よくある質問です

E-Series storage systems

NetApp
April 21, 2025

目次

よくある質問です

どの設定がインポートされますか？

設定のインポート機能は、1つのストレージアレイから複数のストレージアレイに構成をロードするバッチ処理です。

この処理でインポートされる設定は、System Managerでソースストレージアレイがどのように設定されているかによって異なります。複数のストレージアレイにインポートできる設定は次のとおりです。

- **Email alerts**--メールサーバのアドレスとアラート受信者の電子メールアドレスを設定します
- **Syslog**アラート-- syslogサーバのアドレスとUDPポートを含む設定。
- *snmp alerts *-- SNMPサーバのコミュニティ名とIPアドレスを含む設定。
- * AutoSupport *--個別の機能（Basic AutoSupport 、AutoSupport OnDemand、Remote Diagnostics）、メンテナンス時間、配信方法、 およびディスパッチスケジュール。
- ディレクトリサービス-- LDAP (Lightweight Directory Access Protocol)サーバーのドメイン名とURL、およびLDAPサーバーのユーザーグループとストレージアレイの定義済みロールとのマッピングが含まれます。
- ストレージ構成--ボリューム(リポジトリボリューム以外のシックボリュームのみ)、ボリュームグループ、プール、およびホットスペアドライブの割り当てが含まれます。
- システム設定--ボリュームのメディアスキャン設定、コントローラのSSDキャッシュ、および自動ロードバランシングが含まれます(ホスト接続レポートは含まれません)。

ストレージアレイが一部表示されないのはなぜですか？

設定のインポート処理の際、ターゲットの選択ダイアログボックスに一部のストレージアレイが表示されないことがあります。

ストレージアレイが表示されない理由は次のとおりです。

- ファームウェアのバージョンが8.50未満である。
- ストレージアレイがオフラインになっている。
- システムがそのアレイと通信できません（アレイに証明書、パスワード、ネットワークの問題がある場合など）。

これらのボリュームがワークロードに関連付けられていないのはなぜですか？

ボリュームをコマンドラインインターフェイス（CLI）を使用して作成した場合や別のストレージアレイから移行（インポート/エクスポート）した場合、それらのボリュームはワークロードに関連付けられません。

選択したワークロードはボリュームの作成にどのように影響しますか？

ボリュームの作成中に、ワークロードの使用状況に関する情報を入力するように求められます。この情報に基づいて最適なボリューム構成が作成されるため、必要に応じて編集することができます。必要に応じて、ボリューム作成のこの手順をスキップできます。

ワークロードは、アプリケーションをサポートするストレージオブジェクトです。アプリケーションごとに1つ以上のワークロードまたはインスタンスを定義できます。一部のアプリケーションでは、特性が似たボリュームで構成されるようにワークロードが設定されます。これらのボリューム特性は、ワークロードがサポートするアプリケーションのタイプに基づいて最適化されます。たとえば、Microsoft SQL Serverアプリケーションをサポートするワークロードを作成し、そのワークロード用のボリュームを作成すると、Microsoft SQL Serverをサポートするようにボリューム特性が最適化されます。

- アプリケーション固有--アプリケーション固有のワークロードを使用してボリュームを作成する場合、アプリケーションワークロードのI/Oとアプリケーションインスタンスからの他のトラフィックの競合を最小限に抑えるために最適化されたボリューム構成が推奨される場合があります。I/Oタイプ、セグメントサイズ、コントローラ所有権、読み取り/書き込みキャッシュなどのボリューム特性が自動的に推奨され、次のアプリケーションタイプ用に作成されるワークロードに合わせて最適化されます。
  - Microsoft SQL Server の場合
  - Microsoft Exchange Server の略
  - ビデオ監視アプリケーション
  - VMware ESXi（ボリュームをVirtual Machine File Systemで使用する場合）

    ボリュームの追加/編集ダイアログボックスを使用して、推奨されるボリューム構成を確認し、システムで推奨されるボリュームや特性を編集、追加、削除できます。
- その他（または特定のボリューム作成サポートのないアプリケーション）- 特定のアプリケーションに関連付けられていないワークロードを作成する場合や、ストレージアレイで使用する予定のアプリケーションに対する最適化が組み込まれていない場合は、その他のワークロードではボリューム構成を手動で指定する必要があります。ボリュームの追加/編集ダイアログボックスを使用して、ボリューム構成を手動で指定する必要があります。

ボリューム、ホスト、またはホストクラスタが一部表示されないのはなぜですか？

ベースボリュームでData Assurance（DA）が有効なSnapshotボリュームを、DA対応でないホストに割り当てることはできません。DA対応でないホストにSnapshotボリュームを割り当てるには、ベースボリュームのDAを無効にする必要があります。

Snapshotボリュームを割り当てるホストについては、次のガイドラインを考慮してください。

- DA対応でないI/Oインターフェイスを使用してストレージアレイに接続されているホストは、DA対応ではありません。
- ホストメンバーが1つでもDA対応でないホストクラスタは、DA対応ではありません。

Snapshot（整合性グループ、Snapshotグループ、Snapshotイメージ、Snapshotボリューム）、ボリュームコピーに関連付けられているボリュームでは、DAを無効にできません。 ミラーリングも可能です。ベースボリュームのDAを無効にするには、最初に関連付けられているすべてのリザーブ容量とSnapshotオブジェクトを削除する必要があります。

選択したワークロードを削除できないのはなぜですか？

このワークロードは、コマンドラインインターフェイス（CLI）を使用して作成されたボリューム、または別のストレージアレイから移行（インポート/エクスポート）されたボリュームのグループで構成されています。そのため、このワークロード内のボリュームはアプリケーション固有のワークロードに関連付けられておらず、ワークロードを削除することはできません。

アプリケーション固有のワークロードはストレージアレイの管理にどのように役立ちますか？

アプリケーション固有のワークロードのボリューム特性は、ワークロードがストレージアレイのコンポーネントとやり取りする方法を決定し、特定の構成下での環境のパフォーマンスを判断するのに役立ちます。

アプリケーションとは、SQL ServerやExchangeなどのソフトウェアです。アプリケーションごとに、サポートするワークロードを1つ以上定義します。一部のアプリケーションについては、ストレージを最適化するボリューム構成が自動的に提示されます。ボリューム構成には、I/Oタイプ、セグメントサイズ、コントローラ所有権、読み取りと書き込みのキャッシュなどの特性が含まれます。

拡張後の容量を認識させるにはどうすればよいですか？

ボリュームの容量を拡張した場合、その拡張した容量がホストですぐに認識されないことがあります。

ほとんどのオペレーティングシステムでは、拡張されたボリューム容量を認識し、ボリューム拡張の開始後に自動的に拡張が行われます。ただし、この処理が行われない場合もあります。拡張されたボリューム容量をOSが自動的に認識しない場合は、ディスクの再スキャンまたはリブートが必要になる可能性があります。

ボリュームの容量を拡張したら、それに応じてファイルシステムのサイズを手動で拡張する必要があります。方法は、使用しているファイルシステムによって異なります。

詳細については、ホストオペレーティングシステムのドキュメントを参照してください。

ホストの割り当てをあとで実行する場合に選択します。

ボリューム作成プロセスの速度を上げる場合は、ホスト割り当ての手順を省略して、新しく作成したボリュームをオフラインにすることができます。

新しく作成するボリュームを初期化する必要があります。システムは、Immediate Available Format（IAF）バックグラウンド初期化プロセスまたはオフラインプロセスのいずれかのモードを使用して初期化できます。

ボリュームをホストにマッピングすると、そのグループ内のすべての初期化中のボリュームがバックグラウンド初期化に強制的に移行します。このバックグラウンド初期化プロセスにより、同時ホストI/Oが可能になりますが、これには時間がかかることがあります。

ボリュームグループ内のいずれのボリュームもマッピングされていない場合、オフライン初期化が実行されます。オフラインプロセスはバックグラウンドプロセスよりもはるかに高速です。

ホストブロックサイズの要件について、どのような点に注意する必要がありますか？

EF300システムとEF600システムの場合は、ボリュームを設定して512バイトまたは4KiBのブロックサイズ（「セクターサイズ」とも呼ばれる）をサポートすることができます。ボリュームの作成時に正しい値を設定する必要があります。可能であれば、適切なデフォルト値が推奨されます。

ボリュームのブロックサイズを設定する前に、次の制限事項とガイドラインを確認してください。

- 一部のオペレーティングシステムと仮想マシン（現時点ではVMwareなど）は512バイトのブロックサイズを必要とし、4KiBをサポートしないため、ボリュームを作成する前にホストの要件を確認してください。通常、最適なパフォーマンスを得るには、ボリュームを4KiBのブロックサイズに設定します。ただし、ホストで4KiB（または「4Kn」）のブロックを使用できることを確認します。
- プールまたはボリュームグループ用に選択したドライブのタイプによって、サポートされるボリュームブロックサイズも次のように決まります。
  - 512バイトブロックに書き込むドライブを使用してボリュームグループを作成する場合、作成できるのは512バイトブロックのボリュームのみです。
  - 4KiBブロックに書き込むドライブを使用してボリュームグループを作成する場合は、512バイトまたは4KiBブロックでボリュームを作成します。
- アレイにiSCSIホストインターフェイスカードが搭載されている場合、すべてのボリュームは（ボリュームグループのブロックサイズに関係なく）512バイトブロックに制限されます。これは、特定のハードウェアの実装が原因です。
- 一度設定したブロックサイズは変更できません。ブロックサイズを変更する必要がある場合は、ボリュームを削除して再作成する必要があります。

ホストクラスタを作成する必要があるのはどのような場合ですか？

複数のホストから同じボリュームセットにアクセスする場合は、ホストクラスタを作成する必要があります。通常、個々のホストには、ボリュームへのアクセスを調整するためのクラスタリングソフトウェアがインストールされています。

正しいホストオペレーティングシステムタイプを特定するにはどうすればよいですか？

Host Operating System Typeフィールドには、ホストのオペレーティングシステムが表

示されます。推奨されるホストタイプをドロップダウンリストから選択できます。

ドロップダウンリストに表示されるホストタイプは、ストレージアレイのモデルとファームウェアバージョンによって異なります。最新バージョンでは、最も一般的なオプションが最初に表示されますが、これは最も適切なオプションです。このリストに表示されるオプションが完全にサポートされているとは限りません。

ホストのサポートの詳細については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

リストに表示されるホストタイプは次のとおりです。

ホストオペレーティングシステムのタイプ	オペレーティングシステム（**OS**）とマルチパスドライバ
Linux DM-MP（カーネル3.10以降）	Device Mapper Multipathのフェイルオーバー解決策と3.10以降のカーネルを使用するLinuxオペレーティングシステムをサポートします。
VMware ESXi	VMwareに組み込みのストレージアレイタイプポリシーモジュールであるSATP_ALUAを使用してNative Multipathing Plug-in（NMP）アーキテクチャを実行するVMware ESXiオペレーティングシステムをサポートします。
Windows（クラスタまたは非クラスタ）	ATTOマルチパスドライバを実行しないWindowsクラスタ構成または非クラスタ構成をサポートします。
ATTOクラスタ（すべてのオペレーティングシステム）	ATTO Technology、Inc.のマルチパスドライバを使用するすべてのクラスタ構成をサポートします。
Linux（Veritas DMP）	Veritas DMPマルチパス解決策 を使用するLinuxオペレーティングシステムをサポートします。
Linux（ATTO）	ATTO Technology、Inc.のマルチパスドライバを使用するLinuxオペレーティングシステムをサポートします。
Mac OS の場合	ATTO Technology、Inc.のマルチパスドライバを使用するMac OSバージョンをサポートします。
Windows（ATTO）	ATTO Technology、Inc.のマルチパスドライバを使用するWindowsオペレーティングシステムをサポートします。
FlexArray （ALUA）	マルチパスにALUAを使用するNetApp FlexArray システムをサポートします。
IBM SVCの場合	IBM SAN Volume Controller構成をサポートします。
工場出荷時のデフォルト	ストレージアレイの初回起動用です。ホストオペレーティングシステムのタイプが工場出荷時のデフォルトに設定されている場合は、接続先ホストで実行されているホストオペレーティングシステムとマルチパスドライバに合わせて変更します。
Linux DM-MP（カーネル3.9以前）	Device Mapper Multipathのフェイルオーバー解決策と3.9以前のカーネルを使用するLinuxオペレーティングシステムをサポートします。

ホストオペレーティングシステムのタイプ	オペレーティングシステム（**OS**）とマルチパスドライバ
Windowsクラスタ（廃止）	ホストオペレーティングシステムのタイプがこの値に設定されている場合は、代わりにWindows（クラスタまたは非クラスタ）の設定を使用します。

ホストポートをホストに一致させるにはどうすればよいですか？

ホストを手動で作成する場合は、まずホストで利用可能な適切なHost Bus Adapter（HBA；ホストバスアダプタ）ユーティリティを使用して、ホストにインストールされている各HBAに関連付けられているホストポート識別子を特定する必要があります。

この情報を確認したら、Create Hostダイアログのリストから、ストレージアレイにログインしているホストポート識別子を選択します。

作成するホストに適したホストポート識別子を選択してください。誤ったホストポート識別子を関連付けると、別のホストからこのデータへの原因 の意図しないアクセスが発生する可能性があります。

デフォルトクラスタとは何ですか？

デフォルトクラスタはシステム定義のエンティティです。ストレージアレイにログインしたホストポート識別子が関連付けられていない場合、そのポートはデフォルトクラスタに割り当てられているボリュームにアクセスできます。

関連付けられていないホストポート識別子は、特定のホストに論理的に関連付けられておらず、ホストに物理的に搭載されてストレージアレイにログインしているホストポートです。

ホストがストレージアレイ内の特定のボリュームにアクセスできるようにする場合は、デフォルトクラスタを使用しないでください。代わりに、ホストポート識別子を対応するホストに関連付ける必要があります。このタスクは、ホスト作成処理中に手動で実行できます。その後、ボリュームを個々のホストまたはホストクラスタに割り当てます。

デフォルトクラスタは、外部ストレージ環境がすべてのホストにアクセスできるようにし、ストレージアレイに接続されているすべてのログイン済みホストポート識別子がすべてのボリュームにアクセスできるようにする（フルアクセスモード）場合にのみ使用してください。 特にストレージアレイやユーザインターフェイスでホストが認識されないようにする必要があります。

最初にボリュームをデフォルトクラスタに割り当てる際には、コマンドラインインターフェイス（CLI）を使用する必要があります。ただし、ボリュームを少なくとも1つデフォルトクラスタに割り当てると、このエンティティを管理できるユーザインターフェイスに表示されます（デフォルトクラスタ）。

冗長性チェックとは何ですか？

冗長性チェックでは、プールまたはボリュームグループ内のボリューム上のデータに整合性があるかどうかが判別されます。冗長性データは、プールまたはボリュームグルー

プ内のいずれかのドライブで障害が発生した場合に、交換用ドライブに迅速に情報を再構築するために使用されます。

このチェックは、一度に1つのプールまたはボリュームグループでのみ実行できます。ボリュームの冗長性チェックでは、次の処理が実行されます。

- RAID 3ボリューム、RAID 5ボリューム、またはRAID 6ボリューム内のデータブロックがスキャンされ、各ブロックの冗長性情報がチェックされます。（RAID 3をボリュームグループに割り当てるには、コマンドラインインターフェイスを使用する必要があります）。
- RAID 1のミラーリングされたドライブ上のデータブロックが比較されます。
- データに整合性がないことがコントローラファームウェアで確認された場合は、冗長性エラーが返されます。

> 同じプールまたはボリュームグループですぐに冗長性チェックを実行すると、原因 でエラーが発生する場合があります。この問題を回避するには、同じプールまたはボリュームグループで別の冗長性チェックを実行する前に、1~2分待ってください。

予約済み容量とは何ですか？

予約済み容量は、ドライブ障害に備えてプール内に確保されている容量（ドライブ数）です。

プールが作成されると、プール内のドライブ数に応じて自動的にデフォルトの予約済み容量が確保されます。

プールの予約済み容量は再構築時に使用されますが、ボリュームグループでは同じ目的でホットスペアドライブが使用されます。予約済み容量を使用する方式は、再構築の時間を短縮できるため、ホットスペアドライブよりも優れています。予約済み容量は、ホットスペアドライブの場合は1本のドライブに確保されるのではなく、プール内の複数のドライブに分散されるため、特定のドライブの速度や可用性に制限されません。

アプリケーションに最適な**RAID**レベルはどれですか？

ボリュームグループのパフォーマンスを最大限に高めるには、適切なRAIDレベルを選択する必要があります。

適切なRAIDレベルを特定するには、ボリュームグループにアクセスしているアプリケーションでの読み取りと書き込みの割合を把握します。これらの割合を取得するには、[パフォーマンス]ページを使用します。

RAIDレベルとアプリケーションパフォーマンス

RAIDには、レベルと呼ばれる一連の構成が採用されており、ユーザデータと冗長性データのドライブに対する書き込み/読み出し方法が決定されます。RAIDレベルごとにパフォーマンス機能が異なります。読み取り比率が高いアプリケーションの場合、RAID 5ボリュームまたはRAID 6ボリュームを使用するとパフォーマンスが向上します。これは、RAID 5およびRAID 6構成の読み取りパフォーマンスが優れているためです。

読み取り比率が低い（書き込み中心の）アプリケーションの場合、RAID 5ボリュームまたはRAID 6ボリュームでは同様のパフォーマンスを実現できません。パフォーマンスの低下は、コントローラがデータと冗長性データをRAID 5ボリュームグループまたはRAID 6ボリュームグループのドライブに書き込む方法に起因します。

次の情報に基づいてRAIDレベルを選択します。

RAID 0

概要 ：

- 冗長性なし、ストライピングモード。
- RAID 0は、ボリュームグループ内のすべてのドライブにデータをストライピングします。

データ保護機能：

- 高可用性が求められる場合、RAID 0は推奨されません。RAID 0は重要度の低いデータに適しています。
- ボリュームグループ内の1本のドライブで障害が発生すると、関連付けられているすべてのボリュームで障害が発生し、すべてのデータが失われます。

必要なドライブ数：

- RAIDレベル0には少なくとも1本のドライブが必要です。
- RAID 0ボリュームグループには30本を超えるドライブを含めることができます。
- ストレージアレイのすべてのドライブを含むボリュームグループを作成できます。

RAID 1または**RAID 10**

概要 ：

- ストライピング/ミラーモード。

どのように機能するか:

- RAID 1では、ディスクミラーリングを使用して、2本のディスクに同時にデータが書き込まれます。
- RAID 10は、ドライブストライピングを使用して、複数のミラーリングされたドライブペアにデータをストライピングします。

データ保護機能：

- RAID 1とRAID 10は、ハイパフォーマンスと最高のデータ可用性を提供します。
- RAID 1とRAID 10は、ドライブミラーリングを使用して、あるドライブから別のドライブにまったく同じコピーを作成します。
- ドライブペアの一方のドライブで障害が発生した場合、ストレージアレイはデータやサービスを失うことなくもう一方のドライブに即座に切り替えることができます。
- 単一ドライブ障害が発生すると、関連付けられているボリュームはデグレード状態になります。ミラードライブがデータへのアクセスを許可します。
- ボリュームグループ内のドライブペアで障害が発生すると、関連付けられているすべてのボリュームで障害が発生し、データが失われる可能性があります。

必要なドライブ数：

- RAID 1には、ユーザデータ用に1本、ミラーデータ用に1本、合計2本以上のドライブが必要です。

- 4本以上のドライブを選択すると、ボリュームグループ全体でRAID 10が自動的に設定されます。ユーザデータ用にドライブが2本、ミラーデータ用にドライブが2本です。
- ボリュームグループのドライブ数は偶数でなければなりません。ドライブ数が偶数ではなく未割り当てのドライブが残っている場合は、「* Pools & Volume Groups」に移動してボリュームグループにドライブを追加し、処理を再試行します。
- RAID 1とRAID 10のボリュームグループは、30本を超えるドライブで構成できます。ストレージアレイのすべてのドライブを含むボリュームグループを作成できます。

RAID 5

概要 ：

- 高I/Oモード。

どのように機能するか:

- ユーザデータと冗長性情報（パリティ）が複数のドライブにストライピングされます。
- 冗長性情報を格納するために、ドライブ1本分の容量が使用されます。

データ保護機能

- RAID 5ボリュームグループで1本のドライブに障害が発生すると、関連付けられているすべてのボリュームがデグレード状態になります。冗長な情報があるので、データには引き続きアクセスできます。
- RAID 5ボリュームグループで複数のドライブに障害が発生すると、関連付けられているすべてのボリュームに障害が発生し、すべてのデータが失われます。

必要なドライブ数：

- ボリュームグループには最低3本のドライブが必要です。
- 通常、ボリュームグループのドライブ数は最大30本に制限されます。

RAID 6

概要 ：

- 高I/Oモード。

どのように機能するか:

- ユーザデータと冗長性情報（デュアルパリティ）が複数のドライブにストライピングされます。
- 冗長性情報を格納するために、ドライブ2本分の容量が使用されます。

データ保護機能：

- RAID 6ボリュームグループで1本または2本のドライブに障害が発生すると、関連付けられているすべてのボリュームがデグレード状態になりますが、冗長性情報があるためデータには引き続きアクセスできます。
- RAID 6ボリュームグループで3本以上のドライブに障害が発生すると、関連付けられているすべてのボリュームに障害が発生し、すべてのデータが失われます。

必要なドライブ数：

- ボリュームグループには最低5本のドライブが必要です。
- 通常、ボリュームグループのドライブ数は最大30本に制限されます。

プールのRAIDレベルは変更できません。ユーザーインタフェースは'プールを自動的にRAID 6として構成します

RAIDレベルとデータ保護

RAID 1、RAID 5、およびRAID 6は、フォールトトレランス用に冗長性データをドライブメディアに書き込みます。冗長性データには、データのコピー（ミラー）、またはデータから導出されたエラー修正コードがあります。ドライブで障害が発生した場合は、冗長性データを使用して交換用ドライブに迅速に情報を再構築できます。

単一のボリュームグループ全体で単一のRAIDレベルを設定します。そのボリュームグループの冗長性データは、すべてボリュームグループ内に格納されます。ボリュームグループの容量は、メンバードライブのアグリゲート容量から冗長性データ用に確保された容量を引いた値です。冗長性を確保するために必要な容量は、使用するRAIDレベルによって異なります。

一部のドライブが表示されないのはなぜですか？

容量の追加ダイアログで、既存のプールまたはボリュームグループに容量を追加できるドライブがすべて表示されるわけではありません。

ドライブを追加できない理由は次のとおりです。

- 未割り当てで、セキュリティ有効でないドライブを指定する必要があります。すでに別のプールやボリュームグループに含まれているドライブ、またはホットスペアとして設定されているドライブは使用できません。未割り当てだが、セキュリティ有効なドライブは、手動で消去すると使用可能になります。
- 最適な状態でないドライブは使用できません。
- 容量が小さすぎるドライブは使用できません。
- プールまたはボリュームグループ内でドライブのメディアタイプが一致している必要があります。次のものを混在させることはできません。
  - ソリッドステートディスク（SSD）搭載のハードディスクドライブ（HDD）
  - NVMeとSASドライブ
  - ボリュームブロックサイズが512バイトおよび4KiBのドライブ
- プールまたはボリュームグループに含まれているドライブがすべてセキュリティ対応の場合は、セキュリティ対応でないドライブは表示されません。
- プールまたはボリュームグループに含まれているドライブがすべて連邦情報処理標準（FIPS）ドライブの場合、非FIPSドライブは表示されません。
- プールまたはボリュームグループに含まれているドライブがすべてData Assurance（DA）対応で、プールまたはボリュームグループにDA有効ボリュームが1つ以上ある場合は、DA非対応のドライブは使用できないためプールまたはボリュームグループに追加できません。ただし、プールまたはボリュームグループにDA有効ボリュームがない場合は、DA非対応のドライブをプールまたはボリュームグループに追加でき

ます。DA対応と非対応のドライブが混在している場合は、DA対応ボリュームを作成できないことに注意してください。

ストレージアレイの容量は、新しいドライブを追加するか、プールまたはボリュームグループを削除することで増やすことができます。

予約済み容量を増やせない場合、どのような理由が考えられますか？

使用可能なすべての容量でボリュームを作成した場合は、予約済み容量を増やせないことがあります。

予約済み容量は、ドライブ障害に備えてプール内に確保されている容量（ドライブ数）です。プールが作成されると、プール内のドライブ数に応じて自動的にデフォルトの予約済み容量が確保されます。使用可能なすべての容量でボリュームを作成している場合は、ドライブを追加するかボリュームを削除してプールに容量を追加しないと、予約済み容量を増やすことはできません。

予約済み容量は、プールおよびボリュームグループから変更できます。編集するプールを選択します。[設定の表示/編集]をクリックし、[設定]タブを選択します。

予約済み容量はプール内の複数のドライブに分散されますが、予約するときはドライブ数で指定します。

Data Assuranceとは何ですか？

Data Assurance（DA）はT10 Protection Information（PI）標準を実装しています。I/Oパスでデータが転送される際に発生する可能性のあるエラーをチェックして修正することで、データの整合性が向上します。

Data Assurance機能の一般的な用途として、コントローラとドライブ間のI/Oパスがチェックされます。DA機能はプールおよびボリュームグループのレベルで提供されます。

この機能を有効にすると、ボリューム内の各データブロックに巡回冗長検査（CRC）と呼ばれるエラーチェック用のコードが付加されます。データブロックが移動されると、ストレージアレイはこれらのCRCコードを使用して、転送中にエラーが発生したかどうかを判断します。破損している可能性があるデータはディスクに書き込まれず、ホストにも返されません。DA機能を使用する場合は、新しいボリュームを作成するときにDAに対応したプールまたはボリュームグループを選択します（プールとボリュームグループの候補の表で、「* DA *」の横の「*はい」*を探します）。

これらのDA対応ボリュームは、必ずDAに対応したI/Oインターフェイスを使用しているホストに割り当ててください。DAに対応したI/Oインターフェイスには、ファイバチャネル、SAS、iSCSI over TCP/IP、NVMe/FC、NVMe/IB、 NVMe/RoCEとiSER over InfiniBand（iSCSI Extensions for RDMA/IB）：SRP over InfiniBandではDAはサポートされていません。

FDE / FIPSセキュリティとは何ですか？

FDE / FIPSセキュリティとは、一意の暗号化キーを使用して書き込み時にデータを暗号化し、読み取り時に復号化するセキュリティ対応ドライブを指します。

セキュリティ対応ドライブは、ストレージアレイから物理的に取り外されたドライブ上のデータへの不正アクセスを防止します。セキュリティ対応ドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。FIPSドライブは認定テストをパスしたドライブです。

FIPSのサポートが必要なボリュームには、FIPSドライブのみを使用します。ボリュームグループまたはプールにFIPSドライブとFDEドライブが混在している場合、すべてのドライブがFDEドライブとして扱われます。また、FIPSドライブのみを含むボリュームグループまたはプールでは、FDEドライブを追加したりスペアとして使用したりすることはできません。

セキュリティ対応（ドライブセキュリティ）とは何ですか？

ドライブセキュリティは、セキュリティ有効ドライブをストレージアレイから取り外したときに、そのドライブ上のデータへの不正アクセスを防止する機能です。

対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。

SSDキャッシュのすべての統計情報を表示するにはどうすればよいですか？また、何が

SSDキャッシュについては、一般統計と詳細統計を表示できます。

一般統計は詳細統計のサブセットです。詳細統計は、すべてのSSD統計を.csvファイルにエクスポートした場合にのみ表示できます。統計を確認および解釈する際には、複数の統計を組み合わせることで見えてくる情報もあることに注意してください。

一般統計

SSDキャッシュの統計を表示するには、* Manage *ページに移動します。メニューを選択します。Provisioning [プールとボリュームグループの構成]。統計を表示するSSDキャッシュを選択し、メニューを選択します。More [View Statistics]公称統計はView SSD Cache Statistics（SSDキャッシュ統計の表示）ダイアログに表示されます。

この機能は、EF600またはEF300ストレージシステムでは使用できません。

このリストには、詳細統計のサブセットである一般統計が表示されます。

詳細統計

詳細統計は、一般統計とその他の統計で構成されます。これらの追加統計は一般統計とともに保存されますが、一般統計とは異なり、View SSD Cache Statistics（SSDキャッシュ統計の表示）ダイアログには表示されません。詳細統計を表示するには、統計を.csvファイルにエクスポートする必要があります。

一般統計のあとに詳細統計が表示されます。

シェルフ損失の保護およびドロワー損失の保護とは何ですか？

シェルフ損失の保護とドロワー損失の保護は、シェルフまたはドロワーで単一障害が発

生した場合にデータアクセスを維持するためのプールとボリュームグループの属性です。

シェルフ損失の保護

シェルフは、ドライブまたはドライブとコントローラを格納するエンクロージャです。シェルフ損失の保護が有効な場合、1台のドライブシェルフとの通信が完全に失われた場合でもプールまたはボリュームグループ内のボリューム上のデータへのアクセスが保証されます。通信が完全に失われるケースには、ドライブシェルフの電源喪失や、両方のI/Oモジュール（IOM）の障害などがあります。

プールまたはボリュームグループですでにドライブに障害が発生している場合は、シェルフ損失の保護は保証されません。この状況で、ドライブシェルフへのアクセス、さらにその結果プールまたはボリュームグループ内の別のドライブへのアクセスを失うと、データが失われます。

シェルフ損失の保護の条件は、次の表で説明するように、保護の手法によって異なります。

レベル	シェルフ損失の保護の条件	必要なシェルフの最小数
プール	プールには少なくとも5つのシェルフのドライブが含まれている必要があり、各シェルフで同じ数のドライブが必要です。シェルフ損失の保護は大容量シェルフには適用されません。大容量シェルフがあるシステムの場合は、ドロワー損失の保護を参照してください。	5.
RAID 6	ボリュームグループに同じドロワーのドライブが3本以上含まれない。	3.
RAID 3またはRAID 5	ボリュームグループ内のドライブがすべて別々のシェルフに配置されている。	3.
RAID 1	RAID 1ペアのドライブがそれぞれ別のシェルフに配置されている。	2.
RAID 0	シェルフ損失の保護は実現できない。	該当なし

ドロワー損失の保護

ドロワーはシェルフのコンパートメントの1つで、引き出してドライブを設置します。ドロワーを備えているのは大容量シェルフのみです。ドロワー損失の保護が有効な場合、1つのドロワーとの通信が完全に失われた場合でもプールまたはボリュームグループ内のボリューム上のデータへのアクセスが保証されます。通信が完全に失われるケースには、ドロワーの電源喪失や、ドロワー内のコンポーネント障害などがあります。

プールまたはボリュームグループですでにドライブに障害が発生している場合は、ドロワー損失の保護は保証されません。この状況でドロワーにアクセスできなくなると（その結果プールまたはボリュームグループ内の別のドライブにアクセスできなくなると）、データが失われます。

ドロワー損失の保護の条件は、次の表で説明するように、保護の手法によって異なります。

レベル	ドロワー損失の保護の基準	必要なドロワーの最小数
プール	プール候補にはすべてのドロワーのドライブを含める必要があり、各ドロワーに同じ数のドライブが必要です。プールには少なくとも5つのドロワーのドライブが含まれている必要があり、各ドロワーに同じ数のドライブが必要です。60ドライブのシェルフでは、プールに含まれる15、20、25、30、35でドロワー損失の保護を実現できます。 40、45、50、55、または60ドライブ。初回作成後に、5の倍数でプールに追加できます。	5.
RAID 6	ボリュームグループに同じドロワーのドライブが3本以上含まれない。	3.
RAID 3または5	ボリュームグループ内のドライブがすべて別々のドロワーに配置されている	3.
RAID 1	ミラーペアのドライブがそれぞれ別のドロワーに配置されている。	2.
RAID 0	ドロワー損失の保護は実現できない。	該当なし

シェルフ損失およびドロワー損失の保護を維持するにはどうすればよいですか？

プールまたはボリュームグループのシェルフ損失およびドロワー損失の保護を維持するには、次の表の基準を使用します。

レベル	シェルフ/ドロワー損失の保護の基準	必要なシェルフ/ドロワーの最小数
プール	シェルフの場合、プールに同じシェルフのドライブが3本以上含まれない。ドロワーの場合、プールに各ドロワーから同数のドライブが含まれている。	ドロワー用のシェルフ5の場合は6
RAID 6	ボリュームグループに同じシェルフまたはドロワーのドライブが3本以上含まれない。	3.
RAID 3またはRAID 5	ボリュームグループ内のドライブがすべて別々のシェルフまたはドロワーに配置されている。	3.

レベル	シェルフ/ドロワー損失の保護の基準	必要なシェルフ/ドロワーの最小数
RAID 1	ミラーペア内のドライブがそれぞれ別のシェルフまたはドロワーに配置されている。	2.
RAID 0	シェルフ/ドロワー損失の保護は実現できない。	該当なし

プールまたはボリュームグループですでにドライブに障害が発生している場合は、シェルフ/ドロワー損失の保護は維持されません。この状況で、ドライブシェルフまたはドロワーへのアクセス、さらにその結果プールまたはボリュームグループ内の別のドライブへのアクセスを失うと、データが失われます。

プールの最適化容量とは何ですか？

SSDドライブでは、その容量の一部が未割り当ての場合に寿命が長くなり、最大書き込みパフォーマンスが向上します。

プールに関連付けられているドライブの未割り当て容量は、プールの予約済み容量、空き容量（ボリュームで使用されていない容量）、および使用可能容量のうちの最適化容量として確保された容量で構成されます。この最適化容量は使用可能容量を減らすことで最小レベルの最適化容量を確保するため、ボリュームの作成には使用できません。

プールの作成時に、パフォーマンス、ドライブの寿命、使用可能容量のバランスに基づいて、推奨される最適化容量が決定されます。プール設定ダイアログにある追加の最適化容量スライダを使用すると、プールの最適化容量を調整できます。スライダを動かすことで、使用可能容量を犠牲にしてパフォーマンスの向上とドライブ寿命の延長を図るか、またはパフォーマンスとドライブ寿命を犠牲にして使用可能容量を増やすことができます。

追加の最適化容量スライダは、EF600およびEF300ストレージシステムに対してのみ使用できます。

ボリュームグループの最適化容量とは何ですか？

SSDドライブでは、その容量の一部が未割り当ての場合に寿命が長くなり、最大書き込みパフォーマンスが向上します。

ボリュームグループに関連付けられているドライブの未割り当て容量は、ボリュームグループの空き容量（ボリュームで使用されていない容量）と、使用可能容量のうちの最適化容量として確保された容量で構成されます。この最適化容量は使用可能容量を減らすことで最小レベルの最適化容量を確保するため、ボリュームの作成には使用できません。

ボリュームグループの作成時に、パフォーマンス、ドライブの寿命、使用可能容量のバランスに基づいて、推奨される最適化容量が決定されます。ボリュームグループ設定ダイアログの最適化容量のスライダを使用して、ボリュームグループの最適化容量を調整できます。スライダを動かすことで、使用可能容量を犠牲にしてパフォーマンスの向上とドライブ寿命の延長を図るか、またはパフォーマンスとドライブ寿命を犠牲にして使用可能容量を増やすことができます。

追加の最適化容量のスライダは、EF600およびEF300ストレージシステムに対してのみ使用できます。

リソースプロビジョニング機能とは何ですか？

リソースプロビジョニングは、EF300およびEF600ストレージアレイで使用できる機能です。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

リソースプロビジョニングボリュームは、SSDグループまたはプール内のシックボリュームです。ボリュームの作成時にはドライブ容量が割り当てられますが（ボリュームに割り当てられます）、ドライブブロックは割り当て解除されます（マッピング解除されます）。これに対し、従来のシックボリュームでは、Data Assurance保護情報のフィールドを初期化し、各RAIDストライプでデータとRAIDパリティの整合性を確保するために、すべてのドライブブロックがバックグラウンドボリューム初期化処理中にマッピングまたは割り当てられます。リソースプロビジョニングボリュームでは、時間制限付きのバックグラウンド初期化は実行されません。代わりに、各RAIDストライプは、ストライプ内のボリュームブロックへの最初の書き込み時に初期化されます。

リソースプロビジョニングボリュームはSSDボリュームグループおよびプールでのみサポートされます。グループまたはプール内のすべてのドライブでNVMeのDeallocated or Unwritten Logical Block Error（DULBE）エラーリカバリ機能がサポートされます。リソースでプロビジョニングされたボリュームを作成すると、そのボリュームに割り当てられていたすべてのドライブブロックが割り当て解除（マッピング解除）されます。また、ホストではNVMe Dataset Managementコマンドを使用して、ボリューム内の論理ブロックの割り当てを解除できます。ブロックの割り当てを解除すると、SSDの消耗度が改善され、書き込みパフォーマンスが最大化されます。向上率はドライブのモデルと容量によって異なります。

リソースでプロビジョニングされるボリューム機能について、どのような点に注意する必要がありますか？

リソースプロビジョニングは、EF300およびEF600ストレージアレイで使用できる機能です。これにより、バックグラウンドの初期化プロセスを実行せずに、ボリュームをただちに使用できます。

リソースプロビジョニング機能は現在使用できません。ビューによっては、コンポーネントがリソースプロビジョニング対応と報告される場合がありますが、リソースプロビジョニングボリュームを作成する機能は、あとで更新するまで無効になっています。

リソースでプロビジョニングされたボリューム

リソースプロビジョニングボリュームは、SSDグループまたはプール内のシックボリュームです。ボリュームの作成時にはドライブ容量が割り当てられますが（ボリュームに割り当てられます）、ドライブブロックは割り当て解除されます（マッピング解除されます）。これに対し、従来のシックボリュームでは、Data Assurance保護情報のフィールドを初期化し、各RAIDストライプでデータとRAIDパリティの整合性を確保するために、すべてのドライブブロックがバックグラウンドボリューム初期化処理中にマッピングまたは割り当てられます。リソースプロビジョニングボリュームでは、時間制限付きのバックグラウンド初期化は実行されません。代わりに、各RAIDストライプは、ストライプ内のボリュームブロックへの最初の書き込み時に初期化されます。

リソースプロビジョニングボリュームはSSDボリュームグループおよびプールでのみサポートされます。グループまたはプール内のすべてのドライブでNVMeのDeallocated or Unwritten Logical Block Error（DULBE）エラーリカバリ機能がサポートされます。リソースでプロビジョニングされたボリュームを作成すると、そのボリュームに割り当てられていたすべてのドライブブロックが割り当て解除（マッピング解除）されます。また、ホストではNVMe Dataset Managementコマンドを使用して、ボリューム内の論理ブロックの割り当てを解除できます。ブロックの割り当てを解除すると、SSDの消耗度が改善され、書き込みパフォーマンスが最大化されます。向上率はドライブのモデルと容量によって異なります。

機能の有効化と無効化

DULBEがサポートされているシステムでは、リソースプロビジョニングがデフォルトで有効になっています。このデフォルト設定は、プールとボリュームグループで無効にできます。リソースプロビジョニングの無効化は、既存のボリュームに対する永続的な処理であり、元に戻すことはできません（つまり、これらのボリュームグループおよびプールのリソースプロビジョニングを再度有効にすることはできません）。

新しいボリュームのリソースプロビジョニングを再度有効にするには、[設定][システム]メニューを使用します。リソースのプロビジョニングを再度有効にすると、新しく作成したボリュームグループとプールのみに影響する点に注意してください。既存のボリュームグループおよびプールは変更されません。必要に応じて、[設定][システム]メニューからリソースプロビジョニングを再度無効にすることもできます。

内部セキュリティキー管理と外部セキュリティキー管理の違いは何ですか？

ドライブセキュリティ機能を実装している場合は、内部セキュリティキーまたは外部セキュリティキーを使用して、セキュリティ有効ドライブがストレージアレイから取り外されたときにデータをロックダウンすることができます。

セキュリティキーは、ストレージアレイのセキュリティ有効ドライブとコントローラで共有される文字列です。内部キーは、コントローラの永続的メモリに保持されます。外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。

セキュリティキーを作成するときは、どのような点に注意する必要がありますか？

セキュリティキーは、ストレージアレイ内のコントローラとセキュリティ有効ドライブによって共有されます。セキュリティ有効ドライブをストレージアレイから取り外すと、セキュリティキーによってデータが不正アクセスから保護されます。

セキュリティキーは次のいずれかの方法で作成および管理できます。

- コントローラの永続的メモリ上での内部キー管理。
- 外部キー管理サーバでの外部キー管理

内部キー管理

コントローラの永続的メモリ上のアクセスできない場所に内部キーが保持され、「非表示」になります。内部セキュリティキーを作成する前に、次の作業を行う必要があります。

1. ストレージアレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブセキュリティ機能が有効になっていることを確認します。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに問い合わせてください。

識別子とパスフレーズを定義して、内部セキュリティキーを作成します。識別子は、セキュリティキーに関連付けられる文字列で、コントローラとキーに関連付けられたすべてのドライブに格納されます。パスフレーズは、バックアップ用にセキュリティキーを暗号化するために使用されます。作成したセキュリティキーは、コントローラ上のアクセスできない場所に格納されます。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

外部キー管理

外部キーは、Key Management Interoperability Protocol（KMIP）を使用して別のキー管理サーバに保持されます。外部セキュリティキーを作成する前に、次の作業を行う必要があります。

1. ストレージアレイにセキュリティ対応ドライブを取り付けます。対応するドライブには、Full Disk Encryption（FDE）ドライブと連邦情報処理標準（FIPS）ドライブがあります。
2. ドライブセキュリティ機能が有効になっていることを確認します。ドライブセキュリティ機能を有効にする手順については、必要に応じてストレージベンダーに問い合わせてください
3. 署名済みのクライアント証明書ファイルを取得します。クライアント証明書は、キー管理サーバがKMIP要求を信頼できるよう、ストレージアレイのコントローラを検証します。
   a. まず、クライアント証明書署名要求（CSR）を生成してダウンロードします。メニューに移動します。Settings [証明書]、[キー管理]、[CSRの作成]の順に選択します。
   b. 次に、キー管理サーバで信頼されているCAから署名済みのクライアント証明書を要求します。（ダウンロードしたCSRファイルを使用して、キー管理サーバからクライアント証明書を作成およびダウンロードすることもできます）。
   c. クライアント証明書ファイルを作成したら、System Managerにアクセスしているホストにそのファイルをコピーします。
4. キー管理サーバから証明書ファイルを取得し、System Managerにアクセスしているホストにそのファイルをコピーします。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるよう、キー管理サーバを検証します。キー管理サーバには、ルート証明書、中間証明書、またはサーバ証明書を使用できます。

キー管理サーバのIPアドレスとKMIP通信に使用するポート番号を定義して、外部キーを作成します。このプロセスでは、証明書ファイルもロードします。作成が完了すると、入力したクレデンシャルを使用してキー管理サーバに接続されます。これで、セキュリティ有効のボリュームグループまたはプールを作成したり、既存のボリュームグループまたはプールでセキュリティを有効にしたりできます。

パスフレーズを定義する必要があるのはなぜですか？

パスフレーズは、ローカルの管理クライアントに格納されているセキュリティキーファイルの暗号化と復号化に使用されます。パスフレーズがないとセキュリティキーを復号化できず、セキュリティ有効ドライブが別のストレージアレイに再設置された場合、データのロック解除にセキュリティキーを使用できません。

著作権に関する情報

商標に関する情報