Dell DL1000 アプライアンス
ユーザーズガイド

メモ、注意、警告

メモ: メモでは、コンピュータ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: 注意では、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: 警告では、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。

2015 - 12

Rev. A01

目次

1

お使いの Dell DL1000 について

Dell DL1000 はバックアップとレプリケーションを一つの統一されたデータ保護製品に組み合わせたもので、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。お使いのアプライアンスは、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（DR）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。

DL1000 は、VMware vSphere 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環境をサポートします。

Dell DL1000 コアテクノロジ

アプライアンスには、次のテクノロジが組み合わされています。

- Live Recovery
- Universal Recovery
- True Global Deduplication
- 暗号化

Live Recovery

Live Recovery は、VM またはサーバーのための即時リカバリテクノロジです。このテクノロジは、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。

Universal Recovery

Universal Recovery 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。

Universal Recovery テクノロジは、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パフォーマンスを損なうことなく回線速度でインライン実行されます。

Dell DL1000 のデータ保護機能

Dell DL1000 Core

Core は、DL1000 展開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、複製、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、内蔵型のネットワーク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動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、実稼動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の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 AppAssure Core 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 AppAssure Core 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的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レプリケーとされたリモートサイトで実行できます。展開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、Universal Recovery、または Live Recovery を使用したリ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 Server（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、顧客の物理サーバーおよび仮想サーバー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 AppAssure 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 展開アーキテクチャ

DL1000 展開アーキテクチャは、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。基本的なローカル展開は、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。ADL1000 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 DL1000 は、アプリケーションアウェアです。バックアップは、アプリケーションア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 の展開を示しています。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、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、ライセンスサブスクリプション、および環境内のエージェントとコアに対するグループと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、およびエージェントとコアの展開を行うことができます。

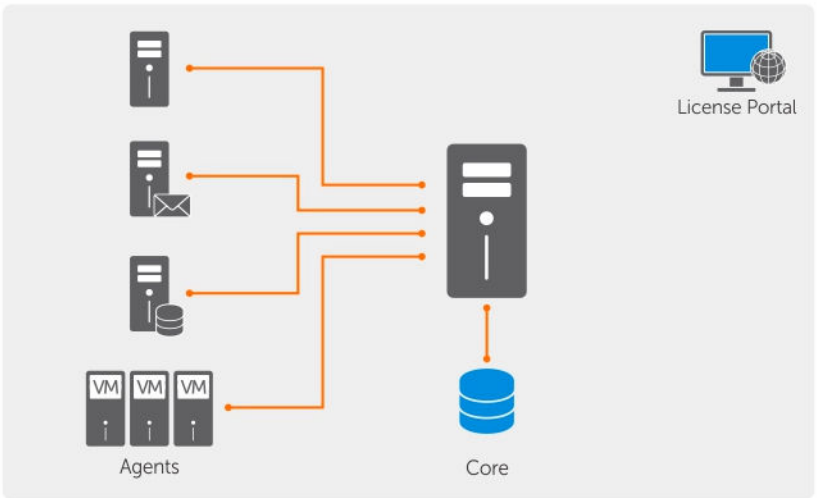

図 2. Dell DL1000 展開アーキテクチャ

次の図に示されているように、複数の DL1000 Core を展開することもできます。中央のコンソールが複数のコアを管理します。

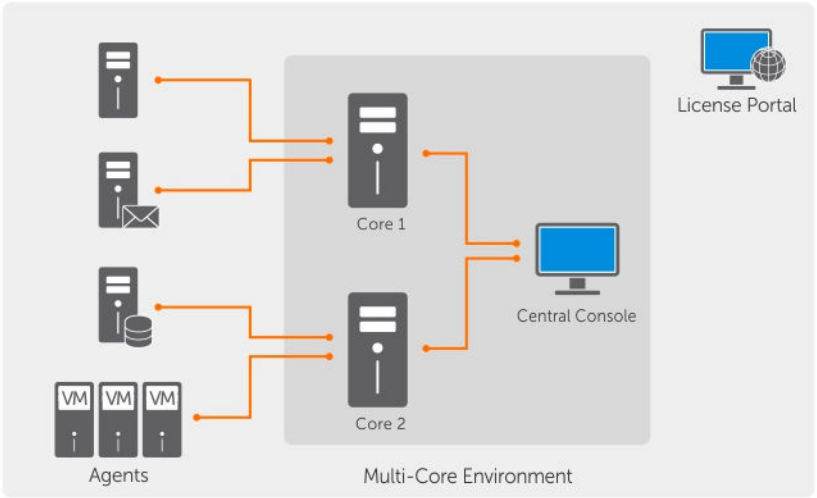

図 3. Dell DL1000 マルチコア展開アーキテクチャ

その他の情報

メモ: すべての Dell OpenManage マニュアルは、**dell.com/openmanagemanuals** にアクセスしてください。

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。

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。

はじめに	システム機能、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。このマニュアルも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 AppAssure ソリューション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。
『Deplooyment Guide』（導入ガイド）	アプライアンスのハードウェア導入、および初期展開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 DL 1000 アプライアンスに関する追加情報と製品情報を提供します。

『Interoperability Guide』(相互運用ガイド)	DL1000 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 ユーザーズガイド)	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。
『Resource Media』(リソースメディア)	システムに付属のメディアには、システムの設定と管理用のマニュアルとツールが収録されています。収録内容には、オペレーティングシステム、システム管理ソフトウェア、システムアップデート、およびシステムと同時に購入されたシステムコンポーネントに関する情報等が含まれます。

2

DL1000 での作業

DL1000 Core Console へのアクセス

DL1000 Core Console へアクセスするには、次の手順を実行します。

1. お使いのブラウザの信頼済みサイトをアップデートします。
2. DL1000 にリモートでアクセスできるようブラウザを設定します。Core Console へのリモートアクセスのためのブラウザの設定を参照してください。
3. DL1000 Core Console にアクセスするには、以下のいずれかの手順を行います。
   - DL1000 コア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。

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 のブラウザ設定を変更するには、次の手順を実行します。

1. Internet Explorer を開きます。
2. **ツール** メニューから、**インターネットオプション**、**セキュリティ** タブを選択します。
3. **信頼済みサイト** をクリックし、**サイト** をクリックします。
4. オプション **このゾーンのサイトにはすべてサーバーの確認（https:）を必要とする** の選択を解除し、http://<*AppAssure Core をホストしているアプライアンスサーバーのホスト名または IP アドレス*> を **信頼済みサイト** に追加します。
5. **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。
6. **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。
7. 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。
8. **OK** をクリックし、**詳細設定** タブを選択します。
9. **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。
10. **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。

Mozilla Firefox の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、AppAssure 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。

ライセンスの管理

Core Console から直接 DL1000 のライセンスを管理できます。このコンソールからは、ライセンスキーを変更したり、ライセンスサーバーと通信することができます。また、Core Console の **Licensing**（ライセンス）ページから Dell AppAssure ライセンスポータルにアクセスすることもできます。

Licensing（ライセンス）ページには以下の情報が含まれています。

- ライセンスタイプ
- ライセンスステータス

- 保護されているマシンの数
- ライセンスサーバーからの最後の応答のステータス
- ライセンスサーバーと最後に通信した時刻
- ライセンスサーバーとの次の通信予定
- ライセンスの制約事項

ライセンスキーの変更

ライセンスキーを変更するには、次の手順を実行します。

1. Core Console に移動して、**Configuration（設定） → Licensing（ライセンス）**を選択します。
   Licensing（ライセンス）ページが表示されます。
2. **License Details**（ライセンス詳細）ページで、**Change**（変更）をクリックします。
   Change License Key（ライセンスキーの変更）ダイアログボックスが表示されます。
3. **Change License Key**（ライセンスキーの変更）ダイアログボックスで、新しいライセンスキーを入力して **OK** をクリックします。

ライセンスポータルサーバーとの通信

AppAssure 5 Core Console は、ライセンスポータルで行われた変更をアップデートするためにポータルサーバーと通信します。ポータルサーバーとの通信は指定された間隔で自動的に行われますが、オンデマンドで通信を開始することもできます。
ポータルサーバーと通信するには、次の手順を実行します。

1. Core Console に移動して、**Configuration（設定） → Licensing（ライセンス）**をクリックします。
   Licensing（ライセンス）ページが表示されます。
2. **License Server**（ライセンスサーバー）オプションから、**Contact Now**（今すぐ通信）をクリックします。

AppAssure 言語の手動変更

AppAssure では、AppAssure アプライアンス設定ウィザードの実行中に選択した言語を、サポートされている任意の言語に変更することができます。
AppAssure 言語を希望の言語に変更するには、次の手順を実行します。

1. `regdit` コマンドを使用してレジストリエディタを起動します。
2. **HKEY_LOCAL_MACHINE → SOFTWARE → AppRecovery → Core → Localization** に移動します。
3. **Lcid** を開きます。
4. **decimal**（10 進数）を選択します。
5. `Value data`（値のデータ）ボックスに必要な言語値を入力します。サポートされている言語値は次のとおりです。

   a. 英語：1033
   b. ポルトガル語（ブラジル）：1046
   c. スペイン語：1034
   d. フランス語：1036
   e. ドイツ語：1031
   f. 簡体字中国語：2052

g. 日本語：1041
h. 韓国語：1042

6. 各サービスを次の順序で右クリックして再起動します。
   a. Windows Management Instrumentation
   b. SRM Web Service
   c. AppAssure Core
7. ブラウザのキャッシュをクリアします。
8. ブラウザを閉じ、デスクトップアイコンからコアコンソールを再起動します。

インストール中の OS 言語の変更

実行中の Windows インストールでは、コントロールパネルを使用して言語パックを選択し、追加の国際対応設定を設定できます。
OS の言語を変更するには、次の手順を実行します。

メモ: OS と AppAssure には同じ言語を設定することをお勧めします。異なる言語を設定した場合、一部のメッセージでそれらの言語が混在して表示されることがあります。

メモ: AppAssure の言語を変更する前に、OS の言語を変更することをお勧めします。

1. **Start**（スタート）ページで、`language`（言語）と入力し、検索範囲が Settings（設定）に設定されていることを確認します。
2. **Results**（結果）パネルで、**Language**（言語）を選択します。
3. **Change your language preferences**（言語の設定の変更）ペインで、**Add a language**（言語の追加）を選択します。
4. インストールする言語を参照または検索します。
   たとえば、Catalan（カタルニア語）を選択し、Add（追加）を選択します。これにより、カタルニア語が使用言語の 1 つとして追加されます。
5. Change your language preferences（言語の設定の変更）ペインで、追加した言語の横にある **Options**（オプション）を選択します。
6. お使いの言語に対して言語パックが利用可能な場合は、`Download and install language pack`（言語パックをダウンロードしてインストールします）を選択します。
7. 言語パックがインストールされると、その言語は Windows の表示言語として使用可能になります。
8. この言語を表示言語にするには、その言語を言語リストの一番上に移動させます。
9. 変更を有効にするために、一度ログアウトして Windows に再度ログインします。

Core 設定の管理

Core 設定は、構成とパフォーマンスに関するさまざまな設定を定義するために使用されます。多くの設定は最適な使用のために設定されていますが、必要に応じて次の設定を変更できます。

- 一般
- Nightly Jobs（夜間ジョブ）
- Transfer Queue（転送キュー）
- Client Timeout Settings（クライアントタイムアウト設定）
- Deduplication Cache Configuration（キャッシュ設定の重複排除）
- Database Connection Settings（データベース接続設定）

Core 表示名の変更

メモ: 表示名には、お使いのアプライアンスの初期設定時に、永続的な表示名を選択することを推奨します。表示名を後から変更する場合は、新しいホスト名が有効になり、アプライアンスが正常に機能するように、いくつかの手順を手動で実行する必要があります。

コア表示名を変更するには、次の手順を実行します。

1. Core Console に移動して、**Configuration（設定）** → **Settings（設定）**をクリックします。
2. **General**（一般）セクションで、**Change**（変更）をクリックします。
   Display Name（表示名）ダイアログボックスが表示されます。
3. **Display Name**（表示名）テキストボックスに Core の新しい表示名を入力します。
4. **OK** をクリックします。

夜間ジョブ時刻の変更

夜間ジョブオプションでは、Core によって保護されるエージェントのロールアップ、接続性可否、切り捨てなどのジョブをスケジュールします。

夜間ジョブ時刻を調整するには、次の手順を実行します。

1. Core Console に移動して、**Configuration（設定）** → **Settings（設定）**を選択します。
2. **Nightly Jobs**（夜間ジョブ）セクションで、**Change**（変更）をクリックします。
   Nightly Jobs（夜間ジョブ）ダイアログボックスが表示されます。
3. **Nightly Jobs Time**（夜間ジョブ時刻）テキストボックスに新しい開始時刻を入力します。
4. **OK** をクリックします。

転送キュー設定の変更

転送キュー設定は、データ転送のための最大同時転送数と最大再試行回数を決定するコアレベルの設定です。

転送キュー設定を変更するには、次の手順を実行します。

1. Core Console に移動して、**Configuration（設定）** → **Settings（設定）**をクリックします。
2. **Transfer Queue**（転送キュー）セクションで、**Change**（変更）をクリックします。
   Transfer Queue（転送キュー）ダイアログボックスが表示されます。
3. **Maximum Concurrent Transfers**（最大同時転送数）テキストボックスに、同時転送数をアップデートするための値を入力します。
   1 から 60 までの値を設定します。値を小さくすると、ネットワークおよびその他のシステムリソースに対する負荷が減少します。処理される容量が増加すると、システムに対する負荷も増加します。
4. **Maximum Retries**（最大再試行回数）テキストボックスに、再試行の最大数をアップデートするための値を入力します。
5. **OK** をクリックします。

クライアントタイムアウト設定の調整

クライアントタイムアウト設定では、クライアントに接続するときにタイムアウトするまでサーバーが待機する時間を秒数または分数で指定します。

クライアントタイムアウト設定を調整するには、次の手順を実行します。

1. Core Console に移動して、**Configuration（設定） → Settings（設定）**をクリックします。
2. **Client Timeout Settings Configuration**（クライアントタイムアウト設定）セクションで、**Change**（変更）をクリックします。

   Client Timeout Settings（クライアントタイムアウト設定）ダイアログボックスが表示されます。
3. **Connection Timeout**（接続タイムアウト）テキストボックスに、接続タイムアウトが発生するまでの分と秒数を入力します。
4. **Read/Write Timeout**（読み取り / 書き込みタイムアウト）テキストボックスに、読み取り / 書き込みイベント中タイムアウトが発生するまでに経過する分と秒数を入力します。
5. **OK** をクリックします。

重複排除キャッシュの設定

グローバル重複排除により、バックアップされたデータの保存に必要なディスクストレージの容量を削減することができます。重複排除ボリュームマネージャ（DVM）は一連の保存場所を 1 つのリポジトリに集約します。重複排除キャッシュには一意のブロックへの参照が保持されます。重複排除キャッシュはデフォルトで 1.5 GB に設定されています。冗長な情報量が大きくなり、重複排除キャッシュが満杯になると、リポジトリは新しく追加されるデータに対してリポジトリ全体での重複排除を最大限に活用できなくなります。その場合は、Core Console で重複排除キャッシュの設定を変更して、重複排除キャッシュの容量を増やすことができます。

重複排除キャッシュを設定するには、次の手順を実行します。

1. Core Console に移動して、**Configuration（設定） → Settings（設定）**をクリックします。
2. **Deduplication Cache Configuration**（重複排除キャッシュ設定）セクションで、**Change**（変更）をクリックします。

   Deduplication Cache Configuration（キャッシュ設定の重複排除）ダイアログボックスが表示されます。
3. **Primary Cache Location**（プライマリキャッシュの場所）テキストボックスに、プライマリキャッシュの新しい場所を入力します。
4. **Secondary Cache Location**（セカンダリキャッシュの場所）テキストボックスに、セカンダリキャッシュの新しい場所を入力します。
5. **Metadata Cache Location**（メタデータキャッシュの場所）テキストボックスに、メタデータキャッシュの新しい場所を入力します。
6. **OK** をクリックします。

   メモ: 変更を有効にするには、Core サービスを再起動する必要があります。

エンジン設定の変更

エンジンの設定を変更するには、次の手順を実行します。

1. Core Console に移動して、**Configuration（設定） → Settings（設定）**をクリックします。
2. **Replay Engine Configuration**（Replay エンジンの設定）セクションで、**Change**（変更）をクリックします。

   Replay Engine Configuration（Replay Engine の設定）ダイアログボックスが表示されます。
3. **Replay Engine Configuration**（Replay エンジン設定）ダイアログボックスで、IP アドレスを指定します。次のいずれかを選択してください。

- お使いの TCP/IP からの優先 IP アドレスを使用するには、**Automatically Determined**（自動設定）をクリックします。
- IP アドレスを手動で入力するには、**Use a specific IP address**（特定の IP アドレスを使用）をクリックします。

4. 次の説明に従って設定情報を入力します。

テキストボックス	説明
Preferable Port（優先ポート）	ポート番号を入力するか、デフォルト設定（デフォルトポートは 8007）を承諾します。このポートはエンジン用の通信チャネルの指定に使用されます。
Admin Group（管理グループ）	管理グループの新しい名前を入力します。デフォルト名は **BUILTIN \Administrators** です。
Minimum Async I/O Length（非同期 I/O 最小長）	値を入力するか、デフォルト設定を選択します。この値は、最小限の非同期入出力の長さを示します。デフォルト設定は 65536 です。
Receive Buffer Size（受信バッファサイズ）	インバウンドバッファサイズを入力するか、デフォルト設定を受け入れます。デフォルト設定は 8192 です。
Send Buffer Size（送信バッファサイズ）	アウトバウンドバッファサイズを入力するか、デフォルト設定を受け入れます。デフォルト設定は 8192 です。
Read Timeout（読み取りタイムアウト）	読み取りタイムアウト値を入力するか、デフォルト設定を選択します。デフォルト設定は 00:00:30 です。
Write Timeout（書き込みタイムアウト）	書き込みタイムアウト値を入力するか、デフォルト設定を選択します。デフォルト設定は 00:00:30 です。

5. **No Delay**（遅延なし）を選択します。
6. **OK** をクリックします。

展開設定の変更

展開の設定を変更するには、次の手順を実行します。

1. Core Console に移動して **Configuration**（設定）タブを選択し、次に **Settings**（設定）をクリックします。
2. **Deploy Settings**（展開設定）ペインで、**Change**（変更）をクリックします。
   Deploy Settings（展開設定）ダイアログボックスが表示されます。
3. **Agent Installer Name**（エージェントインストーラ名）テキストボックスに、エージェント実行ファイルの名前を入力します。デフォルトは **Agentweb. exe** です。
4. **Core Address**（Core アドレス）テキストボックスに、そのコアのアドレスを入力します。
5. **Failed Receive Timeout**（受信失敗タイムアウト）テキストボックスに、アクティビティをタイムアウトさせずに待機する時間を分単位で入力します。
6. **Max Parallel Installs**（最大並行インストール）テキストボックスに、並行してインストールできるインストールの最大数を入力します。
7. 次の設定オプションのいずれか、または両方を選択します。

- Automatic reboot after install（インストール後に自動再起動）
- Protect After Deploy（展開後に保護）

8. **OK** をクリックします。

データベース接続設定の変更

データベース接続設定を変更するには、次の手順を実行します。

1. Core Console に移動して、**Configuration（設定） → Settings（設定）**をクリックします。
2. **Database Connection Settings**（データベース接続設定）セクションで、次のいずれかを行います。
   - デフォルト設定に復元するには、**Restore Default**（デフォルトの復元）をクリックします。
   - データベース接続設定を変更するには、**Change**（変更）をクリックします。

   変更をクリックすることにより、**Database Connection Settings**（データベース接続設定）ダイアログボックスが表示されます。
3. 次の説明に従って、データベース接続を変更する設定を入力します。

テキストボックス	説明
ホスト名	データベース接続のためのホスト名を入力します。
ポート	データベース接続のためのポート番号を入力します。
User Name（ユーザー名）（オプション）	データベース接続設定へのアクセスと管理のためのユーザー名を入力します。この名前は、データベース接続にアクセスするためのログイン資格情報を指定するために使用されます。
Password（パスワード）（オプション）	データベース接続設定へのアクセスと管理のためのパスワードを入力します。
Retain event and job history for, days（イベントおよびジョブ履歴を保持：日間）	データベース接続用にイベントとジョブ履歴を保持する日数を入力します。

4. **Test Connection**（接続のテスト）をクリックして、設定を検証します。
5. **保存** をクリックします。

イベントの管理

Core には、Core またはバックアップジョブでの重要な問題について管理者に通知するために使用できる事前定義されたイベントセットが含まれています。

Events（イベント）タブから、通知グループ、電子メールの SMTP 設定、サーバー設定、有効化済みトレースログ、クラウド設定、繰り返し削減、イベント保持を管理できます。

通知グループオプションでは通知グループを管理することが可能であり、そこから以下の操作を実行できます。

- 以下についてのアラートを生成したいイベントを指定する。
  - クラスタ

  - 接続性可否
  - ジョブ
  - ライセンス
  - ログの切り捨て
  - アーカイブ
  - コアサービス
  - エクスポート
  - 保護
  - レプリケーション
  - ロールバック
- アラートのタイプ（エラー、警告、および情報）を指定する。
- アラートがどこのだれに送信されるかを指定する。以下のオプションがあります。
  - Email Address（電子メールアドレス）
  - Windows Events Logs（Windows イベントログ）
  - Syslog Server（シスログサーバー）
- 繰り返しの時間しきい値を指定する。
- すべてのイベントの保持期間を指定する。

通知グループの設定

通知グループを設定するには、次の手順を実行します。

1. Core Console で、**Configuration（設定）→ Events（イベント）**を選択します。
2. **Add Group**（グループの追加）をクリックします。

   Add Notification Group（通知グループを追加）ダイアログボックスが開き、2 つのパネルが表示されます。
   - **アラートの有効化**
   - **Notification Options（通知オプション）**

アラートを有効にする

アラートを有効にすると、ログの記録、レポートの作成、アラートの設定をする一連のシステムイベントを定義することができます。

メモ: すべてのイベントでアラートを作成するには、**All Alerts**（すべてのアラート）を選択します。

- エラー、警告、情報メッセージ、またはそれらの組み合わせに対して特定のアラートを作成するには、次のいずれかを選択します。
  - 赤い三角形のアイコン（エラー）
  - 黄色い三角形のアイコン（警告）
  - 青色の円（情報）
  - U 字型の矢印（デフォルトの復元）
- 特定のイベント用にアラートを作成するには、関連するグループの横にある **>** 記号をクリックしてチェックボックスを選択し、アラートを有効にします。

通知オプションの設定

1. **Notification Options**（通知オプション）パネルで、通知プロセスの処理方法を指定します。

通知オプションには、次があります。

テキストボックス	説明
Notify by e-mail（E-メールで通知）	電子メール通知の受信者を指定します。次に示すように、個別の複数電子メールアドレスの他、ブラインドカーボンコピーを指定することもできます。 • **To:** • **CC:** • **BCC:**
Notify by Windows Event Log（Windows イベントログで通知）	Windows イベントログを通してアラートの通知を報告する場合はこのオプションを選択します。
Notify by sys logd（sys logd で通知）	sys logd を介してアラートが報告されるようにするには、このオプションを選択します。次のテキストボックスで、sys logd の詳細を入力します。 • **Hostname:（ホスト名：）** • **Port:1（ポート：1）**
Notify by Toast alerts（Toast アラートで通知）	アラートを画面の右下隅にポップアップで表示させたい場合はこのオプションを選択します。

2. **OK** をクリックします。

   メッセージ **The Group name cannot be changed after the creation of the Notification Group. are you sure you want to use this name?**（通知グループの作成後にグループ名を変更することはできません。この名前を使用してもよろしいですか ?）が表示されます。

   - グループ名を保存するには、**Yes**（はい）をクリックします。
   - グループ名を変更するには、**No**（いいえ）をクリックします。**Notification Options**（通知オプション）ウィンドウに戻ってグループ名およびその他の通知グループの設定を更新してから、作業内容を保存します。

電子メールサーバーの設定

メモ: 電子メールアラートメッセージを送信する前に、**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があります。

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 Console で、**Configuration（設定）→ Events（イベント）**をクリックします。
2. **Email Settings**（電子メール設定）ペインで、**SMPT server**（SMPT サーバー）をクリックします。

   SMTP Server Settings（SMTP サーバー設定）ダイアログボックスが表示されます。
3. 電子メールサーバーに次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。
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。
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。
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。 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。

4. **Send Test Email**（テスト電子メールの送信）をクリックして次の手順を実行します。
   a. Send Test Email（テスト電子メールの送信）ダイアログボックスで、テストメッセージ用の宛先電子メールアドレスを入力して **Send**（送信）をクリックします。
   b. テストメッセージが失敗した場合は、エラーダイアログボックスおよび **Send Test Email**（テスト電子メールの送信）ダイアログボックスを閉じて、電子メールサーバーの設定を再度確認します。手順 4 を繰り返します。
   c. **OK** をクリックして確定します。
   d. テスト電子メールが送信されたかどうかを確認します。
   e. SMTP サーバー設定ダイアログボックスに戻り、**Save**（保存）をクリックしてダイアログボックスを閉じて設定を保存します。

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する必要があります。

メモ: 電子メールアラートメッセージを受信するには、通知グループを設定して、**Notify by email**（電子メールで通知）を有効にします。

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 Console で、**Configuration（設定）→ Events（イベント）**をクリックします。
2. **Email Settings**（電子メール設定）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。

3. **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
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。

4. **Send Test Email**（テスト電子メールの送信）をクリックして次の手順を実行します。
   a. Send Test Email（テスト電子メールの送信）ダイアログボックスで、テストメッセージ用の宛先電子メールアドレスを入力して **Send**（送信）をクリックします。
   b. テストメッセージが失敗した場合は、エラーダイアログメッセージおよびテスト電子メールの送信ダイアログボックスを閉じてから、**OK** をクリックして現在の電子メールテンプレート設定を保存し、お使いの電子メールサーバーの設定を変更します。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を参照してください。その電子メールアカウントのパスワードを再度入力するようにしてください。設定を保存して、手順 4 に戻ります。
   c. **OK** をクリックして確定します。
   d. テスト電子メールが送信されたかどうかを確認します。
   e. **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に戻り、**OK** をクリックしてダイアログボックスを閉じ、設定を保存します。

繰り返し削減の設定

繰り返し削減を設定するには、次の手順を実行します。

1. Core Console で、**Configuration（設定）** → **Events（イベント）**をクリックします。
2. **Repetition Reduction**（繰り返し削減）セクションで、**Change**（変更）をクリックします。
   Enable Repetition Reduction（繰り返し削減の有効化）ダイアログボックスが表示されます。
3. **Enable Repetition Reduction**（繰り返し削減を有効にする）を選択します。
4. **Store events for**（イベントの保存期間）テキストボックスに、繰り返し削減のためにイベントを保存する期間を分単位で入力します。
5. **OK** をクリックします。

イベント保持の設定

イベント保持を設定するには、次の手順を実行します。

1. Core Console で、**Configuration（設定）** → **Settings（設定）**をクリックします。
2. **Database Connection Settings**（データベース接続設定）で、**change**（変更）をクリックします。
   Database Connection Settings（データベース接続設定）ダイアログボックスが表示されます。
3. **Retain event and job history for**（イベントおよびジョブ履歴を保持する期間）テキストボックスに、イベントに関する情報を保持する日数を入力します。
   たとえば、30 日（デフォルト）を選択することができます。
4. **保存** をクリックします。

リポジトリの管理

リポジトリは、保護対象ワークステーションおよびサーバーから取得されたスナップショットを保存します。DL1000 のリポジトリは事前設定済みです。リポジトリはお使いのシステムの内蔵ストレージに格納されています。

リポジトリに関する主な概念と考慮事項は、以下のとおりです。

- リポジトリは、AppAssure 拡張可能オブジェクトファイルシステムに基づいています。
- リポジトリ内に保存されているすべてのデータは、グローバルに重複排除されます。
- 拡張可能オブジェクトファイルシステムは、グローバルデータ重複排除、暗号化、および保持管理と連携して拡張可能な I/O パフォーマンスを実現します。

リポジトリ詳細の表示

リポジトリの詳細を表示するには、次の手順を実行します。

1. Core Console で、**Configuration（設定） → Repositories（リポジトリ）**とクリックします。
2. 詳細を表示するリポジトリの **Status**（ステータス）列の横にある **>** をクリックします。
3. リポジトリの詳細には、ストレージの場所と統計情報が含まれます。ストレージの場所の詳細には、メタデータパス、データパス、およびサイズが含まれます。統計情報には、次の情報があります。
   - **Deduplication**（重複排除）- ブロック重複排除のヒット数とミス数、およびブロック圧縮率として報告されます。
   - **Record I/O**（レコード I/O）- 速度（MB/s）、読み取り速度（MB/s）、および書き込み速度（MB/s）で構成されます。
   - **Storage Engine**（ストレージエンジン）- 速度（MB/s）、読み取り速度（MB/s）、および書き込み速度（MB/s）が含まれます。

リポジトリのチェック

Core Console は、エラー発生時にリポジトリボリュームの診断チェックを実行できます。コアエラーの原因には、不適切なシャットダウンやハードウェア障害などがあります。

メモ: この手順は、診断目的でのみ使用する必要があります。

リポジトリをチェックするには、次の手順を実行します。

1. **Configuration（設定） → Repositories（リポジトリ）**とクリックします。
2. **Actions**（アクション）ボタン下の Compression Ratio（圧縮率）列の横にある Settings（設定）アイコンをクリックします。
3. **Check**（チェック）をクリックします。

   Check Repository（リポジトリのチェック）ダイアログボックスが表示されます。
4. **Check Repository**（リポジトリのチェック）ダイアログボックスで、**Check**（チェック）をクリックします。

   メモ: チェックを実行すると、このリポジトリに関連付けられているアクティブタスクのすべてがキャンセルされます。チェックが開始される前に、チェックの続行を確認するためのメッセージが表示されます。リカバリポイントキャッシュの再構築が推奨されます。チェックが不合格の場合は、アーカイブからのリポジトリの復元が必要になります。

セキュリティの管理

DL1000 は強力な暗号化機能を提供します。暗号化することにより、保護対象マシンのバックアップはアクセス不能になり、暗号化キーを持つユーザーのみがデータに対するアクセスおよび暗号解除を行うことができます。暗号化がパフォーマンスに影響することはありません。主なセキュリティ概念と考慮事項は次のとおりです。

- 暗号化は、SHA-3 に準拠した暗号ブロック連鎖（CBC）モードで 256 ビット AES を使用して実行されます。
- 重複排除は、機密性を確実にするために暗号化ドメイン内で実行されます。
- 暗号化はパフォーマンスに影響することなく実行されます。
- Core 上で設定された暗号化キーの追加、除去、インポート、エクスポート、変更、および削除を実行できます。

暗号化キーの追加

暗号化キーを追加するには、次の手順を実行します。

1. Core Console で、**Configuration（設定）** → **Security（セキュリティ）**をクリックします。
2. **Actions**（アクション）ドロップダウンメニューで、**Add Encryption Key**（暗号化キーの追加）をクリックします。

   Create Encryption Key（暗号化キーを作成）ダイアログボックスが表示されます。
3. **Create Encryption Key**（暗号化キーを作成）ダイアログボックスで、次の説明どおりにキーの詳細を入力します。

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。
説明	暗号化キーの説明を入力します。暗号化キーの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。

4. **OK** をクリックします。

注意: パスフレーズは保護することが推奨されます。パスフレーズを失うと、データを回復できなくなります。

暗号化キーの編集

暗号化キーを編集するには、次の手順を実行します。

1. Core Console で、**Configuration（設定）** → **Security（セキュリティ）**をクリックします。

   Encryption Keys（暗号化キー）画面が表示されます。
2. 編集する暗号化キーの名前の横にある **>** をクリックして、**Edit**（編集）をクリックします。

   Edit Encryption Key（暗号化キーを変更）ダイアログボックスが表示されます。

3. **Edit Encryption Key**（暗号化キーを編集）ダイアログボックスで、暗号化キーの名前を編集するか、説明を変更します。
4. **OK** をクリックします。

暗号化キーのパスフレーズの変更

暗号化キーのパスフレーズを変更するには、次の手順を実行します。

1. Core Console で、**Configuration（設定）→ Security（セキュリティ）**をクリックします。
2. 編集する暗号化キーの名前の横にある **>** をクリックして、**Change Passphrase**（パスフレーズの変更）をクリックします。

   Change Passphrase（パスフレーズの変更）ダイアログボックスが表示されます。
3. **Change Passphrase**（パスフレーズの変更）ダイアログボックスで、暗号化の新しいパスフレーズを入力し、入力した内容を確認するためにパスフレーズを再入力します。
4. **OK** をクリックします。

△ 注意: パスフレーズは保護することが推奨されます。パスフレーズを失うと、システム上のデータにアクセスできなくなります。

暗号化キーのインポート

暗号化キーをインポートするには、次の手順を実行します。

1. Core Console で、**Configuration（設定）→ Security（セキュリティ）**をクリックします。
2. **Actions**（アクション）ドロップダウンメニューから **Import**（インポート）をクリックします。

   Import Key（キーのインポート）ダイアログボックスが表示されます。
3. **Import Key**（キーのインポート）ダイアログボックスで、**Browse**（参照）をクリックしてインポートする暗号化キーの場所を指定し、**Open**（開く）をクリックします。
4. **OK** をクリックします。

暗号化キーのエクスポート

暗号化キーをエクスポートするには、次の手順を実行します。

1. Core Console で、**Configuration（設定）→ Security（セキュリティ）**をクリックします。
2. エクスポートする暗号化キーの Configuration（設定）ドロップダウンメニューで **Export**（エクスポート）を選択します。

   Export Key（キーのエクスポート）ダイアログボックスが表示されます。
3. **Export Key**（キーのエクスポート）ダイアログボックスで、**Save File**（ファイルの保存）をクリックして暗号化キーを保存し、安全な場所に保管します。
4. **OK** をクリックします。

暗号化キーの削除

暗号化キーを削除するには、次の手順を実行します。

1. Core Console で、**Configuration（設定）→ Security（セキュリティ）**をクリックします。
2. 削除する暗号化キーの Configuration（設定）ドロップダウンメニューで **Delete**（削除）を選択します。

   Remove Key（キーの削除）ダイアログボックスが表示されます。
3. **Remove Key**（キーの削除）ダイアログボックスで、**OK** をクリックして、暗号化キーを削除します。

メモ: 暗号化キーを削除すると、データが復号化されます。

クラウドアカウントの管理

DL アプライアンスでは、リカバリポイントのバックアップアーカイブをクラウドに作成することによるデータのバックアップが可能です。クラウドストレージプロバイダを通じてクラウドアカウントを作成、編集、管理することができます。データは、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を使用してクラウドにアーカイブすることができます。クラウドアカウントを管理するための次のトピックを参照してください。

- クラウドアカウントの追加
- クラウドアカウントの編集
- クラウドアカウントの設定
- クラウドアカウントの削除

クラウドアカウントの追加

アーカイブデータをクラウドにエクスポートする前に、Core Console でお使いのクラウドプロバイダのアカウントを追加します。

クラウドアカウントを追加するには、次の手順を実行します。

1. Core Console で **Tools**（ツール）タブをクリックします。
2. 左メニューで **Clouds**（クラウド）をクリックします。
3. **Clouds**（クラウド）ページで **Add New Account**（新規アカウントの追加）をクリックします。

   Add New Account（新規アカウントの追加）ダイアログボックスが開きます。
4. **Cloud Type**（クラウドタイプ）ドロップダウンリストから、互換性のあるクラウドのプロバイダを選択します。
5. 手順 4 で選択したクラウドタイプに基づいて、次の表に説明されている詳細を入力します。

表 1. クラウドアカウントの追加

クラウドタイプ	テキストボックス	説明
Microsoft Azure	Storage Account Name（ストレージアカウント名）	Windows Azure ストレージアカウントの名前を入力します。
	Access Key（アクセスキー）	アカウントのアクセスキーを入力します。
	表示名	AppAssure でのアカウントの表示名（例：Windows Azure 1）を作成します。
Amazon S3	Access Key（アクセスキー）	Amazon クラウドアカウントのアクセスキーを入力します。
	Secret Key（シークレットキー）	このアカウントのシークレットキーを入力します。
	表示名	AppAssure でのアカウントの表示名（例：Amazon 1）を作成します。

クラウドタイプ	テキストボックス	説明
Powered by OpenStack	ユーザー名	OpenStack ベースのクラウドアカウントのユーザー名を入力します。
	API Key（API キー）	アカウントの API キーを入力します。
	表示名	AppAssure でのアカウントの表示名（例：OpenStack 1）を作成します。
	Tenant ID（テナント VM）	このアカウントのテナント ID を入力します。
	Authentication URL（認証 URL）	このアカウントの認証 URL を入力します。
Rackspace クラウドブロックストレージ	ユーザー名	Rackspace クラウドアカウントのユーザー名を入力します。
	API Key（API キー）	このアカウントの API キーを入力します。
	表示名	AppAssure でのアカウントの表示名（例：ORackspace 1）を作成します。

6. **追加** をクリックします。
   ダイアログボックスが閉じ、お使いのアカウントが Core Console の **Clouds**（クラウド）ページに表示されます。

クラウドアカウントの編集

クラウドアカウントを編集するには、次の手順を実行します。

1. Core Console で **Tools**（ツール）タブをクリックします。
2. 左メニューで **Clouds**（クラウド）をクリックします。
3. 編集するクラウドアカウントの横にあるドロップダウンメニューをクリックして、**Edit**（編集）をクリックします。
   Edit Account（アカウントの編集）ウィンドウが開きます。
4. 詳細を必要に応じて編集し、**Save**（保存）をクリックします。

メモ: クラウドタイプを編集することはできません。

クラウドアカウントの設定

クラウドアカウントの設定では、AppAssure がクラウドへの接続を試みる回数、タイムアウトになるまで接続の試行に費やす時間を決めることができます。。
クラウドサービスの接続を設定するには、次の手順を実行します。

1. Core Console で、**Configuration**（設定）タブをクリックします。
2. 左側のメニューで **Settings**（設定）をクリックします。
3. **Settings**（設定）ページで、**Cloud Configuration**（クラウドの設定）までスクロールダウンします。

4. 設定するクラウドアカウントの横にあるドロップダウンメニューをクリックして、次のいずれかを実行します。
   - **Edit**（編集）をクリックします。
     Cloud Configuration（クラウド設定）ダイアログボックスが表示されます。
     1. 上矢印および下矢印を使用して、次のいずれかのオプションを編集します。
        - **Request Timeout**（要求タイムアウト）: 分、および秒で表示され、クラウドアカウントへの接続時に遅延がある場合に AppAssure が単一の接続に費やす時間を決定します。
        - **Retry Count**（再試行回数）: クラウドアカウントに到達できないと判断するまで AppAssure が接続の試行を行う回数を決定します。
        - **Write Buffer Size**（書き込みバッファサイズ）: アーカイブデータのクラウドへの書き込み用に予約するバッファのサイズを決定します。
        - **Read Buffer Size**（読み取りバッファサイズ）: クラウドからアーカイブデータの読み取り用に予約するブロックサイズを決定します。
     2. **Next**（次へ）をクリックします。
   - **Reset**（リセット）をクリックすると、設定が次のデフォルト設定に戻ります。
     - **Request Timeout**（要求タイムアウト）: 01:30（分および秒）
     - **Retry Count**（再試行回数）: 3 （回）

クラウドアカウントの削除

クラウドアカウントを削除して、クラウドサービスを中止、または特定のコアでのサービスの使用を停止することができます。
クラウドアカウントを削除するには、次の手順を実行します。

1. Core Console で **Tools**（ツール ）タブをクリックします。
2. 左メニューで **Clouds**（クラウド）をクリックします。
3. 編集するクラウドアカウントの横にあるドロップダウンメニューをクリックして、**Remove**（削除）をクリックします。
4. **Delete Account**（アカウントの削除）ウィンドウで、**Yes**（はい）をクリックしてアカウントの削除を確定します。
5. クラウドアカウントが現在使用中の場合は、2 つ目のウィンドウでアカウント削除を続行するかどうかを確認するメッセージが表示されます。**Yes**（はい）をクリックして確定します。

   メモ: 現在使用中のアカウントを削除すると、このアカウントでスケジュールされているすべてのアーカイブジョブが失敗します。

DL1000 の監視

DL1000 Appliance サブシステムのステータスは、**Overall Status**（全体ステータス）ページの **Appliance**（アプライアンスサーバー）タブを使用して監視できます。**Overall Status**（全体ステータス）ページには、各サブシステムの横に、ステータスライト、およびサブシステムの正常性を説明するステータスの説明が表示されます。

Overall Status（全体ステータス）ページには、各サブシステムの詳細情報をドリルダウンするツールへのリンクも表示されます。これらは、警告やエラーのトラブルシューティングに便利です。Appliance Hardware サブシステムと Storage Hardware サブシステム用に使用できる **System Administrator**（システム管理者）リンクでは、ハードウェアの管理に使用されるシステム管理者用アプリケーションへのログオンが求められます。システム管理者用アプリケーションの詳細については、**dell.com/support/manuals** にある

『OpenManage Server Administrator User's Guide』（OpenManage Server Administrator ユーザーズガイド）を参照してください。

DL1000 のアップグレード

メモ: デルでは、インストーラを使用して Dell License Activation ポータルから最新バージョンの AppAssure をダウンロードすることをお勧めしています。

メモ: その他のソフトウェアのアップグレードについては、最新バージョンへのアップグレードを案内する通知が送信されます。

DL1000 の修復

メモ: 修復プロセスを開始する前に、Core サービスを停止してください。

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 を実行するには、次の手順を実行します。

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. 作成した RASR USB キーを挿入します。
2. RASR USB キーを使用してアプライアンスを再起動します。
3. **Rapid Appliance Self Recovery** をクリックします。
   ようこそ画面が表示されます。
4. **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。
5. **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）**
6. **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。
7. **Next**（次へ）をクリックします。
   Storage Configuration（ストレージ構成）画面が表示されます。
8. **OS Recovery**（OS リカバリ）画面で、警告メッセージ `This operation will recover the operating system. All OS disk data will be overwritten.`（この操作はオペレーティングシステムを回復します。すべての OS ディスクのデータが上書きされます。）がダイアログボックスに表示されます。
9. **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。

10. **Finish**（終了）をクリックします。

RASR USB キーの作成

メモ: ソフトウェア初期設定の完了後、**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。**Appliance**（アプライアンス）タブの ステータス アイコンは黄色になっています。

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. **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 ドライブの安全な取り外し、または Windows のドライブ取り出し機能を使用して、USB キーを取り外す準備をします。それをしない場合、USB キー内のコンテンツが破損するか、USB キーが正常に動作しない可能性があります。

   キーを取り出してラベルを貼り、今後の使用のために保管します。

3

ワークステーションとサーバーの保護

ワークステーションとサーバーの保護について

DL1000 を使用してデータを保護するには、Core Console で保護するワークステーションとサーバー（たとえば、Exchange サーバー、SQL Server、Linux サーバーなど）を追加します。

メモ: 本章では、マシンという言葉はそのマシンにインストールされている AppAssure Agent ソフトウェアも意味します。

Core Console では、AppAssure Agent ソフトウェア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の指定、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を行うことができます。Core Console にアクセスしてワークステーションおよびサーバーを保護する方法の詳細については、「マシンの保護」を参照してください。

エージェントの展開（プッシュインストール）

DL1000 では、保護のために個々の Windows マシンに AppAssure Agent Installer を展開できます。エージェントにインストーラをプッシュするには、次の手順を実行します。複数のマシンに同時にエージェントを展開するには、複数マシンへの展開を参照してください。

メモ: エージェントには、リモートインストールを可能にするセキュリティポリシーが設定されている必要があります。

エージェントを展開するには、次の手順を実行します。

1. Core Console の左側にあるナビゲーションエリアで、**Protected Machines**（保護対象マシン）をクリックします。
2. **Actions（アクション）** → **Deploy Agent（エージェントの展開）**とクリックします。
   Deploy Agent（エージェントを展開）ダイアログボックスが表示されます。
3. **Deploy Agent**（エージェントの展開）ダイアログボックスで、次の表の説明に従ってログオン設定を入力します。

テキストボックス	説明
Machine（マシン）	展開するマシンのホスト名または IP アドレスを入力します。
ユーザー名	このマシンに接続するためのユーザー名（administrator など）を入力します。
パスワード	このマシンに接続するためのパスワードを入力します。
Automatic reboot after install（インストール後に自動再起動）	これを選択して、AppAssure Agent Installer の展開およびインストールの完了時にコアを起動させるかどうかを指定します。

4. 入力した資格情報を検証するには、**Verify**（確認）をクリックします。

Deploy Agent（エージェントの展開）ダイアログボックスに、検証が実行中であることを示すメッセージが表示されます。

5. 検証処理をキャンセルするには **Abort**（中止）をクリックします。
   検証処理の完了後、検証処理が完了したことを示すメッセージが表示されます。
6. **Deploy**（展開）をクリックします。
   展開が開始されたことを示すメッセージが表示されます。進捗状況は **Events**（イベント）タブで確認できます。
7. エージェント展開のステータスに関する詳細情報を表示するには、**Show details**（詳細の表示）をクリックします。
8. **OK** をクリックします。

マシンの保護

このトピックでは、指定したマシン上でデータの保護を開始する方法について説明します。

メモ: マシンを保護するには、マシンに AppAssure Agent ソフトウェアがインストールされている必要があります。この手順を行う前に AppAssure Agent ソフトウェアをインストールする、または **Connection（接続）**ダイアログボックスで保護を定義するときにソフトウェアをエージェントに展開することができます。マシンの保護プロセス中に AppAssure Agent ソフトウェアをインストールするには、「Agent を保護する時のエージェントソフトウェアの展開」を参照してください。

保護を追加する際は、保護するマシンの名前または IP アドレス、およびそのマシン上で保護するボリュームを指定するとともに、各ボリュームに対する保護スケジュールを定義する必要があります。

複数のマシンをまとめて保護するには、複数マシンの保護を参照してください。

マシンを保護するには、次の手順を実行します。

1. AppAssure Agent ソフトウェアがインストールされたマシンをまだ再起動していない場合は、再起動します。
2. コアマシン上の Core Console から、ボタンバーで **Protect（保護）** → **Protect Machine（マシンの保護）**とクリックします。
   Protect Machine Wizard（マシンの保護ウィザード）が表示されます。
3. **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。
   - 今後 **Protect Machine Wizard**（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。
4. **次へ** をクリックします。
5. **Connection**（接続）ページで、次の表に説明されているとおり、接続先のマシンに関する情報を入力します。

テキストボックス	説明
Host（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	AppAssure Core がマシン上のエージェントと通信する際に使用するポート番号。デフォルトのポート番号は 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（administrator など）。

テキストボック ス　説明

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。

6. **Next**（次へ）をクリックします。**Protect Machine Wizard**（マシンの保護ウィザード）の隣に **Protection**（保護）ページが表示される場合は、手順 7 に進みます。

   メモ: Install Agent（エージェントのインストール）ページが **Protect Machine Wizard**（マシンの保護ウィザード）の隣に表示される場合は、Agent ソフトウェアが指定されたマシンにまだインストールされていないことを示します。**Next**（次へ）をクリックして、エージェントソフトウェアをインストールしてください。Core へのバックアップの前に、Agent ソフトウェアを保護するマシンにインストールし、再起動する必要があります。インストーラにエージェントマシンを再起動させるには、**Next**（次へ）をクリックする前に、**After installation, restart the machine automatically (recommended)**（インストール後にマシンを自動的に再起動する（推奨））オプションを選択します。

7. **Connect**（接続）ダイアログボックスで指定したホスト名または IP アドレスがこのテキストフィールドに表示されます。オプションで、Core Console に表示されるマシンの新しい名前を入力します。
8. 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、**Schedule Settings（スケジュール設定）**オプションで、**Default protection (hourly snapshots of all volumes)（デフォルトの保護（3 時間間隔ですべてのボリュームのスナップショットを作成））**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と、Core は 3 時間ごとに 1 回エージェントマシンのスナップショットを作成します。エージェントマシンのスナップショットは 1 時間に 1 回作成することができます（最少の場合）。保護設定はウィザードを終了した後の任意のタイミングで変更する場合は（これには保護するボリュームの選択が含まれます）、特定のエージェントマシンの Summary（サマリ）タブに移動します。
   - 別の保護スケジュールを定義するには、**Schedule Settings**（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. 次のいずれか 1 つを選択します。
   - **Protect Machine**（マシンの保護）ウィザードで Typical（標準）を選択し、デフォルトの保護設定を指定した場合、**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 AppAssure Core 上のリポジトリに転送されます。
   - **Protect Machine**（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。保護スケジュールのカスタマイズの詳細については、カスタム保護スケジュールの作成を参照してください。
   - **Protect Machine**（マシンの保護）ウィザードの詳細設定と、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 12 に進み、リポジトリと暗号化のオプションを設定します。
   - **Protect Machine**（マシンの保護）ウィザードの詳細設定を選択し、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 10 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、保護したいエージェントマシンのボリュームを指定します。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、Check（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: System Reserved（システムにより予約済み）ボリュームと、オペレーティングシステムがあるボリューム（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ます。
12. **Repository**（リポジトリ）ページで、 **Use an existing repository**（既存のリポジトリを使用する）を選択します。

13. **次へ** をクリックします。

    Encryption（暗号化）ページが表示されます。

14. オプションで暗号化を有効にするには、**Encryption**（暗号化）ページで **Enable Encryption**（暗号化の有効化）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: 暗号化を有効にした場合、このエージェントマシン上の保護対象ボリュームに適用されます。この設定は、Core Console の **Configuration**（設定）タブから後ほど変更できます。

    注意: AppAssure は、256 ビットキーの暗号ブロック連鎖 (CBC) モードで 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、パスフレーズを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は回復できません。

15. 次の表で説明されているとおりに情報を入力して、Core 用の暗号化キーを追加します。

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。
説明	暗号キーに関する追加の詳細情報を提供する説明文を入力します。
Passphrase (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。
Confirm Passphrase (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。

16. **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、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、定義したスケジュールに従って Core 上のリポジトリに転送されます。

保護の一時停止と再開

保護を一時停止すると、現在のマシンからのデータ転送のすべてが一時的に停止されます。

保護を一時停止するには、次の手順を実行します。

1. Core Console の左側のナビゲーションエリアで、 **Protected Machines**（保護対象マシン）ドロップダウンメニューをクリックします。
2. 保護を一時停止するマシンで **Pause Protection**（保護の一時停止）を選択します。

   Pause Protection（保護の一時停止）ダイアログボックスが表示されます。
3. 次のいずれかを選択して、**OK** をクリックします。
   - 明示的に再開するまで保護を一時停止する場合は、**Pause until resumed**（再開するまで一時停止）を選択します。
   - 特定期間中保護を一時停止する場合は、**Pause for** （一時停止する期間）を選択し、Days（日）、Hours（時） Minutes（分）制御に適切な一時停止期間を入力または選択します。

   メモ: 保護を再開するには、**Protected Machines**（保護対象マシン）ドロップダウンメニューで **Resume Protection**（保護の再開）を選択します。

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展開

エージェントを保護のために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展開することができます。

メモ: この手順は、保護するマシンにエージェントソフトウェアをすでにインストールした場合は必要ありません。

エージェントを保護するために追加するプロセス中にエージェントを展開するには、次の手順を実行します。

1. 左側のナビゲーションペインで **Protected Machines**（保護対象マシン）をクリックします。
2. **Actions（アクション）→ Deploy Agent（エージェントの展開）**とクリックします。
   Deploy Agent（エージェントを展開）ダイアログボックスが表示されます。
3. 次のようにログオンおよび保護設定を入力します。
   - **Host name**（ホスト名）— 保護するマシンのホスト名または IP アドレスを指定します。
   - **User name**（ユーザー名）— このマシンに接続するために使用されるユーザー名を指定します。例えば、administrator です。
   - **Password**（パスワード）— このマシンに接続するために使用されるパスワードを指定します。
   - **Protect machine after install**（インストール後にマシンを保護）— このオプションを選択すると、保護のためのマシン追加後における AppAssure によるデータのベーススナップショットの取得が可能になります。このオプションは、デフォルトで選択されています。このオプションの選択を解除する場合は、データ保護を開始する準備が整ったときにスナップショットを手動で強制する必要があります
   - **Display name**（表示名）— Core Console 上に表示されるマシン用の名前を指定します。表示名はホスト名と同じ値にすることができます。
   - **Port**（ポート）— Core がマシン上のエージェントと通信するポートの番号を指定します。デフォルト値は 8006 です。
   - **Repository**（リポジトリ）— エージェントからのデータを保存するためのリポジトリを選択します。

     メモ: 単一のリポジトリに複数のエージェントからのデータを保存することができます。
   - **Encryption Key**（暗号化キー）— リポジトリに保存されるこのマシン上の全ボリュームのデータに暗号化を適用するかどうかを指定します。

     メモ: リポジトリの暗号化設定は、Core Console の **Configuration**（設定）タブで定義します。
4. **Deploy**（展開）をクリックします。
   Deploy Agent（エージェントの展開）ダイアログボックスが閉じます。保護対象マシンのリストでの選択したエージェントの表示は遅れる場合があります。

保護スケジュールの理解

保護スケジュールは保護対象のエージェントマシンから AppAssure Core にいつバックアップを転送するかを定義します。

保護スケジュールは、まず最初に **Protect Machine Wizard**（マシンの保護ウィザード）または **Protect Multiple Machines Wizard**（複数マシンの保護ウィザード）を使用して定義します。その後、特定のエージェントマシンに対する既存のスケジュールを、サマリタブからいつでも変更することができます。

AppAssure は、定義済み期間での 2 つの保護スケジュールをデフォルトで提供します。第一期間は、平日（月～金）の単一時間帯（ 12:00 AM ～ 11:59 PM）が定義されています。デフォルトの間隔（スナップショ

ット間の間隔）は 3 時間です。第二期間は週末（土曜日と日曜日）です。第二期間でのデフォルト間隔は 3 時間です。

保護が初めて有効になると、スケジュールがアクティブ化されます。従って、デフォルトの設定を使用すると、その日の現在時刻に関係なく、最初のバックアップは 3 時間おきに発生することになります。

Core に保存された最初のバックアップ転送は、ベースイメージスナップショットと呼ばれます。指定されたボリューム上（オペレーティングシステム、アプリケーション、および設定を含む）すべてにある全データが Core に保存されます。その後、増分スナップショット（エージェントでの前回のバックアップからの変更分のみで構成される小規模バックアップ）が定義された間隔に基づいて定期的に Core に保存されます。

カスタムスケジュールを作成して、バックアップの頻度を変更することができます。たとえば、平日のバックアップの間隔を 60 分に変更して、1 時間おきにスナップショットを取ることができます。または、週末の間隔を 60 分から 180 分に引き上げて、トラフィックが少ないときにはスナップショットを 3 時間おきにすることができます。

Protection Schedule Wizard（保護スケジュールウィザード）ページ内のその他のオプションには、日次保護時間の設定があります。これにより、定義された時間に毎日 1 度バックアップが行われます（デフォルト設定は 12:00 PM です）。

保護を当初一時停止するオプションは、明示的に保護を再開するまでベースイメージの発生が妨げられます（実際、すべてのバックアップが妨げられます）。設定された保護スケジュールに基づいてマシンの保護を開始する準備が整ったら、保護を明示的に再開する必要があります。

カスタムスケジュールの作成

1. **Protect Machine**（マシンの保護）の **Protection Schedule**（保護スケジュール）ページ、または **Protect Multiple Machines Wizard**（複数マシンの保護ウィザード）で任意の期間のスケジュール間隔を変更するには、次の手順を実行します。
   a. **Periods**（期間）を選択します。
      既存の期間が表示され、変更できるようになります。編集可能なフィールドは、各期間の開始時刻、終了時刻、および間隔（分単位）です。
   b. 間隔のフィールドをクリックして、適切な間隔を分単位で入力します。
      たとえば、既存の間隔をハイライト表示して値を **60** と入力しなおして、この間隔で 60 分おきにスナップショットを実行します。
2. 平日のピークとオフピーク期間を作成するには、24 時間の期間を含まないように平日期間の時間範囲を変更します。ピーク時の最適な間隔を設定するには、**Take snapshots for the remaining time**（残りの時間にスナップショットを取る）を選択し、次の手順を実行して、オフピーク時の間隔を設定します。
   a. **Periods**（期間）を選択します。
      既存の期間が表示され、変更できるようになります。
   b. この期間の開始時刻を変更するには **From**（開始時刻）ボックスをクリックします。
      Choose Time（時間の選択）ダイアログボックスが表示されます。
   c. 希望する開始時間へ時間と分のスライダコントロールをドラッグして、**Done**（終了）をクリックします。現在の時刻で指定する場合は、**Now**（今すぐ実行）をクリックします。
   d. **To**（終了時刻）ボックスをクリックして、この期間の終了時刻を変更します。
      Choose Time（時間の選択）ダイアログボックスが表示されます。
   e. 希望する開始時間へ時間と分のスライダコントロールをドラッグして、**Done**（終了）をクリックします。現在の時刻で指定する場合は、**Now**（今すぐ実行）をクリックします。
3. バックアップが毎日一回発生するように設定するには、**Daily protection time**（日次保護時間） を選択して、時間を HH:MM AM（何時：何分 AM）の形式で入力します。

4. 最初のバックアップなしでスケジュールを定義するには、**Initially pause protection**（保護を当初一時停止）を選択します。

   ウィザードから保護を一時停止すると、明示的に再開するまで保護が一時停止状態のままとなります。保護を再開すると、設定したスケジュールに従ってバックアップが発生します。
5. **Finish**（終了）または **Next**（次へ）をクリックします。

保護スケジュールの変更

マシン上の特定のボリュームに対する保護スケジュールを変更できます。

保護スケジュールを変更するには、次の手順を実行します。

1. Core Console で、変更する定義済み保護スケジュールがあるマシンを選択します。

   Summary（サマリ）タブに、選択したマシンが表示されます。
2. 変更する保護対象マシンのボリュームを選択し、**Set a schedule**（スケジュールの設定）をクリックします。すべてのボリュームを一度に選択するには、ヘッダ列のチェックボックスをクリックします。

   当初、すべてのボリュームが同じ保護スケジュールを共有しています。一般的には、少なくともシステム予約済みボリュームとオペレーティングシステムのあるボリューム（通常は C ドライブ）を保護することが適切です。

   Protection Schedule（保護スケジュール）ダイアログボックスが表示されます。
3. 以前に保護スケジュールを作成したことがあり、そのテンプレートをこのエージェントに適用する場合は、**Protection Schedule**（保護スケジュール）ダイアログボックスでドロップダウンリストからそのテンプレートを選択して、手順 9 に進みます。
4. この新しい保護スケジュールをテンプレートとして保存する場合は、テキストボックスにテンプレートの名前を入力します。
5. スケジュールから既存の期間を削除する場合は、各期間オプションの横にあるチェックボックスをクリアします。オプションは次のとおりです。
   - **Mon - Fri.**（月曜日～金曜日）この時間の範囲は、一般的な週休二日制を意味します。
   - **Sat - Sun.**（土曜日～日曜日）この時間の範囲は、一般的な週末を意味します。
6. 平日開始で、開始時間と終了時間が 12:00 AM から 11:59 PM の場合は、単一の期間が存在することになります。定義済みの期間の開始時間または終了時間を変更するには、次の手順を実行します。
   a. 該当する期間を選択します。
   b. この期間の開始時間を変更するには **Start Time**（開始時間）ボックスをクリックします。
   c. 希望する開始時間へ時間と分のスライダコントロールをドラッグして、**Done**（終了）をクリックします。現在の時刻で指定する場合は、**Now**（今すぐ実行）をクリックします。
   d. この期間の終了時間を変更するには **Start Time**（終了時間）ボックスをクリックします。

      Choose Time（時間の選択）ダイアログボックスが表示されます。
   e. 希望する開始時間へ時間と分のスライダコントロールをドラッグして、**Done**（終了）をクリックします。現在の時刻で指定する場合は、**Now**（今すぐ実行）をクリックします。
   f. 間隔は必要に応じて変更してください。たとえば、ピーク期間を定義するには、間隔を 60 分から 20 分に変更して 1 時間に 3 回スナップショットを作成します。
7. 手順 6 で 12:00 AM ～ 11:59 PM 以外の時間を定義した場合に残り時間範囲内でバックアップを発生させるには、次の手順にを行って、保護を定義する追加期間を追加します。
   a. **+ Add period**（期間の追加）をクリックします。

      適切なカテゴリ（平日または週末）に、新しい期間が表示されます。最初の期間が 12:00 AM より後の開始になっている場合、AppAssure は自動的にこの期間を 12:00 に開始します。上の例と同様に、この 2 番目の期間は 12:00 AM に開始されます。開始および終了時間の時間と分を調整する必要がある場合があります。

b. 希望する開始時間と終了時間へ合わせるため。時間と分のスライダコントロールを適切にドラッグします。
c. 間隔は必要に応じて変更してください。たとえば、オフピーク期間を定義するには、間隔を 60 分から 120 分に変更して 2 時間ごとにスナップショットを作成します。

8. 必要な場合は、引き続き追加期間、開始時間、終了時間、および間隔を適切に設定します。

   メモ: 追加済みの期間を削除する場合は、その期間の右端にある **X** をクリックします。期間を間違って削除した場合は **Cancel**（キャンセル）をクリックできます。

9. 必要な保護スケジュールが設定できたら、**Apply**（適用）をクリックします。
   Protection Schedule（保護スケジュール）ダイアログボックスが閉じます。

保護対象マシンの設定

AppAssure でマシンに対する保護を追加した後は、基本的なマシン設定（名前、ホスト名など）、保護設定（マシン上ボリュームの保護スケジュールの変更、ボリュームの追加と削除、または保護の一時停止）、およびその他多くの変更を行うことができます。

構成設定の表示と変更

構成設定を表示して変更するには、次の手順を実行します。

1. Core Console から、変更するマシンに移動します。
2. **Configuration（設定）→ Settings（設定）**とクリックします。
3. **Change**（変更）をクリックして、次の表にあるマシン設定を変更します。

テキストボックス	説明
表示名	マシンの表示名を入力します。 Core Console に表示されるマシン用の名前です。デフォルトでは、マシンのホスト名になります。必要に応じて、表示名をユーザーフレンドリーな名前に変更できます。
ホスト名	マシンのホスト名を入力します。
ポート	マシンのポート番号を入力します。 Core は、このマシンと通信する際にデフォルトポート 8006 を使用します。
暗号化キー	必要に応じて暗号化キーを編集します。リポジトリに保存されている、マシン上のすべてのボリュームのデータに暗号化を適用するかどうかを指定します。
リポジトリ	リカバリポイント用のリポジトリを選択します。このマシンからのデータを保存する Core のリポジトリを表示します。 **メモ:** この設定は、リカバリポイントがない場合、または以前のリポジトリが欠落している場合にのみ変更できます。

マシンのシステム情報の表示

Core Console に、すべての保護対象マシンが表示されます。

マシンのシステム情報を表示するには、次の手順を実行します。

1. Core Console の左側のナビゲーションエリアで、 **Protected Machines**（保護対象マシン）から詳細なシステム情報を表示するマシンを選択します。
2. **Tools**（ツール）タブをクリックします。

   System Information（システム情報）タブが以下の情報を表示します。

   - ホスト名
   - OS バージョン
   - OS アーキテクチャ
   - メモリ（物理）
   - 表示名
   - 完全修飾ドメインネーム
   - 仮想マシンのタイプ（該当する場合）

   このマシンに含まれるボリュームの詳細情報は、次のとおりです。

   - 名前
   - デバイス ID
   - File System
   - 容量（未処理、フォーマット済み、使用済みを含む）

   表示されるその他のマシン情報は次のとおりです。

   - プロセッサ
   - ネットワークアダプタ
   - このマシンに関連付けられた IP アドレス

ライセンス情報の表示

マシンにインストールされた AppAssure Agent ソフトウェアの現在のライセンスステータス情報を表示できます。
ライセンス情報を表示するには、次の手順を実行します。

1. Navigation（ナビゲーション）ペインで、表示するマシンを選択します。
2. **Configuration（設定）→ Licensing（ライセンス）**とクリックします。

   Status（ステータス）画面に、製品ライセンスの詳細が表示されます。

転送設定の変更

保護対象マシンのデータ転送プロセスを管理する設定を変更できます。本項で説明する転送設定は、エージェントレベルの設定です。コアレベルでの転送を設定するには、「転送キュー設定の変更」を参照してください。

注意: 転送設定を変更すると、AppAssure 環境に劇的な影響を与える可能性があります。転送設定値を変更する前に、Dell AppAssure Knowledge Base にある『Transfer Performance Tuning Guide』（転送パフォーマンスチューニングガイド）を参照してください。

DL1000 には、次の 3 つの転送タイプがあります。

スナップショット　保護対象マシン上のデータをバックアップする転送です。

VM Export（VM エクスポート）	マシンを保護するために定義されたスケジュールに指定されているとおりのバックアップ情報とパラメータのすべてを持つ仮想マシンを作成する転送タイプです。
復元	保護対象マシン上のバックアップ情報を復元するプロセスです。

DL1000 でのデータ転送には、AppAssure Agent マシンから Core までの、ネットワーク経由での大量のデータ転送が伴います。レプリケーションの場合、送信元またはソース Core からターゲット Core までの転送も発生します。

データ転送は、一部のパフォーマンスオプション設定を使用して、お使いのシステムに合わせた最適化を行うことができます。これらの設定により、エージェントマシンのバックアップ中、VM エクスポートの実行中、またはロールバックの実行中でのデータ帯域幅の使用量が制御されます。データ転送のパフォーマンスに影響する要因には次のものがあります。

- 同時エージェントデータ転送数
- 同時データストリーム数
- ディスク上のデータ変更量
- 使用可能なネットワーク帯域幅
- リポジトリディスクサブシステムのパフォーマンス
- データバッファリングに使用可能なメモリ量

ビジネスニーズへの最適な対応とお使いの環境に基づいたパフォーマンスの微調整を行うために、これらのパフォーマンスオプションを調整できます。

転送設定を変更するには、次の手順を実行します。

1. Core Console で、変更するマシンに移動します。
2. **Configuration**（設定）タブをクリックし、**Transfer Settings**（転送設定）をクリックします。
   現在の **Transfer Settings**（転送設定）ページが表示されます。
3. **Transfer Settings**（転送設定）ページで、**Change**（変更）をクリックします。
   Transfer Settings（転送設定）ダイアログボックスが表示されます。
4. 次の表の説明に従って、マシンに対する **Transfer Settings**（転送設定）オプションを入力します。

テキストボックス	説明
Priority（優先順位）	保護対象マシンの間で転送の優先順位を設定します。ほかの保護対象マシンとの比較で優先順位を割り当てることができます。1 が最高の優先順位となるように、1 から 10 までの数字を選択します。デフォルトの設定では、優先順位は 5 になります。 **メモ:** 優先順位はキューに入っている転送に適用されます。
Maximum Concurrent Streams（最大同時ストリーム）	Core に送信される TCP リンクが各エージェントで並列に処理される最大数を設定します。 **メモ:** この値は 8 に設定することを推奨します。パケットのドロップが発生する場合は、この設定を大きくします。

テキストボックス	説明
Maximum Concurrent Writes（最大同時書き込み）	エージェント接続あたりの同時ディスク書き込み操作の最大数を設定します。 **メモ:** この値は Maximum Concurrent Streams（最大同時ストリーム）に選択した値と同じに設定することを推奨します。パケット損失が発生する場合は、この値を少し小さくします。たとえば、Maximum Current Streams（最大同時ストリーム）が 8 に設定されている場合は、このオプションを 7 に設定します。
Maximum Retries（最大再試行回数）	操作の一部が完了しなかった場合に、保護されたマシンそれぞれに対して再試行する最大回数を設定します。
Maximum Segment Size（最大セグメントサイズ）	コンピュータが単一の TCP セグメントで受信できる最大データ量（バイト単位）を指定します。デフォルトの設定は 4194304 です。 **注意: このオプションはデフォルトの設定から変更しないでください。**
Maximum Transfer Queue Depth（転送キューの最大の深さ）	同時に送信可能なコマンドの数を指定します。お使いのシステムで同時入力 / 出力操作の数が大きい場合は、このオプションをより大きい値に調整できます。
Outstanding Reads per Stream（ストリームあたりの未処理の読み取り数）	バックエンドに保存されるキュー内の読み取り操作の数を指定します。この設定は、エージェントのキューイングの制御に利用できます。 **メモ:** この値は 24 に設定することを推奨します。
Excluded Writers（除外するライター）	除外するライターを選択します。リストに表示されるライターは、設定作業を行っているマシンに固有のものなので、一部のライターは表示されない可能性があります。表示される可能性のあるライターの一部を次に示します。 • ASR Writer（ASR ライター） • BITS Writer（BITS ライター） • COM+ REGDB Writer（COM+ REGDB ライター） • Performance Counters Writer（パフォーマンスカウンタライター） • Registry Writer（レジストリライター） • Shadow Copy Optimization Writer（シャドウコピー最適化ライター） • SQLServerWriter（SQL Server ライター） • System Writer（システムライター） • Task Scheduler Writer（タスクスケジューラライター） • VSS Metadata Store Writer（VSS メタデータストアライター） • WMI Writer（WMI ライター）
Transfer Data Server Port（データ転送サーバーポート）	転送用のポートを設定します。デフォルトの設定は 8009 です。

テキストボックス	説明
Transfer Timeout（転送タイムアウト）	パケットが転送されずに静止していられる時間を分と秒の単位で指定します。
Snapshot Timeout（スナップショットタイムアウト）	スナップショットの取得の最大待機時間を分と秒の単位で指定します。
Network Read Timeout（ネットワーク読み取りタイムアウト）	読み取り接続の最大待機時間を分と秒の単位で指定します。ネットワーク読み取りをその時間内に実行されないと、その操作は再試行されます。
Network Write Timeout（ネットワーク書き込みタイムアウト）	書き込み接続の最大待機時間を秒単位で指定します。ネットワーク書き込みをその時間内に実行されないと、その操作は再試行されます。

5. **OK** をクリックします。

データのアーカイブ

バックアップが短期（高速かつ高価な）メディアに保存される期間は保持ポリシーによって決定されます。特定のビジネス要件と技術要件によっては、これらのバックアップ保持期間の延長が必須となる場合がありますが、高速ストレージの使用はコストが高く現実的ではありません。従って、このような要件は、長期（低速かつ安価な）ストレージの必要を生じます。ビジネスでは、準拠データと非準拠データの両方のアーカイブに長期ストレージが頻繁に使用されます。AppAssure 5 のアーカイブ機能は、コンプライアンスデータと非コンプライアンスデータの保持期間の延長をサポートするために使用されます。また、リモートのレプリカコアにレプリケーションデータをシーディングするときにも使用されます。

アーカイブの作成

アーカイブを作成するには、次の手順を実行します。

1. Core Console で、**Tools （ツール） → Archive （アーカイブ） → Create （作成）** をクリックします。**Add Archive Wizard**（アーカイブの追加ウィザード）ダイアログボックスが表示されます。
2. **Add Archive Wizard**（アーカイブの追加ウィザード）の **Create**（作成）ページで、**Location Type**（場所のタイプ）ドロップダウンリストから、次のオプションのうち 1 つを選択します。
   - ローカル
   - ネットワーク
   - クラウド
3. 手順 3 で選択した場所のタイプに基づき、次の表の説明に従ってアーカイブの詳細を入力します。

表 2. アーカイブの作成

オプション	テキストボックス	説明
ローカル	Output Location（出力先）	出力先を入力します。これは、アーカイブを格納する場所のパス

オプション	テキストボックス	説明
		を定義するために使用されます。たとえば、d:\work\archive などです。
ネットワーク	Output Location（出力先）	出力先を入力します。これは、アーカイブを格納する場所のパスを定義するために使用されます。たとえば、\\servername \sharename などです。
	ユーザー名	ユーザー名を入力します。これは、ネットワーク共有のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。これは、ネットワーク共有のログオン資格情報を確立するために使用されます。
クラウド	Account（アカウント）	ドロップダウンリストからアカウントを選択します。 **メモ:** クラウドアカウントを選択するには、まずそのアカウントを Core Console を追加する必要があります。クラウドアカウントの追加を参照してください。
	Container（コンテナ）	ドロップダウンメニューからお使いのアカウント関連づけられているコンテナを選択します。
	フォルダ名	アーカイブされたデータを保存するフォルダの名前を指定します。デフォルトの名前は AppAssure-5-Archive-[作成日]-[作成時間] です。

4. **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、どの保護対象マシンにアーカイブするリカバリポイントが格納されているかを選択します。
6. **次へ** をクリックします。
7. **Options**（オプション）ページで、次の表の情報を入力します。

テキストボックス	説明
Maximum size（最大サイズ）	大規模なデータのアーカイブは複数のセグメントに分割することができます。次の操作のいずれかを行って、アーカイブ作成のために予約する容量の最大値を選択します。

テキストボックス	説明
	• Entire Target（ターゲット全体）を選択して、手順 4 で入力した出力先で提供されたパスで使用できる全ての容量を予約します（たとえば、場所が D:\work\archive である場合、D: ドライブで利用可能なすべての容量が予約されます）。 • 予約したい最大容量をカスタマイズするには、空のテキストボックスを選択し、上矢印と下矢印を使用して値を入力して、ドロップダウンメニューから値の単位を選択します。 **メモ:** Amazon のクラウドアーカイブは、自動的に 50 GB のセグメントに分割されます。Windows Azure のクラウドアーカイブは、自動的に 200 GB のセグメントに分割されます。
Recycle action（リサイクルアクション）	次のリサイクルアクションオプションのいずれかを選択します。 • **Do not reuse**（再使用しない）：その場所の既存データの上書き、またはクリアは行われません。その場所が空ではない場合、アーカイブの書き込みは失敗します。 • **Replace this core**（このコアを置き換える）：このコアに関連する既存アーカイブデータを上書きしますが、他のコアのデータはそのまま残します。 • **Erase Completely**（完全に消去）：新しいアーカイブを書き込む前に、そのディレクトリからすべてのアーカイブ済みデータを消去します。 • **Incremental**（差分）：既存アーカイブにリカバリポイントを追加することができますアーカイブ中にすでに存在しているデータとの重複を回避するため、リカバリポイントが比較されます。
Comment（コメント）	アーカイブに対して入手する必要がある追加情報を入力します。このコメントは、後でこのアーカイブをインポートする場合に表示されます。
Use compatible format（互換性のある形式を使用する）	このオプションを選択して、コアの過去のバージョンと互換性がある形式でデータをアーカイブします。 **メモ:** 新しい形式はより優れたパフォーマンスを提供しますが、古いコアとの互換性はありません。

8. **次へ** をクリックします。
9. Date Range（日付範囲）ページでは、アーカイブするリカバリポイントの Start Date（開始日）と Expiration Date（有効期限日）を入力します。
   - 時刻を入力するには、表示されている時刻（デフォルトは午前 8:00）をクリックして、時間と分を選択するためのスライドバーを表示します。
   - 日付を入力するには、テキストボックスをクリックしてカレンダーを表示し、目的の日付をクリックします。
10. **終了** をクリックします。

アーカイブのインポート

アーカイブをインポートするには、次の手順を実行します。

1. Core Console で、**Tools（ツール）** → **Archive（アーカイブ）** → **Import（インポート）**の順にクリックします。
2. **Location Type**（場所のタイプ）には、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。

- ローカル
- ネットワーク
- クラウド

3. 手順 3 で選択した場所のタイプに基づき、次の表の説明に従ってアーカイブの詳細を入力します。

表 3. アーカイブのインポート

オプション	テキストボックス	説明
ローカル	Output Location（出力先）	出力先を入力します。これは、アーカイブを格納する場所のパスを定義するために使用されます。たとえば、`d:\work\archiveea` などです。
ネットワーク	Output Location（出力先）	出力先を入力します。これは、アーカイブを格納する場所のパスを定義するために使用されます。たとえば、\\servername \sharename などです。
	ユーザー名	ユーザー名を入力します。これは、ネットワーク共有のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。これは、ネットワーク共有のログオン資格情報を確立するために使用されます。
クラウド	Account（アカウント）	ドロップダウンリストからアカウントを選択します。 **メモ:** クラウドアカウントを選択するには、まずそのアカウントを Core Console を追加する必要があります。クラウドアカウントの追加を参照してください。
	Container（コンテナ）	ドロップダウンメニューからお使いのアカウント関連づけられているコンテナを選択します。
	フォルダ名	アーカイブされたデータを保存するフォルダの名前を指定します。デフォルトの名前は AppAssure-5-Archive-[作成日]-[作成時間] です。

4. **Check File**（ファイルのチェック）をクリックして、インポートするアーカイブの存在を検証します。**Restore**（復元）ダイアログボックスが表示されます。
5. **Restore**（復元）ダイアログボックスで、ソースコアの名前を確認します。
6. アーカイブからインポートするエージェントを選択します。

7. リポジトリを選択します。
8. **Restore**（復元）をクリックして、アーカイブをインポートします。

クラウドへのアーカイブ

データを Core Console から直接さまざまなクラウドプロバイダにアップロードすることで、データをクラウド上にアーカイブすることができます。互換性のあるクラウドには、Windows Azure、Amazon、Rackspace、および OpenStack ベースの任意のプロバイダが含まれます。

アーカイブをクラウドにエクスポートするには、次の手順を実行します。

- お使いのクラウドアカウントを Core Console に追加します。詳細についてはクラウドアカウントの追加を参照してください。
- データをアーカイブし、それをクラウドアカウントにエクスポートします。
- アーカイブデータは、クラウドの場所からデータをインポートすることによって取得します。

システム診断の表示

AppAssure では、任意の保護対象マシンのマシンログデータを表示するために診断情報が利用できます。さらに、Core の診断情報を表示したり、アップロードしたりすることも可能です。

マシンログの表示

マシンに関するエラーや問題が発生したときは、ログを表示するとトラブルシューティングに役立つ場合があります。

マシンログを表示するには、次の手順を実行します。

1. Core Console で、**Tools（ツール）** → **Diagnostics（診断）** → **View Log（ログの表示）**とクリックします。

   Download Core Log（コアログのダウンロード）ページが表示されます。
2. **Click here to begin the download**（ここをクリックしてダウンロードを開始）を選択します。

   ファイルを開く、または保存するように警告するメッセージが表示されます。
3. ログファイルを処理するための希望方法を選択します。

マシンログのアップロード

1. Core Console で、**Tools（ツール）** → **Diagnostics（診断）** → **Upload Log（ログのアップロード）**とクリックします。

   Upload Log（ログのアップロード）ページが表示されます。
2. **Click here to begin the download**（ここをクリックしてアップロードを開始）を選択します。

   Events（イベント）タブに、Core、およびすべての保護対象マシンのログ情報のアップロード進捗状況が表示されます。

マシン上の操作のキャンセル

マシンに対して現在実行中の操作をキャンセルできます。現在のスナップショットをキャンセル、または現在のすべての操作（エクスポートおよびレプリケーションを含む）をキャンセルすることができます。

マシン上の操作をキャンセルするには、次の手順を実行します。

1. Core Console で、操作をキャンセルするマシンを選択します。
2. **Events**（イベント）で、キャンセルするイベントまたは操作のイベント詳細を展開します。
3. **Cancel**（キャンセル）をクリックします。

マシンのステータスおよびその他詳細の表示

マシンのステータスおよびその他詳細を表示するには、次の手順を実行します。

1. Core Console で、表示する保護対象マシンに移動します。

マシンの情報が **Summary**（サマリ）ページに表示されます。表示される詳細には、次の情報が含まれます。

- ホスト名
- 最後に取得したスナップショット
- 次に予定されているスナップショット
- 暗号化ステータス
- バージョン番号
- マウント可否チェックステータス
- Checksum チェックステータス
- 最後に実行されたログ切り捨て

このマシンに収容されているボリュームの詳細情報も表示されます。これには、次の情報が含まれます。

- 名前
- ファイルシステムタイプ
- 容量の使用率
- 現在のスケジュール
- 次回スナップショット
- 合計サイズ
- Used Space（使用容量）
- 空き容量

SQL Server がマシンにインストールされている場合、サーバーの詳細情報も表示されます。これには、次の情報が含まれます。

- オンラインステータス
- 名前
- インストールパス
- Version（バージョン）

Exchange Server がマシンにインストールされている場合、サーバーとメールストアの詳細情報も表示されます。これには、次の情報が含まれます。

- Version（バージョン）
- インストールパス
- Data Path（データパス）
- Name Exchange データベースのパス

- ログファイルのパス
- ログプレフィックス
- システムパス
- メールストアタイプ

複数マシンの管理

このトピックでは、複数の Windows マシンに対して AppAssure Agent ソフトウェアを同時に展開するために管理者が行うタスクについて説明しています。

複数のエージェントを展開して保護するには、次のタスクを実行します。

1. AppAssure を複数のマシンに展開。
   複数マシンへの展開を参照してください。
2. バッチ展開のアクティビティを監視します。
   複数マシンの展開の監視を参照してください。
3. 複数のマシンを保護します。
   複数マシンの保護を参照してください。

   メモ: 展開時に Protect Machine After Install（インストール後にマシンを保護する）オプションを選択した場合、この手順は省略できます。
4. バッチ保護のアクティビティを監視します。
   複数マシンの保護の監視を参照してください。

複数マシンへの展開

AppAssure の Bulk Deploy（一括展開）機能を使用することにより、AppAssure Agent ソフトウェアを複数の Windows マシンに展開するタスクをシンプル化できます。次のマシンに対する一括展開が可能です。

- VMware vCenter/ESXi 仮想ホスト上のマシン
- Active Directory ドメイン上のマシン
- その他のホスト上のマシン

Bulk Deploy（一括展開）機能は、ホスト上のマシンを自動的に検出し、それらの中から展開先となるマシンを選択することができます。その代わりに、ホストとマシンの情報を手動で入力することもできます。

メモ: AppAssure はウェブバージョンの AppAssure Agent Installer を使用してインストールコンポーネントを展開することから、展開するマシンにはビットデータをダウンロードしてインストールためのインターネットへのアクセスが必要です。インターネットにアクセスできない場合は、Core マシンから AppAssure Agent インストールプログラムをプッシュできます。Core とエージェントのアップデートはライセンスポータルからダウンロードできます。

複数マシンの展開の監視

複数マシンに対する AppAssure Agent ソフトウェア展開の進捗状況を表示することができます。

複数マシンの展開を監視するには、次の手順を実行します。

1. Core Console で **Events（イベント）** → **Alerts（アラート）** とクリックします。
2. AppAssure Core Home タブに移動して **Events** （イベント）タブをクリックします。

アラートイベントがリストに表示され、イベントが開始された時刻とメッセージを表示します。正常に展開された各 Agent ソフトウェアについて、保護対象マシンが追加されたことを示すアラートが表示されます。

3. オプションとして、保護対象マシンへの任意のリンクをクリックします。
   選択したマシンの Summary（サマリ）タブが表示され、次を含む関連情報を表示します。
   - 保護対象マシンのホスト名
   - 最後のスナップショット（該当する場合）
   - 選択した保護スケジュールに基づいた次回スナップショットのスケジュール時間
   - 残り時間
   - この保護対象エージェントで使用される暗号化キー（存在する場合）
   - Agent ソフトウェアのバージョン

複数マシンの保護

AppAssure Agent ソフトウェアを Windows マシンに一括導入した後は、データを保護するためにマシンを保護する必要があります。エージェントの展開時に **Protect Machine After Install**（インストール後にマシンを保護する）を選択した場合は、この手順を省略できます。

メモ: エージェントマシンには、リモートインストールを可能にするセキュリティポリシーが設定されている必要があります。

複数のマシンを保護するには、次の手順を実行します。

1. Core Console で、**Protect（保護） → Bulk Protect（一括保護）**とクリックします。
   Protect Multiple Machines Wizard（複数マシンの保護ウィザード）ウィンドウが表示されます。
2. 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。
   - 今後 Protect Machine Wizard（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. **次へ** をクリックします。
   Connection（接続）ページが表示されます。
4. 次のいずれかのオプションをクリックして、保護するマシンを追加します。
   - **Active Directory** をクリックして Active Directory ドメイン上のマシンを指定します。下の表の説明どおりに資格情報を入力し、**Next**（次へ）をクリックします。
   - **vCenter/ESXi** をクリックして vCenter/ESXi 仮想ホスト上の仮想マシンを指定します。下の表の説明どおりに資格情報を入力し、**Next**（次へ）をクリックします。

テキストボックス	説明
Host（ホスト）	Active Directory ドメインまたは VMware vCenter Server/ESX(i) 仮想ホストのホスト名または IP アドレスです。
ユーザー名	このマシンに接続するためのユーザー名（Administrator など）を入力します。
パスワード	このマシンに接続するためのセキュアなパスワードを入力します。

   - 手動でマシンを追加するには、**Add the machines manually**（手動でマシンを追加する）を選択して **Next**（次へ）をクリックします。
5. **Machines**（マシン）ページでマシンを手動で指定するには、別の行に各マシンの接続詳細 `hostname::username::password::port` を入力してから、**Next**（次へ）をクリックします。

6. **Machines**（マシン）ページで、Active Directory ドメインまたは VMware vCenter/ESX(i) 仮想ホストから認識されたマシンを指定するには、該当する保護対象の各マシンをリストから選択し、**Next**（次へ）をクリックします。

   システムが追加した各マシンを自動的に検証し **Protection**（保護）ページが表示されます。

7. **Protection**（保護）ページで、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、**Schedule Settings**（スケジュール設定）オプションで **Default protection (hourly snapshots of all volumes)**（デフォルト保護（全ボリュームの 1 時間ごとのスナップショット））を選択します。
   - 別の保護スケジュールを定義する場合は、Schedule Settings（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、**Next**（次へ）をクリックします。
8. 次のように設定を行います。
   - **Protect Multiple Machines Wizard**（複数マシンの保護ウィザード）で Typical（標準）設定およびデフォルト保護を選択した場合は、**Finish**（終了）を選択して選択内容を確定し、ウィザードを終了して指定したマシンを保護します。
   - **Protect Multiple Machines Wizard**（複数マシンの保護ウィザード）で Typical（標準）設定を選択して、カスタム保護を指定した場合は、**Next**（次へ）をクリックしてカスタムスケジュールを設定します。
   - Protect Machine Wizard（マシンの保護ウィザード）で Advanced（詳細）設定を選択した場合は、**Next**（次へ）をクリックして手順 9 に進み、リポジトリと暗号化オプションを表示します。
9. **Repository**（リポジトリ）ページで、**Use an existing repository**（既存リポジトリの使用）を選択します。
10. **次へ** をクリックします。

    Encryption（暗号化）ページが表示されます。

11. 暗号化を有効にするには、**Encryption**（暗号化）ページで **Enable Encryption**（暗号化の有効化）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: 暗号化を有効にした場合、保護用に指定したマシンに対するすべての保護対象ボリュームのデータに適用されます。Core Console の **Configuration**（設定）タブで後ほど設定を変更することができます。暗号化についての詳細は、セキュリティの管理を参照してください。

12. 次の表で説明されているとおりに情報を入力して、Core 用の暗号化キーを追加します。

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。
説明	暗号キーに関する追加の詳細情報を提供する説明文を入力します。
Passphrase (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。
Confirm Passphrase (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。

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

複数マシンの保護の監視

AppAssure がマシンに対して保護ポリシーおよびスケジュールを適用する進捗状況を監視することができます。

複数マシンの保護を監視するには、Core Console Home タブに移動して **Events**（イベント）をクリックします。

Events（イベント）タブは、タスク、アラート、およびイベントを表示します。ボリュームが転送されると、ステータス、開始時間、終了時間がタスクペインに表示されます。タスクをステータス（アクティブ、待機中、完了、失敗）でフィルタすることもできます。

各保護対象マシンが追加されるたびに、操作が正常に行われたかどうか、またはエラーがログされたかどうかを示すアラートがログされます。

4

データのリカバリ

リカバリの管理

AppAssure Core では、リカバリポイントから物理または仮想マシンに対して、データの回復またはマシンの復元を瞬時に行うことができます。リカバリポイントには、ブロックレベルでキャプチャされたエージェントボリュームスナップショットが含まれます。これらのスナップショットはアプリケーションアウェアであり、すべての未処理トランザクションと進行中トランザクションのログが完了し、キャッシュがディスクにフラッシュされてから、スナップショットが作成されます。アプリケーションアウェアのスナップショットと Verified Recovery を使用することにより、次を含む複数のタイプのリカバリを Core で実行できます。

- ファイルとフォルダのリカバリ
- Live Recovery を使用したデータボリュームのリカバリ
- Live Recovery を使用した Microsoft Exchange Server および Microsoft SQL Server のデータボリュームのリカバリ
- Universal Recovery を使用したベアメタル復元
- Universal Recovery を使用した異種ハードウェアへのベアメタル復元
- 仮想マシンへのアドホックおよび継続エクスポート

スナップショットとリカバリポイントの管理

リカバリポイントは、個々のディスクボリュームに対して取得されたスナップショットの集合体であり、リポジトリに保存されます。スナップショットは、データを生成するアプリケーションの使用中に所定のポイントインタイムでのディスクボリュームの状態を取得して保存します。AppAssure では、スナップショットの強制実行、スナップショットの一時停止、およびリポジトリ内の現在のリカバリポイントのリストの表示を行うことができる他、必要に応じてそれらを削除することもできます。リカバリポイントは、保護対象マシンの復元、またはローカルファイルシステムへのマウントに使用されます。

AppAssure がキャプチャするスナップショットは、ブロックレベルで行われ、アプリケーションアウェアです。したがって、スナップショットが作成される前に、未開始トランザクションと進行中トランザクションすべてのログが完了され、キャッシュがディスクにフラッシュされることになります。

AppAssure は、低レベルのボリュームフィルタドライバを使用します。このドライバは、マウントされているボリュームにアタッチされ、次回のスナップショットのためにブロックレベルの変更をすべて追跡します。アプリケーションクラッシュ整合なスナップショットの促進しは Microsoft Volume Shadow Services (VSS) が使用されます。

リカバリポイントの表示

リカバリポイントを表示するには、次の手順を実行します。

1. Core Console の左のナビゲーションエリアで、リカバリポイントを表示するマシンを選択し、**Recovery Points**（リカバリポイント）タブをクリックします。

次の表の説明に従って、マシンに関するリカバリポイントの情報を表示することができます。

情報	説明
ステータス	リカバリポイントの現在のステータスを示します。
暗号化済み	リカバリポイントが暗号化されているかどうかを示します。
内容	リカバリポイントに含まれているボリューム一覧を示します。
タイプ	ベースまたは差分としてリカバリポイントを定義します。
作成日	リカバリポイントが作成された日付を表示します。
Size（サイズ）	リポジトリ内でリカバリポイントが消費する容量を表示します。

特定のリカバリポイントの表示

特定のリカバリポイントを表示するには、次の手順を実行します。

1. Core Console の左側にあるナビゲーションエリアで、リカバリポイントを表示するマシンを選択し、**Recovery Points**（リカバリポイント）を選択します。
2. リスト内のリカバリポイントの横にある **>** をクリックして表示を展開します。
   選択したマシンのリカバリポイントの内容についてさらに詳細な情報を表示できるだけでなく、次の表に説明されているリカバリポイントで実行可能な各種操作にもアクセスできます。

情報	説明
処置	**Actions**（アクション）メニューには、選択したリカバリポイントに対して実行できる次の操作が含まれています。 **Mount**（マウント） — 選択したリカバリポイントをマウントするには、このオプションを選択します。選択したリカバリポイントのマウントの詳細については、Windows マシンのリカバリポイントのマウントを参照してください。 **Export**（エクスポート） — Export（エクスポート）オプションで、選択したリカバリポイントを ESXi、VMware ワークステーション、または HyperV にエクスポートできます。 **Restore**（復元） — このオプションを選択して、選択したリカバリポイントから指定するボリュームへの復元を実行します。
内容	Contents（内容）エリアには、各ボリュームの次の情報をリストした、拡張リカバリポイント内の各ボリュームの列があります。 **Status**（ステータス）はリカバリポイントの現在のステータスを示します。 **Title**（タイトル）はリカバリポイント内の特定のボリュームをリストします。 **Size**（サイズ）はリポジトリ内でリカバリポイントが消費する容量を表示します。

3. 選択したリカバリポイント内のボリュームの横にある **>** をクリックして表示を展開します。

展開されたリカバリポイント内で選択したボリュームについて、次の表に説明されている情報を表示できます。

テキストボックス	説明
Title（タイトル）	リカバリポイント内の特定のボリュームを示します。
Raw Capacity（未処理容量）	ボリューム全体で未処理のストレージ容量を示します。
Formatted Capacity（フォーマット済み容量）	フォーマット後のボリューム上でデータに使用可能なストレージ容量を示します。
使用済み容量	ボリューム上で現在使用されているストレージ容量を示します。

Windows マシンへのリカバリポイントのマウント

AppAssure では、ローカルファイルシステムを介して保存データにアクセスするため、Windows マシンにリカバリポイントをマウントすることができます。

Windows マシンにリカバリポイントをマウントするには、次の手順を実行します。

1. Core Console から、ローカルファイルシステムにマウントするマシンを選択します。
   選択したマシンの **Summary**（サマリ）タブが表示されます。
2. **Recovery Points**（リカバリポイント）タブを選択します。
3. リカバリポイントのリストで、**>** をクリックしてマウントするリカバリポイントを展開します。
4. そのリカバリポイントに対して展開された詳細情報内で、**Mount**（マウント）をクリックします。
   Mount Recovery Points（リカバリポイントのマウント）ダイアログボックスが表示されます。
5. 次の表の説明に従って、**Mount**（マウント）ダイアログボックスで、リカバリポイントのマウントに関するテキストボックスを編集します。

テキストボックス	説明
Mount Location: Local Folder（マウントの場所 : ローカルフォルダ）	マウントされたリカバリポイントへのアクセスに使用するパスを指定します。
Volume Images（ボリュームイメージ）	マウントするボリュームイメージを指定します。
Mount Type（マウントタイプ）	マウントされたリカバリポイントのデータにアクセスする方法を指定します。 • Mount Read-only（読み取り専用のマウント）。 • Mount Read-only with previous writes（以前の書き込みで読み取り専用のマウント）。 • Mount Writable（書き込み可能のマウント）。
Create a Windows share for this Mount（このマウント用に Windows 共有を作成する）	オプションとして、マウントされたリカバリポイントを共有できるかどうかを指定するチェックボックスを選択して、共有名やアクセスグループを含むリカバリポイントへのアクセス権を設定します。

6. **Mount**（マウント）をクリックして、リカバリポイントをマウントします。

選択したリカバリポイントのマウント解除

選択したリカバリポイントをマウント解除するには、次の手順を実行します。

1. Core Console へ移動して **Tools（ツール）** → **Mounts（マウント）**とクリックします。
2. **Local Mounts**（ローカルマウント）のページで、マウント解除するリカバリポイントのマウントポイントの横にある **Dismount**（マウント解除）をクリックします。
3. Dismounting the Recovery Point（リカバリポイントのマウント解除）ウィンドウで、**Yes**（はい）をクリックして確定します。

すべてのリカバリポイントのマウント解除

すべてのリカバリポイントをマウント解除するには、次の手順を実行します。

1. Core Console へ移動して **Tools（ツール）** → **Mounts（マウント）**とクリックします。
2. **Local Mounts**（ローカルマウント）ページで、**Dismount All**（すべてをマウント解除）をクリックします。
3. **Dismounting the Recovery Point**（リカバリポイントのマウント解除）ウィンドウで、**Yes**（はい）をクリックして確定します。

Linux マシンへのリカバリポイントのマウント

AppAssure の **aamount** ユーティリティを使用して、Linux マシン上で、リカバリポイントからローカルボリュームとしてボリュームをリモートでマウントできます。

1. リカバリポイントをマウントするための新しいディレクトリを作成します（**mkdir** コマンドなどを使用します）。
2. 作成したディレクトリが存在することを確認します（**ls** コマンドなどを使用します）。
3. AppAssure の **aamount** ユーティリティを root として、またはスーパーユーザーとして実行します。（例：**sudo aamount**）
4. AppAssure のマウントプロンプトで、コマンド **lm** を入力して保護対象マシンのリストを表示します。
5. プロンプトが表示されたら、Core サーバーの IP アドレスまたはホスト名を入力します。
6. Core サーバーのログオン資格情報であるユーザー名とパスワードを入力します。

   AppAssure サーバーによって保護されているマシンのリストが表示されます。各マシンは、マシンのラインアイテム番号、ホスト / IP アドレス、ID 番号によって識別されています（例：293cc667-44b4-48ab-91d8-44bc74252a4f）。
7. コマンド **lr <line_number_of_machine>** を入力して、指定したマシン用に使用できるリカバリポイントのリストを表示します。
8. コマンド **m <volume_recovery_point_ID_number> <path>** を入力して、指定したリカバリポイントを選択し、それを指定したマウントポイント / パスにマウントします。
9. マウントが正常に行われたかどうかを確認するには、連結されたリモートボリュームのリストを表示する **l** コマンドを入力します。

リカバリポイントの削除

特定のマシンのリカバリポイントをリポジトリから簡単に削除することができます。AppAssure でリカバリポイントを削除する場合は、次のいずれかのオプションを指定できます。

テキストボックス	説明
Delete All Recovery Points（すべてのリカバリポイントを削除）	選択したエージェントマシンのすべてのリカバリポイントをリポジトリから削除します。
Delete a Range of Recovery Points（一定範囲のリカバリポイントを削除）	現在より前からベースイメージまでの指定範囲のすべてのリカバリポイント、つまりマシン上のすべてのデータおよび、現在から次のベースイメージまでのすべてのリカバリポイントを削除します。

メモ: 削除したリカバリポイントを元に戻すことはできません。

リカバリポイントを削除するには、次の手順を実行します。

1. Core Console の左のナビゲーションエリアで、リカバリポイントを表示するマシンを選択し、**Recovery Points**（リカバリポイント）タブをクリックします。
2. **Actions**（アクション）メニューをクリックします。
3. 次のオプションのいずれかを選択します。
   - 現在保存されているすべてのリカバリポイントを削除するには、**Delete All**（すべて削除）をクリックします。
   - 特定のデータ範囲内のリカバリポイントをまとめて削除するには、**Delete Range**（削除範囲）をクリックします。**Delete**（削除）ダイアログボックスが表示されます。**Delete Range**（削除範囲）ダイアログボックスで、削除するリカバリポイントの範囲を開始日時と終了日時を使用して指定し、**Delete**（削除）をクリックします。

孤立リカバリポイントチェーンの削除

孤立リカバリポイントとは、ベースイメージに関連付けられていない増分スナップショットです。後続のスナップショットは、このリカバリポイント上に引き続き構築されます。ベースイメージなしでは作成されたリカバリポイントが不完全となり、リカバリを完了するために必要なデータが不足している可能性が高くなります。これらのリカバリポイントは、孤立リカバリポイントチェーンの一部であると見なされます。この状況が発生する場合の最善の解決策は、チェーンを削除し、新しいベースイメージを作成することです。ベースイメージの強制の詳細については、スナップショットの強制を参照してください。

メモ: 孤立リカバリチェーンを削除する機能は、ターゲットコア上の複製リカバリポイントには使用できません。

孤立リカバリポイントチェーンを削除するには、次の手順を実行します。

1. Core Console で、孤立リカバリポイントチェーンを削除する保護対象マシンを選択します。
2. **Recovery Points**（リカバリポイント）タブをクリックします。
3. **Recovery Points**（リカバリポイント）で、孤立リカバリポイントを展開します。
   このリカバリポイントの **Type**（タイプ）列には **Incremental Orphaned**（孤立した増分）というラベルが表示されています。
4. **Actions**（アクション）の横にある **Delete**（削除）をクリックします。
   Delete Recovery Points（リカバリポイントを削除）ウィンドウが表示されます。
5. **Delete Recovery Points**（リカバリポイントの削除）ウィンドウで、**Yes**（はい）をクリックします。

注意: このリカバリポイントを削除すると、次のベースイメージまでの以前と以後の増分リカバリポイントも含まれるリカバリポイントチェーン全体が削除されます。この操作は取り消すことができません。

スナップショットの強制実行

スナップショットを強制実行することにより、現在の保護対象マシンに対してデータ転送を強制実行できます。スナップショットを強制実行する場合、転送はただちに開始されるか、キューに追加されます。以前のリカバリポイントから変更されたデータのみが転送されます。前のリカバリポイントがない場合は、保護対象ボリューム上のすべてのデータが転送されます。これは、ベースイメージと呼ばれます。

スナップショットを強制実行するには、次の手順を実行します。

1. Core Console で、スナップショットを強制実行するリカバリポイントを持つマシンまたはクラスタを選択します。
2. **Volumes**（ボリューム）のセクションの **Summary**（サマリ）タブをクリックしてから、次に説明されるオプションのいずれかを選択します。
   - **Force Snapshot**（スナップショットの強制）- 最後のスナップショット以降に更新されたデータの増分スナップショットを取得します。
   - **Force Base Image**（ベースイメージの強制）- マシンのボリューム上のすべてのデータの完全なスナップショットを取得します。
3. スナップショットがキュー登録されたという通知が **Transfer Status**（転送ステータス）ダイアログボックスに表示されたら、**OK** をクリックします。

   Machines（マシン）タブ内のマシンの横には、スナップショットの進捗状況を示すプログレスバーが表示されます。

データの復元

AppAssure を使用すると、Windows マシンの保存されたリカバリポイントから物理マシン（Windows または Linux マシンの場合）または仮想マシンにデータを瞬時に回復カバリまたは復元できます。本項の各トピックでは、Windows マシンの特定のリカバリポイントを仮想マシンにエクスポート、またはマシンを以前のリカバリポイントにロールバックする方法について説明します。

2 つのコア（ソースとターゲット）間にレプリケーションがセットアップされている場合、最初のレプリケーションが完了した後でのみ、ターゲットコアからデータをエクスポートすることが可能になります。

Windows マシンから仮想マシンへの保護対象データのエクスポートについて

AppAssure では、仮想マシンへの Windows バックアップ情報の 1 回限りのエクスポートまたは連続エクスポートの両方（仮想スタンバイをサポートするため）がサポートされています。仮想スタンバイマシンにデータをエクスポートすることにより、データの高可用性コピーが提供されます。保護対象マシンがダウンしても、仮想マシンを起動してからリカバリを実行することが可能になります。

次の図は、データを仮想マシンにエクスポートするための一般的な導入を示しています。

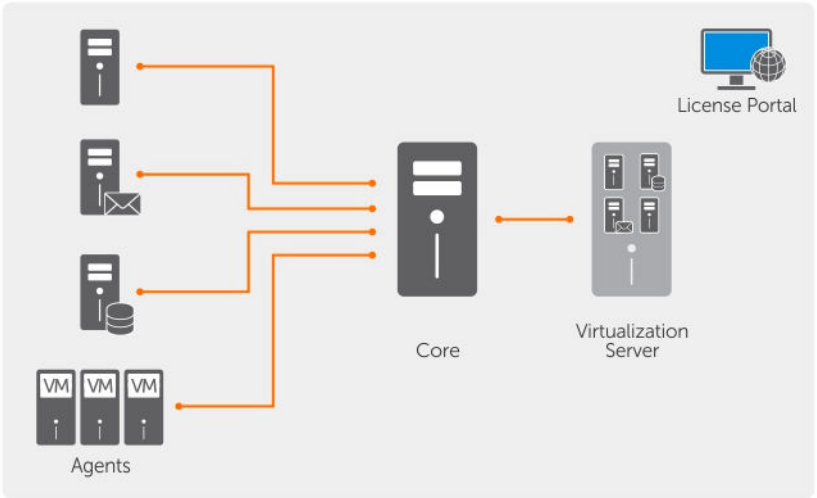

図 4. 仮想マシンへのデータのエクスポート

仮想スタンバイは、保護対象データを Windows マシンから仮想マシンへ継続的にエクスポートすることにより作成されます。仮想マシンにエクスポートするときに、リカバリポイントのすべてのバックアップデータと、マシンの保護スケジュールに定義されているパラメータがエクスポートされます。

保護対象 Windows マシンまたは Linux マシンのリカバリポイントの仮想エクスポートは、VMware、ESXi、Hyper-V、および Oracle VirtualBox に対して実行できます。

メモ: Appliance（アプライアンス）タブに、Hyper-V および ESXi 仮想マシンの管理のみをサポートするすべての仮想マシンが表示されます。他の仮想マシンを管理するには、ハイパーバイザー管理ツールを使用します。

メモ: エクスポート先の仮想マシンは、ESXi、VMware Workstation、または Hyper-V のライセンスバージョンである必要があります。試用版や無償版にはエクスポートできません。

動的および標準ボリュームサポートの制限事項

Dell AppAssure は、すべての動的ボリュームおよび標準ボリュームのスナップショットの取得をサポートしています。また、単一の物理ディスク上にあるシンプル動的ボリュームのエクスポートもサポートしています。シンプル動的ボリュームは、ストライピング、ミラーリング、スパニングされたボリュームではありません。

動的ディスク（上で説明したシンプル動的ディスクを除く）は、Export Wizard（エクスポートウィザード）での選択肢にはありません。非シンプルな動的ボリュームには、完全に解釈できない任意のディスクジオメトリがあるため、AppAssure は複雑または非シンプル動的ボリュームのエクスポートをサポートしていません。

エクスポートの管理

Core Console の **Virtual Standby**（仮想スタンバイ）タブで、仮想スタンバイの 1 回限りのエクスポートおよび連続エクスポートを含む、セットアップ済みのエクスポートのステータスを表示することができます。このタブでは、エクスポートの一時停止、停止、削除、または次回のエクスポートのキューの表示によってエクスポートを管理することができます。

メモ: 1 回限りのエクスポートと連続エクスポート（仮想スタンバイ）の機能がサポートされるのは、2 つの VM を持つ 3 TB の構成の Dell DL1000 のみです。

1. Core Console で、**Virtual Standby**（仮想スタンバイ）タブに移動します。
   Virtual Standby（仮想スタンバイ）タブでは、次の表で説明する情報が含まれる保存済みのエクスポート設定の表を表示できます。

メニュー	説明
ステータス	**メモ:** 仮想スタンバイ設定のステータスは、アイコンの色によって定義されています。 緑色 – 仮想スタンバイは正常に設定されており、アクティブで一時停止されていません。次の仮想スタンバイエクスポートは次のスナップショットの後に実行されます。 黄色 – 仮想スタンバイはコアによって保存されていますが、一時停止になっています。ただし新しい転送後もエクスポートジョブが自動的に開始されず、このエージェントに対する新しい仮想スタンバイエクスポートはなくなります。
Machine Name（マシン名）	ソースマシンの名前です。
送信先	データがエクスポートされる仮想マシンおよびパスです。
エクスポートタイプ	エクスポートの仮想マシンプラットフォームのタイプ（ESXi、VMware、Hyper-V、または VirtualBox など）です。
Last Export（最後のエクスポート）	最後のエクスポートの日付と時間です。エクスポートが追加されたばかりで、まだ完了していない場合は、エクスポートがまだ実行されていないというメッセージが表示されます。エクスポートに失敗した場合、またはエクスポートがキャンセルされた場合は、対応するメッセージも表示されます。

2. 保存済みのエクスポート設定を管理するには、エクスポートを選択して、次のいずれかをクリックします。
   - **Pause**（一時停止）：エクスポートを一時停止します。
   - **Resume**（再開）：一時停止状態のエクスポートを再開します。
   - **Force**（強制）：新しいエクスポートを強制します。このオプションは、仮想スタンバイが一時停止された後に再開された場合、つまり新しい転送後にのみエクスポートジョブが再開されるときに便利です。 新しい転まで待ちたくない場合は、エクスポートを強制することができます。
3. エクスポートをシステムから削除するには、**Remove**（削除）をクリックします。エクスポートを削除すると、システムから恒久的に削除され、再開できなくなります。
4. 現在キューに入っている完了予定のアクティブなエクスポートについての詳細を表示するには、**Show Export Queue**（エクスポートキューの表示）をクリックします。
   次の表が表示されます。

メニュー	説明
Machine Name（マシン名）	ソースマシンの名前です。

メニュー	説明
送信先	仮想スタンバイは正常に設定されており、アクティブで一時停止されていません。次の仮想スタンバイエクスポートは次のスナップショットの後に実行されます。
エクスポートタイプ	仮想スタンバイはコアによって保存されていますが、一時停止になっています。ただし新しい転送後もエクスポートジョブが自動的に開始されず、このエージェントに対する新しい仮想スタンバイエクスポートはなくなります。
Schedule Type（スケジュールタイプ）	1 回限りまたは連続のいずれかのエクスポートタイプです。
ステータス	エクスポートの進捗状況が進捗状況バーにパーセントで表示されます。

Windows マシンから仮想マシンへのバックアップ情報のエクスポート

リカバリポイントからのバックアップ情報の他、お使いのマシンの保護スケジュール用に定義されたパラメータをすべてエクスポートすることにより、Windows マシンからのデータを仮想マシン（VMware、ESXi、および Hyper-V）にエクスポートすることができます。

メモ: 1 回限りのエクスポートと連続エクスポート（仮想スタンバイ）の機能がサポートされるのは、2 つの VM を持つ 3 TB の構成の Dell DL1000 のみです。

Windows バックアップ情報を仮想マシンにエクスポートするには、次の手順を実行します。

1. Core Console で **Protected Machines**（保護対象マシン）タブをクリックします。
2. 保護対象マシンのリストから、エクスポートするリカバリポイントを持つマシンまたはクラスタを選択します。
3. そのマシンに対する **Actions**（アクション）ドロップダウンメニューで **Export**（エクスポート）をクリックし、実行するエクスポートのタイプを選択します。次のオプションから選択できます。
   - One-time（1 回限り）
   - Virtual Standby（仮想スタンバイ）

   Export Wizard（エクスポートウィザード）ダイアログボックスが表示されます。

ESXi エクスポートを使用した Windows データのエクスポート

AppAssure では、1 回限りのエクスポート、または連続エクスポートを実行することにより、ESXi エクスポートを使用したデータのエクスポートを選択できます。

1 回限りの ESXi エクスポートの実行

1 回限りの ESXi エクスポートを実行するには、次の手順を実行します。

1. Core Console で、エクスポートするマシンに移動します。
2. **Summary**（サマリ）タブで、**Actions（アクション）→ Export（エクスポート）→ One-time（1 回限り）**とクリックします。

   Export Wizard（エクスポートウィザード）が **Protected Machines**（保護マシン）ページに表示されます。
3. エクスポートするマシンを選択して、**Next**（次へ）をクリックします。
4. **Recovery Points**（リカバリポイント）のページで、エクスポートするリカバリポイントを選択し、**Next**（次へ）をクリックします。

ESXi エクスポートを実行するための仮想マシン情報の定義

ESXi エクスポートを実行するために仮想マシン情報を定義するには、次の手順を実行します。

1. **Export Wizard**（エクスポートウィザード）の **Destination**（宛先）ページで、**Recover to a Virtual Machine**（仮想マシンへの復元）ドロップダウンメニューから **ESXi** を選択します。
2. 仮想マシンにアクセスするためのパラメータを次の説明に従って入力します。

テキストボックス	説明
ホスト名	ホストマシンの名前を入力します。
ポート	ホストマシンのポートを入力します。デフォルトポートは 443 です。
ユーザー名	ホストマシンのログオン資格情報を入力します。
パスワード	ホストマシンのログオン資格情報を入力します。

3. **Virtual Machine Options**（仮想マシンオプション）ページで、次の表で説明されている情報を入力します。

テキストボックス	説明
Resource Pool（リソースプール）	ドロップダウンリストからリソースプールを選択します。
Data Store（データストア）	ドロップダウンリストからデータストアを選択します。
Virtual Machine Name（仮想マシン名）	仮想マシンの名前を入力します。
メモリ	メモリ使用率を指定します。
ディスクプロビジョニング	ディスクプロビジョニングのタイプを Thin（シン）または Thick（シック）から選択します。
Disk Mapping（ディスクマッピング）	ディスクマッピングのタイプを Automatic（自動）または Manual（マニュアル）のどちらかに指定します。
Version（バージョン）	仮想マシンのバージョンを選択します。

4. **次へ** をクリックします。
5. **Volumes**（ボリューム）ページで、エクスポートするボリュームを選択して **Next**（次へ）をクリックします。
6. **Summary**（サマリ）ページで、**Finish**（終了）をクリックしてウィザードを完了し、エクスポートを開始します。

メモ: Virtual Standby（仮想スタンバイ）または **Events**（イベント）タブを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

連続（仮想スタンバイ）ESXi エクスポートの実行

連続（仮想スタンバイ）ESXi エクスポートを実行するには、次の手順を実行します。

1. Core Console で、次のいずれかを実行します。
   - Virtual Standby（仮想スタンバイ）タブで **Add**（追加）をクリックして **Export Wizard**（エクスポートウィザード）を起動します。**Export Wizard**（エクスポートウィザード）の **Protected Machines**（保護対象マシン）ページで、エクスポートする保護対象マシンを選択して、**Next**（次へ）をクリックします。
   - エクスポートするマシンに移動して、**Actions（アクション）** → **Export（エクスポート）** → **Virtual Standby（仮想スタンバイ）**とクリックします。
2. **Export Wizard**（エクスポートウィザード）の **Destination**（宛先）ページで、**Recover to a Virtual Machine**（仮想マシンへの復元）ドロップダウンメニューから **ESXi** を選択します。
3. 次の表の説明に従って、仮想マシンへのアクセスのための情報を入力し、**Next**（次へ）をクリックします。

テキストボックス	説明
ホスト名	ホストマシンの名前を入力します。
ポート	ホストマシンのポートを入力します。デフォルトは 443 です。
ユーザー名	ホストマシンのログオン資格情報を入力します。
パスワード	ホストマシンのログオン資格情報を入力します。

4. **Virtual Machine Options**（仮想マシンオプション）ページで、次の表で説明されている情報を入力します。

テキストボックス	説明
Resource Pool（リソースプール）	ドロップダウンリストからリソースプールを選択します。
Data Store（データストア）	ドロップダウンリストからデータストアを選択します。
Virtual Machine Name（仮想マシン名）	仮想マシンの名前を入力します。
メモリ	Use a specific amount of RAM（特定容量の RAM を使用）をクリックして、使用する RAM の容量（4,096 MB など）を指定します。指定可能な最小容量は 512 MB です。指定可能な最大容量は、ホストマシンの機能と制限によって決まります（推奨）。
ディスクプロビジョニング	ディスクプロビジョニングのタイプを Thin（シン）または Thick（シック）から選択します。
Disk Mapping（ディスクマッピング）	ディスクマッピングのタイプを Automatic（自動）または Manual（マニュアル）のどちらかに指定します。

テキストボックス	説明
Version（バージョン）	仮想マシンのバージョンを選択します。

5. **次へ** をクリックします。
6. **Volumes**（ボリューム）ページで、エクスポートするボリュームを選択して **Next**（次へ）をクリックします。
7. **Summary**（サマリ）ページで、**Finish**（終了）をクリックしてウィザードを完了しエクスポートを開始します。

   メモ: Virtual Standby（仮想スタンバイ）または **Events**（イベント）タブを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

VMware Workstation エクスポートを使用した Windows データのエクスポート

AppAssure では、1 回限りのエクスポートまたは連続エクスポートを実行することにより、VMware Workstation エクスポートを使用したデータのエクスポートを選択できます。適切なエクスポートタイプのための VMware Workstation エクスポートを使用してエクスポートするには、次のエクスポート方法の手順を完了します。

1 回限りの VMware Workstation エクスポートの実行

1 回限りの VMware Workstation エクスポートを実行するには、次の手順を実行します。

1. Core Console で、エクスポートするマシンに移動します。
2. **Summary**（サマリ）で、**Actions（アクション）** → **Export（エクスポート）** → **One-time（1 回限り）** とクリックします。

   Export Wizard（エクスポートウィザード）が **Protected Machines**（保護マシン）ページに表示されます。
3. エクスポートするマシンを選択して、**Next**（次へ）をクリックします。
4. **Recovery Points**（リカバリポイント）のページで、エクスポートするリカバリポイントを選択し、**Next**（次へ）をクリックします。

VMware Workstation エクスポート実行のための 1 回限りの設定の定義

VMware Workstation エクスポート実行のために 1 回限りの設定を定義するには、次の手順を実行します。

1. **Export Wizard**（エクスポートウィザード）の **Destination**（宛先）ページで、**Recover to Virtual machine**（仮想マシンへの回復）ドロップダウンメニューから **VMware Workstation** を選択して **Next**（次へ）を選択します。
2. **Virtual Machine Options**（仮想マシンオプション）ページで、次の表の説明どおりに仮想マシンにアクセスするためのパラメータを入力します。

テキストボックス	説明
Location（場所）	仮想マシンを作成するローカルフォルダまたはネットワーク共有のパスを指定します。

テキストボックス	説明
	メモ: ネットワーク共有パスを指定した場合は、そのターゲットマシンに登録されているアカウントの有効なログオン資格情報を入力する必要があります。このアカウントには、ネットワーク共有に対する読み取りと書き込みの許可がある必要があります。
ユーザー名	仮想マシンのログオン資格情報を入力します。 • ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウント用に有効なユーザー名を入力する必要があります。 • ローカルパスを入力した場合は、ユーザー名は必要ありません。
パスワード	仮想マシンのログオン資格情報を入力します。 • ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウント用に有効なパスワードを入力する必要があります。 • ローカルパスを入力した場合は、パスワードは必要ありません。
Virtual Machine Name（仮想マシン名）	作成される仮想マシンの名前（例：VM-0A1B2C3D4）を入力します。 **メモ:** デフォルト名は、ソースマシンの名前です。
Version（バージョン）	仮想マシン用の VMware Workstation のバージョンを指定します。次から選択できます。 • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
メモリ	次のいずれかをクリックして、仮想マシン用のメモリ使用率を指定します。 • Use the same amount of RAM as the source machine（ソースマシンと同じ容量の RAM を使用） - RAM 設定がソースマシンと同じであることを指定します。 • Use a specific amount of RAM（特定容量の RAM を使用） - 使用する RAM の容量を指定します（4,096 メガバイト（MB）など）。指定可能な最小容量は 512 MB です。指定可能な最大容量は、ホストマシンの機能と制限事項に応じて決定されます（推奨）。

3. **次へ** をクリックします。
4. **Summary**（サマリ）ページで、**Finish**（終了）をクリックしてウィザードを完了しエクスポートを開始します。

   メモ: Virtual Standby（仮想スタンバイ）または **Events**（イベント）タブを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

連続（仮想スタンバイ）VMware Workstation エクスポートの実行

連続（仮想スタンバイ）VMware Workstation エクスポートを実行するには、次の手順を実行します。

1. Core Console で、次のいずれかを実行します。

- Virtual Standby（仮想スタンバイ）タブで **Add**（追加）をクリックして **Export Wizard**（エクスポートウィザード）を起動します。**Export Wizard**（エクスポートウィザード）の **Protected Machines**（保護対象マシン）ページで、エクスポートする保護対象マシンを選択して、**Next**（次へ）をクリックします。
- エクスポートするマシンへ移動して、そのマシンの **Actions**（アクション）ドロップダウンメニューの **Summary**（サマリ）タブで、 **Export（エクスポート）→ Virtual Standby（仮想スタンバイ）**とクリックします。

2. **Export Wizard**（エクスポートウィザード）の **Destination**（エクスポート先）ページで、**Recover to a Virtual Machine（仮想マシンへの復元）→ VMware Workstation（VMware ワークステーション）**とクリックします。
3. **次へ** をクリックします。
4. **Virtual Machine Options**（仮想マシンオプション）ページで、次の表の説明どおりに仮想マシンにアクセスするためのパラメータを入力します。

テキストボックス	説明
Target Path（ターゲットパス）	仮想マシンを作成するローカルフォルダまたはネットワーク共有のパスを指定します。 **メモ:** ネットワーク共有パスを指定した場合は、そのターゲットマシンに登録されているアカウントの有効なログオン資格情報を入力します。このアカウントには、ネットワーク共有に対する読み取りと書き込みの許可がある必要があります。
ユーザー名	仮想マシンのログオン資格情報を入力します。 • ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウント用に有効なユーザー名を入力する必要があります。 • ローカルパスを入力した場合は、ユーザー名は必要ありません。
パスワード	仮想マシンのログオン資格情報を入力します。 • ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウント用に有効なパスワードを入力する必要があります。 • ローカルパスを入力した場合は、パスワードは必要ありません。
Virtual Machine（仮想マシン）	作成される仮想マシンの名前（例：VM-0A1B2C3D4）を入力します。 **メモ:** デフォルト名は、ソースマシンの名前です。
Version（バージョン）	仮想マシン用の VMware Workstation のバージョンを指定します。次から選択できます。 • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
メモリ	次のいずれかをクリックして、仮想マシン用のメモリを指定します。 • Use the same amount of RAM as the source machine（ソースマシンと同じ容量の RAM を使用） - RAM 設定がソースマシンと同じであることを指定します。 • Use a specific amount of RAM（特定容量の RAM を使用） - 使用する RAM の容量を指定します（4,096 メガバイト（MB） など）。指定可能な最小容量

テキストボックス	説明
	は 512 MB です。指定可能な最大容量は、ホストマシンの機能と制限事項に応じて決定されます。

5. スケジュールされている次のスナップショットの後ではなく、今すぐ仮想エクスポートを実行するには、**Perform initial ad-hoc export**（初回アドホックエクスポートの実行）を選択します。
6. **次へ** をクリックします。
7. **Volumes**（ボリューム）ページで、エクスポートするボリューム（例：C:\ および D:\ など）を選択して、**Next**（次へ）をクリックします。
8. **Summary**（サマリ）ページで、**Finish**（終了）をクリックしてウィザードを完了しエクスポートを開始します。

メモ: Virtual Standby（仮想スタンバイ）または **Events**（イベント）タブを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

Hyper-V エクスポートを使用した Windows データのエクスポート

AppAssure では、1 回限りのエクスポートまたは連続エクスポートを実行することにより、Hyper-V エクスポートを使用したデータのエクスポートを選択できます。適切なエクスポートタイプのための Hyper-V エクスポートを使用してエクスポートするには、次の項目の手順を実行します。

1 回限りの Hyper-V エクスポートの実行

1 回限りの Hyper-V エクスポートを実行するには、次の手順を実行します。

1. Core Console で、エクスポートするマシンに移動します。
2. Summary（サマリ）タブで、**Actions（アクション）→ Export（エクスポート）→ One-time（1 回限り）**とクリックします。

   Export Wizard（エクスポートウィザード）が **Protected Machines**（保護対象マシン）ページに表示されます。
3. エクスポートするマシンを選択して、**Next**（次へ）をクリックします。
4. **Recovery Points**（リカバリポイント）のページで、エクスポートするリカバリポイントを選択し、**Next**（次へ）をクリックします。

Hyper-V エクスポート実行のための 1 回限りの設定の定義

Hyper-V エクスポート実行のために 1 回限りの設定を定義するには、次の手順を実行します。

1. Hyper-V ダイアログボックスで **Use local machine**（ローカルマシンを使用）をクリックして、Hyper-V 役割が割り当てられたローカルマシンへの Hyper-V エクスポートを実行します。
2. **Remote host**（リモートホスト）オプションをクリックして、Hyper-V サーバーがリモートマシン上にあることを指定します。Remote host（リモートホスト）オプションを選択した場合は、次の説明に従ってリモートホストのパラメータを入力します。

テキストボックス	説明
Host Name（ホスト名）	Hyper-V サーバーの IP アドレスまたはホスト名を入力します。リモート Hyper-V サーバーの IP アドレスまたはホスト名を表します。
Port（ポート）	マシンのポート番号を入力します。Core がこのマシンと通信するときに使用するポートを表します。

テキストボックス	説明
User Name（ユーザー名）	Hyper-V サーバー搭載のワークステーションに管理者権限を持つユーザーのユーザー名を入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。
Password（パワード）	Hyper-V サーバー搭載のワークステーション上の管理者権限を持つユーザーアカウントのパスワードを入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。

3. **Next**（次へ）をクリックします。
4. **VM Machine Location**（VM マシンの場所）テキストボックスの **Virtual Machines Options**（仮想マシンオプション）ページで、仮想マシンのパスまたは場所を入力します（たとえば、**D:\export**）。VM の場所には、仮想マシンに必要な VM メタデータと仮想ドライブを格納するのに十分な容量が必要です。
5. 仮想マシンの名前を **Virtual Machine Name**（仮想マシン名）テキストボックスに入力します。

   入力する名前は、Hyper-V Manager コンソールの仮想マシンリストに表示されます。
6. 次のいずれか 1 つをクリックします。
   - **Use the same amount of RAM as the source machine**（ソースマシンと同じ容量の RAM を使用）をクリックして、仮想マシンとソースマシン間の RAM 使用量が同じであることを特定します。
   - **Use a specific amount of RAM**（特定容量の RAM を使用）をクリックして、エクスポート後の仮想マシンのメモリ容量を指定します（たとえば、4096 MB（推奨値））。
7. ディスクのフォーマットを指定するには **Disk Format**（ディスクフォーマット）の横で、次のいずれかをクリックします。
   - **VHDX**
   - **VHD**

   メモ: ターゲットマシンで Windows 8（Windows Server 2012）またはそれ以降が実行されている場合は、Hyper-V Export が VHDX ディスクフォーマットをサポートします。VHDX がお使いの環境でサポートされていない場合は、オプションが無効になっています。
8. **Volumes**（ボリューム）ページで、エクスポートするボリュームを選択します。仮想マシンを保護対象マシンの効果的なバックアップにするには、保護対象マシンの起動ドライブを含めます（たとえば、C:\）。

   VHD では選択するボリュームは 2040 GB 以下にする必要があります。選択したボリュームが 2040 GB より大きく、VHD フォーマットが選択されている場合は、エラーを受け取ります。
9. **Summary**（サマリ）ページで **Finish**（終了）をクリックしてウィザードを完了し、エクスポートを開始します。

連続（仮想スタンバイ）Hyper-V エクスポートの実行

メモ: 1 回限りのエクスポートと連続エクスポート（仮想スタンバイ）の機能がサポートされるのは、2 つの VM を持つ 3 TB の構成の DL1000 のみです。

連続（仮想スタンバイ）Hyper-V エクスポートを実行するには、次の手順を実行します。

1. **Virtual Standby**（仮想スタンバイ）タブの Core Console で、**Add**（追加）をクリックして **Export Wizard**（エクスポートウィザード）を起動します。**Export Wizard**（エクスポートウィザード）の **Protected Machines**（保護対象マシン）ページで次の手順を実行します。
2. エクスポートするマシンを選択し **Next**（次へ）をクリックします。
3. **Summary**（サマリ）タブで、**Export（エクスポート）→ Virtual Standby（仮想スタンバイ）**とクリックします。
4. Hyper-V ダイアログボックスで **Use local machine**（ローカルマシンを使用）をクリックして、Hyper-V 役割が割り当てられたローカルマシンへの Hyper-V エクスポートを実行します。

5. **Remote host**（リモートホスト）オプションをクリックして、Hyper-V サーバーがリモートマシン上にあることを指定します。Remote host（リモートホスト）オプションを選択した場合は、次の説明に従ってリモートホストのパラメータを入力します。

テキストボックス	説明
Host Name（ホスト名）	Hyper-V サーバーの IP アドレスまたはホスト名を入力します。リモート Hyper-V サーバーの IP アドレスまたはホスト名を表します。
Port（ポート）	マシンのポート番号を入力します。Core がこのマシンと通信するときに使用するポートを表します。
User Name（ユーザー名）	Hyper-V サーバー搭載のワークステーションに管理者権限を持つユーザーのユーザー名を入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。
Password（パワード）	Hyper-V サーバー搭載のワークステーション上の管理者権限を持つユーザーアカウントのパスワードを入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。

6. **VM Machine Location**（VM マシンの場所）テキストボックスの **Virtual Machines Options**（仮想マシンオプション）ページで、仮想マシンのパスまたは場所を入力します（たとえば、D:\export）。VM の場所には、仮想マシンに必要な VM メタデータと仮想ドライブを格納するのに十分な容量が必要です。
7. 仮想マシンの名前を **Virtual Machine Name**（仮想マシン名）テキストボックスに入力します。
   入力する名前は、Hyper-V Manager コンソールの仮想マシンリストに表示されます。
8. 次のいずれか 1 つをクリックします。
   - **Use the same amount of RAM as the source machine**（ソースマシンと同じ容量の RAM を使用）をクリックして、仮想マシンとソースマシン間の RAM 使用量が同じであることを特定します。
   - **Use a specific amount of RAM**（特定容量の RAM を使用）をクリックして、エクスポート後の仮想マシンのメモリ容量を指定します（たとえば、4096 MB（推奨値））。
9. Generation（生成）を指定するには、次のいずれかをクリックします。
   - Generation 1（生成 1）（推奨）
   - Generation 2（生成 2）
10. ディスクのフォーマットを指定するには **Disk Format**（ディスクフォーマット）の横で、次のいずれかをクリックします。
    - **VHDX**（デフォルト値）
    - **VHD**

    メモ: ターゲットマシンで Windows 8（Windows Server 2012）以上が実行されている場合、Hyper-V エクスポートは VHDX ディスク形式をサポートします。VHDX がお使いの環境でサポートされていない場、このオプションは無効になります。Network Adapters（ネットワークアダプタ）ページで、スイッチに接続する仮想アダプタを選択します。
11. **Volumes**（ボリューム）ページで、エクスポートするボリュームを選択します。仮想マシンを保護対象マシンの効果的なバックアップにするには、保護対象マシンの起動ドライブを含めます（たとえば、C:\）。
    VHD では選択するボリュームは 2040 GB 以下にする必要があります。選択したボリュームが 2040 GB より大きく、VHD フォーマットが選択されている場合は、エラーを受け取ります。
12. **Summary**（サマリ）ページで、**Finish**（終了）をクリックしてウィザードを完了しエクスポートを開始します。

メモ: **Virtual Standby**（仮想スタンバイ）または **Events**（イベント）タブを表示して、エクスポートの状態や進捗状況を監視することができます。

Oracle VirtualBox エクスポートを使用した Windows データのエクスポート

AppAssure では、VirtualBox Export を使用した 1 回限りのエクスポートまたは連続エクスポート、または連続エクスポートの確立を選択して、データをエクスポートすることができます。

適切なタイプのエクスポートをするために次の項目の手順を実行します。

メモ: このタイプのエクスポートを実行するには、Core マシンに Oracle VirtualBox がインストールされている必要があります。Windows ホストには VirtualBox バージョン 4.2.18 以上がサポートされています。

1 回限りの Oracle VirtualBox エクスポートの実行

1 回限りの Oracle VirtualBox エクスポートを実行するには、次の手順を実行します。

1. Core Console で、エクスポートする Linux マシンに移動します。
2. **Summary**（サマリ）タブで、**Actions（アクション）→ Export（エクスポート）→ One-time（1 回限り）**とクリックします。

   Export Wizard（エクスポートウィザード）が **Protected Machines**（保護対象マシン）ページに表示されます。
3. エクスポートするマシンを選択して、**Next**（次へ）をクリックします。
4. **Recovery Points**（リカバリポイント）のページで、エクスポートするリカバリポイントを選択し、**Next**（次へ）をクリックします。
5. **Export Wizard**（エクスポートウィザード）の **Destination**（宛先）ページで、**Recover to Virtual machine**（仮想マシンへの回復）ドロップダウンメニューから **VirtualBox** を選択して **Next**（次へ）を選択します。
6. **Virtual Machine Options**（仮想マシンオプション）ページで **Remote Linux Machine**（リモート Linux マシン）を選択します。
7. 次のとおりに仮想マシンにアクセスするためのパラメータを入力します。

テキストボックス	説明
VirtualBox Host Name（VirtualBox ホスト名）	VirtualBox サーバーの IP アドレスまたはホスト名を入力します。このフィールドはリモート VirtualBox サーバーの IP アドレスまたはホスト名を表します。
ポート	マシンのポート番号を入力します。この番号は Core がこのマシンと通信するときに使用するポートを表します。
Virtual Machine Name（仮想マシン名）	仮想マシンを作成するためのターゲットパスを指定します。
ユーザー名	ターゲットマシン上のアカウントのユーザー名（例：root）です。
パスワード	ホストマシンのログオン資格情報を入力します。
メモリ	仮想マシン用のメモリを指定します。

8. **Volumes**（ボリューム）ページで、エクスポートするデータのボリュームを選択して **Next**（次へ）をクリックします。

9. **Summary**（サマリ）ページで、**Finish**（終了）をクリックしてウィザードを完了しエクスポートを開始します。

   メモ: Virtual Standby（仮想スタンバイ）または Events（イベント）タブを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

連続（仮想スタンバイ）Oracle VirtualBox エクスポートの実行

連続（仮想スタンバイ）VirtualBox エクスポートを実行するには、次の手順を実行します。

1. Core Console で、次のいずれかを実行します。
   - **Virtual Standby**（仮想スタンバイ）タブで、**Add**（追加）をクリックして **Export Wizard**（エクスポートウィザード）を起動します。**Export Wizard**（エクスポートウィザード）の **Protected Machines**（保護対象マシン）ページで、エクスポートする保護対象マシンを選択して、**Next**（次へ）をクリックします。
   - エクスポートするマシンに移動して、そのマシンの **Actions**（アクション）ドロップダウンメニューの **Summary**（サマリ）タブで、 **Export（エクスポート）→ Virtual Standby（仮想スタンバイ）**とクリックします。
2. **Export Wizard**（エクスポートウィザード）の **Destination**（宛先）ページで、**Recover to Virtual machine**（仮想マシンへの回復）ドロップダウンメニューから **VirtualBox** を選択して **Next**（次へ）を選択します。
3. **Virtual Machine Options**（仮想マシンオプション）ページで **Use Windows machine**（Windows マシンの使用）を選択します。
4. 次の表の説明に従って、仮想マシンへのアクセスのためのパラメータを入力します。

テキストボックス	説明
Virtual Machine Name（仮想マシン名）	作成中の仮想マシンの名前を入力します。 **メモ:** デフォルト名は、ソースマシンの名前です。
Target Path（ターゲットパス）	ローカルまたはリモートのターゲットパスを指定して、仮想マシンを作成します。 **メモ:** ルートディレクトリはターゲットパスにしないでください。 ネットワーク共有パスを指定した場合は、ターゲットマシンで登録されたアカウントに対する有効なログイン資格情報（ユーザー名およびパスワード）を入力する必要があります。アカウントにはネットワーク共有への書き込みおよび読み取り許可が必要です。
メモリ	仮想マシン用のメモリを指定します。 • **Use the same amount of RAM as the source machine**（ソースマシンと同じ容量の RAM を使用）をクリックして、RAM 設定がソースマシンと同じであることを指定します。 • 使用する RAM の容量（4,096 メガバイト（MB） など）を指定するには、**Use a specific amount of RAM**（特定容量の RAM を使用）をクリックします。指定可能な最小容量は 512 MB です。指定可能な最大容量は、ホストマシンの機能と制限によって決まります。

5. 仮想マシンのユーザーアカウントを指定するには、**Specify the user account for the exported virtual machine**（エクスポートされた仮想マシンのユーザーアカウントの指定）を選択し、次の情報を入力します。これは仮想マシン上に複数のユーザーアカウントがある場合に仮想マシンが登録される特定のユーザーアカウントを意味します。このユーザーアカウントがログオンすると、VirtualBox マネージャで

は、このユーザーのみにこの仮想マシンが表示されます。アカウントが指定されない場合は、仮想マシンは VirtualBox のある Windows マシン上のすべての既存ユーザーに登録されます。

- User name（ユーザー名）- 仮想マシンが登録されているユーザー名を入力します。
- Password（パスワード）- このユーザーアカウントのパスワードを入力します。

6. スケジュールされている次のスナップショットの後ではなく、今すぐ仮想エクスポートを実行するには、**Perform initial ad-hoc export**（初回アドホックエクスポートの実行）を選択します。
7. **次へ** をクリックします。
8. **Volumes**（ボリューム）ページで、エクスポートするボリューム（例：C:\ および D:\ など）を選択して、**Next**（次へ）をクリックします。
9. **Summary**（サマリ）ページで、**Finish**（終了）をクリックしてウィザードを完了しエクスポートを開始します。

メモ: Virtual Standby（仮想スタンバイ）または **Events**（イベント）タブを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

リカバリポイントからのボリュームの復元

AppAssure Core に保管されているリカバリポイントから保護対象マシンでボリュームを復元することができます。リカバリポイントからボリュームを復元するには、次の手順を実行します。

1. Core Console で、**Restore**（復元）タブをクリックします。

   Restore Machine Wizard（マシンの復元ウィザード）が表示されます。
2. **Protected Machines**（保護対象マシン）のページで、データを復元する保護対象マシンを選択し、**Next**（次へ）をクリックします。

   メモ: 保護対象マシンには Agent ソフトウェアがインストールされている必要があり、復元操作の実行元となるリカバリポイントがある必要もあります。

   Recovery Points（リカバリポイント）ページが表示されます。
3. リカバリポイントのリストから、エージェントマシンに復元するスナップショットを検索します。

   メモ: 必要な場合は、ページの一番下にあるナビゲーションボタンを使用して追加のリカバリポイントを表示します。または、ウィザードの Recovery Points（リカバリポイント）ページに表示されるリカバリポイントの数量を制限する場合は、ボリューム（定義されている場合）、またはリカバリポイントの作成日でフィルタすることができます。
4. 任意のカバリポイントをクリックして選択し、**Next**（次へ）をクリックします。

   Destination（宛先）ページが表示されます。
5. **Destination**（宛先）ページで、データ復元先のマシンを次のように選択します。
   - 選択したリカバリポイントから同じエージェントマシン（例えばマシン 1）にデータを復元する場合、および復元するボリュームにシステムボリュームが含まれていない場合は、**Recover to a protected machine (only non-system volumes)**（保護対象マシンへの復元（非システムボリュームのみ）を選択し、復元先マシン（マシン 1）が選択されていることを確認して、**Next**（次へ）をクリックします。**Volume Mapping**（ボリュームマッピング）ページが表示されます。手順 7 に進みます。
   - 選択したリカバリポイントから別の保護対象マシンにデータを復元する場合（例えば、マシン 2 の内容をマシン 1 のデータに置き換える場合）は、**Recover to a protected machine (only non-system volumes)**（保護対象マシンへの復元（非システムボリュームのみ））を選択し、復元先マシン（例えばマシン 2）をリストから選択して、**Next**（次へ）をクリックします。**Volume Mapping**（ボリュームマッピング）ページが表示されます。手順 7 に進みます。
   - 起動 CD を使用して同じマシンまたは別のマシンに選択したリカバリポイントを復元しており、復元するボリュームにシステムボリュームが含まれていない場合は、**Recover to any target machine using a boot CD**（起動 CD を使用して任意のターゲットマシンに回復する）を選択します。

- 選択したリカバリポイントからの情報での起動 CD の作成を続行するには、**Next**（次へ） をクリックして手順 10 に進みます。
- 起動 CD を既に作成済みで、ターゲットマシンがその起動 CD で起動されている場合は、手順 17 へ進みます。
- リカバリポイントからシステムボリュームへ復元する場合は（例 : マシン 1 と命名されたエージェントマシンの C ドライブ）、BMR を実行する必要があります。Windows 向け BMR の実行についての詳細は、Windows マシンのベアメタル復元の開始を参照してください。
- Linux での BMR 実行の詳細については、Linux マシンでのベアメタル復元実行用のロードマップの Linux マシンのベアメタル復元の開始を参照してください。

6. ターゲットマシンで Universal Recovery Console（URC）に接続するには、次の手順を実行します。
   a. **I already have a boot CD running on the target machine**（ターゲットマシンで既に実行中の起動 CD があります）を選択します。
   b. IP address（IP アドレス）テキストボックスで、起動 CD のあるターゲットマシンの IP アドレスを入力します。
   c. Authentication Key（認証キー）テキストボックスで、ターゲットマシン上の URC の認証キーを入力し、**Next**（次へ）をクリックします。

   Disk Mapping（ディスクマッピング）ページが表示されます。手順 20 に進みます。
7. **Volume Mapping**（ボリュームのマッピング）ページで、復元するリカバリポイント内の各ボリュームに対し、適切な宛先ボリュームを選択します。ボリュームを復元しない場合は、Destination Volumes（宛先ボリューム）列で **Do not restore**（復元しない）を選択します。
8. **Show advanced options**（詳細オプションの表示）を選択して、次の手順を実行します。
   - Windows マシンへの復元で、Live Recovery を使用する場合は、**Live Recovery** を選択します。
     AppAssure の即時リカバリテクノロジーである Live Recovery を使用することにより、Microsoft Windows 記憶域スペースを含む Windows マシンの保存済みリカバリポイントから、お使いの物理マシンまたは仮想マシンに対して瞬時にデータを回復または復元することができます。Live Recovery は、Linux マシンでは使用できません。
   - 強制的にマウントを解除したい場合は、**Force Dismount**（マウント解除の強制）を選択します。
     データの復元前にマウント解除を強制実行しない場合、ボリュームの使用中エラーで復元が失敗する可能性があります。
9. 手順 20 に進みます。
10. Boot CD（起動 CD）ページで、次の手順を実行します。
    a. **Output path**（出力パス）テキストフィールドに、起動 CD ISO イメージが保管されているパスを入力します。
    b. **Environment**（環境）で、復元しているハードウェアに最も適したアーキテクチャを選択します。
       - 64 ビットアーキテクチャの Windows マシンで復元するには、**Windows 8 64-bit**（Windows 8 64 ビット ）を選択します。
       - 32 ビット（x86）アーキテクチャのマシンで復元するには、**Windows 7 32-bit**（Windows 7 32 ビット ）を選択します。
11. オプションで、復元されたエージェントのネットワークパラメータを設定、UltraVNC を使用するには、**Show advanced options**（詳細オプションの表示）を選択して次のいずれかを実行します。
    - 復元されたマシンのネットワーク接続を確立するには、次の表の説明に従って **Use the following IP address**（次の IP アドレスを使用） を選択します。

オプション	説明
IP Address（IP アドレス）	復元されたマシンの IP アドレスまたはホスト名を指定します。

オプション	説明
Subnet Mask（サブネットマスク）	復元されたマシンのサブネットマスクを指定します。
Default Gateway（デフォルトゲートウェイ）	復元されたマシンのデフォルトゲートウェイを指定します。
DNS Server（DNS サーバー）	復元されたマシンのドメインネームサーバーを指定します。

- UltraVNC 情報を定義するには、次の表の説明に従って **Add UltraVNC**（UltraVNC の追加）を選択します。このオプションは、リカバリコンソールへのリモートアクセスが必要な場合に使用します。起動 CD を使用している間は Microsoft Terminal Services を使用してログインすることはできません。

オプション	説明
Password（パワード）	この UltraVNC 接続用のパスワードを指定します。
Port（ポート）	この UltraVNC 接続用のポートを指定します。デフォルトポートは 5900 です。

12. **Next**（次へ）をクリックします。
13. ドライバを導入するには、次の手順を実行します。
    a. **Add an archive of drivers**（ドライブのアーカイブの追加）を選択します。
    b. アーカイブが格納された ZIP ファイルに移動して、ZIP ファイルを選択してから **Open**（開く）をクリックします。アーカイブがアップロードされ、Driver Injection（ドライバ導入）ページに表示されます。
    c. **Next**（次へ）をクリックします。
14. ISO Image（ISO イメージ）ページで、起動 CD ISO イメージの作成ステータスが表示されます。起動 CD が正常に完了したら、**Next**（次へ）をクリックします。

    Connection（接続）ページが表示されます。
15. 起動 CD からデータを復元するエージェントマシンを起動します。
    - 可能な場合は、ISO イメージからエージェントマシンを起動します。
    - 不可能な場合は、ISO イメージを物理メディア（CD または DVD）にコピーして、エージェントマシンにディスクをロードしてから、マシンが起動 CD からロードするように設定します。その後、起動 CD から再起動します。

    メモ: 最初にロードされるボリュームが起動 CD になるようにエージェントマシンの BIOS 設定を変更する必要がある場合があります。

    起動 CD から起動された場合、エージェントマシンは Universal Recovery Console（URC）インタフェースを表示します。この環境は、システムドライブ、または選択されたボリュームディレクトリを AppAssure Core から直接復元するために使用されます。URC の IP アドレスと認証キー資格情報は起動 CD から起動されるたびに変更されるため、メモしておきます。
16. **Connection**（接続）ページの Core Console で、復元するマシンの URC インスタンスから認証情報を次のように入力します。
    a. IP Address（IP アドレス）テキストボックスにリカバリポイントから復元しているマシンの IP アドレスを入力します。
    b. Authentication Key（認証キー）テキストボックスに URC からの情報を入力します。
    c. **Next**（次へ）をクリックします。

    Disk Mapping（ディスクマッピング）ページが表示されます。

17. ボリュームを手動でマップするには、手順 18 に進みます。自動的にボリュームをマップするには、次の手順を実行します。
    a. **Automatic volume mapping**（自動ボリュームマッピング）を選択します。
    b. **Automatic volume mapping**（自動ボリュームマッピング）エリアで、復元するボリュームを選択します。 リストされたボリュームを復元したくない場合は、オプションをクリアします。

    メモ: 復元を実行するには、少なくとも 1 つのボリュームを選択する必要があります。

    c. 復元用の宛先ディスクを選択します。
    d. **Next**（次へ）をクリックし、手順 19 に進みます。
18. ボリュームを手動でマップする場合は、以下を実行します。
    a. **Automatic volume mapping**（手動ボリュームマッピング）を選択します。
    b. **Manual volume mapping**（手動ボリュームマッピング）エリアで、各ボリュームの **Destination Volumes**（宛先ボリューム）のドロップダウンリストから、復元するボリュームを選択します。リストされたボリュームを復元したくない場合は、オプションをクリアします。

    メモ: 復元を実行するには、少なくとも 1 つのボリュームを選択する必要があります。

    c. **Finish**（終了）をクリックします。

    注意: Finish（終了）を選択すると、ターゲットドライブ上にあるすべてのパーティションおよびデータは完全に削除され、選択したリカバリポイントの内容に置き換えられます。これには、オペレーティングシステムおよびすべてのデータが含まれます。

    Restore Machine Wizard（マシンの復元ウィザード）が閉じ、リカバリポイントの選択されたボリュームからターゲットマシンにデータが復元されます。手順 22 に進みます。
19. **Disk Mapping Preview**（ディスクマッピングプレビュー）ページで、選択した復元アクションのパラメータを確認します。復元を実行するには、**Finish**（終了）をクリックします。

    注意: Finish（終了）を選択すると、ターゲットドライブ上にあるすべてのパーティションおよびデータは完全に削除され、選択したリカバリポイントの内容に置き換えられます。これには、オペレーティングシステムおよびすべてのデータが含まれます。

    Restore Machine Wizard（マシンの復元ウィザード）が閉じ、リカバリポイントの選択されたボリュームからターゲットマシンにデータが復元されます。手順 22 に進みます。
20. 復元したいボリュームに SQL や Microsoft Exchange データベースが含まれている場合は、**Dismount Databases**（データベースのマウント解除）ページでそれらをマウント解除するプロンプトが表示されます。オプションとして、復元完了後にこれらのデータベースを再マウントしたい場合は、**Automatically remount all databases after the recovery point is restored**（リカバリポイントの復元後にすべてのデータベースを自動的に再マウントする）を選択します。**Finish**（終了）をクリックします。
21. **OK** をクリックして、復元プロセスが開始されたことを示すステータスメッセージを確認します。
22. 復元アクションの進行状況を監視するには、Core Console で **Events**（イベント）をクリックします。

コマンドラインを使用した Linux マシンへのボリュームの復元

AppAssure では、コマンドライン `aamount` ユーティリティを使用してお使いの保護対象 Linux マシンのボリュームを復元することができます。 コマンドラインユーティリティを使用して Linux マシンでボリュームを復元するには、次の手順を実行します。

注意: システムまたはルート（/）ボリュームの復元は試みないでください。

1. 次のように、AppAssure `aamount` ユーティリティをルートとして実行します。

   ```
   sudo aamount
   ```
2. AppAssure のマウントプロンプトで、次のコマンドを入力して保護対象マシンのリストを表示します。

   ```
   lm
   ```

3. プロンプトが表示されたら、AppAssure Core サーバーの IP アドレスまたはホスト名を入力します。
4. このサーバーに対するログオン資格情報、つまり、ユーザー名とパスワードを入力します。

   この AppAssure サーバーによって保護されるマシンのリストが表示されます。このリストには、ラインアイテム番号、ホスト /IP アドレス、およびマシンの ID 番号（例：`293cc667-44b4-48ab-91d8-44bc74252a4f`）で検出されたエージェントマシンが表示されます。
5. 次のコマンドを入力して、指定のマシンに対して現在マウントされているリカバリポイントを表示します。

   ```
   lr <machine_line_item_number>
   ```

   メモ: このコマンドでは、ラインアイテム番号の代わりにマシン ID 番号を入力することもできます。

   そのマシンのベースおよび増分リカバリポイントのリストが表示されます。このリストには、ラインアイテム番号、日付 / タイムスタンプ、ボリュームの場所、リカバリポイントのサイズ、およびリカバリポイントを特定するシーケンス番号を末尾に含むボリュームの ID 番号
   （例：`"293cc667-44b4-48ab-91d8-44bc74252a4f:2"`）が表示されます。
6. ロールバックのリカバリポイントを選択するには、次のコマンドを入力します。

   ```
   r [volume_recovery_point_ID_number] [path]
   ```

   このコマンドは、ID で指定されたボリュームイメージを Core から指定のパスにロールバックします。ロールバックのパスは、デバイスのファイル記述子のパスであり、マウント先のディレクトリではありません。

   メモ: また、リカバリポイントを識別するために、リカバリポイントの ID 番号の代わりにコマンドにライン番号を指定することもできます。その場合は、`r [machine_line_item_number] [recovery_point_line_number] [volume_letter] [path]` のように、エージェント / マシンライン番号（`lm` の出力からのもの）を使用し、その後にリカバリポイントライン番号とボリューム文字、最後にパスを続けます。このコマンドでは、[path] は実際のボリュームのファイル記述子です。

   たとえば、`lm` の出力に 3 つのエージェントマシンが示され、番号 2 のマシンに対して `lr` コマンドを入力し、リカバリポイント 23 のボリューム b をディレクトリ `/mnt/data` にマウントされたボリュームにロールバックする場合、コマンドは `r2 23 b /mnt/data` となります。
7. 続行するかどうかを尋ねるプロンプトが表示されたら、Yes を示す `y` を入力します。

   ロールバックが続行されると、ステータスを示す一連のメッセージが表示されます。
8. ターゲットが以前に保護およびマウントされていた場合は、ロールバックに成功した時点で `aamount` ユーティリティがカーネルモジュールをロールバックボリュームに自動的にマウントして、再アタッチします。それ以外の場合は、ロールバックボリュームをローカルディスクにマウントして、ファイルが復元されたことを確認してください。

   たとえば、`sudo mount` コマンドを使用し、次に `ls` コマンドを使用できます。

Windows マシンのベアメタル復元の起動

AppAssure では、ハードウェアが同種であるか異種であるかに関係なく、Windows マシンに対してベアメタル復元（BMR）を実行することができます。このプロセスには、起動 CD イメージの作成、ディスクへのイメージの焼き付け、ディスクからのターゲットサーバーの起動、リカバリコンソールインスタンスへの接続、ボリュームのマッピング、リカバリの開始、およびプロセスの監視が含まれます。ベアメタル復元の完了後は、続けて復元されたサーバー上にオペレーティングシステムとソフトウェアアプリケーションをロードし、独自の設定を行うことができます。

ベアメタル復元の実行を選択するその他の状況としては、ハードウェアのアップグレードやサーバーの交換などがあります。

BMR 機能は、保護対象 Linux マシンに対しても、コマンドラインの `aamount` ユーティリティによってサポートされます。詳細については、Linux マシンのベアメタル復元の開始を参照してください。

Windows マシンのベアメタル復元を実行するためのロードマップ

Windows マシンの BMR を実行するには、次の手順を実行します。

1. 起動 CD を作成します。
2. イメージをディスクにコピーします。
3. 起動 CD からターゲットサーバーを起動します。
4. リカバリディスクに接続します。
5. ボリュームをマップします。
6. リカバリを開始します。
7. 進捗状況を監視します。

起動可能 CD ISO イメージの作成

Windows マシンの BMR を実行するには、Core Console で起動可能 CD/ISO イメージを作成する必要があります。このイメージには、AppAssure Universal Recovery Console インタフェースが含まれています。AppAssure Universal Recovery Console は、システムドライブまたはサーバー全体を AppAssure Core から直接復元するために使用される環境です。

作成する ISO イメージは、復元されるマシンに合わせてカスタマイズされます。したがって、このイメージには正しいネットワークドライバと大容量ストレージドライバが含まれている必要があります。起動 CD を作成しているマシンとは異なるハードウェアに復元することを想定している場合は、ストレージコントローラおよびその他ドライバを起動 CD に含める必要があります。起動 CD へのドライバの導入を参照してください。

メモ: 国際標準化機構（ISO）は、ファイルシステムの標準を決定および設定する、さまざまな国家組織の代表で構成された国際団体です。ISO 9660 は、データ交換用の光学ディスクメディアに使用されるファイルシステム標準であり、Windows などの各種オペレーティングシステムをサポートします。ISO イメージは、ディスクの各セクタとディスクファイルシステムのデータを格納するアーカイブファイルまたはディスクイメージです。

起動可能な CD ISO イメージを作成するには、次の手順を実行します。

1. 復元するサーバーが配置されている Core Console から **Core**（コア）を選択し、**Tools**（ツール）タブをクリックします。
2. **Boot CDs**（起動 CD）をクリックします。
3. **Actions**（アクション）を選択し、**Create Boot ISO**（起動 ISO の作成）をクリックします。

   Create Boot CD（起動 CD の作成）ダイアログボックスが表示されます。ダイアログボックスを完了するには、次の手順を使用します。

起動CD ファイルの命名とパスの設定

起動 CD ファイルに名前を付け、パスを設定するには、次の手順を実行します。

Create Boot CD（起動 CD の作成）ダイアログボックスで、Core サーバー上での起動イメージの保存場所となる ISO パスを入力します。

イメージを保存する共有のディスク容量が残り少ない場合、必要に応じてパスを設定できます（例：D:\filename.iso）。

メモ: ファイル拡張子は .iso にする必要があります。パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。英字 a～z は大文字と小文字が区別されません。スペースは使用しないでください。その他の記号および句読点は使用できません。

接続の作成

接続を作成するには、次の手順を実行します。

1. **Connection Options**（接続オプション）で、次のいずれかを実行します。
   - Dynamic Host Configuration Protocol（DHCP）を使用して IP アドレスを動的に取得するには、**Obtain IP address automatically**（IP アドレスを自動的に取得する）を選択します。
   - オプションで、リカバリコンソールの静的 IP アドレスを指定するには、**Use the following IP address**（次の IP アドレスを使用する）を選択し、IP アドレス、サブネットマスク、デフォルトゲートウェイ、および DNS サーバーをそれぞれ対応するフィールドに入力します。これらのフィールドはすべて指定する必要があります。
2. 必要に応じて、**UltraVNC Options**（UltraVNC オプション）で **Add UltraVNC**（UltraVNC の追加）を選択し、UltraVNC オプションを入力します。UltraVNC 設定により、リカバリコンソールを使用中にリモートで管理できます。

   メモ: この手順はオプションです。リカバリコンソールへのリモートアクセスが必要な場合は、UltraVNC を設定して使用する必要があります。起動 CD の使用中は、Microsoft Terminal Services を使用してログオンすることはできません。

起動CD へのドライバの導入

ドライバ導入は、ターゲットサーバー上のリカバリコンソール、ネットワークアダプタ、およびストレージ間の操作性を容易にするために使用されます。

異種ハードウェアへの復元が予想される場合は、ストレージコントローラ、RAID、AHCI、チップセットなどのドライバを起動 CD に導入する必要があります。これらのドライバにより、オペレーティングシステムがすべてのデバイスを検出し、それらを正常に動作させることが可能になります。

メモ: 起動 CD には、Windows 7 PE 32 ビットドライバが自動的に含められることに注意してください。

起動 CD にドライバを導入するには、次の手順を実行します。

1. メーカーのウェブサイトからサーバー用のドライバをダウンロードし、解凍します。
2. WinZip などのファイル圧縮ユーティリティを使用して、それらのドライバが保存されているフォルダを圧縮します。
3. **Create Boot CD**（起動 CD の作成）ダイアログボックスの **Drivers**（ドライバ）ペインで、**Add a Driver**（ドライバの追加）をクリックします。
4. 圧縮されたドライバファイルの場所までファイルシステム内を移動します。ファイルを選択し、**Open**（開く）をクリックします。

   導入されたドライバが、**Drivers**（ドライバ）ペインでハイライト表示されます。

起動 CD の作成

起動 CD を作成するには、起動 CD の命名、パスの指定、接続の確立を行い、必要に応じてドライバを導入してから、**Create Boot CD**（起動 CD の作成）画面で **Create Boot CD**（起動 CD の作成）をクリックします。これで ISO イメージが作成されます。

ISO イメージ作成の進捗状況の表示

ISO イメージ作成の進捗状況を表示するには、**Events**（イベント）タブを選択します。その後、**Tasks**（タスク）で ISO イメージ作成の進捗状況を監視できます。

メモ: ISO イメージ作成の進捗状況は、**Monitor Active Task**（アクティブタスクの監視）ダイアログボックスでも表示できます。

ISO イメージ作成が完了すると、**Boot CDs**（起動 CD）ページで使用可能になり、**Tools**（ツール）メニューからアクセスできます。

ISO イメージへのアクセス

ISO イメージにアクセスするには、指定した出力パスに移動するか、リンクをクリックして、新規のシステムにそのイメージをロードする元となる場所（ネットワークドライブなど）にイメージをダウンロードします。

起動 CD のロード

起動 CD イメージを作成したら、新たに作成した起動 CD を使用してターゲットサーバーを起動します。

メモ: DHCP を使用して起動 CD を作成した場合は、IP アドレスおよびパスワードを控えておいてください。

起動 CD をロードするには、次の手順を実行します。

1. 新規サーバーに移動し、起動 CD をロードしてから、マシンを起動します。
2. **Boot from CD-ROM**（CD-ROM から起動）を指定します。これにより、次のソフトウェアがロードされます。
   - Windows 7 PE
   - AppAssure Agent ソフトウェア

   AppAssure Universal Recovery Console が起動し、マシンの IP アドレスと認証パスワードが表示されます。
3. Network Adapters Settings（ネットワークアダプタの設定）ペインに表示された IP アドレスと Authentication（認証）ペインに表示された認証パスワードを記録します。この情報は、データリカバリ処理中にコンソールに再度ログオンするために後で使用します。
4. IP アドレスを変更する場合は、IP アドレスを選択し、**Change**（変更）をクリックします。

   メモ: Create Boot CD（起動 CD の作成）ダイアログボックスで IP アドレスを指定した場合、Universal Recovery Console によってこのアドレスが使用され、**Network Adapter settings**（ネットワークアダプタの設定）画面で表示されます。

ターゲットサーバーへのドライブの導入

異なるハードウェアに復元を行う場合、ストレージコントローラ、RAID、AHCI、チップセットなどのドライバが起動 CD 上にまだ存在しない場合は、それらを導入する必要があります。これらのドライバにより、オペレーティングシステムは、ターゲットサーバー上のすべてのデバイスを正常に動作させることができるようになります。

ターゲットサーバーに必要なドライバが不明な場合は、Universal Recovery Console で System Info（システム情報）タブをクリックします。このタブには、復元するターゲットサーバーのすべてのシステムハードウェアとデバイスタイプが表示されます。

メモ: ターゲットサーバーには、Windows 7 PE 32 ビットドライバが自動的に含められることに留意してください。

ターゲットサーバーにドライバを導入するには、次の手順を実行します。

1. メーカーのウェブサイトからサーバー用のドライバをダウンロードし、解凍します。
2. ファイル圧縮ユーティリティ（Win Zip など）を使用して、それらのドライバが保存されているフォルダを圧縮し、ターゲットサーバーにコピーします。
3. Universal Recovery Console で、**Driver Injection**（ドライバ導入）をクリックします。
4. 圧縮されたドライバファイルの場所までファイルシステム内を移動し、そのファイルを選択します。
5. 手順 3 で **Driver Injection**（ドライバ導入）をクリックした場合は、**Add Driver**（ドライバの追加）をクリックします。手順 3 で **Load driver**（ドライバのロード）をクリックした場合は、**Open**（開く）をクリックします。

   選択したドライバが導入され、ターゲットサーバーの再起動後にオペレーティングシステムへロードされます。

Core からの復元の開始

Core から復元を開始するには、次の手順を実行します。

1. 復元するシステム上の NIC がチーム化（結合）されている場合、ネットワークケーブル 1 本を残してすべて取り外します。

   メモ: AppAssure Restore は、チーム化された NIC を認識しません。複数のアクティブ接続が提示されると、このプロセスはどの NIC を使用するかを解決できません。
2. Core サーバーに戻り、Core Console を開きます。
3. **Machines**（マシン）タブで、データの復元元になるマシンを選択します。
4. そのマシンの **Actions**（アクション）メニューで、**Recovery Points**（リカバリポイント）をクリックして、そのマシンの全リカバリポイントのリストを表示します。
5. 復元したいリカバリポイントを展開して、**Rollback**（ロールバック）をクリックします。
6. **Rollback**（ロールバック）ダイアログボックスの **Choose Destination**（復元先の選択）から、**Recovery Console Interface**（リカバリコンソールインタフェース）を選択します。
7. **Host**（ホスト）テキストボックスと **Password**（パスワード）テキストボックスにデータの復元先になる新規サーバーの IP アドレスと認証パスワードを入力します。

   メモ: Host（ホスト）値と Password（パスワード）値は、前のタスクで記録した資格情報です。詳細については、起動 CD のロードを参照してください。
8. **Load Volumes**（ボリュームのロード）をクリックし、ターゲットボリュームを新規マシンにロードします。

ボリュームのマッピング

ターゲットサーバー上のディスクにボリュームを自動または手動でマップすることができます。自動ディスクアラインメントの場合、ディスクのクリーニングとパーティションの再作成が行われ、データはすべて削除されます。このアラインメントはボリュームのリスト順に行われ、各ボリュームはサイズなどに応じて適切なディスクに割り当てられます。複数のボリュームが同じディスクを使用することができます。ドライブを手動でマップする場合は、同じディスクを 2 回使用することはできません。

手動マッピングでは、復元を行う前に新しいマシンが既に正しくフォーマットされている必要があります。

ボリュームをマップするには、次の手順を実行します。

1. ボリュームを自動でマップするには、次を行います。
   a. **Restore Machine Wizard**（マシンの復元ウィザード）の **Disk Mapping**（ディスクのマッピング）ページで、**Automatically Map Volumes**（自動的にボリュームをマップ）タブを選択します。
   b. **Disk Mapping**（ディスクマッピング）領域の **Source Volume**（ソースボリューム）の下で、ソースボリュームが選択されていること、および適切なボリュームが下に一覧表示され、選択されていることを確認します。
   c. 自動マッピングの宛先ディスクが正しいターゲットボリュームになっていれば、**Destination Disk**（宛先ディスク）を選択します。
   d. **Restore**（復元）をクリックし、手順 3 に進みます。
2. ボリュームを手動でマップするには、次を行います。
   a. **Restore Machine Wizard**（マシンの復元ウィザード）の **Disk Mapping**（ディスクのマッピング）ページで、**Manually Map Volumes**（手動でボリュームをマップ）タブを選択します。
   b. **Volume Mapping**（ボリュームマッピング）領域の **Source Volume**（ソースボリューム）の下で、ソースボリュームが選択されていること、および適切なボリュームが下に一覧表示され、選択されていることを確認します。
   c. **Destination**（宛先）のドロップダウンメニューから、選択したリカバリポイントのベアメタル復元を実行するためのターゲットボリュームとなる適切な宛先を選択し、**Rollback**（ロールバック）をクリックします。
3. **RollbackURC** 確認ダイアログボックスで、リカバリポイントのソースのマッピングと、ロールバックの宛先ボリュームを確認します。ロールバックを実行するには、**Restore**（復元）をクリックします。

   注意: Begin Rollback（ロールバックの開始）をクリックすると、ターゲットドライブ上にあるすべてのパーティションおよびデータは完全に削除され、選択したリカバリポイントの内容に置き換えられます。これには、オペレーティングシステムおよびすべてのデータが含まれます。

リカバリ進捗状況の表示

リカバリ進捗状況を表示するには、次の手順を実行します。

1. ロールバックプロセスを開始した後、**Active Task**（アクティブタスク）ダイアログボックスが表示されることにより、ロールバックアクションの開始が示されます。

   メモ: Active Task（アクティブタスク）ダイアログボックスの表示は、タスクが正常に完了したことを意味しているわけではありません。
2. オプションで、ロールバックタスクの進捗状況を監視するには、Active Task（アクティブタスク）ダイアログボックスから、**Open Monitor Window**（モニタウィンドウを開く）をクリックします。**Monitor Open Task**（開いているタスクの監視）ウィンドウからリカバリのステータスおよび開始 / 終了時刻を確認できます。

   メモ: Active Task（アクティブタスク）ダイアログボックスからソースマシンのリカバリポイントに戻るには、**Close**（閉じる）をクリックします。

復元されたターゲットサーバーの起動

復元されたターゲットサーバーを起動するには、次の手順を実行します。

1. ターゲットサーバーに移動し、**AppAssure Universal Recovery Console** インタフェースで **Reboot**（再起動）をクリックして、マシンを起動します。
2. Windows を通常起動するように指定します。
3. マシンにログオンします。
   システムは、ベアメタル復元の前の状態に復元されます。

起動時問題の修復

異種ハードウェアに復元している場合は、ストレージコントローラ、RAID、AHCI、チップセットなどのドライバを起動 CD に導入する必要があります（まだ導入されていない場合）。これらのドライバにより、オペレーティングシステムがお使いのターゲットサーバー上にあるすべてのデバイスを正常に動作させることが可能になります。

起動時の問題を修復するには、次の手順を実行します。

1. 復元したターゲットサーバーの起動時に問題が発生する場合は、起動 CD を再ロードして Universal Recovery Console を開きます。
2. Universal Recovery Console で、**Driver Injection**（ドライバ導入）をクリックします。
3. Driver Injection（ドライバ導入）ダイアログで、**Repair Boot Problems**（起動の問題の修復）をクリックします。

   ターゲットサーバーの起動レコードの起動時パラメータが自動的に修復されます。
4. Universal Recovery Console で、**Reboot**（再起動）をクリックします。

Linux マシンのベアメタル復元の開始

DL1000 では、Linux マシンに対して、システムボリュームのロールバックを含むベアメタル復元（BMR）を実行できます。AppAssure コマンドラインユーティリティの `aamount` を使用して、起動ボリュームのベースイメージにロールバックします。Linux マシンの BMR を実行するには、まず最初に次の操作を行っておく必要があります。

- AppAssure サポートから、Linux の起動可能バージョンが保存された BMR Live CD ファイルを取得します。

  メモ: Linux Live CD ファイルは **https://licenseportal.com** にあるライセンスポータルからもダウンロードできます。
- ソースボリュームを格納する宛先パーティションをターゲットマシン上に作成するために、ハードドライブ上に十分な容量が存在することを確認します。宛先パーティションのサイズは、オリジナルのソースパーティションと同じかそれ以上にする必要があります。
- ロールバックのパスを確認します。このパスは、デバイスファイル記述子で表されます。デバイスファイル記述子で表されたパスを確認するには、ターミナルウィンドウから `fdisk` コマンドを使用します。

  メモ: AppAssure コマンドの利用を開始する前に、screen ユーティリティをインストールできます。screen ユーティリティでは、リカバリポイントのリストなど、大量のデータを表示する際に画面をスクロールさせることができます。

Linux マシンのベアメタル復元を実行するには、次の手順を実行します。

1. AppAssure から受け取った Live CD ファイルを使用して Linux マシンを起動し、ターミナルウィンドウを開きます。
2. 必要な場合は、たとえば `fdisk` コマンドを root として実行するなどの方法で新しいディスクパーティションを作成し、`a` コマンドを使用してこのパーティションを起動可能にします。
3. 次のように、AppAssure `aamount` ユーティリティをルートとして実行します。

   ```
   sudo aamount
   ```
4. AppAssure のマウントプロンプトで、次のコマンドを入力して保護対象マシンのリストを表示します。

   ```
   lm
   ```
5. プロンプトが表示されたら、AppAssure Core サーバーの IP アドレスまたはホスト名を入力します。
6. このサーバーに対するログオン資格情報、つまり、ユーザー名とパスワードを入力します。

この AppAssure Core サーバーによって保護されているマシンのリストが表示されます。このリストには、ラインアイテム番号、ホスト /IP アドレス、およびマシンの ID 番号（例：293cc667-44b4-48ab-91d8-44bc74252a4f）で検出されたマシンがリストされます。

7. 復元するマシンに現在マウントされているリカバリポイントのリストを表示するには、次のコマンドを入力します。

   `lr <machine_line_item_number>`

   メモ: このコマンドでは、ラインアイテム番号の代わりにマシン ID 番号を入力することもできます。

   そのマシンのベースおよび増分リカバリポイントのリストが表示されます。このリストには、ラインアイテム番号、日付 / タイムスタンプ、ボリュームの場所、リカバリポイントのサイズ、およびリカバリポイントを特定するシーケンス番号を末尾に含むボリュームの ID 番号（例：293cc667-44b4-48ab-91d8-44bc74252a4f:2）が表示されます。

8. ロールバック用のベースイメージリカバリポイントを選択するには、次のコマンドを入力します。

   `r <volume_base_image_recovery_point_ID_number> <path>`

   注意: システムボリュームがマウントされていないことを確認する必要があります。

   このコマンドは、ID で指定されたボリュームイメージを Core から指定のパスにロールバックします。ロールバックのパスは、デバイスのファイル記述子のパスであり、マウント先のディレクトリではありません。

   メモ: また、リカバリポイントを識別するために、リカバリポイントの ID 番号の代わりにコマンドにライン番号を指定することもできます。**r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>** のようにエージェント / マシンライン番号（lm の出力からのもの）を使用し、その後にリカバリポイントライン番号とボリューム文字、最後にパスを続けます。このコマンドでは、<path> は実際のボリュームのファイル記述子です。

9. 続行するかどうかを尋ねるプロンプトが表示されたら、Yes を示す y を入力します。

   ロールバックが続行されると、ステータスを通知する一連のメッセージが表示されます。

10. ロールバックが成功したら、必要に応じて復元したブートローダーでメインの起動レコードをアップデートします。

    メモ: ブートローダーの修復またはセットアップは、このディスクが新しい場合のみ必要です。同一ディスクへの単純なロールバックである場合、ブートローダーのセットアップは必要ありません。

    注意: 保護対象 Linux ボリュームを手動でマウント解除しないでください。保護対象 Linux ボリュームを手動でマウント解除する必要がある場合は、ボリュームをマウント解除する前に、bsctl -d <path to volume> コマンドを実行する必要があります。

    このコマンドで、<path to volume> はボリュームのマウントポイントではなく、ボリュームのファイル記述子を参照しています。形式は **/dev/sda1** のようにする必要があります。

screen ユーティリティのインストール

AppAssure コマンドの利用を開始する前に、screen ユーティリティをインストールできます。screen ユーティリティでは、リカバリポイントのリストなど、大量のデータを表示する際に画面をスクロールさせることができます。

screen ユーティリティをインストールするには、次の手順を実行します。

1. Live CD ファイルを使用して、Linux マシンを起動します。

ターミナルウィンドウが開きます。

2. コマンド `sudo apt-get install screen` を入力します。
3. screen ユーティリティを起動するには、コマンドプロンプトで `screen` と入力します。

Linux マシンでの起動可能パーティションの作成

Linux マシン上でコマンドラインを使用して起動可能パーティションを作成するには、次の手順を実行します。

1. **bsctl** ユーティリティを使用してすべてのデバイスに接続します。これには、`sudo bsctl --attach-to-device /dev/<restored volume>` コマンドを root で実行します。

   メモ: この手順を復元ボリュームごとに繰り返します。

2. 次のコマンドを使用して、各復元ボリュームをマウントします。

   ```
   mount /dev/<restored volume> /mnt

   mount /dev/<restored volume> /mnt
   ```

   メモ: システム構成によっては、ルートボリュームの一部として起動ディレクトリが含まれる場合があります。

3. 次のコマンドを使用して、各復元ボリュームのスナップショットメタデータをマウントします。

   ```
   sudo bsctl --reset-bitmap-store /dev/<restored volume>

   sudo bsctl --map-bitmap-store /dev/<restored volume>
   ```

4. `blkid` コマンドか、`ll /dev/disk/by-uuid` コマンドを使用して、汎用一意識別子（UUID）に新しいボリュームが含まれていることを確認します。
5. `/etc/fstab` にルートボリュームと起動ボリュームの正しい UUID が含まれていることを確認します。
6. 次のコマンドを使用して、Grand Unified Bootloader（GRUB）をインストールします。

   ```
   mount --bind /dev/ /mnt/dev

   mount --bind /proc/ /mnt/proc

   chroot/mnt/bin/bash

   grub-install/dev/sda
   ```

7. **/boot/grub/grub.conf** ファイルにルートボリュームの正しい UUID が含まれていることを確認するか、必要に応じてテキストエディタを使用してアップデートします。
8. Live CD ディスクを CD-ROM ドライブから取り出し、Linux マシンを再起動します。

5

リカバリポイントの複製

Replicatoin（複製）

レプリケーションとは、災害リカバリを目的として、リカバリポイントをコピーしてセカンダリの場所に転送するプロセスのことです。このプロセスには、2 つのコア間におけるペアリングされたソース-ターゲット関係が必要です。レプリケーションは保護対象マシン単位で管理されます。つまり、保護対象マシンのバックアップスナップショットがターゲットレプリケーションコアにレプリケートされるということです。レプリケーションがセットアップされると、ソースコアは増分スナップショットデータをターゲットコアに対して非同期的かつ継続的に送信します。このアウトバウンドレプリケーションは、会社が所有するデータセンターやリモート災害復旧サイト（つまり「自己管理型」ターゲットコア）、またはオフサイトバックアップおよび災害復旧サービスを提供するマネージドサービスプロバイダ（MSP）に対して設定することができます。MSP に対してレプリケーションを行うときは、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することができます。

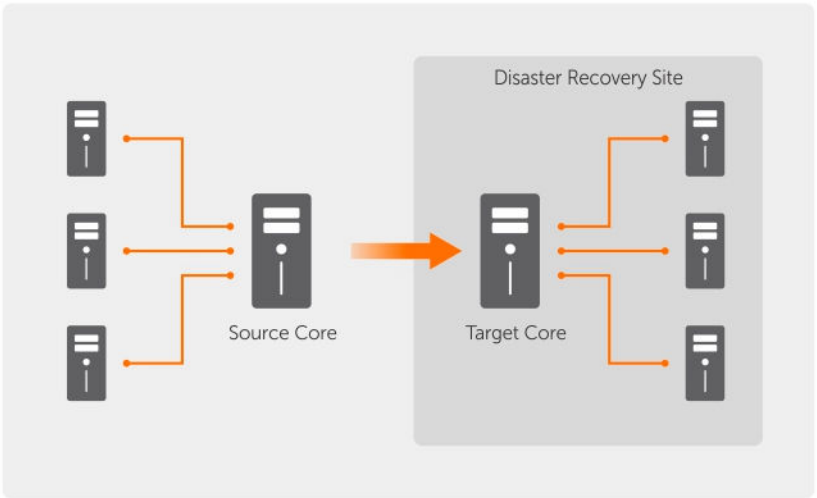

図 5. 基本的な複製アーキテクチャ

レプリケーションでは、シーディング（保護対象エージェント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。最初のレプリケーションは、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レプリケーションされます。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、新たにレプリケーションされた増分リカバリポイントは自動的に同期されます。

レプリケーション実行のためのロードマップ

AppAssure を使用してデータを複製するには、ソースコアおよびターゲットコアをレプリケーション用に設定する必要があります。レプリケーションの設定後、保護対象マシンデータの複製、レプリケーションの監視と管理、およびリカバリの実行を行うことができます。

AppAssure でのレプリケーションの実行には、以下の操作の実行が含まれます。

- 自己管理レプリケーションの設定。自己管理ターゲットコアへの複製についての詳細は、「自己管理コアへの複製」を参照してください。
- 第三者レプリケーションの設定。第三者ターゲットコアへの複製についての詳細は、「第三者が管理するコアへの複製」を参照してください。
- ソースコアに接続された新しい保護対象マシンの複製。保護対象マシンの複製の詳細については、「新しい保護対象マシンの複製」を参照してください。
- 既存の保護対象マシンの複製。レプリケーション用エージェントの設定についての詳細は、「マシン上のエージェントデータの複製」を参照してください。
- エージェントのレプリケーション優先順位の設定。エージェントのレプリケーションの優先順位付けの詳細については、「エージェントのレプリケーション優先度の設定」を参照してください。
- 必要に応じたレプリケーションの監視。レプリケーションの監視の詳細については、「レプリケーションの監視」を参照してください。
- 必要に応じたレプリケーション設定の管理。レプリケーション設定の管理についての詳細は、「レプリケーション設定の管理」を参照してください。
- 災害またはデータ損失発生時における複製済みデータのリカバリ。複製済みデータのリカバリについての詳細は、「複製済みデータのリカバリ 」を参照してください。

自己管理コアへの複製

自己管理コアとは、自分がアクセスできるコアのことであり、多くの場合、オフサイトロケーションにおいて自社が管理しているコアのことです。データのシーディングを選択しない限り、複製はソースコア上で完全に実行できます。シーディングを行う場合は、ソースコア上で複製を設定した後、ターゲットコア上でシードドライブを取り込む必要があります。

メモ: この設定は、オフサイトロケーション、および相互レプリケーションへのレプリケーションに適用されます。Core は、すべてのソースおよびターゲットマシンにインストールされている必要があります。お使いのシステムをマルチポイントツーポイントレプリケーション用に設定している場合は、このタスクをすべてのソースコア、および 1 つのターゲットコアで実行する必要があります。

自己管理ターゲットコアへ複製するソースコアの設定

自己管理ターゲットコアへ複製するようにソースコアを設定するには、次の手順を実行します。

1. Core で、**Replication**（レプリケーション）タブをクリックします。
2. **Add Target Core**（ターゲットコアの追加）をクリックします。
   Replication（レプリケーション）ウィザードが表示されます。
3. **I have my own Target Core**（ターゲットコアを所有しています）を選択し、次の表の説明どおりに情報を入力します。

テキストボックス	説明
ホスト名	レプリケート先のコアマシンのホスト名または IP アドレスを入力します。
ポート	AppAssure Core がマシンとの通信に使用するポート番号を入力します。デフォルトのポート番号は 8006 です。
ユーザー名	マシンにアクセスするためのユーザー名（たとえば **Administrator**）を入力します。
パスワード	マシンにアクセスするためのパスワードを入力します。

追加する Core が以前にこのソースコアとペアになっていた場合は、次の手順を実行します。

a. **Use an existing target core**（既存ターゲットコアの使用）を選択します。
b. ドロップダウンリストからターゲットコアを選択します。
c. **次へ** をクリックします。
d. 手順 7 に進みます。

4. **次へ** をクリックします。
5. **Details**（詳細）ページで、このレプリケーション設定の名前を入力します（例：SourceCore1 など）。以前のレプリケーション設定を再開または修復している場合は、**My Core has been migrated and I would like to repair replication**（コアは移行済みなのでレプリケーションを修復します）を選択します。
6. **次へ** をクリックします。
7. **Agents**（エージェント）ページで、複製するエージェントを選択し、**Repository**（リポジトリ）列のドロップダウンリストを使用して各エージェントのリポジトリを選択します。
8. ベーステータ転送用のシーディングプロセスを実行する予定がある場合は、次の手順を実行します。

メモ: 量のデータをポータブルストレージデバイスにコピーする必要があるため、ポータブルストレージデバイスには eSATA、USB 3.0、またはその他の高速接続の使用をお勧めします。

a. **Agents**（エージェント）ページで、**Use a seed drive to perform initial transfer**（シードドライブを使用して初回転送を実行）を選択します。現在、1 つ以上のマシンがターゲットコアに複製されている場合は、**With already replicated**（複製済みに含める）を選択して、それらの保護対象マシンをシードドライブに含めることができます。
b. **次へ** をクリックします。
c. **Seed Drive Location**（シードドライブの場所）ページで、**Location type**（場所のタイプ）ドロップダウンリストを使用して次のいずれかを選択します。
   - ローカル：**Location**（場所）テキストボックスで、シードドライブを保存する場所（例：D:\work\archive など）を入力します。
   - ネットワーク：**Location**（場所）テキストボックスで、シードドライブを保存する場所を入力し、**User name**（ユーザー名）および **Password**（パスワード）テキストボックスにネットワーク共有の資格情報を入力します。
   - クラウド：**Account**（アカウント）テキストボックスでアカウントを選択します。クラウドアカウントを選択するには、最初にそのアカウントを Core Console に追加している必要があります。詳細については、クラウドアカウントの追加を参照してください。お使いのアカウントに関連付けられた **Container**（コンテナ）を選択します。アーカイブデータの保存先となる **Folder Name**（フォルダ名）を選択します。
d. **Next**（次へ）をクリックします。

9. **Seed Drive Option**（シードドライブオプション）ダイアログボックスで、次に説明する情報を入力します。

テキストボックス	説明
Maximum size（最大サイズ）	大規模なデータのアーカイブは複数のセグメントに分割することができます。次の操作のいずれかを行って、シードドライブ作成のために予約するセグメントの最大サイズを選択します。 • Seed Drive Location（シードドライブの場所）ページで入力したパスに、今後の使用のために使用可能な容量をすべて予約するには、**Entire Target**（ターゲット全体）を選択します（例：場所が D:\work\archive になっていると、シードドライブのコピーに必要な場合に D: ドライブ上の使用可能な容量すべてが予約されますが、コピープロセスを開始してすぐには予約されません）。 • 予約したい最大容量をカスタマイズするには、空のテキストボックスを選択し、値を入力して、ドロップダウンメニューから値の単位を選択します。
Customer ID（カスタマ ID）（オプション）	オプションとして、サーバープロバイダによってユーザーに割り当てられたカスタマ ID を入力します。
Recycle action（リサイクルアクション）	パスにすでにシードドライブが含まれている場合は、次のいずれかのオプションを選択します。 • **Do not reuse**（再使用しない）— その場所の既存のデータを上書きしたり、クリアしたりしません。その場所が空の場合、シードドライブの書き込みは失敗します。 • **Replace this core**（このコアを置き換える）— このコアに関連する既存のデータを上書きしますが、他のコアのデータはそのまま残します。 • **Erase completely**（完全に消去）— シードドライブを書き込む前にディレクトリからすべてのデータをクリアします。
Comment（コメント）	アーカイブについてのコメントまたは説明を入力します。
Add all Agents to Seed Drive（シードドライブにすべてのエージェントを追加する）	シードドライブを使用してレプリケートするエージェントを選択します。
Build RP chains (fix orphans)（RP チェーンを構築する（孤立の修復））	リカバリポイントチェーン全体をシードドライブに複製するには、このオプションを選択します。このオプションはデフォルトで選択されています。 AppAssure での一般的なシーディングでは、最新のリカバリポイントのみをシードドライブに複製することによって、シードドライブの作成に必要な時間と容量を軽減します。シードドライブへのリカバリポイント（RP）チェーンの構築を選択すると、指定されたエージェントからの最新リカバリポイントを保存するために十分な容量がシードドライブ上に必要であり、その作業を完了するためにさらに時間がかかる場合があります。
Use compatible format（互換性のある形式を使用する）	AppAssure Core の新旧両バージョンとの互換性のあるフォーマットでシードドライブを作成する場合は、このオプションを選択します。

10. **Agents**（エージェント）ページで、シードドライブを使用してターゲットコアに複製するエージェントを選択します。
11. **終了** をクリックします。
12. シードドライブを作成した場合は、お使いのターゲットコアに送信します。

    ソースコアのターゲットペアへのペアリングが完了しました。レプリケーションが開始されますが、シードドライブが消費され、必要なベースイメージが提供されるまでは、ターゲットコアに孤立したリカバリポイントが作成されます。

ターゲットコア上のシードドライブの消費

この手順は、自己管理 Core 用レプリケーションの設定中にシードドライブを作成した場合にのみ、必要になります。
ターゲットコア上でシードドライブを取り込むには、次の手順を実行します。

1. シードドライブを USB ドライブなどのポータブルストレージデバイスに保存した場合は、ドライブをターゲットコアに接続します。
2. ターゲットコア上の Core Console から、**Replication**（レプリケーション）タブを選択します。
3. **Incoming Replication**（受信複製）にあるドロップダウンメニューを使用して正しいソースコアを選択し、**Consume**（消費）をクリックします。

   Consume（消費）ウィンドウが表示されます。
4. **Location Type**（場所のタイプ）には、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。
   - Local（ローカル）
   - Network（ネットワーク）
   - Cloud（クラウド）
5. 必要に応じて次の情報を入力します。

テキストボックス	説明
Location（場所）	USB ドライブやネットワーク共有など、シードドライブの場所を表すパスを入力します（D:\ など）。
User Name（ユーザー名）	共有ドライブまたはフォルダのユーザー名を入力します。ネットワークパスの場合にのみユーザー名が必要です。
Password（パワード）	共有ドライブまたはフォルダのパスワードを入力します。ネットワークパスの場合にのみパスワードが必要です。
Account（アカウント）	ドロップダウンリストからアカウントを選択します。クラウドアカウントを選択するには、最初にそのアカウントを Core Console に追加している必要があります。
Container（コンテナ）	ドロップダウンメニューからお使いのアカウント関連づけられているコンテナを選択します。
Folder Name（フォルダ名）	アーカイブデータが保存されたフォルダの名前（例 : -Archive-[DATE CREATED]-[TIME CREATED]）を入力します。

6. **Check File**（ファイルのチェック）をクリックします。

   Core がファイルをチェックした後、Core はそのシードドライブに格納されている最古および最新のリカバリポイントの日付を **Date Range**（日付範囲）に自動で入力します。また、Configuring Replication

For A Self-Managed Core（自己管理 Core 用レプリケーションの設定）で入力したコメントもインポートします。

7. **Consume**（消費）ウィンドウの **Agent Names**（エージェント名）で、データを取り込むマシンを選択し、**Consume**（消費）をクリックします。

   メモ: データ取り込みの進捗状況を監視するには、**Events**（イベント）タブを選択します。

未処理のシードドライブの破棄

ターゲットコアで取り込むことを意図してシードドライブを作成したにもかかわらず、そのシードドライブをリモートロケーションに送信しないことを選択した場合、ソースコアの **Replication**（レプリケーション）タブに未処理のシードドライブのリンクが残ります。未処理のシードドライブは、別のシードデータや最新のシードデータを優先するために放棄することができます。

メモ: この手順により、未処理のシードドライブへのリンクがソースコア上の Core Console から削除されますが、ドライブ自体は保存先のストレージの場所から削除されません。

未処理のシードドライブを放棄するには、次の手順を実行します。

1. ソースコア上の Core Console から、**Replication**（レプリケーション）タブを選択します。
2. **Outstanding Seed Drive (#)**（未処理のシードドライブ（#））をクリックします。

   Outstanding seed drives（未処理のシードドライブ）セクションが表示されます。このセクションには、リモートターゲットコアの名前、シードドライブが作成された日時、およびシードドライブ上に含まれているリカバリポイントのデータ範囲が含まれます。
3. 破棄するドライブのドロップダウンメニューをクリックし、**Abandon**（放棄）を選択します。

   Outstanding Seed Drive（未処理のシードドライブ）ウィンドウが表示されます。
4. **Yes**（はい）をクリックして、アクションを確定します。

   シードドライブが削除されます。ソースコア上にシードドライブが 1 つも存在しなくなると、次回 **Replication**（レプリケーション）タブを開くときに、**Outstanding Seed Drive (#)**（未処理のシードドライブ（#））リンクと **Outstanding seed drives**（未処理のシードドライブ）セクションは表示されません。

第三者が管理するコアへの複製

第三者コアとは、MSP によって管理とメンテナンスが行われているターゲットコアのことです。第三者が管理するコアに複製する場合は、ターゲットコアにアクセスする必要はありません。お客様がソースコア上で複製を設定した後、MSP がターゲットコア上の設定を行います。

メモ: この設定は、ホストされているレプリケーション、クラウドレプリケーションに適用されます。AppAssure Core はすべてのソースコアマシンにインストールされている必要があります。

新規エージェントの複製

保護のために AppAssure Agent をソースコアに追加する時、AppAssure は新規エージェントを既存のターゲットコアに複製するオプションを提供します。

新規エージェントを複製するには、次の手順を実行します。

1. Core Console に移動し、**Machines**（マシン）タブをクリックします。
2. **Actions**（アクション）ドロップダウンメニューで、**Protect Machine**（マシンを保護）をクリックします。
3. **Protect Machine**（マシンの保護）ダイアログボックスで、次の表の説明に従って情報を入力します。

テキストボックス	説明
Host（ホスト）	保護するマシンのホスト名または IP アドレスを入力します。
Port（ポート）	AppAssure Core がマシン上のエージェントと通信するために使用するポート番号を入力します。
Username（ユーザー名）	このマシンに接続するためのユーザー名（Administrator など）を入力します。
Password（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を入力します。

4. **Connect**（接続）をクリックして、このマシンに接続します。
5. **Show Advanced Options**（詳細オプションの表示）をクリックし、必要に応じて次の設定を編集します。

テキストボックス	説明
Display Name（表示名）	Core Console 内で表示されるマシンの新しい名前を入力します。
Repository（リポジトリ）	このマシンのデータを保存する AppAssure Core 上のリポジトリを選択します。
Encryption Key（暗号化キー）	リポジトリに保存されるマシン上の各ボリュームのデータに暗号化を適用するかどうかを指定します。 **メモ:** リポジトリの暗号化設定は、Core Console の **Configuration**（設定）タブで定義されます。
Remote Core（リモートコア）	エージェントの複製先にするターゲットコアを指定します。
Remote Repository（リモートリポジトリ）	このマシンからの複製されたデータを保存するターゲットコア上のリポジトリの名前です。
Pause（一時停止）	レプリケーションを一時停止する場合にこのチェックボックスを選択します。たとえば、AppAssure が新規エージェントのベースイメージを取得するまで一時停止するなどです。
Schedule（スケジュール）	次のオプションのいずれかを選択します。 • Protect all volumes with default schedule（すべてのボリュームをデフォルトスケジュールで保護） • Protect specific volumes with custom schedule（特定のボリュームをカスタムスケジュールで保護） **メモ:** デフォルトのスケジュールは 15 分ごとです。
Initially pause protection（保護を当初一時停止）	保護を一時停止する場合にこのチェックボックスを選択します。例えば、使用ピーク時後までは AppAssure がベースイメージを取得しないようにするなどです。

6. **Protect**（保護）をクリックします。

マシン上のエージェントデータの複製

レプリケーションとは、同一サイト、またはエージェント単位で低速リンクを使用する 2 つのサイトにまたがったターゲットコアとソースコアの関係です。2 つのコア間でレプリケーションがセットアップされると、ソースコアは非同期的に特定のエージェントの増分スナップショットデータをターゲットコアまたはソースコアに送信します。アウトバウンドレプリケーションは、オフサイトバックアップおよび災害復旧サービスを提供するマネージドサービスプロバイダ、または自己管理コアに設定できます。マシン上のエージェントデータを複製するには、次の手順を実行します。

1. Core Console で **Machines**（マシン）タブをクリックします。
2. 複製するマシンを選択します。
3. **Actions**（アクション）ドロップダウンメニューで **Replication**（レプリケーション）をクリックし、次のオプションのひとつを完了します。
   - レプリケーションのセットアップ中の場合は、**Enable**（有効化）をクリックします。
   - すでに既存のレプリケーションセットアップがある場合は、**Copy**（コピー）をクリックします。

   Enable Replications（レプリケーションを有効にする）ダイアログボックスが表示されます。
4. **Host**（ホスト）テキストボックスにホスト名を入力します。
5. **Agents**（エージェント）から、複製するエージェントとデータを持つマシンを選択します。
6. 必要に応じて、**Use a seed drive to perform initial transfer**（シードドライブを使用して初期転送を実行する）チェックボックスをオンにします。
7. **Add**（追加）をクリックします。
8. 複製を一時停止または再開するには、**Actions**（アクション）ドロップダウンメニューで **Replication**（複製）をクリックし、必要に応じて **Pause**（一時停止）または **Resume**（再開）をクリックします。

エージェントに対するレプリケーション優先度の設定

エージェントのレプリケーション優先度を設定するには、次の手順を実行します。

1. Core Console で、レプリケーション優先度を設定する保護対象マシンを選択し、**Congifutartion**（設定）タブをクリックします。
2. **Select Transfer Settings**（転送設定の選択）をクリックし、**Priority**（優先度）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。
   - **デフォルト**
   - **Highest（最高）**
   - **Lowest（最低）**
   - **1**
   - **2**
   - **3**
   - **4**

   メモ: デフォルト優先度は 5 です。あるエージェントに優先度 1 を与え、別のエージェントに優先度 Highest（最高）を与えた場合、優先度 1 のエージェントよりも先に Highest（最高）優先度のエージェントの複製が行われます。
3. **OK** をクリックします。

レプリケーションの監視

レプリケーションがセットアップされると、ソースコアおよびターゲットコアに対するレプリケーションタスクのステータスを監視できるようになります。ステータス情報の更新、レプリケーションの詳細表示などの操作が可能です。

レプリケーションを監視するには、次の手順を実行します。

1. Core Console で、**Replication**（レプリケーション）タブをクリックします。
2. このタブで、以下に説明されているとおり、複製タスクのステータスの監視と情報の表示を行うことができます。

表 4. レプリケーションの監視

セクション	説明	利用可能なアクション
Pending Replication Requests（保留中のレプリケーションリクエスト）	複製リクエストが第三者サービスプロバイダに送信されたときのカスタマー ID、E-メールアドレス、およびホスト名をリストします。MSP がリクエストを受け入れるまでここにリストされます。	ドロップダウンメニューで、**Ignore**（無視）をクリックして、リクエストを無視または拒否します。
Outstanding Seed Drives（未処理のシードドライブ）	書き込まれたものの、ターゲットコアにまだ取り込まれていないシードドライブを示します。これには、リモートコア名、作成された日付、および日付範囲が含まれます。	ドロップダウンメニューで、**Abandon**（放棄）をクリックして、シードプロセスを放棄またはキャンセルします。
Outgoing Replication（送信レプリケーション）	ソースコアがレプリケーションを行っているすべてのターゲットコアを示します。これには、リモートコア名、存在状態、レプリケーションされている保護対象マシンの数、およびレプリケーション転送の進捗状況が含まれます。	ソースコアでは、ドロップダウンメニューから以下のオプションを選択できます。 • **Details**（詳細）- 複製されたコアの ID、URI、表示名、状態、カスタマー ID、E-メールアドレス、およびコメントをリストします。 • **Change Settings**（設定の変更）— 表示名を示し、ターゲットコアのホストとポートを編集できるようにします。 • **Add Agents**（エージェントの追加）— ドロップダウンリストからホストを選択して、レプリケーション用の保護対象マシンを選択し、新しい保護対象マシンの初期転送に使用するシードドライブを作成できます。
Incoming Replication（受信レプリケーション）	ターゲットがレプリケートされたデータを受信する、すべてのソースマシンをリストします。こ	ターゲットコアでは、ドロップダウンメニューから以下のオプションを選択できます。 • **Details**（詳細）- 複製されたコアの ID、ホスト名、カスタ

セクション	説明	利用可能なアクション
	れには、リモートコア名、状態、マシン、および進捗状況が含まれます。	マー ID、E-メールアドレス、およびコメントをリストします。 • **Consume**（消費）- シードドライブから初期データを取り込み、ローカルリポジトリに保存します。

3. **Refresh**（更新）ボタンをクリックして、このタブのセクションを最新情報でアップデートします。

レプリケーション設定の管理

ソースコアおよびターゲットコアでのレプリケーションの実行方法について多くの設定を調整できます。
レプリケーション設定を管理するには、次の手順を実行します。

1. Core Console で、**Replication**（レプリケーション）タブをクリックします。
2. **Actions**（アクション）ドロップダウンメニューで、**Settings**（設定）をクリックします。
3. **Replication Settings**（レプリケーション設定）ウィンドウで、以下の説明どおりにレプリケーション設定を編集します。

オプション	説明
Cache lifetime（キャッシュの有効期間）	ソースコアによって実行される各ターゲットコアのステータス要求間の時間間隔を指定します。
Volume image session timeout（ボリュームイメージセッションタイムアウト）	ソースコアがターゲットコアへのボリュームイメージの転送試行に費やす時間を指定します。
Max. concurrent replication jobs（最大同時レプリケーションジョブ数）	ターゲットコアに一度に複製できる保護対象マシンの数を指定します。
Max. parallel streams（最大パラレルストリーム数）	1 つの保護対象マシンがマシンのデータを一度に複製するために使用できるネットワーク接続の数を指定します。

4. **Save**（保存）をクリックします。

レプリケーションの削除

レプリケーションを中断して、いくつかの方法で保護されたマシンをレプリケーションから削除できます。
次のオプションがあります。

- ソースコア上のレプリケーションからのエージェントの削除
- ターゲットコア上のエージェントの削除
- レプリケーションからのターゲットコアの削除
- レプリケーションからのソースコアの削除

メモ: ソースコアを削除すると、そのコアによって保護されたすべての複製済みマシンが削除されます。

ソースコア上のレプリケーションからの保護対象マシンの削除

ソースコア上のレプリケーションから保護対象マシンを削除するには、次の手順を実行します。

1. ソースコアから Core Console を開き、**Replication**（レプリケーション）タブをクリックします。
2. **Outgoing Replication**（送信レプリケーション）セクションを展開します。
3. レプリケーションから削除する保護対象マシンのドロップダウンメニューで **Delete**（削除）をクリックします。
4. **Outgoing Replication**（送信レプリケーション）ダイアログボックスで、**Yes**（はい）をクリックして削除を確定します。

ターゲットコア上の保護対象マシンの削除

ターゲットコア上の保護対象マシンを削除するには、次の手順を実行します。

1. ターゲットコアで Core Console を開き、**Replication**（レプリケーション）タブをクリックします。
2. **Incoming Replication**（受信レプリケーション）セクションを展開します。
3. レプリケーションから削除する保護対象マシンのドロップダウンメニューで **Delete**（削除）をクリックしてから、以下のオプションのいずれを選択します。

オプション	説明
Relationship Only（関係のみ）	レプリケーションから保護対象マシンを削除しますが、複製されたリカバリポイントは残します。
With Recovery Point（リカバリポイントも含む）	レプリケーションから保護対象マシンを削除して、そのマシンから受信した複製リカバリポイントをすべて削除します。

レプリケーションからのターゲットコアの削除

レプリケーションからターゲットコアを削除するには、次の手順を実行します。

1. ソースコアで Core Console を開き、**Replication**（レプリケーション）タブをクリックします。
2. **Outgoing Replication**（送信レプリケーション）で、削除したいリモートコアの横にあるドロップダウンメニューをクリックして、**Delete**（削除）をクリックします。
3. **Outgoing Replication**（送信レプリケーション）ダイアログボックスで、**Yes**（はい）をクリックして削除を確定します。

レプリケーションからのソースコアの削除

メモ: ソースコアを削除すると、そのコアによって保護されていた複製済みエージェントがすべて削除されます。

レプリケーションからソースコアを削除するには、次の手順を実行します。

1. ターゲットコアで Core Console を開き、**Replication**（レプリケーション）タブをクリックします。
2. **Incoming Replication**（受信レプリケーション）にあるドロップダウンメニューで、**Delete**（削除）をクリックして、以下のいずれかのオプションを選択します。

オプション	説明
Relationship Only（関係のみ）	レプリケーションからソースコアを削除しますが、複製されたリカバリポイントは残します。
With Recovery Points（リカバリポイントあり）	レプリケーションからソースコアを削除して、そのマシンから受信した複製されたリカバリポイントをすべて削除します。

3. **Incoming Replication**（受信レプリケーション）ダイアログボックスで、**Yes**（はい）をクリックして削除を確定します。

複製されたデータのリカバリ

毎日実行のレプリケーション機能はソースコア上で維持されますが、災害リカバリに必要な機能はターゲットコアのみが完了できます。

災害リカバリの場合、ターゲットコアはレプリケートされたリカバリポイントを使用して、保護されたエージェントとコアを回復できます。

ターゲットコアから以下のリカバリオプションを実行できます。

- Mount recovery points（リカバリポイントをマウントする）。
- Roll back to recovery points（リカバリポイントにロールバックする）。
- Perform a virtual machine（VM）export（仮想マシン（VM）エクスポートを実行する）。
- Perform a bare metal restore（BMR）（ベアメタル復元（BMR）を実行する）。
- Perform Failback（フェールバックを実行する）（フェールオーバー / フェールバックレプリケーション環境のセットアップがある場合）。

フェールオーバーおよびフェールバックの理解

ソースコアとエージェントに障害が発生するような深刻な停電が発生した場合、AppAssure は複製環境でのフェールオーバーとフェールバックをサポートします。フェールオーバーとは、ソースコアおよび関連付けられたエージェントのシステム障害や異常終了が発生したときに、冗長またはスタンバイのターゲット AppAssure Core に切り替える操作を指します。フェールオーバーの主な目的は、不具合のあるエージェントと同一の新しいエージェントを起動することです。第 2 の目的は、ターゲットコアを新しいモードに切り替えることによって、ターゲットコアが、ソースコアの故障前に当初のエージェントを保護していたものと同じ方法でフェールオーバーエージェントを保護するようにすることです。ターゲットコアは、レプリケーとされたエージェントからインスタンスを回復し、フェールオーバーされたマシンに対してただちに保護を開始できます。

フェールバックは、元の状態（障害発生前）にエージェントとコアを復元するプロセスです。フェールバックの主な目的は、新規の一時エージェントの最新状態と同じ状態に、エージェント（ほとんどの場合、これは不具合のあるエージェントと交換した新しいマシン）を復元することです。エージェントが復元されると、復元されたソースコアによって保護されます。レプリケーションも復元され、ターゲットコアは再びレプリケーションターゲットとして機能します。

フェールオーバーの実行

ソースコアと関連エージェントが故障した災害状況が発生した場合、AppAssure のフェールオーバーを有効にして、保護を同一フェールオーバー（ターゲット）コアに切り替えることができます。ターゲットコアは環境内でデータを保護する唯一のコアとなり、その後新しいエージェントを起動して、故障したエージェントの一時的な代替とします。

ターゲットコアでフェールオーバーを実行するには、次の手順を実行します。

1. ターゲットコアで Core Console に移動して、**Replication**（レプリケーション）タブをクリックします。
2. **Incoming Replication**（受信複製）で、ソースコアを選択し、個々のエージェントの詳細を展開します。
3. そのコアの **Actions**（アクション）メニューで、**Failover**（フェールオーバー）をクリックします。
   Fail Over（フェールオーバー）ダイアログが開き、フェールオーバーを完了するための次の手順がリストされます。
4. **続行** をクリックします。
5. **Protected Machines（保護対象マシン）**の左側のナビゲーションエリアで、リカバリポイントに関連する AppAssure Agent ソフトウェアがあるマシンを選択します。
6. そのエージェント上のバックアップリカバリポイント情報を仮想マシンにエクスポートします。
7. そのエージェント上のバックアップリカバリポイント情報を仮想マシンにエクスポートします。
8. 現在エクスポートされたバックアップ情報を持つ仮想マシンを起動します。
   デバイスドライバソフトウェアがインストールされるまで待つ必要があります。
9. 仮想マシンを再起動して、エージェントサービスが開始するまで待ちます。
10. ターゲットコアの Core Console に戻り、**Protected Machines**（保護マシン）と **Incoming Replication**（受信レプリケーション）にある **Replication**（レプリケーション）タブに、新しいエージェントが表示されていることを確認します。
11. 複数スナップショットを強制実行して、正しく実行されたことを確認します。
    詳細については、スナップショットの強制を参照してください。
12. これで、フェールバックの実行に進むことができます。
    詳細については、フェールバックの実行を参照してください。

フェールバックの実行

障害の発生したオリジナルのソースコアおよびエージェントを修復または交換した後、フェールオーバーしたマシンからデータを移動してソースマシンを復元する必要があります。

フェールバックを実行するには、次の手順を実行します。

1. ターゲットコアで Core Console に移動して、**Replication**（レプリケーション）タブをクリックします。
2. **Incoming Replication**（受信レプリケーション）でフェールオーバーエージェントを選択して、詳細を展開します。
3. **Actions**（アクション）メニューで、**Failback**（フェールバック）をクリックします。
   Fail Back（フェールバック）ダイアログボックスが表示され、**Continue**（続行）ボタンをクリックしてフェールバックを完了する前に行う必要がある手順について説明します。
4. **Cancel**（キャンセル）をクリックします。
5. フェールオーバーされたマシンが Microsoft SQL Server または Microsoft Exchange Server を実行している場合、これらのサービスを停止させます。
6. マシンのスナップショットを強制します。詳細については、スナップショットの強制を参照してください。
7. フェールオーバーされたマシンをシャットダウンします。
8. フェールオーバーされたエージェントのアーカイブを作成して、ディスクまたはネットワーク共有の場所に出力します。
   アーカイブの作成の詳細については、アーカイブの作成を参照してください。

9. アーカイブの作成後、新たに修復されたソースコア上の Core Console に移動して、**Tools**（ツール）タブをクリックします。
10. 手順 8 で作成したアーカイブをインポートします。

    詳細については、アーカイブのインポートを参照してください。
11. ターゲットコアの Core Console に移動して、**Replication**（レプリケーション）タブをクリックします。
12. **Incoming Replication**（受信レプリケーション）でフェールオーバーエージェントを選択して、詳細を展開します。
13. **Failback**（フェールバック）ダイアログボックスで、**Continue**（続行）をクリックします。
14. エクスポートされた、フェールオーバーの間に作成されたエージェントを含むマシンをシャットダウンします。
15. ソースコアとエージェントに対してベアメタル復元（BMR）を実行します。

    メモ: 復元を開始する際は、ターゲットコアから仮想マシン上のエージェントにインポートされたリカバリポイントを使用する必要があります。
16. BMR 再起動とエージェントサービスが再起動するのを待ち、マシンのネットワーク接続詳細を表示および記録します。
17. ソースコア上の Core Console に移動して、**Machines**（マシン）タブで、マシン保護設定を変更して新しいネットワーク接続詳細を追加します。

    詳細については、マシンの設定を参照してください。
18. ターゲットコアの Core Console に移動して、**Replication**（レプリケーション）タブからエージェントを削除します。
19. ソースコアの Core Console で、**Replication**（レプリケーション）タブをクリックしてからレプリケーション用にターゲットコアを追加することにより、ソースとターゲット間のレプリケーションをもう一度セットアップします。

6

レポート

レポートについて

お使いの DL アプライアンスでは、複数のコアマシンおよびエージェントマシンについてのコンプライアンス、エラー、およびサマリ情報を生成し、表示することができます。

レポートはオンラインで表示するか、印刷するか、エクスポートしてサポート対象のいずれかのフォーマットで保存できます。次のフォーマットから選択できます。

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- イメージ

レポートツールバーについて

すべてのレポートに使用可能なツールバーでは、2 とおりの方法でレポートを印刷および保存することができます。次の表で、印刷オプションおよび保存オプションについて説明します。

アイコン	説明
	レポートを印刷します。
	現在のページを印刷します。
	レポートをエクスポートしてディスクに保存します。
	レポートをエクスポートして新しいウィンドウに表示します。 他のユーザーがレポートをウェブブラウザで表示できるように、このオプションを使用して URL をコピー、貼り付けし、電子メールで送信します。

コンプライアンスレポートについて

コンプライアンスレポートは、Core と AppAssure Agent に対して使用できます。このレポートを使用して、選択したコアまたはエージェントによって実行されたジョブのステータスを表示できます。失敗したジョブは、赤色のテキストで表示されます。エージェントに関連付けられていないコアコンプライアンスレポート内の情報は空になります。

ジョブの詳細は、次のカテゴリを含む列ビューに表示されます。

- Core（コア）
- Protected Agent（保護されたエージェント）
- Type（タイプ）
- Summary（サマリ）
- Status（ステータス）
- Error（エラー）
- Start Time（開始時刻）
- End Time（終了時刻）
- Time（時刻）
- Total Work（作業合計）

エラーレポートについて

エラーレポートはコンプライアンスレポートのサブセットであり、Core と AppAssure Agent に対して使用できます。エラーレポートには、コンプライアンスレポートにリストされている失敗ジョブのみが含められ、それらのジョブを印刷およびエクスポート可能な単一のレポートにまとめられています。

エラーの詳細は、次のカテゴリを含む列ビューに表示されます。

- Core（コア）
- Agent（エージェント）
- Type（タイプ）
- Summary（サマリ）
- Error（エラー）
- Start Time（開始時刻）
- End Time（終了時刻）
- Elasped Time（経過時間）
- Total Work（作業合計）

。

コアサマリレポートについて

コアサマリレポート には、選択した Core 上のリポジトリについて、およびそのコアによって保護されているエージェントについての情報が含まれます。これらの情報は、1 つのレポート内で 2 つのサマリとして表示されます。

リポジトリサマリ

Core Summary Report（コアサマリレポート）の **Repositories**（リポジトリ）部分には、選択されたコア上のリポジトリに関するデータが含まれます。リポジトリの詳細は、次のカテゴリの列に表示されます。

- Name（名前）
- Data Path（データパス）
- Metadata Path（メタデータパス）
- Allocated Space（割り当て済み容量）

- Used Space（使用容量）
- Free Space（空き容量）
- Compression/Dedupe Ratio（圧縮 / 重複排除比）

エージェントサマリ

Core Summary Report（コアサマリレポート）の **Agents**（エージェント）部分には、選択されたコアによって保護されているすべてのエージェントのデータが含まれます。

エージェントの詳細は、次のカテゴリの列に表示されます。

- Name（名前）
- Protected Volumes（保護対象ボリューム）
- Total protected space（保護対象容量の合計）
- Current protected space（現在保護されている容量）
- Change rate per day（1 日あたりの変化率）（**Average**（平均）、**Median**（中央値））
- Jobs Statistic（ジョブ統計）（**Passed**（合格）、**Failed**（失敗）、**Canceled**（キャンセル））

コアまたはエージェントのレポートの生成

コアまたはエージェントのレポートを生成するには、次の手順を実行します。

1. Core Console に移動し、レポートを実行する Core またはエージェントを選択します。
2. **Tools**（ツール）タブをクリックします。
3. **Tools**（ツール）タブで、左のナビゲーション領域内の **Reports**（レポート）を展開します。
4. 左のナビゲーション領域で、実行するレポートを選択します。使用可能なレポートは、手順 1 で行った選択に応じて異なります。それらを以下に説明します。

Machine（マシン）	Available Reports（使用可能なレポート）
Core（コア）	Compliance Report（コンプライアンスレポート） Summary Report（サマリレポート） Errors Report（エラーレポート）
Agent（エージェント）	Compliance Report（コンプライアンスレポート） Errors Report（エラーレポート）

5. **Start Time**（開始時刻）ドロップダウンカレンダーで、開始日付を選択してから、レポートの開始時刻を入力します。

   メモ: コアまたはエージェントが展開される以前の使用可能なデータはありません。
6. **End Time**（終了時刻）ドロップダウンカレンダーで、終了日付を選択してから、レポートの終了時刻を入力します。
7. **Core Summary Report**（コアサマリレポート）の場合、**Start Time**（開始時刻）と **End Time**（終了時刻）でコアの全期間を設定する場合は、**All Time**（全期間）チェックボックスをオンにします。
8. **Core Compliance Report**（コアコンプライアンスレポート）または **Core Errors Report**（コアエラーレポート）の場合、**Target Cores**（ターゲットコア）ドロップダウンリストを使用して、データを表示するコアを選択します。
9. **Generate Report**（レポートの生成）をクリックします。

レポートの生成後、ツールバーを使用してそのレポートを印刷またはエクスポートできます。

Central Management Console Core レポートについて

DL アプライアンスでは、複数の Core についてのコンプライアンス、エラー、およびサマリ情報を生成し、表示することができます。Core についての詳細は、本項で説明したものと同じカテゴリがある列ビューに表示されます。

Central Management Console からのレポートの生成

Central Management Console からレポートを生成するには、次の手順を実行します。

1. **Central Management Console Welcome**（Central Management Console へようこそ）画面から、右上隅にあるドロップダウンメニューをクリックします。
2. ドロップダウンメニューから、**Reports**（レポート）をクリックし、以下のいずれかのオプションを選択します。
   - **Compliance Report（コンプライアンスレポート）**
   - **Summary Report（サマリレポート）**
   - **Failure Report（障害レポート）**
3. 左のナビゲーション領域から、レポートを実行する Core 、または複数の Core を選択します。
4. **Start Time**（開始時刻）ドロップダウンカレンダーで、開始日付を選択してから、レポートの開始時刻を入力します。

   メモ: Core が展開される以前の使用可能なデータはありません。
5. **End Time**（終了時刻）ドロップダウンカレンダーで、終了日付を選択してから、レポートの終了時刻を入力します。
6. **Generate Report**（レポートの生成）をクリックします。

   レポートの生成後、ツールバーを使用してそのレポートを印刷またはエクスポートできます。

7

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

AppAssure および DL1000 Appliance 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 Core Console から利用できます。

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. 左ペインで **Appliance（アプライアンス）** → **Documentation（マニュアル）**リンクに移動します。

Software updates（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. 左ペインで **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

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。

セールス、テクニカルサポート、またはカスタマーサービス問題についての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、フォームに記入し、**Submit（送信）**をクリックしてフィードバックを送信します。