Dell DL4300 アプライアンス
導入ガイド

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

© 2016 Dell Inc. 無断転載を禁じます。この製品は、米国および国際著作権法、ならびに米国および国際知的財産法で保護されています。Dell、および Dell のロゴは、米国および / またはその他管轄区域における Dell Inc. の商標です。本書で使用されているその他すべての商標および名称は、各社の商標である場合があります。

2016 - 09

Rev. A03

目次

1 DL4300 アプライアンスのセットアップ.....5

はじめに.....5

本書で使用される用語.....5

利用可能な構成.....5

インストールの必要条件.....6

ネットワーク要件.....6

推奨ネットワークインフラストラクチャ.....6

ハードウェアのセットアップ.....6

ラックへのアプライアンスの取り付け.....6

ストレージエンクロージャ設定スイッチの設定.....6

システムへのストレージエンクロージャの接続.....7

ケーブル処理アームの接続（オプション）.....8

アプライアンスの配線.....8

アプライアンスへの電源投入.....8

DL4300 ディスク設定.....8

2 ソフトウェアの初回セットアップ.....10

AppAssure アプライアンスの設定ウィザード.....10

ネットワークインタフェースの設定.....11

ホスト名とドメインの設定.....11

SNMP の設定.....12

Windows および RASR 仮想ディスクの作成.....12

DL アプライアンスの設定ウィザード.....13

ネットワークインタフェースの設定.....14

登録およびホスト設定.....14

アラートと監視.....15

アクセスと管理.....15

Windows バックアップの設定.....16

ストレージのプロビジョニング.....16

保持ポリシーおよびアップデートのオプションの設定.....17

Recovery and Update Utility.....18

Rapid Appliance Self Recovery.....18

RASR USB キーの作成.....18

RASR の実行.....19

内蔵デュアル SD モジュールを使用した RASR の実行.....20

ストレージのプロビジョニング.....20

Fibre Channel ストレージを使用した DL4300 の構成（オプション）.....22

3 インストール後のタスク.....23

Core Console へのアクセス.....23

Internet Explorer での信頼済みサイトのアップデート.....23

Core Console にリモートでアクセスするためのブラウザの設定 23
Internet Explorer と Chrome でのブラウザ設定 24
Firefox でのブラウザ設定 24
保持期間の確認 24
エージェントスナップショットデータの暗号化 25
電子メールサーバーと電子メール通知テンプレートの設定 25
ストリーム数の調整 26

4 サーバを保護する準備 27
概要 27
クライアントでのエージェントのインストール 27
エージェントを保護する時のエージェントソフトウェアの導入 27
Windows マシンでの Rapid Recovery Agent ソフトウェアのインストール 28
Rapid Recovery Agent ソフトウェアの 1 つまたは複数のマシンへの導入 29
Linux マシンでのエージェントソフトウェアのインストールについて 32
Linux Agent ファイルの場所 34
エージェントの依存関係 34
Debian または Ubuntu での Rapid Recovery Agent ソフトウェアのインストール 35
Suse Linux Enterprise Server での Rapid Recovery Agent ソフトウェアのインストール 35
Red Hat Enterprise Linux と CentOS でのエージェントのインストール 36
オフラインの Linux マシンでのエージェントソフトウェアのインストール 36
Windows Server Core Edition マシンでの Agent ソフトウェアのインストール 38
Linux マシンでの Rapid Recovery Agent の設定 38
マシンの保護 39
ネットワーク接続性のチェック 42
ファイアウォール設定のチェック 42
名前解決の確認（該当する場合） 42
ネットワークアダプタのチームミング 43

5 困ったときは 45
マニュアルおよびソフトウェアのアップデートの入手方法 45
ソフトウェアアップデートの入手方法 45
デルへのお問い合わせ 45
マニュアルのフィードバック 45

1

DL4300 アプライアンスのセットアップ

はじめに

Dell DL4300 アプライアンスは、最新世代の Backup To Disk Appliance – Powered By Rapid Recovery ソフトウェアです。このアプライアンスは次の機能を備えています。

- スケール可能なストレージ能力により、あらゆる規模の組織に対応。
- 従来のテープデバイスやバックアップ方法よりもさらに速いバックアップと迅速な回復。
- オプションの重複排除機能。
- データセンターおよびリモートオフィスサーバーに対する連続的なデータ保護。
- 迅速かつ容易な展開で、重要データの保護の準備に必要な時間を短縮。
- オプションの Fibre Channel 構成

本書で使用される用語

次の表には、本書で使用されている DL4300 アプライアンスの各種ハードウェアおよびソフトウェアのコンポーネントを示す用語がリストされています。

表 1. DL4300 アプライアンスハードウェアおよびソフトウェアコンポーネント

コンポーネント	使用されている用語
DL4300 アプライアンス	アプライアンス
Dell Storage MD1400 ストレージエンクロージャ	ストレージエンクロージャ
Dell AppAssure ソフトウェア	AppAssure
Rapid Recovery ソフトウェア	Rapid Recovery

利用可能な構成

DL アプライアンスには、Standard Edition および High Capacity Edition の 2 つの構成があります。

表 2. DL4300 Standard Edition 容量構成

容量	ハードウェア構成
5 TB	12 台の 1 TB ドライブ、4 台の 1 TB 内蔵ドライブ
10～20 TB	12 台の 2 TB ドライブ、4 台の 2 TB 内蔵ドライブ
30～40 TB	12 台の 4 TB ドライブ、4 台の 4 TB 内蔵ドライブ
50～60 TB	12 台の 6 TB ドライブ、4 台の 6 TB 内蔵ドライブ

表 3. DL4300 High Capacity Edition 容量構成

容量	ハードウェア構成
40 TB、50 TB、60 TB、70 TB、80 TB、90 TB、100 TB、110 TB、120 TB	12 台の 6 TB ドライブ、4 台の 6 TB 内蔵ドライブ

メモ: 追加ストレージは、拡張シェルフ（Dell Storage MD1400）の使用によって追加できます。追加のストレージを任意のモデルに追加することができますが、Standard Edition がサポートするストレージ容量は最大 60TB、High Capacity Edition がサポートするストレージ容量は最大 120TB です。いずれのエディションでも、最大 4 台の拡張シェルフをサポートしています。

各構成には次のハードウェアとソフトウェアも含まれます。

- Dell DL4300 システム
- Dell PowerEdge RAID コントローラ（PERC）
- プリインストールされた OS および Dell OpenManage システムとストレージ管理ソフトウェア
- AppAssure ソフトウェア

メモ: お使いのアプライアンスの設定に Dell Storage MD1400 ストレージエンクロージャが含まれていない場合は、Dell Storage MD1400 とストレージエンクロージャに関するこのマニュアルの記述は無視してください。

インストールの必要条件

ネットワーク要件

お使いのアプライアンスに必要なネットワーク環境は次のとおりです。

- 使用可能なイーサネットケーブルおよび接続を備えたアクティブなネットワーク
- Dynamic Host Configuration Protocol（DHCP）によって提供されない場合は、静的 IP アドレスおよび DNS サーバー IP アドレス
- Administrator 権限を持つユーザー名とパスワード

推奨ネットワークインフラストラクチャ

デルは、極めて優れた堅牢性を持つ環境のため、企業では Rapid Recovery、および 10 GbE ネットワークとの使用における効率的なパフォーマンスのために 1 GbE バックボーンを使用することをお勧めします。

ハードウェアのセットアップ

アプライアンスは、単一の DL4300 システムと共に出荷されます。アプライアンスハードウェアをセットアップする前に、アプライアンスに同梱されている『*Dell DL4300 Appliance Getting Started With Your System*』（Dell DL4300 Appliance はじめに）マニュアルを参照してください。DL アプライアンスハードウェアを開梱してセットアップします。

メモ: ソフトウェアはアプライアンスにプリインストールされています。システムに含まれているメディアはいずれも、システムリカバリが必要な場合以外は使用しないでください。

DL アプライアンスハードウェアをセットアップするには、次の手順を実行します。

1. DL4300 システムとストレージエンクロージャをラックに取り付け、配線します。
2. ストレージエンクロージャの電源を入れてから、DL4300 システムの電源を入れます。

ラックへのアプライアンスの取り付け

お使いのシステムにレールキットが含まれる場合は、ラックキットに同梱の『*Rack Installation Instructions*』（ラック取り付け手順）を取り出します。レールをラックユニットに取り付ける手順と、システムとストレージエンクロージャをラックに取り付ける手順に従ってください。

ストレージエンクロージャ設定スイッチの設定

以下の図に示すように、ストレージエンクロージャのストレージモードを統合モードに設定します。

メモ: 設定スイッチの設定はストレージエンクロージャの電源を入れる前に行う必要があります。ストレージエンクロージャに電源を入れた後に設定モードを変更しても、システムの電源サイクルを行うまではエンクロージャ設定には適用されません。詳細については、Dell.com/support/home で『*Dell Storage MD1400 Enclosures Hardware Owner's Manual*』（Dell Dell Storage MD1400 Enclosures ハードウェアオーナーズマニュアル）を参照してください。

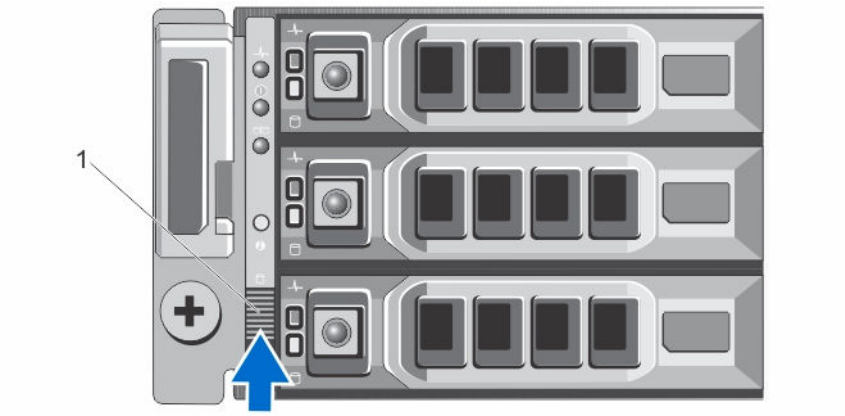

図 1. PowerVault MD1400 ストレージエンクロージャ設定スイッチの設定

1. 設定スイッチ

システムへのストレージエンクロージャの接続

データケーブルを、Dell DL4300 システムに取り付けられた PowerEdge RAID コントローラ（PERC）から、ストレージエンクロージャのプライマリエンクロージャ管理モジュール（EMM）SAS 入力ポートへ接続します。

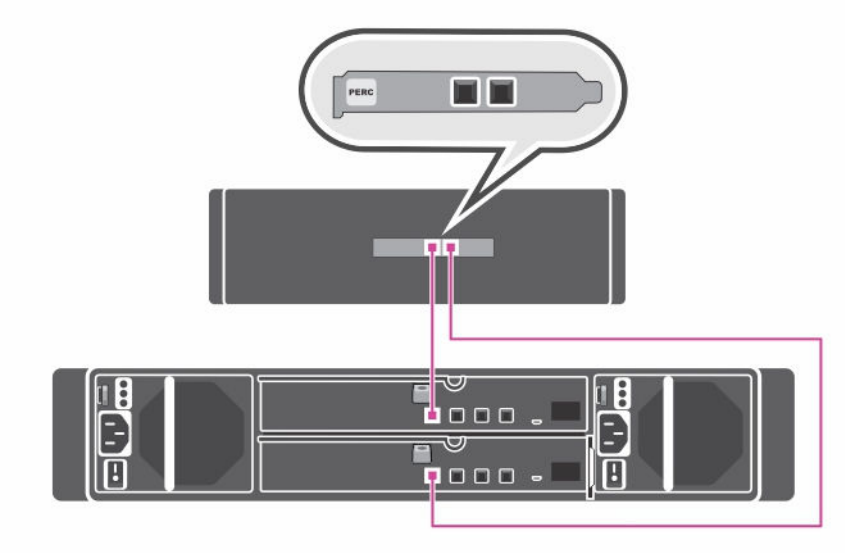

図 2. DL4300 システムから MD1400 ストレージエンクロージャへの接続

冗長ポートの構成

冗長ポートの構成には、次の手順を実行します。

1. 各 SAS ケーブルの一端を、DL4300 システム PERC コントローラのポート 0 とポート 1 に接続します。
2. SAS ケーブルのもう一方の端を、MD1400 ストレージ エンクロージャにある各エンクロージャ管理モジュール（EMM）のポート 1 に接続します。

シングルポート構成

シングルポートの構成については、次の手順を実行します。

1. SAS ケーブルの一端を、DL4300 システム PERC コントローラのポート 0 に接続します。
2. SAS ケーブルのもう一方の端を、MD1400 ストレージ エンクロージャにあるエンクロージャ管理モジュール（EMM）のポート 1 に接続します。

マルチチェーン設定

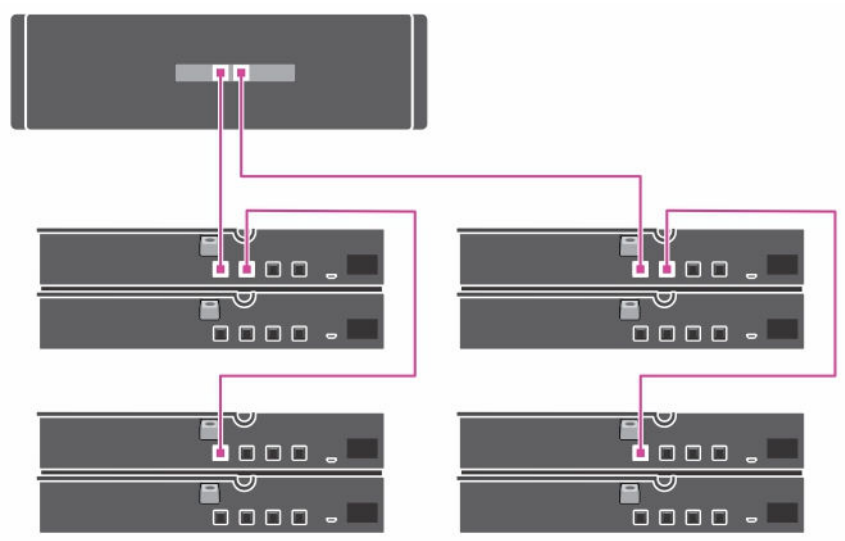

図 3. マルチチェーン設定

マルチチェーン構成は最大 4 台のエンクロージャーをサポートします。最初 2 台のエンクロージャはデイジーチェーン接続されており、そのうち 1 台のエンクロージャがコントローラカードの単一ポートに接続されています。2 組目の 2 台のエンクロージャもデイジーチェーン接続されており、そのうち 1 台のエンクロージャがコントローラカードの 2 番目のポートに接続されています。

ケーブル処理アームの接続（オプション）

アプライアンスにケーブル処理アーム（CMA）が含まれている場合は、CMA キットに同梱の『*CMA の取り付け手順*』を取り出し、その説明に従って CMA を取り付けます。

アプライアンスの配線

Dell.com/support/home で、アプライアンスに同梱されている『*Getting Started With Your System*』（はじめに）マニュアルを参照します。手順に従い、キーボード、マウス、モニタ、電源、およびネットワークケーブルをアプライアンスに接続します。

アプライアンスへの電源投入

アプライアンスのケーブル配線後、MD1400 ストレージエンクロージャの電源を入れ、次に DL4300 システムの電源を入れます。

メモ: 最高の信頼性と可用性を得るために、アプライアンスを無停電電源装置（UPS）に接続することをお勧めします。

DL4300 ディスク設定

DL4300 は二アライン SAS ドライブおよび SAS ドライブの両方をサポートしています。OS は、スロット 12 および 13 にある RAID 1（ミラー）仮想ディスク上に格納されています。これらのディスクの詳細については、**Dell.com/support/home** の『*Dell*

DL4300 Owner's Manual』（Dell DL4300 オーナーズマニュアル）を参照してください。スロット 0〜11 と 14〜17 で使用可能なドライブは、AppAssure アプライアンス設定ウィザード（推奨）を使用して自動的に設定できますが、必要に応じて手動でカスタム設定を行うことも可能です。ディスクは、RAID 6 として自動的にプロビジョニングされます。オプションで、MD1400 ストレージエンクロージャを使用して容量を拡張できます。

2

ソフトウェアの初回セットアップ

初めてアプライアンスの電源を入れ、システムパスワードを変更した後に **AppAssure Appliance Configuration Wizard**（AppAssure アプライアンス設定ウィザード）が自動的に実行されます。

1. システムの電源を入れた後に、Windows 言語オプションからお使いのオペレーティングシステムの言語を選択します。
   Settings（設定）ページに Microsoft EULA（エンドユーザーライセンス契約）が表示されます。
2. エンドユーザー使用許諾条件に同意するには、**I accept**（同意する）ボタンをクリックします。
   管理者パスワードを変更する画面が表示されます。
3. 管理者パスワードの変更を求めるメッセージで **OK** をクリックします。
4. 新しいパスワードを入力して確認します。
   パスワードの変更を確認するメッセージが表示されます。
5. **OK** をクリックします。
6. **Dell readme.htm** 画面から、スクロールダウンして **Proceed**（続行）をクリックします。
7. 変更済みの管理者パスワードを使用してログインします。
   Select the language for AppAssure Appliance（AppAssure アプライアンスの言語の選択）画面が表示されます。
8. 対応言語のリストからお使いのアプライアンス用の言語を選択します。
   AppAssure Appliance Configuration Wizard（AppAssure アプライアンス設定ウィザード）のようこそ画面が表示されます。

メモ: AppAssure Appliance Configuration Wizard（AppAssure アプライアンス設定ウィザード）は、システムコンソール上に表示されるまでに最大 30 秒かかる場合があります。

メモ: AppAssure Appliance Configuration Wizard（AppAssure アプライアンス設定ウィザード）を閉じずに、すべての作業を完了してください。

AppAssure アプライアンスの設定ウィザード

注意: アプライアンスで他のタスクや設定の変更を実行する前に、AppAssure Appliance Configuration Wizard（AppAssure アプライアンス設定ウィザード）のすべての手順が完了していることを確認します。ウィザードを完了するまで、Control Panel（コントロールパネル）を使用して変更を行ったり、Microsoft Windows Update を使用したり、AppAssure ソフトウェアを更新したり、ライセンスをインストールしたりしないでください。

AppAssure Appliance Configuration Wizard（AppAssure アプライアンス設定ウィザード）は、アプライアンスのソフトウェアを設定するための次の手順をガイドします。

- ネットワークインタフェースの設定
- ホスト名とドメインの設定
- SNMP の設定
- Windows および RASR 仮想ディスクの作成

ウィザードを使用したインストールが完了したら、Core Console が自動的に起動します。

ネットワークインタフェースの設定

使用可能なネットワークインタフェースを設定するには、次の手順を実行します。

1. **AppAssure Appliance Configuration Wizard Welcome**（AppAssure アプライアンス設定ウィザード - ようこそ）画面で、**Next**（次へ）をクリックします。

   network interfaces（ネットワークインタフェース）ページでは、接続されている使用可能なネットワークインタフェースが表示されます。
2. 設定するネットワークインタフェースを選択します。

   メモ: **AppAssure Appliance Configuration Wizard**（**AppAsure** アプライアンス設定ウィザード）は、ネットワークインタフェースを個別のポート（チーミングされていない）として設定します。処理パフォーマンスを向上させるため、**NIC** をチームミングすることによって、より大きい処理チャネルを作成できますが、これはアプライアンスの初期設定後に行う必要があります。
3. 必要に応じて、追加のネットワークインタフェースを接続して **Refresh**（更新）をクリックします。

   追加の接続済みネットワークインタフェースが表示されます。
4. **次へ** をクリックします。

   Configure selected network interface（選択されたネットワークインタフェースの設定）ページが表示されます。
5. 選択されたインタフェースに適切なインターネットプロトコルを選択します。

   IPv4 または **IPv6** を選択できます。

   選択したインターネットプロトコルに応じてネットワークの詳細が表示されます。
6. インターネットプロトコル詳細を割り当てるには、次のいずれかを行います。
   - 選択したインターネットプロトコル詳細を自動的に設定するには、**Obtain an IPV4 address automatically**（IPV4 アドレスを自動的に取得する）を選択します。
   - ネットワーク接続を手動で割り当てるには、**Use the following IPv4 address**（次の IPv4 アドレスを使用する）を選択して次の詳細を入力します。
     - **IPv4 Address**（IPv4 アドレス）または **IPv6 Address**（IPv6 アドレス）
     - IPv4 の **Subnet mask**（サブネットマスク）および IPv6 の **Subnet prefix length**（サブネットプレフィックス長）
     - デフォルトゲートウェイ
7. DNS サーバー詳細を割り当てるには、次のいずれかを行います。
   - DNS サーバーアドレスを自動的に設定するには、**Obtain DNS server address automatically**（DNS サーバーアドレスを自動的に取得する）を選択します。
   - DNS サーバーを手動で設定するには、**Use the following DNS server address**（次の DNS サーバーアドレスを使用する）を選択して次の詳細を入力します。
     - **Preferred DNS sever**（優先 DNS サーバー）
     - **Alternate DNS server**（代替 DNS サーバー）
8. **次へ** をクリックします。

   Configure hostname and domain setting（ホスト名とドメインの設定）ページが表示されます。

NIC チーミングについての情報は、「ネットワークアダプタのチームミング」を参照してください。

ホスト名とドメインの設定

アプライアンスにはホスト名を割り当てる必要があります。ホスト名は、バックアップを開始する前に変更することをお勧めします。デフォルトでは、ホスト名はオペレーティングシステムが割り当てるシステム名です。

メモ: ホスト名を変更する予定の場合は、この段階で変更することが推奨されます。**AppAssure Appliance Configuration**（**AppAssure** アプライアンスの設定）ウィザード完了後のホスト名の変更には、いくつかの手順を手動で行う必要が生じます。

ホスト名とドメインを設定するには、次の手順を実行します。

1. **Configure hostname and domain setting**（ホスト名とドメインの設定）ページで、アプライアンスのホスト名を変更するために **New hostname**（新しいホスト名）に適切なホスト名を入力します。
2. アプライアンスをドメインに参加させたくない場合は、**Do you want this appliance to join a domain?**（このアプライアンスをドメインに参加させますか?）で **No**（いいえ）を選択します。

   デフォルトでは **Yes**（はい） が選択されています。
3. アプライアンスをドメインに参加させるには、次の詳細を入力します。
   - ドメイン名
   - ドメインユーザー名

     メモ: ドメインユーザーは、ローカル管理者権限を持つ必要があります。
   - ドメインユーザーパスワード
4. 次へ をクリックします。

   メモ: ホスト名またはドメインの変更にはマシンの再起動が必要です。マシンの再起動後、**AppAssure Appliance Configuration wizard**（**AppAssure** アプライアンス設定ウィザード）が自動的に起動します。アプライアンスがドメインに参加している場合は、マシンの再起動後、管理者権限を持つドメインユーザーとしてアプライアンスにログインする必要があります。

   Configure SNMP Settings（SNMP の設定）ページが表示されます。

SNMP の設定

シンプルネットワーク管理プロトコル（SNMP）は一般的に使用されているネットワーク管理プロトコルで、デバイスの検出、監視、およびイベント生成などの SNMP 対応の管理機能を可能にします。SNMP は、TCP/IP プロトコルのネットワーク管理を提供します。

アプライアンスの SNMP アラートを設定するには、次の手順を実行します。

1. **Configure SNMP Settings**（SNMP の設定）ページで、**Configure SNMP on this appliance**（このアプライアンスで SNMP を設定）を選択します。

   メモ: アプライアンスで **SNMP** の詳細とアラートを設定しない場合は、**Configure SNMP on this appliance**（このアプライアンスで **SNMP** を設定）の選択を解除して、手順 **6** に進みます。
2. **Communities**（コミュニティ）で、1 つ、または複数の SNMP コミュニティ名を入力します。

   複数のコミュニティ名はコンマで区切ってください。
3. **Accept SNMP packets from these hosts**（これらのホストからの SNMP パケットを受け入れる）で、アプライアンスが通信できるホストの名前を入力します。

   ホスト名はコンマで区切るか、すべてのホストとの通信を許可する場合は、空白のままにしてください。
4. SNMP アラートを設定するには、SNMP アラートの **Community Name**（コミュニティ名）と **Trap destinations**（トラップの宛先）を入力して、**Add**（追加）をクリックします。

   この手順を繰り返して、さらに SNMP アドレスを追加します。
5. 設定済みの SNMP アドレスを削除するには、**Configured SNMP addresses**（設定された SNMP アドレス）で、該当する SNMP アドレスを選択して **Remove**（削除）をクリックします。
6. 次へ をクリックします。

   Create Windows and RASR virtual disk(s) （**Windows** および **RASR** 仮想ディスクの作成）ページが表示されます。

Windows および RASR 仮想ディスクの作成

DL4300 システムは次をサポートします。

- 2 台のオペレーティングシステムドライブ、12 台のデータドライブ、4 台の内蔵ハードドライブ
- ベアメタルリストア（BMR）情報を保存するための論理ユニット番号（LUN）の作成オプション
- Windows バックアップ RASR ファイル用の独立したスペースを作成するオプション。

オプションの仮想ディスクを作成するには、次の手順を実行します。

1. 次の仮想ディスクを選択します。
   a. Windows バックアップ仮想ディスク

      注意: AppAssure Appliance Configuration Wizard（AppAssure アプライアンス設定ウィザード）でこのオプションをスキップした場合、Windows Server バックアップの作成およびバックアップポリシーの設定を行うことはできません。

      Windows バックアップ仮想ディスクは、Windows Server バックアップを作成するターゲット領域を提供します。デフォルトでは、作成される Windows バックアップ仮想ディスクに 75 GB のディスク容量が割り当てられ、Windows バックアップ仮想ディスクのサイズを増やすことはできません。時間が経過すると、バックアップされるデータが 75 GB を超える場合がありますが、その場合、バックアップを実行したり、**Backup（バックアップ）**ページでバックアップポリシーを設定することはできなくなり、容量不足エラーが表示されます。この場合、Windows バックアップをネットワーク共有か、DL アプライアンス上の別のディスクボリュームに再設定することができます。詳細については、**Dell.com/supportmanuals** で *『Recovering a Dell™ DL Backup and Recovery Appliance using Rapid Appliance Self Recovery（RASR）』(Rapid Appliance Self Recovery（RASR）を使用した Dell™ DL Backup and Recovery Appliance のリカバリ）*を参照してください。
   b. ブータブル RASR 仮想ディスク

      ブータブル RASR 仮想ディスクは RASR リカバリを実行するための冗長リカバリボリュームを提供します。POST 中に <F8> キーを押すと、冗長リカバリボリュームに再起動できます。再起動した後、RASR の実行の手順に従ってください。
2. **Next（次へ）**をクリックします。

   システムの構成中に、サンキューメッセージが表示されます。設定の完了メッセージも表示されます。
3. **Exit（終了）**をクリックします。

   Core Console が自動的に起動します。
4. ストレージのプロビジョニングによる設定プロセスを続行します。

DL アプライアンスの設定ウィザード

メモ: 最新の RUU を使用してアプライアンスをアップグレードする時のみ、DL アプライアンスの設定ウィザードが表示されます。

注意: アプライアンスで他のタスクを実行したり設定を変更する前に、DL アプライアンス設定ウィザードのすべての手順が完了していることを確認してください。ウィザードが完了するまでは、コントロールパネルでの変更、Microsoft Windows Update の使用、Rapid Recovery ソフトウェアのアップデート、またはライセンスのインストールを行わないでください。設定プロセス中は、Windows アップデートサービスが一時的に無効化されます。DL アプライアンス設定ウィザードを完了前に終了すると、システム操作でのエラーの原因となる場合があります。

DL アプライアンス設定ウィザードは、アプライアンスのソフトウェアを設定するための次の手順をガイドします。

- ネットワークインタフェースの設定
- 登録およびホスト設定
- アラートと監視
- アクセスと管理
- Windows バックアップの設定
- ストレージのプロビジョニング
- 保持ポリシーおよびアップデートのオプションの設定

メモ: アプライアンス設定を完了すると、ウィザードをスキップするか、またはマシンの保護、レプリケーション、仮想マシンのエクスポート / スタンバイの実行を続行することができます。ウィザードのスキップを選択した場合は、Core Console が自動的に起動し、後半の段階でマシンの保護、レプリケーション、仮想マシンのエクスポートを実行できます。

マシン保護、レプリケーション、および仮想マシンのエクスポートの実行に関する詳細については、**www.dell.com/support/home** の『*Rapid Recovery on DL Appliances ユーザーズガイド*』を参照してください。

ネットワークインタフェースの設定

使用可能なネットワークインタフェースを設定するには、次の手順を実行します。

1. **DL Appliance Configuration Wizard Welcome**（**DL アプライアンス設定ウィザード - ようこそ**）画面で、**Next**（**次へ**）をクリックします。

   ライセンス契約 ページが表示されます。
2. 契約に同意するには、**I accept license agreement**（**契約に同意します**）をクリックして、**Next**（**次へ**）をクリックします。

   Network Settings（**ネットワーク設定**）ページでは、接続されている使用可能なネットワークインタフェースが表示されます。
3. 必要に応じて、追加のネットワークインタフェースを接続して **Refresh**（**更新**）をクリックします。

   接続された追加ネットワークインタフェースが表示されます。
4. お使いの環境に適した、適切なネットワークインタフェースを選択します。

   オプションは次のとおりです。IPV4 および IPV6

   選択したインターネットプロトコルに応じてネットワークの詳細が表示されます。
5. IPV4 を有効にするには、**Enable an IPV4 interface**（**IPV4 インタフェースを有効にする**）を選択します。
   a. IPV4 インタフェースのインターネットプロトコル詳細を割り当てるには、次のいずれかを行います。
      - 選択したインターネットプロトコル詳細を自動的に設定するには、**Obtain an IPV4 address automatically**（**IPV4 アドレスを自動的に取得する**）を選択します。
      - ネットワーク接続を手動で割り当てるには、**Set manually IPV4 address**（**手動で IPV4 アドレスを設定する**）を選択して次の詳細を入力します。
        - **IPv4 アドレス**
        - **サブネットマスク**
        - **Default Gateway**（**デフォルトゲートウェイ**）
6. IPV6 を有効にするには、**Enable an IPV6 interface**（**IPV6 インタフェースを有効にする**）を選択します。
   a. IPV6 インタフェースのインターネットプロトコル詳細を割り当てるには、次のいずれかを行います。
   - 選択したインターネットプロトコル詳細を自動的に割り当てるには、**Obtain an IPV6 address automatically**（**IPV6 アドレスを自動的に取得する**）を選択します。
   - ネットワーク接続を手動で割り当てるには、**Set manually IPV6 address**（**手動で IPV6 アドレスを設定する**）を選択して次の詳細を入力します。
     - **IPv6 アドレス**
     - **サブネットプレフィクスの長さ**
     - **Default Gateway**（**デフォルトゲートウェイ**）
7. NIC チーミングを有効にするには、**Enable NIC teaming**（**NIC チーミングを有効にする**）を選択します。

   NIC チーミングの詳細については、「」を参照してくださいネットワークアダプタのチームミング。
8. **Next**（**次へ**）をクリックします。

   登録 ページが表示されます。

登録およびホスト設定

お使いのアプライアンスの機能を適切に活用できるように、適切なライセンスキーでアプライアンスを登録します。バックアップを開始する前に、ホスト名を変更することをお勧めします。デフォルトでは、ホスト名はオペレーティングシステムが割り当てるシステム名です。

メモ: ホスト名を変更する場合は、この段階で変更することをお勧めします。DL アプライアンス設定ウィザード）の完了後のホスト名の変更には、いくつかの手順が必要です。

1. **Registration**（登録）ページで、以下のオプションのいずれかを選択する必要があります。
   - **今すぐ登録** – 購入済みのライセンスでアプライアンスを登録します。ライセンス数テキストボックスにライセンスの数を入力し、メールアドレステキストボックスに有効なメールアドレスを入力します。

- **試用ライセンスを使用** – 試用ライセンスでアプライアンスを登録します。 試用ライセンスの有効期限は 30 日間です。中断することなく製品の使用を継続するには、その期間内にアプライアンスを登録してください。

2. **Next**（次へ）をクリックします。

   Host Settings（ホスト情報）ページが表示されます。

3. デフォルトでは、アプライアンスのホスト名がホスト名ボックスに表示されます。アプライアンスのホスト名を変更するには、**ホスト名**テキストボックスに適切な名前を入力します。

4. アプライアンスをドメインに参加させたい場合は、**このシステムをドメインに参加させる**チェックボックスにチェックを入れて、次の情報を指定します。

   参加させない場合は、手順 5 へ進みます。

   メモ: ドメインへの参加は Windows Server 2012 R2 Foundation Edition では行えません。この場合、このシステムをドメインに参加させるチェックボックスは無効です。

テキストボックス	説明
ドメインのアドレス	システムを追加するドメインのアドレスです
ドメイン管理者	ドメイン管理者
パスワード	パスワード

5. **Next**（次へ）をクリックします。

   Alerts and Monitoring（アラートと監視）ページが表示されます。

アラートと監視

ハードウェアとソフトウェアの両方の変更に対するアラートを有効にするには、SNMP と SMTP の 2 つのオプションがあります。簡易ネットワーク管理プロトコル (SNMP) は、デバイスの検出、監視、イベントの生成などの SNMP 対応の管理機能を許可する一般的に使用される管理プロトコルです。SNMP は、TCP/IP プロトコルのネットワーク管理を提供します。簡易ネットワーク管理プロトコル (SNMP)、または簡易メール転送プロトコル (SMTP) を使用してお使いのアプライアンスのアラートおよび監視を設定することができます。
通知を受信するには、ここでオプションを設定します。

メモ: アラートを設定することをお勧めします。アラートの設定をスキップするオプションもあります。アラートの設定をスキップするには、手順 3 に進みます。

1. アラートを有効にするには、次のオプションがあります。
   - システムの SNMP アラートを有効にするには、**システムの SNMP アラートを有効にする**を選択します。
     1. SNMP コミュニティで、1 つまたは複数の SNMP コミュニティ名を入力します。コンマを使って複数のコミュニティ名を区切ります。
     2. SNMP トラップの送信先にトラップの送信先を入力して、**Add**（追加）をクリックします。
   - ソフトウェアの SNMP アラートを有効にするには、**ソフトウェアの SNMP アラートを有効にする**オプションを選択します。
     1. SNMP コミュニティで、1 つまたは複数の SNMP コミュニティ名を入力します。コンマを使って複数のコミュニティ名を区切ります。
     2. SNMP トラップの送信先にトラップの送信先を入力して、**Add**（追加）をクリックします。
2. 電子メールでソフトウェアのアラートを通知するように設定するには、**電子メールで通知**オプションを選択して有効な電子メールアドレスを入力します。
3. **Next**（次へ）をクリックします。

Access and Management（アクセスと管理）ページが表示されます。

アクセスと管理

お使いのアプライアンスにアクセスして管理するには、アクセスと管理の設定を行う必要があります。

お使いのアプライアンスのアクセスと管理の設定を行うには、次の手順を実行します。

1. **アクセスと管理**ページで次のオプションを選択または選択解除して、以下からアプライアンスにアクセスし管理します。
   - リモートデスクトップを有効にする
   - Windows ファイアウォールを有効にする
   - IE セキュリティ強化を有効にする
   - Windows アップデートを有効にする
   - プロキシサーバを使用する
2. **プロキシサーバを使用する**を選択する場合は、プロキシアドレステキストボックスにプロキシアドレスを入力し、ポートテキストボックスにポート番号を入力します。
3. **メモ: アクセスと管理設定をデフォルトオプションに設定する場合は、Reset to Default（デフォルトにリセット）ボタンをクリックします。**

   Next（次へ）をクリックします。

   アプライアンス設定のバックアップオプションページが表示されます。

Windows バックアップの設定

メモ: DL 1000 を除く全ての DL シリーズが Windows バックアップ機能をサポートしています。

アプライアンス設定のバックアップオプションでアプライアンス設定をバックアップする頻度を設定することができます。Windows バックアップデータは、障害前の状態からのアプライアンス設定のリカバリに役立ちます。

1. **アプライアンス設定のバックアップオプション**で、**アプライアンス設定のバックアップの実行**を選択します。

   オプションは次のとおりです。毎日、毎週、毎月
2. Windows バックアップの頻度を設定するには、次のオプションのうちのいずれかを選択します。

オプション	説明
毎日	毎日午前 12:01 に設定のバックアップを開始します。
毎週	毎週日曜日の午前 12:01 に設定のバックアップを開始します。
毎月	毎月日曜日の午前 12:01 に設定のバックアップを開始します。

3. **Next**（次へ）をクリックします。

   Storage Provisioning（ストレージのプロビジョニング）ページが表示されます。

ストレージのプロビジョニング

お使いのアプライアンスで、ホストリポジトリおよび仮想スタンバイ、アーカイブ、またはその他の目的のために仮想ディスク（VD）を作成するように内部ストレージを設定できます。

1. **ストレージのプロビジョニングページ**で、ストレージに対する次の設定オプションを選択します。

   リポジトリ名はデフォルトで**リポジトリ 1** として表示されます。

   メモ: リポジトリのサイズは、アプライアンスの登録時に適用されるライセンスによって異なります。
   - アプライアンスの登録時に試用ライセンスを適用した場合、リポジトリのサイズに制限はありません。
   - アプライアンスの登録時に購入済みのライセンスを適用した場合、リポジトリのサイズはモデルに対応します。例：DL 4300 5 TB アプライアンスでは、 5 TB のリポジトリが作成されます。拡張ライセンスを適用することで、**プロビジョニング** ページからレポジトリを拡張できるオプションがあります。詳細については、『*Rapid Recovery 6.0 on DL Appliance ユーザーズガイド*』を参照してください。
   - 購入済みの拡張ライセンスを適用した場合、リポジトリのサイズは適用されるライセンスに対応します。例：DL43005 TB アプライアンスでは、購入済みライセンス (N TB) が登録時に適用されている場合、5+N TB のリポジトリが作成されます。
2. **仮想スタンバイ、アーカイブ、またはその他の目的のためにストレージの一部を割り当てる** を選択します。
3. スライダを使用してリポジトリを作成した後に、使用可能なストレージのスペースの割合を割り当てます。サイズボックスを使用して正確なサイズを指定することもできます。

仮想スタンバイ VM のホスティング、アーカイブ、その他の目的のために指定した容量を持つ仮想ディスクが作成されます。

4. **Next**（次へ）をクリックします。
   初期リポジトリが作成され、VM のホスティング、またはその他の目的のための VD が作成されます。

   Retention Policy（保持ポリシー）ページが表示されます。

保持ポリシーおよびアップデートのオプションの設定

保持ポリシーは、バックアップが短期（高速かつ高価）メディアに保存される期間を決定します。特定の事業および技術要件によって、これらのバックアップの延長保持が必要となることがありますが、高速ストレージの使用は非常に高額です。お使いのアプライアンスでは、保持ポリシーをカスタマイズして、バックアップのリカバリポイントが保守される期間を指定することができます。リカバリポイントの保持期間が終わりに近づくと、保持期間を越えた時点で、そのリカバリポイントは保持プールから削除されます。

1. 次のオプションで、保護対象マシンのバックアップスナップショットを保存する期間を決め、古いバックアップの結合と削除のロールアッププロセスを変更できます。**Retention Policy**（保持ポリシー）ページに次のオプションが表示されます。

   表 4. デフォルトの保持ポリシーのスケジュールオプション

テキストボックス	説明
すべてのリカバリポイントを n [保持期間] 保持	リカバリポイントの保持期間を指定します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは 3 日間です。 日、週、月、または年から選択できます。
...さらに、1 時間につき 1 つのリカバリポイントを n [保持期間] 保持	より詳細なレベルの保持を指定します。このオプションはビルディングブロックとしてプライマリ設定と共に使用され、リカバリポイントを維持する期間をさらに詳細に定義します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは 2 日間です。 日、週、月、または年から選択できます。
...さらに、1 日につき 1 つのリカバリポイントを n [保持期間] 保持	より詳細なレベルの保持を指定します。このオプションはビルディングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは 4 日間です。 日、週、月、または年から選択できます。
...さらに、1 週間につき 1 つのリカバリポイントを n [保持期間] 保持	より詳細なレベルの保持を指定します。このオプションはビルディングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは 3 週間です。 週、月、または年から選択できます。
...さらに、1 月につき 1 つのリカバリポイントを n [保持期間] 保持	より詳細なレベルの保持を指定します。このオプションはビルディングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは 2 カ月間です。 月または年から選択できます。
...さらに、1 年につき 1 つのリカバリポイントを n [保持期間] 保持	保持期間を示す数字を入力し、期間を選択します。 年から選択できます。

2. **Next**（次へ）をクリックします。
   Update Options（アップデートのオプション）ページが表示されます。

3. アプライアンスソフトウェアのアップデートを確認するには、**Check for appliance software update**（アプライアンスソフトウェアのアップデートの確認）オプションを選択します。

   アップデートがある場合は、ウィザードの完了時にダウンロードされインストールされます。

4. Rapid Recovery Core のアップデートを有効にするには、**Enable Rapid Recovery Core updates**（**Rapid Recovery Core** のアップデートの有効化）を選択し、次のいずれかのオプションを選択します。
   - アップデートについて通知するが、自動手にインストールしない
   - アップデートを自動的にインストールする
5. **Finish**（終了）をクリックします。

   アプライアンスの設定が適用されます。

Recovery and Update Utility

Recovery and Update Utility（RUU）は、DL アプライアンス（DL1000、DL1300、DL4000 および DL4300）のソフトウェアを回復してアップデートする、オールインワンのインストーラです。これには、Rapid Recovery Core ソフトウェアおよびアプライアンス固有のコンポーネントが含まれています。

RUU は、Windows Server の役割と機能、.Net 4.5.2、LSI Provider、DL アプリケーション、OpenManage Server Administrator および Rapid Recovery Core ソフトウェアの、アップデートされたバージョンで構成されています。また、Recovery and Update Utility は、 Rapid Appliance Self Recovery（RASR）コンテンツもアップデートします。

メモ: 現在 AppAssure Core バージョン、Rapid Recovery Core バージョン 6.0.2.144 以前のいずれかを使用している場合、RUU はペイロードで利用可能な最新バージョンへのアップデートを強制します。アップデートをスキップすることはできません。またこのアップデートは復帰不可能です。Core ソフトウェアをアップグレードしない場合は、RUU を実行しないでください。

RUU の最新バージョンをインストールするには、次の手順を実行します。

1. ダウンロードセクションの下のライセンスポータルに移動するか、または **support.dell.com** にアクセスして RUU インストーラをダウンロードします。
2. RUU プロセスを開始するには、RUU パッケージの launchRUU.exe ファイルを実行します。

   メモ: お使いのシステムは、 RUU の更新処理中に再起動する場合があります。

Rapid Appliance Self Recovery

Rapid Appliance Self Recovery（RASR）は、お使いのアプライアンスを動作状態に素早く復元できる、ベアメタルの復元プロセスです。

RASR は 2 つの復元のオプションを提供します。

- 工場出荷時設定の復元
- 障害発生時直前の状態にお使いのアプライアンスを回復（OS、構成、設定を復元）

RASR USB キーの作成

RASR USB キーを作成するには、次の手順を実行します。

1. **Appliance**（アプライアンス）タブへ移動します。
2. 左ペインのナビゲーションを使用して **Appliance**（アプライアンス） → **Backup**（バックアップ）と選択します。

   Create RASR USB Drive（**RASR USB** ドライブの作成）ウィンドウが表示されます。

   メモ: 16 GB 以上の USB キーを挿入してから、RASR キーを作成します。

3. 16 GB またはそれ以上の USB キーを挿入した後、**Create RASR USB Drive now**（**RASR USB** ドライブを今すぐ作成）をクリックします。

   Prerequisite Check（前提条件チェック）メッセージが表示されます。

前提条件チェックの完了後、**Create the RASR USB Drive**（**RASR USB ドライブの作成**）ウィンドウに USB ドライブの作成に必用な最低限のサイズと **List of Possible target paths**（**可能なターゲットパスのリスト**）が表示されます。

4. ターゲットを選択し、**Create**（**作成**）をクリックします。
   警告ダイアログボックスが表示されます。
5. **Yes**（**はい**）をクリックします。
   RASR USB ドライブキーが作成されます。
6. **メモ: USB キーの取り外し準備には、Windows のドライブ取り出し機能を使用するようにしてください。使用しなければ、USB キー内のコンテンツが破損する、または USB キーが期待通りに動作しない可能性があります。**

   各 DL アプライアンス、ラベル用に作成した RASR USB キーを取り外し、今後の使用のために保管します。

RASR の実行

メモ: デルでは、アプライアンスをセットアップした後で RASR USB キーを作成することをお勧めします。RASR USB キーの作成については、「RASR USB キーの作成」の項を参照してください。

メモ: RUU が最新でお使いのアプライアンスに到達可能であることを確認します。

。

メモ: RASR を使用してシステムリカバリを実行するには、Dell.com/support/home で ***「Recovering a Dell™ DL Backup and Recovery Appliance using Rapid Appliance Self Recovery (RASR)」（Rapid Appliance Self Recovery (RASR) を使用した Dell™ DL Backup and Recovery Appliance のリカバリ）*** **マニュアルを参照してください。**

工場出荷時の状態にリセットするには、次の手順を実行します。

1. 作成した RASR USB キーを挿入します。
2. アプライアンスを再起動して、**Boot Manager**（**F11**）（**ブートマネージャ**（**F11**））を選択します。
3. **Boot Manager Main Menu**（**ブートマネージャメインメニュー**）で **One-shot BIOS Boot Menu**（**ワンショット BIOS 起動メニュー**）を選択します。
4. **Boot Manager Boot Menu**（ブートマネージャ起動メニュー）で、接続されている USB ドライブを選択します。
5. キーボードのレイアウトを選択します。
6. **Troubleshoot**（**トラブルシューティング**） → **Rapid Appliance Self Recovery** とクリックします。
7. ターゲットのオペレーティングシステム（OS）を選択します。
   RASR が起動され、**welcome**（**ようこそ**）画面が表示されます。
8. **Next**（**次へ**）をクリックします。
   Prerequisites（**前提条件**）のチェック画面が表示されます。

   メモ: RASR を実行する前にすべてのハードウェア、およびその他の前提条件が満たされていることを確認します。
9. **Next**（**次へ**）をクリックします。
   Recovery Mode Selection（**リカバリモード選択**）画面に 3 つのオプションが表示されます。
   - **System Recovery**（**システムリカバリ**）
   - **Windows Recovery Wizard**（**Windows リカバリウィザード**）
   - **Factory Reset**（**工場出荷時の状態にリセット**）
10. **Factory Reset**（**工場出荷時の状態にリセット**）オプションを選択します。
    このオプションでは、工場出荷時のイメージからオペレーティングシステムのディスクを回復します。
11. **Next**（**次へ**）をクリックします。
    `This operation will recover the operating system. All OS disk data will be overwritten` という警告メッセージがダイアログボックスに表示されます。
12. **Yes**（**はい**）をクリックします。
    オペレーティングシステムのディスクの工場出荷時のリセット状態への復元が開始されます。
13. リカバリ処理が完了したら、 **RASR Completed**（**RASR が完了しました**）ページが表示されます。**Finish**（**終了**）をクリックします。

14. 復元後にシステムを起動します。
15. **メモ: AppAssure アプライアンス設定ウィザードが表示された場合のみさらに続行します。それ以外は、手順 17 に進みます。**

    AppAssure アプライアンス設定ウィザードのロードを待ってから閉じる必要があります。 Windows タスクマネージャを使用してウィザードを閉じます。
16. RUU パッケージの launchRUU.exe ファイルを実行します。指示に従ってオプションを選択し、RUU のインストールを続行して完了させます。
17. **DL アプライアンス設定ウィザード**が起動し、復元プロセスの残りの手順を案内します。

これでお使いのアプライアンスが正常に動作します。

内蔵デュアル SD モジュールを使用した RASR の実行

お使いのシステムは、内蔵デュアル SD モジュールと 16 GB の容量の SD カードが同梱されています。

内蔵デュアル SD モジュール（IDSDM）を使用して RASR を実行するには、以下の手順を実行します。

1. IDSDM を介してアプライアンスを再起動します。

   注意: スロットに SD カードが挿入されていることを確認してください。

   次のメッセージが表示されます。

   ```
   The secondary SD card is missing, not responding, or in write-protected mode. Do one of
   the following: 1) Install a SD card media in the secondary SD card reader. 2) Reseat or
   replace the SD card media.3) If write-protected mode is expected, then no respose
   action is required.
   ```

   上記のメッセージは無視してください。
2. 内蔵 SD モジュールを使用した RASR の実行を続行するには、「RASR USB キーを使用して RASR を実行」セクションの手順 5～13 を実行してください。

ストレージのプロビジョニング

アプライアンスは、使用可能な内部ストレージ、および接続されている対応外部ストレージエンクロージャのすべてを次のために設定します。

- リポジトリ

  メモ: Fibre Channel の HBA が設定されている場合は、リポジトリの作成プロセスは手動で行われます。Rapid Recovery がリポジトリをルートディレクトリに自動的に作成することはありません。詳細については、Fibre Channel ストレージを使用した DL4300 の構成（オプション）の項を参照してください。

  \
- スタンバイ VM、またはその他の目的のためのディスクボリューム

  メモ: れ 830 コントローラに接続された、1 TB, 2 TB, 4 TB、6 TB（大容量用）ドライブ付き MD1400s がサポートされています。MD1400s は最大 4 台までサポートされています。

  メモ: 大容量構成の DL4300 は、H830 PERC SAS アダプタまたは 2 個の Fibre Channel HBA をサポートします。Fibre Channel HBA の構成の詳細については、Dell.com/support/home にある *『DL4xxx — Fibre Channel Implementation』（DL4xxx — Fibre Channel 実装）*ホワイトペーパーを参照してください。

ディスク上でストレージのプロビジョニングを開始する前に、スタンバイ仮想マシンに割り当てるストレージの容量を決定します。スタンバイ仮想マシンをホストするために、Rapid Recovery リポジトリの作成後に残っている使用可能な容量から、任意の割合の容量を割り当てることができます。たとえば、Storage Resource Management（SRM）を使用している場合、Rapid Recovery リポジトリの作成後に残っている容量のうち最大 100 パーセントまでを割り当てることができます。スタンバイ VM に容量を割り当てることができるのは、仮想マシンをホストするためにプロビジョニングされたアプライアンスのみです。アプライアンスで保護されているサーバに障害が発生した場合、Rapid Recovery のライブリカバリ機能を使用して、それらのサーバを仮想マシンに素早く置き換えることができます。

スタンバイ仮想マシンを必要としない中規模の環境では、すべてのストレージを使用してかなりの数のエージェントをバックアップすることができます。一方、スタンバイ仮想マシン用に追加のリソースを必要とし、より少ない数のエージェントマシンをバックアップする場合は、より大きな VM 用により多くのリソースを割り当てることができます。

Appliance（アプライアンス） → **Provisioning（プロビジョニング）** タブを選択すると、Rapid Recovery アプライアンスソフトウェアは、システム内のサポートされているすべてのコントローラに対して使用可能なストレージ容量の場所を特定し、ハードウェアが要件を満たしていることを検証します。

使用可能なすべてのストレージのディスクプロビジョニングを完了するには、次の手順を実行します。

1. **Appliance（アプライアンス）** → **Provisioning（プロビジョニング）** をクリックします。
   Provisioning（プロビジョニング） 画面**リポジトリ**と**ストレージボリューム**の項が表示されます。

   注意: 作業を進める前に、本手順の手順 2 ～ 手順 4 が実施されていることを確認します。

2. 以下の作成に利用可能なストレージのプロビジョニング
   - リポジトリ
   - スタンバイ VM、またはその他の目的のためのディスクボリューム
3. リポジトリを作成するには、次の手順を実行します。
   a. **provisioning（プロビジョニング）** ページの**リポジトリ**セクションで、**Add New Repository（新規リポジトリを追加）** をクリックします。
      Add New Repository（新規リポジトリを追加） ダイアログボックスが表示されます。
   b. 次の表の説明に従って、情報を入力します。

      表 5. ストレージのプロビジョニング

テキストボックス	説明
リポジトリ名	リポジトリの表示名を入力します。 デフォルトでは、このテキストボックスは「リポジトリ」という単語と、この Core のリポジトリ番号に対応する番号で構成されます。たとえば、これが 2 番目のリポジトリである場合、デフォルトの名前はリポジトリ 2 です。必要に応じて名前を変更します。 リポジトリの名前には、1 ～ 40 文字の英数字（スペースを含む）を入力する必要があります。「禁止文字」または「禁止語句」は使用できません。詳細については、『*Dell Data Protection | Rapid Recovery 6.0 ユーザーガイド*』の「禁止文字」および「禁止語句」のトピックを参照してください。
コントローラ	リポジトリを内部ストレージ、またはダイレクトアタッチドストレージエンクロージャのどちらで作成しているかによって、適切なストレージコントローラを選択します。
エンクロージャ	適切なストレージエンクロージャを選択します。
RAID のタイプ	適切な RAID レベルを選択します。RAID 構成のオプションは次のとおりです。1、5、または 6 **メモ: お使いのシステムでは、ストレージが構成され工場以外で利用可能な RAID レベルでのみリポジトリを作成できます。希望する RAID 構成でリポジトリを作するには、希望の RAID レベルで、ストレージを設定する必要があります。希望の RAID レベルでストレージを設定するには、www.dell.com/support/home で Dell アダプタマニュアルを参照してください。**
容量見積もり	リポジトリの作成に使用可能な容量の見積もりを表示します。
コントローラの空き領域	コントローラ上の空き領域が表示されます。
サイズ	リポジトリのサイズを入力します。

   c. **Creat（作成）** をクリックします。
      新しいリポジトリが作成されます。

4. スタンバイ VM、またはその他の目的のためのディスクボリュームを作成するには、次の手順を実行します。
   a. **ストレージボリューム** セクションで **Creat Volume**（ボリュームの作成）をクリックします。
   b. **Creat Volume**（ボリュームの作成）ダイアログボックスで、新しいディスクボリュームの次の情報を指定します。ボリューム名、コントローラ、エンクロージャ、RAID タイプ、およびサイズ

      コントローラの空き領域がデフォルトで表示されます。次の RAID 構成のいずれかを選択できます。1、5、または 6
   c. **Creat**（作成）をクリックします。

      新しいストレージボリュームが作成されます。

Fibre Channel ストレージを使用した DL4300 の構成（オプション）

DL4300 大容量エディションは Fibre Channel HBA ストレージオプションを提供し、Fibre Channel ストレージアレイを使用したリポジトリの作成が可能です。

メモ: Fibre Channel 構成での発注の場合は、スロットに装着されている H830 PERC SAS アダプタを交換します。

メモ: 以下の手順に関する必要条件、前提、詳細については、ホワイトペーパー『*DL4xxx — Fibre Channel Implementation*』（DL4xxx — Fibre Channel 実装）（dell.com/support/home）を参照してください。

Fibre Channel ストレージを使用して DL4300 を統合および構成するには、次の手順を実行します。

1. DL4300 Fibre Channel HBA を SAN スイッチに接続します。
2. システムで注文したアダプタに、Qlogic または Emulex HBA 管理ソフトウェアをインストールします。
3. ストレージアレイのマルチパスソフトウェアをインストールします。
4. Fibre Channel のゾーニングを実行します。
5. DL4300 のリポジトリとして割り当てて使用する Fibre Channel LUN を作成します。
6. Fibre Channel ストレージ LUN をマウントします。
7. DL4300 Fibre Channel ストレージを、バックアップリポジトリとして設定します。

3

インストール後のタスク

DL Appliance Configuration Wizard（**DL アプライアンス設定ウィザード**）が完了したら、次の手順を実行して、お使いのバックアップアプライアンスと、アプライアンスがバックアップしているサーバが正しく設定されていることを確認します。

メモ: アプライアンスは、30 日間有効な一時使用向け Rapid Recovery ソフトウェアライセンスで設定されます。永続ライセンスキーを取得するには、www.dell.com/DLActivation の Dell AppAssure License Portal（Dell AppAssure ライセンスポータル）にログオンします。Rapid Recovery ソフトウェアでのライセンスキーの変更方法の詳細については、『*Dell Data Protection | Rapid Recovery License Portal ユーザーガイド*』を参照してください。

Core Console へのアクセス

「Internet Explorer での信頼済みサイトのアップデート」のトピックでで説明されているとおりに信頼済みサイトをアップデートし、「Core Console にリモートでアクセスするためのブラウザの設定」のトピックで説明されているとおりにお使いのブラウザを設定するようにしてください。Internet Explorer で信頼済みサイトをアップデートし、ブラウザを設定した後は、次の操作のいずれかを実行して Core Console にアクセスします。

- Rapid Recovery コアサーバにローカルでログインして、**Core Console**（**コアコンソール**）アイコンをダブルクリックします。
- ウェブブラウザに次の URL のどちらかを入力。
  - **https://<yourCoreServerName>:8006/apprecovery/admin/core**
  - **https://<yourCoreServerIPaddress>:8006/apprecovery/admin/core**

Internet Explorer での信頼済みサイトのアップデート

Internet Explorer で信頼済みサイトをアップデートするには、次の手順を実行します。

1. Internet Explorer を開きます。
2. **ファイル**、**ビューの編集**、およびその他のメニューが表示されない場合は、<F10> を押します。
3. **ツール** メニューをクリックして、**インターネットオプション** を選択します。
4. **インターネットオプション** ウィンドウで、**セキュリティ** タブをクリックします。
5. **信頼済みサイト** をクリックし、**サイト** をクリックします。
6. **この Web サイトをゾーンに追加する** に、表示名用に指定した新しい名前を使用して **https://[表示名]** を入力します。
7. **追加** をクリックします。
8. **この Web サイトをゾーンに追加する** に、**about:blank** と入力します。
9. **追加** をクリックします。
10. **閉じる** をクリックして、**OK** をクリックします。

Core Console にリモートでアクセスするためのブラウザの設定

リモートマシンから Core Console にアクセスするには、ブラウザの設定を変更する必要があります。

メモ: ブラウザの設定を変更するには、管理者としてシステムにログインします。

メモ: Google Chrome は Microsoft Internet Explorer の設定を使用するため、Chrome ブラウザの設定は Internet Explorer を使用して変更してください。

メモ: **Core Web Console** にローカルまたはリモートでアクセスするときは、**Internet Explorer** セキュリティ強化の構成がオンになっていることを確認します。 **Internet Explorer** セキュリティ強化の構成 をオンにするには、次の手順を実行します。

1. **サーバーマネージャー** を開きます。
2. 右側に表示される **ローカルサーバー IE セキュリティ強化の構成** を選択します。このオプションが **オン** になっていることを確認します。

Internet Explorer と Chrome でのブラウザ設定

Internet Explorer と Chrome でのブラウザ設定を行うには、次の手順を実行します。

1. **インターネットオプション**画面から、**セキュリティ**タブを選択します。
2. **信頼済みサイト**をクリックし、**サイト**をクリックします。
3. オプション **このゾーンのサイトにはすべてサーバの確認 (https:) を必要とする**の選択を解除し、http://<*Rapid Recovery Core をホストしているアプライアンスサーバのホスト名または IP アドレス*> を **信頼済みサイト**に追加します。
4. **閉じる**をクリックし、**信頼済みサイト**を選択し、**レベルのカスタマイズ**をクリックします。
5. **その他 → 混在したコンテンツを表示する**までスクロールし、**有効にする**を選択します。
6. 画面の一番下の**ユーザー認証 → ログオン**までスクロールし、**現在のユーザー名とパスワードで自動的にログオンする**を選択します。
7. **OK** をクリックし、**詳細設定**タブを選択します。
8. **マルチメディア**までスクロールし、**Web ページのアニメーションを再生する**を選択します。
9. **セキュリティ**までスクロールし、**統合 Windows 認証を使用する**をチェックし、**OK** をクリックします。

Firefox でのブラウザ設定

Firefox でブラウザ設定を変更するには、次の手順を実行します。

1. Firefox のアドレスバーに **about:config** と入力し、プロンプトが表示されたら **I'll be careful, I promise**（細心の注意を払って使用する）をクリックします。
2. 用語 **ntlm** を検索します。
   検索結果が 3 件以上表示されます。
3. **network.automatic-ntlm-auth.trusted-uris** をダブルクリックし、お使いのマシンに合わせて次の設定を入力します。
   - ローカルマシンの場合、ホスト名を入力します。
   - リモートマシンの場合、Core をホストしているアプライアンスシステムのホスト名または IP アドレスをコンマで区切って入力します（例：*IP アドレス,ホスト名*）。
4. Firefox を再起動します。

保持期間の確認

Rapid Recovery は、スナップショットの取得頻度と保持期間を決めるデフォルトの保持期間を設定します。保持期間はお使いの環境要件に基づくようにする必要があります。例えば、頻繁に変更されるミッションクリティカルなデータを持つサーバをバックアップしている場合は、より頻繁にスナップショットを取得する必要があります。

保持期間を確認して変更するには、次の手順を実行します。

1. Core Console を開きます。
2. **Configuration**（設定）タブを選択し、**Retention Policy**（保持ポリシー）をクリックします。
3. 組織のニーズに基づいて保持ポリシーを調整します。
4. **Apply**（適用）をクリックします。

エージェントスナップショットデータの暗号化

Core では、リポジトリ内のエージェントスナップショットデータの暗号化が可能です。DL4000 は、レジストリ全体を暗号化するかわりに、リポジトリ内のエージェントの保護中に暗号化キーを指定できます。これにより、キーを異なるエージェントで再利用することができます。

エージェントスナップショットデータを暗号化するには、次の手順を実行します。

1. AppAssure Core から、**Configuration**（設定）→ **Manage**（管理）→ **Security**（セキュリティ）をクリックします。
2. **Actions**（アクション）をクリックして、**Add Encryption Key**（暗号化キーを追加）をクリックします。

   Create Encryption Key（暗号化キーの作成）ページが表示されます。
3. 以下の情報をすべて入力します。

フィールド	説明
名前	暗号化キーの名前を入力します。
Comment（コメント）	暗号化キーのコメントを入力します。これは、暗号化キーの追加詳細を提供するために使用されます。
Passphrase（パスフレーズ）	パスフレーズを入力します。アクセスを制御するために使用されます。
Confirm Passphrase（パスフレーズの確認）	パスフレーズを再入力します。パスフレーズの入力を確認するために使用されます。

メモ: 暗号化パスフレーズを失うとデータがアクセス不能になることから、パスフレーズを記録することが推奨されます。

電子メールサーバーと電子メール通知テンプレートの設定

イベントについての E-メール通知を受け取るには、E-メールサーバーと E-メール通知テンプレートを設定します。

メモ: **Notify by email**（電子メールでの通知）オプションを有効にする操作等では、通知グループ設定の設定も行った後に、電子メール警告メッセージを送信する必要があります。電子メール警告を受信するイベントの指定の詳細に関しては、『*Dell DL4300 Appliance User's Guide*』（Dell DL4000 Appliance ユーザーズガイド）にある「**Configuring Notification Groups For System Events**」（システムイベントのための通知グループの設定）を参照してください。

E-メールサーバーと E-メール通知テンプレートを設定するには、次の手順を実行します。

1. Core から **Configuration**（設定）タブを選択します。
2. **Manage**（管理）オプションから、**Events**（イベント）をクリックします。
3. **Email SMTP Settings**（E-メール SMTP 設定）ペインで、**Change**（変更）をクリックします。

   Edit Email Notification Configuration（電子メール通知設定の編集）ダイアログボックスが表示されます。
4. **Enable Email Notifications**（E-メール通知を有効にする）を選択し、次で説明されている E-メールサーバーの詳細を入力します。

テキストボックス	説明
SMTP サーバー	E-メール通知テンプレートによって使用される E-メールサーバーの名前を入力します。命名規則には、ホスト名、ドメイン、およびサフィックスが含まれます。たとえば、**smtp.gmail.com** と入力します。
ポート	ポート番号を入力します。この番号は E-メールサーバー用のポートの識別に使用されます。たとえば、Gmail の場合はポート 587 を入力します。

テキストボックス	説明
	デフォルト値は 25 です。
Timeout（seconds）（タイムアウト（秒））	接続の試行がタイムアウトするまでの時間の長さを指定するために、整数値を入力します。この数値は E-メールサーバーへの接続試行時にタイムアウトするまでの時間を秒単位で設定するために使用されます。 デフォルトは 30 秒 です。
TLS	このオプションは、メールサーバーがトランスポート層セキュリティ（TLS）またはセキュアソケット層（SSL）などのセキュア接続を使用する場合に選択します。
ユーザー名	E-メールサーバーのユーザー名を入力します。
パスワード	E-メールサーバーにアクセスするためのパスワードを入力します。
From（差出人）	返信用 E-メールアドレスを入力します。これは、E-メール通知テンプレート用の返信 E-メールアドレスを指定するために使用されます。たとえば、**noreply@localhost.com** と入力します。
Email Subject（E-メールの件名）	E-メールテンプレートの件名を入力します。これは、E-メール通知テンプレートの件名を定義するために使用されます。たとえば、`<hostname> - <level> <name>` と入力します。
Email（E-メール）	イベント、発生日時、および重要度を示すテンプレートの本文の情報を入力します。

5. **Send Test Email**（テスト E-メールの送信）をクリックして、結果を確認します。
6. テストの結果に問題がないことを確認したら、**OK** をクリックします。

ストリーム数の調整

デフォルトでは、Rapid Recovery はアプライアンスに対して 3 つの同時ストリームを許可するように設定されています。ストリーム数は、最適な性能のため 10 ～ 15 の間で設定することが推奨されます。

同時ストリーム数を変更するには、次の手順を実行します。

1. **Configuration**（設定）タブを選択して **Settings**（設定）をクリックします。
2. **Transfer Queue**（転送キュー）で **change**（変更）を選択します。
3. **Maximum Concurrent Transfers**（最大同時転送数）を最適な性能のため 10 ～ 15 の間の数字に変更しても、性能が十分でないと思われる場合は、手動で調整してみてください。

4

サーバを保護する準備

概要

DL ,,, 4300 を使用してデータを保護するには、保護のために Core Console でワークステーションや、Exchange サーバ、SQL Server、Linux サーバなどのサーバを追加する必要があります。

Core Console では、エージェントがインストールされているマシンを識別し、保護するボリューム（例えば Microsoft Windows 記憶域容量）を指定することができ、保護スケジュールの定義、暗号化などのセキュリティ対策の追加なども実行できます。ワークステーションおよびサーバを保護するために、Core Console にアクセスする方法については、マシンの保護を参照してください。

クライアントでのエージェントのインストール

DL 4300,,, アプライアンスによってバックアップされる各クライアントには、Rapid Recovery エージェントがインストールされている必要があります。Rapid Recovery Core コンソールでは、エージェントをマシンに導入することが可能です。エージェントをマシンに導入するには、クライアントにプッシュするためのエージェントを 1 タイプ選択する事前設定が必要です。この方法は、すべてのクライアントが同じオペレーティングシステムを実行している場合に便利です。ただし、異なるバージョンのオペレーティングシステムがあるときは、マシン上にエージェントをインストールする方が簡単な場合もあります。

また、マシンを保護するプロセスの最中に、エージェントソフトウェアをエージェントマシンに導入することも可能です。このオプションは、まだエージェントソフトウェアがインストールされていないマシンで利用できます。マシン保護中のエージェントソフトウェアの導入についての詳細は、**Dell.com/support/home** で『*Rapid Recovery on DL Appliance ユーザーズガイド*』を参照してください。

エージェントを保護する時のエージェントソフトウェアの導入

保護のためにエージェントを追加するプロセス中に、エージェントをダウンロードして導入することができます。

メモ: この手順は、保護するマシンに Agent ソフトウェアをすでにインストールしている場合は必要ありません。マシンを保護する前に Agent ソフトウェアをインストールしていないと、このウィザードの一部として保護のための特定のボリュームを選択できません。この場合、デフォルトではエージェントマシンのすべてのボリュームが保護に含まれます。 Rapid Recovery は EISA パーティションで構成されるマシンの保護とリカバリをサポートします。サポートは Windows 回復環境（Windows RE）を使用している Windows 8 および 8.1、Windows 2012 および 2012 R2 のマシンにも適応されます。

1. 次の手順のいずれか 1 つを実行します。
   - マシンの保護ウィザードから開始する場合は、手順 2 に進みます。
   - Rapid Recovery Core Console から開始する場合は、ボタンバーの **Protect**（保護）をクリックします。

   Protect Machine Wizard（マシンの保護ウィザード）が表示されます。
2. **Welcome**（ようこそ）ページで、適切なインストールオプションを選択します。
   - リポジトリの定義または暗号化の確立が必要ない場合は、**Typical**（標準）を選択します。
   - リポジトリを作成する必要がある場合、選択したマシンのバックアップ用に別のリポジトリを定義する必要がある場合、またはウィザードを使用して暗号化を設定する必要がある場合は、**詳細（オプションの手順を表示）**を選択します。
   - 今後マシンの保護ウィザードで **Welcome**（ようこそ）ページを表示したくない場合は、**Skip this Welcome page the next time the wizard opens**（次回ウィザードを開く際にようこそページをスキップする）オプションを選択します。

3. Welcom（ようこそ）ページの選択内容に問題がなければ、**Next**（次へ）をクリックします。

   Connection（接続）ページが表示されます。

4. **Connection**（接続）ページで、次の表の説明通りに接続するマシンに関する情報を入力し、**Next**（次へ）をクリックします。

   表 6. マシンの接続設定

テキストボックス	説明
ホスト	保護するマシンのホスト名または IP アドレス。
ポート	Rapid Recovery Core がマシン上のエージェントと通信する際のポート番号。 デフォルトポート番号は 8006 です。
ユーザー名	このマシンへの接続に使用するユーザー名（例、管理者 (または、マシンがドメイン内にある場合は [ドメイン名]\管理者))。
パスワード	このマシンに接続するために使用するパスワード。

   次にマシン保護ウィザードで **Install Agent**（エージェントのインストール）ページが表示された場合、これは Rapid Recovery がマシン上で Rapid Recovery Agent を検出せず、ソフトウェアの現在のバージョンをインストールすることを意味します。

5. **メモ: Core にバックアップする前に、保護するマシンにエージェントソフトウェアをインストールして、そのマシンを再起動する必要があります。インストーラで保護対象マシンを再起動するには、インストール後にマシンを自動的に再起動（推奨）オプションを選択してから Next（次へ）をクリックします。**

   Next（次へ）をクリックします。

Windows マシンでの Rapid Recovery Agent ソフトウェアのインストール

『*Dell Data Protection | Rapid Recovery 6.0 インストールおよびアップグレードガイド*』のトピック「Rapid Recovery Agent ソフトウェアのインストール」で説明されている方法の 1 つを使用して、保護するマシンに Rapid Recovery Agent のインストーラファイルを導入します。次に、以下の説明に従ってインストーラプログラムを起動し、Rapid Recovery Core で保護する各 Windows マシンにソフトウェアをインストールまたはアップグレードします。

メモ: ローカルの管理者権限でインストーラを実行する必要があります。

1. 保護対象のマシンから、実行可能ファイルである Rapid Recovery Agent のインストーラファイルをダブルクリックしてインストーラを開始します。

   お使いのマシンの設定によっては、「ユーザー アカウント制御」ウィンドウまたは「ファイルを開く - セキュリティ警告」ウィンドウが表示される可能性があります。

2. インストールの許可を求めるプロンプトが表示された場合は、インストーラを実行してシステムに変更を加えることを同意します。
3. .NET コンポーネントがない、またはアップグレードする必要がある場合は、フレームワークをダウンロードしてインストールすることを求めるプロンプトに同意します。
4. 言語フィールドで適切な言語を選択して、**OK** をクリックします。
5. 次のいずれかを選択します。
   - このマシンで初めて Rapid Recovery Agent ソフトウェアをインストールする場合は、インストーラがインストール準備を行った後で、Rapid Recovery Agent のインストールウィザードが表示されます。手順 6 に進みます。
   - このマシンに以前のバージョンの AppAssure Agent または Rapid Recovery Agent ソフトウェアがインストールされている場合は、現在のバージョンにアップグレードするかどうかを尋ねるメッセージが表示されます。

     1. **Yes**（はい）をクリックします。

        Rapid Recovery Agent のインストールウィザードが開き、ウィザードの **Progress**（進捗状況）ページが表示されます。アプリケーションが宛先フォルダにダウンロードされます。進捗状況は進捗バーに表示されます。終了すると、ウィザードは自動的に **Completed**（完了）ページに進みます。

     2. 手順 12 に進みます。

6. Rapid Recovery Agent のインストールウィザードの **Welcome**（ようこそ）ページで **Next**（次へ）をクリックし、インストールを続行します。

   License Agreement（ライセンス契約）ページが表示されます。

7. **License Agreement**（ライセンス契約）ページで、**I accept the terms in the license agreement**（ライセンス契約の条件に同意します）をクリックしてから、**Next**（次へ）をクリックします。

   Prerequisites（前提条件）ページが表示されます。

8. Rapid Recovery Agent のインストーラで、前提条件ファイルが存在するかどうか検証されます。
   - 前提条件ファイルが存在すると、すべての前提条件ファイルがマシンにインストールされていることを示すメッセージが表示されます。
   - 前提条件ファイルが存在しない場合、Rapid Recovery Agent のインストーラによって必要なファイルが識別され、その結果が表示されます。たとえば、CRT 2013（x64）ENU（Microsoft Visual Studio®用の再頒布可能コード）、または SQL Server 2008 R2（x64）用の Microsoft System CLR タイプなどが表示されます。**Install Prerequisites**（インストールの前提条件）をクリックします。

9. 必須ファイルのインストールが完了したら、**Next**（次へ）をクリックします。

   Installation Options（インストールオプション）ページが表示されます。

10. **Installation Options**（インストールオプション）ページで、インストールオプションを確認します。オプションは、必要に応じて以下の説明に従って変更します。
    - **Destination Folder**（宛先フォルダ）テキストフィールドで、インストール先フォルダを確認します。場所を変更する場合は、次の手順を実行します。
      - フォルダアイコンをクリックします。
      - **Browse to Destination Folder**（宛先フォルダの参照）ダイアログボックスで、新しい場所を選択します。
      - **OK** をクリックします。
    - **ポート番号**テキストフィールドに、保護対象マシンの Agent ソフトウェアと Rapid Recovery Core 間の通信に使用するポート番号を入力します。

      メモ: デフォルト値は 8006 です。ポート番号を変更する場合は、後で設定の調整が必要になる場合に備えて、その番号をメモしておきます。

    - デルに診断情報と使用状況情報を送信するには、**Allow Agent to automatically send diagnostic and usage information to Dell Inc.**（**Agent** がデルに診断情報および使用状況情報を自動送信することを許可する）を選択します。この情報を送信しない場合は、このオプションをクリアしてください。

11. インストールオプションに問題がなければ、**Install**（インストール）をクリックします。

    Progress（進捗状況）ページが表示されます。このページには、インストールの進捗状況を監視できるステータスバーが含まれています。

    インストールが完了すると、**Completed**（完了）ページが表示されます。手順 12 に進みます。

12. **Completed**（完了）ページで、インストールを有効にするためにシステムを再起動する必要があるというメッセージが表示された場合は、次のいずれかの手順を実行します。
    - すぐに再起動するには、**Yes, I want to restart my computer now**（はい、今すぐコンピュータを再起動します）を選択します。
    - 後で再起動するには、**Yes, I want to restart my computer now**（はい、今すぐコンピュータを再起動します）オプションをクリアします。

13. **Completed**（完了）ページで **Finish**（終了）をクリックします。

    インストーラウィザードが閉じ、Agent のインストールが完了します。

Rapid Recovery Agent ソフトウェアの 1 つまたは複数のマシンへの導入

Rapid Recovery Agent ソフトウェアを 1 つまたは複数の Windows マシンに導入するタスクは、Agent ソフトウェアの導入ウィザードを使用して簡略化することができます。

メモ: これまで、この機能は「一括導入」と呼ばれていました。

Agent ソフトウェアの導入ウィザードを使用すると、Rapid Recovery はホスト上のマシンを自動的に検知することができるようになり、ユーザーは導入するマシンを選択できます。Active Directory、vCenter、ESX(i) 以外のドメインまたはホスト上のマシンは、IP アドレスと適切な資格情報を使用して個々のマシンに手動で接続することができます。また、ローカルの Rapid Recovery Core に既に保護されているマシンに、ソフトウェアのアップグレードをプッシュすることもできます。

Core Console 内から、次のいずれかのタスクを実行できます。

- Active Directory ドメイン上のマシンへの導入
- VMware vCenter/ESX(i) 仮想ホスト上のマシンへの導入

メモ: 同時に導入できるマシンの数を 50 以下に制限して、導入操作が失敗する原因となる可能性があるリソースの制約が起きないようにすることをお勧めします。

クライアントでの Microsoft Windows エージェントのインストール

エージェントをインストールするには、次の手順を実行します。

1. クライアントに the Microsoft .NET 4 framework がインストールされていることを確認します。
   a. クライアントで **Windows Server Manager** を起動します。
   b. **Configuration**（設定） → **Services**（サービス）をクリックします。
   c. Microsoft .NET Framework がサービスのリストに表示されていることを確認します。
      インストールされていない場合は、**microsoft.com** からコピーを入手できます。
2. エージェントをインストールします。
   a. お使いのアプライアンスで、バックアップする予定のクライアントのディレクトリ C:\Program Files\AppRecovery を共有します。
   b. クライアントシステムで、DL アプライアンス上の C:\Program Files\AppRecovery にドライブをマップします。
   c. クライアントシステムで C:\Program Files\AppRecovery ディレクトリを開き、クライアントシステム用に正しいエージェントをダブルクリックして、インストールを開始します。

Active Directory ドメイン上のマシンへの導入

Rapid Recovery Agent ソフトウェアを 1 つまたは複数の Active Directory ドメイン上のマシンに同時に導入するには、次の手順を実行します。
この手順を開始する前に、Active Directory サーバのドメイン情報とログオン資格情報を準備しておきます。

1. Rapid Recovery Core Console で、**Protect**（保護）ドロップダウンメニューをクリックして、**Deploy Agent Software**（エージェントソフトウェアの導入）をクリックします。
   エージェントソフトウェアの導入ウィザード が開きます。
2. ウィザードの **Connection**（接続）ページで、**Source**（ソース）ドロップダウンリストから **Active Directory** を選択します。
3. 次の表の説明に従って、ドメイン情報とログオン資格情報を入力します。

   表 7. ドメイン情報と資格情報

テキストボックス	説明
ホスト	Active Directory ドメインのホスト名または IP アドレス。
ユーザー名	ドメインへの接続に使用するユーザー名（例、管理者、またはマシンがドメイン内にある場合は [ドメイン名]\管理者）。
パスワード	このドメインへの接続に使用するセキュアなパスワード。

4. **Next**（次へ）をクリックします。
5. **Machines**（マシン）ページで、Rapid Recovery Agent ソフトウェアを導入するマシンを選択します。
6. エージェントがインストールされた後に、必要に応じて自動的に保護対象マシンを再起動するには、**エージェントのインストール後に、マシンを自動的に再起動する（推奨）**を選択します。
7. **Finish**（終了）をクリックします。
   システムは選択されている各マシンを自動的に検証します。
   Rapid Recovery が自動検証中に問題点を検出した場合は、ウィザードが警告ページに進み、このページでマシンを選択対象からクリアして手動で選択済みのマシンを検証することができます。追加したマシンが自動検証に合格した場合は、マシンへのエージェントの導入ペインに表示されます。
8. 警告ページが表示されたが選択が適切である場合は、**Finish**（終了）をもう一度クリックします。

Rapid Recovery Agent ソフトウェアが指定されたマシンに導入されます。マシンはまだ保護されていません。マシンを保護するには、『*Rapid Recovery 6.0 on DL Appliances ユーザーズガイド*』の「Active Directory ドメインでの複数マシンの保護」のトピックを参照してください。

VMware vCenter/ESX(i) 仮想ホスト上のマシンへの導入

Rapid Recovery エージェントのソフトウェアを VMware vCenter/ESX(i) 仮想ホスト上の 1 つまたは複数のマシンに同時に導入するには、次の手順を実行します。
この手順を開始する前に、次の情報が必要です。

- VMware vCenter/ESX(i) 仮想ホストのためのログオン資格情報。
- ホストの場所。
- 保護する各マシンのログオン資格情報。

メモ: すべての仮想マシンに、VMware ツールがインストールされている必要があります。インストールされていないと、Rapid Recovery は導入先の仮想マシンのホスト名を検出できません。Rapid Recovery ではホスト名の代わりに仮想マシン名を使用するため、ホスト名が仮想マシン名と異なると問題が発生する場合があります。

1. Rapid Recovery Core Console で、**Protect（保護）**ドロップダウンメニューをクリックして、 **Deploy Agent Software（エージェントソフトウェアの導入）**をクリックします。

   エージェントソフトウェアの導入ウィザードが開きます。
2. ウィザードの **Connection（接続）**ページで、**Source（ソース）**ドロップダウンリストから **vCenter / ESX(i)** を選択します。
3. 次の表の説明に従って、ホスト情報とログオン資格情報を入力します。

   表 8. vCenter/ESX(i) 接続設定

テキストボックス	説明
ホスト	VMware vCenter Server/ESX(i) 仮想ホストの名前または IP アドレス。
ポート	仮想ホストへの接続に使用するポート。 デフォルト設定は 443 です。
ユーザー名	仮想ホストへの接続に使用するユーザー名（例、管理者 (または、マシンがドメイン内にある場合は [ドメイン名]\管理者))。
パスワード	この仮想ホストへの接続に使用するセキュアなパスワード。

4. **Next（次へ）**をクリックします。
5. ウィザードの **Machines（マシン）**ページで、ドロップダウンリストから次のオプションのいずれかを選択します。
   - ホストとクラスタ
   - VM とテンプレート
6. マシンのリストを展開し、ソフトウェアを導入する VM を選択します。

   Rapid Recovery によりマシンがオフラインであるか VMware ツールがインストールされていないことが検出された場合は、通知が表示されます。
7. 導入後に自動的にマシンを再起動する場合は、**エージェントのインストール後にマシンを自動的に再起動（推奨）**を選択します。
8. **Next（次へ）**をクリックします。

   Rapid Recovery は選択された各マシンを自動的に検証します。
9. ウィザードの **Adjustments（調整）**ページに、各マシンの資格情報を次の形式で入力します。
   `hostname::username::password`

   メモ: 各行に 1 台のマシンを入力してください。
10. **Finish（終了）**をクリックします。

    システムは選択されている各マシンを自動的に検証します。

Rapid Recovery が自動検証中に問題点を検出した場合は、ウィザードが警告ページに進み、このページでマシンを選択対象からクリアして手動で選択済みのマシンを検証することができます。追加したマシンが自動検証に合格した場合は、マシンへのエージェントの導入ペインに表示されます。

11. 警告ページが表示されたが選択が適切である場合は、**Finish**（終了）をもう一度クリックします。

Rapid Recovery Agent ソフトウェアが指定されたマシンに導入されます。

Linux マシンでのエージェントソフトウェアのインストールについて

保護する Linux マシンでエージェントソフトウェアをインストールする場合は、次のガイダンスを使用します。インストールが完了したら、『*Dell Data Protection | Rapid Recovery 6.0 インストールおよびアップグレードガイド*』の「Linux マシンでの Rapid Recovery Agent の設定」のトピックで説明されているように Agent を設定します。

注意: Linux マシンで新しくインストールされたエージェントソフトウェアを設定したら、マシンを再起動します。再起動により、マシンを保護するための適切なカーネルドライババージョンが使用されていることが保証されます。

Linux マシンでのエージェントソフトウェアのインストール方法と削除方法が変更されました。リリース 6.0.1 では、次の事項が適用されます。

- 現在インターネット接続されている Linux マシンに Agent をインストールする場合は、1 つのまとまった手順が適用されます。これをオンラインインストールと呼びます。シェルスクリプトを使用する代わりに、パッケージマネージャを使用してローカルの Linux マシンで参照されるリポジトリから Rapid Recovery ソフトウェアをインストールまたは削除します。

  メモ: リポジトリは関連するパッケージマネージャのファイルのステージングに使用されます。このリポジトリは、Rapid Recovery のリポジトリとは関係がありません。

- インターネット接続がない Linux マシン（エアギャップマシンや保護されたスタンドアロンマシンなど）に Agent をインストールする場合は、これをオフラインインストールと呼びます。このプロセスでは、最初にインターネット接続がある Linux マシンからインストールパッケージをダウンロードしておく必要があり、次にそれらのインストールファイルをインストールするためにセキュリティ保護されたコンピュータへ移動します。

オンラインインストールでは、サポート対象の Linux ディストリビューションごとに異なるパッケージマネージャを使用しているため、サポート対象の Linux OS で Agent をインストール、アップグレードまたは削除する手順は、使用するパッケージマネージャによって異なります。パッケージマネージャとサポートする Linux ディストリビューションについては、次の表に記載します。

表 9. パッケージマネージャとサポートする Linux ディストリビューション

パッケージマネージャ	Linux ディストリビューション
yum	Red Hat Enterprise Linux（RHEL）をベースとした Linux ディストリビューション（RHEL、CentOS、および Oracle Linux など）
zypper	SUSE Linux Enterprise Server（SLES）バージョン 11、12
apt	Debian をベースとした Linux ディストリビューション（Debian 7 または 8、および Ubuntu 12.04 以降）

各 Linux マシンに対して 1 回のみのセットアップ手順を実行するには、パッケージマネージャが Dell Rapid Recovery のインストールファイルを取得する場所を示す、ローカルソフトウェアリポジトリを設定する必要があります。

メモ: このプロセスでは、インストール手順ごとに 1 ～ 4 のステップがあります。リポジトリが設定された Linux マシンで今後 Rapid Recovery Agent のエディションをアップグレードする場合は、これらのステップを実行する必要はありません。

Linux マシンでソフトウェアリポジトリを設定したら、パッケージマネージャは Rapid Recovery Agent ソフトウェアとその関連コンポーネントのインストールまたは削除に必要なパッケージの取得とインストールを実行できるようになります。関連するコンポーネントには、aamount（現在の local mount）、aavdisk（現在の rapidrecovery-vdisk）、および Mono（オープンソースで、ECMA 標準準拠の .NET フレームワーク対応ツールセットであり、Linux プラットフォームに Agent ソフトウェアを移植するために使用）などがあります。

各パッケージマネージャでは、Rapid Recovery パッケージのダウンロード用の設定が行われていることを確認する、適切なコマンドをコマンドラインで実行することができます。これらのコマンドを、次の表に示します。

表 10. パッケージマネージャのリポジトリ設定を表示するコマンド

パッケージマネージャ	設定されているリポジトリのリストを表示するコマンド
yum	yum replolist
zypper	zypper repos
apt	ls /etc/apt/sources.list.d

Rapid Recovery Agent バージョンをインストールし、Rapid Recovery Core を使用して Linux マシンを保護する前に、以前のバージョンの AppAssureAgent ソフトウェアを Linux マシンから完全に削除しておく必要があります。これは、オンラインインストールまたはオフラインインストールのどちらの場合にも当てはまります。AppAssure Agent の削除では、シェルスクリプトを使用します。アンインストール手順は、使用中の Linux ディストリビューションに応じて異なります。Linux マシンからの AppAssure Agent のアンインストールについては、『*Dell Data Protection | Rapid Recovery 6.0 インストールおよびアップグレードガイド*』の「Linux マシンからの AppAssure Agent ソフトウェアのアンインストール」を参照してください。

メモ: 新しい Rapid Recovery Agent ソフトウェアを削除する場合は、各ディストリビューションのパッケージマネージャを使用します。したがって、Rapid Recovery Agent をアンインストールする場合は、『*Dell Data Protection | Rapid Recovery 6.0 インストールおよびアップグレードガイド*』の「Linux マシンからの Rapid Recovery Agent ソフトウェアのアンインストール」のトピックに記載されている適切な手順を参照してください。

AppAssure Agent をインストールしたことがない Linux マシンに Rapid Recovery Agent をインストールする場合は、前の表から適切なパッケージマネージャを決定します。その後、適切なインストール手順に従います。

Linux マシンで新しくインストールされた Agent ソフトウェアの設定が完了したら、マシンを再起動する必要があります。再起動により、マシンを保護するための適切なカーネルドライババージョンが使用されていることが保証されます。

このように、AppAssure から Rapid Recovery へのアップグレードには、次のインストールプロセスが含まれます。

- AppAssure Agent ソフトウェアの削除（初回インストールの場合は不要）
- お使いの Linux ディストリビューションに関連するパッケージマネージャの確認
- ソフトウェアリポジトリの設定を含む、Linux マシンでの Rapid Recovery Agent のインストール手順の実行（インストール手順のステップ 1 ～ 4）
- 設定ユーティリティの実行による、ポートの設定、ユーザー設定、ファイアウォール除外の追加、カーネルモジュールのインストール、および Agent サービスの開始
- Linux マシンの再起動

Linux マシンへの Agent ソフトウェアのインストール手順は、使用する Linux ディストリビューションに応じてわずかに異なります。インターネットに接続されている Linux マシンへの Agent ソフトウェアの事前作業およびインストールの詳細については、該当するトピックを参照してください。次のいずれかの項を選択できます。

- Debian または Ubuntu での Rapid Recovery Agent ソフトウェアのインストール
- Suse Linux Enterprise Server での Rapid Recovery Agent ソフトウェアのインストール

インターネットに接続されていない Linux マシンへの Agent ソフトウェアの事前作業およびインストールの詳細については、次のトピックを参照してください。

- オフラインの Linux マシンでのエージェントソフトウェアのインストール

Agent ソフトウェアのインストールを開始する前に、『*Dell Data Protection | Rapid Recovery 6.0 インストールおよびアップグレードガイド*』の次のトピックを参照してください。「Linux ディストリビューションのダウンロード」、「セキュリティについて」、「Linux Agent ファイルの場所」、「Agent の依存関係」、「Linux スクリプトの詳細」

Linux Agent ファイルの場所

Linux マシン上の Rapid Recovery Agent ソフトウェアをサポートするために必要なファイルがいくつかあります。サポート対象のすべての Linux ディストリビューションでは、これらのファイルは次のディレクトリに格納されています。

- mono：
  `/opt/apprecovery/mono`
- agent：
  `/opt/apprecovery/agent`
- local mount：
  `/opt/apprecovery/local_mount`
- rapidrecovery-vdisk および aavdctl：
  `/usr/bin/aavdisk`
- rapidrecovery-vdisk の設定ファイル：
  `/etc/apprecovery/aavdisk.conf`
- agent および local_mount のラッパー
  `/usr/bin/agent`

  `/usr/bin/local_mount`
- agent および rapidrecovery-vdisk の自動実行スクリプト：
  `/etc/init.d/rapidrecovery-agent`

  `/etc/init.d/rapidrecovery-vdisk`

エージェントの依存関係

次の依存関係は必須であり、エージェントインストーラパッケージの一部としてインストールされます。

- Debian および Ubuntu の場合：
  - rapidrecovery-agent に必要：
    ```
    dkms, gcc, make, linux-headers-`uname-r`
                    libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3
    ```
  - rapidrecovery-mono に必要：
    ```
    libc6 (>=2.7-18)
    ```
- Red Hat Enterprise Linux、CentOS、および Oracle Linux の場合：
  - nbd-dkms に必要：
    ```
    dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r`
    ```
  - rapidrecovery-agent に必要：
    ```
    dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r`,
                    nbd-dkms, libblkid, pam, pcre
    ```
  - rapidrecovery-mono に必要：
    ```
    glibc >=2.11
    ```
- SUSE Linux Enterprise Server の場合：
  - nbd-dkms に必要：
    ```
    dkms, gcc, make, kernel-syms
    ```
  - rapidrecovery-agent に必要：
    ```
    dkms, kernel-syms, gcc, make, libblkid1, pam, pcre
    ```
  - rapidrecovery-mono に必要：
    ```
    glibc >= 2.11
    ```

Debian または Ubuntu での Rapid Recovery Agent ソフトウェアのインストール

Rapid Recovery Agent の .deb ファイルは、apt パッケージマネージャに固有のリポジトリ情報を含むアーカイブです。Debian または Ubuntu のマシンに Rapid Recovery Agent をオンラインでインストールするには、次の手順を実行します。

メモ: この手順は、インターネットに接続されている Linux マシンに適用されます。オフラインで Linux マシンに Rapid Recovery Agent をインストールするには、オフラインの Linux マシンでのエージェントソフトウェアのインストールを参照してください。

1. root アクセス権でターミナルセッションを開きます。
2. PWD と入力して **Enter** を押し、現在の作業ディレクトリを確認します。たとえば、現在の作業ディレクトリが **/home/rapidrecovery/** であるとします。
3. 適切な Rapid Recovery Agent の .deb インストールファイルを、ライセンスポータル (https://licenseportal.com) から現在の作業ディレクトリにダウンロードします。

   ライセンスポータルの詳細については、『*Dell Data Protection | Rapid Recovery ライセンスポータル ユーザーガイド*』を参照してください。
4. お使いの Linux マシンと、Rapid Recovery ソフトウェアおよびコンポーネントが保存されているリモートの Dell リポジトリとの間で永続的な接続を確立するには、次のコマンドを入力します。

   ```
   dpkg -i <.deb installation file you downloaded>
   ```

   たとえば、ディレクトリ **/home/rapidrecovery/** に rapidrecovery-repo-6.0.2.999.deb という名前のインストーラファイルがある場合は、次のコマンドを入力して **Enter** を押します。

   ```
   dpkg -i rapidrecovery-repo-6.0.2.999.deb
   ```

   Agent に必要なパッケージまたはファイルが欠落している場合は、リモートリポジトリからダウンロードされ、スクリプトの一部として自動的にインストールされます。

   メモ: Linux マシンへのインストールにおける依存関係の詳細については、エージェントの依存関係を参照してください。
5. apt パッケージマネージャを呼び出し、リポジトリマネージャをアップデートして、Rapid Recovery Agent をインストールします。次のコマンドを入力して **Enter** を押します。

   ```
   apt-get update
   ```
6. Rapid Recovery Agent ソフトウェアをインストールするようパッケージマネージャに指示します。次のコマンドを入力して **Enter** を押します。

   ```
   apt-get install rapidrecovery-agent
   ```
7. パッケージマネージャにより、すべての依存ファイルのインストール準備が行われます。署名のないファイルのインストールを確認するプロンプトが表示される場合は、**y** を入力して **Enter** を押します。

   Rapid Recovery Agent のファイルがインストールされます。

Suse Linux Enterprise Server での Rapid Recovery Agent ソフトウェアのインストール

Rapid Recovery Agent の .rpm ファイルは、SUSE Linux Enterprise Server（SLES）のリポジトリ情報を含むアーカイブです。このディストリビューションでは、zypper パッケージマネージャを使用します。SLES に Rapid Recovery Agent をインストールするには、次の手順を実行します。

メモ: この手順は、インターネットに接続されている Linux マシンに適用されます。オフラインで Linux マシンに Rapid Recovery Agent をインストールするには、オフラインの Linux マシンでのエージェントソフトウェアのインストールを参照してください。

1. root アクセス権でターミナルセッションを開きます。
2. PWD と入力して **Enter** を押し、現在の作業ディレクトリを確認します。たとえば、現在の作業ディレクトリが **/home/rapidrecovery/** であるとします。
3. 適切な Rapid Recovery Agent の .rpm インストールファイルを、ライセンスポータル（https://licenseportal.com）から現在の作業ディレクトリにダウンロードします。

ライセンスポータルの詳細については、『*Dell Data Protection | Rapid Recovery ライセンスポータル ユーザーガイド*』を参照してください。

4. お使いの Linux マシンと、Rapid Recovery ソフトウェアおよびコンポーネントが保存されているリモートの Dell リポジトリとの間で永続的な接続を確立するには、次のコマンドを入力します。

```
rpm -ivh <.rpm installation file you downloaded>
```

たとえば、ディレクトリ **/home/rapidrecovery/** に rapidrecovery-repo-6.0.2.999.rpm という名前のインストーラファイルがある場合は、次のコマンドを入力して **Enter** を押します。

```
rpm -ivh rapidrecovery-repo-6.0.2.999.rpm
```

Agent に必要なパッケージまたはファイルが欠落している場合は、リモートリポジトリからダウンロードされ、スクリプトの一部として自動的にインストールされます。

メモ: Linux マシンへのインストールにおける依存関係の詳細については、エージェントの依存関係を参照してください。

5. zypper パッケージマネージャを起動してリポジトリマネージャをアップデートし、Rapid Recovery Agent をインストールします。次のコマンドを入力して **Enter** を押します。

```
apt-get update
```

6. Rapid Recovery Agent ソフトウェアをインストールするようパッケージマネージャに指示します。次のコマンドを入力して **Enter** を押します。

```
apt-get install rapidrecovery-agent
```

7. パッケージマネージャにより、すべての依存ファイルのインストール準備が行われます。署名のないファイルのインストールを確認するプロンプトが表示される場合は、**y** を入力して **Enter** を押します。

Rapid Recovery Agent のファイルがインストールされます。

Red Hat Enterprise Linux と CentOS でのエージェントのインストール

メモ: これらの手順を行う前に、Red Hat または CentOS 向けのインストーラパッケージを /home/system directory にダウンロードするようにしてください。以下の手順は、32 ビット環境でも 64 ビット環境でも同じです。

Red Hat Enterprise Linux と CentOS でエージェントをインストールするには、次の手順を実行します。

1. root アクセス権でターミナルセッションを開きます。
2. エージェントインストーラを実行可能ファイルにするには、次のコマンドを入力します。

`chmod +x appassure-installer__rhel_amd64_5.x.x.xxxxx.sh` と入力して、<Enter> を押します。

メモ: 32 ビットの環境では、インストーラは `appassureinstaller__ rhel_i386_5.x.x.xxxxx.sh` と命名されます。

ファイルが実行可能ファイルになります。

3. エージェントを解凍してインストールするには、次のコマンドを入力します。

`/appassure-installer_rhel_amd64_5.x.x.xxxxx.sh` と入力して、<Enter> を押します。

Linux エージェントが解凍とインストールの処理を開始します。エージェントが必要とするパッケージやファイルがない場合は、スクリプトの一部で自動的にダウンロードおよびインストールされます。

エージェントが必要とするファイルの詳細に関しては、エージェントの依存関係 を参照してください。

インストーラが完了すると、Agent がマシンで実行されます。Core によるこのマシンの保護に関する詳細は、**Dell.com/support/home** で『*Rapid Recovery 6.0 on DL Appliances ユーザーズガイド*』の「ワークステーションとサーバの保護について」のトピックを参照してください。

オフラインの Linux マシンでのエージェントソフトウェアのインストール

このタスクを実行するには、オンラインの Linux マシンとリムーバブルストレージメディアへのアクセス、および最終的なオフラインの Linux マシンへのアクセスが可能である必要があります。オフラインの Linux マシンに AppAssure Agent がインストールされている場合は、Rapid Recovery Agent をインストールする前に AppAssure Agent をアンインストールする必要があります。詳細については、『*Dell Data Protection | Rapid Recovery インストールおよびアップグレードガイド*』の「Linux マシンからの AppAssure Agent ソフトウェアのアンインストール」の項を参照してください。

インターネットにアクセスできない Linux マシンに Agent ソフトウェアをインストールする場合は、この手順に従ってください。インストールが完了したら、Linux マシンでの Rapid Recovery Agent の設定のトピックで説明されているように Agent を設定します。

メモ: 複数の Linux ディストリビューションでインストールする場合は、この手順を各ディストリビューションごとに 1 度ずつ実行します。

1. インターネットにアクセスできる Linux マシンから、ターミナルウィンドウを開き、次のコマンドを入力します。

   ```
   wget http://s3.amazonaws.com/repolinux/6.0.2/packages-downloader.sh
   ```

   シェルスクリプトが現在のディレクトリにダウンロードします。
2. 次のコマンドを実行して、シェルスクリプトを実行します。

   ```
   bash packages-downloader.sh
   ```

   スクリプトが実行され、特定の Linux ディストリビューションとアーキテクチャを選択するよう求めるプロンプトが表示されます。
3. インストールするインストールパッケージの番号を入力し **Enter** を押します。

   たとえば、Red Hat Enterprise Linux 7 のインストールパッケージを取得するには、3 を入力して **Enter** を押します。

   適切なインストーラは、~/rapidrecovery.packages/ ディレクトリに抽出されます。

   メモ: チルダ文字「~/」は、自分のホームディレクトリを表します。
4. Rapid Recovery Agent のパッケージをリムーバブルメディアにコピーします。リムーバブルメディアで指定される場所は、Linux ディストリビューションによって異なる場合があります。次のコマンドを入力して **Enter** を押します。

   ```
   cp -R ~/rapidrecovery.packages/ <your_removable_media>
   ```

   たとえば、/media/USB-drive-1 にマウントされているリムーバブル USB ドライブを使用する場合は、次のコマンドを入力して **Enter** を押します。

   ```
   cp -R ~/rapidrecovery.packages /media/USB-drive-1
   ```

   必要なファイルがすべてリムーバブルメディアにコピーされます。
5. リムーバブルメディアをオフラインの Linux マシンに持っていき、そのドライブをマウントします。
6. データを、マウントされたデバイスから自分のホームディレクトリまたはその他の目的の場所にコピーします。たとえば、次のコマンドを入力して **Enter** を押します。

   ```
   cp -R /media/USB-drive-1 ~/rapidrecovery.packages
   ```
7. Rapid Recovery ディレクトリに変更します。たとえば、次のコマンドを入力して **Enter** を押します。

   ```
   cd ~/rapidrecovery.packages
   ```
8. root 権限で Agent のインストールを実行します。このコマンドは、Linux ディストリビューションによって異なります。
   - Red Hat、SLES、Oracle、および CentOS の場合は、次のコマンドを入力して **Enter** を押します。

     ```
     sudo rpm -i *.rpm
     ```
   - Debian および Ubuntu の場合は、次のコマンドを入力して **Enter** を押します。

     ```
     sudo dpkg -i *.deb
     ```

   ローカルに保存されたパッケージマネージャで、Rapid Recovery Agent のインストールを実行します。

インストールが完了したら、Linux マシンでの Rapid Recovery Agent の設定のトピックで説明されているように Agent を設定します。

注意: Linux マシンで新しくインストールされた Agent ソフトウェアの設定が完了したら、マシンを再起動する必要があります。再起動により、マシンを保護するための適切なカーネルドライババージョンが使用されていることが保証されます。

Windows Server Core Edition マシンでの Agent ソフトウェアのインストール

Windows Server Core マシンで Agent ソフトウェアをインストールするには、次の手順を実行します。

メモ: 次の手順では、コンソールモードで Agent ソフトウェアをインストールします。サイレントモードでインストールするには、コマンドラインでインストーラファイル名に `/silent` を付け加えます。たとえば、`Agent-X64-6.X.X.xxxxx.exe /silent` のようにします。

1. Rapid Recovery Agent インストーラファイルを Dell Data Protection | Rapid Recovery ライセンスポータルまたは Rapid Recovery Core からダウンロードします。
2. コマンドプロンプトから、Rapid Recovery Agent インストーラファイルを含むディレクトリに移動し、インストーラファイル名を入力して、インストールを開始します。

   ```
   Agent-X64-6.x.x.xxxxx.exe
   ```

   インストールプログラムによって Agent ソフトウェアがインストールされ、コンソールに進捗状況が表示されます。完了すると、インストール済みの新環境によりマシンが自動で再起動されます。Agent のアップグレードでは、マシンを再起動する必要はありません。

Linux マシンでの Rapid Recovery Agent の設定

Linux マシンに Rapid Recovery Agent ソフトウェアをインストールしたら、Rapid Recovery の設定ユーティリティを実行します。これにより、Core で保護する Linux マシン上でカーネルモジュールがコンパイルおよびインストールされます。

設定ユーティリティにはいくつかの設定オプションがあり、特定の設定情報を検知した場合には、手順番号が付いたステップにヒントが表示されます。

Linux マシンで Rapid Recovery Agent ソフトウェアを設定するには、下記の手順を実行します。一部の設定オプションは、インストールしている Linux ディストリビューションに応じて異なります。

1. root アクセス権でターミナルセッションを開きます。
2. 次のコマンドを入力して設定ユーティリティを起動し、<Enter> を押します。

   ```
   sudo /usr/bin/rapidrecovery-config
   ```

   設定ユーティリティが開始します。開始すると複数の設定オプションがリストされます。これらには、適切な設定手順のための入力用インデックス番号が付いています。
3. 次のコマンドを入力してこの保護対象マシンのポートを設定し、<Enter> を押します。デフォルトポートは 8006 です。

   ```
   1 <agent_port>
   ```

   たとえば、デフォルトポートを使用する場合は、次のコマンドを入力します。

   ```
   1 8006
   ```
4. 次のコマンドを入力して保護機能を使用できるユーザーを設定し、<Enter> を押します。

   ```
   1 <user_names_separated_by_comma>
   ```

   たとえば、ユーザー名が michael である管理者とユーザー名 test_user1 を使用する場合は、次のコマンドを入力します。

   ```
   2 michael,administrator,test_user1
   ```
5. ファイアウォールのルールを設定して、ファイアウォールの設定マネージャを選択します。これにより、手順 1 で指定されたポート用のファイアウォールの例外が設定されます。

ユーティリティが 1 つまたは複数のファイアウォールの設定マネージャ（lokkit や firewalld など）を検知した場合は、ユーティリティの 3 行目に各ファイアウォールがリストされます。適切な設定マネージャを選択して入力し、コマンド番号 (3) で開始して <Enter> を押します。

```
3 <firewall_configuration>
```

たとえば、firewalld を使用している場合は、次のコマンドを入力します。

```
3 firewalld
```

6. コマンド番号を入力して <Enter> を押し、ユーティリティから互換性のあるカーネルモジュールをリストするように問い合わせます。

```
4
```

サブシェルによって、インストールで互換性のあるすべてのカーネルモジュールが返されます。たとえば、次のように返されます。

```
Searching for all available for installation kernels.
This might take a while, depending on the Internet connection speed.
Kernels compatible for module installation:
 0 - linux-image-3.16.0.23-generic
 1 - linux-image-3.16.0.31-generic
 2 - linux-image-3.16.0.33-generic
 3 - linux-image-3.16.0.34-generic
Input indices of the kernel modules you wish to install, delimited by space; use 'all'
to install into all supported kernels, or 'q' to quit.
```

7. 適切な Rapid Recovery カーネルモジュールを設定します。

たとえば、3.16.0-23 および 3.16.0-34 のカーネルモジュールを入力し、`1 4` を入力して、<Enter> を押します。

すべてのカーネルモジュールを入力するには、`all` を入力して <Enter> を押します。

8. 新しくインストールされた Agent ソフトウェアの設定が完了したら、マシンを再起動します。再起動により、マシンを保護するための適切なカーネルドライバが使用されていることが保証されます。

このプロセスが完了すると、その Linux マシン上でローカルリポジトリが設定されます。Agent ソフトウェアがインストールされ、カーネルモジュールがロードされます。

次の手順で、Rapid Recovery Core 上のマシンを保護します。

マシンの保護

保護するマシンに Rapid Recovery Agent ソフトウェアをすでにインストールしているのに、それをまだ再起動していない場合は、すぐにマシンを再起動してください。

このトピックでは、Protect Machine（マシンの保護）ウィザードを使用して、指定した 1 つのマシン上のデータの保護を開始する方法について説明します。

保護を追加するときには、IP アドレスやポートなどの接続情報の定義と、保護するマシンの資格情報の入力が必要です。必要に応じて、IP アドレスの代わりに Core Console に表示される表示名を入力できます。表示名を入力すると、Core Console で詳細を表示したときに、保護対象マシンの IP アドレスが表示されなくなります。また、マシンの保護スケジュールも定義します。

環境によっては、保護ウィザードのワークフローが若干異なる場合があります。たとえば、保護するマシンに Rapid Recovery Agent ソフトウェアがインストールされている場合、ウィザードでエージェントソフトウェアをインストールするように求められることはありません。同様に、Core にリポジトリが既に存在している場合、リポジトリを作成するように求められることはありません。

1. 次の手順のいずれか 1 つを実行します。
   - マシンの保護ウィザードから開始する場合は、手順 2 に進みます。
   - Rapid Recovery Core Console から開始する場合は、ボタンバーの **Protect（保護）** をクリックします。

Protect Machine Wizard（マシンの保護ウィザード）が表示されます。

2. **Welcome**（ようこそ）ページで、適切なインストールオプションを選択します。
   - リポジトリの定義または暗号化の確立が必要ない場合は、**Typical**（標準）を選択します。
   - リポジトリを作成する必要がある場合、選択したマシンのバックアップ用に別のリポジトリを定義する必要がある場合、またはウィザードを使用して暗号化を設定する必要がある場合は、**詳細（オプションの手順を表示）**を選択します。
   - 今後マシンの保護ウィザードで **Welcome**（ようこそ）ページを表示したくない場合は、**Skip this Welcome page the next time the wizard opens**（次回ウィザードを開く際にようこそページをスキップする）オプションを選択します。
3. Welcom（ようこそ）ページの選択内容に問題がなければ、**Next**（次へ）をクリックします。

   Connection（接続）ページが表示されます。
4. **Connection**（接続）ページで、次の表の説明通りに接続するマシンに関する情報を入力し、**Next**（次へ）をクリックします。

   表 11. マシンの接続設定

テキストボックス	説明
ホスト	保護するマシンのホスト名または IP アドレス。
ポート	Rapid Recovery Core がマシン上のエージェントと通信する際のポート番号。 デフォルトポート番号は 8006 です。
ユーザー名	このマシンへの接続に使用するユーザー名（例、管理者 (または、マシンがドメイン内にある場合は [ドメイン名]\管理者))。
パスワード	このマシンに接続するために使用するパスワード。

次にマシン保護ウィザードで **Install Agent**（エージェントのインストール）ページが表示された場合、これは Rapid Recovery がマシン上で Rapid Recovery Agent を検出せず、ソフトウェアの現在のバージョンをインストールすることを意味します。手順 7 に進みます。

次にウィザードで **Upgrade Agent**（エージェントのアップグレード）ページが表示された場合は、保護するマシンに旧バージョンのエージェントソフトウェアが存在することを示します。

メモ: Core にバックアップする前に、保護するマシンにエージェントソフトウェアをインストールして、そのマシンを再起動する必要があります。インストーラで保護対象マシンを再起動するには、インストール後にマシンを自動的に再起動（推奨）オプションを選択してから Next（次へ）をクリックします。

5. **Upgrade Agent**（エージェントのアップグレード）ページで、次のいずれかを実行します。
   - Rapid Recovery Core のバージョンに合わせて、エージェントソフトウェアの新規バージョンを導入するには、**エージェントをソフトウェアの最新バージョンにアップグレード**を選択します。
   - エージェントソフトウェアのバージョンを更新せずにマシンの保護を継続するには、オプションの**エージェントをソフトウェアの最新バージョンにアップグレード** をクリアします。
6. **Next**（次へ）をクリックします。
7. Rapid Recovery Core Console で、この保護対象マシンを IP アドレスではなく名前で表示するには、**Protection**（保護）ページで、ダイアログボックスの**表示名**フィールドに名前を入力します。

   64 文字まで入力できます。『*Rapid Recovery on DL Appliances ユーザーズガイド*』の「禁止文字」のトピックで説明した特殊文字は使用しないでください。また、表示名の先頭に、『*Rapid Recovery on DL Appliances ユーザーズ*』の「禁止文字」トピックで説明した文字の組み合わせを使用しないでください。
8. 次の説明に従って、適切な保護スケジュールを選択します。
   - デフォルトの保護スケジュールを使用するには、スケジュール設定のオプションで、**Default protection**（デフォルト保護）を選択します。

   デフォルトの保護スケジュールでは、Core で 1 時間ごとに保護対象マシンのすべてのボリュームのスナップショットが取得されます。ウィザードを閉じた後に任意のタイミングで保護設定（保護するボリュームなど）を変更するには、特定の保護対象マシンの サマリ ページに移動します。

   - 別の保護スケジュールを定義するには、スケジュール設定オプションで、**Custom protection**（カスタム保護）を選択します。

9. 次のように設定を行います。
   - マシンの保護ウィザードで Typical（標準）設定を選択し、デフォルトの保護を指定した場合、**Finish**（終了）をクリックして選択内容を確定し、ウィザードを閉じると、指定したマシンが保護されます。

     マシンに対してはじめて保護が追加されると、保護を当初一時停止するように指定していない限り、定義したスケジュールに従ってベースイメージ（保護対象ボリューム内の全データのスナップショット）が Rapid Recovery Core 上のリポジトリに転送されます。
   - マシンの保護 ウィザードで Typical(標準) 設定を選択し、カスタム保護を指定した場合、**Next**（次へ） をクリックしてカスタム保護スケジュールをセットアップします。 カスタム保護スケジュールの定義に関する詳細は、『*Rapid Recovery 6.0 on DL Appliances ユーザーズガイド*』の「カスタム保護スケジュールの作成」セクションを参照してください。
   - マシンの保護ウィザードの Advanced（詳細）設定と、デフォルトの保護を選択した場合は、**Next**（次へ）をクリックして手順 14 に進み、リポジトリと暗号化のオプションを参照します。
   - マシンの保護ウィザードの Advanced（詳細）設定を選択し、カスタム保護を指定した場合は、**Next**（次へ）をクリックして手順 11 に進み、保護するボリュームを選択します。
10. **Protection Volumes**（保護ボリューム）ページで、保護するボリュームを選択します。保護の対象にしたくないボリュームがリストにある場合、チェック列をクリックして選択を解除します。その後、**Next**（次へ）をクリックします。

    メモ: 通常、少なくともシステムで予約されているボリュームとオペレーティングシステムのボリューム（通常は C ドライブ）を保護することをお勧めします。
11. **Protection Schedule**（保護スケジュール）ページで、カスタム保護スケジュールを定義して **Next**（次へ）をクリックします。カスタム保護スケジュールの定義に関する詳細は、『*Rapid Recovery 6.0 on DL Appliances ユーザーズガイド*』の「カスタム保護スケジュールの作成」セクションを参照してください。

    リポジトリ情報がすでに設定されており、手順 1 で Advanced（詳細）オプションを選択した場合、Encryption（暗号化）ページが表示されます。手順 13 に進みます。
12. 暗号化を有効にするには、**Encryption**（暗号化）ページで必要に応じて **暗号化を有効にする** を選択します。

    Encryption key（暗号化キー）フィールドが **Encryption**（暗号化）ページに表示されます。

    メモ: 暗号化を有効にすると、このマシンのすべての保護対象ボリュームのデータに適用されます。暗号化の設定は、後で Rapid Recovery Core Console で変更できます。暗号化の詳細については、www.dell.com/support/home で『*Rapid Recovery 6.0 on DL Appliances ユーザーズガイド*』を参照してください。

    注意: Rapid Recovery は 256 ビットキーを持つ CBC（Cipher Block Chaining、暗号文ブロック連鎖）モードの AES 256 ビット暗号化を使用します。暗号化はオプションですが、暗号化キーを設定し、定義したパスフレーズを保護することを強くお勧めします。データの回復に非常に重要であることから、パスフレーズは安全な場所に保管してください。パスフレーズがないとデータを回復できません。
13. **Encryption**（暗号化）ページで、次のいずれかを実行します。
    - Rapid Recovery Core ですでに定義されている暗号化キーを使用してこの保護対象マシンを暗号化する場合は、**既存の暗号化キーを使用してデータを暗号化**を選択して、ドロップダウンメニューから適切なキーを選択します。次の手順に進みます。
    - Core に新しい暗号化キーを追加して、そのキーをこの保護対象マシンに適用する場合は、次の表の説明に従って情報を入力します。

      表 12. 暗号化キーの設定

テキストボックス	説明
名前	暗号化キーの名前を入力します。 暗号化キーの名前には、1 ～ 130 文字の英数字を入力する必要があります。逆スラッシュ、順スラッシュ、パイプ、コロン、アスタリスク、引用符、疑問符、開き/閉じ括弧、アンパサンド、ナンバー記号などの特殊文字を含めることはできません。この情報は、Core Console から暗号化キーを表示するときに Description（説明）フィールドに表示されます。
説明	暗号化キーのコメントを入力します。 この情報は、Core Console から暗号化キーを表示するときに Description（説明）フィールドに表示されます。
パスフレーズ	アクセスの制御に使用するパスフレーズを入力します。

テキストボックス	説明
	ベストプラクティスは、上記の特殊文字を使用しないことです。 パスフレーズは安全な場所で記録してください。デルサポートでは、パスフレーズをリカバリできません。暗号化キーを作成して 1 つ以上の保護対象マシンに適用した後でパスフレーズを損失した場合は、データをリカバリできません。
パスフレーズの確認	テキストボックスに先ほど入力したパスフレーズを再度入力します。

14. **Finish**（終了）をクリックして、設定を保存し適用します。

    マシンに対してはじめて保護が追加されると、保護を当初一時停止するように指定していない限り、定義したスケジュールに従ってベースイメージ（保護対象ボリューム内の全データのスナップショット）が Rapid Recovery Core 上のリポジトリに転送されます。
15. エラーメッセージが表示される場合は、アプライアンスがバックアップ対象のマシンに接続できません。この問題を解決するには、次の手順を実行します。
    a. ネットワーク接続性をチェックします。
    b. ファイアウォール設定をチェックします。
    c. Rapid Recovery サービスと RPC が実行されていることを確認します。
    d. ドメイン名サービスルックアップを確認します（該当する場合）。

ネットワーク接続性のチェック

ネットワーク接続性をチェックするには、次の手順を実行します。

1. 接続先となるクライアントシステムで、コマンドラインインタフェースを開きます。
2. コマンド **ipconfig** を実行して、クライアントの IP アドレスをメモします。
3. アプライアンスでコマンドラインインタフェースを開きます。
4. コマンド **ping <IP address of client>** を実行します。
5. 結果に応じて、次のいずれかを行います。
   - クライアントが ping に応答しない場合は、サーバーの接続性とネットワーク設定を確認します。
   - クライアントが応答する場合は、ファイアウォール設定が Rapid Recovery コンポーネントの実行を許可していることをチェックします。

ファイアウォール設定のチェック

クライアントがネットワークに適切に接続されているにもかかわらず Core Console で認識できない場合は、ファイアウォールをチェックして、必要なインバウンドおよびアウトバウンド通信が許可されていることを確認してください。

Rapid Recovery Core と、Core がバックアップしているクライアントでファイアウォール設定をチェックするには、次の手順を実行します。

1. アプライアンスで、**Start**（スタート）→ **Control Panel**（コントロールパネル）とクリックします。
2. **コントロールパネル**で**システムとセキュリティ**をクリックし、**Windows ファイアウォール**で**ファイアウォールステータスのチェック**をクリックします。
3. **詳細設定**をクリックします。
4. **セキュリティが強化された Windows ファイアウォール**画面で、**受信の規則**をクリックします。
5. Rapid Recovery Core とポートが**有効**列で**はい**を示していることを確認します。
6. 規則が有効になっていない場合は、Rapid Recovery Core を右クリックして**規則の有効化**を選択します。
7. **送信の規則**をクリックして、Rapid Recovery Core について同じことを確認します。

名前解決の確認（該当する場合）

バックアップしようとしているマシンが DNS を使用する場合は、DNS 前方ルックアップと逆引きルックアップが正しいことを確認してください。

逆引きルックアップが正しいことを確認するには、次の手順を実行します。

1. アプライアンスで、C:\Windows\system32\drivers\etc ホストに移動します。
2. DL4300 にバックアップされる各クライアントの IP アドレスを入力します。

ネットワークアダプタのチームミング

デフォルトでは、DL4300 アプライアンス上のネットワークアダプタ（NIC）はバインドされておらず、システムのパフォーマンスに影響を与えます。NIC を 1 つのインタフェースにチーム化することをお勧めします。NIC のチーミングには次が必要です。

- Broadcom Advanced Control Suite の再インストール
- NIC チームの作成
- Hyper-V 仮想スイッチの設定

Broadcom Advanced Configuration Suite の再インストール

Broadcom Advanced Configuration Suite（BACS）を再インストールする：

1. お使いのシステム の NIC を識別します。NIC を識別するには、次の手順を実行します。
   a. Dell Open Manage Server Administrator（OMSA）にアクセスします。
   b. メインページで **System**（システム）→ **Main Sytem Chassis**（メインシステムシャーシ）→ **Slots**（スロット）をクリックします。
2. 以前のバージョンの Broadcom ドライバおよび管理アプリケーションをアンインストールします。
3. 適切な Broadcom ドライバおよび BACS をお使いのアプライアンスにダウンロードします。

   次のドライバは、**dell.com/support** で入手可能です。

   - QLogic ドライバ

     Servers, storage, & Networking（サーバー、ストレージ、ネットワーキング）→ **Dell Software DL 4300**（Dell ソフトウェア DL 4300）→ **Drivers & downloads**（ドライバ & ダウンロード） → **Category**（カテゴリ） → **Network**（ネットワーク） → **QLogic BCM57xx and BCM57xxx**（QLogic BCM57xx および BCM57xxx）の順にクリックします。
   - Broadcom ドライバ

     Servers, storage, & Networking（サーバー、ストレージ、ネットワーキング）→ **Dell Software DL 4300**（Dell ソフトウェア DL 4300）→ **Drivers & downloads**（ドライバ & ダウンロード） → **Category**（カテゴリ） → **Network**（ネットワーク） → **Broadcom Windows 64bit driver update for NetXtreme Ethernet adapters**（NetXtreme Ethernet アダプタ用 Broadcom Windows 64 ビットドライバのアップデート）の順にクリックします。
4. インストールウィザードを実行してインストールを完了します。

NIC チームの作成

メモ: Windows 2012 Server のネイティブチーミングインタフェースは使用しないことをお勧めします。チーミングアルゴリズムはインバウンドトラフィックではなく、アウトバウンドトラフィック用に最適化されており、チーム内により多くのネットワークポートがある場合にでも、バックアップ作業負荷でのパフォーマンスが不十分です。

NIC チーミングを作成するには、次の手順を実行します。

1. **Start**（スタート） → **Search**（検索） → **Broadcom Advanced Control Suite** と進みます。

   メモ: Broadcom Advanced Control Suite を使用するときは、Broadcom ネットワークカードのみを選択してください。
2. **Broadcom Advanced Control Suite** で、**Teams**（チーム） → **Go to Team View**（チームビューに移動）を選択します。
3. 左側の **Hosts list**（ホストリスト）で、DL4300 アプライアンスのホスト名を右クリックして **Create Team**（チームの作成）を選択します。

   Broadcom Teaming Wizard（Broadcom チーミングウィザード）ウィンドウが表示されます。
4. **次へ** をクリックします。
5. チームの名前を入力して **Next**（次へ）をクリックします。
6. **Team Type**（チームタイプ）を選択して **Next**（次へ）をクリックします。

7. チームに参加させるアダプタを選択して **Add**（追加）をクリックします。
8. チームに参加させるその他すべてのアダプタでこの手順を繰り返します。
9. チーム用のアダプタをすべて選択したら、**Next**（次へ）をクリックします。
10. チームで障害が発生したときにデフォルトとして使用できる NIC を希望する場合は、スタンバイ NIC を選択します。
11. **LiveLink** を設定するかどうかを選択して、**Next**（次へ）をクリックします。
12. **Skip Manage VLAN**（VLAN の管理を省略）を選択して、**Next**（次へ）をクリックします。
13. **Commit changes to system**（変更をシステムにコミット）を選択して、**Finish**（終了）をクリックします。
14. ネットワーク接続が中断されたことを警告されたら **Yes**（はい）をクリックします。

メモ: チームの構築には約 5 分かかる場合があります。

Hyper-V 仮想スイッチの設定

仮想スタンバイマシンが実稼働環境内で通信するには、仮想スイッチを作成してください。外部仮想スイッチを作成するには、**www.technet.microsoft.com** で「*仮想ネットワークの設定*」の項を参照してください。

5

困ったときは

マニュアルおよびソフトウェアのアップデートの入手方法

Rapid Recovery Core コンソールには、Rapid Recovery、アプライアンスのマニュアル、およびソフトウェアアップデートへの直接リンクがあります。リンクにアクセスするには、**Appliance**（アプライアンス）タブをクリックしてから **Overall Status**（全体ステータス）をクリックします。ソフトウェアアップデートおよびマニュアルへのリンクは **Documentation**（マニュアル）セクションの下にあります。

ソフトウェアアップデートの入手方法

Rapid Recovery Core Console から、Rapid Recovery および DL4300 アプライアンスのソフトウェアアップデートへの直接リンクを利用できます。ソフトウェアアップデートへのリンクにアクセスするには、**Appliance**（アプライアンス）タブを選択し、**Overall Status**（全体ステータス）をクリックします。ソフトウェアアップデートへのリンクが **Documentation**（マニュアル）セクションの下に表示されます。

デルへのお問い合わせ

メモ: お使いのコンピュータがインターネットに接続されていない場合は、購入時の納品書、出荷伝票、請求書、またはデルの製品カタログで連絡先をご確認ください。

デルでは、オンラインおよび電話ベースのサポートとサービスオプションをいくつかご用意しています。アクティブなインターネット接続がない場合は、 ご購入時の納品書、出荷伝票、請求書、またはデル製品カタログで連絡先をご確認いただけます。これらのサービスは国および製品によって異なり、お住まいの地域では一部のサービスがご利用いただけない場合があります。販売、テクニカルサポート、またはカスタマーサービスの問題に関するデルへのお問い合わせは、**software.dell.com/support** にアクセスしてください。

マニュアルのフィードバック

デルのマニュアルページのいずれかで **Feedback**（フィードバック）リンクをクリックして、フォームに入力し、**Submit**（送信）をクリックしてフィードバックを送信します。