



Proxmox VEワークロードの事業継続性 NetApp virtualization solutions

NetApp
October 29, 2026

This PDF was generated from <https://docs.netapp.com/ja-jp/netapp-solutions-virtualization/proxmox/proxmox-business-continuity.html> on October 29, 2026. Always check docs.netapp.com for the latest.

目次

Proxmox VEワークロードの事業継続性	1
SnapMirror active syncを使用したProxmox VEのビジネス継続性について学ぶ	1
顧客の課題	1
ソリューションの概要	2
ソリューションが障害にどのように対応するか	6
SnapMirror active sync と MetroCluster の選択	8
Proxmox VEストレッチクラスターにおけるCorosyncに関する考慮事項	12
Proxmox用ストレージマネージャーとの統合	13
NAS向けSnapMirror active syncを備えたNFS共有ストレージ	14
関連情報	18
Proxmox VEのビジネス継続性をNASストレージで構成する	18
ステップ1：メディアエーターを設定する	19
ステップ2：SnapMirrorアクティブ同期を使用してNFS SVMを保護する	21
ステップ3：レイヤ3ネットワーク用にBGPを使用したVIP LIFを設定する	22
ステップ4：QDeviceを使用してProxmox VEストレッチクラスターを作成する	24
ステップ5：保護されたNFS共有ストレージをプロビジョニングする	25
ステップ6：HAとVMバックアップの設定	26
ステップ7：計画されたフェイルオーバーをテストする	27
関連情報	28
Proxmox用Storage Managerの設定と使用	28
Proxmox 用 Storage Manager について学ぶ	28
Proxmox 用の Storage Manager をインストールしてセットアップする	30
Proxmox 用の Storage Manager の設定	32
ストレージのプロビジョニング	37
仮想マシンの保護	48
仮想マシンまたはデータストアをリストアする	54
仮想マシンのクローニング	58
運用の監視	60
まとめ	62

Proxmox VEワークロードの事業継続性

SnapMirror active syncを使用したProxmox VEのビジネス継続性について学ぶ

Proxmox Virtual Environment (VE) でビジネス クリティカルな仮想マシン (VM) を実行する企業や、Proxmox VEで顧客のVMをホストするサービスプロバイダは、ストレージシステムやデータセンター全体がオフラインになった場合でも、それらのVMを稼働させ続ける必要があります。ONTAP SnapMirror active syncは、2つのサイトに拡張されたProxmox VEクラスタの共有ストレージを同期レプリケーションし、ストレージを自動的に稼働中のサイトにフェイルオーバーします。目標復旧時点 (RPO) ゼロ、スクリプトやランブックなしの自動復旧、両サイトでの同一の共有ストレージを実現できるため、Proxmox VEの高可用性 (HA) により、ストレージを再構成することなくVMを再起動できます。NFS共有ストレージの場合、このソリューションはNAS向けのSnapMirror active syncを使用します。

顧客の課題

Proxmox VEのストレージとサイトの耐障害性をネイティブツールだけで構築するのは困難です：

- *サイト障害後のデータ損失。*Proxmox VEのストレージレプリケーションとProxmox Backup Serverは非同期です。プライマリサイトに障害が発生すると、前回のレプリケーションまたはバックアップ以降に加えられた変更は失われます。
- *手動による時間のかかるリカバリ。*セカンダリサイトでの復旧は通常、レプリカの昇格、別のアドレスでのストレージのマウント、`/etc/pve/storage.cfg`の更新、およびVMの再起動を伴います。手作業による各手順は、ダウンタイムを増加させ、システム停止中のエラーのリスクを高めます。
- *ホストリソースをめぐってVMと競合するストレッチドストレージ*ハイパーコンバージド・ストレッチド・ストレージ（たとえば、ストレッチモードのCephなど）は、Proxmox VEノード上で動作し、各サイトにすべてのオブジェクトのレプリカを2つ保持します。レプリケーション、リカバリ、およびリバランスのトラフィックは、VMを実行する同じノード上のCPU、メモリ、およびネットワーク リソースを消費します。
- *2つのクォーラムの決定が一致する必要があります。*どのような2サイト設計でも、Proxmox VEクラスタとストレージ用に、第3の障害ドメインにウィットネスが必要です。サイト間リンクの障害後にクラスタとストレージが異なる存続サイトを選択した場合、VMはアクティブなストレージに到達できないノード上で再起動します。
- *両方のサイトで有効なストレージアドレス。*ストレージのフェイルオーバー後、Proxmox VEノードは同じアドレスで共有ストレージにアクセスする必要があります。そのアドレスは両方のサイトからアクセス可能である必要があり、通常はサイト間に拡張されたレイヤ2 VLANを意味します。

サービスプロバイダーの課題

Proxmox VE上でクラウド サービスを構築するサービスプロバイダーは、テナントのサービスレベル契約 (SLA) に加えて、同様の課題に直面します：

- *ストレージシステムは共通障害点です。*Proxmox VE HAは、テナントVMをホストの障害から保護しますが、VMのディスクをホストするストレージシステムの障害からは保護しません。ストレージの障害が1

件発生すると、そのシステムを利用しているすべてのテナントに影響が及びます。

- *より高い可用性を販売する方法はありません。*同期レプリケーションと自動ストレージフェイルオーバーがなければ、プロバイダーはデータ損失ゼロで稼働率の保証がより強力なプレミアム可用性ティアを提供することはできません。
- *復旧中のテナント分離。*復旧、保守、および災害復旧テストは、プラットフォーム全体ではなく、関係するテナントにのみ影響するようにする必要があります。

企業の課題

ミッションクリティカルなワークロードを他のハイパーバイザーからProxmox VEに移行する企業は、データベースや基幹業務アプリケーションのデータ損失ゼロ、手動の手順書なしでの復旧など、以前と同様のサイトの回復力を期待しています。Proxmox VEのネイティブツールだけでその期待に応えるには、相当な設計、スクリプト作成、および運用上の労力が必要となります。

ソリューションの概要

このソリューションは、2つのサイトにあるNetApp AFF システム上のSnapMirrorアクティブ同期と、Proxmox VEストレッチクラスタを組み合わせています：

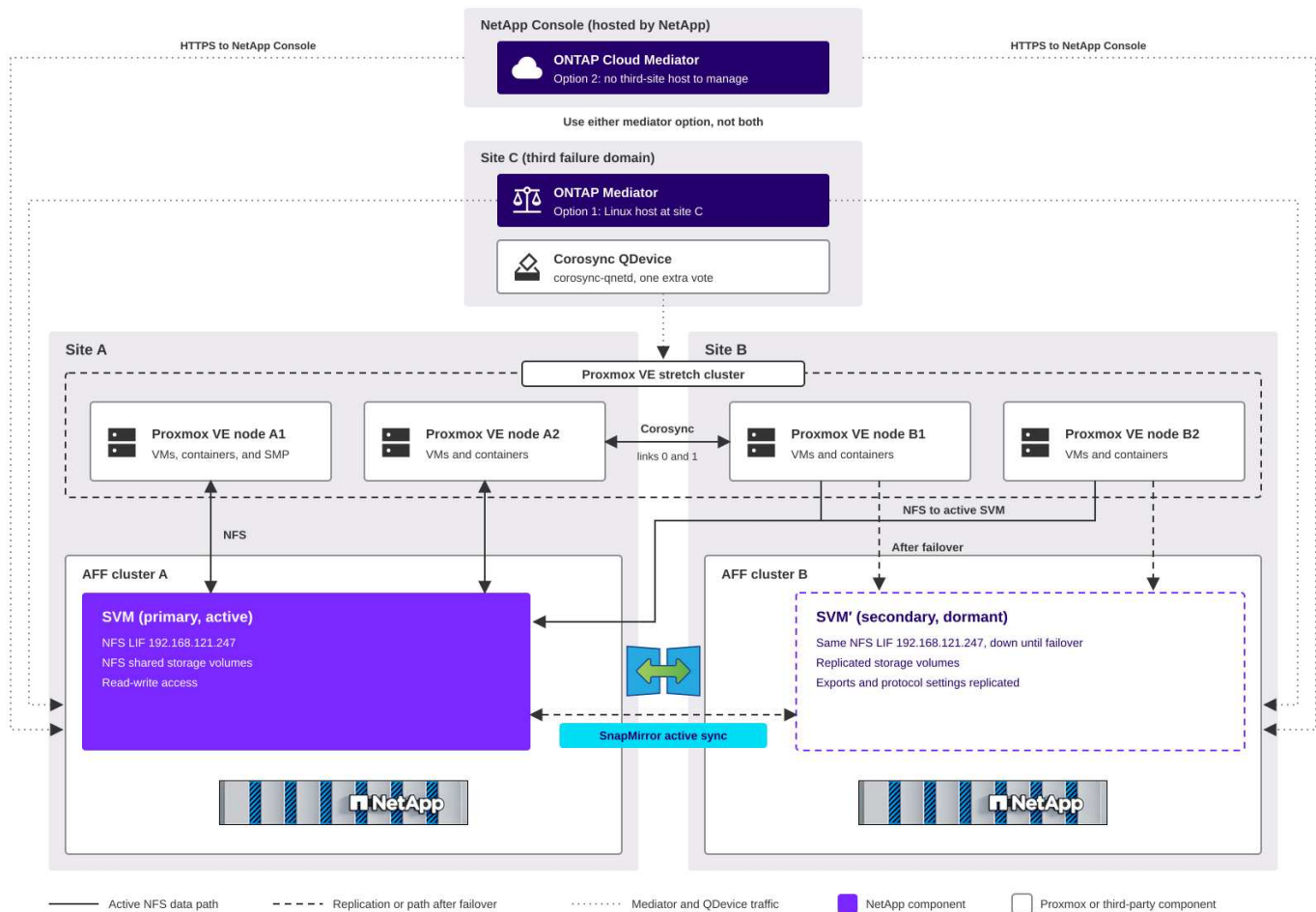
- *RPOゼロ。*ONTAPは、サイトAのプライマリクラスタからサイトBのセカンダリクラスタへ、共有ストレージへのすべての書き込みを同期的に複製します。
- *両サイトで同じ共有ストレージ*フェイルオーバー後、セカンダリクラスタはProxmox VEに同じストレージを提供するため、`/etc/pve/storage.cfg`内のストレージ定義は有効なままです。
- *自動フェイルオーバー。*メディアエーターは、2つのサイトの外部で監視役として機能します。ONTAP Mediatorを3つ目のサイトにインストールするか、NetApp ConsoleでホストされるサービスであるONTAP Cloud Mediatorを使用できます。プライマリ ストレージまたはサイトに障害が発生した場合、ONTAPは手動での介入なしにサイトBにフェイルオーバーします。
- *きめ細かな制御。*保護するワークロードを選択し、サイトのメンテナンスのために1つのテナントやアプリケーションを移動する場合など、ワークロードを個別にフェイルオーバーできます。
- *セカンダリコピーの使用。*レプリケーションに影響を与えることなく、開発、テスト、またはディザスタリカバリのテスト用にセカンダリコピーのクローンを作成できます。

このソリューションが課題にどのように対処するか

課題	このソリューションがどのように役立つか	まだ計画が必要な事項
データ損失と手動復旧	同期レプリケーションではRPOはゼロになります。ONTAPは自動的にフェイルオーバーし、セカンダリSVMは同じNFSアドレスを提示するため、`/etc/pve/storage.cfg`は有効なままです。	Proxmox VE HAは、引き続き障害が発生したサイトから仮想マシンを再起動します。

課題	このソリューションがどのように役立つか	まだ計画が必要な事項
ホスト上の拡張ストレージ	レプリケーションはProxmox VEノードではなくAFFコントローラ上で実行されるため、ホストCPU、メモリ、ネットワークは引き続きVMで利用できます。ONTAPは各サイトにコピーを1つずつ保持し、ストレージ効率化は両方のコピーに適用されます。	他の同期レプリケーションと同様に、このソリューションではサイトBに完全な2つ目のコピーが必要であり、レプリケーションによって両方のAFFクラスタに負荷がかかります。レプリケーションのワークロードに合わせて、両方のクラスタのサイジングを行ってください。
定足数に関する2つの決定	ONTAP Mediator、またはNetApp ConsoleのサービスであるONTAP Cloud Mediatorは、データパス外の軽量なウィットネスです。このソリューションは、corosync QDeviceをプライマリクラスタと連携させ、両方が同じサイトを選択するようにする方法を示しています。	QDeviceには、3つ目の設置場所が引き続き必要です。ONTAP Mediatorにも必要ですが、ONTAP Cloud Mediatorには必要ありません。 Mediatorオプション を参照してください。
両サイトのストレージアドレス	セカンダリSVMは同じNFS LIFアドレスを引き継ぐため、再マウントやストレージの再構成は必要ありません。	NFSサブネットは両方のサイトからアクセス可能である必要があります。通常は拡張レイヤ2 VLANを使用します。VIP LIFの資格ステータスについては、 VIP LIFとBGPを備えたレイヤ3ネットワーク を参照してください。

次の図は、NFS共有ストレージを使用したソリューション アーキテクチャを示しています。



サイトAとサイトB

各サイトには、AFF 2ノードクラスタとProxmox VEノードの半分が配置されています。サイトAにあるプライマリクラスタは、すべてのProxmox VEノードに共有ストレージを提供します。サイトBのノードは、サイト間ネットワークを介してプライマリクラスタに接続します。NFSストレージを使用する場合、サイトBのセカンダリSVMはフェイルオーバーが発生するまで休止状態を維持します。

サイトC

3番目の障害ドメインは、corosync QDeviceデーモン(`corosync-qnetd`) と、オプション1を選択した場合はONTAP Mediatorをホストします。QDeviceは追加の投票権を提供することで、いずれかのサイトに障害が発生した場合でもProxmox VEクラスタがクォーラムを維持できるようにします。

NetApp Console

オプション2を選択した場合、ONTAP Cloud Mediatorは、NetAppがホストおよび管理するNetApp Consoleでサービスとして実行されます。両方のAFFクラスタがHTTPS経由で接続するため、メディエーターホストをインストールしたり保守したりする必要はありません。

メディエーター

ONTAP MediatorまたはONTAP Cloud Mediatorは、ONTAPがどのクラスタからデータを提供するかを決定するのに役立ちます。両方ではなく、いずれか一方を使用してください。比較については、[Mediatorオプション](#)を参照してください。

Proxmox VE ストレッチクラスタ

すべてのProxmox VEノードは1つのクラスタに属し、同じストレージ定義を共有します。Proxmox VE HA

は、障害が発生したサイトのVMを、稼働中のノード上で再起動します。Storage Manager for Proxmox (SMP) は、クラスタ上でHA VMとして動作し、共有ストレージのプロビジョニング、VMのバックアップ、リストア、クローン作成を行います。

Mediatorオプション

SnapMirrorアクティブ同期は、受動的な監視役としてメディエーターを使用します。ネットワークの分断や1つのクラスタの障害が発生した場合、ONTAPはメディエーターを使用して、どのコピーが引き続きI/Oを処理するかを決定します。メディエーターはデータパスには存在せず、メディエーター自体がフェイルオーバーを開始することはありません。以下のいずれかのオプションを使用できますが、両方を同時に使用することはできません。

考慮事項	オプション1：ONTAP Mediator	オプション2：ONTAP Cloud Mediator
稼働場所	独立した電源とネットワークインフラを備えた、サイトCなどの第3の障害ドメインにインストールして管理するLinuxホスト	NetApp Consoleのクラウドサービスです。NetAppがホストおよび管理するため、第3のサイトに仲介ホストを用意する必要はありません。
ONTAPのバージョン	NAS向けSnapMirrorアクティブ同期用のONTAP 9.19.1以降。	ONTAP Cloud Mediatorは、ONTAP 9.17.1以降で利用可能です。SnapMirrorのNAS向けアクティブ同期には、ONTAP 9.19.1以降が必要です。
クラスタ接続	両方のクラスタはメディエータホストに接続します。デフォルトのサービスポートは31784です。	どちらのクラスタも、直接またはHTTPプロキシ経由で、HTTPSを使用してNetApp Consoleにアウトバウンド接続します。NetApp Consoleへの推奨pingレイテンシは200 ms未満です。
セットアップ	パッケージをLinuxホストにインストールし、ホストアドレスとメディエーターユーザを使用してクラスタに追加します。	*ONTAP Mediator Setup Role*を持つNetApp Consoleサービスアカウントを作成し、組織ID、クライアントID、およびクライアントシークレットを使用して、メディエーターをクラスタに追加します。
操作	ホストにパッチを適用してアップグレードし、利用可能な状態を維持します。	パッチ適用やアップグレードを行うホストはありません。両方のサイトからのインターネットアクセスと、NetApp Consoleサービスの可用性に依存します。
ベストフィット	第三サイトが存在する環境、またはストレージクラスタがインターネットに接続できない環境。	メディエーター用の第3サイトがない環境、またはメディエーターの運用を避けたい環境。

選択する際には、以下の点に留意してください：

- *QDeviceには引き続き3つ目の設置場所が必要です。*ONTAP Cloud Mediatorは、corosync QDeviceホストではなく、メディエーターホストを削除します。QDeviceには、すべてのProxmox VEノードがTCPポート5403でアクセスできる小規模なLinuxホストが必要ですが、corosyncの低レイテンシ要件はありません。
- *両方のクラスタはNetApp Consoleにアクセスできる必要があります。*クラスタでプロキシを使用する場合は、プロキシのルートCA証明書を両方のクラスタにインストールします。NetAppでは、クラスタごと

に異なるプロキシ サーバを使用することを推奨しています。

- *どちらのオプションでも同じ障害時の動作を想定して計画してください。*メディエーターが利用できない場合、レプリケーションはデータ損失なく継続されますが、メディエーターが再び利用可能になるまで、自動および計画的なフェイルオーバーは実行できません。ONTAP Cloud Mediatorを使用する場合、これにはクラスタからNetApp Consoleへの接続の喪失が含まれます。



このセクションのメディエーターオプションは、SnapMirrorアクティブ同期に適用されます。MetroClusterの場合、このソリューションではONTAP MediatorまたはMetroCluster Tiebreakerを使用します。デプロイする前に、ご使用のONTAPバージョン、メディエーターオプション、およびProxmox VEバージョンが"[NetApp Interoperability Matrix Tool \(IMT\)](#)"と一緒に記載されていることを確認してください。

サービスプロバイダにとってのメリット

- *ホストHAを超えるVMの可用性。*テナントVMは、ディスクをホストするストレージシステムに障害が発生しても稼働し続けます。ONTAPは2番目のAFFクラスタにフェイルオーバーし、VMは再起動することなく同じ共有ストレージ上でI/Oを再開します。
- *プレミアム可用性ティア*同じクラスタ内の保護されていないストレージ上の標準ティアと並行して、RPOゼロでストレージ耐障害性に優れたVMサービスをアドオンとして提供できます。
- *テナントごとの保護とフェイルオーバー*テナントまたはサービス階層ごとに個別の保護ストレージを使用することで、他のテナントに影響を与えることなく、各テナントの保護、フェイルオーバー、およびディザスタリカバリのテストを個別に実行できます。
- *両サイトをより有効活用する。*一部のワークロードをサイトAでプライマリにし、他のワークロードをサイトBでプライマリにすることで、両方のデータセンターがアクティブなワークロードに対応できるようになります。

企業にとってのメリット

- ストレージ障害またはサイト障害の発生時における、ビジネス クリティカルな**VM**のデータ損失ゼロ。
- スクリプト、ストレージの再マウント、または `etc/pve/storage.cfg` への変更を必要としない*自動リカバリ*。
- **ONTAP**に組み込まれており、Proxmox VEノード上に追加のソフトウェアレイヤは不要です。
- *1つのインターフェイスで日常業務を管理。*Storage Manager for Proxmoxは、保護された共有ストレージをプロビジョニングし、ONTAPスナップショットとFlexCloneテクノロジーを使用してVMのバックアップ、リストア、クローン作成を行います。

ソリューションが障害にどのように対応するか

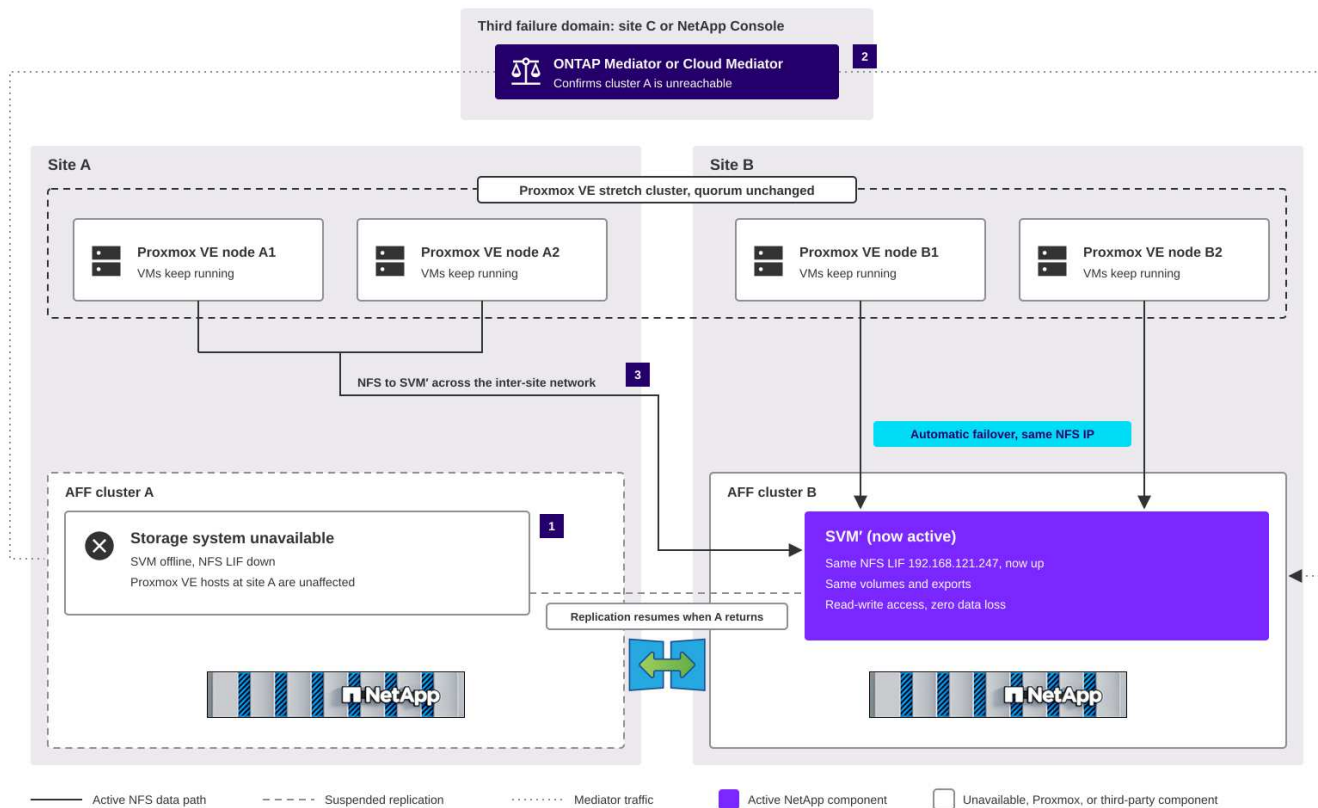
ONTAPとProxmox VEは、独立してクォーラムの決定を行います。この設計により、両者が同じ存続サイトを選択するように調整されています。

イベント	ONTAPの動作	Proxmox VEの動作
サイトAに障害が発生	メディエーターが障害を確認すると、ONTAPは自動的に共有ストレージをクラスタBにフェイルオーバーします。	サイトBのノードとQDeviceはクォーラムを維持します。HAはサイトAのノードをフェンスし、サイトBのノード上でそれらのVMを再起動します。ストレージの

イベント	ONTAPの動作	Proxmox VEの動作
AFFクラスタAに障害が発生しても、サイトAのProxmox VEノードは引き続き稼働する	メディアエーターはクラスタAに到達できないことを確認し、ONTAPは共有ストレージを自動的にクラスタBにフェイルオーバーします。	クォーラムの変更やVMの再起動はありません。ストレージのフェイルオーバー後、すべてのノード上のVMは同じ共有ストレージ上でI/Oを再開し、サイトAのノードはサイト間ネットワークを介してクラスタBに接続します。
サイトAのAFFコントローラ1台に障害が発生する	ローカルHAテイクオーバーでは、パートナーコントローラがテイクオーバーします。SnapMirrorアクティブ同期のフェイルオーバーは発生しません。	影響なし。VMはテイクオーバー中にI/Oを一時的に停止します。
サイトBに障害が発生	クラスタAは引き続きデータを提供します。サイトBが復旧すると、レプリケーションが再開されます。	サイトAのノードとQDeviceはクォーラムを維持します。HAは、サイトAのノード上でサイトBのVMを再起動します。
サイト間リンクの障害	クラスタAは引き続きデータを提供します。フェイルオーバーは発生しません。	タイブレーカーがプライマリクラスタと一致した場合、QDeviceはサイトAパーティションに投票します。サイトBのノードはクォーラムを失って自己フェンシングを行い、HAはサイトAでそれらのVMを再起動します。
サイトCに障害が発生するか、クラスタがNetApp Consoleへのアクセスを失う	レプリケーションはデータ損失なしで継続されますが、メディアエーターが利用可能になるまでは、自動および計画的なフェイルオーバーは実行できません。ONTAP Cloud Mediatorを使用する場合、サイトCの障害はQDeviceにのみ影響します。	クラスターは、4つのノードの投票によってクォーラムを維持します。影響を受けるVMはありません。
1つのProxmox VEノードで障害が発生	影響はありません。	HAは、そのノード上のVMを他のノード上で再起動し、同じサイト内のノードを優先します。

ストレージシステム障害

ストレージシステム障害は、ホストレベルのHAだけでは対処できないケースであり、SnapMirrorアクティブ同期がサービスプロバイダに最大の価値をもたらすケースでもあります。次の図は、NFS共有ストレージを使用するすべてのProxmox VEノードがオンライン状態を維持している間にAFFクラスタAに障害が発生したあとの状態を示しています。



1. AFFクラスターAが利用できなくなります。サイトAのProxmox VEノードは稼働し続けるため、クラスターはクォーラムを失わず、HAもどのノードもフェンスしません。
2. メディエーター（サイトCのONTAP Mediator、またはNetApp ConsoleのONTAP Cloud Mediator）がクラスターAに到達できないことを確認すると、ONTAPは同じNFS LIFアドレス、ボリューム、エクスポートポリシーを使用してクラスターBのセカンダリSVMをアクティブ化します。
3. すべてのProxmox VEノードは、同じ共有ストレージ上でI/Oを再開します。サイトBのノードはローカルでクラスターBに接続し、サイトAのノードはサイト間ネットワークを介してクラスターBに接続します。VMはフェイルオーバー中にI/Oを一時停止し、再起動せずに実行を継続します。

クラスターAが復旧すると、レプリケーションが再開されます。サイトAのVMが再びローカルストレージにアクセスできるように、メンテナンス期間中にクラスターAへのフェイルバックを計画してください。

サイト障害

サイト障害時には、そのサイトのストレージシステムとProxmox VEノードの両方がオフラインになります。ONTAPは共有ストレージを稼働中のクラスターにフェイルオーバーし、Proxmox VE HAは表に示されているように、障害が発生したサイトのVMを稼働中のノードで再起動します。

SnapMirror active sync と MetroCluster の選択

NetApp MetroCluster構成は、Proxmox VEストレッチクラスターに対してRPOゼロと自動リカバリも提供します。この2つのソリューションは、保護する対象が異なります：

- *MetroClusterはすべてのワークロードを保護します。*MetroClusterは、アレイベースのクラスタリングと同期レプリケーションを組み合わせます。ミラーリングされたすべてのアグリゲート内のデータ、不揮発性メモリ（NVRAM）、および各SVMの構成をパートナーサイトにミラーリングするため、ワークロードごとのセットアップなしでクラスター上のすべての共有ストレージが保護されます。

- *SnapMirror active syncは、ワークロードの一部を保護します。*保護するSVMまたはボリュームを選択し、それぞれを独立してフェイルオーバーできます。保護されていないワークロードは、同じクラスタを共有できます。

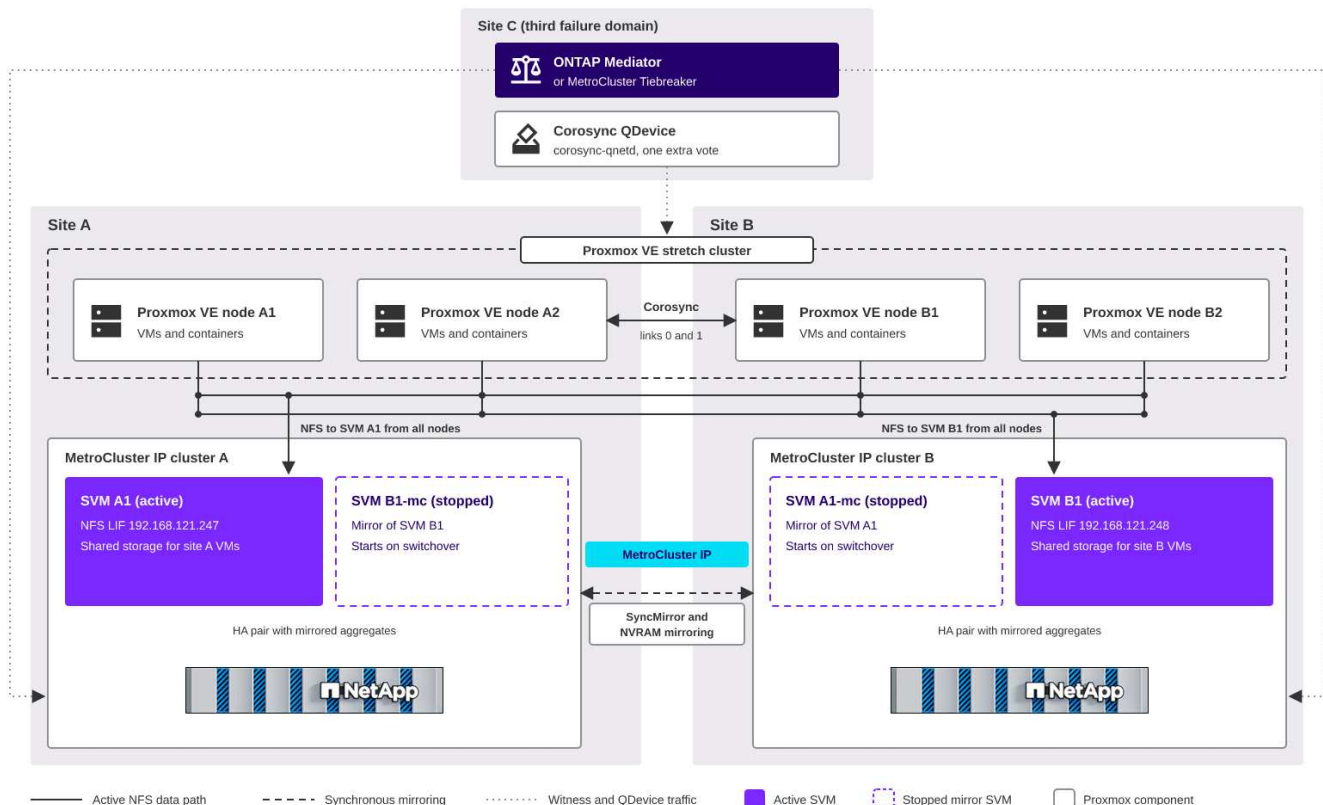
どちらのソリューションも、保護対象データの完全なコピーを各サイトに保持し、第3の障害ドメインに監視サーバーを必要とし、ストレージコントローラにレプリケーション負荷を追加します。これらは、保護範囲、フェイルオーバーの粒度、およびクラスタ設計において異なります。



いずれかのソリューションを導入する前に、ONTAPのバージョン、MetroClusterまたはSnapMirrorアクティブ同期構成、およびProxmox VEのバージョンが"[NetApp Interoperability Matrix Tool \(IMT\)](#)"と一緒に記載されていることを確認してください。

Proxmox VEを使用したMetroClusterアーキテクチャ

次の図は、4ノードのMetroCluster IP構成とNFS共有ストレージを備えたProxmox VEストレッチクラスタを示しています。



MetroCluster IPクラスタ

各サイトには、ミラーリングされたアグリゲートを備えたHAペアがあります。MetroCluster IPバックエンドネットワークは、データ（SyncMirror）とNVRAMをパートナーサイトに同期的にミラーリングします。

両サイトのSVM

各サイトは独自のSVMを提供できます。各SVMについて、MetroClusterは、パートナーサイトに同じ構成とLIFアドレスを持つ、`-mc`サフィックスが付いた停止状態のミラーSVMを保持します。

すべてのノードからのNFSアクセス

Proxmox VEの各ノードは、アクティブなSVMであるSVM A1とSVM B1の両方の共有ストレージをマウントするため、HA機能によりどのノード上のどのVMでも再起動できます。サイトBのノードはサイト間ネットワークを介してSVM A1に到達し、サイトAのノードはSVM B1に到達します。これは、SnapMirrorアクティブ同期と同じアクセスモデルです。

スイッチオーバー

サイト障害が発生した場合、サイトCのONTAP MediatorまたはMetroCluster Tiebreakerによって自動スイッチオーバーが有効になります。稼働中のサイトのミラーSVMが起動して同じNFSアドレスですべての共有ストレージを提供し、Proxmox VE HAが障害が発生したサイトのVMを再起動します。単一のコントローラ障害は、スイッチオーバーを行わずに、ローカルHAのテイクオーバーによって処理されます。障害が発生したサイトを修復したあと、アグリゲートを修復してスイッチバックします。

MetroClusterが障害に対応する仕組み

次の表は、MetroCluster IP構成とProxmox VEストレッチクラスタが、[\[ソリューションが障害にどのように対応するか\]](#)と同じ障害にどのように対応するかを示しています。この例では、SVM A1はサイトAでアクティブであり、SVM B1はサイトBでアクティブです。

イベント	ONTAPの動作	Proxmox VEの動作
サイトAに障害が発生	ONTAP MediatorまたはMetroCluster Tiebreakerが障害を確認し、ONTAPがサイトAをスイッチオーバーします。SVM A1-mcは、同じNFS LIFアドレスを使用してサイトBで起動します。SVM B1はデータの提供を継続します。	サイトBのノードとQDeviceはクォーラムを維持します。HAはサイトAのノードをフェンスし、サイトBのノード上でそれらのVMを再起動します。サイトBのノードで既に稼働していたVMは引き続き稼働し、SVM A1上のVMは切り替え後にI/Oを再開します。
MetroCluster IPクラスタAに障害が発生しても、サイトAのProxmox VEノードは引き続き稼働する	ONTAP MediatorまたはMetroCluster Tiebreakerは、クラスターAに到達できないことを確認し、ONTAPはサイトAをスイッチオーバーします。SVM A1-mcは、同じNFS LIFアドレスでサイトBで起動します。	クォーラムの変更もVMの再起動もありません。SVM A1上のVMはスイッチオーバー後にI/Oを再開し、サイトAのノードはサイト間ネットワークを介してサイトBに到達します。
サイトAのコントローラ1台が故障	サイトAのHAパートナーがローカルHAテイクオーバーでテイクオーバーします。スイッチオーバーは発生しません。	影響なし。VMはテイクオーバー中にI/Oを一時的に停止します。
サイトBに障害が発生	ONTAPはサイトBをスイッチオーバーします。SVM B1-mcは、同じNFS LIFアドレスを使用してサイトAで起動します。SVM A1はデータの提供を続けます。	サイトAのノードとQDeviceはクォーラムを維持します。HAはサイトAノード上でサイトBのVMを再起動し、サイトAにあるSVM B1にアクセスします。
サイト間リンクの障害	両方のクラスタがまだ稼働しているため、スイッチオーバーは発生しません。各サイトは引き続き独自のSVMを提供し、リンクが復旧するまでパートナーサイトへのミラーリングは一時停止されます。	タイブレーカーがサイトAと一致した場合、QDeviceはサイトAパーティションに投票します。サイトBノードはクォーラムを失い、自己フェンス状態になります。HAは、サイトAノード上のSVM A1でVMを再起動します。サイトAのノードがSVM B1に到達できないため、リンクが復旧するまでSVM B1上のVMは再起動できません。

イベント	ONTAPの動作	Proxmox VEの動作
サイトCで障害が発生	ミラーリングはデータ損失なしで継続されますが、Witnessが利用可能になるまで自動スイッチオーバーはできません。手動でスイッチオーバーすることは可能です。	クラスターは、4つのノードの投票によってクォーラムを維持します。影響を受けるVMはありません。
1つのProxmox VEノードで障害が発生	影響はありません。	HAは、そのノード上のVMを他のノード上で再起動し、同じサイト内のノードを優先します。

サイト間のリンク障害は、プライマリサイトが1つだけの設計との主な違いです。両方のサイトでアクティブなSVMがホストされている場合、MetroClusterまたは2つのSnapMirrorアクティブ同期SVMが反対方向に動作している場合、corosyncタイブレーカーは1つのサイトのみを優先できます。アクティブなSVMが別のサイトにあるVMは、リンクが復旧するまでダウンしたままになります。影響を最小限に抑えるため、冗長なサイト間リンクを別々の物理パスで使用し、最も重要なVMを、タイブレーカーが優先するサイトのSVM上に配置してください。

機能比較

考慮事項	SnapMirror NAS 向けアクティブシンク	MetroCluster IP
保護範囲	選択されたSVMとボリューム	構成内のすべてのミラーリングされたアグリゲートとすべてのSVM
フェイルオーバーの粒度	各SVMは独立して	スイッチオーバーによるサイト全体
保護されていないワークロード	同じクラスタ内の保護されていないSVM上で実行する	ミラーリングされていないアグリゲートを使用できます。これらは切り替え後にオフラインになり、オンラインに戻すまでオフライン状態になります。
クラスタ設計	IPネットワークを介してピアリングされた2つの独立したクラスタ	専用のMetroCluster IPバックエンド ネットワークを備えた2つのパートナー クラスターの1つの構成
サイトCのWitness	ONTAP MediatorまたはONTAP Cloud Mediator	ONTAP MediatorまたはMetroCluster Tiebreaker
保護されたデータのコピー	各サイトに1つずつ	各サイトに1つずつ、ミラーリングされたアグリゲート内
レプリケーションパス	クラスタ間LIFを介したSnapMirror同期	SyncMirror と NVRAM ミラーリング (MetroCluster IP バックエンド ネットワーク経由)
両サイトのNFSアドレス	拡張レイヤ2 VLAN。BGP対応VIP LIF (認定待ち)	拡張レイヤー2 VLAN、またはBGPを使用したVIP LIF
サイト障害後のリカバリ	各SVMをフェイルバックする	アグリゲートを修復してから、サイトをスイッチバックしてください

選定ガイダンス

- ストレージ上のすべての、またはほぼすべてのワークロードでRPOをゼロにする必要がある場合

は、MetroClusterを選択してください。たとえば、企業がクラスタ上でミッションクリティカルなVMのみを実行している場合や、サービスプロバイダがすべてのテナントに同じ可用性階層を提供している場合などです。ワークロードごとの設定なしで、1つの保護ドメインが提供されます。

- 一部のテナント向けのプレミアム階層など、ワークロードのサブセットのみにRPOゼロが必要な場合、または一度に1つのテナントまたはアプリケーションに対してフェイルオーバーやディザスタリカバリのテストを行う必要がある場合は、SnapMirror active syncを選択してください。
- NAS向けのSnapMirrorアクティブ同期は、MetroCluster構成ではサポートされていません。クラスタの各ペアには、いずれか1つのソリューションを使用してください。
- このソリューションにおけるcorosync、QDevice、およびHAに関するガイダンスは、どちらにも適用されます。MetroClusterを使用する場合、サイト間リンクに障害が発生したときにデータの提供を継続するサイトにQDeviceタイブレーカーを合わせ、HAノードアフィニティルールを使用してVMをアクティブなSVMと同じサイトに維持します。
- MetroCluster IPは、サイト間のレイヤ3ネットワーク向けにBGPを使用したVIP LIFもサポートしています。

Proxmox VEストレッチクラスタにおけるCorosyncに関する考慮事項

Proxmox VEは、クラスタメンバーシップとクォーラムにcorosyncを使用します。Corosyncは、SnapMirror active syncよりもサイト間ネットワークの影響を受けやすいため、まずクラスタネットワークを計画してください。

レイテンシとネットワーク設計

- SnapMirrorアクティブ同期には、クラスタ間の往復時間（RTT）が10 ms未満である必要があります。Proxmoxは、すべてのノード間のcorosyncレイテンシを5 ms未満にすることを推奨しているため、corosyncの要件がソリューションの距離制限を決定します。
- Corosyncは、高い帯域幅よりも、低く安定したレイテンシを必要とします。ストレージのバーストによってcorosyncのタイムアウトが発生しないように、ストレージやライブマイグレーションのトラフィックとは別に、corosync専用のネットワークを使用してください。
- サイト間の別々の物理パス上に、少なくとも2つのcorosyncリンク（例えば、リンク0とリンク1）を設定してください。CorosyncはKronosnetを使用して、いずれかのパスに障害が発生した場合に自動的にリンクを切り替えます。

第三サイトのQDeviceとのクォーラム

Proxmox VEノードをサイトAとサイトBに均等に分散させ、サイトCにQDeviceを追加します。4つのノードと1つのQDeviceでクラスタは5票を持ち、クォーラムには3票が必要となるため、どちらかのサイトで障害が発生してもクォーラムは失われません。QDeviceはTCPポート5403経由でクラスタに接続し、corosyncのような低レイテンシの要件がないため、サイトCをONTAP Mediatorと共有できます。ONTAP Cloud Mediatorを使用する場合でも、QDevice用に3つ目の場所が必要になりますが、Mediatorをホストしない小規模なLinuxホストを使用することもできます。

プライマリクラスタとのタイブレーカーアライメント

サイト間リンクに障害が発生しても、両方のサイトがサイトCに到達できる場合、ONTAPはサイトAのプライマリクラスタでデータの提供を継続します。QDeviceは同じサイトに投票する必要があります。デフォルトでは、QDeviceはノードIDが最も小さいパーティションを選択します。

ベストプラクティス： サイトAのノードでProxmox VEクラスタを作成し、サイトBのノードを参加させる前

に他のサイトAのノードを参加させて、サイトAが最も小さいノードIDを保持するようにします。プライマリストレージが長期間サイトBに移動する場合は、QDevice `tie\_breaker` の設定をサイトBのノードIDに更新します。

QDeviceがサイトBを優先した場合、サイトAのノードは自己フェンスを行い、HAはサイトAのアクティブストレージにアクセスできないサイトBノード上のVMを再起動します。

HAの動作とVMの配置

- Proxmox VE HAは通常、障害が発生したノードを検出し、60秒のウォッチドッグフェンシングタイムアウトを含めて約2分でVMを復旧します。サイト障害時には、SnapMirror active syncのフェイルオーバーとProxmox VE HAのリカバリが並行して実行されます。
- HA ノードアフィニティルールとノード優先度を使用して VM をプライマリストレージと同じサイトのノードに配置し、別のサイトにフェイルオーバーできるようにします。
- サイトのフェイルオーバー後、ストレージをフェイルバックするまで、影響を受けるVMのHA `failback` プロパティを `0` に設定します。そうしないと、アクティブなストレージがまだサイトBにあるにもかかわらず、サイトAのノードが復旧し次第、HAがVMをサイトAのノードに移行してしまいます。
- ゲストOSのディスクタイムアウトを、想定されるフェイルオーバー時間よりも長く設定してください。そうすることで、ストレージフェイルオーバー中にゲストOSがI/Oエラーを報告しなくなります。

Proxmox用ストレージマネージャーとの統合

Storage Manager for Proxmox (SMP) は、Proxmox VE 管理者に、ONTAP 共有ストレージをプロビジョニングし、ONTAP スナップショットと FlexClone テクノロジーを使用して VM のバックアップ、リストア、クローン作成を行うための単一のインターフェイスを提供します。SMP は API を介して Proxmox VE クラスタおよび ONTAP に接続するため、Proxmox VE ノードにエージェントを配置する必要はありません。

SMPとSnapMirror active syncは、異なる種類の障害から保護します。SnapMirror active syncは、ストレージ障害やサイト障害が発生してもVMの実行を継続させますが、誤った削除、ゲストの更新失敗、ランサムウェアによって暗号化されたデータなど、すべての書き込みを同期的にレプリケートします。SMPスナップショットは、これらの論理障害からリカバリするためのポイントインタイムコピーを提供します。これらを組み合わせることで、同じONTAPストレージから継続的な可用性と迅速な運用リカバリを提供します。

保護層	から保護します	リカバリ ポイント	管理元
SnapMirrorアクティブ同期	ストレージシステム障害およびサイト障害	データ損失ゼロ	ONTAP
SMPバックアップ (ONTAPスナップショット)	誤削除、データ破損、アップデートの失敗、ランサムウェア	最後にスケジュールされた、またはオンデマンドのバックアップ	SMP
SnapMirror非同期フェイルアウトまたはProxmox Backup Server	両サイトの喪失と長期保持	最後のレプリケーションまたはバックアップ	ONTAPまたはProxmox Backup Server

バックアップとリカバリ

SMPは、オンデマンドまたはポリシーに基づいて、ストレージボリュームのONTAPスナップショットとして「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態またはファイル整合性のあるバックアップを作成し、個々のVM、ストレージ、またはリソースグループを復元します：

- リソースグループとバックアップポリシーを使用して、テナントまたはアプリケーションの仮想マシンに同じスケジュールと保持期間を適用します。
- QEMUゲストエージェントを実行するVMにはファイル整合性バックアップを使用し、ONTAPがスナップショットを作成する前にゲストファイルシステムが静止されるようにします。
- SMPはアクティブなストレージを管理します。SnapMirrorアクティブ同期のフェイルオーバー後、バックアップまたはリストア操作を実行する前に、SMPで検出を実行してストレージをクラスタBにマッピングします。
- 2つのサイト以外の3番目のコピー、またはより長い保存期間が必要な場合は、保護対象ボリュームからSnapMirror非同期ファンアウト関係を追加するか、Proxmox Backup Serverを使用してください。
- 改ざん防止スナップショットはSnapMirrorアクティブ同期ではサポートされていないため、保護対象ボリュームのSMPでスナップショットロックを有効にしないでください。

VMのクローニング

SMPは、ONTAP FlexCloneテクノロジーを使用して、開発、テスト、および迅速なプロビジョニングのためのスペース効率に優れたVMクローンを作成します。保護されたストレージに作成したクローンは、両方のサイトでレプリケーションの帯域幅と容量を消費します。ビジネス継続性を必要としないクローンやテストストレージは、SnapMirrorアクティブ同期保護から除外してください。

SMPの配置

- ストレージまたはサイト障害の発生後もSMPを引き続き利用できるように、SnapMirrorアクティブ同期で保護された共有ストレージ上のHAリソースとしてSMP VMを実行します。
- SMPがどちらのサイトのアクティブストレージにもアクセスできるように、SMPにProxmox VEクラスタと両方のONTAPクラスタを登録します。

NAS向けSnapMirror active syncを備えたNFS共有ストレージ

ONTAP 9.19.1以降、SnapMirrorアクティブ同期はNASワークロードを保護します。以下の考慮事項は、NFS共有ストレージにのみ適用されます。NFSストレージを使用してソリューションを導入するには、["NASの設定ワークフロー"](#)に従ってください。

SVMレベルの保護とネットワークID

- SnapMirror active sync for NASは、ストレージVM (SVM) 全体を保護します。SVM内のすべてのボリュームを保護することも、選択したボリュームを除外することもできます。サポートされるのはFlexVolボリュームのみであり、SVMにLUNを含めることはできません。
- セカンダリSVMは、フェイルオーバーが発生するまで、LIFがダウンした状態で休止状態を維持します。ONTAPは、LIF IPアドレス、エクスポートポリシー、NFS設定などのSVM構成を複製するため、フェイルオーバー後もセカンダリSVMは同じNFSエンドポイントを提供します。
- NFSv3以降では、フェイルオーバーは中断を伴いません。
- SnapMirror NASのアクティブ同期はアクティブ / パッシブであるため、サイトBノード上のVMは、サイト間ネットワークを介してプライマリSVMとの間で読み書きを行います。両サイトでアクティブなワークロードを実行する場合は、レプリケーション方向が逆の2つのSVMを使用し、各サイトに1つずつプライマリSVMを配置し、各VMのノードアフィニティルールをプライマリSVMのサイトに合わせます。
- NAS向けSnapMirrorアクティブ同期は、AFF AシリーズおよびCシリーズの2ノードクラスタでサポートされています。

NFSクライアント設定

NFSストレージにはNFSv3またはNFSv4.1を使用してください。デフォルトのハードマウント動作を維持し、フェイルオーバー中にNFS I/Oが失敗する代わりに再試行されるように、`soft`マウントオプションは追加しないでください。

パフォーマンスと耐障害性を向上させるため、ストレージへのTCP接続を複数使用してください。nConnectまたはセッションランキングのいずれかを使用し、両方は使用しないでください：

- ***nConnect.***単一の NFS LIF アドレスへの複数の TCP 接続を開きます（例：nconnect=4）。nConnect は NFSv3 および NFSv4.1 と単一の VIP LIF アドレスで動作するため、レイヤ 3 ネットワークを含む NAS 向け SnapMirror アクティブ同期に推奨されるオプションです。
- ***セッションランキング。***複数のデータLIFを1つのNFSv4.1セッションにグループ化します（たとえば vers=4.1, trunkdiscovery, max_connect=16）。セッションランキングにはNFSv4.1以降が必要です。保護対象のSVMに、拡張レイヤー2ネットワークなど、クライアントが両方のサイトからアクセスできる複数のデータLIFがある場合にのみ使用してください。詳細については、["NFSランキング"](#)を参照してください。

マウントオプションのコマンドと検証手順については、["Proxmox VEのNFSストレージを構成する"](#)を参照してください。

SMPを使用したNFSストレージ プロビジョニング

SMPはONTAPボリュームをプロビジョニングし、エクスポートポリシーを作成または選択して、選択したProxmox VEノードにNFS共有ストレージとしてボリュームをマウントします。保護されたSVM内のストレージの場合：

- プライマリSVMにボリュームをプロビジョニングし、NFS LIF、またはレイヤー3ネットワークの場合はVIP LIFを優先LIFとして選択します。セカンダリSVMはフェイルオーバー後も同じアドレスを使用するため、ストレージ定義は有効なまま維持されます。
- HAがどのノードでもVMを再起動できるように、両サイトのすべてのProxmox VEノードにストレージをマウントしてください。
- エクスポートポリシーで、両サイトのProxmox VEノードが許可されていることを確認してください。ONTAPはエクスポートポリシーをセカンダリSVMに複製します。
- プロビジョニング後、ボリュームがSnapMirrorアクティブ同期保護に含まれていることを確認します。

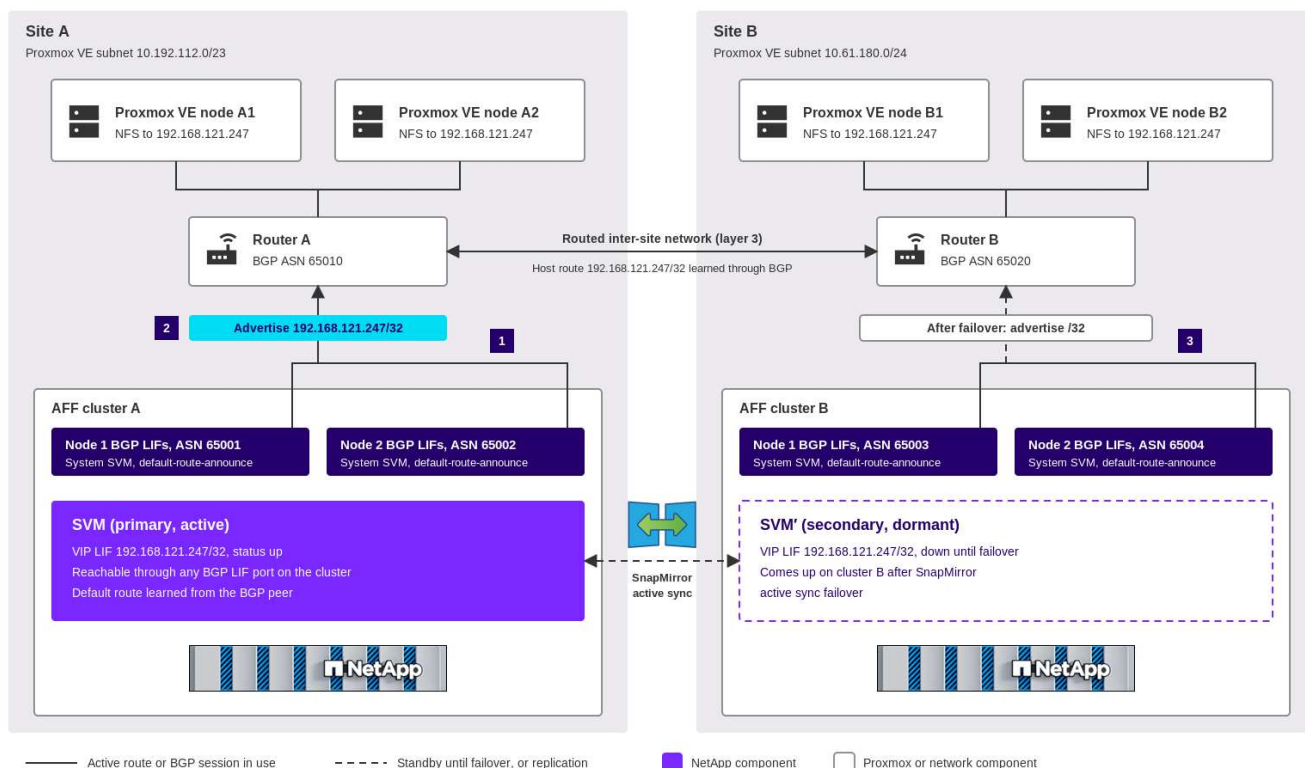
VIP LIFとBGPを備えたレイヤ3ネットワーク

SnapMirrorのNAS向けアクティブ同期には、プライマリSVMとセカンダリSVMで同じIPアドレスが必要です。NFS VLANがサイト間で拡張されている場合、LIF IPアドレスはSVMとともに移動します。サイトがルーティングされたレイヤ3ネットワークで接続されている場合、サイトAのLIFのサブネットはサイトBには存在しません。



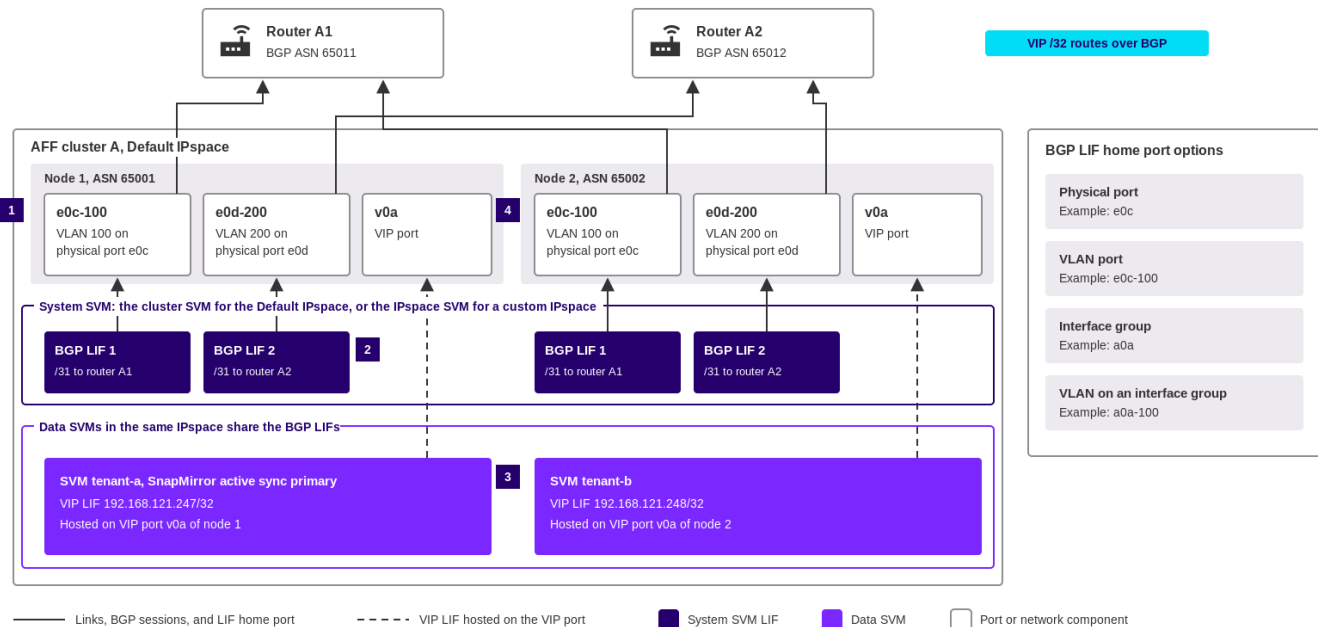
発行時点では、NetApp は NAS 向け SnapMirror アクティブ同期の認定構成として、BGP を使用した VIP LIF を文書化していません。レイヤ 3 設計を計画する前に、NetApp に現在のサポート状況を確認してください。それ以外の場合は、サイト間で NFS VLAN を拡張してください。MetroCluster IP 構成は、BGP を使用した VIP LIF をサポートしています。

ONTAP仮想IP (VIP) LIFはこの問題を解決します。VIP LIFはどのサブネットにも属しません。ONTAPは、ボーダーゲートウェイプロトコル (BGP) を使用してVIPアドレスを/32ホストルートとしてピアルータにアドバタイズするため、VLANを拡張することなくアドレスをサイト間で移動させることができます。



1. 両サイトの各ノードは、システムSVM内にBGP LIFを持ち、それぞれのサイトのルーターとピアリング接続を確立しています。BGP LIFはノード固有のものであり、複製されないため、両方のクラスタで設定する必要があります。
2. プライマリSVMはNFS VIP LIFをホストします。クラスターAは/32ホストルートをアドバタイズし、両サイトのProxmox VEノードはルーティングされたネットワークを介してストレージにアクセスします。
3. SnapMirrorアクティブ同期フェイルオーバーが発生したあと、セカンダリSVM上でVIP LIFが起動し、クラスターBがホストルートをアドバタイズし、ルーターがサイトBに収束します。

ONTAPで初めてBGPを計画する際、どのSVMが各LIFを所有しているかを知っておくと役立ちます。BGP LIFは、データSVMではなく、IPspaceのシステムSVMに属します。各クラスタ上の1組のBGP LIFが、そのIPspace内のすべてのデータSVMのVIP LIFを処理するため、テナントごとにBGP LIFを作成する必要はありません。次の図は、VLANポート上にBGP LIFが配置された、1つのクラスタにおけるLIFとポートのレイアウトを示しています。



1. 各ノードにはBGP用のポートが2つあります。この例ではVLANポート `e0c-100` および `e0d-200` です。各ポートはそれぞれ異なるルーターに直接接続されます。
2. 各ノードはシステムSVM内に2つのBGP LIFを持ち、各ポートに1つずつ配置され、/31サブネットと1つのルーターへのBGPピアグループが設定されています。デフォルトのIPspaceの場合、システムSVMはクラスターSVMです。カスタムIPspaceの場合、IPspaceと同じ名前のSVMです。
3. 同じIPspace内のデータSVMはVIP LIFをホストし、独自のBGP LIFは必要ありません。BGPピアグループは、IPspace内のすべてのSVMに対してVIPルートをアドバタイズします。
4. 最初のBGPピアグループを作成すると、ONTAPは各ノードにVIPポート（たとえば `v0a` など）を作成します。VIP LIFはVIPポートでホストされ、IPspace内でBGP LIFをホストするノード上のすべてのポートからアクセスできます。

BGP LIFのホームポートは、物理ポート、VLANポート、インターフェースグループ、またはインターフェースグループ上のVLANのいずれかになります。インターフェースグループは必須ではありません。NetApp技術報告書TR-4949では、各IPspaceに対して2つの別々のポートに2つのBGP LIFを設定し、それぞれを異なるファーストホップルーターに直接接続することを推奨しています。

次のガイドラインに注意してください。

- BGP LIFはフェイルオーバーしません。冗長性は、ノードごとに2つのBGP LIFが存在し、それぞれが異なるルーターとピアリングすることで実現されます。ノードがSVMのすべてのBGPセッションを失った場合、ONTAPはVIP LIFを、そのSVMに対してアクティブなBGPセッションを持つ別のノードに移動します。
- 各ONTAPノードと各ルーターに、固有のプライベート自律システム番号（ASN）を持つ外部BGP（eBGP）を使用します。
- 各BGP LIFとそのルーターには、/31サブネット（ネットマスク255.255.255.254）を使用してください。奇数番のアドレスをBGP LIFに、偶数番のアドレスをルーターに割り当ててください。
- ONTAPはルーターからのルート进行处理しません。ONTAPからの/32ホストルートを受け入れ、クラスターにルート更新を送信しないようにルーターを設定します。
- Proxmox VEノードは、VIPアドレスと同じサブネットを共有してはなりません。ノードとストレージ間の

経路には、例えばVRRPやHSRPを備えた冗長なレイヤー3ルーターを設置する必要があります。

- 各クラスタがローカルルータからデフォルトルートを学習するように、`-use-peer-as-next-hop true`を使用してBGPピアグループを設定します。サイトAのゲートウェイを指すルートは、フェイルオーバー後のサイトBでは無効になります。
- マルチパスルーティングを有効にして、送信VIPトラフィックが利用可能なすべてのBGP LIFポートを使用するようにします。
- BGPのホールド時間をデフォルトの180秒から短縮します。TR-4949では、3秒のホールド時間を推奨しています。ルーターが障害の発生したクラスターからルートを取り消すのは、ホールドタイマーが満了したときのみであり、ストレージシステム障害の発生中もサイトAのルーターはオンライン状態を維持します。

関連情報

- ["ONTAP SnapMirror アクティブ同期アーキテクチャ"](#)
- ["ONTAP SnapMirror Active Syncの前提条件"](#)
- ["ONTAP Cloud Mediatorの設定準備"](#)
- ["SnapMirror アクティブ同期用に ONTAP Cloud Mediator を設定する"](#)
- ["ONTAP MetroCluster仮想IPとBGPに関する考慮事項"](#)
- ["MetroClusterデータ保護と災害復旧"](#)
- ["Proxmox用Storage Managerの設定と使用"](#)
- ["TR-4949：データセンターにおけるONTAPでのBGP/VIP"](#)
- ["Proxmox VEクラスタ マネージャ"](#)
- ["Proxmox VEの高可用性"](#)

Proxmox VEのビジネス継続性をNASストレージで構成する

ONTAP SnapMirror active sync for NASとProxmox VEストレッチクラスタを組み合わせることで、Proxmox仮想環境（VE）VMをサイト障害から保護します。NetApp Consoleでメディエーター（ONTAP MediatorまたはONTAP Cloud Mediator）を設定し、NFSストレージVM（SVM）を保護し、必要に応じて仮想IP（VIP）LIFとBorder Gateway Protocol（BGP）を使用してルーティングされたネットワーク全体でNFSアドレスをポータブルにし、QDeviceを使用してストレッチクラスタを構築してから、Storage Manager for Proxmoxを使用して共有ストレージをプロビジョニングし、高可用性（HA）とVMバックアップを構成します。その結果、データ損失はゼロとなり、生存サイトでのVMの自動復旧が実現します。

このワークフローについて

始める前に、["ソリューション アーキテクチャ、障害時の動作、およびcorosync設計上の考慮事項"](#)を確認してください。`<primary\_svm>`などの山括弧内の値を、環境に合わせた値に置き換えてください。

開始する前に

- サイトAに1つ、サイトBに1つの、計2つのAFF A-SeriesまたはC-Seriesの2ノードクラスタで、ONTAP 9.19.1以降を実行している必要があります。

- ONTAP Oneに含まれるSnapMirrorおよびSnapMirror同期ライセンスを、両方のクラスタにインストールする必要があります。
- クラスタはデフォルトのIPspaceでピアリングされている必要があります、クラスタ間の往復時間（RTT）は10 ms未満でなければなりません。
- 調停者オプションを1つ選択する必要があります。比較については、"[Mediatorオプション](#)"を参照してください。
 - ONTAP Mediatorの場合、LinuxホストをサイトC、または別の第3の障害ドメインにインストールし、両方のクラスタのクラスタおよびノード管理LIFからアクセスできるようにする必要があります。
 - ONTAP Cloud Mediatorの場合、両方のクラスタからNetApp ConsoleへのアウトバウンドHTTPSアクセス（直接またはプロキシ経由）が必要であり、ping遅延は200ms未満である必要があります。また、NetApp Consoleの組織と、サービスアカウントを作成する権限も必要です。
- サイトAのSVMは、Proxmox VEノードにNFSを提供する必要があります。SVMには、LUNを含まないNAS用のFlexVolボリュームのみを含める必要があります、そのエクスポートポリシーではすべてのProxmox VEノードを許可する必要があります。
- Proxmox VE 9.0以降のノードを偶数個インストールし、サイトAとサイトBに均等に分散させ、すべてのノード間のcorosyncレイテンシを5ms未満にする必要があります。
- サイトC、または別の第3の場所にあるLinuxホストは、corosync QDeviceデーモンに使用でき、すべてのProxmox VEノードからTCPポート5403でアクセス可能である必要があります。どちらのメディエーターオプションを使用する場合でも、このホストが必要です。
- NFS VLANは、サイトAとサイトBの間でストレッチする必要があります。ルーテッドレイヤ3ネットワークの場合は、各サイトにBGP対応ルータが必要です。また、BGPを使用するVIP LIFがNAS向けSnapMirrorアクティブ同期でサポートされているかどうかをNetAppに確認する必要があります。
- ONTAPおよびProxmox VEのバージョンが、"[NetApp Interoperability Matrix Tool \(IMT\)](#)"と一緒に記載されている必要があります。
- 共有ストレージをプロビジョニングしてVMをバックアップするには、Proxmox VEノードと両方のONTAPクラスタへのネットワーク アクセスが可能な状態でStorage Manager for Proxmoxをインストールする必要があります。

ステップ1：メディエーターを設定する

SnapMirrorアクティブ同期関係を初期化する前に、クラスタ ピア関係にメディエーターを追加します。ONTAPが計画的および自動フェイルオーバーを実行するには、メディエーターが必要です。メディエーターはどちらのクラスタからでも追加でき、ONTAPがもう一方のクラスタに自動的に追加します。メディエーターのオプションは1つだけ使用し、両方は使用しないでください。

次のいずれかのオプションを選択します。

ONTAP Mediator

サイトCのLinuxホストにメディエーターをインストールする場合は、このオプションを使用してください。インストールについては、"[ONTAPメディエーターをインストールまたはアップグレードする](#)"を参照してください。

手順

1. いずれかのクラスタで、メディエーターを追加します：

```
snapmirror mediator add -peer-cluster <peer_cluster> -type on-prem  
-mediator-address <mediator_ip> -username <mediator_user>
```

プロンプトが表示されたら、メディエーターのパスワードを入力してください。

2. メディエーターが接続されており、クォラムのステータスが `true` であることを確認します：

```
snapmirror mediator show
```

ONTAP Cloud Mediator

このオプションを使用して、メディエーターをNetApp Consoleのサービスとしてホストすることで、第3のサイトにメディエーターホストを用意する必要がなくなります。

開始する前に

- 両サイトのファイアウォールで、両方のクラスタからNetApp Console APIエンドポイントへのHTTPSトラフィックを許可する必要があります。現在のエンドポイントのホスト名については、["ONTAP Cloud Mediatorの設定準備"](#)を参照してください。
- クラスタがプロキシ サーバを使用している場合は、プロキシのIPアドレス、ポート、およびクレデンシャルを用意してください。各クラスタには異なるプロキシ サーバを使用してください。プロキシのルートCA証明書がONTAPにインストールされている必要があります。
- ONTAPにはよく知られているルートCA証明書が含まれているため、通常はNetApp Console証明書をインストールする必要はありません。確認するには、次を実行します `security certificate show -common-name Sectigo*|USERTrust*|AAA*`。

手順

1. NetApp Consoleで、組織IDをコピーします。
2. NetApp Consoleで、メンバーサービスアカウントを作成します：
 - a. 組織を、ONTAP Cloud Mediatorを使用する組織に設定します。
 - b. カテゴリを*アプリケーション*に設定します。
 - c. 役割を*ONTAP Mediator Setup Role*に設定します。
 - d. アカウントを作成する際に、クライアントIDとクライアントシークレットを保存してください。
3. いずれかのクラスタで、メディエーターを追加します：

```
snapmirror mediator add -peer-cluster <peer_cluster> -type cloud  
-org-id <console_org_id> -service-account-client-id <client_id> -use  
-http-proxy-local <true|false> -use-http-proxy-remote <true|false>
```

プロンプトが表示されたら、クライアントシークレットを入力してください。

System Managerを使用することもできます。保護 > 概要 > メディエーター > *追加*を選択し、メディエーターの種類として*クラウド*を選択して、組織ID、クライアントID、およびクライアントシークレットを入力します。

4. メディエーターのタイプが `cloud`、接続ステータスが `connected`、クォーラムのステータスが `true`であることを確認します：

```
snapmirror mediator show
```

ステップ2：SnapMirrorアクティブ同期を使用してNFS SVMを保護する

サイトBクラスタ上に休止状態の宛先SVMを作成し、サイトAのSVMをそこに複製します。ONTAPはデータを同期的に複製し、NFS LIFアドレスやエクスポートポリシーを含むSVM構成も複製します。System Managerで、SVMに対して*保護*を選択し、`AutomatedFailOver`ポリシーを選択することで、この手順を完了することもできます。

手順

1. サイトBクラスタで、宛先SVMを作成します：

```
vserver create -vserver <secondary_svm> -sub-type dp-destination
```

2. サイトBクラスタで、プライマリSVMとのSVMピア関係を作成します：

```
vserver peer create -vserver <secondary_svm> -peer-vserver <primary_svm>  
-peer-cluster <site_a_cluster> -applications snapmirror
```

3. サイトAクラスタで、SVMピアリクエストを承認します：

```
vserver peer accept -vserver <primary_svm> -peer-vserver <secondary_svm>
```

4. サイトBクラスタで、SnapMirrorアクティブ同期関係を作成します：

```
snapmirror create -source-path <primary_svm>: -destination-path  
<secondary_svm>: -policy AutomatedFailOver
```

5. 関係を初期化します：

```
snapmirror initialize -destination-path <secondary_svm>:
```

6. 関係が同期していることを確認してください：

```
snapmirror show -destination-path <secondary_svm>:
```

`Mirror State`は `Snapmirrored`であり、 `Relationship Status`は `InSync`です。

7. 必要に応じて、スクラッチボリュームやテストボリュームなど、保護を必要としないボリュームを除外します：

```
volume modify -vserver <primary_svm> -volume <volume_name> -smas  
-protection unprotected
```

ステップ3：レイヤ3ネットワーク用にBGPを使用したVIP LIFを設定する



出版時点では、NetAppはNAS向けSnapMirrorアクティブ同期の認定構成としてBGPを使用したVIP LIFを文書化していません。この手順を完了する前に、NetAppに現在のサポート状況を確認してください。そうでない場合は、NFS VLANをサイト間で拡張し、この手順をスキップしてください。

NFS VLANがサイトAとサイトBの間で拡張されている場合は、この手順をスキップしてください。サイトがルーティングされたネットワークで接続されている場合は、両方のクラスタのすべてのノードにBGP LIFを作成し、プライマリSVMのVIP LIFにNFSアドレスをホストします。VIPアドレスは、Proxmox VEノードのサブネットに属してはいけません。

開始する前に

- 各ルータは、そのサイトのBGP LIFからのBGPセッションを受け入れ、/32ホストルートを受け入れ、ONTAPにルートアップデートを送信しないように設定する必要があります。
- 各ONTAPノードと各ルータは一意のプライベートASNを持つ必要があり、各BGP LIFとルータのペアは/31サブネットを持つ必要があります。

手順

1. 各クラスタで、高度な権限レベルに変更します：

```
set -privilege advanced
```

2. 両方のクラスタの各ノードで、ノードに一意のONTAP ASN、3秒のホールドタイム、およびルータIDとしてのノード管理IPアドレスを指定して、BGP設定を作成します：

```
network bgp config create -node <node_name> -asn <node_asn> -holdtime 3  
-routerid <node_mgmt_ip>
```

3. 必要に応じて、両クラスタの各ノードにおいて、ルータに接続する2つのポートそれぞれにVLANポートを作成します：

```
network port vlan create -node <node_name> -vlan-name <port_name>-
```

```
<vlan_id>
```

物理ポート、インターフェースグループ、またはインターフェースグループ上のVLANをBGP LIFホームポートとして使用することもできます。ポートはIPspace内のブロードキャストドメインに属している必要があります。

4. 両クラスタの各ノードにおいて、システムSVM内に2つのBGP LIFを作成します。各ポートに1つずつ作成し、そのポート上のルータへのサブネットを/31に設定します：

```
network interface create -vserver <system_svm> -lif <bgp_lif_name>  
-service-policy default-route-announce -home-node <node_name> -home-port  
<vlan_or_port> -address <bgp_lif_ip> -netmask-length 31
```

デフォルトのIPspaceの場合、`<system\_svm>`はクラスタ名です。カスタムIPspaceの場合は、IPspace名です。BGP LIFはノードごとに1回作成され、IPspace内のすべてのデータSVMのVIP LIFにサービスを提供します。

5. 各BGP LIFについて、そのルータとのBGPピアグループを作成し、そのルータからデフォルトルートを学習します：

```
network bgp peer-group create -peer-group <peer_group_name> -ipspace  
<ipspace> -bgp-lif <bgp_lif_name> -peer-address <router_ip> -peer-asn  
<router_asn> -use-peer-as-next-hop true
```

6. 各ピアグループが稼働していることを確認してください：

```
network bgp peer-group show -ipspace <ipspace>
```

7. 各クラスタで、マルチパスルーティングを有効にします：

```
network options multipath-routing modify -is-enabled true
```

8. サイトAクラスタで、プライマリSVMにNFS VIP LIFを作成します：

```
network interface create -vserver <primary_svm> -lif <vip_lif_name>  
-role data -data-protocol nfs -home-node <node_name> -address  
<vip_address> -is-vip true -failover-policy broadcast-domain-wide
```

9. サイトAのクラスタで、すべてのノードのプライマリSVMのBGPステータスが`up`であることを確認します：

```
network bgp vserver-status show
```

10. 両方のルーターで、VIPアドレスの/32ルートがクラスタAから学習されていることを確認してください。

ステップ4：QDeviceを使用してProxmox VEストレッチクラスタを作成する

サイトAのノードからクラスタを作成して、サイトAのノードに最小のノードIDが割り当てられるようにし、サイトCにQDeviceを追加します。サイト間リンクに障害が発生した場合、QDeviceはサイトAに投票権を与えます。これは、ONTAPがアクティブに維持するSVMと一致します。

手順

1. 最初のサイトAノードで、別々のネットワーク上に2つのcorosyncリンクを持つクラスタを作成します：

```
pvecm create <cluster_name> --link0 <node_link0_ip> --link1  
<node_link1_ip>
```

2. 残りの各サイトAノード、そして各サイトBノードで、クラスタに参加します：

```
pvecm add <first_node_ip> --link0 <node_link0_ip> --link1  
<node_link1_ip>
```

3. サイトAのノードのノードIDが最も小さいことを確認してください：

```
pvecm nodes
```

4. サイトCまたは別の第三の場所にあるQDeviceホストに、QDeviceデーモンをインストールします：

```
apt install corosync-qnetd
```

5. すべての Proxmox VE ノードに QDevice クライアントをインストールします：

```
apt install corosync-qdevice
```

6. 1つのProxmox VEノードで、QDeviceをクラスタに追加します：

```
pvecm qdevice setup <qdevice_ip>
```

7. QDeviceの投票によってクラスタがクォーラムを満たしていることを確認します：

```
pvecm status
```

4ノードのクラスタの場合、Expected votes`は`5、`Quorum`は`3`であり、`Flags`には`Quorate Qdevice`が含まれます。

ステップ5：保護されたNFS共有ストレージをプロビジョニングする

プライマリSVMにNFSストレージをプロビジョニングし、両方のSVMが共有するNFS LIFまたはVIPアドレスを使用して、両サイトのすべてのProxmox VEノードにマウントします。Storage Manager for Proxmox (SMP) は、ONTAPボリューム、エクスポート ポリシー、およびProxmox VEストレージ定義を1つのワークフローで作成します。SMPを使用しない場合は、ONTAPでボリュームを作成し、Proxmox VE CLIを使用してNFSストレージとして追加します。

ストレージをプロビジョニングするには、以下のいずれかの方法を選択してください。

Proxmox用ストレージマネージャー

ストレージのプロビジョニングにはSMPを使用します。SMPがインストールされており、Proxmox VE クラスタと両方のONTAPクラスタがプランとして追加されている必要があります。詳細については、"[Proxmox用Storage Managerの設定と使用](#)"を参照してください。

1. SMPで、プロビジョニング > *ボリュームの追加*を選択し、次に*NFS*を選択します。
2. **ONTAP**詳細 で、プライマリSVMを選択し、ボリューム名とサイズを入力して、優先LIFとしてNFS LIFまたはVIP LIFを選択します。
3. 両方のサイトの Proxmox VE ノードを許可するエクスポート ポリシーを選択するか、新しいポリシーを作成してください。
4. *Proxmoxの詳細*で、クラスタと両サイトのすべてのノードを選択し、NFS v3またはNFS v4.1を選択して、コンテンツタイプを選択します。
5. 「データストアをマウントする」が選択されていることを確認し、「プロビジョニング」を選択します。
6. サイトAのクラスタで、ボリュームがSnapMirrorアクティブ同期保護に含まれていることを確認します：

```
volume show -vserver <primary_svm> -volume <volume_name> -fields  
smas-protection
```

CLI

Proxmox VE CLIを使用して、プライマリSVMに既に存在するボリュームをNFSストレージとして追加します。

1. Proxmox VEノードの1つにNFSストレージを追加します：

```
pvesm add nfs <storage_id> --server <nfs_lif_or_vip_address>  
--export <export_path> --content images,rootdir --options
```

```
vers=<nfs_version>,nconnect=4
```

`3`または`4.1`を`<nfs\_version>`に使用してください。`soft`マウントオプションを追加しないでください。

2. すべてのノードでストレージがアクティブになっていることを確認してください：

```
pvesm status --storage <storage_id>
```

NFSマウントオプションを設定します

パフォーマンスと耐障害性を向上させるために、nConnectを使用してNFS LIFまたはVIPアドレスへの複数のTCP接続を開きます。保護対象のSVMに、両方のサイトでクライアントがアクセスできる複数のデータLIFがある場合は、代わりにNFSv4.1セッション トランキングを使用できます。nConnectまたはセッション トランキングのいずれかを使用し、両方は使用しないでください。詳細については、"[Proxmox VEのNFSストレージを構成する](#)"を参照してください。

手順

1. SMPを使用して、またはnConnectなしでストレージをプロビジョニングした場合は、1つのProxmox VE ノードでマウントオプションを設定します：

```
pvesm set <storage_id> --options vers=<nfs_version>,nconnect=4
```

代わりにセッション トランキングを使用するには、次を設定します：

```
pvesm set <storage_id> --options vers=4.1,trunkdiscovery,max_connect=16
```

Proxmox VEは、ストレージが次回マウントされる際に、新しいマウントオプションを適用します。VMをそのノードから移行した後、メンテナンス時間中に各ノードでストレージを再マウントしてください。

2. `/etc/pve/storage.cfg`のオプションを確認します。
3. 各Proxmox VEノードで、NFSサーバ アドレスへの複数の接続があることを確認します：

```
ss -an | grep :2049
```

ステップ6：HAとVMバックアップの設定

プライマリSVMがデータを提供するサイトAを優先するノードアフィニティルールを使用して、VMをHAに追加します。次に、SMPバックアップポリシーを使用して、誤削除やランサムウェアなどの論理的な障害からVMを保護します。SnapMirror active syncはこれらの障害を同期的にレプリケートするため、ポイントインタイム バックアップの代わりにはなりません。

手順

1. 保護対象の各仮想マシンをHAに追加します：

```
ha-manager add vm:<vm_id> --state started
```

2. サイトAのノードを優先し、サイトBのノードへのフェイルオーバーを許可するノードアフィニティルールを作成します：

```
ha-manager rules add node-affinity <rule_name> --resources  
vm:<vm_id>,vm:<vm_id> --nodes  
"<site_a_node1>:2,<site_a_node2>:2,<site_b_node1>:1,<site_b_node2>:1"
```

3. 必要に応じて、各ゲストオペレーティングシステムのディスクタイムアウトを、想定されるストレージフェイルオーバー時間よりも長く設定してください。
4. SMPでは、保護 > バックアップ > *リソースグループ*を選択し、各テナントまたはアプリケーションのVMまたはストレージ用のリソースグループを作成します。
5. 保護 > バックアップ > ポリシー > *追加*を選択し、リソースグループのバックアップ頻度と保持期間を設定したポリシーを作成します。

QEMUゲストエージェントを実行するVMの場合は、*詳細オプション*で*VMの一貫性*を選択してください。

6. オンデマンドバックアップを実行し、そこからテストVMを復元してポリシーを検証します。

ステップ7：計画されたフェイルオーバーをテストする

本番環境のVMを共有ストレージに配置する前に、設計を検証してください。計画的なフェイルオーバーでは、データ損失なしでアクティブなSVMをサイトBに移動するため、メンテナンスウィンドウ中にテストして、その後フェイルバックすることができます。

手順

1. テスト用仮想マシンをサイトBのノードにライブマイグレーションします。
2. フェイルオーバーの前に、HAがVMをサイトAノードに戻さないようにします：

```
ha-manager set vm:<vm_id> --failback 0
```

3. サイトBのクラスターで、計画的なフェイルオーバーを開始します：

```
snapmirror failover start -destination-path <secondary_svm>:
```

4. フェイルオーバーが完了するまで監視してください：

```
snapmirror failover show
```

5. すべてのProxmox VEノードで、VMのI/Oが継続し、ストレージがアクティブな状態を維持していることを確認してください。
6. VIP LIFを使用する場合は、両方のルーターがクラスタBから/32ルートを学習していることを確認してください。
7. SMPで、ONTAPプランの検出を実行してから、オンデマンドバックアップを実行して、SMPがサイトBのSVMからVMを保護していることを確認します。
8. テストが完了したらサイトAにフェイルバックし、テストVMの`failback`を`1`に戻します。

結果

Proxmox VE VMは、アクティブなSVMがサイト間を移動している間も同じNFS共有ストレージ上で実行され続け、クラスタは計画外のサイト障害から自動的に復旧します。

関連情報

- ["ONTAP SnapMirror アクティブ同期で NAS を保護する"](#)
- ["ONTAP VIP LIF を設定する"](#)
- ["ONTAPメディアエーターのインストール準備"](#)
- ["ONTAP Cloud Mediatorの設定準備"](#)
- ["SnapMirror アクティブ同期用に ONTAP Cloud Mediator を設定する"](#)
- ["SnapMirror Mediator add"](#)
- ["Proxmox VEのNFSストレージを構成する"](#)
- ["Proxmox VE corosync 外部投票サポート"](#)

Proxmox用Storage Managerの設定と使用

Storage Manager for Proxmox (SMP) は、NetApp ONTAPストレージシステムを使用したProxmox環境における仮想マシンの包括的なストレージ プロビジョニングとライフサイクル管理を提供します。SMPにより、管理者はストレージを直接管理できるようになり、自動プロビジョニング、バックアップ、リストア、クローニング機能によって運用が簡素化されます。

Proxmox 用 Storage Manager について学ぶ

Proxmox用ストレージマネージャー (SMP) は、NetAppストレージシステムを利用するProxmox環境内の仮想マシンに対して、エンドツーエンドのストレージ管理を提供します。SMPは、管理者がストレージを直接管理できるようにすることで、Proxmox環境におけるストレージとデータ管理の両方のタスクを簡素化します。

主な機能

- エンドツーエンドのストレージ管理：SMPは、ストレージ プロビジョニングからバックアップとリカバ

りまで、仮想マシンの完全なライフサイクル管理を提供します。

- **ダイレクト ストレージ管理:** Proxmox の管理者はストレージを直接管理できるため、運用が効率化され、複雑さが軽減されます。
- **スタンドアロンインストーラー:** SMPは、APIを介してProxmoxノードにシームレスに接続するスタンドアロンインストーラーとして提供されます。

機能

SMPの各コンポーネントは、ストレージ管理の効率性を向上させるように設計されています。

- **ストレージ プロビジョニング:** Proxmoxホストおよび関連する仮想マシンのストレージ リソースを簡単に割り当て、管理できます。
 - **NFS ストレージ プロビジョニング:** Proxmox 環境で使用する ONTAP NFS ストレージをセットアップして設定します。
 - **iSCSI ストレージ プロビジョニング:** 堅牢で効率的な iSCSI ストレージ管理のために、マルチパスを使用したシック LVM を実装します。
- **バックアップとリカバリ:** データの整合性と可用性を確保するために、信頼性の高いバックアップと迅速なリカバリを実行します。
 - **「crash consistent state (障害など予期しないシャットダウン時と同様)」の状態のバックアップとファイル整合性バックアップ:** 「crash consistent state (障害など予期しないシャットダウン時と同様)」の状態とファイル整合性の両方のバックアップメカニズムを設定することで、データの整合性を確保します。
 - **VM復元操作:** 仮想マシンの復元プロセスを実行して、データを復旧し、システムの可用性を維持します。
- **ストレージ効率:** ONTAPは、データに必要なストレージ容量を最小限に抑えるように設計された、包括的なストレージ効率化技術スイートを提供します。これらの技術は、ストレージ消費量を削減するだけでなく、システムパフォーマンスを向上させ、以下の効果をもたらします：
 - **迅速なVMプロビジョニング:** 仮想マシンのプロビジョニングを効率化し、より迅速な展開を実現します。
 - **データセットのコピーを高速化:** データセットの複製を高速化し、効率的なデータ管理を実現します。

前提条件

先に進む前に、以下の項目をすべて完了していることを確認してください。

- 動作するProxmox Virtual Environment (PVE) 9.x以降のクラスター。
- SVM レベルで NFS および iSCSI プロトコルが有効になっている ONTAP All Flash FAS (AFF) ストレージ。手順については、["ONTAPを使用したNFSデータストアの設定"](#)および["ONTAP ストレージを使用した iSCSI 用に Proxmox VE 9.x を設定"](#)を参照してください。



iSCSI LUN構成の場合、以下の項目を有効にする必要があります：

すべての **Proxmox** ホストにマルチパスと **iSCSI** をインストールします：

```
apt update
```

```
apt install open-iscsi multipath-tools -y
systemctl enable --now iscsid multipathd
```

iSCSI イニシエータを設定し、iSCSI 経由で接続します (Proxmox ホスト上) :

作成または更新 /etc/multipath.conf :

```
touch /etc/multipath.conf
```

または以下を使用してください :

```
cat << 'EOF' > /etc/multipath.conf
defaults {
    user_friendly_names yes
    find_multipaths yes
}
blacklist {
    devnode "^sd[a]$"
}
EOF
```

- ProxmoxホストとONTAPストレージは、SMPホストからネットワーク経由でアクセス可能です。

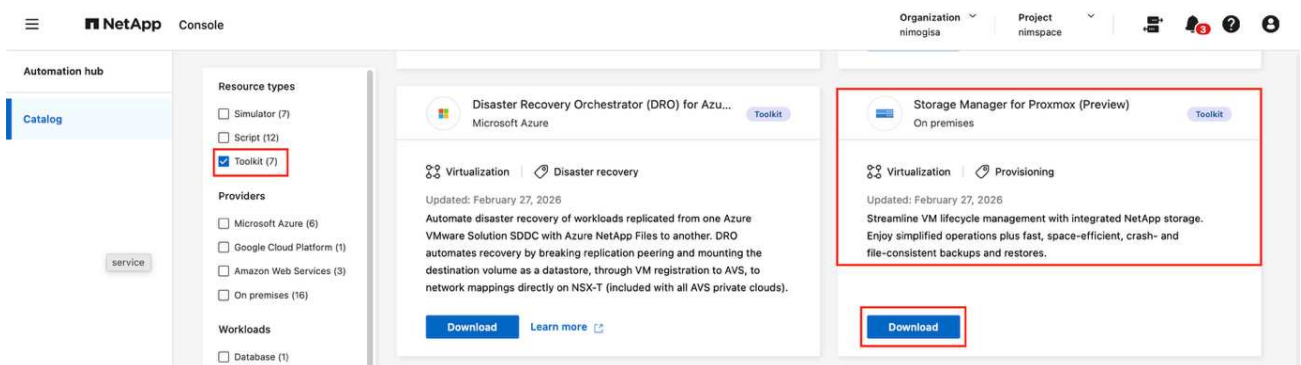
Proxmox 用の Storage Manager をインストールしてセットアップする

SMPを使い始めるには、指定された仮想マシン上でWindowsオペレーティングシステムを使用してください。SMPは、Windows Server 2019、2022、および2025で実行できます。

手順

1. SMPパッケージ (約17MB) を "NetApp Console オートメーションハブ" からダウンロードしてください。

▼ SMPダウンロードページを表示

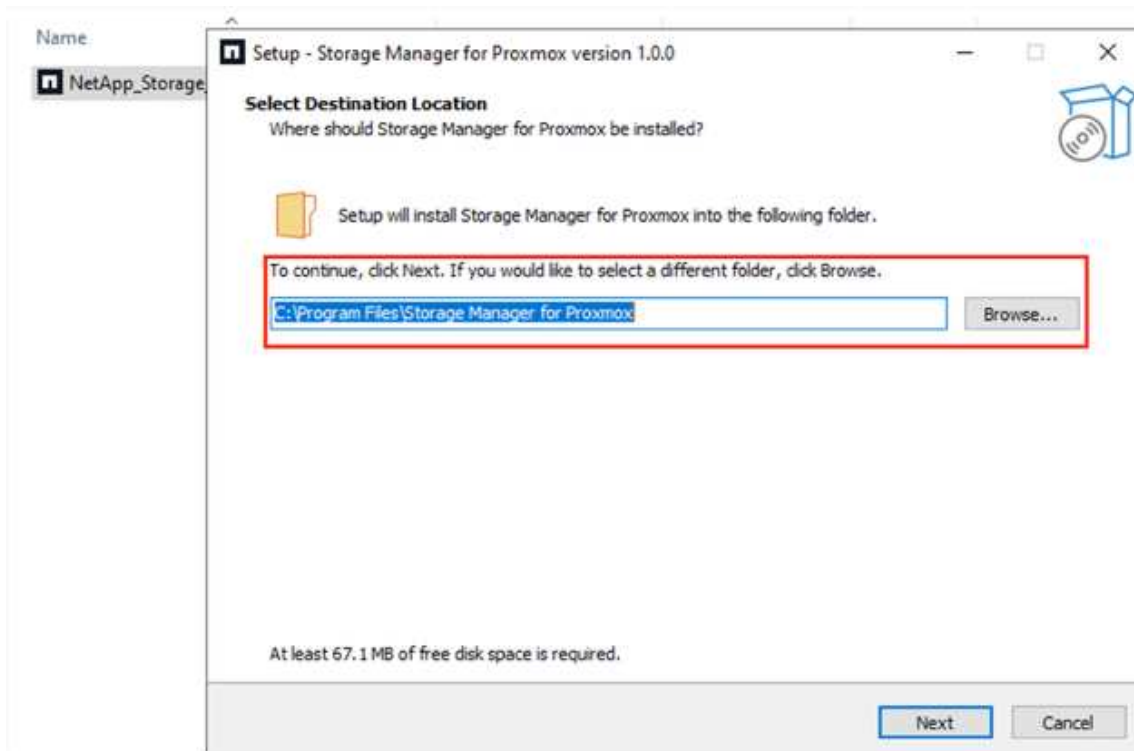


2. パッケージを解凍します。
3. 実行ファイルを実行して、サービスをインストールおよび起動してください。



SMPは利用可能なAPIを活用してプロビジョニングとデータ保護のワークフローをオーケストレーションするため、追加のパッケージ依存関係は必要ありません。

▼ SMPインストールウィザードを表示



Shift ツールキットを使用した代替インストール

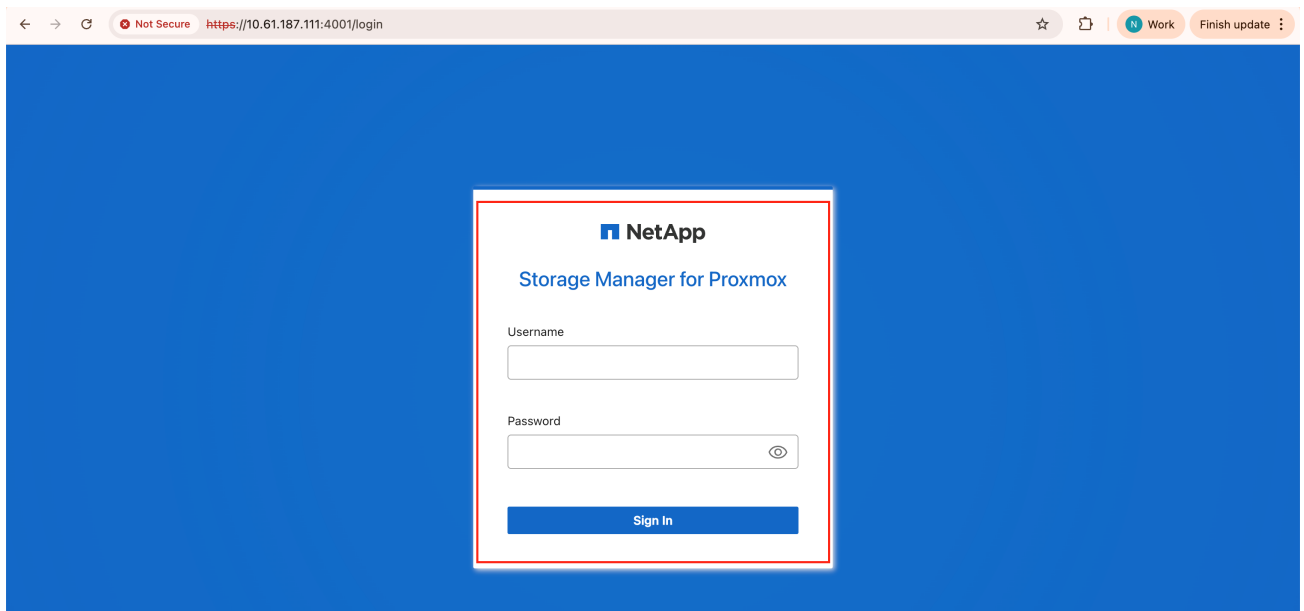
スタンドアロンインストーラーの代わりに、Shift ツールキットを使用して Proxmox VE Storage Manager をインストールすることもできます：

- Open Shift Toolkitを開きます。
- 設定 > 詳細設定 > ストレージマネージャー の順に移動します。
- トグルスイッチを使用して Proxmox VE を有効にします。
- システムが必要なコンポーネントを自動的にインストールするまでお待ちください。
- インストールが完了したら、*View*をクリックするか、Webブラウザを開いて `https://<Shift\_server\_IP>:4001`Storage Managerにアクセスします。

例： <https://10.61.187.117:4001>

4. ウェブブラウザを開き、 `https://<IP address specified during installation>:4001`を入力してSMP UIにアクセスします

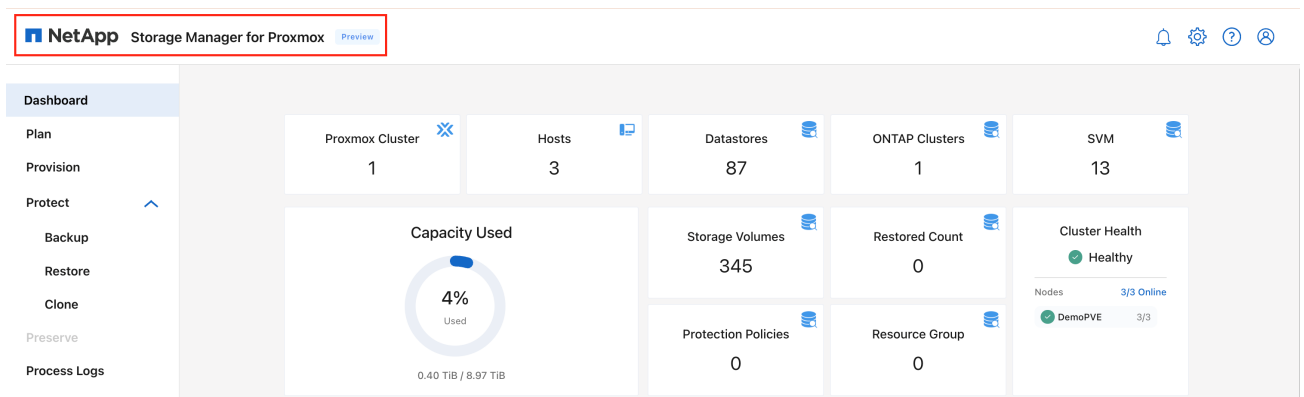
▼ SMPログイン画面を表示



5. デフォルトのユーザー名 `admin` とパスワード `admin` を使用してSMPにログインします。

指示が表示されたら、デフォルトのパスワードを変更してください。Shiftツールキットを使用してSMPをインストールする場合も、同じデフォルトの認証情報が適用されます。

▼ SMPホーム画面を表示



Proxmox 用の Storage Manager の設定

ストレージとストレージおよびProxmoxノードへの接続が適切に構成されたら、SMPを構成して、ONTAPスナップショットとFlexClone機能を活用した仮想マシンのプロビジョニングと保護を自動化します。

最初のステップは、ONTAPストレージエンドポイントを検出して追加し、次にターゲットのProxmoxノードをSMPに追加することです。

開始する前に

次の前提条件が満たされていることを確認してください。

- SMPがインストールされています
- SMPインスタンスはProxmoxノードおよびストレージシステムへの接続性を備えています。
- ONTAP クラスタで NFS または iSCSI ストレージ プールを提供

- DNS名を使用する場合、DNS解決が行われます。それ以外の場合は、検出にIPアドレスを使用してください。
- この環境は、サポートされているバージョンのProxmox Virtual Environmentサーバーを使用しています。

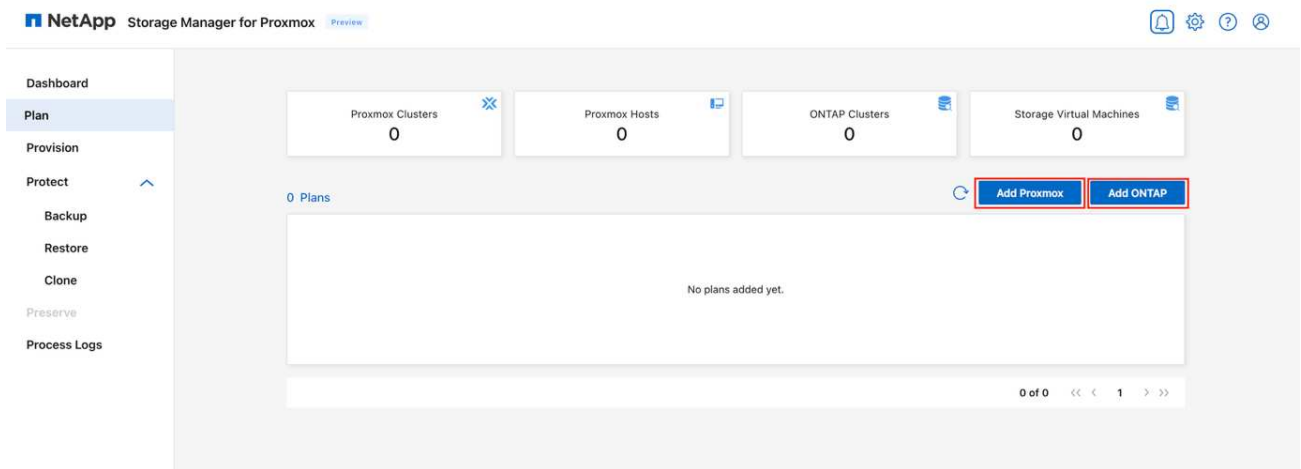
タスク概要

ハイパーバイザーとストレージ間の接続が確立された後、設定は数回のクリックと約2分で完了します。

手順

1. SMPにログインします。
2. SMPの左側のナビゲーションから*Plan*を選択します。
3. **Add Plan** をクリックします。

▼ プランの追加を表示



4. *ONTAP の追加*をクリックして、ONTAP ストレージ システムのクレデンシャルを追加します。

クラスタエンドポイントまたはSVM管理LIFのいずれかを使用してONTAPを追加できます。

5. クラスタエンドポイントを使用して追加するには、次の詳細を指定します。
 - a. クラスタ IP アドレスまたは FQDN
 - b. ONTAPクラスタにアクセスするためのユーザー名
 - c. ONTAP クラスタにアクセスするためのパスワード
 - d. **Accept self-signed certificate** を選択し、**Add Storage Cluster** をクリックします

▼ ONTAP の追加を表示：クラスタエンドポイント

NetApp Storage Manager for Proxmox

Dashboard

Plan

Provision

Protect

Backup

Restore

Clone

Preserve

Process Logs

ONTAP Cluster Details

Connection Type

Cluster

SVM

Connect to cluster management IP to access all SVMs

Cluster Name

SMPProxClus

Cluster Management IP

10.192.102.41

Admin Username

admin

Password

Accept self-signed certificates

Cancel Add Storage Cluster

6. SVM管理LIFを使用して追加するには、以下の詳細情報を入力してください：
- SVM管理LIFまたはFQDN
 - SVMにアクセスするためのユーザー名
 - SVMにアクセスするためのパスワード
 - Accept self-signed certificate** を選択し、**Add Storage Cluster** をクリックします

▼ ONTAP の追加を表示：SVM 管理 LIF

NetApp Storage Manager for Proxmox

Dashboard

Plan

Provision

Protect

Backup

Restore

Clone

Preserve

Process Logs

ONTAP SVM Details

Connection Type

Cluster

SVM

Connect directly to a single SVM using its management LIF

SVM Name

SMPProxSVM

SVM Management LIF IP

10.61.187.155

Admin Username

vasdmin

Password

Accept self-signed certificates

Cancel Add Storage SVM

7. *Proxmoxを追加*をクリックして、SMPに登録するProxmoxノードの認証情報を追加します。

Proxmoxノードを追加するには、既存のProxmoxノードのいずれかのIPアドレスを指定します。検出ジョブは、クラスターに自動的にクエリを実行して、必要な構成の詳細をすべて収集します。

8. 次の詳細を入力します。

- a. Proxmox スタンドアロン IP アドレスまたは FQDN
- b. Proxmoxにアクセスするためのユーザー名
- c. リソースのインベントリを実行するために Proxmox ホストにアクセスするためのパスワード
- d. **Accept self-signed certificate** を選択し、**Continue** をクリックします

▼ Proxmoxの追加を表示：ノード認証情報

NetApp Storage Manager for Proxmox

Proxmox Details

Plan Name: SMPProxmox-Username

Proxmox Endpoint: 10.193.172.225

Authentication Method: ☒ Username / Password ☐ API Token

Proxmox Username: root

Proxmox Password: NetApp123

☒ Accept self-signed certificates

Cancel Add Site

または、APIトークンを使用してAPIにアクセスするには、以下を提供してください：

- APIトークンID
- APIトークンシークレット



今回のリリースでは、APIトークンはNFS処理でのみ使用できます。

▼ Proxmox の追加を表示：API トークン

9. 検出ジョブが正常に実行され、各プランのステータスが **Success** とマークされていることを確認してください。

追加されると、SMPは自動的に検出スキャンを実行し、仮想マシンとその関連メタデータを表示します。既存のストレージ ボリュームやマッピングされたLUNも検出されます。

▼ プランの検出結果を表示する

Name	Endpoint	Type	Discover Status
SMPProxmox-ApiToken	10.193.172.221:8006	Proxmox	In Progress
SMPProxmox-Username	10.193.172.225:8006	Proxmox	Success
SMPProxmox-Userpassword	10.192.102.41	ONTAP	Success

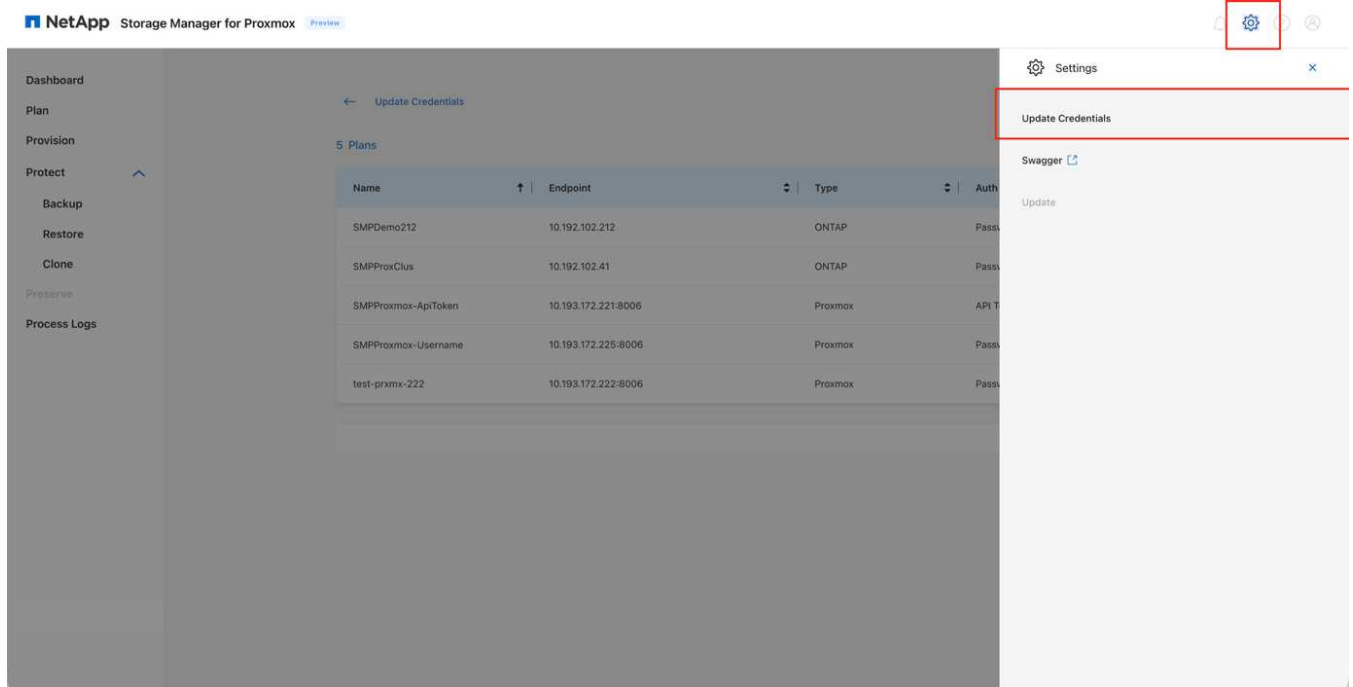
終了後の操作

- Proxmoxノードまたはストレージに変更が加えられた場合は、ディスカバリを実行して最新情報を取得してください。プラン名の横にある3つの点をクリックし、*Discover*をクリックしてください。
- ONTAP ストレージ システムが最初に追加されていることを確認してください。これにより、検出ジョブで既存のリソースを適切にマッピングできます。Proxmox が最初に追加された場合は、ONTAP に対して

検出ジョブを実行してください。

- 認証情報またはAPIトークンを後で更新する必要がある場合は、*設定*に移動し、*認証情報の更新*オプションを選択してください。

▼ 更新認証情報を表示



ストレージのプロビジョニング

ボリュームをストレージプール（一般的にはデータストアと呼ばれる）としてプロビジョニングすると、仮想マシンとその仮想ディスク（QCOW2またはRAW）のための論理コンテナが作成されます。SMPを使用すると、データストアをプロビジョニングし、それを単一のホストまたはクラスタ内のすべてのホストに接続できます。

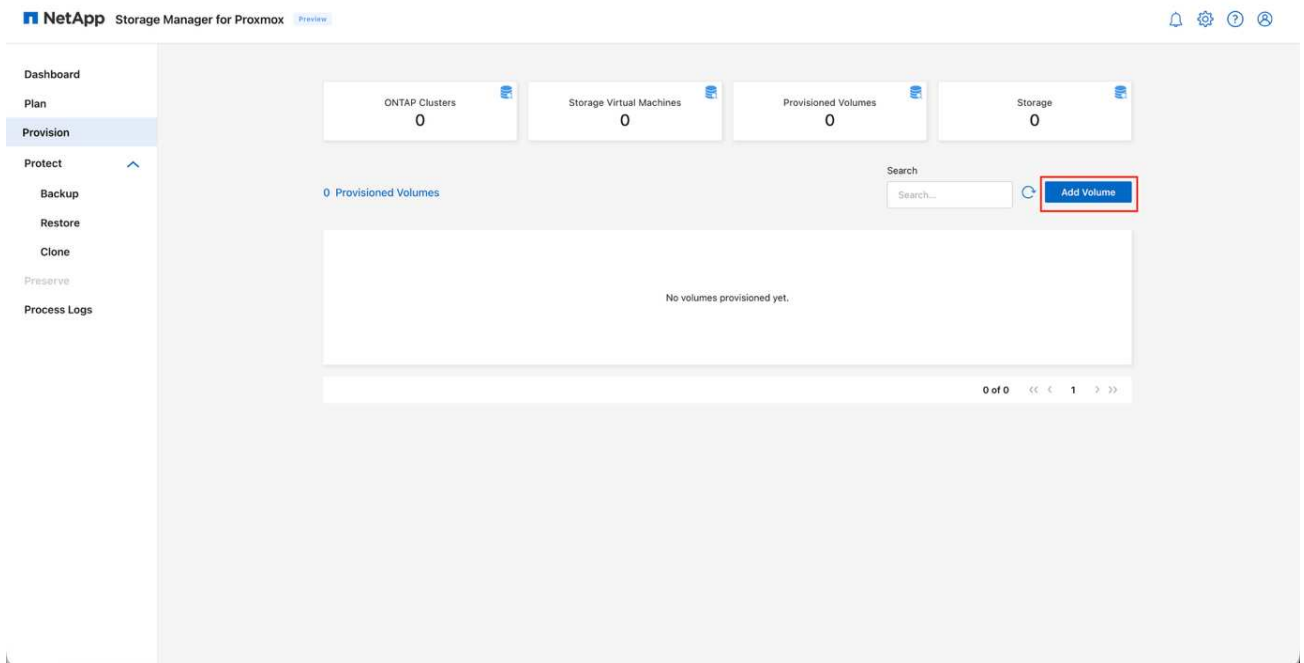
NFSストレージのプロビジョニング

SMPを使用して、ONTAPボリュームをNFSデータストアとしてプロビジョニングおよびマウントします。

手順

1. SMP GUIで、*プロビジョニング*タブに移動します。
2. *ボリュームの追加*に移動します。

▼ プロビジョニングタブを表示：ボリュームを追加

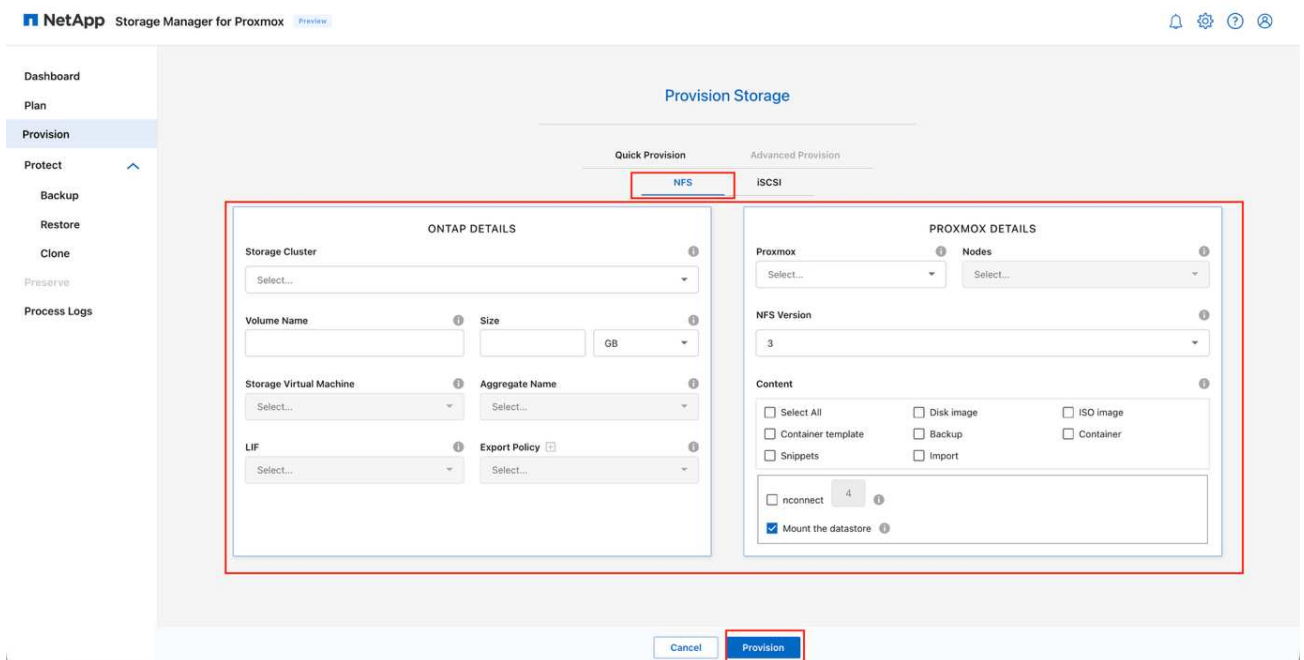


3. 新規ボリュームウィザードの「クイックプロビジョニング」ステップで、*NFS*を選択します。



NFSがデフォルトで選択されています。クイックプロビジョニングは、標準的な導入のデフォルト設定を使用して、より高速なセットアップを実現します。高度なプロビジョニングでは、HAおよびBCDR機能の拡張オプションが提供されます。これらは今後のリリースで導入される予定です。

▼ 新規ボリュームウィザードの表示：NFS



4. *ONTAP詳細*セクションで、以下の情報を入力します：

- a. *ストレージクラスター*ドロップダウンからONTAPクラスターまたは指定されたStorage Virtual Machine (SVM) を選択します

- b. * Volume Name *フィールドに一意の値を指定します
- c. データストアボリュームに必要な容量を*サイズ*フィールドに入力します
- d. 以下の適切なオプションを選択して、ONTAPストレージリソースを選択します：
 - アグリゲート名
 - Storage Virtual Machine (SVM)
 - データストアへのアクセスに使用する優先LIF
- e. 既存の*Export Policy*を選択するか、必要に応じて (+) をクリックしてカスタムポリシーを作成します。

▼ ONTAP詳細の表示：NFS

Type	Read-only Access	Read/Write Access	Super user access
All	☒	☒	☒
All (as Anonymous user)	☐	☐	☐
Unix	☒	☒	☒
Kerberos 5	☒	☒	☒
Kerberos 5i	☒	☒	☒
Kerberos 5p	☒	☒	☒

5. *Proxmoxの詳細*セクションで、以下の情報を入力します：
 - a. *Proxmox*フィールドでターゲットクラスタを選択し、データストアへのアクセスが必要なすべてのノードを選択します
 - b. *NFS Version*フィールドで、優先するNFSプロトコル（NFS v3またはNFS v4.1）を選択します
 - c. *Content*セクションで、このデータストアで有効にするコンテンツタイプを選択します：
 - ディスクイメージ
 - ISOイメージ
 - コンテナテンプレート
 - バックアップ
 - スニペット
 - インポート
 - または*すべて*のコンテンツタイプを選択します
 - d. (オプション) 複数のTCP接続が必要な場合は、*nconnect*オプションを有効にします
 - e. **Mount the datastore** がチェックされていることを確認してください。そうすることで、選択した

Proxmox ノード全体にデータストアがマウントされます。

▼ Proxmoxの詳細を表示：NFS

NetApp Storage Manager for Proxmox

Dashboard
Plan
Provision
Protect
Backup
Restore
Clone
Preserve
Process Logs

Provision Storage

Quick Provision Advanced Provision

NFS iSCSI

ONTAP DETAILS

Storage Cluster: SMPProxClus

Volume Name: SMPDemoVol Size: 2 GB

Storage Virtual Machine: svm_sie_dev_func01 Aggregate Name: NSOL_NetApp_A400_T11U3_02_HV...

LIF: 192.168.118.223 (Preferred LIF) Export Policy: demoExportPolicy

PROXMOX DETAILS

Proxmox: SMPProxmox-ApiToken Nodes: sie-dev-proxmox-node01

NFS Version: 3

Content: ☒ Select All ☒ Container template ☒ Snippets ☒ Disk image ☒ Backup ☒ Import ☒ ISO image ☒ Container

nconnect: 3 M: nconnect = 3

testing_110
LIF: 192.168.118.223
NFS Version: 3
Total Storages: 10

Cancel Provision

6. *Provision*をクリックして、ONTAPボリュームを作成し、選択したProxmoxクラスタ内にデータストア（ストレージプール）を登録します。

▼ NFSプロビジョニング結果を表示する

NetApp Storage Manager for Proxmox

Dashboard
Plan
Provision
Protect
Backup
Restore
Clone
Preserve
Process Logs

Provision Storage

Provisioning Storage

NFS Volume Setup

Please wait while storage is being provisioned. This may take 1-2 minutes.

Validating parameters...

Loading site configurations...

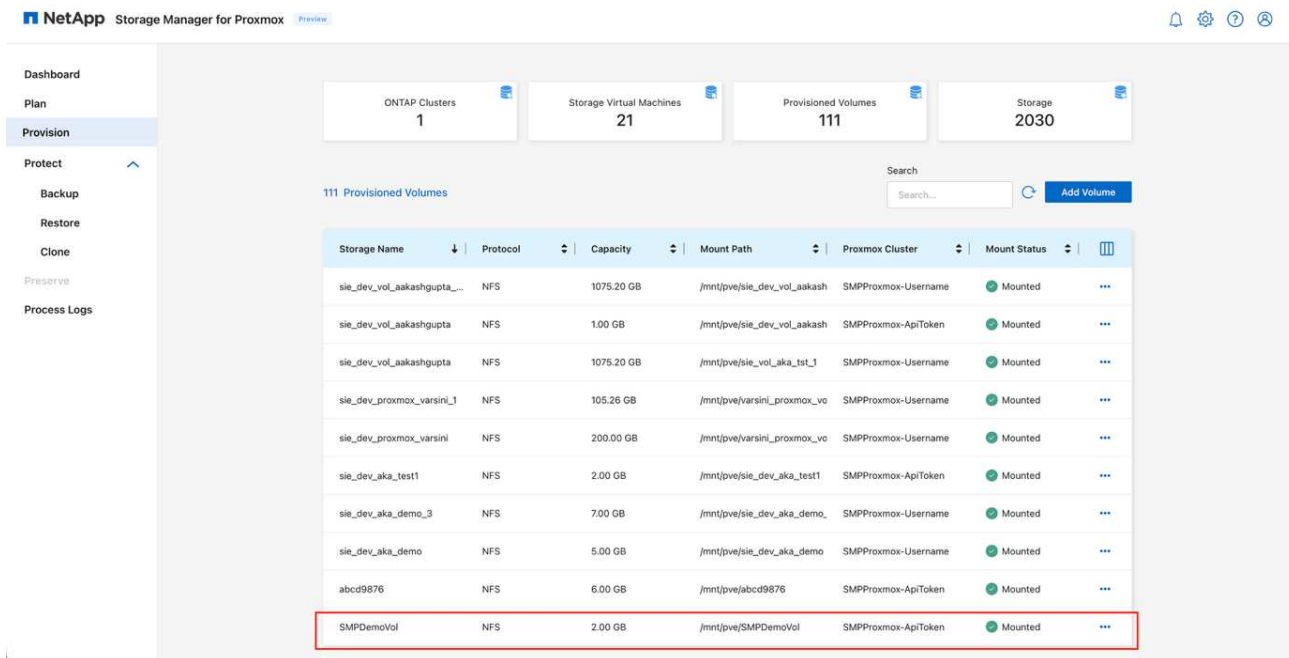
Provisioning ONTAP NFS volume...

Waiting for NFS export to be ready...

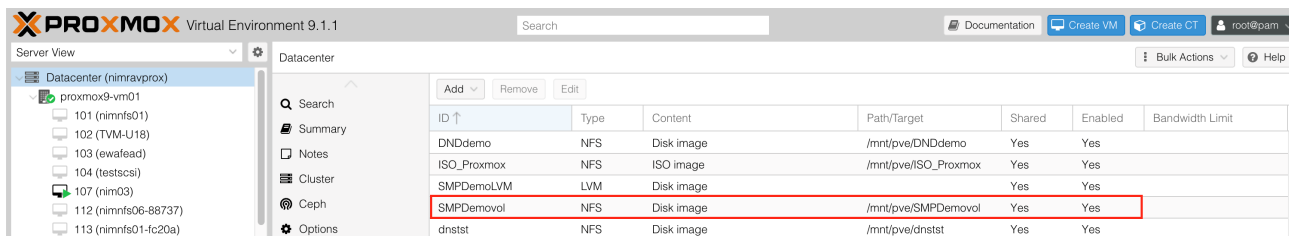
Mounting NFS storage in Proxmox...

Progress 2 / 5 steps

Cancel Provision



▼ ProxmoxでNFSデータストアを表示する



プロビジョニング済みボリュームを編集する

プロビジョニング後にボリューム設定を変更するには、SMPを使用します。

手順

1. SMP GUIで、*プロビジョニング*タブからボリュームを探します。
2. ボリュームの横にある縦に並んだ3つの点（:）をクリックします。
3. コンテキストメニューから*Edit*を選択して、ボリューム設定を開きます。

▼ ボリューム編集ダイアログを表示

4. 必要に応じてボリューム設定を変更します。

- ボリュームのサイズ変更：ボリュームのストレージ容量を調整します



サイズ変更はNFSボリュームにのみ適用されます。

- **Snapshot**ロック：Snapshotの削除や変更を防止するために有効にします



これには、クラスタに SnapLock ライセンスがインストールされており、クラスタのコンプライアンスロックが初期化されている必要があります。

- ランサムウェア対策：ランサムウェア攻撃の兆候となる可能性のある異常なアクティビティを事前に検知し、警告を発します。
- エクスポートポリシー：エクスポートポリシーを更新または変更する

5. 変更を適用するには、*保存*をクリックします。

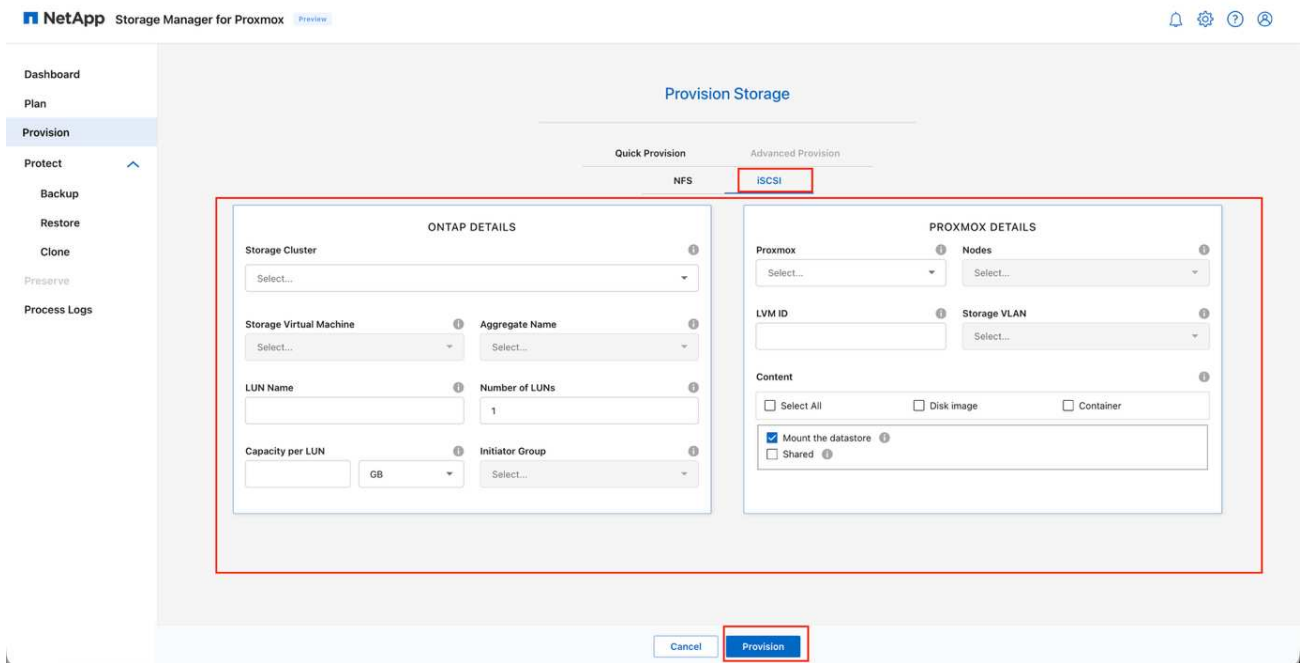
iSCSIストレージをプロビジョニングする

SMPを使用して、仮想マシン用のiSCSIバックエンドをセットアップします。

手順

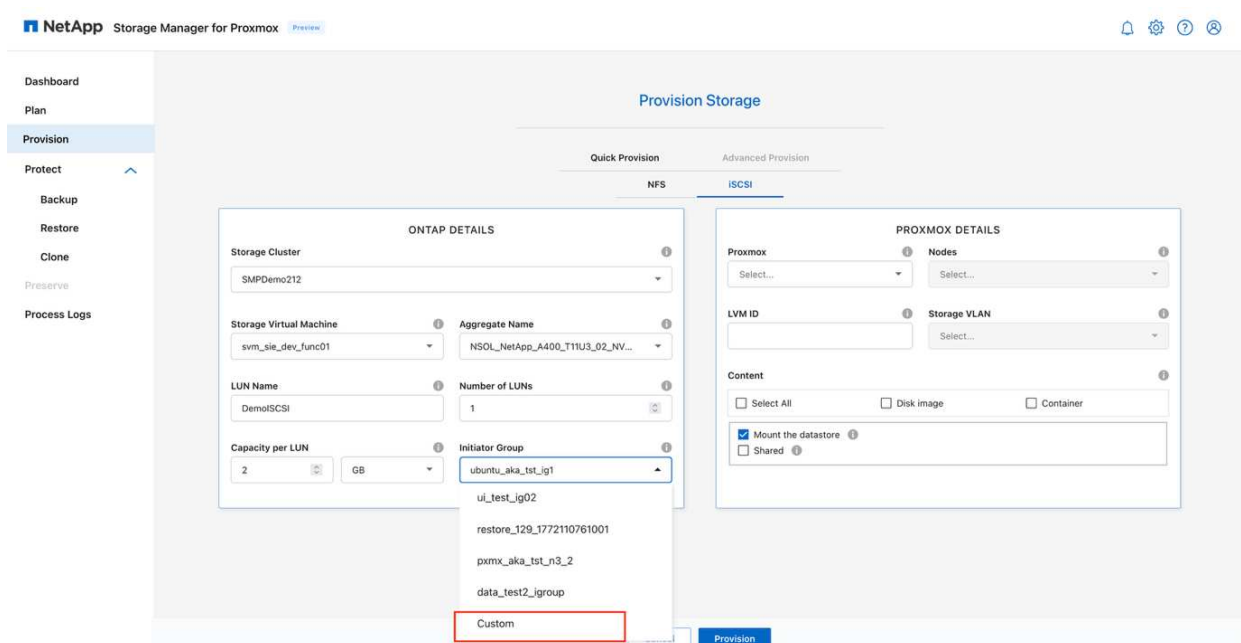
1. SMP GUIで、*プロビジョニング*タブに移動します。
2. *ボリュームの追加*に移動します。
3. 新規ボリュームウィザードの「クイックプロビジョニング」ステップで、*iSCSI*を選択します。

▼ 新規ボリュームウィザードの表示：iSCSI

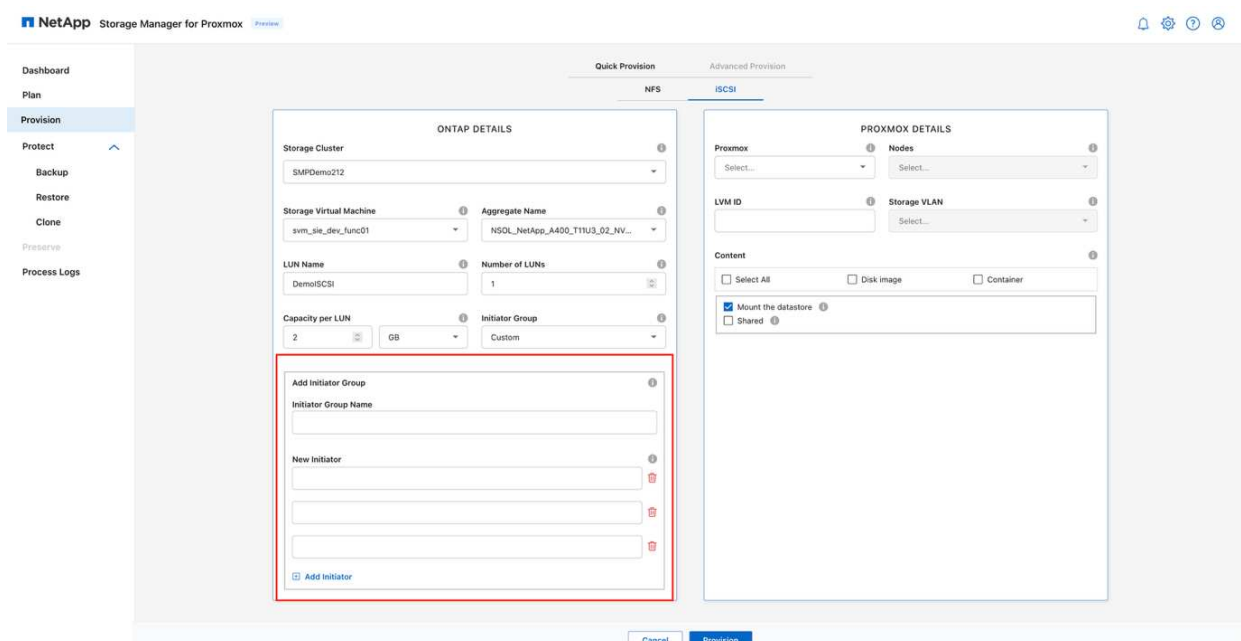


4. iSCSIプロトコルでは、*ONTAP詳細*セクションで、以下の情報を入力します：
- *ストレージ クラスター*ドロップダウンから、適切なONTAPクラスタまたは指定されたStorage Virtual Machine（SVM）を選択します
 - 以下のオプションを選択します。
 - アグリゲート名
 - Storage Virtual Machine（SVM）
 - *LUN Name*フィールドに一意の値を入力します
 - *Number of LUNs*フィールドに必要なLUN数を入力します（デフォルトは1、同じサイズの追加LUNを並行して作成できます）
 - *Capacity per LUN*フィールドに、各LUNの希望サイズを入力します
 - iSCSIアクセス制御用の*イニシエータグループ*（igroup）を選択します。既存のigroupを選択するか、新しいigroupを作成できます。

▼ ONTAP詳細の表示：iSCSI LUN構成



▼ iSCSI igroupの選択を表示



5. *Proxmoxの詳細*セクションで、以下の情報を入力します：

- Proxmox** ドロップダウンからターゲットクラスターを選択し、ストレージへのアクセスが必要なすべてのノードを選択します
- Proxmox内でiSCSIベースのストレージプールを表す適切な*LVM ID*を選択してください
- *Nodes* フィールドで、提示されたiSCSIターゲットへのアクセスが必要なすべてのノードを選択します
- (オプション) VLANセグメンテーションが必要な場合は、目的の*Storage VLAN*を選択してください。
- *Content*セクションで、このデータストアでサポートされているコンテンツタイプを選択します：
 - ディスクイメージ

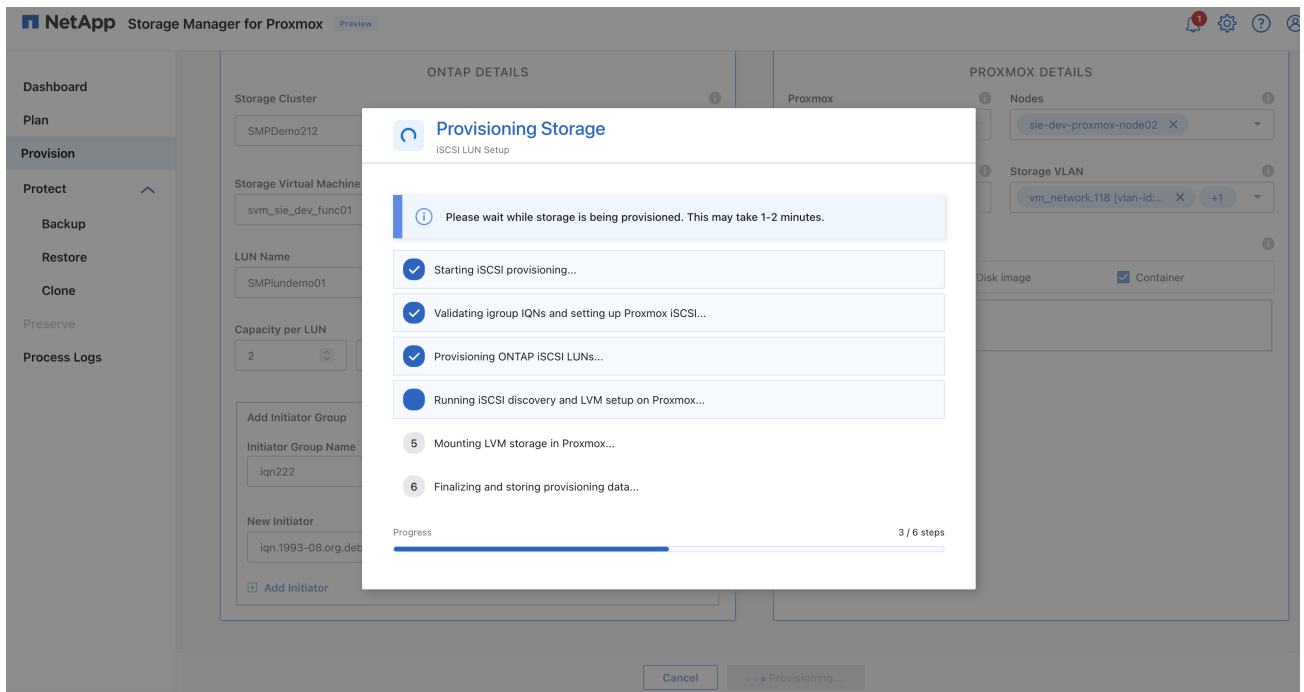
- Container
 - または*すべて*のコンテンツタイプを選択します
- f. ストレージが選択した Proxmox ノード全体で利用可能になるように、*データストアをマウントする*が選択されていることを確認してください。
- g. (オプション) ストレージプールが複数のノードから同時にアクセスされる場合は、*共有*を有効にしてください。

▼ Proxmoxの詳細を表示：iSCSI

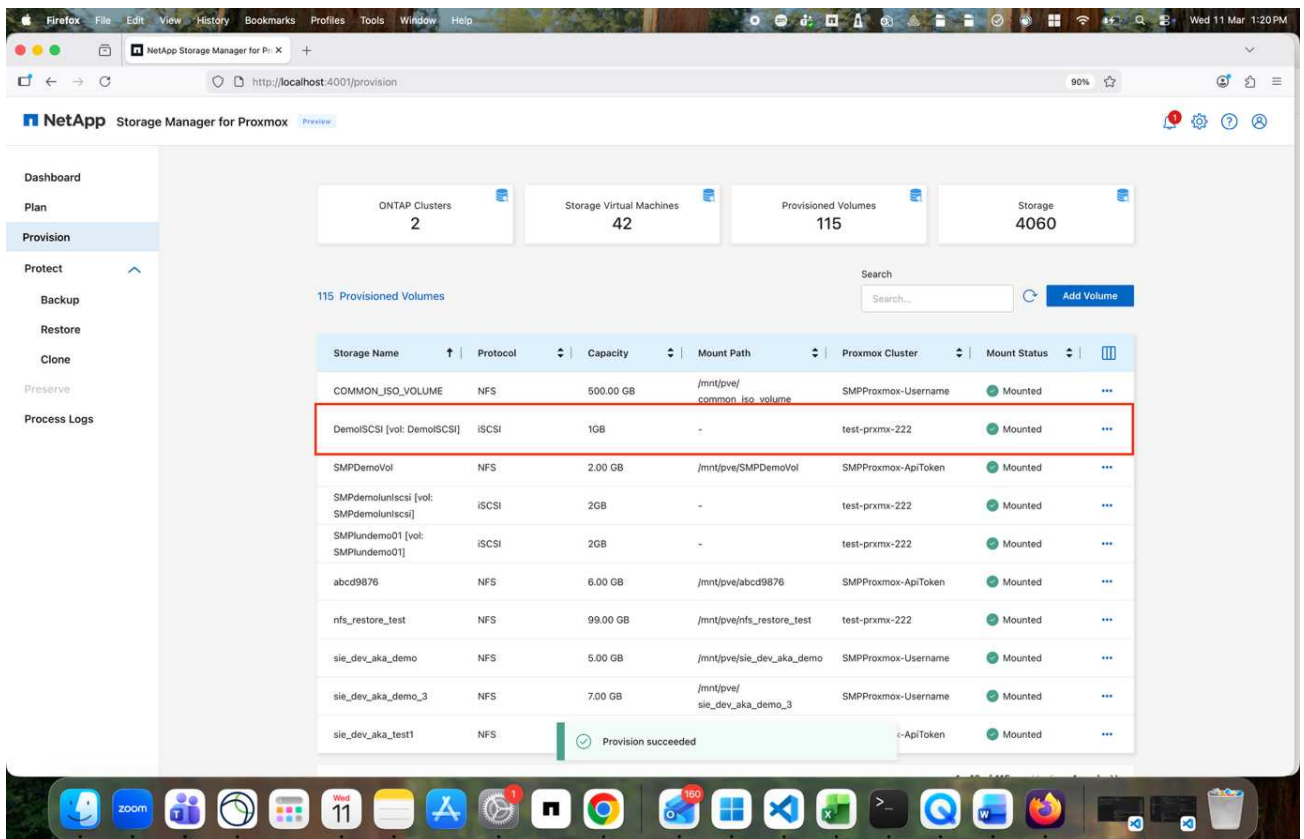
6. *Provision*をクリックして、ONTAP LUNを作成し、選択したProxmoxクラスタ内にデータストア（ストレージプール）を登録します。

▼ iSCSI LUNのプロビジョニングを表示する

▼ iSCSIプロビジョニングの完了を表示



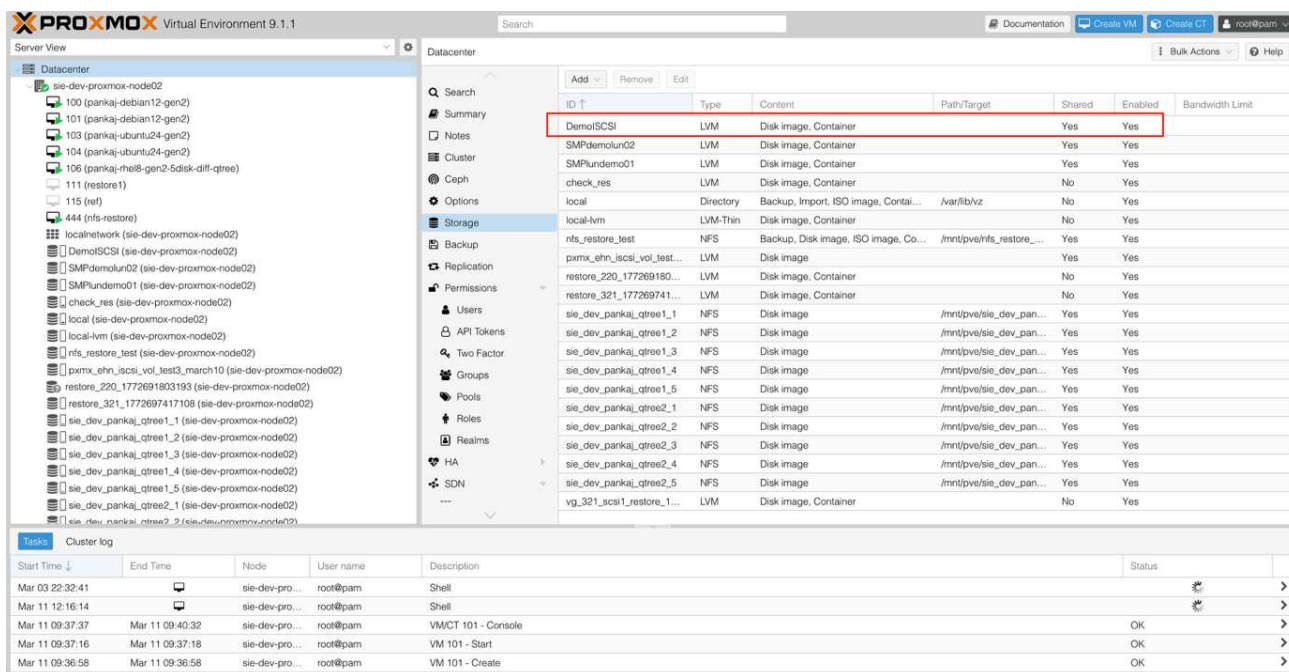
▼ ProxmoxでiSCSIデータストアを表示する



7. Proxmoxエンドポイントにアクセスして、NFSおよびiSCSI LUNが接続されていることを確認します。

接続されたストレージは、仮想マシンのプロビジョニングに使用できるようになりました。

▼ Proxmoxストレージビューを表示



ボリューム構成オプション

SMPが新しいONTAP FlexVolボリュームとLUNをプロビジョニングする場合、いくつかのデフォルト設定値が自動的に適用されます：

ONTAP 設定	デフォルト値
Snapshotリザーブ (-percent-snapshot-space)	0%
フラクショナルリザーブ (-fractional-reserve)	0%
アクセス時刻の更新 (-atime-update)	無効
最小先読み (-min-readahead)	無効
スケジュールされたSnapshot	なし
ストレージ効率	有効
ボリューム ギャランティ	なし (シンプロビジョニング)
ボリュームのオートサイズ	grow_shrink
LUNスペース リザーベーション	無効
LUN スペース割り当て	有効

NConnectの動作

Proxmox VEでNFSストレージを使用する場合は、Linux NFSクライアント（Proxmox VEのベースOSであるDebianで使用されているもの）の特定の動作に注意してください。Linuxカーネルは、NFSエクスポートがノードに初めてマウントされたときのマウントパラメータを再利用する可能性があります。同じエクスポートを異なるマウントオプションで再度マウントした場合、新しいオプションが適用されない可能性があります。

ベストプラクティスとして、個別のエクスポートを作成してマウントし、異なるNFSサーバIPアドレス（個別のデータLIFなど）を使用します。SMPは既存の接続とその関連するnconnect値を自動的に検出し、新しい接続に適切なnconnect値を適用します。

仮想マシンの保護

仮想マシンが ONTAP ベースの NFS データストアで実行される場合、最も効率的な保護方法は、Proxmox にファイルシステムの一貫性を確立させ、ONTAP がストレージ レイヤで実際のバックアップ ポイントをキャプチャすることです。ONTAP スナップショットは、高速でスペース効率に優れた、データストア ボリュームのポイントインタイム コピーを提供し、後でデータストア全体、個々のファイル、または VM コンテンツをリカバリするために使用できます。

SMPは、「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態およびVM整合性のあるデータ保護とクローン管理のためのシンプルなオーケストレーターを提供します。このソフトウェアは、複数のジョブに適用できるバックアップ ポリシーを作成することで、バックアップ、リストア、クローン作成のライフサイクルを簡素化します。これらのポリシーは、スケジュール、保持期間、レプリケーション、およびその他の機能を定義できます。ファイル整合性スナップショットのオプション選択が可能です。このアプローチでは、ONTAPスナップショットを取得する前に、QEMUの機能を使用してI/Oを静止させます。

SMP では、1 つの ONTAP NFS ボリュームに複数の VM が含まれるデータストア全体、複数のデータストアにまたがる VM のグループ、または個々の VM レベルで保護できます。

仮想マシンのバックアップ

ONTAP ボリュームがプロビジョニングされたら、バックアップ オプションを使用して、Proxmox クラスタで実行されているすべての VM を一覧表示し、仮想マシンの「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態またはファイル整合性バックアップを実行します。

手順

1. 左側のナビゲーション ペインから * Protect * > * Backup * にアクセスします。

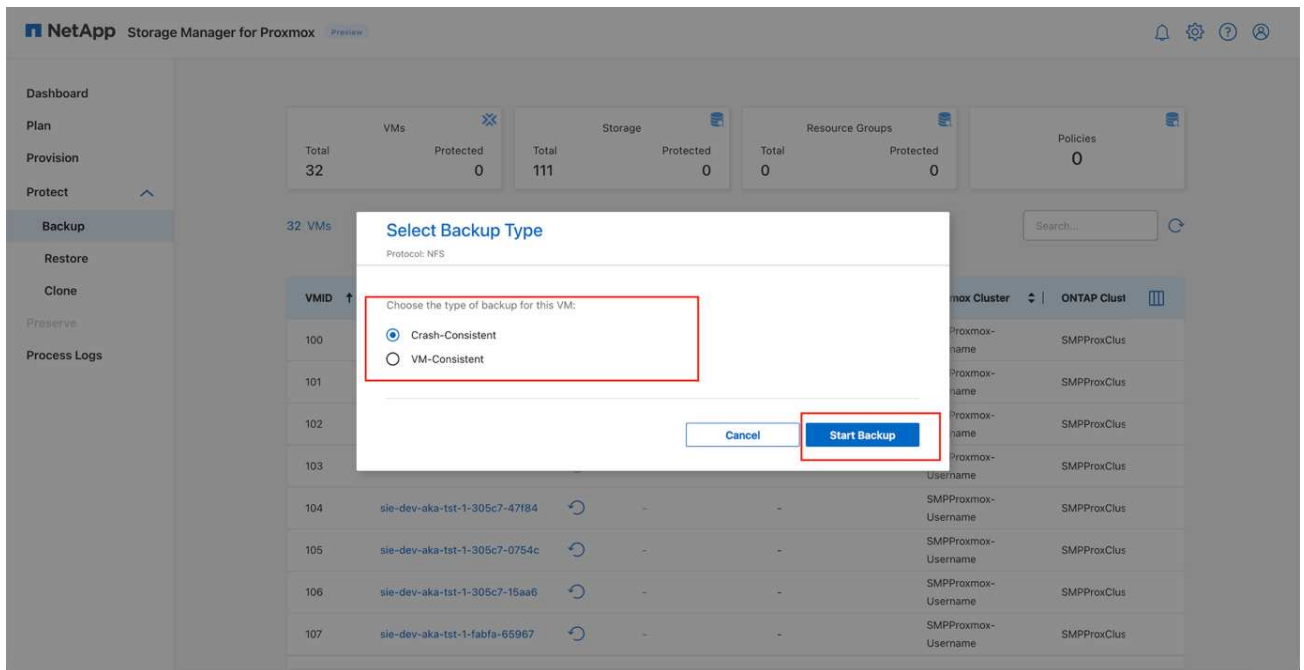
▼ Protect Backupページを表示

The screenshot shows the NetApp Storage Manager for Proxmox interface. The left sidebar has a 'Backup' link highlighted. The main content area displays a table of VMs. The table has the following columns: VMID, Name, Backup status, Backup Status, Last Backup Date, Proxmox Cluster, and ONTAP Cluster. The table contains 8 rows of data, with VMIDs ranging from 100 to 107. A red box highlights the table.

VMID	Name	Backup status	Backup Status	Last Backup Date	Proxmox Cluster	ONTAP Cluster
100	sie-dev-aka-tst-1-89a2e	🔄	-	-	SMPProxmox-Username	SMPProxClus
101	sie-dev-aka-tst-1-fc39f	🔄	-	-	SMPProxmox-Username	SMPProxClus
102	sie-dev-aka-tst-1-ce32c	🔄	-	-	SMPProxmox-Username	SMPProxClus
103	sie-dev-aka-tst-1	🔄	-	-	SMPProxmox-Username	SMPProxClus
104	sie-dev-aka-tst-1-305c7-47f84	🔄	-	-	SMPProxmox-Username	SMPProxClus
105	sie-dev-aka-tst-1-305c7-0754c	🔄	-	-	SMPProxmox-Username	SMPProxClus
106	sie-dev-aka-tst-1-305c7-15aa6	🔄	-	-	SMPProxmox-Username	SMPProxClus
107	sie-dev-aka-tst-1-fabfa-65967	🔄	-	-	SMPProxmox-Username	SMPProxClus

2. バックアップする仮想マシンを選択し、*Backup*をクリックします。

▼ バックアップダイアログの表示：VMの選択



3. バックアップ ワークフローでは、「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態とファイル整合性保護のいずれかを選択できます。

ファイル整合性モードでは、スナップショット取得前にゲストOS内のファイルシステムが静止状態になるように、オプションでQEMU fsfreezeを使用します。fsfreezeが失敗した場合、システムはProxmoxスナップショットを使用するようにフォールバックします。



このフォールバックメカニズムは、NFSボリュームに保存されている仮想マシンにのみ適用されます。

▼ バックアップの表示ダイアログ：整合性オプション

Start Time	End Time	Node	User name	Description	Status
Feb 25 02:55:28		proxmox9-...	root@pam	Shell	
Mar 10 08:51:01	Mar 10 08:51:01	proxmox9-...	root@pam	VM 116 - Delete Snapshot	OK
Mar 10 08:50:56	Mar 10 08:50:57	proxmox9-...	root@pam	VM 116 - Snapshot	OK

▼ バックアップの進行状況を表示する

Dashboard

Plan

Provision

Protect

Backup

Restore

Clone

Preserve

Process Logs

VMs	Storage	Resource Groups	Policies
Total 32	Total 111	Total 0	Total 0
Protected 0	Protected 0	Protected 0	Protected 0

32 VMs VMs Storage Resource groups Policies

Search...

VMID ↑	Name	Backup	Backup Status	Last Backup Date	Proxmox Cluster	ONTAP Clust
100	sie-dev-aka-tst-1-89a2e		Success	11/03/2026, 11:44:00	SMPProxmox-Username	SMPProxClus
101	sie-dev-aka-tst-1-fc39f		-	-	SMPProxmox-Username	SMPProxClus
102	sie-dev-aka-tst-1-ce32c		-	-	SMPProxmox-Username	SMPProxClus
103	sie-dev-aka-tst-1		-	-	SMPProxmox-Username	SMPProxClus
104	sie-dev-aka-tst-1-305c7-47f84		-	-	SMPProxmox-Username	SMPProxClus
105	sie-dev-aka-tst-1-305c7-0754c		-	-	SMPProxmox-Username	SMPProxClus
106	sie-dev-aka-tst-1-305c7-15aa6		-	-	SMPProxmox-Username	SMPProxClus
107	sie-dev-aka-tst-1-fabfa-65967		VM backup completed: 1 successful, 0 failed	-	SMPProxmox-Username	SMPProxClus

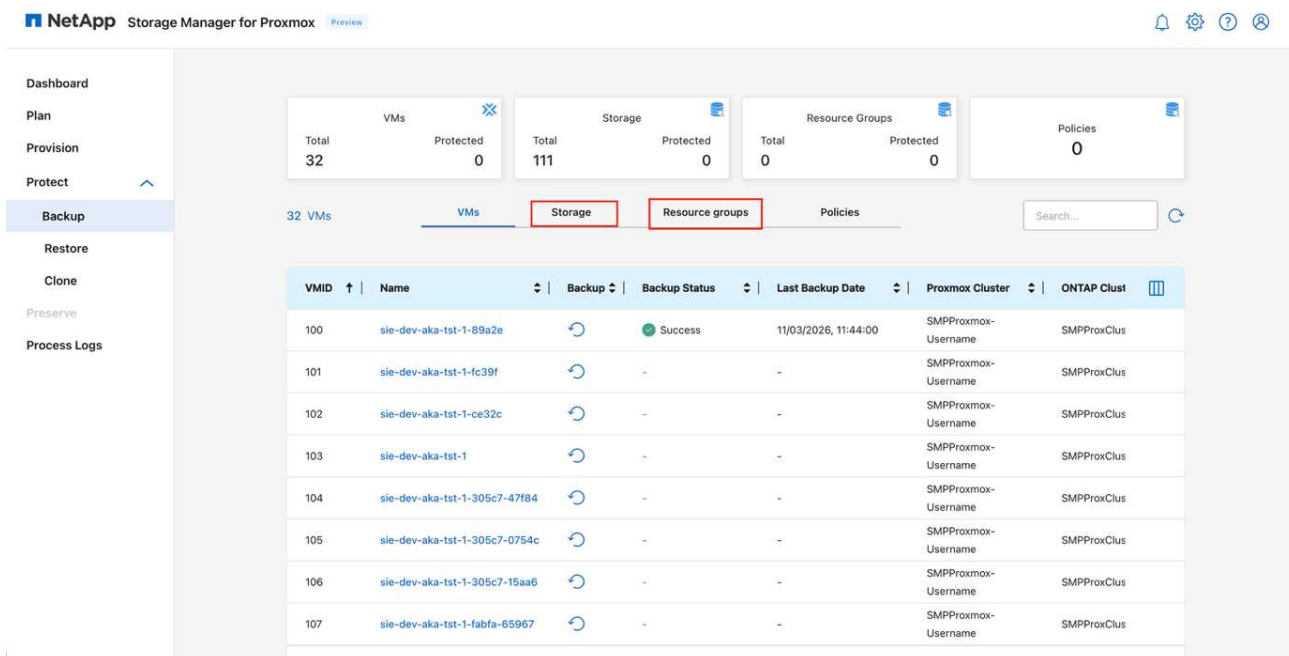


ONTAPスナップショットはボリュームレベルで取得され、NFSデータストア内のすべてのVMディスクと構成ファイルを単一のスナップショットにキャプチャします。VM整合性保護が選択されている場合、fsfreezeは選択されたVMに対してのみ発行されます。ボリューム内の他のすべてのVMは、同じONTAPスナップショット内に「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態として含まれます。

追加のバックアップ オプション

- 単一のデータストアをバックアップするには、ストレージ*タブを選択し、*バックアップ オプションを選択します。
- 複数のデータストアを1つの単位としてバックアップする場合、または異なるデータストアにまたがるVMグループを保護する場合は、*Resource Group*オプションを使用します。リソースグループを使用すると、データストアや仮想マシンを論理的な保護セットに編成できます。

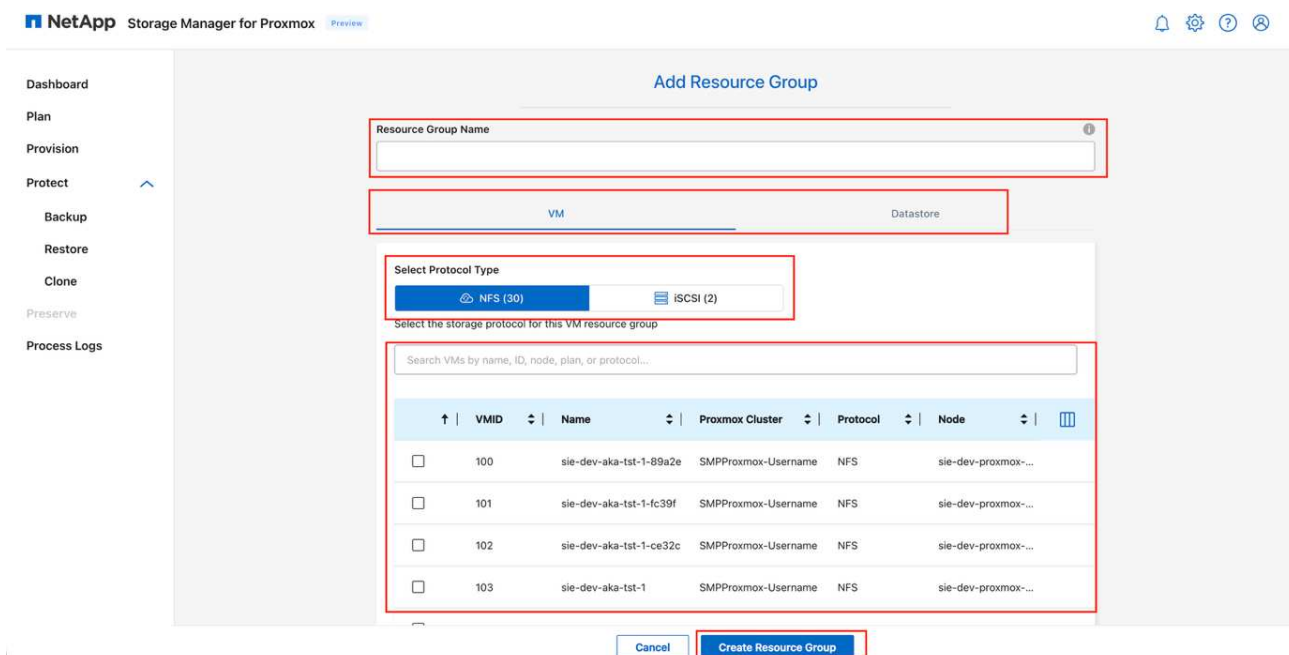
▼ リソース グループ タブを表示



リソースグループを作成する

1. **Resource Group** タブを開き、**Add** を選択します。
2. 新しいリソースグループの名前を入力します。
3. リソースの種類を選択してください：**VM** または **Datastore**。
4. 適切な*プロトコル*を選択してください。
5. 選択したリソースタイプに基づいて、含める特定のVMまたはデータストアを選択します。
6. **Create Resource Group** をクリックして設定を完了します。

▼ リソースグループの作成ダイアログを表示します



データストア（ボリューム）レベルで取得されたバックアップは常に「crash consistent state

（障害など予期しないシャットダウン時と同様）」の状態です。リソース グループには、仮想マシンまたはデータストアのいずれか1種類のリソース タイプのみを含めることができます。iSCSIベースのストレージの場合、バックアップは常に「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態です。

バックアップ ワークフローの詳細

概要のバックアップ ワークフローには、次のものが含まれます。

1. 保護範囲を定義します：保護対象がデータストア（ONTAP ボリューム）、リソース グループ（複数のボリュームまたは VM）、または個々の VM のいずれであるかを選択します。
2. 整合性方式の確認：ONTAPスナップショットの作成前に整合性を確保する方法を選択します。
 - QEMUゲストエージェントのフリーズ/解凍機能により、ゲスト内ファイルシステムの休止状態維持とWindows VSSとの統合を実現します。
3. **VM**構成ファイルをダンプします。
4. **ONTAP**スナップショットの作成：VMが一貫性のある状態にあるときに、データストア ボリュームのONTAPスナップショットをキャプチャします。これが保持されるバックアップ コピーとなります。
5. 一時的な **Proxmox** スナップショットの削除：ONTAP スナップショットの完了後に Proxmox スナップショットを削除して、差分ファイルの増大を防ぎます。
6. 保持ポリシーとレプリケーション ポリシーの適用（ポリシーの使用）：設定されたONTAP保持ポリシーを適用し、ディザスタ リカバリ レプリケーションが有効になっている場合はSnapshotセットをレプリケートします。

この手法では、変更された情報のみを保存することで、ストレージ容量とネットワーク帯域幅を最小限に抑えます。Snapshot コピーを使用して、パフォーマンスに影響を与えることなく VM またはデータストアのクイック コピーを作成し、NetApp SnapMirror テクノロジーを使用してセカンダリ システムに送信することで、長期的なオフサイト データ保護を実現します。

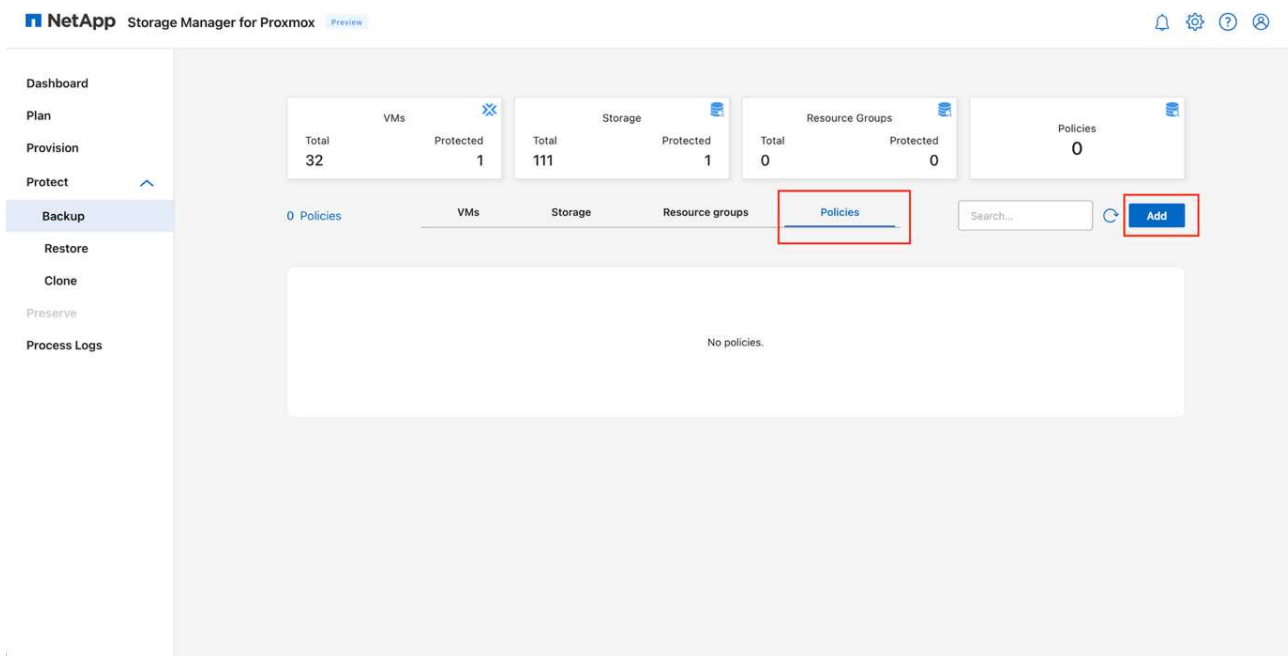
VMバックアップタスクを自動化する

スケジュールを設定することで、Proxmox VMのバックアップを自動化します。定期的なバックアップを作成することは、データ保護と災害復旧にとって非常に重要です。

手順

1. * Protect * > * Backup * > * Policies * の順に選択し、* Add * をクリックして新しいバックアップ ポリシーとスケジュールを追加します。

▼ バックアップ ポリシー ページを表示



2. 一般設定を構成する：

- a. ポリシーの名前を入力します
- b. ポリシー タイプ（ボリュームまたはリソース グループ） を選択します
- c. 選択したタイプに基づいて*ターゲット*を選択します
- d. * バックアップ頻度 *（毎時、毎日、毎週、または毎月）を設定します
- e. 「保持日数」または「保持件数」のいずれかを使用して、*保持ポリシー*を設定します（デフォルトの保持期間は7です）
- f. *レプリケーション モード*を選択します（現在のリリースでは無効）：
 - Update SnapMirror after backup
 - Update SnapVault after backup



SnapMirrorレプリケーションは、CLIまたはSystem Managerを使用してONTAPで設定する必要があります。

3. *詳細オプション*で、ONTAPスナップショットをトリガーする前にProxmoxスナップショットまたはfsfreezeを使用する場合は、*VM整合性*を有効にします。
4. * Create Policy * をクリックして設定を保存します。

▼ バックアップ ポリシーの表示：スケジュールと保持

NetApp Storage Manager for Proxmox Preview

Dashboard
Plan
Provision
Protect
Backup
Restore
Clone
Preserve
Process Logs

Add Policy

Name: demoPolicy01 Policy Type: Volume

Select Volume: SMPDemoVol

Frequency: Hourly

Retention: Days to keep: 7

Replication:
 ☐ Update SnapMirror after backup
☐ Update SnapVault after backup

Advanced Options

Cancel Create Policy

▼ バックアップ ポリシーの表示：レプリケーションと詳細オプション

NetApp Storage Manager for Proxmox Preview

Dashboard
Plan
Provision
Protect
Backup
Restore
Clone
Preserve
Process Logs

VMs: Total 32, Protected 1

Storage: Total 111, Protected 1

Resource Groups: Total 0, Protected 0

Policies: 1

1 Policies

Policy Name	Type	Target	Schedule	Retention	Status	Last Backup
demoPolicy01	datastore	SMPDemoVol	hourly	7 days	Enabled	-

1 - 1 of 1



リソース グループのスケジュールされた実行時間を待つことなく、*バックアップ*をクリックすることで、VMバックアップ ジョブを即座にトリガすることもできます。

仮想マシンまたはデータストアをリストアする

SMPを使用して、Proxmox VMをバックアップからリストアします。

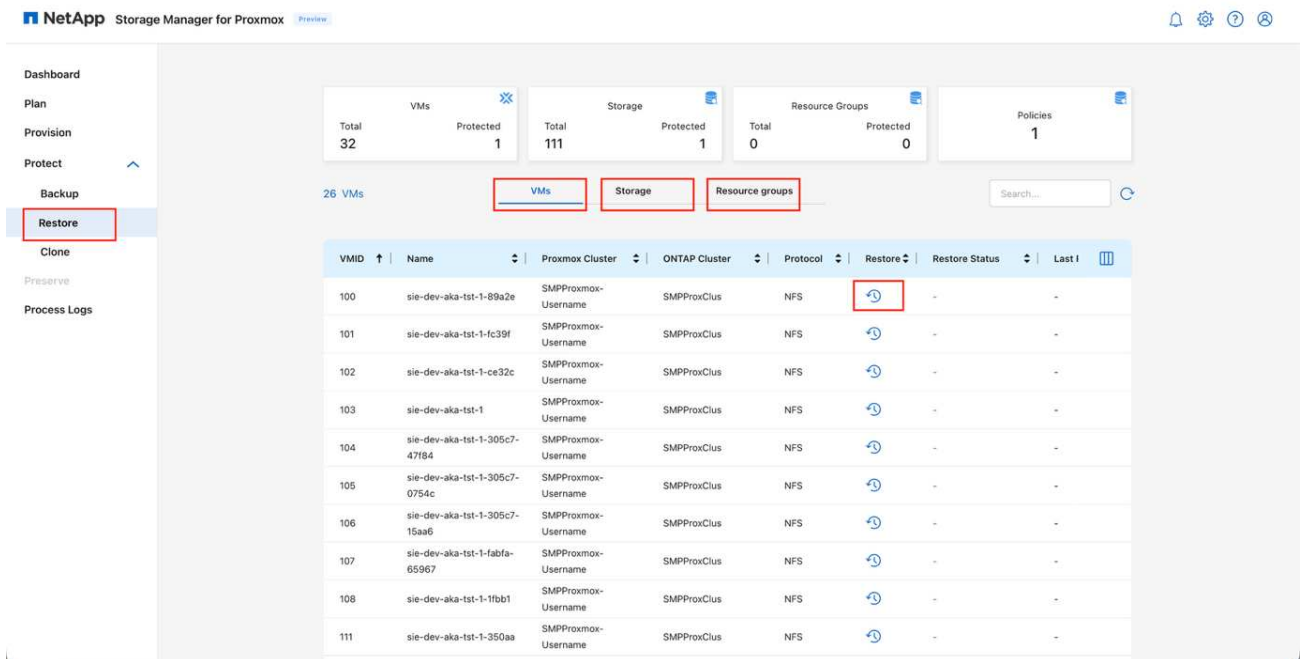
開始する前に

復元操作を実行する前に、仮想マシンの電源をオフにする必要があります。

手順

1. Web インターフェ이스の左側のナビゲーション ペインから * Restore * オプションを選択します。
2. 復元が必要な仮想マシン、ストレージ、またはリソース グループを選択します。

▼ 復元ページを表示



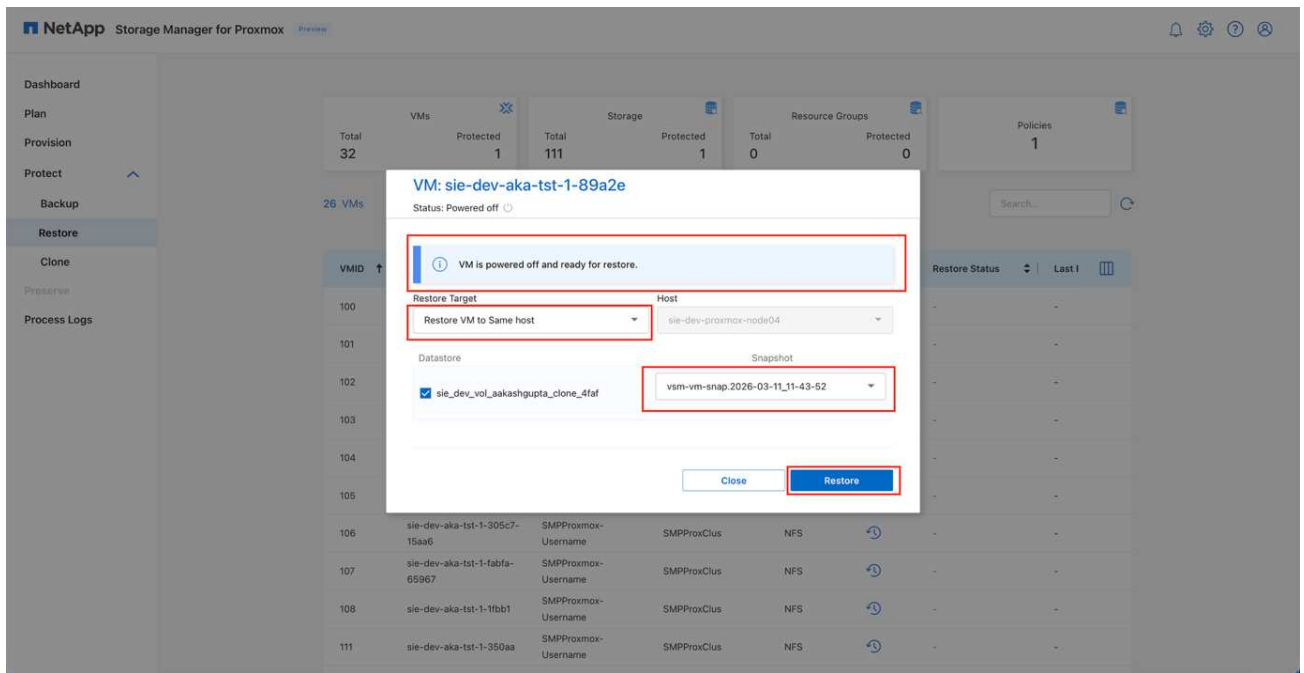
3. **Restore** アイコンをクリックします。

選択内容（VM、ストレージ、リソース グループのいずれか）に応じて、リストア ポップアップ ウィンドウが開きます。



選択したリソースに応じて、それぞれのコンポーネント用に作成されたスナップショットが表示されます。たとえば、リソース グループ レベルで作成されたスナップショットは、リソース グループが選択されている場合にのみ表示されます。ストレージについても同様です。ただし、仮想マシンの場合、コンポーネント全体で作成されたすべてのスナップショットが選択のために表示されます。

▼ リストア ダイアログの表示：Snapshot の選択

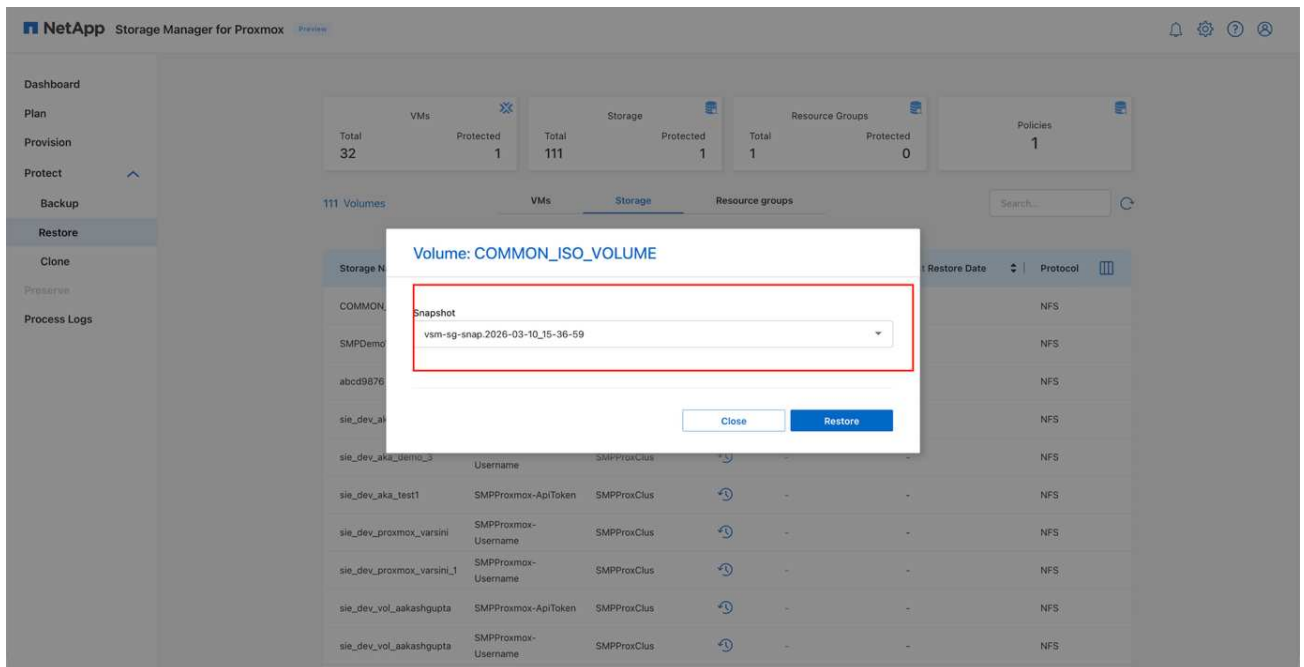


4. 必要なオプションを選択します。

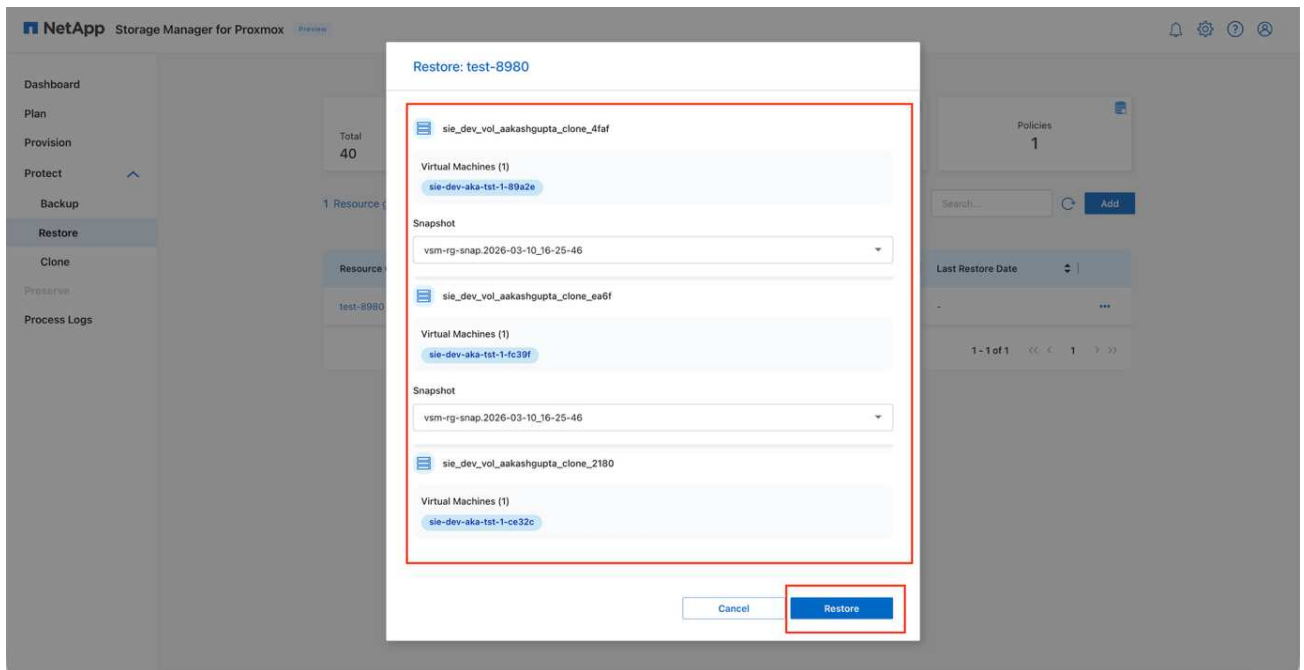
- リストア ターゲット：同じホストまたは別のホストにリストアするオプション
- ホスト：代替ホストを選択した場合、ドロップダウンリストからクラスター内の利用可能なホストを選択できます。
- スナップショット：ポイントインタイム リストアに適したスナップショットを選択します

5. * Restore * をクリックします。

▼ 進行中のリストアを表示

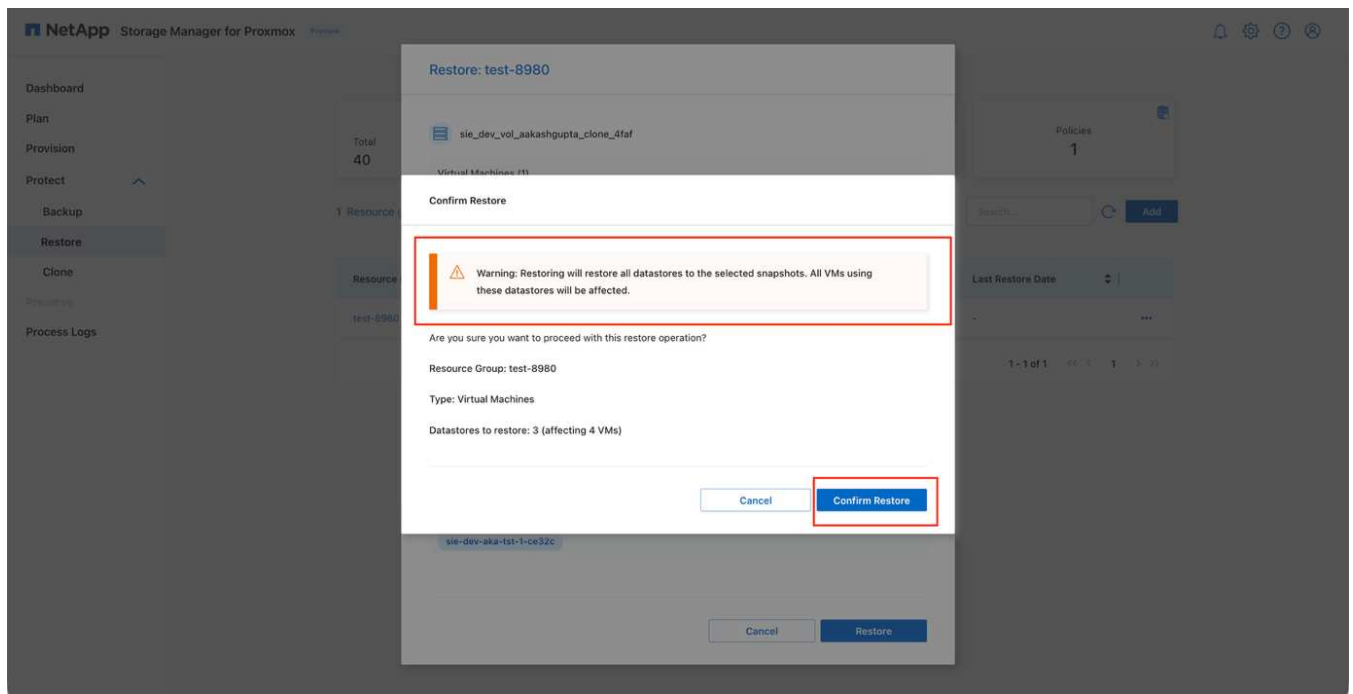


▼ 復元が完了しました



ストレージレベルのリストアが開始されると、そのボリュームまたはLUN上のすべての仮想マシンの電源がオフになり、ストレージ エンティティ全体が一括でリストアされます。

▼ ストレージレベルのリストアを表示



リストア ワークフローの詳細

リストア ワークフローは、基盤となるストレージの種類によって異なり、以下の主要な手順が含まれます：

1. 復元範囲を定義します：保護対象がデータストア（ONTAP ボリューム）、リソース グループ（複数のボリュームまたは VM）、または個々の VM のいずれかを選択します。
2. リストア処理を実行：VMのリストア プロセスは、ストレージ プロトコルによって異なります。

- **NFS** ベースのリストア：NFS上のボリュームまたはデータストアをリストアする場合、SMPはターゲット ボリューム上でボリューム スナップ リストア操作を開始します。NFSボリューム上でホストされているVMの場合、SMPはVM ID、スナップショット名、サイトID、ストレージ タイプなどのリストア パラメータを検証します。VMが実行中の場合、SMPはVMのステータスをポーリングし、停止コマンドを発行することでVMを停止します。システムはその後、ファイルレベルのリストア操作を使用して、スナップショットからVMディスクをリストアします。
- **iSCSI** ベースのリストア：iSCSI データストアまたは LUN の場合、SMP はスナップショットから LUN をリストアし、リストアされたデバイスを検証し、Proxmox ノード全体で iSCSI の再スキャンを実行し、デバイスへのアクセス可能性を確保します。iSCSI ストレージ上に存在する VM の場合、SMP はスナップショット LUN をクローンし、クローンされた LUN を Proxmox ホストにマッピングし、iSCSI 検出を実行してそれらをインポートします。リストアされたストレージが追加され、VM 構成が更新されます。VM ディスクは、VM ごとに進捗状況が追跡された上で、元のストレージに戻されます。このプロセスは、一時ストレージの削除やクローンされた LUN の削除などのクリーンアップ作業で完了します。

仮想マシンのクローニング

SMPを使用して、開発、テスト、または迅速なプロビジョニングのために仮想マシンのクローンを作成します。

手順

1. *保護*セクションを開き、左側のナビゲーションメニューから*クローン*を選択します。
2. VM リストから必要な VM を見つけ、[アクション]列の[クローン]をクリックします。
3. Clone VM ウィンドウで、クローンを作成する **Target Node** を選択します。

▼ Clone VMダイアログを表示

The screenshot shows the NetApp Storage Manager for Proxmox interface. On the left, the 'Protect' section is expanded, and the 'Clone' option is selected. The main area displays a table of VMs. The table has columns for VMID, Name, Proxmox Cluster, ONTAP Cluster, Protocol, and Actions. The 'Actions' column for each VM contains a 'Clone' button, which is highlighted with a red box in the image.

VMID	Name	Proxmox Cluster	ONTAP Cluster	Protocol	Actions
100	sie-dev-aka-tst-1-89a2e	SMPProxmox-Username	SMPDemo212	NFS	Clone
101	sie-dev-aka-tst-1-fc39f	SMPProxmox-Username	SMPDemo212	NFS	Clone
102	sie-dev-aka-tst-1-ce32c	SMPProxmox-Username	SMPDemo212	NFS	Clone
103	sie-dev-aka-tst-1	SMPProxmox-Username	SMPDemo212	NFS	Clone
104	sie-dev-aka-tst-1-305c7-47f84	SMPProxmox-Username	SMPDemo212	NFS	Clone
105	sie-dev-aka-tst-1-305c7-0754c	SMPProxmox-Username	SMPDemo212	NFS	Clone
106	sie-dev-aka-tst-1-305c7-15aa6	SMPProxmox-Username	SMPDemo212	NFS	Clone
107	sie-dev-aka-tst-1-fabfa-65967	SMPProxmox-Username	SMPDemo212	NFS	Clone
108	sie-dev-aka-tst-1-1fb01	SMPProxmox-Username	SMPDemo212	NFS	Clone
111	sie-dev-aka-tst-1-350aa	SMPProxmox-Username	SMPDemo212	NFS	Clone

4. クローンのソースとして使用する **Snapshot** を選択します。



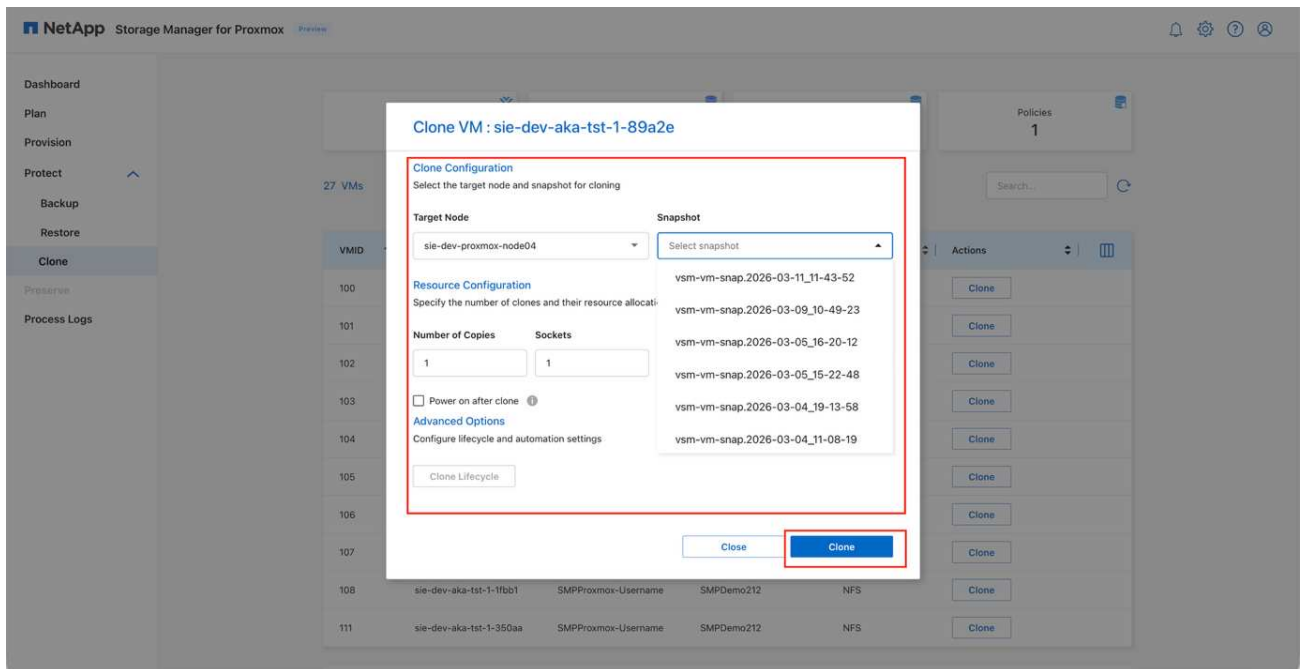
現在のリリースでは、クローンはアクティブ ファイル システムに対して実行されます。今後のリリースでは、クローンワークフローでスナップショットを選択できるようになります。選択したスナップショットから作成された新しいボリュームを使用してファイルクロ

ーンが実行されます。

5. クローンする仮想マシンの*コピー数*、**CPU**コア数、ソケット数、および*メモリ容量*を指定してください。
6. (オプション) クローンされた VM が作成後に自動的に起動するようにするには、**Power on after clone** を有効にします。
7. (オプション) クローンを新しく作成したデータストアに配置する場合は、*新しいデータストアを作成する*を選択します。
8. *詳細オプション*で、ネットワーク設定をクローンに自動的に適用する場合は*ネットワーク構成*を有効にします。
9. **Clone** をクリックしてクローニング プロセスを開始します。

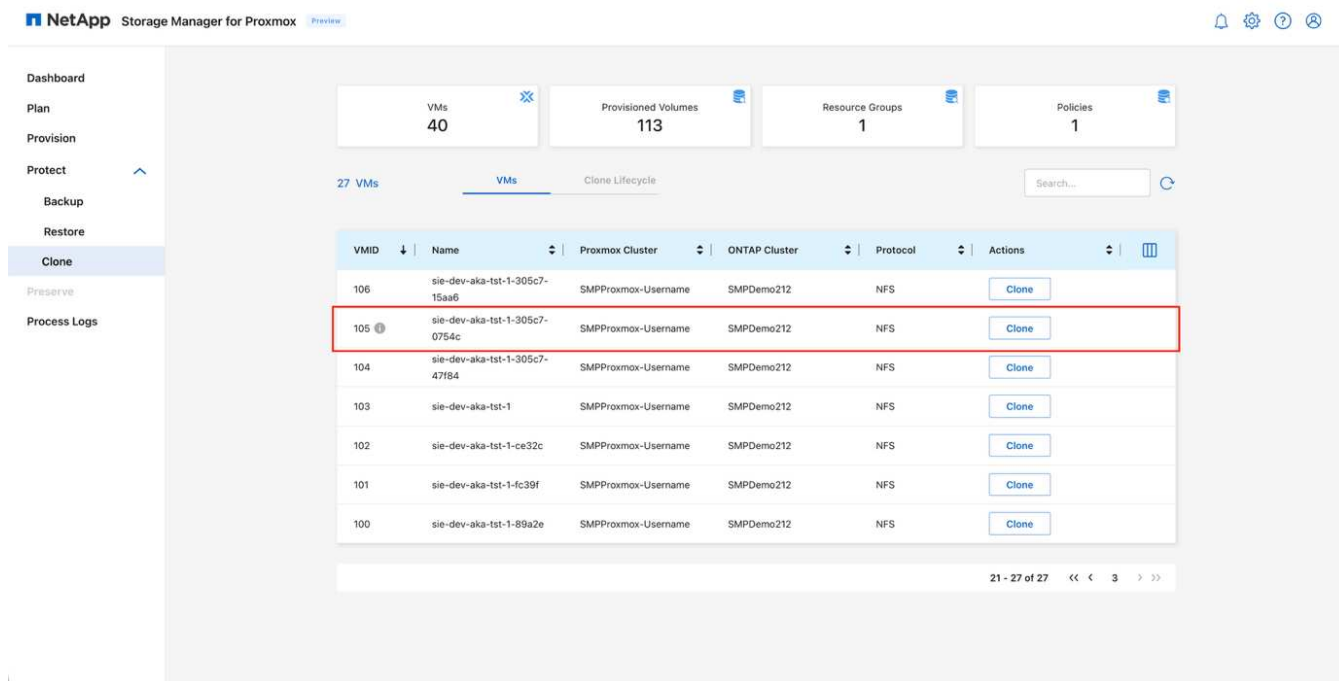
クローンワークフローは、ONTAPの高速クローニングAPIを使用して新しいVMをプロビジョニングし、クローン化されたインスタンスに一意的5桁のGUIDを割り当てます。

▼ クローン操作を表示



クローンされた VM はバックアップリストとクローンリストの両方に表示され、既存のバックアップポリシーを使用して保護できます。これらのリストにクローンされた VM を表示するには、Proxmox および ONTAP プランに対して検出を実行します。

▼ クローン VM をリストに表示



クローンワークフローの詳細

SMP は、重い処理を ONTAP にオフロードして、ホスト側でのファイルコピーではなく、ストレージ側でのクローン作成を実行することで、VM の高速クローン作成を自動化します。内部では、SMP は ONTAP FlexClone セマンティクス（スナップショットベース、書き込み可能、スペース効率に優れたクローン）を利用するため、クローンは迅速に作成され、初期段階では消費容量が少なくなります。また、可能な限り Proxmox ホストを介したデータの読み書きを回避します。

このアプローチは、クローン作業を ONTAP にプッシュすることで VM プロビジョニングを加速し、開発/テスト環境、ラボ、および迅速な更新サイクルに適した、高速で軽量、ストレージ効率の高いクローンを提供します。

デフォルトでは、クローンはアクティブ ファイル システムに対して実行されます。クローンワークフローではスナップショットを選択することも可能で、その場合は選択したスナップショットから作成された新しいボリュームを使用してファイルクローンが実行されます。

運用の監視

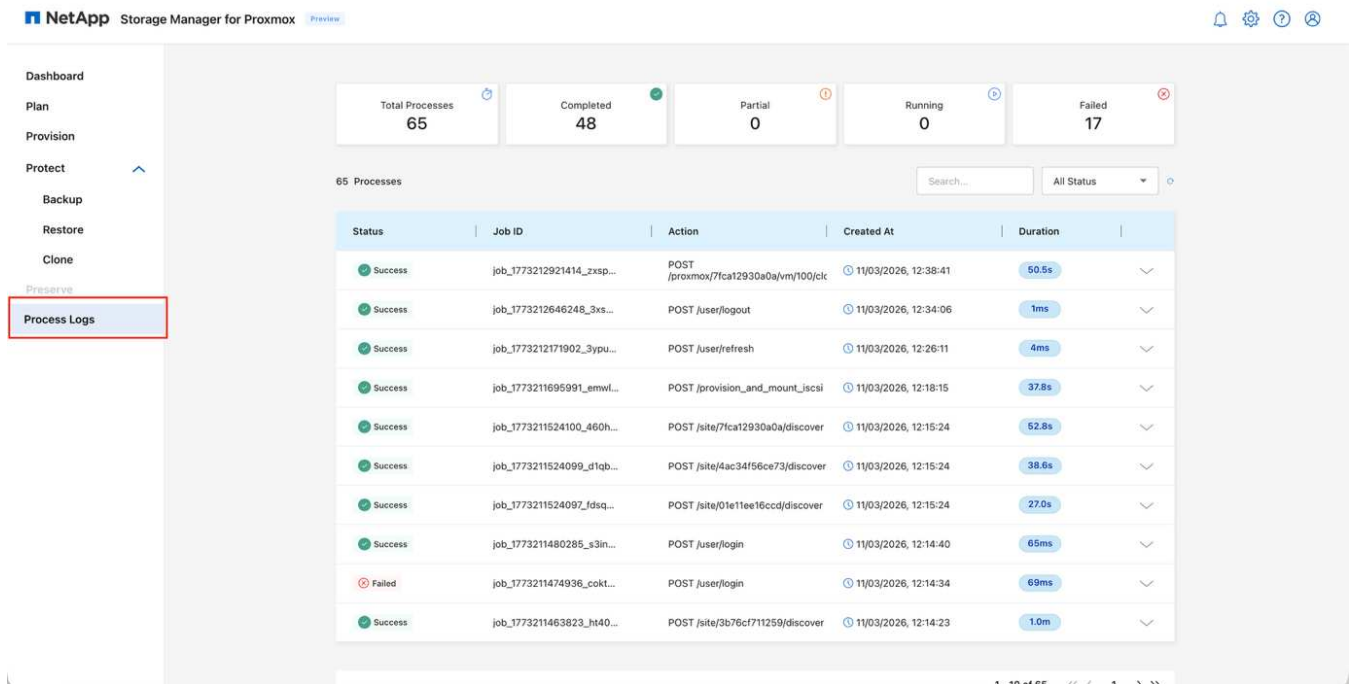
プロセスログとダッシュボードビューを使用して、SMP の操作を監視および追跡します。

プロセスログ

プロセスログビューには、Storage Manager for Proxmoxを通じて実行されたすべての操作の統合記録が表示されます。各項目には、ジョブのステータス、ジョブID、実行されたアクション、開始時刻、および所要時間が表示されます。これにより、完了したタスクの追跡、失敗した操作や部分的な操作の特定、および環境内で実行された一連のアクションの確認が容易になります。

フィルタと検索オプションを使用すると、特定のジョブをすばやく検索したり、ステータスでリストを絞り込めます。

▼ プロセスログビューの表示

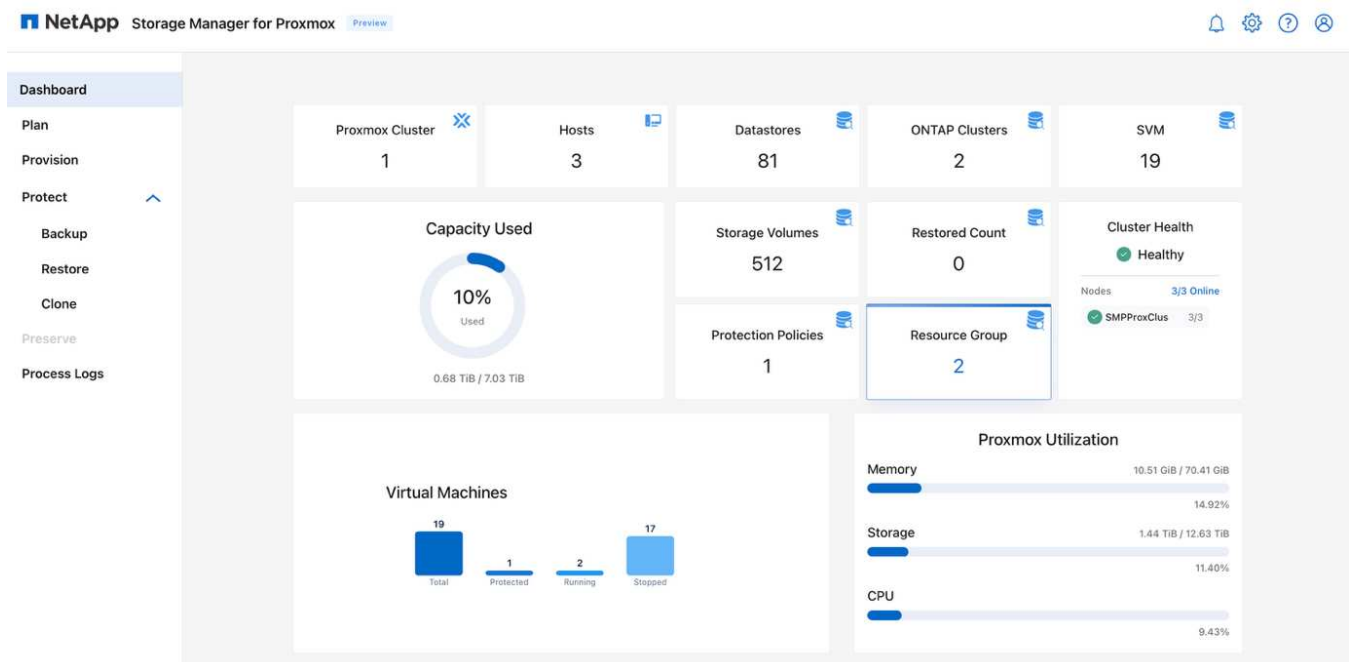


ダッシュボード

ダッシュボードは、Proxmox用Storage Manager環境全体の概要を一目で確認できる機能を提供します。Proxmoxクラスター、ホスト、データストア、ONTAPクラスター、保護された仮想マシンの数などの主要なインベントリを要約します。システムの使用状況を明確に把握できるよう、容量使用量、総ストレージボリューム、保護ポリシー、リソースグループも表示されます。

クラスターの状態が目立つように表示され、接続されているすべてのノードの状態を示します。ダッシュボードの下部には、VM の分布（合計、実行中、停止中）が強調表示され、メモリ、ストレージ、CPU のリアルタイム Proxmox リソース使用率が表示されます。このビューは、システムの健全性を迅速に評価し、リソースの負荷を特定し、全体的な運用状態を監視するのに役立ちます。

▼ ダッシュボードを表示



まとめ

Storage Manager for Proxmoxは、Proxmox環境全体にわたる保護、クローニング、およびリカバリ操作を、効率的かつ統一的に管理する方法を提供します。ONTAPと直接統合することで、このソリューションは、エンタープライズクラスのストレージの効率性、信頼性、およびパフォーマンスを日常的なVMワークフローにもたらしめます。ONTAPのスペース効率に優れたスナップショット、高速クローニング機能、および組み込みのレプリケーションにより、一貫性のある予測可能なデータ保護が実現され、SMPはこれらの機能を直感的でタスク中心のインターフェースに簡素化します。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。