# Cisco HyperFlex Data Platform リリース 2.5 バックアップ統合ガイド

初版：2017 年 12 月 1 日


シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

© 2017 Cisco Systems, Inc. All rights reserved.

# Full Cisco Trademarks with Software License

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

# 目 次

**Full Cisco Trademarks with Software License** iii

第 1 章

**HyperFlex バックアップ統合の概要** 1

スナップショットを使用するバックアップ ソリューション 1

バックアップ製品に関する考慮事項 3

スナップショット用語 4

Sentinel スナップショット 5

バックアップ ソリューションを適用する準備 6

第 2 章

**Veeam と HX Data Platform バックアップ ソリューションの統合** 9

Cisco HyperFlex 2.5 と Veeam v9.5 Update 2 の統合 9

Veeam の要件 10

ESXi ファイアウォールの選択肢の適用 13

ESX ファイアウォールの設定 14

HyperFlex ストレージ クラスタ IP アドレスを使用したデータストアへの直接接続 14

VIB の ESXi ファイアウォールへの適用 15

ESXi ホスト上のファイアウォールを一時的に開く 16

Veeam とデータストアの直接接続 18

Veeam ストレージ インフラストラクチャへの Cisco HyperFlex の追加 18

HyperFlex クラスタの Veeam への追加に関するトラブルシューティング 20

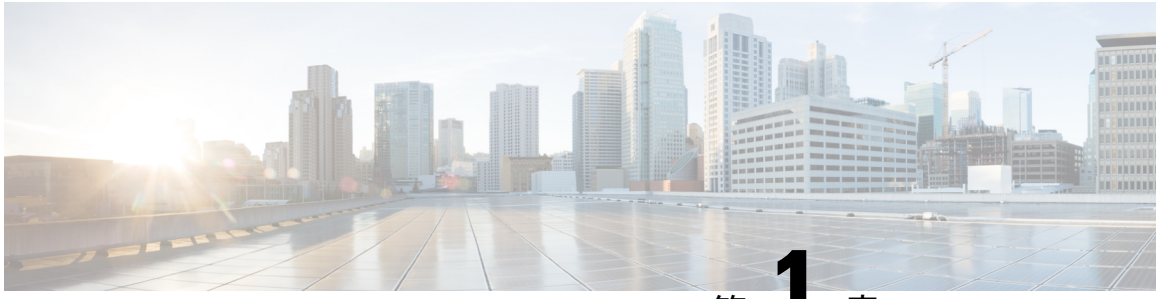
HX スナップショット バックアップおよびレプリケーション用 Veeam ジョブの設定 21

Cisco HyperFlex ネイティブ スナップショットの確認 22

プロキシ ネットワークの設定：仮想マシン 22

プロキシ サーバ ネットワークの設定：物理サーバ 23
ジャンボ フレームによる ping の確認 24

第 3 章 バックアップ ソリューションでの HX API の使用 25
HX API 統合によるバックアップ製品の使用 25
REST API のログインと呼び出し 25
スナップショット REST API の概要 26
REST Explorer 26
スナップショット HX API のサンプル 26
スナップショットの参照 26
VM スナップショットの作成 27
VM スナップショットの削除 27
HX Data Platform ネットワークへの VM のマッピング 28
バックアップ HX API 応答コード 29



第 1 章

# HyperFlex バックアップ統合の概要


- スナップショットを使用するバックアップ ソリューション （1 ページ）
- バックアップ製品に関する考慮事項 （3 ページ）
- バックアップ ソリューションを適用する準備 （6 ページ）


## スナップショットを使用するバックアップソリューション

このドキュメントでは、HX Data Platform ネイティブ スナップショットをバックアップ ソリューションの一部として使用する方法について説明します。使用している HX インターフェイスによって方法が異なります。

- HX アプリケーション プログラミング インターフェイス（API）
  - HX API と統合されたサード パーティ製バックアップ製品向け。
  - 通常、統合タスクはアプリケーション統合プログラマによって実行されます。
- HX Data Platform のユーザ インターフェイス：HX Data Platform Plug-in、HX コマンド ライン インターフェイス（CLI）など。
  - HX と統合されていないサード パーティ製バックアップ製品向け。
  - 通常、手動による介入タスクは IT 管理者によって実行されます。
- サード パーティの設定要件と手順。
  - 特定のサード パーティ製バックアップ ソリューション用に、主要な設定情報が提供されています。
  - このドキュメントに含まれる情報は、サード パーティ製バックアップ ソリューションの元のドキュメントを補足するもので、これに代わるものではありません。

### バックアップ製品について

バックアップ製品は通常、バックアップの実行にVMスナップショットを使用します。バックアップにVMスナップショットを使用するバックアップ ソリューションは、2つの時点でのVMの違いを追跡できる必要があります。バックアップ ソリューションは、バックアップが完全なコピーかVM内の変更されたバイトのみのコピーかがはっきりしている必要があります。

### スナップショットについて

スナップショットは、アクティブVMのバージョン（状態）を保存するバックアップ機能です。スナップショットはVMの「ポイントインタイム」キャプチャを提供します。これには、スナップショット作成時にすべてのVMディスク上にあるデータの状態、およびVMの電源の状態（オン、オフ、またはサスペンド）が含まれます。スナップショットには仮想ディスクと仮想マシン構成、および場合によってはメモリが含まれます。

スナップショットが作成されるので、必要に応じてVMを以前の状態に戻す（復元する）ことができます。スナップショットは、クラッシュ、ゲストOS、およびアプリケーション レベルの整合性を保ちます。バックアップ ジョブ（ゲストの休止）用に設定されたスナップショットでは、アプリケーション レベルの整合性が保たれます。OSやハイパーバイザではなくアプリケーションVSSライターを呼び出せる、高性能なバックアップ アプリケーションを使用することを強くお勧めします。

VMが電源オン、オフ、またはサスペンド状態のときに、スナップショットを取得できます。VMwareスナップショットの追加情報については、次のリンクからVMwareのナレッジベース『Understanding virtual machine snapshots in VMware ESXi and ESX (1015180)』の記載を参照してください。
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180

HX Data Platformは、一般的なスナップショット機能を扱うためのHX APIを提供します。VMwareでは、仮想ディスクおよびメモリ単位だけでなく、さまざまな休止状況でvSphere APIを使用したVMスナップショットの管理が可能です。

一般的なスナップショット機能には、スナップショットの作成、任意のスナップショットへの復元、スナップショットの削除が含まれます。これらのタスクを実行するために、HX Data Platformネイティブ スナップショットはSentinel機能を使用します。Sentinelスナップショットの説明については、Sentinel スナップショット （5 ページ）を参照してください。VMwareスナップショットは、redoログ技術を使用します。

スナップショットは次のような場面で使用できます。

- 必要に応じて復元可能なローカルのポイントインタイムキャプチャとして使用できます。通常は、ゲストOSやアプリケーションで障害が発生した場合に使用されます。
- バックアップのシーディング用に一貫性のあるポイント イン タイムを確立するために使用できます。
- 仮想マシン クローンおよび仮想デスクトップ ソリューションのシーディングに使用できます。

### 統合されたバックアップ製品

| バックアップ製品 | 統合レベル |
|---|---|
| Veeam | HX バージョン 2.5 以降と統合されています。Veeam と HX Data Platform バックアップ ソリューションの統合 （9 ページ）で説明されている構成時の設定に従ってください。 |
| Veeam | HX バージョン 2.0 以降と統合されています。HX API を使用します。 |
| Veeam | バージョン 1.8.1 以前の HX とは統合されていません。HX UI による手動の方法を使用してください。 |
| 他のバックアップ製品 | 統合されていません。HX UI による手動の方法を使用してください。 |

# バックアップ製品に関する考慮事項

HyperFlex のスナップショットは、ネイティブ スナップショット テクノロジーに基づく仮想マシン スナップショットです。HyperFlex は VMware VAAI プログラムと統合されて、ネイティブ スナップショットおよびクローンテクノロジーを提供します。HyperFlex は、ネイティブのリダイレクト オン ライト技術を使用してネイティブ スナップショットとクローニングを実行します。HX ネイティブ スナップショットと HX readyclone の詳細については、『Cisco HyperFlex Data Platform Administration Guide』を参照してください。

HX API は、VM レベルのスナップショットを作成および削除するためのインターフェイスを提供します。HX API により、サード パーティのバックアップ製品は自身のバックアップ ソリューションと HyperFlex ネイティブ スナップショットを統合できます。

次のリストは、サードパーティのバックアップ製品を使用する際の考慮事項です。これらの考慮事項は、バックアップ製品が統合されているかどうかにかかわらず適用されます。

- **使用時のヒント**：最初の HX ネイティブ スナップショットを手動で作成します。その後、HX API を使ったジョブの実行にバックアップ製品を使用します。
- **VMware スナップショット**：パフォーマンスと拡張性の理由から、VMware スナップショットよりも HX スナップショットを使用することが推奨されています。HX スナップショットは、延々と続くスナップショットやスナップショットの削除に起因する I/O ペナルティ、仮想ディスクの統合にかかる時間や I/O ペナルティなど、redo ログベースのスナップショットによる影響を回避します。
- **変更ブロック追跡**：HX データストアの FlatVer2 および SeSparse 形式の仮想ディスクでは、変更ブロック追跡を使用した HX スナップショットがサポートされます。VM スパンデータストアを含むような特定のレイアウトはサポートされていません。
- **リソース プールおよびフォルダ**：HX API では VM に焦点が当てられています。バックアップ オブジェクトとしてリソース プールまたはフォルダを指定することはできません。

リソース プールまたはフォルダ内のすべての VM を選択して、バックアップ タスクに追加することは可能です。

- **同時操作**：HX ネイティブ スナップショットは、VM で管理操作が同時に行われていない場合にのみ許可されます。

  特定の VM の HX 機能（Scheduled Snapshot、Snapshot Now、Ready Clone など）によって、HX スナップショットの作成要求と削除要求が発行される場合があります。仮想マシンには、VM の状態を監視および制御して、許可する操作（電源オン、電源オフ、vMotion、スナップショットなど）を決定するプロセスがあります。

  バックアップ製品は、管理要求が同時実行された場合に、これらのビジー期間に対応してスナップショット操作を再試行できる必要があります。

- **停止スナップショット**：既存の HX スナップショットで VM の停止スナップショットを作成すると、VM が無期限に機能停止する可能性があります。

  VM の停止に VMware ゲスト ツールを使用しないバックアップ ソリューションを使用してください。たとえば、Veeam Enterprise v 9.2 は別の方法を使用して VM を停止します。

- **redo ログ スナップショット**：VMware の redo ログ スナップショットを削除すると、VM が無期限に機能停止する可能性があります。

  VM の I/O ワークロードが大きいと、VM の機能停止期間が長くなります。この制限は VMware スナップショット テクノロジーによるものです。

- **共有モードの GPU**：共有モードで GPU が装着されている VM は、VMware VM または HX スナップショットでサポートされていません。これらのタイプの VM は、スナップショットベースのバックアップ ソリューションを使用してバックアップできません。

# スナップショット用語

スナップショットという用語は、さまざまな用途で使用されます。以下に概要を示します。

- **バックアップスナップショット**：バックアップ製品を使用して取得されるスナップショットの総称。これは、VMware API によるスナップショットまたは HX API によるスナップショットのいずれかです。

- **クローン**：同じ仮想マシンの複数のコピーを展開する際に使用されます。クローンはバックアップ ソリューションではありません。

- **ネイティブ スナップショット**：HX Data Platform インターフェイス（HX API または UI HX）を介して取得されるスナップショット。ネイティブ スナップショットは VM の複製で、ネイティブ スナップショットが作成された時点での、すべての VM ディスク上のデータの状態と VM の電源の状態（オン、オフ、またはサスペンド）が含まれます。

- **スナップショット**：スナップショットの総称。スナップショットは、動作している VM のバージョン（状態）を保存するバックアップ機能として使用できます。VM をスナップショットに復元して、スナップショットが作成されたときにキャプチャされた VM の状態に戻すことができます。

- **Sentinel スナップショット**：VM の最初のスナップショットを作成したとき、または既存のスナップショットがある VM に vmdk を追加したときに、HX によって作成されます。Sentinel は、復元された VM が VMware redo ログ ベースの仮想ディスクを保持しないようにします。
- **VMware スナップショット**：HX ネイティブ スナップショットが存在しない場合に、VMware インターフェイスを介して取得されるスナップショットのタイプ。VMware タイプの redo ログ スナップショットまたはデルタ ディスク スナップ ショットは、既存の HX ネイティブ スナップショットが存在せず、スナップショットの作成に VMware インターフェイス（API または UI）が使用された場合にのみ作成されます。VMware スナップショットには redo ログ ベースの仮想ディスクが含まれます。

その他の関連用語。

- **SeSparse**：仮想ディスク形式の一種。これらの形式の仮想ディスクを含む VM は、HX ネイティブ スナップショットではサポートされていません。
- **VlatVer2**：ディスク バックアップをサポートする仮想ディスク形式の一種。HX ネイティブ スナップショットによってサポートされています。

# Sentinel スナップショット

HX Data Platform ネイティブ スナップショットは、動作している VM のバージョン（状態）を保存するバックアップ機能です。VM をネイティブ スナップショットに戻すことができます。ネイティブ スナップショットの作成と復元は、HX Data Platform Plug-in、またはバックアップ製品を使用する HX API を通じて実行できます。

HyperFlex を使用して VM の最初のスナップショットを作成する場合、HyperFlex は Sentinel スナップショットと呼ばれるベース スナップショットを作成します。Sentinel スナップショットの後続のスナップショットはすべて、redo ログ ベースのスナップショットではなくネイティブ スナップショットになります。スナップショット呼び出しのシーケンスに応じて仮想ディスクが最初のスナップショットの後に追加されると、VM に複数の Sentinel スナップショットが存在する場合があります。

**Sentinel スナップショットの使用**

- Sentinel スナップショットは削除しないでください。
- VM を Sentinel スナップショットに復元しないでください。

バックアップ製品によって作成されたスナップショットは、ユーザが要求したスナップショットです。バックアップ製品で HyperFlex API を使用すると、バックアップ スナップショットに加えて Sentinel スナップショットが作成されます。バックアップ製品で HyperFlex API が使用されず、HyperFlex ネイティブ スナップショットが存在しない場合は、VMware API を使用して redo ログ ベースのスナップショットが作成されます。

**トラップされたストレージ**

VMデータ コンテンツの変更率が高い場合、スナップショットの作成と削除の長いシーケンス後に、Sentinel スナップショットは、VM の最初のスナップショットに基づいてスペースのブロックをトラップすることがあります。次に例を示します。

1. 40 GB の vmdk を備えた VM はデータでいっぱいになっています（contentA）。
2. バックアップ製品は、HyperFlex API を使用してスナップショットを要求します。

   これにより、Sentinel と Snap1 という 2 つのスナップショットが作成されます。
3. バックアップ製品は、HyperFlex API を使用して後続のスナップショットを要求します。

   これにより、追加のスナップショット（Snap2、Snap3、Snap4 と続く）が作成されます。
4. 一定期間が経過し、VM のデータ コンテンツ全体が置き換えられます（contentB）。

   Sentinel は、元のスナップショット「Snap1」のコンテンツを保持します。Sentinel は、Snap1 が削除されても contentA のためにスペースを消費し続けます。

   これは、「トラップされたストレージ」と呼ばれます
5. Sentinel を更新して、トラップされたストレージを解放することが推奨されます。
   - 方法 1：
     1. すべての HyperFlex スナップショットを削除します。
     2. 新しい HyperFlex ネイティブ スナップショットを作成します。
   - 方法 2：

     HyperFlex REST API を使用してスナップショットを削除し、`updateSentinel` フラグを指定します。

# バックアップ ソリューションを適用する準備

バックアップ ソリューションを実装する前に、ご利用のソリューションに対応する手順を確認して実行してください。

### 手順

- **統合された Veeam Enterprise v 9.2**

  バックアップを設定して最適なパフォーマンスを実現するには、事前にすべての VMware スナップショットを削除します。

  Veeam バックアップ ソリューション：

  - HX スナップショットを暗黙的に使用します。選択した redo ログ VM の問題を防止できます。

- 独自の休止メカニズムがあります。既存の HX スナップショットがある場合に、VM の機能停止問題を防止できます。
- HX API を使用して Sentinel スナップショットを作成し、自動更新します。パフォーマンスとトラップされたスペースの両方の問題を防止できます。

- **統合されていないバックアップ ベンダー**（例：Commvault、Avamar）

  バックアップを設定する前にすべての HX スナップショットを削除します。

  redo ログスナップショットが存在する場合、バックアップのスナップショット削除フェーズ中に、ハイ I/O の VM が無期限に機能停止する可能性があります。

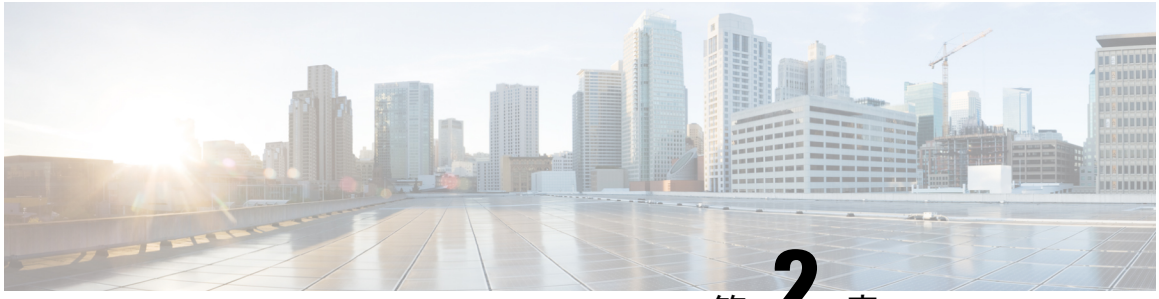
- **遅延の影響を受けやすい非休止 VM**

  Veeam Enterprise v 9.2 以外のバックアップ ソリューションを使用する場合は、遅延の影響を受けやすい VM が存在するため、VMware の [Guest Tools Quiesce] オプションを使用する必要はありません。

  - VM の HX スナップショットを使用します。
  - VMware の [Guest Tools Quiesce] オプションが選択されていないことを確認します。
  - 定期的に手動ですべての HX スナップショットを削除し、トラップされたブロックを再利用します。管理者ロールが必要です。詳細については、Sentinel スナップショット （5 ページ）を参照してください。
  - バックアップが設定されている VM の新しい HX スナップショットを作成します。

### 次のタスク

バックアップ ソリューションの実装方法が説明されている項に進みます。



第 2 章

# Veeam と HX Data Platform バックアップ ソリューションの統合


- Cisco HyperFlex 2.5 と Veeam v9.5 Update 2 の統合 （9 ページ）
- Veeam の要件 （10 ページ）
- ESXi ファイアウォールの選択肢の適用 （13 ページ）
- Veeam ストレージ インフラストラクチャへの Cisco HyperFlex の追加 （18 ページ）
- HX スナップショット バックアップおよびレプリケーション用 Veeam ジョブの設定 （21 ページ）
- Cisco HyperFlex ネイティブ スナップショットの確認 （22 ページ）
- プロキシ ネットワークの設定：仮想マシン （22 ページ）
- プロキシ サーバ ネットワークの設定：物理サーバ （23 ページ）
- ジャンボ フレームによる ping の確認 （24 ページ）


## Cisco HyperFlex 2.5 と Veeam v9.5 Update 2 の統合

Veeam Backup & Replication は、Cisco HX Data Platform ネイティブ スナップショット API を介して Cisco HyperFlex Systems と統合されます。これらの API により、HyperFlex クラスタでホストされている VMware vSphere 仮想マシンのバックアップとレプリケーションのパフォーマンスが向上します。

HyperFlex スナップショットは、VMware vSphere Storage APIs Array Integration（VAAI）を利用します。VAAI によって、VMware ESXi ホストはストレージデバイスと通信して、ストレージ操作（スナップショットの作成やクローニングなど）をストレージコントローラにオフロードできるようになります。

Veeam Backup & Replication は、HyperFlex ネイティブ スナップショットを使用して VM データを処理できます。これにより、バックアップおよびレプリケーション操作が高速化し、バックアップおよびレプリケーションアクティビティによる実稼働環境への影響が軽減され、目標復旧時点（RPO）が改善されます。

HyperFlex ネイティブ スナップショットと Veeam のエージェントレス VM 取り込みプロセスを使用して、アプリケーションに対応したバックアップおよびレプリケーションの整合性を維持

することで、Veeam は VMware VM の redo ログ スナップショットを使用する必要がなくなります。

### VMware redo ログ スナップショットと HyperFlex ネイティブ スナップショット

最初に Veeam 統合を使用できない場合は、VMware redo ログ スナップショットと HyperFlex ネイティブ スナップショットを利用できます。

- デフォルトで、vSphere Webclient、PowerCLI、およびサード パーティ製バックアップ アプリケーションは、VMware API を使用して VMware redo ログ ベースのスナップショットを作成します。
- ただし、サード パーティ製バックアップ アプリケーションは、HyperFlex API を使用して HyperFlex ネイティブ スナップショットを作成することもできます。

  HyperFlex ネイティブ スナップショットは、VMware redo ログ スナップショットよりも優れたパフォーマンスを実現します。ネイティブ スナップショットは、redo ログ スナップショットが存在しない場合にのみ作成できます。最初に作成されたスナップショットがネイティブ スナップショットである場合は、以降のスナップショットもすべてネイティブ スナップショットになります。HyperFlex は、すべてのスナップショット呼び出しをインターセプトして、redo ログ スナップショットの呼び出しであってもネイティブ スナップショットを作成します。

HyperFlex API 統合を使用しなくても、次の方法でネイティブ スナップショットを作成できます。

- Cisco HX Data Platform Plug-in

  vSphere Webclient：**[VM]** > **[Cisco HX Data Platform]** > **[Snapshot Now]** を右クリックします。
- HyperFlex ストレージ コントローラのコマンドラインで次のコマンドを使用します。

  ```
  stcli vm snapshot
  ```

# Veeam の要件

HX Data Platform ネイティブ スナップショットで Veeam Backup & Replication を使用するために統合を行うには、次の要件を満たしている必要があります。

（注） Veeam の使用方法を理解している必要があります。

Veeam の手順については、Veeam のマニュアルを参照してください。このガイドでは、HyperFlex 統合に Veeam を適用して Veeam バックアップ サービスを使用するための手順のみを説明します。

- **Versions**

- Veeam Backup & Replication Enterprise Plus Edition 9.5 Update 2（ビルド 9.5.0.1038）以降。
- Cisco HyperFlex 2.0 以降。

- **Veeam の設定**
  - Veeam バックアップ サーバに Veeam ライセンスをインストールします。
  - Cisco HyperFlex を Veeam ストレージ インフラストラクチャに追加します。表示される可能性のあるエラー メッセージとトラブルシューティングについては、Veeam ストレージ インフラストラクチャへの Cisco HyperFlex の追加 （18 ページ）を参照してください。
  - HX クラスタに関連付けられている VMware vCenter Server を Veeam バックアップ インフラストラクチャに追加します。
  - Veeam の **[job settings]** > **[Storage]** > **[Integration]** で [Enable backup from storage snapshots] を選択します。
  - HX ネイティブ スナップショットからデータを読み取るように、Veeam 転送モードを設定します。[Veeam Transport Mode] フィールドを [Direct storage access] に設定します。

    ダイレクト ストレージ アクセスでは、NFS プロトコルを使用して HyperFlex データストアに直接接続します。最適なパフォーマンスが実現されて、ESXi ホストのオーバーヘッドが最も低くなります。このモードの場合、Veeam Backup & Replication は ESXi ホストをバイパスし、HX クラスタ データ ネットワークを介して HyperFlex データストアとデータの読み取り/書き込みを直接行います。

    自動選択を利用せずに、明確に [Direct storage access] を設定すると、たとえば、ファイアウォールが設定されていなくても、必ずダイレクト ストレージ アクセスが使用されます。その他の仮想アプライアンスやネットワークが代替的に使用される可能性があるので、[Automatic] オプション（**デフォルト**）**は使用しないでください**。

- **Veeam バックアップ プロキシ**

  2 種類の Veeam プロキシがあります。バックアップ プロキシは、Veeam と HyperFlex 間の通信リンクを提供します。サーバ プロキシは、Veeam と vSphere、vCenter、および ESX サーバ間の通信リンクを提供します。

  - Veeam を HyperFlex データストアに直接接続してより高速なバックアップを可能にする方法は次のとおりです。

    Veeam バックアップ プロキシを HyperFlex クラスタ データ ネットワーク（ストレージ コントローラ データ ネットワーク）上に配置します。

    Veeam バックアップ プロキシを [Direct Storage Access] に設定します。

  - Veeam バックアップ プロキシが HyperFlex クラスタ データ ネットワークとネットワーク接続されていることを確認します。たとえば、Veeam バックアップ プロキシが

HyperFlex（ストレージ コントローラ データ ネットワーク）の VLAN と通信できることを確認します。

- ESX ファイアウォールを使用する場合は、必ず Veeam アクセスを許可するように設定する必要があります。VIB の ESXi ファイアウォールへの適用 （15 ページ）を参照してください。

- **VM データストア**
  - すべての VM が HX ストレージ クラスタ ホストのデータストアに含まれていることを確認します。

    （注） データストア名にコロン（:）を使用しないでください。

  - VM のすべてのディスクが同じデータストアに含まれていることを確認します。

    複数のデータストアに分散されたディスクをスナップショットに含めることはできません。追加のデータストア上のディスクを選択し、ステータスを [Independent] に変更します。

    Veeam バックアップから個々の VM ディスクを無効にするには、VMware vCenter にログインして **[VM]** > **[VM configuration]** > **[Edit Settings]** を選択し、個々のハードディスクを展開して **[Disk Mode]** > **[Independent]** を選択します。

- **VM スナップショット**

  必須の設定は次のとおりです。

  - Veeam の [job settings] で [Enable backup from storage snapshots] を選択します。これがデフォルト設定ですが、選択されていることを必ず確認してください。

    Veeam で [job] を右クリックし、**[Properties]** > **[Storage]** > **[Advanced]** > **[Integration]** > **[Enable backup from storage snapshots]** を選択します。

  - HyperFlex ネイティブ スナップショットのみを使用します。

  可能な場合は、VMware スナップショットを削除します。

  - VMware スナップショットがある VM は、バックアップまたはレプリケーション時にスキップされます。
  - すべての VMware スナップショットを手動で削除すると、次の Veeam バックアップ時のジョブによって HyperFlex ネイティブ スナップショットが作成され、バックアップが実行されます。
  - この同じ Veeam の [job settings] 統合タブで、**[standard backup option]** > **[Failover]** を設定すると、統合が失敗した場合に VMware API が呼び出されます。

# ESXi ファイアウォールの選択肢の適用

実稼働環境では通常、複数のバックアップ ジョブが実行され、それぞれに独自のタイミングや VM の選択が指定されています。HyperFlex クラスタの ESXi ホストにも分散されるバックアップ サービスをこれらの VM に提供し、HyperFlex リソースやネットワーク スループット機能を十分に活用するには、Veeam プロキシが ESXi ファイアウォール経由で HyperFlex ストレージ クラスタのすべての ESXi ホストにアクセスする必要があります。

HyperFlex を Veeam ストレージ インフラストラクチャに追加するための前提条件は、ESXi ホストへの Veeam のアクセスを許可する方法を選択して設定を適用することです。

次に示す選択肢を使用すると、Veeam は HyperFlex クラスタ データストアに接続できます。HyperFlex クラスタ データストアは、HyperFlex クラスタ ストレージ全体へのアクセスにストレージ統合を使用し、HyperFlex クラスタ管理ネットワーク（ストレージ コントローラ管理ネットワーク）と ESXi ホストをバイパスします。

- ESXi ファイアウォール経由：Veeam は確実にすべての ESXi ホスト、データストア、および VM に直接アクセスできます。この選択肢を使用する場合は、Veeam 統合**ジョブ** オプションとして [Backup from storage snapshots] を指定する必要があります。この選択を実行する方法を選択します。
  - 新しい Veeam VIB を作成するか、Veeam コミュニティの既存の VIB を使用して、各 ESXi ホストに追加する。
  - または、非永続的オプション用に ESXi `services.xml` ファイルを編集する。
- Veeam 転送モード「ダイレクト ストレージ アクセス」の使用：1 台の Veeam プロキシをグローバル HyperFlex ストレージ クラスタの IP アドレスに接続します。データストア経由で VM にアクセします。スループットが、単一の ESXi ホスト上の HyperFlex ストレージ コントローラ VM に対する割り当てに制限されます。この選択肢を使用する場合は、Veeam 統合**ジョブ** オプションとして [Backup from storage snapshots] を指定する必要があります。
- Veeam 転送モード「ネットワーク アクセスへのフェールオーバー」の使用：Veeam は HyperFlex ストレージ クラスタ管理ネットワークを介してすべてのトラフィックを送信します。Veeam 転送モードの「Automatic selection」で ESXi ホストに直接接続できない場合に、デフォルトの代替方法として使用されます。最も低速でリソースに大きく依存する方法です。

ESXi ファイアウォール経由でアクセスしない場合、Veeam は、HyperFlex クラスタ データ ネットワーク（ストレージ コントローラ データ ネットワーク）上の単一のストレージ コントローラ VM の IP アドレスを介して VM にバックアップ サービスを提供します。これはスケーラブルではなく、データストアに接続する上記の方法とは異なります。この方法では、HyperFlex クラスタのすべての ESXi ホストにアクセスすることはできません。HyperFlex クラスタ リソースの使用は、クラスタ内の単一ノードに制限されます。この方法を使用すると、Veeam の同時実行タスクの数も制限されます。HyperFlex ストレージ クラスタ IP アドレスを使用したデータストアへの直接接続 （14 ページ）を参照してください。

# ESX ファイアウォールの設定

HyperFlex クラスタ内のすべての ESXi ホストに IO Visor が備わっています。これは、プレインストールされた VMware ESXi vSphere Installation Bundle（VIB）で、個別の仮想マシンに接続された仮想ディスク ドライブに ESXi ハイパーバイザがアクセスできるように、ネットワーク ファイル システム（NFS）マウント ポイントを提供します。ESXi ハイパーバイザからは、単にネットワーク ファイル システムに接続されているように見えます。

Veeam が IO Visor を使用して、ESXi ホストのファイアウォールを開くようにすることを推奨します。その後、Veeam バックアップ プロキシは、HyperFlex クラスタのすべての ESXi ホストのリソースに接続し、これを使用して VM をバックアップできます。そのためには、以下を許可するルールを ESX ファイアウォールに追加する必要があります。

- HyperFlex クラスタの各 ESXi ホストの IO Visor に対する Veeam プロキシ アクセス。
- ESXi 着信ポートを介して通信する IO Visor スタティック ポート。
  - HyperFlexバージョン 2.5 以降：ポート 111、2049、2449。
  - HyperFlexバージョン 2.0：ポート 0 ～ 65535。
- Veeam プロキシで設定されている、HyperFlex クラスタ データ ネットワーク（ストレージ コントローラ データ ネットワーク）の IP アドレスを介したアクセス。

Veeam が HyperFlex クラスタ ESXi ホストと存在する VM にアクセスできるように、ESXi ホストのファイアウォールを開く方法は次のとおりです。

- **VIB を使用して ESX ファイアウォールを設定する**

  VMware Installation Bundle（VIB）を適用する方法は 2 つあります。VIB を作成するか、既存の Veeam コミュニティ VIB を使用します。VIB がある場合は、HyperFlex クラスタの各 ESXi ホストにインストールします。VIB の ESXi ファイアウォールへの適用 （15 ページ）を参照してください。

- **ESXi services.xml ファイルを編集してファイアウォールを一時的に設定する**

  手動で HyperFlex クラスタのすべての ESXi ホストに非永続（ホストの再起動後に残らない）ファイアウォール ルールを作成します。この方法はテスト環境でのみ使用することをお勧めします。必要な特定のポートは、HyperFlex バージョンによって異なります。ESXi ホスト上のファイアウォールを一時的に開く （16 ページ）を参照してください。

# HyperFlex ストレージ クラスタ IP アドレスを使用したデータストアへの直接接続

（注） これは、推奨される方法では**ありません**。

Veeam がバックアップ ジョブを実行して、ESXi ファイアウォール アクセスが許可されない場合のデフォルト アクションは次のとおりです。

1. **[Transport Mode]** > **[Automatic selection]** を使用すると、Veeam は ESX で実行されている IO Visor に接続できません。
2. 次に、Veeam は **[Transport Mode Option]** > **[Failover to network mode if primary mode fails, or is unavailable]** を適用します。
3. ネットワーク モードになると、Veeam はバックアップ対象の VM を取得するために HX スタック全体を調べます。これは、リソース、スループット、および時間を消費します。

   [Failover to network mode if primary mode fails, or is unavailable] がオフになっていると、ジョブは失敗します。

また、Veeam がバックアップ ジョブを実行して、ESXi ファイアウォール アクセスが許可されない場合は、HyperFlex ストレージ クラスタ データストアに直接アクセスするように Veeam を設定します。

Veeam の **[Transport Mode]** > **[Direct storage access]** を設定します。

ESXi ファイアウォールを通過する方法ほど効率的ではありませんが、ネットワーク モードよりも高速です。この方法では、Veeam をデータストアに接続し、HyperFlex クラスタ管理リソースを保存します。制限を次に示します。

- Veeam は単一のコントローラを介してのみバックアップ サービスを提供することができます。このコントローラは、HyperFlex クラスタ データ ネットワーク（ストレージ コントローラ データ ネットワーク）の IP アドレスを所有しているコントローラ VM です。
- Veeam は、単一のストレージ コントローラのコンピューティング リソースによる制約を受けます。
- HyperFlex クラスタ管理ネットワーク（ストレージ コントローラ管理ネットワーク）の単一のストレージ コントローラのスループットは、10 GbE に制限されます。
- Veeam は、同時実行タスクの数を Veeam プロキシ サーバのコア数に制限します。各バックアップ ジョブには、複数のタスクが含まれる場合があります。

クラスタ データ ネットワーク（ストレージ コントローラ データ ネットワーク）の HyperFlex ストレージ コントローラの IP アドレスに直接接続するように Veeam を設定するには、Veeam とデータストアの直接接続 （18 ページ）を参照してください。

# VIB の ESXi ファイアウォールへの適用

VMware Installation Bundle（VIB）は ESXi サーバに設定を適用します。次のいずれかの方法を使用して、Veeam プロキシによる ESXi ファイアウォールの通過を可能にする VIB を適用します。これらのオプションのいずれかによって、バックアップ プロセス用の IO Visor 通信が有効になります。

手順

- **VMware ESXi ホスト VIB の作成**：ファイアウォール ルールを作成し、すべてのホストにインストールして有効化し、許可されている Veeam プロキシ IP アドレスを設定するホスト拡張ファイル。

  これは永続的な方法で、手動による介入なしでホストの再起動を処理します。

  VEEAM KB2291（https://www.veeam.com/kb2291）で詳細を参照してください。

- **定義済みの VMware ESXi ホスト拡張 VIB の使用**：Veeam コミュニティ GitHUB プロジェクトのファイル。

  これは永続的な方法で、手動による介入なしでホストの再起動を処理します。

  VEEAM KB2298（https://www.veeam.com/kb2298）で詳細を参照してください。

# ESXi ホスト上のファイアウォールを一時的に開く

テスト環境の HyperFlex クラスタにあるすべての ESXi ホストに、手動で非永続（ホストの再起動後に残らない）ファイアウォール ルールを作成します。必要なポートは、Cisco HyperFlex 2.0/2.1 または 2.5 以降のどちらを使用しているかによって異なります。

次の例は、ESXi ホストの SSH 接続でファイアウォールを開くために必要なすべての手順を示しています。

（注） 次の手順は、HyperFlex クラスタの各コンバージド ノードで実行する必要があります。

**ステップ 1** HyperFlex ストレージ クラスタの ESXi ホストにログインします。

**ステップ 2** 現在の `services.xml` ファイルをバックアップします。コマンドを実行します。

```
# cp /etc/vmware/firewall/service.xml /etc/vmware/firewall/service.xml.bak
```

**ステップ 3** `service.xml` ファイルのアクセス権限を変更して書き込みを許可します。コマンドを実行します。

```
# chmod 644 /etc/vmware/firewall/service.xml
# chmod +t /etc/vmware/firewall/service.xml
```

**ステップ 4** テキスト エディタで `service.xml` ファイルを開きます。次に例を示します。

```
# vi /etc/vmware/firewall/service.xml
```

**ステップ 5** `service.xml` ファイルにルールを追加します。

a) **HyperFlex 2.0/2.1**：`services.xml` ファイルに次のファイアウォール ルールを追加します。

```
<!--Cisco Firewall configuration information -->
   <service id='9230'>
     <id>VeeamCiscoFirewall</id>
     <rule id='0000'>
       <direction>inbound</direction>
```

```
        <protocol>tcp</protocol>
        <porttype>dst</porttype>
        <port>
          <begin>0</begin>
          <end>65535</end>
        </port>
      </rule>
    </service>
```

b) **HyperFlex 2.5 以降**：`services.xml` ファイルに次のファイアウォール ルールを追加します。

```
<!--Cisco Firewall configuration information -->
<service id='9230'>
    <id>VeeamCiscoFirewall</id>
    <rule id='0000'>
      <direction>inbound</direction>
      <protocol>tcp</protocol>
      <porttype>dst</porttype>
      <port>111</port>
    </rule>
    <rule id='0001'>
      <direction>inbound</direction>
      <protocol>tcp</protocol>
      <porttype>dst</porttype>
      <port>2049</port>
    </rule>
    <rule id='0002'>
      <direction>inbound</direction>
      <protocol>tcp</protocol>
      <porttype>dst</porttype>
      <port>2449</port>
    </rule>
<enabled>false</enabled>
<required>false</required>
</service>
```

**ステップ 6** `services.xml` ファイルのアクセス権限をデフォルトの読み取り専用に戻します。コマンドを実行します。

```
# chmod 444 /etc/vmware/firewall/service.xml
```

**ステップ 7** ファイアウォール ルールを更新して変更内容を反映します。コマンドを実行します。

```
# esxcli network firewall refresh
```

**ステップ 8** 新しいファイアウォール ルールを有効にします。コマンドを実行します。

```
# esxcli network firewall ruleset set -r "VeeamCiscoFirewall" -e true -a false
```

**ステップ 9** ファイアウォール ルールをすべての Veeam プロキシ サーバ データ ネットワーク IP にバインドします。プロキシ サーバごとにコマンドを実行します。

```
# esxcli network firewall ruleset allowedip add -r "VeeamCiscoFirewall" -i "<yourVeeamProxyIP>"
```

**ステップ 10** IP バインディングを確認します。コマンドを実行します。

```
# esxcli network firewall ruleset allowedip list | grep -v "All"
```

**ステップ 11** ファイアウォール ルールが有効になっているかどうかを確認します。コマンドを実行します。

```
# esxcli network firewall ruleset list
```

# Veeam とデータストアの直接接続

Veeam が ESX ファイアウォールを通過できない場合は、ストレージ データ ネットワーク（ストレージ コントローラ データ ネットワーク）の HyperFlex クラスタ IP アドレスを使用してデータストアに直接接続するように設定する必要があります。

HyperFlex データストアは HyperFlex クラスタのすべての ESXi ホストに適用され、すべての VM もクラスタのすべての ESXi ホストに分散されるため、この方法は有効です。これにより、HyperFlex クラスタのすべての VM に直接アクセスできるようになります。

[Direct storage access] オプションを使用すると、HyperFlex はすべての ESXi ホストの IO Visor にアクセスでき、それに関連するメリットも提供します。この方法では、単一のコントローラ VM へのアクセスに制限され、リソースもその単一の ESXi ホストのリソースに制限されます。一方で、Veeam を ESXi ファイアウォール経由で IO Visor に直接接続すると、すべての ESXi ホストとそのリソースにアクセスできるようになります。

**ステップ 1** Veeam で **[Backup Infrastructure]** > **[Backup Proxies]** を選択します。

**ステップ 2** [Add Proxy] をクリックするか、既存のプロキシを選択して [Edit Proxy] をクリックします。

複数のプロキシによって、より多くのジョブの同時実行が許可される可能性があります。

各プロキシは物理マシンまたは VM のいずれかで稼働し、有限のリソースを保持しています。リソースを分散するには、複数のプロキシを作成します。

**ステップ 3** [Transport Mode] ダイアログボックスを表示します。

**[Server]** > **[Transport mode]** > **[Choose]** を選択します。

**ステップ 4** [Direct storage access] を選択します。[OK]、[Finish] の順にクリックします。

これにより、デフォルトの [Automatic selection] が変更されます。

**ステップ 5** HyperFlex ストレージ クラスタの VM のバックアップに使用するすべての Veeam バックアップ プロキシでこの手順を繰り返します。

# Veeam ストレージ インフラストラクチャへの Cisco HyperFlex の追加

HyperFlex クラスタの Veeam ストレージ インフラストラクチャへの追加は、Veeam によるバックアップ サービスの提供を有効にするために必要な設定手順の 1 つです。

（注） このタスクは、Veeam バックアップ サービスを使用する必要がある HyperFlex クラスタごとに実行します。

HyperFlex クラスタを Veeam ストレージ インフラストラクチャに追加します。

**始める前に**

Veeam の要件 （10 ページ）に記載されている要件を確認して、これを満たします。

ESX ファイアウォール オプションを特定して適用します。ESXi ファイアウォールの選択肢の適用 （13 ページ）を参照してください。

---

**ステップ 1** Veeam にログインして [Storage Infrastructure] > [Add Storage] > [Cisco Hyperflex] を選択します。

**ステップ 2** HyperFlex クラスタ管理ネットワーク（ストレージ コントローラ管理ネットワーク）の IP アドレスを指定します。

HyperFlex クラスタ管理ネットワークはルーティング不可能なネットワークです。HyperFlex クラスタの作成時に入力した IP アドレスが必要です。この IP アドレスによって、HyperFlex クラスタへのアクセスが可能になります。このアドレスには `eth0:mgmtip` のラベルが付いています。

IP アドレスをメモしていない場合は、次の手順でアドレスを確認します。

1. HyperFlex クラスタの ESXi ホスト上にあるストレージ コントローラ VM のコマンド ラインにログインします。
2. `ipconfig` を実行し、戻り値で `eth0:mgmtip : xx.xx.xx.xx` を確認します。

   グローバルに HyperFlex ストレージ クラスタを表すストレージ コントローラ VM にのみ、`eth0:mgmtip` が表示されます。
3. `ipconfig` の戻り値に `eth0:mgmtip` が含まれていない場合は、`ipconfig` が `eth0:mgmtip` IP アドレスを返すまで手順 a と b を繰り返します。

**ステップ 3** HyperFlex クラスタのルート ユーザ クレデンシャルを指定します。

**ステップ 4** Veeam バックアップ プロキシ サーバのアクセス方法を指定します。デフォルトは [Automatic selection] です。

**ステップ 5** HyperFlex が Veeam ストレージ インフラストラクチャに正常に追加されていることを確認します。

以下の場合は設定が正しく行われています。

- Veeam プロキシが HyperFlex クラスタ データ ネットワーク上にある。
- ESX ファイアウォール ルールが追加されている。
- HyperFlexクラスタのルート ユーザ クレデンシャルが使用されている。

**[System]** > **[Storage discovery]** > **[Log]** に次のメッセージが表示されます。

- `Cisco HyperFlex xx.xx.xx.xx configuration refresh completed`
- `Whitelisted backup proxy IP addresses on system xx.xx.xx.xx`
- `Found NFS ESXi IP addresses suitable for backup from HyperFlex snapshots ...`
- `Cisco HyperFlex xx.xx.xx.xx rescan completed`

**ステップ 6** Veeam への HyperFlex の追加によってエラーが生成された場合は、HyperFlex クラスタの Veeam への追加に関するトラブルシューティング （20 ページ）を参照してください。

# HyperFlex クラスタの Veeam への追加に関するトラブルシューティング

次のリストに、Veeam の [Add Storage] ウィザードに表示される可能性のあるエラーを示します。

HyperFlex を Veeam ストレージ インフラストラクチャに追加すると、**[System]** > **[Storage discovery]** > **[Log]** に次のメッセージが表示されることがあります。

### ユーザ認証エラー

エラー メッセージ全体：`Cannot find NFS IP addresses suitable for backup from HyperFlex snapshot from system xx:xx:xx:xx Error: User authentication failed.`

これは、HyperFlex のルート ユーザ クレデンシャルを使用しない場合に発生することがあります。

このエラーが発生した場合は、次の処置を実行します。

1. Veeam ストレージ インフラストラクチャから HyperFlex クラスタを削除します。
2. HyperFlex クラスタを Veeam ストレージ インフラストラクチャに再度追加して、HyperFlex クラスタの作成時に使用したルート ユーザ クレデンシャルを使用します。

### VMware バックアップ プロキシ エラー

エラー メッセージ全体：`Cannot find any NFS ESXi IP addresses suitable for backup from HyperFlex snapshots from system xx.xx.xx.xx using backup proxy VMware Backup Proxy.`

これは、Veeam プロキシが HyperFlexクラスタ データ ネットワーク上の ESXi ホストおよび IP アドレスに接続できない場合に発生することがあります。

このエラーが発生した場合は、次の処置を実行します。

1. Veeam ストレージ インフラストラクチャから HyperFlex クラスタを削除します。
2. HyperFlex クラスタ データ ネットワーク（ストレージ コントローラ データ ネットワーク）に NIC を追加します。
   - NIC に IP アドレスを設定します。
   - ping を実行して、HyperFlex クラスタ データ ネットワーク上の ESXi ホストおよびストレージ コントローラ VM への NIC ネットワーク接続を確認します。
3. HyperFlex クラスタを Veeam ストレージ インフラストラクチャに再度追加します。

### ESX ファイアウォール エラー

エラー メッセージ全体：`Cannot find any NFS ESXi IP addresses suitable for backup from HyperFlex snapshots from system xx.xx.xx.xx using backup proxy VMware Backup Proxy.`

これは、Veeam プロキシが HyperFlex クラスタ データ ネットワーク上にあるにもかかわらず、ESX ファイアウォールが設定されていない場合に発生することがあります。

このエラーが発生した場合は、次の処置を実行します。

1. Veeam ストレージ インフラストラクチャから HyperFlex クラスタを削除します。
2. ESX ファイアウォール オプションを選択します。次の 3 種類があります。
   - 各 ESXi ホストに Veeam VIB をインストールして ESX ファイアウォールを設定します。
   - ESXi ファイアウォール ルールを手動で編集します。
   - HyperFlex データ ネットワーク データストアに直接接続するように、Veeam のバックアップ プロキシを編集します。
3. HyperFlex クラスタを Veeam ストレージ インフラストラクチャに再度追加します。

# HXスナップショットバックアップおよびレプリケーション用 Veeam ジョブの設定

Veeam を使用して HyperFlex ストレージ クラスタ VM をバックアップするには、Veeam ジョブを作成します。

### 始める前に

Veeam の要件 （10 ページ）に記載されている要件を確認して、これを満たします。

HyperFlex を Veeam ストレージ インフラストラクチャに追加します。Veeam ストレージ インフラストラクチャへの Cisco HyperFlex の追加 （18 ページ）を参照してください。

---

**ステップ 1** Veeam で **[Backup & Replication]** > **[New Backup Job]** を選択します。必要に応じて [Virtual Machines] を選択します。

**ステップ 2** [Storage] ステップで、データ転送に使用する [Backup proxy] を選択します。

選択したバックアップ プロキシが HyperFlex クラスタ データ ネットワーク（ストレージ コントローラ データ ネットワーク）と通信できることを確認します。

デフォルトの [Automatic selection] を使用する場合は、すべてのバックアップ プロキシが HyperFlex クラスタ内のサーバ上にあることを確認します。

**ステップ 3** [Storage] ステップで **[Advanced]** > **[Integration]** をクリックします。

a) [Enable backup from storage snapshots] チェックボックスをオンにします。

このオプションはデフォルトで選択されますが、間違いなくオンになっていることを確認してください。

b) 通常のデータ処理モードにフェールオーバーする必要がある場合は、[Failover to standard backup] をオンにします。

完全統合モードで Veeam ジョブが VM の処理に失敗すると、HyperFlex ストレージ クラスタでホストされている VM のバックアップまたはレプリケーションは実行されません。

Veeam の標準バックアップでは、VMware API を使用して VMware redo ログ スナップショットが作成されます。

# Cisco HyperFlex ネイティブ スナップショットの確認

これは、Veeam と HyperFlex の接続を確認およびトラブルシューティングするためのタスクです。

**始める前に**

Veeam バックアップ インフラストラクチャで、すべての Veeam プロキシ サーバがダイレクト ストレージ アクセスに設定されていることを確認します。

**ステップ 1** Veeam バックアップ ジョブの進捗状況パネルを開きます。

**ステップ 2** メッセージのアクション リストを表示します。

アクション メッセージが、`Creating VM Snapshot` ではなく `Creating VM native CiscoHX snapshot` であることを確認します。

# プロキシ ネットワークの設定：仮想マシン

これは、Veeam と HyperFlex の接続を確認およびトラブルシューティングするためのタスクです。

**発生する可能性のあるエラー**：HyperFlex クラスタ データ ネットワーク上の ESXi ホストまたはストレージ コントローラ VM に接続できない。

**バックグラウンド**：Veeam バックアップ プロキシが HyperFlex クラスタに存在する VM である場合、HyperFlex ストレージ データ ネットワーク（ストレージ コントローラ データ ネットワーク）にネットワーク カードを設定したり、VM にネットワーク カードを追加したりできます。HyperFlex クラスタ データ ネットワークはルーティングされず、DHCP がある可能性は低いので、使用可能な静的 IP アドレスをゲスト内で割り当てる必要があります。ネットワーク カードのプロパティを変更して、9000 MTU のジャンボ フレームを有効にしてください。

**ステップ 1** VM のネットワーク カードを変更するか、ネットワーク カードを追加します。

a) Veeam で **[Virtual Machines Properties]** > **[Add Hardware]** > **[Network Connection]** を選択します。

b) 指定のラベルが付いた名前付きのネットワークで、ストレージ コントローラ データ ネットワークを選択します。

**ステップ 2** ネットワーク カードが 9000 MTU のジャンボ フレーム用に設定されていることを確認します。図 8）Cisco HyperFlex の追加

a) Veeam で **[Virtual Machines Properties]** > **[Add Hardware]** > **[Network Connection]** > **[Advanced]** を選択します。

b) [Property] で [Jumbo Packet] を選択します。[Value] で [9014 Bytes] を選択します。

# プロキシ サーバ ネットワークの設定：物理サーバ

これは、Veeam と HyperFlex の接続を確認およびトラブルシューティングするためのタスクです。

Veeam バックアップ プロキシが物理サーバである場合：

- サーバは、HyperFlex クラスタが存在するファブリック インターコネクト（FI）に接続する必要があります。

  Veeam バックアップ プロキシ サーバが FI に直接接続されている、または FI に直接接続しているネクサス 9000 に接続されていることを確認します。

- Veeam バックアップ プロキシが FI に直接接続されている場合は、サーバ VLAN が HyperFlex クラスタ データ ネットワーク（ストレージ コントローラ データ ネットワーク）の VLAN と一致する必要があります。これは、UCS Manager を使用して設定します。

**ステップ 1** 準備ステップを実行します。物理サーバをスイッチに接続します。スイッチ トラックを FI に接続します。HyperFlex クラスタ ストレージデータ ネットワークの VLAN にアクセスするサーバ ポートを接続します。ネットワーク管理者に、物理サーバをストレージ コントローラ データ ネットワークの VLAN に接続してもらいます。ジャンボ フレーム ネットワークを使用してサーバおよび VLAN に ping を実行します。

**ステップ 2** Veeam プロキシ物理サーバが FI に直接接続されている場合：

HyperFlex クラスタ ストレージ データ ネットワークの VLAN と一致するように、UCS Manager を使用して物理サーバの VLAN を設定します。

次の vNIC テンプレートを使用して、物理 Veeam プロキシ サーバに HyperFlex サービス プロファイルを関連付けます。

- vNIC hv-mgmt-a
- vNIC hv-mgmt-b
- vNIC storage-data-a
- vNIC storage-data-b

VLAN を決定する 1 つの方法は、UCS Manager で vNIC のプロパティを確認することです。

**ステップ 3** ファブリック インターコネクトに直接接続しているネクサス 9000 に物理 Veeam プロキシ サーバが接続されている場合：

そのサーバはファブリック インターコネクトによって管理されていないので、サービス プロファイルを割り当てることはできません。

以下を実行する必要があります。

- 物理サーバからネクサス 9000 に接続されているポートにトランク モードを明確に割り当てる。
- ストレージ データ ネットワークとストレージ管理ネットワークの両方の VLAN を許可する。

# ジャンボ フレームによる ping の確認

これは、Veeam と HyperFlex の接続を確認およびトラブルシューティングするためのタスクです。

ジャンボフレームを使用して、HyperFlex クラスタ データ ネットワーク（ストレージ コントローラ データ ネットワーク）上の ESXi とストレージ コントローラ VM の IP アドレスの両方に ping を実行できることを確認します。デフォルトでは Windows VM にジャンボ フレームがないため、Veeam プロキシでジャンボ フレームを有効にする必要があります。

**ステップ 1** ESX から ping を実行します。

a) ESXi ホストの 1 つに SSH で接続します。

b) `# vmkping -I vmk1 -s 8000 <veeam_proxy_IP_on_storage_data_network>`

c) ping が成功することを確認します。

**ステップ 2** ストレージ コントローラ VM から ping を実行します。

a) ストレージ コントローラ VM の 1 つに SSH で接続します。

b) `# ping -s 8000 <veeam_proxy_IP_on_storage_data_network>`

c) ping が成功することを確認します。

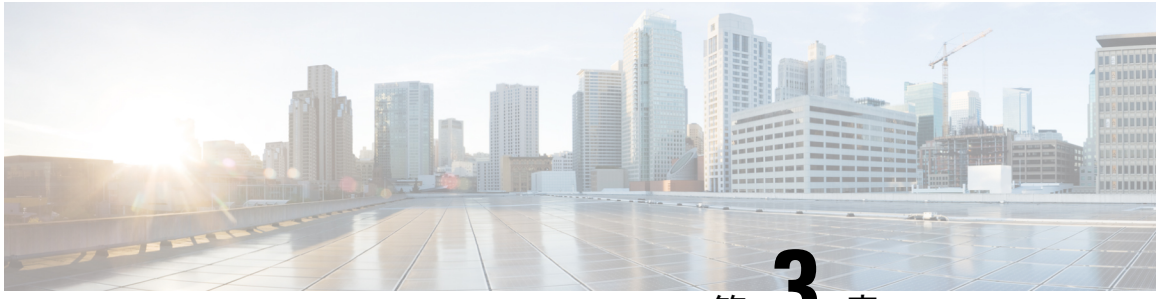
**ステップ 3** Veeam バックアップ プロキシ（Windows）から ping を実行します。

a) Veeam バックアップ プロキシにログインします。

b) `# ping -l 8000 <esx_host_IP_on_storage_data_network>`

c) `# ping -l 8000 <storage_controller_IP_on_storage_data_network>`

d) `# ping -l 8000 <hx_storage_cluster_IP_on_storage_data_network>`



第 3 章

# バックアップ ソリューションでの HX API の使用


- HX API 統合によるバックアップ製品の使用 （25 ページ）
- スナップショット HX API のサンプル （26 ページ）
- バックアップ HX API 応答コード （29 ページ）


## HX API 統合によるバックアップ製品の使用

### REST API のログインと呼び出し

サード パーティ製バックアップ ソリューション用にスナップショット HX API を呼び出すには、HX Data Platform クラスタ管理の IP アドレスを使用して、ログイン クレデンシャルを提供し、REST コールを実行します。

（注） 現在サポートされているサードパーティ製バックアップ ソリューションは、Veeam バックアップ アプリケーションのみです。

**ステップ 1** HX Data Platform クラスタ管理の IP アドレスを使用します。

**ステップ 2** サポートされているクレデンシャルから選択します。

- HX Data Platform に関連付けられている Virtual Center の Virtual Center SSO ユーザ。この SSO ユーザには、Virtual Center のルート フォルダの読み取り権限、書き込み権限、変更権限が必要です。
- http ヘッダーで Base64 エンコード形式にエンコードされている、コントローラ VM のユーザ名とパスワード。

**ステップ 3** REST コールを定義します。このガイドのサンプルでは、コントローラ VM のルート クレデンシャルで Curl コマンド ライン ツールを使用します。

# スナップショット REST API の概要

VM レベルのスナップショット操作と用語は VMware API 仕様と一致しています。特に記載のない限り、引数はオプションの VMware 定義を反映します。詳細については、http://pubs.vmware.com/vsphere-55/index.jsp#com.vmware.sdk.doc/GUID-E0BBED4C-8C5A-4C01-B21A-575F85E9A650.html の『*vSphere API and SDK Documentation*』参照してください。

## REST Explorer

コマンド ラインで Curl を使用する代替手段として、HyperFlex には REST Explorer があらかじめバンドルされています。

HyperFlex REST Explorer へのアクセス方法は、次のとおりです。

1. HX ストレージ クラスタ管理 ip にログインします。たとえば、次のような URL を入力します。

```
https://<hxdp_management_ip>/rest-explorer
```

# スナップショット HX API のサンプル

このガイドのサンプルでは Curl を使用します。HX API にアクセスするための REST Explorer も HyperFlex で提供されます。

状況や必要に応じてサンプルの内容を変更してください。

サンプルではスナップショットの `moid` を扱います。https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1017126 で VMware ナレッジ ベース『Looking up Managed Object Reference (MoRef) in vCenter Server (101726)』を参照してください。

## スナップショットの参照

スナップショット REST API を使用した HX スナップショットの参照はサポートされていません。HX スナップショットの参照および表示には、VMware スナップショット マネージャを使用できます。

# VM スナップショットの作成

### VM スナップショットの作成

要求 URL

```
https://<HyperFlexClusterManagementIP>/rest/api/v1/vaai/vm/<serverUuid>_<VM MoId>/snapshot
```

次の構造を使用して、VM のスナップショットを作成します。

```
{
  "snapshotName": "string",
           // Name of the snapshot.
  "description": "string",
          // Description of the snapshot.
  "memory": false,
          // If TRUE, a dump of the memory is included in the snapshot.
  "quiesce": false
         // Quiesce the VM guest using guest tools.
}
```

### 要求

```
curl -k -u "vc-administrator@vsphere.local:PASSWORD"
-X POST
--header "Content-Type: application/json"
--header "Accept: application/json"
-d
"{
\"snapshotName\": \"s1\",
\"description\": \"string\",
\"memory\": false,
\"quiesce\": false
}"
"https://ucs-stctlvm-184-1/rest/api/v1/vaai/vm/
<serverUuidValue>_vm-1109/snapshot"
```

### 応答

```
{"snapshotId":"snapshot-1172"}
    // snapshot-id is the moid of the snapshot that is created.
```

# VM スナップショットの削除

### VM スナップショットの削除

要求 URL

```
https://<HyperFlexClusterManagementIP>/rest/api/v1/vaai/vm/<serverUuid>_<VM
MoId>/snapshot/<Snapshot MoId>
```

次の構造を使用して、VM のスナップショットを作成します。

```
{
  "removeChildren": false,
          // Flag to specify removal of the entire snapshot subtree. Incompatible with
the updateSentinel option.
  "consolidate": false,
```

```
         // If set to true, the virtual disk associated with this snapshot is merged
with other disk if possible. Defaults to true.
  "updateSentinel": true
        // Sentinel snapshot(s) are updated, if feasible. If Sentinel update is done,
the moid of the snapshot
        // to be deleted is reused as the Sentinel snapshot. Incompatible with the
removeChildren option.
}
```

### 要求

`updateSentinel` が `true` に設定されていることを確認します。

```
curl -k -u "vc-administrator@vsphere.local:PASSWORD"
-X PUT
--header "Content-Type: application/json"
--header "Accept: application/json"
-d
"{
\"removeChildren\": false,
\"consolidate\": false,
\"updateSentinel\": true
}"
"https://ucs-stctlvm-184-1/rest/api/v1/vaai/vm/<serverUuidValue>_vm-1109
/snapshot/snapshot-1172"
```

### 応答

スナップショット「snapshot-1172」の名前が「Sentinel」に変更されます。古い Sentinel スナップショット「snapshot-1171」が削除されます。

```
{"snapshotIds":["snapshot-1171"]}
   // List of Sentinel snapshots that are deleted if updateSentinel was provided and
   // 1 or more Sentinel snapshots were deleted. The moid of the snapshot that is
   // successfully deleted otherwise.
```

# HX Data Platform ネットワークへの VM のマッピング

スナップショット HX API を使用して、VM が実行されている ESX ホスト上の HX データ ネットワーク ポート グループの IP を取得します。

### HX Data Platform ネットワークへの VM のマッピング

要求 URL

```
https://<HyperFlexClusterManagementIP>/rest/api/v1/vaai/vm/<serverUuid>_<VM
Moid>/datanetworkip
```

### 要求

```
curl -k -u "vc-administrator@vsphere.local:PASSWORD"
-X GET
--header "Accept: application/json"
"https://ucs-stctlvm-184-1/rest/api/v1/vaai/vm/
<serverUuidValue>_vm-1109/datanetworkip"
```

### 応答

```
{"dataNetworkIp":"<Ipv4 address>"}
```

# バックアップ HX API 応答コード

### HTTP 成功コード

| HTTP 成功コード | HTTP の説明 | コンテキストの説明 |
|---|---|---|
| 201 | Created | オブジェクトが正常に作成されました。つまり、VMのスナップショットが作成されました。 |
| 200 | OK | 要求された操作（オブジェクトの作成以外）が正常に完了しました。 |

### HTTP エラー コード

| HTTP エラー コード | HTTP の説明 | コンテキストの説明 |
|---|---|---|
| 404 | Not Found | 要求された操作の対象オブジェクトが使用できなくなっています（削除された VM 上のスナップショットの操作など）。 |
| 400 | Bad Request | ユーザが、サポートされていない操作を要求したか、無効な引数を入力しました。 |
| 409 | Conflict | 操作が競合しているため、現時点では実行できません（別のスナップショット要求が処理されている同じ VM のスナップショットを要求した場合など）。 |
| 503 | Service Unavailable | 要求に対応するサービスが停止しています（stMgr が停止しているなど）。 |
| 500 | Internal Server Error | 上記以外の理由で、サービスが要求された操作を実行できませんでした。 |