windows サービスを起動します。
  - NetBackup Relational Database Manager
  - Veritas Private Branch Exchange
  - NetBackup Enterprise Media Manager

メモ: NetBackup コマンドは PBX の停止と起動を行わないため、PBX 処理はすでに動作していることがあります。

NetBackup Relational Database Manager サービスについて詳しくは、『NetBackup トラブルシューティングガイド』を参照してください。

10 DR 環境の一部ではないメディアサーバーを無効にします。次のコマンドを実行します。

```
nbemmcmd -updatehost -machinename <Media Server> -machinestateop
set_admin_pause -machinetype media -masterserver <Master Server>
```

11 EMM データベースからすべてのテープデバイスを削除します。次のコマンドを実行します。

```
nbemmcmd -deletealldevices -allrecords
```

12 環境内に NAT クライアントがある場合、この手順が必要です。

NetBackup Messaging Broker (または nbmqbroker) サービスを構成した場合、カタログのリストア後に、configureMQ -enableCluster コマンドを使用してクラスタでサービスの監視を有効にする必要があります。

コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

13 NetBackup を再起動します。

14 デバイスの構成ウィザードを使って、新しいテープドライブとライブラリの構成を作成します。

15 バーコードマスキング規則が手順 9 で使われた場合は、同じ規則がここに設定されていることを確認します。必要に応じて、それらを追加します。

16 NetBackup 管理コンソールを使ってすべてのリカバリメディアが非ロボットに設定されているかどうかを確認します。

17
- 非ロボットに設定される必要のあるリカバリメディアがまだある場合、次の操作を実行します。
- ロボットメディアを選択し、右クリックして[移動 (Move)]を選択します。
- [ロボット (robot)]フィールドを[スタンドアロン (Standalone)]に変更します。
- [OK]をクリックして、変更を保存します。

18 すべてのリカバリメディアが非ロボットに設定されたら、[すべてのテープライブラリのインベントリの実行 (Inventory all the tape libraries)]フィールドでメディアが正しいライブラリで識別されていることを確認します。

これで本番データセンターにバックアップされているクライアントデータのリストア操作とリカバリ操作を開始できます。

NetBackup Web サーバー用に外部 CA が署名した証明書を構成した場合は、アクティブノードで configureWebServerCerts コマンドを実行して、フェールオーバー後に確実に外部証明書が使用されるようにします。

コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

すべてのクラスタノードで、次の操作を行います。

- ノードの構成ファイルで、外部証明書構成オプション (ECA_CERT_PATH、ECA_CRL_PATH など) を定義します。
- ノードで nbcertcmd -enrollCertificate を実行します。
  詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

完全カタログリストア後の DR 環境の一貫性の保持

本番サイトで重要なインシデントが発生した場合は、基本的なリカバリが完了した後しばらくしてから DR サイトから操作してください。DR 環境が操作可能になったら、DR 環境の一貫性を保持するために次の追加のタスクを必要に応じて実行できます。

DR 環境の一貫性を保持する方法

1. DR パッケージリカバリ後すぐにカタログリカバリが実行されない場合は、DR 環境の一貫性を保持するため、次の操作を行います。
   - NetBackup CA が署名した証明書がホストの通信に使用されている場合は、すべてのノードで次のコマンドを実行します。
     - nbcertcmd -getcacertificate
     - nbcertcmd -getcertificate
   - 外部 CA が署名した証明書がホストの通信に使用されている場合は、すべてのノードの外部証明書の構成オプションが正しく定義されているかどうかを確認し、すべてのノードで次のコマンドを実行します。
     - nbcertcmd -enrollCertificate
2. DR サイトで利用可能なストレージユニットを使うように、カタログバックアップポリシーを含むバックアップポリシーを修正し、有効にします。
3. 不要になったバックアップポリシーを削除します。
4. メディアサーバーに関連付けられており、DR 環境の一部ではないストレージユニットを削除します。
5. 削除したストレージユニットを使うストレージライフサイクルポリシーを修正します。

部分的なカタログリカバリについて

部分的なカタログリカバリは複数ドメイン構成に推奨されます。部分的なカタログリカバリは、少数のメディアサーバー、様々なライブラリ形式などを含む本番サイトとは異なるサーバーレイアウトの DR サイトに使われます。部分的なカタログリカバリは、インポートなしのリカバリ方式の 1 つです。同じ多数の制約の影響を受けます。詳しくは、次のリンクを参照してください。

部分的なカタログリカバリは、フラットファイルコンポーネントのみをリカバリし、リレーショナルデータベースはリカバリしません。従って、DR サイトの既存のインフラストラクチャ (サーバー、デバイス等) の詳細はリカバリ処理の間に失われません。また、バックアップと関連付けられているメディアサーバー情報がリカバリされないことも意味します。メディアサーバーは、データベースに手動で加えられなければならず割り当てられていません。誤って上書きされることがないプールにメディアサーバーが配置されていることを確認してください。

部分的なカタログリカバリには完全カタログリカバリと比較して次の利点があります。

- 構成の要素を削除または再検出する必要がありません。リカバリ処理は DR 環境の一般的な構成には影響しません。
- サーバートポロジーには影響しません。DR サイトのマスターサーバートポロジーは本番サイトのトポロジーを反映する必要はありません。従って、クラスタ化されたマスターサーバーからのカタログバックアップを DR サイトのスタンドアロンマスターサーバーにリストアできます。
- 2 つの環境で使われるクライアント名、バックアップポリシー名、テープラベルの範囲が一意の場合、DR サイトは本番サイトにできます。また、別の本番バックアップドメインに部分的なリカバリを実行することも可能です。

部分的なカタログリカバリでは、DR サイトでプライマリサイトからのテープ情報をリカバリできません。テープが誤って上書きされていないことを確認してください。これらのテープは DR サイトでのバックアップのために簡単に使われてはなりません。

部分的なカタログリストアの実行

部分的なカタログの方法では、テープを特定のメディアプールに割り当て済みにすることや配置することはリストア操作に必要ないと想定しています。テープが EMM に存在し、NetBackup がリストアのためにテープをマウントし、読み込むことができることも想定されています。次の手順はリストアを開始する前に実行する必要があります。

部分的なカタログリストアを準備する方法

1. UNIX と Linux のマスターサーバーで、`bp.conf` と `vm.conf` ファイルのコピーを作成します。
2. NetBackup のカタログイメージと構成ファイルのみをリカバリします。
   - NetBackup 管理コンソールを使用した場合は、メッセージが表示されたら[部分的カタログリカバリ (Partial catalog recovery)]オプションを選択します。
   - または `bprecover -wizard` コマンドを実行します。

メモ: DR マスターサーバーの名前は本番マスターサーバーの名前と同じでなければなりません。

メモ: 別のメディアサーバーで作成されたカタログバックアップが使われる場合は、同じ名前のメディアサーバーがカタログリカバリに必要になります。

---

3. レプリケートされたリレーショナルデータベースバックアップからメタデータをエクスポートするには、`cat_export -all -staging` を実行します。

4 アクティブなリレーショナルデータベースに、エクスポートされたメタデータをインポートするには、コマンド `cat_import -all` を実行します。または、マスターサーバープラットフォームに応じて bp.conf ファイルまたはレジストリでパラメータ LIST_FS_IMAGE_HEADERS を YES に設定します。これにより、次のカタログのクリーンアップジョブで、エクスポートされたメタデータが自動的にインポートされます。

5 バックアップが自動的に開始されないようにすべてのバックアップポリシーを無効にします。

- NetBackup 管理コンソールを使ってこれを手動でできます。
- または、`bpplinfo <policy> -modify -inactive` CLI を実行します。

6 NetBackup を停止します。

7 UNIX と Linux のマスターサーバーで、カタログバックアップからリストアされた `bp.conf` と `vm.conf` ファイルを手順 1 で作成したコピーと置き換えます。

8 NetBackup を起動します。

9 テープが非スクラッチメディアプールに確実に追加されるようにすべてのテープライブラリをインベントリ処理します。このプールは有効なバックアップポリシーによってテープが後で誤って上書きされることを防ぎます。

これで本番データセンターにバックアップされているクライアントデータのリストア操作とリカバリ操作を開始できます。

部分的なカタログリストア後の DR 環境の一貫性の保持

本番サイトで重要なインシデントが発生した場合は、基本的なリカバリが完了した後しばらくしてから DR サイトから操作してください。DR 環境が操作可能になったら、DR 環境の一貫性を保持するために次の追加のタスクを必要に応じて実行できます。

DR 環境の一貫性を保持する方法

1 バックアップポリシーと、DR サイトで必要なカタログバックアップポリシーを修正し、有効にします。

2 もはや必要でないポリシーを削除します。

DR ドメインのディスクリカバリについて

OpenStorage と他の AdvancedDisk 形式の導入によって、重複排除ディスクはバックアップストレージメディアとしてテープストレージより優先されます。ディスクストレージを使って、セカンダリの場所の別のディスクデバイスにディスクデバイスの内容をレプリケートできます。このレプリケーションによってディザスタリカバリサイトに物理的なバックアップメディアをトランスポートする必要がなくなります。

単一ドメインレプリケーションの DR 環境でのディスクリカバリ

NetBackup の同じドメイン内のバックアップを複製するとき、重複を排除するディスクのレプリケーションを最適化するためにストレージライフサイクルポリシーを使うことができます。これは本番サイトと同じマスターサーバーによって制御されるディザスタリカバリサイトでバックアップイメージの複製コピーを作成する効率的な方法です。ただし、最適化された重複排除は単一ドメインレプリケーションでのみ有効です。

自動イメージレプリケーション

自動イメージレプリケーションでは、別のドメインにバックアップを複製するという概念が拡張されており、DR ドメインに個々のバックアップコピーを送信できます。自動イメージレプリケーションを使って作成されたバックアップコピーは DR ドメインで自動的にカタログ化されるため、DR ドメイン内で追加のリカバリ手順を実行する必要はありません。自動イメージレプリケーションについて詳しくは、『NetBackup 管理者ガイド Vol.1』を参照してください。

クロスドメインレプリケーションの DR 環境でのディスクリカバリ

使われるディスク技術が自動イメージレプリケーションをサポートしない場合の代替手法としては、単にストレージ全体をレプリケートしてから、カタログリカバリと nbcatsync ユーティリティの組み合わせを使ってディザスタリカバリの場所でカタログを入力します。

nbcatsync ユーティリティは EMM データベースとイメージデータベースのメタデータコンポーネントに記録されたディスクメディア ID が異なっていてもレプリケーションを実行しやすくします。nbcatsync ユーティリティはディザスタリカバリドメインの EMM データベースのメディア ID とイメージデータベースのメタデータのディスクメディア ID を合わせます。本番サイトで行われる通常のバックアップとカタログバックアップはレプリケートするディスクストレージに書き込まれます。カタログバックアップのディザスタリカバリファイルはディザスタリカバリドメインに送信されます。

nbcatsync ユーティリティはすべてのマスターサーバープラットフォームでサポートされています。NetBackup によってサポートされるすべての Advanced Disk 形式で使うことができます。

障害が発生した場合にクロスドメインレプリケーション環境でディスクをリカバリするには、DR ドメインのマスターサーバーで次の手順を実行します。

1. DR ドメインの EMM データベースのディスクメディア ID 情報とカタログバックアップの DR ファイルのディスクメディア ID 情報を合わせます。そのために、次のコマンドを実行します。

   ```
   nbcatsync -sync_dr_file <DR file name>
   ```

2. 次のコマンドを実行して、レプリケートされたカタログバックアップから部分的なカタログリカバリを実行します。

   ```
   bprecover -wizard
   ```

3. レプリケートされたリレーショナルデータベースバックアップからメタデータをエクスポートするには、コマンド `cat_export -all -staging` を実行します。

4. アクティブなリレーショナルデータベースに、エクスポートされたメタデータをインポートするには、コマンド `cat_import -all` を実行します。

5. 部分的なカタログリカバリによってリカバリされたイメージレコードと関連付けられているディスクメディア ID を DR ドメインに存在するディスクメディア ID と合わせます。そのために、次のコマンドを実行します。

   ```
   nbcatsync -backupid <restored catalog backup ID>
   ```

3

自動イメージとカタログレプリケーションによるサイトの損失保護について

この章では以下の項目について説明しています。

- 自動イメージレプリケーション (AIR) について
- NetBackup カタログレプリケーションについて

自動イメージレプリケーション (AIR) について

自動イメージレプリケーション機能は NetBackup ドメイン間でのバックアップの複製を可能にし、バックアップの複製時にターゲットドメインにカタログエントリを自動的に作成します。ベリタスは、ディザスタリカバリサイトで NetBackup カタログを入力する手段としてライブカタログレプリケーションではなく自動イメージレプリケーションを使うことを推奨します。自動イメージレプリケーションについて詳しくは、『NetBackup 管理者ガイド』の関連するセクションを参照してください。このマニュアルでは、ネットワーク環境が自動イメージレプリケーションの使用に適さない場合にカタログデータをレプリケートするための代替手法について説明しています。

NetBackup カタログレプリケーションについて

NetBackup のデータ保護戦略を決定するには、DR サイトを同じ NetBackup ドメインの一部にするか、または別の NetBackup ドメインにするかを決定する必要があります。

NetBackup は次のようなカタログレプリケーションを使って構成できます。

- 複数サイト単一ドメインレプリケーション
  p.31 の「複数サイト単一ドメインレプリケーションについて」を参照してください。

- 複数サイトクロスドメインレプリケーション
p.34 の「複数サイトクロスドメインレプリケーションについて」を参照してください。

レプリケートされた NetBackup カタログのサポートの条件について

レプリケーション用に準備された NetBackup 環境であれば、他の NetBackup サーバーと同様にサポートされます。レプリケートされたカタログボリュームが失敗し、適度な時間内で回復不能な場合、NetBackup サポートの推奨事項は、レプリケートされないカタログの回復不能なディスクエラーの場合の推奨事項と同じです。プライマリマスターサーバー上の最新の利用可能なカタログバックアップからカタログをリストアする必要があります。

メモ: データはいずれのデータレプリケーションソリューションでも失われる場合があります。NetBackup カタログを保護するには、レプリケーションテクノロジに失敗リスクがあるため、レプリケーションテクノロジのみに頼ってはなりません。NetBackup プライマリサーバーのデータが、ホットスタンバイ状態の NetBackup セカンダリサーバーへ複製したことが原因で壊れることがあります。したがって、頻繁に NetBackup サーバーカタログをバックアップしてください。

警告: レプリケーションはアプリケーションパフォーマンスに悪影響を及ぼすことがあります。NetBackup カタログへの変更をコミットする追加の時間が必要になるので、全体的なバックアップ時間に影響することがあります。自己の責任においてレプリケーションを使用してください。ベリタスには、正しくレプリケーションソリューションをインストールし、構成し、監視しなかった場合の、いかなるレプリケーションエラーについても責任はありません。

NetBackup カタログのレプリケーションのサポート条件は次の通りです。

- 使用されるレプリケーションテクノロジは、一貫性があり、書き込み順になっているデータのコピーを常に保持する必要があります。
- 非同期レプリケーションテクノロジの使用は、書き込み順序の忠実性が維持できれば、許可されます。
- 時間ごとのスナップショットなど、スケジュールされたレプリケーションテクノロジの使用はサポートされません。
- NetBackup マスターサーバーは、単一のエンティティとして制御される仮想サーバーと同じ仮想サーバー上に設置する必要があります。
- プライマリマスターサーバーとセカンダリマスターサーバーは類似の形式、仕様、オペレーティングシステムであり、同じ仮想ホスト名を使用する必要があります。
- セカンダリマスターサーバーは、プライマリマスターサーバーと同じドメインにあっても別のドメインにあっても、NetBackup の他のどの機能も持ってはなりません。たとえ

ば、マスターサーバーとして使わない場合に、メディアサーバーとしてセカンダリマスターサーバーを使うことはできません。また、NetBackup の別のドメインのマスターサーバーとして使うこともできません。カタログはレプリケートされますが、結合できません。

- サーバーの物理ホスト名と IP アドレスとは別の NetBackup マスターサーバーの仮想ホスト名と IP アドレスを使うには、クラスタ環境と非クラスタ環境の両方を構成してください。別の仮想ホスト名と IP アドレスは、DNS ルーティングによってアクティブマスターサーバーノードを制御することを可能にします。また、それはプライマリマスターサーバーとセカンダリマスターサーバーがドメインで同時にアクティブになることを防ぎます。クラスタ環境の場合、この要件はクラスタ構成によって自動的に満たされます。非クラスタ環境の場合、仮想ホスト名をインストール中に指定する必要があります。
- プライマリマスターサーバーとセカンダリマスターサーバーが同じバージョンの NetBackup とそのコンポーネントを使用していることを確認してください。オペレーティングシステム、NetBackup のバイナリ、EEB、そしてこれらのパス以外に存在するファイルが複製対象に指定されていることを確認してください。
- クラスタ化されたマスターサーバーとクラスタ化されていないマスターサーバー間のレプリケーションは可能ではありません。サーバーのペアはクラスタ化されるか、またはクラスタ化されないかのいずれかである必要があります。
- NetBackup カタログのマウントポイントはプライマリサイトとセカンダリサイトの両方で同じである必要があります。
- カタログデータのみがサーバー間でレプリケートされ、レプリケーション用の単一のボリュームかボリュームセットの同じ場所にすべて配置される必要があります。クラスタ化されたマスターサーバーの場合、クラスタの共通ボリュームがレプリケートされます。クラスタ化されていないマスターサーバーの場合、レプリケーション用にボリュームセットにリンクする必要があるパスについて詳しくは、次を参照してください。
- 仮想名か DNS エイリアスがプライマリホストとセカンダリホスト両方に同時に解決されないことを確認してください。
- カタログレプリケーションはカタログバックアップの要件を排除しません。イメージの不慮の期限切れ、またはプライマリサイトのカタログに発生し、セカンダリサイトにレプリケートされる他の不整合から保護するために、プライマリマスターサーバーから NetBackup カタログを定期的にバックアップしてください。
- カタログが (プライマリドメインのメディアサーバーにアクセスできるセカンダリサーバーへよりもむしろ) NetBackup ドメイン間でレプリケートされる場合、テープに書き込まれるバックアップとレプリケート済み BasicDisk ストレージのみがディザスタリカバリのドメインにリストアできます。
- セカンダリマスターサーバーへのカタログのレプリケーションは、プライマリマスターサーバーの短期間の停止の間にデータをリストアすることを可能にします。クロスドメインのレプリケーション構成では、フェールオーバー後にバックアップを実行できることを確認してください。カタログはデータを損失することなく、後日フェールオーバー

でプライマリサーバーに戻せる必要があります。延長された停止時間に DR サイトでバックアップを作成し、DR サイトで作成されるバックアップについての情報を失うことなくプライマリサイトに戻ることを計画する場合は、このサポート条件を考慮してください。

- NetBackup がセカンダリサイトのレプリケートされたコピーを使用している場合は確認してください。このような使用はサポートの要件ではありません。
- カタログとバックアップイメージは両方セカンダリサイトでアクセス可能である必要があります。
  ユーザーは、バックアップイメージの有効なコピーの可用性に関連する手順に対処する必要があります。また、ユーザーはセカンダリサイトでイメージからリストアするように NetBackup サーバーを有効にするための手順を定義する必要があります。この文書ではこれらの手順に対処しません。
- ユーザーはデータレプリケーションソリューションのインストール、構成、監視を行います。ユーザーは、一貫性があり、書き込み順になっている NetBackup カタログボリュームのコピーをレプリケーションテクノロジが継続的に保持していることを確認する必要があります。
- Microsoft 社の分散ファイルシステムレプリケーション (DFSR) テクノロジは、レプリケート対象ファイルの書き込み順の一貫性を保証しないため、サポートされません。
  詳しくは、https://www.veritas.com/support/en_US/article.100043283 を参照してください。

カタログの同期について

レプリケーションは、サイト間のテープの移動と比較すると、ほぼ瞬時の処理です。DR ドメインで示されるレプリケーションカタログデータは、先に本番ドメインから振り分けられ DR ドメインで利用可能な在庫テープよりも新しい場合があります。リストア操作中は、テープがリストア用に本番ドメインから振り分けられる前に作成されるバックアップのみを選択してください。

複数サイト単一ドメインレプリケーションについて

複数サイト単一ドメインは両方のサイトのクライアントサーバーとメディアサーバーが共通のマスターサーバーの制御の下にある場合に使われます。どちらのサーバーも同じドメインの一部を成すため、同じメディアサーバーとクライアントを認識し、よって NetBackup カタログはセカンダリマスターサーバーで全面的に有効となります。

複数サイト単一ドメインモデルでは、NetBackup カタログはサイト間でレプリケートされます。プライマリサイトで問題が発生した場合に、マスターサーバーはセカンダリサイトのスタンバイノードにフェールオーバーされます。バックアップは両方のサイトに (構成に応じてインラインコピーか複製のいずれかによって) 作成されます。従って、単一サイトの損失は本当の災害ではなく、いくつかのアプリケーションサーバーの損失を意味します。バックアップドメインが両方のサイトにまたがるため、単一サイトの損失の結果、バックアップ環

境が破壊されるのではなく、バックアップおよびリストア機能が減少します。複数サイト単一ドメインモデルはマスターサーバーのクラスタ化とストレージのレプリケーションを組み合わせて使います。この組み合わせによりマスターサーバーをセカンダリの場所に簡単にすばやく再配置できます。

複数サイト単一ドメインモデルは次の方法で構成できます。

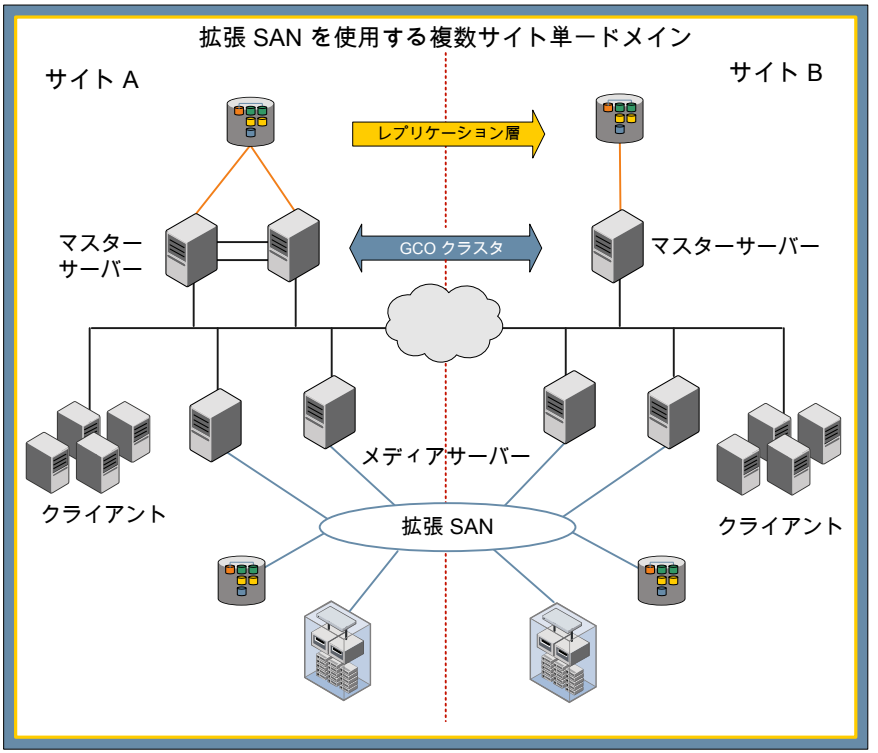
- 拡張 SAN を使用する複数サイト単一ドメイン
  p.32 の「拡張 SAN を使用する複数サイト単一ドメインについて」を参照してください。
- 最適化複製を使用する複数サイト単一ドメイン
  p.33 の「最適化複製を使用する複数サイト単一ドメインについて」を参照してください。

拡張 SAN を使用する複数サイト単一ドメインについて

拡張 SAN を使用する複数サイト単一ドメインを構成するには、各サイトのメディアサーバーが両方のサイトのバックアップデバイスに SAN アクセスするように構成する必要があります。このアクセスにより、メディアサーバーはサイト間でバックアップを書き込み、複製できます。この構成は、サイト間が 50 マイルまでの間隔ではよく機能しますが、間隔と遅延が増加するにつれて効果は低下します。

図 3-1 に、レプリケートされたグローバルクラスタが拡張 SAN を使用する複数サイト単一ドメインでどのように構成されるかを示します。

図 3-1 拡張 SAN を使用する複数サイト単一ドメイン

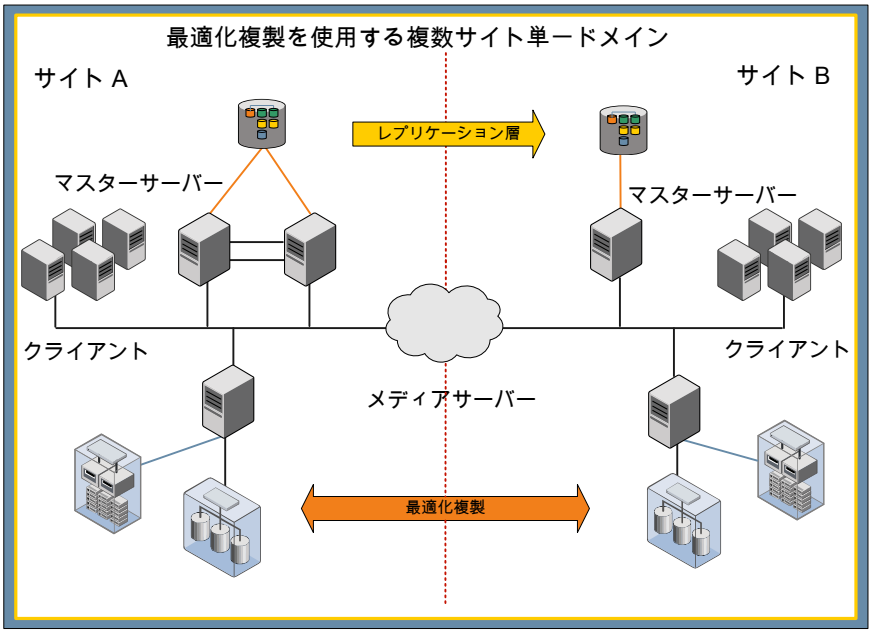


最適化複製を使用する複数サイト単一ドメインについて

最適化複製を使用する複数サイト単一ドメインを構成するには、拡張 SAN を、最適化複製を実行する OpenStorage デバイス間の接続に置き換える必要があります。この構成では、より小さいデータボリュームがサイト間で交換されるので地理的な距離を大きくすることができます。ストレージライフサイクルポリシーの階層的な複製機能を使って、1 つのサイトで OpenStorage デバイスのバックアップを作成することが可能です。それからそれらを他のサイトの OpenStorage デバイスに複製し、最終的に複製コピーを長期保存用テープに複製します。

図 3-2 に、レプリケートされたグローバルクラスタが最適化複製を使用する複数サイト単一ドメインでどのように構成されるかを示します。

図 3-2　最適化複製を使用する複数サイト単一ドメイン



複数サイトクロスドメインレプリケーションについて

複数サイトでドメインを超えての複製は、DR サイトが本番ドメインとは別の NetBackup ドメインである場合に使われます。DR サイトには様々なメディアサーバーとデバイスがあります。

複数サイトクロスドメインレプリケーションはテープと BasicDisk ストレージ用にのみサポートされます。AdvancedDisk 形式には特定のメディアサーバーまたはデバイスの構成要件があり、これらの構成要件では、ディザスタリカバリドメインで AdvancedDisk 形式にアクセスできません。

複数サイトクロスドメインと BasicDisk ストレージについて

ドメイン間のステージングされていない BasicDisk ストレージで保存されるイメージをレプリケートできます。レプリケーション先は DR ドメインのメディアサーバーの同じマウントポイントに対してマウントする必要があります。また、正しいメディアサーバーが選択されていることを確認するために FAILOVER_RESTORE_MEDIA_SERVER パラメータを設定してください。たとえば、本番ドメインのメディアサーバー prdmed1 のマウントポイント /BD1 を使って BasicDisk ストレージユニットを DR ドメインにレプリケートできます。DR マスターサーバーの `bp.conf` ファイルが FAILOVER_RESTORE_MEDIA_SERVER = prdmed1 drmed1 を設定するように編集される場合、/BD1 はメディアサーバー drmed1

でマウントできます。ステージングストレージユニットとして機能せず、ステージングストレージユニットまたは他のディスク形式でサポートされない BasicDisk ストレージユニットの場合にのみこの設定が可能です。

クロスドメインレプリケーションのディザスタリカバリドメインの計画

DR ドメインのセカンダリマスターサーバーでカタログのレプリケーションデータを使うには、マスターサーバー、メディアサーバー、ネットワーク接続、NetBackup ソフトウェアが機能していることを確認します。

ベリタスは、特に DR ドメインが通常どおり構成されていない場合に DR 構成手順を文書化することを推奨します。このマニュアルは、ドメインが専門の DR サービス会社が提供する施設である場合に非常に重要です。次のディザスタリカバリ計画の準備手順を参照してください。

クロスドメインレプリケーションのディザスタリカバリドメインの計画

1. 本番ドメインで使用する DR ドメインのマスターサーバー、メディアサーバー、クライアントに NetBackup の同じバージョンをインストールします。

   メモ: 本番ドメインに古いバージョンの NetBackup があるメディアサーバーが存在する場合、DR ドメインのメディアサーバーに古いバージョンをインストールしないでください。DR ドメインのマスターサーバーとメディアサーバーには同じバージョンを使ってください。

   完全カタログレプリケーション方式が使われ、本番ドメインのマスターサーバーがクラスタ化されている場合、クラスタ化されたマスターサーバーも DR ドメインに存在する必要があります。クラスタのメンバーノードは、本番ドメインのノードと同じである必要はありません。部分的なカタログレプリケーション方式が使われる場合、DR ドメインのクラスタ化されたマスターサーバーは必要になりません。

2. テストバックアップポリシーを使って、クライアントとサーバー間のネットワークの接続と認証をテストします。テストの後でポリシーを無効にします。
3. テープドライブとライブラリはメディアサーバーに接続する必要があります。DR ドメインで使われるテープドライブは本番ドメインからのテープと読み込み互換性がある必要があります。これらは NetBackup の同じメディア形式として構成する必要があります。
4. DR ドメインのメディアサーバーを使ってバックアップをリストアできるように本番ドメインのメディアサーバーへのバックアップの書き込みを許可するために FAILOVER_RESTORE_MEDIA_SERVER パラメータを設定します。
5. 部分的なレプリケーション方式が使われる場合、いずれのバックアップポリシーによっても使われない非スクラッチメディアプールを作成します。バックアップテープが確実にそのプールに自動的に追加されるようにバーコード規則を構成します。

6 DRドメインと本番ドメインで異なるライブラリ形式が使われる場合、バーコードマスキングが同じように機能することを確認します。必要な場合は終了文字を削除します。この操作を管理する規則を構成できます。

7 次の項目について確認します。

- 元のバックアップテープを DR 用に使う場合、DR ドメインのテープライブラリにロードする必要があります。
- バックアップが DR 用にセカンダリテープに複製される場合、テープライブラリにオフサイトテープをロードします。また、適切なコピー番号を含む ALT_RESTORE_COPY_NUMBER ファイルが作成されます。

メモ: ベリタスは、テープが DR ドメインのライブラリに配置される前に物理的に書き込みをロックすることを推奨します。このロックは有効なバックアップを誤って上書きするリスクを減らします。

完全カタログレプリケーションについて

完全カタログレプリケーションでは、カタログのすべての部分がセカンダリマスターサーバーにレプリケートされます。完全カタログレプリケーションでは、本番ドメイン、メディアプール、その他の割り当てからのテープ情報は保有されます。バックアップは、本番ドメインで使われるのと同じテープとポリシーを使ってDRドメインで実行できます。レプリケーションは逆方向に行うことができます。それにより、本番ドメインに戻す移行が単純化されます。ただし、リレーショナルデータベースのコンポーネントをレプリケートすることは本番ドメインのデバイス構成とサーバー設定がDRドメインにレプリケートされることを意味します。この構成情報は使うことができません。また、DR ドメインの構成はリカバリの後で検出する必要があります。

完全カタログレプリケーションはクロスドメインレプリケーションには推奨ではないです。

完全カタログレプリケーションを使ったカタログのリカバリ

完全カタログレプリケーションでは、完全なカタログバックアップが DR マスターサーバーにリカバリされます。DR 環境に存在しないメディアサーバーは不要なプールを避けるために無効にする必要があります。DR サイトのデバイス構成が本番サイトと異なる可能性があるため、すべてのデバイスレコードが削除されます。さらに、EMM データベースを更新するためにデバイスの検出が実行されます。

このアプローチは、NetBackup が DR ドメインのセカンダリのマスターサーバーとメディアサーバーにインストールされているが、実行されていないことを想定しています。また、セカンダリのマスターサーバーとメディアサーバーは互いに通信するように構成されます。

リストアを開始する前に、完全カタログリストアを準備するために次の手順を実行します。DR 計画としてこの手順を文書化してください。

1 プライマリサイトとセカンダリサイト間のレプリケーションが停止していることを確認します。

レプリケーションは、プライマリマスターサーバーが利用不能であるか、またはレプリケーションリンクが無効になれば停止します。

2 レプリケートされたボリュームをセカンダリマスターサーバーの適切なマウントポイントにマウントします。

3 新しいマスターサーバーで NetBackup Relational Database Manager、NetBackup PBX、EMM サービスを起動します。

- UNIX と Linux マスターサーバーで、次のコマンドを実行します。
  - `/usr/openv/netbackup/bin/nbdbms_start_stop start`
  - `/opt/VRTSpbx/bin/pbx_exchange`
  - `"/usr/openv/netbackup/bin/nbemm -maintenance`
- Windows マスターサーバーで、次の Windows サービスを起動します。
  - NetBackup Relational Database Manager
  - Veritas Private Branch Exchange
  - NetBackup Enterprise Media Manager

メモ: NetBackup の起動コマンドと停止コマンドによって停止と起動が行われないため、PBX 処理はすでに動作していることがあります。

4 DR 環境の一部ではないメディアサーバーを無効にします。次のコマンドを実行します。

```
nbemmcmd -updatehost -machinename <Media Server> -machinestateop
set_admin_pause -machinetype media -masterserver <Master Server>
```

5 DR ドメインの任意のメディアサーバーが本番ドメインのメディアサーバーと同じ名前である場合、EMM データベースからすべてのテープデバイスを削除します。次のコマンドを実行します。

```
nbemmcmd -deletealldevices -allrecords
```

メモ: この手順はメディアサーバーで起こる可能性のあるデバイス構成の競合を解決します。DR ドメインのメディアサーバーは本番ドメインのメディアサーバーの名前と異なる名前である場合は、この手順をスキップします。

6 NetBackup を再起動します。

7 必要に応じて、バックアップが自動的に開始されないようにすべてのバックアップポリシーを無効にできます。

- NetBackup 管理コンソールを使ってバックアップポリシーを手動で無効にできます。
- または `bppllist<policy> -set -inactive` CLI を実行します。

8 各メディアサーバーの NetBackup を開始することによって DR 環境の一部になるメディアサーバーを EMM に登録します。

9 デバイスの構成ウィザードを使って、新しいテープドライブとライブラリの構成を作成します。

10 NetBackup 管理コンソールを使ってすべてのリカバリメディアが非ロボットに設定されているかどうかを確認します。

11 非ロボットに設定される必要のあるリカバリメディアがまだある場合、次の操作を実行します。

- ロボットメディアを選択し、右クリックして[移動 (Move)]を選択します。
- [ロボット (robot)]フィールドを[スタンドアロン (Standalone)]に変更します。
- [OK]をクリックして、変更を保存します。

12 すべてのリカバリメディアが非ロボットに設定されたら、[すべてのテープライブラリのインベントリの実行 (Inventory all the tape libraries)]フィールドでメディアが正しいライブラリで識別されていることを確認します。

これで本番データセンターにバックアップされているクライアントデータのリストア操作とリカバリ操作を開始できます。

完全カタログレプリケーションを使用した DR 環境の一貫性の保持

本番サイトで重要なインシデントが発生した場合は、基本的なリカバリが完了した後しばらくしてから DR サイトから操作してください。DR 環境が操作可能になったら、DR 環境の一貫性を保持するために次の追加のタスクを必要に応じて実行できます。

DR 環境の一貫性を保持する方法

1 カタログバックアップポリシーと、DR ドメインで必要な他のバックアップポリシーを修正し、有効にします。

2 もはや必要でないポリシーを削除します。

3 DR 環境の一部ではないメディアサーバーに関連付けられているストレージユニットを削除します。

部分的なカタログレプリケーションについて

部分的なカタログレプリケーションでは、イメージデータベース、ポリシー、クライアント構成のみを複製し、リレーショナルデータベースのコンポーネントの複製は行いません。これにより、ディザスタリカバリドメインでメディアサーバーとデバイスを事前設定できます。セカンダリマスターサーバーへのフェールオーバーの場合にそれらを再検出する必要はありません。

部分的なカタログのレプリケーションでは NetBackup カタログのリレーショナルデータベースのコンポーネントを複製しません。そのため、バックアップをリストアするには、ディザスタリカバリのマスターサーバーにフェールオーバーした後で追加手順が必要です。

部分的なカタログレプリケーションに必要な環境の準備

リストア操作の実行に必要なカタログイメージメタデータはリレーショナルデータベースに保存されるので、リレーショナルデータベースのバックアップを一定の間隔で実行し、フラットファイル情報と共にレプリケートする必要があります。

1. リレーショナルデータベースのステージング領域がレプリケートされたストレージに配置されるように、ソース (実働) マスターサーバーの構成を変更します。この処理は次のようにして実行できます。
   - レプリケートされたストレージに適切なディレクトリを作成します。
   - 次のコマンドを使ってこのディレクトリをステージング領域にします。

     ```
     nbdb_admin -vxdbms_nb_staging <directory>
     ```

2. スケジュールされたスクリプトで次のコマンドを実行して、リレーショナルデータベースをステージング領域に 1 日に数回 (理想的には 1 時間ごとに) バックアップします。

   ```
   nbdb_backup -online <directory>-truncate_tlog
   ```

部分的なカタログレプリケーションでの環境のリカバリ

ソースマスターサーバーの消失の場合に (または障害リカバリテスト中) 次の手順を実行します。

1. プライマリサイトとセカンダリサイト間のレプリケーションが停止していることを確認します。

   レプリケーションは、プライマリマスターサーバーが利用不能であるか、またはレプリケーションリンクが無効になれば停止します。

2. レプリケートされたボリュームをセカンダリマスターサーバーの適切なマウントポイントにマウントします。

3 対象の (ディザスタリカバリ) マスターサーバーでレプリケートされたストレージの場所にリレーショナルデータベースのステージング領域を指すのにコマンド `nbdb_admin -vxdbms_nb_staging <directory>` を使います。

4 レプリケートされたリレーショナルデータベースバックアップからメタデータをエクスポートするには、コマンド `cat_export -all -staging` を実行します。

5 アクティブなリレーショナルデータベースに、エクスポートされたメタデータをインポートするには、コマンド `cat_import -all` を実行します。

6 セカンダリマスターサーバーの NetBackup を起動します。

7 バックアップポリシーがレプリケートされたら、バックアップが自動的に開始されないようにすべてのバックアップポリシーを無効にします。

- NetBackup 管理コンソールを使ってバックアップポリシーを手動で無効にできます。
- またはコマンド `bpplist<policy> -set -inactive` を実行します。

8 セカンダリサイトのメディアサーバーを通してリストア操作を指示するように適切な FAILOVER_RESTORE_MEDIA_SERVER 設定が定義済みであることを確認します。

9 テープからバックアップをリストアするには、テープをテープライブラリに配置し、ライブラリのインベントリを実行することで、ディザスタリカバリマスターサーバーのカタログに追加する必要があります。テープが手違いでディザスタリカバリマスターサーバーを上書きしないようにするために、グローバルなスクラッチプールではなく、どのバックアップポリシーでも使用されていないボリュームプールにテープを追加するバーコードルールがあるはずです。テープには物理的に書き込みロックもするのが理想的です。

10 ディスクベースのバックアップのために、ストレージサーバーおよびディスクプールは、ディスクストレージサーバーウィザードの実行によってディザスタリカバリマスターサーバーに追加する必要があります。

ディスクストレージが存在する場合、ディスクメディア ID を調整する次のコマンドを実行してください。

```
nbcatsync -backupid <catalog backup ID> -prune_catalog
```

`<catalog backup ID>` 値はごく最近のカタログバックアップのバックアップ ID で、カタログバックアップのディザスタリカバリファイルにあります。テープが追加され、ディスクメディア ID が調整されると、リストア操作を開始できます。

ディザスタリカバリ環境と部分的なカタログレプリケーションを一致させる

実働サイトで重要なインシデントが発生した場合、リカバリ完了後しばらくしてからディザスタリカバリサイトで操作します。ディザスタリカバリ環境が操作可能になったら、ディザスタリカバリ環境の一貫性を保持するために次の追加タスクを必要に応じて実行できます。

ディザスタリカバリ環境と部分的なカタログレプリケーションを一致させるには

1. カタログバックアップポリシーと、ディザスタリカバリドメインで必要な他のバックアップポリシーを変更し、有効にします。
2. もはや必要でないポリシーを削除します。

部分的なカタログレプリケーションを使ったテープ管理の注意事項

本番ドメインからのテープはディザスタリカバリドメインには割り当てられません。データベースに手動でテープを追加し、誤って上書きされることのないプールに配置する必要があります。これはまた、バーコード規則とロボットインベントリコマンドを組み合わせて使用することによっても実行できます。

ディザスタリカバリマスターサーバーにテープが割り当てられておらず、バックアップが期限切れになってもグローバルなスクラッチプールにリリースされないので、これらのテープを手動でリサイクルする必要があります。

注意: 注意すべきなのは、テープを手動でグローバルなスクラッチプールに移動するのは、有効なバックアップがないときだけだということです。

これを調べる最も簡単な方法は、`bpimagelist -d "01/01/1970 00:00:00" -media -l` と `vmquery -pn <private pool name> -b` コマンドを実行してリストを作成し、2 つのリストを比較することです。2 番目のリストにはあるのに、最初のリストにはないテープには、有効なイメージがないため、`vmchange -p <scratch pool number> -m <media id>` コマンドを実行してスクラッチプールに移動することができます。

4

完全カタログレプリケーションを使ったNetBackupマスターサーバーの配備

この章では以下の項目について説明しています。

レプリケーションの注意事項について

カタログレプリケーションを使って NetBackup を配備するには、実際の配備を計画するための次の要因を考慮してください。

表 4-1　　レプリケーションの注意事項

注意事項	説明
マスターサーバーの注意事項	ベリタスは、マスターサーバーとメディアサーバーの両方として機能する 1 台のマスターサーバーを動作させることを推奨しません。異なるサイトで利用可能なストレージデバイスに互換性がなければ、それはストレージユニット定義とバックアップエラーに関する問題の原因となる場合があります。 カタログレプリケーションはカタログバックアップの代用にはならず、カタログは定期的にバックアップする必要があります。

注意事項	説明
ネットワークの注意事項	複数サイト単一ドメイン構成では、マスターサーバーは両方のサイトのメディアサーバーを制御します。メタデータはサイト間を通過する必要があります。このメタデータの通信はサイト間の標準 I/P リンクを介して送信されます。同じリンクはグローバルクラスタ制御のハートビートリンクとして使うことができます。ベリタスは、この通信を処理するために少なくとも 10 Mb/秒、理想としては 100 Mb/秒のリンクをサイト間に提供することを推奨します。 ホストベースのレプリケーションが使われる場合、追加の I/P 帯域幅がレプリケーション層に必要になります。追加の帯域幅も考慮する必要があります。
DNS の注意事項	セカンダリサイトのマスターサーバーノードがプライマリサイトのマスターサーバーノードと異なるサブネットにあれば、DNS の変更がフェールオーバー処理の一部として必要になります。クラスタフェールオーバー処理の使用によって DNS の変更を自動的に開始できます。また、処理を手動で開始できます。バックアップシステムは変更が全面的に伝播されるまで正しく機能しません。これはサイトのフェールオーバーのリカバリ時間に影響する場合があります。 **メモ:** クラスタサービスグループによって DNS の変更を自動的に伝播するには、DNS のリソースを NetBackup の起動後にオンラインにする必要があります。
プライマリとセカンダリのマスターサーバーの注意事項	カタログのレプリケーション時にフェールオーバーを実行するには、プライマリとセカンダリのマスターサーバーで同じトポロジーを使う必要があります。 プライマリとセカンダリのサイトマスターサーバーノードは、両方ともクラスタ化するかまたは両方とも非クラスタ化する必要があります。 **メモ:** 各サイトのクラスタマスターサーバーでノードの数が同じである必要はありません。 詳しくは、https://www.veritas.com/support/ja_JP/article.000090837を参照してください。

5

クラスタでの NetBackup を使用したバックアップおよびリストア

この章では以下の項目について説明しています。

- クラスタでの NetBackup を使用したバックアップとリストアについて
- クラスタでサポートされる NetBackup アプリケーションエージェントについて

クラスタでの NetBackup を使用したバックアップとリストアについて

この章では、クラスタ内のデータのユーザー主導バックアップおよびリストアを行う手順へのリンクについて説明します。また、バックアップおよびリストアを実行する具体的な手順については、他の NetBackup のマニュアルを参照してください。NetBackup エージェントとオプションについて詳しくは、『NetBackup バックアップ、アーカイブおよびリストアスタートガイド』と、NetBackup の各管理者ガイドを参照してください。

バックアップとリストアの処理は、クラスタ環境であるか非クラスタ環境であるかにかかわらず同じです。バックアップ処理とアーカイブ処理およびリストア処理について詳しくは、『NetBackup トラブルシューティングガイド』を参照してください。

クラスタでのNetBackup を使用したユーザー主導バックアップ

クラスタでユーザー主導バックアップを実行する場合、ノード名またはクライアントの仮想名を使用してバックアップを実行することができます。仮想名を選択した場合、バックアップは任意のクラスタノードからリストアできます。また、自動バックアップも構成できます。

Windows クライアントでユーザー主導バックアップを実行する方法

1. バックアップ、アーカイブおよびリストアコンソールを開きます。
2. [ファイル (File)]メニューで[NetBackup マシンの指定 (Specify NetBackup Machines)]をクリックします。
3. [ソースクライアント (Source client)]リストから、目的のノードまたは仮想名を選択 (または追加) します。

UNIX または Linux クライアントでユーザー主導バックアップを実行する方法

1. バックアップ、アーカイブおよびリストアコンソールを開きます。
2. [ログイン (Login)]ダイアログボックスで、クライアントの名前 (ノードまたは仮想クライアント名) を入力します。

   目的のノードまたは仮想クライアントにログインする必要があります。Java インターフェースでは、ローカルクライアント以外のクライアントを指定することはできません。

クラスタ内のデータのリストアについて

すべてのファイルのリストア操作については、『NetBackup バックアップ、アーカイブおよびリストアスタートガイド』のリストア方法の手順に従います。ファイルを共有ディスクドライブにリストアする場合は、それらのファイルを仮想サーバー名にリストアします。

各データベースファイルをリストアする場合は、データベースアプリケーションがインストールされているクライアントに対応する仮想サーバー名に、対象のファイルをリストアします。

メモ: クラスタ環境では、コンピュータに複数の仮想名があるため、複数のクライアント名のコンテキストでファイルをバックアップできます。バックアップポリシーを慎重に計画することで、この問題を回避できます。ただし、バックアップイメージを検索するために複数のクライアント名を参照する必要のある場合があります。また、必要なすべてのファイルをリストアするために、複数のリストアの実行が必要になる場合もあります。

バックアップ、アーカイブおよびリストアコンソールは、そのクライアント名のコンテキストで動作します。リダイレクトリストアを実行して、仮想サーバー名を使用してバックアップされた共有ディスクにファイルをリストアする必要があります。NetBackup では、NetBackup マスターサーバーで必要な構成を行った場合にのみ、リダイレクトリストアを実行できます。リダイレクトリストアを許可する方法については、『NetBackup 管理者ガイド Vol. 1』を参照してください。

この他にも、マスターサーバー上に適切な `altnames` ディレクトリエントリを作成することが必要な状況があります。NetBackup によってクライアントからのファイルのリストアが試行される時、処理が失敗し、次のエラーメッセージが表示される場合があります。

```
131 client is not validated to use this server
```

このメッセージが表示された場合、処理を成功させるためには altnames ディレクトリを設定する必要があります。たとえば、必要なネットワークインターフェースパラメータにクライアントの有効なネットワーク名が設定されているとします。しかし、この名前は、そのクライアントの NetBackup クライアント名パラメータと一致するとは限りません。この状況は、クラスタ内の NetBackup クライアントで頻繁に発生します。 代わりに、サーバー主導リストアを実行して、altnames ディレクトリを設定せずに済むようにすることもできます。

p.46 の「例: NetBackup クラスタ内のユーザー主導リストアの実行」を参照してください。

例: NetBackup クラスタ内のユーザー主導リストアの実行

たとえば、クラスタ仮想サーバー名が TOE、クラスタノード名が TIC および TAC であるとします。共有ディスク上のファイルは、クライアントリストに TOE を含む NetBackup ポリシーによってバックアップする必要があります。

共有ディスクでファイルのサーバー主導リストアを実行するには、ソースクライアントと宛先クライアントの両方を TOE に設定します。サーバー主導リストアでは、リストア時に共有ディスクを制御しているノードを認識する必要はありません。

NetBackup クラスタ内のファイルのユーザー主導リストアを実行する方法

1. マスターサーバー上に次のファイルを作成します。

   UNIX または Linux サーバーの場合

   ```
   /usr/openv/netbackup/db/altnames/tic
   /usr/openv/netbackup/db/altnames/tac
   ```

   Windows サーバーの場合

   ```
   shared_drive_install_path¥NetBackup¥db¥altnames¥tic
   shared_drive_install_path¥NetBackup¥db¥altnames¥tac
   ```

2. 両方のファイルで、ファイル内の 1 行に仮想サーバー名 (TOE) を追加します。
3. 共有ディスクを制御するノード (TIC または TAC) を特定します。
4. そのノードで、バックアップ、アーカイブおよびリストアインターフェースを起動し、ソースクライアントおよびサーバーとして仮想サーバー名 (TOE) を選択します。
   - Windows コンピュータでは、[ファイル (File)]メニューで[NetBackup マシンの指定 (Specify NetBackup Machines)]をクリックします。
   - UNIX または Linux コンピュータでは、[処理 (Actions)]メニューで[NetBackup マシン (NetBackup Machines)]をクリックします。
5. 共有ディスクから仮想サーバー名 (TOE) を使用して、バックアップファイルを参照し、必要に応じてリストアします。

クラスタでサポートされる NetBackup アプリケーションエージェントについて

クラスタ環境では特定のデータベースエージェントおよび NetBackup オプション製品のみがサポートされます。

クラスタでのデータベースエージェントおよびオプション製品のインストールおよび構成については、そのエージェントまたはオプション製品の管理者ガイドを参照してください。

クラスタ内のデータベースファイルのバックアップ	データベースアプリケーションは、仮想サーバーとしてクラスタにインストールされます。これらの仮想サーバーのデータを保護するには、クラスタの各ノードに適切な NetBackup データベースエージェントをインストールします。 Windows 版 NetBackup では、データベースエージェントは NetBackup サーバーおよび NetBackup クライアントと一緒にインストールされます。また、そのデータベースエージェント用にバックアップポリシーを作成します。クラスタ内にアプリケーションまたはデータベースのポリシーを構成する場合、ポリシー内のクライアント名として、常にそのアプリケーションまたはデータベースの仮想サーバー名を使用します。特定のデータベースエージェントのインストールおよび構成の手順については、そのエージェント用の NetBackup のマニュアルを参照してください。
ユーザーバックアップ	クラスタの各ノードで実行するユーザーバックアップは、通常、NetBackup 仮想サーバーのバックアップではなく、ノードのバックアップとして実行されます。 スケジュールバックアップを使用する方が、ユーザーバックアップより簡単にクラスタのデータを保護できる場合があります。
クラスタ内の NetBackup クライアント	クラスタ内に NetBackup クライアントのみをインストールすることができます。この構成では、ネットワーク全体のクラスタから、データを各 NetBackup サーバーへバックアップできます。この場合、テープデバイス、メディアなどに対する NetBackup 固有の構成作業が、クラスタ自体の設定や保守作業から分離されます。ただし、NetBackup クライアント自体のフェールオーバーは実行できません。 WSFC、VCS、SunCluster、Service Guard または HACMP クラスタに NetBackup クライアントをインストールする方法 NetBackup クライアントは、クラスタ環境でない場合と同じようにクラスタにインストールされます。 NetBackup クライアントのインストール方法については、『Veritas NetBackup インストールガイド』を参照してください。 Windows システムの場合、クラスタ上のデータをバックアップする際に名前解決に問題が発生する場合があります。(このデータは、ローカルデータまたは共有データのいずれかになります。) 各クライアントの［必要なネットワークインターフェース (Required network interface)］パラメータに、NetBackup クライアントをインストールするノードの完全修飾名を設定することを検討してください。

クラスタ内のデータベースファイルのバックアップについて

データベースアプリケーションは、仮想サーバーとしてクラスタにインストールされます。これらの仮想サーバーのデータを保護するには、クラスタの各ノードに適切な NetBackup データベースエージェントをインストールします。Windows 版 NetBackup では、データベースエージェントは NetBackup サーバーおよび NetBackup クライアントと一緒にインストールされます。また、そのデータベースエージェント用にバックアップポリシーを作成します。クラスタ内にアプリケーションまたはデータベースのポリシーを構成する場合、ポリシー内のクライアント名として、常にそのアプリケーションまたはデータベースの仮想サーバー名を使用します。特定のデータベースエージェントのインストールおよび構成の手順については、そのエージェント用の NetBackup のマニュアルを参照してください。

ユーザーバックアップについて

クラスタの各ノードで実行するユーザーバックアップは、通常、NetBackup 仮想サーバーのバックアップではなく、ノードのバックアップとして実行されます。スケジュールバックアップを使用する方が、ユーザーバックアップより簡単にクラスタのデータを保護できる場合があります。

クラスタ内の NetBackup クライアントについて

クラスタ内に NetBackup クライアントのみをインストールすることができます。この構成では、ネットワーク全体のクラスタから、データを各 NetBackup サーバーへバックアップできます。この場合、テープデバイス、メディアなどに対する NetBackup 固有の構成作業が、クラスタ自体の設定や保守作業から分離されます。ただし、NetBackup クライアント自体のフェールオーバーは実行できません。

MSCS、VCS、SunCluster、Service Guard または HACMP クラスタに NetBackup クライアントをインストールする方法

NetBackup クライアントは、クラスタ環境でない場合と同じようにクラスタにインストールされます。NetBackup クライアントのインストール方法については、『Symantec NetBackup インストールガイド』を参照してください。Windows システムの場合、クラスタ上のデータをバックアップする際に名前解決に問題が発生する場合があります。(このデータは、ローカルデータまたは共有データのいずれかになります。) 各クライアントの［必要なネットワークインターフェース (Required network interface)］パラメータに、NetBackup クライアントをインストールするノードの完全修飾名を設定することを検討してください。

索引

さ

な

は

ま

や