Dell EMC Avamar for VMware

バージョン 18.2

ユーザー ガイド

302-005-120
REV 02

DELL EMC

2019 年 1 月発行

掲載される情報は、発信現在で正確な情報であり、予告なく変更される場合があります。

本文書に記載される情報は、「現状有姿」の条件で提供されています。本文書に記載される情報に関する、どのような内容についても表明保証条項を設けず、特に、商品性や特定の目的に対する適応性に対する黙示的保証はいたしません。この資料に記載される、いかなる Dell ソフトウェアの使用、複製、頒布も、当該ソフトウェアライセンスが必要です。

EMC ジャパン株式会社
〒 151-0053 東京都渋谷区代々木 2-1-1 新宿マインズタワー
www.DellEMC.com/ja-jp/index.htm
お問い合わせは
www.DellEMC.com/ja-jp/index.htm

目次

図

図

表

表

はじめに

製品ラインを改善するための努力の一環として、ソフトウェアおよびハードウェアのリビジョンを定期的にリリースしています。そのため、本書で説明されている機能の中には、現在お使いのソフトウェアまたはハードウェアのバージョンによっては、サポートされていないものもあります。製品のリリース ノートには、製品の機能に関する最新情報が掲載されています。

製品が正常に機能しない、またはこのドキュメントの説明どおりに動作しない場合には、テクニカル サポート プロフェッショナルにお問い合わせください。

注

このマニュアルには、発行時点で正確だった情報が記載されています。このドキュメントの最新バージョンを確認するには、オンライン サポート（https://support.EMC.com）にアクセスしてください。

目的

本書では、VMware™仮想マシンを保護するためのさまざまな方法と戦略について説明します。

対象読者

本書に記載の情報は、以下に精通したシステム管理者を対象としています。

- 「Avamar Administration Guide」に記載されている基本的な Avamar システム管理の原則および手順
- さまざまな Avamar クライアント ガイドに記載されている、その他の Avamar クライアント ソフトウェアの情報（主に、インストールと構成手順）

クライアント、データセット、スケジュール、保存ポリシー、バックアップ ポリシーなどの基本的な Avamar システム管理の概念と原則に関する包括的な説明は、本書の範囲外です。詳細については、「Avamar Administration Guide」を参照してください。

リビジョン履歴

次の表に、このドキュメントのリビジョン履歴を示します。

リビジョン	日付	説明
02	2018 年 1 月 25 日	プロキシ アップグレード手順を更新。 VMware Cloud on AWS における Avamar イメージ バックアップ/リストアの「サポート対象外の Avamar 操作」を更新。 「VMware Cloud on AWS Web ポータルのコンソールの設定」セクションの NSX-T に関する前提条件を追加。
01	2018 年 12 月 14 日	Avamar 18.2.の GA リリース。

関連ドキュメント

次に示す Dell EMC 資料に補足情報が記載されています。

- https://elabnavigator.emc.com/eln/modernHomeDataProtection の「 E-Lab Navigator」

- 「Avamar リリース ノート」
- 「Avamar Administration Guide」
- 「Avamar オペレーションのベスト プラクティス ガイド」
- 「Avamar 製品セキュリティ ガイド」
- 「Avamar バックアップ クライアント ユーザー ガイド」
- 「Avamar for Exchange VSS ユーザー ガイド」
- 「Avamar for IBM DB2 ユーザー ガイド」
- 「Avamar for Lotus Domino ユーザー ガイド」
- 「Avamar for Oracle ユーザー ガイド」
- 「Avamar for SharePoint VSS ユーザー ガイド」
- 「Avamar for SQL Server ユーザー ガイド」
- 「Avamar vSphere Web Client 管理ガイド」「」

次に示す VMware 関連の資料に補足情報が記載されています。

- 「VMware vSphere の概要」
- 「ESX の準備」
- 「vSphere 基本システム管理」
- 「vSphere リソース管理ガイド」
- 「vSphere Web Access 管理者ガイド」
- 「VMware ESX および vCenter Server のインストール ガイド」
- 「VMware ESX 構成ガイド」
- 「VMware データリカバリ管理ガイド」

このマニュアルで使用される特記事項の表記規則
特別な注意を要する事項には次の表記法を使用します。

危険

回避しなかった場合に死亡または重傷を招く危険な状況を示します。

警告

回避しなかった場合に死亡または重傷を招く可能性がある危険な状況を示します。

注意

回避しなかった場合に軽度または中程度の傷害を招く可能性がある危険な状況を示します。

通知

負傷に関連しない作業を示します。

注

重要ではあるが、危険ではない情報を表します。

表記規則
このドキュメントではこれらのタイプの表記規則を使用します。

表 1 表記規則

[太字]	ウィンドウ名、ダイアログ ボックス、ボタン、フィールド、タブ名、キー名、メニュー パスなど、インタフェースの構成要素（ユーザーが明示的に選択またはクリックする対象）の名前に使用します。
「斜体」	本文内で参照される出版物の完全なタイトルを示す
Monospace	以下の場合に使用： • システム コード • エラー メッセージやスクリプトなどのシステム出力 • パス名、ファイル名、プロンプト、構文 • コマンドおよびオプション
モノスペース斜体	変数に使用
モノスペース太字	ユーザーによる入力値を示す
[ ]	オプション値
|	縦棒は、選択肢を示し、「または」を意味する
{ }	中括弧内は、ユーザーが指定する必要のある内容を示す（例：x、y、z）
...	省略記号は、例の中で省略される必須ではない情報を示す

問い合わせ先

Avamar サポート ページを利用すると、ライセンス情報、製品ドキュメント、アドバイザリ、ダウンロード、ハウツーおよびトラブルシューティングの情報にアクセスできます。カスタマー サポートに問い合わせる前に、この情報に基づいて、製品に関する問題を解決できる場合があります。

Avamar サポート ページにアクセスするには、次の手順を実行します。

1. https://www.dell.com/support/home/us/en/19 に移動します。
2. [**Enter a Service Tag, Serial Number, Service Request, Model, or Keyword**] 検索ボックスに、製品名を入力します。
3. 表示されたリストから製品名を選択します。製品を選択すると、[**Product Support**] ページが自動的にロードされます。
4. （オプション）[**Product Support**] ページの右上隅の [**Add to My Saved Products**] をクリックして、製品を [**My Products**] リストに追加します。

ドキュメント

Avamar 製品ドキュメントには、包括的な機能概要、運用管理業務、テクニカル リファレンス情報が記載されています。製品管理ガイドおよびユーザー ガイドの補足情報については、次のドキュメントを確認してください。

- リリース ノートには、リリースに関する新機能の概要と既知の制限事項が記載されている。
- テクニカル ノートには、特定の製品機能に関する技術的詳細が記載されており、必要に応じて手順をステップごとに説明した内容も含まれている。
- ホワイト ペーパーには、重要なビジネス上の問題や要件に適用される、製品の技術的観点からの詳細な説明がある。

ナレッジベース

ナレッジベースには適用可能なソリューションが含まれており、ソリューション番号（たとえば、KB000xxxxxx）またはキーワードで検索することができます。

ナレッジベースを検索するには、以下の手順を実行します。

1. https://www.dell.com/support/home/us/en/19 に移動します。
2. ［**Support**］タブで、［**Knowledge Base**］をクリックします。
3. 検索ボックスにソリューション番号またはキーワードを入力します。（オプション）検索ボックスに製品名を入力し、表示されたリストから製品を選択して、検索を特定の製品に限定することができます。

オンライン コミュニティ
製品サポートおよびソリューションに関して共通の関心を持つユーザーとの連絡、会話、製品サポートおよびソリューションの内容については、コミュニティ ネットワーク（https://community.EMC.com）にアクセスしてください。すべての製品について、対話形式により、カスタマー、パートナー、認定専門資格保持者とオンラインで対話します。

ライブ チャット
ライブ インタラクティブ チャットを使用してカスタマー サポートにアクセスするには、Avamar サポート ページの［**Service Center**］パネルの［**Join Live Chat**］をクリックします。

サービス リクエスト
カスタマー サポートからの詳細なヘルプが必要な場合は、Avamar サポート ページの［**Service Center**］パネルの［**Create Service Requests**］をクリックしてサービス リクエストを送信します。

注

サービス リクエストを利用するには、有効なサポート契約が結ばれている必要があります。有効なサポート契約の入手方法の詳細や、アカウントに関する質問については、担当営業にお問い合わせください。

未処理のサービス リクエストを確認する場合は、［**Service Center**］パネルで［**Service Center**］リンクをクリックして、［**View and manage service requests**］をクリックします。

サポート強化
すべての Avamar システムで、次のように ConnectEMC と Email Home を有効にすることを推奨します。

- ConnectEMC は、高い優先度を持つイベントに対するサービス リクエストを自動的に生成する。
- Email Home は、構成、容量、一般的なシステム情報をカスタマー サポートにメールで連絡します。

コメントと質問
ドキュメントの正確性、構成、品質を向上するため、お客様のご意見をお待ちしております。本書についてのご意見を DPAD.DOC.Feedback@emc.com にお送りください。

以下の情報を記載してください。

- 製品名とバージョン
- マニュアル名、パーツ番号、リビジョン（例：01）
- ページ番号
- その他、マニュアルの問題解決に役立つ情報

第 1 章

概要

本章は、次のトピックで構成されています。

データ保護の概要

Avamar には、VMware 仮想マシン上のデータを保護する基本的な方法が 2 つあります。

- イメージ バックアップ
- ゲスト バックアップ

注

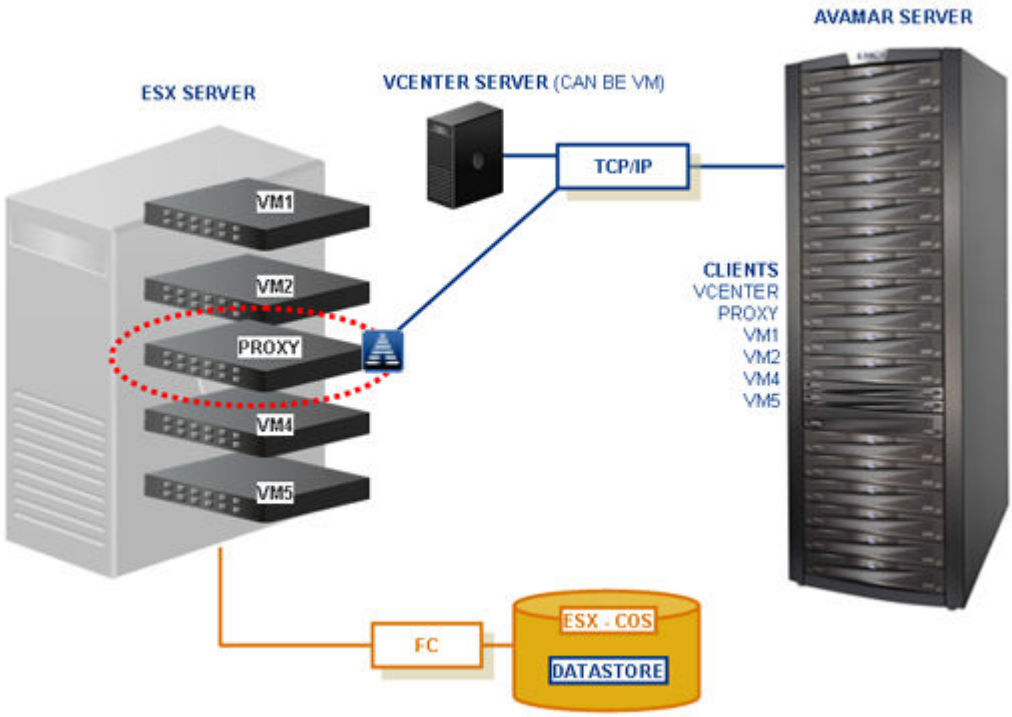
Avamar AUI は、スタンドアロン環境でのみサポートされます。

イメージ バックアップ

イメージ バックアップは、VADP（VMware vStorage API for Data Protection）を使用して仮想マシン データを保護します。

イメージ バックアップは、VMware vCenter Server と完全に統合され、仮想マシン クライアントを検出するため、バックアップ ジョブの効率的な一元管理が可能となります。

図 1 イメージ バックアップの概要図



プロキシ

イメージのバックアップとリストアには、vCenter 内にプロキシ仮想マシン クライアントの導入が必要です。

プロキシは Avamar ソフトウェアを Linux 仮想マシン内部で実行し、アプライアンス テンプレート（`.ova`）ファイルまたは Proxy Deployment Manager を使用して展開されます。

展開すると、プロキシにより次の処理が行われます。

- Microsoft Windows および Linux 仮想マシンのバックアップ（イメージ全体または特定のドライブ）
- Microsoft Windows および Linux 仮想マシンのリストア（イメージ全体または特定のドライブ）
- 個々のフォルダーとファイルの Microsoft Windows および Linux 仮想マシンへの選択的リストア

各プロキシは、どのような組み合わせでも同時に 8 件のバックアップ/リストア処理を実行することができます。

プロキシは、vCenter Server ドメインまたはサブドメインを除き、Avamar Administrator アカウント管理ツリーのすべての場所で許可されます。さらに、root ドメイン（/）へのプロキシをアクティブ化しないでください。アクティブ化すると、このアクションが原因でシステム移行時に問題が発生します。

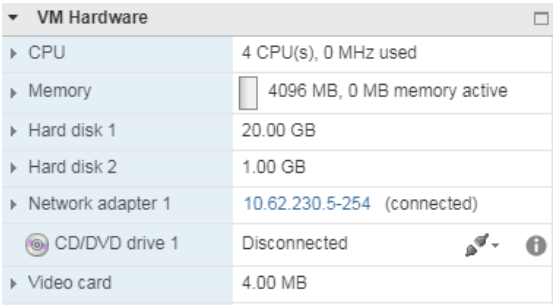
データセンター間でリストアを行う（あるデータセンターに導入されているプロキシを使用して別のデータセンターの仮想マシンにファイルをリストアする）ことは可能ですが、プロキシとターゲット仮想マシンが同じデータセンターにある場合によりも、リストアには相当な時間を要します。最高のパフォーマンスを実現するには、Proxy Deployment Manager を使用して、理想的な導入構成を行うことを推奨します。

プロキシ仮想マシンのデフォルトの仕様
次の図は、プロキシ仮想マシンのデフォルトの要件の概要を示しています。

注

ネットワーク アダプタに割り当てられている IP アドレスは、ゲスト ネットワークに属しています。

図 2 プロキシ仮想マシンのデフォルトの仕様



スナップショット

イメージ バックアップ プロセスには、仮想マシンのスナップショットの一時的な作成が必要です。

バックアップ時に仮想マシンが実行中の場合、このスナップショットはディスク I/O に影響し、仮想マシンが存在するデータストアのディスク領域を消費します。バックアップ中に仮想マシンが重いディスク I/O ワークロードを実行している場合は、スナップショットの作成と削除に長時間かかる可能性があります。

Avamar のイメージ バックアップは、次の仮想ディスク タイプをサポートします。

- フラット（バージョン 1 および 2）
- RDM（raw デバイス マッピング）、仮想モードのみ（バージョン 1 および 2）
- スパース（バージョン 1 および 2）

他の仮想ディスク タイプはサポートされていません。

サポートされるストレージ アーキテクチャ

イメージ バックアップでは、次のストレージ アーキテクチャを完全にサポートしています。

- VMFS または RDMS をホスティングしているファイバー チャネル SAN ストレージ
- iSCSI SAN ストレージ
- NFS

イメージ バックアップ システムの制限事項

イメージ バックアップには次のシステム全体の制限事項が適用されます。

データセンター、データストア、フォルダー、仮想マシンの名前に特殊文字を使用することはできない
vCenter ソフトウェアの既知の制限事項のため、データセンター、データストア、フォルダー、仮想マシンの名前に特殊文字が使用されていると、.vmx ファイルがバックアップに含まれません。

この問題は、特殊文字に%、&、*、$、#、@、!、\、/、:、*、?、"、<、>、|、;、'、+、=、?、~が使用される場合に発生します。
この問題の長期的な解決策は、この問題が解決されたバージョンに VMware ソフトウェアをアップグレードすることです。ただし、修正が VMware から提供されるまでは、データセンター、データストア、フォルダー、仮想マシンの名前を変更し、これらの特殊文字を使用しないようにしてください。

Avamar サーバーのアップグレードにプロキシの再起動が必要である
Avamar サーバー ソフトウェアをアップグレードした後で、このサーバーに接続されているすべてのプロキシを手動で再起動する必要があります。

ゲスト バックアップ

ゲスト バックアップは、物理マシンであるかのように Avamar クライアント ソフトウェアを仮想マシンにインストールし、Avamar サーバーにそのクライアントを登録してアクティブ化することによって仮想マシンのデータを保護します。特別な構成は必要ありません。

注

ゲスト バックアップによって保護されている仮想マシン クライアントを登録するとき、vCenter ドメインには登録しないでください。登録すると、管理者はその仮想マシンを Avamar Administrator で検索、あるいは管理することができなくなります。したがって、ゲスト バックアップによって保護されている仮想マシン クライアントは、他のドメインまたはサブドメイン（たとえば、/clients）に登録してください。

次の表は、仮想マシンに Avamar クライアント ソフトウェアをインストールする際の詳細な説明が記載されている参考資料の一覧です。

表 2 ゲスト バックアップのインストールに関する参考資料

クライアント	ドキュメント名
IBM AIX ファイル システム	「Avamar バックアップ クライアント ユーザー ガイド」
Linux ファイル システム： • Debian • CentOS • Red Hat • SUSE • Ubuntu	「Avamar バックアップ クライアント ユーザー ガイド」

表 2 ゲスト バックアップのインストールに関する参考資料 （続き）

クライアント	ドキュメント名
Novell NetWare ファイル システム	「Avamar バックアップ クライアント ユーザー ガイド」
UNIX ファイル システム： • FreeBSD • HP-UX • SCO Open Server と UnixWare • Solaris	「Avamar バックアップ クライアント ユーザー ガイド」
IBM AIX、Red Hat と SUSE Linux、Microsoft Windows でホスティングされている IBM DB2 データベース	「Avamar for IBM DB2 ユーザー ガイド」
Lotus Domino データベース	「Avamar for Lotus Domino ユーザー ガイド」
Mac OS X ファイル システム	「Avamar バックアップ クライアント ユーザー ガイド」
Microsoft Exchange データベース	「Avamar for Exchange VSS ユーザー ガイド」
Microsoft Office SharePoint インプリメンテーション	「Avamar for SharePoint VSS ユーザー ガイド」
Microsoft SQL Server データベース	「Avamar for SQL Server ユーザー ガイド」
Microsoft Windows ファイル システム	「Avamar バックアップ クライアント ユーザー ガイド」
IBM AIX、Red Hat と SUSE Linux、Sun Solaris、Microsoft Windows でホスティングされている Oracle データベース	「Avamar for Oracle ユーザー ガイド」

考慮事項

イメージ バックアップまたはゲスト バックアップのいずれかを使用して仮想マシン データを保護する際には、さまざまな考慮事項があります。

一般的な用途のガイドライン

vCenter でホストされる仮想マシンの場合、イメージ バックアップにより、最小限の労力で複数の仮想マシンを保護することができます。

Windows Vista/2008 以降の仮想マシンでは、イメージ バックアップは完全にアプリケーションとの整合性がとれていて、Microsoft Exchange、Microsoft Office SharePoint、Microsoft SQL Server を含むほとんどの用途に対して十分対応できます。ただし、イメージ バックアップは、VADP（VMware vStorage API for Data Protection）で提供される機能に制限されているため、導入によっては、VADP で提供されるものより高度な機能が必要な場合があります。そのような場合、ゲスト バックアップで提供される追加機能の方が、より良いソリューションとなる場合があります。

次の導入は、イメージ バックアップの代わりにゲスト バックアップを使用した方がよいことで知られています。

- Exchange DAG（データベース可用性グループ）
- SharePoint Server ファーム
- ログのトランケートが必要な SharePoint の導入

ゲスト バックアップは、vCenter でホストされない仮想マシンを保護するための唯一の方法です（デスクトップやラップトップなど）。

容易な導入

イメージ バックアップ：

- vCenter を活用して、仮想マシンを検出し、Avamar サーバーにまとめて追加可能
- ある程度の初期セットアップと構成が必要

ゲスト バックアップ：

- Avamar クライアント ソフトウェアに必要なオペレーティング システムを実行している仮想マシンをサポート
- DB2、Exchange、Oracle、SQL Server データベースなどのアプリケーションをサポート
- ほとんどの既存のバックアップ スキームに容易に適合し、日常のバックアップ手順は変わらない
- クライアント ソフトウェアは、個々にインストールが必要で、各仮想マシン内部で管理される

効率性

イメージ バックアップ：

- ある程度の重複排除効率性を提供
- バックアップ時にゲスト仮想マシンの CPU、RAM、ディスク リソースを消費しない
- バックアップ時に ESX Server の CPU、RAM、ディスク リソースを消費する

ゲスト バックアップ：

- 最高レベルのデータ重複排除効率性を提供
- バックアップ生時のゲスト仮想マシンの CPU、RAM、ディスク リソースの消費量はわずかである
- バックアップ時に VMware ESX Server の CPU、RAM、ディスク リソースを消費しない

バックアップおよびリストア

イメージ バックアップ：

- イメージ バックアップは現在 VMware によってサポートされているすべてのマシンに対してサポートされている
- バックアップは、仮想マシン イメージ全体（すべてのドライブ）または選択したドライブ（`.vmdk` ファイル）から構成可能
- 個々のフォルダーとファイルのリストアは、Windows および Linux 仮想マシンの両方に対してサポートされている
- バックアップは最適化されない（一時ファイル、スワップ ファイルなどを含む）
- 未使用のファイル システムの領域はバックアップされる
- 仮想マシンは、Avamar サーバーへのネットワーク接続が不要。
- 仮想マシンは、バックアップの発生のために稼働中である必要はない

ゲスト バックアップ：

- バックアップは、高度に最適化される（一時ファイル、スワップ ファイルなどは含まれない）
- バックアップは、高度にカスタマイズ可能（すべての包含および除外機能をサポート）

- データベース バックアップは、トランザクション ログ トランケートおよびその他の高度な機能をサポート
- 未使用のファイル システムの領域はバックアップされない
- 個々のフォルダーおよびファイル リストアは、サポート対象のすべての仮想マシンに対してサポートされている（Linux や Windows だけではない)
- バックアップとリストア ジョブは前処理および後処理スクリプトを実行可能
- 仮想マシンは、Avamar サーバーへのネットワーク接続が必要。
- 仮想マシンは、バックアップの発生のために稼働中でなければならない

VMware に関する必要な知識

イメージ バックアップには VMware に関するある程度の知識が必要です。インテグレーターは、お客様のサイトで使用されている vCenter トポロジーの知識（すなわち、どの VMware ESX Server が各データストアをホスティングしているか、どのデータストアが各仮想マシンのデータを保存しているか）が必要です。また、管理者権限で vCenter にログインできる必要もあります。

ゲスト バックアップとリストアには、高度なスクリプト作成または VMware に関する知識は必要ありません。

イメージ バックアップとゲスト バックアップの両方の使用

仮想マシンは、ゲスト バックアップとイメージ バックアップの両方で保護することができます。たとえば、日次ゲスト バックアップを特定のファイルの保護に使用し、マシン全体の保護には、不定期またはオン デマンド フル イメージ バックアップを使用することが可能です。このスキームにより限られたバックアップ ウィンドウでさまざまな状況に対応できます。

イメージ バックアップおよびゲスト バックアップの両方の使用をサポートして、同一の仮想マシンを保護するためには、重複するクライアント名を許可するように Avamar MCS を構成する必要があります。

更新ブロック追跡

更新ブロック追跡は、仮想マシン上のどのファイル システム ブロックがバックアップとバックアップの間に変更されたかを追跡する VMware の機能です。

更新ブロック追跡により、仮想マシンの初期バックアップ中に仮想ディスク上の未使用スペースが特定され、前のバックアップ以降変更されていないスペースが空になります。Avamar データ重複排除も類似の機能を果たします。ただし、この機能を使用すると、バックアップ プロセスの早い段階で貴重な I/O が減少します。更新ブロック追跡は、SAN 接続性が使用できない場合、パフォーマンスを大幅に向上させます。

更新ブロック追跡が有効化されていない場合、各仮想マシンのファイル システム イメージは、バックアップごとに完全に処理されるため、バックアップ ウィンドウが許容できないレベルの長さとなり、バックエンド ストレージの読み取り/書き込みアクティビティが過剰になります。

更新ブロック追跡は、リストア処理中の不要な書き込みを自動的に除去することにより、仮想マシンを最新のバックアップ イメージにリストア（「ロール バック」）する際に要する時間を短縮することもできます。

更新ブロック追跡は、次のタイプの仮想ディスク フォーマットを使用する次のタイプの仮想マシンでのみ利用可能です。

- 仮想マシン バージョン 7 以降
  仮想マシンの前のバージョン 4 は、一般に、ESX 3.X のホスト、および ESX 3.X と 4.0 のホストをサポートするテンプレートから展開された仮想マシンで使用されます。基盤の VMware ESX ホストがアップグレードされるとき、仮想マシンのバージョンは変更されません。多くの市販

のアプライアンスが、VMware ESX 3.x ホストへの展開を見越してバージョン 4 を採用しています。

vCenter バージョン 4 では、バージョン 4 の仮想マシン ハードウェアをバージョン 7 の仮想マシン ハードウェアにアップグレード可能です。このアップグレードは元に戻せないため、仮想マシンは、以前のバージョンの VMware ソフトウェア製品と互換性がなくなります。詳しくは、vCenter オンライン ヘルプを参照してください。

- ディスクは物理互換 RDM にはなれない
- 同じディスクを複数の仮想マシンにマウントできない
- 仮想マシンは、スナップショットをサポートする構成であることが必要

更新ブロック追跡を有効にしても、次のいずれかのアクションが仮想マシンで発生するまで、有効になりません。再起動、電源オン、中断後の再開、移行。

イメージ バックアップでの仮想マシンの停止

イメージ バックアップでは、VADP（VMware vStorage API for Data Protection）が提供する機能以外に追加の仮想マシンの停止機能は提供されません。

イメージ バックアップを実行する前に、以下の 3 レベルの仮想マシンの停止が可能です。

- クラッシュ コンシステント停止
- ファイル システム コンシステント停止
- アプリケーション コンシステント停止

クラッシュ コンシステント停止はお勧めできるレベルの停止ではありません。バックアップ中の仮想ディスク イメージが、物理コンピューターへの電源を切った場合に発生する現象と一致するからです。ファイル システムの書き込みは、電源が遮断されたときに進行中の場合とそうでない場合があります。この問題のため、常に、ある程度のデータ消失の可能性があります。

ファイル システム コンシステント停止は、ディスクがバックアップされる前に仮想マシンがファイル システムの書き込みを完了できるため、より望ましい方法です。このレベルの停止は、Windows VSS（Volume Snapshot Service）サービスを提供でき、VMware Tools を実行している Windows 仮想マシンでのみ使用可能です。

アプリケーション コンシステント停止は、最も望ましいレベルの停止です。ファイル システム コンシステント停止のメリットに加え、アプリケーションは、バックアップが発生したという通知を受けるため、トランザクション ログをクリアすることができます。

アプリケーション コンシステント停止は、Windows Vista/2008、およびそれ以降の VMware ツールを実行している仮想マシンでのみ使用可能です。

AWS（Amazon Web Services）でのイメージ バックアップ/リカバリのサポート

Avamar プロキシは、VMware Cloud on AWS でのイメージのバックアップ/リストアをサポートします。

Avamar を使用して、すべての VMware オンプレミスと AWS 環境全体で VMware のワークロードをシームレスに導入し管理することができます。

次の点を考慮してください。

- VMware vSphere 6.5 以上が必要。
- VMware Cloud on AWS 上では、ESXi ホストと Avamar プロキシ間のネットワーク接続がない。通信には、vCenter が必要。

- VMware Cloud on AWS でのユーザー権限には制限がある。
- ワークロード サービス プールに存在する仮想マシンのサポート。
- Avamar Virtual Edition での SSO サービスを使用した VMware タグのサポート。

制限事項

次の機能はサポートされていません。

- アプリケーション コンシステントなバックアップ
- NSX-V を使用している場合のイメージ レベルのバックアップからのファイル レベルのリストア。NSX-T を使用している場合、これは制限されない点に注意してください。
- Proxy Deployment Manager。プロキシを手動で導入する必要がある
- イメージ レベル バックアップのインスタント アクセス リカバリ
- 非常時のリストア（vCenter をバイパスして ESXi ホストに直接行うイメージ リストア）
- NBD または NBDSSL 転送モードを使用するイメージ レベルのバックアップ/リストア
- 高度なポリシー ベースの、Avamar を使用した MS SQL 向けデータ保護
- MS-SQL および MS-Exchange 向けアプリケーション認識のイメージ バックアップ
- データセンターがフォルダーの下にある場合のイメージのバックアップ/リストア
- データ除外
- デュアル スタックまたは IPv6 専用に構成されているプロキシ アプライアンス
- NBD、NBDSSL、SAN。HotAdd のみがサポートされる
- 動的なポリシーの VMware タグ ベースのルール選択基準
- 新規 vApp へのリストア
- IPV6
- 仮想マシン テンプレートのバックアップ

第 2 章

構成とセットアップ

本章は、次のトピックで構成されています。

ベスト プラクティス

システムを構成する際は、これらのベスト プラクティスに従ってください。

VMware ESX および vCenter 証明書を検証する
VMware ESX および vCenter 用の DNS 名と一致する信頼できるプロバイダーからの適切に登録された証明書を使用します。

完全修飾 ESX Server のホスト名を使用する
新しい ESX Server を vCenter 環境に追加する際は、ESX Server に（IP アドレスやシンプルなホスト名ではなく）完全修飾ホスト名を付ける VMware 推奨事例に従います。完全修飾ホスト名以外を使用すると、不正な SSL 証明書処理により、ネットワーク接続に障害が発生する可能性があります。

変更率が高いクライアントに関する推奨事項
データベース ホストなどの変更率の高いクライアントを保護する場合は、ゲスト バックアップを使用するか、イメージ バックアップを Data Domain システムに格納します。

プロキシの間接 root ログインを使用する
Avamar 18.1 以降では、プロキシの直接 root ログインは使用できなくなりました。その代わりに、手順で root アクセスが必要な場合は、管理者ユーザーとしてログインし、**su -**と入力して root ユーザーに変更します。この動作は、Avamar サーバーの既存の root ログイン設定に対応しています。

ネットワーク設定
リストア処理の後にネットワーク設定をリストアしない場合は、操作が完了した後に、必ずネットワーク設定を手動で構成してください。

（オプション）複数の vCenter のサポートを構成する

Avamar サーバーでは、最大 15 個の vCenter がサポートされ、追加の構成は必要ありません。しかし、15 個を超える vCenter を保護する場合、または Avamar サーバーを旧バージョンからアップグレードした場合は、手動による構成が必要になります。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
   - シングル ノード サーバーには、admin としてサーバーにログインします。
   - マルチ ノード サーバーの場合、admin としてユーティリティ ノードにログインします。
2. 次のコマンドを入力して、MCS を停止します。

   ```
   dpnctl stop mcs
   ```

3. UNIX テキスト エディターで`/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml`を開きます。
4. `max_number_of_vcenters`の設定が、保護対象の vCenter の数以上であることを確認します。
   a. `max_number_of_vcenters`エントリー キーを見つけます。
   b. `max_number_of_vcenters`の設定を **num** に変更します。num は、保護対象の vCenter の数以上の整数です。

      例えば、この設定によって、15 個もの vCenter をこの Avamar サーバーで保護できます。

```
<entry key="max_number_of_vcenters" value="15" />
```

5. 50 個以上の vCenter を保護する場合は、次の手順で `maxJavaHeap` の設定も**-Xmx2G** に変更します。
   a. `maxJavaHeap` エントリー キーを見つけます。
   b. 次のように `maxJavaHeap` の設定を**-Xmx2G** に変更します。

      ```
      <entry key="maxJavaHeap" value="-Xmx2G" />
      ```

      `maxJavaHeap` パラメーターは、デフォルトで 2G になっています。次のコマンドを使用して、パラメーターを変更します：

      ```
      entry key="maxJavaHeap" value="-Xmx3G" merge="keep"
      ```

6. `mcserver.xml` を終了して、変更を保存します。
7. 次のコマンドを入力して、MCS およびスケジューラを開始します。

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

Avamar Administrator ソフトウェアのインストール

Windows コンピューターに Avamar Administrator ソフトウェアをインストールします。

手順

1. Web ブラウザを開き、次の URL を入力します。

   ```
   https://Avamar_server/dtlt/home.html
   ```

   ここで、Avamar_server は Avamar サーバーの DNS 名または IP アドレスです。

   ［**Avamar Web Restore**］ページが表示されます。
2. ［**Downloads**］をクリックします。
3. 32 ビットの Windows ソフトウェア インストール パッケージを含むフォルダーに移動します。
4. JRE（Java Runtime Environment）インストール パッケージを探します（通常はフォルダーの最後のエントリーにある）。
5. クライアント コンピューターの JRE が Avamar サーバーでホストされている JRE よりも古い場合は、次の手順で新しい JRE をダウンロードして、インストールします。
   a. ［**jre-version-windows-i586-p**］リンクをクリックします。
   b. インストール ファイルを開くか、またはファイルをダウンロードし、その後保存した場所からそのファイルを開きます。
   c. 画面の指示に従って JRE のインストールを完了します。
6. ［**AvamarConsoleMultiple-windows-x86-version.exe**］リンクをクリックします。
7. インストール ファイルを開くか、またはファイルをダウンロードし、その後保存した場所からそのファイルを開きます。
8. 画面の指示に従って Avamar Administrator ソフトウェアのインストールを完了します。

vCenter-to-Avamar 認証の構成

保護対象の各 vCenter に vCenter-to-Avamar 認証を構成します。

vCenter-to-Avamar 認証を構成する上で最も安全な方法は、vCenter 認証証明書を Avamar MCS キーストアに追加することです。これは、保護対象の各 vCenter で実行する必要があります。

vCenter 認証証明書を Avamar MCS キーストアに追加することを希望しない場合は、すべての vCenter-to-Avamar MCS 通信で証明書認証を無効化する必要があります。

vCenter 認証証明書を MCS キーストアに追加

vCenter 認証証明書を MCS キーストアに追加して、vCenter-to-Avamar 認証を構成します。この処理は、保護対象の各 vCenter で実行します。

手順

1. 管理者権限で Avamar AUI にログインします。Web ブラウザを開き、次の URL を入力します。

   `https://Avamar_server/aui`

   ここで、Avamar_server は Avamar サーバの DNS 名または IP アドレスです。

   注

   お使いの環境が HTTPS 証明書の検証要件を満たしていない場合は、証明書の検証は失敗し、パッケージのダウンロードを続行するかどうかの確認を求めるエラー メッセージが表示されます。証明書の検証を無視すると、セキュリティの問題が発生する可能性があります。

   a. [**Avamar Username**] フィールドに、管理権限を持つユーザー名を入力します。

   b. [**Avamar Password**] フィールドに、この管理ユーザーのパスワードを入力します。

   c. [**Auth Type**] に [**Avamar**] を選択します。

   d. [ログイン] をクリックします。

2. 左側の AUI ナビゲーション ペインで、[≫] をクリックし、次に [**Administration**] > [**System**] をクリックします。

   [**System**] ウィンドウが表示されます。

3. [**Certificate**] タブを選択し、[**Trust Certificate**] タブの下の [＋] をクリックします。

   [**Import Certificate**] ダイアログ ボックスが表示されます。

4. 次の情報を指定して、vCenter 信頼証明書をインポートします。

   a. [**Base Information**] ウィンドウで、次の操作を実行します。

      a. vCenter 証明書のエイリアス名を指定します。

      b. [**BROWSE**] ボタンをクリックし、vCenter 証明書を参照してインポートします。

      c. [**NEXT**] をクリックします。

   b. [**Validation**] ウィンドウで、vCenter の IP アドレス、ポート番号を **`443`** と指定して、[**VALIDATE**] ボタンをクリックします。

［**Validation Result**］ポップアップ ウィンドウが表示され、検証に成功したか失敗したかを確認できます。検証に失敗した場合は、再度入力を確認します。

5. ［**FINISH**］ボタンをクリックします。

   正常にインポートされた vCenter 証明書が［**Trust Certificate**］タブに表示されます。［View］アイコンと［Delete］アイコンをクリックすると、vCenter 証明書を表示および削除できます。

注

vCenter 証明書を MCS キーストアにインポートした後、MCS を再起動する必要はありません。

MCS 証明書認証の無効化

vCenter 認証証明書を Avamar MCS キーストアに追加することを希望しない場合は、すべての vCenter-to-Avamar MCS 通信で証明書認証を無効化する必要があります。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
   - シングル ノード サーバーには、admin としてサーバーにログインします。
   - マルチ ノード サーバーの場合、admin としてユーティリティ ノードにログインします。
2. 次のコマンドを入力して、MCS を停止します。

   ```
   dpnctl stop mcs
   ```

3. UNIX テキスト エディターで`/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` を開きます。
4. `ignore_vc_cert` エントリー キーを見つけます。
5. `ignore_vc_cert` の設定を **`true`** に変更します。

   ```
   <entry key="ignore_vc_cert" value="true" />
   ```

6. `mcserver.xml` を終了して、変更を保存します。
7. 次のコマンドを入力して、MCS およびスケジューラを開始します。

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

専用の vCenter ユーザー アカウントの作成

厳密に Avamar でのみ使用する専用の個別のユーザー アカウントを各 vCenter に設定することを強く推奨します。

別個の vCenter ユーザー アカウントを使用することにより、vCenter ログを調べることが必要になった場合、不明な点がより明確となります。「Administrator」のような一般的なユーザー アカウントを使用すると、どのアクションが Avamar サーバーと実際に連携または通信しているかが不明になり、将来トラブルシューティングを行う際に障害になる可能性があります。

注

保護対象の各 vCenter で、最上位（root）レベルにユーザー アカウントを追加する必要があります。他のレベル（例えば、データセンターのレベル）でユーザー アカウントを作成すると、バックアップが失敗します。

表 3 最低限必要な vCenter ユーザー アカウント権限

権限の種類	必要な権限
アラーム	• アラームの作成 • アラームの編集
データストア	• 領域の割り当て • データストアの参照 • データストアの構成 • 低レベルのファイル操作 • データストアの移動 • データストアの削除 • ファイルの削除 • データストアの名称変更
拡張機能	• 拡張機能の登録 • 拡張機能の登録解除 • 拡張機能のアップデート
フォルダ	• フォルダを作成
グローバル	• タスクのキャンセル • メソッドの無効化 • メソッドの有効化 • ライセンス • イベントのログ • カスタム属性の管理 • カスタム属性の設定 • 設定
ホスト	• 構成> ストレージ パーティション構成
ネットワーク	• ネットワークの割り当て • 構成
リソース	• 仮想マシンのリソース プールへの割り当て
セッション	• セッションの確認
タスク	• タスクの作成

表 3 最低限必要な vCenter ユーザー アカウント権限 （続き）

権限の種類	必要な権限
	• タスクの更新
仮想マシン-構成	• 既存ディスクの追加 • 新しいディスクの追加 • デバイスの追加または削除 • 拡張 • CPU 数の変更 • リソースの変更 • 管理される構成 • ディスク変更の追跡 • ディスクのリース • 仮想ディスクの拡張 • ホスト USB デバイス • メモリ • デバイス設定の変更 • Raw デバイス • パスから再ロード • ディスクの削除 • 名前の変更 • ゲスト情報のリセット • 注釈の設定 • 設定 • Swapfile の配置 • 仮想マシン互換性のアップグレード
仮想マシン-ゲスト操作	• ゲスト操作の変更 • ゲスト操作のプログラム実行 • ゲスト操作のクエリー
仮想マシン-インタラクション	• コンソールの対話 • DeviceConnection • VIX API によるゲスト オペレーティング システムの管理 • 電源オフ • 起動 • リセット • VMware Tools のインストール
仮想マシン-インベントリ	• 既存から作成

表 3 最低限必要な vCenter ユーザー アカウント権限 （続き）

権限の種類	必要な権限
	• 新規作成 • 登録 • 削除 • 登録解除
仮想マシン-プロビジョニング	• ディスク アクセスの許可 • 読み取り専用ディスク アクセスの許可 • 仮想マシン ダウンロードの許可 • 仮想マシンの複製 • テンプレートとしてマーク
仮想マシン-スナップショット管理	• スナップショットの作成 • スナップショットの削除 • スナップショットに戻る
vApp	• エクスポート • インポート • vApp アプリケーションの構成

VMware vCenter クライアントの登録または追加

保護対象の各 vCenter をの Avamar クライアントとして追加する必要があります。

クライアント登録は、Avamar サーバーで vCenter クライアントの ID を確立するプロセスです。Avamar がクライアントを「認識」すると、固有 CID（クライアント ID）を割り当てます。この CID がアクティベーションの際にクライアントに送信されます。

クライアントを追加して登録したら、ドメインとグループのシステムにクライアントを追加できます。これにより高度なコントロールが可能となります。例えば、特定のデータセット、スケジュール、保存ポリシーを割り当てることができます。ただし、数多くのクライアントを追加するには、非常に時間がかかります。

手順

1. 左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］をクリックします。
2. ドメイン ツリーで、クライアントの vCenter ドメインまたはサブドメインを選択します。

   サブドメイン クライアントを選択するには、［**Include Sub-domain**］スイッチをオンに切り替えます。
3. ［**ADD CLIENT**］の横にある［ ⋮ ］をクリックして、［**Add VMware vCenter**］を選択します。

   ［**New vCenter Client**］ウィザードが表示されます。

4. ［**New Client Name or IP**］フィールドに、クライアント名を入力して、［**NEXT**］をクリックします。

   ［**vCenter Information**］パネルが表示されます。

5. ［**vCenter Information**］パネルで、vCenter について次の情報を入力します。

   a. ［**User Name**］フィールドに、vCenter Server 管理者のユーザー アカウント名を入力します。

   b. ［**Password**］フィールドに、vCenter ユーザー アカウントのパスワードを入力します。

   c. ［**Verify Password**］フィールドに、vCenter ユーザー アカウントのパスワードを再度入力します。

   d. ［**Port**］フィールドに、vCenter の Web サービス リスナー データ用ポート番号を入力します。

      デフォルト設定は、443 です。

   e. ［**NEXT**］をクリックします。

［**Advanced**］パネルが表示されます。このパネルでは、ルールによる動的な仮想マシンのインポートまたは更新ブロック追跡を含む、次の自動検出機能を有効にすることができます。

6. ルールによる動的な仮想マシンのインポートを有効化するには、［**Enable Dynamic VM import by rule**］を選択して、次のステップを実行します。

注

仮想マシンが自動検出されると、Avamar ソフトウェアでユーザー定義のルールを使用して、自動検出された仮想マシンを Avamar ドメインにマップします。ユーザー定義のルールは、バックアップ ポリシーを自動検出された仮想マシンに自動的に割り当てる用途にも使用されます。

- ルールを追加するには、以下の手順を実行します。

  a. ［**ADD RULE**］をクリックします。

  b. ［**Rule**］フィールドで、リストからルールを選択します。

  c. ［**Domain**］フィールドで、自動検出された仮想マシンを含める必要のあるドメインを入力します。
  ここで入力したドメインが存在しない場合は、自動的に作成されます。

- ルールを作成するには、次の手順を実行します。
  ルールを使用して、自動検出された仮想マシンをドメインに自動的にマッピングして、自動検出された仮想マシンにバックアップ ポリシーを割り当てます。ルールでは、1 つまたは複数のフィルタリング メカニズムを使用して、仮想マシンがルール下で認定されるかどうかを決定します。

  a. ［**CREATE RULE**］をクリックします。

  b. ［**Rule Name**］フィールドに、ルールの名前を入力します。

  c. ［**Match Type**］フィールドで、ルールがリストにあるフィルター メカニズムの一部に一致する必要があるのか（［**Any**］）、またはすべてに一致する必要があるのか（［**All**］）を選択します。
  この選択によって、仮想マシンを選択する複数の異なるフィルターを設定でき、設定したフィルターが相互に作用して正しい仮想マシンを選択する方法を決定できます。たとえば、仮想マシンを選択するために仮想マシンのフォルダーのパスを使用するフィルターと、仮想マシンの命名規則を使用する別のフィルターを作成することができます。

つまり、このオプションは、次のようにこのルール下に含める仮想マシンの決定に使用できます。

- 定義済みのフォルダー パスにあり、命名規則にも従っている仮想マシンのみを含めるには［**All**］を選択します。このステップでは、フォルダー パスにあるが、命名規則に従っていない仮想マシンを除外し、また命名規則に従っているがフォルダーのパスにない仮想マシンを除外します。
- 仮想マシンのフォルダー パスにある仮想マシンまたは命名規則に従っている仮想マシンのいずれかを含めるには、［**Any**］を選択します。

d. ［**Filter**］フィールドで、フィルター タイプを選択します。
たとえば、仮想マシンの命名規則を使用するフィルターを作成するには、［**VM Name**］を選択し、vCenter 仮想マシンのタグを使用するフィルターを作成するには、［**VM Tag**］を選択します。

注

［**VM Tag**］の選択は、vCenter 6.0 以降でのみ利用可能です。

---

e. ［**Operator**］フィールドで、オペランドを選択します。
たとえば、フィルター タイプに［**VM Name**］を選択し、オペランドに［**begins with**］を選択した場合は、フィルター テキストで始まるすべての仮想マシンが選択されます。

f. ［**Value**］フィールドに、フィルター テキストを入力します。
たとえば、名前がテキスト文字列 **HR_**で始まるすべての仮想マシンを選択するフィルターを作成するには、フィルター タイプに［**VM Name**］、オペランドに［**begins with**］を選択し、フィルター テキストに **HR_**と入力します。

g. 追加のフィルターを作成するには、プラス記号（［**+**］）をクリックします。
このステップによって、フィルターのリストに行が追加されます。既存の行を削除するには、［**Delete**］をクリックします。

h. ［**SUMBIT**］をクリックします。
タグに変更を加えると、変更が有効になるまで最大で 12 時間かかる可能性があります。このため、タグの編集は慎重に行うか、vCenter が Avamar サーバと自動同期する、同期化された vCenter の操作を実行します。

ルールの作成のベスト プラクティスは、ルールが相互に排他的であることを確認し、1 台の仮想マシンを複数のルール下で認定される状況が起こらないようにすることです。

- 更新ブロック追跡を有効にするには、［**Enable Change Block Tracking**］を選択します。
更新ブロック追跡が有効になっていない場合、各仮想マシン イメージはバックアップごとに完全に処理され、バックアップ ウィンドウが長くなるか、あるいはバックエンド ストレージの読み取りおよび書き込みアクティビティが過剰になることがあります。

  更新ブロック追跡を有効にしても、次のいずれかのアクションが仮想マシンで発生するまで、有効になりません。

  - 再起動
  - 起動
  - 中断後の再開
  - 移行

7. ［**NEXT**］をクリックします。

［**Optional Information**］パネルが表示されます。

8. （オプション）連絡先名、電話番号、メール、場所など、オプションの連絡先情報を入力し、［**NEXT**］をクリックします。

   ［**Summary**］パネルが表示されます。

9. クライアントのサマリー情報を確認して、［**ADD**］をクリックします。

   ［**Finish**］パネルが表示されます。

10. ［**FINISH**］をクリックします。

結果

AUI で vCenter Client を追加すると、次のことが自動的に行われます。

- vCenter Client をデフォルト グループに追加。
  ただし、このクライアントは通常の Avamar クライアントのようにはアクティブ化されません。したがって、デフォルト グループに代わってバックアップが実行されることはありません。
- vCenter Server のドメイン階層の作成。
- その vCenter Server ドメイン階層内に VirtualMachines サブドメインを作成。
- Default Virtual Machine Group を作成します。
  このグループは、ターゲット仮想マシンに対してスケジュール設定されたバックアップを実行します。このグループは、最初に仮想センター ドメインを削除しない限り削除できません。

vCenter が通常のバックアップ クライアントとしてすでに登録されている場合は（例えば、ゲスト レベルのバックアップをサポートするため）、同一の vCenter を vCenter Client として追加しようとすると失敗します。これは、同一のクライアントを 2 度登録することができないためです。この場合は、次の手順を実行する必要があります。

1. AUI にある既存の vCenter Client を破棄します。
2. vCenter を vCenter Client として追加します（この処理手順を使用）。
3. 破棄した vCenter Client を通常のクライアントとして再度招待し、vCenter Server からのゲスト レベルのバックアップをサポートします。

仮想マシンの自動検出

Avamar リリース 7.4 では、vCenter に追加されている仮想マシンを自動検出するように Avamar vCenter クライアントを構成することができます。仮想マシンが自動検出されると、Avamar ソフトウェアでユーザー定義のルールを使用して、自動検出された仮想マシンを Avamar ドメインにマップします。ユーザー定義のルールは、バックアップ ポリシーを自動検出された仮想マシンに自動的に割り当てる用途にも使用されます。

新しい仮想マシンの自動検出に加えて、vCenter から別の vCenter への仮想マシンの vMotion も Avamar ソフトウェアで自動検出されます。Avamar で仮想マシンをホストしている新しい vCenter を設定する場合、この仮想マシンは元の vCenter クライアントから同じユーザー定義のルールを使用している新しい vCenter クライアントへ自動的に移動して、ドメインとバックアップ ポリシーを割り当てます。仮想マシンが vCenter から削除された場合、vCenter クライアントから自動的に削除されます。

自動検出機能は、vCenter 5.5 以降のリリースでサポートされています。ただし、ルールで VM タグを使用するには、vCenter はリリース 6.0 以上である必要があります。vCenter ではなく ESXi ホストを保護している場合、仮想マシン名とルート フォルダーのみがルールでサポートされます。

タグの変更がイベントによってトリガーされていないため、仮想マシンのタグを変更する場合は、すぐに vCenter 操作と同期して、タグの変更を有効にします。この操作を実行しない場合は、次のような状況で変更が有効になります。

1. MCS（Management Console Server）を再起動する。
2. 12 時間毎のフル スキャン スケジュールを待機する。
3. ルール ドメイン マッピングの追加または削除など、vCenter を更新する。

注

Avamar では、テンプレート VM の自動検出をサポートしていません。

仮想マシンの自動検出のためのドメイン マッピング規則

ドメイン マッピング規則は、新規または移動済みの仮想マシンを自動検出中に Avamar ドメインにマッピングするために使用されます。

［**Enable dynamic VM import by rule**］が vCenter クライアントの構成中に選択された場合に、ルールが選択されるか、または作成されます。

役割の作成

ルールを使用して、自動検出された仮想マシンをドメインに自動的にマッピングして、自動検出された仮想マシンにバックアップ ポリシーを割り当てます。ルールでは、1 つまたは複数のフィルタリング メカニズムを使用して、仮想マシンがルール下で認定されるかどうかを決定します。

vCenter クライアントの構成時にルールを適用または作成することができます。

ルール作成の詳細については、「Avamar Administration Guide」を参照してください。

プロキシの導入

イメージ バックアップで保護する各 vCenter で 1 個以上のプロキシを導入します。

DRS（Distributed Resource Scheduler）対応クラスタにプロキシが導入される場合は、このクラスタで Storage vMotion を使用して、プロキシを移動できます。プロキシを別のストレージに移行している間、そのプロキシで管理されているジョブは、リスクにさらされます。HotAdd は、DRS クラスターに配置されているプロキシでは動作しません。そのため、導入された Avamar プロキシ仮想マシンの DRS を無効化します。

詳細については、VMware のドキュメントを参照してください。

Proxy Deployment Manager

Proxy Deployment Manager は、vCenter 環境での Avamar プロキシの導入および管理において管理者を支援する機能です。

Proxy Deployment Manager は、プロキシを導入するための推奨方法です。必要に応じて、手動によるプロキシ導入も引き続きサポートされています。

プロキシ導入について

Proxy Deployment は、各 vCenter で導入される必要があるプロキシ数に関する推奨事項と、プロキシごとに推奨される ESX ホストの場所を提供することにより、管理者のプロキシ導入を支援します。

推奨事項を生成する際に、Proxy Deployment は、仮想インフラストラクチャの静的ポイント インタイム解析を実行します。この解析は、仮想マシン数、データストア数、各データストアでホストされる仮想マシン数など、仮想インフラストラクチャに関するデータを収集します。

ユーザーは、自分のサイトについてデータ変更率およびバックアップ ウィンドウの期間を指定します。

その後、Proxy Deployment は、これらの仮想マシンのバックアップをバックアップ ウィンドウによって割り当てられた時間内で行うのに必要な、最適なプロキシ数を計算します。また、Proxy Deployment は、データストアと VMware ESX ホスト トポロジーを考慮し、すべてのデータストアが保護されるように、プロキシごとに最適な VMware ESX ホストの場所を提示します。

この計算されたプロキシ導入トポロジーは、推奨事項として提供されます。この推奨事項は、提供されたとおりに受け入れることも、特定のサイト要件を満たすように変更することもできます。

プロキシを導入する前に、推奨されるプロキシごとに、次の内容を指定して構成する必要があります。

- プロキシ名
- プロキシが常駐する Avamar サーバー ドメイン
- プロキシ IP アドレス
- データストアの割り当て
- ネットワーク設定：
  - 使用する既存の仮想ネットワーク
  - DNS サーバー
  - ネットワーク ゲートウェイ
  - ネットワーク マスク
  - NTP

すべてのプロキシが構成された後で、✓をクリックすると、指定された構成設定で、プロキシ仮想マシンが作成されます。

新しいプロキシ導入の推奨事項はいつでも生成できます。これは、仮想インフラストラクチャで大幅な変更が発生した場合に、プロキシ導入を定期的に再評価し、最適化するのに役立ちます。

考慮事項とベスト プラクティス

Proxy Deployment は、ほとんどのお客様環境との幅広い互換性を確保することを意図して設計されています。そのため、一般的なお客様環境、およびそれらの環境における妥当なプロキシ機能に関する特定の設計上の前提条件を作成する必要がありました。これらの設計上の前提条件を理解すれば、サイトでのプロキシ導入をさらに最適なものにできる Proxy Deployment の推奨事項について、より良く理解できるようになります。また、いくつかのベスト プラクティスについても説明します。

データ変更率

データ変更率は、バックアップ間で実際に変更するクライアント ファイル システムの割合です。データ変更率は、必要な仮想マシンすべての正常なバックアップを、バックアップ ウィンドウによって割り当てられた時間内で行うのに必要となるプロキシ数に直接影響します。バックアップするデータが多くなればなるほど、時間、プロキシ、またはその両方がさらに必要になります。

経験に即したフィールド データが示すクライアントのデータ変更率が日常的に 1 日あたり 3～4%である場合でも、Proxy Deployment は、デフォルトで、クライアントのデータ変更率を 1 日あたり 12%と想定します。設計上の前提条件としてこの 12%という数字を意図的に使用して、バッファーを提供します。

サイトでのクライアント データ変更率が常にこれらの想定値よりも低いか高い場合は、必要に応じてプロキシを追加または削除することができます。バックアップ ウィンドウを短くしたり、長くしたりすることもできます。

プロキシ データ取得率

プロキシ データ取得率は、必要な仮想マシンすべての正常なバックアップを、バックアップ ウィンドウによって割り当てられた時間内で行うのに必要となるプロキシ数に直接影響する、もう 1 つのパラメー

ターです。デフォルトで、Proxy Deployment は、各プロキシが 8 個のコンカレント バックアップ ジョブを実行し、1 時間あたり 500 GB のデータを処理可能であることを想定しています。

想定されるプロキシ データ取得率である 1 時間あたり 500 GB は、非常に控えめな見積もりですが、各お客様サイトにおける様々な要因が、実際のプロキシ データ取得率に直接影響します。それらの要因には、次のものがあります。

- Avamar サーバー アーキテクチャ（vCenter でホストされるバックエンド ストレージと仮想 Avamar サーバー用に Data Domain システムを使用する物理 Avamar サーバー）
- プロキシ ストレージに使用するストレージ メディアのタイプ
- ネットワーク インフラストラクチャおよび接続速度
- SAN インフラストラクチャおよび接続速度

サイトでのプロキシ データ取得率が 1 時間あたり 500 GB より常に低いか高い場合は、必要に応じて、プロキシを追加または削除することができます。バックアップ ウィンドウを短くしたり、長くしたりすることもできます。

サイトのプロキシ データ取得率が一貫して大幅に異なる場合（つまり、1 時間あたり 500 GB より大幅に低いか高い場合）、デフォルトのプロキシ データ取得率の設定を永続的に変更することができます。これは今後のすべてのプロキシ導入の推奨事項に影響します。これを行うには、次の手順を実行します。

1. コマンド シェルを開き、ユーザー**管理者**として Avamar サーバーにログインします。
2. `su -` と入力して、ユーザーを root に切り換えます。
3. UNIX テキスト エディターで`/etc/vcs/dm.properties` を開きます。
4. `proxy_ingest_rate_gb_per_hour` 設定を変更します。
5. 変更内容を保存し、`/etc/vcs/dm.properties` を閉じます。

プロキシのオーバーコミットに対する保護

デフォルトでは、各 Avamar プロキシは、8 個のコンカレント バックアップ ジョブを許可するように構成されています。この設定は、ほとんどのお客様サイトに適していることが分かっています。

Dell EMC では、コンカレント ジョブ数を 9 個以上に増やすことは推奨していません。既定のプロキシ用にキューイングされるバックアップ ジョブ数が多くなりすぎてしまう可能性があるためです（プロキシ オーバーコミット）。このような状況では、プロキシ間のバックアップ ジョブの不均等な分散が生じ、そうでない場合よりもバックアップ ジョブの完了に時間がかかるというボトルネックが生じる可能性もあります。

サイトによっては、許可するコンカレント バックアップ ジョブ数をもっと少なくするように一部のプロキシを構成する方がよい場合があります。これには通常、追加のプロキシの導入が必要ですが、仮想インフラストラクチャの特定の領域でのバックアップの集中やクラスタリングとは対照的に、プロキシ間のバックアップ ジョブをより均等に分散できます。

レベル 1 増分/変更ブロック バックアップの最適化

Proxy Deployment がプロキシ導入の推奨事項を生成する場合、通常のバックアップ運用を維持するのに必要なプロキシ数を計算して行います。通常のバックアップ運用に関する前提条件の 1 つは、バックアップがレベル 1 増分バックアップまたは変更ブロック バックアップであり、レベル 0 フル バックアップではないことです。

レベル 0 バックアップは、本質的に時間がかかり、より多くのプロキシ リソースを使用します。したがって、新規の大型仮想マシンを導入すると、必要なすべてのバックアップを、バックアップ ウィンドウによって割り当てられた時間内に完了する能力に悪影響を及ぼす可能性があります。

そのため、新規の大型仮想マシンの導入は、可能な場合は常に段階的に行い、必要なレベル 0 バックアップ取得の機会をシステムに与えます。

段階的な導入が不可能な場合は、別の方法として、プロキシ オーバー コミットによって発生するバックアップの失敗を許容する方法があります。システムが安定し始めると、プロキシ リソースはコミット

状態になり、これらの仮想マシンは最終的にバックアップされます。管理者は、システムが安定し、仮想マシンが最終的に正常にバックアップされることを確認するために、状況を注意深く監視する必要があります。

注

Avamar では、必要に応じてプロキシの導入を試みますが、環境に関する詳細をすべて知ることは不可能であるため、Proxy Deployment が、サポートされる最大数を超えてプロキシを過剰に割り当てていないか確認することが重要です。

プロキシの導入

イメージ バックアップで保護する各 vCenter で 1 個以上のプロキシを導入します。

DRS（Distributed Resource Scheduler）対応クラスタにプロキシが導入される場合は、このクラスタで Storage vMotion を使用して、プロキシを移動できます。プロキシを別のストレージに移行している間、そのプロキシで管理されているジョブは、リスクにさらされます。HotAdd は、DRS クラスターに配置されているプロキシでは動作しません。そのため、導入された Avamar プロキシ仮想マシンの DRS を無効化します。

手順

1. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Proxy Management**］をクリックします。

   ［**Proxy Deployment**］ページが表示されます。

2. ［**Config**］パネルで、次の設定を行います。

   a. ［**vCenter**］を選択します。

   b. ［**Data Change Rate (%)**］を設定します。

   c. ［**Backup Window (minutes)**］を設定します。

   d. この推奨事項に DAS を使用した仮想マシンを含めるには、［**Protect Virtual Machines on Local Storage**］チェックボックスを選択します。

      このオプションにより、クラスタ化されたホストのローカル ストレージ上の仮想マシンが無視されます。

3. ［**CREATE RECOMMENDATION**］をクリックします。

   下側のパネルにあるリストに、推奨事項が追加されます。

   ［**Recommendations**］パネルに、提示された導入トポロジーが表示されます。提示された新しいプロキシが、［**New proxy**］という名前で各 ESX ホストの下に表示されます。

4. 導入する推奨プロキシごとに、次のようにプロキシを構成します。

   a. ［**Recommendations**］パネルで、［**New proxy**］を選択します。

   b. [✎] をクリックします。

      ［**New Proxy**］ダイアログ ボックスが表示されます。

   c. ［**Name**］フィールドにプロキシ名を入力します。

   d. このプロキシが存在する Avamar サーバーの［**Domain**］を選択します。

   e. ［**IP**］フィールドに IP アドレスを入力します。

   f. ［**Datastore**］リストからデータストアを選択します。

g. [**Network**] リストから仮想ネットワークを選択します。

h. [**DNS String**] フィールドに完全修飾 DNS サーバー名または IP アドレスを入力します。

i. [**Gateway**] フィールドにネットワーク ゲートウェイ IP アドレスを入力します。

j. [**Netmask**] フィールドに、ネットワーク マスクを入力します。

k. [[保存]] をクリックします。

5. （オプション）導入するその他のプロキシを追加します。

注

追加するプロキシごとに、プロキシ名、IP アドレス、完全修飾 DNS サーバー名または IP アドレス、ネットワーク ゲートウェイ、ネットワーク マスクを指定する準備をする必要があります。

---

a. ツリー パネルで、ESX ホストを選択します。

b. [**New Proxy**] をクリックします。

[**New Proxy**] ダイアログ ボックスが表示されます。

c. [**Name**] フィールドにプロキシのホスト名を入力します。

d. このプロキシが存在する Avamar サーバーの [**Domain**] リストを選択します。

e. [**IP**] フィールドに IP アドレスを入力します。

f. [**Datastore**] リストからデータストアを選択します。

g. [**Network**] リストから仮想ネットワークを選択します。

h. [**DNS String**] フィールドに完全修飾 DNS サーバー名または IP アドレスを入力します。

i. [**Gateway**] フィールドにネットワーク ゲートウェイ IP アドレスを入力します。

j. [**Netmask**] フィールドに、ネットワーク マスクを入力します。

k. （オプション）[**NTP**] フィールドに NTP サーバー アドレスを入力します。

l. [[保存]] をクリックします。

6. （オプション）導入しないプロキシをすべて削除します。

a. ツリー パネルで、プロキシを選択します。

b. [⊗] をクリックします。

c. [**YES**] をクリックします。

7. プロキシ トポロジーを更新するには、[⚡] をクリックします。

8. 提示された導入トポロジーが満足いくものである場合は、[✓] をクリックし、変更を適用してプロキシを導入します。

結果

プロキシを導入できない場合、そのプロキシはシステムから完全に削除されます。そのホスト名および IP アドレスは、その後のプロキシの導入で使用されます。

プロキシのアップグレード

このセクションでは、Avamar ソフトウェアのサポート対象リリースを実行するプロキシをアップグレードする方法について説明します。リリース 7.3.x 以前を実行している Avamar プロキシの場合、本書の過去のリリースで詳細を確認してください。

- Proxy Deployment Manager を使用してプロキシを導入した場合は、Avamar プロキシのアップグレード（43 ページ）を使用します。
- プロキシを手動で導入した場合は、必要な情報を記録し、既存のプロキシを削除してから、新しいプロキシを再導入する必要があります。詳細については、7.5.1 以前のサポート対象リリースから Avamar プロキシをアップグレードする（43 ページ）を参照してください。

注

Proxy Deployment Manager に、手動で導入されたプロキシが表示されないことがあります。

同じバージョンの SLES OS を実行しているリリースにアップグレードするには、ISO のみを使用することができます。したがって、ISO を使用して、以前のリリース（SLES 11 SP3）からリリース 7.5.1 以降（SLES 12 SP1）にプロキシをアップグレードすることはできません。SLES OS のバージョンが異なる旧リリースのプロキシを手動で導入した場合は、プロキシを削除してから、Proxy Deployment Manager を使用して新しいプロキシを導入する必要があります。

次のトピックでは、一部の旧 Avamar リリースでは Avamar Web ユーザー インターフェイス（AUI）をサポートしていないため、Avamar Administrator を使用する手順について説明します。使用可能な場合は、代わりに AUI 内で Proxy Deployment Manager を使用できます。詳細については、プロキシの導入（38 ページ）を参照してください。

Avamar プロキシのアップグレード

手順

1. Avamar Administrator で、［**VMware**］ > ［**Proxy Deployment Manager**］を選択します。

   ［**Proxy Deployment Manager**］ウィンドウが表示されます。

2. vCenter を選択してから、［**Create Recommendation**］をクリックします。

   アップグレードする必要がある選択された vCenter のトポロジー ツリーにある既存のプロキシが、プロキシに保留中の更新があることを示すツールチップとともに［**!**］記号で指定されます。

3. ［**Apply**］をクリックします。

7.5.1 以前のサポート対象リリースから Avamar プロキシをアップグレードする

このセクションでは、既存のプロキシがリリース 7.5.1 より前のリリース レベルである場合に、サポート対象の Avamar プロキシ ソフトウェアをアップグレードするための情報と手順を示します。

既存のプロキシ構成：

プロキシをアップグレードする前に以下の情報を収集し、アップグレード前の値にプロキシ設定をリストアする必要があります。

- VM コンテナー

  - 名前
  - ホスト
  - データストア
  - ネットワーク
  - フォルダー
- VM クライアント
  - IP アドレス
  - ゲートウェイ
  - DNS サーバ
  - ネットマスク
- ポリシー
  - ドメイン
  - データストアの保護
  - グループ メンバーシップ

次のチャートは、プロキシをアップグレードする前の情報を収集する方法を例示しています。

表 4 プロキシ情報の収集例のチャート

名前	ホスト	データストア	ネットワーク	フォルダー	IP
Proxy1	vcenter.com/host1	DS2	NW1	/proxies	x.x.x.x
Proxy2	vcenter.com/host2	DS2	NW1	/proxies	x.x.x.x

表 5 プロキシ情報の収集例のチャート（続き）

ゲートウェイ	DNS	ネットマスク	ドメイン	データストアの保護	グループの保護
x.x.x.x	x.x.x.x,x.x.x.x	x.x.x.x	/clients	DS1,DS2	Default Virtual Machine Group
x.x.x.x	x.x.x.x,x.x.x.x	x.x.x.x	/clients	DS1,DS2	他のグループ

VM 構成を表示

手順

1. vSphere Client または vSphere Web Client で、［**VMs and Templates**］ビューに移動します。
2. 既存のプロキシを見つけます。各プロキシに対して：
   a. VM 名およびフォルダー名を記録します。
   b. ［**Summary**］タブを選択します。
   c. ホスト、ストレージ（データストア）、ネットワークを記録します。

d. 右クリックして［**Edit Settings...**］を選択します。

3. 各プロキシに対して：
   - vSphere Web Client を使用している場合は、［**vApp Options**］タブに移動して IP、ゲートウェイ、DNS、ネットマスクを記録します。
   - vSphere クライアント（Windows）を使用している場合は、
   a. ［**Options**］タブに移動します。
   b. ［**vApp Options > Advanced**］を選択します。
      右側のペインに vApp オプションフィールドが表示されます。
   c. 右側のペインで［**Properties > Properties**］の順にクリックします。
      ［**Advanced Properties Configuration**］ウィンドウが表示されます。
   d. ［Properties］テーブルで、［**Key**］列の以下のキーに対応する［**Value**］列の IP アドレス、ゲートウェイ、DNS、ネットマスク値を記録します。

キー	値
vami.ip0.EMC_Avamar_Virtual_Machine_Combined_Proxy	IP アドレス
vami.gateway.EMC_Avamar_Virtual_Machine_Combined_Proxy	ゲートウェイ
vami.DNS.EMC_Avamar_Virtual_Machine_Combined_Proxy	DNS サーバー
vami.netmask0.EMC_Avamar_Virtual_Machine_Combined_Proxy	ネットマスク

データストアの割り当てとグループ メンバーシップの表示

手順

1. Avamar Administrator で、［**Administration**］起動リンクをクリックします。
   ［**Administration**］ウィンドウが表示されます。
2. ［**Account Management**］タブをクリックします。
3. プロキシを見つけ、ドメインを記録します。
4. プロキシを選択して、［**Edit**］をクリックします。
   ［**Edit Client**］ダイアログ ボックスが表示されます。
5. ［**Datastores**］タブをクリックし、選択されているデータストアを記録します。
6. ［**Groups**］タブをクリックし、選択されているグループを記録します。
7. すべてのグループのチェックを外してこのプロキシを削除します。
8. ［**OK**］をクリックします。

既存のプロキシの削除

手順

1. vSphere Client または Web Client で、既存のプロキシを見つけます。
2. 各プロキシに対して：
   a. マウスを右クリックし、［**Power > Power off**］を選択します。

b. プロキシがオフになるまで待ち、右クリックして［**Delete from Disk**］を選択します。

［**Confirm Delete**］確認画面が表示されます。

c. ［**Yes**］をクリックします。

3. Avamar Administrator で、［**Administration**］起動リンクをクリックします。

［**Administration**］ウィンドウが表示されます。

4. ［**Account Management**］タブをクリックします。
5. 既存のプロキシを見つけ、各プロキシに対して：

a. 右クリックして［**Retire Client...**］を選択します。

［**Retire Client**］ウィンドウが表示されます。

b. ［**OK**］をクリックします。

データストアの割り当てとグループ メンバーシップのリストア

手順

1. Avamar Administrator で、［**Administration**］起動リンクをクリックします。

［**Administration**］ウィンドウが表示されます。

2. ［**Account Management**］タブをクリックします。
3. 更新されたプロキシを選択し、［**Edit**］をクリックします。

［**Edit Client**］ダイアログ ボックスが表示されます。

4. ［**Datastores**］タブをクリックし、既存のプロキシ構成：（43 ページ）で作成されたチャートに基づいて、クライアントがデータストアで保護されていることを確認します。
5. ［**Groups**］タブをクリックし、既存のプロキシ構成：（43 ページ）で作成されたチャートに基づいて、プロキシがこのグループのメンバーであることを確認します。
6. ［**OK**］をクリックします。

Proxy Deployment Manger を使用した再導入プロキシ

使用可能な場合は、代わりに AUI 内で Proxy Deployment Manager を使用できます。詳細については、プロキシの導入（38 ページ）を参照してください。

手順

1. Avamar Administrator で、［**VMware**］ > ［**Proxy Deployment Manager**］を選択します。

［**Proxy Deployment Manager**］ウィンドウが表示されます。

2. ［vCenter］を選択します。
3. ［**Data change rate**］を［**0**］に設定します。

この設定により、［**Proxy Deployment Manager**］が VMware 環境の分析に基づいてプロキシを推奨することがなくなります。

4. ［**Create Recommendation**］をクリックします。

ツリー ペインで VMware のトポロジーが表示されます。［**New proxy**］と表示された推奨プロキシがないことを確認します。

5. 既存のプロキシ構成：（43 ページ）で作成されたチャートの各プロキシに対して、以下の手順を実行します。

a. ［**Proxy Deployment Manager**］でホストを見つけ、選択します。

b. ［**New Proxy...**］をクリックします。

［**New Proxy**］ウィンドウが表示されます。

c. チャートの情報に基づいて、［**Name**］、［**Domain**］、［**IP**］、［**Datastore**］、［**Network**］、［**DNS**］、［**Gateway**］、［**Netmask**］を入力します。

d. ［**Save**］をクリックします。

6. ［**Apply**］をクリックします。

新しいプロキシが導入されます。障害が発生した場合、［**Apply**］を再びクリックすることで操作を再試行できます。

プロキシの維持

このセクションの内容は次のとおりです。

プロキシの Avamar サーバーへの再登録

次の手順に従って、既存のプロキシを Avamar サーバーに再登録します。

手順

1. vSphere Client または vSphere Web Client を起動して、vCenter Server にログインします。
2. 再登録するプロキシを見つけます。
3. 右クリックして、［**Power**］ > ［**Shut Down Guest**］を選択します。
4. ［**Yes**］をクリックして、ゲスト オペレーティング システムをシャットダウンすることを確認します。
5. 右クリックして、［**Power**］ > ［**Power Off**］を選択します。
6. ［**Yes**］をクリックして、プロキシ仮想マシンの電源をオフにすることを確認します。
7. ［**Open Console**］を右クリックします。

コンソール ウィンドウが表示されます。

8. 右クリックして、［**Power**］ > ［**Power On**］を選択します。
9. 次のメッセージが表示されるまで、コンソール ウィンドウを監視します。

```
Please press a key now if you want to re-register this
proxy with Avamar Administrator. Continuing in 10
seconds...
```

10. コンソール ウィンドウ内でクリックして、［**Enter**］キーを押します。
11. Avamar サーバーの DNS 名を入力して、［**Enter**］キーを押します。
12. Avamar サーバーのドメイン名を入力して、［**Enter**］キーを押します。

デフォルトのドメインは「clients」です。ただし、Avamar システム管理者が他のドメインおよびサブドメインを定義している可能性があります。このクライアントを登録する際に使用するドメインについては、Avamar システム管理者に問い合わせてください。

注

サブドメイン（例えば、clients/MyClients）を入力する場合、先頭の文字としてスラッシュ（/）を含めないでください。先頭の文字としてスラッシュを含めると、エラーが発生し、このクライアントを登録できなくなります。

プロキシのゲスト オペレーティング システムの管理者パスワードを変更する

注

ssh ログインの root アカウントが無効になっています。

手順

1. コマンド シェルを開き、admin としてプロキシにログインします。
2. **passwd** と入力します。
3. 現在のゲスト オペレーティング システムの管理者パスワードを入力し、［**Enter**］をクリックします。
4. 新しいゲスト オペレーティング システムの管理者パスワードを入力し、［**Enter**］をクリックします。
5. パスワードを再度入力して新しいパスワードを確認し、［**Enter**］をクリックします。

注

プロキシを導入したら、パスワードを変更します。

プロキシのゲスト オペレーティング システムの root パスワードを変更する

手順

1. コマンド シェルを開き、admin としてプロキシにログインします。
2. 以下のように入力して、ユーザーを root に切り換えます。

   ```
   su -
   ```

3. **passwd** と入力します。
4. 現在のゲスト オペレーティング システムの root パスワードを入力し、［**Enter**］をクリックします。
5. 新しいゲスト オペレーティング システムの root パスワードを入力し、［**Enter**］をクリックします。
6. パスワードを再度入力して新しいパスワードを確認し、［**Enter**］をクリックします。

注

プロキシを導入したら、パスワードを変更します。

追加の Avamar サーバーの構成

プロキシの自動選択の構成

プロキシを自動的に選択するインテリジェントな機能では、3 種類のアルゴリズムによって、バックアップおよびリストア処理で使用するプロキシを決定します。アルゴリズムの構成は、`mcserver.xml` **proxy_selection_algorithm** の設定を手動で変更することによってのみ可能です。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
   - シングル ノード サーバーには、**admin** としてサーバーにログインします。
   - マルチ ノード サーバーの場合、**admin** としてユーティリティ ノードにログインします。
2. 次のコマンドを入力して、MCS を停止します。

   ```
   dpnctl stop mcs
   ```

3. UNIX テキスト エディターで`/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` を開きます。
4. `proxy_selection_algorithm` エントリー キーを見つけます。
5. `proxy_selection_algorithm` の設定を次の値のいずれかに変更します。
   - `hot_add_preferred`：MCS によって、ホット アド機能に基づいたプロキシがインテリジェントに優先され、自動的に選択されます。ホット アド機能に基づいたプロキシが見つからない場合、MCS ではホット アド機能のないプロキシの使用にフォールバックします。これはデフォルト設定です。
   - `hot_add_only`：MCS によって、ホット アド機能に基づいたプロキシがインテリジェントに優先され、自動的に選択されます。ホット アド機能に対応したプロキシが見つからない場合、MCS はバックアップまたはリストア処理を一時停止し、ホット アド機能に対応したプロキシが利用可能になるまで待ちます。
   - `ignore_associated_datastores`：この設定では、選択プロセスで既知のプロキシとデータストアの関連付けが無視されます。これにより、MCS はより広範な利用可能なプロキシのプールからプロキシを選択できます。`hot_add_preferred` 設定と同様、この設定でもホット アド機能の付いたプロキシがホット アド機能のないプロキシよりも優先されます。ただし、ホット アド機能に対応したプロキシが見つからない場合、MCS ではホット アド機能のないプロキシの使用にフォールバックします。

   例：

   `<entry key="proxy_selection_algorithm" value="`**`hot_add_only`**`" />`により、**hot_add_only** アルゴリズムを使用するプロキシの自動選択メカニズムが構成されます。
6. `mcserver.xml` を終了して、変更を保存します。
7. 次のコマンドを入力して、MCS およびスケジューラを開始します。

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

ゲスト バックアップおよびイメージ バックアップの両方をサポートするように MCS を構成する

イメージ バックアップおよびゲスト バックアップの両方の使用をサポートして、同一の仮想マシンを保護するためには、重複するクライアント名を許可するように Avamar MCS を構成する必要があります。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
   - シングル ノード サーバーには、admin としてサーバーにログインします。
   - マルチ ノード サーバーの場合、admin としてユーティリティ ノードにログインします。
2. 次のコマンドを入力して、MCS を停止します。

   ```
   dpnctl stop mcs
   ```

3. UNIX テキスト エディターで `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` を開きます。
4. `allow_duplicate_client_names` エントリー キーを見つけます。
5. `allow_duplicate_client_names` の設定を **`true`** に変更します。

   ```
   <entry key="allow_duplicate_client_names" value="true" />
   ```

6. `mcserver.xml` を終了して、変更を保存します。
7. 次のコマンドを入力して、MCS およびスケジューラを開始します。

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

第 3 章

管理

本章は、次のトピックで構成されています。

クライアントとコンテナー

イメージ バックアップを使用して、vCenter にある次の VMware エンティティのすべてを管理および保護できます。

- 仮想マシン
- vApp
- 仮想マシンのフォルダー（データセンター レベルの下に存在するフォルダー）
- リソース プール

AUI では、仮想マシンと vApp はクライアントとして管理され、フォルダーとリソース プールはコンテナとして管理されます。

コンテナーにより、複数の仮想マシン、vApp、仮想マシン フォルダー、リソース プールを単一の論理オブジェクトとして管理する機能が提供されます。

注

フォルダーやリソース プールなどの空のコンテナーは、MCS に追加できます。VM または vApp がコンテナーに追加されると、これらは Avamar により自動的に保護されます。バックアップ時、MCS は空のコンテナーをスキップします。

動的コンテナーと静的コンテナーの比較

コンテナを AUI に追加する際に、動的または静的のいずれかに設定します。

動的コンテナ：vCenter コンテナのすべてのコンテンツを含みますが、vCenter 内のコンテナ エンティティの継続的な監視も行い、変更が発生した場合（例えば、仮想マシンまたはフォルダーが追加または削除された場合）、これらの変更が自動的に AUI に反映されます。

静的コンテナー：Avamar に追加された時点で vCenter コンテナーに存在するもののみが含まれます。その後に vCenter で変更が発生しても、AUI には反映されません。

動的コンテナーの動作

［**Recursive Protection**］チェックボックスを使用して動的コンテナを追加すると、サブコンテナを含むすべての子エンティティが AUI に追加されます。サブコンテナに存在する仮想マシンまたは vApp は、自動的に AUI に追加されます。

仮想マシン クライアントが vCenter のコンテナから削除され、そのコンテナが AUI の動的コンテナとして保護されている場合は、仮想マシン クライアントは動的コンテナの一部として Avamar に引き続き常駐します。ただし、アイコンの色が青からグレーに変わります。これにより、過去のバックアップを将来のリストアに使用できます。ただし、仮想マシン クライアントが vCenter には存在しなくなるため、新しいバックアップは実行されません。

Avamar 動的コンテナーから 1 個以上の仮想マシン クライアントを削除または破棄する必要がある場合は、まずそのコンテナーを静的コンテナーに変更します。代替方法として、これらの仮想マシン クライアントを vCenter の別のコンテナーに移動することも可能です。

単独の保護とコンテナー保護の相互作用の仕組み

仮想マシンが単独で保護されており、さらにコンテナ メンバーとしても保護されている場合、この仮想マシンの破棄または削除には特別な条件が適用されます。

次のネストされたコンテナ構造とシナリオを見てみましょう。

図 3 単独の保護とコンテナー保護の例

この例では、vm-1 が仮想マシン クライアントとして Avamar に追加されます。これは単独で保護されています。vApp-1 コンテナが Avamar に追加されると、vm-1 は、vApp-1 コンテナのメンバーとしても保護されます。Avamar は次の 2 つのコンテキストに同一の仮想マシンが存在することを認識します。

- スタンドアロンの仮想マシン クライアント vm-1 として、単独に保護された仮想マシン
- vApp-1 コンテナーのメンバーとして保護された仮想マシン

vApp-1 コンテナが破棄または削除されると、vm-1 はスタンドアロンの仮想マシン クライアントとして Avamar に存続します。これは、vApp-1 コンテナのメンバーとして保護される前に、スタンドアロンの仮想マシンとして明示的に追加されたためです。スタンドアロンのコンテキストが、コンテナ メンバーのコンテキストよりも優先されます。vm-1 を破棄または削除する必要がある場合、vApp-1 コンテナを削除または破棄することはできません。スタンドアロンのインスタンスも破棄または削除する必要があります。スタンドアロン インスタンスを削除しない場合、vm-1 はスケジュール設定されたバックアップで保護され続けます。

VMware クライアントの追加

手順

1. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Asset Management**］をクリックします。
2. ドメイン ツリーで、クライアントの VCenter ドメインまたはサブドメインを選択します。
3. ［**ADD CLIENT**］をクリックします。

   注

   ［VMware vCenter™］、［Image Proxy］、［Virtual Machine］のクライアント タイプについては、「Avamar for VMware ユーザー ガイド」を参照してください。

   ［**Select VMware Entity**］パネルが表示されます。
4. ［**Select VMware Entity**］ウィンドウで、次のタスクを実行します。
   - vSphere 仮想マシンとテンプレートを表示するには、［**Host/Cluster**］スイッチをオフに切り替えます。
   - vSphere のホストとクラスターを表示するには、［**Host/Cluster**］スイッチをオンに切り替えます。

   左のパネルで選択された VMware エンティティに基づいて、右のパネルに vCenter インベントリ リストが表示されます。

   注

   リソース プールは、［vSphere Virtual Machines and Templates］ビューに表示されません。リソース プールは、［Hosts and Clusters］ビューにのみ表示されます。

a. 右側のパネルで、フォルダー、リソース プール、仮想マシン、vApp のいずれかを選択し、[⊕] をクリックします。

VMware エンティティが下側のパネルに表示されます。

b. コンテナを追加する場合は、右側のパネルで［**Dynamic**］スイッチをオンに切り替えて、動的なコンテナにします。

この設定により、動的ポリシーが有効になります。

c. コンテナを追加する場合は、右側のパネルで、［**Static**］スイッチをオンに切り替えて、静的なコンテナにします。

d. 更新ブロック追跡を有効化するには、右側のパネルで、［**CBT**］スイッチをオンに切り替えます。

更新ブロック追跡が有効になっていない場合、各仮想マシンのイメージはバックアップごとに完全に処理され、バックアップ ウィンドウが長くなり、あるいはバックエンド ストレージの読み取りおよび書き込みアクティビティが過剰になることがあります。

注

更新ブロック追跡を有効にしても、次のいずれかのアクションが仮想マシンで発生するまで、有効になりません。

- 再起動
- 電源オン
- 中断後の再開
- 移行

---

e. 再帰的な保護を使用する動的コンテナを追加するには、右側のパネルで［**Recursive**］スイッチをオンに切り替えます。

このタスクにより、サブコンテナ、仮想マシン、およびサブコンテナに存在する vApps を含むすべての子エンティティが自動的に追加されます。

5. ［**OK**］をクリックします。
6. 次の手順に従って、更新ブロック追跡を有効化します。
   a. vSphere Client で、該当する仮想マシンを見つけます。
   b. 各仮想マシンで、
      - 再起動
      - 電源オン
      - 中断後の再開
      - 移行
7. フォルダー、リソース プール、仮想マシン、vApp を削除するには、下側のパネルで［⊖］クリックします。
8. ［**YES**］をクリックします。

VMware クライアントの削除

クライアントとクライアントのすべてのバックアップを削除します。必要に応じて、レプリケーション ターゲット システムに存在するすべてのレプリカの削除を選択できます。

クライアントを削除すると、Avamar はそのクライアントに格納されているバックアップをすべて完全に削除します。クライアントを削除するのは、そのクライアントのバックアップを保持する必要がないと確信している場合に限られます。確信がない場合は、代わりにクライアントを廃棄します。

手順

1. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Asset Management**］をクリックします。
2. 階層［**Domain**］ツリーで、vCenter ドメインまたはサブドメインを選択します。
3. クライアントのリストで、削除するクライアントを選択します。

   ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。
4. ［**MORE ACTIONS**］ > ［**Delete Client**］をクリックします。

   ［**Delete Client**］ダイアログ ボックスが表示され、クライアントの既存バックアップの数が表示されます。
5. ［**I understand this action is permanent and irreversible**］を選択します。

   このフィールドは、クライアントとクライアントのバックアップを誤って削除しないようにする安全策です。
6. ［**YES**］をクリックします。

更新ブロック追跡の有効化

更新ブロック追跡が有効になっていない場合、各仮想マシンのイメージはバックアップごとに完全に処理され、バックアップ ウィンドウが長くなり、あるいはバックエンド ストレージの読み取りおよび書き込みアクティビティが過剰になることがあります。

更新ブロック追跡を有効にしても、次のいずれかのアクションが仮想マシンで発生するまで、有効になりません。

- 再起動
- 電源オン
- 中断後の再開
- 移行

手順

1. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Asset Management**］をクリックします。
2. 階層［**Domain**］ツリーで、vCenter ドメインまたはサブドメインを選択します。

   サブドメイン クライアントを含めるには、［**Include Sub-domain**］スイッチをオンに切り替えます。
3. クライアントのリストで、編集するクライアントを選択します。

   ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。

4. ［**MORE ACTIONS**］ > ［**Edit Client**］をクリックします。

   ［**Edit Client**］ダイアログ ボックスが表示され、クライアントの既存バックアップの数が表示されます。

5. 更新ブロック追跡を有効にするには、次の手順に従います。

   a. ［**VMware**］タブを選択します。

   b. ［**CBT**］フィールドで、チェックボックスをオンにします。

   c. ［**UPDATE**］をクリックします。

Avamar Administrator で保護されている仮想マシンを表示する

［**Protection**］タブから、すべての仮想マシンのバックアップ保護の状態を表示できます。このタブでは何もアクションを実行できません。

手順

1. Avamar Administrator で、［**Administration**］起動リンクをクリックします。

   ［**Administration**］ウィンドウが表示されます。

2. vCenter domain をクリックします。
3. ［**Account Management**］タブをクリックします。
4. ［**Protection**］タブをクリックします。

Avamar Administrator でレプリケートされた仮想マシン名を表示する

この機能は、REPLICATE ドメインにあるすべての仮想マシンの仮想マシン名を表示するために使用します。

この機能は、REPLICATE ドメイン以外の場所では無効になっています。

非仮想マシン クライアントの情報を参照しようとすると、`No Information` が表示されます。

手順

1. Avamar Administrator で、［**Administration**］起動リンクをクリックします。

   ［**Administration**］ウィンドウが表示されます。

2. ［**Account Management**］タブをクリックします。
3. ツリーで、REPLICATE ドメインにある仮想マシン クライアントを選択します。
4. ［**Actions**］ > ［**Account Management**］ > ［**View Information**］を選択します。

   仮想マシン名を示すダイアログ ボックスが表示されます。

5. ［**OK**］をクリックします。

Avamar Administrator における vCenter 接続の監視

Avamar Administrator では、vCenter Server への接続のプールを維持します。他の重要なサービス同様、［**Administration**］ウィンドウの［**Services Administration**］タブには、vCenter 接続の継続的なステータスが表示されます。

手順

1. Avamar Administrator で、［**Administration**］起動リンクをクリックします。

   ［**Administration**］ウィンドウが表示されます。

2. ［**Services Administration**］タブをクリックします。
3. ［**VMware vCenter Connection Monitor**］サービス エントリーをダブル クリックします。

   ［**VMware vCenter Connection Monitor**］ダイアログ ボックスが表示されます。有効な接続の状態は、Active と Idle です。

結果

vCenter への接続は、停止、開始、再開することができます。vCenter のアップグレードのために接続を停止し、アップグレードの完了後に開始します。vCenter がシャットダウンされると、接続は無効になるため、再度確立する必要があります。シャットダウンされると、Avamar Administrator は vCenter 構造または仮想マシンを表示できません。

vCenter と AUI の手動による同期化

Avamar Administrator は定期的に監視する vCenter と自動的に同期化しますが、いつでも手動で同期化できます。

手順

1. 左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］をクリックします。
2. 階層［**Domain**］ツリーで、vCenter を選択します。
3. vCenter と AUI を同期するには、次のいずれかの手順を実行します。
   - オーバーフロー メニュー［⋮］をクリックして、［**Sync vCenter**］を選択します。
   - ［**DOMAIN ACTIONS**］パネルで、［**Sync vCenter**］を選択します。
4. ［**Yes**］をクリックして、確認メッセージを閉じます。

vCenter Client の名前を変更する

既存の vCenter Client の DNS 名が変更されると、Avamar サーバーはその vCenter への接続を失います。これにより、スケジュール設定されたバックアップなど、vCenter との相互作用が妨げられます。これが発生する場合は、AUI で vCenter Client の名前を手動で変更する必要があります。

これは、vCenter Client の名前を変更する際の唯一の方法です。AUI では、vCenter Client の名前は、常に完全修飾 DNS 名か、有効な IP アドレスであることが必要です。

手順

1. 左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］をクリックします。
2. ドメイン ツリーで、vCenter Client を選択します。
3. ［**MORE ACTIONS**］ > ［**Edit Client**］をクリックします。

   ［**Edit Client**］ウィンドウが表示されます。

4. ［**Name**］フィールドに、新しい完全修飾 DNS 名を入力します。

5. ［**UPDATE**］をクリックします。

   確認のメッセージが表示されます。

6. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
   - シングル ノード サーバーには、admin としてサーバーにログインします。
   - マルチ ノード サーバには、
     a. admin としてユーティリティ ノードにログインします。
     b. 次のコマンドを入力して、admin OpenSSH キーをロードします。

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```

7. 次のコマンドを入力して、MCS を停止します。

   ```
   dpnctl stop mcs
   ```

8. 次のコマンドを入力して、MCS およびスケジューラを開始します。

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

9. 次の手順に従って、この vCenter にあるすべての Avamar プロキシを再起動します。
   a. vSphere Client または vSphere Web Client を起動して、vCenter Server にログインします。
   b. Avamar プロキシを見つけます。
   c. 右クリックして、［**Power**］ > ［**Shut Down Guest**］を選択します。
   d. ［**Yes**］をクリックして、ゲスト オペレーティング システムをシャットダウンすることを確認します。
   e. 右クリックして、［**Power**］ > ［**Off**］を選択します。
   f. ［**Yes**］をクリックして、仮想マシンの電源をオフにすることを確認します。
   g. 右クリックして、［**Power**］ > ［**On**］を選択します。

VMware Image Dataset

VMware Image Dataset は、イメージ バックアップで VMware エンティティを保護するためのデフォルトのデータセットです。

さまざまな点において、VMware Image Dataset は他のデータセットより簡素化されています。

- 使用可能なソース データ プラグ インは、Linux と Windows 仮想ディスクのみです。いずれもデフォルトで選択されています。
- ［**Select Files and/or Folders**］オプションのほか、［**Exclusions**］タブ、［**Inclusions**］タブは無効になっています。
- 更新ブロック追跡は、組み込みの `utilize_changed_block_list=true` プラグ イン オプションのステートメントを使用して、デフォルトで有効化されています。

ゲスト バックアップのスロットリング パラメーターを Avamar Administrator のデータセットに追加する

同一の ESX Server 上にある仮想マシンのスケジュール設定されたゲスト バックアップを実行する際に、Avamar データセットにスロットリング パラメーターを追加します。

これは、Avamar MCS で一定のロードの制約を受けるため、Avamar ができるだけ多くのバックアップを開始しようとするからです。ただし、同一の VMware ESX Server 上にある仮想マシンで複数のゲスト バックアップを実行しようとする場合、CPU 使用率が急上昇し、VMware ESX Server 全体のパフォーマンスに悪影響を及ぼす可能性があります。

手順

1. Avamar Administrator で［**Tools**］ > ［**Manage Datasets**］を選択します。

   ［**Manage All Datasets**］ウィンドウが表示されます。

2. リストからデータセットを選択して、［**Edit**］をクリックします。

   ［**Edit Dataset**］ダイアログ ボックスが表示されます。

3. ［**Options**］タブをクリックして、［**Show Advanced Options**］をクリックします。

4. クライアントが Network usage throttle をサポートしている場合は、［**Network usage throttle (Mbps)**］フィールドにゼロ値以外を入力します。

   20 のような小さい値から始めてください。次のバックアップ セッションを監視して、これによって ESX サーバーの CPU 使用率の問題が解決するかどうかを確認します。

5. ［**OK**］をクリックします。

グループ

イメージ バックアップおよびリストアで使用されるグループには、重要な動作上の相違点があります。

デフォルト プロキシ グループ

デフォルト プロキシ グループはすべてのプロキシが存在する場所です。このグループは削除できません。

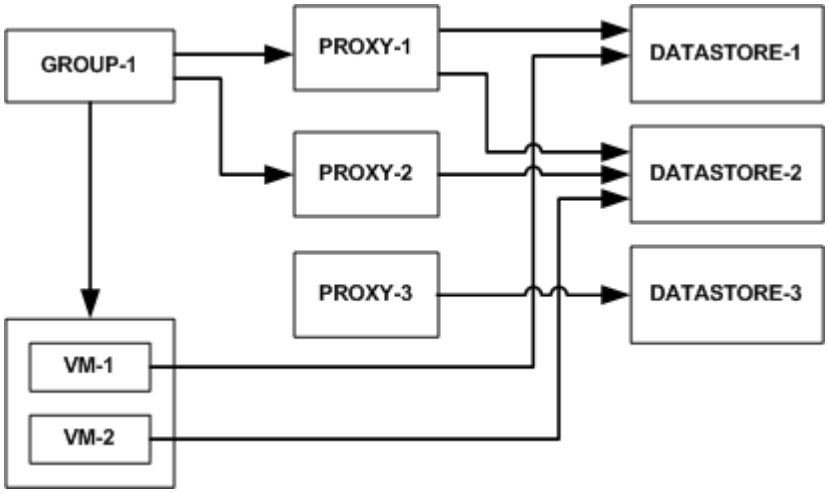
Default Virtual Machine Group

Default Virtual Machine Group は、新しい仮想マシン クライアントが登録時に自動的に追加される場所にあります。このグループは手動で削除することはできませんが、vCenter ドメインが削除されると自動的に削除されます。

グループ内の仮想マシンとプロキシの関係

以下の簡素化した構成例を見てみます。

図 4 グループ内の仮想マシンとプロキシの関係



仮想マシン VM-1 と VM-2 は、それぞれ、DATASTORE-1 と DATASTORE-2 にデータを保存します。

Avamar Administrator 内で、プロキシは、vCenter データストアを保護するため、次のように割り当てられます。

- PROXY-1 は、DATASTORE-1 と DATASTORE-2 に割り当てられています
- PROXY-2 は、DATASTORE-2 に割り当てられています
- PROXY-3 は、DATASTORE-3 に割り当てられています

データストアの割り当ては、［**Edit Client**］ダイアログ ボックスのプロキシ レベルで行われます。

グループ（GROUP-1）が作成され、仮想マシン VM-1 および VM-2 がこのグループに追加されます。

これらの仮想マシンを保護するには、次のように、プロキシをこのグループに追加することも必要です。

- PROXY-1 は、DATASTORE-1 と DATASTORE-2 の両方に割り当てられているため、VM-1 と VM-2 の両方を保護できます。
- PROXY-2 は、DATASTORE-2 のみに割り当てられているため、Proxy-1 がグループに存在する限り、オプションです。
- PROXY-3 は、DATASTORE-3 にのみ割り当てられているため、VM-1 または VM-2 を保護することはできません。

すべてのグループで、すべてのクライアントに割り当てられたすべてのデータストアをサポートするために十分なプロキシを含める必要があります。プロキシが不足すると、バックアップが開始され、バックアップを実行するためのプロキシが見つからない場合、バックアップは失敗し、アクティビティ監視ステータスが `no proxy` となります。

Avamar Administrator でのプロキシ データストアとグループの割り当ての変更

手順

1. Avamar Administrator で、［**Policy**］起動リンクをクリックします。

   ［**Policy**］ウィンドウが表示されます。

2. ［**Policy Management**］タブをクリックした後、［**Clients**］タブをクリックします。
3. プロキシを選択して、［**Edit**］をクリックします。

注

［**Show sub-domain clients**］をクリックすると、利用可能な仮想マシン クライアントがすべて表示されます。

［**Edit Client**］ダイアログ ボックスが表示されます。

4. ［**VMware**］タブをクリックした後、［**Datastores**］タブをクリックします。
5. 1 つ以上のデータストアを選択します。
6. ［**Groups**］タブをクリックします。
7. 1 つまたは複数のグループを選択します。
8. ［**OK**］をクリックします。

第 4 章

バックアップ

本章は、次のトピックで構成されています。

制限事項

VMware イメージ バックアップにおける Avamar の既知の制限事項は次のとおりです。

すべてのバックアップは AUI または Avamar Administrator から開始する必要がある
すべてのイメージ バックアップは AUI または Avamar Administrator から開始する必要があります。仮想マシンまたはプロキシからバックアップを開始することはできません。

仮想マシンのディスク構成を変更するとフル バックアップが強制される
仮想マシンのディスク構成を変更すると（ディスクの追加または取り外し）、次の全体イメージ バックアップは、フル バックアップとして処理され（すなわち、すべての仮想ディスクが処理され更新ブロック追跡が使用されない）、完了までにさらに時間がかかります。特定のディスクのバックアップは、そのディスクが今も Avamar にとって不明でない限り、影響を受けません。

複数のデータストアにディスクを搭載したバージョン 8 以降の仮想マシン
異なるデータストアに存在する複数のディスクを持つハードウェア バージョン 8 または 9 の仮想マシンをバックアップする場合、すべてのデータストアの孤立したスナップショットの確認が行われるわけではありません。すべての仮想ディスクが同じデータストアに存在するように仮想マシンを構成するのが、既知の唯一の対処法です。

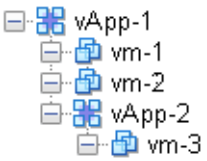
物理 RDM ディスクにかかわるバックアップ
仮想ディスクと物理 RDM ディスクの両方を持つ仮想マシンをバックアップする場合、バックアップは仮想ディスクを正常に処理し、RDM ディスクをバイパスし、完了すると次のイベント コードを表示します。

```
Event Code: 30929
Category: Application
Severity: Process
Summary: Virtual machine client contains disks that cannot be
backed up or restored.
```

ContainerClients ドメイン
ContainerClients ドメインは特別なシステム ドメインであり、VMware コンテナー エンティティに存在する仮想マシンが含まれます。Avamar では、VMware コンテナーが Avamar に追加されると、このコンテナーとその中のすべての仮想マシンが単一のオブジェクトとして常に管理されるものと見なします。そのため、これらの仮想マシンを VMware の親コンテナーに追加せずに、個々のマシンとしてバックアップ グループに追加すると、バックアップされません。

ネストされたコンテナーの制限事項
他のコンテナーを含む VMware コンテナー（つまり、ネストされたコンテナー構造）をバックアップする際、Avamar では階層の最上位レベルのみをバックアップします。次のネストされたコンテナー構造の例を見てみましょう。

図 5 ネストされたコンテナー構造の例



vApp-1 が Avamar にバックアップされると、vApp バックアップ イメージには vm-1 と vm-2 の仮想マシン バックアップ イメージのみが含まれます。vApp-1 バックアップがリストアされると、vm-1 と vm-2 のデータのみがリストアされます。vApp-2 コンテナーと vm-3 コンテナーも存在しますが、データは含まれません。

この制限に対して、2 つの暫定ソリューションがあります。

- コンテナー構造を平坦化する。
  たとえば、vm-3 を vApp-1 の下に移動します。そうすれば、vApp-1 がバックアップされたとき、3 個の仮想マシンがすべてバックアップされます。
- vApp-1 と vApp-2 の両方を別個のコンテナー エンティティとして Avamar に追加し、個別にバックアップできるようにします。
  リストアの際、vApp-1 を最初にリストアしてから、vApp-2 を vApp-1 にリストアします。

サブ仮想マシンのバックアップに失敗すると、vApp のバックアップも失敗する

vApp をバックアップする際、この vApp 内にあるすべての仮想マシンのバックアップも正常に完了する必要があります。そうでなければ、バックアップ全体が記録されません。正常に完了された仮想マシンのバックアップは、ContainerClients ドメインに保存されます。最大限のデータ保護を確保するため、失敗したバックアップすべてについて直ちに調査および修正を行うことが推奨されます。

AUI を使用して仮想マシンのオンデマンド バックアップを実行する

既存のスケジュールとポリシーから独立しているインスタンスのバックアップを実行できます。

手順

1. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Asset Management**］をクリックします。

   ［**Asset Management**］ウィンドウが表示されます。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、仮想マシン クライアント、VMware フォルダー、リソース プール、vApp のいずれかを選択します。
4. ［**BACKUP**］をクリックします。

   ［**Backup**］ウィザードが表示されます。［**Plugin**］パネルで、クライアント上のプラグ インのリストが表示されます。
5. ［**Plugin**］パネルで、次の手順を実行します。
   a. バックアップするデータを参照して、その横に表示されるチェックボックスを選択します。
   b. ［**NEXT**］をクリックします。

      ［**Basic Configuration**］ウィンドウが表示されます。
6. ［**Basic Configuration**］パネルでは、次の手順を実行します。
   a. バックアップの保存ポリシー設定を選択します。
      - ある特定の時間が経過した後に、Avamar サーバからこのバックアップを自動的に削除する場合は、［**Retention period**］を選択します。保存期間の日数、週数、月数、年数を指定します。
      - ある特定のカレンダー日付に、Avamar サーバからこのバックアップを自動的に削除する場合は、［**End date**］を選択し、カレンダーでその日付を探します。
      - このクライアントが Avamar サーバーでアクティブである限り、このバックアップを保持する場合は、［**No end date**］を選択します。

   b. ［**Avamar encryption method**］リストで、バックアップ中にクライアントと Avamar サーバー間のデータ転送に使用する暗号化方式を選択します。

      クライアント/サーバー間の接続における暗号化テクノロジーおよびビットの強度は、クライアントのオペレーティング システムおよび Avamar サーバーのバージョンをはじめ、さまざま

な要因によって異なります。詳細については、「Avamar 製品セキュリティ ガイド」を参照してください。

c. [**Optionally select a proxy to perform backup**] リストで、プロキシを選択します。

デフォルト設定は [**Automatic**] であり、これにより Avamar サーバーはこの操作に最適なプロキシを選択できます。

d. [**NEXT**] をクリックします。

[**More Options**] ウィンドウが表示されます。

7. [**More Options**] パネルで、プラグイン オプションを次のように設定します。

[**Show Advanced Options**] スイッチをオンにして、詳細な構成オプションを表示します。高度なバックアップ オプションの詳細については、Set advanced plug-in options in the AUI を参照してください。

基本的なバックアップ オプションの詳細については、VMware Image backup plug-in options を参照してください。

8. [**FINISH**] をクリックします。

以下のステータス メッセージが表示されます：

```
Backup initiated.
```

AUI における詳細プラグ イン オプションの設定

オン デマンド バックアップを実行する場合は、[**More Options**] ウィンドウで次のオプション タスクを実行します。

手順

1. [**Show Advanced Options**] スイッチをオンに切り替えます。
2. 更新ブロック追跡を有効化するには、[**Use Changed Block Tracking (CBT) to increase performance**] チェックボックスを選択します。
3. Avamar サーバが最新のバックアップと最新の正常なバックアップに関する情報を vSphere Client にレポートできるようにするには、[**Set Annotionation Tag LastBackupStatus and LastSuccessfulBackup**] チェック ボックスを選択します。

選択した場合、vSphere Web Client に次の情報が表示されます。

- LastSuccessfulBackupStatus-com.dellemc.avamar：最新の正常なバックアップの日時。
- LastBackupStatus-com.dellemc.avamar：成功か失敗かにかかわらず、最新のバックアップの日時。

4. VMware イメージ バックアップのインデックスを作成するには、[**Index VMware Image Backups**] を選択します。
5. バックアップから Windows のページ ファイル（`pagefile.sys`）を除外するには、[**Exclude page file blocks when performing image backup on Windows VM**] を選択します。

注

ページ ファイルの除外は、Windows Server 2008 R2 以降のバージョンに対してのみサポートされます。クライアント バージョンの Windows では、このオプションは効果がありません。このページ ファイルは、この設定に関係なく、Windows クライアントのバックアップに含まれています。

6. 削除されたファイル ブロックをバックアップから除外するには、［**Exclude deleted file blocks when performing image backup on Windows VM**］を選択します。
7. ［**Exclude files with path and filter**］フィールドには、除外するファイルを入力します。

注

バックアップ中にファイルを除外してから、除外されたファイルのリストアを試行した場合、除外されたファイルは表示されますが、不安定です。

8. このバックアップを Data Domain システムに保存するには、［**Store backup on Data Domain System**］チェックボックスを選択した後、リストから Data Domain システムを選択します。
9. ［**Encryption method to Data Domain system**］リストから、バックアップ中にクライアントと Data Domain システム間のデータ転送に使用する暗号化方式を選択します。
10. Windows VMware イメージ プラグインの場合のみ、1 つ以上のスナップショットのキューエス オプションを選択します。オプションには、次のようなものがあります。
    - スナップショットのキューエス エラーでのバックアップ失敗。
    - VMware Tools が実行されていない場合は、完了したバックアップを「Completed w/ Exception」としてマークします（アプリケーションは停止しません）。
11. ［**Max times to retry snapshot delete**］オプションで、スナップショットの削除操作が試行される最大回数を入力します。
12. ［**Guest Credentials**］に、バックアップの前後にスクリプトを実行できる権限を持った仮想マシンのゲスト OS のユーザー アカウント名とパスワードを入力します。

    Exchange サーバーのログ トランケート バックアップの場合、ゲスト認証情報には管理者権限が必要です。複数の仮想マシンをバックアップする場合、すべての仮想マシンに対して同じゲスト認証情報を使用する必要があります。
13. vmdk スナップショットの前にスクリプトを実行するには、次の手順を実行します。
    a. 実行するスクリプトのフル パスとファイル名を入力します。
    b. スクリプトを完了するために十分なスクリプトのタイムアウトが設定されていることを確認します。
14. バックアップが完了して vmdk スナップショットが削除された後に、スクリプトを実行するには、以下の手順を実行します。
    a. 実行するスクリプトのフル パスとファイル名を入力します。
    b. スクリプトを完了するために十分なスクリプトのタイムアウトが設定されていることを確認します。
15. Windows VMware イメージ プラグ インに対してのみ、［**Snapshot quiesce timeout (minutes)**］フィールドで、スナップショットの停止操作が失敗したと見なされるまでの待機時間（分）を入力します。

16. Microsoft SQL Server のイメージ バックアップを実行する場合は、認証のタイプを選択します。
    - ［**NT Authentication**］には、認証について［**Guest Credentials**］に入力した認証情報が使用されます。
    - ［**Application Authentication**］では、［**SQL Server Username**］と［**SQL Server Password**］を使用して SQL Server にログインします。
17. Microsoft SQL Server のイメージ バックアップを実行する場合は、バックアップ後のアクションのオプションを特定します。
    - バックアップ後の処理（post-action）操作が失敗したと見なされるまでの最大待機時間（分）を、［**Post Action Timeout (minutes)**］オプションに入力します。
    - バックアップ後の処理の操作タイプを選択します。［**LOG Truncation**］では、バックアップが正常に完了した後にログのトランケートを実行します。
    - 仮想マシンのすべてのディスクをオン デマンド バックアップ用に選択する必要があります。選択しない場合は、ログのトランケートは発生しません。
18. Microsoft Exchange Server のイメージ バックアップを実行する場合は、バックアップ後の処理の操作タイプを選択します。［**LOG Truncation**］では、バックアップが正常に完了した後にログのトランケートを実行します。
19. ［**FINISH**］をクリックします。

AUIPolicy ウィザードを使用したバックアップのスケジュール設定

スケジュール設定されたバックアップは自動的に実行され、バックアップが継続的に実行されるようにします。バックアップを毎日、毎週、毎月実行するようにスケジュール設定できます。

Policy ウィザードを使用してバックアップ ポリシーを作成することにより、バックアップのスケジュールを設定できます。

［**Policy**］ウィザードで次の手順を実行します。ポリシー、データセット、スケジュール、および保存設定の詳細については、「Avamar Administration Guide」を参照してください。

手順

1. 新しいバックアップ ポリシーにメンバーを割り当てます。
2. 新しいバックアップ ポリシーにデータセットを割り当てます。

   データセットを作成するには、［Policy］ウィザードを使用するか、［**Settings**］ > ［**Dataset**］ > ［**Add**］を選択します。
3. 新しいバックアップ ポリシーをスケジュールに割り当てます。

   スケジュールを作成するには、［Policy］ウィザードを使用するか、［**Settings**］ > ［**Schedule**］ > ［**Add**］を選択します。
4. 新しいバックアップ ポリシーに保存ポリシーを割り当てます。

   保存ポリシーを作成するには、［Policy］ウィザードを使用するか、［**Settings**］ > ［**Retention**］ > ［**Add**］を選択します。
5. バックアップ ポリシーのスケジュール設定を有効にします。

データセットの作成

データセットでは、スケジュール設定されたバックアップに含まれるデータと、バックアップに使用するオプションを指定します。1 個のクライアントまたはクライアントのグループで実行するスケジュール設定され

たバックアップ用に、少なくとも 1 個のデータセットを作成してください。クライアント データを分離するには、複数のデータセットを作成します。

手順

1. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Settings**］をクリックします。

   ［**Setting**］パネルが表示されます。

2. ［**Dataset**］タブをクリックします。
3. ［**ADD**］をクリックします。

   ［**Create Dataset**］ウィンドウが表示されます。

4. ［**Dataset Name**］フィールドに、データセットの名前を入力します。

   名前には、英数字（A-Z、a-z、0-9）および次の特殊文字を含めることができます。ピリオド（.）、ハイフン（-）、下線（_）。Unicode 文字または次に示す特殊文字は使用しないでください。` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?

5. ［**Plugins**］リストで、ご使用のオペレーティング システムに適した［**VMware**］プラグインを選択します。

   ［**VMware**］プラグイン オプションが表示されます。

6. ［**Options**］タブをクリックし、プラグイン オプションを設定します。

   ［**Show Advanced Options**］を選択して、詳細オプションを表示します。

   Plug-in Options では、VMware プラグイン オプションの詳細なリストが表示されます。

7. ［**Source Data**］タブをクリックして、プラグイン オプションを次のように設定します。

   - すべての仮想マシンを含めるには、［**All virtual disks**］を選択します。
   - データセットを特定のアイテムだけに制限するには、次の手順を実行します。

     a. ［**File/Folder Path**］で、ファイル パスを入力します。

     b. ［**ADD**］をクリックします。

   デフォルトでは、データセット エントリーに絶対パス表記を使用します。例：

   ```
   [datastore1] VM1/VM1.vmdk
   ```

   ただし、相対パス表記を使用して、特定の .vmdk が常にバックアップに含まれるようにすることが可能です。Storage vMotion を使用して、その仮想マシンを別のデータストアに移行した場合もこれを含めることができます。例えば、次のような同等のデータセット エントリーでは、相対パス表記を使用します。

   ```
   \[.*\] VM1/VM1.vmdk
   ```

8. ［[**Submit**]］をクリックします。

バックアップ ポリシーの作成

バックアップ ポリシーは、スケジュール設定されたバックアップを実装するために、同じデータセット、スケジュール、保存期間の設定を使用する Avamar クライアントのコレクションです。

メンバー クライアントは、すべて同じ Avamar ドメインに存在する必要があります。バックアップ ポリシーを作成するときに、スケジュール設定されたバックアップに適用するデータセット、スケジュール、保存期間の設定を定義します。これらのバックアップ ポリシーによって構成される設定は、これらの設定がクライアント レベルでオーバーライドされない限り、バックアップ ポリシーの全メンバーのバックアップ動作を制御します。

バックアップ ポリシー、スケジュール、または保存期間の設定の作成と編集については、「Avamar Administration Guide」を参照してください。

バックアップ ポリシーのスケジュール バックアップを有効にする

スケジュール バックアップは、有効化されたバックアップ ポリシーでのみ実行されます。［**New Group**］ウィザードの最初のページで［**Enabled**］チェックボックスを選択しない限り、バックアップ ポリシーはデフォルトで無効化されています。バックアップ ポリシーを作成したときに有効化しなかった場合は、［**Policy**］ウィンドウのメニュー オプションを使用して、バックアップを有効化します。

手順

1. 左側の AUI ナビゲーション ペインで、［≫］をクリックしてから、［**Backup Policy**］をクリックします。

   ［**Policy**］ページが表示されます。
2. ドメイン ツリーで、バックアップ ポリシーのドメインまたはサブドメインを選択します。

   バックアップ ポリシーのサブドメインを選択するには、［**Include Sub-domain**］スイッチをオンに切り替えます。
3. リストからバックアップ ポリシーを選択します。
4. バックアップ ポリシーを有効化するには、［**MORE ACTIONS**］ > ［**Enable Policy**］をクリックします。
5. バックアップ ポリシーを無効化するには、［**MORE ACTIONS**］ > ［**Disable Policy**］をクリックします。

自動的にバックアップ ポリシーに仮想マシンを含む

自動検出機能の一環として、自動検出された仮想マシンがルールを使用して自動的にバックアップ ポリシーに割り当てられます。このように、仮想マシンが vCenter で作成されたときにバックアップ ポリシーを自動的に割り当てることができます。この処理手順では、自動検出された仮想マシンにバックアップ ポリシーを自動的に割り当てるルールを使用するようにスケジュール設定されたバックアップを設定する方法について説明します。

注

仮想マシンの自動検出（37 ページ） で、仮想マシンの自動検出の設定方法について説明します。

手順

1. バックアップ ポリシーの作成
2. ポリシー ウィザードの［**Members**］ページで、［**Enable Dynamic rule**］を選択します。
3. ［**Rule**］ドロップダウン リストから、次のいずれかのステップを実行します。
   - 既存のルールを選択。
   - ［**New Rule...**］を選択。
     ［**New Rule...**］を選択した場合、ルールを作成します。

   ルールを選択してこのバックアップ ポリシーに自動的に割り当てられた仮想マシンが表示されます。
4. 自動的に割り当てられていないバックアップ ポリシーにクライアントを追加するには、次のステップを実行します。

a. クライアントのリストで、追加するクライアントを選択します。
b. [**NEXT**] をクリックします。

注

一般的に、仮想マシンの自動検出を使用しているバックアップ ポリシーに、クライアントを手動で含めることはお勧めしません。自動メンバー選択を本来の目的のみに使用するようにバックアップ ポリシーを維持し、自動検出されない仮想マシンのクライアント用に別のバックアップ ポリシーを作成することをお勧めします。

このタスクが完了すると、Avamar サーバーは選択したクライアントにバックアップ ポリシーを適用します。

5. 自動的に割り当てられたこのバックアップ ポリシー内のクライアントを除外するには、次のステップを実行します。
   a. クライアントのリストで、削除するクライアントを選択します。
   b. [**NEXT**] をクリックします。

   この手順により、選択したクライアントとバックアップ ポリシー間の関連が削除されます。このタスクが完了すると、バックアップ ポリシーが選択したクライアントに適用されることはありません。

   注

   一般的に、仮想マシンの自動検出を使用しているバックアップ ポリシーで、クライアントを手動で除外することはお勧めしません。グループに含まれる必要のある仮想マシンだけがそのバックアップ ポリシーに自動的に割り当てられるように、ルールと仮想マシンを適切に設定することをお勧めします。

   ---

6. [**NEXT**] をクリックします。

役割の作成

ルールを使用して、自動検出された仮想マシンをドメインに自動的にマッピングして、自動検出された仮想マシンにバックアップ ポリシーを割り当てます。ルールでは、1 つまたは複数のフィルタリング メカニズムを使用して、仮想マシンがルール下で認定されるかどうかを決定します。

ルール作成の詳細については、「Avamar Administration Guide」を参照してください。

ログ トランケート バックアップ

Avamar リリース 7.4 以降では、Microsoft SQL および Microsoft Exchange のイメージ バックアップが正常に実行された後のログのトランケートをサポートしています。これにより、バックアップ ウィンドウを短縮できるとともに、データベースのログに必要なディスク領域も縮小できます。次のセクションでは、スケジュール設定されたログ トランケート バックアップを設定する方法について説明します。

Microsoft SQL ログのトランケートを伴うスケジュール設定されたバックアップ

バックアップの完了後に、SQL Server データベースのログのトランケートを実行します。

このセクションでは、ログのトランケートを実行するバックアップのスケジュール設定方法について説明します。

複数の仮想マシンを含むバックアップのスケジュール設定には、SQL データベースをホストする仮想マシンを選択する自動化されたメカニズムが必要です。ルールには、仮想マシン名または VM タグな

どのフィルター メカニズムが含まれ、ルールに基づき認定する仮想マシンが判断されます。vCenter 内から SQL データベースを正しくホストする仮想マシンを構成し、対応するルールを設定すると、複数仮想マシンのバックアップ内のどの仮想マシンでログのトランケートが実行されたのかを判断できます。

SQL ログ トランケートの実行前に必要なフル バックアップ

ログ トランケートを実行する前に、フル バックアップが必要です。

まだフル バックアップを取ったことのないデータベースのバックアップを実行すると、ログのトランケートは失敗します。ログのトランケートを実行する前に、SQL Server のネイティブ バックアップまたはフル Avamar バックアップを使用してフル データベース バックアップを実行する必要があります。

ログのトランケート用 Microsoft SQL Server のバックアップのスケジュール設定

Microsoft SQL Server のログのトランケート用にスケジュール設定されたバックアップは、次の処理手順を使用して設定されます。

次の手順に従って、Microsoft SQL Server バックアップ用のデータセットを作成し、ログのトランケート用に Microsoft Exchange Server のバックアップをスケジュール設定します。

手順

1. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Settings**］をクリックします。

   ［**Setting**］パネルが表示されます。
2. ［**Dataset**］タブをクリックします。
3. ［**ADD**］をクリックします。

   ［**Create Dataset**］ウィンドウが表示されます。
4. ［**Dataset Name**］フィールドに、データセットの名前を入力します。

   名前には、英数字（A-Z、a-z、0-9）および次の特殊文字を含めることができます。ピリオド（.）、ハイフン（-）、下線（_）。Unicode 文字または次に示す特殊文字は使用しないでください。` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?
5. ［**Plugins**］リストで、［**Windows VMware Image**］プラグインを選択します。
6. ［**Options**］タブをクリックして、次のステップを実行します。
   a. 詳細オプションを表示するには、［**Show Advanced Options**］チェックボックスを選択します。
   b. ［**Guest Credentials**］フィールドに、バックアップの前後にスクリプトを実行できる権限を持った仮想マシンのゲスト OS のユーザー アカウント名とパスワードを入力します。
   c. ［**Microsoft SQL Server authentication**］フィールドで、認証のタイプを選択します。
      - ［**NT Authentication**］には、認証について［**Guest Credentials**］に入力した認証情報が使用されます。Windows 認証をすべての SQL Server インスタンスで有効にする必要があります。ログのトランケートを使用する場合、ここで入力するユーザーは、すべての SQL Server インスタンスのすべてのデータベースでログのトランケートを実行するための十分な権限が必要です。
      - ［**Application Authentication**］では、［**SQL Server Username**］と［**SQL Server Password**］を使用して SQL Server にログインします。ここのリストにあるユーザー資格情報は、ターゲット仮想マシンで実行しているすべての SQL Server インスタンスへのログインに使用されます。

d. [**Microsoft SQL Server post action**] フィールドで、バックアップ後の処理オプションを識別します。

- バックアップ後の処理（post-action）操作が失敗したと見なされるまでの最大待機時間（分）を、[**Post Action Timeout (minutes)**] オプションに入力します。
- バックアップ後の処理の操作タイプを選択します。[**LOG Truncation**] では、バックアップが正常に完了した後にログのトランケートを実行します。

e. [Options] タブで、必要に応じてその他の情報を入力します。

データセットの作成と設定の詳細については、「Avamar Administration Guide」を参照してください。

7. [**Source Data**] タブをクリックして、[**All virtual disks**] を選択します。
8. [[**Submit**]] をクリックします。
9. 複数のゲスト仮想マシンをこのバックアップ ポリシーの一部としてバックアップする場合は、ログのトランケートを実行する適切な仮想マシンの選択に使用するルールを作成します。
10. バックアップのバックアップ ポリシーを作成します。

バックアップ ポリシーの作成プロセスでは、次の操作を実行します。

a. 新しいデータセットを新しいバックアップ ポリシーに割り当てます。

b. スケジュールを新しいバックアップ ポリシーに割り当てます。

c. 保存ポリシーを新しいバックアップ ポリシーに割り当てます。

d. このバックアップ ポリシーの一部として複数のゲスト仮想マシンがバックアップされている場合は、[Policy] ウィザードの [**Members**] パネルで、[**Enable Dynamic rule**] を選択し、以前に作成したルールを選択します。

バックアップ ポリシー、ルール、データセット、スケジュール、保存ポリシーの詳細については、「Avamar Administration Guide」を参照してください。

11. バックアップ ポリシーのスケジュール設定を有効にします。

Microsoft Exchange ログのトランケートを伴うスケジュール設定されたバックアップ

Avamar では、バックアップの完了後に、Exchange Server データベースのログのトランケートを実行します。

このセクションでは、ログのトランケートを実行するバックアップのスケジュール設定方法について説明します。

複数の仮想マシンを含むバックアップのスケジュール設定には、Exchange データベースをホストする仮想マシンを選択する自動化されたメカニズムが必要です。ルールには、仮想マシン名または VM タグなどのフィルター メカニズムが含まれ、ルールに基づき認定する仮想マシンが判断されます。vCenter 内で Exchange データベースを正しくホストする仮想マシンを構成し、対応するルールを設定すると、複数仮想マシンのバックアップ内のどの仮想マシンでログのトランケートが実行されたのかを判断できます。

Microsoft Exchange でログのトランケートは、以下の場合にサポートされます。

- vSphere 6.5 以降および ESXi 6.5 以降
- Windows Server 2008 R2 以降
- Exchange 2007 以降

- VMware Tools リリース 10.1 以降が Exchange サーバーをホストする仮想マシンにインストールされている。

ログのトランケート用 Microsoft Exchange Server のバックアップのスケジュール設定

Microsoft Exchange Server のログのトランケート用にスケジュール設定されたバックアップは、次の処理手順を使用して設定されます。

次の手順に従って、Exchange Server バックアップ用のデータセットを作成し、ログのトランケート用に Microsoft Exchange Server のバックアップをスケジュール設定します。

手順

1. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Settings**］をクリックします。

   ［**Setting**］パネルが表示されます。
2. ［**Dataset**］タブをクリックします。
3. ［**ADD**］をクリックします。

   ［**Create Dataset**］ウィンドウが表示されます。
4. ［**Dataset Name**］フィールドに、データセットの名前を入力します。

   名前には、英数字（A-Z、a-z、0-9）および次の特殊文字を含めることができます。ピリオド（.）、ハイフン（-）、下線（_）。Unicode 文字または次に示す特殊文字は使用しないでください。` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?
5. ［**Plugins**］リストで、［**Windows VMware Image**］プラグインを選択します。
6. ［**Options**］タブをクリックして、次のステップを実行します。
   a. 詳細オプションを表示するには、［**Show Advanced Options**］チェックボックスを選択します。
   b. ［**Guest Credentials**］フィールドに、バックアップの前後にスクリプトを実行できる権限を持った仮想マシンのゲスト OS のユーザー アカウント名とパスワードを入力します。
   c. バックアップ後の処理の操作タイプを選択します。［**LOG Truncation**］では、バックアップが正常に完了した後にログのトランケートを実行します。
   d. ［**Options**］タブで、必要に応じてその他の情報を入力します。

      データセットの作成と設定の詳細については、「Avamar Administration Guide」を参照してください。
7. ［**Source Data**］タブをクリックして、［**All virtual disks**］を選択します。
8. ［[**Submit**]］をクリックします。
9. 複数のゲスト仮想マシンをこのバックアップ ポリシーの一部としてバックアップする場合は、ログのトランケートを実行する適切な仮想マシンの選択に使用するルールを作成します。
10. バックアップのバックアップ ポリシーを作成します。

    バックアップ ポリシーの作成プロセスでは、次の操作を実行します。
    a. 新しいデータセットを新しいバックアップ ポリシーに割り当てます。
    b. スケジュールを新しいバックアップ ポリシーに割り当てます。
    c. 保存ポリシーを新しいバックアップ ポリシーに割り当てます。
    d. このバックアップ ポリシーの一部として複数のゲスト仮想マシンがバックアップされている場合は、［Policy］ウィザードの［**Members**］パネルで、［**Enable Dynamic rule**］を選択し、以前に作成したルールを選択します。

バックアップ ポリシー、ルール、データセット、スケジュール、保存ポリシーの詳細については、「Avamar Administration Guide」を参照してください。

11. バックアップ ポリシーのスケジュール設定を有効にします。

バックアップのモニタリング

［**Activity Monitor**］を使用して、バックアップ/リストア処理のステータス情報を監視および表示することができます。

［**Activity Monitor**］にアクセスするには、ナビゲーション ペインを開き、［**Activity**］をクリックします。［**Activity Monitor**］に、すべてのアクティビティのリストが表示されます。

注

AUI ［**Activity Monitor**］ウィンドウは、1366 ピクセル以上の画面に合わせて最適化されています。小さな画面では、表示の問題が発生する可能性があります。AUI を正しく表示するには、ディスプレイの幅が 1366 ピクセル以上であることを確認します。

［**Activity Monitor**］には、表示される情報をフィルターするためのオプションが用意されています。

- アクティビティを期間別にフィルター：デフォルトでは、［**Activity Monitor**］には最新の 5000 クライアント アクティビティが表示されます。別の期間を選択するには、［**Filter activities by duration**］ドロップダウン リストで、［**Last 24 hours**］または［**Last 72 hours**］を選択します。
- ドメイン別にアクティビティをフィルター：デフォルトでは、［**Activity Monitor**］にはドメインに関係なくすべてのアクティビティが表示されます。特定のドメインのアクティビティのみを表示するには、［**Filter activities by domain**］ドロップダウン リストで、ドメインまたはサブドメインを選択します。
- ステータス別にアクティビティをフィルター：デフォルトでは、［**Activity Monitor**］にはステータスに関係なくすべてのアクティビティが表示されます。
  特定のステータスのアクティビティのみを表示するには、［**Activity Monitor**］の上部で、次のいずれかのオプションを選択します。
  - キャンセル済み
  - Completed
  - Completed with Exceptions（完了したが例外発生）
  - Failed
  - Running
  - Waiting

アクティビティをクライアント、開始時刻、プラグ イン、またはタイプ別にフィルターするには、それぞれの列で［ ］をクリックします。

［**Activity Monitor**］には、アクティビティの開始日時と、アクティビティ中に検証された合計バイト数が表示されます。

アクティビティの詳細を表示するには、［ ］をクリックして、［**Details**］パネルを展開します。

バックアップのキャンセル

バックアップは完了前であればいつでもキャンセルできます。キャンセルには、5 分以上かかる場合があります。バックアップがキャンセルよりも前に完了することがあります。

手順

1. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Activity**］をクリックします。

   ［**Activity Monitor**］にアクティビティのリストが表示されます。
2. リストからバックアップを選択します。
3. ［**CANCEL**］をクリックします。

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

インフライト バックアップ用 vCenter HA フェールオーバーのサポート

vCenter のフェールオーバーの間、Avamar ソフトウェアはフェールオーバー プロセスを監視し、次のアクションを実行します。

1. vCenter のフェールオーバー イベントを自動的に検出して、vCenter のフェールオーバーが完了するまで待機します。
2. vCenter の HA フェールオーバーが原因で異常停止しているバックアップ ジョブをキャンセルします。
3. マウントされている HotAdded ディスクをプロキシ アプライアンスから削除します。
4. vCenter HA フェールオーバーの間にすべての未完了のバックアップを再開します。

VMware 暗号化をサポートするバックアップの構成

Avamar では、暗号化された仮想マシンのバックアップをサポートします。

はじめに

- VMware 暗号化をサポートするバックアップを構成する上で、既知の制限事項を確認します。
- 暗号化された仮想マシンをバックアップまたはリストアするには、プロキシ アプライアンスも暗号化されていることを確認します。
- プロキシ アプライアンスがバックアップ ポリシーに手動でマッピングされていることを確認します。

仮想マシン暗号化の詳細については、VMware の「vSphere Security Guide」を参照してください。

暗号化された仮想マシンをバックアップする場合は、次のステップを実行します。

手順

1. 仮想マシンの暗号化を確立します。
   a. KMS をセットアップします。
   b. VM 暗号化ポリシーを作成します。
2. プロキシ アプライアンスを暗号化します。

3. Linux テキスト エディタを使用して`/usr/local/avamarclient/var/vddkconfig.ini` を開きます。
4. 値 `vixDiskLib.transport.hotadd.NoNFCSession` を見つけます。
5. 値を 0 に変更します。

   この変更は、暗号化された仮想マシンのホット アドを阻害する VMware VDDK バグを上書きします。詳細については、VMware リリース ノートに記されています。
6. ファイルを保存して閉じます。
7. Avamar 管理者ロールに対して次の権限を設定します。

   [**Crytopgraphic Operations**] > [**Add Disk**]。

   [**Crytopgraphic Operations**] > [**Direct Access**]。

VMware 暗号化サポートに関する制限事項

VMware 暗号化サポートに関して、以下に示す Avamar の既知の制限事項を考慮してください。

- NoNFCSession を無効化した結果、VMware Cloud on AWS でのバックアップとリストアはサポートされません。この VMware の制限事項については、vddk の更新で対処します。
- 暗号化された仮想マシンとバックアップからリストアする場合、リストアされたデータは暗号化されません。
- 仮想マシンをリストアするには、ソース vCenter と同じ KMS（キー管理サービス）ホストに対してターゲット vCenter が構成されている必要があります。
- 暗号化された仮想マシンでアプリケーション コンシステントなキューエス スナップショットを実行しようとすると、ファイル システム コンシステントなスナップショットにフェイルバックされます。このプロセスにより、vCenter にエラー メッセージが生成されます。これは無視しても問題ありません。これは、VMware の制限によるものです。
- 新しいイメージとして仮想マシンをリストアする場合は、次のようになります。
  - デフォルトでは、新しい仮想マシンは暗号化されません。暗号化が必要な場合は、必要なストレージ ポリシーを適用します。
  - イメージ バックアップを実行する前に、デフォルト以外の起動順序が実装されていた場合、元の起動順序はリストアされません。この場合、リストアが完了した後、正しいブート デバイスを選択する必要があります。または、デフォルト以外の起動順序を VMX ファイルに入力して、リストアされた仮想マシンが再構成せずに開始されるようにすることもできます。
    この制限は、デフォルトの起動順序を使用する仮想マシンには影響しません。

vSAN 暗号化をサポートするバックアップの構成

Avamar では、暗号化された vSAN のバックアップがサポートされています。

はじめに

vSAN 暗号化の詳細については、VMware の「Administering VMware vSAN Guide」を参照してください。

vSAN 暗号化をサポートするバックアップを構成する前に、次の点を考慮します。

- vSAN データストアに存在する仮想マシンをバックアップまたはリストアするには、vSAN データストアにプロキシを導入します。

- ホット アドまたは nbdssl 転送モードを使用して、vSAN データストアに導入されているプロキシを使用し、他の vSAN データストア（暗号化済みまたは暗号化されていない）の仮想マシンをバックアップすることができます。
- ホット アドまたは nbdssl 転送モードを使用して、vSAN データストアに導入されているプロキシを使用し、他の vSAN データストア以外の仮想マシンをバックアップすることができます。
- Avamar では、暗号化された vSAN 仮想マシンのすべてのバックアップ/リストア機能がサポートされています。
- Avamar では、暗号化された vSAN 仮想マシンの暗号化されていないデータストアを持つ別の vCenter へのリストアがサポートされています。

手順

1. Avamar 管理者ロールに対して次の権限を設定します。

   ［**Cryptographic Operations**］ > ［**Add Disk**］。

   ［**Cryptographic Operations**］ > ［**Direct Access**］。

2. バックアップのバックアップ ポリシーを作成します。

   注

   vSAN 仮想マシンをバックアップするには、vSAN データストアにプロキシを導入します。

Data Domain へのバックアップ適用

Data Domain システムへバックアップを適用するように Avamar サーバーが構成されている場合、サーバーは、Data Domain に送信されないバックアップを拒否します。この適用は、Avamar Administrator、AUI、コマンドライン インターフェイス、その他のツールから構成したバックアップを対象としています。

これらのバックアップには、ストレージ ターゲットを示す追加のフラグが必要です。バックアップの適用および関連するクライアントのバージョン要件の詳細については、「Avamar および Data Domain システム統合ガイド」を参照してください。バックアップの適用は、デフォルトでは無効になっています。

第 5 章

リストア

本章は、次のトピックで構成されています。

イメージ リストアとファイル レベル リストアのガイドライン

Avamar は、仮想マシン データのリストアに関して 2 つの特徴的なメカニズムを提供します。イメージ リストアは、イメージ全体または選択したドライブをリストアでき、ファイル レベル リストアは、特定のフォルダーまたはファイルをリストアできます。

イメージ リストアは、あまりリソースを消費しないため、大量のデータの迅速なリストアに最適です。

ファイル レベルのリストアは、より多くのリソースを消費するため、比較的少量のデータのリストアに最適です。

大量のフォルダーやファイルをリストアする場合、パフォーマンスの観点から、イメージ全体または選択したドライブを一時的な場所（新しい一時仮想マシンなど）にリストアした方が望ましいでしょう。リストアの後で、目的の場所にそれらのファイルをコピーします。

リストアの監視

［**Activity Monitor**］では、バックアップおよびリストア処理のステータス情報を監視および表示することができます。

［**Activity Monitor**］にアクセスするには、ナビゲーション ペインを開き、［**Activity**］をクリックします。［**Activity Monitor**］に、すべてのアクティビティのリストが表示されます。

注

AUI ［**Activity Monitor**］ウィンドウは、1366 ピクセル以上の画面に合わせて最適化されています。小さな画面では、表示の問題が発生する可能性があります。AUI を正しく表示するには、ディスプレイの幅が 1366 ピクセル以上であることを確認します。

［**Activity Monitor**］には、表示される情報をフィルターするためのオプションが用意されています。

- アクティビティを期間別にフィルター：デフォルトでは、［**Activity Monitor**］には最新の 5000 クライアント アクティビティが表示されます。別の期間を選択するには、［**Filter activities by duration**］ドロップダウン リストで、［**Last 24 hours**］または［**Last 72 hours**］を選択します。
- ドメイン別にアクティビティをフィルター：デフォルトでは、［**Activity Monitor**］にはドメインに関係なくすべてのアクティビティが表示されます。特定のドメインのアクティビティのみを表示するには、［**Filter activities by domain**］ドロップダウン リストで、ドメインまたはサブドメインを選択します。
- ステータス別にアクティビティをフィルター：デフォルトでは、［**Activity Monitor**］にはステータスに関係なくすべてのアクティビティが表示されます。
  特定のステータスのアクティビティのみを表示するには、［**Activity Monitor**］の上部で、次のいずれかのオプションを選択します。
  - キャンセル済み
  - Completed
  - Completed with Exceptions（完了したが例外発生）
  - Failed
  - Running
  - Waiting

アクティビティをクライアント、開始時刻、プラグ イン、またはタイプ別にフィルターするには、それぞれの列で［ ］をクリックします。

［**Activity Monitor**］には、アクティビティの開始日時と、アクティビティ中に検証された合計バイト数が表示されます。

アクティビティの詳細を表示するには、［《］をクリックして、［**Details**］パネルを展開します。

リストアのキャンセル

リストアは完了前であれいつでもキャンセルできます。キャンセルには、5 分以上かかる場合があります。リストアがキャンセルの終了よりも前に完了することがあります。

手順

1. 左側の AUI ナビゲーション ペインで、［»］をクリックしてから［**Activity**］をクリックします。

   ［**Activity Monitor**］にアクティビティのリストが表示されます。
2. リストからリストアを選択します。
3. ［**CANCEL**］をクリックします。

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

インスタント アクセス

Data Domain システムに保存されているバックアップから仮想マシン全体をリストアする場合は、「インスタント アクセス」と呼ばれる特別な機能を使用できます。

インスタント アクセスは、イメージ バックアップを新しい仮想マシンにリストアする操作に類似していますが、リストアされた仮想マシンを Data Domain システムから直接起動できる点が異なります。このステップにより、仮想マシン全体のリストアの所要時間が短縮されます。

インスタント アクセスを可能にするには、次のタスクを実行します。

1. 仮想マシンをリストアします。
   - インスタント アクセスが開始されます。
   - 選択した VMware バックアップが、Data Domain システムの一時 NFS 共有にコピーされます。
2. リストア後の移行とクリーンアップを実行します。
   - vSphere Client または vSphere Web Client から、仮想マシンの電源をオンにし、Storage vMotion を使用して仮想マシンを Data Domain NFS 共有から vCenter 内のデータストアに移行します。
   - Storage vMotion が完了すると、リストアされた仮想マシンのファイルは Data Domain システムに存在しなくなります。
   - Avamar Administrator から、Data Domain NFS 共有が削除されていることを確認します。

注

リリース 6.0 より前の Data Domain システムを使用している場合、Data Domain システムへのオペレーショナル インパクトを最小限に抑えるために、一度に実行できるインスタント アクセスは 1 件のみです。リリース 6.0 以上の Data Domain システムの場合は、同時に実行できるインスタンス アクセス プロセスは 32 件です。複数のインスタント アクセス プロセスのターゲットに同じ ESXi ホストを使用する場合、32 件のインスタント アクセス プロセスを実行するには、ESXi ホストでの次の設定の値をサポートされている最大値に増やす必要があります。

- NFS で、NFS.MaxVolumes を更新します。
- Net で、Net.TcpipHeapSize を更新します。
- Net で、Net.TcpipHeapMax を更新します。

この設定の制限を増やす方法の詳細については、VMware KB 記事 2239 を参照してください。仮想マシンの同時移行の制限事項についての VMware ドキュメントも参照してください。

仮想マシンのリストア

手順

1. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Asset Management**］をクリックします。

   ［**Asset Management**］ウィンドウが表示されます。

2. ドメイン ツリーで、仮想マシン クライアントまたは VMware コンテナを含むドメインを選択します。

   ログイン アカウントの対象となるドメイン外のクライアントは表示することはできません。すべてのクライアントを表示するには、root ドメインにログインします。

3. クライアントのリストから、仮想マシン クライアントまたは VMware コンテナを選択します。

   このインスタンスの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、インスタンスのリストアに使用できます。

4. （オプション）日付によりバックアップを検索するには、次のようにします。

   a. 右側のパネルで、［**VIEW MORE**］をクリックします。

   b. ［**SEARCH**］をクリックします。

   c. ［**From**］フィールドおよび［**To**］フィールドで、日付範囲を指定します。

   d. ［**RETRIEVE**］をクリックします。

   e. バックアップのリストから、Data Domain 上に存在するバックアップを選択します。

   その日付範囲のバックアップのリストが表示されます。

5. ［**RESTORE**］タブをクリックします。

   ［**Select Restore Content**］ダイアログ ボックスが表示され、バックアップ内に含まれているボリュームのリストが表示されます。ボリューム名は、元のマウント ポイントを識別します。

6. ［**Select Restore Content**］ダイアログ ボックスで、次の手順を実行します。

   a. 階層ツリーで、リストアする仮想ディスクを選択します。

   b. ［Contents］パネルで、フォルダー内に含まれるファイルを選択します。

   c. ［**NEXT**］をクリックします。

［**Restore**］ウィザードが表示され、［**Basic Config**］パネルが開きます。

7. ［**Basic Config**］パネルで、次の手順を実行します。
   a. ［**Destination**］フィールドで、［**Instant Access**］を選択します。
   b. ［**NEXT**］をクリックします。

   ［**Advanced Config**］パネルが表示されます。
8. ［**Advanced Config**］パネルで、次の手順を実行します。
   a. ［**VM Name**］フィールドで、新しい仮想マシンの一意の名前を入力します。
   b. ［**NEXT**］をクリックします。

   ［**Location**］パネルが表示されます。
9. ［**Location** ］パネルで、次の手順を実行します。
   a. インベントリ ツリーで、データセンターとフォルダーの場所を選択します。
   b. ［**NEXT**］をクリックします。

   ［**Host/Cluster**］パネルが表示されます。
10. ［**Host/Cluster**］パネルで、次の手順を実行します。
    a. インベントリ ツリーで、ホストまたはクラスターを選択します。
    b. ［**NEXT**］をクリックします。

    ［**Resource Pool**］パネルが表示されます。
11. ［**Resource Pool**］パネルで、次のステップを実行します。
    a. インベントリ ツリーで、リソース プールを選択します。
    b. ［**NEXT**］をクリックします。

    ［**Summary**］パネルが表示されます。
12. ［**Summay**］パネルで、提供されている情報を確認し、［**FINISH**］をクリックします。

    次のステータス メッセージが表示されます：

    ```
    Restore request initiated.
    ```

リストア後の移行とクリーンアップの実行

手順

1. vSphere Client または vSphere Web Client を起動して、vCenter Server にログインします。
2. リストアした仮想マシンを見つけます。
3. Storage vMotion を使用して、この仮想マシンを Data Domain NFS 共有から vCenter 内のデータストアに移行します。

   Storage vMotion が完了すると、リストアされた仮想マシンのファイルは Data Domain システムに存在しなくなります。

   MCS NFS データストア ポーラーは未使用の Data Domain NFS マウントを 1 日 1 回自動的にアンマウントします。ただし、以降の処理手順を実行して、NFS マウントがアンマウントされ、削除されているかを確認することが推奨されます。
4. Avamar Administrator で、［**Server**］起動リンクをクリックします。

   ［**Server**］ウィンドウが表示されます。

5. ［**Data Domain NFS Datastores**］タブを選択します。
6. リストアした仮想マシンのエントリーがないことを確認します。

   エントリーがある場合は、これを選択して、［**Unmount/Remove**］をクリックします。

AUI を使用した VM バックアップ インスタンスのリストア

正常なバックアップのすべてのインスタンスは、そのインスタンスのコピーのリストアに使用できます。日付別にリストアするバックアップを見つけることができます。リストアを実行する際は、元の場所、異なる場所、複数の場所のいずれかにリストアできます。

リストアを実行する場合は、元の仮想マシン、新しい仮想マシン、別の仮想マシンのいずれかにリストアできます。

リストアするバックアップ インスタンスの選択

この手順は、次のプラグイン タイプに適用されます。

- Microsoft Windows ファイル システム
- Linux ファイル システム
- VMware イメージ
- Linux VMware File Level Restore（FLR）
- Microsoft SQL
- Microsoft Hyper-V
- Microsoft Exchange

このリストに含まれていないその他すべてのプラグイン タイプについては、Avamar Administrator を使用します。

手順

1. 左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］をクリックします。

   ［**Asset Management**］ウィンドウが表示されます。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、リカバリするクライアント コンピューターを選択します。

   このインスタンスの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、インスタンスのリストアに使用できます。
4. （オプション）日付によりバックアップを検索するには、次のようにします。
   a. 右側のパネルで、［**VIEW MORE**］をクリックします。
   b. ［**SEARCH**］をクリックします。
   c. ［**From**］フィールドおよび［**To**］フィールドで、日付範囲を指定します。
   d. ［**RETRIEVE**］をクリックします。
   e. バックアップの一覧から、バックアップを選択します。

   その日付範囲のバックアップのリストが表示されます。
5. ［**RESTORE**］タブをクリックします。

   ［**Select Restore Content**］ダイアログ ボックスが表示され、バックアップ内に含まれているボリュームのリストが表示されます。ボリューム名は、元のマウント ポイントを識別します。

6. （オプション）コンテンツの FLR（ファイル レベル リストア）を実行するには、次の手順を実行します。

   a. ［**FLR**］スイッチをオンに切り替えます。

      フォルダーのリストが表示されます。

   b. リストアするフォルダーまたはファイルを選択して、［**RESTORE**］をクリックします。

   FLR 機能は、フル リストア操作を完了する必要なく、バックアップからファイルを取得します。この機能により、特定のバックアップのボリュームから特定のファイルをリストアしたり、バックアップ ボリュームに含まれているファイルを参照したりすることができます。

7. ［**Select Restore Content**］ダイアログ ボックスで、次の手順を実行します。

   a. 階層ツリーで、リストアするフォルダーを選択します。

   b. ［Contents］パネルで、フォルダー内に含まれるファイルを選択します。

   c. ［**NEXT**］をクリックします。

   ［**Restore**］ウィザードが表示され、［**Basic Config**］ページが表示されます。
   元の仮想マシンにリストアする方法については、Restore data to the original virtual machine を参照してください。

元の仮想マシンへのデータのリストア

［Restore］ウィザードにアクセスするには、左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］ > ［**Restore**］をクリックします。

手順

1. 左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］をクリックします。

   ［**Asset Management**］ウィンドウが表示されます。

2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、リカバリするクライアント コンピューターを選択します。

   このインスタンスの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、インスタンスのリストアに使用できます。

4. （オプション）日付によりバックアップを検索するには、次のようにします。

   a. 右側のパネルで、［**VIEW MORE**］をクリックします。

   b. ［**SEARCH**］をクリックします。

   c. ［**From**］フィールドおよび［**To**］フィールドで、日付範囲を指定します。

   d. ［**RETRIEVE**］をクリックします。

   e. バックアップの一覧から、バックアップを選択します。

   その日付範囲のバックアップのリストが表示されます。

5. ［**RESTORE**］タブをクリックします。

   ［**Select Restore Content**］ダイアログ ボックスが表示され、バックアップ内に含まれているボリュームのリストが表示されます。ボリューム名は、元のマウント ポイントを識別します。

6. （オプション）コンテンツの FLR（ファイル レベル リストア）を実行するには、次の手順を実行します。

a. [**FLR**] スイッチをオンに切り替えます。

フォルダーのリストが表示されます。

b. リストアするフォルダーまたはファイルを選択して、[**RESTORE**] をクリックします。

FLR 機能は、フル リストア操作を完了する必要なく、バックアップからファイルを取得します。この機能により、特定のバックアップのボリュームから特定のファイルをリストアしたり、バックアップ ボリュームに含まれているファイルを参照したりすることができます。

7. [**Select Restore Content**] ダイアログ ボックスで、次の手順を実行します。

a. 階層ツリーで、リストアするフォルダーを選択します。

b. [**Contents**] パネルで、フォルダー内に含まれるファイルを選択します。

c. [**NEXT**] をクリックします。

[**Restore**] ウィザードが表示され、[**Basic Config**] ページが開きます。

8. [**Destination Client**] フィールドで、次の手順を実行します。

a. [**Restore to Original Virtual Machine**] を選択します。

b. [**NEXT**] をクリックします。

[**Backups**] パネルが表示されます。

9. [**Backup Content**] パネルで、次の手順を実行します。

a. 階層 [Domain] ツリーで、リストアするクライアントを選択します。

[**Contents of Backup**] パネルには、そのフォルダー内に含まれるファイルのリストが表示されます。

b. 右側のパネルで、リストアする仮想マシンのバックアップを選択します。

c. [**Destination Location**] をクリックします。

[**Destination Location**] パネルが表示されます。

10. [**Destination Location**] パネルで、[**Restore to Original Virtual Machine**] を選択します。

[**More Options**] パネルが表示されます。

11. [**More options**] パネルで、プラグイン オプションを次のように設定します。

a. [**Post Restore Options**] フィールドで、オプションを選択します。

b. 仮想マシン構成をリストアするには、[**Restore Virtual Machine Configuration**] を選択します。

c. 新しいディスクとして仮想マシンをリストアするには、[**Restore as a new disk**] を選択します。

d. CBT（更新ブロック追跡）を使用してパフォーマンスを向上させるには、[**Use CBT to increase performance**] を選択します。

e. [**Proxy**] フィールドで、オプションを選択します。

プラグイン オプションの完全リストについては、Plug-in Options を参照してください。

12. [**NEXT**] をクリックします。

[**Summary**] パネルが表示されます。

13. ［**Summary**］パネルで、提供されている情報を確認し、［**FINISH**］をクリックします。

    以下のステータス メッセージが表示されます：

    ```
    Restore request initiated.
    ```

別の仮想マシンへのデータのリストア

［Restore］ウィザードにアクセスするには、左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］ > ［**Restore**］をクリックします。

手順

1. 左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］をクリックします。

   ［**Asset Management**］ウィンドウが表示されます。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、リカバリするクライアント コンピューターを選択します。

   このインスタンスの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、インスタンスのリストアに使用できます。
4. （オプション）日付によりバックアップを検索するには、次のようにします。
   a. 右側のパネルで、［**VIEW MORE**］をクリックします。
   b. ［**SEARCH**］をクリックします。
   c. ［**From**］フィールドおよび［**To**］フィールドで、日付範囲を指定します。
   d. ［**RETRIEVE**］をクリックします。
   e. バックアップの一覧から、バックアップを選択します。

   その日付範囲のバックアップのリストが表示されます。
5. ［**RESTORE**］タブをクリックします。

   ［**Select Restore Content**］ダイアログ ボックスが表示され、バックアップ内に含まれているボリュームのリストが表示されます。ボリューム名は、元のマウント ポイントを識別します。
6. （オプション）コンテンツの FLR（ファイル レベル リストア）を実行するには、次の手順を実行します。
   a. ［**FLR**］スイッチをオンに切り替えます。

      フォルダーのリストが表示されます。
   b. リストアするフォルダーまたはファイルを選択して、［**RESTORE**］をクリックします。

   FLR 機能は、フル リストア操作を完了する必要なく、バックアップからファイルを取得します。この機能により、特定のバックアップのボリュームから特定のファイルをリストアしたり、バックアップ ボリュームに含まれているファイルを参照したりすることができます。
7. ［**Select Restore Content**］ダイアログ ボックスで、次の手順を実行します。
   a. 階層ツリーで、リストアするフォルダーを選択します。
   b. ［Contents］パネルで、フォルダー内に含まれるファイルを選択します。
   c. ［**NEXT**］をクリックします。

   ［**Restore**］ウィザードが表示され、［**Basic Config**］ページが開きます。

8. ［**Basic Config**］パネルで、次の手順を実行します。
   a. ［**Destination**］フィールドで、［**Restore to a different (existing) Virtual Machine**］を選択します。
   b. ［**Post Restore Options**］フィールドで、オプションを選択します。
   c. 新しいディスクとして仮想マシンをリストアするには、［**Restore as a new disk**］を選択します。
   d. CBT（更新ブロック追跡）を使用してパフォーマンスを向上させるには、［**Use CBT to increase performance**］チェックボックスを選択します。
   e. ［**Proxy**］フィールドで、オプションを選択します。

   プラグイン オプションの完全リストについては、Plug-in Options を参照してください。

   ［**Advanced Config**］ページが表示されます。
9. ［**Advanced Config**］パネルで、次の操作を実行します。
   a. ホストを表示するには、［**Host/Cluster**］をオフに切り替えます。
   b. クラスタを表示するには、［**Host/Cluster**］をオンに切り替えます。
   c. ［**Host/Cluster**］パネルで、ドメイン名を展開し、ホストまたはクラスタを選択します。

      選択した IP アドレスが表示されます。
10. ［**NEXT**］をクリックします。

    ［**Summary**］パネルが表示されます。
11. ［**Summary**］パネルで、提供されている情報を確認し、［**FINISH**］をクリックします。

    以下のステータス メッセージが表示されます：

    ```
    Restore request initiated.
    ```

新しい仮想マシンへのデータのリストア

［Restore］ウィザードにアクセスするには、左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］ > ［**Restore**］をクリックします。

手順

1. 左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］をクリックします。

   ［**Asset Management**］ウィンドウが表示されます。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、リカバリするクライアント コンピューターを選択します。

   このインスタンスの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、インスタンスのリストアに使用できます。
4. （オプション）日付によりバックアップを検索するには、次のようにします。
   a. 右側のパネルで、［**VIEW MORE**］をクリックします。
   b. ［**SEARCH**］をクリックします。
   c. ［**From**］フィールドおよび［**To**］フィールドで、日付範囲を指定します。
   d. ［**RETRIEVE**］をクリックします。

e. バックアップの一覧から、バックアップを選択します。

その日付範囲のバックアップのリストが表示されます。

5. ［**RESTORE**］タブをクリックします。

［**Select Restore Content**］ダイアログ ボックスが表示され、バックアップ内に含まれているボリュームのリストが表示されます。ボリューム名は、元のマウント ポイントを識別します。

6. （オプション）コンテンツの FLR（ファイル レベル リストア）を実行するには、次の手順を実行します。

a. ［**FLR**］スイッチをオンに切り替えます。

フォルダーのリストが表示されます。

b. リストアするフォルダーまたはファイルを選択して、［**RESTORE**］をクリックします。

FLR 機能は、フル リストア操作を完了する必要なく、バックアップからファイルを取得します。この機能により、特定のバックアップのボリュームから特定のファイルをリストアしたり、バックアップ ボリュームに含まれているファイルを参照したりすることができます。

7. ［**Select Restore Content**］ダイアログ ボックスで、次の手順を実行します。

a. 階層ツリーで、リストアするフォルダーを選択します。

b. ［Contents］パネルで、フォルダー内に含まれるファイルを選択します。

c. ［**NEXT**］をクリックします。

［**Restore**］ウィザードが表示され、［**Basic Config**］ページが開きます。

8. ［**Basic Config**］パネルで、次の手順を実行します。

a. ［**Destination**］フィールドで、［**Restore to new Virtual Machine**］を選択します。

b. ［**Post Restore Options**］フィールドで、オプションを選択します。

c. CBT（更新ブロック追跡）を使用してパフォーマンスを向上させるには、［**Use CBT to increase performance**］チェックボックスを選択します。

d. ［**Proxy**］フィールドで、オプションを選択します。

プラグイン オプションの完全リストについては、Plug-in Options を参照してください。

［**Advanced Config**］ページが表示されます。

9. ［**Advanced Config**］パネルで、次の操作を実行します。

a. ［**vCenter**］フィールドで、vCenter を選択します。

b. ［**VM Name**］フィールドに、仮想マシンの名前を入力します。

c. ［**NEXT**］をクリックします。

10. ［**Location**］パネルで、次の手順を実行します。

a. ドメイン名を展開し、次にリストア先を選択します。

選択した場所が表示されます。

b. ［**NEXT**］をクリックします。

11. ［**Host/Cluster**］パネルで、以下の手順を実行します。

a. ドメイン名を展開し、次にホストまたはクラスタを選択します。

選択した IP アドレスが表示されます。

b. [**NEXT**] をクリックします。

12. [**Resource Pool**] パネルで、以下の手順を実行します。
    a. ドメイン名を展開し、次にリソース プールを選択します。
       選択したリソース プールが表示されます。
    b. [**NEXT**] をクリックします。
13. [**Datastore**] ペインで、次の手順を実行します。
    a. データストアを選択します。
    b. [**NEXT**] をクリックします。
14. [**NEXT**] をクリックします。
    [**Summary**] パネルが表示されます。
15. [**Summary**] パネルで、提供されている情報を確認し、[**FINISH**] をクリックします。
    以下のステータス メッセージが表示されます：

```
Restore request initiated.
```

イメージ バックアップの概要

イメージ バックアップでは、3 レベルのリストア機能を提供しています。それは、イメージ リストア、FLR（ファイル レベル リストア）に加えて、特定のドライブを Windows イメージ バックアップからマウントして、アプリケーション レベルのリカバリをサポートする機能です。

[**Select for Restore**] コンテンツ パネルの上に 3 つのボタンが表示されます。これらのボタンは、VMware 以外のイメージ バックアップが選択されている場合は表示されません。

表 7 イメージ リストアのツールバー ボタン

ボタン	ツールチップ	説明
	Browse for Image Restore	イメージ リストアを開始します。
	Browse for Granular Restore	ファイル レベル リストアを開始します。
	Mount Windows VMDK	Windows イメージ ドライブにある選択したドライブをマウントして、アプリケーション レベルのリカバリをサポートします。

イメージ リストアを実行する際に表示される [**Restore Options**] ダイアログ ボックスは、通常の [**Restore Options**] ダイアログ ボックスとは多少異なります。主な違いは、仮想マシン情報が表示され、リストア先として次の 3 つの選択肢が提供される点です。

- 元の仮想マシン
- 異なる（既存の）仮想マシン
- 新しい仮想マシン

リストア先を選択すると、以降の処理手順はそれぞれ若干異なります。

イメージ レベル リストアの制限事項

次の制限事項は、仮想マシンのバックアップからのイメージ レベル リストアに適用されます。

仮想マシンの電源の状態
イメージ リストアを使用して、イメージ全体または選択したドライブをリストアする際は、ターゲット仮想マシンの電源をオフにする必要があります。

物理 RDM ディスクにかかわるリストア
物理 RDM ディスクを備えた仮想マシンから取得したバックアップを使用してデータをリストアする際は、そのデータを新しい仮想マシンにリストアすることはできません。

ネストされたコンテナーの制限事項
他のコンテナーを含む VMware コンテナー（つまり、ネストされたコンテナー構造）をリストアする際、Avamar では階層の最上位レベルのみをリストアします。次のネストされた vApp 構造の例を見てみましょう。

図 6 ネストされたコンテナー構造の例

vApp-1 が Avamar にバックアップされると、vApp バックアップ イメージには vm-1 と vm-2 の仮想マシン バックアップ イメージのみが含まれます。vApp-1 バックアップがリストアされると、vm-1 と vm-2 のみが存在します。

この制限に対して、2 つの暫定ソリューションがあります。

- コンテナー構造を平坦化する。
  たとえば、vm-3 を vApp-1 の下に移動します。そうすれば、vApp-1 がバックアップされたとき、3 個の仮想マシンがすべてバックアップされます。
- vApp-1 と vApp-2 の両方を別個のコンテナー エンティティとして Avamar に追加し、個別にバックアップできるようにします。
  リストアの際、vApp-1 を最初にリストアしてから、vApp-2 を vApp-1 にリストアします。

フル イメージまたは選択されたドライブを元の仮想マシンにリストアする

手順

1. vSphere Client または vSphere Web Client で、ターゲット仮想マシンの電源がオフになっていることを確認します。
2. 左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］をクリックします。

   ［**Asset Management**］ウィンドウが表示されます。
3. ドメイン ツリーで、仮想マシン クライアントまたは VMware コンテナを含むドメインを選択します。
4. クライアントのリストから、仮想マシン クライアントまたは VMware コンテナを選択します。

   このインスタンスの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、インスタンスのリストアに使用できます。
5. （オプション）日付によりバックアップを検索するには、次のようにします。

a. 右側のパネルで、［**VIEW MORE**］をクリックします。

b. ［**SEARCH**］をクリックします。

c. ［**From**］フィールドおよび［**To**］フィールドで、日付範囲を指定します。

d. ［**RETRIEVE**］をクリックします。

e. バックアップの一覧から、バックアップを選択します。

その日付範囲のバックアップのリストが表示されます。

6. ［**RESTORE**］タブをクリックします。

［**Select Restore Content**］ダイアログ ボックスが表示され、バックアップ内に含まれているボリュームのリストが表示されます。ボリューム名は、元のマウント ポイントを識別します。

7. （オプション）コンテンツの FLR（ファイル レベル リストア）を実行するには、次の手順を実行します。

a. ［**FLR**］スイッチをオンに切り替えます。

フォルダーのリストが表示されます。

b. リストアするフォルダーまたはファイルを選択して、［**RESTORE**］をクリックします。

FLR 機能は、フル リストア操作を完了する必要なく、バックアップからファイルを取得します。この機能により、特定のバックアップのボリュームから特定のファイルをリストアしたり、バックアップ ボリュームに含まれているファイルを参照したりすることができます。

8. ［**Select Restore Content**］ダイアログ ボックスで、次の手順を実行します。

a. 階層ツリーで、リストアするフォルダーを選択します。

b. ［**Contents**］パネルで、フォルダー内に含まれるファイルを選択します。

c. ［**NEXT**］をクリックします。

［**Restore**］ウィザードが表示され、［**Basic Config**］ページが開きます。

9. ［**Basic Configuration** ］フィールドで、次の手順を実行します。

a. ［**Destination**］フィールドで、［**Restore to Original Virtual Machine**］を選択します。

b. ［**Post Restore Options**］フィールドで、オプションを選択します。

c. 仮想マシンの構成をリストアするには、［**Restore Virtual Machine Configuration**］チェックボックスを選択します。

d. 新しいディスクとして仮想マシンをリストアするには、［**Restore as a new disk**］チェックボックスを選択します。

e. CBT（更新ブロック追跡）を使用してパフォーマンスを向上させるには、［**Use CBT to increase performance**］チェックボックスを選択します。

f. ［**Proxy**］フィールドで、オプションを選択します。

g. ［**NEXT**］をクリックします。

［**Summary**］パネルが表示されます。

10. ［**NEXT**］をクリックします。

［**Summary**］パネルが表示されます。

11. ［**Summary**］パネルで、提供されている情報を確認し、［**FINISH**］をクリックします。

以下のステータス メッセージが表示されます：

```
Restore request initiated.
```

12. リストアのターゲット仮想マシンで今後のバックアップ用に更新ブロック追跡が使用される場合は、その仮想マシンで再起動、電源オン、中断後の再開、移行のいずれかのアクションを実行して更新ブロック追跡を有効にします。

フル イメージまたは選択されたドライブを別の仮想マシンにリストアする

手順

1. vSphere Client または vSphere Web Client で、ターゲット仮想マシンの電源がオフになっていることを確認します。
2. 左側の AUI ナビゲーション ペインで、[≫] をクリックしてから［**Asset Management**］をクリックします。

   ［**Asset Management**］ウィンドウが表示されます。
3. ドメイン ツリーで、仮想マシン クライアントまたは VMware コンテナを含むドメインを選択します。
4. クライアントのリストから、仮想マシン クライアントまたは VMware コンテナを選択します。

   このインスタンスの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、インスタンスのリストアに使用できます。
5. （オプション）日付によりバックアップを検索するには、次のようにします。
   a. 右側のパネルで、［**VIEW MORE**］をクリックします。
   b. ［**SEARCH**］をクリックします。
   c. ［**From**］フィールドおよび［**To**］フィールドで、日付範囲を指定します。
   d. ［**RETRIEVE**］をクリックします。
   e. バックアップの一覧から、バックアップを選択します。

   その日付範囲のバックアップのリストが表示されます。
6. ［**RESTORE**］タブをクリックします。

   ［**Select Restore Content**］ダイアログ ボックスが表示され、バックアップ内に含まれているボリュームのリストが表示されます。ボリューム名は、元のマウント ポイントを識別します。
7. （オプション）コンテンツの FLR（ファイル レベル リストア）を実行するには、次の手順を実行します。
   a. ［**FLR**］スイッチをオンに切り替えます。

      フォルダーのリストが表示されます。
   b. リストアするフォルダーまたはファイルを選択して、［**RESTORE**］をクリックします。

   FLR 機能は、フル リストア操作を完了する必要なく、バックアップからファイルを取得します。この機能により、特定のバックアップのボリュームから特定のファイルをリストアしたり、バックアップ ボリュームに含まれているファイルを参照したりすることができます。
8. ［**Select Restore Content**］ダイアログ ボックスで、次の手順を実行します。
   a. 階層ツリーで、リストアするフォルダーを選択します。
   b. ［**Contents**］パネルで、フォルダー内に含まれるファイルを選択します。

c. [**NEXT**] をクリックします。

[**Restore**] ウィザードが表示され、[**Basic Config**] ページが開きます。

9. [**Basic Configuration**] フィールドで、次の手順を実行します。

a. [**Destination**] フィールドで、[**Restore to a different (existing) Virtual Machine**] を選択します。

b. [**Post Restore Options**] フィールドで、オプションを選択します。

c. 新しいディスクとして仮想マシンをリストアするには、[**Restore as a new disk**] チェックボックスを選択します。

d. CBT（更新ブロック追跡）を使用してパフォーマンスを向上させるには、[**Use CBT to increase performance**] チェックボックスを選択します。

e. [**Proxy**] フィールドで、オプションを選択します。

f. [**NEXT**] をクリックします。

[**Advanced Configuration**] パネルが表示されます。

10. [**Advanced Config**] パネルで、次の操作を実行します。

a. ホストを表示するには、[**Host/Cluster**] をオフに切り替えます。

b. クラスタを表示するには、[**Host/Cluster**] をオンに切り替えます。

c. [**Host/Cluster**] パネルで、ドメイン名を展開し、ホストまたはクラスタを選択します。

選択した IP アドレスが表示されます。

11. [**NEXT**] をクリックします。

[**Summary**] パネルが表示されます。

12. [**Summary**] パネルで、提供されている情報を確認し、[**FINISH**] をクリックします。

以下のステータス メッセージが表示されます：

```
Restore request initiated.
```

13. リストアのターゲット仮想マシンで今後のバックアップ用に更新ブロック追跡が使用される場合は、その仮想マシンで再起動、電源オン、中断後の再開、移行のいずれかのアクションを実行して更新ブロック追跡を有効にします。

イメージ バックアップからの Windows VMDK のマウント

Avamar は、Windows 仮想マシンの VMware イメージ バックアップから VMDK をマウントするメカニズムを提供します。この機能は通常、データ マイニングと高度なデータ リカバリを実行する Kroll OnTrack PowerControls のようなサード パーティのツールを有効にするために使用されます。

リカバリ ターゲット マシンの構成

このタスクでは、Windows の物理マシンまたは仮想マシンを、イメージ バックアップからの Windows VMDK をマウントするためのリカバリ ターゲットとして構成します。

はじめに

リカバリ ターゲット マシンは 64 ビット Windows 物理マシンまたは仮想マシンでなければなりません。

注

リカバリ ターゲットは、物理マシンまたは仮想マシンのどちらでも構いません。リカバリ ターゲットに仮想マシンを使用したい場合は、ゲスト バックアップを実施する場合のように、Avamar ソフトウェアを仮想マシンに直接インストールします。

手順

1. 「Avamar バックアップ クライアント ユーザー ガイド」の手順を使用して、Avamar Windows クライアント ソフトウェアをリカバリ ターゲット マシンにインストールします。
2. 「Avamar バックアップ クライアント ユーザー ガイド」の手順を使用して、リカバリ ターゲット マシンを、マウントするイメージ バックアップを保存するのと同じ Avamar サーバーにクライアントとして登録します。
3. Windows VMware GLR プラグ イン ソフトウェアをインストールするには、次のようにします。
   a. Windows 管理者権限を使用してリカバリ ターゲット マシンにログインします。
   b. Avamar サーバーから［**AvamarVMWareGLR-windows-x86_64-version.msi**］インストール パッケージをダウンロードします。
   c. インストール パッケージを開き、画面の指示に従います。
   d. コンピューターを再起動します。

Windows VMDK のリストアとマウント

はじめに

リカバリ ターゲットのマシンが適切に構成されていることを確認します。

- Avamar Windows クライアントおよび Windows VMware GLR プラグ イン ソフトウェアがインストールされていること
- リカバリ ターゲットのマシンが、VMDK をマウントする元となるイメージ バックアップを保存する同一の Avamar サーバーに、クライアントとして登録され、アクティブ化されていること

手順

1. vSphere Client または vSphere Web Client で、ターゲット仮想マシンの電源がオンになっていることを確認します。
2. Avamar Administrator で、［**Backup & Restore**］起動リンクをクリックします。

   ［**Backup, Restore and Manage**］ウィンドウが表示されます。
3. ［**Restore**］タブをクリックします。

   左上のパネルにドメインのリストが表示されます。
4. 次の手順に従って、仮想マシン クライアントまたは VMware コンテナーを選択します。
   a. 仮想マシン クライアントまたは VMware コンテナーを含むドメインを選択します。

      ログイン アカウントの対象となるドメイン外のクライアントは表示することはできません。すべてのクライアントを表示するには、root ドメインにログインします。

      Avamar クライアントのリストが、ドメイン リストの下のパネルに表示されます。
   b. クライアントのリストから、仮想マシン クライアントまたは VMware コンテナーを選択します。
5. 次の手順に従って、バックアップを選択します。

a. ［**By Date**］タブをクリックします。

b. カレンダーからバックアップ日付を選択します。その日付に実行された有効なバックアップが黄色にハイライト表示されます。

その日に実行されたバックアップのリストが、カレンダーの横の［**Backups**］テーブルに表示されます。

c. ［**Backups**］テーブルからバックアップを 1 つ選択します。

6. ［Contents］パネルで仮想ディスクを選択します。
7. ［**Mount Windows VMDK**］ボタン（ ）をクリックします。

［**Select Destination Client**］ダイアログ ボックスが表示されます。

8. ［**Client**］ボックスの横の［**Browse**］をクリックします。

［**Browse for Restore Destination Client**］ダイアログ ボックスが表示されます。

9. リカバリ ターゲットの仮想マシンを選択して、［**OK**］をクリックします。

［**Browse Backup Status**］ダイアログ ボックスが表示されます。

10. ［**OK**］をクリックして、操作の続行を確認します。

［**Restore Browse Options**］ダイアログ ボックスが表示されます。

11. ［**Amount of time to leave VMDKs mounted**］リストからタイムアウト値を選択して、［**OK**］をクリックします。

結果

フォルダー パスが右の［Backup Contents］パネルに表示されます。これで、Windows VMDK がそのフォルダーにマウントされました。

Avamar Administrator を使用してフル イメージまたは選択したドライブを新しい仮想マシンにリストアする

手順

1. Avamar Administrator で、［**Backup & Restore**］起動リンクをクリックします。

［**Backup, Restore and Manage**］ウィンドウが表示されます。

2. ［**Restore**］タブをクリックします。

左上のパネルにドメインのリストが表示されます。

3. 次の手順に従って、仮想マシン クライアントまたは VMware コンテナーを選択します。

a. 仮想マシン クライアントまたは VMware コンテナーを含むドメインを選択します。

ログイン アカウントの対象となるドメイン外のクライアントは表示することはできません。すべてのクライアントを表示するには、root ドメインにログインします。

Avamar クライアントのリストが、ドメイン リストの下のパネルに表示されます。

b. クライアントのリストから、仮想マシン クライアントまたは VMware コンテナーを選択します。

4. 次の手順に従って、バックアップを選択します。

a. ［**By Date**］タブをクリックします。

b. カレンダーからバックアップ日付を選択します。その日付に実行された有効なバックアップが黄色にハイライト表示されます。

その日に実行されたバックアップのリストが、カレンダーの横の［**Backups**］テーブルに表示されます。

c. ［**Backups**］テーブルからバックアップを 1 つ選択します。

5. コンテンツ パネルのすぐ上の［**Browse for Image Restore**］ボタン（ ）をクリックします。
6. ［Contents］パネルで以下を実行します。
   - イメージ全体をリストアする場合は、［**All virtual disks**］フォルダー チェックボックスを選択します。
   - 特定のドライブのみをリストアする場合は、対象ドライブを選択します（複数可）。
7. ［**Actions**］ > ［**Restore Now**］を選択します。

   ［**Restore Options**］ダイアログ ボックスが表示されます。
8. リストア先として［**Restore to a new virtual machine**］を選択します。

   注

   イメージ バックアップを新しい仮想マシンにリストアする際、［**Restore virtual machine configuration**］オプションが選択され、無効化（グレー表示）されます。これは、新しい仮想マシンを構成するためにこれらの構成ファイルが常に必要になるからです。
9. 次の手順に従って、新しい仮想マシンの場所と設定を指定します。
   a. ［**Configure Destination**］をクリックします。

      ［**Configure Virtual Machine**］ダイアログ ボックスが表示されます。

   b. ［**Browse**］をクリックします。

      ［**New Virtual Machine**］ウィザードが表示されます。

   c. ［**Name and Location**］スクリーンで、新しい仮想マシンの一意の［名前］を入力し、インベントリ ツリーでデータセンターとフォルダーの場所を選択した後、［**Next**］をクリックします。

   d. ［**Summary**］スクリーンに表示される情報を確認して、［**Finish**］をクリックします。

   e. ［**Configure Virtual Machine**］ダイアログ ボックスで［**OK**］をクリックします。
10. ［**Avamar encryption method**］リストから、リストア中に Avamar サーバーとクライアント間のデータ転送に使用する暗号化方式を選択します。

    クライアント/サーバー間の接続における暗号化テクノロジーおよびビットの強度は、クライアントのオペレーティング システムおよび Avamar サーバーのバージョンをはじめ、さまざまな要因によって異なります。詳細については、「Avamar 製品セキュリティ ガイド」を参照してください。
11. （オプション）オプションで、リストアを実行するプロキシを選択します。[]

    デフォルト設定は［**Automatic**］であり、これにより Avamar サーバーはこの操作に最適なプロキシを選択できます。
12. ［**More Options**］をクリックします。

    ［**Restore Command Line Options**］ダイアログ ボックスが表示されます。
13. ［**Use Changed Block Tracking (CBT) to increase performance**］を選択または選択解除します。
14. ［**Encryption method from Data Domain system**］リストから、リストア中に Data Domain システムとクライアント間のデータ転送に使用する暗号化方式を選択します。

15. ［**Select Post Restore Options**］リストで次の設定のいずれかを選択します：
    - ［**Do not power on VM after restore**］.
    - ［**Power on VM with NICs enabled**］.
    - ［**Power on VM with NICs disabled**］.
16. （オプション）このリストアに追加のプラグ イン オプションを含めるには、［**Enter Attribute**］と［**Enter Attribute Value**］設定を入力します。
17. ［**Restore Command Line Options**］ダイアログ ボックスで、［**OK**］をクリックします。
18. ［**Restore Options**］ダイアログ ボックスで、［**OK**］をクリックします。

    次のようなステータス メッセージが表示されます。`Restore initiated`。
19. ［**OK**］をクリックします。
20. リストアのターゲット仮想マシンで今後のバックアップ用に更新ブロック追跡が使用される場合は、その仮想マシンで再起動、電源オン、中断後の再開、移行のいずれかのアクションを実行して更新ブロック追跡を有効にします。

FLR（ファイル レベルのリストア）

Avamar では、インスタンス バックアップから FLR（ファイル レベルのリストア）をサポートしているため、ユーザーはフル リストア処理を実行することなく、バックアップからファイルを取得することができます。この機能により、特定のバックアップのボリュームから特定のファイルをリストアしたり、バックアップ ボリュームに含まれているファイルを参照したりすることができます。

注

FLR 機能を使用するには、仮想マシンの電源が入っていることを確認します。

ファイル レベル リストアのパフォーマンス向上

Avamar 7.4 以降では、ファイル レベル リストアの実行で HTTPS プロトコルがデフォルトで使用されます。これにより、ファイル コピーを使用する以前のメカニズムよりも高速なファイル転送のメカニズムを提供することで、リストアのパフォーマンスが向上します。

HTTPS を使用できない場合は、ファイル レベル リストアの実行には以前のファイル コピーを使用するメカニズムが使用されます。リストア中に、次の警告メッセージが表示されます。

```
Target VM: server cannot reach proxy: proxy via https due to
incorrect network configuration. Restoration process may take
significantly longer time. Press 'continue' to start the restore.
```

ここで、

- server は Avamar サーバの名前。
- proxy はプロキシの名前。

［**Yes**］を選択して、ファイル コピーを使用するリストア処理を続行します。このリストアには大幅に長く時間がかかります。

注

この実装では、`wget` コマンドが必要です。パフォーマンスの向上を活用するには、クライアントに `wget` をインストールしている必要があります。

ファイル レベルのリストアがサポートされる構成

次のサポートされる構成には、プロキシ バージョンと Avamar サーバーの両方が Avamar リリース 7.5 Service Pack 1 以降である必要があります。

パーティショニング スキーム

次の表は、FLR（ファイル レベル リストア）のパーティショニング スキームの概要を示します。

表 8 FLR でサポートされるパーティショニング スキーム

パーティショニング スキーム	ゲスト OS	FLR	コメント
MBR	Windows/Linux	サポート	
EBR（論理パーティション）	Windows/Linux	サポート	
GPT	Windows/Linux	一部サポート	Linux では GPT ベースの BTRFS と LVM（論理ボリューム マネージャ）をサポート
MixedGPT	Windows/Linux	サポート対象外	Hybrid MBR

ファイル システム サポート

次の表は、FLR のファイル システム サポートの概要を示します。

表 9 FLR のファイル システム サポート

ファイル システム タイプ	ゲスト OS	パーティショニング スキーム	パーティション ID	パーティションのないディスク	LVM
ext2	Linux	MBR、EBR	0x83	サポート	サポート
ext3	Linux	MBR、EBR	0x83	サポート	サポート
ext4	Linux	MBR、EBR	0x83	サポート	サポート
NTFS	Windows	MBR、EBR、GPT	0x04/0x07	サポート	サポート
VFAT	Windows	MBR、EBR	0x06/0x0E	サポート	サポート
XFS	Linux	MBR、EBR	0x83	サポート	サポート
ReiserFS	Linux	MBR、EBR	0x83	サポート	サポート
Btrfs	Linux	MBR、EBR、GPT	0x83	サポート	サポート

LVM サポート

次の表は、FLR の LVM サポートの概要を示します。

表 10 FLR の LVM サポート

LV タイプ	FLR
リニアな LV	サポート
ストライピングされた LV	サポート
ミラーリングされた LV	サポート
RAID LV	サポート
シン LV	サポート

複数デバイスのサポート

次の表は、FLR の複数デバイス サポートの概要を示します。

表 11 FLR の複数デバイス サポート

RAID	発生	FLR
RAID 0/ストライピング	LVM/BTRFS	サポート
RAID 1/ミラーリング	LVM/BTRFS	サポート
RAID 4	LVM	サポート
RAID 5	LVM	サポート
RAID 6	LVM	サポート
RAID10	LVM/BTRFS	サポート

ファイル レベル リストアの制限事項

ファイル レベル リストアには次の制限事項があります。

- シンボリック リンクをリストアまたは参照することはできません。
- バックアップ内に含まれている特定のディレクトリ、またはリストア先の参照は、合計 5 万個のファイルまたはフォルダーに制限されます。
- リストアは、同じリストア処理で 2 万オブジェクト（ファイルまたはフォルダー）に制限されます。
- Windows バックアップのファイルは Windows マシンのみに、Linux バックアップのファイルは Linux マシンのみにリストアできます。
- vCenter を AUI の root ドメインに追加する必要があります。vCenter ドメインの他の場所はサポートされません。
- `/tmp` へのファイル レベル リストアを実行する場合、Avamar ソフトウェアはデータをプライベートな`/tmp` にリダイレクトします。
  例： `/tmp/systemd-private-*`
- すべての仮想マシン クライアントは、AUI の/vCenter/VirtualMachines サブフォルダーにある必要があります。VM の他の場所はサポートされません。
- 既存のファイルまたはフォルダーの ACL を上書きするには、そのユーザーが上書きされているターゲット ファイルまたはフォルダーの所有権を持っていることを確認します。
- AUI に対して構成できる vCenter は 1 つのみです。

注

Avamar で複数の vCenter が構成されている場合は、Avamar サーバーの `vcenter-sso-info.cfg` が VC_hostname パラメーターに適切な vCenter サーバーを反映していることを確認する必要があります。たとえば、サンプル ファイル `/usr/local/avamar/var/ebr/server_data/prefs/vcenter-sso-info.cfg`:

```
vcenter-sso-hostname=<VC_hostname>
vcenter-sso-port=7444
# configure only if more than one vCenter
vcenter-hostname=<VC_hostname>
```

サポートされない仮想ディスク構成
ファイル レベルのリストアでは、次の仮想ディスク構成はサポートされません。

- FLR をサポートするファイルシステムでは、プロキシ オペレーティング システムよりも上位のカーネルが必要になる（3.12）
  - XFS Free Inode B-Tree（finobt）
  - Ext4 sparse_supper2（3.16）、metdata_csum（3.18）、encrypt（4.1）、project（4.5）
- Windows ダイナミック ディスク
- 暗号化/圧縮されたパーティションまたはブートローダ
- 重複排除された NTFS
- 未フォーマット ディスク
- 複数のアクティブなディスク/パーティションを参照します。参照用に、最初のアクティブなディスク/パーティションのみが表示されます。

注

LVM（論理ボリューム マネージャー）構成を使用した仮想マシン上での FLR 操作は、LVM 構成が完了している場合のみサポートされます。完全な LVM 構成は、1 つ以上の物理ボリュームで構成される 8E-Linux LVM タイプのパーティションで構成されます。これらの物理ボリュームには、1 つ以上の論理ボリュームで構成される 1 つ以上のボリューム グループが含まれます。

AUI を使用した FLR（ファイル レベル リストア）操作の実行

FLR 機能は、フル リストア操作を完了する必要なく、バックアップからファイルを取得します。この機能により、特定のバックアップのボリュームから特定のファイルをリストアしたり、バックアップ ボリュームに含まれているファイルを参照したりすることができます。

はじめに

ファイル レベル リストアを実行する場合：

- ソース VM が VMware に存在しており、電源がオンで登録されていることを確認します。
- ソース VM で、最新バージョンの VMware Tools がインストールされ、実行されていることを確認します。
- Windows 以外のプラットフォームでは、ユーザーは標準または管理者グループの一部にすることができます。

- Windows VM の場合は、ローカル管理者ユーザーのみがファイル レベル リストアを実行できます。さらに、UAC(ユーザー アカウント制御）を無効化していることを確認します。詳細については、ナレッジ ベース記事（https://support.emc.com/kb/477118）を参照してください。

［Restore］ウィザードにアクセスするには、左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］ > ［**Restore**］をクリックします。

手順

1. 左側の AUI ナビゲーション ペインで、［≫］をクリックしてから［**Asset Management**］をクリックします。

   ［**Asset Management**］ウィンドウが表示されます。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、リカバリするクライアント コンピューターを選択します。

   このインスタンスの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、インスタンスのリストアに使用できます。
4. （オプション）日付によりバックアップを検索するには、次のようにします。
   a. 右側のペインで、［**VIEW MORE**］をクリックします。
   b. ［**SEARCH**］をクリックします。
   c. ［**From**］フィールドおよび［**To**］フィールドで、日付範囲を指定します。
   d. ［**RETRIEVE**］をクリックします。
   e. バックアップの一覧から、バックアップを選択します。

   その日付範囲のバックアップのリストが表示されます。
5. ［**RESTORE**］タブをクリックします。

   ［**Select Restore Content**］ダイアログ ボックスが表示され、バックアップ内に含まれているボリュームのリストが表示されます。ボリューム名は、元のマウント ポイントを識別します。
6. コンテンツの FLR（ファイル レベル リストア）を実行するには、次の手順を実行します。
   a. ［**FLR**］スイッチをオンに切り替えます。

      フォルダーのリストが表示されます。
   b. リストアするフォルダーまたはファイルを選択して、［**RESTORE**］をクリックします。

   FLR 機能は、フル リストア操作を完了する必要なく、バックアップからファイルを取得します。この機能により、特定のバックアップのボリュームから特定のファイルをリストアしたり、バックアップ ボリュームに含まれているファイルを参照したりすることができます。

   ［**Basic Config**］パネルが表示されます。
7. ［**Basic Config**］パネルで、次の手順を実行します。
   a. クライアントを選択するには、次の手順を実行します。
      a. ［**SELECT CLIENT**］をクリックします。
         ［**Select Client**］パネルが表示されます。
      b. ドメイン ツリーで、クライアントのドメインを選択します。
      c. ［**Client**］パネルで、宛先クライアントを選択します。
      d. ［**OK**］をクリックします。

b. [**Username**] フィールドに、宛先クライアントのユーザー名を入力します。

c. [**Password**] フィールドに、宛先クライアントのパスワードを入力します。

d. [**Location**] フィールドで、リストアのパスを指定します。

e. （オプション）[**Restore ACL**] を選択し、ACL をリストアします。

注

[**Restore ACL**] オプションが選択されている場合、リストアを実行するユーザーは、リストアを実行するために、元のファイルのファイル所有権が必要です。バックアップが実行され、リストアを実行するユーザーが適切なファイル所有権を持たないためにファイルの所有権を変更した場合、リストアに失敗します。

---

f. [**Proxy**] フィールドで、プロキシを選択します。

8. [**NEXT**] をクリックします。

   [**Summary**] パネルが表示されます。

9. [**Summary**] パネルで、提供されている情報を確認し、[**FINISH**] をクリックします。

   以下のステータス メッセージが表示されます：

   ```
   Restore request initiated.
   ```

第 6 章

バックアップ検証

本章は、次のトピックで構成されています。

概要

イメージ バックアップでは、バックアップ検証メカニズムは仮想マシンのバックアップを新しい仮想マシンにリストアする場合と類似しています。ただし、バックアップが検証されると、新しい仮想マシンが自動的に vCenter から削除される点が異なります。

バックアップ検証は、必要に応じて（オン デマンドで）単一の仮想マシンのバックアップで開始したり、仮想マシンのグループ全体用にスケジュールを設定したりすることが可能です。スケジュール設定されたバックアップの検証では、仮想マシン グループの各メンバーの完了した最新のバックアップを常に使用します。

検証される内容

デフォルトの検証では、リストア後に仮想マシンの電源がオンになり、オペレーティング システムが起動されることを確認します。

バックアップ検証では、ユーザー定義のスクリプトを実行するオプション機能も提供されており、カスタム アプリケーション レベルの検証を実行できます。スクリプトは、検証するバックアップに存在する必要があります。バックアップ検証中に外部のスクリプトを実行することはできません。

サポートされるスクリプトのタイプは、Linux 仮想マシン用のシェル スクリプトと、Windows 仮想マシン用の DOS バッチ ファイルです。Perl スクリプトはサポートされていません。

VM バックアップ検証グループ

スケジュール設定されたバックアップの検証は、特別な VM バックアップ検証グループを使用して実装されます。このグループは、自動バックアップ検証を実行するためのみに使用され、他の用途では使用できません。

VM バックアップ検証グループは、次の点で他のグループと異なります。

- VM バックアップ検証グループは、保存ポリシーが割り当てられていません。
- 各 VM バックアップ検証グループに割り当てられるデータセットは、グループの作成時に自動的に作成されます。データセット名は VM バックアップ検証グループ名と同じです。
- 各 VM バックアップ検証グループは、バックアップ検証中に一時的に作成された新しい仮想マシンの場所（つまり、ESX ホストまたはクラスター、データストア、フォルダー）も保存します。

オン デマンド バックアップ妥当性検査の実行

手順

1. Avamar Administrator で、［**Backup & Restore**］起動リンクをクリックします。

   ［**Backup, Restore and Manage**］ウィンドウが表示されます。
2. ［**Manage**］タブをクリックします。
3. 次の手順に従って、仮想マシン クライアントまたは VMware コンテナーを選択します。
   a. 仮想マシン クライアントまたは VMware コンテナーを含むドメインを選択します。

      ログイン アカウントの対象となるドメイン外のクライアントは表示することはできません。すべてのクライアントを表示するには、root ドメインにログインします。

      Avamar クライアントのリストが、ドメイン リストの下のパネルに表示されます。

b. クライアントのリストから、仮想マシン クライアントまたは VMware コンテナーを選択します。

4. 次の手順に従って、バックアップを選択します。

   a. [**By Date**] タブをクリックします。

   b. カレンダーからバックアップ日付を選択します。その日付に実行された有効なバックアップが黄色にハイライト表示されます。

      その日に実行されたバックアップのリストが、カレンダーの横の [**Backups**] テーブルに表示されます。

   c. [**Backups**] テーブルからバックアップを 1 つ選択します。

5. [**Actions**] > [**Validate Backup**] を選択します。

   [**Validate Options**] ダイアログ ボックスが表示されます。

6. [**Configure Destination**] をクリックします。

   [**Configure Location**] ウィザードが表示されます。

7. vCenter を選択し、[**Next**] をクリックします。

8. インベントリ ロケーション名を入力して、ツリーのデータセンター フォルダーを選択し、[**Next**] をクリックします。

9. ホストまたはクラスターを選択し、[**Next**] をクリックします。

10. リソース プールを選択し、[**Next**] をクリックします。

11. データストアを選択し、[**Next**] をクリックします。

12. [**Summary** 画面] で、[**Finish**] をクリックします。

13. [**Avamar encryption method**] リストから、バックアップ妥当性検査中にクライアントと Avamar サーバーの間のデータ転送に使用する暗号化手法を選択します。

    クライアント/サーバー間の接続における暗号化テクノロジーおよびビットの強度は、クライアントのオペレーティング システムおよび Avamar サーバーのバージョンをはじめ、さまざまな要因によって異なります。詳細については、「Avamar 製品セキュリティ ガイド」を参照してください。

14. （オプション）妥当性検査の一環として、ユーザー定義のスクリプトを実行するには、次のようにします。

    注

    スクリプトは妥当性検査を行うバックアップに、すでに入っていなければなりません。バックアップの妥当性検査中に外部のスクリプトを実行することはできません。

    a. [**More Options**] をクリックします。

       [**Validate Command Line Options**] ダイアログ ボックスが表示されます。

    b. スクリプトの実行に十分な権限のある仮想マシンのゲスト OS のユーザー アカウント名とパスワードを入力します。

    c. 妥当性検査スクリプトのフル パスとファイル名を入力します。

       注

       これが Windows 仮想マシンの場合は、スクリプト パスとファイル名の後に、**`exit /B exitcode`** と入力します。**exitcode** は、ユーザー定義による終了メッセージです。

d. [**Maximum script run time (minutes)**] の設定が、スクリプトの完了に十分な時間であることを確認します。

e. [**OK**] をクリックします。

15. [**Validate Options**] ボックスで [**OK**] をクリックします。

次のようなステータス メッセージが表示されます。`Restore request initiating.`

16. [**Close**] をクリックします。

バックアップ妥当性検査のスケジュール

仮想マシンのグループ全体のバックアップ妥当性検査のスケジュールをするには、VM Backup Validation Group を作成します。

手順

1. Avamar Administrator で、[**Policy**] 起動リンクをクリックします。

[**Policy**] ウィンドウが表示されます。

2. [**Policy Management**] タブをクリックし、[**Groups**] タブをクリックします。
3. ツリーで、グループの場所を選択します。
4. [**Actions**] > [**Group**] > [**New**] > [**VM Backup Validation Group**] を選択します。

[**New VM Backup Validation Group**] ウィザードが表示されます。

5. [**General**] 画面で次のようにします。

a. [グループ名] を入力します。

b. [**Disabled**] チェックボックスを選択または選択解除します。

このチェックボックスを選択すると、このグループについてスケジュール設定されたバックアップの開始を延期します。そうしたくない場合は、このチェックボックスを選択解除して、次回の実行予定として割り当てられた時刻に、このジョブについてスケジュール設定されたバックアップが実行されるようにしてください。

c. バックアップ妥当性検査中のクライアント/サーバーのデータ転送の [**Avamar** 暗号化手法] を選択します。

注

クライアント/サーバー間の接続における暗号化テクノロジーおよびビットの強度は、クライアントのオペレーティング システムおよび Avamar サーバーのバージョンをはじめ、さまざまな要因によって異なります。詳細については、「Avamar 製品セキュリティ ガイド」を参照してください。

---

d. [**Next**] をクリックします。

6. [**Membership**] 画面で次のようにします。

a. 妥当性検査グループのメンバーにしたい仮想マシンの隣のチェックボックスを選択します。

b. [**Next**] をクリックします。

7. [**Location**] 画面で次のようにします。

a. [**Configure Location**] をクリックします。

[**Configure VM Backup Validation Location**] ウィザードが表示されます。

b. vCenter を選択し、［**Next**］をクリックします。

c. ツリーからデータセンター フォルダーを選択し、［**Next**］をクリックします。

d. ホストまたはクラスターを選択し、［**Next**］をクリックします。

e. リソース プールを選択し、［**Next**］をクリックします。

f. データストアを選択し、［**Next**］をクリックします。

g. ［**Summary**］画面で設定をレビューし、［**Finish**］をクリックします。

h. ［**Next**］をクリックします。

8. ［**Schedule**］画面でリストからスケジュールを選択し、［**Next**］をクリックします。
9. ［**Overview**］画面で設定をレビューし、［**Finish**］をクリックします。
10. スケジューラーが実行されていることを確認します。

第 7 章

vCenter 管理インフラストラクチャの保護

本章は、次のトピックで構成されています。

概要

このトピックでは、vCenter 管理インフラストラクチャ（その環境内の仮想マシンではない）を保護する方法について取り上げます。

vCenter は 32 ビットまたは 64 ビットの Windows ホストで実行されます。異なるホストで実行可能なデータベース サーバーも構成します。一部のオプションの vSphere コンポーネントは、vCenter と同じホストまたは異なるデータベース サーバー ホストで、ホスティング可能な追加のデータベースを必要とします。

注

VMware イメージ バックアップ プロキシ アプライアンスを使用する Avamar を使用して vCenter 6.5 の導入を保護する方法の詳細については、Backup and Restore of the vCenter Server using the Avamar VMware Image Protection Solution ホワイトペーパーを参照してください。

---

vCenter 管理インフラストラクチャを保護する方法は、仮想ホストごとにゲスト バックアップを実装することです。データセットは、次の重要な vCenter 管理インフラストラクチャ コンポーネントのみをバックアップする必要があります。

- ライセンス ファイル
- SSL 証明書
- 監査ログ
- Windows ゲストのカスタマイズ（sysprep）ファイル
- データベース ホスト構成の設定
- UpdateManager データベース
- SRM（Site Recovery Manager）データベース

Avamar バックアップを使用した vCenter 管理インフラストラクチャのリカバリは、2 ステップのプロセスです。最初に最新のオペレーティング システム イメージでリストア ターゲット仮想マシンを作成します。次に、最新の Avamar バックアップから vCenter 管理インフラストラクチャ コンポーネントをリストアします。

Avamar で vCenter 管理インフラストラクチャを保護するメリットは、Avamar バックアップを使用して vCenter アップグレードを容易に行うことも可能であるという点です（例えば、32 ビットまたは 64 ビットの Windows 仮想マシンから vCenter ホストをアップグレードする）。

vCenter 管理インフラストラクチャのバックアップ

vCenter 管理インフラストラクチャを保護する方法は、重要な vCenter 管理インフラストラクチャ コンポーネントのみをバックアップするカスタム データセットを使用して、各仮想ホストにゲスト バックアップを実装することです。

その後、vCenter Avamar クライアントをグループに追加し、一定間隔でこれらのバックアップをスケジュール設定します。

vCenter 管理インフラストラクチャのゲスト バックアップの実装

手順

1. 「Avamar バックアップ クライアント ユーザー ガイド」の説明に従って、vCenter ホストに Windows 用 Avamar クライアント ソフトウェアをインストールして登録します。

2. 「Avamar for SQL Server ユーザー ガイド」のような、各種データベース固有のドキュメントの説明に従って、適切な Avamar データベース ソフトウェアを、各データベース ホストにインストールして登録します。

vCenter 管理インフラストラクチャ用のデータセットの作成

最適な結果を得るために、vCenter 管理インフラストラクチャ コンポーネントをバックアップする際に使用するカスタム データセットを正確に定義します。

カスタム データセットを使用すると、バックアップとリストアの時間が短縮されるだけではなく、Avamar バックアップを使用して vCenter アップグレードを容易に行うこともできます（例えば、32 または 64 ビットの Windows 仮想マシンから vCenter ホストへのアップグレード）。

手順

1. Avamar Administrator で［**Tools**］ > ［**Manage Datasets**］を選択します。

   ［**Manage All Datasets**］ウィンドウが表示されます。

2. ［New］をクリックします。

   ［**New Dataset**］ダイアログ ボックスが表示されます。

3. この新しいデータセットの名前（例えば、vCenter-1）を入力します。
4. ［**Source Data**］タブをクリックします。
5. ［**Enter Explicitly**］を選択し、［**Select Plug-In Type**］リストから［**Windows File System**］プラグ インを選択します。
6. ダイアログ ボックス下部のバックアップ ターゲットのリストで、エントリーを選択し、［**-**］をクリックして、［**Windows File System**］プラグ イン以外のすべてのエントリーを削除します。
7. 各 vCenter 管理インフラストラクチャ コンポーネントを、次のようにデータセットに追加します。

   a. ［**Files and/or Folders**］を選択して、［**...**］をクリックします。

      ［**Select Files And/Or Folders**］ダイアログ ボックスが表示されます。

   b. vCenter 管理インフラストラクチャ コンポーネントを見つけて、選択します。

表 12 重要な vCenter 管理インフラストラクチャ コンポーネント

コンポーネント	デフォルトの場所

ライセンス ファイル	正確な場所は、VMware および Windows のバージョンによって異なりますが、一般的には次のフォルダーのいずれかです。
	`C:\Program Files(x86)\VMware \Infrastructure\VirtualCenter Server\licenses\site`
	`C:\Program Files\VMware \VMware License Server \Licenses`

SSL 証明書	正確な場所は、VMware および Windows のバージョンによって異なりますが、一般的には次のフォルダーのいずれかです。

表 12 重要な vCenter 管理インフラストラクチャ コンポーネント （続き）

コンポーネント	デフォルトの場所
	C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL C:\ProgramData\VMWare\VMware VirtualCenter\SSL
監査ログ	正確な場所は、VMware および Windows のバージョンによって異なりますが、一般的には次のフォルダーのいずれかです。 C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\Logs C:\ProgramData\VMWare\VMware VirtualCenter\Logs
Windows ゲストのカスタマイズ（sysprep）ファイル	正確な場所は、VMware および Windows のバージョンによって異なりますが、一般的には次のフォルダーのいずれかです。 C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\sysprep C:\ProgramData\VMWare\VMware VirtualCenter\sysprep

c. [**OK**] をクリックします。

d. 重要な vCenter 管理インフラストラクチャ コンポーネントそれぞれについて、これらのステップを繰り返します。

8. [**OK**] をクリックします。

vCenter データベース ホスト用バックアップの追加

vCenter、Update Manager、SRM などで使用されるデータベースの場所は、Windows データ ソース（ODBC）管理ツールを実行することによって決めることができます。

手順

1. 「Avamar for SQL Server ユーザー ガイド」のような、データベース固有のドキュメントの説明に従って、Avamar データベース バックアップ エージェントをデータベース ホストにインストールします。
2. スケジュール設定されたバックアップを、データベースを保護するように構成します。

   各バックアップの後で、vCenter データベースのトランザクション ログをトランケートしてください。このステップは、SQL Server プラグ インの [**Truncate database log**] オプションを選択して行うことができます。データベースのトランザクション ログをトランケートすることによって、ログが大きくなりすぎることがなくなり、また、Avamar サーバ上のスペースを過剰に消費することがなくなります。

Avamar バックアップを使用した vCenter 管理インフラストラクチャのリカバリ

Avamar バックアップからの vCenter 管理インフラストラクチャのリカバリは、2 ステップのプロセスです。最初に最新のオペレーティング システム イメージでリストア ターゲット仮想マシンを作成し、次に、最新の Avamar バックアップから vCenter 管理インフラストラクチャ コンポーネントをリストアします。詳細については、「Avamar Administration Guide」を参照してください。「Avamar Administration Guide」

インフライト バックアップ用 vCenter HA フェールオーバーのサポート

vCenter のフェールオーバーの間、Avamar ソフトウェアはフェールオーバー プロセスを監視し、次のアクションを実行します。

1. vCenter のフェールオーバー イベントを自動的に検出して、vCenter のフェールオーバーが完了するまで待機します。
2. vCenter の HA フェールオーバーが原因で異常停止しているバックアップ ジョブをキャンセルします。
3. マウントされている HotAdded ディスクをプロキシ アプライアンスから削除します。
4. vCenter HA フェールオーバーの間にすべての未完了のバックアップを再開します。

第 8 章

ESX ホストの保護

本章は、次のトピックで構成されています。

概要

イメージ バックアップを構成して、スタンドアロン ESX ホストに存在する仮想マシンを保護することができます。

この機能には、主に次の 2 つの用途があります。

1. 最小限のお客様の構成をサポート。
   一部のお客様のサイトでは、単一の ESX ホストと、その ESX ホストに存在する 1 個以上の仮想マシンで構成されるシンプルな VMware トポロジーを使用している場合があります。このようなサイトでは、通常 vCenter 管理レイヤーは実装されていません。しかし、データ消失から保護するためには、スタンドアロン ESX ホストに存在する仮想マシンもバックアップする必要があります。スタンドアロン ESX ホストを Avamar vCenter Client として追加すれば、ゲスト バックアップではなく、イメージ バックアップを使用して、これらの仮想マシンをバックアップすることが可能になります。
2. 仮想 vCenter の災害復旧。
   ESX ホストを Avamar vCenter Client として追加すると、特定の ESX ホスト上に存在する仮想マシンをリストアする必要があるものの、vCenter が動作していない場合に便利です。これは、仮想 vCenter を Avamar バックアップからリカバリする必要がある場合に多く発生します。スタンドアロン ESX ホストを Avamar vCenter Client として追加すると、vCenter 管理インフラストラクチャの仮想マシンをリストアし、vCenter を再起動することが可能になります。

制限事項

Avamar のスタンドアロン ESX ホストに存在する仮想マシンを保護する際の、既知の制限事項は次のとおりです。

ESX のバージョン
この機能のサポートは、ESX 5.5 以降に制限されています。それより古いバージョンではサポートされていません。

仮想 vCenter の災害復旧
仮想化 vCenter を ESX ホストからリカバリする目的でこの機能を使用する場合は、ESX ホストに仮想マシンをリストアする前に、まず ESX ホストと vCenter の関連付けを解除する必要があります。

ESX ホストの保護
ESX ホストを保護している間、リストアされた仮想マシンには VMX ファイルに空の `vc.uuid` があることがあります。そのため、リストアされた仮想マシンを Avamar に追加する場合、このフラグを手動で設定する必要があります。

タスク リスト

スタンドアロン ESX ホストに存在する仮想マシンを保護するために、次のタスクを実行します。

1. Avamar サーバーが ESX ホストと通信でき、認証されていることを確認します。
   ESX ホスト証明書を Avamar MCS キーストアに追加します。追加しない場合は、すべての MCS 通信で証明書認証を無効化する必要があります。
2. （オプション） Avamar で使用する専用のユーザー アカウントを ESX ホスト上に作成します。
3. ESX ホストを vCenter Client として Avamar に追加します。

これにより、ESX ホストに存在する仮想マシンを動的に検出して、ゲスト バックアップではなく、イメージ バックアップを使用して仮想マシンをバックアップできるようになります。

4. ESX ホストに 1 個以上のプロキシを導入します。
5. ESX ホストに存在する仮想マシンのオン デマンドのイメージ バックアップまたはスケジュール設定されたイメージ バックアップを実行します。

ESX ホスト認証証明書を MCS キーストアに追加

ESX ホスト認証証明書を MCS キーストアに追加します。これは、保護対象の各 ESX ホストで実行します。

この処理手順では、java `keytool` ユーティリティを使用して、証明書キーを管理します。`keytool` ユーティリティは、Java bin フォルダー（`/usr/java/version/bin`）にあります。ここで、version は現在 MCS にインストールされている JRE（Java Runtime Environment）のバージョンです。このフォルダーがパスにない場合は、パスにそれを追加するか、`keytool` を使用するときに完全なパスを指定します。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
   - シングル ノード サーバーには、admin としてサーバーにログインします。
   - マルチ ノード サーバーの場合、admin としてユーティリティ ノードにログインします。
2. 次のコマンドを入力して、MCS を停止します。

   ```
   dpnctl stop mcs
   ```

3. 次のコマンドを入力して、ユーザーを root に切り替えます。

   ```
   su -
   ```

4. ESX ホスト マシンから、Avamar ユーティリティ ノードまたはシングル ノード サーバー上の`/tmp` に`/etc/vmware/ssl/rui.crt` をコピーします。
5. 次を入力して、MCS キーストアを`/tmp` にコピーします。

   ```
   cp /usr/local/avamar/lib/rmi_ssl_keystore /tmp/
   ```

   これにより、ライブ MCS キーストアの一時バージョンが`/tmp` に作成されます。
6. 次のように入力して、デフォルトの ESX ホスト証明書を一時 MCS キーストア ファイルに追加します。

   ```
   cd /tmp
   $JAVA_HOME/bin/keytool -import -file rui.crt -alias alias -
   keystore rmi_ssl_keystore
   ```

   ここで、alias はこの証明書のユーザー定義名であり、通常はファイル名を使います。
7. キーストア パスワードを入力します。
8. `yes` と入力し、［**Enter**］キーを押して、この証明書を信用します。
9. （オプション）この Avamar サーバーで複数の ESX ホストを保護する場合は、ここでこれらの ESX ホスト証明書を追加します。
10. 以下のように入力して、ライブ MCS キーストアをバックアップします。

    ```
    cd /usr/local/avamar/lib
    cp rmi_ssl_keystore rmi_ssl_keystore.date
    ```

ここで、date は今日の日付です。

11. 以下のように入力して、一時 MCS キーストアを利用可能な場所にコピーします。

```
cp /tmp/rmi_ssl_keystore /usr/local/avamar/lib/
```

12. **exit** と入力して、root サブシェルを終了します。
13. 次のコマンドを入力して、MCS およびスケジューラを開始します。

```
dpnctl start mcs
dpnctl start sched
```

ESX ホストの専用ユーザー アカウントの作成

厳密に Avamar でのみ使用する専用の個別のユーザー アカウントを各 ESX ホストに設定することを強く推奨します。

「Administrator」のような一般的なユーザー アカウントを使用すると、どのアクションが Avamar サーバーと実際に連携または通信しているかが不明になり、将来トラブルシューティングを行う際に障害になる可能性があります。個別の ESX ホストのユーザー アカウントを使用することで、ESX ホストのログを分析する必要が生じた場合に、ログが最大限に明確化されます。

注

保護対象の各 ESX ホストで、最上位（root）レベルにユーザー アカウントを追加する必要があります。

次の表に挙げられた権限を持つ ESX ホスト ユーザー アカウントを作成します。

表 13 最小限必要な ESX ホストのユーザー アカウントの権限

権限の種類	必要な権限
アラーム	• アラームの作成
データストア	• 領域の割り当て • データストアの参照 • 低レベルのファイル操作 • ファイルの削除
拡張機能	• 拡張機能の登録 • 拡張機能の登録解除 • 拡張機能のアップデート
フォルダ	• フォルダを作成
グローバル	• タスクのキャンセル • メソッドの無効化 • メソッドの有効化 • ライセンス • イベントのログ

表 13 最小限必要な ESX ホストのユーザー アカウントの権限 （続き）

権限の種類	必要な権限
	• カスタム属性の管理 • 設定
ホスト> 構成	• 接続 • ストレージ パーティション構成
ネットワーク	• ネットワークの割り当て • 構成
リソース	• 仮想マシンのリソース プールへの割り当て
セッション	• セッションの確認
タスク	• タスクの作成 • タスクの更新
vApp	• インポート
仮想マシン	
システム構成	• 既存ディスクの追加 • 新しいディスクの追加 • デバイスの追加または削除 • 拡張 • CPU 数の変更 • リソースの変更 • ディスク変更の追跡 • ディスクのリース • 仮想ディスクの拡張 • ホスト USB デバイス • メモリ • デバイス設定の変更 • Raw デバイス • パスから再ロード • ディスクの削除 • 名前の変更 • ゲスト情報のリセット • 設定 • Swapfile の配置 • 仮想マシン互換性のアップグレード

表 13 最小限必要な ESX ホストのユーザー アカウントの権限 （続き）

権限の種類	必要な権限
ゲスト操作	• ゲスト操作の変更 • ゲスト操作のプログラム実行 • ゲスト操作のクエリー
対話	• コンソールの対話 • DeviceConnection • VIX API によるゲスト オペレーティング システムの管理 • 電源オフ • 起動 • リセット • VMware Tools のインストール
インベントリ	• 新規作成 • 登録 • 削除 • 登録解除
プロビジョニング	• ディスク アクセスの許可 • 読み取り専用ディスク アクセスの許可 • 仮想マシン ダウンロードの許可 • テンプレートとしてマーク
スナップショットの管理	• スナップショットの作成 • スナップショットの削除 • スナップショットに戻る • 管理
状態	

ESX ホストを vCenter Client として追加

手順

1. Avamar Administrator で、［**Administration**］起動リンクをクリックします。

   ［**Administration**］ウィンドウが表示されます。
2. ［**Account Management**］タブをクリックします。
3. ツリーで最上位レベルの（root）ドメインを選択して、［**Actions**］ > ［**Account Management**］ > ［**New Client(s)**］の順に選択します。

   ［**New Client**］ダイアログ ボックスが表示されます。
4. 以下の設定を行います。

a. [**Client Type**] リストで [**VMware vCenter**] を選択します。
b. [**New Client Name or IP**] フィールドに ESX ホストの完全修飾 DNS 名または IP アドレスを入力します。
c. [**Port**] フィールドに ESX ホストの Web サービス リスナー データ用ポート番号を入力します。

   デフォルト設定は、443 です。
d. [**User Name**] フィールドに ESX ホストの管理ユーザー アカウント名を入力します。
e. [**Password**] フィールドに ESX ホストの管理ユーザー アカウントのパスワードを入力します。
f. [**Verify Password**] フィールドに ESX ホストの管理ユーザー アカウントのパスワードを再度入力します。
g. (オプション) [**Contact**] フィールドに連絡先名を入力します。
h. (オプション) [**Phone**] フィールドに連絡先電話番号を入力します。
i. (オプション) [**Email**] フィールドに連絡先メール アドレスを入力します。
j. (オプション) [**Location**] フィールドに連絡先の場所を入力します。

5. [**OK**] をクリックします。

スタンドアロン ESX ホストでプロキシを導入する

はじめに

1. 導入する予定の各プロキシに DNS エントリーを追加します。
   プロキシの導入中に、各プロキシに一意の IP アドレスを割り当てるように求められます。ESX ホストは、確実にホスト名に解決するために、その IP アドレスの DNS 逆引き参照を実行します。最適な結果を得るために、この手順の未処理部分に進む前に、導入を予定しているすべてのプロキシに対してすべての必要な DNS エントリーを設定します。
2. Avamar サーバーからプロキシ アプライアンス テンプレート ファイルをダウンロードします。
3. vSphere クライアントを Windows コンピューターにインストールします。

vSphere Client を使用した ESX ホストでのプロキシ アプライアンスの導入

手順

1. vSphere Client を起動し、ESX ホストにログインします。
2. [**File**] > [**Deploy OVF Template**] を選択します。

   [**Deploy OVF Template**] ウィザードが表示されます。
3. [**Source**] スクリーンで次の操作を実行します。
   a. [**Browse**] をクリックします。

      [**Open**] ダイアログ ボックスが表示されます。
   b. [**Files of Type**] リストから、[**Ova files (*.ova)**] を選択します。
   c. すでにダウンロードしたアプライアンス テンプレート ファイルを参照します。
   d. アプライアンス テンプレート ファイルを選択して、[**Open**] をクリックします。

アプライアンス テンプレート ファイルへのフル パスが、［**Source**］スクリーンの［**Deploy from file**］フィールドに表示されます。

e. ［**Next**］をクリックします。

4. ［**OVF Template Details**］スクリーンで次の操作を実行します。
   a. テンプレート情報が正しいことを確認します。
   b. ［**Next**］をクリックします。
5. ［**Name and Location**］スクリーンで次の操作を実行します。
   a. ［**Name**］フィールドに、一意の完全修飾ホスト名を入力します。

      プロキシは 3 つの異なる名前を持つことが可能です。

      - プロキシが実行される仮想マシンの名前。
      - プロキシ仮想マシンに割り当てられた DNS 名。
      - プロキシがサーバーに登録され、アクティブ化された後の Avamar クライアント名。

      注

      混乱を避け、潜在的問題を回避するためにも、3 つのすべてのコンテキストで、このプロキシに対して常に同じ完全修飾ホスト名を使用することを強く推奨します。

   b. ［**Next**］をクリックします。
6. ［**Resource Pool**］スクリーンで次の操作を実行します。
   a. ESX ホストまたはリソース プールを選択します。
   b. ［**Next**］をクリックします。
7. ［**Storage**］スクリーンで次の操作を実行します。
   a. このプロキシのストレージの場所を選択します。
   b. ［**Next**］をクリックします。
8. ［**Disk Format**］スクリーンで次の操作を実行します。
   a. このプロキシのディスク フォーマットを選択します。
   b. ［**Next**］をクリックします。
9. ［**Network Mapping**］スクリーンで次の操作を実行します。
   a. リストからターゲット ネットワークを選択します。
   b. ［**Next**］をクリックします。
10. ［**Ready To Complete**］スクリーンで次の操作を実行します。
    a. 情報が正しいことを確認します。
    b. ［**Finish**］をクリックします。

プロキシ ネットワーク設定の手動構成

手順

1. vSphere Client を起動し、ESX ホストにログインします。
2. 構成するプロキシを見つけます。

3. ［**Open Console**］を右クリックします。

   コンソール ウィンドウが表示されます。

4. コンソールの［**Main Menu**］で 2 キーを押して終了します。
5. 初期スクリーンで［**Log in**］を選択した後、［**Enter**］キーを押します。
6. admin ユーザーとしてログインします。
7. 以下のように入力して、root ユーザーに切り換えます。

   ```
   su -
   ```

8. **/opt/vmware/share/vami/vami_config_net** と入力して、［**Enter**］キーを押します。

   ［**Main Menu**］が表示されます。

9. ［**Main Menu**］で［**6**］を選択し、［**Enter**］キーを押して、eth0 の IP アドレスを構成します。

   IPv6 アドレス、固定 IPv4 アドレス、動的 IPv4 アドレスのいずれかを構成できます。画面のプロンプトに従って、使用しているサイトに適切なアドレス タイプを構成します。

10. ［**Main Menu**］で［**4**］を選択し、［**Enter**］キーを押して、DNS を構成します。

    画面のプロンプトに従って、サイトで使用するプライマリおよびセカンダリ DNS サーバーを指定します。

11. ［**Main Menu**］で［**3**］を選択し、［**Enter**］キーを押して、ホスト名を構成します。
12. プロキシ ホスト名を入力して、［**Enter**］キーを押します。
13. ［**Main Menu**］で［**2**］を選択し、［**Enter**］キーを押して、デフォルト ゲートウェイを構成します。
14. IPv4 デフォルト ゲートウェイを入力して、［**Enter**］キーを押します。
15. ［**Enter**］キーを押して、デフォルトで設定されている IPv6 デフォルト ゲートウェイを受け入れます。
16. ［**Main Menu**］で［**Enter**］キーを押して、現在の構成を表示します。
17. 設定が正しいことを確認します。
18. 1 キーを押して、プログラムを終了します。

プロキシを Avamar サーバーに登録し、アクティブ化する

vCenter に導入された各プロキシを Avamar サーバーで登録およびアクティブ化します。

はじめに

1. vCenter でプロキシ アプライアンスを導入します。
2. ESX ホストを vCenter Client として Avamar に追加します。

注

最適な結果が得られるように、このタスクの説明に従って、プロキシを登録し、アクティブ化します。プロキシを Avamar Administrator から招待するという代替手段もありますが、その結果は予測不能です。

このタスクを ESX ホストに導入する各プロキシで実行します。

手順

1. vSphere Client から、Avamar イメージ バックアップ プロキシを見つけて、選択します。
2. 右クリックして、［**Power**］ > ［**Power On**］を選択します。
3. ［**Open Console**］を右クリックします。

   コンソール ウィンドウが表示されます。
4. ［**Main Menu**］で 1 を入力して、［**Enter**］キーを押します。
5. Avamar サーバーの DNS 名を入力して、［**Enter**］キーを押します。
6. Avamar サーバーのドメイン名を入力して、［**Enter**］キーを押します。

   デフォルトのドメインは「clients」です。ただし、Avamar システム管理者が他のドメインおよびサブドメインを定義している可能性があります。このクライアントを登録する際に使用するドメインについては、Avamar システム管理者に問い合わせてください。

   注

   サブドメイン（例えば、clients/MyClients）を入力する場合、先頭の文字としてスラッシュ（/）を含めないでください。先頭の文字としてスラッシュを含めると、エラーが発生し、このクライアントを登録できなくなります。

   ---
7. ［**Main Menu**］で 2 を入力し、［**Enter**］キーを押して終了します。
8. （オプション）プロキシ証明書認証が必要な場合は、次を参照してください：vCenter-to-Avamar 認証の構成（30 ページ）

vCenter から ESX ホストの関連付けを削除する

このタスクを実行できるのは、関連付けられている vCenter が稼働していない状態で、仮想マシンを ESX ホストにリストアしている場合のみです。

手順

1. vSphere クライアントまたは vSphere Web クライアントを起動し、ESX ホストにログインします。
2. ［サマリー］タブをクリックします。
3. ［**Host Management**］ペインで、［**Disassociate host from vCenter Server**］をクリックします。
4. ［**Yes**］をクリックしてアクションを確定します。

第 9 章

AWS（Amazon Web Services）での VMware クラウド向け Avamar イメージ バックアップ/リカバリ

本章は、次のトピックで構成されています。

VMware Cloud on AWS 向け Avamar イメージ バックアップ/リカバリ

Avamar では、AWS（Amazon Web Services）での VMware クラウドのイメージ バックアップとリストアのサポートを提供します。

VMware Cloud on AWS を実行している仮想マシンを Avamar を使用して保護することは、オンプレミス データセンターで仮想マシンを保護する方法と似ています。このセクションでは、ネットワーク構成要件、VMware Cloud on AWS の Avamar のベスト プラクティス、VMware Cloud on AWS でサポートされない Avamar の操作について説明します。

VMware Cloud on AWS Web ポータルのコンソールの設定

DNS（Domain Name System）の解決は、Avamar の導入、および Avamar サーバ、Avamar プロキシ、Data Domain アプライアンスの構成にとって非常に重要です。すべてのインフラストラクチャ コンポーネントは、FQDN（完全修飾ドメイン名）を介して解決される必要があります。解決とは、コンポーネントが前方（A）と逆引き（PTR）の両方の参照を使用してアクセス可能であることを意味します。

VMware Cloud on AWS Web ポータル コンソールで、次の要件が満たされていることを確認してください。

- デフォルトでは、SDDC（ソフトウェア デファインド データセンター）で vCenter Server システムへの外部アクセスはありません。ファイアウォール ルールを設定して、vCenter Server システムへのアクセスを開くことができます。SDDC 論理ネットワークから vCenter のパブリック IP アドレスへの通信を有効にするには、VMware Cloud on AWS のコンピューティング ゲートウェイでファイアウォール ルールを設定します。SDDC でファイアウォール ルールが設定されていない場合、Avamar サーバでは vCenter Server の追加が許可されません。
- コンピューティング ゲートウェイのデフォルトのファイアウォール ルールでは、仮想マシンのすべてのトラフィックがインターネットに到達できません。Avamar サーバ仮想マシンがインターネットに接続できるようにするためには、コンピューティング ゲートウェイのファイアウォール ルールを作成します。このアクションにより、Avamar サーバ仮想マシンが接続している論理ネットワークでのアウトバウンド トラフィックが可能になります。
- SDDC 内のマシンが、インターネットに属する IP アドレスに対する FQDN（完全修飾ドメイン名）を解決できるように DNS を設定します。SDDC で DNS サーバが構成されていない場合、Avamar サーバではサーバのパブリックな FQDN または IP アドレスを使用して vCenter Server を追加できません。
- Amazon VPC（Virtual Private Cloud）では、Data Domain システムを仮想アプライアンスとして導入することをお勧めします。SDDC の作成時に、AWS アカウントに SDDC を接続してから、そのアカウント内の VPC とサブネットを選択します。
- Amazon VPC を実行している Data Domain システムは、VMware Cloud ENI（Elastic Network Interface）を通じて VMware SDDC に接続する必要があります。このアクションにより、SDDC、AWS VPC 内のサービス、AWS アカウントのサブネットは、トラフィックをインターネット ゲートウェイ経由指定にしなくても通信できます。
  ENI の設定の詳細については、https://vmc.vmware.com/console/aws-link を参照してください。
- DDVE が Amazon VPC で実行されている場合は、Data Domain 接続用コンピューティング ゲートウェイのインバウンドおよびアウトバウンドのファイアウォール ルールを設定します。

- NSX-T を使用する場合は、vCenter Server の内部 IP アドレスに解決するように DNS を構成します。［**SDDC Management**］ > ［**Settings**］ > ［**vCenter FQDN**］に移動し、［**Private vCenter IP address**］を選択します。これで、内蔵ファイアウォール上の管理ネットワークに直接アクセスできます。さらに、管理ゲートウェイとコンピューティング ゲートウェイの両方で、vCenter Server の TCP ポート 443 が開いていることを確認します。
  また、NSX-T をファイル レベルのリストア処理に使用する場合は、プロキシ アプライアンス上の `axionfs.cmd` ファイルを、Avamar サーバーの IPv4 アドレスで更新する必要があります。Avamar サーバーで Avamar プロキシ アプライアンスを登録してアクティブ化した後、**root** として各 Avamar プロキシ アプライアンスにログインし、UNIX テキスト エディタで `/usr/local/avamar/var/axionfs.cmd` ファイルを開きます。ファイル内で、**--server** エントリー キーを見つけ、対応する値を Avamar サーバーの IPv4 アドレスに更新します。たとえば、**--server=192.168.2.150**。

Amazon AWS Web ポータルの要件

Amazon AWS Web ポータルでは、次の要件を必ず満たしてください。

- Amazon VPC で Data Domain を実行している場合は、VMware SDDC コンピューティング ゲートウェイと Data Domain との間の接続を提供するように、Amazon VPC セキュリティ グループのインバウンドとアウトバウンドのファイアウォール ルールを設定します。
- 1 つの Data Domain システムを別の Data Domain システムにレプリケートする場合は、AWS でセキュリティ グループに使用するインバウンド ルールを、Amazon VPC で実行している Data Domain Virtual Edition のそれぞれのプライベート IP アドレスからのすべてのトラフィックを許可するように設定します。
- レプリケーションを実行する AWS で実行されている Data Domain が複数ある場合は、双方の Data Domain システムで FQDN を使用して相互に ping を実行する機能がある必要があります。

vCenter Server インベントリの要件

お使いの SDDC の vCenter Server インベントリで、次の要件が満たされていることを確認します。

- 内部の DNS 名検索サーバは、vCenter インベントリ内で実行している必要があります。この検索サーバは、VMware SDDC で実行しているすべてのワークロードによって参照されます。
- 内部の DNS サーバで、インターネットにアクセスするために［**Forwarders**］が有効になっている必要があります。この処理は、vCenter Server のパブリック FQDN を解決するために必要です。
  フォワーダは、サーバが解決できないレコードの DNS クエリーを解決するためにサーバが使用できる DNS サーバです。

VMware Cloud on AWS における vCenter Server での vProxy OVA の導入

HTML5 vSphere Web Client を使用して vCenter Server から Avamar プロキシ アプライアンスの OVA を導入するには、次の手順を実行します。

はじめに

VMware Cloud on AWS Web ポータルのコンソールの設定（128 ページ）セクションを確認します。

手順

1. cloudadmin アカウントの認証情報を使用して、HTML5 vSphere Web Client にログインします。
2. ［**Menu**］ > ［**Hosts and Clusters**］の順にクリックします。
3. インベントリのパネルで、vCenter を展開し、次に SDDC クラスタ内の［**compute resource pool**］を展開します。
4. OVA を導入するリソース プールを右クリックしてから、［**Deploy OVF template**］を選択します。
5. ［**Select an OVF template**］ウィンドウで、OVA パッケージの URL パスを入力するか、［**Choose Files**］をクリックして OVA パッケージの場所に移動して、［**Next**］をクリックします。
6. ［**Select a name and folder**］ウィンドウで、以下の手順を実行します。
   a. 仮想アプライアンスの名前を指定します。
   b. インベントリの場所を指定します。
   c. ［**Next**］をクリックします。
7. ［**Select a compute resource**］ウィンドウで、OVA を導入する vApp またはリソース プールを選択し、［**Next**］をクリックします。
8. ［**Review details**］ウィンドウで、製品名、バージョン、ベンダー、パブリッシャー、ダウンロードサイズなどの製品詳細をレビューしてから［**Next**］をクリックします。
9. ［**Select storage**］ウィンドウで、ディスク フォーマットと、仮想アプライアンスのファイルの格納先となるデータストアを選択し、［**Next**］をクリックします。

   仮想アプライアンスに割り当てられたストレージ容量を確実に使用できるようにするために、［**Thick Provision Lazy Zeroed**］を選択します。
10. ［**Select networks**］ウィンドウで、［**Destination Network**］を選択します。
    a. IP アドレスを指定します
    b. ［**Next**］をクリックします。
11. ［**Customize Template**］ウィンドウで、［**Networking properties**］を展開します。
    a. ［**Network IP address**］フィールドで、Avamar プロキシの IP アドレスを入力します。
    b. ［**Network Netmask/Prefix**］フィールドで、IPv4 ネットワークの IP アドレスのネットマスクを指定します。
    c. ［**DNS**］フィールドに、DNS サーバの IP アドレスをコンマで区切って入力します。
    d. ［**NTP**］フィールドに、ゲートウェイ ホストの IP アドレスを入力します。
    e. ［**Default gateway**］フィールドで、ゲートウェイ ホストの IP アドレスを入力します。
12. ［**Next**］をクリックします。

    ［［**Ready to Complete**］］ウィンドウが表示されます。
13. ［**Ready to Complete**］ウィンドウで、導入構成の詳細を確認し、［**Finish**］をクリックします。

結果

［**Deploying template**］タスクが vCenter に表示され、導入に関するステータス情報が表示されます。

VMware Cloud on AWS 向け vCenter-to-Avamar 認証の構成

vCenter-to-Avamar 認証を構成する上で最も安全な方法は、vCenter 認証証明書を Avamar MCS キーストアに追加することです。このタスクは、保護対象の各 vCenter に対して実行する必要があります。

VMware Cloud on AWS の認証証明書をインポートするには、次の手順を実行します。

手順

1. Entrust の Web サイトからルート証明書をダウンロードします。

   https://www.entrustdatacard.com/pages/root-certificates-download に移動します。

2. Avamar サーバにルート証明書を配置し、vCenter 認証証明書を MCS キーストアに追加（30 ページ）セクションの指示に従います。
3. vCenter を Avamar サーバに追加します。

VMware Cloud on AWS 向け Avamar イメージ バックアップ/リストアのベスト プラクティス

VMware Cloud on AWS を実行している仮想マシンの保護に Avamar を使用する場合は、次のベスト プラクティスを考慮してください。

- Avamar サーバまたはプロキシを導入または構成する場合は、vCenter インベントリを実行している内部 DNS サーバを示す DNS サーバの IP アドレスを指定するようにします。
- 内部 DNS サーバでの前方参照および逆引き参照の両方のエントリーが、Avamar サーバ、Avamar プロキシ アプライアンス、DDVE（Data Domain Virtual Edition）などの必要なすべてのコンポーネント内の必要な場所にあるようにします。
- NSX-T を使用する場合は、vCenter Server の内部 IP アドレスに解決するように DNS を構成します。［**SDDC Management**］ > ［**Settings**］ > ［**vCenter FQDN**］に移動し、［**Private vCenter IP address**］を選択します。これで、内蔵ファイアウォール上の管理ネットワークに直接アクセスできます。さらに、管理ゲートウェイとコンピューティング ゲートウェイの両方で、vCenter Server の TCP ポート 443 が開いていることを確認します。
  また、NSX-T をファイル レベルのリストア処理に使用する場合は、プロキシ アプライアンス上の `axionfs.cmd` ファイルを、Avamar サーバーの IPv4 アドレスで更新する必要があります。Avamar サーバーで Avamar プロキシ アプライアンスを登録してアクティブ化した後、**`root`** として各 Avamar プロキシ アプライアンスにログインし、UNIX テキスト エディタで `/usr/local/avamar/var/axionfs.cmd` ファイルを開きます。ファイル内で、**`--server`** エントリー キーを見つけ、対応する値を Avamar サーバーの IPv4 アドレスに更新します。たとえば、**`--server=192.168.2.150`**。
- Avamar サーバに vCenter Server を追加するには、次のオプションのいずれかを使用します。
  - vCenter Server のパブリック FQDN
  - vCenter Server のパブリック IP アドレス。

  FQDN を使用することをお勧めします。
- vCenter Server を Avamar サーバに追加する場合は、cloudadmin ユーザーのログイン認証情報を指定します。

- vCenter 認証を使用して AUI にアクセスする場合は、`/usr/local/avamar/var/mc/server_data/prefs/application-production.properties` ファイルに次のパラメーターを追加して、mcs サービスを再起動します。
  `vmc.vcenters=VMware Cloud vCenter FQDN`

サポート対象外の Avamar の操作

VMware Cloud on AWS での Avamar のイメージ バックアップ/リストアでは、現在次の操作はサポートされていません。

- アプリケーション コンシステントなバックアップ
- Proxy Deployment Manager。プロキシを手動で導入する必要がある
- NSX-V を使用している場合のイメージ レベルのバックアップからのファイル レベルのリストア。NSX-T を使用している場合、この操作はサポートされる点に注意してください。
- イメージ レベル バックアップのインスタント アクセス リカバリ
- 非常時のリストア（vCenter をバイパスして ESXi ホストに直接行うイメージ レベル リストア）
- NBD または NBDSSL 転送モードを使用するイメージ レベルのバックアップ/リストア
- 高度なポリシー ベースの、Avamar を使用した MS SQL 向けデータ保護
- MS-SQL および MS-Exchange 向けアプリケーション認識のイメージ バックアップ
- データセンターがフォルダーの下にある場合のイメージのバックアップ/リストア
- Windows イメージ バックアップからのページ ファイルまたはユーザー定義ファイルの除外
- デュアル スタックまたは IPv6 専用に構成されている vProxy アプライアンス
- NBD、NBDSSL、SAN。HotAdd のみがサポートされる
- 動的なポリシーの VMware タグ ベースのルール選択基準
- 新規 vApp へのリストア
- IPV6
- 仮想マシン テンプレートのバックアップ

付録 A

プロキシの手動導入

本付録は、次のトピックで構成されます。

概要

Avamar 7.2 以降、Proxy Deployment Manager は、プロキシを導入するための推奨方法です。必要に応じて、手動によるプロキシ導入も引き続きサポートされています。

プロキシ アプライアンス テンプレート ファイルのダウンロード

Avamar サーバーからプロキシ アプライアンス テンプレート ファイルをダウンロードします。

注

複数のプロキシを追加する場合、このタスクは一度の実行で済みます。

手順

1. Web ブラウザを開き、次の URL を入力します。

   `https://Avamar-server`

   ここで、Avamar-server は Avamar サーバーのネットワーク ホスト名または IP アドレスです。

   ［**Avamar Web Restore**］ページが表示されます。
2. ［**Downloads**］をクリックします。
3. `VMware vSphere\EMC Avamar VMware Image Backup\FLR Appliance` フォルダに移動します。
4. ［**AvamarCombinedProxy-linux-sles12sp1-x86_64-version.ova**］リンクをクリックします。
5. ［**AvamarCombinedProxy-linux-sles12sp1-x86_64-version.ova**］を、`C:\Temp` などの一時フォルダーまたはデスクトップに保存します。

vCenter でのプロキシ アプライアンスの導入

Windows コンピューターで稼働する vSphere Client（別名「シック クライアント」）、または vSphere Web Client のいずれかを使用して、イメージ バックアップで保護する対象の各 vCenter に 1 個以上のプロキシを導入します。

はじめに

1. 導入する予定の各プロキシに DNS エントリーを追加します。
   プロキシの導入中に、各プロキシに一意の IP アドレスを割り当てるように求められます。vCenter は、確実にホスト名に解決するために、その IP アドレスの DNS 逆引き参照を実行します。最適な結果を得るために、この手順の未処理部分に進む前に、導入を予定しているすべてのプロキシに対してすべての必要な DNS エントリーを設定します。
2. Avamar サーバーからプロキシ アプライアンス テンプレート ファイルをダウンロードします。

vSphere Web Client を使用した vCenter でのプロキシ アプライアンスの導入

手順

1. Web ブラウザーを開いて、次の URL を入力し、vCenter Server に接続します。

   `http://vCenter-server:9443/`

   ここで、vCenter-server は vCenter Server のネットワーク ホスト名または IP アドレスです。

   ［**vSphere Web Client**］ページが表示されます。

2. 次の手順に従って、vSphere Client Integration プラグ インをダウンロードし、インストールします。

   注

   これらのステップは、vSphere Web Client を使用して、この vCenter Server に初めて接続する際にのみ実行する必要があります。それ以降の vSphere Web Client セッションでは、これらのステップをスキップすることができます。

   a. ［**Download Client Integration Plug-in**］リンクをクリックします。

   b. サーバー上でインストール ファイルを直接開くか、ダウンロードしたインストール ファイルをダブル クリックします。

      インストール ウィザードが表示されます。

   c. 画面上に表示される指示に従います。

3. Web ブラウザーを開いて、次の URL を入力し、vCenter Server に再接続します。

   `http://vCenter-server:9443/`

   ここで、vCenter-server は vCenter Server のネットワーク ホスト名または IP アドレスです。

   ［**vSphere Web Client**］ページが表示されます。

4. ［ユーザー名］と［パスワード］を入力して、［**Login**］をクリックし、vCenter Server にログインします。

5. ［**Home**］ > ［**vCenter**］ > ［**Hosts and Clusters**］を選択します。

6. ［**Actions**］ > ［**Deploy OVF Template**］を選択します。

7. プラグ インのアクセス制御を許可します。

   ［**Deploy OVF Template**］ウィザードが表示されます。

8. ［**Source**］スクリーンで次の操作を実行します。

   a. ［**Local file**］を選択して、［**Browse**］をクリックします。

      ［**Open**］ダイアログ ボックスが表示されます。

   b. ［**Files of Type**］リストから、［**Ova files (*.ova)**］を選択します。

   c. すでにダウンロードしたアプライアンス テンプレート ファイルを参照します。

d. アプライアンス テンプレート ファイルを選択して、［**Open**］をクリックします。

アプライアンス テンプレート ファイルへのフル パスが、［**Source**］スクリーンの［**Deploy from file**］フィールドに表示されます。

e. ［**Next**］をクリックします。

9. ［**OVF Template Details**］スクリーンで次の操作を実行します。

a. テンプレート情報が正しいことを確認します。

b. ［**Next**］をクリックします。

10. ［**Select name and Location**］スクリーンで次の操作を実行します。

a. ［**Name**］フィールドに、一意の完全修飾ホスト名を入力します。

プロキシは 3 つの異なる名前を持つことが可能です。

- プロキシが実行される仮想マシンの名前。これも vCenter 内で管理され、認識できる名前です。
- プロキシ仮想マシンに割り当てられた DNS 名。
- プロキシがサーバーに登録され、アクティブ化された後の Avamar クライアント名。

注

混乱を避け、潜在的問題を回避するためにも、3 つのすべてのコンテキストで、このプロキシに対して常に同じ完全修飾ホスト名を使用することを強く推奨します。

b. ツリーで、このプロキシのデータセンターとフォルダーの場所を選択します。

c. ［**Next**］をクリックします。

11. ［**Select a resource**］スクリーンで次の操作を実行します。

a. ESX ホスト、クラスター、vApp、リソース プールのいずれかを選択します。

b. ［**Next**］をクリックします。

12. ［**Select Storage**］スクリーンで次の操作を実行します。

a. このプロキシのストレージの場所を選択します。

b. ［**Next**］をクリックします。

13. ［**Setup networks**］スクリーンで次の操作を実行します。

a. リストから［ターゲット］ ネットワークを選択します。

b. リストから［**IP** プロトコル］を選択します。

c. ［**Next**］をクリックします。

14. ［**Customize template**］スクリーンで次の操作を実行します。

注

Avamar サーバにプロキシが登録され、アクティブ化されると、プロキシ ネットワークの設定を変更するのは難しくなります。そのため、［**Customize template**］スクリーンで入力する設定が正確であることを確認してください。

a. ［**Default Gateway**］フィールドにネットワークのデフォルト ゲートウェイ IP アドレスを入力します。

b. DHCP を使用しない場合は、［**DNS**］フィールドに、1 つ以上の DNS（ドメイン ネーム サーバー）IP アドレスを入力します。複数のエントリーはコンマで区切ります。

c. DHCP を使用しない場合は、このプロキシの有効な IP アドレスを［**Isolated Network IP Address**］フィールドに入力します。

d. ［**Isolated Network Netmask**］フィールドに、ネットワーク マスクを入力します。

e. ［**Next**］をクリックします。

15. ［**Ready To Complete**］スクリーンで次の操作を実行します。

a. 情報が正しいことを確認します。

b. ［**Finish**］をクリックします。

プロキシを Avamar サーバーに登録し、アクティブ化する

vCenter に導入された各プロキシを Avamar サーバーで登録およびアクティブ化します。

はじめに

1. vCenter でプロキシ アプライアンスを導入します。
2. ESX ホストを vCenter Client として Avamar に追加します。

注

最適な結果が得られるように、このタスクの説明に従って、プロキシを登録し、アクティブ化します。プロキシを Avamar Administrator から招待するという代替手段もありますが、その結果は予測不能です。

このタスクを ESX ホストに導入する各プロキシで実行します。

手順

1. vSphere Client から、Avamar イメージ バックアップ プロキシを見つけて、選択します。
2. 右クリックして、［**Power**］ > ［**Power On**］を選択します。
3. ［**Open Console**］を右クリックします。

   コンソール ウィンドウが表示されます。
4. ［**Main Menu**］で 1 を入力して、［**Enter**］キーを押します。
5. Avamar サーバーの DNS 名を入力して、［**Enter**］キーを押します。
6. Avamar サーバーのドメイン名を入力して、［**Enter**］キーを押します。

   デフォルトのドメインは「clients」です。ただし、Avamar システム管理者が他のドメインおよびサブドメインを定義している可能性があります。このクライアントを登録する際に使用するドメインについては、Avamar システム管理者に問い合わせてください。

   注

   サブドメイン（例えば、clients/MyClients）を入力する場合、先頭の文字としてスラッシュ（/）を含めないでください。先頭の文字としてスラッシュを含めると、エラーが発生し、このクライアントを登録できなくなります。

   ---
7. ［**Main Menu**］で 2 を入力し、［**Enter**］キーを押して終了します。

8. （オプション）プロキシ証明書認証が必要な場合は、次を参照してください：vCenter-to-Avamar 認証の構成（30 ページ）

Avamar Administrator でのプロキシ設定の構成

vCenter にプロキシ アプライアンスを導入し、Avamar サーバに登録した後、Avamar Administrator でデータストア、グループ、担当者（オプション）の設定を構成します。

はじめに

1. vCenter でプロキシ アプライアンスを導入します。
2. プロキシを Avamar サーバーに登録し、アクティブ化します。

手順

1. Avamar Administrator で、［**Administration**］起動リンクをクリックします。

   ［**Administration**］ウィンドウが表示されます。
2. ［**Account Management**］タブをクリックします。
3. ツリーでプロキシを選択した後、［**Actions**］ > ［**Account Management**］ > ［**Client Edit**］を選択します。

   ［**Edit Client**］ダイアログ ボックスが表示されます。
4. ［**Datastores**］タブをクリックし、このプロキシで保護する仮想マシンをホストするすべての vCenter データストアを選択します。
5. ［**Groups**］タブをクリックし、各グループの横の［**Select**］チェックボックスをクリックして、1 つまたは複数のグループにこのプロキシを割り当てます。
6. （オプション）次の手順で連絡先情報を入力します。
   a. ［**Contact**］フィールドに連絡先名を入力します。
   b. ［**Phone**］フィールドに連絡先電話番号を入力します。
   c. ［**Email**］フィールドに連絡先メール アドレスを入力します。
   d. ［**Location**］フィールドに連絡先の場所を入力します。
7. ［**OK**］をクリックします。

オプションのプロキシ パフォーマンス最適化の実行

デフォルトで、Avamar プロキシは 4 個の仮想 CPU ソケットとソケットあたり 1 個のコアで構成されています。ただし、使用する ESXi ホストに 2 個以上の物理 CPU が搭載されている場合は、4 個の仮想 CPU ソケットとソケットあたり 2 個のコアにプロキシ構成を変更すると、バックアップおよびリストアのパフォーマンスが向上されます。

付録 B

vSphere データ ポート

本付録は、次のトピックで構成されます。

必要なデータ用ポート

これらは vSphere 環境に必要なデータ用ポートです。

表 14 必要な vSphere データ用ポート

ポート	ソース	ターゲット	機能	関連情報
22	Avamar Administrator	プロキシ	SSH	診断サポート。これはオプションですが、推奨事項です。
53	プロキシ	DNS サーバー	DNS	UDP+TCP
443	Avamar Deployment Manager	VMware ESXi ホスト	vSphere API	
443	プロキシ	VMware ESXi ホスト	vSphere API	
443	プロキシ	vCenter	vSphere API	
443	Avamar MCS	vCenter	vSphere API	
902	プロキシ	VMware ESX ホスト	VDDK	
5489	Avamar Deployment Manager	プロキシ	CIM サービス	プロキシを登録するために使用します。
7444	Avamar MCS	vCenter	vCenter 認証情報のテスト	
27000	プロキシ	Avamar サーバー	GSAN の通信	非セキュアな通信
28009	Avamar MCS	プロキシ	プロキシ ログにアクセス	
28102～28109	Avamar MCS	プロキシ	`avagent` ページング ポート	Avamar 7.0 および 7.1
29000	プロキシ	Avamar サーバー	GSAN の通信	セキュアな通信
30001	プロキシ	Avamar MCS	`avagent` から MCS への通信	Avamar 7.2
30102～30109	Avamar MCS	プロキシ	`avagent` ページング ポート	Avamar 7.2

注

別途記載がない限り、すべてのポートは TCP です。

付録 C

VMware vRealize Log Insight の使用方法

本付録は、次のトピックで構成されます。

VMware vRealize Log Insight について

ログ管理を一元化するために VMware vRealize Log Insight にログを転送するように、イメージ プロキシを設定できます。このステップにより、エラー タイプのパターンと頻度を識別するとともに、ログのローテーションによるログ エントリーの消失を避けるためのメカニズムを実装できます。

Avamar で Log Insight をサポートするには、vRealize Log Insight アプライアンスが vCenter に導入されている必要があります。この機能はプロキシまたはその他のクライアントにインストールされている LFA（Log Forwarding Agent）を使用して、LCRS（Log Central Reporting Service）にログの内容をプッシュします。LCRS は、ユーティリティ ノードまたは Avamar Virtual Edition サーバーにインストールされています。LCRS は、vCenter を実行している vRealize Log Insight サーバーにログを転送します。

注

Avamar サーバーがアップグレードされるたびに、アップグレードされた Avamar サーバーで次のステップを実行します。

1. Log Central Reporting Service の設定
2. ログ転送エージェントの構成

この付録では、Avamar サーバで実行している LCRS、およびプロキシと他のクライアントで実行している LFA の設定について説明します。

Log Central Reporting Service の設定

LCRS（Log Central Reporting Service）は、ユーティリティ ノードまたは AVE（Avamar Virtual Edition）サーバで実行します。以下の処理手順を使用して、プロキシから vRealize Log Insight アプライアンスへログ情報を転送するように設定します。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
   - シングル ノード サーバの場合は、admin としてサーバにログインし、**su -**と入力してユーザーを root に切り替えます。
   - マルチ ノード サーバの場合は、admin としてユーティリティ ノードにログインし、**su -**と入力してユーザーを root に切り替えます。
2. `/usr/local/emc-lcrs/etc/`ディレクトリに移動します。
3. `lcrs.ini` をテキスト エディタで開きます。
4. 次のようにこのファイルを編集します。

```
server.port=8080
forward.server=Log_Insight_Server_IP
forward.port=Log_Insight_Server_port
forward.messagePerSend=10
forward.type=LogInsight
upload.forward=true
forward.delete=true
forward.dispatch=true
```

ここで、Log_Insight_Server_IP は vRealize Log Insight アプライアンスの IP アドレス、Log_Insight_Server_port は vRealize Log Insight アプライアンスによって使用されるポートです。

5. ファイルを保存して閉じます。

ログ転送エージェントの構成

LFA（ログ転送エージェント）を構成するには、次の処理手順に従います。

手順

1. ログ メッセージを LCRS（Log Central Reporting Service）に転送するように構成されるプロキシに admin としてログインします。
2. 次のコマンドを入力して、ユーザーを root に切り替えます。

   su -

3. 以下のコマンドを入力します。

   /usr/local/avamarclient/etc/proxylfa_setup.sh

   次のように表示されます。

   ```
   Avamar VMware Log Forwarding Agent Setup
   Main Menu
   ---------
   1) Setup LCRS IP address
   2) Enable Avamar VMware Log Forwarding Agent cron job
   3) Disable Avamar VMware Log Forwarding Agent cron job
   4) quit
   Your choice:
   ```

4. プロンプトで **1** と入力して、Avamar ユーティリティ ノード、または LCRS（Log Central Reporting Service）を実行している AVE の IP アドレスを入力します。
5. プロンプトで **2** と入力し、LFA cron ジョブを有効にします。

   cron ジョブはプロキシから LCRS へ 10 分間隔でログを転送します。

6. プロンプトで **4** と入力してプログラムを終了します。

付録 D

プラグ イン オプション

本付録は、次のトピックで構成されます。

プラグ イン オプションの設定方法

プラグ イン オプションにより、オン デマンド バックアップ、リストア、スケジュール設定されたバックアップの特定のアクションを制御することができます。操作とプラグ インのタイプによって、利用可能なプラグ イン オプションが異なります。

AUI のプラグ イン オプションは、オン デマンド バックアップまたはリストア ウィザードに対して、またはスケジュール設定されたバックアップのデータセットを作成するときに、指定することができます。プラグ イン オプションは、GUI（グラフィカル ユーザー インターフェイス）コントロール（テキスト ボックス、チェックボックス、ラジオ ボタンなど）で設定します。［**Key**］フィールドと［**Value**］フィールドにオプションと値を入力します。

通知

Avamar ソフトウェアは、［**More Options**］パネルの［**Show Free Form**］セクションに入力された情報のチェックまたは妥当性検査を行いません。［**Key**］および［**Value**］フィールドの値によって、オプションの GUI コントロールで指定された設定はオーバーライドされます。

VMware Image プラグ インのバックアップ オプション

これらのバックアップ オプションは、Avamar VMware Image プラグ インで利用可能です。

表 15 Avamar VMware Image プラグ インのバックアップ オプション

設定	説明
Use Changed Block Tracking (CBT) to increase performance	これを選択すると、最後のバックアップ以降に変更された仮想マシン ファイル システムのエリアを特定し、次のバックアップでその変更されたエリアのみを処理するために、VMware 更新ブロック追跡機能が使用されます。 注 更新ブロック追跡は、この機能が動作するように、仮想マシン レベルで有効化されている必要があります。
Set Annotionation Tag LastBackupStatus and LastSuccessfulBackup	これを選択すると、最新のバックアップと最新の正常なバックアップに関する情報を、Avamar サーバが vSphere Web Client または従来の Windows ベースの vSphere Client にレポートできるようにします。 これを選択した場合は、vSphere Web Client の注釈リストに次の情報が表示されます。 • ［**LastSuccessfulBackupStatus-com.dellemc.avamar**］: 最新の正常なバックアップの日時。 • ［**LastBackupStatus-com.dellemc.avamar**］: 成功か失敗かにかかわらず、最新のバックアップの日時。

表 15 Avamar VMware Image プラグ インのバックアップ オプション （続き）

設定	説明
Exclude page file blocks when performing image backup on Windows VM	これを選択すると、Windows ページ ファイル（`pagefile.sys`）がすべてのパーティションのバックアップから除外されます。これは、プライマリ パーティションに限定されません。 注 ページ ファイルの除外は、Windows Server 2008 R2 以降のバージョンに対してのみサポートされます。クライアント バージョンの Windows では、このオプションによる影響はなく、この設定に関係なくページ ファイルは Windows クライアントのバックアップに含まれます。 注 プロキシは、ページ ファイル ブロックを読み取るために内部的に NBD 転送モードを使用します。必要となるブロックを認識した後、バックアップ/リストア処理に応じて使用可能なモード（hotadd/nbdssl/nbd）を使用します。
Exclude deleted file blocks when performing image backup on Windows VM	これを選択すると、すべてのパーティションのバックアップから削除されたファイル ブロックを除外します。これは、プライマリ パーティションに限定されません。
Exclude files with path and filter	すべてのパーティションのバックアップから、パスとフィルターを使用してファイルを除外します。これは、プライマリ パーティションに限定されません。 ファイルまたはフォルダーのフル パスまたはファイルとフォルダーのフィルター パスを入力します。複数のエントリーはコンマで区切ります。 パスおよびフィルターを使用してファイルを除外するには、次の形式でパスを入力します。 • ドライバ文字で始まる • フォルダーを除外するには「/」で終わる • ファイルを除外するには最後に「/」を付けない • すべてファイルを除外するにはファイル名でワイルドカードとして「*」を使用してください。ファイル パスでワイルドカードとして「*」を使用しないでください。 例： ▪ `*:/*/*.TXT` はサポートされていません。 ▪ `D:/folder/*.txt` はサポートされています。 ▪ `D:/folder/*`はサポートされています。

表 15 Avamar VMware Image プラグ インのバックアップ オプション （続き）

設定	説明
Store backups on Data Domain system	Avamar サーバーの代わりに Data Domain システムへバックアップを保存するには、チェックボックスをオンにして、リストから Data Domain システムを選択します。 注 Data Domain システムを Avamar の構成に追加すると、このオプションは有効になります。手順については、「Avamar および Data Domain システム統合ガイド」を参照してください。
Encryption method to Data Domain system	バックアップ中にクライアントと Data Domain システム間のデータ転送に使用される暗号化方式を指定します。Avamar リリース 7.5 時点では、サポートされる暗号化方式は「高」のみです。
［スナップショットの削除の再試行］	
Max times to retry snapshot delete	スナップショットの削除操作が試行される最大回数。
［ゲスト認証情報 ］	
Username	スクリプトの実行に十分な権限のあるゲスト オペレーティング システムのユーザー アカウント。
Password	ゲスト オペレーティング システムのユーザー名のパスワード。
［プレスナップショット スクリプト ］	
Script file	vmdk スナップショットの前に実行されるスクリプトのフルパスとファイル名。
Maximum script run time (minutes)	このスクリプトがタイムアウトの前に実行できる最大分数。
［ポストスナップショット スクリプト ］	
Script file	バックアップが完了して vmdk スナップショットが削除された後に、実行されるスクリプトのフルパスとファイル名。
Maximum script run time (minutes)	このスクリプトがタイムアウトの前に実行できる最大分数。
［スナップショットの停止タイムアウト］	
Snapshot quiesce timeout (minutes)	スナップショットの停止操作が失敗したと見なされるまでに待機する最大時間（分）（Windows VMware イメージ プラグ インのみ）
［**Microsoft SQL Server** 認証］	
NT Authentication	認証について［Guest Credentials］に入力した認証情報が使用されます。ユーザーは管理権限を持っ

表 15 Avamar VMware Image プラグ インのバックアップ オプション （続き）

設定	説明
	ている必要があり、ファイル システムに対する書き込みアクセス権および Windows レジストリに対する読み取り権限がある必要があります。
Application Authentication	SQL Server のユーザー名と SQL Server のパスワードを使用して SQL Server にログインします。
［**Microsoft SQL Server** のバックアップ後の処理］	
Post Action Timeout (minutes)	バックアップ後の処理操作が失敗したと見なされるまでに待機する最大時間（分）。デフォルトは 900 秒です。
Post Action Type of MSSQL	実行するバックアップ後の処理の操作タイプ。唯一の使用可能なオプションは［LOG Truncation］です。これは、バックアップの実行後にログのトランケートを実行します。単一の仮想マシンをバックアップする場合は、仮想マシンのすべてのディスクを選択する必要があります。選択しない場合は、ログのトランケートは発生しません。

VMware Image プラグ インのリストア オプション

これらのリストア オプションは、Avamar VMware Image プラグ インで利用可能です。

表 16 Avamar VMware Image プラグ インのリストア オプション

設定	説明
Use Changed Block Tracking (CBT) to increase performance	これを選択すると、最後のバックアップ以降に変更された仮想マシン ファイル システムのエリアを特定し、このリストア作業中に変更されたエリアのみを処理するために、VMware 更新ブロック追跡機能が使用されます。 注 更新ブロック追跡は、この機能が動作するように、仮想マシン レベルで有効化されている必要があります。
Encryption method from Data Domain system	リストア中に Data Domain システムとクライアントの間のデータ転送に使用する暗号化手法を選択します。Avamar リリース 7.5 時点では、サポートされる暗号化方式は「高」のみです。

Windows VMware GLR プラグ イン オプション

バックアップ オペレーションは、Avamar Windows VMware GLR プラグ インではサポートされていません。また、ユーザーが構成可能なリストア オプションも使用できません。

付録 E

トラブルシューティング

本付録は、次のトピックで構成されます。

インストールと構成の問題および解決策

ここでは、インストールと構成の共通の問題および解決策を説明します。

vCenter Server を Avamar クライアントとして追加するときの問題

vCenter Server を Avamar クライアントとして追加するときに問題が発生した場合は、次を確認します。

- vCenter のホスト名、ユーザー名、パスワードが正しいこと。
- ポート 443 が、Avamar サーバーと vCenter の間で開いていること。

それでも問題が解決しない場合は、すべての vCenter と間の Avamar MCS 通信に対して証明書認証をオフにしてください。

プロキシ ネットワークの設定

プロキシが誤った IP アドレスまたは DNS エントリーで導入されると、Avamar サーバーに、正しいホスト名ではなくローカルホストとして登録される可能性があります。

プロキシは vCenter によって管理される仮想アプライアンスであるため、一旦プロキシが Avamar サーバに登録されると、ネットワーク設定の変更が難しくなります。難しくない場合は、このステップでプロキシの Avamar サーバからの削除、vCenter のネットワーク設定の変更、Avamar サーバでの再アクティブ化を行います。

たいていの場合、最も有効な解決策は、設定の正しい新しいプロキシを導入し、古いプロキシを Avamar と vCenter の両方から削除することです。

仮想アプライアンス ネットワーク設定の変更手順については、vCenter のドキュメントに記載されています。

ゲスト バックアップまたは Windows リカバリ ターゲット クライアントの登録時にエラー

仮想マシンが vCenter ドメインにあるために Avamar サーバに追加されており、ゲスト バックアップを使って同じ仮想マシンを保護したい場合、または、同じ仮想マシンを、Windows VMDK をマウントするためのリカバリ ターゲットとして使用したい場合は、`mcserver.xmlallow_duplicate_client_names` プリファレンス設定を［true］に変更する必要があります。

バックアップの問題と解決策

一般的なバックアップの問題と解決策は次のとおりです。

バックアップが開始されない

バックアップ アクティビティを開始できない場合は、以下を確認します。

- Avamar イメージ バックアップ プロキシが正しく導入されていること。
- ソース仮想マシンのデータストアが、稼働中のプロキシ サーバー上で選択されていること。

それでも問題が解決しない場合は、vCenter への接続に使用されているアカウントの権限が十分でない可能性があります。

アカウントの権限を確認するには、そのユーザー名とパスワードを使用して、vSphere Client または vSphere Web Client にログインします。そのクライアント上のデータストアにアクセスできるかどうかを確認します。できない場合は、そのアカウントには必要な権限がありません。

バックアップが失敗して、「No Proxy」または「No VM」というエラーが表示される

バックアップが失敗して、「No Proxy」または「No VM」というエラーが表示される場合は、仮想マシンまたはプロキシをホストしている vCenter と Avamar Administrator を手動で同期化することを試みてください。

更新ブロック追跡が有効にならない

Avamar Administrator で更新ブロック追跡を有効にしても、再起動、電源オン、中断後の再開、移行のいずれかのアクションが仮想マシンで発生するまで、有効になりません。

更新ブロック追跡を有効にしても予想されるパフォーマンスの向上が実現されない場合は、vSphere Client または vSphere Web Client を使用して、更新ブロック追跡を有効化したすべての仮想マシンを見つけ、再起動、電源オン、中断後の再開、移行のアクションのいずれかを実行します。

プロキシがバックアップ ジョブに割り当てられていない

MCS を再起動する場合は常に、すべてのプロキシが MCS に再接続され、バックアップで利用できるようになるまでにしばらく時間がかかります。MCS を停止して、5 分以内に再起動しない場合は、プロキシが少なくとも 40 分間、スリープ モードになります。

プロキシが MCS に接続できることを確認するには、プロキシの avagent.log ファイルで、次のようなメッセージがログ ヒストリの末尾に表示されていることを確認します。

```
2014-03-20 20:34:33 avagent Info <5964>:
Requesting work from 10.7.245.161
2014-03-20 20:34:33 avagent Info <5264>:
Workorder received: sleep
2014-03-20 20:34:33 avagent Info <5996>:
Sleeping 15 seconds
```

使用可能なスペースの事前評価が誤っていると VM スナップショットのバックアップに失敗する

snapshot_max_change_percent フラグは、プロキシにデータストアの空きスペースを事前に評価させ、VM スナップショット用の十分なストレージを確保します。デフォルト値を 5%に設定します。ストレージの不足によりプロキシがバックアップに失敗すると、そのポリシーのユーザーがパーセントを「0」に変更するか、プロキシ コマンド ファイルの値を永続的にオーバーライドすることで値を上書きします。

このプロキシのチェックインを永続的にオーバーライドするには、各プロキシにログインし、次の行を含むように「/usr/local/avamarclient/avvcbimageAll.cmd」ファイルを修正します。

```
-- snapshot_max_change_percent=0
```

これによって、この機能が無効になります。

vFlash 読み取りキャッシュが有効化された仮想マシンのバックアップとリストアで、NBD 転送モードが使用される

vCenter に次のエラーが表示されます。

```
The
device or operation specified at index '0' is not supported for the
current virtual machine version 'vmx-07'. A minimum version of
'vmx-10' is required for this operation to succeed
```

ホット アドを希望する場合は、vmx-10 以降のプロキシ ハードウェアのバージョンにアップグレードしてください。

プロキシが vFlash リソースが構成されていないホスト上にある場合、ホット アドが試行されバックアップが NBD モードにフォールバックして成功する間に `The available virtual flash resource '0' MB ('0' bytes) is not sufficient for the requested operation` というエラーが VC に表示されることがあります。これは予期された動作ですが、ホット アドがどうしても必要な場合は、vFlash リソースが構成されているホストにプロキシを移動してください。

VMDK が vSphere を介して暗号化される場合は Exchange ログのトランケートがサポートされない

VMDK が vSphere を介して暗号化される場合は、VMware Tools はアプリケーション コンシステント停止に VSS を使用しません。その代わりに、暗号化されたイメージ バックアップは、ファイル レベルで整合性がとれています。Exchange サーバのログのトランケート プロセスに VSS Writer が含まれているため、VSS Writer はスナップショットの停止には関連せず、ログのトランケートがトリガーされません。

注

SQL サーバのログのトランケートに、VSS Writer は不要です。SQL ログのトランケートがサポートされます。

リストアの問題および解決策

これらは、リストアの共通の問題および解決策です。

既存のスナップショットが原因でリストアが失敗する

仮想マシンのリストアは、その仮想マシンのスナップショットがすでに存在している場合は失敗します。この場合、リストア作業により次のようなエラー メッセージが返されます。

```
2012-12-07 09:30:26 avvcbimage FATAL <0000>: The pre-existing
snapshots from VMX '[VNXe3300-Datastore1] vm-example/vm-
example.vmx' will not permit a restore.

2012-12-07 09:30:26 avvcbimage FATAL <0000>: If necessary, use
the '--skip_snapshot_check' flag to override this pre-existing
snapshot check.

2012-12-07 09:30:26 avvcbimage Error <9759>: createSnapshot:
snapshot creation failed
```

この状態を解決するには、影響を受ける仮想マシンの新しいリストアを実行し、［**Restore Options**］ダイアログ ボックスで `skip_snapshot_check` プラグ イン オプションを含める必要があります。これにより、リストア作業で既存のスナップショットが上書きされ、リストアを正常に完了することができます。

`skip_snapshot_check` プラグ イン オプションを使用してリストアを実行するには、次のようにします。

1. 影響を受ける仮想マシンへのイメージ リストアを開始します。
2. ［**Restore Options**］ダイアログ ボックスでリストア オプションを設定するように指示する点に達したら、次のステップを実行します。
   a. ［**More Options**］をクリックします。
   ［**Restore Command Line Options**］ダイアログ ボックスが表示されます。
   b. ［**More**］をクリックします。
   c. ［**Enter Attribute**］フィールドに **`[avvcbimage]skip_snapshot_check`** を入力します。
   d. ［**Enter Attribute Value**］フィールドに **`true`** を入力します。
   e. ［**+**］をクリックします。
   [avvcbimage]skip_snapshot_check=true エントリーがプラグ イン オプション リストに表示されます。
   f. ［**OK**］をクリックします。
3. 残りのリストア手順を続けます。

物理 RDM ディスクがかかわるとき、新しい仮想マシンへのリストアができない

仮想ディスクと物理 RDM（Raw Device Mapping）ディスクの両方を持つ仮想マシンをバックアップする場合、バックアップは仮想ディスクを正常に処理し、RDM ディスクをバイパスします。

ただし、これらのバックアップの 1 つからデータをリストアするとき、データを下の仮想マシンにリストア、あるいは別の既存の仮想マシンにリダイレクトすることができます。しかし、データを新しい仮想マシンにリストアすることはできません。

物理 RDM ディスクはバックアップ中に処理されないため、物理 RDM ディスクに存在するデータはリストアできないことに注意してください。

データを新しい仮想マシンにリストアする必要がある場合は、次の手順を実行する必要があります。

1. 新しい仮想マシンを vCenter に手動で作成します。
2. この新しい仮想マシンは、バックアップが実行された元の仮想マシンと同じ数の仮想ディスクを持つ必要があります。
3. 新しい仮想マシンを Avamar に手動で追加します。
4. この仮想マシンにデータをリストアします。

パーティション テーブルを使用しない、細分性の高いディスク バックアップの FLR 参照はサポートされていない

非 LVM の細分性の高いディスク バックアップが、パーティション テーブルがないディスクで実行されると、バックアップの FLR 参照はエラーで失敗します。

```
Failed to mount disks. Verify that all the disks on the VM have
valid/supported partitions.
```

この問題の回避策は、VM 上ですべてのディスクのフル イメージ バックアップを実行した後、パーティション テーブルがないディスクからファイルまたはフォルダーをリストアすることです。

新しい仮想マシンへのリストアの実行時にフォールト トレランスが無効になる

新しい仮想マシンに、フォールト トレラントの仮想マシンがリストアされると、フォールト トレランスが無効になります。マシンが新しい仮想マシンにリストアされた後、フォールト トレランスを有効にする必要があります。VMware のドキュメントには、フォールト トレランスを有効化する方法に関する情報が含まれています。

Virtual SAN 5.5 となる新しい仮想マシンへのリストアが失敗する

Virtual SAN 5.5 となる新しい仮想マシンにリストアすると、データストア タイプの組み合わせ（VSAN と VMFS または NFS）を使用する複数のディスク仮想マシンへのリストアであり、最初のディスクのリストアが非 VSAN データストアに対するものである場合、`unable to access file` メッセージで失敗します。この問題を回避するには、仮想マシンの最初のディスクに VSAN データストアを選択します。この問題は、VSAN 6.0 では発生しません。

フラッシュ容量が構成されていないホストへの即時アクセス vFlash-VM バックアップの電源投入が失敗する

フラッシュ容量が構成されていないホストへの即時アクセス vFlash-VM バックアップの電源投入が、次のエラーで失敗します。

```
The available virtual flash resource '0' MB ('0' bytes) is not
sufficient for the requested operation
```

この問題を回避するには、電源をオンにする前に、仮想マシンのフラッシュ キャッシュを無効化します。

インスタント アクセスでの NFS マウントの最大数の問題

インスタント アクセス機能を使用しているときに、次のエラー メッセージが表示された場合は、vSphere で設定されている NFS マウントの最大数が不十分なことがあります。

```
vmir Error <0000>: Mount NFS datastore failed to start with error:
Failed to create Data Domain
```

次のような関連するメッセージが vSphere に表示される場合があります。

```
vmir Error <0000>: NFS has reached the maximum number of supported
volumes.
```

この問題の解決策は、vSphere で設定されている NFS マウント ポイントの数を増やすことです。マウント ポイントの数を増やすための情報と手順については、VMware ナレッジベースの記事（https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2239）を参照してください。

RHEL5 でのファイル レベル リストアには標準 C++ライブラリが必要

RHEL 5.x 上で FLR パフォーマンスを向上するために HTTPS を使用している場合、標準 C++ライブラリがインストールされていないと ACL がリストア後に不正確になります。

特定の特殊文字を含むフォルダー名またはファイル名のファイル レベル リストアが失敗する

フォルダー名またはファイル名でのバックスラッシュ（\）または二重引用符（"）の使用は FLR ではサポートされません。

管理者承認モードを有効にすると、ユーザー プロファイルへのファイル レベルのリストアが失敗する

Microsoft Windows AAM（管理者承認モード）が有効（FilterAdministratorToken=1）な場合、管理者ユーザーは FLR を使用してエンド ユーザーのプロファイルにファイルまたはフォルダーをリストアできません。

リストアを行おうとすると、次のエラーが表示されます。

```
Unable to browse Destination
The directory cannot be browsed. Please check the directory of the VM
```

この問題を解決するには、管理者ユーザーは、C:\Users\内からエンド ユーザーのフォルダーを開く必要があります。Windows UAC の次のメッセージが表示されます。

```
You don't currently have permission to access this folder.
```

永続的に、管理者ユーザーがフォルダーにアクセスできるようにするには、[**Continue**] をクリックします。

用語集

記号

バックアップ ポリシー AUI では、バックアップ ポリシーはクライアントまたはクライアントのグループに適用されるデータセット、スケジュール、保存期間の設定を指定します。バックアップ ポリシーには、少なくとも 1 個の Avamar クライアントを含める必要があります。バックアップ ポリシーに 2 個以上のクライアントが含まれる場合は、これらのクライアントは同一の Avamar ドメインに属している必要があります。クライアント レベルでバックアップ　ポリシーの設定をオーバーライドできます。

A

Avamar Administrator サポートされている Windows または Linux クライアント コンピューターからリモートで Avamar システムを管理するために使用するグラフィカル管理コンソール ソフトウェア アプリケーション。

Avamar サーバー Avamar クライアント/サーバー システムのサーバー コンポーネント。Avamar サーバーは、すべての保護対象のクライアントから効率的にバックアップを保存する、高可用性を備えたフォールト トレラント システムです。このサーバーには、データのリストア、クライアント アクセス、リモート システム管理に不可欠なプロセスとサービスも備えられています。Avamar サーバーは、複数のネットワーク ストレージ ノードに対する分散アプリケーションとして実行されます。

C

CBT（更新ブロック追跡） バックアップの合間に変更された仮想マシンのファイル システム ブロックを追跡する VMware の機能。

D

Data Domain システム エンタープライズ環境にデータ保護と災害復旧（DR）を提供するディスク ベースの重複排除アプライアンスおよびゲートウェイ。

E

ESX/ESXi Server 物理サーバー上で稼働する仮想化レイヤーであり、プロセッサ、メモリ、ストレージ、リソースを複数の仮想マシンに抽出します。ESX Server では、統合されたサーバー コンソールが提供されますが、ESXi Server では提供されません。

M

MCS 管理コンソール サーバー。Avamar サーバーの一元管理（スケジュール設定、モニタリング、管理）を提供するサーバー サブシステム。MCS は、［Avamar Administrator］で使用されるサーバー側のプロセスも実行します。

S

Storage vMotion ライブ仮想マシンをデータストア間で移行することを可能にする VMware 機能。

V

vCenter Server 1 個以上の VMware データセンター用の一元化された管理および制御ポイント。

vSphere Client vCenter の制御と管理に使用する VMware ソフトウェア アプリケーション。vSphere Client は「シック クライアント」とも呼ばれます。

vSphere Web Client vCenter の制御と管理に使用する VMware Web インターフェイス。

あ

アクティベーション CID（クライアント ID）をクライアントに送信するプロセス。クライアントは受け取った CID を、クライアント ファイル システム上の暗号化ファイルに保存します。

以下も参照してください。 クライアントのアクティベーション

アプリケーション コンシステント 仮想ファイル システムへの書き込みが完了し、実行しているアプリケーションのすべてが停止された仮想マシンの状態。

い

イメージ バックアップ vCenter でホストされる仮想マシンを保護する方法の 1 つであり、仮想ディスク イメージ全体のバックアップが取得されます。VMware 用 Avamar イメージ バックアップは、VMware vCenter Server と完全に統合され、仮想マシン クライアントを検出するため、バックアップ ジョブの効率的な一元管理が可能となります。

く

クライアント登録 Avamar サーバーでの同一性を確立するプロセス。Avamar は、クライアントを認識すると、一意の CID（クライアント ID）をクライアントに割り当てます。クライアント ID は［クライアントのアクティベーション］の際にクライアントに送信されます。

以下も参照してください。 登録

クライアントのアクティベーション クライアント ID（CID）をクライアントに送信するプロセス。クライアントは受け取った CID を、クライアント ファイル システム上の暗号化ファイルに保存します。

以下も参照してください。 アクティベーション

クラッシュ コンシステント 物理コンピューターへの電源供給を中断することで発生する状態と等しい仮想マシンの状態。電源の中断時にファイル システムへの書き込みが進行中の場合も、そうでない場合もあるため、クラッシュ コンシステントなファイル システムのバックアップでは常に一部のデータ消失が生じる可能性があります。

グループ 1 つ以上の Avamar クライアントで構成される Avamar Administrator 内の組織のレベル。Avamar グループのすべてのクライアントでは、同一のグループ ポリシーを使用し、これには [データセット]、[スケジュール]、[保存ポリシー] が含まれます。

グループ ポリシー Avamar Administration では、グループ ポリシーは、Avamar グループのすべてのクライアントの [Dataset]、[Schedule]、および [Retention Policy] として定義されます。

け

ゲスト バックアップ 仮想マシンの保護方法の 1 つであり、バックアップ ソフトウェアが物理マシンのようにゲスト オペレーティング システムに直接インストールされます。

す

スケジュール グループ内のクライアントのバックアップの実行頻度と、実行日の開始時刻および終了時刻を制御する機能。スケジュールは、名前を付けて複数のグループに関連付けることができる永続的で再利用可能な Avamar ポリシーです。

て

データストア VMware vSphere 環境で、データストアとはデータセンターによって使用されるストレージ リソースです。

データセット クライアント グループ全体のバックアップに含まれる、または排除される、サポートされた各プラットフォームの一連のファイル、ディレクトリ、およびファイル システムを定義するポリシー。データセットは、名前をつけて複数のグループに関連づけることができる固定の再利用可能な Avamar ポリシー。

データセンター VMware vSphere 環境で、データセンターは基本的な物理ビルディング ブロックを構成します。これらの物理ビルディング ブロックには、仮想化サーバー、ストレージ ネットワークおよびアレイ、IP ネットワーク、単一のマネージメント サーバーが含まれます。各 vSphere vCenter が複数のデータセンターを管理できます。

と

登録 Avamar サーバーでの同一性を確立するプロセス。Avamar は、クライアントを認識すると、一意の CID（クライアント ID）をクライアントに割り当てます。クライアント ID は［クライアントのアクティベーション］の際にクライアントに送信されます。

以下も参照してください。 クライアント登録

は

バックアップ 個々のファイル、選択されたデータ、またはバックアップ全体としてリストアできるクライアント データのポイント イン タイム コピー。

ふ

ファイル システム コンシステント 仮想ファイル システムが停止した仮想マシンの状態（つまり、すべてのファイル システムへの書き込みが完了している状態）。

プラグ イン クライアント上に常駐する特定の種類のデータを認識する Avamar クライアント ソフトウェア。

プラグ イン オプション バックアップまたはリストア機能を制御するためにバックアップ時やリストア時に指定するオプション。

プロキシ 他の仮想マシンのイメージ バックアップ、イメージ リストア、およびファイル レベル リストアの実行に使用する仮想マシン。プロキシは Avamar ソフトウェアを Linux 仮想マシン内部で実行し、アプライアンス・テンプレート（.ova）ファイルを使用して vCenter 内で展開されます。

ほ

保存設定 Avamar サーバー上のバックアップを自動的に削除する時間設定。Avamar サーバーから削除しないバックアップには、永続的な保存設定を指定できます。保存設定は、名前を付けて複数のグループに関連付けることができる永続的かつ再利用可能な Avamar ポリシーです。

り

リストア 1 つ以上のファイル システム、ディレクトリ、ファイル、データ オブジェクトをバックアップから取得し、そのデータを指定された場所に書き込む処理。