KVM/DR

ホワイトペーパー | クロスハイパーバイザー DR シリーズ | 第 1 部（全 2 部）

Proxmox VE と oVirt：同じエンジン、異なる世界

クロスハイパーバイザー DR で何ができて何ができないのか、そして復旧の挙動がプラットフォームごとに異なる理由

KVMDR AI Ltd | kvmdr.ai | 2026 年 11 月

概要

Proxmox VE と oVirt はどちらも KVM と QEMU で仮想マシンを動かすため、VM はデータを保ったまま両者の間を移動できます。しかし両プラットフォームの管理方式は大きく異なり、その違いがそれぞれの側で災害対策に何ができるかを左右します。本書では両者のアーキテクチャを比較し、各方向で何が可能かを整理し、oVirt をターゲットとする復旧が Proxmox への復旧より多くの計画を必要とする理由を説明したうえで、実践的なベストプラクティスのチェックリストを示します。第 2 部では、KVMDR がクロスハイパーバイザー DR をどのように実現しているかを説明します。

1. クロスハイパーバイザー DR が重要な理由

現在、多くの組織が複数の KVM プラットフォームを運用しています。oVirt や Red Hat Virtualization から Proxmox VE へ移行中の組織もあれば、データセンターでは oVirt や Oracle Linux Virtualization Manager を使い、エッジやセカンダリサイトでは Proxmox を使う組織もあります。いずれの場合も同じ問いが生まれます。一方のプラットフォームで他方を保護できるのか、という問いです。

答えは「できる」です。仮想マシン自体は両側で同じ、つまり QEMU デバイスと VirtIO ドライバーを持つ KVM ゲストだからです。異なるのは VM を取り巻くすべての部分であり、そこにこそ計画が必要になります。

> **要点**
> Proxmox は、各ホストが自らを管理するホストの集まりです。oVirt は、中央のエンジンがホストを管理します。Proxmox への復旧は DR ホストだけに依存します。oVirt への復旧は、oVirt エンジンが稼働していることにも依存します。

2. 2 つのアーキテクチャ

Proxmox VE：各ホストが自らを管理する

Proxmox の各ノードは、独自の API、Web インターフェース、コマンドラインツールを持ちます。ノードは設定を共有するクラスターを構成できますが、中央の管理サーバーはありません。どのノードも、LVM thin、ZFS、ディレクトリ、Ceph など自身が到達できるストレージを使って、仮想マシンとコンテナを単独で作成、起動、停止できます。

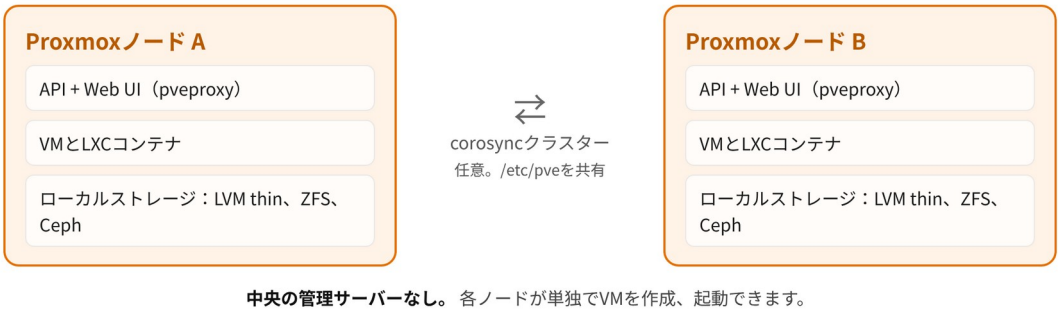
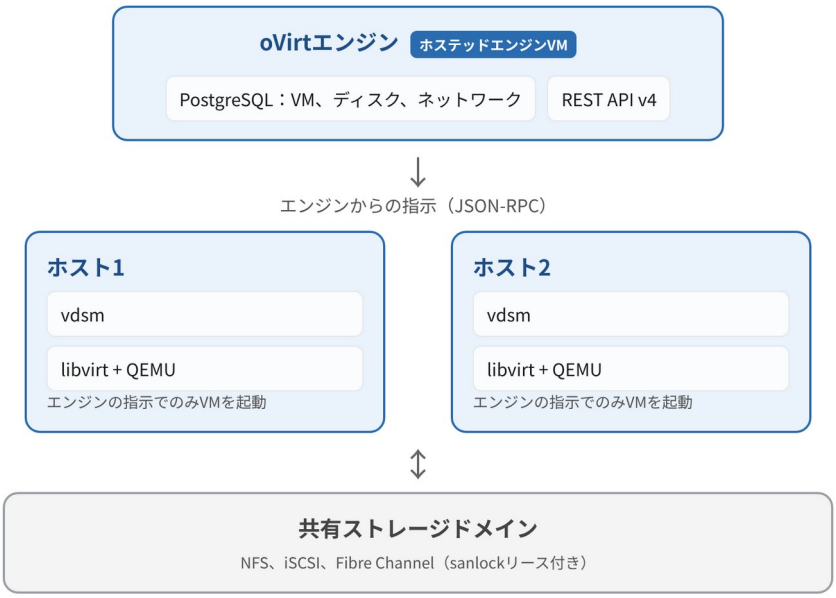


図 1. Proxmox VE：各ノードが自らを管理する

oVirt、OLVM、RHV：中央のエンジンがすべてを制御する

oVirt では、エンジンがすべての VM、ディスク、ネットワーク、ストレージドメインのデータベースを保持します。ホストは vdsm サービスを実行し、エンジンの指示があった場合にのみ VM を起動します。ディスクは NFS、iSCSI、Fibre Channel 上の共有ストレージドメイン内のイメージです。エンジン自体は通常、同じホスト上でホステッドエンジン VM として稼働します。

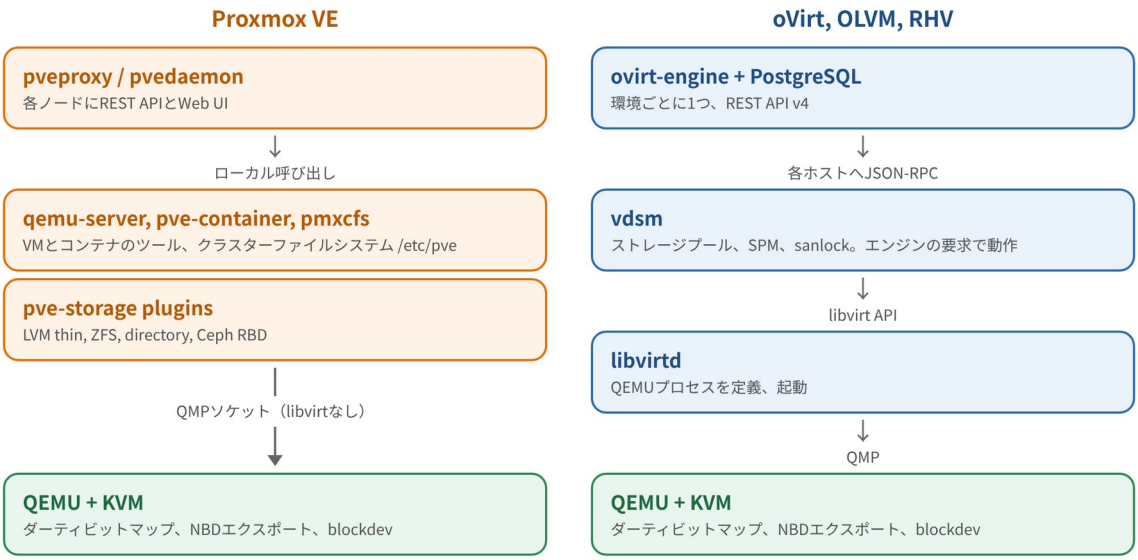


VMはエンジンのデータベース上にのみ存在。 エンジンなしでは新しいVMは起動できません。

図2. oVirt、OLVM、RHV：中央のエンジンがホストを管理する

ソフトウェアスタックの内側

両プラットフォームの行き着く先は同じ、KVM ゲストを実行する QEMU プロセスです。違いが生じるのは QEMU より上の層であり、その層がレプリケーション、スナップショット、復旧の仕組みを決定します。



最下層は同じ、その上の制御が異なる。 ProxmoxはQEMUを直接制御。oVirtはエンジン、vdsm、libvirt、QEMUの順に経由。

図3. ソフトウェアスタック（上から下へ）

レイヤー	Proxmox VE	oVirt、OLVM、RHV
管理 API	各ノード上の pveproxy と pvedaemon	ovirt-engine（環境ごとに 1 つ）
VM の定義	/etc/pve/qemu-server 内のテキストファイル。pmxcfs が corosync 経由で複製	エンジンの PostgreSQL データベース内の行
ホストエージェント	qemu-server と pve-container（各ノードの一部）	vdsm（エンジンの要求に応じてのみ動作）
QEMU の制御	QMP ソケット経由で直接。Proxmox は libvirt を使用しない	vdsm が操作する libvirt 経由
ストレージ層	pve-storage プラグイン：LVM thin、ZFS、ディレクトリ、Ceph RBD	ストレージドメインで構成されるストレージプール。SPM ホストが調整
ロック	pmxcfs のクラスターロック	共有ストレージ上の sanlock リース

ストレージの内部動作

Proxmox は各 VM ディスクをストレージプラグインに渡します。LVM thin ではディスクは device mapper のシンボリューム、ZFS では zvol です。スナップショットはストレージ自体（dm thin スナップショットまたは ZFS スナップショット）によってほぼ瞬時に作成され、単独で使用できる独立したブロックデバイスになります。

oVirt はストレージを、ストレージドメインで構成されるストレージプールとしてまとめます。ファイルドメイン（NFS）では、各ディスクは 1 つ以上のボリュームファイルを持つイメージディレクトリで、各ボリュームにはメタデータファイルと sanlock リースがあります。ブロックドメイン（iSCSI、FC）では、各ストレージドメインが LVM ボリュームグループ、各ボリュームが論理ボリュームです。oVirt のスナップショットは既存ボリュームの上に新しい qcow2 ボリュームを追加し、チェーンを形成します。ボリュームの作成は共有メタデータを変更するため、エンジンの指示により、選出された 1 台のホストであるストレージプールマネージャー（SPM）が実行します。

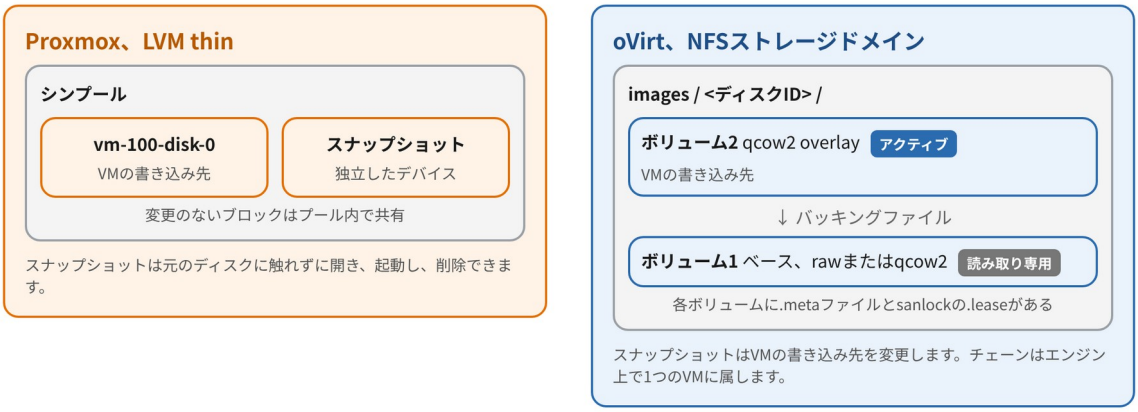


図 4. スナップショットを 1 つ持つディスク

この違いは災害対策にとって重要です。Proxmox ではスナップショットは独立したデバイスであり、DR ツールは元のディスクに触れずに開き、起動し、破棄できます。oVirt ではスナップショットは VM の書き込み先ボリュームを変更し、そのチェーンはエンジンのデータベース上で 1 つの VM に属します。

エンジン自体の配置

多くの oVirt 環境では、エンジンは同じホスト上でホステッドエンジン VM として稼働します。各ホストの 2 つのサービス、ovirt-ha-agent と ovirt-ha-broker が、共有ストレージ上の sanlock ロックスペースを使ってエンジンを稼働させ続けます。broker が停止したり、ロックスペースを取得できなかったりすると、ホステッドエンジンは停止したままとなり、復旧した VM の起動を含むすべてのエンジン操作ができなくなります。

項目	Proxmox VE	oVirt、OLVM、RHV
管理	各ノードが独自の API と UI を持つ	すべてのホストを 1 つの中央エンジンが管理
VM が定義される場所	ノード上の設定ファイル	エンジンのデータベース
VM を起動する主体	どのノードでも単独で可能	エンジン（vdsm 経由）
ディスクの配置	ノードストレージ上のボリューム	共有ストレージドメイン内のイメージ
コンテナ	あり（LXC）	なし
VM 名	有効なホスト名であること。アンダースコア不可	アンダースコア可
保護が必要なコンポーネント	なし。各ノードが独立	エンジン

3. 各方向で可能なこと

機能	Proxmox から oVirt へ	oVirt から Proxmox へ
VM レプリケーション	可能	可能
コンテナ（LXC）	不可。oVirt にはコンテナがないため、Proxmox から Proxmox へ保護	該当なし
ターゲットストレージ	oVirt ファイルストレージドメイン（NFS）	DR ホスト上のシンプロビジョニングストレージ
業務を止めない DR テスト	可能。テスト用ベースラインの追加容量が必要	可能。容量効率が高い
フェイルオーバー	可能。oVirt エンジンの稼働が必要	可能。DR ホストのみで実行
フェイルオーバー時の IP 変更（Re IP）	可能	可能

機能	Proxmox から oVirt へ	oVirt から Proxmox へ
ターゲット上の VM 名	維持	アンダースコアはハイフンに変換
稼働中 VM へのファイル復元	可能（QEMU ゲストエージェントが必要）	可能（QEMU ゲストエージェントが必要）

現在の制限事項

- **コンテナは Proxmox 上に限定。** oVirt はコンテナに対応していないため、LXC コンテナは Proxmox から Proxmox へ保護します。
- **oVirt ではファイルストレージドメインのみ。** iSCSI および Fibre Channel のストレージドメインは、現時点ではターゲットとしてサポートされていません。
- **エンジンなしでは oVirt へのフェイルオーバー不可。** oVirt ホストはエンジンなしでは新しい VM を起動できません。

4. oVirt ターゲットで復旧が異なる理由

エンジンが稼働している必要がある

Proxmox では、復旧は DR ホストと直接やり取りし、DR ホストは単独で VM を作成、起動できます。oVirt では、すべての VM とディスクをエンジンに登録する必要があり、VM を起動できるのもエンジンだけです。ホステッドエンジンが停止しているか正常でない場合、復旧は待機状態になります。これが 2 つのターゲットの最大の違いです。

ディスクはストレージドメイン内に置く必要がある

Proxmox では、DR ディスクは DR ホスト上にあり、すばやく作成、入れ替えできます。oVirt では、ディスクはストレージドメイン内のイメージであり、エンジンを通じて作成されます。ターゲットのストレージドメインは事前に選択し、保護対象データに見合う容量を確保しておく必要があります。

oVirt ではテストにより多くの容量が必要

Proxmox での DR テストには追加容量がほとんど必要ありません。oVirt ではテスト用ベースラインのコピーを保持するため、ストレージドメインには保護対象データに加えてそのベースライン分の容量が必要です。理由と各ターゲットのサイジング方法は、本シリーズ第 2 部で説明します。

名前とネットワークは変換される

Proxmox の VM 名にはアンダースコアを使用できません。ネットワークのモデルも異なり、Proxmox は vmbr0 などの Linux ブリッジ、oVirt は論理ネットワークと vNIC プロファイルを使用します。すべてのソースネットワークに、明確なターゲットネットワークが必要です。

5. ベストプラクティス チェックリスト

保護を開始する前に

1. VM ごとにどちらのプラットフォームをプライマリとするかを決め、一貫させる。
2. oVirt をターゲットとする場合は、エンジンを少なくとも 2 台のホスト上で高可用性のホステッドエンジンとして稼働させる。

3. oVirt をターゲットとする場合は、保護対象データとテスト用ベースラインを収容できる容量の NFS データドメインを作成する。
4. コンテナは Proxmox から Proxmox への保護とする。
5. VirtIO ディスクと NIC を使用し、すべての VM に QEMU ゲストエージェントをインストールする。
6. Proxmox 上で稼働する可能性のある VM の名前にはアンダースコアを使わない。

ネットワーク

1. すべてのソースブリッジまたはネットワークをターゲットネットワークにマッピングする。
2. フェイルオーバー時に IP アドレスを変更するか維持するかを VM ごとに決める。

テスト

1. 各 VM は保護開始後にテストし、その後は少なくとも月 1 回テストする。
2. VM が起動すること、想定どおりのアドレスを取得すること、アプリケーションが応答すること、ゲストエージェントが応答することを確認する。
3. oVirt をターゲットとする場合は、毎回のテストにエンジンの健全性確認を含める。

フェイルオーバーとフェイルバック

1. フェイルオーバーは実際の障害時にのみ実行し、スケジュールしない。
2. 復旧した VM にユーザーがターゲットネットワーク上で到達できることを確認する。
3. フェイルバックはメンテナンス時間帯に計画する。

6. まとめ

Proxmox VE と oVirt は同じ KVM 仮想マシンを動かすため、両者間のクロスハイパーバイザー DR は現在すでに実用的です。成功の鍵は、各プラットフォームの管理方式を尊重することにあります。Proxmox は単独で復旧でき、oVirt はエンジンを通じて復旧します。ストレージ、ネットワーク、エンジンの可用性を事前に計画し、定期的にテストすれば、どちらのプラットフォームでも他方を保護できます。

本シリーズ第 2 部では、KVMDR がこれらの違いをどのように吸収し、運用担当者から見てクロスハイパーバイザー復旧が同じ手順で行えるようにしているかを説明します。

KVMDR について

KVMDR AI Ltd は、KVM ベースのハイパーバイザー（Proxmox VE、oVirt、Oracle Linux Virtualization Manager、Red Hat Virtualization）向けの災害対策（DR）製品を開発する英国企業です。KVMDR は、ニア同期レプリケーション、ランサムウェアからのポイントインタイム復旧、業務を止めない DR テスト、AI による脅威検知を 1 つのプラットフォームで提供します。7 日間の無料トライアルは kvmdr.ai から開始できます。