Dell DL4300 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

Dell DL4300 アプライアンスについて

本章では、DL4300 の概要と、その特徴、機能、およびアーキテクチャについて説明します。トピックは次のとおりです。

- コアテクノロジ
- True Scale アーキテクチャ
- 導入アーキテクチャ
- 製品の特徴

アプライアンスは、バックアップ、レプリケーション、およびリカバリを単一のソリューションに結合させることにより、統合データ保護の新たな標準を確立します。このソリューションは、仮想マシン（VM）、物理マシン、およびクラウド環境を保護するために最も高速で信頼性の高いバックアップとなるように設計されています。

アプライアンスは、組み込みのグローバル重複除外、圧縮、暗号化、および任意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を使用して最大数ペタバイトのデータを処理できます。データ保持（DR）とコンプライアンスのために、サーバーアプリケーションとデータは、数分でリカバリできます。

お使いのアプライアンスは、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ー環境をサポートします。

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
- Verified Recovery
- Universal Recovery
- True Global Deduplication

これらのテクノロジは、クラウド災害復旧のためのセキュアな統合で設計されており、高速かつ信頼性の高いリカバリを提供します。拡張可能なオブジェクトストアにより、アプライアンスは組み込みのグローバル重複除外、圧縮、暗号化、および任意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を使用して最大数ペタバイトのデータを非常に高速に処理できます。

AppAssure は、そのコアテクノロジと、プライベートとパブリックの両方のクラウドで構成される VMware vSphere および Microsoft Hyper-V 上で動作する環境を含むマルチハイパーバイザー環境のサポートによって、このような複雑性と非効率に対応します。AppAssure は、IT 管理とストレージコストを大幅に削減しながら、これらの最新テクノロジを提供します。

コアテクノロジ

AppAssure のコアテクノロジについての詳細は、次のトピックで説明されています。

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、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中断のほとんどないアクセスを実現し、ボリューム全体をゼロ分に近い RTO および RPO で回復することができます。

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 や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。サーバーの使用は、本番ストレージへのデータ復元の完了を待つことなく、バックアップファイルから直接再開することが可能です。ユーザーは生産性を維持し、IT 部門はリカバリ期間を短縮して、厳しさを増す今日の Recovery Time Objective（RTO）および Recovery Point Objective（RPO）サービスレベル契約に対応します。

Verified Recovery

Verified Recovery では、自動化されたリカバリテストとバックアップの検証を実行できます。その対象には、ファイルシステム、Microsoft Exchange 2007、2010、2013、および Microsoft SQL Server 2005、2008、2008 R2、2012、2014 の各種バージョンなどがあります。Verified Recovery は、仮想環境および物理環境においてアプリケーションおよびバックアップをリカバリできます。アーカイブ操作、レプリケーション操作、およびデータシーディング操作中にバックアップ内の各ディスクブロックが正しいことをチェックする、256 ビット SHA キーに基づいた包括的な整合性チェックアルゴリズムを備えています。これにより、データの破損が早期に識別されるようになり、破損したデータブロックがバックアッププロセス時に維持または転送されることがなくなります。

Universal Recovery

Universal Recovery テクノロジにより、無制限のマシン復元の柔軟性が実現されます。バックアップは、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。たとえば、P2V、V2V、V2P、P2P、P2C、V2C、C2P、C2V などが可能です。

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。AppAssure の使用により、データを物理からクラウド、または仮想からクラウドに回復またはエクスポートすることが可能になります。

True Global Deduplication

お使いのアプライアンスには、データストレージ要件を満たしながら、50:1 を超える容量削減比を提供することによって、物理ディスクドライブ容量の要件を削減する True Global Deduplication 機能が備わっています。回線速度パフォーマンスでの AppAssure True Scale インラインブロックレベルの圧縮と重複排除、および組み込みの整合性チェックによって、データ破損がバックアップおよびアーカイブプロセスの品質に影響しないようにします。

True Scale アーキテクチャ

アプライアンスは、AppAssure True Scale アーキテクチャに基づいて構築されています。このアーキテクチャでは、企業環境に安定したパフォーマンスを一貫して提供するように最適化された、動的な、マルチコアのパイプラインアーキテクチャが活用されています。True Scale は、直線的な拡張と、大型データの効率的

な保存および管理を行い、パフォーマンスを損なうことなく数分の RTO と RPO を実現するように設計されています。これは、グローバル重複排除、圧縮、暗号化、レプリケーション、および保持が統合された専用のオブジェクトとボリュームマネージャで構成されます。次の図は、AppAssure True Scale アーキテクチャを説明しています。

図 1. AppAssure True Scale アーキテクチャ

AppAssure Volume Manager と拡張可能なオブジェクトストアが AppAssure True Scale アーキテクチャの土台となります。拡張可能なオブジェクトストアでは、仮想サーバーと物理サーバーからキャプチャされるブロックレベルのスナップショットが保存されます。ボリュームマネージャは、共通のリポジトリまたは必要に応じたジャストインタイムのストレージを提供することにより、多数のオブジェクトストアを管理します。オブジェクトストアは、最小限の遅延で高いスループットを実現するとともにシステム使用率を最大化する非同期の I/O によってすべてを同時にサポートします。リポジトリは、ストレージエリアネットワーク（SAN）、ダイレクトアタッチストレージ（DAS）、またはネットワークアタッチストレージ（NAS）などの多様なストレージテクノロジ上に常駐します。

AppAssure Volume Manager の役割は、オペレーティングシステムにおけるボリュームマネージャの役割に似ています。サイズやタイプが異なることのあるさまざまなストレージデバイスを、ストライプまたはシーケンシャル割り当てポリシーを使用して論理的なボリュームにまとめます。オブジェクトストアは、アプリケーションアウェアのスナップショットから得られたオブジェクトを保存、取得、維持し、複製します。ボリュームマネージャは、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 パフォーマンスを提供します。

導入アーキテクチャ

アプライアンスは、企業内で、またはマネージドサービスプロバイダにより提供されるサービスとして、柔軟に導入される拡張可能なバックアップおよびリカバリ製品です。導入のタイプは、顧客の規模と要件によって異なります。アプライアンスの導入準備には、ネットワークストレージトポロジ、コアハードウェアと災害復旧インフラストラクチャ、およびセキュリティの計画が含まれます。

導入アーキテクチャは、ローカルおよびリモートのコンポーネントで構成されます。オフサイトリカバリ用に災害復旧サイトやマネージドサービスプロバイダを利用する必要のない環境では、リモートコンポーネントを省略することもできます。基本的なローカル導入は、コアと呼ばれるバックアップサーバーと、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、DR 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になります。コアは、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、アプライアンスは、包括的な保護と効果的なリカバリを実現するために、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し、依存関係に基づいてこれらのボリュームを自動的にグループ化できるため、アプリケーションアウェアになっています。これにより、リカバリを実行するときに、不完全なバックアップが存在しないことが保証されます。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。アプライアンスは、保護対象の Microsoft Exchange サーバーと SQL サーバーのログの切り捨ても実行できます。

次の図は、単純な導入を示しています。この図では、AppAsure エージェントソフトウェアが、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、単一のコアで保護されています。これには、構成要素として中央リポジトリも存在しています。ライセンスポータルは、ライセンスサブスクリプション、および環境内の保護対象マシン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、お使いの環境に対してライセンス単位で、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、および保護対象マシンとコアの導入を行うことができます。

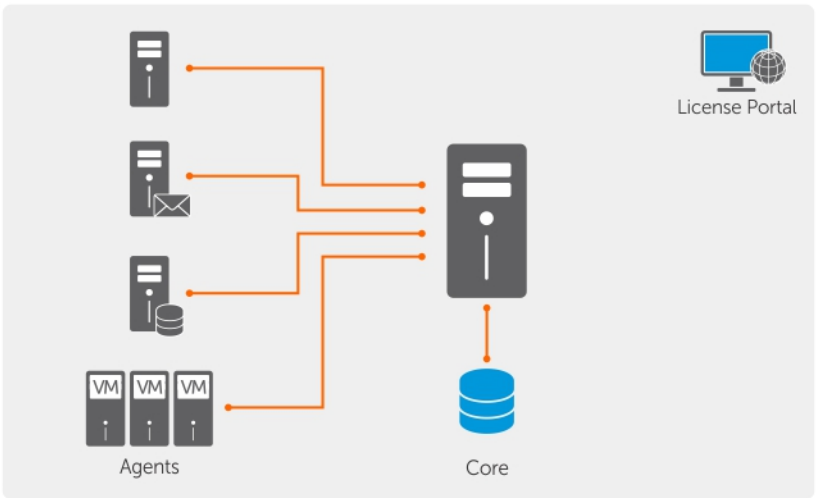


図 2. 基本的な導入アーキテクチャ

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

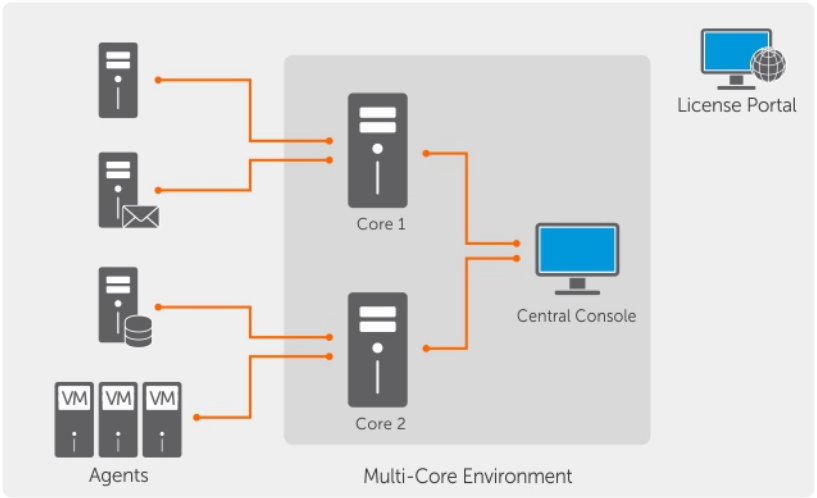


図 3. 複数コアの導入アーキテクチャ

Smart Agent

Smart Agent は、ディスクボリュームの変更されたブロックを追跡し、事前定義された保護の間隔で変更されたブロックのイメージをスナップします。この永続的な増分ブロックレベルスナップショットにより、保護対象マシンからコアへの同じデータが繰り返しコピーされなくなります。Smart Agent は、コアで保護されるマシンにインストールされます。

Smart Agent は、アプリケーションアウェアであり、CPU 使用率がほぼゼロ（0）で、メモリオーバーヘッドが 20 MB 未満の未使用時には休止状態になります。Smart Agent がアクティブの場合は、最大 2〜4 パーセントのプロセッサ使用率と 150 MB 未満のメモリが使用されます（コアへのスナップショットの転送も含まれます）。

Smart Agent は、アプリケーションアウェアであり、インストールされているアプリケーションのタイプとデータの場所も検出します。Smart Agent は、効果的な保護と迅速なリカバリを実現するためにデータベースなどの依存関係を持つデータボリュームを自動的にグループ化し、それらをまとめてログに記録します。AppAssure Agent ソフトウェアは、設定完了後に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なマルチスレッドのソケットベース接続を使用してコアへ速やかに転送されます。保護対象マシン上での CPU 帯域幅とメモリの消費を抑えるために、Smart Agent はソース側でデータの暗号化や重複排除を実行せず、保護対象マシンは保護のためにコアとペアリングされます。

DL4300 Core

Core は、導入アーキテクチャの中心的なコンポーネントです。すべてのマシンバックアップを保存および管理し、バックアップ、リカバリ、保持、レプリケーション、アーカイブ、および管理のためにコアサービスを提供します。Core は 64 ビットバージョンの Microsoft Windows オペレーティングシステムが実行されている自己完結型のネットワークアドレス対応コンピュータです。アプライアンスは、保護対象マシンから受信したデータのターゲットベースのインライン圧縮、暗号化、および重複排除を実行します。Core は、ストレージエリアネットワーク（SAN）やダイレクトアタッチストレージ（DAS）などのリポジトリにスナップショットバックアップを保存します。

リポジトリは、Core 内の内部ストレージにも常駐させることができます。Core は、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。内部的には、

すべてのコアサービスは、REST API を介してアクセスできます。コアサービスには、コア内からアクセスすることも、HTTP/HTTPS リクエストの送信と HTTP/HTTPS レスポンスの受信が可能な任意のアプリケーションからインターネット経由で直接アクセスすることもできます。すべての API 操作は、SSL を使用して実行され、X.509 v3 証明書で相互認証されます。

Core は、レプリケーションのために他の Core とペアになります。

スナップショットプロセス

スナップショットは、ベースイメージが保護対象マシンからコアに転送されるときに実行されます。通常の操作でマシンの完全なコピーがネットワークで転送されるのはこのときだけであり、これ以降は増分スナップショットが実行されます。Windows 向け AppAssure Agent ソフトウェアは、Microsoft Volume Shadow Copy Service（VSS）を使用して、ディスクへのアプリケーションデータをフリーズおよび静止状態にし、ファイルシステムとアプリケーションで整合的なバックアップをキャプチャします。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 VSS とライターは、コンテンツがディスクに書き込まれることを防ぎます。ディスクへのコンテンツの書き込みが停止されている場合、すべてのディスク I/O 操作はキューに入れられ、スナップショットの完了後に再開されます（すでに競合している操作は完了し、開いているすべてのファイルが閉じられます）。シャドーコピーの作成プロセスは、本番稼動システムのパフォーマンスに大きな影響を与えません。

AppAssure は Microsoft VSS を使用します。これは、Microsoft VSS では、NTFS、レジストリ、Active Directory など、Windows のすべての内部テクノロジについて、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機能がビルトインサポートされているからです。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）は、VSS Writer プラグインを使用して、スナップショットの準備中の通知や、使用中の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的な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ります。VSS の使用目的は、スナップショットを作成することではなく、システムとアプリケーションのデータをディスクに対して静止状態にすることであることに注意してください。キャプチャされたデータは、コアに速やかに転送され、保存されます。バックアップに VSS を使用しても、スナップショットを実行する時間の長さは数時間ではなく数秒であるため、アプリケーションサーバーが長い時間にわたってバックアップモードになることはありません。スナップショットはボリュームレベルで機能するので、バックアップに VSS を使用すると、AppAsssure Agent ソフトウェアが一度に大量のデータのスナップショットを取得できるという利点もあります。

災害復旧サイトまたはサービスプロバイダのレプリケーション

レプリケーションプロセスには、2 つのコア間でのソースとターゲットのペアの関係が必要です。ソースコアは保護対象マシンのリカバリポイントをコピーし、それら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。このオフサイトの場所は、会社が所有するデータセンター（自己管理コア）または第三者のマネージドサービスプロバイダ（MSP）の場所にすることも、クラウド環境にすることもできます。MSP に複製する場合、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。最初のデータ転送には、データシーディングの実行に外部メディアを使用できます。これは、データが大量にある場合やサイト間のリンクが低速の場合に便利です。

深刻な機能の停止が発生した場合、アプライアンスはレプリケーション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。広範囲にわたって機能の停止が発生した場合、セカンダリサイト内のターゲットコアは、複製された保護対象マシントからインスタンスを回復し、フェールオーバーマシン上で保護をただちに開始できます。プライマリサイトの復旧後、複製されたコアは、回復されたインスタンスからプライマリサイトの保護対象マシンにデータをフェールバックできます。

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。導入がローカル保護およびオプションのレプリケーションで安定した状態になると、DL1000 Core では、Recovery Assure、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。

製品の特徴

次の機能と機能性を使用して、重要なデータの保護とリカバリを管理できます。

- リポジトリ
- True Global Deduplication（機能）
- 暗号化
- レプリケーション
- Recovery-as-a-Service（RaaS）
- 保持とアーカイブ
- 仮想化とクラウド
- アラートとイベント管理
- ライセンスポータル
- ウェブコンソール
- サービス管理 API

リポジトリ

リポジトリは、それぞれがストレージエリアネットワーク（SAN）、ダイレクトアタッチストレージ（DAS）、またはネットワーク接続ストレージ（NAS）、クラウドストレージなど、さまざまなストレージテクノロジ上に存在する可能性のある複数のボリュームをサポートするボリュームマネージャの実装に重複排除ボリュームマネージャ（DVM）を使用します。各ボリュームは、重複排除を備えた拡張可能なオブジェクトストアで構成されます。この拡張可能なオブジェクトストアはレコードベースのファイルシステムとして動作し、ストレージ割り当ての単位はレコードと呼ばれる固定サイズのデータブロックになります。このアーキテクチャは、圧縮と重複排除にブロックサイズのサポートを設定できるようにします。ロールアップ操作は、データではなくレコードだけを移動するようになるため、ディスクへの負荷の高い操作から、メタデータ操作へと簡略化されます。

DVM は、オブジェクトストアセットを統合して 1 つのボリュームにすることができます。また、追加のファイルシステムを作成することにより、それらのオブジェクトストアを拡張することができます。オブジェクトストアファイルは事前に割り当てられており、ストレージ要件の変化に応じてオンデマンドで追加することができます。1 つの Core には最大 255 個の独立したリポジトリを作成することができ、新しいファイルエクステントを追加することによって、リポジトリサイズをさらに拡大することができます。拡張されたリポジトリには、異なるストレージテクノロジにまたがるエクステントを最大 4,096 個含めることができます。リポジトリの最大サイズは 32 エクサバイトです。1 つのコアには、複数のリポジトリが存在できます。

True Global Deduplication

True Global Deduplication は、冗長または重複するデータを排除することにより、バックアップストレージの需要を効果的に削減する方法です。重複排除が効果的なのは、複数のバックアップ間に固有のデータが存在するとき、そのインスタンスがリポジトリ内に 1 つだけ保存されることによるものです。冗長データは保

存されますが、実際のデータが保存されるわけではありません。リポジトリ内にある 1 つの固有のデータインスタンスへのポインタに単純に置き換えられます。

従来のバックアップアプリケーションでは週ごとに完全なバックアップが繰り返し実行されていますが、アプライアンスではマシンのブロックレベルの増分バックアップが実行されます。この永続的な増分バックアップとデータ重複排除の組み合わせにより、ディスクにコミットされるデータの総量を大幅に削減できます。

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。ほとんどの環境では、管理者の多くが、導入と管理を効果的に行うために、複数のシステムにわたって共通の種類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します。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 4. 重複排除の図解

お使いのアプライアンスは、ターゲットベースのインラインデータの重複排除を実行します。この場合、スナップショットデータは、重複排除される前に Core に送信されます。インラインデータの重複排除とは、単にデータがディスクにコミットされる前に重複排除されることを意味します。これは、データが保存用のターゲットに送信される前に重複排除されるソースでの重複排除、またはデータがターゲットに未処理（raw）の状態で送信され、ディスクにコミットされた後で分析および重複排除される処理後の重複排除とは異なります。ソースでの重複排除では、マシン上の貴重なシステムリソースが消費され、処理後のデータ重複排除では、重複排除処理を開始する前にディスク上の必須データがすべて必要になります（初期容量のオーバーヘッドが増大）。一方、インラインデータの重複排除は、重複排除処理用としてソースや Core で追加のディスク容量および CPU サイクルを必要としません。繰り返しますが、従来のバックアップアプリケーションでは、週ごとに完全なバックアップが繰り返し実行され、アプライアンスではマシンのブロックレベルバックアップが永続的に実行されます。この永続的な増分バックアップとデータの重複排除により、ディスクにコミットされるデータの合計量が最大 50:1 の削減比で大幅に削減されます。

暗号化

お使いのアプライアンスは、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。そのデータにアクセスし、暗号を解読できるのは、暗号化キーを持つユーザーのみです。システム上に作成および保存できる暗号化キーの数に制限はありません。DVM では、256 ビットキーを使用した暗号ブロック連鎖（CBC）モードの AES 256 ビット

暗号化が使用されます。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。これは、DVM の実装がマルチスレッド化され、導入先のプロセッサ固有のハードウェアアクセラレーションが使用されるためです。

暗号化はマルチテナントに対応しています。重複排除は、同じキーで暗号化されたレコードのみに明確に制限されています。異なるキーで暗号化された 2 つの同じレコードは互いに重複排除されることはありません。この設計により、異なる暗号化ドメイン間で重複排除を使用してデータが漏洩することがなくなります。これは、テナント（顧客）が自分以外のテナントのデータを表示したり、アクセスしたりできない状態であり、複数のテナントの複製されたバックアップを単一コア上に保存できるため、マネージドサービスプロバイダにとって利点となります。アクティブな各テナント暗号化キーにより、キーの所有者のみがデータを表示、アクセス、使用できる暗号化ドメインがリポジトリ内に作成されます。マルチテナントのシナリオでは、データは暗号化ドメイン内でパーティション化され、重複排除されます。

レプリケーションシナリオでは、お使いのアプライアンスは SSL 3.0 を使用してレプリケーショントポロジ内の 2 つのコア間の接続をセキュア化し、データの盗聴や改ざんを防ぎます。

レプリケーション

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

ソースコアは、選択された保護対象マシンのリカバリポイントをコピーし、増分スナップショットデータをリモート災害復旧サイトにあるターゲットコアに非同期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。

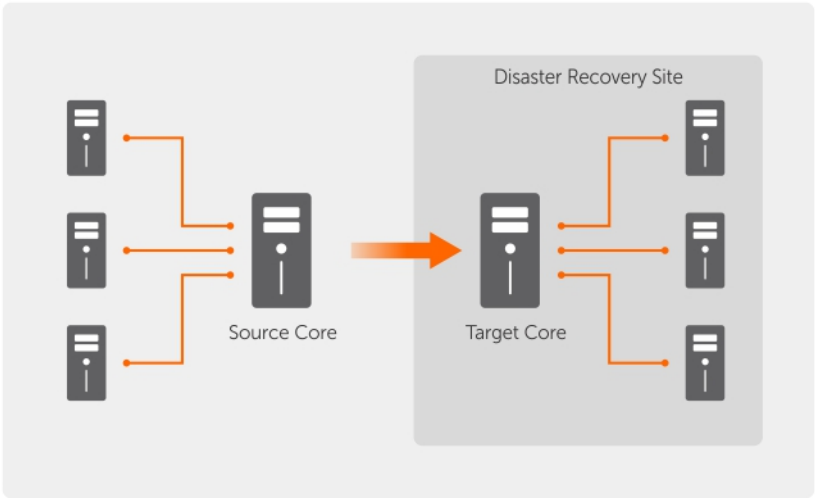


図 5. 基本的なレプリケーションアーキテクチャ

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。

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外部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。データがターゲットコアに転送された後、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。

Recovery-as-a-Service（RaaS）

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、アプライアンス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そのデータと共にサービスプロバイダのクラウドに仮想マシンとして複製して、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ことによって、完全なクラウド内リカバリを実現します。クラウド内リカバリを実行する顧客は、ローカルコアで保護対象マシンに対して 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 が顧客のためにすぐに仮想マシンをスピンアップすることができます。

MSP は、通常は単一サーバーまたはサーバーグループでセキュリティやデータを共有しない複数の組織および個別の組織、あるいはビジネスユニット（テナント）をホストできる、マルチテナント型 AppAssure ベースの RaaS インフラストラクチャを導入できます。各テナントのデータは、他のテナントやサービスプロバイダから隔離され、セキュアに保護されます。

保持とアーカイブ

アプライアンスでは、バックアップおよび保持ポリシーは柔軟であるため、設定が容易です。組織のニーズに合わせて保持ポリシーを調整する機能は、コンプライアンス要件を満たすために役立つだけでなく、そのために RTO を損なうことがありません。

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要に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。したがって、このような要件により、長期（低速かつ安価な）ストレージが必要になります。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よく使用されます。アーカイブ機能は、準拠データと非準拠データの長期的な保持をサポートするほか、レプリケーションデータをターゲットコアにシーディングするためにも使用されます。

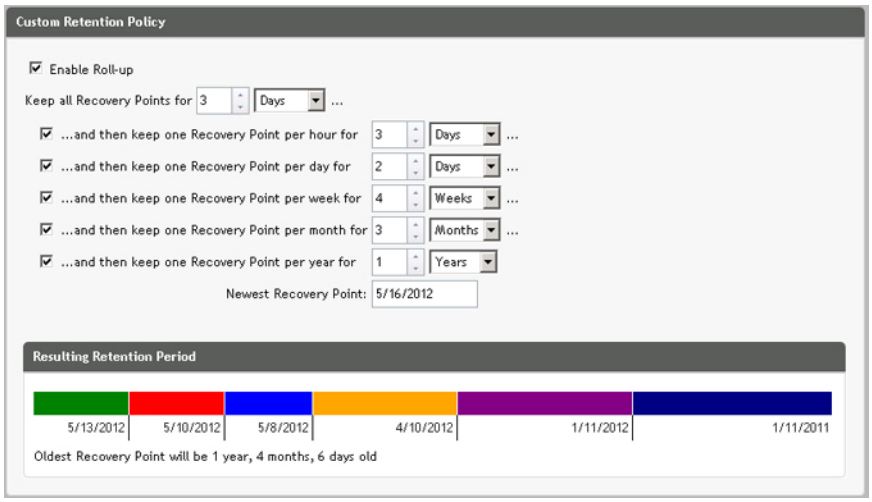


図 6. カスタム保持ポリシー

アプライアンスでは、保持ポリシーをカスタマイズして、バックアップリカバリポイントが維持される期間を指定することができます。リカバリポイントの有効期間が保持期間の終了に近づき、リカバリポイントの有効期間が期限切れになると、そのリカバリポイントは保持プールから削除されます。通常、このプロセスはデータの量と保持期間が急速に増加し始めると効率が悪くなり、最終的には失敗します。アプライアンスは、複雑な保持ポリシーで大量データの保持を管理し、効率的なメタデータ操作を使用して古いデータのロールアップを実行することにより、大規模データの問題を解決します。

バックアップは数分間隔で実行することができます。これらのバックアップが日、月、年の単位で古くなるにつれ、保持ポリシーは、古いバックアップのエージングと削除を管理します。エージングプロセスは、単純なウォーターフォール方法によって定義されます。ウォーターフォール内のレベルは、分、時、日、週、月、年の単位で定義されます。保持ポリシーは、夜間のロールアッププロセスで適用されます。

長期アーカイブのために、アプライアンスには、リムーバブルメディア上にソースコアまたはターゲットコアのアーカイブを作成する機能が備わっています。アーカイブは内部で最適化され、アーカイブ内のすべてのデータは圧縮、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できる容量よりも大きい場合、アーカイブはメディア上の空き容量に基づいて複数のデバイスにまたがって保存されます。また、アーカイブはパスフレーズでロックすることができます。アーカイブからのリカバリに新しいコアは必要ありません。管理者がパスフレーズと暗号化キーを持っていれば、任意のコアでアーカイブを取り込み、データを回復できます。

仮想化とクラウド

Core はクラウドに対応で、クラウドのコンピューティング能力をリカバリに活用できます。

アプライアンスは、任意の保護対象またはレプリケーション対象マシンをライセンスバージョンの VMware や Hyper-V などの仮想マシンにエクスポートできます。一回のみの仮想エクスポートを実行するか、または継続的な仮想エクスポートを確立することによって、仮想スタンバイ VM を確立することもできます。継続的なエクスポートでは、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非常に高速であり、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のエクスポートタイプは、フォルダ上の VMware Workstation または VMware Server、vSphere/VMware ESX（i）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）、2008 R2、2012（x64）および 2012 R2 上の Microsoft Hyper-V Serve へのエクスポート（Hyper-V 第 2 世代 VM のサポートも含む）です。

さらに 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、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。

アラートとイベント管理

アプライアンスには、HTTP REST API に加え、電子メール、Syslog、Windows イベントログを使用してイベントの記録および通知を行う豊富な機能セットも含まれます。電子メールによる通知は、アラートに応じたさまざまなイベントの状態またはステータスをユーザーやグループに警告するために使用できます。Syslog および Windows イベントログメソッドは、複数のオペレーティングシステムがある環境のリポジトリへの一元化されたロギングを行うために使用され、Windows のみの環境では、Windows イベントログだけが使用されます。

ライセンスポータル

ライセンスポータルには、ライセンス権利を管理するための使い勝手のよいツールが用意されています。ライセンスキーのダウンロード、アクティブ化、表示、および管理を行ったり、会社のプロファイルを作成してライセンス資産を追跡したりすることができます。また、サービスプロバイダやリセラーはこのポータルを利用して、顧客のライセンスを追跡し、管理することができます。

ウェブコンソール

アプライアンスは、分散されたコアを一元的に管理する、新しいウェブベースの中央コンソールを備えています。複数の分散型コアを持つ MSP および企業カスタマーは、一元管理のために統合されたビューを得るために、中央コンソールを導入できます。中央コンソールは、管理対象コアを階層的な組織単位で分類する機能を提供します。これらの組織単位は、事業部門、所在地、または役割ベースのアクセス権を持つ MSP の顧客などにすることができます。中央コンソールは、管理対象コア全体のレポートを実行することもできます。

サービス管理 API

お使いのアプライアンスにはサービス管理 API がバンドルされており、Central Management Console から利用可能なすべての機能に対するプログラムからのアクセスを提供します。サービス管理 API は REST API です。すべての API 操作は SSL 経由で実行され、X.509 v3 証明書で相互認証されます。管理サービスには、環境内からアクセスすることも、HTTPS リクエストとレスポンスを送受信可能な任意のアプリケーションからインターネット経由で直接アクセスすることもできます。このアプローチにより、Relationship Management Methodology（RMM）ツールや請求システムなどのウェブアプリケーションとの統合が容易になります。また、アプライアンスには、PowerShell スクリプティング用の SDK クライアントもバンドルされています。

2

DL4300 Core での作業

DL4300 Core Console へのアクセス

Core Console へアクセスするには、次の手順を実行します。

1. お使いのブラウザで信頼済みサイトをアップデートします。「Internet Explorer での信頼済みサイトのアップデート」を参照してください。
2. Core Console 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. 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。
   - DL4300 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

Microsoft 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

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 のブラウザ設定の構成

メモ: Firefox の最新バージョンで Mozilla Firefox のブラウザ設定を変更するには、プロテクションを無効にします。URL の左にある [Site Identify]（サイトアイデンティティ）ボタンを右クリックし、**オプション** に移動して **Disable protection for now**（現在の保護を無効にする）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。

Core を設定するためのロードマップ

設定には、バックアップスナップショットを保存するリポジトリの作成および設定、保護対象データを保護するための暗号化キーの定義、通知とアラートの設定などのタスクが含まれます。Core の設定が完了したら、エージェントの保護およびリカバリの実行が可能になります。

Core の設定には、特定の概念と以下の初期操作の実行について理解する必要があります。

- リポジトリの作成
- 暗号化キーの設定
- イベント通知の設定
- 保持ポリシーの設定
- SQL アタッチ可否の設定

メモ: このアプライアンスを使用している場合は、Core の設定に **Appliance**（アプライアンス）タブを使用することが推奨されます。初期インストール後の Core の設定に関する詳細については、**dell.com/support/home** にある『Dell DL4300 Appliance Deployment Guide 』（Dell DL4000 アプライアンス導入ガイド）を参照してください。

ライセンスの管理

Core Console から直接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）ページからライセンスポータルにアクセスすることもできます。

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
- ライセンスの制約事項
- 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 に移動します。
2. **Configuration（設定）→ Licensing（ライセンス）**の順に選択します。
   Licensing（ライセンス）ページが表示されます。
3. **License Details**（ライセンス詳細）のセクションで、**Change License**（ライセンス変更）をクリックします。
   Change License（ライセンスの変更）ダイアログボックスが表示されます。
4. **Change License**（ライセンスの変更）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 **Continue**（続行）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

Core Console は、頻繁にポータルサーバーと通信して、ライセンスポータルに対する変更を反映した最新の状態を維持します。通常、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 に移動します。
2. **Configuration（設定）→ Licensing（ライセンス）**とクリックします。
3. **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。ほとんど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。詳細については、「手動によるホスト名の変更」を参照してください。

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 に移動します。
2. **Configuration（設定）** → **Settings（設定）**の順にクリックします。
3. **General**（一般）ペインで、**Change**（変更）をクリックします。

   General Settings（一般設定）ダイアログボックスが表示されます。
4. **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。

   この名前が、Core Console 内で表示される名前となります。最大 64 文字まで入力できます。
5. **Web Server Port**（ウェブサーバーポート）テキストボックスに、ウェブサーバーのポート番号を入力します。デフォルトは 8006 です。
6. **Service Port**（サービスポート）にサービスのポート番号を入力します。デフォルトは 8006 です。

7. **OK** をクリックします。

夜間ジョブ時刻の調整

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 に移動します。
2. **Configuration（設定）** → **Settings（設定）**の順にクリックします。
3. **Nightly Jobs**（夜間ジョブ）領域で、**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。
4. **Nightly Jobs Time**（夜間ジョブ時刻）テキストボックスに、夜間ジョブを実行する新しい時刻を入力します。
5. **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、データを転送する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 に移動します。
2. **Configuration（設定）** → **Settings（設定）**の順にクリックします。
3. **Transfer Queue**（転送キュー）ペインで、**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。
4. **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。
5. **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。
6. **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を調整するには、次の手順を実行します。

1. Core Console に移動します。
2. **Configuration（設定）** → **Settings（設定）**の順にクリックします。
3. **Client Timeout Settings Configuration**（クライアントタイムアウト設定）領域で、**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。
4. **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。
5. **Connection UI Timeout**（接続 UI タイムアウト）テキストボックスに、接続 UI タイムアウトが発生するまでの分と秒数を入力します。
6. **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。
7. **Read/Write UI Timeout**（読み取り / 書き込み UI タイムアウト）テキストボックスに読み取り / 書き込み UI 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。

8. **OK** をクリックします。

重複排除キャッシュの設定

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 に移動します。
2. **Configuration（設定）** → **Settings（設定）**の順にクリックします。
3. **Deduplication Cache Configuration**（重複排除キャッシュ設定）領域で、**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。
4. **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、アップデートされた値を入力してプライマリキャッシュの場所を変更します。
5. **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、アップデートされた値を入力してセカンダリキャッシュの場所を変更します。
6. **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、アップデートされた値を入力してメタデータキャッシュの場所を変更します。
7. **Dedupe Cache Size**（重複排除キャッシュサイズ）テキストボックスに、重複排除キャッシュに割り当てる空き容量となる値を入力します。

   単位サイズドロップダウンフィールドで、GB（ギガバイト）または TB（テラバイト）を選択し、Dedupe Cache Size（重複排除キャッシュサイズ）テキストボックスに測定単位の値を指定します。
8. **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

温度設定を変更するには、次の手順を実行します。

1. Core Console に移動します。
2. **Configuration（設定）** → **Settings（設定）**の順にクリックします。
3. **Replay Engine Configuration**（Replay エンジンの設定）ペインで、**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。
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
IP address（IP アドレス）	• 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 address**（特定のアドレスを使用）をクリックします。
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。
Port in use（ポートが使用中）	Replay Engine の設定に使用中のポートを示しています。

テキストボックス	説明
Allow port auto-assigning（自動ポート割り当ての許可	自動 TCP ポートの割り当てを許可するにはこれをクリックします。
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。
No Delay（遅延なし）	このチェックボックスにチェックを入れるとネットワークの効率性を損なうため、チェックはオフのままにしておくことが推奨されています。この設定を変更する必要があると判断した場合は、デルサポートにお問い合わせください。

5. **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 に移動します。
2. **Configuration（設定）→ Settings（設定）**の順にクリックします。
3. **Database Connection Settings**（データベース接続設定）領域で、次のいずれかを行います。
   - **Apply Default**（デフォルトを適用）をクリックします。
   - **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。
4. 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
Host Name（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。
Port（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。
Max connection pool size（最大接続プールサイズ）	動的な再利用を可能にするためにキャッシュされるデータベース最大接続数を設定します。デフォルト設定は 100 です。
Min connection pool size（最小接続プールサイズ）	動的な再利用を可能にするためにキャッシュされるデータベース最小接続数を設定します。デフォルト設定は 0 です。

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

リポジトリについて

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キャプチャされたスナップショットを保存します。リポジトリは、ストレージエリアネットワーク（SAN）、ダイレクトアタッチストレージ（DAS）、またはネットワーク接続ストレージ（NAS）などのさまざまなストレージテクノロジー上に配置することができます。

リポジトリを作成すると、Core は、データおよびメタデータに必要なストレージ容量を指定された場所に事前に割り当てます。単一のコアでは、異なるストレージテクノロジにまたがる最大 255 の独立したリポジトリを作成できます。さらに、新しいファイルエクステントまたは仕様を追加することによってリポジトリのサイズを拡張できます。拡張されたリポジトリには、異なるストレージテクノロジにまたがる最大 4096 のエクステントを格納できます。

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。

メモ: DL4300 リポジトリは、プライマリストレージデバイスに格納されます。Data Domain などのアーカイブ用のストレージデバイスはパフォーマンス制限によりサポートされません。同様に、クラウドに階層化された NAS ファイラにもリポジトリを格納できません。このようなデバイスには、プライマリストレージとして使用される場合にパフォーマンスの制限が発生する傾向があるためです。

リポジトリ管理のロードマップ

リポジトリ管理のロードマップには、リポジトリの作成、設定、および表示などのタスクがあり、次のトピックで構成されています。

- Core Console へのアクセス
- リポジトリの作成
- リポジトリ詳細の表示
- リポジトリ設定の変更
- 既存のリポジトリへのストレージの場所の追加
- リポジトリのチェック
- リポジトリの削除
- リポジトリのリカバリ

メモ: リポジトリの設定には、**Appliance**（アプライアンス）タブを使用することが推奨されています。

お使いのアプライアンスの使用を開始する前に、Core サーバーで 1 つ、または複数のリポジトリをセットアップする必要があります。リポジトリには、保護されたデータが保存されます。具体的には、環境内の保護対象サーバーからキャプチャされたスナップショットが保存されます。

リポジトリを設定すると、Core サーバー上でデータストレージを配置する場所、各リポジトリに追加できる場所の数、リポジトリの名前、リポジトリがサポートする現在の操作の数の指定などのさまざまなタスクを行うことができます。

リポジトリを作成すると、Core によって、データおよびメタデータを保存するために必要なスペースが指定の場所に事前に割り当てられます。1 つのコアで最大 255 の独立したリポジトリを作成できます。さらに 1 つのリポジトリのサイズを拡張するには、新しいストレージの場所またはボリュームを追加します。

リポジトリの追加または変更は、Core Console で行うことができます。

リポジトリの作成

メモ: このアプライアンスを SAN として使用する場合は、**Appliance**（アプライアンス）タブを使用してリポジトリを作成することをお勧めします。「選択したストレージのプロビジョニング」を参照してください。

リポジトリを手動で作成するには、次の手順を実行します。

1. Core Console に移動します。
2. **Configuration（設定）** → **Repositories（リポジトリ）**とクリックします。
3. **Add new**（新しく追加）をクリックします。
   Add New Repository（新規リポジトリを追加）ダイアログボックスが表示されます。
4. 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
Repository Name（リポジトリ名）	リポジトリの表示名を入力します。デフォルトでは、このテキストボックスは Repository という単語と、新しいリポジトリに 1 から順に付与されるインデックス番号で構成されます。この名前は必要に応じて変更できます。最大 150 文字まで入力できます。
Concurrent Operations（同時操作）	リポジトリで対応する同時要求の数を定義します。デフォルトの値は 64 です。
コメント	オプションで、このリポジトリの説明を入力します。

5. リポジトリ用の具体的なストレージの場所またはボリュームを定義するには、**Add Storage Location**（ストレージの場所の追加）をクリックします。

   注意: この手順で作成している AppAssure リポジトリが後で削除されると、リポジトリのストレージの場所にあるすべてのファイルが削除されます。リポジトリファイルを保存する専用のフォルダを定義しなければ、リポジトリファイルはルートに保存されます。このリポジトリを削除すると、ルートのすべてのコンテンツも削除され、データが壊滅的に失われます。

   メモ: リポジトリは、プライマリストレージデバイスに格納されます。Data Domain などのアーカイブ用のストレージデバイスはパフォーマンス制限によりサポートされません。同様に、クラウドに階層化された NAS ファイラにもリポジトリを格納できません。このようなデバイスには、プライマリストレージとして使用される場合にパフォーマンス制限を伴う傾向があるためです。

   Add Storage Location（ストレージの場所の追加）ダイアログボックスが表示されます。

6. ストレージの場所にファイルを追加する方法を指定します。ファイルは、ローカルディスクまたは CIFS 共有に追加できます。

   - ローカルマシンを指定するには、**Add file on local disk**（ローカルディスク上にファイルを追加）をクリックし、次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
Data Path（データパス）	保護されたデータを保存するための場所を入力します。たとえば、**X:\Repository\Data** と入力します。 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。
Metadata Path（メタデータパス）	保護されたメタデータを保存するための場所を入力します。たとえば **X:\Repository\Metadata** と入力します。 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。

   - あるいは、ネットワーク共有の場所を指定するには、**Add file on CIFS share**（CIFS 共有上にファイルを追加）をクリックし、次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
UNC Path（UNC パス）	ネットワーク共有の場所のパスを入力します。 この場所がルートに位置する場合は、専用のフォルダ名を定義します（Repository など）。このパスは \\ で始まる必要があります。この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。
ユーザー名	ネットワーク共有の場所にアクセスするためのユーザー名を指定します。
パスワード	ネットワーク共有の場所にアクセスするためのパスワードを指定します。

7. **Details**（詳細）ペインで、**Show/Hide Details**（詳細を表示 / 非表示）をクリックし、次の説明に従ってストレージの場所の詳細を入力します。

テキストボックス	説明
Size（サイズ）	ストレージの場所のサイズまたは容量を設定します。デフォルトは 250 MB です。次の単位を選択できます。 • MB • GB • TB **メモ:** 指定するサイズは、ボリュームのサイズを超えることはできません。 **メモ:** ストレージの場所が Windows XP または Windows 7 を使用した New Technology File System（NTFS）ボリュームの場合、ファイルサイズの上限は 16 TB です。 ストレージの場所が Windows 8 または Windows Server 2012 を使用した NTFS ボリュームの場合、ファイルサイズの上限は 256 TB です。 **メモ:** オペレーティングシステムを検証する場合は、Windows Management Instrumentation（WMI）が対象のストレージの場所にインストールされている必要があります。
Write Caching Policy（ライトキャッシングポリシー）	ライトキャッシングポリシーは、リポジトリでの Windows Cache Manager の使用を制御し、さまざまな構成で最適なパフォーマンスを得られるようにリポジトリを調整します。 次のいずれかの値に設定します。 • オン • オフ • Sync（同期） この値を On（オン）に設定すると（デフォルト）、Windows がキャッシングを制御します。

テキストボックス	説明
	メモ: ライトキャッシングポリシーを On（オン）に設定すると、パフォーマンスが向上する可能性があります。Server 2012 よりも古いバージョンの Windows Server を使用している場合は、設定を **Off**（オフ）にすることを推奨します。 **Off**（オフ）に設定すると、AppAssure がキャッシングを制御します。 **Sync**（同期）に設定すると、Windows が同期入出力に加えてキャッシングも制御します。
Bytes per Sector（セクタあたりのバイト数）	各セクタに包含するバイト数を指定します。デフォルト値は 512 です。
Average Bytes per Record（レコードあたりの平均バイト数）	レコードあたりの平均バイト数を指定します。デフォルト値は 8192 です。

8. **保存** をクリックします。
   Repositories（リポジトリ）画面の表示に、新しく追加されたストレージの場所が反映されます。
9. リポジトリ用のストレージの場所をさらに追加するには、手順 4～7 を繰り返します。
10. **Create**（作成）をクリックして、リポジトリを作成します。
    Configuration（設定）タブに **Repository**（リポジトリ）情報が表示されます。

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 に移動します。
2. **Configuration（設定）→ Repositories（リポジトリ）**とクリックします。
3. 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。
4. 展開されたビューから、次のアクションを実行できます。
   - 設定の変更
   - ストレージの場所の追加
   - リポジトリのチェック
   - リポジトリの削除

   リポジトリの詳細も表示され、ストレージの場所と統計情報が示されます。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ています。統計情報には、次の情報が含まれます。
   - 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。
   - 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。
   - 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。

リポジトリ設定の変更

リポジトリを追加した後、説明や最大同時操作数などのリポジトリ設定を変更できます。また、リポジトリ用に新しいストレージの場所を作成することもできます。

リポジトリ設定を変更するには、次の手順を実行します。

1. Core Console に移動します。
2. **Configuration（設定）→ Repositories（リポジトリ）**とクリックします。
3. **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。

   Repository Settings（リポジトリの設定）ダイアログボックスが表示されます。
4. 次の説明に従ってリポジトリ情報を編集します。

フィールド	説明
Repository Name（リポジトリ名）	リポジトリの表示名を表します。デフォルトで、このテキストボックスの内容は単語「Repository」と、リポジトリの番号に対応するインデックス番号で構成されます。 **メモ:** リポジトリ名は編集できません。
Description（説明）	オプションで、このリポジトリの説明メモを入力します。
Maximum Concurrent Operations（最大同時操作数）	レポジトリがサポートする同時要求の数を定義します。
Enable Deduplication（重複排除を有効化）	重複排除を無効にするには、このチェックボックスの選択を解除します。重複排除を有効にするには、このチェックボックスを選択します。 **メモ:** この設定の変更が適用されるのは、設定変更後に行われるバックアップのみです。既存のデータ、別のコアから複製されたデータ、またはアーカイブからインポートされたデータは、データが保護対象マシンからキャプチャされたときに設定された重複排除の値を維持します。
Enable Compression（圧縮を有効化）	圧縮を無効にするには、このチェックボックスの選択を解除します。圧縮を有効にするには、このチェックボックスを選択します。 **メモ:** この設定が適用されるのは、設定変更後に行われるバックアップのみです。既存のデータ、別のコアから複製されたデータ、またはアーカイブからインポートされたデータは、データが保護対象マシンからキャプチャされたときに設定された圧縮値を維持します。

5. **Save**(保存）をクリックします。

既存のリポジトリの拡張

お使いのアプライアンスに MD1400 DAS を追加する場合は、使用可能なストレージを使用して既存のリポジトリを拡張することができます。

既存のリポジトリを拡張するには、次の手順を実行します。

1. MD1400 DAS を取り付けた後、Core Console を開いて **Appliance**（アプライアンス）タブを選択し、**Tasks**（タスク）をクリックします。
2. **Tasks**（タスク）画面で、新しいストレージの横にある **Provision**（プロビジョニング）をクリックします。
3. **Provisioning Storage**（ストレージのプロビジョニング）画面で、**Expand the existing repository**（既存のリポジトリの拡張）を選択し、拡張するリポジトリを選択します。
4. **Provision**（プロビジョニング）をクリックします。

   Tasks（タスク）画面のストレージデバイスの横にある **Status Description**（状態の説明）に **Provisioned**（プロビジョニング済み）と表示されます。

既存リポジトリへのストレージ場所の追加

ストレージの場所を追加すると、リポジトリまたはボリュームを保存する場所を定義できます。

ストレージの場所を既存のリポジトリに追加するには、次の手順を実行します。

1. ストレージの場所を追加するリポジトリの **Status**（ステータス）列の横にある **>** をクリックします。
2. **Add Storage Location**（ストレージの場所の追加）をクリックします。

   Add Storage Location（ストレージの場所の追加）ダイアログボックスが表示されます。
3. ストレージの場所にファイルを追加する方法を指定します。ファイルは、ローカルディスクまたは CIFS 共有に追加できます。
   - ローカルマシンを指定するには、**Add file on local disk**（ローカルディスク上にファイルを追加）をクリックし、次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
Metadata Path（メタデータパス）	保護されたメタデータを保存するための場所を入力します。
Data Path（データパス）	保護されたメタデータを保存するための場所を入力します。

   - ネットワーク共有の場所を指定するには、**Add file on CIFS share**（CIFS 共有上にファイルを追加）をクリックし、次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
UNC Path（UNC パス）	ネットワーク共有の場所のパスを入力します。
User Name（ユーザー名）	ネットワーク共有の場所にアクセスするためのユーザー名を指定します。
Password（パワード）	ネットワーク共有の場所にアクセスするためのパスワードを指定します。
4. **Details**（詳細）セクションで、**Show/Hide Details**（詳細を表示 / 非表示）をクリックし、次の説明に従ってストレージの場所の詳細を入力します。

テキストボックス	説明
Size（サイズ）	ストレージの場所のサイズまたは容量を設定します。デフォルトサイズは 250 MB です。次の単位を選択できます。 • MB • GB • TB **メモ:** 指定するサイズは、ボリュームのサイズを超えることはできません。 **メモ:** ストレージの場所が Windows XP または Window 7 を使用した NTFS ボリュームの場合、ファイルサイズの上限は 16 TB です。 ストレージの場所が Windows 8 または Windows Server 2012 を使用した NTFS ボリュームの場合、ファイルサイズの上限は 256 TB です。 **メモ:** オペレーティングシステムを検証するには、WMI が対象のストレージの場所にインストールされている必要があります。
Write Caching Policy（ライトキャッシングポリシー）	ライトキャッシングポリシーは、リポジトリでの Windows Cache Manager の使用を制御し、さまざまな構成で最適なパフォーマンスを得られるようにリポジトリを調整します。 • On（オン） • Off（オフ） • Sync（同期） デフォルト値である **On**（オン）に設定すると、Windows がキャッシングを制御します。 **メモ:** ライトキャッシングポリシーを **On**（オン）に設定すると、パフォーマンスを高速化できますが、推奨される設定は **Off**（オフ）です。 **Off**（オフ）に設定すると、AppAssure がキャッシングを制御します。 **Sync**（同期）に設定すると、Windows が同期入出力に加えてキャッシングも制御します。
Bytes per Sector（セクタあたりのバイト数）	各セクタに包含するバイト数を指定します。デフォルト値は 512 です。
Average Bytes per Record（レコードあたりの平均バイト数）	レコードあたりの平均バイト数を指定します。デフォルト値は 8192 です。

5. **Save**(保存）をクリックします。
   Repositories（リポジトリ）画面の表示に、新しく追加されたストレージの場所が反映されます。
6. リポジトリ用のストレージの場所をさらに追加するには、手順 4～7 を繰り返します。
7. **OK** をクリックします。

リポジトリのチェック

アプライアンスは、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）タブで **Repositories**（リポジトリ）をクリックしてから、チェックしたいリポジトリの横にある **>** を選択します。
2. **Actions**（アクション）ペインで、**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。
3. **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: チェックが不合格の場合は、アーカイブからリポジトリを復元します。

リポジトリの削除

リポジトリを削除するには、次の手順を実行します。

1. **Configuration**（設定）タブで **Repositories**（リポジトリ）をクリックし、削除したいリポジトリの横にある **>** を選択します。
2. **Actions**（アクション）ペインで **Delete**（削除）をクリックします。
3. **Delete Repository**（リポジトリの削除）ダイアログボックスで **Delete**（削除）をクリックします。

   注意: リポジトリが削除されると、リポジトリに含まれるデータは破棄され、回復できなくなります。

   リポジトリを削除する場合、Open Manage System Administrator でリポジトリが格納された仮想ディスクを削除する必要があります。仮想ディスクを削除した後に、ディスクの再プロビジョニングを行い、リポジトリを再度作成することができます。

ボリュームの再マウント

ボリュームを再マウントするには、次の手順を実行します。

1. Core Console に移動します。
2. **Appliance（アプライアンス）→ Tasks（タスク）**。
3. **Remount Volumes**（ボリュームの再マウント）をクリックします。
   ボリュームが再マウントされます。

外部ボリュームの解決

プロビジョニングされた MD1400 が電源オフまたは切断状態になり、その後電源オンの状態に復帰すると、MD1400 が接続されたことを報告するイベントが Core Console に表示されますが、**Appliance**（アプライアンス）タブの **Tasks**（タスク）画面には、その MD1200 のリカバリを可能にするタスクが表示されません。**Enclosures**（エンクロージャ）画面では、MD1400 が外部状態であり、外部仮想ディスク上のリポジトリはオフラインであると報告されます。

外部ボリュームを解決するには、次の手順を実行します。

1. Core Console から、**Appliance**（アプライアンス）タブを選択し、**Remount Volumes**（ボリュームの再マウント）をクリックします。
   ボリュームが再マウントされます。
2. **Configuration**（設定）タブを選択し、**Repositories**（リポジトリ）をクリックします。
3. ステータスインジケータが赤色のリポジトリを、**Status**（ステータス）の横にある **>** をクリックして展開します。
4. リポジトリの整合性を検証するには、**Actions**（アクション）で **Check**（チェック）をクリックします。

リポジトリのリカバリ

アプライアンスは、リポジトリのインポートに失敗すると、**Tasks**（タスク）画面でタスクステータスを赤い円で示してその失敗を報告し、ステータスの説明に **Error, Completed - Exception**（エラー、完了 - 例外）と示します。**Tasks**（タスク）画面でエラーの詳細を表示するには、**Status**（ステータス）列の横にある **>** をクリックしてタスクの詳細を展開します。**Status Details**（ステータスの詳細）にリカバリタスクステータスが例外であることが示され、**Error Message**（エラーメッセージ）列にエラー状態の詳細が表示されます。

インポートに失敗した状態からリポジトリをリカバリするには、次の手順を実行します。

1. Core Console に移動します。
   Repositories（リポジトリ）画面に、失敗したリポジトリが赤いステータスインジケータで表示されます。
2. **Configuration（設定）→ Repositories（リポジトリ）**とクリックします。
3. 失敗したリポジトリを、**Status**（ステータス）の横にある **>** をクリックして展開します。
4. **Actions**（アクション）セクションから、**Check**（チェック）をクリックし、**Yes**（はい）をクリックしてチェックの実行を確定します。
   アプライアンスによってリポジトリが回復されます。

セキュリティの管理

Core は、リポジトリ内の保護対象マシンスナップショットデータを暗号化できます。リポジトリ全体を暗号化する代わりに、リポジトリ内のマシンを保護する間に暗号化キーを指定することができ、これによって異なる保護対象マシンに対してこのキーを再使用することが可能になります。アクティブな各暗号化キーはそれぞれ暗号化ドメインを作成するので、暗号化がパフォーマンスに影響することはなく、単一のコアが複数の暗号化ドメインをホストすることによってマルチテナントをサポートすることが可能になります。マルチテナント環境では、データは暗号化ドメイン内でパーティション化され、重複排除されます。ユーザーが暗号化キーを管理することから、ボリュームの損失でキーが漏出することはありません。キーのセキュリティには、以下の概念と考慮事項があります。

- 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。
- コア上に作成できる暗号化キーの数に制限はありません。

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 に移動します。
2. **Configuration（設定）** → **Security（セキュリティ）**の順にクリックします。
   Encryption Keys（暗号化キー）ページが表示されます。
3. **Actions**（アクション）をクリックして、**Add Encryption Key**（暗号化キーを追加）をクリックします。
   Create Encryption Key（暗号化キーを作成）ダイアログボックスが表示されます。
4. **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
Name（名前）	暗号化キーの名前を入力します。
Description（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。

5. **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、データにアクセスできなくなります。

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 に移動します。
2. **Configuration（設定）** → **Security（セキュリティ）**の順にクリックします。
   Encryption Keys（暗号化キー）画面が表示されます。
3. 編集する暗号化キーを選択し、**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。
4. **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。
5. **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 に移動します。
2. **Configuration（設定）** → **Security（セキュリティ）**の順にクリックします。
   Encryption Keys（暗号化キー）ページが表示されます。

3. 変更する暗号化キーを選択して、**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。
4. **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。
5. **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 に移動します。
2. **Configuration（設定）→ Security（セキュリティ）**の順にクリックします。
3. **Actions**（アクション）ドロップダウンメニューを選択し、**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。
4. **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。
5. **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 に移動します。
2. **Configuration（設定）→ Security（セキュリティ）**の順にクリックします。
3. エクスポートする暗号化キーの名前の横にある **>** をクリックして、**Export**（エクスポート）をクリックします。
   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。
4. **Export Key**（キーのエクスポート）ダイアログボックスで、**Download Key**（キーのダウンロード）をクリックして、暗号化キーを安全な場所に保存します。
5. **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 に移動します。
2. **Configuration（設定）→ Security（セキュリティ）**の順にクリックします。
3. 削除する暗号化キーの名前の横にある **>** をクリックして、**Remove**（削除）をクリックします。
   Remove Key（キーの削除）ダイアログボックスが表示されます。
4. **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。
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。

クラウドタイプ	テキストボックス	説明
	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。

レプリケーションについて

ワークステーションとサーバーの保護について

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: 本項では基本的に、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。

レプリケーションについて

レプリケーションは、リカバリポイントをコピーして、災害復旧用の第 2 の場所に送信するプロセスです。このプロセスには、2 つのコア間にペアリングされたソース / ターゲット関係が必要です。ソースコアは保

護対象マシンのリカバリポイントをコピーし、それら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。このオフサイトの場所は、会社が所有するデータセンター（自己管理コア）または第三者のマネージドサービスプロバイダ（MSP）の場所にすることも、クラウド環境にすることもできます。MSP に複製する場合、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。レプリケーションには次のシナリオが考えられます。

- **Replication to a Local Location**（ローカルロケーションへの複製）。ターゲットコアは、ローカルデータセンターまたはオンサイトの場所に配置され、複製は常に維持されます。この構成では、Core が失われてもリカバリは妨げられません。
- **Replication to an Off-site Location**（オフサイトロケーションへの複製）。ターゲットコアは、損失発生時のリカバリ用にオフサイトの災害復旧施設に配置されます。
- **Mutual Replication**（相互レプリケーション）。2 か所に配置された 2 つのデータセンターそれぞれにコアがあり、これらのコアがエージェントを保護し、相互のオフサイト災害復旧バックアップとして機能します。このシナリオでは、各コアが、もう一方のデータセンターにあるコアに保護対象マシンを複製します。
- **Hosted and Cloud Replication**（ホストされている複製およびクラウド複製）。AppAssure MSP パートナーは、データセンターまたはパブリッククラウドに複数のターゲットコアを維持します。MSP パートナーはこれらの各コアで、1 件または複数の顧客が各自のサイトのソースコアから MSP のターゲットコアにリカバリポイントを有料で複製できるようにします。

メモ: このシナリオでは、顧客は自分のデータにだけアクセスできます。

レプリケーションの設定としては以下のものがあります。

- **Point to Point**（ポイントツーポイント）。1 つの保護対象マシンを 1 つのソースコアから 1 つのターゲットコアに複製します。

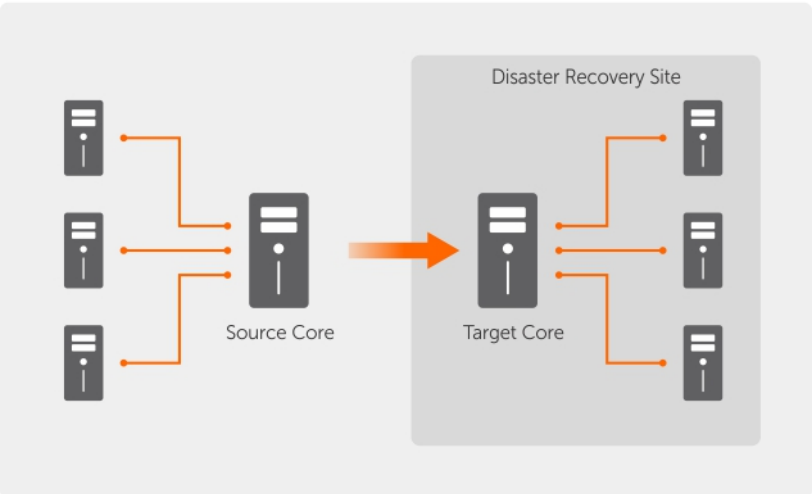


図 7. 基本的な複製アーキテクチャの図

- **Multi-Point to Point**（マルチポイントツーポイント）。複数のソースコアを 1 つのターゲットコアに複製します。

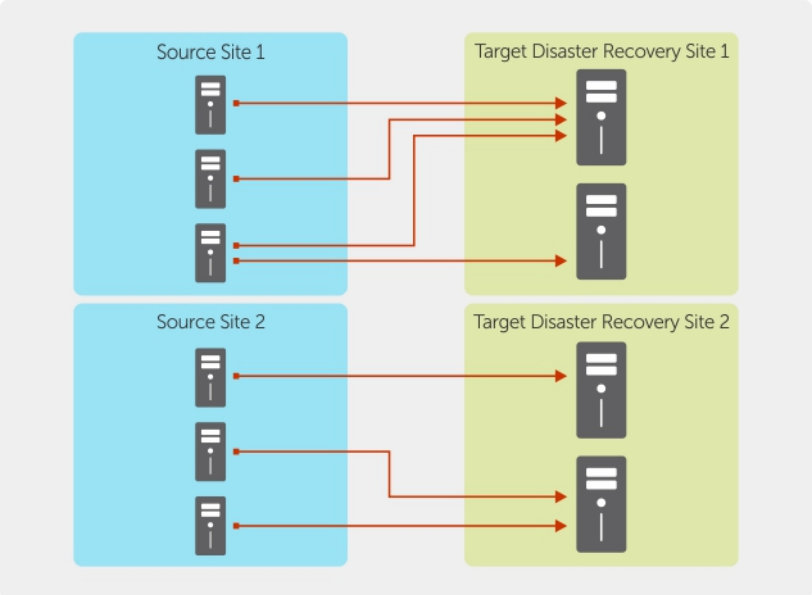


図 8. マルチポイント複製アーキテクチャの図

シーディングについて

レプリケーションは、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、最大数百または数千ギガバイトのデータが追加されることがあります。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、大規模なデータセットやサイト間のリンクが低速の場合に役立ちます。

メモ: ネットワーク接続を介してベースデータをシーディングすることもできますが、推奨されません。初期シーディングは、非常に大量のデータを伴う可能性があり、通常の WAN 接続では対応できない場合があります。たとえば、シードデータが 10 GB で、WAN リンクが 24 Mbps を送信する場合、送信が完了するまでの所要日数が 40 日を超えることがあります。

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。

シーディングは 2 段階のプロセスで構成されます（コピーと消費）。

- 最初の段階であるコピーは、最初にレプリケートされたデータのリムーバブルメディアソースへの書き込みです。コピーによって、ソースコアの既存のリカバリポイントがすべてローカルのリムーバブルストレージデバイス（USB ドライブなど）にレプリケートされます。コピーが完了したら、ソースコアの場所からリモートターゲットコアの場所にドライブを移動させる必要があります。
- 次の段階の消費は、ターゲットコアが、移動されたドライブを受け取り、複製されたデータをリポジトリにコピーするときに行われます。ターゲットコアはリカバリポイントを消費し、それらを使用して複製された保護対象マシンを形成します。

メモ: 増分スナップショットのレプリケーションはシーディングが完了する前にソースコアとターゲットコア間で発生する可能性がありますが、ソースからターゲットに転送されるレプリケートされたデータは、初期データが消費されるまで「孤立」したままになり、レプリケートされたベースイメージと組み合わせられます。

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。

フェールオーバーおよびフェールバックについて

ソースコアおよび保護対象マシンが故障したような深刻な機能停止が発生した場合、DL Appliance はレプリケーション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保護対象マシン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コア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、故障したソースコアによって保護されていた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ことです。ターゲットコアは、複製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すぐ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）に保護対象マシン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、保護対象マシン（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。保護対象マシンが復元されると、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。

レプリケーションと暗号化されたリカバリポイントについて

シードドライブにはソースコアレジストリと証明書のバックアップは含まれませんが、ソースからターゲットにレプリケートされるリカバリポイントが暗号化されている場合は、ソースコアからの暗号化キーが含まれます。レプリケートされたリカバリポイントは、ターゲットコアに転送された後も暗号化された状態を維持します。ターゲットコアの所有者または管理者には、暗号化されたデータを復号するためのパスフレーズが必要です。

レプリケーションの保持ポリシーについて

レプリケーションタスクは、ロールアップまたはアドホックの削除の結果としてマージされたリカバリポイントを転送するため、ソースコアの保持ポリシーが、ターゲットコアに複製されたデータの保持ポリシーを決定します。

メモ: ターゲットコアでは、ロールアップも、リカバリポイントのアドホック削除もできません。これらのアクションは、ソースコアからのみ実行できます。

レプリケートされたデータ転送のパフォーマンスに関する考慮事項

ソースコアとターゲットコア間の帯域幅で、保存されているリカバリポイントの転送に対応できない場合、ソースコアで保護されている特定のサーバーからのベースイメージとリカバリポイントをターゲットコアにシーディングすることからレプリケーションが始まります。このシーディングプロセスは、定期的にスケジュールされたレプリケーションに必要な基礎となるので、1 度だけしか実行する必要はありません。

レプリケーションを準備するときは、以下の点に注意する必要があります。

変更レート

変更レートは、保護されたデータの量が蓄積されるレートです。このレートは、保護されたボリューム上で変更されるデータの量と、ボリュームの保護間隔によって異なります。ボリューム上の 1 組のブロックが変更される場合は、保護間隔を短くすると変更レートが下がります。

帯域幅

帯域幅は、ソースコアとターゲットコア間で可能な転送スピードです。スナップショットによって作成されるリカバリポイントを常に維持できるように、帯域幅はレプリケーションの変更レートよりも大きいことが重要です。コアからコアに送信されるデータ量に応じて、複数のパラレルストリームは最大 1 GB イーサネット接続速度のワイヤスピードで実行される必要がある場合があります。

メモ: ISP によって指定される帯域幅は、使用可能な合計帯域幅です。送信帯域幅は、ネットワーク上のすべてのデバイスで共有されます。変更レートに対応できるレプリケーション用の十分な帯域幅があることを確認してください。

保護対象マシンの数

ソースコアごとに保護されるマシンの数と、ターゲットに複製する予定の数を考慮することが重要です。AppAssure では、保護対象サーバー単位でレプリケーションを実行できるので、特定のサーバーを複製するように選択できます。これは、保護対象のすべてのサーバーを複製する必要があるとき、特にソースコアとターゲットコア間の帯域幅が複製されるリカバリポイントの量とサイズに対して十分でない場合に、変更レートに大きな影響を及ぼします。

ネットワーク設定によっては、レプリケーションは非常に時間のかかるプロセスになります。

次の表に、妥当な変更レートを維持するために必要なギガバイトあたりの帯域幅の例を示します。

メモ: 最適な結果を得るため、次の表に示す推奨事項に従ってください。

WAN 接続タイプごとの最大変更レート

表 2. WAN 接続タイプごとの最大変更レート

ブロードバンド	帯域幅	最大変更レート
DSL	768 Kbps 以上	330 MB/ 時
ケーブル	1 Mbps 以上	429 MB/ 時
T1	1.5 Mbps 以上	644 MB/ 時
ファイバー	20 Mbps 以上	838 GB/ 時

データ転送中にリンクが切れた場合、レプリケーションはリンク機能の回復後に前回の不具合ポイントから再開されます。

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。

テキストボックス	説明
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。

第三者が管理するターゲットコアへのレプリケーションの設定

メモ: この設定は、ホストされているレプリケーションおよびクラウドレプリケーションに適用されます。AppAssure をマルチポイントツーポイントレプリケーション向けに設定している場合、すべてのソースコアでこのタスクを実行する必要があります。

第三者が管理するコアにレプリケーションを設定するには、次の手順を実行します。

1. Core Console に移動し、**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、**Add Remote Core**（リモートコアを追加）をクリックします。
3. **Select Replication Type**（レプリケーションタイプの選択）ダイアログボックスで、**I have a subscription to a third-party providing off-site backup and disaster recovery services, and wish to replicate my backups to that service**（第三者提供のオフサイトバックアップおよび災害復旧サービスを契約しており、バックアップをそのサービスに複製したい）オプションを選択し、次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 Name（ホスト名）	リモートコアマシンのホスト名、IP アドレス、または FQDN を入力します。
Port（ポート）	第三者サービスプロバイダから提供されたポート番号を入力します。

テキストボックス	説明
	デフォルトポート番号は 8006 です。

4. **Continue**（続行）をクリックします。
5. **Add Remote Core**（リモートコアを追加）ダイアログボックスで、次を行います。
   a. 複製する保護対象マシンを選択します。
   b. 保護対象マシンごとにリポジトリを選択します。
   c. 契約時の電子メールアドレスとサービスプロバイダによって割り当てられたカスタマー ID を入力します。
6. ベースデータの転送のためにシーディングプロセスを実行することを計画している場合は、**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）の横にあるチェックボックスを選択します。
7. **Submit Request**（リクエストを送信）をクリックします。

   メモ: 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）を選択すると、**Copy to Seed Drive**（シードドライブにコピー）ダイアログボックスが表示されます。
8. **Copy to Seed Drive**（シードドライブにコピー）ダイアログボックスで、次の表に説明されているとおりにシードドライブの情報を入力します。

テキストボックス	説明
Location（場所）	初期データを保存したいドライブ（ローカル USB ドライブなど）へのパスを入力します。
User name（ユーザー名）	ドライブに接続するためのユーザー名を入力します。 **メモ:** シードドライブがネットワーク共有上にある場合、これは必須です。
Password（パワード）	ドライブに接続するためのパスワードを入力します。 **メモ:** シードドライブがネットワーク共有上にある場合、これは必須です。
Maximum size（最大サイズ）	次のオプションのいずれかを選択します。 • The entire target（ターゲット全体）。 • A portion of the drive's available space（ドライブの使用可能なスペースの一部）。 ドライブの一部を指定するために次の手順を実行します。 a. テキストボックスに希望の容量を入力します。 b. 単位を選択します。
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。

テキストボックス　説明

- **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。

Agents（エージェント）　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。

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。

9. **Start**（開始）をクリックして、指定したパスにシードドライブを書き込みます。
10. 第三者サービスプロバイダの指示に従ってシードドライブを送信します。

レプリケーションリクエストの確認

レプリケーションリクエストはソースコアから第三者のターゲットコアに送信されます。第三者はそのリクエストを確認した後、承認して顧客のレプリケーションを開始したり、拒否してレプリケーションを中止したりできます。

第三者のターゲットコアで複製リクエストを確認するには、次の手順を実行します。

1. ターゲットコア上で Core Console を開き、**Replication**（レプリケーション）タブを選択します。
2. **Pending Requests (#)**（保留中のリクエスト（#））をクリックします。
   Pending Replication Requests（保留中の複製リクエスト）セクションが表示されます。
3. 確認するリクエストの横にあるドロップダウンメニューから、**Review**（レビュー）を選択します。
   Review Replication Request（レプリケーションリクエストの確認）ウィンドウが表示されます。

   メモ: 顧客が実行したリクエストに従って、**Source Core Identity**（ソースコアアイデンティティ）セクションに情報が表示されます。
4. Review Replication Request（複製リクエストの確認）ウィンドウで、次のいずれかを実行します。
   - リクエストを拒否するには、**Deny**（拒否）をクリックします。
   - リクエストを承認するには、次の手順を実行します。
     1. – **Replace an existing replicated Core**（既存のレプリケーション済みコアの置き換え）を選択して、ドロップダウンリストからコアを選択します。
        – **Create a new source Core**（新規ソースコアの作成）を選択します。**Core Name**（コア名）、顧客の **Email Address**（E-メールアドレス）、及び **Customer ID**（顧客 ID）を確認して、必要に応じて情報を編集します。
     2. **Agents**（エージェント）で承認を適用するマシンを選択し、ドロップダウンリストで各マシンの適切なリポジトリを選択します。
     3. オプションで、**Comment**（コメント）ボックスに表示するメモを入力します。
     4. **Send Response**（応答の送信）をクリックします。

        複製が承認されます。

レプリケーション要求の無視

ターゲットコアの第三者サービスプロバイダとして、顧客から送信されたレプリケーションリクエストを無視することができます。このオプションは、顧客が誤ってリクエストを送信した場合や最初に確認を行わずにリクエストを拒否する場合に使用できます。

複製リクエストを無視するには、次の手順を実行します。

1. 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。
2. Replication（複製）タブで、**Pending Requests (#)**（保留中のリクエスト（#））をクリックします。
   Pending Replication Requests（保留中の複製リクエスト）セクションが表示されます。
3. 無視するリクエストの横にあるドロップダウンメニューを使用して、**Ignore**（無視）を選択します。
   リクエストが無視されたことを示す通知が、ターゲットコアからソースコアに送信されます。

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 3. 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

セクション	説明	利用可能なアクション
		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。	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。

オプション	説明
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）。

フェールオーバーとフェールバックのロードマップ

ソースコアとそれに関連する保護対象マシンに障害が発生する災害状況が発生した場合は、AppAssure でフェールオーバーを有効にして、同一フェールオーバー（ターゲット）コアに保護を切り替え、障害が発生し

たエージェントと同じ新しい（レプリケーションされた）エージェントを起動できます。ソースコアとエージェントが修復された後は、フェールオーバーされたコアとエージェントからソースコアとエージェントにデータを復元するためのフェールバックを実行することができます。AppAssure では、フェールオーバーとフェールバックに関して次の手順を実行します。

- フェールオーバー用に環境をセットアップする。
- ターゲットコアとそれに関連するエージェントに対してフェールオーバーを実行する。
- フェールバックを実行してソースコアを復元する。

フェールオーバーのための環境のセットアップ

フェールオーバー用に環境をセットアップするには、ソースおよびターゲットの Core とそれに関連するエージェントをレプリケーション用にセットアップしておく必要があります。この処置の手順を実行して、フェールオーバー用にレプリケーションをセットアップします。

フェールオーバー用に環境をセットアップするには、次の手順を実行します。

1. ソース用のコアとターゲット用のコアをインストールします。
2. ソースコアで保護する AppAssure Agent をインストールします。
3. レポジトリをソースコアに 1 つ、ターゲットコアに 1 つ作成します。
   詳細については、「リポジトリの作成」を参照してください。
4. ソースコア下に保護用のエージェントを追加します。
   詳細については、「マシンの保護」を参照してください。
5. ソースからターゲットコアへのレプリケーションをセットアップして、保護対象エージェントをすべてのリカバリポイントでレプリケートします。
   「自己管理コアへのレプリケーション」の手順に従って、レプリケーション先にターゲットコアを追加します。

ターゲットコアでのフェールオーバーの実行

ソースコアおよび関連する保護対象マシンが故障する災害状況が発生した場合、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を一時的に置き換えます。

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**（受信レプリケーション）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。
   このマシンに対する表内のステータスが **Failover**（フェールオーバー）に変わります。
4. **Machines**（マシン）タブをクリックして、リカバリポイントを持つ関連 AppAssure エージェントを持つマシンを選択します。
5. 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。
6. AppAssure エージェントを持つマシンをシャットダウンします。
7. 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。
8. 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。

9. ターゲットコアの Core Console に戻り、**Protected Machines**（保護マシン）にある **Machines**（マシン）タブと **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。
10. 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実行」を参照してください。
11. 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

障害の発生した元のソースコアおよび保護対象マシンを修復または交換した後に、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。
   Failback Warnings（フェールバック警告）ダイアログボックスが表示され、**Start Failback**（フェールバックの開始）ボタンをクリック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. ターゲットコアの Core Console で、**Tools**（ツール）タブをクリックします。
7. 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。
8. 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。
9. 手順 7 で作成したアーカイブをインポートします。
10. 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。
11. **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。
12. **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。
13. **Failback Warnings**（フェールバック警告）ダイアログボックスで、**Start Failback**（フェールバックの開始）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。
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。

イベントの管理

コアイベントの管理は、コアの正常性および使用率の監視に役立ちます。コアには定義済みのイベントセットが含まれており、これらのイベントは、コアまたはバックアップジョブに関する重大な問題を管理者に通知するために使用できます。

Events（イベント）タブから、通知グループ、E-メールの SMTP 設定、繰り返し削減、および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でき、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
  - アタッチ可否
  - 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
  - 複製
  - ロールバック
  - SMTP サーバー設定
  - 有効化されたトレースログ
  - クラウド設定
- 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。
  - E-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 から **Configuration**（設定）タブを選択します。
2. **Manage**（管理）オプションから、**Events**（イベント）をクリックします。
3. **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、3 つのパネルが表示されます。

- **General（一般）**
- **Enable Events（イベントの有効化）**
- **Notification Options（通知オプション）**

4. **General**（一般）パネルで、次のように通知グループの基本情報を入力します。

テキストボックス	説明
Name（名前）	イベント通知グループの名前を入力します。これは、イベント通知グループを識別するために使用されます。
Description（説明）	イベント通知グループの説明を入力します。これはイベント通知グループの目的を説明するために使用されます。

5. **Enable Events**（イベントの有効化）パネルで、イベントログ（アラート）を作成して報告する状態を選択します。
   以下についてのアラートを作成できます。
   - **すべてのイベント**
   - **アプライアンスイベント**
   - **起動 CD**
   - **セキュリティ**
   - **データベース保持**
   - **ローカルマウント**
   - **クラスタ**
   - **通知**
   - **Power Shell スクリプト**
   - **プッシュインストール**
   - **夜間ジョブ**
   - **アタッチ可否**
   - **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**
   - **複製**
   - **リポジトリ**
   - **ロールバック**
   - **ロールアップ**
6. **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）	E-メール通知の受信者を指定します。別々の複数 E-メールアドレスのほか、ブラインドカーボンコピーを指定することもできます。次の選択が可能です。 • **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。これは、Windows イベントログを介してアラート通知を報告する必要があるかどうかを指定するために使用されます。
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 の詳細を指定します。 • **Hostname:（ホスト名：）** • **Port:1（ポート：1）**

7. **OK** をクリックします。

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

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

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

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

1. Core から **Configuration**（設定）タブを選択します。
2. **Manage**（管理）オプションから、**Events**（イベント）をクリックします。
3. **Email SMTP Settings**（E-メール SMTP 設定）ペインで、**Change**（変更）をクリックします。
   Edit Email Notification Configuration（電子メール通知設定の編集）ダイアログボックスが表示されます。
4. **Enable Email Notifications**（E-メール通知を有効にする）を選択し、次で説明されている E-メールサーバーの詳細を入力します。

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

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

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

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 から、**Configuration**（設定）タブをクリックします。
2. **Manage**（管理）オプションから、**Events**（イベント）をクリックします。
3. **Repetition Reduction**（繰り返し削減）領域から、**Change**（変更）をクリックします。
   Repetition Reduction（繰り返し削減）ダイアログボックスが表示されます。
4. **Enable Repetition Reduction**（繰り返し削減を有効にする）を選択します。
5. **Store events for X minutes** （次のイベントを X 分間保存）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分数を入力します。
6. **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 から、**Configuration**（設定）タブをクリックします。
2. **Manage**（管理）オプションから、**Events**（イベント）をクリックします。
3. **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。

4. **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。
5. **保存** をクリックします。

リカバリの管理

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

システム情報について

AppAssure では、お使いのシステムの情報、ローカルおよびマウントされたボリューム、AppAssure エンジンの接続を含む、Core についての情報を表示できます。

コア上にローカルにマウントされた各リカバリポイントまたはすべてのリカバリポイントをマウント解除する場合は、**Tools**（ツール）タブの **Mount**（マウント）オプションからこれを実行できます。

システム情報の表示

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 に移動して、**Tools**（ツール）タブを選択します。
2. **Tools**（ツール）オプションから **System Info**（システム情報）をクリックします。

インストーラのダウンロード

インストーラを Core からダウンロードできます。**Tools**（ツール）タブから、Agent Installer または Local Mount Utility をダウンロードする選択ができます。

メモ: Agent Installer へのアクセスについては、「Agent Installer のダウンロードとインストール」を参照してください。Agent Installer 導入の詳細については、**Dell.com/support/home** にある『*Dell DL4300 Appliance Deployment Guide*』（Dell DL4300 アプライアンス導入ガイド）を参照してください。Local Mount Utility Installer へのアクセスについては、「Local Mount Utility について」を、Local Mount Utility の詳細については、「Local Mount Utility のダウンロードとインストール」を参照してください。

Agent Installer について

Agent Installer は、Core によって保護する予定のマシン上に、AppAssure Agent アプリケーションをインストールするために使用します。Agent Installer を必要とするマシンがある場合は、Core の **Tools**（ツール）タブからウェブインストーラをダウンロードできます。

メモ: Core のダウンロードは、ライセンスポータルから実行します。Core インストーラをダウンロードするには、**https://licenseportal.com** にアクセスしてください。

Agent Installer のダウンロードおよびインストール

Agent Installer は、Core で保護される任意のマシンにダウンロードして導入することができます。

Agent Installer をダウンロードおよびインストールするには、次の手順を実行します。

1. Agent Installer をライセンスポータルまたは Core からダウンロードします。
   例：**Agent-X64-5.3.x.xxxxx.exe**
2. **Save File**（ファイルの保存）をクリックします。
   エージェントのインストールの詳細については、**Dell.com/support/home** にある『*Dell DL4300 Appliance Deployment Guide*』（DL4300 アプライアンス導入ガイド）を参照してください。

Local Mount Utility について

Local Mount Utility（LMU）はダウンロード可能なアプリケーションであり、このユーティリティを使用して任意のマシンからリモートの Core にリカバリポイントをマウントできます。この軽量ユーティリティには、`aavdisk` ドライバと `aavstor` ドライバが含まれますが、サービスとしては動作しません。このユーティリティをインストールすると、デフォルトでディレクトリ **C:\Program Files\AppRecovery\Local Mount Utility** にインストールされ、マシンのデスクトップにショートカットが表示されます。

このユーティリティはコアへのリモートアクセス用に設計されていますが、コアに LMU をインストールすることもできます。これがコアで実行されると、アプリケーションがそのコアからのすべてのマウント（Core Console を介して実行されたマウントを含む）を認識し、表示します。同様に、LMU で実行されたマウントもコンソールに表示されます。

Local Mount Utility のダウンロードとインストール

Local Mount Utility のダウンロードとインストールを行うには、次の手順を実行します。

1. LMU をインストールするマシンから、ブラウザにコンソール URL を入力してユーザー名とパスワードでログインすることによって、Core Console にアクセスします。
2. Core Console で **Tools**（ツール）タブをクリックします。
3. **Tools**（ツール）タブで、**Downloads**（ダウンロード）をクリックします。
4. **Local Mount Utility** で、**Download web installer**（ウェブインストーラをダウンロード）リンクをクリックします。
5. **Opening LocalMountUtility-Web.exe**（LocalMountUtility-Web.exe を開いています）ウィンドウで、**Save File**（ファイルの保存）をクリックします。
   ファイルがローカルダウンロードフォルダに保存されます。ブラウザによっては、このフォルダが自動的に開きます。

6. **ダウンロード** フォルダで、**LocalMountUtility-Web** 実行可能ファイルを右クリックして、**開く** をクリックします。

   お使いのマシンの設定によっては、**ユーザーアカウント制御** ウィンドウが表示されることがあります。
7. **ユーザーアカウント制御** ウィンドウが表示された場合は、**はい** をクリックして、プログラムがマシンに変更を加えることができるようにします。

   AppAssure Local Mount Utility Installation（AppAssure Local Mount Utility インストール）ウィザードが起動します。
8. **AppAssure Local Mount Utility Installation**（AppAssure Local Mount Utility インストール）ウィザードの **Welcome**（ようこそ）画面で、**Next**（次へ）をクリックして **License Agreement**（ライセンス契約）ページに進みます。
9. **License Agreement**（ライセンス契約）ページで、**I accept the terms in the license agreement**（ライセンス契約の条件に同意します）を選択し、**Next**（次へ）をクリックして **Prerequisites**（前提条件）ページに進みます。
10. **Prerequisites**（前提条件）ページで、必要な前提条件があればインストールし、**Next**（次へ）をクリックして **Installation Options**（インストールオプション）ページに進みます。
11. **Installation Options**（インストールオプション）ページで、以下のタスクを行います。
    a. **Change**（変更）ボタンをクリックして、LMU 向けの宛先フォルダを選択します。

       メモ: デフォルトの宛先フォルダは C:\Program Files\AppRecovery\LocalMountUtility です。
    b. **Allow Local Mount Utility to automatically send diagnostic and usage information to AppAssure Software, Inc.**（Local Mount Utility が診断情報と使用情報を自動的に AppAssure Software, Inc. に送信することを許可する）かどうかを選択します。
    c. **Next**（次へ）をクリックして **Progress**（進捗状況）ページに進み、アプリケーションをダウンロードします。アプリケーションは、プログレスバーに進捗状況を表示しながら宛先フォルダにダウンロードされます。ダウンロードが完了すると、ウィザードは自動的に **Completed**（完了しました）ページに進みます。
12. **Finish**（完了）をクリックしてウィザードを閉じます。

Local Mount Utility へのコアの追加

リカバリポイントをマウントするには、コアを LMU に追加する必要があります。追加できるコアの数に制限はありません。

Local Mount Utility にコアを追加するには、次の手順を実行します。

1. LMU がインストールされているマシンから、デスクトップアイコンをダブルクリックして LMU を起動します。
2. **User Account Control**（ユーザーアカウント制御）ウィンドウが表示された場合は、**Yes**（はい）をクリックして、プログラムがマシンに変更を加えることができるようにします。
3. AppAssure Local Mount Utility ウィンドウの左上隅で、**Add core**（コアの追加）をクリックします。
4. **Add Core**（コアの追加）ウィンドウで、次の説明に従って、要求される資格情報を入力します。

テキストボックス	説明
Host name(ホスト名)	リカバリポイントのマウント元であるコアの名前。 **メモ:** コアに LMU をインストールしている場合、LMU は自動的に localhost マシンを追加します。
Port(ポート)	コアと通信するために使用されるポート番号。

テキストボックス	説明
	デフォルトポート番号は 8006 です。
Use my Windows user credentials（自分の Windows ユーザー資格情報を使用する）	コアにアクセスするために使用する資格情報が Windows 資格情報と同じである場合は、このオプションを選択します。
Use specific credentials（特定の資格情報を使用する）	コアにアクセスするために使用する資格情報が Windows 資格情報と異なる場合は、このオプションを選択します。
User name(ユーザー名)	コアマシンにアクセスするために使用するユーザー名。 **メモ:** 特定の資格情報を使用することを選択した場合のみ、このオプションを使用できます。
Password(パスワード)	コアマシンにアクセスするために使用するパスワード。 **メモ:** 特定の資格情報を使用することを選択した場合のみ、このオプションを使用できます。

5. **接続** をクリックします。
6. 複数のコアを追加する場合は、必要に応じて手順 3～5 を繰り返します。

Local Mount Utility を使用したマウント済みリカバリポイントの検索

メモ: リカバリポイントをマウントした後すぐに検索する場合は、マウント手順完了時にリカバリポイントを含むフォルダが自動的に開くため、この手順は必要ありません。

Local Mount Utility を使用してマウントされたリカバリポイントを検索するには、次の手順を実行します。

1. LMU がインストールされているマシンから、デスクトップアイコンをダブルクリックして LMU を起動します。
2. メインの **Local Mount Recovery**（ローカルマウントリカバリ）画面で、**Active mounts**（アクティブなマウント）をクリックします。

   Active Mounts（アクティブなマウント）ウィンドウが開き、マウントされているすべてのリカバリポイントが表示されます。
3. 回復したいリカバリポイントの横にある **Explore**（検索）をクリックして、重複排除されたボリュームのフォルダを開きます。

Local Mount Utility を使用したリカバリポイントのマウント

リカバリポイントをマウントするには、まず、Local Mount Utility をリカバリポイントが保存されている Core に接続する必要があります。「Local Mount Utility への Core の追加」で説明されているとおり、LMU に追加できるコアの数に制限はありませんが、このアプリケーションが接続できるのは一度に 1 つのコアだけです。たとえば、1 つのコアで保護されているエージェントのリカバリポイントをマウントしてから、別のコアで保護されているエージェントのリカバリポイントをマウントする場合、LMU は自動的に最初のコアから接続解除して、2 番目のコアとの接続を確立します。

Local Mount Utility を使用して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. LMU がインストールされているマシンから、デスクトップアイコンをダブルクリックして LMU を起動します。
2. メインの **AppAssure Local Mount Utility** ウィンドウから、ナビゲーションツリーで目的のコアを拡張して、保護対象エージェントを表示します。
3. ナビゲーションツリーから目的のエージェントを選択します。
   リカバリポイントがメインフレーム内に表示されます。
4. マウントするリカバリポイントを展開して、個々のディスクのボリュームまたはデータベースを表示します。
5. マウントするリカバリポイントを右クリックして、次のいずれかを選択します。
   - Mount（マウント）
   - Mount writable（書き込み可能マウント）
   - Mount with previous writes（以前の書き込みでマウント）
   - Advanced mount（高度なマウント）
6. **Advanced Mount**（高度なマウント）ウィンドウから、次に示すオプションを設定します。

テキストボックス	説明
Mount point path（マウントポイントのパス）	デフォルトマウントポイントのパス以外のリカバリポイントのパスを選択するには、**Browse**（参照）ボタンをクリックします。
Mount type（マウントタイプ）	次のオプションのいずれかを選択します。 • Mount read-only（読み取り専用マウント） • Mount writable（書き込み可能マウント） • Mount read-only with previous writes（以前の書き込みで読み取り専用マウント）

7. **Mount**（マウント）をクリックします。

LMU が、マウントされたリカバリポイントを含むフォルダを自動的に開きます。

メモ: すでにマウントされているリカバリポイントを選択すると、リカバリポイントのマウント解除を促す **Mounting**（マウント）ダイアログボックスが表示されます。

Local Mount Utility を使用したリカバリポイントのマウント解除

Local Mount Utility を使用して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. LMU がインストールされているマシンから、デスクトップアイコンをダブルクリックして LMU を起動します。
2. メインの **Local Mount Recovery**（ローカルマウントリカバリ）画面で、**Active mounts**（アクティブなマウント）をクリックします。
   Active Mounts（アクティブなマウント）ウィンドウが開き、マウントされているすべてのリカバリポイントが表示されます。
3. リカバリポイントをマウント解除するには、以下の表に説明されているいずれかのオプションを選択します。

オプション	説明
Dismount（マウント解除）	隣接したリカバリポイントのみをマウント解除します。 a. 選択したリカバリポイントの横にある **Dismount**（マウント解除）をクリックします。 b. ウィンドウを閉じます。
Dismount all（すべてをマウント解除）	マウントされたリカバリポイントのすべてをマウント解除します。 a. **Dismount all**（すべてをマウント解除）をクリックします。 b. **Dismount All**（すべてをマウント解除）ウィンドウで、**Yes**（はい）をクリックして確定します。 c. ウィンドウを閉じます。

Local Mount Utility のトレイメニューについて

LMU のトレイメニューは、デスクトップのタスクバーにあります。アイコンを右クリックすると、次のオプションが表示されます。

Browse Recovery Points（リカバリポイントの参照）	LMU メイン画面が開きます。
Active Mounts（アクティブなマウント）	Active Mounts（アクティブなマウント）画面が開きます。
オプション	Options（オプション）画面が開きます。ここで、**Default Mount Point Directory**（デフォルトのマウントポイントディレクトリ）、**Default Core Credentials**（デフォルトの Core 資格情報）、および LMU ユーザーインタフェースの **Language**（言語）を変更できます。
バージョン情報	ライセンス情報のスプラッシュ画面を開きます。
終了	アプリケーションを閉じます。

メモ: メイン画面の上部の隅にある X を使用すると、アプリケーションがトレイ内に最小化されます。

コアとエージェントオプションの使用

メイン LMU 画面でコアまたはエージェントを右クリックすることで、特定のオプションを使用できます。次のオプションがあります。

- Localhost オプション
- Remote Core（リモートコア）オプション
- Agent（エージェント）オプション

Localhost オプションへのアクセス

Localhost オプションにアクセスするには、Core またはエージェントを右クリックし、Core への **Reconnect**（再接続）をクリックします。Core からの情報（最近追加されたエージェントなど）がアップデートされ、更新されます。

リモートコアオプションへのアクセス

リモートコアオプションにアクセスするには、Core またはエージェントを右クリックしてから、次の説明に従ってリモートコアオプションのいずれかを選択します。

オプション	説明
Reconnect to core（コアへの再接続）	最近追加されたエージェントなどのコアの情報をアップデートして更新します。
Remove core（コアの削除）	**Local Mount Utility** からコアを削除します。
Edit core（コアの編集）	**Edit Core**（コアの編集）ウィンドウが開きます。ここで、ホスト名、ポートおよび資格情報を変更できます。

エージェントオプションへのアクセス

エージェントオプションにアクセスするには、Core またはエージェントを右クリックして、**Refresh recovery points**（リカバリポイントの更新）をクリックします。選択したエージェントのリカバリポイントのリストがアップデートされます。

保持ポリシーの管理

すべての保護対象サーバーの定期バックアップスナップショットは、長期にわたって Core に蓄積されます。保持ポリシーは、バックアップスナップショットの保持期間を延長したり、これらのバックアップスナップショットの管理に利用したりするために使用されます。保持ポリシーは、古いバックアップのエージングと削除に役立つ夜間ロールアッププロセスによって適用されます。保持ポリシーの設定については、「保持ポリシー設定のカスタマイズ」を参照してください。

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。

アーカイブについて

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。したがって、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、**Configuration**（設定）タブをクリックします。
2. **Manage**（管理）オプションから、**Archive**（アーカイブ）をクリックします。
   Create Archive（アーカイブを作成）ダイアログボックスが表示されます。
3. **Create Archive**（アーカイブの作成）ダイアログボックスで、次の説明に従ってアーカイブの詳細を入力します。

テキストボックス	説明
Date range（日付範囲）	日付範囲を指定するには、開始日と終了日を選択します。
Archive password（アーカイブのパスワード）	アーカイブのパスワードを入力します。これは、アーカイブを保護するためのログイン資格情報の確立に使用されます。
Confirm（確認）	アーカイブを保護するためのパスワードを再入力します。これは、**Archive Password**（アーカイブのパスワード）テキストボックスに入力した情報の検証に使用されます。
Output Location（出力先）	出力先を入力します。これは、アーカイブを配置する場所のパスを定義するために使用されます。これには、ローカルディスクまたはネットワーク共有を指定できます。たとえば、**d:\work\archive**、またはネットワークパスの場合は **\\servername\sharename** となります。 **メモ:** 出力先がネットワーク共有の場合、ネットワーク共有に接続するためのユーザー名とパスワードを入力します。
User name(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。
Password(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。
Maximum size（最大サイズ）	アーカイブに使用する容量を入力します。次の中から選択できます。 • Entire Target（ターゲット全体） • 指定の容量（MB または GB 単位）
Recycle action（リサイクルアクション）	適切なリサイクルアクションを選択します。
Comment（コメント）	アーカイブをキャプチャするために必要な追加情報を入力します。

4. **Archive**（アーカイブ）をクリックします。

スケジュールアーカイブの設定

スケジュールアーカイブ機能では、選択されたマシンが自動的に作成される時間や、特定の場所へ保存する時間を設定できます。この機能を使用すると、この機能によってマシンのアーカイブを頻繁に保存する場合にアーカイブを手動で作成する手間が省けます。自動アーカイブをスケジュールするには次の手順に従います。
スケジュールアーカイブを設定するには、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. **Archive**（アーカイブ）オプションで、**Scheduled**（スケジュール）をクリックします。
3. Scheduled Archive（スケジュールアーカイブ）ページで、**Add**（追加）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。
4. **Add Archive Wizard**（アーカイブの追加ウィザード）の **Location**（場所）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いずれかを選択します。
   - Local: Output location（ローカル：出力場所） – 出力の場所を入力します。アーカイブを保管する場所へのパスを定義します。
   - ネットワーク
     - Output location（出力場所）： – 出力の場所を入力します。アーカイブを保管する場所へのパスを定義します。
     - User Name（ユーザー名）：ユーザー名を入力します。ネットワーク共有のためのログイン資格情報です。
     - Password（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。ネットワーク共有のためのログイン資格情報です。
   - 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。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 に追加しておく必要があります。
     - 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）：アーカイブされたデータを保存するフォルダの名前を入力します。デフォルトの名前は AppAssure-5-Archive-[作成日]-[作成時間] です。
5. **Next**（次へ）をクリックします。
6. 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。
7. **Next**（次へ）をクリックします。
8. **Options**（オプション）ページで、ドロップダウンリストから次の Recycle Actions（リサイクルアクション）のいずれかを選択します。
   - **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。
9. **Schedule**（スケジュール）ページで、以下の送信データの頻度オプションのいずれかを選択します。
   - Daily: At time（毎日：時刻） – 毎日アーカイブ作成を行う時刻を選択します。
   - Weekly（毎週）
     - At day of week（曜日）：アーカイブを自動作成する曜日を選択します。

- At time（時刻）：アーカイブを作成する時刻を選択します。

- Monthly（毎月）
  - At day of months（日）：アーカイブを作成する日を選択します。
  - At time（時刻）：アーカイブを作成する時刻を選択します。

10. アーカイブを一時停止して、後に再開するには **Initial pause archiving**（アーカイブ作業の初期一時停止）を選択します。

    アーカイブ作業を再開する前にターゲットの場所を準備する時間が必要な場合は、スケジュール済みのアーカイブを一時停止することができます。このオプションを選択しない場合は、スケジュールされた時間アーカイブ作業を開始します。
11. **Finish**（終了）をクリックします。

スケジュールアーカイブの一時停止または再開

Setting a Scheduled Archive（スケジュールアーカイブの設定）を行った際に最初にアーカイブ作業を一時停止した場合は、スケジュール済みのアーカイブ作業を後に再開することになります。
スケジュールアーカイブを一時停止または再開するには、次の手順を実行します。

1. **Core Console** に移動し、**Tools**（ツール）タブをクリックします。
2. **Archive**（アーカイブ）オプションで、**Scheduled**（スケジュール済み）をクリックします。
3. **Scheduled Archive**（スケジュール済みアーカイブ）ページで、次のいずれかを実行します。
   - 希望するアーカイブを選択して、次の処置から適切なものを 1 つクリックします。
     - Pause（一時停止）
     - Resume（再開）
   - 希望するアーカイブの横でドロップダウンメニューをクリックして、次の処置から適切なものを 1 つクリックします。
     - Pause（一時停止）
     - Resume（再開）

   アーカイブのステータスが **Schedule**（スケジュール）の列に表示されます。

スケジュール済みアーカイブの編集

1. Core Console で **Tools**（ツール）タブをクリックします。
2. **Archive**（アーカイブ）オプションで、**Scheduled**（スケジュール済み）をクリックします。
3. Scheduled Archive（スケジュール済みアーカイブ）のページで、変更するアーカイブ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。

   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。
4. **Add Archive Wizard**（アーカイブの追加ウィザード）の **Location**（場所）ページで、**Location Type**（場所のタイプ）ドロップダウンリストから、次のオプションのいずれかを選択します。
   - Local: Output location（ローカル：出力場所） – 出力の場所を入力します。アーカイブを保管する場所へのパスを定義します。
   - Network（ネットワーク）
     - Output location（出力場所）： – 出力の場所を入力します。アーカイブを保管する場所へのパスを定義します。

- User Name（ユーザー名）: ユーザー名を入力します。ネットワーク共有のためのログイン資格情報です。
- Password（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。ネットワーク共有のためのログイン資格情報です。

• Cloud（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。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 に追加しておく必要があります。
- 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）: アーカイブされたデータを保存するフォルダの名前を入力します。デフォルトの名前は AppAssure-5-Archive-[作成日]-[作成時間] です。

5. **Next**（次へ）をクリックします。
6. 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。
7. **Next**（次へ）をクリックします。
8. **Schedule**（スケジュール）ページで、以下の送信データの頻度オプションのいずれかを選択します。
   - Daily: At time（日毎：時刻） – 日毎のアーカイブ作成を行う時刻を選択します。
   - Weekly（毎週）
     - At day of week（曜日）: アーカイブを自動作成する曜日を選択します。
     - At time（時刻）: アーカイブを作成する時刻を選択します。
   - Monthly（毎月）
     - At day of months（日）: アーカイブを作成する日を選択します。
     - At time（時刻）: アーカイブを作成する時刻を選択します。
9. アーカイブを一時停止して、後に再開するには **Initial pause archiving**（アーカイブ作業の初期一時停止）を選択します。

   アーカイブ作業を再開する前にターゲットの場所を準備する時間が必要な場合に、スケジュール済みのアーカイブを一時停止することができます。このオプションを選択しない場合は、スケジュールされた時間にアーカイブ作業を開始します。
10. **Finish**（終了）をクリックします。

アーカイブのチェック

アーカイブチェックを実行することにより、アーカイブ構造の整合性をスキャンすることができます。このチェックによって必要なすべてのファイルがアーカイブ内に存在することを確認します。アーカイブチェックを実行するには、次の手順に従ってください。

1. Core Console で **Tools**（ツール）タブをクリックします。
2. **Archive**（アーカイブ）オプションで **Check Archive**（アーカイブのチェック）をクリックします。

   Check Archive（アーカイブのチェック）ダイアログボックスが表示されます。
3. ドロップダウンリストから次のオプションのいずれか選択します。
   - Local: Output location（ローカル：出力場所） – 出力の場所を入力します。アーカイブを保管する場所へのパスを定義します。
   - Network（ネットワーク）
     - Output location（出力場所）: – 出力の場所を入力します。アーカイブを保管する場所へのパスを定義します。

- User Name（ユーザー名）: ユーザー名を入力します。ネットワーク共有のためのログイン資格情報です。
- Password（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。ネットワーク共有のためのログイン資格情報です。

• Cloud（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。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 に追加しておく必要があります。
- 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に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）: アーカイブされたデータを保存するフォルダの名前を入力します。デフォルトの名前は AppAssure-5-Archive-[作成日]-[作成時間] です。

4. 構造の整合性チェックを実行するには、**Structure integrity**（構造の整合性）を選択します。
5. **Check File**（ファイルのチェック）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、**Configuration**（設定）タブを選択します。
2. **Manage**（管理）オプションから **Archive**（アーカイブ）をクリックし、次に **Import**（インポート）をクリックします。

   Import Archive（アーカイブをインポート）ダイアログボックスが表示されます。
3. **Import Archive**（アーカイブのインポート）ダイアログボックスで、次の説明に従ってアーカイブのインポートの詳細を入力します。

テキストボックス	説明
Input Location（入力元）	アーカイブのインポートの場所を選択します。
User name(ユーザー名)	アーカイブへの安全なアクセスを確立するために、ログオン資格情報を入力します。
Password(パスワード)	アーカイブにアクセスするためのパスワードを入力します。

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。

SQL アタッチ可否の管理

SQL アタッチ可否設定により、Core は Microsoft SQL Server のローカルインスタンスを使用して SQL サーバーのスナップショット内の SQL データベースとログファイルをアタッチできるようになります。アタッチ可否テストでは、Core が SQL データベースの整合性をチェックし、バックアップスナップショット内のすべてのデータファイル（MDF および LDF ファイル）が使用可能であることが確認されます。アタッチ可

否チェックは、特定のリカバリポイントに対してオンデマンド実行することも、夜間ジョブの一部として実行することもできます。

アタッチ可否には、AppAssure Core マシン上の Microsoft SQL Server のローカルインスタンスが必要です。このインスタンスは、Microsoft から直接あるいは正規の再販売業者経由で入手したフルライセンスバージョンの SQL Server でなければなりません。Microsoft は、パッシブ SQL ライセンスの使用を認めてはいません。

アタッチ可否では、SQL Server 2005、2008、2008 R2、2012 および 2014 がサポートされます。テストを実行する際に使用するアカウントには、SQL Server インスタンス上で sysadmin 役割が付与されている必要があります。

SQL Server のディスク型ストレージフォーマットは、64 ビット環境と 32 ビット環境の両方で同じであり、アタッチ可否は両方のバージョンで機能します。ある環境で実行されているサーバーインスタンスからデタッチされたデータベースは、別の環境で実行されているサーバーインスタンス上にアタッチすることができます。

注意: Core 上の SQL Server のバージョンは、SQL Server がインストールされているすべてのエージェントの SQL Server バージョンと同じ、またはそれ以降のバージョンである必要があります。

SQL アタッチ可否の設定

保護対象 SQL データベースに対するアタッチ可否チェックを実行する前に、エージェントマシンに対するチェックを実行する際に使用する、Core マシン上の SQL Server のローカルインスタンスを選択します。

メモ: アタッチ可否には、AppAssure Core マシン上の Microsoft SQL Server のローカルインスタンスが必要です。このインスタンスは、Microsoft から直接あるいは正規の再販売業者経由で入手したフルライセンスバージョンの SQL Server でなければなりません。Microsoft は、パッシブ SQL ライセンスの使用を認めてはいません。

SQL アタッチ可否を設定するには、次の手順を実行します。

1. Core Console に移動してタブをクリックします。
2. **Configuration（設定）→ Settings（設定）**の順にクリックします。
3. Nightly Jobs（夜間ジョブ）ペインで、**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。
4. **Attachability Check Job**（アタッチ可否チェックジョブ）を選択して、**Settings**（設定）をクリックします。
5. ドロップダウンメニューを使用して、次のオプションから Core にインストールされている SQL サーバーのインスタンスを選択します。
   次から選択できます。
   - **SQL Server 2005**
   - **SQL Server 2008**
   - **SQL Server 2008 R2**
   - **SQL Server 2012**
   - **SQL Server 2014**
6. 資格情報タイプを選択します。
   次から選択できます。
   - **Windows**
   - **SQL**
7. 次の説明に従って、Windows または SQL Server インスタンスに対する管理者権限を持つ資格情報を指定します。

テキストボックス	説明
Username（ユーザー名）	SQL Server へのログオン許可のためのユーザー名を入力します。
Password(パスワード)	SQL アタッチ可否のためのパスワードを入力します。これにより、ログオンアクティビティが制御されます。

8. **Test Connection**（テスト接続）をクリックします。

   メモ: 資格情報の入力が正しくない場合、資格情報テストに失敗したことを警告するメッセージが表示されます。資格情報を修正し、接続テストを再度実行してください。

9. **Save**（保存）をクリックします。
   これで、保護対象 SQL Server データベース上で実行するアタッチ可否チェックが使用可能になりました。
10. Nightly Jobs（夜間ジョブ）ウィンドウで、 **OK** をクリックします。
    アタッチ可否チェックが夜間ジョブで実行されるようスケジュールされました。

夜間 SQL アタッチ可否チェックとログの切り捨ての設定

夜間 SQL アタッチ可否チェックとログの切り捨てを設定するには、次の手順を実行します。

1. Core の左のナビゲーション領域で、夜間アタッチ可否チェックとログ切り捨てを設定するマシンを選択し、**SQL Server Settings**（SQL サーバー設定）をクリックします。
2. Core Console に移動します。
3. **Configuration（設定）→ Settings（設定）**の順にクリックします。
4. **Nightly Jobs**（夜間ジョブ）セクションで、**Change**（変更）をクリックします。
5. 組織での必要性に基づいて、以下の SQL Server 設定を選択またはクリアします。
   - **Attachability Check Job（アタッチ可否チェックジョブ）**
   - **Log Truncation Job（ログの切り捨てジョブ、単純なリカバリモデルのみ）**
6. **OK** をクリックします。
   保護対象 SQL Server で、アタッチ可否とログの切り捨ての設定が有効になります。

Exchange データベースのマウント可否チェックとログの切り捨ての管理

AppAssure を使用して Microsoft Exchange サーバーをバックアップする場合、スナップショットが実行されるたびにすべての Exchange データベース上でマウント可否チェックを実行することができます。この破損検出機能は、潜在的な障害を管理者に警告し、障害が発生した場合に Exchange サーバー上のすべてのデータが正常に回復されることを確実にします。

メモ: マウント可否チェックとログの切り捨て機能は、Microsoft Exchange 2007、2010、および 2013 にのみ適用されます。さらに、AppAssure Agent サービスアカウントが Exchange の組織の管理者役割に割り当てられている必要があります。

Exchange データベースのマウント可否とログの切り捨ての設定

Exchange データベースサーバー設定（自動マウント可否チェック、夜間 Checksum チェック、夜間ログ切り捨てなど）を表示、有効化、または無効化できます。

Exchange データベースのマウント可否とログの切り捨てを設定するには、次の手順を実行します。

1. Core Console の左のナビゲーション領域で、マウント可否チェックおよびログの切り捨てを設定するマシンを選択します。
   選択されたマシンの **Summary**（サマリ）タブが表示されます。
2. **Exchange Server Settings**（Exchange Server 設定）をクリックします。
   Exchange Server Settings（Exchange Server 設定）ダイアログボックスが表示されます。
3. 所属組織での必要性に基づいて、以下の Exchange Server の設定を選択またはクリアします。
   - **Enable automatic mountability check（自動マウント可否チェックを有効にする）**
   - **Enable nightly checksum check（夜間 Checksum チェックを有効にする）**
   - **Enable nightly log truncation（夜間ログ切り捨てを有効にする）**
4. **OK** をクリックします。
   保護された Exchange サーバーで、マウント可否とログの切り捨ての設定が有効になります。

   メモ: ログの切り捨て強制の詳細については、「ログの切り捨ての強制」を参照してください。

マウント可否チェックの強制実行

マウント可否チェックを強制実行するには、次の手順を実行します。

1. Core Console の左のナビゲーション領域で、マウント可否チェックの強制実行先のマシンを選択して、**Recovery Points**（リカバリポイント）タブをクリックします。
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。
3. **Force Mountability Check**（マウント可否チェックを強制）をクリックします。
   マウント可否チェックを強制実行するかどうかを尋ねるメッセージが表示されます。
4. **はい** をクリックします。

   メモ: アタッチ可否チェックのステータスを表示する方法については、「イベントおよびアラートの表示」を参照してください。

   システムがマウント可否チェックを実行します。

Checksum チェックの強制実行

Checksum チェックを強制実行するには、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、Checksum チェックを強制実行するマシンを選択して、**Recovery Points**（リカバリポイント）タブをクリックします。
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。
3. **Force Checksum Check**（Checksum チェックを強制）をクリックします。
   Force Attachability Check（アタッチ可否チェックの強制）ウィンドウにより、Checksum チェックを強制実行するかどうかを確認するためのプロンプトが表示されます。
4. **はい** をクリックします。
   システムが Checksum チェックを実行します。

   メモ: アタッチ可否チェックのステータスを表示する方法の詳細に関しては、「イベントおよびアラートの表示」を参照してください。

ログの切り捨ての強制

メモ: このオプションは Exchange または SQL マシンでのみ利用できます。

ログの切り捨てを強制するには、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. **Machines**（マシン）タブから、次のいずれかを実行します。
   - ログを切り捨てるマシンのハイパーリンクをクリックします。
   - または、Navigation（ナビゲーション）ペインで、ログを切り捨てるマシンを選択します。
3. そのマシンの **Actions**（アクション）ドロップダウンメニューで、**Force Log Truncation**（ログの切り捨ての強制）をクリックします。
4. ログの切り捨ての強制を続行するかどうかを確定します。

リカバリポイントステータスインジケータ

保護対象 SQL または Exchange Server でのリカバリポイント作成後、アプリケーションが対応するカラーステータスインジケータが **Recovery Points**（リカバリポイント）テーブルを表示します。表示される色は、次の表で説明されるとおり、保護対象マシンのチェック設定とそれらのチェックの成功または失敗に基づいています。

メモ: リカバリポイントの表示についての詳細は、「リカバリポイントの表示」を参照してください。

次の表に、SQL データベースについて表示されるステータスインジケータをリストします。

SQL データベースのリカバリステータスポイントカラー

ステータスカラー	説明
白色	以下の状況のいずれかが存在することを示します。 • SQL データベースが存在しなかった。 • アタッチ可否チェックが有効化されていなかった。 • アタッチ可否チェックがまだ実行されていない
黄色	SQL データベースがオフラインでチェックを実行できなかったことを示します。
赤色	アタッチ可否チェックが失敗したことを示します。
緑色	アタッチ可否チェックに合格したことを示します。

次の表に、Exchange データベースについて表示されるステータスインジケータをリストします。

Exchange データベースのリカバリステータスポイントカラー

用語見出し	説明見出し
白色	以下の状況のいずれかが存在することを示します。 • Exchange データベースが存在しなかった。 • マウント可否チェックが有効化されていなかった

用語見出し	説明見出し
	メモ: これはリカバリポイント内の特定のボリュームに該当します。
黄色	Exchange データベースのマウント可否チェックは有効になっていますが、チェックがまだ実行されていないことを示します。
赤色	少なくとも 1 つのデータベースで、マウント可否チェックまたは Checksum チェックが失敗したことを示します。
緑色	マウント可否チェックまたは Checksum チェックに合格したことを示します。

メモ: Exchange または SQL データベースが関連付けられていないリカバリポイントは、白色のステータスインジケータで表示されます。リカバリポイントに Exchange と SQL の両方のデータベースが存在する場合は、リカバリポイントについて最も重要なステータスインジケータが表示されます。

3

アプライアンスの管理

Core Console には **Appliance**（アプライアンス）タブがあります。このタブを使用して、容量のプロビジョニング、アプライアンスの状態の監視、および管理ツールへのアクセスを行うことができます。

アプライアンスのステータスの監視

アプライアンス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）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、ステータスライト（各サブシステムの横にある）とサブシステムの正常性を示す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に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利用できます。**System Administrator**（システム管理者）リンク（Appliance Hardware サブシステムと Storage Hardware サブシステムで使用可能）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を要求されます。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/home** 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。**Provisioning Status**（プロビジョニングステータス）リンク（Storage Provisioning サブシステムで使用可能）では、該当するサブシステムのプロビジョニングステータスを表示する **Tasks**（タスク）画面が開きます。ストレージがプロビジョニング可能な場合、プロビジョニングタスクの横にある **Actions**（アクション）において **Provision**（プロビジョニング）へのリンクが表示されます。

ストレージのプロビジョニング

アプライアンスは、使用可能な DL4300 内部ストレージ、および接続されている外部ストレージエンクロージャのすべてを次のために設定します。

- AppAssure リポジトリ

  メモ: Fibre Channel の HBA が設定されている場合は、リポジトリの作成プロセスは手動で行われます。AppAssure がリポジトリをルートディレクトリに自動的に作成することはありません。詳細については、『*Dell DL4300 Appliance Deployment Guide*』（Dell DL4000 Appliance 導入ガイド）を参照してください。
- 保護されたマシンの仮想スタンバイ

メモ: H830 コントローラに接続された、1 TB, 2 TB, 4 TB、6 TB（大容量用）ドライブ付き MD1400s がサポートされています。MD 400s は最大 4 台までサポートされています。

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

ディスク上でストレージのプロビジョニングを開始する前に、スタンバイ仮想マシンに必要なストレージの容量を決定します。スタンバイ仮想マシンをホストするために、使用可能な容量から任意の割合の容量を割

り当てることができます。たとえば、Storage Resource Management（SRM）を使用している場合、仮想マシンをホストするために、プロビジョニングされている任意のデバイス上で最大 100 パーセントの容量を割り当てることができます。アプライアンスで保護されているサーバーに障害が発生した場合、AppAssure のライブリカバリ機能を使用して、それらのサーバーを仮想マシンに素早く置き換えることができます。

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

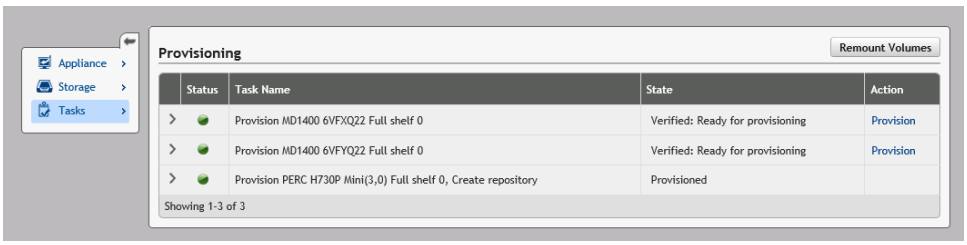
Appliance（アプライアンスサーバー）タブを選択すると、AppAssure Appliance ソフトウェアは、システム内のサポートされているすべてのコントローラに対して使用可能なストレージ容量の場所を特定し、ハードウェアが要件を満たしていることを検証します。

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

1. **Appliance**（アプライアンスサーバー）タブで、**Tasks（タスク）→ Provisioning（プロビジョニング）**をクリックします。

   Provisioning（プロビジョニング）画面にはプロビジョニングの推定容量が表示されます。この容量は、新しい AppAssure リポジトリの作成に使用されます。

   注意: 作業を進める前に、本手順の手順 2 ～ 手順 4 が実施されていることを確認します。
2. プロビジョンを行うストレージの横にあるアクションコラム内の **Provision**（プロビジョン）をクリックして **Provisioning Storage**（ストレージのプロビジョン）ウィンドウを開きます。
3. **Optional Storage Reserve**（オプションのストレージ予備）のセクションで、**Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes**（プロビジョンされているストレージの一部をスタンバイ仮想マシンまたはその他の目的に割り当てる）の横にあるボックスを選択して割り当てるストレージをパーセントで示します。この作業を行なわない場合は、**Optional Storage Reserve**（オプションの予備ストレージ）に示されるストレージのパーセントはアタッチされているすべてのディスクから取得されます。
4. **Provision**（プロビジョニング）をクリックします。



選択したストレージのプロビジョニング

選択したストレージをプロビジョニングするには、次の手順を実行します。

1. **Appliance**（アプライアンス）タブで、**Tasks（タスク）→ Provisioning（プロビジョニング）**をクリックします。

   Provisioning（プロビジョニング）画面に、プロビジョニング用の推定容量が表示されます。この容量は、新しい AppAssure リポジトリの作成に使用されます。
2. 使用可能な容量の一部のみをプロビジョニングするには、プロビジョニングするストレージ容量の横にある **Action**（アクション）で **Provision**（プロビジョニング）をクリックします。

- 新しいリポジトリを作成するには、**Create a new repository**（新規のリポジトリの作成）を選択し、リポジトリの名前を入力します。

  リポジトリ名として Repository 1 がデフォルトで表示されます。この名前は上書きすることができます。
- 既存のリポジトリに容量を追加するには、**Expand the existing repository**（既存のリポジトリの拡張）を選択し、**Existing Repositories**（既存のリポジトリ）リストからリポジトリを選択します。

メモ: 容量を追加するときは、リポジトリを追加するのではなく、既存のリポジトリを拡張することを推奨します。別々に作成されたリポジトリは、それらの間で重複排除が行われないため、容量の利用効率が悪くなります。

3. **Optional Storage Reserve**（オプションのストレージリザーブ）で、**Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes**（スタンバイ仮想マシンまたは他の目的のためにプロビジョニングされるストレージの一部を割り当てる）を選択し、VM 用に割り当てるストレージの割合を指定します。
4. **Provision**（プロビジョニング）をクリックします。

   ディスクプロビジョニングが開始され、**Tasks**（タスク）画面の **Status**（ステータス）領域に AppAssure リポジトリ作成のステータスが表示されます。**State**（状態）には **Provisioned**（プロビジョニング済み）と示されます。
5. ディスクプロビジョニングの完了後、詳細情報を表示するには、ステータスライトの横にある **>** をクリックします。

   Tasks（タスク）ページが拡張され、ステータス、リポジトリ、および仮想ディスク（割り当てられている場合）の詳細が表示されます。

仮想ディスク用の容量割り当ての削除

この手順を開始する前に、削除する仮想ディスクを確認します。Core Console から、**Appliance**（アプライアンス）タブを選択し、**Tasks**（タスク）をクリックし、仮想ディスクが含まれているリポジトリを展開して、仮想ディスクの詳細情報を確認します。
仮想ディスクの容量割り当てを削除するには、次の手順を実行します。

1. OpenManage Server Administrator アプリケーションから、**Storage**（ストレージ）を展開します。
2. 仮想ディスクを収容しているコントローラを展開し、**Virtual Disks**（仮想ディスク）を選択します。
3. 削除する仮想ディスクを選択し、**Tasks**（タスク）ドロップダウンメニューから **Delete**（削除）を選択します。
4. 削除を承認した後、Core Console の **Appliance**（アプライアンス）タブの **Tasks**（タスク）画面に、削除した容量がプロビジョニング可能な容量として表示されます。

失敗したタスクの解決

AppAssure は、検証タスク、プロビジョニングタスク、およびリカバリタスクの失敗を Core Console ホームページ上でイベントとして報告します。これらは、**Appliance**（アプライアンス）タブの **Tasks**（タスク）画面にも表示されます。

失敗したタスクの解決方法を確認するには、**Appliance**（アプライアンス）タブを選択し、**Tasks**（タスク）をクリックします。失敗したタスクを **Status**（ステータス）の横にある **>** をクリックして展開し、エラーメッセージおよび推奨される対処方法を確認します。

アプライアンスのアップグレード

アプライアンスをアップグレードするには、次の手順を実行します。

1. **Recovery and Update Utility** を **dell.com/support** から DL4300 Backup to Disk アプライアンスにダウンロードします。
2. そのユーティリティをアプライアンスのデスクトップにコピーし、ファイルを解凍します。
3. **launchRUU** アイコンをダブルクリックします。
4. プロンプトが表示されたら、リストされているいずれのプロセスも実行していないことを確認して **Yes**（はい）をクリックします。
5. **Recovery and Update Utility** 画面が表示されたら、**Start**（開始）をクリックします。
6. 再起動のプロンプトが表示されたら、**OK** をクリックします。

   Windows Server の役割と機能、ASP .NET MVC3、LSI Provider、DL Applications、OpenManage Server Administrator、および AppAssure Core Software のアップデートされたバージョンが Recovery and Update Utility の一部としてインストールされます。Recovery and Update Utility は、これらに加えて RASR コンテンツもアップデートします。

   メモ: Recovery and Upgrade Utility は、AppAssure Core Software アップグレードプロセスの一環として、現在インストールされている AppAssure バージョンを通知し、Core Software をユーティリティにバンドルされているバージョンにアップグレードすることを確認するプロンプトを表示します。AppAssure Core Software のダウングレードはサポートされていません。
7. プロンプトが表示されたら、システムを再起動します。
8. すべてのサービスとアプリケーションのインストールが完了したら、**Proceed**（続行）をクリックします。

   Core Console が起動します。

アプライアンスの修復

アプライアンスを修復するには、次の手順を実行します。

1. **Recovery and Update Utility**（リカバリおよびアップデートユーティリティ）を **dell.com/support** からアプライアンスにダウンロードします。
2. そのユーティリティをアプライアンスのデスクトップにコピーし、ファイルを解凍します。
3. **launchRUU** アイコンをダブルクリックします。
4. プロンプトが表示されたら、リストされているいずれのプロセスも実行していないことを確認して **Yes**（はい）をクリックします。
5. Recovery and Update Utility 画面が表示されたら、**Start**（開始）をクリックします。
6. 再起動のプロンプトが表示されたら、**OK** をクリックします。

   Windows Server の役割と機能、ASP .NET MVC3、LSI Provider、DL Applications、OpenManage Server Administrator、および AppAssure Core Software の最新バージョンが Recovery and Update Utility の一部としてインストールされます。
7. ユーティリティにバンドルされているバージョンがインストール済みのバージョンと同じ場合、Recovery and Update Utility は、修復インストールを実行することを確認するプロンプトを表示します。AppAssure Core の修復インストールが不要な場合は、この手順を省略できます。
8. ユーティリティにバンドルされているバージョンがインストール済みのバージョンよりも上の場合、Recovery and Update Utility は、AppAssure Core Software をアップグレードすることを確認するプロンプトを表示します。

メモ: AppAssure Core Software のダウングレードはサポートされていません。

9. プロンプトが表示されたら、システムを再起動します。
10. すべてのサービスとアプリケーションのインストールが完了したら、**Proceed**（続行）をクリックします。

    修復後にシステムを再設定する必要がある場合は、AppAssure アプライアンス設定ウィザードが起動されます。それ以外の場合は、Core Console が起動されます。

4

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

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: 本項では基本的に、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。

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. 保護対象マシンの追加後、次のいずれかを実行します。
   - Core Console から **Machines**（マシン）タブをクリックし、変更するマシンのハイパーリンクをクリックします。
   - **Navigation**（ナビゲーション）ペインから変更するマシンを選択します。
2. **設定** タブをクリックします。
   Settings（設定）ページが表示されます。
3. **Edit**（編集）をクリックして、次の表の説明に従って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。

テキストボックス	説明
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このポートを使用します。
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。
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。

マシンのシステム情報の表示

Core Console には、マシンのリストを含めることにより保護されるすべてのマシンと各マシンのステータスが表示されます。
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 **Protected Machines**（保護対象マシン）で、詳細なシステム情報を表示するマシンを選択します。
2. そのマシンの **Tools**（ツール）タブをクリックします。
   マシンの情報が **System Information**（システム情報）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
   - 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
   - ファイルシステム
   - 容量（未処理、フォーマット済み、使用済みを含む）
   - プロセッサ
   - プロセッサのタイプ
   - 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

システムイベントの通知グループの設定

AppAssure では、通知グループを作成することによって、マシンに対してシステムイベント（システムアラートやエラーなど）を報告する方法を設定できます。

システムイベントの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 **Machines**（マシン）タブをクリックします。
2. **Machines**（マシン）タブから、次のいずれかを実行します。
   - 変更するマシンのハイパーリンクをクリックします。
   - Navigation（ナビゲーション）ペインで、変更するマシンを選択します。

   Summary（サマリ）タブが表示されます。
3. **Configuration**（設定）タブをクリックし、**Events**（イベント）をクリックします。
   Notification Groups（通知グループ）ページが表示されます。
4. **Use custom alert settings**（カスタムアラート設定を使用）をクリックし、**Apply**（適用）をクリックします。
   Custom Notification Groups（カスタム通知グループ）画面が表示されます。
5. **Add Group**（グループの追加）をクリックして、システムイベントのリストを送信する新規の通知グループを追加します。
   Add Notification Group（通知グループの追加）ダイアログボックスが表示されます。

   メモ: デフォルトのアラート設定を使用するには、**Use Core alert settings**（コアアラート設定の使用）オプションを選択します。
6. 次の表の説明どおりに通知オプションを追加します。

テキストボックス	説明
Name（名前）	通知グループの名前を入力します。
Description（説明）	通知グループの説明を入力します。
Enable Events（イベントの有効化）	この通知グループと共有するイベントを選択します。**All**（すべて）を選択することも、次のようなイベントのサブセットを選択することもできます。 • **BootCd（起動 CD）** • **LocalMount（ローカルマウント）** • **Metadata（メタデータ）** • **Clusters（クラスタ）** • **Notification（通知）** • **PowerShellScripting（PowerShell スクリプティング）** • **PushInstall（プッシュインストール）** • **Attachability（アタッチ可否）** • **Jobs（ジョブ）** • **Licensing（ライセンス）** • **LogTruncation（ログの切り捨て）** • **Archive（アーカイブ）** • **CoreService（コアサービス）** • **Export（エクスポート）** • **Protection（保護）** • **Replicatoin（複製）** • **Rollback（ロールバック）**

テキストボックス	説明
	• **Rollup（ロールアップ）** 次のタイプ別に選択することもできます。 • **Info（情報）** • **Warning（警告）** • **Error（エラー）** **メモ:** タイプで選択する場合、該当するイベントがデフォルトで自動的に有効になります。たとえば警告を選択すると、アタッチ可否、ジョブ、ライセンス、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、およびロールバックイベントが有効になります。
Notification Options（通知オプション）	通知の処理方法を選択して指定します。次のオプションから選択できます。 • **Notify by Email**（E-メールで通知）- To（宛先）、CC、および BCC テキストボックスに、イベントを送信する E-メールアドレスを指定します。 **メモ:** E-メールを受信するには、事前に SMTP が設定されている必要があります。 • **Notify by Windows Event log**（Windows イベントログで通知）— Windows イベントログが通知を制御します。 • **Notify by syslogd**（syslogd で通知）— イベントを送信するホスト名およびポートを指定します。 – **Host**（ホスト）— サーバーのホスト名を入力します。 – **Port**（ポート）— サーバーとの通信に使用するポート番号を入力します。

7. **OK** をクリックして変更を保存します。
8. 既存の通知グループを編集するには、編集する通知グループの隣にある **Edit**（編集）をクリックします。
   設定を編集できる **Edit Notification Group**（通知グループの編集）ダイアログボックスが開きます。

システムイベントの通知グループの編集

システムイベントの通知グループを編集するには、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. **Machines**（マシン）タブから、次のいずれかを実行します。
   - 変更するマシンのハイパーリンクをクリックします。
   - または、ナビゲーションペインで、削除するマシンを選択します。

   Summary（サマリ）タブが表示されます。
3. **Configuration**（設定）タブをクリックし、**Events**（イベント）をクリックします。
4. **Use custom alert settings**（カスタムアラート設定を使用）をクリックし、**Apply**（適用）をクリックします。
   Custom Notification Groups（カスタム通知グループ）画面が表示されます。
5. **Action**（アクション）列の下にある **Edit**（編集）アイコンをクリックします。
   Edit Notification Group（通知グループを編集）ダイアログボックスが表示されます。
6. 次の表の説明に従って、通知オプションを編集します。

テキストボックス	説明
Name（名前）	通知グループの名前を表示します。 **メモ:** 通知グループの名前を編集することはできません。
Description（説明）	通知グループの説明を入力します。
Enable Events（イベントの有効化）	通知グループと共有するイベントを選択します。**All**（すべて）を選択することも、次を含むイベントのサブセットを選択することもできます。 • **BootCd（起動 CD）** • **LocalMount（ローカルマウント）** • **Metadata（メタデータ）** • **Clusters（クラスタ）** • **Notification（通知）** • **PowerShellScripting（PowerShell スクリプティング）** • **PushInstall（プッシュインストール）** • **Attachability（アタッチ可否）** • **Jobs（ジョブ）** • **Licensing（ライセンス）** • **LogTruncation（ログの切り捨て）** • **Archive（アーカイブ）** • **CoreService（コアサービス）** • **Export（エクスポート）** • **Protection（保護）** • **Replicatoin（複製）** • **Rollback（ロールバック）** • **Rollup（ロールアップ）** 次のタイプ別に選択することもできます。 • **Info（情報）** • **Warning（警告）** • **Error（エラー）** **メモ:** タイプで選択する場合、該当するイベントがデフォルトで自動的に有効になります。たとえば警告を選択すると、アタッチ可否、ジョブ、ライセンス、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、およびロールバックイベントが有効になります。
Notification Options（通知オプション）	通知の処理方法を選択して指定します。次のオプションから選択できます。 • **Notify by Email**（E-メールで通知）— To（宛先）、CC、および BCC テキストボックスに、イベントを送信する E-メールアドレスを指定します。 **メモ:** E-メールを受信するには、事前に SMTP が設定されている必要があります。

テキストボックス	説明
	• **Notify by Windows Event log**（Windows イベントログで通知）— Windows イベントログが通知を制御します。 • **Notify by syslogd**（syslogd で通知）— イベントを送信するホスト名およびポートを指定する必要があります。 – **Host**（ホスト）— サーバーのホスト名を入力します。 – **Port**（ポート）— サーバーとの通信に使用するポート番号を入力します。

7. **OK** をクリックします。

保持ポリシー設定のカスタマイズ

マシンの保持ポリシーは、エージェントマシンのリカバリポイントがリポジトリ内に保存される期間を指定します。保持ポリシーを使用することで、バックアップスナップショットの保持期間を長くしたり、これらのバックアップスナップショットの管理に役立てたりすることができます。保持ポリシーはロールアッププロセスによって実施され、古いバックアップのエージングと削除に役立ちます。このタスクは「クラスタノード設定の変更プロセス」の手順でもあります。

保持ポリシー設定をカスタマイズするには、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. **Machines**（マシン）タブから、次のいずれかを実行します。
   - 変更するマシンのハイパーリンクをクリックします。
   - Navigation（ナビゲーション）ペインで、変更するマシンを選択します。

   Summary（サマリ）タブが表示されます。
3. **Configuration**（設定）タブをクリックし、**Retention Policy**（保持ポリシー）をクリックします。

   メモ: Core 用に設定されたデフォルトの保持ポリシーを使用する場合は、Use Core default retention policy（コアのデフォルト保持ポリシーを使用する）オプションを選択するようにしてください。

   Retention Policy（保持ポリシー）画面が表示されます。
4. カスタマイズされたポリシーを設定するには、**Use custom retention policy**（カスタム保持ポリシーを使用する）をクリックします。

   Custom Retention Policy（カスタム保持ポリシー）画面が表示されます。
5. **Enable Rollup**（ロールアップの有効化）を選択し、必要に応じてバックアップデータを保持する時間間隔を指定します。保持ポリシーオプションの説明は次のとおりです。

テキストボックス	説明
Keep all recovery points for n [retention time period]（すべてのリカバリポイントを n [保持期間] 保持）	リカバリポイントの保持期間を指定します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは **3** です。 次から選択できます。 • **Days（日）** • **Weeks（週）** • **Months（月）**

テキストボックス	説明
	• **Years（年）**
...and then keep one Recovery Point per hour for n [retention time period]（...さらに、1 時間につき 1 つのリカバリポイントを n [保持期間] 保持）	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとしてプライマリ設定と共に使用され、リカバリポイントを維持する期間をさらに詳細に定義します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは 2 です。 次から選択できます。 • **Days（日）** • **Weeks（週）** • **Months（月）** • **Years（年）**
...and then keep one Recovery Point per day for n [retention time period]（...さらに、1 日につき 1 つのリカバリポイントを n [保持期間] 保持）	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは 4 です。 次から選択できます。 • **Days（日）** • **Weeks（週）** • **Months（月）** • **Years（年）**
...and then keep one Recovery Point per week for n [retention time period]（...さらに、1 週につき 1 つのリカバリポイントを n [保持期間] 保持）	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは 3 です。 次から選択できます。 • **Weeks（週）** • **Months（月）** • **Years（年）**
...and then keep one Recovery Point per month for n [retention time period]（...さらに、1 月につき 1 つのリカバリポイントを n [保持期間] 保持）	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは 2 です。 次から選択できます。 • **Months（月）** • **Years（年）**
...and then keep one Recovery	保持期間を示す数字を入力し、期間を選択します。

テキストボックス　説明

Point per year for n [retention time period]（...さらに、1 年につき 1 つのリカバリポイントを n [保持期間] 保持）

Newest Recovery Point（最新のリカバリポイント）テキストボックスには、最新のリカバリポイントが表示されます。最も古いリカバリポイントは、保持ポリシーの設定によって決まります。

次に、保持期間の計算方法の例を示します。
すべてのリカバリポイントを 3 日間保持。

...さらに、1 時間ごとに 1 つのリカバリポイントを 3 日間保持

...さらに、1 日ごとに 1 つのリカバリポイントを 4 日間保持

...さらに、1 週ごとに 1 つのリカバリポイントを 3 週間保持

...さらに、1 月ごとに 1 つのリカバリポイントを 2 ヶ月間保持

...さらに、1 月ごとに 1 つのリカバリポイントを 1 年間保持

Newest Recovery Point（最新のリカバリポイント）は、現在の年月日に設定されます。

この例では、最も古いリカバリポイントは、1 年 4 か月 6 日前のものになります。

6. **Apply**（適用）をクリックして変更を保存します。
7. マシンの現在の保持ポリシーに基づいてロールアップを実行するには、**Force Rollup**（ロールアップの強制）を選択します。あるいは、定義した保持ポリシーが毎晩行われるロールアップ中に適用されるようにします。

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. Core Console で **Machines**（マシン）タブをクリックします。
2. **Machines**（マシン）タブから、次のいずれかを実行します。
   - 表示するマシンのハイパーリンクをクリックします。
   - 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。
3. **Configuration**（設定）タブをクリックし、**Licensing**（ライセンス）をクリックします。
   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。

保護スケジュールの変更

AppAssure では、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 **Machines**（マシン）タブをクリックします。
2. **Machines**（マシン）タブから、次のいずれかを実行します。
   - 変更するマシンのハイパーリンクをクリックします。
   - Navigation（ナビゲーション）ペインで、変更するマシンを選択します。
3. 次の手順のいずれか 1 つを実行します。
   - マシンの **Summary**（サマリ）タブにある **Volumes**（ボリューム）表で、カスタマイズするボリュームに対する保護スケジュールのハイパーリンクをクリックします。
   - **Configuration**（設定）タブをクリックし、**Protection Settings**（保護設定）をクリックします。ボリュームのリスト内で、カスタマイズするボリュームの横にある **Edit**（編集）アイコンをクリックします。

   Protection Schedule（保護スケジュール）ダイアログボックスが表示されます。
4. **Protection Schedule**（保護スケジュール）ダイアログボックスで、データを保護するためのスケジュールオプションを必要に応じて編集します。次の表に各オプションについて説明します。

オプション	説明
Interval（間隔）	**Weekday**（平日）— 特定の時間間隔（15 分毎など）でデータを保護するには、**Interval**（間隔）を選択して次の操作を行います。 • ピーク時間にデータを保護する時間をカスタマイズするには、**Start Time**（開始時刻）、**End Time**（終了時刻）、および **Interval**（間隔）をドロップダウンメニューから選択できます。 • オフピーク時間にデータを保護するには、**Protection interval during off-peak times**（オフピーク時間中の保護間隔）チェックボックスを選択し、ドロップダウンメニューから保護間隔を選択します。 **Weekends**（週末）— 週末にデータを保護するには、**Protection interval during weekends**（週末の保護の間隔）チェックボックスを選択して、ドロップダウンメニューから間隔を選択します。 **メモ:** SQL または Exchange のデータベースとログが異なるボリューム上にある場合、それらのボリュームは 1 つの保護グループに属している必要があります。
毎日	データを毎日保護するには、**Daily**（毎日）オプションを選択し、**Protection Time**（保護時刻）ドロップダウンメニューでデータの保護を開始する時刻を選択します。
No Protection（保護なし）	このボリュームから保護を削除するには、**No Protection**（保護なし）オプションを選択します。

   このマシンのすべてのボリュームに対してこれらのカスタム設定を適用する場合は、**Apply to All Volumes**（すべてのボリュームに適用）を選択します。
5. 必要な変更が完了したら、**OK** をクリックします。

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、お使いの環境に劇的な変化をもたらす可能性があります。転送設定の値を変更する前に、Dell AppAssure Knowledge Base（https://support.software.dell.com/appassure/kb）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。

転送には次の三種類があります。

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 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。
ロールバック	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。

データ転送には、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、次のいずれかを実行します。
   - **Machines**（マシン）タブをクリックし、変更するマシンのハイパーリンクをクリックします。
   - Navigation（ナビゲーション）ペインで、変更するマシンをクリックします。
2. **Machines**（マシン）タブから、次のいずれかを実行します。
   - 変更するマシンのハイパーリンクをクリックします。
   - Navigation（ナビゲーション）ペインで、変更するマシンを選択します。
3. **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。
   現在の転送設定が表示されます。
4. **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。
5. 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。
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）

テキストボックス	説明
	• 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。
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。

6. **OK** をクリックします。

サービスの再開

サービスを再開するには、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. **Machines**（マシン）タブから、次のいずれかを実行します。
   - 再開するマシンのハイパーリンクをクリックします。
   - **Navigation**（ナビゲーション）ペインで、再開するマシンを選択します。
3. **Tools**（ツール）タブをクリックし、**Diagnostics**（診断）をクリックします。
4. **Restart Service**（サービスの再開）オプションを選択し、**Restart Service**（サービスの再開）ボタンをクリックします。

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場合は、ログを表示してトラブルシューティングしてください。

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 **Machines**（マシン）タブをクリックします。
2. **Machines**（マシン）タブから、次のいずれかを実行します。
   - 表示するログが保存されているマシンのハイパーリンクをクリックします。
   - **Navigation**（ナビゲーション）ペインで、表示するログが保存されているマシンを選択します。
3. **Tools**（ツール）タブをクリックし、**Diagnostics**（診断）をクリックします。
4. **View Log**（ログの表示）リンクをクリックします。

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 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 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 Agent ソフトウェアをインストールする手順については、「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」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. Agent ソフトウェアのインストール後にマシンを再起動していない場合は、そのマシンを再起動します。
2. コアマシン上の Core Console から、次のいずれかを実行します。
   - **Protected machines**（保護対象マシン）の **Home**（ホーム）タブで、**Protect Machine**（マシンの保護）をクリックします。
   - **Machines**（マシン）タブを選択し、**Actions**（アクション）ドロップダウンメニューで **Protect Machine**（マシンの保護）をクリックします。

   Connect（接続）ダイアログボックスが表示されます。
3. **Connect**（接続）ダイアログボックスで、接続先のマシンに関する情報を次の表の説明に従って入力します。

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。
Port（ポート）	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。
Username（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）。
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。

4. **Connect**（接続）をクリックして、このマシンに接続します。

メモ: Agent ソフトウェアが指定したマシン上にまだインストールされていない場合は、「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」の手順に従ってください。Agent ソフトウェアのインストール後 Agent のマシンを再起動して次の手順に進んでください。

5. **Protect**（保護）ダイアログボックスで、次の表の説明どおりに、必要に応じて設定を編集します。

フィールド	説明
Display Name（表示名）	**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。 **メモ:** 表示名は、既存のマシンの **Configuration**（設定）タブにアクセスすることにより、後から変更することもできます。
Repository（リポジトリ）	このマシンのデータを保存する 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）タブで定義されます。
Initially pause protection（保護を当初一時停止）	マシンが保護のために追加されると、AppAssure はデータのベーススナップショットの取得を自動的に開始します。このチェックボックスをオンにすると、保護を当初一時停止できます。その場合、データの保護を開始する準備ができたら、手動でスナップショットを強制実行する必要があります。手動によるスナップショットの強制実行の詳細については、「スナップショットの強制実行」を参照してください。
Volume Groups（ボリュームグループ）	Volume Groups（ボリュームグループ）では、どのボリュームを保護するかを定義し、保護スケジュールを作成できます。 マシン上のすべてのボリュームに対して 60 分ごとのデフォルトの保護スケジュールを設定するには、**Apply Default**（デフォルトを適用）をクリックします。 マシン上の任意のボリュームを選択し、個別に保護パラメータを定義することもできます。 初期設定では、60 分ごとのデフォルトの保護スケジュールが適用されます。ボリュームのスケジュールを変更するには、該当するボリュームに対して **Edit**（編集）をクリックします。それにより、スナップショットを取得する間隔を詳細に定義したり（週末の独立したスケジュールの定義も含む）、スナップショットを開始する毎日の時刻を指定したりすることができます。 選択したボリュームの保護スケジュールの編集については、「ボリュームのためのカスタムスケジュールの作成」を参照してください。

6. **Protect**（保護）をクリックします。
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）の Core 上へのリポジトリの転送がただちに開始されます。

注意: Linux マシンを保護した場合は、保護対象ボリュームを手動でマウント解除しないようにする必要があります。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、コマンド bsctl -d [path_to_volume] を実行する必要があります。このコマンド内の [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ます。これは、たとえば /dev/sda1 のような形式にする必要があります。

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. **Protect Machine**（マシンの保護）→ **Connect**（接続）ダイアログボックスで適切な接続設定を入力した後、**Connect**（接続）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表示されます。
2. **Yes**（はい）をクリックして、エージェントソフトウェアをリモートでマシンに展開します。
   Deploy Agent（エージェントの展開）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。
   - **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。
   - **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。
   - **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。
   - **Protect machine after install**（インストール後にマシンを保護する）- このオプションを選択すると、マシンを保護対象に追加した後、AppAssure がデータのベーススナップショットを取得できます。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した場合は、データ保護の開始準備が整ってから手動でスナップショットを強制実行する必要があります。手動でスナップショットを強制実行する方法の詳細に関しては、『*Dell DL4300 Appliance User's Guide*』（Dell DL4000 アプライアンスユーザーズガイド）の「Forcing A Snapshot」（スナップショットの強制）を参照してください。
   - **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。

ボリュームのためのカスタムスケジュールの作成

ボリュームのためのカスタムスケジュールを作成するには、次の手順を実行します。

1. **Protect Machine**（マシンの保護）ダイアログボックス（このダイアログボックスへのアクセス方法については、「マシンの保護」を参照）の **Volume Group**（ボリュームグループ）で、保護するボリュームを選択して **Edit**（編集）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表示されます。

2. **Protection Schedule**（保護スケジュール）ダイアログボックスで、次に説明されている、データを保護するためのスケジュールオプションの中から 1 つを選択します。

テキストボックス	説明
Interval（間隔）	次から選択できます。 • **Weekday**（平日）— 特定の間隔でデータを保護するには、**Interval**（間隔）を選択して、次の操作を行います。 – ピークタイムにデータを保護する時間をカスタマイズするには、**Start Time**（開始時刻）、**End Time**（終了時刻）、および **Interval**（間隔）をドロップダウンメニューから指定できます。 – オフピークタイムにデータを保護するには、**Protection interval during off-peak times**（オフピーク時間中の保護間隔）チェックボックスをオンにして、**Time**（時刻）ドロップダウンメニューから保護間隔を選択します。 • **Weekends**（週末）— 週末にデータを保護するには、**Protection interval during weekends**（週末の保護間隔）チェックボックスをオンにして、ドロップダウンメニューから **Interval**（間隔）を選択します。
Daily（毎日）	データを毎日保護するには、**Daily Protection**（毎日保護）オプションを選択し、**Time**（時刻）ドロップダウンメニューでデータの保護を開始する時刻を選択します。
No Protection（保護なし）	このボリュームから保護を削除するには、**No Protection**（保護なし）オプションを選択します。

   このマシンのすべてのボリュームに対してこれらのカスタム設定を適用する場合は、**Apply to All Volumes**（すべてのボリュームに適用）を選択します。

3. 必要な変更が完了したら、**OK** をクリックします。
4. カスタマイズするボリュームごとに手順 2 と手順 3 を繰り返します。
5. **Protect Machine**（マシンの保護）ダイアログボックスで、**Protect**（保護）をクリックします。

Exchange Server 設定の変更

Microsoft Exchange サーバーからのデータを保護している場合は、Core Console で追加の設定を行う必要があります。

Exchange Server 設定を変更するには、次の手順を実行します。

1. 保護対象の Exchange Server マシンを追加した後、Core Console の **Navigation**（ナビゲーション）ペインでマシンを選択します。

そのマシンの **Summary**（サマリ）タブが表示されます。

2. **Summary**（サマリ）タブから、**Exchange Server Settings**（Exchange Server 設定）リンクをクリックします。

   Exchange Server Settings（Exchange Server 設定）ダイアログボックスが表示されます。

3. **Exchange Server Settings**（Exchange Server 設定）ダイアログボックスでは、次の設定の選択や選択解除を行うことができます。
   - Enable automatic mountability check（自動マウント可否チェックを有効にする）
   - Enable nightly checksum check（夜間 Checksum チェックを有効にする）。次のオプションを選択することで、この設定をさらにカスタマイズできます。
     - Automatically truncate Exchange logs after successful checksum check（Checksum チェックの成功後エクスチェンジログを自動的に切り捨てる）
     - Truncate log before checksum check completes（チェックサムチェックが完了する前にログを切り捨てる）
4. Exchange Server のログオン資格情報を変更することもできます。これには、**Exchange Server Information**（Exchange Server 情報）セクションにスクロールして、**Change Credentials**（資格情報の変更）をクリックします。

   Set Exchange Credentials（Exchange 資格情報の設定）ダイアログボックスが表示されます。

5. 新しい資格情報を入力し、**OK** をクリックします。

SQL Server 設定の変更

Microsoft SQL Server からのデータを保護している場合は、Core Console で設定する必要のある追加設定があります。

SQL Server 設定を変更するには、次の手順を実行します。

1. 保護対象の SQL Server マシンを追加した後、Core Console の **Navigation**（ナビゲーション）ペインでマシンを選択します。

   そのマシンの **Summary**（サマリ）タブが表示されます。

2. Summary（サマリ）タブから、**SQL Server settings**（SQL Server 設定）リンクをクリックします。

   SQL Server Settings（SQL Server 設定）ダイアログボックスが表示されます。

3. **SQL Server Settings**（SQL Server 設定）ダイアログボックスで、必要に応じて次の設定を編集します。
   - Enable nightly attachability check（夜間アタッチ可否チェックを有効にする）
   - Truncate log after successful attachability check（simple recovery model only）（正常なアタッチ可否チェック後、ログを切り捨てる（シンプルリカバリモデルのみ））
4. SQL Server のログオン資格情報を変更することもできます。変更するには、**SQL Server Information**（SQL Server 情報）テーブルまで下にスクロールし、**Change Credentials**（資格情報の変更）をクリックします。

   Set SQL Server Credentials（SQL サーバー資格情報の設定）ダイアログボックスが表示されます。

5. 新しい資格情報を入力し、**OK** をクリックします。

エージェントの展開（プッシュインストール）

AppAssure では、エージェントのインストールに microsoft.net が必要です。手動またはプッシュインストールプロセスでエージェントをインストールする前に、microsoft.net を各クライアントマシン上にインストールしておく必要があります。

AppAssure では、保護用のために個々の 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、次の処置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、「複数のマシンへの展開」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 で **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、**Deploy Agent**（エージェントの展開）をクリックします。
   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。
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。

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。

マシンの管理

本項では、AppAssure 環境からのマシンの削除、レプリケーションのセットアップ、ログの切り捨ての強制、操作のキャンセルなど、マシンの管理において実行できるさまざまなタスクについて説明します。

マシンの削除

1. Core Console に移動し、**Machines**（マシン）タブをクリックします。
2. **Machines**（マシン）タブから、次のいずれかを実行します。
   - 削除するマシンのハイパーリンクをクリックします。
   - または、Navigation（ナビゲーション）ペインで、削除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、**Remove Machines**（マシンの削除）をクリックし、次の表で説明されているオプションのいずれかを選択します。

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。

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。

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だけをキャンセルすることも、現在のすべての操作（エクスポートやレプリケーションなどを含む）をキャンセルすることもできます。

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 **Machines**（マシン）タブをクリックします。
2. 操作をキャンセル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、**Cancel**（キャンセル）をクリックし、次に説明されているいずれかのオプションを選択します。

テキストボックス	説明
All Operations（すべての操作）	選択したマシンに対してすべてのアクティブな操作をキャンセルします。
Snapshot（スナップショット）	現在実行中のスナップショットをキャンセルします。

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 の Navigation（ナビゲーション）ペインで、次のいずれかを実行します。
   - **Machines**（マシン）タブを選択し、表示するマシンのハイパーリンクをクリックします。

- Navigation（ナビゲーション）ペインで、表示するマシンをクリックします。

Summary（サマリ）タブが表示されます。
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。

- 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。

- 名前
- インストールパス
- Version（バージョン）
- バージョン番号
- データベース名
- オンラインステータス

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。

- 名前
- 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 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ので、展開するマシンはインターネットにアクセスしてビットデータをダウンロードし、インストールできなければなりません。インターネットにアクセスできない場合は、AppAssure Agent インストールプログラムを Core マシンからプッシュできます。Core マシンから Agent インストールをプッシュする方法については、「コアマシンからの Agent インストールプログラムのプッシュ」を参照してください。コア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。

コアマシンからのエージェントインストールプログラムのプッシュ

導入対象のサーバーがインターネットにアクセスできない場合は、実際のエージェントインストールファイルを Core マシンからプッシュできます。お使いのアプライアンスには、エージェントインストールプログラムファイルが含まれています。

メモ: ライセンスポータルから Core とエージェントのアップグレードをダウンロードします。

エージェントインストールプログラムを Core マシンからプッシュするには、次の手順を実行します。

1. Core マシンで、エージェントインストールファイル **Agent-X64-5.x.x.xxxxx.exe** を **C:\Program Files \apprecovery\core\installers** ディレクトリにコピーします。
2. Core Console から、**Configuration**（設定）タブを選択し、**Settings**（設定）をクリックします。
3. **Deploy Settings**（導入設定）セクションで、**Agent Installer Name**（エージェントインストーラ名）を編集します。

Active Directory ドメイン上のマシンへの展開

この手順を開始する前に、Active Directory サーバーのドメイン情報とログオン資格情報を用意しておく必要があります。

エージェントを Active Directory ドメインの複数のマシンに展開するには、次の手順を実行します。

1. Core Console で、**Tools**（ツール）タブ、次に **Bulk Deploy**（一括展開）とクリックします。
2. **Deploy Agent to Machines**（マシンへのエージェントの展開）ウィンドウで、**Active Directory** をクリックします。
3. **Connect to Active Directory**（Active Directory への接続）ダイアログボックスで、次の表の説明に従ってドメイン情報とログオン資格情報を入力します。

テキストボックス	説明
Domain（ドメイン）	Active Directory ドメインのホスト名または IP アドレス。
User name(ユーザー名)	このドメインへの接続に使用するユーザー名（Administrator など）。
Password(パスワード)	このドメインへの接続に使用するセキュアなパスワード。

4. **Connect**（接続）をクリックします。
5. **Add Machines from Active Directory**（Active Directory からマシンを追加）ダイアログボックスで、AppAssure Agent を展開するマシンを選択し、**Add**（追加）をクリックします。

   追加したマシンが **Deploy Agent on Machines**（マシンへのエージェントの展開）ウィンドウに表示されます。
6. マシンのパスワードを入力するには、マシンに対してリポジトリの選択、暗号化キーの追加、あるいはその他の設定の編集を行った後、そのマシンの **Edit**（編集）リンクをクリックし、次の手順を実行します。
   a. **Edit Settings**（設定の編集）ダイアログボックスで、次の表の説明に従って設定を指定します。

テキストボックス	説明
Host name(ホスト名)	手順 3 から自動的に入力されます。
Display name（表示名）	手順 3 で入力したホスト名に基づいて自動的に割り当てられます。
Port(ポート)	Core がマシン上のエージェントと通信するときに使用するポート番号。
User name(ユーザー名)	手順 3 から自動的に入力されます。
Password(パスワード)	マシン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）	展開後に自動的にマシンを再起動するかどうかを指定します。 **メモ: Protect Machine After Install**（インストール後にマシンを保護する）ボックスにチェックを入れて展開後に自動的にマシンを保護する場合、このオプションは必須です。
Protect Machine After Install（イン	展開後にマシンを自動的に保護するかどうかを指定します。この設定によって、**Protecting Multiple Machines**（複数マシンの保護）を省略できます。

テキストボックス	説明
ストール後にマシンを保護する）	
Repository（リポジトリ）	ドロップダウンリストを使用して、マシンからのデータを保存する Core 上のリポジトリを選択します。選択したリポジトリは、保護されるすべてのマシンに対して使用されます。 **メモ:** このオプションは、**Protect machine after install**（インストール後にマシンを保護する）を選択した場合にのみ使用できます。
Encryption Key（暗号化キー）	（オプション）ドロップダウンリストを使用して、リポジトリに保存されるマシン上のデータに暗号化を適用するかどうかを指定します。この暗号化キーは、保護されるすべてのマシンに割り当てられます。 **メモ:** このオプションは、**Protect machine after install**（インストール後にマシンを保護する）を選択した場合にのみ使用できます。

b. **Save**（保存）をクリックします。

7. AppAssure が各マシンに正常に接続できることを確認するには、**Deploy Agent on Machines**（マシンへのエージェントの展開）ウィンドウの各マシンを選択し、**Verify**（確認）をクリックします。
8. **Deploy Agent on Machines**（マシンへのエージェントの展開）ウィンドウで、各マシンの横に展開準備の状態を反映した次のアイコンが表示されます。

テキストボックス	説明
緑色のアイコン	AppAssure はマシンに接続可能で、展開の準備が整っています。
黄色のアイコン	AppAssure はマシンに接続可能ですが、エージェントはすでにコアマシンとペアになっています。
赤色のアイコン	AppAssure はマシンに接続できません。原因としては、ログオン資格情報が間違っている、マシンがシャットダウンされている、ファイアウォールがトラフィックをブロックしている、などが考えられます。修正するには、ツールバーの **Edit Settings**（設定の編集）か、マシンの横にある **Edit**（編集）リンクをクリックします。

9. マシンの確認が正常に行われた後は、AppAssure Agent を展開する各マシンを選択し、**Deploy**（展開）をクリックします。
10. **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、展開に成功した後、マシンは自動的に再起動し、保護が有効になります。

VMware vCenter または ESXi 仮想ホスト上のマシンへの展開

この手順を開始する前に、VMware vCenter/ESXi 仮想ホストの場所情報およびログオン資格情報を用意しておく必要があります。

メモ: すべての仮想マシンに、VM Tools がインストールされている必要があります。インストールされていないと、AppAssure は展開先の仮想マシンのホスト名を検出できません。AppAssure ではホスト名の代わりに仮想マシン名を使用するので、ホスト名が仮想マシン名と異なると問題が発生します。

vCenter/ESXi 仮想ホスト上の複数のマシンに展開するには、次の手順を実行します。

1. Core Console で、**Tools**（ツール）タブ、次に **Bulk Deploy**（一括展開）とクリックします。
2. **Deploy Agent on Machines**（マシンへのエージェントの展開）ウィンドウで、**vCenter/ESXi** をクリックします。
3. **Connect to VMware vCenter Server/ESXi**（VMware vCenter Server/ESXi への接続）ダイアログボックスで、次のようにホスト情報とログオン資格情報を入力し、**OK** をクリックします。

テキストボックス	説明
Host（ホスト）	VMware vCenter Server/ESX（i）仮想ホストの名前または IP アドレスを入力します。
User Name（ユーザー名）	仮想ホストへの接続に使用するユーザー名（administrator など）を入力します。
Password(パスワード)	この仮想ホストへの接続に使用するセキュアなパスワードを入力します。

4. **Add Machines from VMware vCenter Server/ESXi**（VMware vCenter Server/ESXi からのマシンの追加）ダイアログボックスで、AppAssure Agent を展開するマシンの横にあるボックスにチェックを入れ、**Add**（追加）をクリックします。
5. **Deploy Agent on Machines**（マシンへのエージェントの展開）ウィンドウで、追加したマシンを確認できます。リポジトリ、暗号化キー、またはマシンに関するその他の設定を選択する場合は、マシンの横のチェックボックスを選択して **Edit Settings**（設定を編集）をクリックします。

   各設定の詳細については、「Active Directory ドメイン上のマシンへの展開」を参照してください。
6. AppAssure が各マシンに正常に接続できることを確認します。**Deploy Agent on Machines**（マシンへのエージェントの展開）ウィンドウの各マシンを選択し、**Verify**（確認）をクリックします。
7. **Deploy Agent on Machines**（マシンへのエージェントの展開）ウィンドウで、各マシンの横に展開準備の状態を反映した次のアイコンが表示されます。

テキストボックス	説明
緑色のアイコン	AppAssure はマシンに接続可能で、展開の準備が整っています。
黄色のアイコン	AppAssure はマシンに接続可能ですが、エージェントはすでにコアマシンとペアになっています。
赤色のアイコン	AppAssure はマシンに接続できません。原因としては、ログオン資格情報が間違っている、マシンがシャットダウンされている、ファイアウォールがトラフィックをブロックしている、などが考えられます。修正するには、ツールバーの **Edit Settings**（設定の編集）か、マシンの横にある **Edit**（編集）リンクをクリックします。

8. マシンの検証が正常に行われた後は、各マシンを選択し、**Deploy**（展開）をクリックします。
9. **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、展開に成功した後でマシンは自動的に再起動し、保護が有効になります。

その他のホスト上のマシンへの展開

その他のホスト上の複数マシンに展開するには、次の手順を実行します。

1. Core Console で、**Tools**（ツール）タブ、次に **Bulk Deploy**（一括展開）とクリックします。
2. **Deploy Agent on Machines**（マシンへのエージェントの展開）ウィンドウで、次のいずれかを実行します。

- **Add Machine**（マシンの追加）ダイアログボックスで複数マシンを指定するには、**New**（新規）をクリックします。これによって、新規のマシンホスト、ログオン資格情報、リポジトリ、暗号化キー、およびその他の情報を入力することができます。各設定の詳細については、「Active Directory ドメイン上のマシンへの展開」を参照してください。

  これらの情報を入力した後、**OK** をクリックして **Deploy Agent on Machines**（マシンへのエージェントの展開）リストに追加するか、**OK と New（新規）**をクリックして別のマシンを追加します。

  メモ: 展開後、自動的にマシンを保護する場合は、**Protect Machine after Install**（インストール後にマシンを保護）チェックボックスを選択します。このチェックボックスを選択すると、保護が有効になる前にマシンが自動的に再起動します。

- **Manually**（手動）をクリックして、リスト内の複数マシンを指定します。各行はそれぞれ展開先のマシンを示します。**Add Machines Manually**（マシンを手動で追加）ダイアログボックスで、次に示すように、ダブルコロンで区切られたマシンの IP アドレスまたは名前、ユーザー名、パスワード、およびポートを入力します。

  ```
  hostname::username::password::port For example:
  10.255.255.255::administrator::&11@yYz90z::8006 abc-
  host-00-1::administrator::99!zU$o83r::168
  ```

3. **Deploy Agent on Machines**（マシンへのエージェントの展開）ウィンドウで、追加したマシンを確認できます。リポジトリ、暗号化キー、またはマシンに関するその他の設定を選択する場合は、マシンの横のボックスにチェックを入れて **Edit Settings**（設定を編集）をクリックします。

   各設定の詳細については、「Active Directory ドメイン上のマシンへの展開」を参照してください。

4. AppAssure が各マシンに正常に接続できることを確認します。**Deploy Agent on Machines**（マシンへのエージェントの展開）ウィンドウの各マシンを選択し、**Verify**（確認）をクリックします。

   Deploy Agent on Machines（マシンへのエージェントの展開）ウィンドウで、各マシンの横に展開準備の状態を反映した次のアイコンが表示されます。

テキストボックス	説明
緑色のアイコン	AppAssure はマシンに接続可能で、展開の準備が整っています。
黄色のアイコン	AppAssure はマシンに接続可能ですが、エージェントはすでにコアマシンとペアになっています。
赤色のアイコン	AppAssure はマシンに接続できません。原因としては、ログオン資格情報が間違っている、マシンがシャットダウンされている、ファイアウォールがトラフィックをブロックしている、などが考えられます。修正するには、ツールバーの **Edit Settings**（設定の編集）か、マシンの横にある **Edit**（編集）リンクをクリックします。

5. マシンの確認が正常に行われた後は、各マシンの横のボックスにチェックを入れて **Deploy**（展開）をクリックします。
6. **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、展開に成功した後でマシンは自動的に再起動し、保護が有効になります。

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 から、**Events**（イベント）タブをクリックしてリスト内で展開ジョブを探してから、**Details**（詳細）列内のボタンをクリックします。

   Monitor Active Task（アクティブタスクの監視）ウィンドウに、導入の詳細が表示されます。

これには、全体の進捗状況情報の他、個々の展開のステータスも含まれています。次の詳細情報が表示されます。

- 開始時刻
- 終了時刻
- 経過時間
- 残り時間
- Progress（進行状況）
- フェーズ

2. 次の手順のいずれか 1 つを実行します。
   - **Open in New window**（新規ウィンドで開く）をクリックして新規ウィンドウを開き、展開の進捗状況を表示します。
   - **Close**（閉じる）をクリックし、導入タスクをバックグラウンドで処理します。

複数マシンの保護

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それらの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、**Tools**（ツール）タブ、次に **Bulk Protect**（一括保護）とクリックします。
   Protect Machines（マシンを保護）ウィンドウが表示されます。
2. 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。
   各オプションの実行の詳細については、「複数マシンへの展開」を参照してください。
   - **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。
   - **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。
   - **New**（新規）をクリックして、Add Machine（マシンの追加）ダイアログボックスで複数のマシンを指定します。
   - **Manually**（手動）をクリックして、ホスト名と資格情報を入力することによってリスト内の複数のマシンを指定します。
3. **Protect Machines**（マシンを保護）ウィンドウで、追加したマシンを確認できます。リポジトリ、暗号化キー、またはマシンに関するその他の詳細設定を選択する場合は、マシンの横のチェックボックスを選択にして **Edit Settings**（設定を編集）をクリックします。
4. 次のように設定を指定して、**OK** をクリックします。

テキストボックス	説明
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のセキュアなパスワードを入力します。
Port（ポート）	Core がマシン上のエージェントと通信するときに使用するポート番号を指定します。

テキストボックス	説明
Repository（リポジトリ）	マシンからのデータが保存されている Core 上のリポジトリを選択します。選択したリポジトリは、保護されているすべてのマシンに使用されます。
Encryption Key（暗号化キー）	リポジトリに保存されているマシン上のエージェントに、暗号化を適用するかどうかを指定します。暗号化キーは、保護されているすべてのマシンに割り当てられます。
Protection Schedule（保護スケジュール）	マシンの保護を行うスケジュールを指定します。デフォルトスケジュールは、ピーク動作時の 60 分と週末の 60 分です。 企業のニーズに合わせてスケジュールを編集するには、**Edit**（編集）をクリックします。 **メモ:** 詳細については、「保護スケジュールの変更」を参照してください。
Initially pause protection（保護を当初一時停止）	オプションで、最初に実行するときに保護を一時停止にすることができます。つまり、手動で保護を再開するまで、コアはマシンのスナップショットを取得しません。

5. AppAssure が各マシンに正常に接続できることを確認します。これには、**Protect Machines**（マシンを保護）ウィンドウで各マシンの横にあるチェックボックスを選択して、**Verify**（確認）をクリックします。
6. **Protect Machines**（マシンの保護）ウィンドウで、各マシンの横に展開準備の状態を反映した次のアイコンが表示されます。

Icon	説明
緑色のアイコン	AppAssure はマシンに接続可能で、保護の準備が整っています。
黄色のアイコン	AppAssure はマシンに接続可能ですが、エージェントはすでにコアマシンとペアになっています。
赤色のアイコン	AppAssure はマシンに接続できません。原因としては、ログオン資格情報が誤っている、マシンがシャットダウンされている、ファイアウォールがトラフィックをブロックしている、などが考えられます。修正するには、ツールバーの **Edit Settings**（設定の編集）か、マシンの横にある **Edit**（編集）リンクをクリックします。

7. マシンの確認が正常に行われた後は、各マシンの横にあるチェックボックスを選択して **Protect**（保護）をクリックします。

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、次の手順を実行します。

1. **Machines**（マシン）タブをクリックして、保護のステータスと進捗状況を表示します。
   Protected Machines（保護マシン）ページが表示されます。
2. **Events**（イベント）タブをクリックして、関連タスク、イベント、およびアラートを表示します。
   Tasks（タスク）ページが表示されます。

テキストボックス	説明
To view task information（タスク情報を表示する）	ボリュームが送信に従い、**Tasks**（タスク）ペインにステータス、開始時刻、および終了時刻が表示されます。**Details**（詳細）をクリックすると、タスクに関するより具体的な情報が表示されます。
To view alert information（アラート情報を表示する）	保護対象マシンが追加されるたびに、操作が成功したか、またはエラーが記録されたかどうかを示すアラートがログに記録されます。アラートのレベルが、トランザクション日付とメッセージとともに表示されます。ページからすべてのアラートを削除するには、**Dismiss All**（すべて無視）をクリックします。
To view event information（イベント情報を表示する）	**Events**（イベント）ペインに、マシンと送信されるデータの詳細が表示されます。イベントのレベル、トランザクション日付、および時刻メッセージが表示されます。

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 の左のナビゲーション領域で、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 Workstation または HyperV にエクスポートすることができます。選択したリカバリポイントのエクスポートの詳細については、 「仮想マシンへの Windows マシンのバックアップ情報のエクスポート」を参照してください。 **Rollback**（ロールバック）— 選択したリカバリポイントから指定ボリュームへの復元を実行するには、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からの復元の実行の詳細については、「AppAssure Core からの復元の開始」を参照してください。

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 で、次のいずれかを実行します。
   - **Machines**（マシン）タブを選択します。

     a. マウントするリカバリポイントを持つマシンまたはクラスタの横で、**Actions**（アクション）ドロップダウンメニューから **Mount**（マウント）を選択します。
     b. **Mount Recovery Point**（リカバリポイントのマウント）ダイアログボックス内のリストからリカバリポイントを選択し、**Next**（次へ）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。
   - 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。

     a. **Recovery Points**（リカバリポイント）タブを選択します。
     b. リカバリポイントのリストで、マウントするリカバリポイントを展開します。
     c. 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。
2. 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。

3. **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

Core 上にローカルマウントされている選択したリカバリポイントをマウント解除できます。

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 から、**Tools**（ツール）タブを選択します。
2. **Tools**（ツール）オプションから **System Info**（システム情報）をクリックします。
3. マウント解除するリカバリポイントのマウント済み表示を選択し、**Dismount**（マウント解除）をクリックします。

すべてのリカバリポイントのマウント解除

Core 上にローカルマウントされているすべてのリカバリポイントをマウント解除できます。
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 から、**Tools**（ツール）タブを選択します。
2. **Tools**（ツール）オプションから **System Info**（システム情報）をクリックします。
3. **Local Mounts**（ローカルマウント）セクションで、**Dismount All**（すべてをマウント解除）をクリックします。

Linux マシンへのリカバリポイントボリュームのマウント

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、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. 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。
   この 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。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. 次のコマンドを入力して、指定した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します。
   ```
   lr <line_number_of_machine>
   ```
   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. 次のコマンドを入力して、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。
   ```
   m <volume_recovery_point_ID_number> <path>
   ```

メモ: このコマンドでは、リカバリポイント ID 番号の代わりにライン番号を指定して、リカバリポイントを特定することもできます。その場合は、エージェント / マシンのライン番号（lm 出力からのもの）、リカバリポイントのライン番号とボリューム文字、およびパスを順に並べて（ `m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>`）使用します。たとえば、`lm` の出力で 3 台のエージェントマシンがリスト表示され、番号 2 のマシンに対して `lr` コマンドを入力し、23 行目のリカバリポイントのボリューム b を **/tmp/mount_dir** にマウントするコマンドは、`m 2 23 b /tmp/mount_dir` になります。

注意: 保護されている Linux ボリュームは手動でマウント解除しないでください。マウント解除する必要がある場合は、その前にコマンド `bsctl -d <path to volume>` を実行する必要があります。このコマンドの `<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ます。これは、たとえば /dev/sda1 のような形式にする必要があります。

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の上に継続して作成されます。ベースイメージが存在しないと、作成されたリカバリポイントは不完全であり、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。この状況が発生した場合、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。

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。

   孤立リカバリポイントチェーンが削除されます。

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 **Machines**（マシン）タブをクリックし、保護対象マシンのリストから、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. 選択したマシンの **Actions**（アクション）ドロップダウンメニューをクリックし、**Force Snapshot**（スナップショットの強制）をクリックして、以下に説明されているいずれかのオプションを選択します。
   - **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。

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。

保護を一時停止して再開するには、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. 保護を一時停止するマシンを選択します。
   このマシンの **Summary**（サマリ）タブが表示されます。

3. そのマシンの **Actions**（アクション）ドロップダウンメニューで、**Pause**（一時停止）をクリックします。
4. 保護を再開するには、**Actions**（アクション）メニューで **Resume**（再開）をクリックします。

データの復元

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）の間にレプリケーションがセットアップされる場合、最初のレプリケーションが完了した後、ターゲットコアからデータをエクスポートすることのみが可能になります。詳細については、「マシンでのエージェントデータのレプリケーション」を参照してください。

メモ: FAT32 EFI パーティションから起動された Window 8、Windows Server 2012 オペレーティングシステム、または Resilient File System（ReFS）ボリュームは保護または回復に利用することはできません。

バックアップ

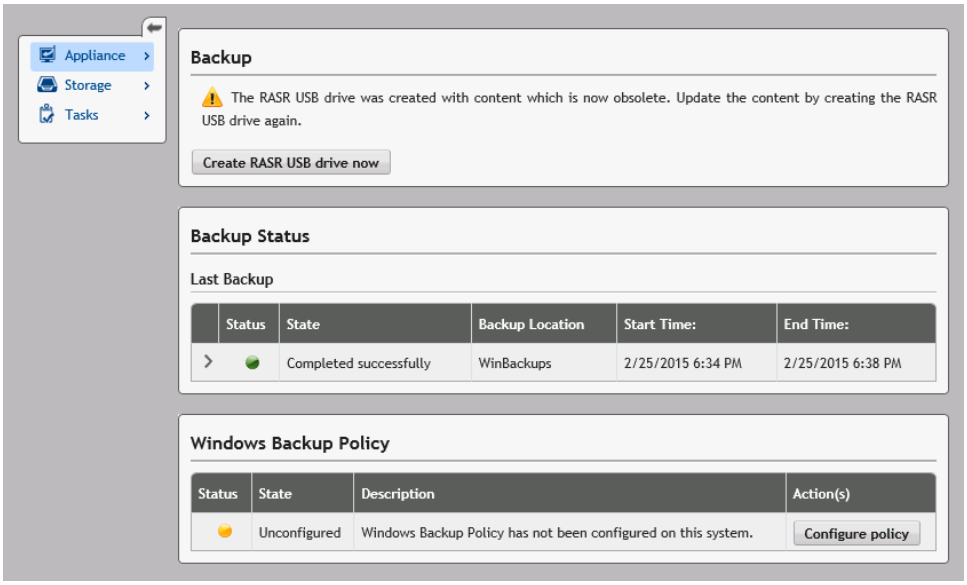
バックアップタブでは、バックアップポリシーを設定し、RASR USB キーまたは IDSDM を使用してシステムを回復できます。この機能を使用するには、Windows Backup 仮想ディスクが必要です。Windows Backup 仮想ディスクは、**AppAssure アプライアンス設定ウィザード**の実行中に作成されます。詳細については、『Dell DL43000 Appliance Deployment Guide』（Dell DL43000 アプライアンス導入ガイド）の「Rapid Appliance Self Recovery」（高速アプライアンスセルフリカバリ）を参照してください。Windows Backup 仮想ディスクがないと、ポリシーを設定したり、Windows バックアップを作成したりすることができません。

バックアップステータス

Microsoft Windows バックアップステータスは、**Last Backup**（最後のバックアップ）タブ下に表示されます。バックアップが現在実行されている場合、その情報は、**Current Backup**（現在のバックアップ）タブ下に表示されます。最後のバックアップを表示するには、次の手順を実行します。

1. Core Console で、**Appliance（アプライアンス）→ Backup（バックアップ）**タブに移動します。
2. **Status**（ステータス）ボタンの横の矢印をクリックして、バックアップのステータスを表示します。
3. **Last Backup**（最後のバックアップ）ペインに、次の情報が表示されます。
   - Status（ステータス）
   - State（状態）
   - Backup Location（バックアップの場所）
   - Start Time（開始時刻）
   - End Time（終了時刻）
   - Error Description（エラーの内容）
   - Items that were backed up（バックアップされたアイテム）

   メモ: 上記の情報は、Windows のバックアップポリシーが実行されたかどうかに関係なく表示されます。



バックアップが実行されている場合は、**Current Backup Progress**（現在のバックアップ進捗状況）と **Start Time**（開始時間）に関する情報が表示されます。

Windows バックアップポリシー

Windows バックアップポリシーを設定するには、次の手順を実行します。

1. Core Console で、**Appliance → Backup（アプライアンス > バックアップ）**に移動します。
2. **Configure Policy**（ポリシーの設定）ボタンをクリックします。
   Windows Backup Policy（Windows バックアップポリシー）ウィンドウが表示されます。
3. 以下に示すようにパラメータを入力します。

テキストボックス	説明
以下のアイテムがバックアップされます。	• OS（C:） • リカバリ • ベアメタルリカバリ • システム状態 上記のすべてのアイテムがデフォルトで選択されます。
バックアップをスケジュールする時間を選択してください。	バックアップをスケジュールする時間を入力します。

4. **Configure**（設定）をクリックします。
   設定後に、**Windows Backup Policy**（Windows バックアップポリシー）ウィンドウで、**Backup now**（今すぐバックアップ）、**Delete policy**（ポリシーの削除）、または **View policy**（ポリシーの表示）のオプションを使用できます。

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。

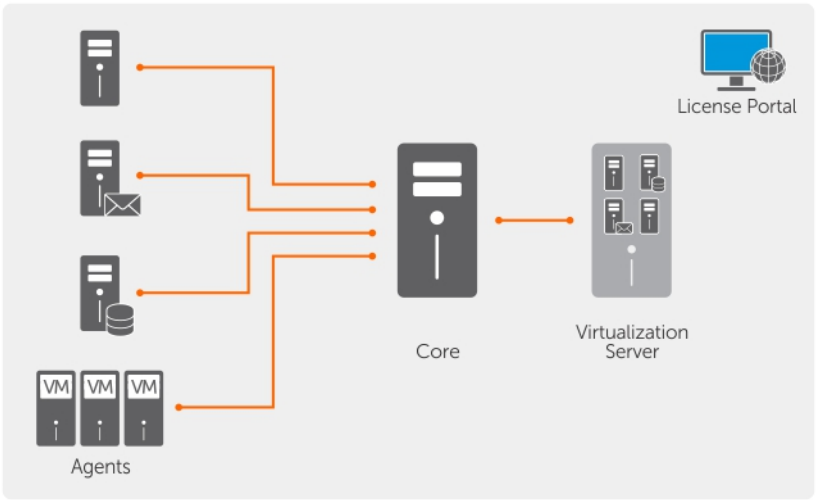


図 9. 仮想マシンへのデータのエクスポート

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

AppAssure はすべての動的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、その名前が示すように、ストライピング、ミラーリング、スパニングのいずれも行われていないボリュームです。非シンプル動的ボリュームは完全には認識できない任意のディスクジオメトリを持つため、エクスポートできません。AppAssure では、複雑なボリュームまたは非シンプル動的ボリュームをエクスポートできます。

AppAssure バージョン 5.3.1.60393 では、エクスポートがシンプルダイナミックボリュームのみに制限されることを知らせるチェックボックスがユーザーインタフェースに追加されました。このバージョンでユーザーインタフェースが変更される前は、複雑なディスクまたは非シンプルダイナミックディスクをエクスポートするオプションが選択肢として表示されていました。これらのディスクをエクスポートしようとしても、そのエクスポートジョブは失敗しました。

Microsoft 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

AppAssure では、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、Microsoft Windows マシンのデータを仮想マシン（VMware、ESXi、Hyper-V、および Oracle VirtualBox）にエクスポートすることができます。

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 **Machines**（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。
   - ESXi Export（ESXi エクスポート）
   - VMware Workstation Export（VMware Workstation エクスポート）
   - Hyper-V Export（Hyper-V エクスポート）
   - Oracle VirtualBox Export（Oracle VirtualBox エクスポート）

   Select Export Type（エクスポートタイプの選択）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. **Select Export Type**（エクスポートタイプの選択）ダイアログボックスで、**One-time export**（1 回限りのエクスポート）をクリックします。
2. **次へ** をクリックします。

   ESXi Export - Select Recovery Point（ESXi エクスポート - リカバリポイントを選択）ダイアログボックスが表示されます。
3. 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。

   Virtual Standby Recovery Point to VMware vCenter Server/ESXi（VMware vCenter Server/ESXi への仮想スタンバイリカバリポイント）ダイアログボックスが表示されます。

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. **Virtual Standby Recovery Point to VMware vCenter Server/ESXi**（VMware vCenter Server/ESXi への仮想スタンバイリカバリポイント）ダイアログボックスで、次の説明に従って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
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。

2. **接続** をクリックします。

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. **Select Export Type**（エクスポートタイプの選択）ダイアログボックスで、**Continuous (Virtual Standby)**（連続（仮想スタンバイ））を選択します。
2. **次へ** をクリックします。

   Virtual Standby Recovery Point to VMware vCenter Server/ESXi（VMware vCenter Server/ESXi への仮想スタンバイリカバリポイント）ダイアログボックスが表示されます。
3. 以下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
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。

4. 接続 をクリックします。
5. **Options**（オプション）タブで、説明どおりに仮想マシンの情報を入力します。

テキストボックス	説明
Virtual Machine Name（仮想マシン名）	作成される仮想マシンの名前（たとえば、VM-0A1B2C3D4）を入力します。 **メモ:** エージェント名から派生する名前またはエージェント名に一致する名前を使用することをお勧めします。また、ハイパーバイザータイプ、IP アドレス、または DNS 名から派生した名前を作成することもできます。
メモリ	メモリの使用量を指定します。次のオプションのいずれかを選択できます。 • Use the same amount of RAM as source machine（ソースマシンと同容量の RAM を使用） • **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）。

テキストボックス	説明
ESXi Datacenter（ESXi データセンター）	ESXi データセンターの名前を入力します。
ESXi Host（ESXi ホスト）	ESXi ホストの資格情報を入力します。
Data Store（データストア）	データストアの詳細を入力します。
Version（バージョン）	仮想マシンのバージョンを選択します。 **メモ:** vSphere クライアントを使用して仮想マシンを管理するには、バージョン 8 以前を選択します。
Resource Pool（リソースプール）	リソースプールの名前を入力します。

6. **Start Export**（エクスポートの開始）をクリックします。

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. **Select Export Type**（エクスポートタイプの選択）ダイアログボックスで、**One-time export**（1 回限りのエクスポート）をクリックします。
2. **次へ** をクリックします。
   VM Export - Select Recovery Point（VM エクスポート - リカバリポイントを選択）ダイアログボックスが表示されます。
3. 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。
   Virtual Standby Recovery Point to VMware Workstation/Server（VMware Workstation/Server への仮想スタンバイリカバリポイント）ダイアログボックスが表示されます。

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. **Virtual Standby Recovery Point to VMware Workstation/Server**（VMware Workstation/Server への仮想スタンバイリカバリポイント）ダイアログボックスで、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
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。

2. **Export Volumes**（ボリュームのエクスポート）ペインで、エクスポートするボリューム（例：**C:** および **D:**）を選択します。
3. Options（オプション）ペインで、以下の説明どおりに仮想マシンの情報とメモリ使用量を入力します。

テキストボックス	説明
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:** エージェント名から派生する名前またはエージェント名に一致する名前を使用することをお勧めします。また、ハイパーバイザータイプ、IP アドレス、または DNS 名から派生した名前を作成することもできます。
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。 • **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）。

4. **Export**（エクスポート）をクリックします。

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. **Select Export Type**（エクスポートタイプの選択）ダイアログボックスで、**Continuous（Virtual Standby）**（連続（仮想スタンバイ））をクリックし、**Next**（次へ）をクリックします。

VM Export - Select Recovery Point（VM エクスポート - リカバリポイントを選択）ダイアログボックスが表示されます。

2. 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。

   Virtual Standby Recovery Point to VMware Workstation/Server（VMware Workstation/Server への仮想スタンバイリカバリポイント）ダイアログボックスが表示されます。

3. 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
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。

4. **Export Volumes**（ボリュームのエクスポート）ペインで、エクスポートするボリューム（例：**C:** および **D:**）を選択します。
5. **Options**（オプション）ペインで、次の表の説明に従って仮想マシンの情報とメモリ使用率を入力します。

テキストボックス	説明
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:** エージェント名から派生する名前またはエージェント名に一致する名前を使用することをお勧めします。また、ハイパーバイザータイプ、IP アドレス、または DNS 名から派生した名前を作成することもできます。
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。 • **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）。

6. **Perform initial ad-hoc export**（初期アドホックエクスポートを実行）をクリックして、データのエクスポートをテストします。

7. **保存** をクリックします。

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

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。
お使いの DL Appliance は、次のホストへの第 1 世代 Hyper-V のエクスポートをサポートします。

- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

お使いの DL Appliance は、次のホストへの第 2 世代 Hyper-V のエクスポートをサポートします。

- Windows 8.1
- Windows Server 2012 R2

メモ: すべての保護対象マシンが、第 2 世代 Hyper-V ホストにエクスポートできるわけではありません。

次の UEFI（Unified Extensible Firmware Interface）オペレーティングシステムを有する保護対象マシンのみが、第 2 世代 Hyper-V ホストへの仮想エクスポートをサポートしています。

- Windows 8（UEFI）
- Windows 8.1（UEFI）
- Windows Server 2012（UEFI）
- Windows Server 2012R2（UEFI）

メモ: Hyper-V ホスト上にエクスポートを実行するのに十分な RAM が割り当てられていない場合は、第 2 世代 VM への Hyper-V エクスポートは失敗します。

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。

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。
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 Microsoft 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を実行するか、連続エクスポート（仮想スタンバイ向け）を確立することにより、Oracle VirtualBox を使用したデータのエクスポートを選択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

このプロセスの手順を実行して、Oracle VirtualBox への 1 回限りのエクスポートを実行します。

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. AppAssure Core Console で、次のいずれかを実行します。
   - ボタンバーから **Export**（エクスポート）をクリックしてエクスポートウィザードを起動し、次の手順を実行します。
     1. **Select Export Type**（エクスポートタイプの選択）ページで、**One-time export**（1 回限りのエクスポート）を選択し、**Next**（次へ）をクリックします。
     2. **Protected Machines**（保護対象マシン）ページで、仮想マシンにエクスポートする保護対象マシンを選択し、**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、**Summary**（サマリ）タブのそのマシンの **Actions**（アクション）ドロップダウンメニューから、**Export**（エクスポート）> **One-time**（1 回限り）を選択します。

   エクスポートウィザードの **Recovery Points**（リカバリポイント）ページが表示されます。
2. **Recovery Points**（リカバリポイント）ページで、エクスポートする AppAssure コアのリカバリポイントを選択し、**Next**（次へ）をクリックします。
3. 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 **Use Windows machine**（Windows マシンの使用）を選択します。
5. 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。

オプション	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。
Memory（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 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。 • **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）。

6. 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、仮想マシンは Oracle VirtualBox で 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。
7. **Next**（次へ）をクリックします。
   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. 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:\）。
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

次の手順を実行して、仮想スタンバイを作成し、Oracle VirtualBox への連続的なエクスポートを実行します。

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. AppAssure 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）をクリックしてエクスポートウィザードを起動します。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、**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. 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）をクリックします。
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。

オプション	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:** エージェント名から派生する名前またはエージェント名に一致する名前を使用することをお勧めします。また、ハイパーバイザータイプ、IP アドレス、または DNS 名から派生した名前を作成することもできます。
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。
Memory（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）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、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）。

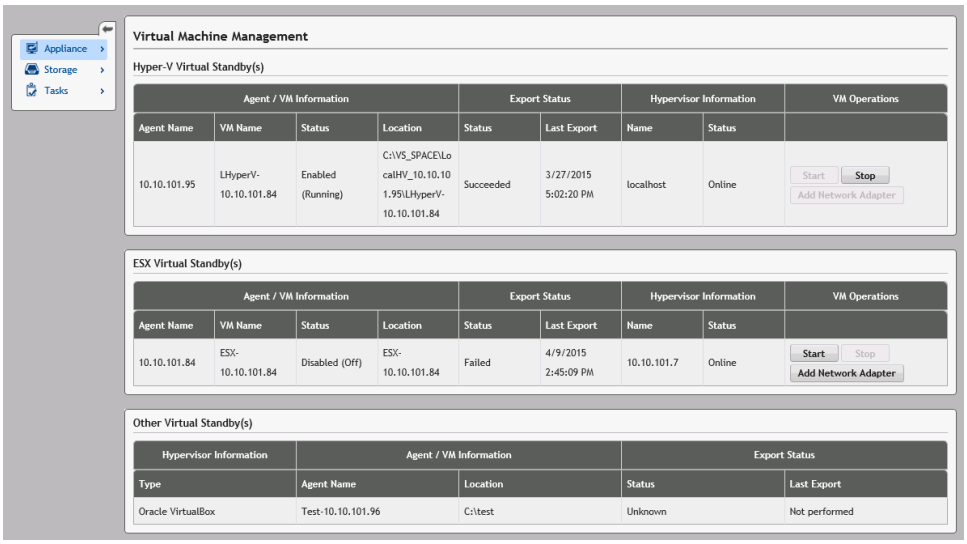
5. 仮想マシンのユーザーアカウントを指定するには、**Specify the user account for the exported virtual machine**（エクスポートされた仮想マシンのユーザーアカウントの指定）を選択し、次の情報を入力します。これは仮想マシン上に複数のユーザーアカウントがある場合に仮想マシンが登録される特定のユーザーアカウントを意味します。このユーザーアカウントがログオンすると、VirtualBox マネージャでは、このユーザーのみにこの仮想マシンが表示されます。アカウントが指定されない場合は、仮想マシンは VirtualBox のある Windows マ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 one-time export**（1 回限りのエクスポートの実行）を選択します。
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:\）。
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。

仮想マシンの管理

VM Management（VM 管理）タブには、保護対象マシンのステータスが表示されます。ネットワークアダプタを開始、停止、および追加することができます（Hyper-V および ESXi 仮想マシンのみに適用されます）。VM Management（VM 管理）タブに移動するには、**Appliance（アプライアンス）→ VM Management（VM 管理）**をクリックします。

メモ: **Appliance（アプライアンス）→ VM Management（VM 管理）**タブが選択されると、Start（開始）、Stop（停止）、および Add Network Adapter（ネットワークアダプタの追加）ボタンが表示されるまで最大 30 秒かかることがあります。



Hyper-V および ESXi 仮想スタンバイの VM 管理

フィールド	説明
Agent / VM Information（エージェント /VM 情報）	**Agent Name**（エージェント名）: 仮想スタンバイを作成した保護対象マシンの名前を示します。 **VM Name**（VM 名）: VM の名前を示します。 メモ: エージェント名から派生する名前またはエージェント名に一致する名前を使用することをお勧めします。また、ハイパーバイザータイプ、IP アドレス、または DNS 名から派生した名前を作成することもできます。 **Status**（ステータス）: 仮想マシンのステータスを示します。可能な値は次のとおりです • 実行中 • 停止 • Starting（起動中） • Suspended

フィールド	説明
	• Stopping（停止中） • Unknown（不明）（一時的なステータス） メモ: 上記のステータス値は、ハイパーバイザータイプによって異なります。すべてのハイパーバイザーで、すべてのステータス値が表示されるわけではありません。 **Location**（場所）: VM の場所を示します（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。
エクスポートステータス	**ステータス** 1. エクスポートプロセスの次のステータスを示します。 • 完了 • 失敗 • 進行中 • Not Performed（未実行） 2. エクスポートが現在進行中である場合は、エクスポートの割合が表示されます。 **Last Export**（最後のエクスポート）: 最後のエクスポートの時刻を示します。
Hypervisor Information（ハイパーバイザー情報）	**Name**（名前）: VM が作成されたハイパーバイザーの名前を示します。 **Status**（ステータス）: Hyper-V および ESXi ハイパーバイザーへの接続のステータスを示します。 • オンライン • オフライン • Unknown（不明）（一時的なステータス） メモ: ステータスは、Hyper-V および ESXi ハイパーバイザーに対してのみ表示されます。
VM 操作	仮想マシンを起動または停止し、ネットワークアダプタを追加できます。

他の仮想スタンバイに対する VM 管理

フィールド	説明
Hypervisor Information（ハイパーバイザー情報）	**Type**（タイプ）: ハイパーバイザーのタイプを示します。
Agent / VM Information（エージェント /VM 情報）	**Agent Name**（エージェント名）: 仮想スタンバイを作成した保護対象マシンの名前を示します。

フィールド	説明
	Location（場所）: VM の場所を示します（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。
エクスポートステータス	**ステータス** 1. エクスポートプロセスの次のステータスを示します。 • 完了 • 失敗 • 進行中 • Not Performed（未実行） 2. エクスポートが現在進行中である場合は、エクスポートの割合がプログレスバーに示されます。 **Last Export**（最後のエクスポート）: 最後のエクスポートの時刻を示します。

仮想ネットワークアダプタの作成

仮想マシンには、インターネットに接続する 1 つまたは複数の Virtual Network Adapter（VNA）が存在する必要があります。VM では、保護対象マシン上の各 Real Network Adapter（RNA）に対する VNA が必要です。VNA および一致する RNA の設定は類似する必要があります。仮想スタンバイを作成する場合、または後で VNA を追加する場合は、VNA を VM に追加できます。

仮想スタンバイを作成する場合は、仮想マシンを設定するときに、保護対象マシンの各アダプタに対して推奨されるアダプタが存在します。これらの推奨アダプタのすべてまたは一部を追加または削除できます。1 つの VM あたりの VNA 最大数は、ハイパーバイザーのタイプによって異なります。Hyper-V の場合は、各仮想マシンに対して最大 8 個のアダプタを追加することができます。

仮想ネットワークアダプタを作成するには、次の手順を実行します。

1. **VM Management**（VM 管理）ページに移動します。
2. VNA を追加する VM に関連する **Add Network Adapter**（ネットワークアダプタの追加）ボタンをクリックします。

   メモ: 保護対象マシンのバックアップまたはエクスポートがまだ実行されている仮想スタンバイ用の VM にはアダプタを追加しないでください。VNA の追加によって、今後のエクスポート操作が失敗することがあります。

   メモ: VNA は、保護対象マシンの代わりに VM を起動する直前に追加することをお勧めします。仮想スタンバイタブで、VM の保留中のすべてのエクスポートを停止または一時停止してください。

   Virtual Network Adapters and Switches（仮想ネットワークアダプタおよびスイッチ）ウィンドウが表示されます。
3. **Create**（作成）をクリックして、仮想ネットワークアダプタを作成します。

   Create Virtual Network Adapter（仮想ネットワークアダプタの作成）ウィンドウが表示されます。
4. ドロップダウンメニューから既存の仮想スイッチを選択します。

   メモ: ESXi 用の仮想スイッチを選択するときに、ドロップダウンには名前に「VM」または「Virtual Machine」が含まれるスイッチだけがリストされます。タイプが **Virtual Machine Port Group**（仮想マシンポートグループ）のスイッチだけを選択します。スイッチのタイプは、ESXi ハイパーバイザーの GUI で確認できます。

5. **Create**（作成）をクリックします。

   メモ: 仮想ネットワークアダプタを削除するには、ハイパーバイザー管理インタフェースを使用します。

VM 操作の開始

VM 操作を開始するには、次の手順を実行します。

1. **VM Management**（VM 管理）ウィンドウに移動します。
2. VM に関連付けられた **Start**（開始）ボタンをクリックして、開始します。

   メモ: GUI にマシンの正しいステータスが表示されるまで遅延が発生することがあります。Start（開始）ボタンは、使用してから最大 30 秒無効になることがあります。Start（開始）ボタンは、仮想マシンを起動できる場合にのみ有効になります。

   メモ: 仮想マシンへのエクスポートタスクが現在実行中である場合や、そのタスクがすぐに始まりそうな場合は、Start（開始）ボタンをクリックしないでください。**Protected Machines**（保護対象マシン）タブと **Virtual Standby**（仮想スタンバイ）タブを表示して、次のエクスポートタスクのスケジュールを確認します。エクスポートタスクが近い将来にスケジュールされている場合は、エクスポートタスクをキャンセルまたは省略するか、エクスポートタスクが完了するのを待ってから仮想マシンを起動します。データのエクスポートは、仮想マシンの稼働中に開始された場合は失敗します。ただし、エクスポートタスクの実行中に仮想マシンを起動することはできます。

   メモ: 仮想スタンバイとして維持されている VM は起動しないことをお勧めします。仮想スタンバイ VM は、障害が発生した保護対象マシンの代替としてアクティブ化または起動することを目的としています。保護対象マシンがまだアクティブである場合は、VM を起動する前に、最初に Virtual Standby（仮想スタンバイ）タブから VM の保留中のすべてのエクスポートを停止または一時停止します。

VM 操作の停止

VM 操作を停止するには、次の手順を実行します。

1. **VM Management**（VM 管理）ウィンドウに移動します。
2. VM に関連付けられた **Stop**（停止）ボタンをクリックして、停止します。

   メモ: Stop（停止）ボタンは、仮想マシンが現在実行中であり、VM の起動後約 30 秒以内に利用できる場合のみ有効になります。

   メモ: Start（開始）ボタンは、VM の停止後約 30 秒以内に有効になります。

   メモ: 保護対象 VM が復元されたら、ハイパーバイザーとその対応する仮想スタンバイから VM を削除します。次に、復元された保護対象マシンの仮想スタンバイを再作成します。これにより、仮想スタンバイ VM は、保護対象マシンを正確にミラーリングするようになります。

ロールバックの実行

AppAssure では、ロールバックとはマシン上のボリュームをリカバリポイントから復元するプロセスです。

メモ: ロールバック機能は、コマンドラインの `aamount` ユーティリティを使用することによって、保護対象の Linux マシンでもサポートされています。詳細については、「コマンドラインを使用した Linux マシンのロールバックの実行」を参照してください。

ロールバックを実行するには、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。

- **Machines**（マシン）タブをクリックし、次を行います。

a. 保護対象マシンのリストで、エクスポートするマシンの横にあるチェックボックスをオンにします。
b. そのマシンの **Actions**（アクション）ドロップダウンメニューで、**Rollback**（ロールバック）をクリックします。
c. **Rollback - Select Recovery Point**（ロールバック - リカバリポイントの選択）ダイアログボックスで、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。
   - AppAssure Core Console の左側にあるナビゲーションエリアで、ロールバックするマシンを選択すると、このマシンの **Summary**（サマリ）タブが開きます。
d. **Recovery Points**（リカバリポイント）タブをクリックし、リストからリカバリポイントを選択します。
e. 選択したリカバリポイントの詳細情報を展開し、**Rollback**（ロールバック）をクリックします。

2. 次の表の説明に従って、ロールバックオプションを編集します。

テキストボックス	説明
Protected Machine（保護対象マシン）	ロールバックの宛先としてオリジナルのエージェントマシンを指定します。ソースは、ロールバックに使用されるリカバリポイントを作成したエージェントを意味します。
Recovery Console Instance（Recovery Console インスタンス）	URC モードで起動したマシンに対してリカバリポイントを復元するために、ユーザー名とパスワードを入力します。

3. **Load Volumes**（ボリュームのロード）をクリックします。

   Volume Mapping（ボリュームマッピング）ダイアログボックスが表示されます。

   メモ: Core Console では Linux ボリュームの自動マッピングは行われません。Linux ボリュームの場所を指定するには、ロールバックするボリュームを参照します。

4. ロールバックするボリュームを選択します。
5. **Destination**（宛先）オプションを使用して、選択されたボリュームがロールバックする宛先ボリュームを選択します。
6. 次のオプションから選択します。
   - **Live Recovery**（ライブリカバリ）。選択されると、Windows ボリュームのロールバックがただちに行われます。デフォルトで選択されています。

     メモ: Live Recovery（ライブリカバリ）オプションは、Linux ボリュームには使用できません。

   - **Force Dismount**（マウント解除の強制実行）。選択されると、ロールバックを実行する前に、マウントされているリカバリポイントが強制的にマウント解除されます。デフォルトで選択されています。
7. **ロールバック** をクリックします。

   選択されたリカバリポイントへのロールバック処理が開始されます。

コマンドラインを使用した Linux マシンのロールバックの実行

ロールバックは、リカバリポイントからマシン上のボリュームを復元するプロセスです。AppAssure では、コマンドラインの `aamount` ユーティリティを使用して、保護対象 Linux マシン上のボリュームのロールバックを実行できます。

注意: システムまたはルート（/）ボリュームではロールバックの実行を試行しないでください。

メモ: ロールバック機能は、Core Console 内の保護対象 Windows マシンに対してサポートされています。詳細については、「ロールバックの実行」を参照してください。

Linux マシン上のボリュームのロールバックを実行するには、次の手順を実行します。

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. 指定した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。
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。

   メモ: / へのロールバックは、Live CD で起動している間にベアメタル復元を実行している場合にのみ可能です。詳細については、「Linux マシンのベアメタル復元の実行」を参照してください。
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。

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。

Windows マシンのベアメタル復元について

サーバーは、予期されるとおりに動作している場合には設定されたタスクを実行しますが、サーバーを操作不能にする破壊的なイベントが発生したときは、サーバーを以前の動作状態に復元するために迅速な対策を講じることが必要です。このプロセスには通常、マシンの再フォーマット、オペレーティングシステムの再インストール、バックアップからのデータのリカバリ、およびソフトウェアアプリケーションの再インストールを伴います。

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実行」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前提条件

Windows マシンに対してベアメタル復元を実行するプロセスを開始するには、まず、次の条件と基準を満たしていることを確認する必要があります。

- サーバー、および機能している Core のバックアップ
- 復元用のハードウェア（新規または既存、同種または異種）
- 空の CD と CD 焼き付けソフトウェア
- VNC ビューア（オプション）
- ターゲットマシン用の Windows 7 PE（32 ビット）対応ドライバ、ストレージおよびネットワークアダプタドライバ
- ターゲットオペレーティングシステム用のストレージコントローラドライバ、RAID ドライバ、AHCI ドライバ、およびチップセットドライバ

メモ: ストレージコントローラドライバは、実行中の復元が異種ハードウェアに対するものである場合のみ必要です。

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。「起動可能 CD ISO イメージの作成」を参照してください。
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。 「起動 CD のロード」を参照してください。
4. リカバリディスクに接続します。
5. ボリュームをマッピングします。 「ボリュームのマッピング」を参照してください。
6. リカバリを開始します。「AppAssure Core からの復元の開始」を参照してください。
7. 進捗状況を監視します。 「リカバリ進捗状況の表示」を参照してください。

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。

手動マッピングの場合は、復元を行う前に新しいマシンを正しくフォーマットしておく必要があります。詳細については、「AppAssure Core からの復元の開始」を参照してください。

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. **RollbackURC** ダイアログボックスで、**Automatically Map Volumes**（ボリュームの自動マッピング）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. **Rollback**（ロールバック）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. **RollbackURC** ダイアログボックスで、**Manually Map Volumes**（ボリュームの手動マッピング）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、**Begin Rollback**（ロールバックの開始）をクリックします。

警告: 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。

起動時間問題の修復

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実行

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。screen ユーティリティのインストールについては、「screen ユーティリティのインストール」を参照してください。

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。

イベントおよびアラートの表示

イベントおよびアラートを表示するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console の Machines（マシン）タブで、イベントを表示するマシンのハイパーリンクをクリックします。
   - Core Console の左側にある **Navigation**（ナビゲーション）領域で、イベントを表示するマシンを選択します。
2. **Events**（イベント）タブをクリックします。

   現在のタスクとアラートに対する全イベントのログが表示されます。

5

サーバークラスタの保護

サーバークラスタ保護について

AppAssure では、サーバークラスタ保護は個々のクラスタノード（つまり、クラスタ内の個々のマシン）にインストールされている AppAssure エージェントと Core に関連付けられており、これにより、これらのエージェントは 1 つの複合マシンとして保護されます。

Core は、クラスタの保護および管理を行うために簡単に設定することができます。Core Console では、クラスタは別のエンティティとして組織されており、関連するノードを含めるための「コンテナ」として機能します。たとえば、左のナビゲーション領域では、Core はナビゲーションツリーの最上位に表示され、クラスタは Core の下にリストされます。クラスタに関連する個々のノード（AppAssure エージェントがインストールされているもの）は各クラスタ内に表示されます。

Core レベルとクラスタレベルにおいて、関連するノードと共有ボリュームのリストなど、クラスタについての情報を表示できます。クラスタは Machines（マシン）タブの Core Console に表示されます。クラスタに含まれるノードは Show/Hide（表示 / 非表示）でビューを切り替えて表示します。クラスタレベルでは、クラスタ内のノードに対応する Exchange および SQL クラスタメタデータも表示できます。クラスタ全体およびそのクラスタ内の共有ボリュームの設定を指定、またはクラスタ内の個々のノード（マシン）に移動して、そのノードと関連するローカルボリュームに対してのみ設定を行うこともできます。

サポートされるアプリケーションとクラスタタイプ

クラスタを適切に保護するには、そのクラスタ内の個々のマシンまたはノードに AppAssure Agent ソフトウェアをインストールしておく必要があります。AppAssure では、次の表に示されているアプリケーションバージョンとクラスタ設定がサポートされています。

表 4. サポートされるアプリケーションとクラスタタイプ

アプリケーション	アプリケーションバージョンと関連するクラスタ設定	Windows Failover Cluster
Microsoft Exchange	2007 シングルコピークラスタ（SCC）	2003、2008、2008 R2
	2007 クラスタ連続レプリケーション（CCR）	
	2010 データベース可用性グループ（DAG）	2008、2008 R2
Microsoft SQL	2005、2008、2008 R2 シングルコピークラスタ（SCC）	2003、2008、2008 R2
	2012 シングルコピークラスタ（SCC）	2008、2008 R2、2012

サポートされるディスクタイプは以下のとおりです。

- 2 TB を超える GUID パーティションテーブル（GPT）ディスク
- ダイナミックディスク
- ベーシックディスク

サポートされるマウントタイプは以下のとおりです。

- ドライブ文字で接続されている共有ドライブ（たとえば、D:）
- 単一物理ディスク上のシンプルダイナミックボリューム（ストライピング、ミラーリング、スパニングのいずれも行われていないボリューム）
- マウントポイントとして接続されている共有ドライブ

クラスタの保護

このトピックでは、AppAssure での保護のためにクラスタを追加する方法について説明します。クラスタを保護に追加するときは、クラスタ、クラスタアプリケーション、または AppAssure Agent を搭載しているクラスタノードまたはマシンのいずれかのホスト名または IP アドレスを指定する必要があります。

メモ: 保護対象ノードからキャプチャされたデータのスナップショットを保存するために、リポジトリが使用されます。クラスタ内のデータの保護を開始する前に、AppAssure Core に関連付けられているリポジトリを少なくとも 1 つセットアップしてください。

リポジトリのセットアップの詳細については、「リポジトリについて」を参照してください。

クラスタを保護するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Home**（ホーム）タブに移動して、**Protect Cluster**（クラスタの保護）ボタンをクリックします。
   - Core Console の **Machines**（マシン）タブで、**Actions**（アクション）をクリックし、**Protect Cluster**（クラスタの保護）をクリックします。
2. **Connect to Cluster**（クラスタへの接続）ダイアログボックスで、次の情報を入力します。

テキストボックス	説明
Host（ホスト）	クラスタのホスト名または IP アドレス、クラスタアプリケーション、または保護したいクラスタノードのひとつ。 **メモ:** ノードのうちの 1 台の IP アドレスを使用する場合は、そのノードに AppAssure エージェントがインストールされ、起動されている必要があります。
Port（ポート）	AppAssure Core がエージェントと通信するマシン上のポート番号。
User name（ユーザー名）	このマシンに接続するために使用するドメイン管理者のユーザー名（たとえば、**domain_name\administrator** または **administrator@domain_name.com**）。 **メモ:** ドメイン名は必須です。ローカルシステム管理者ユーザー名を使用してクラスタに接続することはできません。
Password（パワード）	このマシンに接続するために使用するパスワード。

3. **Protect Cluster**（クラスタの保護）ダイアログボックスで、このクラスタのリポジトリを選択します。
4. デフォルト設定に基づいてクラスタを保護するには、デフォルト保護のノードを選択して、**Protect**（保護）をクリックします。

メモ: デフォルト設定では、すべてのボリュームが 60 分ごとのスケジュールで保護されます。

5. クラスタのカスタム設定を入力するには（たとえば、共有ボリュームの保護スケジュールをカスタマイズする）、以下を行います。
   a. **settings**（設定）をクリックします。
   b. **Volumes**（ボリューム）ダイアログボックスで、保護するボリュームを選択して、**Edit**（編集）をクリックします。
   c. **Protection Schedule**（保護スケジュール）ダイアログボックスで、以下の表の説明のとおり、データを保護するためのいずれかのスケジュールオプションを選択します。

テキストボックス	説明
Interval（間隔）	次から選択できます。 • **Weekday**（平日）— 特定の間隔でデータを保護するには、**Interval**（間隔）を選択して、次の操作を行います。 – ピーク時間中にデータを保護する時間をカスタマイズするには、開始時刻、終了時刻、および間隔を指定できます。 – オフピーク時間にデータを保護するには、**Protect during off-peak times**（オフピーク時間に保護する）チェックボックスをオンにして、保護の間隔を選択します。 • **Weekends**（週末）— 週末にもデータを保護するには、**Protect during weekends**（週末に保護する）チェックボックスをオンにして、間隔を選択します。
Daily（毎日）	毎日データを保護するには、**Daily**（毎日）オプションを選択して、**Protection Time**（保護時刻）で、データの保護を開始する時刻を選択します。
No Protection（保護なし）	このボリュームから保護を削除するには、**No Protection**（保護なし）オプションを選択します。

6. すべての必要な変更を行ったら、**Save**（保存）をクリックします。
7. クラスタ内のノードのカスタム設定を入力するには、ノードを選択し、そのノードの横にある **Settings**（設定）リンクをクリックします。
   • 保護スケジュールを編集するには、手順 5 を繰り返します。

   ノードのカスタマイズの詳細については、「クラスタ内のノードの保護」を参照してください。
8. **Protect Cluster**（クラスタの保護）ダイアログボックスで、**Protect**（保護）をクリックします。

クラスタ内のノードの保護

このトピックでは、AppAssure エージェントがインストールされているクラスタノードまたはマシン上のデータを保護する方法について説明します。保護を追加する場合、使用可能なノードのリストからノードを選択するとともに、ホスト名およびドメイン管理者のユーザー名とパスワードを指定する必要があります。

クラスタ内のノードを保護するには、次の手順を実行します。

1. クラスタを追加した後は、そのクラスタに移動して **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をクリックして、**Protect Cluster Node**（クラスタノードを保護）をクリックします。
3. **Protect Cluster Node**（クラスタノードを保護）ダイアログボックスで、次の情報を必要に応じて選択するか入力し、**Connect**（接続）をクリックして、マシンまたはノードを追加します。

テキストボックス	説明
Host（ホスト）	クラスタ内の保護可能なノードのドロップダウンリストです。
Port（ポート）	Core がノード上のエージェントと通信するときに使用するポート番号。
User name（ユーザー名）	このノードに接続するために使用するドメイン管理者のユーザー名です（たとえば、**administrator@example_domain.com** の **example_domain \administrator**）。
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。

4. **Protect**（保護）をクリックして、デフォルト保護設定でこのマシンの保護を開始します。

   メモ: デフォルト設定では、マシン上のすべてのボリュームが 60 分ごとのスケジュールで保護されます。

5. このマシンのカスタム設定を入力するには（たとえば、表示名の変更、暗号化の追加、または保護スケジュールのカスタマイズを行う）、**Show Advanced Options**（詳細オプションの表示）をクリックします。
6. 次の説明に従い、必要に応じて設定を編集します。

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 Core 上のリポジトリを選択します。
Encryption（暗号化）	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。
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）。 • 特定のボリュームをカスタムスケジュールで保護します。この場合、**Volumes**（ボリューム）でボリュームを選択し、**Edit**（編集）をクリックします。カスタム間隔の設定については、「クラスタの保護」を参照してください。

クラスタノード設定の変更プロセス

クラスタノードに保護を追加したら、これらのマシンまたはノードの基本設定（表示名、ホスト名など）、保護設定（マシン上のローカルボリュームの保護スケジュールの変更、ボリュームの追加または削除、保護の一時停止）などを簡単に変更できます。

クラスタノード設定を変更するには、次のタスクを実行してください。

1. 次の手順のいずれか 1 つを実行します。

- 変更するノードを含むクラスタに移動し、**Machines**（マシン）タブをクリックして、変更するマシンまたはノードを選択します。
- または、**Navigation**（ナビゲーション）ペインから、**Cluster**（クラスタ）見出しの下で、変更したいマシンまたはノードを選択します。

2. 構成設定を変更、表示するには、「構成設定の表示および変更」を参照してください。
3. システムイベントの通知グループを設定するには、「システムイベントの通知グループの設定」を参照してください。
4. 保持ポリシー設定をカスタマイズするには、「保持ポリシー設定のカスタマイズ」を参照してください。
5. 保護スケジュールを変更するには、「保護スケジュールの変更」を参照してください。
6. 転送設定を変更するには、「転送設定の変更」を参照してください。

クラスタ設定のロードマップ

クラスタ設定のロードマップには、次のタスクの実行が含まれます。

- クラスタ設定の変更
- クラスタイベント通知の設定
- クラスタ保持ポリシーの変更
- クラスタ保護スケジュールの変更
- クラスタ転送設定の変更

クラスタ設定の変更

クラスタの追加後は、基本設定（たとえば表示名）や保護設定（たとえば保護スケジュール、ボリュームの追加または削除、保護の一時停止）などを簡単に変更できます。

クラスタ設定を変更するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックし、変更するクラスタを選択します。
   - 左のナビゲーション領域で、変更するクラスタを選択します。
2. **設定** タブをクリックします。

   Settings（設定）ページが表示されます。
3. **Edit**（編集）をクリックして、次に説明されているこのページにあるクラスタの設定を変更します。

テキストボックス	説明
Display Name（表示名）	クラスタの表示名を入力します。 Core Console にこのクラスタの名前が表示されます。デフォルトでは、これはクラスタのホスト名になっています。必要に応じて、より説明的な名前に変更できます。
Host Name（ホスト名）	この設定はクラスタのホスト名を表します。この設定は情報目的のみで表示されており、変更はできません。
Repository（リポジトリ）	クラスタに関連付けられたコアリポジトリを入力します。

テキストボックス	説明

メモ: このクラスタのスナップショットがすでに作成されている場合、この設定は通知目的でのみここに表示され、変更はできません。

Encryption Key（暗号化キー）	必要に応じて暗号化キーを編集して選択します。 リポジトリに保存されるこのクラスタ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。

クラスタイベント通知の設定

通知グループを作成することにより、クラスタのシステムイベントの報告方法を設定できます。これらのイベントにはシステムアラートやエラーがあります。

クラスタイベント通知を設定するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックし、変更するクラスタを選択します。
   - 左のナビゲーション領域で、変更するクラスタを選択します。
2. **Configuration**（設定）タブをクリックし、**Events**（イベント）をクリックします。
3. 次の表で説明するいずれか 1 つのオプションを選択します。

テキストボックス	説明
Use Core alert settings（コアアラート設定を使用）	関連するコアで使用されている設定を採用します。 a. **Apply**（適用）をクリックします。 b. 手順 5 を完了します。
Use Custom alert settings（カスタムアラート設定を使用）	カスタム設定ができます。手順 4 に進みます。

4. **Custom alert settings**（カスタムアラート設定）を選択する場合は、**Add Group**（グループの追加）をクリックして、システムイベントのリストを送信するための新しい通知グループを追加します。

   Add Notification Group（通知グループの追加）ダイアログボックスが表示されます。
5. 次の表の説明どおりに通知オプションを追加します。

テキストボックス	説明
Name（名前）	通知グループの名前を入力します。
Description（説明）	通知グループの説明を入力します。
Enable Events（イベントの有効化）	通知対象のイベントを選択します（例えば、クラスタ）。次のタイプで選択することもできます。 • **Error（エラー）** • **Warning（警告）**

テキストボックス	説明
	• **Info（情報）** **メモ:** タイプで選択する場合、該当するイベントがデフォルトで自動的に有効になります。たとえば警告を選択すると、アタッチ可否、ジョブ、ライセンス、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、およびロールバックイベントが有効になります。
Notification Options（通知オプション）	通知の処理方法を選択して指定します。次のオプションから選択できます。 • **Notify by Email**（E-メールで通知）— To（宛先）、CC、および BCC テキストボックスに、イベントを送信する E-メールアドレスを指定します。 • **Notify by Windows Event log**（Windows イベントログで通知）— Windows イベントログが通知を制御します。 • **Notify by syslogd**（syslogd で通知）— イベントを送信するホスト名およびポートを指定します。

6. **OK** をクリックして変更を保存し、**Apply**（適用）をクリックします。
7. 既存の通知グループを編集するには、リストの通知グループの横にある **Edit**（編集）をクリックします。
   設定を編集するための **Edit Notification Group**（通知グループを編集）ダイアログボックスが表示されます。

クラスタ保持ポリシーの変更

クラスタの保持ポリシーは、クラスタ内の共有ボリュームのリカバリポイントがリポジトリ内に保存される期間を指定します。保持ポリシーを使用することで、バックアップスナップショットの保持期間を長くしたり、これらのバックアップスナップショットの管理に役立てることができます。保持ポリシーは、古いバックアップのエージングと削除を援助するロールアッププロセスによって実施されます。

1. 次の手順のいずれか 1 つを実行します。
   - **Core Console** で **Machines**（マシン）タブをクリックして、変更するクラスタを選択します。
   - 左のナビゲーション領域で、変更するクラスタを選択します。
2. **Configuration**（設定）タブをクリックし、**Retention Policy**（保持ポリシー）をクリックします。
3. 次の表で説明するオプションのいずれかを選択します。

テキストボックス	説明
Use Core default retention policy（コアのデフォルト保持ポリシーを使用する）	関連するコアで使用されている設定を採用します。**Apply**（適用）をクリックします。
Use Custom retention policy（カスタム保持ポリシーを使用する）	カスタム設定を実行できます。

メモ: Custom alert settings（カスタムアラート設定）を選択した場合は、「保持ポリシー設定のカスタマイズ」の手順 4 以降に記載されているカスタム保持ポリシーの設定手順に従ってください。

クラスタ保護スケジュールの変更

クラスタが共有ボリュームを持つ場合のみ保護スケジュールを変更できます。
クラスタ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. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックし、変更するクラスタを選択します。
   - 左のナビゲーション領域で、変更するクラスタを選択します。
2. **Configuration**（設定）タブをクリックし、**Protection Settings**（保護設定）をクリックします。
3. 「保護スケジュールの変更」の手順 2 以降の説明のとおりに保護設定の変更手順に従ってください。

クラスタ転送設定の変更

AppAssure では、設定を簡単に変更して、保護対象クラスタのデータ転送プロセスを管理できます。

メモ: クラスタ転送設定は、クラスタが共有ボリュームを持つ場合にのみ変更できます。

AppAssure には、次の 3 つの転送タイプがあります。

テキストボックス	説明
Snapshots（スナップショット）	保護対象クラスタ上のデータをバックアップします。
VM Export（VM エクスポート）	クラスタを保護するために定義されたスケジュールによって指定されたすべてのバックアップ情報とパラメータを持つ仮想マシンを作成します。
Rollback（ロールバック）	保護対象クラスタのバックアップ情報を復元します。

クラスタ転送設定を変更するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックし、変更するクラスタを選択します。
   - 左のナビゲーション領域で、変更するクラスタを選択します。
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。
3. 「保護スケジュールの変更」の手順 2 からの説明に従って保護設定を変更します。

保護されたクラスタノードのエージェントへの変換

AppAssure では、保護されているクラスタノードを、Core による管理を維持したままクラスタから除外するために、AppAssure エージェントに変換することができます。これは、たとえば、クラスタノードを保護された状態のままクラスタから削除したい場合に役立ちます。
保護されたクラスタノードをエージェントに変換するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で、**Machines**（マシン）タブをクリックし、変換するマシンが含まれているクラスタを選択します。そのクラスタの **Machines**（マシン）タブをクリックします。

- 左のナビゲーション領域から、変換したいマシンが含まれているクラスタを選択して、**Machines**（マシン）タブをクリックします。

2. 変換するマシンを選択して、Machines（マシン）タブの上部にある **Actions**（アクション）ドロップダウンメニューをクリックし、**Convert to Agent**（エージェントに変換）をクリックします。
3. マシンをクラスタに戻すには、マシンを選択して、**Summary**（サマリ）タブ、**Actions**（アクション）メニュー、**Convert to Node**（ノードに変換）とクリックします。

サーバークラスタ情報の表示

クラスタシステム情報の表示

クラスタシステム情報を表示するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックして、表示するクラスタを選択します。
   - 左の **navigation**（ナビゲーション）領域で、表示するクラスタを選択します。
2. **Tools**（ツール）タブをクリックします。

   System Information（システム情報）ページに、名前、含まれるノードとそれに関連付けられている状態および Windows バージョン、ネットワークインタフェース情報、ボリューム容量情報などの、クラスタについてのシステム詳細が示されます。

クラスタのイベントとアラートの表示

クラスタ内の個々のマシンまたはノードのイベントとアラートを表示する方法については、「イベントおよびアラートの表示」を参照してください。

クラスタのイベントとアラートを表示するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックして、表示するクラスタを選択します。
   - 左の **Navigation**（ナビゲーション）領域の **Clusters**（クラスタ）で、表示するクラスタをクリックします。
2. **Events**（イベント）タブをクリックします。

   ログに現在のタスクに関するすべてのイベントの他、クラスタに関するアラートが表示されます。
3. イベントのリストをフィルタリングするには、必要に応じて、**Active**（アクティブ）、**Complete**（完了）、または **Failed**（失敗）チェックボックスを選択、または選択解除します。
4. **Alerts**（アラート）テーブルで、**Dismiss All**（すべて無視）をクリックして、リスト内のすべてのアラートを無視します。

サマリ情報の表示

サマリ情報を表示するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックして、表示するクラスタを選択します。
   - 左の **Navigation**（ナビゲーション）領域の **Clusters**（クラスタ）で、表示するクラスタをクリックします。
2. **Summary**（サマリ）タブで、クラスタ名、クラスタタイプ、クォーラムタイプ（該当する場合）、クォーラムパス（該当する場合）などの情報を確認できます。

   このタブには、サイズや保護スケジュールを含む、このクラスタ内のボリュームについての一覧情報も表示されます。

3. この情報を最新の状態に更新するには、**Actions**（アクション）ドロップダウンメニューをクリックし、**Refresh Metadata**（メタデータを更新）をクリックします。

   クラスタ内の個々のマシンまたはノードのサマリ情報とステータス情報を表示する方法については、「マシンのステータスおよびその他詳細の表示」を参照してください。

クラスタリカバリポイントでの作業

リカバリポイント（スナップショットとも呼ばれる）は、クラスタ内の共有ボリューム用のフォルダおよびファイルのポイントインタイムコピーであり、リポジトリに保存されます。リカバリポイントは、保護対象マシンのリカバリやローカルファイルシステムへのマウントを行います。AppAssure では、リポジトリ内のリカバリポイントのリストを表示することができます。リカバリポイントを確認するには、次の手順を実行します。

メモ: DAG または CCR サーバークラスタのデータを保護している場合、関連付けられたリカバリポイントはクラスタレベルでは表示されません。これらのリカバリポイントは、ノードまたはマシンレベルでのみ表示できます。

クラスタ内の個々のマシンのリカバリポイントを表示する方法については、「リカバリポイントの表示」を参照してください。

クラスタリカバリポイントでの作業には、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックして、リカバリポイントを表示したいクラスタをクリックします。
   - 左のナビゲーション領域の **Clusters**（クラスタ）で、リカバリポイントを表示したいクラスタを選択します。
2. **Recovery Points**（リカバリポイント）タブをクリックします。
3. 特定のリカバリポイントについての詳細情報を表示するには、リスト内のリカバリの横にある **>** をクリックして表示を展開します。

   リカバリポイントで実行可能な操作の詳細については、「特定のリカバリポイントの表示」を参照してください。
4. マウントするリカバリポイントを選択します。

   リカバリポイントをマウントする方法の詳細については、「Windows マシンへのリカバリポイントのマウント」の手順 2 以降を参照してください。
5. リカバリポイントの削除については、「リカバリポイントの削除」を参照してください。

クラスタのスナップショットの管理

スナップショットを強制実行するか、現在のスナップショットを一時停止することによってスナップショットを管理できます。スナップショットの強制実行では、現在保護されているクラスタの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と、ただちに転送が開始されるか、キューに追加されます。以前のリカバリポイント転送から変更されたデータだけが転送されます。以前のリカバリポイントが存在しない場合は、保護対象ボリューム上のすべてのデータ（ベースイメージ）が転送されます。スナップショットを一時停止すると、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。

クラスタ内の個々のマシンに対するスナップショットの強制実行については、「スナップショットの強制実行」を参照してください。クラスタ内の個々のマシンに対するスナップショットの一時停止と再開については、「保護の一時停止と再開」を参照してください。

クラスタのスナップショットの強制実行

クラスタの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. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックして、リカバリポイントを表示したいクラスタをクリックします。
   - 左のナビゲーション領域の **Clusters**（クラスタ）で、リカバリポイントを表示したいクラスタを選択します。
2. **Summary**（サマリ）タブの **Actions**（アクション）ドロップダウンメニューで、**Force Snapshot**（スナップショットの強制）をクリックします。

クラスタスナップショットの一時停止と再開

クラスタスナップショットを一時停止および再開するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックして、リカバリポイントを表示したいクラスタをクリックします。
   - 左のナビゲーション領域の **Clusters**（クラスタ）で、リカバリポイントを表示したいクラスタを選択します。
2. **Summary**（サマリ）タブの Actions（アクション）ドロップダウンメニューをクリックし、**Pause Snapshots**（スナップショットの一時停止）をクリックします。
3. **Pause Protection**（保護の一時停止）ダイアログボックスで、次に説明されているオプションのひとつを選択します。

テキストボックス	説明
Pause until resumed（再開まで一時停止）	手動で保護を再開するまでスナップショットを一時停止します。保護を再開するには、**Actions**（アクション）メニューをクリックし、**Resume**（再開）をクリックします。
Pause for（一時停止）	スナップショットを一時停止する時間を日、時間、分単位で指定できます。

ローカルリカバリポイントのマウント解除

ローカル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. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックし、リカバリポイントをマウント解除したいクラスタをクリックします。
   - 左のナビゲーション領域で、リカバリポイントをマウント解除したいクラスタを選択します。
2. **Tools**（ツール）タブの **Tools**（ツール）メニューで **Mounts**（マウント）をクリックします。
3. ローカルマウントのリストで、次のいずれかを行います。
   - 単一のローカルマウントをマウント解除するには、マウント解除したいリカバリポイントのマウントを特定して選択し、**Dismount**（マウント解除）をクリックします。
   - すべてのローカルマウントをマウント解除するには、**Dismount All**（すべてをマウント解除）ボタンをクリックします。

クラスタとクラスタノードのロールバックの実行

ロールバックとは、マシン上のボリュームをリカバリポイントから復元するプロセスです。サーバークラスタの場合、ロールバックはノード（マシン）レベルで実行します。本項では、クラスタボリュームに対してロールバックを実行する際のガイドラインについて説明します。

CCR（Exchange）と DAG クラスタのロールバックの実行

SCC（Exchange、SQL）クラスタのロールバックを実行するには、次の手順を実行します。

1. 1 台を除くすべてのノードの電源をオフにします。
2. 「ロールバックの実行」および「コマンドラインを使用した Linux マシンのロールバックの実行」に記載されている AppAssure の標準手順を使用してロールバックを実行します。
3. ロールバックが終了したら、クラスタボリュームのすべてのデータベースをマウントします。
4. ほかのすべてのノードの電源をオンにします。
5. Exchange の場合、Exchange Management Console に移動し、各データベースに対して、**Update Database Copy**（データベースコピーの更新）操作を実行します。

SCC（Exchange、SQL）クラスタのロールバックの実行

SCC（Exchange、SQL）クラスタのロールバックを実行するには、次の手順を実行します。

1. 1 台を除くすべてのノードの電源をオフにします。
2. 「ロールバックの実行」および「コマンドラインを使用した Linux マシンのロールバックの実行」に記載されている AppAssure の標準手順を使用してロールバックを実行します。
3. ロールバックが終了したら、クラスタボリュームのすべてのデータベースをマウントします。
4. 他のすべてのノードの電源を 1 つずつオンにします。

メモ: クォーラムディスクをロールバックする必要はありません。クォーラムディスクは、自動で、またはクラスタサービス機能を使用して再生できます。

クラスタデータのレプリケーション

クラスタのデータをレプリケーションするときは、そのクラスタ内の個々のマシンにおけるマシンレベルでレプリケーションを設定します。また、共有ボリュームのリカバリポイントをレプリケートするようにレプリケーションを設定することもできます。たとえば、ソースからターゲットにレプリケートしたいエージェントが 5 つ存在する場合などです。

データのレプリケーションの詳細および手順については、「マシンでのエージェントデータのレプリケーション」を参照してください。

保護からのクラスタの削除

保護からクラスタを削除するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックし、削除するクラスタを選択します。
   - 左のナビゲーション領域で、削除したいクラスタを選択して **Summary**（タブ）を表示します。
2. **Actions**（アクション）ドロップダウンメニューをクリックして、**Remove Machine**（マシンの削除）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。

オプション	説明
Keep Recovery Points（リカバリポイントを維持）	このクラスタ用に現在保存されているすべてのリカバリポイントを維持します。
Remove Recovery Points（リカバリポイントを削除）	このクラスタ用に現在保存されている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。

保護からのクラスタノードの削除

以下の手順に従ってクラスタノードを保護から削除します。クラスタからノードを 1 つだけ削除する場合は、「保護対象クラスタノードのエージェントへの変換」を参照してください。保護からクラスタノードを削除するには次を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックし、削除するノードが含まれているクラスタを選択します。クラスタの **Machines**（マシン）タブで、削除するノードを選択します。
   - 左のナビゲーション領域の関連するクラスタで、削除したいノードを選択します。
2. **Actions**（アクション）ドロップダウンメニューをクリックして、**Remove Machine**（マシンの削除）をクリックします。
3. 次の表で説明するいずれか 1 つ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。

クラスタ内全ノードの保護からの削除

クラスタ内のすべてのノードを保護対象から削除するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックし、削除したいノードが含まれているクラスタを選択します。次に、そのクラスタの **Machines**（マシン）タブをクリックします。
   - 左のナビゲーション領域から、削除したいノードが含まれているクラスタを選択して、**Machines**（マシン）タブをクリックします。
2. **Machines**（マシン）タブ上部にある **Actions**（アクション）ドロップダウンメニューをクリックし、**Remove Machines**（マシンの削除）をクリックします。
3. 次の表で説明するいずれか 1 つ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。

オプション	説明
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。

クラスタまたはノードレポートの表示

クラスタおよび個々のノードに関する AppAssure のアクティビティについて、コンプライアンスレポートおよびエラーレポートを作成し、表示することができます。レポートには、クラスタ、ノード、および共有ボリュームについての AppAssure アクティビティ情報が含まれます。AppAssure レポートの詳細については、「レポートについて」を参照してください。

レポートツールバーにあるエクスポートオプションおよび印刷オプションの詳細については、「レポートツールバーについて」を参照してください。

クラスタまたはノードレポートを表示するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。
   - Core Console で **Machines**（マシン）タブをクリックして、レポートを作成するクラスタまたはノードを選択します。
   - 左の **Navigation**（ナビゲーション）領域で、レポートを作成するクラスタまたはノードを選択します。
2. **Tools**（ツール）タブをクリックし、**Reports**（レポート）メニューで次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）**
   - **Errors Report（エラーレポート）**
3. **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: AppAssure Core または AppAssure Agent ソフトウェアが導入される前のデータはありません。
4. **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。
5. **Generate Report**（レポートの生成）をクリックします。

   レポートが複数のページにわたる場合は、レポート結果の上部にあるページ番号または矢印ボタンをクリックして、結果のページを切り替えることができます。

   レポート結果がページ内に表示されます。
6. レポート結果を使用可能なフォーマット（PDF、XLS、XLSX、RTF、MHT、HTML、TXT、CSV、またはイメージ）のいずれかでエクスポートするには、ドロップダウンリストからエクスポートのフォーマットを選択し、次のいずれかを実行します。
   - 1 つ目の **Save**（保存）アイコンをクリックしてレポートをエクスポートし、ディスクに保存します。
   - 2 つ目の **Save**（保存）アイコンをクリックしてレポートをエクスポートし、新規のウェブブラウザウィンドウに表示します。
7. レポート結果を印刷するには、次のいずれかを実行します。
   - 1 つ目の **Printer**（プリンタ）アイコンをクリックして、レポート全体を印刷します。
   - 2 つ目の **Printer**（プリンタ）アイコンをクリックして、レポートの現在のページを印刷します。

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

DL4300 アプライアンスのフルリカバリの完了

DL4300 Backup To Disk アプライアンスのデータドライブは、スロット 0～11 および 14～17 に RAID 6 フォーマットで配置されており、データを失うことなく、最大 2 つのドライブ障害に耐えることができます。オペレーティングシステムはドライブ 12 と 13 に常駐し、RAID 1 仮想ディスクとしてフォーマットされています。この両方のディスクに障害が発生した場合は、アプライアンスを再び機能させるために、ドライブを交換して必要なソフトウェアを再インストールする必要があります。アプライアンスの完全リカバリを完了させるには、次の操作を行う必要があります。

- オペレーティングシステムの RAID 1 パーティションの作成
- オペレーティングシステムのインストール
- Recovery and Update Utility の実行
- ボリュームの再マウント

オペレーティングシステムの RAID 1 パーティションの作成

△ **注意: これらの操作は、オペレーティングシステムを格納する RAID 1 仮想ディスクに対してのみ実行することが重要です。データを格納する RAID 6 仮想ディスクに対してはこれらの操作を実行しないでください。**

RAID 1 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. スロット 12 と 13 のディスクが動作中のディスクとして認識されていることを確認します。
2. DL4300 Backup to Disk Appliance を起動します。
3. 起動プロセス中にプロンプトが表示されたら、<Ctrl><R> を押します。

   PERC BIOS Configuration Utility（PERC BIOS 設定ユーティリティ）画面が表示されます。
4. **VD Management**（VD 管理）タブの最上部にあるコントローラをハイライト表示にしてから <F2> を押し、**Create New VD**（新規 VD の作成）を選択します。

   メモ: RAID-1 OS VD がすでに存在する場合は、RAID-1 OS VD を高速初期化します。
5. **Virtual Disk Management**（仮想ディスクの管理）ページで、RAID レベルに RAID 1 を選択します。
6. **Physical Disks**（物理ディスク）ボックス内の両方のディスクを選択します。

   メモ: 仮想ディスクのサイズは 278.87 GB を超えないようにする必要があります。
7. オペレーティングシステムを格納する仮想ディスクであることを示す VD 名（「OS」など）を入力します。
8. <Tab> を押してカーソルを Initialize（初期化）に移動させ、<Enter> を押します。

   メモ: この段階で実行される初期化は、高速初期化です。
9. **OK** をクリックして選択を完了させるか、<Ctrl><N> を 2 回押します。

Ctrl Mgt（制御管理）ページが表示されます。

10. **Select boot device**（起動デバイスの選択）フィールドに移動し、オペレーティングシステムが格納されている仮想ディスクを選択します。

    このディスクの容量は約 278 GB です。

11. **Apply**（適用）を選択し、<Enter> を押します。
12. **PERC BIOS Configuration**（PERC BIOS 設定）ユーティリティを終了し、<Ctrl><Alt><Del> を押してシステムを再起動します。

OS のインストール

お使いのアプライアンスで Unified Server Configurator - Lifecycle Controller Enabled（USC-LCE）ユーティリティを使用して、オペレーティングシステムを回復します。

1. オペレーティングシステムのインストールメディアを準備します。
2. メディアを実行するドライブがあることを確認します。

   USB 光学ドライブまたは仮想メディアデバイスを使用できます。仮想メディアは、iDRAC を介してサポートされます。iDRAC を介した仮想メディアのセットアップについては、お使いのシステムの iDRAC デバイスに関するユーザーガイドを参照してください。

   インストールメディアが破損している、または読み取り不可能であると、USC が対応光学ドライブを検出できない場合があります。この場合、使用可能な光学ドライブがないことを示すエラーメッセージを受信する可能性があります。メディアが有効でない場合は（CD または DVD が適切でない場合など）、適切なインストールメディアを挿入するように要求するメッセージが表示されます。

3. システムを起動し、Dell のロゴが表示されてから 10 秒以内に <F10> キーを押して、USC を開始します。
4. 左ペインで **OS Deployment**（OS 導入）をクリックします。
5. 右ペインで **Deploy OS**（OS の導入）をクリックします。
6. 関連するオペレーティングシステムを選択し、**Next**（次へ）をクリックします。

   USC によって、選択したオペレーティングシステムに必要なドライバが解凍されます。これらのドライバは、**OEMDRV** という名前の内部 USB ドライブに解凍されます。

   メモ: ドライバの解凍には数分かかることがあります。

   メモ: OS 導入ウィザードによってコピーされたドライバは、すべて 18 時間後に削除されます。コピーされたドライバを使用できる 18 時間以内に、オペレーティングシステムのインストールを完了する必要があります。18 時間が過ぎる前にドライバを削除するには、システムを再起動して <F10> キーを押し、USC を再び起動します。<F10> キーを使用してオペレーティングシステムのインストールをキャンセルするか、再起動時に USC を再起動すると、18 時間の経過前にドライバが削除されます。

7. ドライバの解凍後に USC がプロンプトを表示したら、、オペレーティングシステムのインストールメディアを挿入します。

   メモ: Microsoft Windows オペレーティングシステムをインストールしている場合は、解凍されたドライバはオペレーティングシステムのインストール時に自動的にインストールされます。

Recovery and Update Utility の実行

Recovery and Update Utility を実行するには、次の手順を実行します。

1. **Recovery and Update Utility** を **dell.com/support** からダウンロードします。
2. このユーティリティを DL4300 Backup to Disk アプライアンスのデスクトップにコピーし、ファイルを解凍します。
3. **launchRUU** をダブルクリックします。
4. プロンプトが表示されたら、リストされているいずれのプロセスも実行していないことを確認して **Yes**（はい）をクリックします。
5. **Recovery and update utility** 画面が表示されたら、**Start**（開始）をクリックします。
6. 再起動のプロンプトが表示されたら、**OK** をクリックします。

   Windows Server の役割と機能、ASP .NET MVC3、LSI Provider、DL Applications、OpenManage Server Administrator、および AppAssure Core Software が Recovery and Update Utility の一部としてインストールされます。
7. プロンプトが再び表示されたら、システムを再起動します。
8. すべてのサービスとアプリケーションのインストールが完了したら、**Proceed**（続行）をクリックします。

   AppAssure Appliance Recovery（AppAssure Appliance リカバリ）ウィザードが起動します。
9. AppAssure Appliance Recovery ウィザードの **Collecting Information and Configuring**（情報の収集と設定）フェーズの手順を実行し、**Next**（次へ）をクリックします。

   Disk Recovery（ディスクリカバリ）フェーズが開始されます。
10. AppAssure サービスのシャットダウンに関する警告を確認したら、**Next**（次へ）をクリックします。

    リポジトリ用の仮想ディスクと仮想スタンバイマシンがすべて復元され、AppAssure サービスが再起動されます。これでリカバリは完了です。

8

手動によるホスト名の変更

ホスト名は、DL4300 Backup to Disk Appliance の初期設定時に選択することをお勧めします。後で **Windows System Properties**（Windows システムのプロパティ）を使用してホスト名を変更する場合は、新しいホスト名を有効にし、アプライアンスを正常に機能させるために、次の手順を手動で実行する必要があります。

1. AppAssure Core サービスの停止
2. AppAssure サーバー証明書の削除
3. コアサーバーとレジストリキーの削除
4. AppAssure での表示名の変更
5. Internet Explorer での信頼済みサイトのアップデート

Core サービスの停止

AppAssure Core サービスを停止するには、次の手順を実行します。

1. **Windows Server Manager** を開きます。
2. 左側のツリーで、**Configuration → Services** と選択します。
3. **AppAssure Core Service**（AppAssure Core サービス）を右クリックし、**Stop**（停止）を選択します。

サーバー証明書の削除

AppAssure サーバー証明書を削除するには、次の手順を実行します。

1. コマンドラインインタフェースを開きます。
2. **Certmgr** と入力し、<Enter> を押します。
3. **Certificate Manager**（証明書マネージャ）ウィンドウで、**Trusted Root Certification Authorities（信頼されたルート証明機関） → Certificates（証明書）** と選択します。
4. **Issue To**（発行先）列に古いホスト名が表示され、**Intended Purpose**（使用目的）列に **Server Authentication**（サーバー認証）が表示されている証明書をすべて削除します。

コアサーバーとレジストリキーの削除

コアサーバーとレジストリキーを削除するには、次の手順を実行します。

1. コマンドラインインタフェースを開きます。
2. **regedit** と入力し、<Enter> を押してレジストリエディタを開きます。
3. ツリー内で **HKEY_LOCAL_MACHINE → SOFTWARE → AppRecovery** と移動し、コアディレクトリを開きます。
4. **webServer** ディレクトリと **serviceHost** ディレクトリを削除します。

新しいホスト名を持つ Core の起動

手動で作成した新しいホスト名を使用して Core を起動するには、次の手順を実行します。

1. AppAssure Core サービスを開始します。
2. デスクトップ上の **AppAssure 5 Core** アイコンを右クリックし、**Properties**（プロパティ）をクリックします。
3. 古いサーバー名を新しい <server name:8006> に置換します。
   たとえば、**https://<servername>:8006/apprecovery/admin/Core** となります。
4. **OK** をクリックし、**AppAssure 5 Core** アイコンを使用して AppAssure Core Console を起動します。

表示名の変更

表示名を変更するには、次の手順を実行します。

1. 管理者として **AppAssure Console** にログオンします。
2. **Configuration**（設定）タブを選択し、**General**（一般）バーにある変更ボタンをクリックします。
3. 新しい **Display Name**（表示名）を入力し、**OK** をクリックします。

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。

9

付録 A — スクリプティング

PowerShell スクリプティングについて

Windows PowerShell は、管理の自動化を目的とした Microsoft .NET Framework 接続環境です。AppAssure には、PowerShell スクリプティング用の包括的なクライアントソフトウェア開発キット（SDK）が含まれており、管理者はこれを利用して、スクリプトを介したコマンドの実行による AppAssure リソースの管理を自動化できます。

また、管理者ユーザーは、ユーザーから提供された PowerShell スクリプトを指定の状況下で実行することもできます。たとえば、スナップショットの前後でアタッチ可否チェックやマウント可否チェックなどを行います。管理者は、AppAssure Core とエージェントの両方からスクリプトを実行できます。スクリプトはパラメータを受け入れることができ、スクリプトの出力はコアおよびエージェントのログファイルに書き込まれます。

メモ: 夜間ジョブの場合は、1 つのスクリプトファイルと JobType 入力パラメータを保持して夜間ジョブを区別します。

スクリプトファイルは **%ALLUSERSPROFILE%\AppRecovery\Scripts** フォルダにあります。

- Windows 7 の場合、**%ALLUSERSPROFILE%** フォルダのパスは **C:\ProgramData** です。
- Windows 2003 の場合、フォルダのパスは **Documents and Settings\All Users\Application Data** です。

メモ: AppAssure スクリプトの使用および実行を開始する前に、Windows PowerShell がインストールされ設定されている必要があります。

PowerShell スクリプティングの前提条件

AppAssure で PowerShell スクリプトの使用と実行を開始するには、Windows PowerShell 2.0 がインストールされている必要があります。

メモ: powershell.exe.config ファイルが PowerShell ホームディレクトリにあることを確認します。たとえば、**C:\WindowsPowerShell\powershell.exe** などです。

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
        <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
<supportedRuntime version="v2.0.50727"/>
</startup>
</configuration>
```

スクリプトのテスト

実行する予定のスクリプトをテストするには、PowerShell グラフィカルエディタの **powershell_ise** を使用できます。また、設定ファイル **powershell_ise.exe.config** は設定ファイル **powershell.exe.config** と同じフォルダに追加する必要があります。

メモ: 設定ファイル powershell_ise.exe.config には、powershell.exe.config ファイルと同じ内容が存在する必要があります。

注意: PowerShell スクリプトの前後の処理が失敗すると、ジョブも失敗します。

入力パラメータ

使用可能なすべての入力パラメータがサンプルスクリプトで使用されています。各パラメータについて次の表で説明します。

メモ: スクリプトファイルは、サンプルスクリプトファイルと同じ名前を処理する必要があります。

表 5. AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

方法	説明
`public uint MaxConcurrentStreams { get; set; }`	データ転送用に Core がエージェントに対して確立する同時 TCP 接続の最大数を取得または設定します。
`public uint MaxTransferQueueDepth { get; set; }`	一連のブロックが転送ストリームから読み取られるとき、その範囲は生成キューまたは消費キューに入ります。消費スレッドはこのキューからブロックを読み取り、エポックオブジェクトに書き込みます。リポジトリの書き込み速度がネットワークの読み取り速度よりも遅いと、このキューは満杯になります。キューが満杯になり、読み取りが停止するポイントが、転送キューの最大の深さです。
`public uint MaxConcurrentWrites { get; set; }`	任意の時点においてエポックに対して未処理とするブロック書き込み操作の最大数を取得または設定します。この数のブロック書き込みが未処理のときに追加のブロックが受信されると、それらの追加ブロックは、いずれかの未処理の書き込みが完了するまで無視されます。
`public ulong MaxSegmentSize { get; set; }`	単一のリクエストで転送する連続ブロックの最大数を取得または設定します。テスト結果に応じて、最適な値は上下します。
`public Priority Priority { get; set; }`	転送リクエストの優先度を取得または設定します。
`public int MaxRetries { get; set; }`	失敗した転送が失敗と判断される前に再試行される最大の回数を取得または設定します。
`public Guid ProviderId{ get; set; }`	このホスト上のスナップショットに使用する VSS プロバイダの GUID を取得または設定します。管理者は一般にデフォルトをそのまま使用します。
`public Collection<ExcludedWriter>ExcludedWriterIds { get; set; }`	VSS ライター ID のコレクションを取得または設定します。このコレクションは、このスナップショットから除外されます。ライター ID は、ライターの名前によって決定されます。この名前は、文書化目的

方法	説明
	でのみ使用され、ライターの名前と完全に一致する必要はありません。
`public ushort TransferDataServerPort { get; set; }`	エージェントから Core へのデータの実際の転送のための Core からの接続を受け入れる TCP ポートを含む値を取得または設定します。エージェントはこのポートに対してリッスンしようとしますが、このポートが使用中の場合、別のポートを代わりに使用することができます。Core は、各スナップボリュームのために `VolumeSnapshotInfo` オブジェクトの `BlockHashesUri` プロパティと `BlockDataUri` プロパティに指定されたポート番号を使用します。
`public TimeSpan SnapshotTimeout { get; set; }`	VSS スナップショット操作が停止およびタイムアウトするまでの待機時間を取得または設定します。
`public TimeSpan TransferTimeout { get; set; }`	スナップショットを破棄するまでの、Core からの追加の通信待機時間を取得または設定します。
`public TimeSpan NetworkReadTimeout { get; set; }`	この転送に関連するネットワーク読み取り操作のタイムアウトを取得または設定します。
`public TimeSpan NetworkWriteTimeout { get; set; }`	この転送に関連するネットワーク書き込み操作のタイムアウトを取得または設定します。

表 6. BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

方法	説明
`public Guid AgentId { get; set; }`	エージェントの ID を取得または設定します。
`public bool IsNightlyJob { get; set; }`	バックグラウンドジョブが夜間ジョブであるかどうかを示す値を取得または設定します。
`public virtual bool InvolvesAgentId(Guid agentId)`	指定されたエージェントがジョブに関わっているかどうかを示す値を判別します。

ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

パラメータ `DatabaseCheckJobRequestBase` から値を継承します。

DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)

パラメータ `BackgroundJobRequest` から値を継承します。

ExportJobRequest（namespace Replay.Core.Contracts.Export）

パラメータ `BackgroundJobRequest` から値を継承します。

方法	説明
`public uint RamInMegabytes { get; set; }`	エクスポートされた VM のメモリサイズを取得または設定します。ゼロ（0）に設定すると、ソースマシンのメモリサイズが使用されます。
`public VirtualMachineLocation Location { get; set; }`	このエクスポートのターゲットの場所を取得または設定します。これは、抽象基底クラスです。
`public VolumeImageIdsCollection VolumeImageIds { get; private set; }`	VM エクスポートに含めるボリュームイメージを取得または設定します。
`public ExportJobPriority Priority { get; set; }`	エクスポートリクエストの優先度を取得または設定します。

NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql)

パラメータ `BackgroundJobRequest` から値を継承します。

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

パラメータ `BackgroundJobRequest` から値を継承します。

TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)

方法	説明
`public Guid SnapshotSetId { get; set; }`	VSS によってこのスナップショットに割り当てられた GUID を取得または設定します。
`public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }`	スナップショット内に含まれる各ボリュームのスナップショット情報のコレクションを取得または設定します。

TransferJobRequest (namespace Replay.Core.Contracts.Transfer)

パラメータ `BackgroundJobRequest` から値を継承します。

方法	説明
`public VolumeNameCollection VolumeNames { get; set; }`	転送のためのボリューム名のコレクションを取得または設定します。
`public ShadowCopyType ShadowCopyType { get; set; }`	転送のためのコピータイプを取得または設定します。使用可能な値は、`Unknown`（不明）、`Copy`（コピー）、および `Full`（フル）です。
`Public AgentTransferConfiguration TransferConfiguration { get; set; }`	転送設定を取得または設定します。
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	ストレージ設定を取得または設定します。
`public string Key { get; set; }`	転送リクエストを認証するための一度限りのパスワードとして使用できる疑似乱数（ただし暗号化でセキュア化されていない）キーを生成します。

方法	説明
`public bool ForceBaseImage { get; set; }`	ベースイメージが強制されたかどうかを示す値を取得または設定します。
`public bool IsLogTruncation { get; set; }`	ジョブがログの切り捨てかどうかを示す値を取得または設定します。

表 7. TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

方法	説明
`public VolumeNameCollection VolumeNames { get; set; }`	転送のためのボリューム名のコレクションを取得または設定します。
`public ShadowCopyType ShadowCopyType { get; set; }`	転送のためのコピータイプを取得または設定します。使用可能な値は、`Unknown`（不明）、`Copy`（コピー）、および `Full`（フル）です。
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	転送設定を取得または設定します。
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	ストレージ設定を取得または設定します。
`public string Key { get; set; }`	転送リクエストを認証するための一度限りのパスワードとして使用できる疑似乱数（ただし暗号化でセキュア化されていない）キーを生成します。
`public bool ForceBaseImage { get; set; }`	ベースイメージが強制されたかどうかを示す値を取得または設定します。
`public bool IsLogTruncation { get; set; }`	ジョブがログの切り捨てかどうかを示す値を取得または設定します。
`public uint LatestEpochSeenByCore { get; set; }`	最新のエポック値を取得または設定します。
`public Guid SnapshotSetId { get; set; }`	VSS によってこのスナップショットに割り当てられた GUID を取得または設定します。
`public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }`	スナップショット内に含まれる各ボリュームのスナップショット情報のコレクションを取得または設定します。

表 8. TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

方法	説明
`public VolumeNameCollection VolumeNames { get; set; }`	転送のためのボリューム名のコレクションを取得または設定します。
`public ShadowCopyType ShadowCopyType { get; set; }`	転送のためのコピータイプを取得または設定します。使用可能な値は、`Unknown`（不明）、`Copy`（コピー）、および `Full`（フル）です。

方法	説明
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	転送設定を取得または設定します。
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	ストレージ設定を取得または設定します。
`public string Key { get; set;}`	転送リクエストを認証するための一度限りのパスワードとして使用できる疑似乱数（ただし暗号化でセキュア化されていない）キーを生成します。
`public bool ForceBaseImage { get; set; }`	ベースイメージが強制されたかどうかを示す値を取得または設定します。
`public bool IsLogTruncation { get; set; }`	ジョブがログの切り捨てかどうかを示す値を取得または設定します。
`public uint LatestEpochSeenByCore { get; set; }`	最新のエポック値を取得または設定します。

表 9. VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

方法	説明
`public string Description { get; set;}`	この場所の可読説明を取得または設定します。
`public string Method { get; set;}`	VM の名前を取得または設定します。

VolumeImageIdsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

パラメータ `System.Collections.ObjectModel.Collection<string>` から値を継承します。

表 10. VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

方法	説明
`public string GuidName { get; set;}`	ボリュームの ID を取得または設定します。
`public string DisplayName { get; set;}`	ボリュームの名前を取得または設定します。
`public string UrlEncode()`	URL 上で安全に渡すことができる URL エンコードされたバージョンの名前を取得または設定します。 **メモ:** .NET 4.0 WCF には既知の問題（**https://connect.microsoft.com/VisualStudio/feedback/ ViewFeedback.aspx?FeedbackID=413312**）が存在しており、パスエスケープ文字が URI テンプレート内で正しく機能しません。ボリューム名には「\」と「?」の両方が含まれるため、特殊文字「\」と「?」を他の特殊文字で置き換える必要があります。
`public string GetMountName()`	ボリュームイメージをいくつかのフォルダにマウントするために有効な、このボリュームの名前を返します。

VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage)

パラメータ System.Collections.ObjectModel.Collection<VolumeName> から値を継承します。

方法	説明
public override bool Equals(object obj)	このインスタンスと指定されたオブジェクト（VolumeNameCollection オブジェクトであることも必要）が同じ値を持っているかどうかを判別します(Object.Equals(Object) を上書きします)。
public override int GetHashCode()	この VolumeNameCollection のハッシュコードを返します（Object.GetHashCode() を上書きします)。

表 11. VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer)

方法	説明
public Uri BlockHashesUri { get; set;}	ボリュームブロックの MD5 ハッシュを読み取ることができる URI を取得または設定します。
public Uri BlockDataUri { get; set;}	ボリュームデータブロックを読み取ることができる URI を取得または設定します。

VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer)

パラメータ System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo> から値を継承します。

Pretransferscript.ps1

PreTransferScript は、スナップショットの転送前にエージェント側で実行されます。

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)

# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];
# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {
        echo 'TransferPrescriptParameterObject parameter is null'
}
else {
        echo
'TransferConfiguration:'$TransferPrescriptParameterObject.TransferConfiguration

        echo 'StorageConfiguration:'
```

```
$TransferPrescriptParameterObject.StorageConfiguration
}
```

Posttransferscript.ps1

PostTransferScript は、スナップショットの転送後にエージェント側で実行されます。

```
 # receiving parameter from transfer job
param([object] $TransferPostscriptParameter)


# building path to Agent's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null


# Converting input parameter into specific object

$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];


# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {
        echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
                echo 'ShadowCopyType:'
$TransferPostscriptParameterObject.ShadowCopyType
        echo 'ForceBaseImage:'
$TransferPostscriptParameterObject.ForceBaseImage                    echo
'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation
}
```

Preexportscript.ps1

PreExportScript は、エクスポートジョブの前にコア側で実行されます。

```
# receiving parameter from export job

param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Converting input parameter into specific object

$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged
```

```
if($ExportJobRequestObject -eq $null) {
                echo 'ExportJobRequestObject parameter is null'
}
else {
                echo 'Location:' $ExportJobRequestObject.Location
                echo 'Priority:' $ExportJobRequestObject.StorageConfiguration
}
```

Postexportscript.ps1

PostExportScript は、エクスポートジョブの後にコア側で実行されます。

メモ: PostExportScript を初期スタートアップ後にエクスポートされたエージェントで 1 度実行する場合には、入力パラメータはありません。標準的なエージェントでは、このスクリプトは **PostExportScript.ps1** として PowerShell スクリプトフォルダに保持されています。

```
# receiving parameter from export job

param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'

# Converting input parameter into specific object

$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged

if($ExportJobRequestObject -eq $null) {
            echo 'ExportJobRequestObject parameter is null'
}
else {
            echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
            echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

Prenightlyjobscript.ps1

PreNightlyJobScript は、コア側ですべての夜間ジョブの前に実行されます。これには **$JobClassName** パラメータがあり、子ジョブを別個に処理するために役立ちます。

```
 # receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]
$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
```

```
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job,
Checksum Check Job and Log  Truncation Job. All of them are triggering the
script, and $JobClassMethod (contain job name that calls the  script) helps to
handle those child jobs separately

switch ($JobClassMethod) {

# working with NightlyAttachability Job
        NightlyAttachabilityJob {
                $NightlyAttachabilityJobRequestObject =
$NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];

                echo 'Nightly Attachability job results:';
                if($NightlyAttachabilityJobRequestObject -eq $null) {
                        echo 'NightlyAttachabilityJobRequestObject parameter is
null';
                }

                else {
                                echo 'AgentId:'
$NightlyAttachabilityJobRequestObject.AgentId;
                                echo 'IsNightlyJob:'
$NightlyAttachabilityJobRequestObject.IsNightlyJob;
                }
                break;
}


# working with Rollup Job
RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
        if($RollupJobRequestObject -eq $null) {
                echo 'RollupJobRequestObject parameter is null';
        }
        else {
                    echo 'SimultaneousJobsCount:'
$RollupJobRequestObject.SimultaneousJobsCount;
                    echo 'AgentId:' $RollupJobRequestObject.AgentId;
                    echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as
"System.Collections.Generic.List``1[System.Guid]"
        if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
        }
        else {
                    echo 'Agents GUIDs:'
                    foreach ($a in $AgentsCollection) {
                        echo $a
                }
        }
        break;
}

# working with Checksum Check Job
        ChecksumCheckJob {
                $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
```

```
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
                echo 'Exchange checksumcheck job results:';
                if($ChecksumCheckJobRequestObject -eq $null) {
                        echo 'ChecksumCheckJobRequestObject parameter is null';
                }
                else {
                                echo 'RecoveryPointId:'
$ChecksumCheckJobRequestObject.RecoveryPointId;
                                echo 'AgentId:'
$ChecksumCheckJobRequestObject.AgentId;
                                echo 'IsNightlyJob:'
$ChecksumCheckJobRequestObject.IsNightlyJob;
                }
                break;
}


# working with Log Truncation Job
        TransferJob {
                $TransferJobRequestObject = $TransferJobRequest -as
                [Replay.Core.Contracts.Transfer.TransferJobRequest];
        echo 'Transfer job results:';
        if($TransferJobRequestObject -eq $null) {
                echo 'TransferJobRequestObject parameter is null';
        }
        else {
                echo 'TransferConfiguration:'
$TransferJobRequestObject.TransferConfiguration;
                echo 'StorageConfiguration:'
$TransferJobRequestObject.StorageConfiguration;
        }
        echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
        break;
    }
}
```

Postnightlyjobscript.ps1

PostNightlyJobScript は、各夜間ジョブの後にコア側で実行されます。これには **$JobClassName** パラメータがあり、子ジョブを別個に処理するために役立ちます。

```
 # receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]
$NightlyAttachabilityJobRequest,  [object]$RollupJobRequest, [object]$Agents,
[object]$ChecksumCheckJobRequest,  [object]$TransferJobRequest, [int]
$LatestEpochSeenByCore, [object]$TakeSnapshotResponse)

# building path to Core's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2= $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null


# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job,
Checksum Check Job and Log Truncation Job. All of them are triggering the
script, and $JobClassMethod (contain job name that calls the script) helps to
```

```
handle those child jobs separately

switch ($JobClassMethod) {


# working with NightlyAttachability Job

NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest
-as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results:';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
                echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
                echo 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;
                echo 'IsNightlyJob:'
$NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
        break;
}


# working with Rollup Job

RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
        if($RollupJobRequestObject -eq $null) {
                echo 'RollupJobRequestObject parameter is null';
        }
        else {
                echo 'SimultaneousJobsCount:'
$RollupJobRequestObject.SimultaneousJobsCount;
                echo 'AgentId:' $RollupJobRequestObject.AgentId;
                echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as
"System.Collections.Generic.List``1[System.Guid]"
        if($AgentsCollection -eq $null) {
                echo 'AgentsCollection parameter is null';
        }
        else {
                echo 'Agents GUIDs:'
                foreach ($a in $AgentsCollection) {
                echo $a
            }
        }
        break;
}


# working with Checksum Check Job
        ChecksumCheckJob {
                $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
                echo 'Exchange checksumcheck job results:';
                if($ChecksumCheckJobRequestObject -eq $null) {
                        echo 'ChecksumCheckJobRequestObject parameter is null';
                }
                else {
                        echo 'RecoveryPointId:'
```

```
$ChecksumCheckJobRequestObject.RecoveryPointId;
                        echo 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
                        echo 'IsNightlyJob:'
$ChecksumCheckJobRequestObject.IsNightlyJob;
                }
        break;
    }


# working with Log Truncation Job
        TransferJob {
                $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
                echo 'Transfer job results:';
                if($TransferJobRequestObject -eq $null) {
                        echo 'TransferJobRequestObject parameter is null';
                }
                else {
                        echo 'TransferConfiguration:'
$TransferJobRequestObject.TransferConfiguration;
                        echo 'StorageConfiguration:'
$TransferJobRequestObject.StorageConfiguration;
                }
                echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
                $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
[Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
                if($TakeSnapshotResponseObject -eq $null) {
                        echo 'TakeSnapshotResponseObject parameter is null';
                }
                else {
                        echo 'ID of this transfer session:'
$TakeSnapshotResponseObject.Id;
                        echo 'Volumes:' $TakeSnapshotResponseObject.Volumes;
                }
                break;
        }
}
```

サンプルスクリプト

次のサンプルスクリプトは、管理者ユーザーが PowerShell スクリプトの実行に役立てることができるように提供されています。

サンプルスクリプトは次のとおりです。

- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

10

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

デルへのお問い合わせ

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

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