vSphere Data Protection管理ガイド

vSphere Data Protection 5.1

本書は、一覧に記載される各製品のバージョンをサポートし、本書が新しい版と差し替えられるまで、後続のバージョンについてもサポートします。本書の最新版をチェックするには、http://www.vmware.com/jp/support/pubsを参照してください。

JA-000846-00

vmware®

最新のテクニカル ドキュメントは、次のVMware Webサイトを参照してください。

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

VMware Webサイトにも最新の製品情報を掲載しています。

本書に関してご意見がある場合は、フィードバックを

docfeedback@vmware.com宛に送信してください。

ヴイエムウェア株式会社
東京本社
〒105-0013
東京都港区浜松町1-30-5
浜松町スクエア13F
www.vmware.com/jp

コンテンツ

本書について

vSphere Data Protection管理ガイドには、SMB向けのバックアップのインストールと管理に関する情報が記載されています。

受講対象者

本書の受講対象者は、vSphere Data Protectionを使用してバックアップ ソリューションを提供する方です。このドキュメントに記載されている情報は、仮想マシン テクノロジーおよびデータセンター運用に精通した、経験豊かなWindowsまたはLinuxシステム管理者を対象としています。

VMware Technical Publications Glossary

VMware Technical Publicationsは、皆様に馴染みのないと思われる用語を定義する用語集です。VMwareテクニカル ドキュメントで使用されている用語の定義については、http://www.vmware.com/jp/support/pubsをご覧ください。

ドキュメントに関するフィードバック

VMwareは、ドキュメントの改善のために皆様のご意見を歓迎します。フィードバックを docfeedback@vmware.comにお寄せください。

テクニカル サポートとエデュケーション リソース

以降のセクションでは、ご利用いただけるテクニカル サポート リソースについて説明します。他のVMwareドキュメントの現在のバージョンにアクセスするには、http://www.vmware.com/jp/support/pubsをご覧ください。

オンライン サポート

オンライン サポートを利用してテクニカル サポート リクエストを送信するには、お使いの製品と契約情報を表示して、製品を登録し、http://www.vmware/support/phone_support.htmlをご覧ください。

サポート オファリング

VMwareサポート オファリングがどのようにビジネス ニーズを満たすかを確認するために、http://www.vmware.com/jp/support/servicesをご覧ください。

VMwareプロフェッショナル サービス

VMwareエデュケーション サービスコースは、広範囲な実習、事例、オン ザ ジョブ リファレンス ツールとして使用することを目的としたコースの資料を用意しています。コースは、オンサイト、クラスルーム、ライブ オンラインのいずれでもご利用いただけます。オンサイト パイロット プログラムおよび導入ベスト プラクティスの場合、VMwareコンサルティング サービスが、仮想環境の評価、計画、構築、管理に役立つ製品を提供します。エデュケーション クラス、認定プログラム、コンサルティング サービスに関する情報にアクセスするには、http://www.vmware.com/jp/servicesをご覧ください。

1 vSphere Data Protectionを理解する

VDP（vSphere Data Protection）は、堅牢で、導入が容易なディスク ベースのバックアップ/リストア ソリューションです。vSphere Data ProtectionはVMware vCenter Serverと完全統合されており、重複排除されたターゲット ストレージにバックアップを格納し、バックアップ ジョブの一元管理と効率的な管理が可能です。

vSphere Data Protectionのメリットは次のとおりです。

- すべての仮想マシンの高速かつ効率的なデータ保護を提供します。これは、仮想マシンがオフでも、あるいは物理ホスト間で移動されていても、可能です。
- すべてのバックアップをスマートに重複排除することにより、バックアップ データが消費するディスク領域を大幅に減少します。
- ブロックの変更履歴およびVMware仮想マシン スナップショットを使用して、仮想マシンのバックアップ コストを削減し、バックアップ ウィンドウを最小限に抑えます。
- 仮想マシンごとにサード パーティ エージェントをインストールする必要がないため、簡単なバックアップが可能になります。
- vSphere内で統合されたコンポーネントをWebポータルによって管理できるため、インストールがシンプルで簡単です。
- 標準のvSphere Webクライアントに統合されたvSphere Data Protectionへの直接アクセス。
- チェックポイントおよびロールバック メカニズムによりバックアップを保護します。
- Webベースのインタフェースからエンド ユーザー開始のファイル レベルのリカバリを使用して、WindowsおよびLinuxファイルのリカバリを合理化します。

この章は、次のトピックで構成されています。

vSphere Data Protectionの概要

VMware vSphere Webクライアント インタフェースは、仮想マシンのバックアップとリカバリの選択、スケジュール、構成、管理に使用されます。

バックアップの間に、vSphere Data Protectionは仮想マシンの静止スナップショットを作成します。バックアップ オペレーションごとに重複排除が自動的に実行されます。

本書では、バックアップ/リカバリのコンテキストで以下の用語が使用されます。

- **データストア**は、データセンターにおける、基盤となる物理ストレージ リソースの組み合わせの仮想表現です。データストアは、仮想マシン ファイルを格納する場所（たとえば、物理ディスク、RAID、SAN）です。
- **CBT（更新ブロック追跡）**は、仮想マシンのストレージ ブロックの変更を追跡するVMkernel機能です。VMkernelは、仮想マシンの変更を追跡し、VMwareのvStorage APIのメリットを活用するために開発されたアプリケーションのバックアップ プロセスを強化します。
- **VMware VADP（vStorage APIs for Data Protection）**により、バックアップ ソフトウェアは、システムを停止することなく、各仮想マシン内でバックアップ タスクを実行するオーバーヘッドなしに、一元化されたVMバックアップを実行できます。
- **VMDK（仮想マシン ディスク）**は、ゲスト オペレーティング システムに対して物理ディスク ドライブとして表示されるファイルまたはファイル セットです。これらのファイルは、ホスト マシンまたはリモート ファイル システムに存在できます。
- **vSphere Data Protectionアプライアンス**は、vSphere Data Protection専用の仮想アプライアンスです。

イメージ レベルのバックアップとリストア

vSphere Data Protectionは、vStorage API for Data Protectionに統合されたイメージ レベルのバックアップを作成します。vSphere内の機能セットにより、バックアップ プロセスのオーバーヘッドをVMからvSphere Data Protectionアプライアンスに解放します。アプライアンスは、vCenter Serverと通信して、VMのVMDKのスナップショットを作成します。重複排除は、特許取得済みの可変長重複排除テクノロジーを使用してアプライアンス内で実行されます。

大規模で常に拡張を続ける多くのVMware環境に対応するために、vSphere Data Protectionアプライアンスは、8台の仮想マシンを同時にバックアップすることが可能で、データ保護ワークロード容量を増進させています。

イメージ レベルのバックアップの効率性を向上させるために、vSphere Data Protectionは、VADP CBT（更新ブロック追跡）機能を利用します。CBTは、vSphere Data Protectionが前回のバックアップ以降に変更されたディスク ブロックのみをバックアップするようにするVMwareの機能です。これにより、特定のVMイメージのバックアップ時間が大幅に減少するため、特定のバックアップ ウィンドウ内に多くのVMを処理することが可能になります。

リストア時にCBTを活用することで、vSphere Data Protectionは、VMを元の場所にリストアする際に、高速かつ効率的なリカバリを実現します。リストア プロセスの間、vSphere Data ProtectionはVADPに問い合わせて、前回のバックアップ以降にどのブロックが変更されたかを確認し、リカバリ時にそのブロックのみをリカバリまたはリプレースします。これにより、リカバリ オペレーション中のvSphere環境内のデータ転送が減少し、何よりも、RTO（Recovery Time Objective：目標復旧時間）が短縮されます。

さらに、vSphere Data Protectionはリストアの方法（フル イメージ リストアまたはCBTを活用したリカバリ）によるワークロードの違いを自動的に評価して、リストア時間が最高速の方法を実行します。これは、リストアされるVMにおける前回のバックアップ以降の変更率が高く、CBT解析オペレーションのオーバーヘッドが直接フル イメージ リカバリよりも高くつく場合に有効です。vSphere Data Protectionは、その環境で最高速のVMイメージ リカバリ時間を実現するのはどの導入方法かをインテリジェントに判断します。

VMwareイメージ バックアップのメリットは次のとおりです。

- ゲスト オペレーティング システムに関係なく、VMのフル イメージ バックアップを提供する
- 利用可能でライセンスがある場合は、効率的なトランスポート方式であるSCSI hotaddを利用し、ネットワークを介したVMDKイメージ全体のコピーを回避する

- イメージ レベルのバックアップからファイル レベルのリカバリを提供する
- vSphere Data Protectionアプライアンスによって保護された.vmdkファイル内、およびすべての.vmdkファイルを重複排除する
- 高速バックアップとリストアを実現するために更新ブロック追跡を使用
- データの重複排除と圧縮によりネットワーク トラフィックを最小限に抑える
- VMごとにバックアップ エージェントを管理する必要性をなくす
- 優れたスループットと実現のために同時バックアップ/リカバリをサポート

重要 VMイメージ バックアップのベスト プラクティスは、仮想マシンごとにVMwareツールをインストールすることです。VMwareツールは、バックアップ前に、ゲストOS上で特定のプロセスを休止させるバックアップ機能を追加します。

ファイル レベルのリカバリ

FLR（ファイル レベル保存期間設定）により、保護されているVMのローカル管理者はローカル マシンに対してバックアップを参照し、マウントすることができます。管理者は、これらのマウントされたバックアップから個々のファイルをリストアすることができます。ファイル レベルのリカバリは、vSphere Data Protectionリストア クライアントを使用して実施されます。

重複排除ストアのメリット

エンタープライズ データは、システム内およびシステム間に同一のファイルまたはデータが存在し、非常に冗長です（たとえば、OSファイルや複数の受信者に送信されたドキュメント）。編集されたファイルも以前のバージョンと合わせて極めて冗長です。従来のバックアップ方法では、冗長データをすべて何度も保存するため、それが拡大されます。vSphere Data Protectionは特許取得済みの重複排除テクノロジーを使用して、ファイル レベルおよびサブファイル データ セグメント レベルの両方で冗長性を排除します。

可変長および 固定長データ セグメント

セグメントまたはサブファイル レベルでの冗長データ排除の主な要因は、セグメント サイズを決定する方法です。スナップショットおよび一部の重複排除テクノロジーでは、固定ブロックまたは固定長セグメントが一般に採用されています。残念ながら、この方法では、データセットの変更がほんのわずかにも関わらず、データセットに小さな変更があると（たとえば、ファイルの先頭にデータを挿入）、データセットのすべての固定長セグメントを変更してしまいます。vSphere Data Protectionは、データを調べて論理境界ポイントを判断するセグメント サイズの決定にインテリジェントな可変長方法を使用して、非効率性を排除します。

論理セグメントの判断

vSphere Data Protectionは、セグメント サイズの判断に、特許取得済みの方法を使用しています。この方法は、システム全体の効率性を最適化するように設計されています。vSphere Data Protectionのアルゴリズムは、状況依存のセグメント境界を判断するために、データセットのバイナリ構造（データセットを構成するすべての0と1）を分析します。可変長セグメントのサイズは平均24 KBで、平均12 KBに圧縮されています。

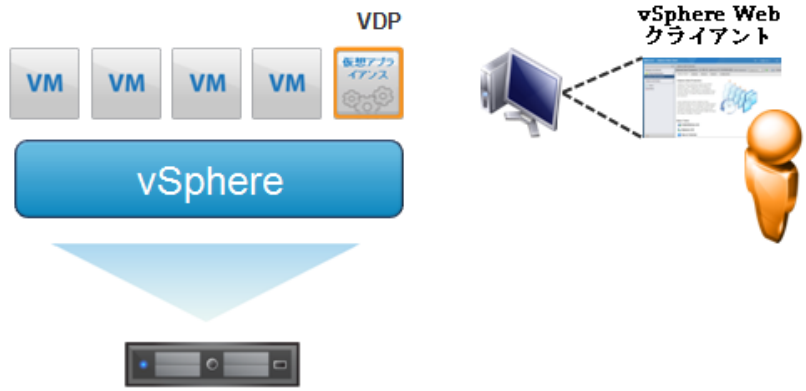
VMDKファイル内のバイナリ構造を分析することにより、vSphere Data Protectionは、すべてのファイルの種類とサイズを対象として、データをインテリジェントに重複排除します。

vSphere Data Protection のアーキテクチャ

VDP（vSphere Data Protection）は、vSphere WebクライアントおよびvSphere Data Protectionアプライアンスを使用して、バックアップを重複排除されたストレージに格納します。

vSphere Data Protectionは、さまざまなマシンで実行されるコンポーネント セットから構成されています(以下の図に示す)。

- vSphere 5.1
- vSphere Data Protectionアプライアンス（ESX/ESXi 4.xまたは5.xにインストール）
- vSphere Webクライアント。



vSphere Data Protectionのインストールと構成

2

この章は、次のトピックで構成されています。

vSphere Data Protection のサイズ設定

vSphere Data Protectionのサイズ設定は、以下の項目に基づいてvSphereデータ保護アプライアンスのサイズおよびアプライアンス数を決定します。

- VM数および種類（VMにはファイル システムまたはデータベースのデータが含まれていますか。）
- データ量
- 保存期間（日単位、週単位、月単位、年単位）
- 一般的な変更率

次の表に、vSphere Data Protectionの推奨サイズ設定を示します。

表 2-1. vSphere Data Protection のサイズ設定の推奨例

VM 数	クライアントあたりのデータ ストレージ	保持期間：日単位	保持期間：週単位	保持期間：月単位	保持期間：年単位	推奨事項
25	20 GB	30	0	0	0	1- 0.5 TB VDP
25	20 GB	30	4	12	7	1- 2 TB VDP
25	40 GB	30	4	12	7	2- 2 TB VDP
50	20 GB	30	0	0	0	1- 1 TB VDP
50	20 GB	30	4	12	7	2- 2 TB VDP
50	40 GB	30	4	12	7	3- 2 TB VDP
100	20 GB	30	0	0	0	1- 2 TB VDP
100	20 GB	30	4	12	7	3- 2 TB VDP
100	40 GB	30	4	12	7	6- 2 TB VDP

上述の推奨項目は（注：ガイドラインとして参照してください）、以下の前提に基づいています。

- VMには、主にファイル システム データが含まれます。VMに、主にデータベース データが含まれている場合は、重複排除率は低くなります。
- ファイル システム データの最初の重複排除率が70%。
- ファイル システム データの日単位の重複排除率が99.7%。
- 年単位増加率は5%。

重要 導入するアプライアンスのサイズが明確でない場合は、より大きなvSphere Data Protectionデータストアを使用することを推奨します。アプライアンスの導入後は、データストアのサイズは変更できません。

ソフトウェア要件

vSphere Data Protection 5.1のソフトウェア要件は以下のとおりです。

- VMware vCenter Server
  - vCenter Server LinuxまたはWindows：バージョン5.1
  - vSphere Webクライアントは、Microsoft Internet Explorer 7および8（IE 8でvSphere Webクライアントを実行する場合、現在既知の問題があります）、あるいはMozilla Firefox 3.6以上でサポートされます。
  - vSphere Webクライアントまたは vSphere Data Protectionの機能にアクセスするには、WebブラウザがAdobe Flash Player 11.3以上に対応していることが必要です。
- VMware ESX/ESXi（以下のバージョンがサポートされます）
  - 4.0、4.0i、4.1i、5.0i、5.1

- アプライアンス バージョン：
  - vSphere Data Protection：5.1

システム要件

vSphere Data Protectionアプライアンスは以下のオプションで利用可能です

- 0.5 TB VDP
- 1 TB VDP
- 2 TB VDP

重要 vSphere Data Protectionの導入後は、サイズの変更はできません。

以下の表にはvSphere Data Protectionの各オプションのシステム要件を指定しています。

	0.5 TB VDP	1 TB VDP	2 TB VDP
vSphere Data Protection専用プロセッサ	vSphere Data Protectionに常時利用可能な最低4つの2 GHzプロセッサ	vSphere Data Protectionに常時利用可能な最低4つの2 GHzプロセッサ	vSphere Data Protectionに常時利用可能な最低4つの2 GHzプロセッサ
vSphere Data Protection専用物理メモリ	4 GB	4 GB	4 GB
ディスク容量	850 GB	1,600 GB	3,100 GB
ネットワーク接続	1 GbE接続	1 GbE接続	1 GbE接続

vSphere Data Protection の仕様

vSphere Data Protectionは次の仕様をサポートします。

- vSphere Data Protectionアプライアンスは、最大100 VMのバックアップをサポートします
- 各vCenter Serverは、最大10個のvSphere Data Protectionのアプライアンスをサポートします
- 0.5 TB、1 TB、2 TBの重複排除ストレージをサポートします

プリインストール構成

vSphere Data Protectionインストールの前に、DNSおよびNTPが構成させている必要があります。

DNSの構成

vSphere Data Protectionを導入する前に、アプライアンスのIPアドレスおよび完全修飾ドメイン名用にDNSサーバにエントリーを追加する必要があります。このDNSサーバは、正引きおよび逆引きをサポートしている必要があります。

重要 DNSを適切に設定しないと多くのランタイムまたは構成の問題を引き起こす場合があります。

DNSが適切に構成されているかを確認するには次のようにします。

1 コマンド プロンプトを開き、次のコマンドを入力します。

nslookup <VDP_IP_address> <DNS_IP_address>

nslookupコマンドは、vSphere Data Protectionアプライアンスの完全修飾ドメイン名を返します。

2 次のコマンドを入力します。

nslookup <FQDN_of_VDP> <DNS_IP_address>

nslookupコマンドは、vSphere Data ProtectionアプライアンスのIPアドレスを返します。

3 これらのnslookupコマンドで正しい情報が返された場合はコマンド プロンプトを閉じ、情報が誤っている場合は、vSphere Data Protectionインストール前のDNS構成を解決します。

NTPの構成

vSphere Data Protectionは、NTP（Network Time Protocol）を使用します。vSphere Data Protectionをインストールする前に、vSphere Data Protectionのインストール先となるvCenter ServerおよびESXiホストでNTPを構成する必要があります。

NTPの構成の詳細については、ESXiおよびvCenter Serverのドキュメントを参照してください。

ユーザー アカウントの構成

vSphere Data ProtectionでvCenterユーザー アカウントを使用、またはvSphere Data ProtectionでSSO adminユーザーを使用するには、これらのユーザーをvCenterルート ノードで管理者として特別に追加する必要があります。vSphereクライアントを使用して、vSphere Data ProtectionユーザーまたはSSO adminユーザーを構成するには、以下の手順を使用します。

1 vSphere Webクライアントにログインし、**［vCenter］ > ［ホストおよびクラスタ］**を選択します。

2 左のパネルで、［vCenter Server］をクリックします。

3 **［管理］**タブをクリック、次に**［権限］**サブ タブをクリックします。

4 **［権限の追加］**アイコンをクリックします。

5 **［追加］**をクリックします。

6 ［ドメイン］ドロップダウン メニューから、［ドメイン］、［サーバ］、［SYSTEM-DOMAIN］のいずれかを選択します。

7 vSphere Data Protectionを管理するまたはSSO adminユーザーとなるユーザーを選択し、**［追加］**をクリックします。

8 **［OK］**をクリックします。

9 ［割り当て済みの役割］ドロップダウンから、［管理者］を選択します。

10 ［子オブジェクトへの伝播］ボックスが選択されていることを確認します。

11 **［OK］**をクリックします。

ユーザーが［管理者］に表示されていることを確認するには、**［ホーム］ > ［管理］ > ［役割マネージャ］**に進み、**［管理者の役割］**をクリックします。追加したばかりのユーザーは、役割の右側に表示されている必要があります。

重要 VDP-configureのUIを使用しているvSphere Data Protectionバックアップ ユーザーがドメイン アカウントに属している場合、vdp-configureは「SYSTEM-DOMAIN\admin」の形式で指定されている必要があります。ユーザー名が「admin@SYSTEM-DOMAIN」の形式で入力されている場合、バックアップ ジョブに関連するタスクが［最新の実行中タスク］に表示されない可能性があります。

OVFテンプレートの配置

動作条件

- vSphere Data Protectionアプライアンスは、ESXi 4.0、4.1、5.0、5.1ホストにインストールします。
- vCenter 5.1が必要です。vSphere Webクライアントからvcenterにログインし、OVFテンプレートを配置します。
- vSphere Data Protectionアプライアンスは、ポート902を使用してESXiに接続します。vSphere Data ProtectionアプライアンスとESXiの間にファイアウォールがある場合、ポート902を開いておく必要があります。
- ご使用のブラウザで、VMwareクライアント統合プラグ イン5.1.0をインストールする必要があります。

手順

1 vSphere Webクライアントにログインし、**[vCenter] > [データセンター]**を選択します。

2 [オブジェクト]タブで、**[アクション] > [OVFテンプレートの配置]**をクリックします。

3 vSphere Data Protectionアプライアンスが配置されているソースを選択します。

4 デフォルトでは、ソースの選択ダイアログはOVF パッケージに設定されています。これを**[OVA パッケージ]**に変更します。

5 アプライアンスを選択し、**[開く]**をクリックします。

6 アプライアンスの.ovaファイルを選択した後、**[次へ]**をクリックします。

7 テンプレートの詳細を確認し、**[次へ]**をクリックします。

8 [EULAの同意]画面で使用許諾契約書を一読し、**[同意する]**、続いて**[次へ]**をクリックします。

9 [名前とフォルダの選択]画面でアプライアンスの名前を入力し、このアプライアンスを配置するフォルダまたはデータセンターをクリックします。**[次へ]**をクリックします。

10 アプライアンスのホストを選択し、**[次へ]**をクリックします。

11 仮想ディスクのフォーマット（42ページの“シンまたはシック プロビジョニングされたディスク選択の影響”に詳細が記載されています）、およびアプライアンスのストレージの場所を選択します。**[次へ]**をクリックします。

12 アプライアンスの[宛先ネットワーク]を選択し、**[次へ]**をクリックします。

13 [テンプレートのカスタマイズ]で、**[デフォルト ゲートウェイ]**、**[DNS]**、**[ネットワーク1のIPアドレス]**、**[ネットワーク1のネットマスク]**を指定します。IPアドレスが正しいことを確認します。このダイアログ ボックスで誤ったIPアドレスを指定すると、.ovaの再配置が必要になります。**[次へ]**をクリックします。

注 vSphere Data ProtectionアプライアンスはDHCPをサポートしません。アプライアンスには、静的IPアドレスが必要です。

14 [完了の準備]画面ですべての配置オプションが正しいことを確認し、**[完了]**をクリックします。

vCenterは、vSphere Data Protectionアプライアンスを導入します。**[最新のタスク]**を監視し、導入が完了するのを確認します。

vSphere Data Protection のインストールと構成

動作条件

vSphere Data Protection .ovfテンプレート（14ページの“OVFテンプレートの配置”を参照）を正しく導入し、vSphere Webクライアントからvcenterサーバにログインする必要があります。

手順

1 **[vCenter Home] > [vCenter] > [VMs and Templates]**を選択します。vCenterツリーを展開して、vSphere Data Protectionアプライアンスを選択します。アプライアンスを右クリックして、**[電源オン]**を選択します。

2 アプライアンスを右クリックして、**[コンソールを開く]**を選択します。

3 インストール ファイルをロードすると、vSphereデータ保護メニューの[ようこそ]画面が表示されます。Webブラウザを開き、以下のように入力します。

https://<VDPアプライアンスのIPアドレス>:8543/vdp-configure/

4 VMwareログイン画面で、以下を入力します。

a ユーザー：**root**

b パスワード：**changeme**

c ［**ログイン**］をクリックします

5 ようこそ画面が表示されます。［**次へ**］をクリックします。

6 ［ネットワーク設定］ダイアログ ボックスが表示されます。以下の項目を指定（または確認）します。

a IPv4 静的アドレス

b ネットマスク

c ゲートウェイ

d プライマリ DNS

e セカンダリ DNS

f ホスト名

g ドメイン

7 ［**次へ**］をクリックします。

8 ［タイム ゾーン］ダイアログ ボックスが表示されます。適切なタイム ゾーンを選択して、［**次へ**］をクリックします。

9 ［vSphere Data Protection認証情報］ダイアログ ボックスが表示されます。［vSphere Data Protection 認証情報］では、vSphere Data Protectionアプライアンスのパスワードを入力します。これは、ユニバーサル構成パスワードになります。以下の条件を満たすパスワードを指定します。

- 9文字
- 大文字を最低1つ使用
- 小文字を最低1つ使用
- 数字を最低1つ使用
- 特殊文字は使用しない

10 ［**次へ**］をクリックします。

11 ［vCenterの登録］ダイアログ ボックスが表示されます。以下を指定します。

a vCenterユーザー名（ユーザーがドメインアカウントに属している場合、「SYSTEM-DOMAIN\admin」の形式でユーザー名を入力する必要があります。）

b vCenterパスワード

c vCenterホスト名（IPアドレスまたは完全修飾ドメイン名）

d vCenterポート

e SSOホスト名（IPアドレスまたは完全修飾ドメイン名）

f SSO ポート

12 ［**接続テスト**］をクリックします。

接続成功メッセージが表示されます。このメッセージが表示されない場合は、設定をトラブルシューティングして、成功メッセージが表示されるまでこの手順を繰り返します。

「Specified user either is not a dedicated VDP user or does not have sufficient vCenter privileges to administer VDP. Please update your user role and try again（指定されたユーザーはVDPの専用ユーザーではなく、またVDPを管理する十分なvCenterの権限もありません。ユーザーの役割を更新し、再度実行してください。）」というメッセージが表示されたら、ユーザーの役割を更新する方法について 14ページの“ユーザー アカウントの構成”を参照してください。

13 ［**OK**］をクリックします。

14 ［**次へ**］をクリックします。

15 ［完了の準備］ページが表示されます。［**終了**］をクリックします。

16 構成完了のメッセージが表示されます。［**OK**］をクリックします。

vSphere Data Protectionアプライアンスの構成が完了しましたが、vSphere Webクライアントに戻りアプライアンスの再起動が必要です。vSphere Webクライアントを使用して、アプライアンスを右クリックし、［**ゲストOSの再起動**］を選択します。［再起動の確認］メッセージで、［**はい**］をクリックします。再起動には最大30分かかります。

インストール後の構成

vSphere Data Protectionのインストール時、構成ユーティリティを初めて実行すると、「インストール」モードで実行されます。このモードでは、初回ネットワーク設定、タイム ゾーン、アプライアンスのパスワード、vCenterの認証情報を入力できます。初回インストールの後、VDP-configureユーティリティは「メンテナンス」モードで実行され、別のユーザー　インタフェースを表示します。

VDP-Configureにアクセスするには、Webブラウザを開き、以下のように入力します。

https://<VDPアプライアンスのIPアドレス>:8543/vdp-configure/

メンテナンス インタフェースは次の目的で使用します。

- ステータスの表示：アプライアンスで実行中（または現在停止している）のサービスを確認できます。
- サービスの開始と停止：アプライアンスの選択されたサービスを開始および停止できます。
- ログ収集：アプライアンスから現在のログをダウンロードできます。
- vSphere Data Protection構成の表示または変更：ネットワーク設定の表示または変更、vCenterの登録の構成、システム設定の表示と編集（タイム ゾーン情報およびvSphere Data Protection認証情報）ができます。
- アプライアンスのロールバック：アプライアンスを既知の有効な状態にリストアすることができます（35ページの“チェックポイントとロールバックの使用”を参照）。
- アップグレード：vSphere Data ProtectionアプライアンスのISOイメージをアップグレードできます。

［ステータス］タブ

［ステータス］タブは、vSphere Data Protectionサービスの表示（および停止または開始）に使用されます。

ステータスオプションの管理

［ステータス］タブの左側画面には、vSphere Data Protectionアプライアンスの主要サービスのステータスが表示されます。以下のサービスのステータスが表示されます。

表 2-2. vSphere Data Protection アプライアンスで実行されるサービスの概要

サービス	説明
コア サービス	アプライアンスのバックアップ エンジンで構成されるサービスです。これらのサービスが無効にされている場合、スケジュールされている、または「オン デマンド」のバックアップ ジョブはすべて実行されません。また、リストア アクティビティも開始されません。
管理サービス	管理サービスを停止する場合は、必ずテクニカル サポートの指示を受けてください。
ファイルシステム サービス	バックアップをファイル レベル リストア操作にマウントできるようにするサービスです。
ファイル レベルのリストア	ファイル レベルのリカバリ操作の管理をサポートするサービスです。

表 2-2. vSphere Data Protection アプライアンスで実行されるサービスの概要

サービス	説明
メンテナンス サービス	バックアップの保存期間が過ぎたかどうかの審査など、メンテナンス タスクを実行するサービスです。メンテナンス サービスは、vSphere Data Protectionアプライアンスの操作後、最初の24～48時間は無効です。これは、最初のバックアップの完了のための付加時間となります。
バックアップ スケジューラ	バックアップ スケジューラは、スケジュールされたバックアップ ジョブを開始するサービスです。このサービスが停止されると、スケジュールされたバックアップは実行されなくなりますが、「オン デマンド」のバックアップは開始できます。

上述のサービスについて表示されるステータスは、次のとおりです。

- 開始
- 開始失敗
- 実行中
- 停止中
- 停止失敗
- 停止
- ロード/取得状態
- リカバリ不能（コア サービスのみ）
- リストア中（メンテナンス サービスのみ）
- リストア失敗（管理サービスのみ）

サービスの開始と停止

ステータス画面で、**[開始]** をクリックして停止されているサービスを開始したり、**[停止]** をクリックして実行中のサービスを停止することができます。一般的には、実行中のサービスを停止する場合は、必ず技術サポートの指示を受ける必要があります。

サービスが停止されている場合、**[開始]** をクリックして再開を試みることはできますが、サービスが正常に機能するには追加でトラブルシューティングの手順が必要になる場合もあります。

ログ ファイルの収集

ログ ファイル バンドルは、サポート担当者へのvSphere Data Protectionアプライアンスのログ送信を円滑にすることが目的です。**[ログ収集]** をクリックすると、vSphere Data Protectionサービスから「バンドルされたログ」としてすべてのログをダウンロードできます。Webブラウザが実行されているマシンのファイル システムにログ バンドルをダウンロードする［名前を付けて保存］ダイアログが表示されます。ログ バンドルは「LogBundle.zip」に名称変更されます。

［構成］タブ

［構成］タブは、vSphere Data Protection構成の表示および編集に使用されます。

vSphere Data Protectionは表示および編集が可能であり、以下の項目が含まれます。

- ネットワーク設定
  - IPアドレス
  - ネットマスク
  - ゲートウェイ
  - プライマリDNS
  - セカンダリDNS

- ホスト名
- ドメイン

- vCenterの登録
  - vCenterユーザー名
  - vCenterパスワード
  - vCenterホスト名
  - vCenterポート
  - SSOホスト名
  - SSOポート
- システム設定
  - タイム ゾーン
  - VDP認証情報（VDPパスワードの変更）

［ロール バック］タブ

［ロール バック］タブを使用すると、vSphere Data Protectionデータが破損した際、既知のチェックポイントにロール バックできます。

注 ロール バックの使用方法は、35 ページの“チェックポイントとロールバックの使用”に記載されています。

［アップグレード］タブ

［アップグレード］タブを使用すると、ISO images on the vSphere Data Protectionアプライアンス のISOイメージをアップグレードできます。

注 アップグレードの実行方法は、19ページの“VDP構成の使用方法”に記載されています。

VDP構成の使用方法

VDP構成は、インストール後の構成に使用します。

動作条件

vSphere Data Protectionアプライアンスは、インストールおよび構成後、vSphere Data Protection管理用アカウントでログインする必要があります。

手順

1 Webブラウザを開き、以下のように入力します。

https://<VDPアプライアンスのIPアドレス>:8543/vdp-configure/

2 VMwareログイン画面で、以下を入力します。

a ユーザー：**root**

b パスワード：**VDPのパスワード**

c ［**ログイン**］をクリックします

3 （オプション）vSphere Data Protectionサービスを表示するには、**［ステータス］**タブをクリックします。vSphere Data Protectionサービスを停止または開始するには、関連する［停止］または［開始］ボタンをクリックします。

4 （VMwareサポートからの要求があった場合のオプション）サポート ログ ファイルを作成するには、**［ステータス］**タブをクリックして、**［ログ収集］**ボタンをクリックします。ログ バンドル ファイルを保存し、VMwareサポートの指示に従ってファイルを送信します。

5 （オプション）vSphere Data Protection構成を表示および編集するには、**［ステータス］**タブをクリックします。

- ネットワーク設定を行うには、構成を表示および編集します。構成を変更する場合は、**［保存］**ボタンをクリックします。
- vCenterの登録を行うには、設定を編集します。設定を編集するには、ロック アイコンをクリックします。vCenterの登録の設定に変更を加えると、現在のバックアップ ジョブの設定が失われ、バックアップ ジョブの再構成をする必要があります。変更後は、**［保存］**ボタンをクリックします。
- システム設定を行う場合は、タイム ゾーンの表示または編集で実行できます。タイム ゾーンを変更する場合は、**［保存］**ボタンをクリックします。vSphere Data Protectionのパスワードを変更するには、**［VDPパスワードの変更］**ボタンをクリックします。

vSphere Data Protection アプライアンスのアップグレード

アップグレード プロセスは以下の手順で行います。

1 vSphere Data Protectionアプライアンスのスナップショットの作成

2 アップグレードのインストール

3 スナップショットの削除

注 アプライアンスをアップグレードした後、最初のvSphere Webクライアントへのログインでは、vSphere Webクライアントは、オプションとしてvSphere Data Protectionを表示しません。vSphere Webクライアントからログアウトし、再度ログインする必要があります。それ以降のログインではオプションとしてvSphere Data Protectionが表示されます。

動作条件

ソフトウェアのアップグレードを行うには、ISOアップグレード イメージをダウンロードして、vSphere Data Protectionをすべて実行している必要があります。

vSphere Data Protectionアプライアンスのスナップショットの作成

インストール時、vSphere Data Protectionアプライアンスによって使用される仮想ディスクは［独立：永続的］に設定されます。ただし、スナップショットを作成するには、ディスクを一時的に［依存］に変更する必要があります。

vSphere Data Protectionアプライアンスのスナップショットを作成するには、以下の操作を実行します。

1 vSphere Webクライアントを使用して、ハードウェア設定の編集とスナップショットの作成を行う権限を持つユーザーとして、vCenter Serverにログインします。

2 **［ホストおよびクラスタ］**をクリックします。

3 vSphere Data Protectionアプライアンスが表示されるまで、左側のツリーの展開矢印をクリックします。

4 vSphere Data Protectionアプライアンスを右クリックし、**［ゲストOSのシャットダウン］**を選択します。

5 **［はい］**をクリックします。vSphere Data Protectionアプライアンスがシャットダウンするまで待ちます。これには数分かかる場合があります。

6 vSphere Data Protectionアプライアンスを右クリックし、**［設定の編集］**を選択します。

7 ハードディスク2から始めて、展開矢印をクリックします。

8 仮想ハードウェア テーブルのディスク モードの列で［**依存**］をクリックします。

9 ハードディスク3も操作を続行し、残りのディスクがすべて［依存］モードに設定されるまで手順8を繰り返します。

10 ［**OK**］をクリックします。

11 vSphere Data Protectionアプライアンスを右クリックし、［**すべてのvCenterのアクション**］＞［**スナップショット**］＞［**スナップショットの作成**］を選択します。

12 スナップショットの名前を入力します。オプションで説明を入力します。［**OK**］をクリックします。

13 vSphere Data Protectionアプライアンスを右クリックし、［**電源オン**］を選択します。

アップグレードのインストール

1 vSphere Webクライアントを使用して、管理者としてvCenterサーバにログインします。

2 ［**ホストおよびクラスタ**］をクリックします。

3 vSphere Data Protectionアプライアンスが表示されるまで、左側のツリーの展開矢印をクリックします。

4 vSphere Data Protectionアプライアンスを右クリックし、［**設定の編集**］を選択します。

5 ［仮想ハードウェア］タブで、CD/DVDドライブを展開します。ドロップダウン メニューから、［**データストアやISOファイル**］を選択します。

6 ファイルの選択で、ISOイメージに移動して選択します。［**OK**］をクリックします。

7 データストアISOの右で、［**接続**］ボックスを選択します。［**OK**］をクリックします。ISOのファイルのサイズによって、マウントするには最大5分間かかります。

8 Webブラウザを開き、以下のように入力します。

https://<VDPアプライアンスのIPアドレス>:8543/vdp-configure/

9 VMwareログイン画面で、以下を入力します。

a ユーザー：**root**

b パスワード：**VDPのパスワード**

c ［**ログイン**］をクリックします

10 ［**アップグレード**］タブをクリックします。ISOイメージが利用可能であり、ステータスの準備ができたことを確認します。利用できない場合は、ISOイメージがロード中の場合があります。

注 ISO イメージが表示されない場合は VDP-Configure からログアウトし、再度ログインします。

11 ［**VDP のアップグレード**］をクリックします。アップグレードはインストールを開始します。アップグレードのインストールには時間がかかる可能性がありますが、インストールの進捗状況はステータスバーに更新されます。

12 アップグレードのインストールが完了したら、［**OK**］をクリックします。vSphere Data Protectionアプライアンスを右クリックし、［**ゲストOSのシャットダウン**］を選択します。

スナップショットの削除

アップグレードが正常に完了したら、スナップショットの削除を強く推奨します。

スナップショットを削除するには、以下の操作を実行します。

1 vSphere Webクライアントを使用して、ハードウェア設定の編集とスナップショットの削除を行う権限を持つユーザーとして、vCenter Serverにログインします。

2 **［ホストおよびクラスタ］**をクリックします。

3 vSphere Data Protectionアプライアンスが表示されるまで、左側のツリーの展開矢印をクリックします。

4 vSphere Data Protectionアプライアンスを右クリックし、**［すべてのvCenterのアクション］＞［スナップショット］＞［スナップショット マネージャ］**を選択します。

5 vSphere Data Protectionアプライアンス用に作成したスナップショットをクリックします。

6 **［削除］**をクリックして、**［Yes］**をクリックします。

7 **［閉じる］**をクリックします。

8 vSphere Data Protectionアプライアンスを右クリックし、**［設定の編集］**を選択します。

9 ハード ディスク2から始めて、展開矢印をクリックします。

10 仮想ハードウェア テーブルのディスク モードの列で**［独立：永続的］**をクリックします。

11 ハード ディスク3も操作を続行し、残りのディスクがすべて［独立：永続的］モードに設定されるまで手順10を繰り返します。

12 ISOイメージをアンマウントします。［仮想ハードウェア］タブで、CD/DVDドライブを展開します。ドロップダウン メニューから、［クライアント デバイス］を選択します。**［OK］**をクリックします。

13 **［OK］**をクリックします。

14 vSphere Data Protectionアプライアンスを右クリックし、**［電源オン］**を選択します。

15 再起動完了後、vSphere Data Protectionアプライアンスを右クリックし、**［設定の編集］**を選択します。

vSphere Data Protectionアプライアンスのアップグレード プロセスが完了しました。

vSphere Data Protectionの使用

3

VDP（vSphere Data Protection）をインストールして構成した後は、vSphere Data Protection向けvSphere Webクライアントから管理することができます。

この章は、次のトピックで構成されています。

vSphere Data Protection のユーザー インタフェースを理解する

vSphere Data Protection向けvSphere Webクライアントは、vSphere Data Protectionの構成と管理に使用できる、数多くの新しいユーザー インタフェース要素を提供します。

vSphere Data Protectionのユーザー インタフェースは5つのタブから構成されています。

- **はじめに**：vSphere Data Protectionの機能の概要およびバックアップ ジョブの作成ウィザードとリストア ウィザードへのクイック リンクを提供します。
- **バックアップ**:スケジュールされたバックアップ ジョブの一覧と各バックアップ ジョブの詳細を提供します。バックアップ ジョブはこのページから作成し、編集できます。このページでは、バックアップ ジョブをただちに実行することもできます。
- **リストア**：リストア可能な成功したバックアップの一覧を表示します。
- **レポート**：vCenterの仮想マシンのバックアップ ステータス レポートを提供します。
- **構成**:vSphere Data Protectionの構成方法に関する情報を表示し、設定の一部を編集することができます。

これらの各タブについては、以降のセクションで説明します。

［はじめに］タブ

［はじめに］タブはvSphere Data Protectionについての導入情報および共通の構成タスクを開始する方法について説明します。

表 3-1.［はじめに］タブ

アイコン	名前	説明
	バックアップ ジョブを作成	バックアップ ジョブ ウィザードを起動します。詳細については、28ページの“バックアップ ジョブ ウィザードの使用”を参照してください。
	VMをリストア	仮想マシン リストア ウィザードを起動します。詳細については、30ページの“バックアップから仮想マシンをリストア”を参照してください。
	概要を参照	現在のビューを［レポート］タブに切り換えます。これにより、既存のジョブのステータスを表示する方法が示されます。詳細については、30ページの“レポートの表示”を参照してください。

［バックアップ］タブ

［バックアップ］タブは、既存のバックアップ ジョブに関する情報とそのステータスを表示します。また、非定型バックアップ ジョブの作成、編集、削除、有効化/無効化、実行方法も示します。

表 3-2.［バックアップ］タブ アイコン

アイコン	名前	説明
	新規	バックアップ ジョブ ウィザードを起動します。詳細については、28ページの“バックアップ ジョブ ウィザードの使用”を参照してください。
	編集	既存のジョブを編集するためにバックアップ ジョブ ウィザードを起動します。
	削除	選択されたバックアップ ジョブを削除します。
	有効/無効	バックアップ ジョブを有効または無効に設定します。
	今すぐバックアップ	非定型バックアップを起動します。

［バックアップ］タブは、作成されたバックアップ ジョブの一覧を表示します。バックアップ ジョブは、以下の情報を記載した表に一覧表示されます。

表 3-3.［バックアップ］タブのコラムの説明

コラム	説明
名前	バックアップ ジョブの名前。
状態	有効または無効。無効化されたバックアップは実行されません。
前回の開始時間	前回ジョブが開始された時間。
期間	前回実行されたジョブが要した時間。
次回の実行時間	次にジョブが実行されるようスケジュールされている時間。
成功数	前回実行されたバックアップ ジョブでバックアップに成功したVMの数。
失敗数	前回実行されたバックアップ ジョブでバックアップに失敗したVMの数。

［リストア］タブ

［リストア］タブは、vSphere Data Protectionアプライアンスにバックアップされた VMの一覧を表示します。バックアップの一覧をナビゲートし、特定のバックアップを選択して、リストアすることができます。時間が経過すると、［リストア］タブに表示される情報は期限切れになります。バックアップに関する最新情報を表示するには、**［更新］**をクリックします。

以下のアイコンは、［リストア］タブで使用されます。

表 3-4. ［リストア］タブ アイコン

アイコン	名前	説明
	リストア	バックアップから仮想マシンをリストアを起動します。これにより、選択したリストア ポイントで保存された状態に仮想マシンをリストアする構成方法が示されます。詳細については、30ページの“バックアップから仮想マシンをリストア”を参照してください。 デフォルトで、vSphere Data Protectionは、バックアップ ジョブで指定された保存ポリシーに従って、ストレージおよび古いリストア ポイントの最終削除を管理します。
	ロック/ロック解除	ロックは、バックアップ ジョブの有効期限ポイントを「終了日なし」に変更します。
	削除	選択されたリストア ポイントが削除されるように指定します。
	すべての選択を解除	［リストア］タブのすべての選択を解除します。

［レポート］タブ

［レポート］タブは、vSphere Data Protectionアプライアンスおよび仮想センターのVMに関する概要情報を示します。

［構成］タブ

［構成］タブにより、vSphere Data Protectionアプライアンスのメンテナンス タスクを管理することができます。このタブには、実行可能なタスクが 3 つあります。

- バックアップ ウィンドウの表示または編集（32ページの“バックアップ ウィンドウの構成”を参照）
- ヘルス チェックの実行（34ページの“手動でヘルス チェックを実行する”を参照）
- メールの構成（34ページの“メール通知の構成”を参照）

vSphere Data Protection へのアクセス

vSphere Data Protectionは、vSphere Webクライアントからアクセスされます。

注 vSphere Data Protectionを管理するのは、vSphere Webクライアントのみです。vSphereクライアントは、vSphere Data Protection管理をサポートしません。

動作条件

vSphere Data Protectionを使用する前に、11ページの“vSphere Data Protectionのインストールと構成”の説明のようにvSphere Data Protectionアプライアンスをインストールして構成する必要があります。

手順

1 Webブラウザから、vSphere Webクライアントにアクセスします。

https://<IP_address_vCenter_Server>:9443/vsphere-client/

2 ［認証情報］ページで、vCenterのユーザー名とパスワードを入力し、**［ログイン］**をクリックします。

vSphere Data Protectionはこの情報を使用してvCenterに接続し、バックアップを実行します。そのため、指定されたユーザー アカウントは管理者権限が必要です。

3 vSphere Webクライアントで、**vSphere Data Protection**を選択します。

4 ［vSphere Data Protectionへようこそ］ページで、vSphere Data Protectionアプライアンスを選択して、**［接続］**をクリックします。

vSphere Data Protection アプライアンスの切り換え

各vCenter Serverは、最大10台のvSphere Data Protectionアプライアンスをサポートします。［Switch Appliance］ラベルの右側にあるドロップダウン リストからアプライアンスを選択して、アプライアンスを切り換えることができます。

注 ドロップダウン リストのvSphere Data Protectionアプライアンスはアルファベット順にソートされており、画面に表示されるリストの最初の項目は現在のアプライアンスと一致しない場合があります。vSphere Data Protection画面の左側にあるアプライアンス名は現在のアプライアンスで、ドロップダウン リストのアプライアンス名は使用可能なアプライアンス リストの最初の項目です。

バックアップ ジョブを作成

バックアップ対象の仮想マシン、バックアップの頻度、バックアップの保存期間を含むバックアップ ジョブを作成できます。vSphere Data Protectionはバックアップ ウィンドウを使用して、新しいバックアップと保存ポリシーを作成するか、特定の古いバックアップを削除します。

仮想マシン

データセンター内のすべてのVMなどVMのコレクションを指定、あるいは、個々のVMを選択することができます。リソース プール全体、ホスト、データセンター、フォルダのいずれかが選択されると、そのコンテナのVMは以降のバックアップに含まれます。VMが1つ選択されると、そのVMに追加されたディスクはバックアップに含まれます。VMが選択されたコンテナから、選択されていない別のコンテナに移動されると、バックアップには含まれなくなります。

バックアップ対象のVMを手動で選択できます。それにより、たとえ移動されても、バックアップが確実に行われます。

注 vSphere Data Protection による vSphere Data Protection アプライアンスのバックアップはサポートされていません。

スケジュール

バックアップ スケジュールにより、選択したバックアップ対象のバックアップの頻度が決定されます。バックアップは、可能な限りバックアップ ウィンドウの開始近くで実行されます。バックアップは、毎日、毎週、特定の日に実行するようにスケジュール設定できます。

保存ポリシー

バックアップの保存ポリシーによって、システムにバックアップを保管する期間を指定できます。

保存ポリシーは、バックアップが行われるとき、各バックアップに割り当てられます。バックアップ保存の有効期限が切れると、バックアップは削除されます。

表 3-5 にバックアップの保存ポリシーに関する説明があります。

表 3-5. 保存ポリシーの設定

保存設定	説明
無期限	バックアップを無期限に維持することが可能です。システムが存続する限り、この保存ポリシーを割り当てたすべてのバックアップを保持する場合には、この設定が便利です。
期間（保存期間）	バックアップ実行後の固定保存期間を日、週、月、年で定義できます。たとえば、バックアップの有効期間が6か月後に切れるように指定することができます。
期限（終了日）	有効期限としてカレンダー日付を割り当てることが可能です。たとえば、バックアップが2013年12月31日に満了になるように指定できます。
期間（このスケジュール）	毎日、毎週、毎月、毎年の保存に基づいて固定保存期間を定義することが可能です。たとえば、バックアップが30日間毎日、52週間毎週、12か月間毎月、2年間毎年保持されるように指定することができます。

完了の準備

バックアップ ジョブの設定を確認します。このページには、次の情報が含まれています。

- バックアップ ジョブの名前。
- このジョブのバックアップ対象の仮想マシン。
- 仮想マシンのバックアップ スケジュール。
- バックアップに対して選択された保存ポリシー。

バックアップ ジョブ ウィザードの使用

バックアップ ジョブ ウィザードを使用して、バックアップ対象の仮想マシンとバックアップがいつ実行されるかを指定します。

手順

1 vSphere Webクライアントで、**vSphere Data Protection**を選択します。

2 ［vSphere Data Protectionへようこそ］ページで、vSphere Data Protectionアプライアンスを選択して、**［接続］**をクリックします。

3 **［バックアップ］**タブをクリックし、**［新規］**をクリックして、バックアップ ジョブ ウィザードを起動します。

4 ［仮想マシン］ページで、個々の仮想マシン、またはバックアップ対象の仮想マシンを含むコンテナを選択して、**［次へ］**をクリックします。

5 ［スケジュール］ページで、ジョブのバックアップ スケジュールを選択して、**［次へ］**をクリックします。

6 ［保存ポリシー］ページで、デフォルトの保存ポリシーを受け入れるか、代替保存ポリシーを指定して、**［次へ］**をクリックします。

7 ［名前］ページで、バックアップ ジョブの名前を入力して、**［次へ］**をクリックします。

8 ［完了の準備］ページで、バックアップ ジョブに関するサマリー情報を確認し、**［完了］**をクリックします。

9 情報ダイアログ ボックスで、バックアップ ジョブが正常に作成されたことを確認します。**［OK］**をクリックします。

今すぐバックアップ

バックアップ ジョブが作成された後、［今すぐバックアップ］アイコンからバックアップ ジョブを手動で開始することができます。

動作条件

［今すぐバックアップ］オプションを使用する前に、vSphere Data Protectionをインストールして構成しておく必要があります。また、バックアップ ジョブが少なくとも1つ必要です。

手順

1 vSphere Webクライアントで、**vSphere Data Protection**を選択します。

2 ［vSphere Data Protectionへようこそ］ページで、vSphere Data Protectionアプライアンスを選択して、**［接続］**をクリックします。

3 **［バックアップ］**タブをクリックして、バックアップ ジョブを選択します。**［今すぐバックアップ］**をクリックして、［すべてのソースをバックアップ］または［古いソースのみをバックアップ］のいずれかを選択します。

   - ［すべてのソースをバックアップ］では、バックアップ対象のすべてのソースを指定します。
   - ［古いソースのみをバックアップ］では、前回のバックアップに失敗したバックアップ ジョブを指定します。

仮想マシンのリストア

リストアする仮想マシン、リストアの方法、リストア先を、仮想マシン リストア ウィザードを使用して指定することができます。

注意 リストア先の VM にスナップショットがある場合は、リストアは失敗します。リストア プロセスを開始する前に、スナップショットを VM から削除してください。

バックアップを選択

［バックアップを選択］では、リストア対象の仮想マシンを指定します。リストアはバックアップ ジョブの作成と似ています。仮想マシンのコンテナまたは特定の仮想マシンを指定することができます。仮想マシンを代替の場所にリストアすることが可能です。

リストア オプションを設定

［リストア オプションを設定］では、バックアップのリストア先を指定します。

以下を指定できます。

- バックアップが元の場所にリストアされる場合
- バックアップが代替の場所にリストアされる場合
  - 新しい名前
  - ターゲット
  - データストアの場所

仮想マシンのクローンを作成するには、リストアする仮想マシンを名称変更します。

完了の準備

リストア ジョブの設定を確認します。サマリーには、リストアされるVMの数および作成されるVMの数に関する情報が含まれます。

バックアップから仮想マシンをリストア

仮想マシン リストア ウィザードを使用して、仮想マシンを以前のバックアップ状態にリストアします。

動作条件

仮想マシンをリストアする前に、vSphere Data Protectionを構成しておく必要があり、リストア元にバックアップが少なくとも1つ必要です。

手順

1 vSphere Webクライアントで、**vSphere Data Protection**を選択します。

2 ［vSphere Data Protectionへようこそ］ページで、vSphere Data Protectionアプライアンスを選択して、**［接続］**をクリックします。

3 **［リストア］**タブをクリックして、**［リストア］**ボタンをクリックします。

4 仮想マシン リストア ウィザードが表示されます。

5 ［バックアップを選択］ページで、仮想マシンのリストア元のソースを指定して、**［次へ］**をクリックします。

6 VMに複数のバックアップ　ポイントがある場合は、リストアしないポイントをすべて選択解除します。バックアップ ポイントは、1つだけ選択してください。

7 ［リストア オプションを設定］ページで、クライアント リストア ポイントおよびバックアップ リストア ポイントが正しいことを確認します。［元の場所にリストアする］を選択するか、代替の場所にリストアする場合は、［元の場所にリストアする］チェックボックスをオフにして、代替のターゲットとデータストアを指定します。**［次へ］**をクリックします。

8 ［完了の準備］ページで、構成を確認し、**［完了］**をクリックします。

仮想マシンは、ウィザードで指定したようにリストアされます。

リストア ジョブの進行状況の表示

リストア ジョブが開始された後、［最近のタスク］パネルに現在のリストアの進行状況が表示されます。

バックアップ ジョブのロック

［ロック］アイコンを使用して、バックアップ ジョブの有効期限ポイントを“終了日なし”に変更します。これにより、バックアップ ジョブが手動で期限切れになることがなくなり、また、有効期限を過ぎた後に自動的に削除されることもなくなります。ロック オプションはバックアップ ジョブの削除を防止できません。管理者はロックされているジョブを手動で削除できます。バックアップ ジョブをロックするには、［リストア］タブでバックアップを選択し、［ロック］アイコンをクリックします。ロックされているバックアップは、バックアップ ジョブ名の左側に黄色の鍵が表示されます。

レポートの表示

［レポート］タブは、現在のステータスを表示します。

- アプライアンス ステータス
- 使用済み容量
- ヘルス チェック ステータス
- 最近成功したバックアップ
- 最近失敗したバックアップ

［レポート］タブのフィルタリング

デフォルトで、［レポート］タブは、vCenter Serverに関連づけられているすべての仮想マシンを表示します。［レポート］タブの［フィルタ］オプションは以下のとおりです。

- すべて表示
- 仮想マシン
  - 名前
  - 状態
  - 最終正常バックアップ
- 前回のバックアップ ジョブ
  - 名前
  - ステータス
  - 日付

構成の管理

［構成］タブは、構成情報の表示および変更に使用されます。以下のトピックはこのセクションで取り上げています。

- 31ページの“バックアップ アプライアンスの詳細の表示と編集”
- 32ページの“バックアップ ウィンドウの構成”
- 33ページの“メンテナンス ウィンドウ設定を変更する”
- 34ページの“手動でヘルス チェックを実行する”
- 34ページの“メール通知の構成”

バックアップ アプライアンスの詳細、ストレージの概要、バックアップ ウィンドウの構成を、［構成］タブから表示することができます。

バックアップ アプライアンスの詳細の表示と編集

バックアップ アプライアンスの詳細には以下の情報が含まれます。

- IPアドレス
- VDPアプライアンスのバージョン
- ステータス
- vCenter Server
- 現在のユーザー
- ローカル時間
- タイム ゾーン
- 空き領域
- 重複排除されたサイズ
- 重複排除されていないサイズ

注 ストレージ容量は、GiB（GB ではない）、すなわち 1,024 MB 単位で表示されます。

バックアップ ウィンドウの構成

1日24時間をバックアップ、サービス停止、メンテナンスの3つのオペレーション ウィンドウに分割し、その間に、さまざまなシステム アクティビティが実行されます。

バックアップ ウィンドウ

バックアップ ウィンドウは、通常のスケジュールされたバックアップを実行するためにリザーブされている1日の割り当て分です。

- オペレーショナル インパクト : デフォルトで、バックアップ ウィンドウ中、メンテナンス アクティビティは実行されません。
- デフォルト設定 : デフォルトのバックアップ ウィンドウは、ローカル サーバ時間の午後8時に開始し、翌朝の午前8時まで12時間にわたり、中断なく続行されます。
- カスタマイズ : バックアップ ウィンドウの開始時間と期間は、特定のサイトの要件に合うようにカスタマイズできます。

vSphere Data Protectionは、バックアップ ウィンドウ中、1日に1回、ジョブ内の各仮想マシンのバックアップを試みます。バックアップは、バックアップ ウィンドウの先頭で開始され、一度に最大8個のバックアップ ジョブを実行できます。

注 同じ仮想マシンをバックアップする vSphere Data Protection アプライアンスが複数ある場合、異なるアプライアンスのバックアップ ジョブが重複しないようにバックアップ ウィンドウを調整する必要があります。バックアップ ジョブが重複すると、バックアップが失敗します。

サービス停止ウィンドウ

サービス停止ウィンドウは、ガベージ コレクションなどのサーバ メンテナンス アクティビティを実行するためにリザーブされている1日の割り当て分で、サーバへの無制限アクセスが必要です。ガベージ コレクションは、システムに保存されているバックアップ内で参照されなくなったデータの孤立したチャンクを削除します。

- オペレーショナル インパクト : サービス停止ウィンドウでは、バックアップまたは管理アクティビティは許可されていません。リストアは実行できます。
- デフォルト設定 : デフォルトのサービス停止ウィンドウは、ローカル サーバ時間の午前8時に開始し、同日の午前11時まで3時間にわたり、中断なく続行されます。
- カスタマイズ : サービス停止ウィンドウ期間は、特定のサイトの要件に合うようにカスタマイズできます。

サービス停止ウィンドウの期間を変更すると、メンテナンス ウィンドウの期間にも影響します。たとえば、サービス停止ウィンドウの期間を3時間から2時間に変更すると、1時間早く開始されることになるため、メンテナンス ウィンドウの期間が1時間延長されます。バックアップ ウィンドウは影響を受けません。

メンテナンス ウィンドウ

メンテナンス ウィンドウは、ヘルス チェックなど、所定のサーバ メンテナンス アクティビティにリザーブされている1日の割り当て分です。

- オペレーショナル インパクト : 短時間の間、バックアップまたは管理アクティビティが許可されない場合があります。

  バックアップはメンテナンス ウィンドウの間に開始できますが、それを行うと、バックアップ アクティビティとメンテナンス アクティビティの両方に影響を及ぼします。そのため、メンテナンス ウィンドウではバックアップ アクティビティと管理アクティビティを最小限に抑えてください。ただし、リストアは実行してもかまいません。

  ヘルス チェックとバックアップが重複することは可能ですが、重複すると、I/Oリソースの競合が発生する可能性があり、両方のアクティビティが完了するまでにより長い時間がかかり、場合によっては失敗することもあります。
- デフォルト設定 : デフォルトのメンテナンス ウィンドウは、ローカル サーバ時間の午前11時に開始し、同日の午後8時まで9時間にわたり、中断なく続行されます。

- カスタマイズ：メンテナンス ウィンドウは直接カスタマイズすることはできませんが、その開始時間と期間は、バックアップ ウィンドウおよびサービス停止ウィンドウの設定に基づきます。

メンテナンス ウィンドウはサービス停止ウィンドウの直後に開始され、バックアップ ウィンドウの開始時刻まで続きます。

ヘルス チェック

このオペレーションは、重複排除ストアのデータの整合性を検証および維持するために実行されます。vSphere Data Protectionは、メンテナンス ウィンドウの間にインクリメンタルまたは完全ヘルス チェックを完了するように設計されています。インクリメンタル ヘルス チェックでは、最新の完全またはインクリメンタル ヘルス チェック以降に重複排除ストアに追加されたチェックポイントの整合性を検証します。また、vSphere Data Protectionは、1日1回、すべてのチェックポイントのヘルス チェックを実行するように設計されています。詳細については、35ページの“チェックポイントとロールバックの使用”を参照してください。

メンテナンス ウィンドウは、ヘルス チェックがコンピューティング リソースを消費する、あるいは、継続中のバックアップ オペレーションに干渉する状況を避けるために使用してください。結果的に、メンテナンス ウィンドウとバックアップ ウィンドウは、重複しないように定義されます。メンテナンスは、定義されたウィンドウ内で完了しない場合、停止されます。メンテナンスが停止されても、ターゲットは、バックアップやリストアなどの他のオペレーションからロック アウトされません。次にターゲット メンテナンス ウィンドウが開くと、オペレーションは、中止されたところから続行します。メンテナンス ウィンドウの構成に関する詳細は、33ページの“メンテナンス ウィンドウ設定を変更する”を参照してください。

また、ヘルス チェックは手動で開始することもできます。ヘルス チェックを手動で開始すると、常に、ターゲット全体の完全ヘルス チェックが実行され、メンテナンス ウィンドウは使用されません。通常、ヘルス チェック進行中は、バックアップおよびリストア処理は重複排除ストアから許可されます。削除のためにリストア ポイントが手動でマークされた場合、ヘルス チェック中、バックアップは許可されませんが、リストア処理は許可されます。ヘルス チェック中に破損したリストア ポイントが重複排除ストアに見つかった場合、削除のために破損したリストア ポイントにマークした後、手動ヘルス チェックを実行する必要があります。この手動で実行したヘルス チェックの間、バックアップおよびリストアは許可されません。ヘルス チェックの手動開始に関する詳細は、34ページの“手動でヘルス チェックを実行する”を参照してください。

vSphere Data Protectionは、ヘルス チェックの進行状況に関する情報を格納します。そのため、vSphere Data Protectionアプライアンスがヘルス チェックを停止した場合、チェックが停止したところから処理を再開できます。それによって、ヘルス チェックを完了した作業結果が失われることがなくなります。アプライアンスは、メンテナンス ウィンドウが終わるとヘルス チェックを停止します。進行状況を追跡すると、ヘルス チェックの完了を確認できます。ユーザー介入により手動で停止されたヘルス チェックは、進行状況情報を保存しません。そのため、このような停止の後は、ヘルス チェックは再度、最初から開始されます。

メンテナンス ウィンドウ設定を変更する

［構成］タブから、メンテナンス ウィンドウ設定を変更します。

動作条件

メンテナンス ウィンドウ設定を変更する前に、vSphere Data Protectionをインストールして構成しておく必要があります。

手順

1 vSphere Webクライアントで、**vSphere Data Protection**を選択します。

2 ［vSphere Data Protectionへようこそ］ページで、vSphere Data Protectionアプライアンスを選択して、**［接続］**をクリックします。

3 **［構成］**タブをクリックします。

4 バックアップ ウィンドウの構成で、**［編集］**をクリックします。

5 バックアップ開始時間、バックアップ期間、サービス停止期間を選択して、**［保存］**をクリックします。

手動でヘルス チェックを実行する

ヘルス チェックは、［構成］タブから手動で実行できます。

動作条件

ヘルス チェックを実行する前に、vSphere Data Protectionを構成しておく必要があります。

手順

1 vSphere Webクライアントで、**vSphere Data Protection**を選択します。

2 ［vSphere Data Protectionへようこそ］ページで、vSphere Data Protectionアプライアンスを選択して、**［接続］**をクリックします。

3 **［構成］**タブをクリックします。

4 バックアップ ウィンドウの構成で、［設定］アイコン（［構成］タブの右上隅）をクリックし、**［ヘルス チェックを実行］**をクリックします。

5 確認ダイアログ ボックスが表示されます。**［はい］**をクリックします。

メール通知の構成

メール通知が有効な場合、以下の情報を含むメールが送信されます。

- VDPアプライアンスのステータス
- バックアップ ジョブのサマリー
- 仮想マシンのサマリー

動作条件

メール レポートを構成する前に、メール アカウントが存在している必要があります。

手順

1 vSphere Webクライアントで、**vSphere Data Protection**を選択します。

2 ［vSphere Data Protectionへようこそ］ページで、vSphere Data Protectionアプライアンスを選択して、**［接続］**をクリックします。

3 **［構成］**タブをクリックします。

4 **［メール］**ボタンをクリックします。

5 画面の右下側にある**［編集］**ボタンをクリックします。

6 以下を指定します。

   a **［メール レポートを有効化］**を選択します。

   b **［送信メール サーバ］**を指定します

   c （オプション）**［このサーバは本人がログインする必要があります］**を選択します。このオプションが選択した場合は、関連づけられた**［ユーザー名］**と**［パスワード］**を指定します。

   d **［差出人アドレス］**を指定します。

   e **［宛先アドレス］**を指定します。

   f **［送信日］**を選択します。

   g **［レポート ロケール］**を選択します。

7 **［保存］**ボタンをクリックします。

チェックポイントとロールバックの使用

チェックポイントは、災害復旧の支援を目的とするシステム全体のバックアップのことです。チェックポイントは、スケジュール設定され、メンテナンス ウィンドウの間に1日1回作成されます。これについては、32ページの“メンテナンス ウィンドウ”に説明があります。vSphere Data Protectionは2つのチェックポイントを格納します（1つは検証済み、もう1つは未検証）。ロールバックとは、検証済みチェックポイントに格納されているデータを使用して、既知の正常な状態にvSphere Data Protectionアプライアンスをリストアするプロセスのことです。デフォルトで、メンテナンス サービスは、アプライアンスの導入後、24～48時間、無効化されます。これにより、長時間のバックアップ ウィンドウが初期バックアップをサポート可能になります。

予期しないシャットダウンが発生すると、アプライアンスは、再起動した際、最新の検証済みチェックポイントにロールバックします。これは予期された動作であり、アライアンスの破損を避けるために使用されます。

アプライアンスが導入されると、非定型チェックポイントが作成されます。このチェックポイントには、インストール時のアプライアンス設定が含まれます。アプライアンスの導入後の最初の24～48時間の間に予期しないシャットダウンが発生すると、アプライアンスは非定型チェックポイントにロールバックします。非定型チェックポイントの作成と予期しないシャットダウンの間に作成されたバックアップ ジョブまたはバックアップは失われます。このウィンドウの間にチェックポイントを作成する場合は、ヘルス チェックを手動で実行してください。詳細については、34ページの“手動でヘルス チェックを実行する”を参照してください。

注 ロールバックを使用すると、選択したチェックポイントの後で発生したバックアップは失われます。

動作条件

ロールバックを実行する前に、vSphere Data Protectionをインストールして構成しておく必要があります。また、チェックポイントを作成して検証しておく必要もあります。

注意 最新の検証済みチェックポイントのみにロールバックすることを強く推奨します。

手順

1 Webブラウザを開き、以下のように入力します。

http://<IP_address_of_VDP_appliance>:8543/vdp-configure/

2 VMwareログイン画面で、以下を入力します。

a ユーザー：**root**

b パスワード：**VDPのパスワード**

c **［ログイン］**をクリックします

3 **［ロールバック］**タブをクリックします。

4 **［ロック解除してVDPのロールバックを有効にします］**をクリックします。

5 選択したチェックポイントの後で発生したバックアップは失われます、という警告ダイアログ ボックスが表示されます。受け入れられる場合は、vSphere Data Protectionアプライアンスのパスワードを入力して、**［OK］**をクリックします。

6 検証済みのチェックポイント（valid=true）を選択して、**［選択したチェックポイントへのVDPのロールバックを実行します］**をクリックします。

ファイル レベルのリカバリの使用

vSphere Data Protectionは、仮想マシン全体のバックアップを作成します。これらのバックアップは、vSphere Data Protection向けvSphere Webクライアントを使用して、完全な状態でリストアすることができます。ただし、これらの仮想マシンから特定のファイルのみリストアしたい場合は、vSphere Data Protectionリストア クライアントを使用してください。

このリストア クライアントにより、特定の仮想マシンのバックアップをファイル システムとしてマウントし、ファイル システムを「参照」して、リストアするファイルを見つけることができます。

リストア クライアントは、以下の2種類のモードのいずれかで操作できます。

- 基本：ログインするマシンから作成されたバックアップのみをマウントできます。リストアするファイルはこのクライアントにリストアされます。

  たとえば、「WS44」という名前のWindowsホストから基本モードでリストア クライアントにログインした場合は、「WS44」のバックアップのみをマウントして参照することができます。

- 高度：vSphere Data Protectionに含まれている任意のバックアップをマウントして参照できます。

一定の時間にマウントできるバックアップの最大数は8個です。

注 ファイル レベルのリカバリが設定されているファイルをリストアするには、リストア クライアントに接続する仮想マシンに VMware ツールがインストールされている必要があります。VMware ツールがインストールされている仮想マシンはリストア クライアントを使用して、VMware ツールがインストールされていないマシンのバックアップからファイルをリストアできますが、VMware ツールがインストールされていない仮想マシンは、リストア クライアントでバックアップされたファイルをリストアすることはできません。

注 リストア クライアントは、VMware vSphere vMotion または VMware vSphere Storage vMotion の使用をサポートしていません。

ファイル レベルのリカバリがサポートされる構成。

ファイル レベルのリカバリは以下のファイル システムのバックアップに対して実行できます。

- NTFS（MBRを持つプライマリ パーティション）
- Ext2（MBRを持つプライマリ パーティション）
- Ext3（MBRを持つプライマリ パーティション）
- ext2のLVM（MBRを持つプライマリ パーティションとext2のスタンドアロン［MBRなし］LVM）
- ext3のLVM（MBRを持つプライマリ パーティションとext3のスタンドアロン［MBRなし］LVM）

ファイル レベルのリカバリの制限

ファイル レベルのリカバリは以下の仮想ディスク構成をサポートしていません。

- 未フォーマット ディスク
- ダイナミック ディスク（Windows）/マルチ ドライブ パーティション（2台以上の仮想ディスクから構成されるパーティション）
- GPT（GUIDパーティション テーブル）ディスク
- ext4ファイルシステム
- FAT16ファイルシステム
- FAT32ファイルシステム
- 拡張パーティション
- 暗号化されたパーティション
- 圧縮されたパーティション

ファイル レベルのリカバリには以下の制限もあります。

- シンボリック リンクは、リストアまたは参照できない
- バックアップ内に含まれている特定のディレクトリ、またはリストア先の参照は、合計5,000個のファイルまたはフォルダに制限されている
- 同じリストア処理で5,000個を超えるフォルダまたはファイルをリストアすることはできない

以下の制限は、論理ボリューム マネージャによって管理されている論理ボリュームに適用されます。

- 1つの物理ボリューム（.vmdk）を正確に1つの論理ボリュームにマッピングする必要がある
- ext2およびext3フォーマットのみサポートされる

ログオン オプション

vSphere Data Protectionリストア クライアントは、以下の2つの方法のいずれかでログインできます。

ファイル レベルのリカバリ サービスは、バックアップがvSphere Data Protectionによって管理されている仮想マシンのみ利用可能です。つまり、リストア クライアントにログインするには、vSphere Data Protectionによってバックアップされた仮想マシンの1つに、vCenterコンソールまたはその他のリモート接続を介してログインする必要があります。

基本ログイン

基本ログインで接続するには、最初に、vSphere Data Protectionによってバックアップされた仮想マシンからリストア クライアントに接続する必要があります。ログインしている仮想マシンのローカル管理認証情報で、リストア クライアントにログインします。リストア クライアントは、ログインしている仮想マシンのバックアップのみ表示し、リストア済みのファイルはすべて現在ログインしている仮想マシンにリストアされます。

高度なログイン

高度なログインで接続するには、vSphere Data Protectionによってバックアップされた仮想マシンからリストア クライアントに接続する必要があります。ログインしている仮想マシンのローカル管理認証情報およびvCenterサーバへの管理認証情報で、リストア クライアントにログインします。リストア クライアントに接続後、vSphere Data Protectionによってバックアップされたあらゆる仮想マシンのファイルをマウント、参照、リストアできるようになります。リストア ファイルはすべて、現在ログインしている仮想マシンにリストアされます。

基本ログイン モードでリストア クライアントを使用する

WindowsまたはLinux仮想マシン上のリストア クライアントを基本ログイン モードで使用して、仮想マシン全体をリストアするのではなく、その仮想マシンのリストア ポイントから個々のファイルにアクセスします。

動作条件

vSphere Data Protectionバックアップの前に、VMにVMwareツールをインストールしておく必要があります（VMwareツールをサポートするオペレーティング システムの一覧いついては、VMwareのWebサイトを参照）。

リストア クライアントは以下のディスク タイプをサポートします。

- Windows（ベーシック ディスク、非拡張）：NTFS
- Linux（ベーシック ディスク、非拡張）：LVM、Ext 2、Ext 3

手順

1 リモート デスクトップ、またはvSphere Webクライアントを使用して、vSphere Data Protectionを通じてバックアップされたローカル ホストにアクセスします。

2 以下からvSphere Data Protectionリストア クライアントにアクセスします。

https://<IP_address_of_VDP_appliance>:8543/flr

3 ［ローカル認証情報］の下の［認証情報］ページで、ローカル ホストの［**ユーザー名**］と［**パスワード**］を指定し、［**ログイン**］をクリックします。

4 ［マウントされたバックアップを管理］ダイアログ ボックスが表示されます。ここには、アクセスするクライアントのすべてのリストア ポイントが一覧表示されます。リストアされるマウント ポイントを選択して、［**マウント**］をクリックします。

5 マウントが完了すると、ドライブ アイコンが緑色のネットワーク ドライブとして表示されます。 

6 **［閉じる］**をクリックします。

7 ［マウントされたバックアップ］ウィンドウで、リカバリするフォルダとファイルを選択します。

8 **［選択したファイルをリストア...］**をクリックします。

9 ［宛先を選択］ダイアログ ボックスで、リカバリ用のドライブと宛先フォルダを選択します。

10 **［リストア］**をクリックします。

11 ［リストア開始］確認ダイアログ ボックスが表示されたら、**［はい］**をクリックします。

12 ［正常に開始されました］ダイアログ ボックスが表示されたら、**［OK］**をクリックします。

13 **［リストアの監視］**タブをクリックしてリストアのステータスを表示します。

14 ジョブ ステータスが完了していることを確認します。

高度なログイン モードでリストア クライアントを使用する

WindowsまたはLinux仮想マシン上のリストア クライアントを高度なログイン モードで使用して、リストア ポイントを含むvCenter Server上の仮想マシンにアクセスし、ファイル レベルのリカバリを実行します。

動作条件

バックアップの前に、VMにVMwareツールをインストールしておく必要があります（VMwareツールをサポートするオペレーティング システムの一覧いついては、VMwareのWebサイトを参照）。

リストア クライアントは以下のディスク タイプをサポートします。

- Windows（ベーシック ディスク、非拡張）：NTFS
- Linux（ベーシック ディスク、非拡張）：LVM、Ext 2、Ext 3

手順

1 リモート デスクトップ、またはvSphere Webクライアントを使用して、仮想マシンにアクセスします。

2 以下からvSphere Data Protectionリストア クライアントにアクセスします。

https://<IP_address_of_VDP_appliance>:8543/flr

3 ［ローカル認証情報］の下の［認証情報］ページで、ローカル ホストの**［ユーザー名］**と**［パスワード］**を指定します。vCenter認証情報で、vCenter管理者**［ユーザー名］**と**［パスワード］**を指定して、**［ログイン］**をクリックします。

4 ［マウントされたバックアップを管理］ダイアログ ボックスが表示されます。ここには、アクセスするクライアントのすべてのリストア ポイントが一覧表示されます。リストアされるマウント ポイントを選択して、**［マウント］**をクリックします。

5 マウントが完了すると、ドライブアイコンが緑色のネットワーク ドライブとして表示されます。 

6 **［閉じる］**をクリックします。

7 ［マウントされたバックアップ］ウィンドウで、リカバリ用の仮想マシン、フォルダ、ファイルを選択します。

8 **［選択したファイルをリストア...］**をクリックします。

9 ［宛先を選択］ダイアログ ボックスで、リカバリ用のドライブと宛先フォルダを選択します。

10 **［リストア］**をクリックします。

11 ［リストア開始］確認ダイアログ ボックスが表示されたら、**［はい］**をクリックします。

12 ［正常に開始されました］ダイアログ ボックスが表示されたら、**［OK］**をクリックします。

［リストアの監視］タブをクリックしてリストアのステータスを表示し、リストアの完了時間を確認できます。

vSphere Data Protection のシャットダウンと起動手順

vSphere Data Protectionアプライアンスをシャットダウンする必要がある場合は、**［ゲストOSのシャットダウン］**アクションを使用します。このアクションにより、アプライアンスのクリーン シャットダウンが自動的に実行されます。［ゲストOSのシャットダウン］アクションが実行されずにアプライアンスをオフにすると、破損が発生する場合があります。アプライアンスがシャットダウンされた後、**［電源オン］**アクションで再起動することができます。

アプライアンスが適切にシャットダウンしない場合、再起動時に、最新の検証済みチェックポイントにロールバックします。チェックポイントと予期しないシャットダウンの間に発生するバックアップ ジョブまたはバックアップへの変更は失われるということです。これは予期されている動作であり、システムの破損が予期しないシャットダウンによって発生しないようにするために使用されます。詳細については、35ページの“チェックポイントとロールバックの使用”を参照してください。

重要 vSphere Data Protectionアプライアンスは、24時間365日メンテナンス操作をサポートし、また、リストア作業が行えるように設計されています。シャットダウンする特別な理由がない限り、シャットダウンしないでください。

vSphere Data Protectionの容量管理

4

この章では、vSphere Data Protectionの容量管理に重点を置き、次のトピックを取り上げます。

シンまたはシック プロビジョニングされたディスク選択の影響

vSphere Data Protectionデータストアに対してシンまたはシック プロビジョニングされたディスクを選択することにはメリットとデメリットがあります。

シン プロビジョニングでは、仮想化テクノロジーを使用し、物理的に利用可能なものよりも多くのディスク リソースの表示が可能になります。これは、管理者がディスク領域をアクティブに監視して、シン ディスクの増加に応じて物理ディスク領域を割り当てることができる場合に使用できます。これが管理されず、領域を割り当てることができないシン プロビジョニングされたディスク上にvSphere Data Protectionデータストアがある場合、vSphere Data Protectionアプライアンスは失敗します。これが発生した場合は、検証済みのチェックポイントにロール バックすることができます（補足情報については、35ページの“チェックポイントとロールバックの使用”を参照）。チェックポイントの後のバックアップは失われます。

シック プロビジョニングでは、ディスクが作成されると、すべての必要なストレージが割り当てられます。vSphere Data Protectionデータストアのベスト プラクティスは、vSphere Data Protectionアプライアンスが導入されたときにシン プロビジョニングされたディスクを作成し（迅速な導入が可能になる）、導入後、ディスクをシン プロビジョニングからシック プロビジョニングに変換することです。

シン プロビジョニングをシック プロビジョニングに変換するには、以下の手順を使用します。この手順では、vSphere Data Protectionアプライアンスをシャットダウンする必要があり、完了には数時間かかります。

動作条件

vSphere Data Protectionアプライアンスはシン プロビジョニングでインストールする必要があります。ディスクをシック プロビジョニングに拡張するために十分なディスク領域が必要です。

手順

1. vSphereクライアントで、vSphere Data Protectionアプライアンスを右クリックして、**[ゲストOSのシャットダウン]**を選択します。
2. アプライアンスをハイライト表示して、**[サマリー]**タブを選択します。**[ストレージ]**セクションで、データストアを右クリックして、**[データストアの参照...]**を選択します。
3. [データストア ブラウザ]画面から、アプライアンスを選択して、関連づけられているデータストアを展開します。
4. .vmdkファイルを右クリックして、**[拡張]**を選択します。
5. 各.vmdkファイルに対してこのステップを繰り返します。
   - 0.5 TB VDPの場合、.vmdkファイルは3個あります。
   - 1 TB VDPの場合、.vmdkファイルは7個あります。
   - 2 TB VDPの場合、.vmdkファイルは13個あります。

初期vSphere Data Protection導入に対するストレージ容量の影響

新しいvSphere Data Protectionアプライアンスを導入すると、アプライアンスは通常、最初の数週間で急速に一杯になります。これは、バックアップされるほぼすべてのクライアントに一意のデータが含まれているためです。vSphere Data Protectionの重複排除は、他の類似のクライアントがバックアップされている場合、または、同じクライアントが少なくとも1回バックアップされている場合に、最も活用されます。

初期バックアップの後、アプライアンスがその後のバックアップでバックアップする一意のデータは少なくなります。初期バックアップが完了し、最長保存期間を超えると、メンテナンス ウィンドウの間に容量を解放するとともに新しいデータを毎日どの程度保存できるかというシステムの能力を考慮して測定できます。

これは、安定状態の容量使用率と呼ばれます。理想的な安定状態の容量使用率は80%です。

vSphere Data Protectionの容量の監視

vSphere Data Protectionの容量をプロアクティブに監視してください。vSphere Data Protectionの容量は、［vSphere Data Protectionレポート］タブの［使用済み容量］から表示できます。

vSphere Data Protectionの容量の閾値

次の表は、主要な容量の閾値に対するvSphere Data Protectionの動作を示します。

表 4-1. vSphere Data Protection の容量の閾値

閾値	値	動作
容量警告	80%	vSphere Data Protectionは警告イベントを発行します。
ヘルス チェックの限度	95%	既存のバックアップは完了できますが、新しいバックアップ アクティビティはすべて一時停止されます。vSphere Data Protectionは警告イベントを発行します。
サーバ読み取り専用制限	100%	vSphere Data Protectionは、読み取り専用モードに移行し、新しいデータは許可されません。

容量管理

80%の容量を超えた場合、以下のガイドラインに従って容量管理を行ってください。

- バックアップ クライアントとしてのVMの追加を停止する
- 不要なバックアップ ジョブを削除する
- 保存ポリシーを再評価して、保存ポリシーを少なくできないか確認する
- vSphere Data Protectionアプライアンスの追加を考慮し、複数のアプライアンス間のバックアップ ジョブのバランスを調整する

vSphere Data Protectionのトラブルシューティング

5

この章は、次のトラブルシューティングのトピックで構成されています。

vSphere Data Protectionアプライアンスのインストール

vSphere Data Protectionアプライアンスのインストールで問題がある場合。

- すべてのソフトウェアがソフトウェアの最小要件を満たすことを確認します（12ページの“ソフトウェア要件”を参照）。
- ハードウェアが最小ハードウェア要件を満たすことを確認します（13ページの“システム要件”を参照）。
- DNSがvSphere Data Protectionアプライアンスに対して適切に構成されていることを確認します。（13ページの“プリインストール構成”を参照）。

vSphere Data Protectionバックアップ

以下は、vSphere Data Protectionバックアップに関する既知の問題です。

「バックアップ ジョブのデータを読み込んでいます」

このメッセージは、1つのバックアップ ジョブに対して多数のVM（100台未満）が選択されている場合に長時間表示される場合があります。この問題は、大きなジョブのロック/ロック解除、更新、削除アクションでも発生します。これは、非常に大きなジョブが選択された場合に予期されている動作です。このメッセージはアクションが完了すると消えますが、最長5分かかることがあります。

「{バックアップ ジョブ名}バックアップ ジョブの作成中、VDPアプライアンスに{クライアント名}クライアントを追加することができませんでした。」

このエラーは、vAppコンテナまたはESX/ESXiホストに重複するクライアント名がある場合に発生します。この場合、バックアップ ジョブは1つだけ追加されます。クライアント名の重複を解決してください。

「次のアイテムが見つからず、選択されませんでした {クライアント名}。」

このエラーは、バックアップされたVMがバックアップ ジョブの編集中に見つからない場合に発生します。これは既知の問題です。

Windows 2008 R2 VMは、「disk.EnableUUID」を「true」に構成すると、バックアップが失敗する場合があります。

VMは、disk.EnableUUIDをtrueに構成すると、Windows 2008 R2のバックアップに失敗する場合があります。この問題を解決するには、手動でvmx構成パラメータのdisk.EnableUUIDをfalseに更新することができます。

vSphere Webクライアントを使用して*disk.EnableUUID*を*false*に構成するには以下の操作を行います。

1 VM を右クリック、[**ゲストOSのシャットダウン**]を選択してVM をシャットダウンします。

2 VM を右クリックして、[**設定の編集**]を選択します。

3 [**VMオプション**]をクリックします。

4 [**詳細**]セクションを展開し、[**編集構成**]をクリックします。

5 disk.EnableUUId名を確認し値を*false*に設定します。

6 [**OK**]をクリックします。

7 [**OK**]をクリックします。

8 VMを右クリックし、[**電源オン**]をクリックします。

構成パラメータを更新すると、2008 R2 VMのバックアップは成功することになります。

vSphere Data Protectionデータストア容量が不足していると、バックアップが失敗します。

vSphere Data Protectionデータストア容量が不足していると、スケジュール設定されたバックアップは92%完了のところで失敗します。vSphere Data Protectionデータストアがシン プロビジョニングで構成されていて、最大容量に達していない場合は、ストレージ リソースを追加してください。vSphere Data Protectionデータストアがシック プロビジョニングで構成されていて、最大容量の場合は、41ページの“vSphere Data Protectionの容量管理”を参照してください。

VMでVMware Fault Toleranceが有効になっていると、バックアップが失敗します。

VMのフォルト トレランスが有効になっていると、バックアップは失敗します。これは予期された動作であり、vSphere Data Protectionはフォルト トレランスが有効化されているVMのバックアップをサポートしません。

VMが異なるクラスタ グループに、またはクラスタ グループから移動された場合、関連づけられたバックアップ ソースが失われることがあります。

ホストが、リソース プールとvAppを保持するオプションを持つクラスタに移動されると、コンテナが再作成され、コピーはされません。結果的に、名前は同じであっても同じコンテナではなくなります。クラスタに、またはクラスタからホストを移動した後、コンテナを保護するバックアップ ジョブを検証するか、再作成してください。

予期しないシャットダウンの後、最新のバックアップ ジョブとバックアップが失われます。

予期しないシャットダウンが発生すると、vSphere Data Protectionアプライアンスは最新の検証済みチェックポイントにロール バックします。これは予期された動作です。詳細については、35ページの“チェックポイントとロールバックの使用”を参照してください。

vSphere Data Protectionリストア

以下は、vSphere Data Protectionリストアに関する既知の問題です。

[リストア] タブに、「バックアップを読み込み中です」というメッセージが表示され、読み込みが遅くなります。

[リストア] タブでのそれぞれのバックアップのロードには、VMバックアップあたり2秒かかります。これは予期された動作です。

VMに関連づけられたスナップショットがある場合、元の場所へのリストアが失敗します。

VMに関連づけられたスナップショットがあると、元の場所へのリストアは失敗します。これは予期された動作であり、vSphere Data Protectionは、スナップショットを持つVMの元の場所へのリストアはサポートしません。VMを代替の場所にリストアするか、元の場所にリストアする前にスナップショットを削除してください。

ファイル レベルのリカバリ

以下は、vSphere Data Protectionリストア クライアントによるファイル レベルのリカバリに関する既知の問題です。

ファイル レベルのリカバリのマウントの間、VMDKファイルが複数のパーティションを含んでいる場合、最後のパーティションのみが表示されます。

リストア クライアントは、拡張ボリュームをサポートしません。これは予期された動作です。イメージ レベルのリカバリを実行して、手動で必要なファイルをコピーしてください。

ファイル レベルのリカバリのマウントの間、サポートされていないパーティションはマウントに失敗します。

リストア クライアントは以下のディスク フォーマットをサポートしないため、リストア クライアントがマウントに失敗するのは予期された動作です。

- 未フォーマット ディスク
- FAT32
- 拡張パーティション
- ダイナミック ディスク
- GPTディスク
- Ext4 fs
- 暗号化されたパーティション
- 圧縮されたパーティション

イメージ レベルのリストアを実行して、手動で必要なファイルをコピーしてください。

必要なファイルをコピーしてください。

シンボリック リンクがリストア クライアントに表示されません。

リストア クライアントは、シンボリック リンクの表示をサポートしていません。

vSphere Data Protectionのレポート作成

以下は、vSphere Data Protectionのレポート作成に関する既知の問題です。

［リストア］タブのロードまたは更新が遅い。

多数のVMがある場合、［リストア］タブはロードまたは更新が遅くなることがあります。テストでは、100台のVMの場合、最長4分半かかりました。

vSphere Data Protectionのポート利用

6

vSphere Data Protectionは次の表に記載されているポートを使用します。

表 6-1. vSphere Data Protection のポート利用

ポート	プロトコル	関連サービス
22	TCP	ssh
80	TCP	http
111	TCP	rpcbind
443	TCP	https
700	TCP	Loginmgrツール
5555	TCP	Postgres
5558	TCP	Postgres
7778	TCP	VDP RMI
7779	TCP	VDP RMI
8509	TCP	Tomcat AJPコネクタ
8543	TCP	Tomcatのリダイレクト
8580	TCP	VDPダウンローダ
9443	TCP	VDP Webサービス
25000	TCP/UDP	VDP内部通信
26000	TCP/UDP	VDP内部通信
27000	TCP	VDPクライアント サーバ通信
28001	TCP	VDP内部プロキシ
28002	TCP	VDP内部プロキシ
28003	TCP	VDP内部プロキシ
28004	TCP	VDP内部プロキシ
28005	TCP	VDP内部プロキシ
28006	TCP	VDP内部プロキシ
28007	TCP	VDP内部プロキシ
28008	TCP	VDP内部プロキシ
28009	TCP	VDP内部プロキシ
29000	TCP	VDP内部クライアントの安全な通信
34250	TCP	ssl/soap gSoap（ローカルホスト）
53	UDP	DNS
111	UDP	RPC
941	UDP	RPC

vSphere Data Protection災害復旧 7

vSphere Data Protectionは、バックアップの保存と管理能力に優れています。障害発生時には、最初に、既知の検証済みチェックポイントにロール バックします（35ページの“チェックポイントとロールバックの使用”を参照）。vSphere Data Protectionアプライアンスの障害から復旧するために、以下の手順で、災害復旧のための、アプライアンスのバックアップおよびすべての関連するvSphere Data Protectionバックアップを作成します。

以下は、vSphere Data Protection災害復旧のガイドラインです。

1 vSphere Data Protectionアプライアンスをシャットダウンする前に、バックアップ タスクやメンテナンス タスクが実行中でないことを確認します。使用するバックアップの方法およびバックアップに要する時間に応じて、何もタスクがスケジュールされていない時間帯に、vSphere Data Protectionバックアップをスケジュール設定します。たとえば、バックアップ ウィンドウが8時間で、バックアップの完了に要する時間がわずか1時間の場合、メンテナンス タスクのスケジュールの前にさらに7時間あります。これは、アプライアンスをシャットダウンしてバックアップするための理想的な時間です。詳細については、32ページの“バックアップ ウィンドウの構成”を参照してください。

2 vSphereクライアントで、アプライアンスを選択します。VMで［ゲストOSのシャットダウン］を実行します。電源はオフにしないでください。電源オフ タスクは、物理サーバの電源プラグを抜くのと同じことで、クリーン シャットダウンが実行されません。詳細については、39ページの“vSphere Data Protectionのシャットダウンと起動手順”を参照してください。

3 アプライアンスがシャットダウンされたことを確認して、選択した保護の方法に進んでください。

4 vSphere Data Protectionのバックアップが完了したこと、およびvSphere Data Protectionに対して実行中のバックアップ/スナップショット/コピーがないことを確認します。

5 vSphereクライアントから、アプライアンスの電源オンを実行します。

インデックス