テクニカル レポート

NetApp All SAN Array

NetApp ASAによるデータの可用性と整合性

2023年5月| TR-4968

概要

このドキュメントでは、NetAppオールSANアレイシステムのさまざまなデータ保護機能とデータ整合性機能に加え、最大限の信頼性を実現するためのSANネットワークの設計、実装、管理のベストプラクティスについて説明します。

目次

表一覧

図一覧

はじめに

NetApp® ONTAP®は、インライン圧縮、ハードウェアの無停止アップグレード、他社製ストレージ アレイからのLUNインポートなど、さまざまな機能を標準搭載した強力なデータ管理プラットフォームです。最大12ノードのクラスタ構成では、iSCSI、Fibre Channel（FC）、Nonvolatile Memory Express（NVMe）の各プロトコルを使用してSANにデータを同時に提供できます。さらに、NetAppスナップショット™テクノロジは、重要なデータセットの数万個のバックアップを作成し、データセットのクローンをほぼ瞬時に作成することを可能にするONTAPの不可欠な要素です。また、包括的なディザスタリカバリ機能も備えています。

NetApp All SAN Array

NetApp All-SAN Array（ASA）システムは、ONTAPを実行するNetApp AFFシステム上に構築されており、複数のワークロードのストレージリソースを統合して共有したいお客様にエンタープライズクラスのSAN解決策を提供します。

AFF SANシステムには次のようなメリットがあります。

- 業界をリードする99.9999%以上の可用性
- スケールアップとスケールアウトの両方に対応した大規模クラスタ
- 業界最高のエンタープライズ・パフォーマンス（SPC-1の監査結果に基づく）
- 先進のStorage Efficiencyテクノロジ
- 最も包括的なクラウド対応接続
- 対費用効果の高い統合データ プロテクション

NetApp ASAシステムは、AFFプラットフォーム上に構築されており、SANの継続的な可用性を実現します。これらのシステムは、計画的または計画外のストレージフェイルオーバー時にデータに中断なくアクセスできるようにし、SANワークロードの実行専用の解決策を通じて、実装、設定、管理の合理化を実現します。NetAppでは、次の要件を満たす場合にASA構成を推奨しています。

- ホストからストレージへの対称アクティブ/アクティブパスが必要なデータベースなど、ミッションクリティカルなワークロード
- SANワークロードを分離するために専用システムを使用するAFFシステムは、

引き続き次のようなお客様に推奨される選択肢です。

- SANクラスタを最大12ノードまでスケールアウトする必要がある。
- アクティブ/アクティブSANパス管理の要件はありません。
- NASとSANの混在ワークロードをサポートするために、ユニファイドプロトコルをサポートするクラスタが望ましい。

AFF ASAアーキテクチャ：データの可用性と整合性

ストレージシステムには、データを確実に保護し、データを利用できるようにするという2つの基本的な要件があります。

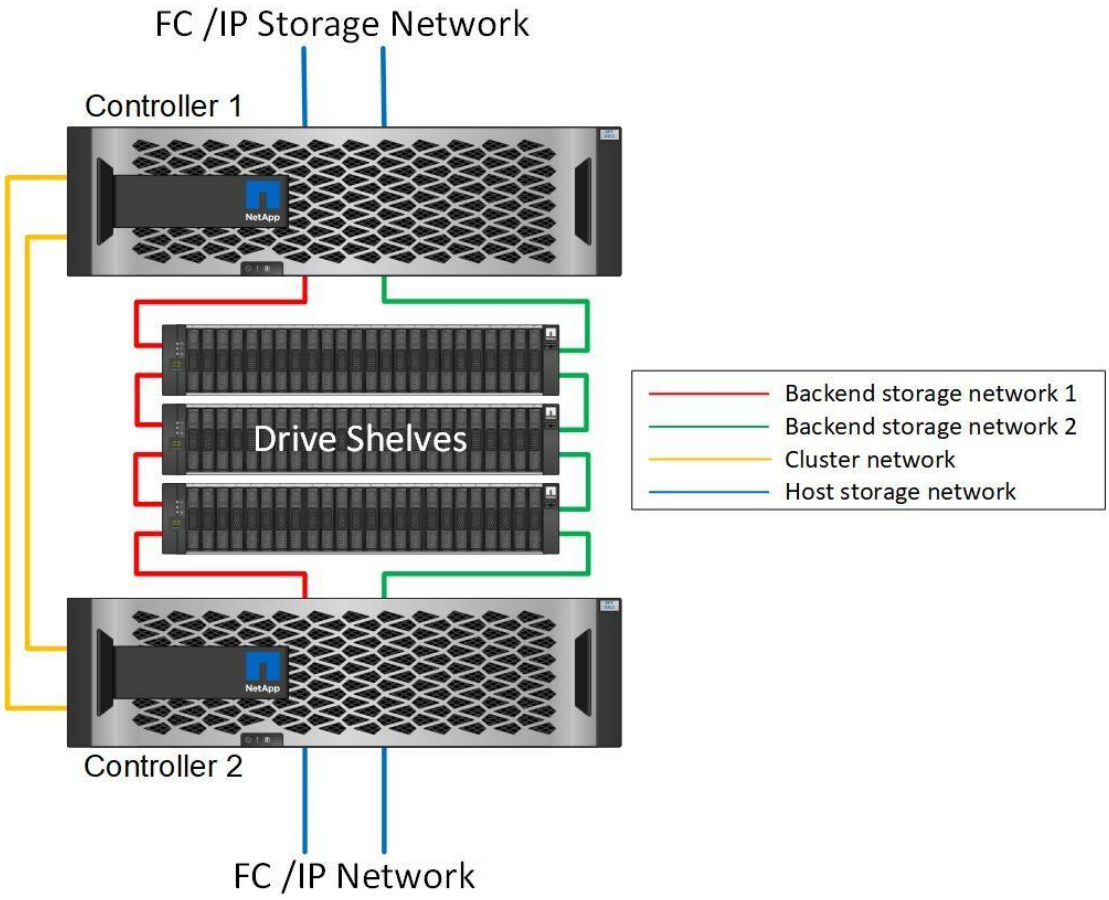
高可用性

概要of ONTAPの高可用性機能は、本ドキュメントでは扱いません。ただし、データ保護と同様に、データベースインフラを設計する際には、この機能の基本的な理解が重要です。

HAペア

ハイアベイラビリティの基本単位はHAペアです。

図1）HAペア



NVRAM

各ペアには、NVRAMデータのレプリケーションをサポートするための冗長リンクが含まれています。NVRAMは書き込みキャッシュではありません。コントローラ内部のRAMは書き込みキャッシュとして機能します。NVRAMの目的は、予期しないシステム障害から保護するためにデータを一時的にジャーナルすることです。この点では、データベースのトランザクションログに似ています。NVRAMとデータベーストランザクションログはどちらもデータを迅速に格納するために使用されるため、データに対する変更をできるだけ早くコミットできます。ドライブ上の永続的データの更新は、チェックポイントと呼ばれるプロセスの後半まで行われません。通常運用時は、NVRAMデータもデータベースのREDOログも読み取られません。

コントローラで突然障害が発生した場合、ドライブにまだ書き込まれていない保留中の変更がNVRAMに保存されている可能性があります。パートナーコントローラが障害を検出し、ドライブを制御して、NVRAMに保存されている必要な変更を適用します。

ケーブルの冗長性

上の図はHAペアのケーブル接続の例ですが、正確なレイアウトはコントローラとドライブのタイプによって異なります。いずれの場合も、冗長データパスは、物理ケーブルであっても、単一シャーシ内のバックプレーン上の電気トレースであっても存在します。コントローラには、NVRAMを介して変更をレプリケートし、I/O処理を実行したり、クラスタ内の通信を容易にしたり、クラスタ内のデータを無停止で再配置したりするためのパスが少なくとも2つあります。

電力の冗長性

すべてのコントローラ、ドライブシェルフ、およびその他のコンポーネントに冗長な電源装置が搭載されています。システムは通常、デュアルPDU（配電ユニット）を備えたサーバラックに配置され、それぞれがデータセンター内の異なるUPS保護回路に接続されます。

テイクオーバーとギブバック

テイクオーバーとギブバックは、HAペアのノード間でストレージリソースの責任を移すプロセスです。テイクオーバーとギブバックには次の2つの側面があります。

- ホストがストレージシステムへのアクセスに使用するネットワーク接続の管理
- ストレージアレイ内のドライブの管理

iSCSIやFCなどのSANブロックプロトコルをサポートするネットワークインターフェイスは、ASAシステムでのテイクオーバーやギブバックの実行中にすぐには再配置されません。コントローラで突然障害が発生した場合、パートナーコントローラはインターフェイスを使用してデータの提供を継続します。このプロセスの後半で、IPアドレスを移動する（iSCSI LIFフェイルオーバー）かHBA WWN（FCPとNVMe/FCの永続ポート）を再配置することで、障害が発生したインターフェイスがパートナーコントローラでオンラインになり、ホストがストレージへの障害パスを認識しなくなります。

注： 大規模なクラスタ内のノード間でのデータの再配置をサポートするように追加のコントローラへのパスを設定することもできますが、これはHAプロセスの一部ではありません。

テイクオーバーとギブバックの2つ目の側面は、ディスク所有権の移行です。具体的なプロセスは、テイクオーバーやギブバックの理由、実行したコマンドラインオプションなど、複数の要因によって異なります。目標は、できるだけ効率的に操作を実行することです。全体的なプロセスには数分かかるように見えるかもしれませんが、ドライブの所有権がノードからノードに移行される実際の瞬間は、通常数秒で測定できます。

テイクオーバーのトリガー

テイクオーバーは、次のようなさまざまな理由で発生します。

- `storage failover takeover` コマンドを使用してテイクオーバーを手動で開始します。
- ソフトウェアまたはシステムの障害が発生し、コントローラがパニック状態になる。パニックが完了してコントローラがリブートすると、ストレージリソースがギブバックされ、システムが通常の状態に戻ります。
- コントローラに電源の喪失など、システム全体の障害が発生し、リブートできない。
- パートナーコントローラがハートビートメッセージを受信できません。この状況は、パートナーでハードウェアまたはソフトウェア障害が発生し、パニックにはならなかったが、正常な機能は失った場合に発生します。

NDO

「ノンストップオペレーション」という用語には、コントローラの突然の障害に対処する機能だけでなく、コントローラをオンラインでアップグレードおよび保守できる機能も含まれます。コントローラがデータサービスの責任をパートナーに委譲すると、管理者はONTAP OSのアップグレード、障害が発生したハードウェアの交換、新しいアダプタの追加、さらにはコントローラ自体の更新を行うことができます。

テイクオーバー時間

NetApp ASAでは、両方のコントローラを経由するアクティブ/アクティブパスを使用できるため、ホストOSはアクティブパスの停止を待ってから代替パスをアクティブ化する必要がありません。ホストはすでにすべてのコントローラのすべてのパスを使用しており、システムが安定した状態であるかコントローラのフェイルオーバー処理を実行しているかにかかわらず、ホストには常にアクティブなパスがあります。

また、ASAには、SANフェイルオーバープロセスを大幅に高速化する独自の機能が搭載されています。各コントローラは、重要なLUNメタデータをパートナーに継続的にレプリケートします。このように、各コントローラには、障害が発生したコントローラで以前管理されていたドライブの使用を開始するために必要なコア情報がすでに用意されているため、パートナーで突然障害が発生した場合でも、すぐにデータの提供が開始されます。

表1）フェイルオーバー時間

タイプ：	IO再開時間
計画的なテイクオーバー	2～3秒
計画外のテイクオーバー	2～3秒

この時間は、オペレーティングシステムでの完全なI/O再開時間を反映しています。フェイルオーバーにかかる時間は、ストレージシステムのIO応答能力だけを測定すると短くなりますが、より重要なのは、ホストから見たI/O再開時間です。

データの整合性

ONTAPでの論理データ保護は、次の3つの重要な要件で構成されます。

- データを破損から保護する必要があります。
- データはドライブ障害から保護する必要があります。
- データの変更は損失から保護する必要があります

これらの3つのニーズについては、以降のセクションで説明します。

ネットワークの破損：チェックサム

最も基本的なデータ保護レベルはチェックサムです。チェックサムは、データと一緒に格納される特別なエラー検出コードです。ネットワーク転送中のデータの破損は、チェックサムを使用して検出されます。場合によっては、複数のチェックサムを使用します。

たとえば、FCフレームには巡回冗長検査（CRC）と呼ばれるチェックサム形式が含まれており、転送中にペイロードが破損していないことを確認できます。送信機は、データのデータとCRCの両方を送信します。FCフレームの受信側は、受信したデータのCRCを再計算して、送信されたCRCと一致することを確認します。新しく計算されたCRCがフレームに接続されたCRCと一致しない場合、データは破損し、FCフレームは破棄または拒否されます。iSCSI I/O処理には、TCP/IPおよびイーサネットレイヤでのチェックサムが含まれます。また、保護を強化するために、SCSIレイヤでオプションのCRC保護を含めることもできます。ワイヤ上のビットの破損はTCPレイヤまたはIPレイヤによって検出され、パケットが再送信されます。FCと同様に、SCSI CRCでエラーが発生すると、処理が破棄または拒否されます。

ドライブの破損：チェックサム

チェックサムは、ドライブに格納されているデータの整合性を検証するためにも使用されます。ドライブに書き込まれたデータブロックは、元のデータに関連付けられた予測不可能な数を生成するチェックサム機能で格納されます。
ドライブからデータが読み取られると、チェックサムが再計算され、保存されているチェックサムと比較されます。一致しない場合は、データが破損しているため、RAIDレイヤでリカバリする必要があります。

データ破損：失われた書き込み

検出するのが最も困難な種類の破損の1つは、書き込みの紛失または置き忘れです。書き込みが確認応答されたら、正しい場所にあるメディアに書き込む必要があります。インプレースデータの破損は、データとともに保存されたシンプルなチェックサムを使用することで、比較的簡単に検出できます。ただし、書き込みが失われただけの場合は、以前のバージョンのデータがメディアに残っている可能性があり、基盤となるブロ

ックのチェックサムが正しいことになります。書き込みが間違った物理的な場所に配置された場合、書き込みによって他のデータが破壊されても、関連するチェックサムは保存データに対して再び有効になります。

この課題に対する解決策は次のとおりです。

- 書き込み処理には、書き込みが予想される場所を示すメタデータが含まれている必要があります。
- 書き込み処理には、何らかのバージョン識別子が含まれている必要があります。

ONTAPがブロックを書き込むときは、そのブロックが属する場所のデータも含まれます。後続の読み取りでブロックが識別されていても、メタデータにブロックが456の場所で見つかったときに123の場所に属していることが示されている場合、書き込みは誤って配置されています。

完全に失われた書き込みを検出することは、より困難です。説明は非常に複雑ですが、基本的には、書き込み処理によってドライブ上の2つの場所が更新されるように、ONTAPはメタデータを格納します。書き込みが失われると、その後のデータおよび関連するメタデータの読み取りで、2つの異なるバージョンIDが表示されます。これは、ドライブによる書き込みが完了しなかったことを示します。

書き込みが失われたり誤って配置されたりすることは非常にまれですが、ドライブが増え続け、データセットがエクサバイト規模になると、リスクが増大します。重要なデータセットをサポートするストレージシステムには、Lost Writeの検出機能を含める必要があります。

ドライブ障害：RAID、RAID DP、RAID-TEC

ドライブ上のデータブロックが破損していることが検出された場合、またはドライブ全体で障害が発生して完全に使用できなくなった場合は、データを再構成する必要があります。これは、パリティドライブを使用するONTAPで実行されます。データが複数のデータドライブにストライピングされ、パリティデータが生成されます。これは元のデータとは別に保存されます。

ONTAPは元々 RAID 4を使用していました。RAID 4は、データドライブのグループごとにパリティドライブを1本使用します。その結果、グループ内のいずれかのドライブで障害が発生してもデータが失われることはありませんでした。パリティドライブで障害が発生してもデータは破損しておらず、新しいパリティドライブを構築できました。1本のデータドライブで障害が発生した場合は、残りのドライブをパリティドライブと一緒に使用して失われたデータを再生成します。

ドライブが小さい場合、2本のドライブで同時に障害が発生する可能性はほとんどありませんでした。ドライブ容量の増大に伴い、ドライブ障害発生後のデータの再構築に必要な時間も増加しています。これにより、2つ目のドライブ障害が発生してデータが失われる時間が長くなりました。また、再構築プロセスでは、稼働しているドライブに多くのI/Oが追加で作成されます。ドライブが古くなると、負荷が増えて2つ目のドライブ障害が発生するリスクも高まります。最後に、RAID 4を継続して使用することでデータ損失のリスクが増加しなかったとしても、データ損失の影響はより深刻になります。RAIDグループで障害が発生した場合に失われるデータが多いほど、データのリカバリにかかる時間が長くなり、ビジネスの中断が長くなります。

これらの問題により、NetAppはRAID 6の一種であるNetApp RAID DP®テクノロジを開発しました。この解決策にはパリティドライブが2本含まれているため、RAIDグループ内の2本のドライブで障害が発生してもデータが失われることはありません。ドライブは成長を続けており、最終的にNetAppは3つ目のパリティドライブを導入するNetApp RAID-TEC™テクノロジを開発しました。

一部のSANのベストプラクティスでは、ストライプミラーリングとも呼ばれるRAID-10の使用が推奨されています。2本のディスクで障害が発生するシナリオが複数あるのに対し、RAID DPでは何も発生しないため、RAID DPよりもデータ保護が劣ります。

また、パフォーマンス上の懸念から、RAID-4 / 5 / 6よりもRAID-10が推奨されることを示す、従来のSANのベストプラクティスドキュメントもいくつかあります。これらの推奨事項は、RAIDペナルティを意味する場合があります。これらの推奨事項は一般的に正しいものですが、ONTAP内でのRAIDの実装には適用されません。パフォーマンスの問題はパリティ再生に関連しています。従来のRAID実装では、書き込みを処理するには、パリティデータを再生成して書き込みを完了するために、複数のディスク読み取りが必要です。ペナルティは、書き込み処理の実行に必要な追加の読み取りIOPSとして定義されます。

書き込みはメモリでステージングされ、パリティが生成されてから単一のRAIDストライプとしてディスクに書き込まれるため、ONTAPではRAIDペナルティは発生しません。書き込み処理を完了するための読み取りは必要ありません。

要約すると、RAID DPとRAID-TECは、RAID 10と比較して使用可能な容量がはるかに多く、ドライブ障害に対する保護が強化され、パフォーマンスが低下することはありません。

ハードウェア障害からの保護:NVRAM

レイテンシの影響を受けやすいワークロードを処理するストレージアレイは、できるだけ早く書き込み処理を承認する必要があります。さらに、電源障害などの予期しないイベントから書き込み処理を損失から保護する必要があります。つまり、書き込み処理は少なくとも2つの場所に安全に格納する必要があります。

ASAシステムは、これらの要件を満たすためにNVRAMを利用しています。書き込みプロセスは次のように機能します。

1. インバウンド書き込みデータはRAMに格納されます。
2. ディスク上のデータに加えなければならない変更は、ローカルノードとパートナーノードの両方のNVRAMに記録されます。NVRAMは書き込みキャッシュではなく、データベースのRedoログに似たジャーナルです。通常の条件下では、読み取りは行われません。I/O処理中に電源障害が発生した場合など、リカバリにのみ使用されます。
3. その後、書き込みがホストに確認応答されます。

この段階の書き込みプロセスはアプリケーションの観点からは完了しており、データは2つの異なる場所に格納されるため、損失から保護されます。最終的に変更はディスクに書き込まれますが、書き込みが確認されたあとに実行されるためレイテンシに影響しないため、このプロセスはアプリケーションの観点からはアウトオブバンドです。このプロセスもデータベースロギングに似ています。データベースに対する変更はできるだけ早くREDOログに記録され、変更がコミットされたことが確認されます。データファイルの更新はかなり遅れて行われ、処理速度に直接影響することはありません。

コントローラで障害が発生すると、パートナーコントローラが必要なディスクの所有権を取得し、ログに記録されたデータをNVRAMに再生して、障害発生時に転送中だったI/O処理をリカバリします。

冗長性エラー：NVFAIL

前述したように、書き込みの確認応答は、少なくとも1台の他のコントローラでローカルのNVRAMとNVRAMに記録されるまで返されません。このアプローチにより、ハードウェア障害や停電が発生しても、転送中のI/Oが失われることはありません。ローカルのNVRAMに障害が発生したり、他のノードへの接続に障害が発生したりすると、データはミラーリングされなくなります。

ローカルNVRAMからエラーが報告されると、ノードはシャットダウンします。このシャットダウンにより、HAペアが使用されている場合はパートナーコントローラにフェイルオーバーされます。MetroClusterでは、動作は選択した全体的な設定によって異なりますが、リモートコントローラへの自動フェイルオーバーが実行される場合があります。

いずれの場合も、障害が発生したコントローラが書き込み処理を認識していないため、データは失われません。データ損失は、確認済みの書き込みが失われることを意味します。ファイルシステムとアプリケーションを使用したブロックストレージ管理の主な原則は、確認応答前の書き込みが永続的ストレージに存在する場合と存在しない場合があります。これは、書き込みがストレージシステムで受信される前にOSが書き込みが失われたかどうかを知る方法がないためです。 認識だけが失われたのかということです確認応答が受信されるまで、書き込みの状態は不確定です。

データ保護

前のセクションでは、ストレージハードウェアに関するデータの可用性と整合性について説明します。データの可用性と整合性の同様に重要な側面は、避けられないユーザやアプリケーションのエラーからリカバリする機能です。ストレージアレイで99.999%のアップタイムを必要とする企業は、大規模化するデータセットを迅速かつ確実にリカバリできるバックアップ/リカバリ戦略も計画する必要があります。

Snapshotコピーによるデータ保護

NetApp ONTAPデータ保護ソフトウェアの基盤となるのが、NetAppのSnapshotテクノロジです。表示される値は次のとおりです。

- **簡易性**Snapshotコピーは、特定の時点のデータコンテナの内容の読み取り専用コピーです。
- **効率性：**Snapshotコピーの作成時にスペースは必要ありません。スペースが消費されるのは、データが変更されたときだけです。
- **管理性：**Snapshotコピーはストレージ**OS**に標準搭載されているため、Snapshotコピーに基づくバックアップ戦略を簡単に設定および管理できます。ストレージシステムの電源がオンになっていれば、バックアップを作成できます。
- **拡張性：**1つのLUNの最大1024個のスナップショットをローカルに保持できます。複雑なデータセットの場合、データの複数のコンテナを、整合性のある単一のSnapshotコピーセットで保護できます。
- ボリュームに1、024個のSnapshotコピーが含まれているかどうかに関係なく、パフォーマンスには影響しません。

そのため、ONTAPで実行されているデータセットの保護はシンプルで拡張性に優れています。バックアップでは、データの移動は必要ありません。したがって、バックアップ戦略は、ネットワーク転送速度、大量のテープドライブ、高価なディスクステージング領域などの制約を受けることなく、ビジネスのニーズに合わせて調整できます。

ONTAP SnapRestoreによるデータのリストア

NetApp SnapRestore® テクノロジを使用して、ONTAPでSnapshotコピーからデータを迅速にリストアできます。表示される値は次のとおりです。

- 個々のファイルやLUNは、16TBのLUNでも4KBのファイルでも、数秒でリストアできます。
- LUNやファイルのコンテナ（NetApp FlexVol®ボリューム）全体を、10GBまたは100TBのデータであれ、数秒でリストアできます。

重要なアプリケーションが停止すると、重要なビジネスの運用が停止します。テープが破損する可能性があり、ディスク・ベースのバックアップからリストアする場合でも、ネットワーク上での転送に時間がかかることがあります。SnapRestoreは、重要なデータセットをほぼ瞬時にリストアすることで、このような問題を回避します。ペタバイト規模のデータベースでも、わずか数分で完全にリストアできます。

SnapMirrorでデータ保護

SnapMirrorは、管理が容易で、拡張性と効率性に優れたレプリケーションテクノロジです。また、データだけでなくスナップショットもレプリケートできます。バックアップの一部またはすべてをリモートサイトやクラウドに選択的に保存できます。は、何があってもバックアップを確実に利用できるようにします。また、スナップショットテクノロジの効率性により、ネットワークインフラストラクチャとストレージ容量に対する要求を最小限に抑えることができます。

ONTAP FlexCloneによるデータのリストア

すべてのデータセットをインプレースで簡単にリストアできるわけではありません。場合によっては、データセットのリストアではなく修復が必要になることがあります。データをリストアできるのと同じテクノロジを使用すれば、現在のデータに影響を与えずにデータのクローンを作成することもできます。

- 個々のファイルやLUNは、16TBのLUNでも4KBのファイルでも、数秒でクローニングできます。
- LUNやファイルのコンテナ（NetApp FlexVolボリューム）全体を、10GBのデータでも100TBのデータでも、数秒でクローニングできます。
- クローンは、データの任意のコピー（ローカル、リモート、クラウド）から作成できます。

管理者は、クローンを検証し、必要に応じてデータを抽出し、データセットを修復できます。

ディザスタ リカバリ

単一のASAシステムで、ハードウェアレベルで最大限の可用性を実現し、高速リストア機能によってユーザやアプリケーションのエラーに対処できます。では、災害はどうなるのでしょうか。電源が完全に遮断された場合やサイトが破壊された場合に、どのようにして継続的なデータ可用性を提供しますか。

NetApp ASAシステムは、NetApp MetroClusterとSnapMirrorビジネス継続性の2つのオプションをサポートしています。

注： 災害時のデータ損失が許容される場合は、ディザスタリカバリのニーズに合わせて、ASAシステムのSnapshotを非同期でレプリケートすることもできます。

MetroClusterテクノロジ

NetApp MetroClusterは、ミッションクリティカルなワークロードに可用性とデータ損失ゼロの解決策を提供します。さらに、MetroClusterなどの統合ソリューションにより、今日の複雑なスケールアウト型エンタープライズアプリケーションや仮想化インフラが簡素化されます。MetroClusterは、複数の外部データ保護製品と戦略を1つのシンプルな中央集中型ストレージアレイに置き換え、単一のクラスタストレージシステム内でバックアップ、リカバリ、ディザスタリカバリ、高可用性（HA）を統合します。

MetroClusterヲシヨウシタHA

MetroClusterレプリケーションは、同期モードへの切り替えが簡単に行えるように設計された、NetApp SyncMirror®テクノロジを基盤としています。この機能は、同期レプリケーションを必要とする一方で、データサービスに高可用性も必要とするお客様の要件を満たします。たとえば、リモートサイトへの接続が切断されている場合は、通常、ストレージシステムを非レプリケート状態で動作させておくことを推奨します。

多くの同期レプリケーションソリューションは、同期モードでしか動作できません。このタイプのall-or-nothingレプリケーションは、Dominoモードと呼ばれることがあります。このようなストレージシステムは、データのローカルコピーとリモートコピーが非同期になるのではなく、データの提供を停止します。レプリケーションが強制的に解除された場合、再同期には非常に時間がかかり、ミラーリングの再確立中にデータが完全に失われる可能性があります。

リモートサイトに到達できない場合にSyncMirrorを同期モードからシームレスに切り替えることができるだけでなく、接続がリストアされたときにRPO=0状態に迅速に再同期することもできます。再同期中にリモートサイトにある古いデータコピーを使用可能な状態で保持することもできるため、データのローカルコピーとリモートコピーを常に維持できます。

MetroClusterとSyncMirror

ONTAPの同期レプリケーションはSyncMirrorによって提供されます。最も単純なレイヤでは、SyncMirrorは2つの異なる場所にRAID保護データの完全なセットを作成します。データセンター内の隣接する部屋に配置することも、数キロメートル離れた場所に配置することもできます。

SyncMirrorはONTAPと完全に統合されており、RAIDレベルのすぐ上で動作します。そのため、Snapshotコピー、SnapRestore、NetApp FlexClone®など、ONTAPの通常の機能はすべてシームレスに動作します。それはまだONTAPです。同期データミラーリングのレイヤが追加されただけです。

SyncMirrorデータを管理するONTAPコントローラの集まりをNetApp MetroClusterと呼びます。多くの構成を使用できます。MetroClusterの主な目的は、一般的な障害やディザスタリカバリのさまざまな障害シナリオで、同期ミラーリングされたデータへの高可用性アクセスを提供することです。

MetroClusterとSyncMirrorを使用したデータ保護の主な価値は次のとおりです。

- 通常運用時には、SyncMirrorは複数のサイト間の同期ミラーリングを保証します。書き込み処理は、両方のサイトの不揮発性メディアに存在するまで確認応答されません。
- サイト間の接続に障害が発生すると、SyncMirrorは自動的に非同期モードに切り替わり、接続が回復する

までプライマリサイトがデータを提供し続けます。リストア時には、プライマリサイトに蓄積された変更を効率的に更新することで、迅速な再同期を実現します。完全な再初期化は必要ありません。

SnapMirrorは、SyncMirrorベースのシステムとも完全に互換性があります。たとえば、プライマリデータベースが2つの地理的なサイトに分散したMetroClusterクラスタで実行されているとします。このデータベースは、長期アーカイブやDevOps環境でのクローン作成のために、バックアップを第3のサイトにレプリケートすることもできます。

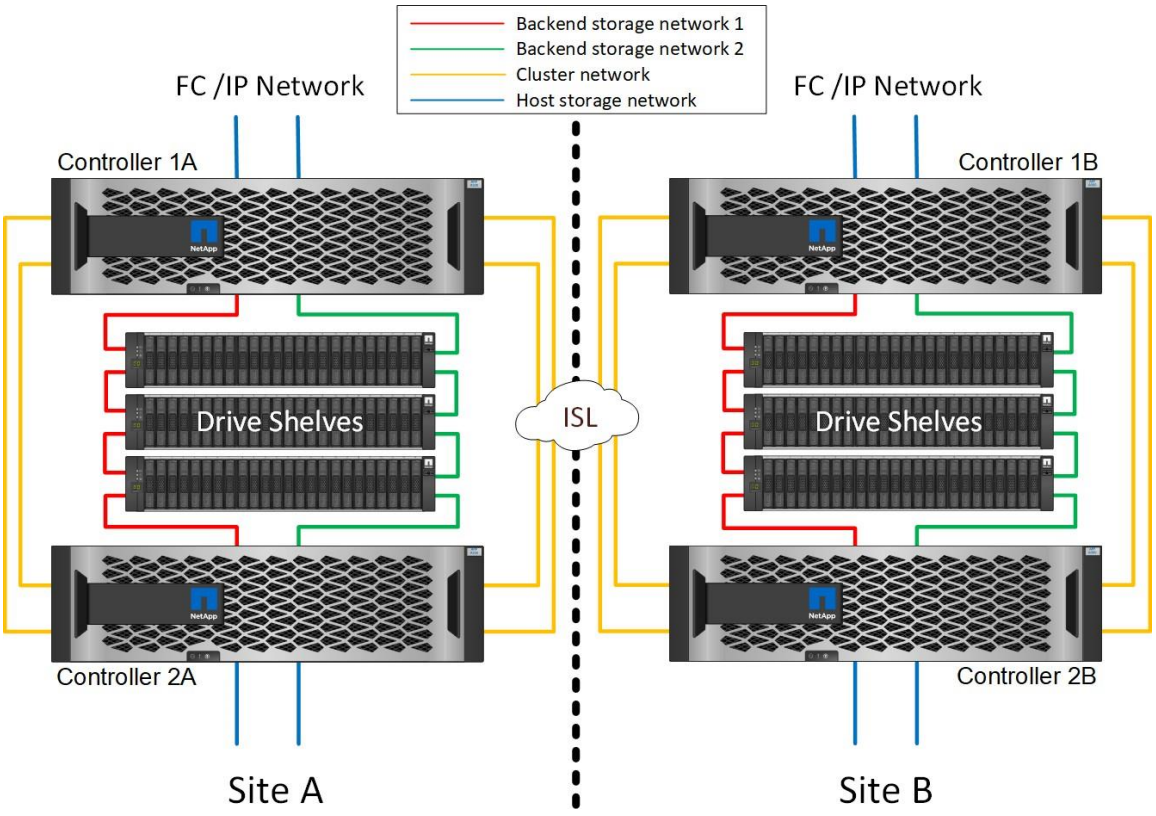
MetroClusterのアーキテクチャ

MetroClusterの完全な説明はこのドキュメントの範囲外ですが、その中核的な可用性機能について理解しておく必要があります。以降のセクションでは、IPベースのMetroClusterを使用して説明します。ほとんどのお客様は、インフラストラクチャ要件がシンプルであるため、IP接続を選択しています。従来は、ダークファイバやFCスイッチを使用した場合、サイト間での高速接続のプロビジョニングは一般的に容易でしたが、今日では、高速で低レイテンシのIP回線がより容易に利用できるようになりました。

追加情報については、ONTAPの公式ドキュメントおよびMetroCluster IP解決策のアーキテクチャと設計を参照してください。

IP接続を使用するMetroClusterシステムは、各サイトでHAペアを使用して構成されます。

図2）MetroCluster IPの基本アーキテクチャ



MetroClusterの耐障害性機能

上の図に示すように、MetroCluster 解決策 には単一点障害（Single Point of Failure）はありません。

- 各コントローラに、ローカルサイトのドライブシェルフへの独立したパスが2つあります。
- 各コントローラに、リモートサイトのドライブシェルフへの独立したパスが2つあります。

- 各コントローラには、反対側のサイトのコントローラへの独立したパスが2つあります。
- HAペア構成では、各コントローラからローカルパートナーへのパスが2つあります。

つまり、構成内のコンポーネントを1つでも削除しても、MetroClusterのデータ提供機能を損なうことはありません。2つのオプションの耐障害性の違いは、サイト障害後もHAペアバージョンが全体的なHAストレージシステムになる点だけです。

サイト障害からの保護：NVRAMとMetroCluster

MetroClusterは、 ローカルパートナーとリモートパートナーの両方にNVRAMデータをレプリケートすることで、NVRAMデータ保護を強化します。書き込みは、すべてのパートナーにレプリケートされるまで確認応答されない

このアーキテクチャは、転送中のI/Oをサイト障害から保護します。このプロセスは、ドライブレベルのデータレプリケーションには関係ありません。アグリゲートを所有するコントローラは、アグリゲート内の両方のプレックスに書き込むことでデータレプリケーションを実行しますが、サイトが失われた場合でも転送中のI/Oの損失からデータを保護する必要があります。レプリケートされたNVRAMデータは、障害が発生したコントローラをパートナーコントローラがテイクオーバーする必要がある場合にのみ使用されます。

サイトおよびシェルフ障害からの保護：SyncMirrorとプレックス

SyncMirrorは、RAID DPやRAID-TECを強化するミラーリングテクノロジですが、これに代わるものではありません。2つの独立したRAIDグループの内容をミラーリングします。論理構成は次のとおりです。

1. ドライブは、場所に基づいて2つのプールに構成されます。1つのプールはサイトAのすべてのドライブで構成され、2つ目のプールはサイトBのすべてのドライブで構成されます。
2. 次に、アグリゲートと呼ばれる共通のストレージプールが、RAIDグループのミラーセットに基づいて作成されます。各サイトから同じ数のドライブが引き出されます。たとえば、20ドライブのSyncMirrorアグリゲートは、サイトAの10本のドライブとサイトBの10本のドライブで構成されます。
3. サイト上の各ドライブセットは、ミラーリングを使用せずに、完全に冗長化された1つ以上のRAID DPグループまたはRAID-TECグループとして自動的に構成されます。ミラーリングの下でRAIDを使用することで、サイトが失われた場合でもデータを保護できます。

図3）SyncMirror

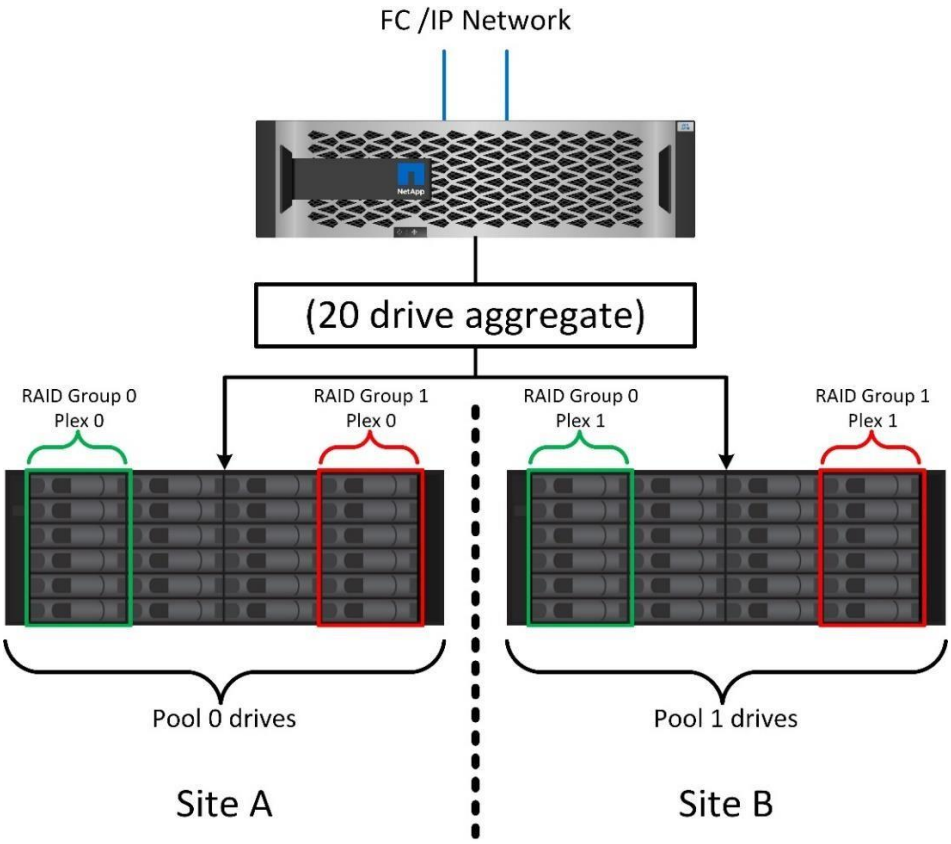


図3 は、SyncMirror構成の例を示しています。24ドライブのアグリゲートをコントローラに作成しました。このアグリゲートは、サイトAで割り当てられたシェルフの12本のドライブと、サイトBで割り当てられたシェルフの12本のドライブで構成されています。ドライブは2つのミラーRAIDグループにグループ化されます。RAIDグループ0には、サイトAの6ドライブのプレックスが含まれており、サイトBの6ドライブのプレックスにミラーリングされています。同様に、RAIDグループ1にはサイトAの6ドライブのプレックスが含まれており、サイトBの6ドライブのプレックスにミラーリングされています。

SyncMirrorは通常、MetroClusterシステムにリモートミラーリングを提供するために使用され、各サイトにデータのコピーが1つずつ配置されます。場合によっては、1つのシステムで追加レベルの冗長性を提供するために使用されます。特に、シェルフレベルの冗長性を提供します。ドライブシェルフにはすでにデュアル電源装置とコントローラが搭載されており、全体的には板金をほとんど使用していませんが、場合によっては追加の保護が保証されることがあります。たとえば、あるNetAppのお客様は、自動車テストで使用するモバイルリアルタイム分析プラットフォームにSyncMirrorを導入しています。システムは、独立した電源供給と独立したUPSシステムを備えた2つの物理ラックに分かれていました。

ハードウェア アシスト テイクオーバー

サービスプロセッサは、AFFおよびFASシステムに組み込まれたアウトオブバンド管理デバイスです。独自のIPアドレスでアクセスされ、コントローラが動作しているかどうかに関係なく、コンソールへの直接アクセスやその他の管理機能に使用されます。

ONTAPだけでは、パートナーノードからのハートビートが検出されなくなり、タイムアウトが発生した場合に、障害が発生したノードのテイクオーバーがトリガーされます。ハードウェアアシストテイクオーバーでは、サービスプロセスを使用して障害をより迅速に検出し、テイクオーバーをすぐに開始することで、テイクオーバープロセスにかかる時間を短縮します。パートナーのハートビートが停止したことをONTAPが認識するまで待機しません。

スイッチオーバーとスイッチバック

スイッチオーバーとスイッチバックという用語は、MetroCluster構成のリモートコントローラ間でボリュームを移行するプロセスを指します。このプロセスでは、リモートノードのみが環境されます。4ボリューム構成でMetroClusterを使用する場合のローカルノードのフェイルオーバーは、前述したテイクオーバーとギブバックのプロセスと同じです。

計画的スイッチオーバーとスイッチバック

計画的スイッチオーバーまたはスイッチバックは、ノード間のテイクオーバーやギブバックと似ています。このプロセスには複数の手順があり、数分かかるように見える場合もありますが、実際には、ストレージリソースとネットワークリソースを複数のフェーズで正常に移行します。完全なコマンドの実行に必要な時間よりもはるかに短時間で制御転送が行われる瞬間。

テイクオーバー/ギブバックとスイッチオーバー/スイッチバックの主な違いは、SAN接続への影響です。ローカルのテイクオーバー/ギブバックでは、ローカルノードへのすべてのSANパスが失われ、ホストのネイティブMPIOを使用して使用可能な代替パスに切り替えます。ポートは再配置されません。スイッチオーバーとスイッチバックでは、コントローラの仮想FCターゲットポートがもう一方のサイトに移行します。一時的にSAN上に存在しなくなり、代わりのコントローラに再表示されます。

MetroCluster IPを使用したONTAPメディエーター

ONTAPメディエーターは、MetroCluster IPおよびその他の特定のONTAPソリューションで使用されます。従来のTiebreakerサービスとして機能します。

その主な機能は、NVRAMとSyncMirrorが同期されているかどうかを判断することです。MetroClusterでは、NVRAMと基盤となるアグリゲートのプレックスが同期されているため、各サイトのデータが同じになるため、データ損失のリスクを伴わずにスイッチオーバーを安全に実行できます。

データが同期されていない場合、ONTAPは、フェイルオーバーまたはスイッチオーバーを強制的に実行しないかぎり、フェイルオーバーまたはスイッチオーバーを許可しません。この方法で条件を変更すると、元のコントローラにデータが残っている可能性があり、データ損失が許容されることが確認されます。

SnapMirrorビジネス継続性

MetroClusterは、災害発生時に環境全体でデータ損失をゼロに抑え、サービスの中断を最小限に抑える必要がある場合に最適な解決策です。ただし、すべてのお客様がRPO=0のデータ保護をアレイ全体で望んでいるわけではありません。一部のデータセットのみがRPO=0の同期データ保護を必要とする場合もあります。

SM-BC（SnapMirrorビジネス継続性）は、このニーズに応えるためにONTAP 9.8で導入されました。SM-BCとSM-S（SnapMirror Synchronous）はレプリケーションエンジンを共有しますが、SM-BCには透過的なアプリケーションフェイルオーバーやフェイルバックなどの追加機能が含まれています。

モード

SM-BCは、2つのモードのいずれかで動作します。同期モードはMetroClusterに似ています。通常運用時にはRPO=0が維持され、すべての書き込みがローカルシステムとリモートシステムにコミットされます。ただし、書き込みをレプリケートできない場合は、同期モードがタイムアウトして処理を続行できます。リモートサイトが元のデータと同期しなくなるため、サイト障害によってデータが失われる

ほとんどのお客様に推奨されるモードですが、変更を両方のレプリカにコミットする必要があるか、まったくコミットしない必要があるワークロードには、SM-BCにStrictSyncモードが含まれています。この場合、変更をレプリケートできなくなると、I/Oを実行しているオペレーティングシステムにエラーが報告されます。これにより、通常はアプリケーションがシャットダウンします。

パスアクセス

SM-BCを使用すると、プライマリとリモートの両方のストレージアレイから、ホストオペレーティングシステムからストレージデバイスを認識できるようになります。

ローカルコントローラのASAへのパスは「アクティブ/最適化パス」に指定され、リモートASAコントローラへのパスは「アクティブ/非最適化パス」になります。通常運用時は、すべてのI/Oがアクティブ/最適化パスをホストしているローカルコントローラによって処理されます。サイト障害やリモートサイトへのストレージフェイルオーバーが発生すると、アクティブ/非最適パスが最適パスに移行されます。

フェイルオーバー

SM-BCでは、計画的フェイルオーバーと計画外フェイルオーバーの2種類のストレージフェイルオーバー処理がサポートされます。どちらの処理も多少異なります。

計画的フェイルオーバーは、リモートサイトへの迅速なスイッチオーバーのために管理者が手動で開始し、計画外フェイルオーバーは3番目のサイトのメディエーターによって自動的に開始されます。計画的フェイルオーバーの主な目的は、パッチ適用とアップグレードを段階的に実行すること、ディザスタリカバリテストを実行すること、または完全なビジネス継続性機能を実証するためにサイト間の運用を年間を通じて切り替える正式なポリシーを採用することです。

ストレージ ハードウェア

他のディザスタリカバリストレージソリューションとは異なり、SM-BCは非対称プラットフォームの柔軟性を提供します。各サイトのハードウェアを同一にする必要はありません。この機能により、SM-BCのサポートに使用するハードウェアのサイズを適正化できます。リモートストレージシステムは、本番環境のワークロードを完全にサポートする必要がある場合はプライマリサイトと同一にすることができますが、災害によってI/Oが減少した場合は、リモートサイトに小規模なシステムを導入した方が対費用効果が高い場合があります。

ONTAP Mediator

ONTAPメディエーターは、NetAppサポートからダウンロードするソフトウェアアプリケーションです。Mediatorは、プライマリサイトとリモートサイトの両方のストレージクラスタのフェイルオーバー処理を自動化します。オンプレミスまたはクラウドでホストされた小規模な仮想マシン（VM）に導入できます。設定後は、両方のサイトのフェイルオーバーシナリオを監視するための第3のサイトとして機能します。

メディエーターはこのスプリットブレインシナリオを認識し、マスターコピーを保持するノードでI/Oを再開します。サイト間の接続がオンラインに戻ると、代替サイトが自動再同期を実行します。

SAN構成のベストプラクティス

SANの可用性を最大限に高めるには、次のベストプラクティスが重要です。そのほとんどはホストとFCのネットワーク構成に該当し、SANの実装、オペレーティングシステム、マルチパスソフトウェアに関するさまざまな側面と制限が原因です。これらのベストプラクティスから一部の逸脱は価値がある場合もありますが、管理者は考えられる結果やリスクを慎重に検討する必要があります。

独立したFCファブリック

FC SANホストでは、ホストまたはネットワークスイッチの1つのポートで障害が発生しても原因が停止しないようにするために、明らかに冗長なネットワーク接続が必要です。この2つのネットワーク接続でも、独立したFCファブリックを使用する必要があります。フルメッシュファブリックを使用すると、ホストに公開されるパスの数が過剰になり、SAN全体にユーザエラーが影響するリスクが高まります。

独立したIPサブネット

最大限の可用性を必要とするiSCSIホストとNVMe/TCPホストは、独立したサブネット上にある少なくとも2つのネットワークアダプタ（NIC）を使用する必要があります。すべてのTCP/IP通信に共通のサブネットを使用すると、その1つのサブネット全体が停止し、システムが停止するリスクが高まります。さらに、多くのOSには内部ルーティングテーブルがあり、ネットワーク通信に使用可能なNICが1つだけ使用されます。追加のNICが存在する場合もありますが、共通のサブネットを共有している場合はOSで使用できません。

LACPトランキングなどのホストボンディングをサブネットごとに使用することもできます。

たとえば、HA iSCSIまたはNVMe/TCPを次のように設定できます。

- アドレス192.168.1.10/24のホスト上のNIC #1
- アドレス192.168.2.10/24のホスト上のNIC #2
- アドレス192.168.1.1/24のONTAPコントローラ#1上の2ポートLACPトランク
- アドレス192.168.2.1/24のONTAPコントローラ#2上の2ポートLACPトランク

その結果、トランクインターフェイス上のONTAPコントローラからSANリソースの可用性がロードバランシングされ、さらにホスト上の冗長性がロードバランシングされます。2つのサブネットを使用すると、ネットワークの中断によってSAN接続が完全に中断されないようにすることができます。

LUNノハスセイケン

最新のネットワークのSANホストでは、通常、LUNまたはネームスペースへのパスが4つ以上必要ではなく、8つ以上のパスに設定することはできません。

パスの数が多すぎると、OSのブートとパスのフェイルオーバーに遅延が発生します。パスの数が多すぎると、パスの検出と管理でホストOSのバグが発生することがあります。最後に、公開されているパスの数が増えると、ホスト上のSANデバイスを管理するユーザエラーのリスクが高まります。

LUN/NSのサイジング

最大規模のONTAPコントローラでも、わずか8個のLUNやネームスペースで100%のパフォーマンス容量を実現できます。1つのアプリケーションが理論上の最大パフォーマンス容量を消費すると予想される場合は、これ以上のパフォーマンスが必要になることがありますが、LUNまたはネームスペースを8個超えた場合は、パフォーマンスが徐々に向上することはほとんどありません。

LUNまたはネームスペースの数が多いほどパスの数が増えるため、上記と同じ問題が発生します。問題を回避するには、LUNのサイズを小さくします。たとえば、サイズが8TBの通常のデータベースは、4つの2TB LUNまたはネームスペースに配置する必要があります。I/Oが特に高い場合は、1TBのLUN /ネームスペースを8個使用すると効果的です。

単一のデータセットをサポートするLUNまたはネームスペースの推奨最大数は、コントローラあたり64個またはコントローラあたり16個です。これは、単一のコントローラから単一のホストにアドバタイズできるストレージリソースの最大数ではありません。ただし、単一のデータセットワークロードに使用するリソースの最大数です。たとえば、10個のデータベースがそれぞれ8個のLUNを持ち、合計80個のワークロードを表すとします。

シングルイニシエータゾーニング

常にシングルイニシエータゾーニングを使用します。マルチイニシエータゾーニングに問題はほとんどありませんが、一部のオペレーティングシステムやHBA /ファームウェアの組み合わせでは、イニシエータのクロストークが原因で断続的に問題が発生します。それは深刻であり、それが発生したときに予期しないことがあります。シングルイニシエータゾーニングでは、イニシエータを別のイニシエータから分離することで、この問題を回避できます。マルチターゲットゾーニングを使用できます。

HBA /ファームウェア/ OSをIMTと照合

特にホストOSやONTAPのアップグレード時に、SAN構成を必ずNetApp Interoperability Matrix（IMT）に照らして検証してください。

NetAppは、さまざまな障害状況下で徹底的なテストを実施し、OS HBAファームウェア、OS SANドライバ、OSファイルシステムの実装のバグをときどき検出します。また、SM-BC、MetroCluster、特にクローニングなど、NetAppのさまざまな機能を使用してSAN構成をテストしました。SANの安定性を最大限に高めるだけでなく、LUNデバイスが頻繁に作成されて構成から削除されるシナリオなど、ユーザがONTAP機能を最大限に活用できる状況でSANが安定していることも確認したいと考えています。

SAN Host Utilitiesのドキュメントに対するSANの設定

ほとんどのオペレーティングシステムはインストールされたとおりに正しく動作しますが、構成によっては、正常に機能するために追加の設定が必要になる場合があります。これらの設定の詳細については、ONTAP SAN HostUtilitiesのマニュアルを参照してください。

sanlunユーティリティを使用したパスの健全性の確認

NetApp Host Utilitiesがサポートされているすべてのオペレーティングシステムにインストールする必要があります。重要なユーティリティは `sanlun` コマンドです。ユーザはを実行し `sanlun lun show -p` てパスの健全性を確認できます。これは、ONTAPまたはSANインフラのアップグレードを実行する前に特に重要です。システム停止を報告する多くのサポートケースでは、最終的にパスがないことが原因であることが判明します。これは、ホストの最初のインストール時に1台のコントローラしかSANにゾーニングされていなかった場合や、構成以降のSANでの一時的な変更が原因で発生した場合です。

正しい数のパスが存在することを確認し、HAペアの両方のコントローラが含まれていることを確認すると、このような監視は防止されます。また、システム停止につながる可能性のあるSANを変更する前に、OSの構成ミスや誤動作の可能性も検出します。

`sanlun` コマンドを使用できない場合は、関連するOSのマルチパス管理ツールを使用できます。

Linux LVMの注意

Linux LVMには設計上の欠陥があり、パスの変更中にI/Oエラーやアプリケーションのクラッシュが発生する可能性があります。ブート時にマルチパスドライバとLVMドライバがほぼ同時に起動するため、競合状態が発生します。ほとんどの場合、multipathdはLVMの起動前にデバイスの作成を完了しますが、これは保証されません。

LVMがデバイスをスキャンしたときにマルチパスデバイスが存在しなかったため、LVMはシングルパスデバイスを使用してPVデバイスを作成する可能性があります。そのPVを使用しているLVがマウントされていて、フェールオーバーが発生した場合、そのPVの唯一のパスが使用できなくなったため、PVは消えます。このバグを引き起こすのに十分なLUNまたはネームスペースを備えた構成はごく一部ですが、NetAppを使用しているお客様でも確認されています。

安全でない状態になっている可能性があることを示す1つの兆候が `pvs` 出力に表示されます。特定のPVSがマルチパスデバイスを使用していないことを警告することがあります。

```
  WARNING: Not using device /dev/mapper/3600a0980383038616e3f4a53716a4c7a for PV 4ZZweF-tjt9-
wLxC-CdPU-oQmT-78Wy-My6st2.
  WARNING: Not using device /dev/mapper/3600a0980383038616e3f4a53716a4d32 for PV O3IihV-zEaH-
J82B-fF8B-NGvz-dlPe-uUgb1r.
  WARNING: Not using device /dev/mapper/3600a0980383038616e3f4a53716a4d31 for PV XvjZty-T1qx-
7aHc-nrtI-yh3N-CWAv-U5gwrX.
  WARNING: Not using device /dev/mapper/3600a0980383038616e3f4a53716a4d30 for PV tl9BmZ-3dCY-
Lfvs-s7xR-3jfN-NLLT-dFGLc0.
```

この問題には、を変更することで対処できます `/etc/lvm/lvm.conf`。デフォルト設定は次のとおりで、lvmdはすべてのデバイスで物理ボリュームをスキャンします。

```
filter = [ "a|.*/|" ]
```

一般的に、次の設定は機能しますが、慎重にテストする必要があります。

```
filter = [ "a|^/dev/sda[1-9]$|", "a|^/dev/mapper/*|", "r|^/dev/*|" ]
global_filter = [ "a|^/dev/sda[1-9]$|", "a|^/dev/mapper/*|", "r|^/dev/*|" ]
```

このフィルタを使用すると、lvmdは /dev/sda*、およびの物理ボリューム /dev/mapper/* のみをスキャンします。ブートデバイスが /dev/sda パーティションでない場合、この設定によってリブートが妨げられる可能性があります。たとえば、サーバのローカルブートデバイスが /dev/xda デバイスとして表示される場合があります。詳細については、LVMの公式ドキュメントを参照してください。

注意： このファイルを変更した場合は、サーバをリブートしてリブートが成功するようにしてください。また、エラーを修正するためにコンソールにログオンする準備をしてください。

/etc/sysconfig/oracleasmエラーに関する注意

ASMlibmでOracleデータベースを使用する場合は、が /etc/sysconfig/oracleasm シングルパスデバイスを検出していないことを確認してください。Linuxのシングルパスデバイスは、引き続きマルチパスデバイスと併用できます。ASMlibは、マルチパスデバイスのみを検出するように設定する必要があります。

例：

```
# ORACLEASM_SCANORDER: Matching patterns to order disk scanning
ORACLEASM_SCANORDER="mpath dm" (OR ORACLEASM_SCANORDER="dm")

# ORACLEASM_SCANEXCLUDE: Matching patterns to exclude disks from scan
ORACLEASM_SCANEXCLUDE="sd"
```

Solarisでのhost_configスクリプトに関する注意

前述したように、必ず ONTAP SAN Host Utilitiesのドキュメントをお読みください。特に、SolarisでONTAPマルチパスデバイスが正しく認識されるようにするには、特定の設定手順が必要です。ホスト設定の手順に従わないと、耐障害性に影響し、ZFSのパフォーマンスに重大な問題が発生する可能性があります。

NVFAIL

重要なデータを含むONTAPストレージ上のSANボリュームは、 nvfail パラメータをに設定する必要があります on。

データベースなどのアプリケーションがディスク上のデータの大規模な内部キャッシュを保持しているため、SANワークロードはフェイルオーバーやスイッチオーバーを強制的に実行した場合に特に破損の影響を受けやすくなります。強制フェイルオーバーが発生した場合、以前に確認された変更は事実上破棄されます。ストレージ アレイの内容は事実上時間を逆方向に進め、データベース キャッシュの状態はディスク上のデータの状態を反映しなくなりました。

nvfail また、この設定は、データの整合性に問題が生じるNVRAMジャーナリングの壊滅的な障害からボリュームを保護します。nvfail パラメータは起動時に有効になります。NVRAMエラーが検出された場合は、コミットされていない変更が失われている可能性があり、ドライブの状態がデータベースキャッシュと一致していない可能性があります。ONTAPは nvfail 、パラメータをに設定してボリュームを on に設定します in- nvfailed-state。その結果、データにアクセスしようとするすべてのプロセスにI/Oエラーが発生し、データベースの保護クラッシュまたはシャットダウンが発生します。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを確認してください。

- ONTAP SAN Host Utilities
  https://docs.netapp.com/us-en/ontap-sanhost/
- NetAppの製品ドキュメント
  https://docs.netapp.com

バージョン履歴

バージョン	日付	ドキュメント バージョン履歴
バージョン1.0	2023年4月	初版リリース
バージョン1.0.1	2023年5月	軽微な誤植を修正

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報