

Dell DL1000 アプリアンス 導入ガイド

メモ、注意、警告

① **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。

1 Dell DL1000 の紹介	5
Dell DL1000 Core テクノロジ.....	5
ライブリカバリ.....	5
ユニバーサルリカバリ.....	5
True Global Deduplication	6
暗号化.....	6
Dell DL1000 のデータ保護機能.....	6
Dell DL1000 Core.....	6
Dell DL1000 Smart Agent.....	7
スナップショットプロセス.....	7
レプリケーション - 災害復旧サイトまたはサービスプロバイダ	7
リカバリ.....	8
Recovery-as-a-Service	8
仮想化とクラウド.....	8
Dell DL1000 導入アーキテクチャ.....	9
その他の情報.....	10
2 Dell DL1000 のインストール	12
はじめに.....	12
利用可能な構成.....	12
インストールの概要.....	12
インストールの必要条件.....	13
ネットワーク要件.....	13
推奨ネットワークインフラストラクチャ.....	13
ハードウェアのセットアップ.....	13
ラックへの DL1000 アプライアンスの取り付け.....	14
ラックなしでのシステムの使用.....	14
アプライアンスの配線.....	14
ケーブル処理アームの接続 (オプション)	15
DL1000 アプライアンスへの電源投入.....	15
ソフトウェアの初回セットアップ.....	15
AppAssure アプライアンスの設定ウィザード.....	15
DL アプライアンスの設定ウィザード.....	18
Rapid Appliance Self Recovery.....	23
RASR USB キーの作成.....	23
RASR の実行.....	24
Recovery and Update Utility.....	25
3 Dell DL1000 の設定	26
設定概要.....	26
オペレーティングシステムのデフォルト設定へのリセット.....	26

DL1000 Core Console にリモートでアクセスするためのブラウザの設定.....	26
Internet Explorer と Chrome でのブラウザ設定.....	27
Firefox でのブラウザ設定.....	27
DL1000 Core Console へのアクセス.....	27
Internet Explorer での信頼済みサイトのアップデート.....	28
エージェントスナップショットデータの暗号化.....	28
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	28
ストリーム数の調整.....	29
4 サーバを保護する準備.....	31
概要.....	31
クライアントでのエージェントのインストール.....	31
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.....	31
Windows マシンでの Rapid Recovery Agent ソフトウェアのインストール.....	32
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.....	34
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.....	36
Linux Agent ファイルの場所.....	38
エージェントの依存関係.....	39
Debian または Ubuntu での Rapid Recovery Agent ソフトウェアのインストール.....	39
Suse Linux Enterprise Server での Rapid Recovery Agent ソフトウェアのインストール.....	40
Red Hat Enterprise Linux と CentOS でのエージェントのインストール.....	41
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.....	41
Windows Server Core Edition マシンでの Agent ソフトウェアのインストール.....	42
Linux マシンでの Rapid Recovery Agent の設定.....	43
マシンの保護.....	44
ネットワーク接続性のチェック	47
ファイアウォール設定のチェック	47
DNS 解決のチェック	47
ネットワークアダプタのチームミング.....	48
5 困ったときは.....	50
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.....	50
マニュアル.....	50
ソフトウェアアップデート.....	50
デルへのお問い合わせ.....	50
マニュアルのフィードバック	50

Dell DL1000 の紹介

Dell DL1000 はバックアップとレプリケーションを一つのデータ保護製品に統合し、バックアップからの信頼性のあるアプリケーションデータリカバリを実現することによって、仮想マシンおよび物理マシンを保護します。お使いのアプリケーションは、ビルトイングローバル重複排除、圧縮、暗号化、および特定のプライベートまたはパブリッククラウドインフラストラクチャへのレプリケーションにより、テラバイトにおよぶデータを処理することが可能です。サーバーアプリケーションおよびデータは、データ保持およびコンプライアンス目的のために、数分で復旧させることができます。

お使いの DL1000 は、VMware vSphere、Oracle VirtualBox、および Microsoft Hyper-V のプライベートクラウドまたはパブリッククラウド上でのマルチハイパーバイザー環境をサポートします。

トピック：

- ・ Dell DL1000 Core テクノロジ
- ・ Dell DL1000 のデータ保護機能
- ・ Dell DL1000 導入アーキテクチャ
- ・ その他の情報

Dell DL1000 Core テクノロジ

アプリケーションには、次のテクノロジーが組み合わされています。

- ・ ライブリカバリ
- ・ ユニバーサルリカバリ
- ・ True Global Deduplication
- ・ 暗号化

ライブリカバリ

ライブリカバリ は、VM またはサーバーのための即時リカバリテクノロジーです。このテクノロジーは、中断がほとんどない仮想サーバーまたは物理サーバー上のデータボリュームへのアクセスを実現します。

DL1000 のバックアップとレプリケーションのテクノロジーは、複数の VM またはサーバーの同時スナップショットを記録し、ほぼ瞬時のデータおよびシステム保護を提供します。リカバリポイントをマウントすることによって、実稼動ストレージへの完全復元が完了するのを待つことなくサーバーの使用を再開できます。

ユニバーサルリカバリ

ユニバーサルリカバリ は、無制限のマシン復元の柔軟性を提供します。物理システムから仮想マシン、仮想マシンから仮想マシン、仮想マシンから物理システム、または物理システムから物理システムへの復元に加え、種類の異なるハードウェアへのベアメタル復元を実行することもできます。

ユニバーサルリカバリ テクノロジーは、VMware から Hyper-V へ、Hyper-V から VMware へといった仮想マシン間でのクロスプラットフォームの移行の高速化も実現します。これは、アプリケーションレベル、アイテムレベル、およびオブジェクトレベルリカバ

リ（個別のファイル、フォルダ、電子メール、カレンダーアイテム、データベース、およびアプリケーション）を取り入れています。

True Global Deduplication

True Global Deduplication は、マシンのブロックレベルの増分バックアップを行うことによって、冗長または重複データを排除します。

サーバーの標準的なディスクレイアウトは、オペレーティングシステム、アプリケーション、およびデータで構成されます。多くの環境で、管理者は、展開と管理を効果的に行うために複数のシステム全体で共通バージョンのサーバーおよびデスクトップオペレーティングシステムを使用することがほとんどです。バックアップが複数のマシンにわたってブロックレベルで同時に実行される場合、バックアップに含まれているものと含まれていないものをソースに関係なく詳細に確認できます。このデータには、環境全体のオペレーティングシステム、アプリケーション、およびアプリケーションデータが含まれます。



図 1. True Global Deduplication の図解

暗号化

DL1000 は、バックアップおよび保存データを不正なアクセスや利用から保護するための内蔵の暗号化を提供することにより、データの機密性を確保します。データには、暗号化キーを使用することによってアクセスし、複合することが可能です。暗号化は、スナップショットデータに対してインラインで行われ、パフォーマンスを損なうことなく回線速度で実行されます。

Dell DL1000 のデータ保護機能

Dell DL1000 Core

Core は、DL1000 導入アーキテクチャの中心的なコンポーネントです。Core は、マシンバックアップを保存および管理し、バックアップ、リカバリ、保持、レプリケーション、アーカイブ、および管理のためのサービスを提供します。Core は、64 ビット版の Microsoft Windows Server 2012 R2 Foundation および Standard オペレーティングシステムを実行する自立ネットワークのアドレス指定可能なコンピュータです。このアプライアンスは、エージェントから受信したデータに対して、ターゲットベースのインライン圧縮、暗号化、およびデータ重複排除を実行します。その後、Core がスナップショットバックアップをアプライアンスに常駐するリポジトリに保存します。Core はレプリケーション用にペアリングされます。

リポジトリは、Core 内の内部ストレージにも常駐します。Core は、JavaScript が有効化されたウェブブラウザから <https://CORENAME:8006/apprecovery/admin> にアクセスすることによって管理されます。

Dell DL1000 Smart Agent

Smart Agent は、Core で保護されているマシンにインストールされています。Smart Agent はディスクボリューム上の変更されたブロックを追跡し、事前定義された保護間隔で、変更されたブロックのイメージのスナップショットを取得します。ブロックレベルの増分スナップショットの永続的アプローチにより、保護対象マシンから Core に同じデータが繰り返しコピーされないようにします。

Agent の設定完了後、Agent は高性能テクノロジーを使用して保護対象ディスクボリューム上の変更されたブロックを追跡します。スナップショットの準備が整うと、そのスナップショットはインテリジェントマルチスレッドのソケットベース接続を使用して Core へ迅速に転送されます。

スナップショットプロセス

DL1000 保護プロセスは、ベースイメージが保護対象マシンから Core に転送された時点で開始されます。このフェーズでは通常稼働するネットワーク経由でマシンの完全なコピーが転送され、それ以降は、永続的に増分スナップショットが転送されます。

DL1000 Agent for Windows は、Microsoft Volume Shadow Copy Service (VSS) を使用してディスクにアプリケーションデータをフリーズおよび静止させ、ファイルシステムおよびアプリケーションと整合性のあるバックアップを取得します。スナップショットが作成されると、ターゲットサーバーのライターである VSS がコンテンツのディスクへの書き込みを防止します。ディスクへのコンテンツの書き込みを中止するプロセス中、すべてのディスク I/O 操作がキューに入り、再開はスナップショットが完成してからのみとなりますが、すでに実行中の操作は完了され、開いているファイルはすべて閉じられます。シャドウコピーを作成するプロセスは、実稼働システムのパフォーマンスに大きな影響を与えることはありません。

Microsoft VSS には、スナップショット前にデータをディスクへフラッシュするための NTFS、レジストリ、Active Directory といった Windows 内部テクノロジーすべてに対するビルドインサポートが装備されているため、DL1000 は Microsoft VSS を使用します。さらに、その他のエンタープライズアプリケーション (Microsoft Exchange や SQL など) も、スナップショットが準備されているとき、および使用済みデータベースページをディスクにフラッシュしてデータベースを整合性のあるトランザクション状態にする必要があるときに、通知を受け取るために、VSS Writer プラグインを使用します。取得されたデータは、迅速に Core に転送され、保存されます。

レプリケーション - 災害復旧サイトまたはサービスプロバイダ

レプリケーションは、災害復旧のために Rapid Recovery コアからリカバリポイントをコピーし、異なる場所にある別の Rapid Recovery コアに送信するプロセスです。このプロセスでは、2 つ以上のコア間でソースとターゲットのペアの関係が必要です。

ソースコアは、選択された保護対象マシンのリカバリポイントをコピーし、増分スナップショットデータをリモート災害復旧サイトにあるターゲットコアに非同期かつ継続的に送信します。会社が所有するデータセンターやリモート災害リカバリサイト (つまり、「自己管理」ターゲットコア) に対するアウトバウンドレプリケーションを設定できます。さらに、第三者のマネージドサービスプロバイダ (MSP) またはオフサイトバックアップと災害復旧サービスをホストするクラウドプロバイダに対するアウトバウンドレプリケーションも設定できます。サードパーティターゲットコアに複製するときは、接続を要求し、自動のフィードバック通知を受け取ることを可能にするビルトインワークフローを使用できます。

レプリケーションは、保護対象マシンごとに管理されます。ソースコアで保護または複製された任意のマシン (またはすべてのマシン) は、ターゲットコアに複製するよう設定できます。

レプリケーションは、重複排除と密接に関連する固有の Read-Match-Write (RMW) アルゴリズムによって自己最適化されます。RMW レプリケーションでは、ソースおよびターゲットのレプリケーションサービスがデータを送信する前にキーの一致を確認し

ます。その後、圧縮化、暗号化、および重複排除されたデータのみを WAN を介してレプリケーションするため、帯域幅要件は 1/10 に削減されます。

複製では、シーディング（保護対象マシンの重複排除されたベースイメージと増分スナップショットの最初の転送）によって開始されますが、これは、数千ギガバイトにおよぶデータになり得ます。最初の複製は、外部メディアを使用してターゲットコアにシーディングすることができます。これは通常、大規模のデータやサイト間のリンクが低速の場合に役立ちます。シーディングアーカイブ内のデータは、圧縮化、暗号化、および重複排除されます。アーカイブの合計サイズがリムーバブルメディアで使用可能な容量よりも大きい場合は、メディアで使用可能なスペースに基づいてアーカイブを複数のデバイスに分けることができます。シーディングプロセス中、増分リカバリポイントがターゲットサイトに複製されます。ターゲットコアがシーディングアーカイブを取り入れた後、新たに複製された増分リカバリポイントは自動的に同期されます。

リカバリ

リカバリは、ローカルサイトまたは複製されたリモートサイトで実行できます。導入がローカル保護およびオプションのレプリケーションで安定した状態になると、DL1000 Core では、Verified Recovery、ユニバーサルリカバリ、またはライブリカバリを使用したりカバリの実行が可能になります。

Recovery-as-a-Service

マネージドサービスプロバイダ（MSP）は、Recovery as a Service（RaaS）を提供するためのプラットフォームとして、DL1000 をフルに活用できます。RaaS は、顧客の物理サーバおよび仮想サーバを複製することによって、クラウド内での完全なリカバリを容易にします。サービスプロバイダのクラウドは、リカバリテストまたは実際のリカバリ操作をサポートする仮想マシンとして使用されます。クラウド内リカバリの実行を希望するカスタマは、ローカルコアの保護対象マシンで Rapid Recovery サービスプロバイダへのレプリケーションを設定することができます。災害発生時には、MSP がカスタマのために即座に仮想マシンをスピンアップすることができます。

DL1000 はマルチテナント型ではありません。MSP は DL1000 を複数のサイトで使用して、そのサイト側でマルチテナント環境を構築することができます。

仮想化とクラウド

DL1000 Core はクラウド対応で、クラウドのコンピューティング能力をリカバリおよびアーカイブ作業に活用することを可能にします。

DL1000 は、任意の保護対象または複製対象マシンをライセンスバージョンの VMware または Hyper-V にエクスポートできます。連続エクスポートでは、スナップショットが実行されるたびに仮想マシンが増分アップデートされます。増分アップデートは高速で実行され、ボタンをクリックするだけで電源投入できる準備が整ったスタンバイクローンを提供します。サポートされている仮想マシンエクスポートは次のとおりです。

- ・ フォルダ上の VMware Workstation または Server
- ・ Vsphere または VMware ESXi ホストへの直接エクスポート
- ・ Oracle VirtualBox へのエクスポート
- ・ Windows Server 2008 (x64) 上の Microsoft Hyper-V サーバー
- ・ Windows Server 2008 R2 上の Microsoft Hyper-V サーバー
- ・ Windows Server 2012 R2 上の Microsoft Hyper-V サーバー

Microsoft Azure、Amazon S3、Rackspace Cloud Block Storage、またはその他の OpenStack ベースのクラウドサービスのプラットフォームを使用して、リポジトリデータをアーカイブすることができるようになりました。

Dell DL1000 導入アーキテクチャ

DL1000 導入アーキテクチャは、ローカルおよびリモートのコンポーネントで構成されます。オフサイトリカバリ用に災害復旧サイトやマネージドサービスプロバイダを利用する必要のない環境では、リモートコンポーネントはオプションです。基本的なローカル導入は、Core と呼ばれるバックアップサーバーと、エージェントと呼ばれる 1 台、または複数台の保護対象マシンで構成されます。オフサイトコンポーネントは、災害リカバリサイトにおける完全なリカバリ機能を提供するレプリケーションを使用して有効化されます。DL1000 Core は、ベースイメージと増分スナップショットを使用して、保護対象エージェントのリカバリポイントを収集します。

また、Microsoft Exchange と SQL の存在をそれぞれのデータベースとログファイルとともに検出できるため、DL1000 はアプリケーションウェアです。バックアップは、アプリケーションウェアなブロックレベルのスナップショットを使用して実行されます。DL1000 は、保護対象 Microsoft Exchange サーバーのログの切り捨ても実行します。

次の図は、シンプルな DL1000 の導入を示しています。DL1000 Agent は、ファイルサーバー、電子メールサーバー、データベースサーバー、または仮想マシンなどのマシン上にインストールされ、これらのマシンは、中央リポジトリを備えた単一の DL1000 Core に接続され、保護されています。デルソフトウェアライセンスポータルは、環境内にある Agent と Core に対するライセンスサブスクリプション、グループ、およびユーザーを管理します。ライセンスポータルでは、ユーザーが環境のライセンスに応じてログイン、アカウントのアクティブ化、ソフトウェアのダウンロード、および Agent と Core の導入を行うことができます。

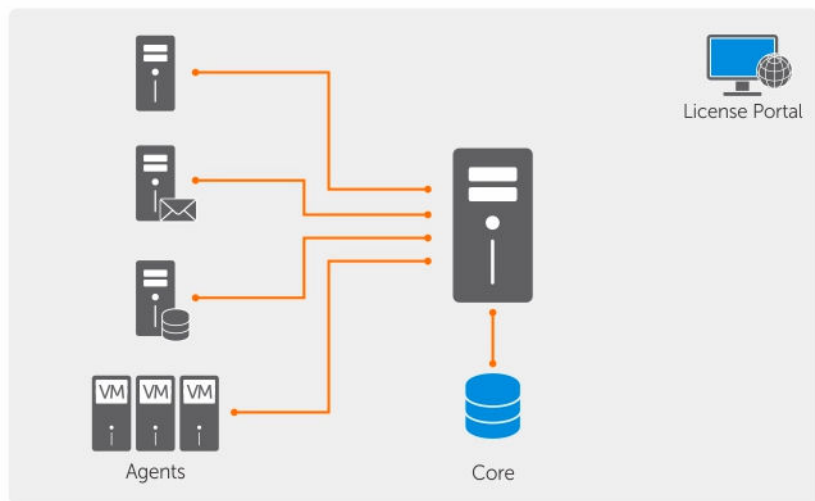


図 2. Dell DL1000 導入アーキテクチャ

次のダイアグラムに示されているように、複数の DL1000 Core を導入することもできます。中央のコンソールが複数の Core を管理します。

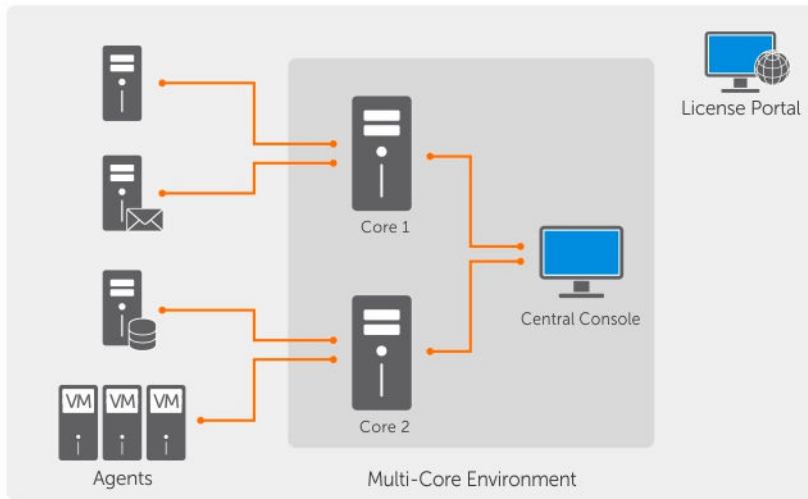


図 3. Dell DL1000 Multi—Core 導入アーキテクチャ

その他の情報

- ① **メモ:** Dell OpenManage マニュアルは、Dell.com/openmanagemanuals にアクセスしてください。
- ① **メモ:** アップデートには他の文書の内容を差し替える情報が含まれている場合がよくあることから、Dell.com/support/home でアップデートがないかどうかを常に確認し、最初にお読みください。
- ① **メモ:** Dell OpenManage Server Administrator に関するマニュアルは、Dell.com/openmanage/manuals を参照してください。

製品のマニュアルには次が含まれます。

- 『Getting Started Guide』 (はじめに) システムのセットアップ、および技術仕様の概要を提供します。このマニュアルはシステムに同梱されています。
- 『System Placemat』 (システムプレースマット) お使いのアプライアンスにおけるハードウェアのセットアップ、およびソフトウェアのインストール方法についての情報を提供します。
- 『Owner's Manual』 (オーナーズマニュアル) システムの機能、システムのトラブルシューティング方法、およびシステムコンポーネントの取り付けまたは交換方法について説明しています。
- 『Deployment Guide』 (導入ガイド) アプライアンスのハードウェア導入、および初期導入についての情報を提供します。
- 『User's Guide』 (ユーザーズガイド) システムの設定および管理についての情報を提供します。
- 『Release Notes』 (リリースノート) Dell DL1000 アプライアンスに関する製品情報と追加情報を提供します。
- 『Interoperability Guide』 (相互運用ガイド) お使いのアプライアンス対応のソフトウェアおよびハードウェアについての情報の他、使用時の考慮事項、推奨事項、および規則についての情報を提供します。
- 『OpenManage Server Administrator User's Guide』 (OpenManage Server Administrator) お使いのシステムを管理するための Dell OpenManage Server Administrator の使用についての情報を提供します。

Server Administrator
ユーザーズガイド)

Dell DL1000 のインストール

はじめに

DL Backup to Disk Appliance では次が可能になります。

- ・ 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。

利用可能な構成

DL アプライアンスには、次の構成のものがあります。

表 1. 利用可能な構成

容量	ハードウェア設定
1 TB、VM なし	200 GB のオペレーティングシステム / ソフトウェアパーティションおよび 1 TB の使用可能なリポジトリ容量を持つ 2 TB ドライブ
2 TB、VM なし	200 GB のオペレーティングシステム / ソフトウェアパーティションおよび 2 TB の使用可能なリポジトリ容量を持つ 3 TB ドライブ
3 TB、VM なし	200 GB のオペレーティングシステム / ソフトウェアパーティションおよび 3 TB の使用可能なリポジトリ容量を持つ 4 TB ドライブ
3 TB、VM 2 個	200 GB のオペレーティングシステム / ソフトウェアパーティション、VM ストレージ用の 300 GB パーティション、および 3 TB の使用可能なリポジトリ容量を持つ 4 TB ドライブ。

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 DL1000 システム
- ・ Dell PowerEdge RAID コントローラ (PERC)
- ・ Dell AppAssure ソフトウェア

インストールの概要

DL1000 のインストールには、保護対象のシステムでの Rapid Recovery Core と Rapid Recovery エージェントサービスのインストールが含まれます。追加のコアがセットアップされている場合は、Rapid Recovery Central Management Console サービスをインストールする必要があります。

DL1000 をインストールするには、次の手順を実行します。

- 1 永久ライセンスキーを取得します。Core Console から、DL1000 ライセンスの直接管理、ライセンスキーの変更、ライセンスサーバーとの通信を行うことができます。また、Core Console の Licensing (ライセンス) ページから Dell Rapid Recovery ライセンスポータルにアクセスすることもできます。

① | **メモ:** アプライアンスには **30 日間有効な一時的なソフトウェアライセンスが設定された状態で出荷されています。**

- 2 インストールの前提条件を確認します。
- 3 ハードウェアをセットアップします。
- 4 初期ソフトウェアをセットアップします (DL Appliance Configuration Wizard (AppAssure アプライアンス設定ウィザード))。
- 5 Core 管理コンソールをインストールします。

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

10 年前の標準バックボーンインフラストラクチャが備えていた速度は、100 メガバイト / 秒でした。ネットワークトラフィックおよび入出力に対する要求は着実に、かつ大幅に拡大しています。これを受け要求に応えるためにネットワークバックボーンの標準は高まっています。今日のネットワークバックボーンでは、ギガビットイーサネット (GbE) などの速度をサポートしています。この場合、毎秒 1 ギガビットまたはその 10 倍の速度である 10 GbE でイーサネットフレームが転送されます。

Rapid Recovery を実行するには、最低でも 1 GbE のネットワークインフラストラクチャが必要です。堅牢な環境が求められる場合は 10 GbE のネットワークを使用することをお勧めします。また、大容量 (5TB 以上) のサーバーを保護する場合は、10 GbE ネットワークをお勧めします。

Core マシンで、NIC チーミング (複数の物理 NIC を単一の論理 NIC にグループ化する機能) をサポートする複数のネットワークインタフェースカード (NIC) が使用可能です。ネットワークのスイッチで NIC チーミングが許可されている場合は、Core で NIC チーミングを使用すると、さらにパフォーマンスを向上させることができます。このような場合、可能であれば、保護対象マシンで NIC チーミングをサポートする予備のネットワークカードをチーミングすることにより、全体的なパフォーマンスも向上できます。

Core で iSCSI または Network Attached Storage (NAS) を使用する場合、Dell では、ストレージとネットワークトラフィック向けに個別の NIC カードを使用することをお勧めします。

想定帯域幅での通信を実現するには、適切な規格のネットワークケーブルを使用してください。お使いのネットワークのパフォーマンスを定期的にテストし、それに応じてお使いのハードウェアを調整することをお勧めします。

これらの提案は、Rapid Recovery の提供するバックアップ、レプリケーション、およびリカバリの各機能だけではなく、事業運営をサポートするためのすべての要求に対応したネットワークインフラストラクチャが必要とする、標準的なネットワーク要件に基づいています。

ハードウェアのセットアップ

アプライアンスは、1 台の DL1000 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お使いのシステム用の『Getting Started Guide』(はじめに) を参照してください。開梱し、DL1000 アプライアンスハードウェアをセットアップします。

① **メモ:** ソフトウェアはアプライアンスに事前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。

DL1000 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 DL1000 システムをラックに取り付けて、ケーブル接続します。
- 2 DL1000 システムの電源を入れます。

ラックへの DL1000 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ている場合は、ラックキットに同梱の『Rack Installation Instructions』（ラック取り付け手順書）を取り出します。ラックにレールと DL1000 を取り付ける手順に従います。

ラックなしでのシステムの使用

システムはサーバーラックなしで使用することができます。ラックなしでシステムを使用しているときは、次のガイドラインに従うようにしてください。

- ・ システムは、システム全体をサポートするしっかりと安定した面に設置する必要があります。

① **メモ:** システムを縦に設置しないようにする必要があります。

- ・ システムは床に設置しないでください。
- ・ システムの上に物を置かないでください。重さで上部パネルが歪み、システムが損傷する恐れがあります。
- ・ 適切な換気のため、システム周辺に十分な空間を確保してください。
- ・ Dell.com/support/home にある『Dell DL1000Appliance Getting Started Guide』（Dell DL1300 アプライアンス - はじめに）の「技術仕様 - 環境」の項に記載されている、推奨温度状態でシステムを取り付けるようにしてください。

△ **注意:** これらのガイドラインに従わない場合、システムの損傷、またはケガの原因となる可能性があります。

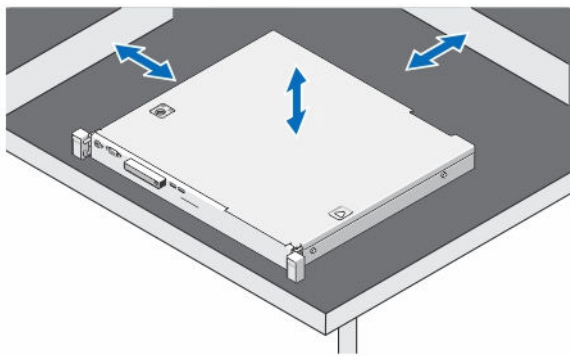


図 4. ラックなしでのシステムの使用

アプライアンスの配線

アプライアンスに同梱されている『Dell DL1000Appliance Getting Started Guide』（Dell DL1300 アプライアンス - はじめに）を取り出し、指示に従って、DL1000 システムにキーボード、マウス、モニター、電源、およびネットワークケーブルを取り付けます。

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。

DL1000 アプライアンスへの電源投入

アプライアンスの配線が終了したら、システムの電源を入れます。

- ① **メモ:** 信頼性と可用性を最大限まで高めるには、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。詳細については、Dell.com/support/manuals で『*Dell DL1000 Getting Started Guide*』（Dell DL1000 - スタートガイド）を参照してください。

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すると **AppAssure Appliance Configuration Wizard**（AppAssure アプライアンス設定ウィザード）が自動的に開始されます。

- 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ページが表示されます。
- 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。
パスワードを入力すると、**Press Ctrl+Alt+Delete to Sign in**（Ctrl+Alt+Del を押してサインイン）画面が表示されます。
- 6 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 Appliance（アプライアンスの言語の選択）画面が表示されます。
- 7 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。
EULA 画面が表示されます。
- 8 EULA に同意するには、**Accept EULA**（EULA に同意する）ボタンをクリックします。

- ① **メモ:** AppAssure Appliance Configuration Wizard（AppAssure および DL アプライアンス設定ウィザード）は、EULA に同意しなければこれ以上実行できません。同意しない場合は、アプライアンスがユーザーをだたちにログオフさせます。

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。

- ① **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。

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を実行したり設定を変更する前に、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てください。ウィザードが完了するまでは、**Control Panel**（コントロールパネル）上での変更、**Microsoft Windows Update** の使用、AppAssure 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せん。AppAssure 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。

AppAssure アプライアンスの設定ウィザードは、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](#)
- ・ [ストレージのプロビジョニング](#)

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。

① **メモ: AppAssure Appliance Configuration Wizard (AppAssure 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。
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 **Next** (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。
 - ・ **優先 DNS サーバー**
 - ・ **代替 DNS サーバー**
- 8 **Next** (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 チーミングの詳細については、「[ネットワークアダプタのチーミング](#)」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。

① **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 Wizard (AppAssure アプライアンス設定ウィザード) 完了後のホスト名の変更には、いくつかの手順が必要です。

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) ページの **New host name** (新しいホスト名) テキストボックス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接続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。

① **メモ:** お使いの DL1000 に Microsoft Windows Server 2012 Foundation エディションがインストールされている場合は、ドメインに参加するためのオプションは無効になります。

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接続したい場合は、次の詳細を入力します。

- ・ ドメイン名
- ・ ドメインユーザー名

① **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 **Next** (次へ) をクリックします。

① **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。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接続している場合は、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。

① **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 **Next** (次へ) をクリックします。
Thank You (ありがとうございました) ページが表示されます。
- 7 設定を完了するには、**Next** (次へ) をクリックします。
- 8 **Configuration Complete** (設定完了) ページで **Next** (次へ) をクリックします。
Core Console が、デフォルトのウェブブラウザで開きます。

ストレージのプロビジョニング

利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して、新しい AppAssure リポジトリを作成するには、次の手順を実行します。

- 1 **Provisioning** (プロビジョニング) ページで **Next** (次へ) をクリックします。
Provisioning (プロビジョニング) ページに、プロビジョニング用に使用可能な容量が表示されます。この容量は、新しい AppAssure リポジトリの作成に使用されます。
① | メモ: DL1000 3 TB (VM 2 つ) 構成のシステムでは、ディスク容量をスタンバイ VM に割り当てることができます。
お使いのシステムのディスクプロビジョニングが完了し、新しいリポジトリが作成されます。
- 2 **Next** (次へ) をクリックします。
Configuration Complete (設定完了) ページが表示されたら、**Exit** (終了) をクリックします。

DL アプライアンスの設定ウィザード

- ① | 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せん。**
- △ | 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ーフェースの設定
- ・ 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

- ① | 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ックスの長さ
 - ・ **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、「**ネットワークアダプタのチーミング**」を参照してください。
- 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。

① **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。

① **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。

① **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 Appliances 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 Appliances 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 Appliances 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 ① **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。

Appliances 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

① **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。

Appliances 設定のバックアップオプションで Appliances 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 Appliances 設定のリカバリに役立ちます。

- 1 **Appliances 設定のバックアップオプション** で、**Appliances 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 Appliances 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。

① **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：DL1000 1TB アプライアンスでは、1TB 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ルールから削除されます。

① **メモ:** 保持ポリシーのライセンス制限がデフォルトの場合は、保持期間を 3 ヶ月以上にするように保持ポリシーを設定することはできません。これを実行しようとすると、エラーメッセージが表示されます。

- 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 2. 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。

テキストボックス

説明

...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。

Rapid Appliance Self Recovery

Rapid Appliance Self Recovery (RASR) は、オペレーティングシステムドライブが工場出荷時のデフォルトイメージに再構築されるベアメタルの復元プロセスです。

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。
 - ① **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要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
 - ① **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

① **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。

① **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。

① **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。

① **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 ① **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。

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。

① | 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。

① | 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。

Dell DL1000 の設定

設定概要

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。

設定には、DL1000 Core Console にリモートでアクセスするためのブラウザの設定、ライセンスの管理、アラートと通知のセットアップなどのタスクが含まれます。Core の設定が完了すると、エージェントを保護し、リカバリを実行することができるようになります。

- ① **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 Data Protection | Rapid Recovery** ライセンスポータルにログインします。ライセンスキーの変更方法の詳細については、dell.com/support/home で『*Rapid Recovery 6.0 on DL Appliances ユーザーズガイド*』の「ライセンスのアップデートまたは変更」のトピックを参照してください。
- ① **メモ:** DL1000 Backup To Disk アプライアンスを使用しているときは、Core の設定に **Appliance** (アプライアンス) タブを使用することをお勧めします。

オペレーティングシステムのデフォルト設定へのリセット

オペレーティングシステムをデフォルト設定にリセットするには、次の手順を実行します。

- 1 管理者としてログインし、コマンドプロンプトを開きます。
- 2 `c:\windows\system32\sysprep` に移動して、コマンド `sysprep.exe/generalize/oobe/reboot` を実行します。
- 3 次を選択します。
 - ・ 言語として **English**
 - ・ 国/地域として **米国**
 - ・ キーボードレイアウトとして **US**

DL1000 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 に正常にアクセスするには、お使いのブラウザの設定を変更する必要があります。次の手順は、Internet Explorer、Google Chrome、および Mozilla Firefox のブラウザ設定の変更方法の詳細を示しています。

- ① **メモ:** ブラウザ設定を変更するには、管理者権限でマシンにログオンする必要があります。
- ① **メモ:** **Chrome** では **Internet Explorer** の設定が使用されるため、**Internet Explorer** を使用して **Chrome** の変更を行う必要があります。
- ① **メモ:** **Core Web Console** へローカルまたはリモートからアクセスする際に、**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、サーバーマネージャ > ローカルサーバー > **Internet Explorer** セキュリティ強化の構成を開いてオプションを表示し、これを **オン** にします。

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。

DL1000 Core Console へのアクセス

トピック「Internet Explorer での信頼済みサイトのアップデート」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、トピック「DL1000 Core Console にリモートでアクセスするためのブラウザの設定」で説明されているとおりにお使いのブラウザを設定してください。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。

- ・ Core サーバーにローカルでログインして、**Core Console** アイコンをダブルクリック。
- ・ 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。

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。DL1000 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 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
-------	----

Name (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 (パスワード)	パスワードを入力します。アクセスを制御するために使用されます。
---------------------------	---------------------------------

Confirm Passphrase (パスワードの確認)	パスワードを再入力します。パスワードの入力を確認するために使用されます。
--------------------------------------	--------------------------------------

- ① **メモ:** パスワードを失うとデータがアクセス不能になることから、暗号化パスワードを記録しておくことをお勧めします。詳細については、『*Dell DL1000 Appliance User's Guide*』(Dell DL1300 アプライアンスユーザーズガイド)の「セキュリティの管理」の章を参照してください。

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電子メール通知を受け取るには、電子メールサーバーと電子メール通知テンプレートを設定します。

- ① **メモ:** また、電子メールアラートメッセージが送信される前に、**Notify by email**（電子メールで通知）オプションの有効化を含む、通知グループ設定を行う必要もあります。電子メールアラートを受け取るイベントの指定についての詳細は、[Dell.com/support/home](https://support.dell.com/home) で『*Dell DL1000 Appliance User's Guide*』（Dell DL1300 アプライアンスユーザーズガイド）の「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。

電子メールサーバーと電子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**（電子メール SMTP 設定）ペインで、**Change**（変更）をクリックします。
Email Notification Configuration（電子メール通知設定）ダイアログボックスが表示されます。
- 4 **Enable Email Notifications**（電子メール通知を有効にする）を選択し、次で説明されている電子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 Server** (SMTP サーバー) 電子メール通知テンプレートによって使用される電子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。
- Port** (ポート) ポート番号を入力します。この番号は電子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。
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。この数値は電子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。
- Username** (ユーザー名) 電子メールサーバーのユーザー名を入力します。
- Password** (パスワード) 電子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) 返信用電子メールアドレスを入力します。これは、電子メール通知テンプレート用の返信電子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** (電子メールの件名) 電子メールテンプレートの件名を入力します。これは、電子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** (電子メール) 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**（テスト電子メールの送信）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。

サーバを保護する準備

概要

DL 1000、1000 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。

トピック：

- ・ クライアントでのエージェントのインストール
- ・ 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
- ・ 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
- ・ マシンの保護

クライアントでのエージェントのインストール

DL 1000、1000 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。

① **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。

- 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くこそページをスキップする) オプションを選択します。
- 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。
- 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 3. 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。

- ①** **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。

- ①** **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。

- 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。
- 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。
- .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。
- 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。
- 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。

① **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ます。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](#)

① **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 お使いのアプリアンスで、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 アプリアンス上の **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 4. 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。

① **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 5. 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。

テキストボックス 説明

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

① | **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。

① | **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 6. 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。

① 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 7. 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 replotlist
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。

① 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。

① **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。

① **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。

① **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。

① **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。

- 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
```
- 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
```
- 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

- ① **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。

- root アクセス権でターミナルセッションを開きます。
- 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。

- ① **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。

- 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。

① **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。

① **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。

① **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 (lokitit 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く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 8. 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。

① **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に表示するには、**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認し、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。

① **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。

① **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 9. 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。 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 <クライアントの IP アドレス>** 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 DL1000 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。

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 DL1000 アプライアンスで、**スタート > 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 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、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、Core について同じことを確認します。

DNS 解決のチェック

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 DL1000 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、DL1000 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 のチーム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

Broadcom Advanced Configuration Suite の再インストール

Broadcom Advanced Configuration Suite を再インストールするには、次の手順を実行します。

- 1 C:\Install\BroadcomAdvanced に移動して **setup** (セットアップ) をダブルクリックします。
InstallShield ウィザードが表示されます。
- 2 **Next** (次へ) をクリックします。
- 3 **Modify** (変更)、**Add** (追加)、または **Remove** (削除) をクリックします。
Custom Setup (カスタムセットアップ) ウィンドウが表示されます。
- 4 **CIM Provider** (CIM プロバイダ) をクリックして、**This feature will be installed on local hard drive** (この機能をローカルハードドライブにインストールする) を選択します。
- 5 **BASP** をクリックして、**This feature will be installed on local hard drive** (この機能をローカルハードドライブにインストールする) を選択します。
- 6 **Next** (次へ) をクリックします。
- 7 **Install** (インストール) をクリックします。
- 8 **Finish** (終了) をクリックします。

NIC チームの作成

① **メモ:** Windows 2012 Server のネイティブチームングインタフェースは使用しないことをお勧めします。チーム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 チーム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。
① **メモ:** Broadcom Advanced Control Suite を使用するときには、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、DL1000 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 チームングウィザード) ウィンドウが表示されます。
- 4 **Next** (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。

① | **メモ:** NIC チームの構築には最大約 5 分かかります。

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

Core Console から、Rapid Recovery および DL1000 アプライアンスのマニュアルと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。

マニュアル

マニュアルのリンクにアクセスするには、次の手順を実行します。

- 1 Core Console で、**Appliance** (アプライアンス) タブをクリックします。
- 2 左ペインから、**Appliance** (アプライアンス) > **Documentation** (マニュアル) リンクに移動します。

ソフトウェアアップデート

ソフトウェアアップデートのリンクにアクセスするには、次の手順を実行します。

- 1 Core Console で、**Appliance** (アプライアンス) タブをクリックします。
- 2 左ペインから、**Appliance** (アプライアンス) > **Software Updates** (ソフトウェアアップデート) リンクに移動します。

デルへのお問い合わせ

① **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。