Veeam Kastenと歩む回復力への道

最初の100日間とそれ以降のロードマップ。

このガイドは、IT管理者向けに、Veeam Kasten *for Kubernetes* の導入、設定、および運用化を段階的に解説します。Helmまたはマーケットプレイスのいずれを通じて導入プロセスを行う場合でも、導入プロセスは迅速かつ安全で、アクセスしやすいように設計されています。100日目までに、Kubernetesネイティブのバックアップ環境、イミュータブルなオフサイトエクスポート、ツールセットやアプリケーションとの統合化、さらに文書化されたリカバリランブックが整備されます。

100日間の旅

フェーズ1 基礎 1日目～14日目	フェーズ2 基本の強化 15日目～45日目	フェーズ3 最適化と強化 46日目～75日目	フェーズ4 価値の検証 76日目～100日目
M1：サイジングと計画	M4：一元管理	M7：可観測性の統合	M10：復元テスト
M2：Veeam Kastenの導入	M5：アプリケーション認識処理	M8：回復力の強化	M11：文書化とレポート作成
M3：最初のバックアップジョブ	M6：ポリシーのベストプラクティス	M9：対象範囲のギャップ解消	M12：継続的な健全性維持

ロードマップ概要

フェーズ	名前	タイムライン	重点
フェーズ1	基礎	1日目～14日目	環境の計画、Veeam Kastenの導入、最初のバックアップジョブの実行
フェーズ2	基本の強化	15日目～45日目	一元管理、アプリ認識処理、ポリシーのベストプラクティス。
フェーズ3	最適化と強化	46日目～75日目	可観測性、回復力とDR、対象範囲のギャップ解消
フェーズ4	価値の検証	76日目～100日目	復元テスト、文書化、継続的な健全性維持。

本ガイドの使い方

日数はあくまで目安であり、厳密な締め切りではありません。小規模な環境ではフェーズ1が1週間に短縮される可能性があり、複雑な環境ではフェーズ3が延長される可能性があります。

各マイルストーンは前の段階を基にしているため、手順は順番通りに進めることを推奨します。

ガイド全体を通して、意思決定ポイント、アーキテクチャのオプション、注意すべき一般的な落とし穴が吹き出しボックスで示されています。

コンテンツ

フェーズ1 • 1日目〜14日目

基礎

目標：インフラストラクチャのサイジング、導入、最初のワークロードの保護。

マイルストーン1：サイジングと計画

実際に展開する前には、計画に時間を費やしてください。このステップを慎重に行うことで、適切に保護され、安定した環境の展開時に生じるほとんどの課題を回避できます。

ワークロードインベントリ

- ワークロードと仮想マシン（VM）の合計数、データフットプリント（ボリュームサイズ／ファイル数など）、推定日次変更率を記録します。
- 最も重要なワークロードを特定してください。これらのワークロードが、目標復旧時点（RPO）および目標復旧時間（RTO）の設定に影響を及ぼします。
- アプリケーション認識処理のメリットが見込めるデータベースとワークロードを記録します。

Veeam Kastenのサイジングと導入計画

- Veeam Kastenには最小限のシステム要件が備わっているため、通常はデフォルト値で十分です。
- 導入方法として「マーケットプレイス/オペレーター」（推奨）または「Helm」を選択します。必要に応じて、インストール後に方法を変更できます。
- ご利用中のKubernetesのバージョンが、最新バージョンのVeeam Kastenと互換性があることを確認してください。そうでない場合は、最初にアップグレードするか、古いバージョンを使用する必要があります。
- この環境が物理的に隔離された環境かどうか確認してください。隔離された環境であれば、オフラインで利用可能なローカルレジストリにVeeam Kastenのイメージをベンダーのマーケットプレイス経由でプッシュするか、当社のレジストリをホワイトリストに追加する必要がある場合があります。
- バックアップトラフィックを専用のVLANに分離してバックアップネットワークを計画することは、セキュリティのベストプラクティスであり、KubernetesではCNIによって可能です。

Helmとマーケットプレイスの比較

Helm：これは最も柔軟性が高く、すべてのKubernetesディストリビューションと互換性があります。

マーケットプレイス/オペレーター：導入とアップグレードのライフサイクルはよりシンプルで、Helmと同じカスタマイズパラメータをサポートしています。また、Red Hat OpenShiftでもよく使用されます。

トレードオフ：マーケットプレイスから新リリースを受け取るまでに遅延が発生する可能性があります。Helmでは更新を即座に利用可能ですが、マーケットプレイスのベンダーは検証テストのために新しいリリースを1日以上遅らせることがあります。

ワークロードストレージアーキテクチャ

- **スナップショット対応ストレージ：**Veeam Kastenは、スナップショットをサポートするほぼすべてのCSIストレージドライバやダイレクトストレージインテグレーションと互換性があります。
- **その他のストレージ（例：汎用NFS、ローカルディスクなど）：**Veeam Kastenはこれらのワークロードを保護できますが、真のスナップショット機能がないため、バックアップの信頼性やパフォーマンスが損なわれます。スナップショット機能を備えたボリュームへのアップグレードを推奨しますが、GSBやNFS tarの固有の制限を許容できる場合は、これらを使用することも可能です。

バックアップストレージアーキテクチャ：オプションの概要

ストレージの選択によって、バックアップデータの回復力とアベイラビリティが左右されます。ロケーションプロファイルとして構成できる各タイプのバックアップストレージの長所と短所の概要を示します。

Veeam Kasten + Veeam Vault

スナップショットは、Veeam Vaultを介してオフサイトの論理的かつ物理的に隔離されたイミュータブルなオブジェクトストレージにエクスポートされます。高度な設定や保守は必要ありません。

Veeam Kasten + Veeam Backup & Replicationリポジトリ

スナップショットは、Veeam Backup & Replicationが管理するインフラストラクチャ（Veeam強化リポジトリやスケールアウトバックアップリポジトリ（SOBR）を含む）にエクスポートされます。ブロックモードが必要です。**注：**9.xより前のバージョンでは、メタデータ用に追加で小規模なロケーションプロファイル（Vault/Object/NFS/CIFS）も必要です。

Veeam Kasten + オブジェクトストレージ

スナップショットはオブジェクトストレージ（例：S3やクラウド）にエクスポートされます。オブジェクトストレージは、オフサイトかつイミュータブル（書き換え不能）になるように設定する必要があります。

Veeam Kasten＋NFS/CIFS

NFS/CIFSに直接エクスポートされたスナップショットは、機能させるためにバージョン管理が必要になるため、WORM対応デバイスであっても通常はイミュータブルにできません。このオプションは完全にサポートされていますが、オフサイトでイミュータブルな複製またはコピーがある場合を除き、推奨されません。

Veeam Kasten + 複数のロケーション プロファイル

スナップショットは2つ以上の場所にエクスポートされます。正しく設計されていれば、少なくとも1つのイミュータブルなオプションを使用することで、最も堅牢な方法となります。**注：**9.xより前のバージョンでは、ポリシーごとに1つのロケーションプロファイルを使用する必要があり、複数のポリシーが必要です。

ストレージモードによって機能が決まる

ストレージのタイプに応じて、次の選択肢が利用可能です。

ボリュームモード：ファイルまたはブロック。どちらもVeeam Kasten（Ceph FSやRBDなど）と互換性があります。

エクスポートモード：ファイルまたはブロック。Veeam Kastenを使用すれば、その両方が可能です。

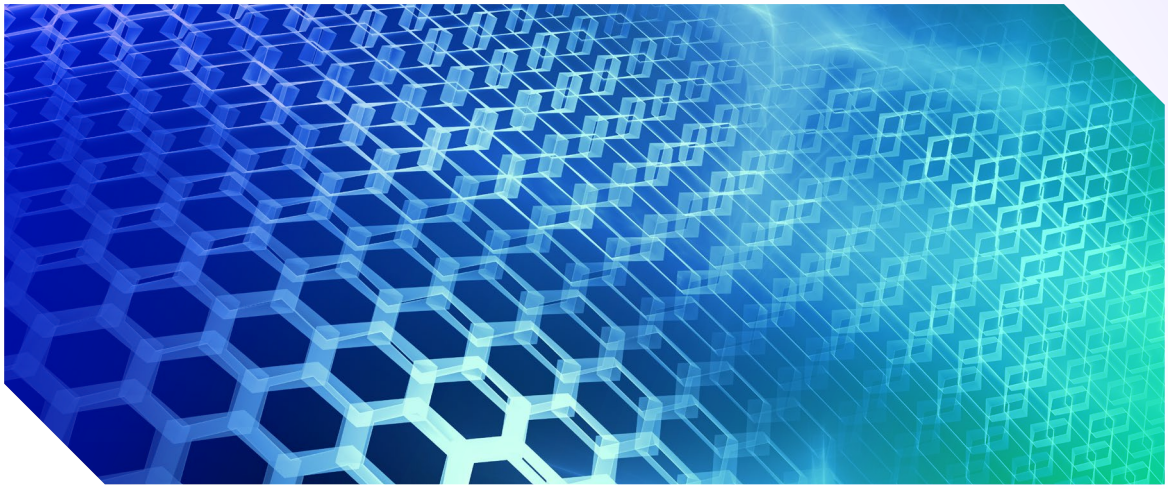
ボリュームがブロックモードの場合は、スナップショットをブロックモードでエクスポートできる可能性があります。これにより、CBT（利用可能な場合）やVeeam Backup & Replicationリポジトリへのエクスポートなどの特別な機能が提供されます。

Veeam Backup & Replication と Veeam Infrastructure Appliance (VIA) を強化リポジトリとして使用する

既存のイミュータブルストレージがない場合、Veeam KastenをVeeam Backup & Replicationと統合し、VIAを導入することが、ローカルのイミュータビリティを実現するための合理的な方法である可能性があります。

強化リポジトリはイミュータブルなローカルバックアップを提供するため、ランサムウェアは保持期間中にそれらを暗号化したり削除したりできません。OSは不正なアクセスに対して強化されており、理想的にはVMではなく保護された物理サーバーで実行する必要があります。

従来、強化リポジトリを構築するには、Linuxディストリビューションを手動でインストールし、セキュリティを強化する必要がありました。VIAは事前に強化されており、ブート可能なISOを使用して展開されるため、この障壁を完全に取り除けます。また、互換性のあるハードウェアに自分で導入することも、認定アプライアンスとしてベンダーから購入することもできます。



マイルストーン2：Veeam Kastenの導入

Veeam Kastenの導入

- プリフライトツールを使用して、要件が満たされていることを確認します（オプション）。
- マーケットプレイス/オペレーター方式：こちらから手順の詳細を確認してください。
- Helm方式：こちらから手順の詳細を確認してください。

ダッシュボードへのアクセスおよび認証統合

- 外部からダッシュボードにアクセスする場合は、Veeam Kasten に Ingress またはルートを追加してください。
- ディストリビューションの認証プロバイダー（例：OpenShift Auth）と統合するのがベストプラクティスですが、直接的なLDAPなどの他のオプションも利用可能です。
- Veeam Kastenダッシュボードが表示されたら、次のステップに進みます。

インフラストラクチャをVeeam Kastenに接続する

- 必要に応じて、（vSphere／クラウド／その他）ストレージインテグレーションのためのインフラストラクチャプロファイルを追加してください。
- バックアップ先を定義するためにロケーションプロファイルを追加します。

マイルストーン3：最初のバックアップジョブ

Kubernetes環境でのバックアップ

ストレージスナップショットは、ストレージプロビジョナーが対応している場合、Kubernetes環境で標準的に認識・管理されるパワフルな機能です。

Veeam Kastenは、この機能や直接統合を活用して、ストレージデバイス上にローカルスナップショットをトリガーします。Veeam Kastenは、これらのスナップショットを利用して、データを外部のロケーションプロファイル（例：NFS、S3、VBRリポジトリ、Vaultなど）へ確実にエクスポートできます。

この方法は、Kubernetesネイティブの機能やAPIを活用し、最大限の互換性を保ちながら、最高の速度と一貫性を実現します。

今すぐ開始するために必要なもの

Veeam KastenはKubernetesネイティブのアプリケーションであるため、インストール担当者はターゲット環境へのkubectlアクセス権、クラスター管理者権限、さらに（存在する場合は）ディストリビューションの管理インターフェイスへのアクセス権も持っていることが理想的です。

ヒント：エラーが発生した場合は、コミュニティやKBサイトでソリューションを探すことができます。

- お使いの環境に該当する場合は、KubeVirt VMの保護の詳細をご覧ください。
- 最初のバックアップポリシーを作成し、ロケーションプロファイルを指定してください。
- まず、適切な保持ポリシーを設定します。ローカルスナップショットは1日1回、ロケーションプロファイルへのエクスポートは、1日1回、週4回、月3回の保持に設定します。
- 非ピーク時間帯にジョブを実行するようにスケジュールし、他の保守時間帯と競合しないことを確認します。
- ジョブを初回は手動で実行し、完了まで監視してください。
- 警告やエラーがないことを確認してから、フェーズ2に進んでください。

初回リストアテスト：必ず実施してください！

フェーズ2に進む前に、重要ではないアプリケーションでリストアを実施し、復元力を確認してください。

リストア可能であることを確認するまで、保護は確立されていないと考えましょう。確認は数分で完了し、後の多大な労力と苦労を回避することができます。

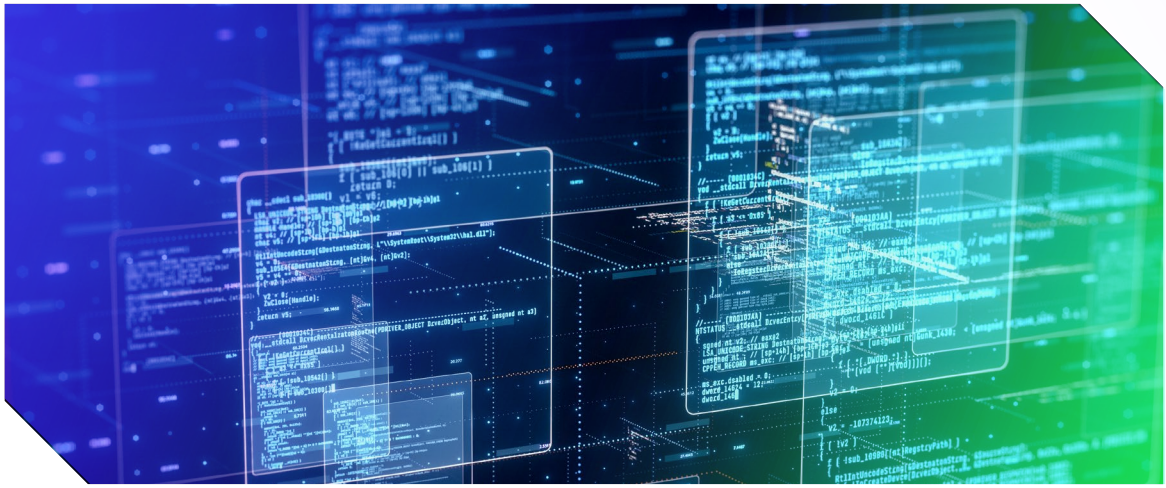
ローカル VS エクスポート

スナップショットは、ストレージデバイス内のみに保存されることに注意してください。つまり、次のことを意味します。

- これらは真のバックアップではありません。
- ローカルスナップショットの保持数が増えると、より多くのプライマリストレージが消費されます。

したがって、スナップショットをロケーションプロファイルにエクスポートし、独立して構成できる保持ポリシーを設定することが重要です。

スナップショットをエクスポートする際、すべてのデータは自動的に重複排除され、圧縮・暗号化され、増分バックアップとして保存されます。



フェーズ2・15日目～45日目

基本の強化

目標：環境全体にわたる一貫した保護、オフサイトコピー、可視性。

マイルストーン4：一元管理（MCM）

マルチクラスターマネージャー（MCM）により、複数のクラスターの一元的な可視性と管理が可能になります。各クラスターには、ワークロードを保護するためにVeeam Kastenがインストールされ、インスタンス同士をリンクすることができます。

- Veeam Kastenを実行している別のクラスターが導入されたら、1つのKastenインスタンスをプライマリに昇格させ、参加トークンを使用してリンクしてください（手順）。エラー防止のために、自己署名証明書が信頼済みであることを確認します。
- MCMダッシュボードから参加しているすべてのクラスターを表示します。
- 環境全体に一貫した設定を配布したい場合は、グローバルポリシーとグローバルプロファイルを定義してください。
- エンタープライズライセンスキーをプライマリMCMクラスターに追加します。ライセンスは他のクラスターにもシームレスに配布され、追加の設定は不要です。

マイルストーン5：アプリケーション認識処理

Kanister Blueprintsを用いたアプリケーション認識処理により、クラッシュ整合性バックアップがアプリケーション整合性または論理エクスポートに変換されます。これは、PostgreSQL、MongoDB、MySQL、Elasticなどのデータベースにとって不可欠です。

- アプリケーションチームとアプリケーションの要件やアクセスについて相談してください。
- カスタマイズ可能な既製のブループリントサンプルを見つけるか、独自のブループリントを作成してください。
- ブループリントをVeeam Kastenに追加します。
- ブループリントをワークロードに手動で関連付けるか、ブループリントバインディングを作成します。
- ブループリントを使用してバックアップとリストアをテストし、エンドツーエンドのアプリケーション復元を検証します。

バックアップの種類

クラッシュ整合性（デフォルト）：この種類のバックアップでは、通常、ストレージプロバイダーのスナップショットを使用して、特定の瞬間にファイルシステム全体をキャプチャします。これは基本的なファイルコピーよりもデータ整合性が高いですが、送信中の書き込みや未フラッシュのトランザクションが見落とされることがあります。

アプリケーション整合性：この種類のバックアップは、アプリケーションのネイティブツールを使用して、スナップショット作成前にすべてがボリュームに書き込まれるよう、アプリケーションを短時間静止させるのが一般的です。

論理：この種類のバックアップは、アプリケーションのネイティブツールを使用して、データの論理ダンプやエクスポートをファイルとして作成します。多くの場合、これはボリューム自体ではなく、S3などの外部の場所にアップロードされます。

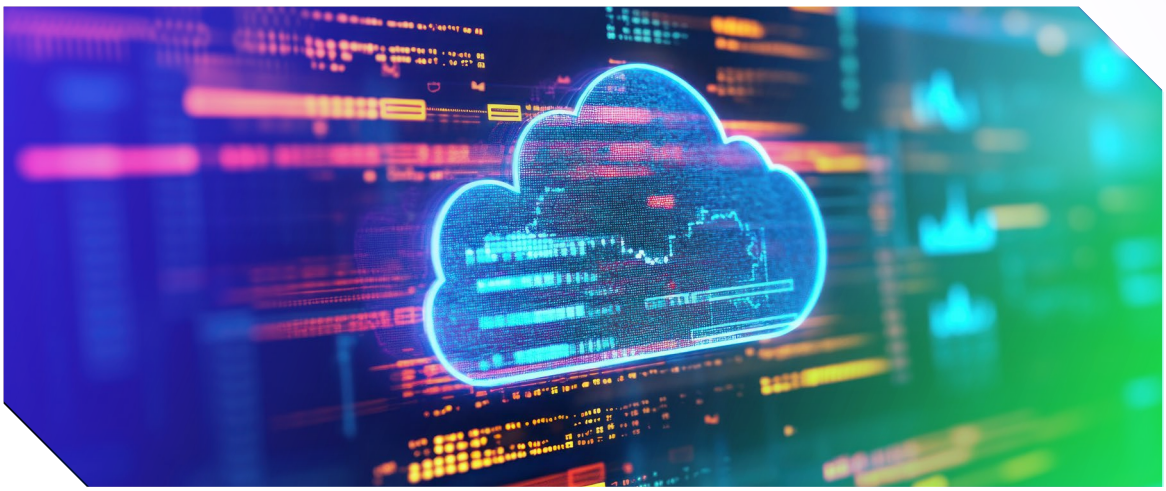
ブループリントはパワフルであるとともに、無限の柔軟性を備えています。さらに、オープンソースであるため、既存のものがない場合は、どのアプリケーションやワークフローにも対応するブループリントを独自に作成することができます。

マイルストーン6：ポリシーのベストプラクティス

このマイルストーンでは、追加のジョブを作成してすべてのワークロードを保護し、高度な設定を使用してその信頼性を確保します。

一般的なシナリオ向けのベストプラクティス

- すべてを保護する1つのワイルドカードポリシーではなく、ラベル付きの複数のジョブを使用してアプリケーションを選択しましょう。
- KubeVirt VMを保護する場合は、名前空間ベースではなくVMベースのポリシーを使用してください。
- クラスタースコープのリソースのみをバックアップする場合は、クラスタースコープのリソースのみを対象とした別のバックアップポリシーを作成してください。
- バックアップウィンドウを定義して、重要な時間帯に本番ワークロードが影響を受けないようにします。
- パフォーマンス向上のため、ジョブを時間差でスケジュールすることを検討してください。
- イミュータブルバックアップ保護を設定してください。
- 除外／リソースフィルター（必要に応じて）。
- （オプション）グローバルリソース、ポリシープリセット



その他のヒント

手動で実行するジョブの場合、有効期限が指定されていない限り、アーティファクトは手動で削除する必要があります。

ジョブがローカル時間で設定されていても、すべての時間はUTCに変換され、ポリシースケジュールは夏時間の影響を受けません。

計算を再確認してください。保持の計算は複雑になることもあります。たとえば、15分間隔で取得した、時間ごとのスナップショットを合計24個保持しても、24時間分ではなく6時間分のスナップショットしか保持されません。

フェーズ3・46日目～75日目

最適化と強化

目標：保護のギャップを解消し、RTO/RPOを改善して可視性を高める。

マイルストーン7：可観測性の統合

- 必要に応じて、Red Hat ACM可観測性の統合を有効化してください。
- 指標を外部の監視システム（Grafana、Datadog、Thanosなど）にエクスポートします。
- 監視システム内にアラートとダッシュボードを作成します（Grafanaの例）。
- レポート機能を有効にします。

マイルストーン8：回復力とDRの強化

すべてのワークロードのバックアップには、Veeam Kasten自体のバックアップも含める必要があります。これはKasten Disaster Recovery（KDR）で実現できます。これとDR環境やDR計画を混同しないようにしてください。これらはすべて、必要な回復力に基づいて検討する必要があります。

KDR（Veeam Kasten Catalogのバックアップ）

- Kasten DRを有効にします。これによってVeeam Kastenのバックアップカタログが保存され、Kastenのインストールにアクセスできなくなった場合でもリストアが可能になります。Veeam Kastenのバックアップファイルは単独ではリストアできず、リストアにはカタログと暗号化パスキーが必要なため、これは非常に重要です。
- Kasten DRを「ローカルカタログスナップショットのエクスポート」に設定し、パスフレーズ、クラスターID、KDRのロケーションプロファイルの詳細、ログイン情報を安全な場所に保存してください。

ワークロードのDR

- 求めるRTO/RPOに基づいて必要な回復力のレベルを決定します。
- 1日以上のRTO/RPOが許容される場合は、バックアップを保持し、必要に応じて環境を再構築するだけで合理的なソリューションとなります。
- RTO/RPOを時間単位や分単位で測定する必要がある場合は、計画の設計には細心の注意が必要です。以下にいくつかの例を示します。

DR設定例（RTO/RPO要件に基づく）

- **未保護のアプリケーション：**リストアポイントは存在しません（ローカルスナップショットやエクスポートもありません）。

  結果：復元不可。

- **エクスポートのみ：**KDRのエクスポートとエクスポートされたリストアポイントは、オフサイトのロケーションプロファイルに保存されます。

  結果：復元するには、まずKubernetes環境を再構築し、Veeam Kastenをインストールして、Kastenカタログを復元し、次にエクスポートされたリストアポイントからアプリケーションを復元します。

- **DR環境＋インポート：**Veeam Kastenがインストールされ、インポートポリシーが定期的に実行されて、リストアポイントがローカルカタログに取り込まれます。

  結果：リストアポイントがセカンダリロケーションに表示され、リストアポイントをリストアする準備が整いました。必要になるまでリソースの使用は最小限に抑えられます。

- **DR環境＋インポート＋リストア、ゼロスケール：**Veeam Kastenがインストールされ、インポート＋リストアポリシーが定期的に実行されてリストアポイントをローカルカタログにインポートし、アプリケーションをKubernetes環境にリストアします。その後、アプリケーションはリストアされますが、トランスフォーム設定レプリカはすべてのワークロードで「0」になります。

  結果：アプリケーションはKubernetesにリストアされます（選択されたポッド、PVなどすべて）。レプリカ数が0なので、ストレージ以外のリソースは必要になるまでほとんど消費されません。

- **DR環境＋インポート＋リストア、フル：**Veeam Kastenがインストールされ、インポート＋リストアポリシーが定期的に実行されて、リストアポイントがローカルカタログにインポートされてから、アプリケーションがKubernetes環境にリストアされます。

  結果：アプリケーションは（ポッドやPVなど、選択されたすべてのものを介して）Kubernetesにリストアされ、本番環境とまったく同じように動作し、フル活用できる状態になります。

災害対策計画

Veeam Kastenはディストリビューション非依存であり、どのKubernetesディストリビューションにも、またTanzuやAzureのようなまったく異なるディストリビューション間でもリストアを実行できます。ただし、リストアを実行するには、動作中のKubernetes環境が存在している必要があります。Kastenはそれ自体をブートストラップできません。インシデントが発生した場合に備えて、適切な災害対策計画を作成し、その計画が目的を達成できていることを定期的に検証してください。

マイルストーン9：ファインチューニング

- **Veeam Kastenダッシュボードを確認してください。**その他のチューニングを行う前に、すべての未保護ワークロードに対応してください。
- **ジョブスケジュールの競合を確認してください。**リソースの競合を防ぐために開始時間をずらしてください。
- 定義したバックアップウィンドウ内にすべてのジョブが完了していることを確認します。
- **RPOコンプライアンスを検証してください：**すべての重要なワークロードが目標リカバリウィンドウ内にリストアポイントを生成していますか？
- すべてのワークロードが、少なくとも1つのイミュータブルなロケーションにエクスポートされていることを確認してください。
- ガベージコレクションを有効にして不要なアクションを削除すると、カタログのパフォーマンスを改善できます。
- アップグレードプロセスをテストしてください。Veeam Kastenの新バージョンは約2週間ごとにリリースされます。

フェーズ4 • 76日目～100日目

価値の検証と運用化

目標：復元力を検証して運用の健全性を確立し、ROIを実証する。

マイルストーン10：復元テスト

重要なのは、リストアできるバックアップのみです。フェーズ4は、文書による証拠を用いて、環境がRTOおよびRPOの要件を満たしていることを証明する段階です。

きめ細かいリストアおよびフルリストアのテスト

- エクスポートから名前空間全体またはVMリストアをテストします。オンプレミス全体の消失をシミュレーションして、オフサイトコピーを検証します。
- アプリケーションアイテムの復元テスト：データベースをリストアし、データベースクエリを実行してデータが正常であることを確認します。
- ファイルレベルの復元テスト（必要に応じて）：個別のファイルをエクスポートからテスト場所に復元します。
- DR計画全体を包括的にテストし、改善のために問題を記録して、計画が利用可能な状態で保持され、それにいつでもアクセスできるようにプロセスの詳細を文書化してください。
- 実際の復旧時間を記録し、RTO目標と比較してください。結果を文書化します。

復元テストのベストプラクティス

必ず本番環境以外のターゲットにリストアし、テスト中は決して稼働中のワークロードを上書きしないでください。

何がリストアされたか、どのリストアポイントからリストアされたか、どのターゲットにリストアされたか、そしてリストアにかかった時間を文書化します。

これらの結果が復元力の証拠となります。それらをコンプライアンスレビューや監査、管理報告のために保存してください。

さらに、同じ環境内でリストアを行う場合（異なる名前空間へのリストアであっても）、特定のリソース（特にネットワークサービス）が競合する可能性があることに注意してください。リストア前に設定内容を必ず確認し、競合を防ぐために別の環境へリストアしたり、トランスフォームを利用したりしてください。

異なる環境へのリストア

異なるサイトやKubernetesディストリビューション、プラットフォームなどに、またはそれらからリストアする場合は、リストア時に設定をシームレスに変更するうえでトランスフォームが便利です。たとえば、ネットワークパスを本番環境からDRに変更する場合や、ストレージクラスを変更する場合です。手動での変更は必要なく、設定を変更した状態や新しい環境でもリストアをすぐに実行できます。

マイルストーン11：文書化とレポート作成

- まだの場合は、レポート機能を有効にします。
- 最終的なバックアップアーキテクチャ（ポリシー一覧、エクスポート先、スケジュール、保持ポリシーを含む）を文書化します。
- Veeam Vaultのストレージ消費量を確認し、利用状況が想定予算と一致していることを確認してください。
- 復元テストの結果をアーキテクチャドキュメントと一緒にアーカイブしてください。

マイルストーン12：継続的な健全性維持の頻度の確立

100日目までに、環境は安定しており、完全に文書化されている必要があります。これらの習慣を通じて以下の状態を維持できます。

- **週次：**Veeam Kastenのダッシュボードを確認し、失敗したジョブや警告のジョブを調査します。それらが蓄積されないようにしてください。
- **月次：**最新のKastenリリースを確認し、定期的に更新します。
- **四半期次：**文書化された復元テストを実施します。毎回異なる種類のワークロードで実施します。
- **年次：**現在のビジネス要件に合わせてバックアップアーキテクチャを見直します。
- **更新前：**Kastenダッシュボードでライセンス使用状況（例：MCMによる全体、または各クラスタごと）を確認し、ライセンスの範囲内であることを確認します。

次のステップ

その他の資料

- Veeam Universityにアクセス
- 他の企業の事例をご覧ください
- カスタマーサクセスとつながる
- データの回復力に関する御社のストーリーをVeeamと共有しましょう

付録：クイックリファレンス

主要コンポーネント：Veeam統合

- **Veeam Software Appliance (VSA)：**Veeam Backup & Replicationがプリインストールされた強化済みのアプライアンス。OVA（VM）またはISO（物理）として導入できます。それ自体が限定的なイミュータブルリポジトリとして機能することもでき、専用VIAを含む他のアプライアンスやバックアップストレージとも連携可能です。
- **Veeam Infrastructure Appliance（VIA）：**強化済みのアプライアンスで、専用の強化リポジトリやその他の役割として導入されます。Linuxの専門知識がなくてもローカルでのイミュータビリティを実現できます。アプライアンスごとに1つのロールが割り当てられます。
- **Veeam Backup & Replication:** VSA上でホストされるコアバックアップエンジン。ジョブ、リポジトリ、プロキシ、およびリカバリ操作を管理します。
- **Scale-out Backup Repository：**ローカルのパフォーマンス層（例：VIA）とキャパシティ層（例：Vault/S3/NFS）を単一のバックアップターゲットにまとめた論理構造。
- **Veeam Vault：**オフサイトコピー用のイミュータブルなクラウドオブジェクトストレージ。Veeamが管理し、別途クラウドアカウントは不要です。

主な用語

- **RPO：**許容可能なデータ消失の最大量（時間で測定）。バックアップスケジュールの頻度を左右します。
- **RTO：**ワークロードが復旧されるまでに許容される最大ダウンタイム。
- **イミュータビリティ（不変性）：**一定の保持期間中、変更や削除ができないバックアップデータ。バックアップファイルのランサムウェアによる暗号化から保護します。
- **Veeam強化リポジトリ：**OSレベルでイミュータビリティが強制されているLinuxベースのバックアップリポジトリ。VIAによってすぐに使用できる状態で提供され、Linuxの管理は必要ありません。
- **KubeVirt：**Kubernetesがコンテナ化されたワークロードと仮想マシン（VM）を併用して実行・管理できるようにするオープンソースプロジェクト。これにより、VMがOpenShift VirtualizationやSUSE HarvesterなどのKubernetesプラットフォーム上で実行可能になります。また、それらのVMはVeeam Kastenで保護することができます。
- **アプリケーション認識処理：**アプリケーション整合性バックアップポイントを作成する処理であり、Veeam Kastenではブループリントを活用して実行できます。
- **ブループリント：**Kanisterブループリントは、Kubernetes上でアプリケーションレベルのデータ管理のためのカスタムタスクを記述するためのオープンソースのメカニズムです。

有用なリソース

- Veeamヘルプセンター
- Veeamカスタマーポータル（ダウンロード）
- Veeamコミュニティフォーラム
- Veeam KB記事
- Veeam Kastenのドキュメント
- Kanisterのブループリントドキュメント

Veeam Softwareについて

VeeamはデータとAIを託す信頼のパートナー。組織が自社のデータとAIを完全に理解し、保護し、回復力を確保することで、安全なAIの大規模な活用を加速できるよう支援しています。データの回復力とデータセキュリティ態勢管理の両方における市場リーダーとして、Veeamはアイデンティティ、データ、セキュリティ、AIリスクを収束させることを念頭に設計されています。

シアトルに本社を置き、30か国以上に事業拠点を構えるVeeamは、世界中で55万社以上のお客様を保護しており、その中にはFortune 500企業の82%が含まれています。

詳細については、veeam.com/jpをご覧になるか、LinkedIn（@veeam-software）およびX（@veeam）でVeeamをフォローしてください。