

VMware vSAN の管理

Update 3

VMware vSphere 8.0

VMware vSAN 8.0

VMware by Broadcom の Web サイトで最新の技術ドキュメントを確認できます

<https://docs.vmware.com/jp/>

VMware by Broadcom

3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2015-2024 Broadcom. All Rights Reserved. 「Broadcom」という語表現は、Broadcom Inc. およびその子会社のいずれかまたは両方を指します。詳細については、<https://www.broadcom.com> を参照してください。本書に記載されるすべての商標、製品名、サービス マークおよびロゴは、各社に帰属します。

目次

『VMware vSAN の管理』について 7

1 更新情報 8

2 vSAN について 9

vSAN の概念 9

vSAN の特性 10

vSAN の用語および定義 12

vSAN と従来のストレージの違い 16

3 vSAN クラスタの構築 17

vSAN デプロイのオプション 18

4 vSAN と他の VMware ソフトウェアの統合 21

5 vSAN の制限事項 22

6 vSAN クラスタの構成および管理 23

vSphere Client を使用した vSAN クラスタの構成 23

既存のクラスタで vSAN を有効にする 26

vSAN をオフにする 26

vSAN 設定の編集 27

vSAN データストアの表示 29

vSAN データストアへのファイルまたはフォルダのアップロード 31

vSAN データストアからのファイルまたはフォルダのダウンロード 32

7 vSAN ポリシーの使用 33

vSAN ポリシーについて 33

vSAN によるポリシー変更の管理方法 40

vSAN ストレージ プロバイダの表示 40

vSAN のデフォルト ストレージ ポリシーについて 41

vSAN データストアのデフォルト ストレージ ポリシーの変更 43

vSphere Client を使用した vSAN のストレージ ポリシーの定義 44

8 vSAN クラスタの拡張および管理 48

vSAN クラスタの拡張 48

vSAN クラスタの容量およびパフォーマンスの強化 49

クイックスタートを使用した vSAN クラスタへのホストの追加 49

vSAN クラスタへのホストの追加	50
ホスト プロファイルを使用した vSAN クラスタ内のホストの構成	51
リモート vSAN データストアの共有	53
リモート vSAN データストアの表示	58
リモート vSAN データストアのマウント	59
リモート vSAN データストアのアンマウント	60
vSphere Client とのデータストア共有の監視	60
データストア ソースとしてのリモート vCenter Server の追加	61
メンテナンス モードでの vSAN クラスタのメンバーの操作	62
vSAN クラスタ内のホストのデータ移行機能の確認	63
vSAN クラスタ メンバーのメンテナンス モードへの切り替え	64
vSAN クラスタのフォルト ドメインの管理	66
vSAN クラスタのフォルト ドメインの新規作成	67
vSAN クラスタの選択したフォルト ドメインへのホストの移動	68
vSAN クラスタのフォルト ドメインからのホストの移動	68
vSAN クラスタのフォルト ドメインの名前変更	69
vSAN クラスタからの選択したフォルト ドメインの削除	69
vSAN クラスタのフォルト ドメインによる追加障害の許容	69
vSAN Data Protection の使用	70
Snapshot Service アプライアンスの展開	73
vSAN Data Protection グループの作成	74
vSAN スナップショットの削除	75
vSAN スナップショットからの仮想マシンのリストア	76
vSAN スナップショットからの仮想マシンのクローン作成	77
vSAN iSCSI ターゲット サービスの使用	77
vSAN iSCSI ターゲット サービスの有効化	78
vSAN iSCSI ターゲットの作成	79
vSAN iSCSI ターゲットへの LUN の追加	79
vSAN iSCSI ターゲットでの LUN のサイズ変更	80
vSAN iSCSI イニシエータ グループの作成	80
vSAN iSCSI イニシエータ グループへのターゲットの割り当て	81
vSAN iSCSI ターゲット サービスをオフにする	82
vSAN iSCSI ターゲット サービスの監視	82
vSAN ファイル サービス	83
vSAN ファイル サービスの制限事項と考慮事項	84
vSAN ファイル サービスの有効化	85
vSAN ファイル サービスの構成	88
vSAN ファイル サービスの編集	93
vSAN ファイル共有の作成	93
vSAN ファイル共有の表示	96
vSAN ファイル共有へのアクセス	96

vSAN ファイル共有の編集	98
vSAN クラスタでの SMB ファイル共有の管理	98
vSAN ファイル共有の削除	99
vSAN 分散ファイル システムのスナップショット	99
vSAN ファイル サービス ホストでのワークロードのリバランス	101
vSAN 分散ファイル システムのマッピング解除による容量の再利用	102
vSAN ファイル サービスのアップグレード	102
vSAN ファイル サービスのパフォーマンスの監視	103
vSAN ファイル共有キャパシティの監視	104
vSAN ファイル サービスとファイル共有の健全性の監視	104
ハイブリッド vSAN クラスタをオールフラッシュ クラスタに移行	105
vSAN クラスタのシャットダウンと再起動	106
クラスタのシャットダウン ウィザードを使用した vSAN クラスタのシャットダウン	106
vSAN クラスタの再起動	107
手動による vSAN クラスタのシャットダウンと再起動	108

9 vSAN クラスタでのデバイス管理 112

vSAN クラスタのストレージ デバイスの管理	112
vSAN クラスタのディスク グループまたはストレージ プールの作成	113
vSAN Original Storage Architecture クラスタのストレージ デバイスの要求	114
vSAN Express Storage Architecture クラスタのストレージ デバイスの要求	115
vSAN Direct 用ディスクの要求	116
vSAN クラスタの個々のデバイスの操作	117
vSAN クラスタのディスク グループへのデバイスの追加	117
vSAN クラスタからのディスクまたはディスク グループのデータ移行機能の確認	118
vSAN からのディスク グループまたはデバイスの削除	119
vSAN クラスタでのディスク グループの再作成	120
vSAN のロケータ LED の使用	120
vSAN でデバイスをフラッシュとしてマークする	121
vSAN でデバイスを HDD としてマークする	122
vSAN でデバイスをローカルとしてマークする	122
vSAN でデバイスをリモートとしてマークする	123
vSAN ディスク グループへのキャパシティ デバイスの追加	123
デバイスからのパーティションの削除	124

10 vSAN クラスタの容量効率の向上 125

vSAN の容量効率機能	125
SCSI マッピング解除による vSAN のストレージ容量の再利用	125
vSAN クラスタでのデデュープおよび圧縮の使用	126
vSAN クラスタのデデュープおよび圧縮の設計に関する考慮事項	128
新規の vSAN クラスタでデデュープおよび圧縮を有効にする	129

- 既存の vSAN クラスタでデデュープと圧縮を有効にする 129
- vSAN クラスタでデデュープおよび圧縮を無効にする 130
- vSAN クラスタにおける仮想マシンの冗長性の低下 131
- デデュープおよび圧縮が有効な場合のディスクの追加または削除 131
- vSAN クラスタでの RAID 5 または RAID 6 イレージャ コーディングの使用 132
- vSAN クラスタの RAID 5 または RAID 6 の設計に関する考慮事項 133

11 vSAN クラスタでの暗号化の使用 134

- vSAN による転送中データの暗号化 134
 - vSAN クラスタでの転送中データの暗号化の有効化 135
- vSAN による保存データの暗号化 135
 - vSAN 保存データの暗号化の仕組み 135
 - vSAN 保存データの暗号化を設計する際の考慮事項 137
 - 標準のキー プロバイダの設定 137
 - 新しい vSAN クラスタでの保存データの暗号化の有効化 143
 - 保存データの暗号化の新しいキーの生成 144
 - 既存の vSAN クラスタでの保存データの暗号化の有効化 145
 - vSAN の暗号化とコア ダンプ 146

12 vSAN クラスタのアップグレード 149

- vSAN のアップグレードの準備 150
- vCenter Server のアップグレード 151
- ESXi ホストのアップグレード 152
- vSAN ディスク フォーマットについて 152
 - vSphere Client を使用した vSAN ディスク フォーマットのアップグレード 153
 - RVC を使用した vSAN のディスク フォーマットのアップグレード 154
 - vSAN ディスク フォーマットのアップグレードの確認 156
- vSAN オブジェクト フォーマットについて 156
- vSAN クラスタのアップグレードの確認 157
- vSAN クラスタのアップグレード中の RVC アップグレード コマンド オプションの使用 157
- vSphere Lifecycle Manager の vSAN ビルドの推奨事項 157

『VMware vSAN の管理』 について

『VMware vSAN の管理』では、VMware vSphere[®] 環境で vSAN クラスタを構成および管理する方法について説明します。

また、『VMware vSAN の管理』では、vSAN クラスタ内でストレージ キャパシティ デバイスとして機能するローカル物理ストレージ リソースを管理する方法や、vSAN データストアにデプロイされた仮想マシンのストレージポリシーを定義する方法について説明します。

VMware では、多様性の受け入れを尊重しています。ユーザー、パートナー、社内コミュニティ内でこの原則を促進するため、包括的な表現でコンテンツを作成します。

対象読者

本書は、仮想化テクノロジー、データセンターの日常的な運用、および vSAN の概念に精通する、豊富な経験をお持ちの仮想化管理者を対象としています。

vSAN の詳細および vSAN クラスタの作成方法については、『vSAN のプランニングとデプロイ』ガイドを参照してください。

vSAN クラスタの監視および問題の解決に関する詳細については、『vSAN の監視とトラブルシューティング』ガイドを参照してください。

更新情報

1

このドキュメントは、製品のリリースごとに、または必要に応じて更新されます。

『VMware vSAN の管理』の更新履歴については、次の表をご確認ください。

リビジョン	説明
2024 年 7 月 25 日	<ul style="list-style-type: none">■ 「リモート vSAN データストアの共有」で vSAN Max のライセンス情報を更新しました。■ 「vSAN スナップショットからの仮想マシンのリストア」に削除された仮想マシンのリストアに関する情報を追加しました。■ マイナー更新を行いました。
2024 年 6 月 25 日	初期リリース。

vSAN について

2

VMware vSAN は ESXi ハイパーバイザーの一部としてネイティブに動作するソフトウェアの分散レイヤーです。

vSAN はホスト クラスタのローカル ディスクまたは直接接続されたキャパシティ デバイスを統合し、vSAN クラスタのすべてのホストで共有される単一のストレージ プールを作成します。vSAN では、共有ストレージを必要とする HA、vMotion、DRS などの VMware 機能をサポートすることで、外部の共有ストレージが不要になり、ストレージ構成や仮想マシンのプロビジョニングを簡素化できます。

次のトピックを参照してください。

- [vSAN の概念](#)
- [vSAN の用語および定義](#)
- [vSAN と従来のストレージの違い](#)

vSAN の概念

VMware vSAN では、仮想マシンの共有ストレージを作成するソフトウェア定義のアプローチを使用します。

ESXi ホストのローカル物理ストレージ リソースを仮想化し、サービス品質要件に沿って仮想マシンとアプリケーションに分割して割り当てることができるストレージのプールに変換します。vSAN は ESXi ハイパーバイザーに直接実装されます。

vSAN は、ハイブリッドまたはオールフラッシュのクラスタのどちらかとして機能するように構成できます。ハイブリッドのクラスタでは、キャッシュ レイヤーにフラッシュ デバイスが使用され、ストレージ容量レイヤーに磁気ディスクが使用されます。オールフラッシュのクラスタでは、キャッシュと容量の両方でフラッシュ デバイスが使用されます。

vSAN は、既存のホスト クラスタまたは新しく作成するクラスタで有効にできます。vSAN は、すべてのローカル キャパシティ デバイスを、vSAN クラスタのすべてのホストによって共有される単一のデータストアに集約します。データストアは、キャパシティ デバイスまたはキャパシティ デバイスが搭載されているホストをクラスタに追加することにより、拡張することができます。vSAN を最適な状態で動作させるには、クラスタのすべての ESXi ホストが、すべてのクラスタ メンバーで類似または同一の構成を共有することをお勧めします。これには、類似または同一のストレージ構成も含まれます。この一貫した構成により、クラスタ内のすべてのデバイスおよびホストで、仮想マシンのストレージ コンポーネントがバランシングされます。ローカル デバイスを持たないホストでも、vSAN データストアでその仮想マシンを参加させて実行することができます。

vSAN Original Storage Architecture (OSA) で、ストレージ デバイスを vSAN データストアに提供する各ホストは、フラッシュ キャッシュ用に少なくとも 1つのデバイスと、キャパシティ用に少なくとも 1つのデバイスを提供する必要があります。提供元のホスト上のデバイスは、1つ以上のディスク グループを形成します。各ディスク グループには、1つのフラッシュ キャッシュ デバイスと、恒久的ストレージ用の 1つまたは複数のキャパシティ デバイスが含まれています。各ホストは、複数のディスク グループを使用するように構成できます。

vSAN Express Storage Architecture (ESA) では、vSAN によって要求されるすべてのストレージ デバイスがキャパシティとパフォーマンスに影響します。vSAN によって要求された各ホストのストレージ デバイスは、ストレージ プールを形成します。ストレージ プールは、ホストによって vSAN データストアに提供されるキャッシュとキャパシティの量を表します。

vSAN クラスタの設計およびサイジングに関するベスト プラクティス、キャパシティの考慮事項、および一般的な推奨事項については、『VMware vSAN 設計とサイジングのガイド』を参照してください。

vSAN の特性

次の特性は、vSAN、そのクラスタ、およびデータストアに適用されます。

vSAN には、データ コンピューティングおよびストレージ環境に回復性と効率性を追加するための多数の機能が含まれています。

表 2-1. vSAN の機能

サポートされている機能	説明
共有ストレージ サポート	vSAN は、HA、vMotion、および DRS など、共有ストレージが必要な VMware 機能をサポートしています。たとえば、ホストの負荷が高くなると、DRS はクラスタ内の他のホストに仮想マシンを移行できます。
オンディスク フォーマット	vSAN のオンディスク仮想ファイル フォーマットは、vSAN クラスタごとに拡張性の高いスナップショットとクローン管理サポートを提供します。vSAN クラスタごとにサポートされる仮想マシン スナップショットとクローンの数については、vSphere の構成の上限 https://configmax.esp.vmware.com/home を参照してください。
オールフラッシュ構成とハイブリッド構成	vSAN は、オールフラッシュまたはハイブリッド クラスタで構成できます。
フォルト ドメイン	vSAN は、vSAN クラスタがデータセンターの複数のラックまたはブレード サーバ シャーシにまたがる場合に、ラックまたはシャーシの障害からホストを保護するフォルト ドメイン構成をサポートしています。
ファイル サービス	vSAN ファイル サービスを使用すると、クライアント ワークステーションまたは仮想マシンがアクセスできる vSAN データストアにファイル共有を作成できます。
iSCSI ターゲット サービス	vSAN iSCSI ターゲット サービスを使用すると、vSAN クラスタ外のホストおよび物理ワークロードが vSAN データストアにアクセスできます。
vSAN ストレッチ クラスタと 2 ノード vSAN クラスタ	vSAN は 2 つの地理的な場所にまたがるストレッチ クラスタをサポートします。

表 2-1. vSAN の機能 (続き)

サポートされている機能	説明
Windows Server Failover Clustering (WSFC) のサポート	<p>vSAN 6.7 Update 3 以降のリリースでは、共有ディスクへのアクセスをノード間で調停するために、Windows Server Failover Clustering (WSFC) で要求される仮想ディスク レベルでの SCSI-3 Persistent Reservations (SCSI3-PR) がサポートされます。SCSI-3 PR がサポートされることにより、vSAN データストアでネイティブに仮想マシン間で共有されているディスク リソースを使用して WSFC を構成できます。</p> <p>現在、以下の構成がサポートされています。</p> <ul style="list-style-type: none"> ■ クラスタあたり最大 6 個のアプリケーション ノード。 ■ ノードあたり最大 64 台の共有仮想ディスク。 <p>注: vSAN では、Microsoft Windows Server 2012 以降で実行される Microsoft SQL Server 2012 以降の動作が確認済みです。</p>
vSAN Health Service	vSAN Health Service には、クラスタ コンポーネントの問題の原因を監視、トラブルシューティング、診断し、潜在的なリスクを識別する事前構成済みの健全性チェック テストが含まれています。
vSAN パフォーマンス サービス	vSAN パフォーマンス サービスには、IOPS、スループット、遅延、および輻輳の監視に使用される統計チャートが含まれています。vSAN クラスタ、ホスト、ディスク グループ、ディスク、および仮想マシンのパフォーマンスを監視できます。
組み込みの vSphere ストレージ機能	vSAN は、従来から VMFS および NFS ストレージとともに使用されている vSphere のデータ管理機能が組み込まれています。これらの機能には、スナップショット、リンク クローン、vSphere Replication が含まれます。
仮想マシン ストレージ ポリシー	<p>vSAN では、仮想マシン ストレージ ポリシーと連携して、仮想マシン中心のストレージ管理をサポートしています。</p> <p>仮想マシンのデプロイ中にストレージ ポリシーを割り当てない場合は、vSAN のデフォルト ストレージ ポリシーが自動的に仮想マシンに割り当てられます。</p>
迅速なプロビジョニング	vSAN では、仮想マシンの作成中およびデプロイ中に、vCenter Server [®] で迅速にストレージをプロビジョニングできます。
デデュープおよび圧縮	vSAN はブロックレベルのデデュープおよび圧縮を実行してストレージ容量を節約します。vSAN オールフラッシュ クラスタでデデュープおよび圧縮を有効にすると、各ディスク グループ内の冗長なデータが削減されます。デデュープと圧縮の設定はクラスタ全体に行いますが、これらの機能はディスク グループ単位で適用されます。圧縮のみの vSAN はディスク単位で適用されます。
保存データの暗号化	vSAN では、保存データの暗号化が提供されます。データの暗号化は、デデュープなどの他のすべての処理が実行された後に行われます。保存データの暗号化を行うと、クラスタからデバイスが削除された場合に備えて、ストレージ デバイス上のデータが保護されます。
転送中データの暗号化	vSAN では、クラスタ内のホスト間で転送中のデータを暗号化できます。転送中データの暗号化を有効にすると、vSAN は、ホスト間で転送されるすべてのデータとメタデータのトラフィックを暗号化します。
SDK サポート	VMware vSAN SDK は、VMware vSphere Management SDK の拡張機能です。これには、開発者が vSAN のインストール、構成、監視、およびトラブルシューティングを自動化する際に役立つドキュメント、ライブラリ、およびコード サンプルが含まれています。

vSAN の用語および定義

vSAN では独自の用語と定義が使用されており、これらを理解することが重要となります。

vSAN の使用を開始する前に、vSAN の重要な用語および定義を確認してください。

ディスク グループ (vSAN Original Storage Architecture)

ディスク グループは、ホストおよび物理デバイス グループでの物理ストレージ容量とパフォーマンスの単位です。これにより、vSAN クラスタのパフォーマンスと容量が決まります。搭載しているローカル デバイスを vSAN クラスタに提供する各 ESXi ホストでは、デバイスがディスク グループに編成されます。

各ディスク グループには、1つのフラッシュ キャッシュ デバイスと1つ以上のキャパシティ デバイスが含まれている必要があります。キャッシュで使用されるデバイスは、ディスク グループ間での共有や、その他の目的で使うことができません。1つのキャッシュ デバイスは、1つのディスク グループ専用にする必要があります。ハイブリッドのクラスタでは、キャッシュ レイヤーにフラッシュ デバイスが使用され、ストレージ容量レイヤーに磁気ディスクが使用されます。オールフラッシュ クラスタでは、キャッシュとキャパシティの両方でフラッシュ デバイスが使用されます。ディスク グループの作成および管理の詳細については、「VMware vSAN の管理」を参照してください。

ストレージ プール (vSAN Express Storage Architecture)

ストレージ プールは、vSAN によって要求されるホスト上のすべてのストレージ デバイスを表します。各ホストには1つのストレージ プールが含まれています。ストレージ プール内の各デバイスは、キャパシティとパフォーマンスの両方を提供します。許可されるストレージ デバイスの数は、ホスト構成によって決まります。

使用される容量

使用される容量とは、任意の時点で1台以上の仮想マシンによって使用される物理容量の合計です。使用される容量は、.vmdk ファイルの使用サイズ、保護レプリカなどの多くの要因によって決定されます。キャッシュサイジングの計算時には、保護レプリカで使用される容量は考慮されません。

オブジェクト ベースのストレージ

vSAN では、オブジェクトと呼ばれる柔軟性の高いデータ コンテナの形でデータを格納および管理します。オブジェクトは、クラスタ全体に分散されているデータおよびメタデータを含む論理ボリュームです。たとえば、スナップショットと同様に、.vmdk はそれぞれが1つのオブジェクトです。vSAN データストアに仮想マシンをプロビジョニングする場合、vSAN は、複数のコンポーネントで構成されるオブジェクト セットを仮想ディスクごとに作成します。また、コンテナ オブジェクトとして仮想マシン ホームの名前空間を作成し、仮想マシンのすべてのメタデータ ファイルを格納します。vSAN は、割り当てられた仮想マシン ストレージ ポリシーに基づいて、各オブジェクトを個別にプロビジョニングおよび管理します。たとえば、すべてのオブジェクトに RAID を構成する場合に使用することができます。

注： vSAN Express Storage Architecture が有効な場合、すべてのスナップショットは新しいオブジェクトではありません。ベース .vmdk とそのスナップショットは、1つの vSAN オブジェクトに含まれています。また、vSAN ESA では、ダイジェストは vSAN オブジェクトによってバックアップされます。

vSAN は、次の要因を考慮して、仮想ディスクのオブジェクトを作成し、クラスタにオブジェクトを分散する方法を決定します。

- vSAN は、指定された仮想マシン ストレージ ポリシー設定に基づいて、仮想ディスク要件が適用されていることを確認します。
- vSAN はプロビジョニングの時点で、正しいクラスタ リソースが使用されていることを確認します。たとえば vSAN は、保護ポリシーに基づいて作成するレプリカの数を決めます。パフォーマンス ポリシーにより、各レプリカに割り当てられる Flash Read Cache の量、各レプリカで作成されるストライプの数、およびそれを配置するクラスタ内の場所が決まります。
- vSAN は、仮想ディスクのポリシーに準拠しているかどうかを継続的に監視してレポートします。ポリシーに準拠していない場合は、原因となっている問題のトラブルシューティングを行って解決する必要があります。

注： 必要に応じて、仮想マシン ストレージ ポリシーの設定を編集できます。ストレージ ポリシーの設定を変更しても、仮想マシンへのアクセスに影響はありません。vSAN は、再構成に使用するストレージとネットワーク リソースを動的に調整して、オブジェクトの再構成が通常のワークロードに与える影響を最小にします。仮想マシン ストレージ ポリシーの設定を変更すると、vSAN が、オブジェクトの再作成プロセスを開始し、その後再同期を行う場合があります。「vSAN の監視とトラブルシューティング」を参照してください。

- vSAN は、ミラーリングや監視などの必要な保護コンポーネントが、異なるホストやフォルト ドメインに配置されていることを確認します。たとえば、障害発生時にコンポーネントを再構築するために、仮想マシン オブジェクトの保護コンポーネントを 2 台の異なるホストに配置するか、フォルト ドメイン全体に配置する必要がある場合、vSAN は配置ルールに適合する ESXi ホストを検索します。

vSAN データストア

クラスタで vSAN を有効にすると、単一の vSAN データストアが作成されます。これは、仮想ボリューム、VMFS、および NFS などを含む使用可能なデータストアのリストに、別のタイプのデータストアとして表示されます。1 つの vSAN データストアで、仮想マシンや仮想ディスクごとに異なるレベルのサービス レベルを提供できます。vCenter Server[®] では、vSAN データストアのストレージ特性が一連の機能として表示されます。これらの機能は、仮想マシンのストレージ ポリシーを定義するときに参照できます。仮想マシンをデプロイする際、vSAN はこのポリシーを使用して、各仮想マシンの要件に基づいて最適な方法で仮想マシンを配置します。ストレージ ポリシーの使用については、『vSphere ストレージ』ドキュメントを参照してください。

vSAN データストアでは、特定の特性について考慮する必要があります。

- vSAN は、クラスタにストレージを提供しているかどうかに関係なく、クラスタ内のすべてのホストがアクセスできる単一の vSAN データストアを提供します。各ホストには、Virtual Volumes、VMFS、または NFS などの他の任意のデータストアをマウントすることもできます。
- Storage vMotion を使用することにより、vSAN データストア間、NFS データストア間、および VMFS データストア間で仮想マシンを移行できます。
- キャパシティとして使用される磁気ディスクとフラッシュ デバイスのみが、データストアの容量に反映できます。フラッシュ キャッシュとして使用されるデバイスは、データストアの一部に含まれません。

オブジェクトとコンポーネント

各オブジェクトは、一連のコンポーネントで構成されます。これらは、仮想マシンのストレージ ポリシーが使用する機能に応じて決定されます。たとえば、[許容される障害の数] が 1 に設定されている場合、vSAN は、レプリカや監視などの保護コンポーネントがそれぞれ vSAN クラスターの個別のホストに配置されるようにします。この場合、各レプリカはオブジェクト コンポーネントとなります。また、同じポリシーで [オブジェクトあたりのディスク ストライプの数] が 2 以上に設定されている場合、vSAN は複数のキャパシティ デバイスにわたってオブジェクトのストライピングも行い、各ストライプが、指定したオブジェクトのコンポーネントとみなされます。必要な場合、vSAN は、大きなオブジェクトを複数のコンポーネントに分割することもあります。

vSAN データストアには、次のオブジェクト タイプが含まれます。

VM Home 名前空間

.vmx、ログ ファイル、.vmdk ファイル、スナップショット差分記述ファイルなどの仮想マシンの構成ファイルすべてが保存されている、仮想マシンのホーム ディレクトリ。

VMDK

仮想マシンのハード ディスク ドライブの内容を格納する、仮想マシンのディスク ファイル (.vmdk ファイル)。

仮想マシン スワップ オブジェクト

仮想マシンのパワーオン時に作成されます。

スナップショット差分 VMDK

仮想マシンのスナップショットの作成時に作成されます。このような差分ディスクは、vSAN Express Storage Architecture 用には作成されません。

メモリ オブジェクト

仮想マシンの作成またはサスペンドで、スナップショット メモリ オプションを選択するときに作成されます。

仮想マシンのコンプライアンス ステータス：準拠および非準拠

仮想マシンの 1 つ以上のオブジェクトが、割り当てられているストレージ ポリシーの要件を満たしていない場合、その仮想マシンは非準拠とみなされます。たとえば、ミラー コピーのいずれかにアクセスできない場合、ステータスは非準拠になります。ストレージ ポリシーに定義されている要件に仮想マシンが準拠している場合、その仮想マシンは準拠していることとなります。[仮想ディスク] ページの [物理ディスクの配置] タブから、仮想マシン オブジェクトのコンプライアンスの状態を確認できます。vSAN クラスターのトラブルシューティングの詳細については「vSAN の監視とトラブルシューティング」を参照してください。

コンポーネントの状態：「低下」および「なし」

vSAN は、コンポーネントの次の障害状態を認識します。

- 低下：vSAN で永続的なコンポーネント障害が検出され、障害が発生したコンポーネントが正常な状態に戻らないと判断される場合、コンポーネントのステータスは「低下」になります。vSAN は低下したコンポーネントの再構築をすぐに開始します。この状態は、障害の発生したデバイスにコンポーネントが存在する場合に発生することがあります。

- なし：vSAN で一時的なコンポーネント障害が検出され、そのすべてのデータを含むコンポーネントがリカバリされて vSAN が元の状態に戻るとみなされる場合、コンポーネントのステータスは「なし」になります。この状態は、ホストを再起動するとき、または vSAN ホストからデバイスを切り離す場合に発生する可能性があります。vSAN は 60 分待ってから、[なし] ステータスのコンポーネントの再構築を開始します。

オブジェクトの状態：[健全] および [非健全]

クラスタ内の障害のタイプと数に応じて、オブジェクトのステータスは次のいずれかになります。

- 健全：少なくとも 1 つの完全な RAID 1 ミラーリングを使用できる場合、または最低限必要な数のデータ セグメントを使用できる場合、オブジェクトは健全であるとみなされます。
- 非健全：オブジェクトは完全なミラーリングが利用できないか、最小限必要なデータ セグメントを RAID 5 または RAID 6 のオブジェクトに使用できないときに、非健全とみなされます。利用可能なオブジェクトの票が 50% に満たない場合は、オブジェクトは非健全です。クラスタで複数の障害が発生すると、オブジェクトが非健全になることがあります。オブジェクトの動作ステータスが非健全とみなされる場合は、関連する仮想マシンの可用性に影響します。

監視

監視は、メタデータのみを含み、実際のアプリケーション データは何も含まないコンポーネントです。障害が発生した後、存続しているデータストアのコンポーネントの可用性に関して決定を下す場合のタイプレカとして機能します。オンディスク フォーマット 1.0 を使用する場合、監視は vSAN データストアでメタデータにおよそ 2 MB の容量を使用し、バージョン 2.0 以降のオンディスク フォーマットでは 4 MB の容量を使用します。

vSAN では、オブジェクトの可用性の判別に、各コンポーネントが 1 つ以上の票を持つ非対称投票システムを使用してクォラムを維持します。票が 50% を超えると、仮想マシンのストレージ オブジェクトはいつでもアクセス可能で、オブジェクトは利用可能とみなされます。票が 50% 以下の場合、すべてのホストがオブジェクトにアクセス可能ですが、オブジェクトは vSAN データストアにアクセスできなくなります。アクセスできないオブジェクトは、関連付けられた仮想マシンの可用性に影響を与えることがあります。

ストレージ ポリシーベースの管理 (SPBM)

vSAN を使用する場合、パフォーマンスや可用性などの仮想マシンのストレージ要件を、ポリシーという形で定義できます。vSAN を使用すると、vSAN データストアにデプロイされる仮想マシンに、少なくとも 1 台の仮想マシン ストレージ ポリシーが割り当てられるようになります。仮想マシンのストレージ要件が分かっている場合は、ストレージ ポリシーを定義し、仮想マシンに割り当てることができます。仮想マシンのデプロイ時にストレージ ポリシーを適用しない場合、vSAN はデフォルトの vSAN ポリシーを自動的に割り当てます。このポリシーでは、[許容される障害の数] が 1 で、各オブジェクトに単一のディスク ストライプが設定され、シン プロビジョニングされた仮想ディスクが使用されます。ベスト プラクティスとして、ポリシーの要件がデフォルトのストレージ ポリシーで定義されている要件と同じ場合でも、独自の仮想マシン ストレージ ポリシーを定義します。vSAN ストレージ ポリシーの使用方法については、「VMware vSAN の管理」を参照してください。

vSphere PowerCLI

VMware vSphere PowerCLI では、vSAN 用にコマンドライン スクリプトのサポートが追加され、構成および管理タスクの自動化を支援します。vSphere PowerCLI は、vSphere API に Windows PowerShell インターフェイスを提供します。PowerCLI には、vSAN コンポーネントを管理するためのコマンドレットが含まれています。vSphere PowerCLI の使用の詳細については、vSphere PowerCLI のドキュメントを参照してください。

vSAN と従来のストレージの違い

vSAN には従来のストレージ アレイと共通する特性が多数ありますが、vSAN の全体的な動作と機能は異なります。たとえば、vSAN は ESXi ホストのみの管理と操作が可能で、1 つの vSAN インスタンスがクラスタの 1 つのデータストアを提供します。

vSAN と従来のストレージは、次のような重要な面においても異なります。

- vSAN では、ファイバ チャンネル (FC) やストレージ エリア ネットワーク (SAN) などの仮想マシン ファイルをリモートで保存する外部ネットワーク ストレージは不要です。
- 従来のストレージでは、ストレージ管理者が異なるストレージ システムに事前にストレージ容量を割り当てます。vSAN は、ESXi ホストのローカル物理ストレージ リソースを自動的に単一のストレージ プールに変換します。これらのプールは、サービスの品質要件に応じて仮想マシンおよびアプリケーションに分割して割り当てることができます。
- vSAN は、LUN や NFS 共有に基づく従来のストレージ ボリュームのように動作しません。iSCSI ターゲット サービスは LUN を使用して、リモート ホスト上でイニシエータを有効にし、ブロック レベルのデータを vSAN クラスタ内のストレージ デバイスに転送します。
- FCP などの一部の標準ストレージ プロトコルは vSAN に適用されません。
- vSAN は vSphere と高度に統合されます。従来のストレージとは異なり、vSAN には専用プラグインやストレージ コンソールは必要ありません。vSphere Client を使用して vSAN をデプロイ、管理、監視できます。
- 専用ストレージ管理者が vSAN を管理する必要はありません。代わりに、vSphere 管理者が vSAN 環境を管理できます。
- vSAN を使用する場合、新しい仮想マシンを展開するときに自動的に仮想マシン ストレージ ポリシーが割り当てられます。ストレージ ポリシーは、必要に応じて動的に変更できます。

vSAN クラスタの構築

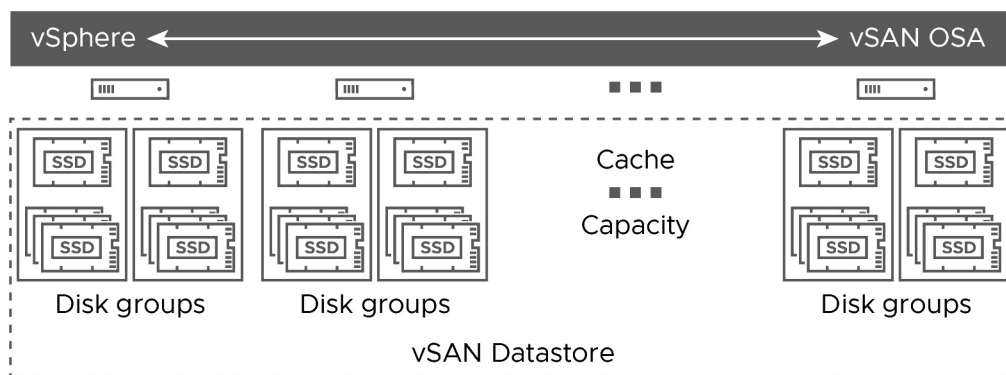
3

vSAN クラスタを作成するときに、ストレージ アーキテクチャと展開オプションを選択できます。

リソースとニーズに最適な vSAN ストレージ アーキテクチャを選択してください。

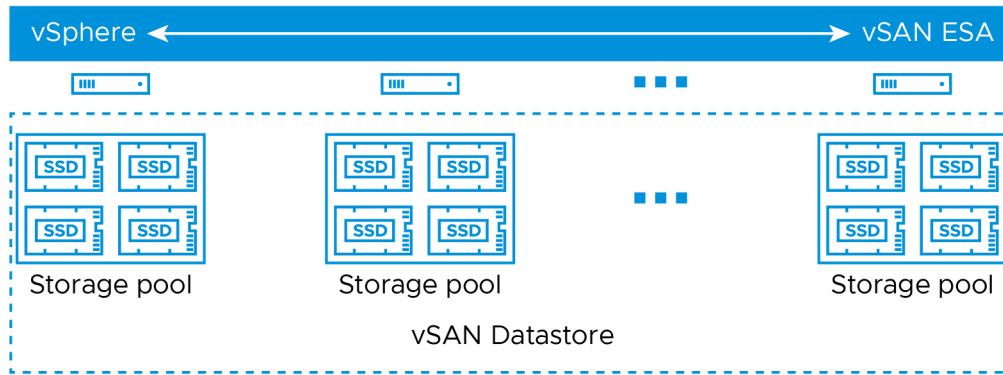
vSAN Original Storage Architecture

vSAN Original Storage Architecture (OSA) は、フラッシュ ソリッド ステート ドライブ (SSD) や磁気ディスク ドライブ (HDD) など、幅広いストレージ デバイス向けに設計されています。ストレージを提供する各ホストには、1つ以上のディスク グループがあります。各ディスク グループには、1つのフラッシュ キャッシュ デバイスと1つ以上のキャパシティ デバイスが含まれます。



vSAN Express Storage Architecture

vSAN Express Storage Architecture (ESA) は、高性能な NVMe ベースの TLC フラッシュ デバイスと高性能ネットワーク向けに設計されています。ストレージを提供する各ホストには、4つ以上のフラッシュ デバイスから構成されるストレージ プールが1つあります。各フラッシュ デバイスは、キャッシュとキャパシティをクラスタに提供します。



要件に応じて、次の方法で vSAN を展開できます。

vSAN ReadyNode

vSAN ReadyNode は、Cisco、Dell、Fujitsu、IBM、Supermicro などの VMware パートナーから提供される vSAN ソフトウェアの事前構成済みソリューションです。このソリューションには、サーバ OEM および VMware が推奨する vSAN デプロイでテストされ、認定済みハードウェア フォーム ファクタで検証されたサーバ構成が含まれます。特定のパートナーにおける vSAN ReadyNode ソリューションの詳細については、VMware パートナーの Web サイトを参照してください。

ユーザー定義 vSAN クラスタ

vSAN クラスタを構築するには、vSAN 互換性ガイド (VCG) Web サイト (<http://www.vmware.com/resources/compatibility/search.php>) に記載されている個々のソフトウェアとハードウェア コンポーネント (ドライバ、ファームウェア、ストレージ I/O コントローラなど) を選択します。VCG Web サイトに記載されている認定された任意のサーバ、ストレージ I/O コントローラ、キャパシティ デバイスとフラッシュ キャッシュ デバイス、メモリ、CPU ごとに必要なコア数を選択できます。vSAN でサポートされているソフトウェアおよびハードウェア コンポーネント、ドライバ、ファームウェア、およびストレージ I/O コントローラを選択する前に、VCG Web サイトで互換性情報を確認します。vSAN クラスタを設計する場合は、VCG Web サイトに記載されているデバイス、ファームウェア、ドライバのみを使用します。VCG に記載されていないソフトウェアおよびハードウェア バージョンを使用すると、クラスタで障害や予期しないデータ損失が発生する可能性があります。vSAN クラスタの設計の詳細については、『vSAN プランニングとデプロイ』の「vSAN クラスタの設計とサイジング」を参照してください。

次のトピックを参照してください。

- [vSAN デプロイのオプション](#)

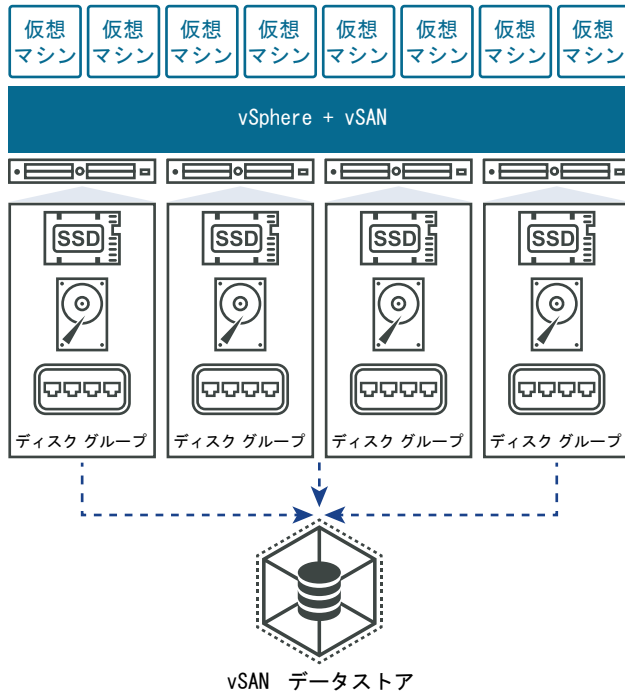
vSAN デプロイのオプション

このセクションでは、vSAN クラスタでサポートされる展開オプションについて説明します。

単一サイトの vSAN クラスタ

単一サイトの vSAN クラスタは、3 台以上のホストで構成されます。通常、単一サイトの vSAN クラスタ内のすべてのホストは単一サイトに配置され、同じレイヤー 2 ネットワークに接続されています。オールフラッシュ構成には 10 Gb ネットワーク接続が必要です。vSAN Express Storage Architecture には 25 Gb ネットワーク接続が必要です。

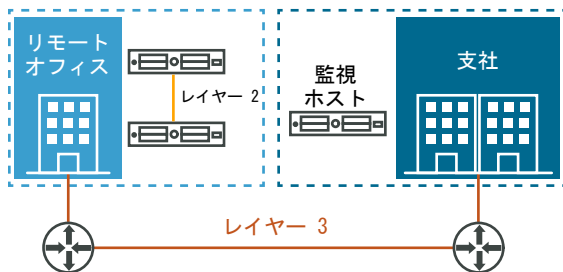
詳細については、「単一サイトの vSAN クラスタの作成」を参照してください。



2 ノード構成の vSAN クラスタ

2 ノード構成の vSAN クラスタは、リモート オフィスや支社などの環境で使用されることが多く、通常は高可用性が必要な少数のワークロードを実行します。2 ノード構成の vSAN クラスタは同じ場所に配置された 2 台のホストで構成され、同じネットワーク スイッチに接続されるか、直接接続されます。2 ノード構成の vSAN クラスタに 3 台目のホストを監視ホストとして追加できます。監視ホストは、支社から離れた場所に配置することが可能です。通常、監視ホストは vCenter Server とともに主要サイトに配置されます。

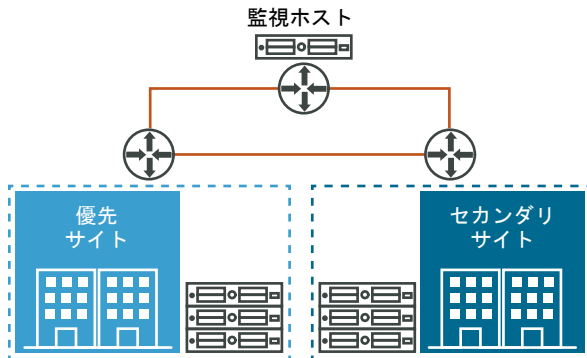
詳細については、「vSAN ストレッチ クラスタまたは 2 ノード クラスタの作成」を参照してください。



vSAN ストレッチ クラスタ

vSAN ストレッチ クラスタはサイト全体の障害に対する回復性を提供します。vSAN ストレッチ クラスタ内のホストは、2つのサイトで均等に分散されます。2つのサイトには、5 ミリ秒 (5ms) 以下のネットワーク遅延が必要です。vSAN 監視ホストは、監視機能を提供する 3 番目のサイトにあります。監視ホストは、2つのデータ サイト間でネットワークパーティションが発生する際のタイブレーカとしても機能します。監視ホストには、監視コンポーネントなどのメタデータのみが保存されます。

詳細については、「[vSAN ストレッチ クラスタまたは 2 ノード クラスタの作成](#)」を参照してください。



vSAN と他の VMware ソフトウェア の統合

4

vSAN を起動して実行すると、残りの VMware ソフトウェア スタックと統合されます。

vSphere コンポーネントや、vSphere vMotion、スナップショット、クローン、Distributed Resource Scheduler (DRS)、vSphere High Availability、VMware Site Recovery Manager などの機能を使用すると、従来のストレージで可能なほとんどの操作を実行できます。

vSphere HA

vSphere HA と vSAN を同じクラスタで有効にできます。従来のデータストアの場合と同様に、vSphere HA では vSAN データストアの仮想マシンに同じレベルの保護が提供されます。このレベルの保護では、vSphere HA と vSAN がやり取りするときに、特定の制限が適用されます。vSphere HA と vSAN の統合に関する具体的な考慮事項については、『vSAN のプランニングとデプロイ』の「vSAN と vSphere HA の使用」を参照してください。

VMware Horizon View

vSAN と VMware Horizon View を統合することができます。統合すると、仮想デスクトップ環境に関して vSAN に次のメリットがあります。

- 自動キャッシュを備えた高性能ストレージ
- 自動修正用のポリシーベースのストレージ管理

vSAN と VMware Horizon の統合の詳細については、VMware with Horizon View のドキュメントを参照してください。vSAN 用の VMware Horizon View の設計およびサイジングについては、『Designing and Sizing Guide for Horizon View』を参照してください。

vSAN の制限事項

5

このトピックでは、vSAN の制限事項について説明します。

vSAN を操作するときは、次の制限事項を考慮してください。

- vSAN では、複数の vSAN クラスタに参加するホストはサポートされません。ただし、クラスタ全体で共有される他の外部ストレージ リソースに、vSAN ホストからアクセスできます。
- vSAN では、vSphere DPM および Storage I/O Control はサポートされません。
- vSAN では、SE スパース ディスクはサポートされません。
- vSAN では、RDM、VMFS、診断パーティション、その他のデバイス アクセス機能はサポートされません。

vSAN クラスタの構成および管理

6

vSphere Client、esxcli コマンド、およびその他のツールを使用して vSAN クラスタを構成および管理できます。

次のトピックを参照してください。

- vSphere Client を使用した vSAN クラスタの構成
- 既存のクラスタで vSAN を有効にする
- vSAN をオフにする
- vSAN 設定の編集
- vSAN データストアの表示
- vSAN データストアへのファイルまたはフォルダのアップロード
- vSAN データストアからのファイルまたはフォルダのダウンロード

vSphere Client を使用した vSAN クラスタの構成

vSphere Client を使用して、既存のクラスタに vSAN を構成できます。

注： クイックスタートを使用して、vSAN クラスタをすばやく作成および設定することができます。詳細については、『vSAN のプランニングとデプロイ』の「クイックスタートを使用した vSAN クラスタの構成および拡張」を参照してください。

前提条件

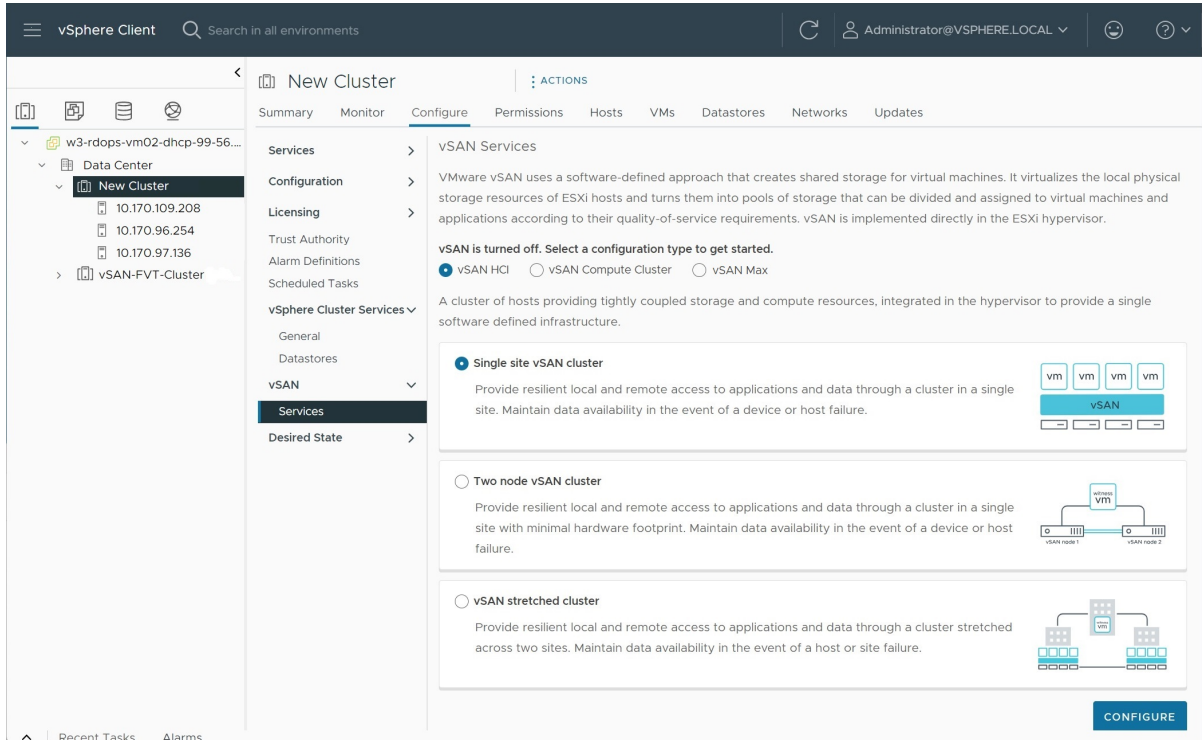
環境がすべての要件を満たしていることを確認します。『vSAN のプランニングとデプロイ』の「vSAN を有効にするための要件」を参照してください。

vSAN を有効にして構成する前に、クラスタを作成してホストを追加します。各ホストのポート プロパティを構成して、vSAN サービスを追加します。

手順

- 1 既存のホスト クラスタに移動します。
- 2 [構成] タブをクリックします。

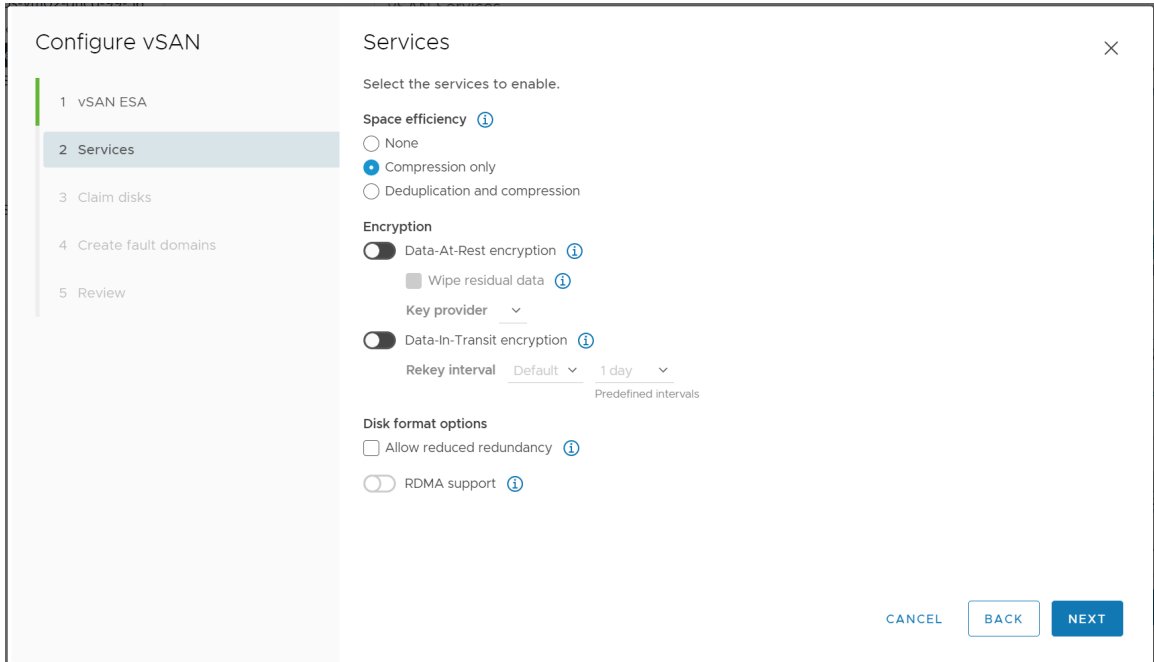
3 [vSAN] の下で [サービス] を選択します。



a HCI 構成タイプを選択します。

- [vSAN HCI] はコンピューティング リソースとストレージ リソースを提供します。データストアは、同じデータセンター内のクラスタ間、およびリモート vCenter Server によって管理されているクラスタ間で共有できます。
- [vSAN コンピューティング クラスタ] は、vSphere コンピューティング リソースのみを提供します。同じデータセンターの vSAN Max クラスタおよびリモート vCenter Server によって提供されるデータストアをマウントできます。

- [vSAN Max] (vSAN ESA クラスタ) はストレージ リソースを提供しますが、コンピューティング リソースは提供しません。データストアは、クライアント vSphere クラスタ、同じデータセンター内の vSAN クラスタ、およびリモート vCenter Server からマウントできます。
- b 展開オプション (単一サイトの vSAN クラスタ、2 ノード vSAN クラスタ、または vSAN ストレッチ クラスタ) を選択します。
- c [構成] をクリックして、[vSAN の構成] ウィザードを開きます。



- 4 クラスタに互換性がある場合は [vSAN ESA] を選択して、[次へ] をクリックします。
- 5 使用する vSAN サービスを構成し、[次へ] をクリックします。

デデュープおよび圧縮、保存データの暗号化、転送中データの暗号化などのデータ管理機能を構成します。ネットワークで RDMA (リモート ダイレクト メモリ アクセス) がサポートされている場合は、[RDMA] を選択します。

- 6 vSAN クラスタのディスクを要求し、[次へ] をクリックします。

vSAN Original Storage Architecture (vSAN OSA) の場合、ストレージを提供する各ホストに、キャッシュ用として少なくとも 1 台のフラッシュ デバイスが必要です。また、キャパシティ用に 1 台以上のデバイスが必要です。vSAN Express Storage Architecture (vSAN ESA) の場合、ストレージを提供する各ホストに 1 つ以上のフラッシュ デバイスが必要です。

- 7 フォルト ドメインを作成して、同時に障害が発生するホストをグループ化します。
- 8 構成を確認して [終了] をクリックします。

結果

vSAN を有効にすると、vSAN データストアが作成され、vSAN ストレージ プロバイダが登録されます。vSAN ストレージ プロバイダは組み込みのソフトウェア コンポーネントで、データストアのストレージ機能と vCenter Server との通信を行います。

次のステップ

vSAN データストアが作成されたことを確認します。「[vSAN データストアの表示](#)」を参照してください。

vSAN ストレージ プロバイダが登録されていることを確認します。

既存のクラスタで vSAN を有効にする

既存のクラスタで vSAN を有効にして、機能とサービスを構成できます。

前提条件

環境がすべての要件を満たしていることを確認します。『[vSAN のプランニングとデプロイ](#)』の「[vSAN を有効にするための要件](#)」を参照してください。

手順

- 1 既存のホスト クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] の下で [サービス] を選択します。
 - a 構成タイプ (単一サイトの vSAN クラスタ、2 ノード vSAN クラスタ、または vSAN ストレッチ クラスタ) を選択します。
 - b クラスタ ホストにディスク グループまたはストレージ プールを追加する場合は、[ローカル vSAN データストアが必要] を選択します。
 - c [構成] をクリックして、[vSAN を構成] ウィザードを開きます。
- 4 クラスタに互換性がある場合は [vSAN ESA] を選択して、[次へ] をクリックします。
- 5 使用する vSAN サービスを構成し、[次へ] をクリックします。

デデュープおよび圧縮、保存データの暗号化、転送中データの暗号化などのデータ管理機能を構成します。ネットワークで RDMA (リモート ダイレクト メモリ アクセス) がサポートされている場合は、[RDMA] を選択します。
- 6 vSAN クラスタのディスクを要求し、[次へ] をクリックします。

vSAN Original Storage Architecture (vSAN OSA) の場合、ストレージを提供する各ホストに、キャッシュ用として少なくとも 1 つのフラッシュ デバイスが必要です。また、キャパシティ用に 1 つ以上のデバイスが必要です。vSAN Express Storage Architecture (vSAN ESA) の場合、ストレージを提供する各ホストに 1 つ以上のフラッシュ デバイスが必要です。
- 7 フォルト ドメインを作成して、同時に障害が発生するホストをグループ化します。
- 8 構成を確認して [終了] をクリックします。

vSAN をオフにする

ホスト クラスタの vSAN をオフにできます。

クラスタで vSAN をオフにすると、vSAN データストアのすべての仮想マシンとデータ サービスにアクセスできなくなります。vSAN Direct を使用して vSAN クラスタのストレージを使用している場合、健全性チェック、容量レポート、パフォーマンス監視などの vSAN Direct 監視サービスも使用できなくなります。vSAN がオフのときに仮想マシンを使用する場合は、必ず vSAN クラスタをオフにする前に仮想マシンを vSAN データストアから別のデータストアに移行します。

前提条件

ホストがメンテナンス モードであることを確認します。詳細については、「[vSAN クラスタのメンバーをメンテナンス モードに切り替える](#)」を参照してください。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で [サービス] を選択します。
- 4 [vSAN をオフにする] をクリックします。
- 5 [vSAN をオフにする] ダイアログで選択内容を確認します。

vSAN 設定の編集

vSAN クラスタの設定を編集してデータ管理機能を構成し、クラスタから提供されるサービスを有効にすることができます。

デデュープおよび圧縮、または暗号化を有効にする場合は、既存の vSAN クラスタの設定を編集します。デデュープおよび圧縮、または暗号化を有効にする場合は、クラスタのオンディスク フォーマットは自動的に最新バージョンにアップグレードされます。

The screenshot displays the VMware vSAN configuration page for a cluster named 'vSAN-FVT-Cluster'. The left sidebar contains navigation options such as 'Services', 'Configuration', 'Licensing', 'Trust Authority', 'Alarm Definitions', 'Scheduled Tasks', 'vSphere Cluster Services', 'vSAN', and 'Desired State'. The main content area is titled 'vSAN Services' and includes several sections:

- Storage:** Shows 'Cluster type' as vSAN HCI and 'Storage types' as vSAN ESA. A description explains that vSAN ESA is a next-generation architecture for high-performance storage.
- vSAN ESA:** Lists 'vSAN managed disk claim' and 'Auto-Policy management', both currently disabled.
- vSAN iSCSI Target Service:** Currently disabled.
- Data Services:** Includes 'Space efficiency' (Storage policy managed compression), 'Data-at-rest encryption' (Disabled), and 'Data-in-transit encryption' (Disabled).
- Performance Service:** Currently enabled.
- File Service:** Currently disabled.
- Advanced Options:** Lists settings like 'Object repair timer' (60 minutes), 'Site read locality' (Enabled), 'Thin swap' (Enabled), 'Guest Trim/Unmap' (Enabled), and 'Automatic rebalance' (Disabled).

手順

- 1 vSAN クラスタに移動します。

2 [構成] タブをクリックします。

a [vSAN] の下で [サービス] を選択します。

b 構成するサービスの [編集] または [有効化] ボタンをクリックします。

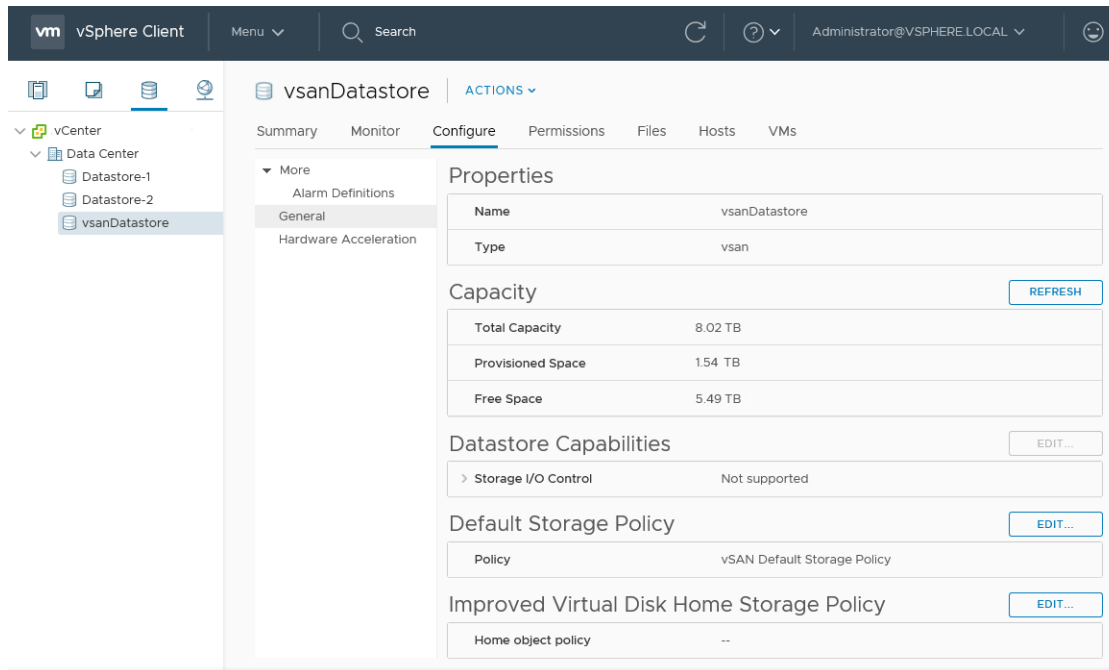
- ストレージを構成します。[リモート データストアのマウント] をクリックして、他の vSAN クラスタのストレージを使用します。
- vSAN パフォーマンス サービスを構成します。詳細については、『vSAN の監視とトラブルシューティング』の「vSAN のパフォーマンスの監視」を参照してください。
- ファイル サービスを有効にします。詳細については、『VMware vSAN の管理』の「vSAN ファイル サービス」を参照してください。
- vSAN ネットワーク オプションを構成します。詳細については、『vSAN のプランニングとデプロイ』の「vSAN ネットワークの構成」を参照してください。
- iSCSI ターゲット サービスを構成します。詳細については、『VMware vSAN の管理』の「vSAN iSCSI ターゲット サービスの使用」を参照してください。
- デデュープと圧縮、保存データの暗号化、転送中データの暗号化などのデータ サービスを構成します。
- vSAN Data Protection を構成します。vSAN Data Protection を使用する前に、vSAN Snapshot Service を展開する必要があります。詳細については、『VMware vSAN の管理』の「Snapshot Service アプライアンスの展開」を参照してください。
- キャパシティの予約とアラートを構成します。詳細については、『vSAN の監視とトラブルシューティング』の「予約済み容量について」を参照してください。
- 詳細オプションを構成します。
 - オブジェクト修復タイマー
 - vSAN ストレッチ クラスタのサイト読み取りのローカリティ
 - シン スワップ プロビジョニング
 - 最大 64 ホストの大規模クラスタのサポート
 - 自動リバランス
- vSAN 健全性サービスの履歴を構成します。

c 要件に合わせて設定を変更します。

3 [適用] をクリックして、選択内容を確認します。

vSAN データストアの表示

vSAN を有効にした後、単一のデータストアが作成されます。vSAN データストアの容量を確認できます。



前提条件

vSAN とディスク グループまたはストレージ プールを構成します。

手順

- 1 [ストレージ] に移動します。
- 2 vSAN データストアを選択します。
- 3 [構成] タブをクリックします。
- 4 vSAN データストアの容量を確認します。

vSAN データストアのサイズは、ESXi ホストごとのキャパシティ デバイスの数と、クラスタ内の ESXi ホストの数によって決まります。たとえば、ホストに 2 TB のキャパシティ デバイスが 7 個あり、クラスタにホストが 8 台含まれる場合、およそのストレージ容量は $7 \times 2 \text{ TB} \times 8 = 112 \text{ TB}$ になります。オールフラッシュ構成を使用している場合、キャパシティにはフラッシュ デバイスが使用されます。ハイブリッド構成の場合、容量には磁気ディスクが使用されます。

一部の容量はメタデータに割り当てられます。

- オンディスク フォーマット バージョン 1.0 では、キャパシティ デバイスあたり約 1 GB が追加されます。
- オンディスク フォーマット バージョン 2.0 では、キャパシティ オーバーヘッドが追加されます（一般的にはデバイスあたり 1～2% の容量にすぎない）。
- オンディスク フォーマット バージョン 3.0 以降では、キャパシティ オーバーヘッドが追加されます（一般的にはデバイスあたり 1～2% の容量にすぎない）。ソフトウェア チェックサムが有効になっているデデュプレおよび圧縮では、デバイスあたり約 6.2% の容量の追加のオーバーヘッドがかかります。

次のステップ

vSAN データストアのストレージ機能を使用して、仮想マシンのストレージ ポリシーを作成します。詳細については、『vSphere のストレージ』ドキュメントを参照してください。

vSAN データストアへのファイルまたはフォルダのアップロード

vSAN データストアには、vmdk ファイルをアップロードできます。

また、vSAN データストアには、フォルダをアップロードすることもできます。データストアの詳細については、『vSphere ストレージ』を参照してください。vSAN データストアに vmdk ファイルをアップロードするときは、次の考慮事項が適用されます。

- vSAN データストアには、ストリーム最適化された vmdk ファイルのみをアップロードできます。VMware ストリーム最適化ファイル形式は、ストリーミング用に圧縮されたモノリシックなスパース形式です。ストリーム最適化形式ではない vmdk ファイルをアップロードする場合は、アップロードを行う前に、vmware-vdiskmanager コマンドライン ユーティリティを使用して、vmdk ファイルをストリーム最適化形式に変換してください。詳細については、『Virtual Disk Manager User's Guide』を参照してください。
- vmdk ファイルを vSAN データストアにアップロードすると、vmdk ファイルは、そのデータストアのデフォルト ポリシーを継承します。vmdk は、ダウンロード元の仮想マシンのポリシーを継承しません。vSAN は、vsanDatastore のデフォルト ポリシー (RAID -1) を適用してオブジェクトを作成します。データストアのデフォルト ポリシーは変更できます。「[vSAN データストアのデフォルト ストレージ ポリシーの変更](#)」を参照してください。
- vmdk ファイルは、仮想マシンのホーム フォルダにアップロードする必要があります。

手順

- 1 vSAN データストアに移動します。
- 2 [ファイル] タブをクリックします。

オプション	説明
ファイルのアップロード	<ol style="list-style-type: none"> a 保存先フォルダを選択し、[ファイルのアップロード] をクリックします。アップロードできる vmdk ファイルは VMware ストリーム最適化形式のみであるというメッセージが表示されます。異なる形式の vmdk ファイルをアップロードしようとすると、内部サーバ エラー メッセージが表示されます。 b [アップロード] をクリックします。 c ローカル コンピュータ上でアップロードするアイテムを検索し、[開く] をクリックします。
フォルダのアップロード	<ol style="list-style-type: none"> a 保存先フォルダを選択し、[フォルダのアップロード] をクリックします。アップロードできる vmdk ファイルは VMware ストリーム最適化形式のみであるというメッセージが表示されます。 b [アップロード] をクリックします。 c ローカル コンピュータ上でアップロードするアイテムを検索し、[開く] をクリックします。

vSAN データストアからのファイルまたはフォルダのダウンロード

ファイルおよびフォルダを vSAN データストアからダウンロードできます。

データストアの詳細については、『vSphere ストレージ』を参照してください。vmdk ファイルは、ファイル名が <vmdkName>_stream.vmdk のストリーム最適化ファイルとしてダウンロードされます。VMware ストリーム最適化ファイル形式は、ストリーミング用に圧縮されたモノリシックなスパス形式です。

VMware ストリーム最適化 vmdk ファイルは、vmware-vdiskmanager コマンドライン ユーティリティを使用して他の vmdk ファイル形式に変換できます。詳細については、『Virtual Disk Manager User's Guide』を参照してください。

手順

- 1 vSAN データストアに移動します。
- 2 [ファイル] タブをクリックし、[ダウンロード] をクリックします。

ファイル名の拡張子が .stream.vmdk である VMware ストリーム最適化形式の vmdk ファイルが vSAN データストアからダウンロードされることを警告するメッセージが表示されます。

- 3 [ダウンロード] をクリックします。
- 4 ダウンロードするアイテムを見つけて、[ダウンロード] をクリックします。

vSAN ポリシーの使用

7

vSAN を使用する場合、パフォーマンスや可用性などの仮想マシンのストレージ要件をポリシーで定義できます。

vSAN を使用すると、vSAN データストアにデプロイされる各仮想マシンに、少なくとも1つのストレージ ポリシーが割り当てられるようになります。ストレージ ポリシー要件を割り当てると、仮想マシンの作成時にその要件が vSAN レイヤーにプッシュされます。仮想デバイスは vSAN データストア全体に分散されて、パフォーマンスと可用性の要件が満たされます。

vSAN はストレージ プロバイダを使用して基盤となるストレージに関する情報を vCenter Server に提供します。この情報により、仮想マシンの配置について適切に決定し、ストレージ環境を監視することができます。

次のトピックを参照してください。

- [vSAN ポリシーについて](#)
- [vSAN によるポリシー変更の管理方法](#)
- [vSAN ストレージ プロバイダの表示](#)
- [vSAN のデフォルト ストレージ ポリシーについて](#)
- [vSAN データストアのデフォルト ストレージ ポリシーの変更](#)
- [vSphere Client を使用した vSAN のストレージ ポリシーの定義](#)

vSAN ポリシーについて

vSAN ストレージ ポリシーによって、仮想マシンのストレージ要件が定義されます。

これらのポリシーによって、必要なサービスのレベルを確保するためにデータストア内で仮想マシンストレージ オブジェクトをプロビジョニングして割り当てる方法が決定されます。ホスト クラスタで vSAN を有効にすると、1つの vSAN データストアが作成され、デフォルト ストレージ ポリシーがそのデータストアに割り当てられます。

仮想マシンのストレージ要件が分かっている場合は、データストアで提供される機能を参照するストレージ ポリシーを作成できます。複数のポリシーを作成して、タイプまたはクラスが異なる要件を取得できます。

vSAN データストアにデプロイされる各仮想マシンに、少なくとも1つの仮想マシン ストレージ ポリシーが割り当てられます。ストレージ ポリシーは、仮想マシンを作成または編集するときに割り当てることができます。

注： 仮想マシンにストレージ ポリシーを割り当てない場合は、vSAN によってデフォルト ポリシーが割り当てられます。デフォルト ポリシーでは [許容される障害の数] が1に設定されており、各オブジェクトに単一のディスク ストライプが設定され、シン プロビジョニングされた仮想ディスクが使用されます。

仮想マシン スワップ オブジェクトと仮想マシン スナップショット メモリ オブジェクトは、仮想マシンに割り当てられたストレージ ポリシーに従います。このポリシーでは、[許容される障害の数] が 1 に設定されています。これらの可用性は、[許容される障害の数] に異なる値を使用するポリシーが割り当てられた他のオブジェクトとは一致しない場合があります。

注： vSAN Express Storage Architecture が有効な場合、すべてのスナップショットは新しいオブジェクトではありません。ベース VMDK とそのスナップショットは、1 つの vSAN オブジェクトに含まれています。また、vSAN ESA では、ダイジェストは vSAN オブジェクトによってバッキングされます。これは、vSAN Original Storage Architecture とは異なります。

表 7-1. ストレージ ポリシー - 可用性

機能	説明
許容される障害の数 (FTT)	<p>仮想マシン オブジェクトで許容できるホストおよびデバイスの障害の数を定義します。n 個の障害が許容される場合、書き込まれる各データは n+1 個の場所に保存されます (RAID -5 または RAID -6 を使用している場合はパリティ コピーを含む)。</p> <p>フォルト ドメインを構成する場合、容量を提供するホストを含む 2n+1 個のフォルト ドメインが必要です。フォルト ドメインに属していないホストは、それ自体のシングル ホスト フォルト ドメインとみなされます。</p> <p>パフォーマンスまたは容量を最適化するデータ レプリケーションの方法を選択できます。RAID-1 (ミラーリング) の場合、オブジェクトのコンポーネントを配置するために使用するディスク容量は増えますが、オブジェクトにアクセスするパフォーマンスは向上します。RAID-5/6 (イレージャ コーディング) の場合、使用するディスク容量は減りますが、パフォーマンスは低下します。次のいずれかのオプションを選択できます。</p> <ul style="list-style-type: none"> ■ [データの冗長性なし]: vSAN で仮想マシン オブジェクトの単一のミラー コピーを保護しない場合は、このオプションを指定します。その場合、データが保護されなくなり、vSAN クラスタでデバイス障害が発生した場合にデータが損失する可能性があります。ホストをメンテナンス モードに切り替えるときに異常な遅延が発生する可能性があります。この遅延は、vSAN がメンテナンス操作を正常に完了できるように、オブジェクトをホストから回避させる必要があるため発生します。 ■ [ホスト アフィニティを使用したデータの冗長性なし]: このオプションは、vSAN データ パーシステンス プラットフォーム上で vSAN Shared Nothing Architecture (SNA) ワークロードを実行する場合にのみ指定します。 ■ [1 件の障害 - RAID-1 (ミラーリング)]: このオプションは、仮想マシン オブジェクトが 1 台のホストまたはデバイスの障害を許容できる場合に指定します。FTT が 1 の RAID-1 (ミラーリング) を使用して 100 GB の仮想マシン オブジェクトを保護する場合、200 GB を使用します。 ■ [1 件の障害 - RAID-5 (イレージャ コーディング)]: このオプションは、仮想マシン オブジェクトが 1 台のホストまたはデバイスの障害を許容できる場合に指定します。vSAN OSA の場合、FTT が 1 の RAID-5 (イレージャ コーディング) を使用して 100 GB の仮想マシン オブジェクトを保護するには、133.33 GB を使用します。 <p>注: vSAN Express Storage Architecture を使用している場合、vSAN は、クラスタ サイズに基づいて最適化された RAID-5 形式を作成します。クラスタ内のホスト数が 6 台未満の場合、vSAN は RAID-5 (2+1) 形式を作成します。ホスト数が 6 台を超えている場合、vSAN は RAID-6 (4+1) 形式を作成します。クラスタ サイズが最終的に拡大または縮小すると、vSAN は、構成の変更から 24 時間後に自動的に形式を再調整します。</p> <ul style="list-style-type: none"> ■ [2 件の障害 - RAID-1 (ミラーリング)]: このオプションは、仮想マシン オブジェクトが最大 2 台のデバイスの障害を許容できる場合に指定します。RAID-1 (ミラーリング) を使用して FTT を 2 にする必要があるため、キャパシティ オーバーヘッドが発生します。FTT が 2 の RAID-1 (ミラーリング) を使用して 100 GB の仮想マシン オブジェクトを保護する場合、300 GB を使用します。 ■ [2 件の障害 - RAID-6 (イレージャ コーディング)]: このオプションは、仮想マシン オブジェクトが最大 2 台のデバイスの障害を許容できる場合に指定します。FTT が 2 の RAID-6 (イレージャ コーディング) を使用して 100 GB の仮想マシン オブジェクトを保護するには、150 GB を使用します。詳細については、「vSAN クラスタでの RAID 5 または RAID 6 イレージャ コーディングの使用」を参照してください。

表 7-1. ストレージ ポリシー - 可用性 (続き)

機能	説明
	<ul style="list-style-type: none"> ■ [3 件の障害 - RAID-1 (ミラーリング)] : このオプションは、仮想マシン オブジェクトが最大 3 台のデバイスの障害を許容できる場合に指定します。FTT が 3 の RAID-1 (ミラーリング) を使用して 100 GB の仮想マシン オブジェクトを保護する場合、400 GB を使用します。 <p>注： ストレージ ポリシーを作成するときに [FTT] の値を指定しないと、vSAN によって仮想マシン オブジェクトの 1 個のミラー コピーが作成され、許容できる障害は 1 つです。ただし、複数のコンポーネント障害が発生した場合、データにリスクが及ぶおそれがあります。</p>
サイトの耐障害性	<p>このルールは、標準、ストレッチ、または 2 ノード クラスタを使用するかどうかを定義します。vSAN ストレッチ クラスタを使用する場合は、データを両方のサイトでミラーリングするか、1 つのサイトでのみミラーリングするかを定義できます。vSAN ストレッチ クラスタの場合は、ホスト アフィニティの優先サイトまたはセカンダリ サイトのデータを保持するように選択できます。</p> <ul style="list-style-type: none"> ■ [なし - 標準クラスタ] がデフォルト値です。これは、サイトに耐障害性がないことを意味します。 ■ [ホスト ミラーリング - 2 ノード クラスタ] は、FTT で定義された障害数に達した後にオブジェクトが許容できる追加の障害数を定義します。vSAN は、ディスク グループレベルでオブジェクト ミラーリングを実行します。このルールを使用するには、データ ホストごとにストレージ プールに少なくとも 3 つのディスク グループまたは 3 つのディスクが必要です。 ■ [サイト ミラーリング - ストレッチ クラスタ] は、FTT で定義された障害数に達した後にオブジェクトが許容できる追加のホスト障害数を定義します。 ■ [なし - 優先サイトにデータを保持 (ストレッチ クラスタ)]。vSAN ストレッチ クラスタ内のオブジェクトにサイト障害許容度を設定せず、「優先」として構成されているサイトでのみオブジェクトにアクセスできるようにする場合は、このオプションを使用します。 ■ [なし - セカンダリでデータを保持 (ストレッチ クラスタ)]。vSAN ストレッチ クラスタ内のオブジェクトにサイト障害許容度を設定せず、セカンダリ サイトでのみオブジェクトにアクセスできるようにする場合は、このオプションを使用します。これらのオブジェクトは、スイッチ間リンク (ISL) または監視ホストの障害による影響を受けません。ポリシーで選択されたサイトにアクセスできる場合は、引き続きアクセスできます。 ■ [なし - ストレッチ クラスタ]。このオプションを選択すると、サイトの 1 つで障害が発生した場合に vSAN はオブジェクトへのアクセスを保証しません。このようなオブジェクトは ISL バンド幅を大量に消費し、サイト ミラーリング ポリシーを使用するオブジェクトの遅延が増大する可能性があります。このポリシーは、クラスタに容量制約 (CPU/メモリ/ストレージ) がある一時的な状況で、他のポリシーを使用できない場合にのみ使用します。

表 7-2. ストレージ ポリシー - ストレージ ルール

機能	説明
暗号化サービス	<p>データストアに展開する仮想マシンの暗号化オプションを定義します。以下のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> ■ [保存データの暗号化]: データストアに保存されているデータに暗号化を適用する場合は、このオプションを指定します。 ■ [暗号化なし]: このオプションは、データに暗号化を適用しない場合に指定します。 ■ [基本設定なし]: 暗号化ルールを明示的に適用しない場合は、このオプションを指定します。このオプションを選択すると、vSAN は両方のルールを仮想マシンに適用します。
容量効率	<p>データストアに展開する仮想マシンの容量効率を定義します。以下のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> ■ [デデュープと圧縮]: データに対してデデュープと圧縮の両方を適用する場合は、このオプションを指定します。 ■ [圧縮のみ]: データに圧縮のみを適用する場合は、このオプションを指定します。 <p>注: vSAN Original Storage Architecture の場合、圧縮はクラスタ レベルの設定です。vSAN Express Storage Architecture の場合、「圧縮のみ」はオブジェクト レベルで実行されます。つまり、1 台の仮想マシンに圧縮を使用できますが、同じクラスタ内の別の仮想マシンには使用できません。</p> <ul style="list-style-type: none"> ■ [容量効率なし]: このオプションは、オブジェクトに圧縮を適用しない場合に指定します。 ■ [基本設定なし]: 容量効率ルールを明示的に適用しない場合は、このオプションを指定します。このオプションを選択すると、vSAN はすべての容量効率ルールを仮想マシンに適用します。
ストレージ階層	<p>ストレージ ポリシーが定義されているすべての仮想マシンにストレージ階層を指定します。以下のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> ■ [オール フラッシュ]: オール フラッシュ環境の仮想マシンと互換性を持たせる場合は、このオプションを指定します。 ■ [ハイブリッド]: ハイブリッド環境の仮想マシンのみと互換性を持たせる場合は、このオプションを指定します。 ■ [基本設定なし]: ストレージ階層ルールを明示的に適用しない場合は、このオプションを指定します。このオプションを選択すると、vSAN は、仮想マシンがハイブリッド環境とオール フラッシュ環境の両方と互換性を持つように設定します。

表 7-3. ストレージ ポリシー - 詳細ポリシー ルール

機能	説明
オブジェクトあたりのディスク ストライプの数	<p>仮想マシン オブジェクトの各レプリカがストライピングされるキャパシティ デバイスの最小数。値が 1 より大きい場合、パフォーマンスが向上することがありますが、システム リソースの使用量も増加します。</p> <p>デフォルト値は 1 です。最大値は 12 です。</p> <p>デフォルトのストライピング値は変更できません。</p> <p>ハイブリッド環境では、ディスク ストライプが磁気ディスクにまたがって分散されます。オールフラッシュ構成の場合は、キャパシティ レイヤーを構成するフラッシュ デバイ스에またがってストライピングされます。要求に対応できる十分なキャパシティ デバイスが vSAN 環境に配置されていることを確認してください。</p>
オブジェクトの IOPS 制限	<p>VMDK などのオブジェクトの IOPS 制限を定義します。IOPS は重み付けされたサイズを使用して I/O 操作の数として計算されます。システムがデフォルトの基本サイズである 32 KB を使用する場合、64-KB I/O は 2 個の I/O 操作を意味します。</p> <p>IOPS の計算では読み取りと書き込みは同等であるとみなされ、キャッシュ ヒット率およびシーケンスは考慮されません。ディスクの IOPS が制限値を超えると I/O 操作が調整されます。[オブジェクトの IOPS 制限] を 0 に設定した場合、IOPS 制限は適用されません。</p> <p>vSAN では、最初の 2 回の操作中または無効期間の後に、オブジェクトが IOPS 制限の比率を 2 倍にできます。</p>
オブジェクト スペースの予約	<p>仮想マシンのデプロイ時に予約する必要がある仮想マシン ディスク (vmdk) オブジェクトの論理サイズの割合 (シック プロビジョニング)。以下のオプションを使用できます。</p> <ul style="list-style-type: none"> ■ シック プロビジョニング (デフォルト) ■ 25% の予約 ■ 50% の予約 ■ 75% の予約 ■ シック プロビジョニング

表 7-3. ストレージ ポリシー - 詳細ポリシー ルール (続き)

機能	説明
Flash Read Cache の予約 (%)	<p>仮想マシン オブジェクトの読み取りキャッシュとして予約されているフラッシュ容量。仮想マシン ディスク (vmdk) オブジェクトの論理サイズのパーセントとして指定されます。予約済みのフラッシュ容量を他のオブジェクトが使用することはできません。予約されていないフラッシュはすべてのオブジェクトで適切に共有されます。特定のパフォーマンス問題に対処する場合にのみ、このオプションを使用します。</p> <p>キャッシュを取得するために予約を設定する必要はありません。キャッシュの予約設定は常にオブジェクトに含まれるため、読み取りキャッシュの予約を設定すると、仮想マシン オブジェクトの移動時に問題が生じることがあります。</p> <p>Flash Read Cache の予約のストレージ ポリシー属性は、ハイブリッド ストレージ構成でのみサポートされます。オールフラッシュ クラスタまたは vSAN ESA クラスタの仮想マシン ストレージ ポリシーを定義する場合は、この属性を使用しないでください。</p> <p>デフォルト値は 0% です。最大値は 100% です。</p> <p>注： デフォルトでは、vSAN により需要に基づいてストレージ オブジェクトに読み取りキャッシュが動的に割り当てられます。この機能により、リソースを最もフレキシブルかつ最適に使用できます。したがって、通常はこのパラメータのデフォルト値である 0 を変更する必要はありません。</p> <p>パフォーマンスの問題を解決するときに値を増やす場合は、十分に注意してください。複数の仮想マシンにわたってキャッシュ予約を過剰にプロビジョニングすると、過剰予約によってフラッシュ デバイスの容量が無駄に使用される場合があります。このようなキャッシュ予約は、特定の時間に必要な容量を使用するワークロードを処理するためには利用できません。このように容量を無駄にしてサービスが提供できなくなると、パフォーマンスが低下するおそれがあります。</p>
オブジェクト チェックサム	<p>このオプションを [いいえ] に設定すると、オブジェクトはチェックサム情報を計算してそのデータの整合性を保ちます。このオプションを [はい] に設定すると、オブジェクトはチェックサム情報を計算しません。</p> <p>vSAN はエンドツーエンド チェックサムを使用して、ファイルの各コピーがソース ファイルとまったく同じであることを確認してデータの整合性を保ちます。システムは読み取り/書き込み操作中にデータの妥当性を確認し、エラーが検出されると、vSAN はデータを修復するかエラーを報告します。</p> <p>チェックサムの不一致が検出された場合、vSAN は正しくないデータを正しいデータで上書きすることによって自動的にデータを修復します。チェックサム計算とエラー修正はバックグラウンド操作として実行されます。</p> <p>クラスタ内のすべてのオブジェクトのデフォルト設定は [いいえ] で、チェックサムは有効です。</p> <p>注： vSAN Express Storage Architecture の場合、オブジェクトのチェックサムは常に有効で、無効にすることはできません。</p>
強制プロビジョニング	<p>このオプションを [はい] に設定すると、データストアがストレージ ポリシーで指定された [許容される障害の数]、[オブジェクトあたりのディスク ストライプの数]、[Flash Read Cache の予約] ポリシーを満たせない場合でも、オブジェクトはプロビジョニングされます。このパラメータは、シナリオをブートストラッピングする場合、および標準のプロビジョニングが行えなくなった停止時に使用します。</p> <p>ほとんどの本番環境では、デフォルトの [いいえ] を許容できます。vSAN では、ポリシー要件が満たされないと仮想マシンのプロビジョニングに失敗しますが、ユーザー定義のストレージ ポリシーは正常に作成されます。</p>

仮想マシン ストレージ ポリシーを操作する場合、ストレージ機能が vSAN クラスタのストレージ容量の使用にどのように影響するかを把握しておく必要があります。ストレージ ポリシーの設計およびサイジングに関する考慮事項の詳細については、『vSAN のプランニングとデプロイ』の「vSAN クラスタの設計とサイジング」を参照してください。

vSAN によるポリシー変更の管理方法

vSAN 6.7 Update 3 以降では、ポリシー変更を管理することにより、クラスタ全体で消費される一時的な容量の大きさを削減しています。

一時的な容量は、vSAN がポリシー変更のためにオブジェクトを再構成するときに生成されます。

ポリシーを変更すると、変更は受け入れられますが、ただちに適用されるわけではありません。vSAN は、一時的な容量を一定に維持するために、ポリシー変更要求をバッチ処理して非同期的に実行します。

5 台のホストのクラスタ上で RAID-5 ポリシーを RAID-6 に変更するなど、容量に関連しない理由の場合、ポリシー変更はただちに拒否されます。

vSAN キャパシティ モニターで、一時的な容量の使用状況を確認できます。オブジェクトのポリシー変更のステータスを確認するには、vSAN Health Service を使用して vSAN オブジェクトの健全性を確認します。

vSAN ストレージ プロバイダの表示

vSAN を有効にすると、vSAN クラスタ内の各ホストでストレージ プロバイダが自動的に構成および登録されます。

vSAN ストレージ プロバイダは組み込みのソフトウェア コンポーネントで、データストア機能を vCenter Server に報告します。ストレージ機能は一般にキーと値のペアで表されます。ここで、キーとはデータストアによって提供される特定のプロパティです。値とは、仮想マシン ホーム ネームスペース オブジェクトや仮想ディスクなど、データストアがプロビジョニングされたオブジェクトについて提供できる数値または範囲です。また、タグを使用してユーザー定義のストレージ機能を作成し、仮想マシンのストレージ ポリシーを定義するときはそのタグを参照できます。データストアでタグを適用および使用方法の詳細については、『vSphere のストレージ』ドキュメントを参照してください。

vSAN ストレージ プロバイダは、一連の基盤となるストレージ機能を vCenter Server に報告します。また、vSAN レイヤーともやり取りして、仮想マシンのストレージ要件が報告されます。ストレージ プロバイダの詳細については、『vSphere のストレージ』ドキュメントを参照してください。

vSAN 6.7 以降のリリースでは、次の URL を使用して、vCenter Server で管理されているすべての vSAN クラスタに対して 1 つの vSAN ストレージ プロバイダを登録します。

```
https://<VC fqdn>:<VC https port>/vsan/vasa/version.xml
```

ストレージ プロバイダが登録されていることを確認します。

手順

- 1 vCenter Server に移動します。
- 2 [構成] タブをクリックし、[ストレージ プロバイダ] をクリックします。

結果

vSAN のストレージ プロバイダがリストに表示されます。

注： vSAN によって使用されるストレージ プロバイダを手動で登録解除することはできません。vSAN ストレージ プロバイダを削除または登録解除するには、vSAN クラスタから対応するホストを削除した後、そのホストを再び追加します。少なくとも1つのストレージ プロバイダがアクティブであることを確認します。

vSAN のデフォルト ストレージ ポリシーについて

vSAN では、vSAN データストアにデプロイされる仮想マシンに、少なくとも1つのストレージ ポリシーが割り当てられている必要があります。

仮想マシンをプロビジョニングするときに、ストレージ ポリシーを明示的に割り当てないと、vSAN は、デフォルト ストレージ ポリシーを仮想マシンに割り当てます。各デフォルト ポリシーには、vSAN ルール セットと一連の基本的なストレージ機能が含まれ、通常、vSAN データストアにデプロイされた仮想マシンの配置に使用されます。

表 7-4. vSAN のデフォルト ストレージ ポリシーの仕様

仕様	設定
許容される障害の数	1
オブジェクトあたりのディスク ストライプの数	1
vSphere Flash Read Cache の予約、つまり読み取りキャッシュに使用されるフラッシュ容量	0
オブジェクト スペースの予約	0
	注： オブジェクト スペースの予約をゼロに設定することは、仮想ディスクがデフォルトでシン プロビジョニングされることを意味します。
強制プロビジョニング	なし

vSAN Express Storage Architecture クラスタを使用する場合は、クラスタのサイズに応じて、ここにリストされている ESA ポリシーのいずれかを使用できます。

表 7-5. vSAN ESA のデフォルト ストレージ ポリシー仕様 - RAID-5

仕様	設定
許容される障害の数	1
オブジェクトあたりのディスク ストライプの数	1
vSphere Flash Read Cache の予約、つまり読み取りキャッシュに使用されるフラッシュ容量	0

表 7-5. vSAN ESA のデフォルト ストレージ ポリシー仕様 - RAID-5 (続き)

仕様	設定
オブジェクト スペースの予約	シン プロビジョニング
強制プロビジョニング	なし

注： vSAN ESA の RAID-5 は、3 つのホスト クラスタをサポートします。自動ポリシー管理を有効にして RAID-5 を使用するには、クラスタに 4 台のホストが必要です。

表 7-6. vSAN ESA のデフォルト ストレージ ポリシー仕様 - RAID-6

仕様	設定
許容される障害の数	2
オブジェクトあたりのディスク ストライプの数	1
vSphere Flash Read Cache の予約、つまり読み取りキャッシュに使用されるフラッシュ容量	0
オブジェクト スペースの予約	シン プロビジョニング
強制プロビジョニング	なし

注： RAID-6 を使用するには、クラスタ内に少なくとも 6 台のホストが必要です。

デフォルトの仮想マシン ストレージ ポリシーの設定の確認は、[仮想マシン ストレージ ポリシー] > デフォルト ストレージ ポリシーの名前 > [ルール セット 1: vSAN] の順に移動して行うことができます。

最適の結果を得るため、ポリシーの要件がデフォルト ストレージ ポリシーで定義されたものと同じであっても、独自の仮想マシン ストレージ ポリシーを作成し、使用することを検討してください。場合によっては、クラスタをスケール アップするときに、「[VMware Cloud on AWS のサービス レベル契約](#)」の要件に準拠するようにデフォルトのストレージ ポリシーを変更する必要があります。

ユーザー定義のストレージ ポリシーをデータストアに割り当てた場合、vSAN は指定されたデータストアにユーザー定義ポリシーの設定を適用します。vSAN データストアのデフォルト ポリシーにできるストレージ ポリシーは 1 つだけです。

vSAN のデフォルト ストレージ ポリシーの特性

vSAN データストアのデフォルト ストレージ ポリシーに適用される特性は次のとおりです。

- 仮想マシンをプロビジョニングするときに他の vSAN ポリシーを割り当てなかった場合は、vSAN データストアのデフォルト ストレージ ポリシーがすべての仮想マシン オブジェクトに割り当てられます。[ストレージの選択] 画面の [仮想マシン ストレージ ポリシー] テキスト ボックスは、[データストアのデフォルト] に設定されます。ストレージ ポリシーの使用の詳細については、『vSphere のストレージ』ドキュメントを参照してください。

注： 仮想マシン スワップおよび仮想マシン メモリのオブジェクトでは、[強制プロビジョニング] が [はい] に設定された状態で、vSAN のデフォルト ストレージ ポリシーが適用されます。

- vSAN のデフォルト ポリシーは、vSAN データストアのみに適用されます。NFS や VMFS データストアなど、非 vSAN データストアにデフォルト ストレージ ポリシーを適用することはできません。
- RAID 0 または RAID 1 構成の vSAN Express Storage Architecture クラスタのオブジェクトには、3 つのディスク ストライプがありますが、デフォルトのポリシーでは 1 つのディスク ストライプのみが定義されています。
- vSAN デフォルト ストレージ ポリシーは vCenter Server のどの vSAN データストアとも互換性があるため、デフォルト ポリシーを使用してプロビジョニングされた仮想マシン オブジェクトを vCenter Server の任意の vSAN データストアに移動できます。
- デフォルト ポリシーのクローンを作成して、ユーザー定義のストレージ ポリシーを作成するためのテンプレートとして使用できます。
- StorageProfile.View 権限がある場合は、デフォルト ポリシーを編集できます。少なくとも 1 台のホストが含まれる vSAN 対応クラスタが少なくとも 1 つ必要です。通常は、デフォルト ストレージ ポリシーの設定を編集しないでください。
- デフォルト ポリシーの名前や説明、または vSAN ストレージ プロバイダの仕様は編集できません。ポリシー ルールを含む他のすべてのパラメータは編集できます。
- デフォルト ストレージ ポリシーは削除できません。
- 仮想マシンをプロビジョニングするときに割り当てたポリシーに vSAN 固有のルールが含まれていない場合は、デフォルト ストレージ ポリシーが割り当てられます。

自動ポリシー管理

vSAN Express Storage Architecture のクラスタは自動ポリシー管理を使用して、クラスタ タイプ（標準またはストレッチ）とホスト数に基づいて最適なデフォルト ストレージ ポリシーを生成できます。vSAN は [サイトの耐障害性] と [許容される障害の数] をクラスタに最適な構成にします。

自動生成されたポリシーの名前は、「ClusterName - 最適なデフォルト データストア ポリシー」のようにクラスタ名に基づいています。

自動ポリシーを有効にすると、vSAN は新しい最適なポリシーを vSAN データストアに割り当て、そのポリシーがクラスタのデータストアのデフォルト ポリシーになります。

自動ポリシー管理を有効にするには、[vSAN] > [サービス] > [ストレージ] > [編集] のスライド コントロールを使用します。

vSAN データストアのデフォルト ストレージ ポリシーの変更

選択した vSAN データストアのデフォルトのストレージ ポリシーは、変更することができます。

前提条件

デフォルト ポリシーとして vSAN データストアに割り当てる仮想マシン ストレージ ポリシーが、vSAN クラスタ内の仮想マシンの要件を満たしていることを確認します。

手順

- 1 vSAN データストアに移動します。
- 2 [構成] をクリックします。
- 3 [全般] で、デフォルト ストレージ ポリシーの [編集] ボタンをクリックして、デフォルト ポリシーとして vSAN データストアに割り当てるストレージ ポリシーを選択します。

注： 強化された仮想ディスクのホーム ストレージ ポリシーを編集することもできます。[編集] をクリックし、ホーム オブジェクトのストレージ ポリシーとして割り当てるホーム ストレージ ポリシーを選択します。

vSAN のデフォルト ストレージ ポリシーや、vSAN のルール セットが定義されたユーザー定義のストレージ ポリシーなど、vSAN のデータストアと互換性のあるストレージ ポリシーのリストが表示されます。

- 4 ポリシーを選択し、[OK] をクリックします。

データストアのストレージ ポリシーを明示的に指定しないで新しい仮想マシンをプロビジョニングすると、このストレージ ポリシーがデフォルト ポリシーとして適用されます。

次のステップ

仮想マシンの新しいストレージ ポリシーを定義できます。「[vSphere Client を使用した vSAN のストレージ ポリシーの定義](#)」を参照してください。

vSphere Client を使用した vSAN のストレージ ポリシーの定義

ストレージ ポリシーを作成して、仮想マシンとその仮想ディスクのストレージ要件を定義できます。

このポリシーでは、vSAN データストアでサポートされるストレージ機能を参照します。

前提条件

- vSAN ストレージ プロバイダを使用できることを確認します。「[vSAN ストレージ プロバイダの表示](#)」を参照してください。

- 必要な権限: [プロファイル駆動型ストレージ。プロファイル駆動型ストレージ ビュー] と [プロファイル駆動型ストレージ。プロファイル駆動型ストレージ更新]

注: vSAN Express Storage Architecture のクラスタでは、自動ポリシー管理を使用できます。詳細については、[「vSAN のデフォルト ストレージ ポリシーについて」](#) を参照してください。

手順

- 1 [ポリシーおよびプロファイル] に移動して、[仮想マシン ストレージ ポリシー] をクリックします。
- 2 [作成] をクリックします。
- 3 [名前および説明] ページで vCenter Server を選択します。
- 4 ストレージ ポリシーの名前と説明を入力し、[次へ] をクリックします。
- 5 [ポリシー構造] 画面で、「vSAN」ストレージのルールの [有効] を選択し、[次へ] をクリックします。

6 [vSAN] 画面で、ポリシー ルールセットを定義し、[次へ] をクリックします。

a [可用性] タブで、[サイトの耐障害性] と [許容される障害の数] を定義します。

[可用性] オプションでは、許容される障害数のルール、データのローカリティおよび障害の許容方法を定義します。

- [サイトの耐障害性] では、仮想マシン オブジェクトに対して使用するサイト障害の許容方法を定義します。
- [許容される障害の数] では、仮想マシン オブジェクトで許容できるホスト障害およびデバイス障害の数、およびデータ レプリケーション方式を定義します。

たとえば、[デュアル サイト ミラーリング] および [2 回の障害 - RAID-6 (イレージャ コーディング)] を選択すると、vSAN は次のポリシー ルールを設定します。

- 許容される障害の数 : 1
- 許容されるセカンダリ レベルの障害数 : 2
- データのローカリティ : なし
- 障害の許容方法 : RAID-5/6 (イレージャ コーディング) - キャパシティ

b [ストレージルール] タブで、リモート データストアを区別するために HCI メッシュとともに使用できる暗号化、容量効率、ストレージ階層ルールを定義します。

- [暗号化サービス] : このポリシーを使用して展開する仮想マシンの暗号化ルールを定義します。次のいずれかのオプションを選択できます。

- [保存データの暗号化] : 仮想マシンで暗号化を有効にします。
- [暗号化なし] : 仮想マシンで暗号化を有効にしません。
- [環境設定なし] : 保存データの暗号化と暗号化なしの両方のオプションと互換性のある仮想マシンにします。

- [容量効率] : このポリシーを使用して展開する仮想マシンの容量効率ルールを定義します。次のいずれかのオプションを選択できます。

- [デデュープおよび圧縮] : 仮想マシンでデデュープおよび圧縮の両方を有効にします。デデュープおよび圧縮は、オールフラッシュ ディスク グループでのみ使用できます。詳細については、[\[vSAN クラスターのデデュープおよび圧縮の設計に関する考慮事項\]](#) を参照してください。
- [圧縮のみ] : 仮想マシンで圧縮のみを有効にします。圧縮は、オール フラッシュ ディスク グループでのみ使用できます。詳細については、[\[vSAN クラスターのデデュープおよび圧縮の設計に関する考慮事項\]](#) を参照してください。
- [容量効率なし] : 仮想マシンで容量効率機能を有効にしません。このオプションを選択するには、容量効率オプションが指定されていないデータストアを有効にする必要があります。
- [環境設定なし] : すべてのオプションと互換性のある仮想マシンにします。

- [ストレージ階層] : このポリシーを使用して展開する仮想マシンにストレージ階層を指定します。次のいずれかのオプションを選択できます。[環境設定なし] を選択すると、ハイブリッド環境とオール フラッシュ環境の両方と互換性のある仮想マシンにします。

- [オール フラッシュ]
 - [ハイブリッド]
 - [環境設定なし]
- c [詳細なポリシー ルール] タブで、オブジェクトあたりのディスク ストライプの数や IOPS の制限などの詳細なポリシー ルールを定義します。
- d [タグ] タブで、[タグ ルールの追加] をクリックし、タグ ルールのオプションを定義します。
- 指定する値が、vSAN データストアのストレージ機能によってアダプタイズされる値の範囲内であることを確認します。
- 7 [ストレージの互換性] ページで、[互換性あり] タブと [互換性なし] タブに表示されているデータストアのリストを確認し、[次へ] をクリックします。
- データストアが適格とみなされるために、ポリシー内のすべてのルール セットを満たす必要はありません。データストアは、少なくとも1つのルール セットと、そのセット内のすべてのルールを満たす必要があります。vSAN データストアが、ストレージ ポリシーに設定されている要件を持たし、互換性のあるデータストアのリストに表示されていることを確認します。
- 8 [確認して完了] 画面でポリシーの設定を確認し、[完了] をクリックします。

結果

新しいポリシーがリストに追加されます。

次のステップ

このポリシーを仮想マシンとその仮想ディスクに割り当てます。vSAN では、ポリシーで指定された要件に沿って仮想マシン オブジェクトを配置します。仮想マシン オブジェクトへのストレージ ポリシーの適用の詳細については、『vSphere のストレージ』ドキュメントを参照してください。

vSAN クラスタの拡張および管理

8

vSAN クラスタの設定後、ホストとキャパシティ デバイスの追加、ホストとデバイスの削除、障害のシナリオの管理を行うことができます。

次のトピックを参照してください。

- vSAN クラスタの拡張
- リモート vSAN データストアの共有
- メンテナンス モードでの vSAN クラスタのメンバーの操作
- vSAN クラスタのフォルト ドメインの管理
- vSAN Data Protection の使用
- vSAN iSCSI ターゲット サービスの使用
- vSAN ファイル サービス
- ハイブリッド vSAN クラスタをオールフラッシュ クラスタに移行
- vSAN クラスタのシャットダウンと再起動

vSAN クラスタの拡張

既存の vSAN クラスタは、進行中の操作を中断せずに、ホストまたはデバイスを既存のホストに追加することによって拡張できます。

次のいずれかの方法を使用して、vSAN クラスタを拡張します。

- サポートされているキャッシュ デバイスとキャパシティ デバイスを使用して構成されているクラスタに、新しい ESXi ホストを追加します。vSAN クラスタへのホストの追加を参照してください。
- ホスト プロファイルを使用して、既存の ESXi ホストを vSAN クラスタに移動し、構成します。ホスト プロファイルを使用した vSAN クラスタ内のホストの構成を参照してください。
- 新しいキャパシティ デバイスを、クラスタ メンバーである ESXi ホストに追加します。vSAN クラスタのディスク グループへのデバイスの追加を参照してください。

vSAN クラスタの容量およびパフォーマンスの強化

vSAN クラスタでストレージ容量が不足するか、パフォーマンスの低下が見られる場合は、クラスタを拡張して、容量およびパフォーマンスを強化できます。

- (vSAN Original Storage Architecture の場合のみ) 既存のディスク グループにストレージ デバイスを追加するか、ディスク グループを追加して、クラスタのストレージ容量を拡張します。新しいディスク グループには、キャッシュのためのフラッシュ デバイスが必要です。ディスク グループへのデバイスの追加の詳細については、「[vSAN クラスタのディスク グループへのデバイスの追加](#)」を参照してください。キャッシュを増やさずにキャパシティ デバイスを追加すると、キャッシュと容量の比率がサポート対象外のレベルに低下する可能性があります。詳細については、『vSAN のプランニングとデプロイ』を参照してください。

少なくとも 1 個のキャッシュ デバイス (フラッシュ) と 1 個のキャパシティ デバイス (フラッシュまたは磁気ディスク) を既存のストレージ I/O コントローラまたは新しいホストに追加することで、クラスタのパフォーマンスが向上します。または、ディスク グループを持つ 1 台以上のホストを追加できます。これにより、vSAN クラスタで vSAN が自動リバランスを完了すると、同様にパフォーマンスが向上します。

- (vSAN Express Storage Architecture の場合のみ) 既存のホストのストレージ プールにフラッシュ デバイスを追加するか、フラッシュ デバイスを備えた 1 台以上の新しいホストを追加して、クラスタのストレージ容量を拡張します。

コンピューティングのみ行うホストを vSAN クラスタに配置して、クラスタ内の他のホストのストレージ容量を使用することはできますが、均一に構成されたホストを追加すると効率的に運用できます。ディスク グループまたはストレージ プールでは性能が同一または類似したデバイスを使用することが理想的ですが、vSAN ハードウェア互換性リスト (HCL) に記載されているデバイスはすべてサポートされています。ホスト全体でキャパシティが均等に分散されるようにしてください。ディスク グループまたはストレージ プールへのデバイスの追加の詳細については、「[vSAN クラスタのディスク グループまたはストレージ プールの作成](#)」を参照してください。

クラスタのキャパシティを拡張してから自動リバランスを有効にし、リソースをクラスタ全体で均等に配分します。詳細については、『vSAN の監視とトラブルシューティング』を参照してください。

クイックスタートを使用した vSAN クラスタへのホストの追加

クイックスタートを使用して vSAN クラスタを構成した場合は、クイックスタート ワークフローを使用してホストとストレージ デバイスをクラスタに追加できます。

vSAN クラスタに新しいホストを追加するときにも、クラスタの構成ウィザードを使用してホストを構成することができます。クイックスタートの詳細については、『vSAN のプランニングとデプロイ』の「クイックスタートを使用した vSAN クラスタの構成および拡張」を参照してください。

注： ホストで vCenter Server を実行している場合、ホストをクイックスタート ワークフローを使用してクラスタに追加するため、メンテナンス モードに切り替えることはできません。同じホストで Platform Services Controller が実行されている可能性もあります。ホスト上の他のすべての仮想マシンはパワーオフする必要があります。

前提条件

- vSAN クラスタでクイックスタート ワークフローが使用可能になっている。

- クイックスタート ワークフローで行ったネットワーク構成が、クイックスタート ワークフローの外部から変更されていない。
- クイックスタートでクラスタの作成時に構成されたネットワーク設定は変更されていません。

手順

- 1 vSphere Client で、クラスタに移動します。
- 2 [構成] タブをクリックし、[構成] > [クイックスタート] の順に選択します。
- 3 [ホストの追加] で、[起動] をクリックして、ホストの追加ウィザードを開きます。
 - a [ホストの追加] 画面で新しいホストの情報を入力するか、既存のホストをクリックして、インベントリにリストされたホストから選択します。
 - b [ホスト サマリ] 画面でホストの設定を確認します。
 - c [設定内容の確認] 画面で [終了] をクリックします。
- 4 [クラスタの構成] で、[起動] をクリックして、クラスタの構成ウィザードを開きます。
 - a [Distributed Switch の設定] 画面で、新しいホストのネットワーク設定を入力します。
 - b (オプション) [ディスクの要求] 画面で、新しい各ホスト上のディスクを選択します。
 - c (オプション) [フォルト ドメインの作成] 画面で、新しいホストを対応するフォルト ドメインに移動します。
 フォルト ドメインの詳細については、[vSAN クラスタのフォルト ドメインの管理](#)を参照してください。
 - d [設定内容の確認] 画面でクラスタの設定を確認し、[終了] をクリックします。

vSAN クラスタへのホストの追加

進行中の操作を中断せずに、稼働中の vSAN クラスタに ESXi ホストを追加できます。

新しいホストのリソースは、クラスタに関連付けられます。

前提条件

- 『VMware 互換性ガイド』 (<http://www.vmware.com/resources/compatibility/search.php>) にドライバ、ファームウェア、およびストレージ I/O コントローラを含むリソースが記載されていることを確認します。
- クラスタ内のデバイス全体でコンポーネントとオブジェクトが均等に分散されるように、vSAN クラスタ内に統一された構成のホストを作成することをお勧めします。ただし、状況によってはクラスタがアンバランスになる可能性があります。特に、メンテナンス中や、仮想マシンを過度にデプロイして vSAN データストアの容量をオーバーコミットした場合にアンバランスになることがあります。

手順

- 1 vSAN クラスタに移動します。

- 2 クラスタを右クリックし、[ホストの追加] を選択します。ホストの追加ウィザードが表示されます。

オプション	説明
新規ホスト	a ホスト名または IP アドレスを入力します。 b ホストに関連付けられているユーザー名とパスワードを入力します。
既存ホスト	a vCenter Server に追加済みのホストから選択します。

- 3 [次へ] をクリックします。
- 4 概要情報を確認して、[次へ] をクリックします。
- 5 設定内容を確認して、[終了] をクリックします。

ホストがクラスタに追加されます。

次のステップ

vSAN ディスク バランス（ディスクの負荷分散）の健全性チェックが緑色であることを確認します。

vSAN クラスタの構成および問題の解決の詳細については、『vSAN の監視とトラブルシューティング』の「vSAN クラスタ構成の問題」を参照してください。

ホスト プロファイルを使用した vSAN クラスタ内のホストの構成

vSAN クラスタ内に複数のホストがある場合は、既存の vSAN ホストのプロファイルを使用して、vSAN クラスタ内のホストを構成できます。

ホスト プロファイルには、ストレージ構成、ネットワーク構成、およびホストのその他の特性に関する情報が含まれています。8、16、32、または 64 台のホストなど、多数のホストが含まれているクラスタを作成する場合は、ホスト プロファイル機能を使用します。ホスト プロファイルを使用すると、一度に複数のホストを vSAN クラスタに追加できます。

前提条件


- ホストがメンテナンス モードであることを確認します。
- 『VMware 互換性ガイド』 (<http://www.vmware.com/resources/compatibility/search.php>) にハードウェア コンポーネント、ドライバ、ファームウェア、およびストレージ I/O コントローラが記載されていることを確認します。

手順

- 1 ホスト プロファイルを作成します。
- ホスト プロファイル ビューに移動します。
 - [ホストからプロファイルを抽出] アイコン（**+**）をクリックします。
 - 参照ホストとして使用するホストを選択し、[次へ] をクリックします。
- 選択したホストはアクティブなホストである必要があります。


- d 新しいプロファイルの名前と説明を入力して、[次へ] をクリックします。
- e 新しいホスト プロファイルの概要情報を確認し、[終了] をクリックします。
新しいプロファイルがホスト プロファイル リストに表示されます。

2 ホストを目的のホスト プロファイルに添付します。

- a ホスト プロファイル ビューのプロファイル リストから、vSAN ホストに適用するホスト プロファイルを選択します。
- b [ホスト プロファイルに対するホストおよびクラスタの添付/分離] アイコン () をクリックします。
- c 展開したリストからホストを選択して [添付] をクリックしてホストをプロファイルに添付します。
添付されたエンティティのリストにホストが追加されます。
- d [次へ] をクリックします。
- e [終了] をクリックして、ホストのプロファイルへの分離を完了します。

3 参照した vSAN ホストをホスト プロファイルから分離します。

ホスト プロファイルがクラスタに添付されると、そのクラスタ内のホストもホスト プロファイルに添付されます。ただし、ホスト プロファイルがクラスタから分離されても、ホストまたはクラスタ内のホストと、ホスト プロファイルの関連付けはそのまま残ります。

- a ホスト プロファイル ビューにあるプロファイル リストから、ホストまたはクラスタから分離するホスト プロファイルを選択します。
- b [ホスト プロファイルに対するホストおよびクラスタの添付/分離] アイコン () をクリックします。
- c 展開されたリストからホストまたはクラスタを選択し、[分離] をクリックします。
- d [すべて分離] をクリックして、リストされたすべてのホストとクラスタをプロファイルから分離します。
- e [次へ] をクリックします。
- f [終了] をクリックして、ホスト プロファイルからのホストの分離を完了します。

- 4 vSAN ホストの添付されたホスト プロファイルへのコンプライアンスを確認し、ホストとホスト プロファイルで指定された構成パラメータに違いがないかどうかを判断します。
 - a ホスト プロファイルに移動します。

[オブジェクト] タブにはすべてのホスト プロファイル、ホスト プロファイルに添付されたホストの数、前回のコンプライアンス チェックの結果の概要が一覧表示されます。
 - b [ホスト プロファイル コンプライアンスの確認] アイコン (🔍) をクリックします。

コンプライアンス エラーのあるホストとホスト プロファイルとの間で異なるパラメータを詳細に表示するには、[監視] タブをクリックし、[コンプライアンス] ビューを選択します。オブジェクト階層を展開し、非準拠ホストを選択します。異なっているパラメータが階層の下の [コンプライアンス] ウィンドウに表示されます。

コンプライアンス エラーがある場合は、修正アクションを使用してホスト プロファイル設定をホストに適用します。このアクションによって、すべてのホスト プロファイル管理対象パラメータは、ホストに添付されたホスト プロファイルに含まれている値に変更されます。
 - c コンプライアンス エラーのあるホストとホスト プロファイルとの間で異なるパラメータを詳細に表示するには、[監視] タブをクリックし、[コンプライアンス] ビューを選択します。
 - d オブジェクト階層を展開し、エラーのあるホストを選択します。

異なっているパラメータが階層の下の [コンプライアンス] ウィンドウに表示されます。
- 5 ホストを修正して、コンプライアンス エラーを解決します。
 - a [監視] タブを選択し、[コンプライアンス] をクリックします。
 - b 修正するホスト (複数可) を右クリックし、[すべての vCenter アクション] - [ホスト プロファイル] - [修正] を選択します。

ホスト プロファイル ポリシーのユーザー入力パラメータを更新または変更するには、ホストをカスタマイズします。
 - c [次へ] をクリックします。
 - d ホスト プロファイルの修正に必要なタスクを確認し、[終了] をクリックします。

ホストは vSAN クラスタの一部となり、ホストのリソースは vSAN クラスタに接続できるようになります。ホストはすべての vSAN クラスタ内の既存の vSAN ストレージ I/O ポリシーにアクセスすることもできます。

リモート vSAN データストアの共有

リモート データストアの共有を使用すると、vSAN クラスタは他のクラスタとデータストアを共有できます。

リモート データストアのストレージ容量を使用するように、ローカル クラスタで実行される仮想マシンをプロビジョニングできます。新しい仮想マシンをプロビジョニングするときに、クライアント クラスタにマウントされたリモート データストアを選択できます。データストアに構成された互換性のあるストレージ ポリシーを割り当てます。

リモート データストアのマウントはクラスタ全体の構成です。リモート データストアを vSAN クラスタにマウントすると、クラスタ内のすべてのホストで使用できるようになります。

vSAN クラスタを作成する場合、または vSAN 用に vSphere クラスタを構成する場合は、HCI 構成タイプを選択できます。

- [vSAN HCI] はコンピューティング リソースとストレージ リソースを提供します。データセンターと vCenter Server 間でデータストアを共有し、他の vSAN HCI クラスタからデータストアをマウントできません。
- [vSAN コンピューティング クラスタ]は、コンピューティング リソースのみを提供する vSphere クラスタです。vSAN Max クラスタによって提供されるデータストアをマウントできます。
- [vSAN Max] (vSAN ESA のみ) はストレージ リソースを提供しますが、コンピューティング リソースは提供しません。データストアは、データセンターおよび vCenter Server 間のリモート vSphere クラスタまたは vSAN HCI クラスタによってマウントできます。

vSAN データストア共有には、次の設計上の考慮事項があります。

- 8.0 Update 1 以降を実行している vSAN Original Storage Architecture クラスタは、同じネットワーク上にある限り、同じデータセンターのクラスタ間、またはリモート vCenter Server によって管理されているクラスタ間でデータストアを共有できます。8.0 Update 2 以降を実行している vSAN Express Storage Architecture クラスタには、この機能があります。
- vSAN HCI または vSAN Max クラスタは、ローカル データストアを最大 10 個のクライアント クラスタに提供できます。
- クライアント クラスタは、1 つまたは複数の vSAN サーバ クラスタから最大 5 つのリモート データストアをマウントできます。
- 1 つのデータストアを最大 128 台の vSAN ホストにマウントできます。ローカルの vSAN サーバ クラスタのホストにもマウントできます。
- 仮想マシンを構成するすべてのオブジェクトは、同じデータストアに配置されている必要があります。
- vSphere HA で vSAN データストア共有を機能させるには、APD を使用して、データストアの障害時対応に「仮想マシンをパワーオフして再起動」を構成します。
- クラスタの一部でないクライアント ホストはサポートされません。単一ホストのコンピューティング専用クラスタを構成できますが、2 台目のホストをクラスタに追加しない限り、vSphere HA は機能しません。
- 転送中データの暗号化はサポートされていません。

次の構成は、vSAN データストア共有でサポートされません。

- iSCSI ボリューム、または CNS パーシステント ボリュームのリモート プロビジョニング。ローカルの vSAN データストアにはプロビジョニングできますが、リモート vSAN データストアにはプロビジョニングできません。
- エアギャップ ネットワークまたは複数の vSAN VMkernel ポートを使用するクラスタ

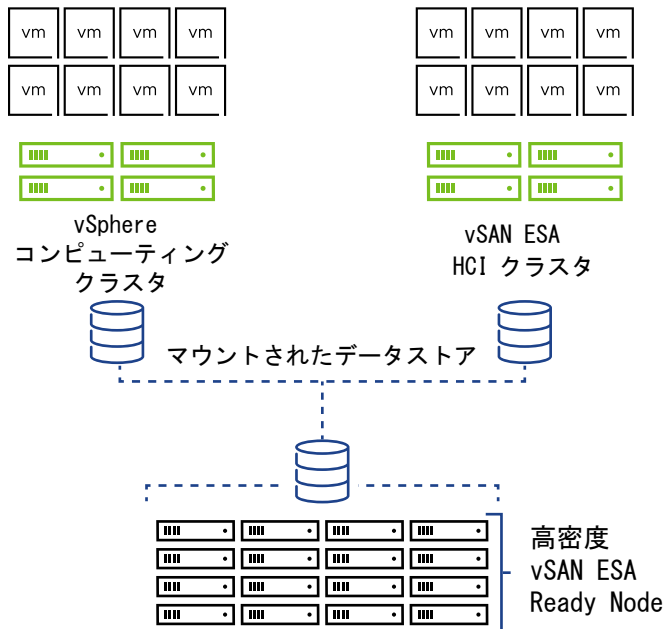
vSAN Max で分離されたストレージ

vSAN Max は、vSphere クラスタおよび vSAN クラスタ向けの、完全に分散されたスケーラブルな共有ストレージソリューションです。ストレージ リソースはコンピューティング リソースから分離されるため、ストレージ リソースとコンピューティング リソースを個別に拡張できます。

vSAN Max は、キャパシティとパフォーマンスを向上するために、vSAN Express Storage Architecture および高密度の vSAN Ready ノードを使用します。

注： vSAN Max は、VMware Cloud Foundation を購入するか、VMware vSphere Foundation の高度なアドオン サービスを取得することによって展開できます。vSAN Max のライセンスは TiB 単位のメトリックに基づいています。これは、環境に必要な Raw ストレージ キャパシティの合計に対応します。

vSAN Max クラスタは、ストレージのみを提供するサーバ クラスタとして機能します。vSAN コンピューティング クラスタまたは vSAN HCI クライアント クラスタとして構成された vSphere クラスタにデータストアをマウントできます。



vSAN Max クラスタには、次の設計上の考慮事項があります。

- vSAN Max で認定された vSAN Ready Node で実行されている vSAN Express Storage Architecture でのみサポートされます。
- vSAN Original Storage Architecture との互換性はありません。
- クライアントとしてではなく、ストレージ サーバとしてのみ機能します。vSAN Max ホストでワークロード仮想マシンを実行しないでください。
- 6 台以上のホストと、ホストあたり 150 TiB が必要です。パフォーマンスを最適化するには、すべてのホストで統一されたストレージ デバイス構成を使用します。
- vSAN Max クラスタ内のホスト間に 100 Gbps のネットワーク接続が必要です。また、コンピューティング クライアントから vSAN Max クラスタへの接続には 10 Gbps の接続が必要です。最高のパフォーマンスを得るには、ジャンボ フレーム (MTU = 9000) のサポートを有効にし、ネットワーク スパインに十分なリソースがあることを確認します。
- 最適なレベルの回復性と容量効率を確保するには、[自動ポリシー管理] ([構成] > [vSAN] > [サービス] > [ストレージ] > [編集]) を有効にします。

- [自動リバランス] ([構成] > [vSAN] > [サービス] > [詳細オプション] > [編集]) を有効にして、均等に分散されたストレージ システムを確保します。

注： vSAN Max は、クラスタの作成時にのみ構成できます。既存の vSAN クラスタを vSAN Max に変換することはできません。また、vSAN Max を vSAN HCI クラスタに変換することもできません。クラスタの vSAN を無効にして、クラスタを再構成する必要があります。

vSAN コンピューティング クラスタ

vSAN コンピューティング クラスタは、vSAN Max データストアをマウントできる小さな vSAN 要素を持つ vSphere クラスタです。コンピューティング クラスタ内のホストには、ローカル ストレージはありません。リモート データストアの容量、健全性、およびパフォーマンスを監視できます。

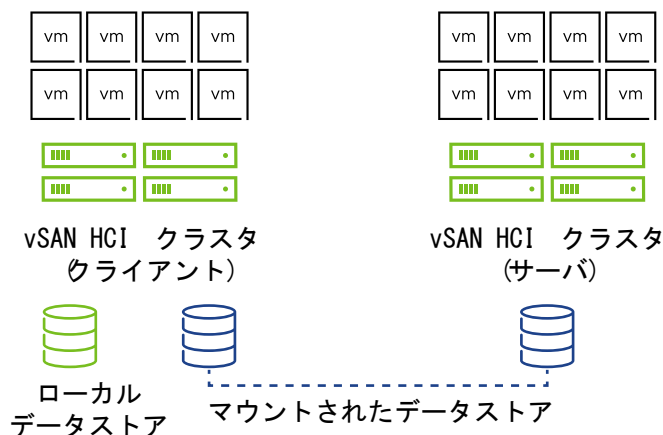
vSAN コンピューティング クラスタには、次の設計の考慮事項があります。

- コンピューティング クラスタ内のホストで vSAN ネットワークを構成する必要があります。
- コンピューティング クラスタ内のホストにストレージ デバイスを配置することはできません。
- コンピューティング クラスタで、データ管理機能を構成することはできません。

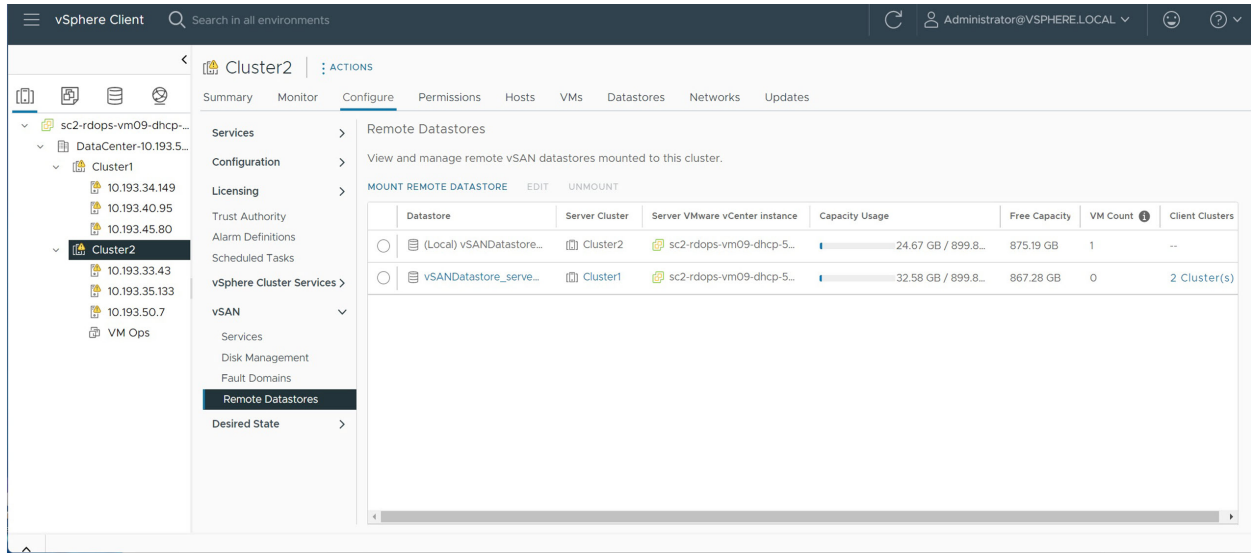
クラスタ間のキャパシティ共有

vSAN HCI クラスタは、他の vSAN HCI クラスタとデータストアを共有できます。vSAN HCI クラスタは、データ ストレージを提供するサーバとして機能します。また、ストレージを使用するクライアントとしても機能します。

vSAN Original Storage Architecture と vSAN Express Storage Architecture は互換性がなく、データストアを相互に共有することはできません。クライアント クラスタは、異なる vSAN アーキテクチャのデータストアをマウントできません。vSAN Original Storage Architecture を使用するデータストアがクラスタにマウントされている場合、vSAN Express Storage Architecture を使用するデータストアはマウントできません。



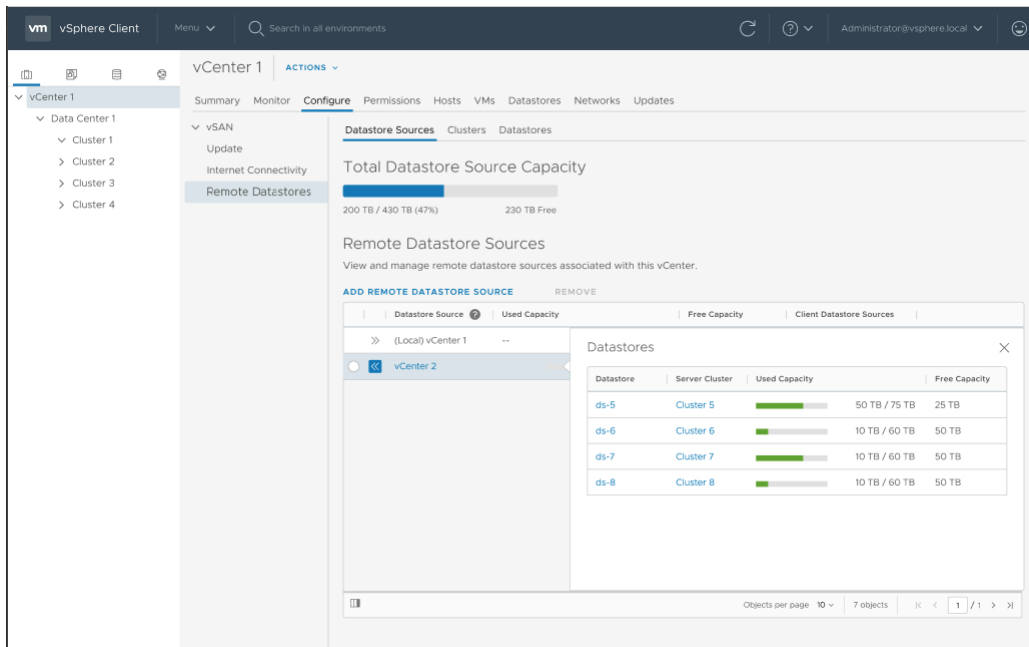
リモート データストア ビューを使用すると、ローカル vSAN クラスタにマウントされたリモート データストアを監視し、管理できます。各クライアント vSAN クラスタは、サーバ vSAN クラスタからリモート データストアをマウントできます。互換性のある各 vSAN クラスタはサーバとして機能し、他の vSAN クラスタにローカル データストアのマウントを許可できます。



仮想オブジェクトの容量、パフォーマンス、健全性、配置の各ビューに、リモート オブジェクトとデータストアのステータスが表示されます。

データストア ソースとしてのリモート vCenter Server の使用

vSAN HCI および vSAN Max クラスタは、vCenter Server 間でリモート データストアを共有できます。ローカル vCenter Server 上のクラスタのデータストア ソースとしてリモート vCenter Server を追加できます。ローカル vCenter Server 上のクライアント クラスタは、リモート vCenter Server に存在するデータストアをマウントできます。



vCenter Server の [リモート データストア] ページを使用して、リモート データストア ソースを管理します ([構成] > [vSAN] > [リモート データベース])。タブをクリックして、vCenter Server 間の共有データストアに関する情報にアクセスします。データストア ソースとして vCenter Server を追加し、データストアをローカル クラスタにマウントします。

[データストア ソース]	リモート vCenter Server にあるデータストア ソースを表示および管理します。ローカル vCenter Server でリモート データストア ソースの追加または削除を実行できます。
[クラスタ]	ローカル vCenter Server のクラスタを表示および管理します。リモート vCenter Server から選択したクラスタでデータストアのマウントまたはアンマウントを実行できます。
[データストア]	この vCenter Server で使用可能なすべてのデータストアを表示します。

vCenter Server 間のデータストア共有には次の設計上の考慮事項があります。

- 各 vCenter Server は、最大 10 個のクライアント vCenter Server を提供できます。
- 各クライアント vCenter Server は、最大 5 個のリモート vCenter Server データストア ソースを追加できます。
- ある vCenter Server によって管理されているクライアント クラスタ上の仮想マシンが、別の vCenter Server によって管理されているサーバのストレージを使用する場合、クライアントの vCenter Server のストレージ ポリシーが優先されます。

リモート vSAN データストアの表示

[リモート データストア] ページには、ローカル vSAN クラスタにマウントされたリモート データストアと、ローカル データストアを共有するクライアント クラスタが表示されます。

The screenshot shows the vCenter Server interface for Datastore Sharing configuration. The left sidebar shows the navigation tree with 'client' selected. The main content area is titled 'Datastore Sharing' and includes a table of datastores.

MOUNT REMOTE DATASTORE		UNMOUNT			
Datastore	Server Cluster	Capacity	Free Space	VM Count	
<input type="radio"/> (Local) vsanDatastore (1)	client	32.98 GB	32.21 GB	3	
<input type="radio"/> vsanDatastore	server	39.97 GB	37.33 GB	7	

手順

- 1 ローカル vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 vSAN で、[リモート データストア] をクリックします。

結果

このビューには、ローカル クラスタにマウントされた各データストアに関する情報が表示されます。

- データストアをホストするサーバ クラスタ
- サーバ クラスタの vCenter Server (該当する場合)
- データストアのキャパシティ使用量
- 使用可能な空き容量
- データストアを使用している仮想マシンの数 (ローカル クラスタでコンピューティング リソースを使用し、サーバ クラスタでストレージ リソースを使用している仮想マシンの数)
- データストアをマウントしているクライアント クラスタ

次のステップ

このページからリモート データストアのマウントまたはアンマウントを行うことができます。

リモート vSAN データストアのマウント

他の vSAN クラスタから 1 つ以上のデータストアをマウントできます。

手順

- 1 ローカル vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 vSAN で、[リモート データストア] をクリックします。
- 4 [リモート データストアのマウント] をクリックしてウィザードを開きます。
- 5 (オプション) データストア ソースとしてリモート vCenter Server を選択します。
- 6 データストアを選択します。
- 7 (オプション) サーバ クラスタが vSAN ストレッチ クラスタの場合は、vSAN HCI サーバとクライアント間の最適なデータ パスを選択するようにサイト結合を構成します。

vSAN ストレッチ クラスタには非対称ネットワークがある場合があります。このネットワークでは、各サイト内のリンクの帯域幅が大きく、サイト間のリンクよりも遅延が少なくなります。対称ネットワークの場合、各サイト内とサイト間で類似のリンクがあります。

- a [ネットワーク トポロジ] ページで、[対称] または [非対称] を選択します。[非対称] を選択すると、[サイト結合] ページが表示されます。
 - b サーバ クラスタ上のサイトを選択して、適切なクライアント サイトと結合します。各クライアント サイトに物理的に近いか、隣接しているサーバ サイトを選択します。
- 8 データストアの互換性を確認し、[終了] をクリックします。

結果

リモート データストアは、ローカルの vSAN クラスタにマウントされます。

次のステップ

仮想マシンをプロビジョニングするときに、ストレージ リソースとしてリモート データストアを選択できます。リモート データストアでサポートされているストレージ ポリシーを割り当てます。

リモート vSAN データストアのアンマウント

vSAN クラスタからリモート データストアをアンマウントできます。

リモート vSAN データストアを使用しているローカル クラスタに仮想マシンがない場合は、ローカルの vSAN クラスタからデータストアをアンマウントできます。

手順

- 1 ローカル vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 vSAN で、[リモート データストア] をクリックします。
- 4 リモート データストアを選択して、[アンマウント] をクリックします。
- 5 [アンマウント] をクリックして確認します。

結果

選択したデータストアがローカル クラスタからアンマウントされます。

vSphere Client とのデータストア共有の監視

vSphere Client を使用して、vSAN データストア共有操作のステータスを監視できます。

リモート データストアがクラスタにマウントされると、vSAN キャパシティ モニターに通知が表示されます。リモート データストアを選択して、その容量情報を確認できます。

仮想オブジェクト ビューには、仮想オブジェクトが配置されているデータストアが表示されます。リモート データストアに配置されている仮想マシンの物理ディスク配置ビューには、リモートの場所に関する情報が表示されます。

The screenshot shows the vSphere Client interface for a VMservice. The 'Monitor' tab is active, displaying 'Physical disk placement'. A notification states: 'This Virtual Machine is placed on a remote datastore managed by vSAN-FVT-Cluster'. Below this, the 'Remote objects' section is expanded, showing a table with the following data:

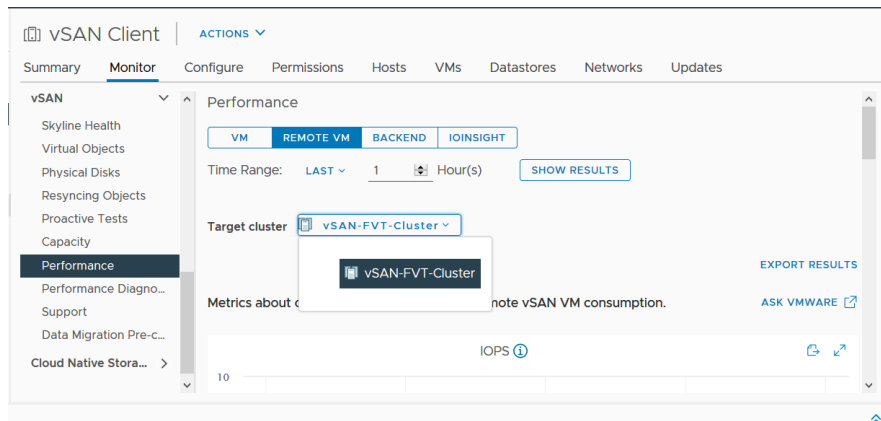
Name	Accessibility	Storage Policy	vSAN Object UUID
Hard disk 1	Remote-accessib...	vSAN Default Storage Policy	d26b445f-5e06-cd69-5fca-0200a99194d9
VM home	Remote-accessib...	vSAN Default Storage Policy	d06b445f-fa3b-8296-60a6-0200a99194...

The table indicates that both objects are accessible and using the vSAN Default Storage Policy. There are 2 objects listed.

vSAN 健全性チェックが HCI 機能のステータスに関するレポートを作成します。

- [データ] > [vSAN オブジェクトの健全性] には、リモート オブジェクトのアクセシビリティ情報が表示されます。
- [ネットワーク] > [サーバ クラスタ パーティション] チェックには、クライアント クラスタとサーバ クラスタのホスト間のネットワーク パーティションに関する情報が表示されます。
- [ネットワーク] > [遅延] では、クライアント クラスタとサーバ クラスタのホスト間の遅延がチェックされます。

vSAN クラスタのパフォーマンス ビューでは、リモート クラスタから見たクライアント クラスタの仮想マシン レベルのパフォーマンスが仮想マシンのパフォーマンス チャートに表示されます。リモート データストアを選択すると、パフォーマンスが表示されます。



リモート データストアでプロアクティブなテストを実行し、仮想マシンの作成とネットワークのパフォーマンスを確認できます。仮想マシンの作成テストでは、リモート データストア上に仮想マシンが作成されます。ネットワーク パフォーマンス テストでは、クライアント クラスタ内のすべてのホストとサーバ クラスタをホストするすべてのホスト間のネットワーク パフォーマンスがチェックされます。

データストア ソースとしてのリモート vCenter Server の追加

ローカル vCenter Server 上のクライアントのリモート データストア ソースとしてリモート vCenter Server を追加できます。

手順

- 1 vSphere Client で vCenter Server に移動します。
- 2 [構成] > [vSAN] > [リモート データストア] を選択します。
- 3 [データストア ソース] タブで、[リモート データストア ソースの追加] をクリックしてウィザードを開きます。
- 4 リモート vCenter Server を指定する情報を入力します。
- 5 互換性をチェックして構成を確認し、[終了] をクリックします。

結果

データストア ソースとしてリモート vCenter Server が追加されます。この vCenter Server 上の vSAN クラスタは、リモート vCenter Server に存在するリモート データストアをマウントできます。

メンテナンス モードでの vSAN クラスタのメンバーの操作

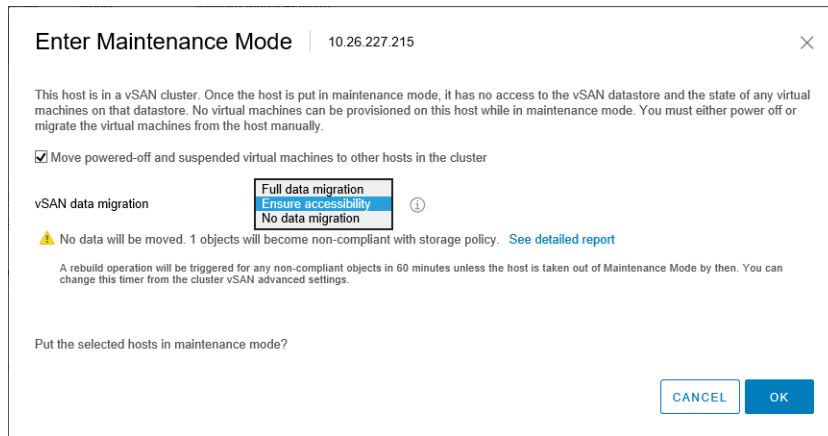
vSAN クラスタのメンバーであるホストは、シャットダウン、再起動または切断する前にメンテナンス モードにする必要があります。

メンテナンス モードで操作する場合、次のガイドラインを考慮します。

- ESXi ホストをメンテナンス モードにする場合、[アクセシビリティの確保] や [全データの移行] など、データ退避モードを選択する必要があります。
- vSAN クラスタのメンバー ホストのいずれかがメンテナンス モードになると、そのメンバー ホストがクラスタにストレージ容量を提供しなくなるため、クラスタ容量が自動的に減少します。
- 仮想マシンの計算リソースはメンテナンス モードになっているホストに存在しない場合があり、仮想マシンのストレージ リソースはクラスタ内の任意の場所に配置されている可能性があります。
- [アクセシビリティの確保] モードは [全データの移行] モードより高速です。これは、[アクセシビリティの確保] では仮想マシンを実行するために不可欠なコンポーネントのみをホストから移行するためです。このモードの場合に障害が発生すると、仮想マシンの可用性に影響があります。[アクセシビリティの確保] モードを選択しても、障害時にデータが再保護されることはなく、予期せぬデータ損失が発生する可能性があります。
- [全データの移行] モードを選択する場合は、リソースが使用可能で、[許容される障害の数] を 1 以上に設定していれば、データは障害に対して自動的に再保護されます。このモードの場合、ホストのすべてのコンポーネントが移行され、ホストに保存されたデータ量によっては移行に長い時間を要する可能性もあります。[全データの移行] モードの場合、仮想マシンでは、予定されていたメンテナンスの期間であっても、障害を許容することができます。
- 3 台のホストのクラスタを操作する場合、[全データの移行] ではサーバをメンテナンス モードにできません。可用性を最大限に高めるには、4 台以上のホストで構成されるクラスタを設計することを検討してください。

ホストをメンテナンス モードにする前に、次の点を確認する必要があります。

- [全データの移行] モードを使用している場合、[許容される障害の数] ポリシーの要件を満たす、十分なホストおよびキャパシティがクラスタにあることを確認します。
- 残りのホストに十分なフラッシュ容量があり、どの vSphere Flash Read Cache 予約でも処理できることを確認します。1 つのホスト障害が原因でクラスタの容量が不足し、クラスタのキャパシティ、キャッシュの予約、およびクラスタ コンポーネントに影響が及ぶ可能性があるかを分析したり、ホストあたりの現在のキャパシティ使用量を分析したりするには、RVC コマンド `vsan.whatif_host_failures` を実行します。RVC コマンドの詳細については、『RVC コマンド リファレンス ガイド』を参照してください。
- ストライブ幅のポリシー要件がある場合は、その要件を処理するための十分なキャパシティ デバイスが残りのホストにあることを確認します。
- 残りのホストに、メンテナンス モードに切り替えるホストから移行が必要なデータ量を処理するための、十分な空き容量があることを確認します。



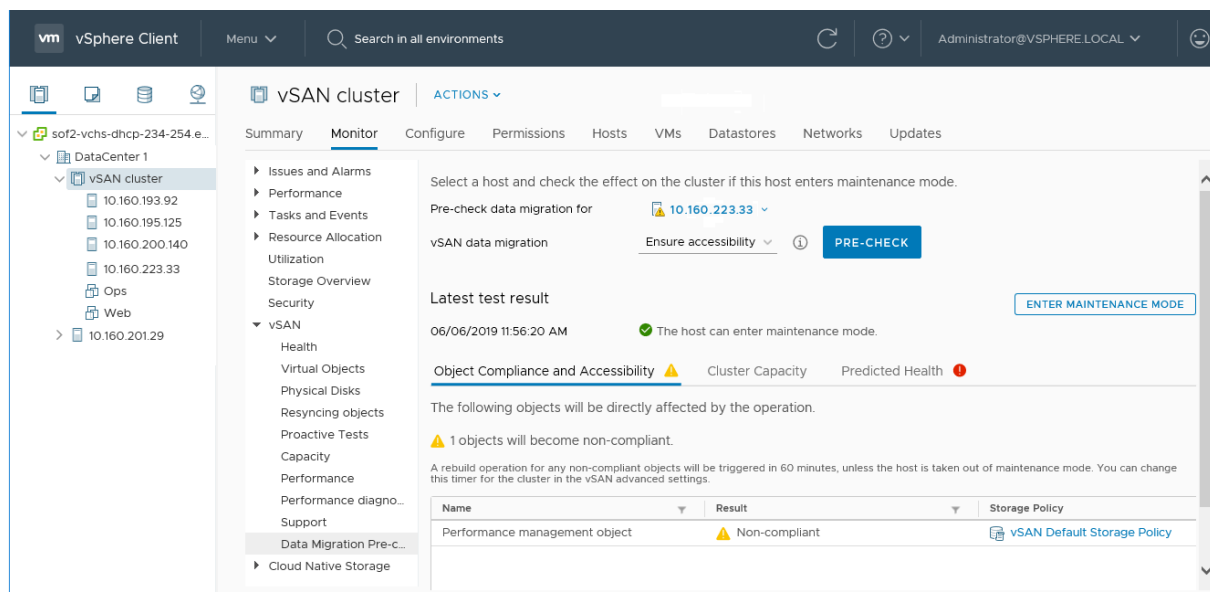
[メンテナンス モードの確認] ダイアログ ボックスは、メンテナンス作業のガイドとなる情報を提供します。ここでは、各データ退避オプションの影響を表示することができます。

- 操作を実行するために必要な容量を使用できるかどうか。
- 移動するデータのサイズ。
- 準拠しなくなるオブジェクトの数。
- アクセスできなくなるオブジェクトの数。

vSAN クラスタ内のホストのデータ移行機能の確認

データ移行の事前チェックを使用して、ホストをメンテナンス モードにしたり、ホストをクラスタから削除したりする際の移行オプションの影響を特定します。

vSAN ホストをメンテナンス モードにする前に、データ移行の事前チェックを実行します。テスト結果から得られる情報は、クラスタ キャパシティへの影響、予測される健全性チェック、コンプライアンスに準拠しなくなると予想されるオブジェクトを判断するのに役立ちます。操作が成功しないと予想される場合、事前チェックからは、必要なリソースに関する情報が提供されます。



手順

- 1 vSAN クラスタに移動します。
- 2 [監視] タブをクリックします。
- 3 [vSAN] の下で、[データ移行の事前チェック] をクリックします。
- 4 ホストとデータ移行オプションを選択し、[事前チェック] をクリックします。

vSAN によってデータ移行の事前チェック テストが実行されます。

- 5 テスト結果を確認します。

事前チェックの結果には、ホストを安全にメンテナンス モードにすることができるかどうかを示されます。

- [オブジェクトのコンプライアンスおよびアクセシビリティ] タブには、データの移行後に問題が発生する可能性のあるオブジェクトが表示されます。
- [クラスタ キャパシティ] タブには、vSAN クラスタに対するデータ移行の影響が、操作を実行する前と後それぞれについて表示されます。
- [予測される健全性] タブには、データ移行によって影響を受ける可能性のある健全性チェックが表示されません。

次のステップ

ホストをメンテナンス モードに切り替えることができると事前チェックによって示されている場合は、[メンテナンス モードに切り替える] をクリックすることにより、データを移行してホストをメンテナンス モードにすることができます。

vSAN クラスタ メンバーのメンテナンス モードへの切り替え

vSAN クラスタのメンバーであるホストは、シャットダウン、再起動または切断する前にメンテナンス モードにする必要があります。

ホストをメンテナンス モードにする場合、[アクセシビリティの確保] や [全データの移行] などのデータ退避モードを選択する必要があります。vSAN クラスタのメンバー ホストのいずれかがメンテナンス モードになると、そのメンバー ホストがクラスタに容量を提供しなくなるため、クラスタ容量が自動的に減少します。

注： vSAN クラスタ内のホストがメンテナンス モードに切り替わると、ホストで実行されている vSAN ファイル サービス仮想マシン (FSVM) が自動的にパワーオフされます。

このホストによって提供されるすべての vSAN iSCSI ターゲットは、クラスタ内の他のホストに転送されます。iSCSI イニシエータは、新しいターゲット所有者にリダイレクトされます。

前提条件

使用環境で、選択するオプションで必要とされる機能が使用可能であることを確認します。

手順

- 1 ホストを右クリックして [メンテナンス モード > メンテナンス モードへの切り替え] の順に選択します。

2 データ退避モードを選択し、[OK] をクリックします。

オプション	説明
アクセシビリティの確保	<p>デフォルトのオプションです。ホストをパワーオフするか、クラスタから削除すると、vSAN は、ホストがメンテナンス モードになった後に各オブジェクトにアクセスするために必要なデータのみを移行します。アップグレードをインストールするときのようにホストを一時的にクラスタから外して後で戻す場合に、このオプションを選択します。このオプションは、クラスタからホストを恒久的に削除する場合には適切ではありません。</p> <p>通常、部分的なデータ退避だけが必要です。ただし、退避中は、仮想マシンが仮想マシン ストレージ ポリシーに対して完全準拠ではなくなる可能性があります。つまり、一部のレプリカにアクセスできなくなることがあります。ホストがメンテナンス モードになっており、[許容される障害の数] が 1 に設定されている場合に障害が発生すると、クラスタでデータが損失する可能性があります。</p> <p>注： 3 台のホスト クラスタ、または 3 つのフォルト ドメインが構成されている vSAN クラスタを使用している場合、これは使用できる唯一の退避モードです。</p>
全データの移行	<p>vSAN は、クラスタ内の他のホストにすべてのデータを退避し、現在のオブジェクトのコンプライアンス状態を維持します。このオプションはホストを恒久的に移行する場合に選択します。クラスタの最後のホストからデータを退避させたら、必ず仮想マシンを別のデータストアに移行してホストをメンテナンス モードにします。</p> <p>この退避モードにすると、大量のデータが転送され、時間とリソースの消費が最も多くなります。選択したホストのローカル ストレージ上のすべてのコンポーネントは、クラスタの別の場所に移行されます。ホストがメンテナンス モードになっている場合、すべての仮想マシンはそのストレージ コンポーネントにアクセスでき、これに割り当てられたストレージ ポリシーに引き続き準拠します。</p> <p>注： 可用性が低下した状態のオブジェクトがある場合、このモードはこのコンプライアンス状態を維持しますが、オブジェクトのコンプライアンスが維持される保証はありません。</p> <p>ホスト上にデータが保存されている仮想マシン オブジェクトにアクセスすることができず、このオブジェクトが完全に退避されない場合、そのホストをメンテナンス モードに切り替えることはできません。</p>
データの移行なし	<p>vSAN はこのホストからデータを退避させません。クラスタからホストをパワーオフまたは削除した場合、仮想マシンによってはアクセス不能になる可能性があります。</p>

3 つのフォルト ドメインが構成されているクラスタには、3 台のホスト クラスタの場合と同じ制約があり、[全データの移行] モードを使用したり、障害後にデータを再保護したりすることはできません。

また、ESXCLI を使用してホストをメンテナンス モードにすることもできます。このモードに切り替える前に、ホストで実行されている仮想マシンをパワーオフしておく必要があります。

メンテナンス モードに切り替える前にアクションを実行するには、ホストで次のコマンドを実行します。

```
esxcli system maintenanceMode set --enable 1 --vsanmode=<str>
```

vsanmode で許可される文字列値は次のとおりです。

- ensureObjectAccessibility - メンテナンス モードに切り替える前に、ディスクからデータを退避して、vSAN クラスタ内のオブジェクトのアクセシビリティを確保します。

注： デフォルト値は ensureObjectAccessibility です。この値は、vsanmode に値を指定しない場合に使用されます。

- evacuateAllData - メンテナンス モードに切り替わる前に、ディスクからすべてのデータを退避します。
- noAction - メンテナンス モードに切り替わる前に、vSAN データをディスクから移動しません。

ホストのステータスを更新するには、次のコマンドを実行します。

```
esxcli system maintenanceMode get
```

メンテナンス モードを終了するには、次のコマンドを実行します。

```
esxcli system maintenanceMode set --enable 0
```

次のステップ

クラスタ内のデータ移行の進行状況を追跡することができます。詳細については、『vSAN の監視とトラブルシューティング』を参照してください。

vSAN クラスタのフォルト ドメインの管理

フォルト ドメインを使用すると、vSAN クラスタが複数のラックまたはブレード サーバ シャーシに分散している場合に、ラックまたはシャーシの障害から保護できます。

フォルト ドメインを作成し、各フォルト ドメインに 1 台以上のホストを追加できます。フォルト ドメインは、データセンターでの物理的な場所に基づいてグループ化された 1 台以上の vSAN ホストで構成されます。フォルト ドメインが構成されている場合、vSAN では、物理ラック全体の障害とともに、単独のホスト、キャパシティ デバイス、ネットワーク リンク、またはフォルト ドメイン専用のネットワーク スイッチの障害を許容できます。

クラスタの [許容される障害の数] ポリシーは、プロビジョニングされる仮想マシンで許容できる仮想マシン障害の数によって異なります。仮想マシンの [許容される障害の数] が 1 に設定されている場合 (FTT=1)、vSAN では、ラック全体の障害を含め、フォルト ドメインでの任意の種類および任意のコンポーネントの単一障害を許容することができます。

ラックでフォルト ドメインを構成し、新規仮想マシンをプロビジョニングすると、vSAN ではレプリカや監視などの保護オブジェクトが確実に異なるフォルト ドメインに配置されるようにします。たとえば、仮想マシン ストレージ ポリシーで [許容される障害の数] が N (FTT=n) に設定されている場合、vSAN ではクラスタ内に最小で $2 * n + 1$ 個のフォルト ドメインが必要です。このポリシーを使用して、フォルト ドメインが構成されているクラスタで仮想マシンがプロビジョニングされると、関連付けられた仮想マシン オブジェクトのコピーが別々のラックに保存されます。

FTT = 1 をサポートするには、少なくとも 3 つのフォルト ドメインが必要です。最適な結果を得るには、クラスタ内で 4 つ以上のフォルト ドメインを構成します。3 つのフォルト ドメインが構成されているクラスタには 3 台のホスト クラスタの場合と同じ制約があります。たとえば、障害後にデータを再保護したり、[全データの移行] モードを使用したりすることはできません。フォルト ドメインの設計およびサイジングの詳細については、『vSAN のプランニングとデプロイ』の「vSAN フォルト ドメインの設計とサイジング」を参照してください。

16 台のホストで構成される vSAN クラスタを使用する場合のシナリオについて考えます。ホストは 4 台のラックに分けて収容されています。つまり、ラックあたり 4 台のホストとなります。ラック全体の障害を許容するには、ラックごとにフォルト ドメインを作成します。[許容される障害の数] を 1 に設定すると、このようなキャパシティをもつクラスタを構成できます。[許容される障害の数] を 2 に設定する場合は、クラスタ内に 5 つのフォルト ドメインを構成します。

1 つのラックで障害が発生すると、ラックの CPU およびメモリを含むすべてのリソースをクラスタで使用できなくなります。発生する可能性のあるラック障害の影響を低減するには、サイズの小さなフォルト ドメインを構成します。フォルト ドメインの数を増やすと、ラック障害が発生した後にクラスタ内で使用できるリソースの総量が増加します。

フォルト ドメインを使用して作業する場合は、次のベスト プラクティスに従います。

- vSAN クラスタで、少なくとも 3 つのフォルト ドメインを構成します。最適な結果を得るには、4 つ以上のフォルト ドメインを構成します。
- フォルト ドメインに含まれないホストは、それ自体のシングルホスト フォルト ドメインに存在しているとみなされます。
- すべての vSAN ホストをフォルト ドメインに割り当てる必要はありません。フォルト ドメインを使用して vSAN 環境を保護する場合は、サイズが同じフォルト ドメインを作成することを考慮します。
- 別のクラスタに移動すると、vSAN ホストは、フォルト ドメインの割り当てを保持します。
- フォルト ドメインを設計する場合は、一定数のホストを各フォルト ドメインに配置します。

フォルト ドメインの設計のガイドラインについては、『vSAN のプランニングとデプロイ』の「vSAN フォルト ドメインの設計とサイジング」を参照してください。

- フォルト ドメインには、任意の数のホストを追加することができます。各フォルト ドメインには、少なくとも 1 つのホストを含める必要があります。

vSAN クラスタのフォルト ドメインの新規作成

仮想マシン オブジェクトがラック障害時でも引き続きスムーズに実行するようにするため、異なるフォルト ドメインでホストをグループ化することができます。

フォルト ドメインを含むクラスタで仮想マシンをプロビジョニングすると、仮想マシンの監視やレプリカなどの保護コンポーネントが、vSAN で異なるフォルト ドメインにまたがって分散されます。その結果、vSAN 環境で、1 台のホスト、ストレージ ディスク、ネットワークの障害に加え、ラック全体の障害を許容できるようになります。

前提条件

- 一意のフォルト ドメイン名を選択します。vSAN では、同じクラスタ内で重複するフォルト ドメイン名をサポートしていません。
- ESXi ホストのバージョンを確認します。フォルト ドメインに含めることができるのは、バージョン 6.0 以降のホストのみです。
- vSAN ホストがオンラインであることを確認します。ハードウェア構成の問題のため、オフラインまたは使用不可のフォルト ドメインにホストを割り当てることはできません。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 vSAN で [フォルト ドメイン] をクリックします。
- 4 プラス記号アイコンをクリックします。[新しいフォルト ドメイン] ウィザードが開きます。
- 5 フォルト ドメイン名を入力します。
- 6 フォルト ドメインに追加する 1 つ以上のホストを選択します。

フォルト ドメインは空にはできません。フォルト ドメインに含めるホストを少なくとも 1 つ選択する必要があります。

- 7 [作成] をクリックします。

選択したホストがフォルト ドメインに表示されます。各フォルト ドメインには、使用済みおよび予約済みのキャパシティ情報が表示されます。これにより、フォルト ドメイン全体でのキャパシティ分布を確認できます。

vSAN クラスタの選択したフォルト ドメインへのホストの移動

vSAN クラスタの選択したフォルト ドメインに、ホストを移動することができます。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 vSAN で [フォルト ドメイン] をクリックします。
- 4 既存のフォルト ドメインに追加するホストをクリックしてドラッグします。

選択したホストがフォルト ドメインに表示されます。

vSAN クラスタのフォルト ドメインからのホストの移動

要件に応じて、フォルト ドメインからホストを移動できます。

前提条件

ホストがオンラインであることを確認します。オフラインまたは使用不可のホストはフォルト ドメインから移動できません。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 vSAN で [フォルト ドメイン] をクリックします。
 - a ホストをクリックして、フォルト ドメインから [スタンドアローン ホスト] 領域にドラッグします。
 - b [移動] をクリックして確認します。

結果

選択したホストが、フォルト ドメインに属さなくなります。フォルト ドメインに含まれないホストは、それ自体のシングルホスト フォルト ドメインに存在しているとみなされます。

次のステップ

フォルト ドメインにホストを追加できます。「[vSAN クラスタの選択したフォルト ドメインへのホストの移動](#)」を参照してください。

vSAN クラスタのフォルト ドメインの名前変更

vSAN クラスタの既存のフォルト ドメインの名前を変更できます。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 vSAN で [フォルト ドメイン] をクリックします。
 - a フォルト ドメインの右側にある [アクション] アイコンをクリックして、[編集] を選択します。
 - b フォルト ドメインの新しい名前を入力します。
- 4 [適用] または [OK] をクリックします。

新しい名前が、フォルト ドメインのリストに表示されます。

vSAN クラスタからの選択したフォルト ドメインの削除

フォルト ドメインが不要になったら、vSAN クラスタから削除できます。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 vSAN で [フォルト ドメイン] をクリックします。
- 4 フォルト ドメインの右側にある [アクション] アイコンをクリックして、[削除] を選択します。
- 5 [削除] をクリックして確認します。

結果

フォルト ドメインのすべてのホストが削除され、選択したフォルト ドメインが vSAN クラスタから削除されます。フォルト ドメインに含まれない各ホストは、それ自体のシングルホスト フォルト ドメインに存在しているとみなされます。

vSAN クラスタのフォルト ドメインによる追加障害の許容

vSAN クラスタのフォルト ドメインを使用すると、回復力が提供されます。障害が発生した場合でも、ポリシーに基づいてデータを確実に使用することができます。

許容する障害数 (FTT) が 1 に設定されている場合、オブジェクトは障害を許容できます。ただし、クラスターで一時的な障害が発生した後に永続的な障害が発生すると、データが失われる可能性があります。フォルト ドメインを追加すると、オブジェクトに FTT を追加することなく、vSAN に持続性コンポーネントを作成できます。計画的な障害または計画外の障害が発生すると、vSAN はこの追加コンポーネントをトリガします。計画外の障害としては、ネットワークの切断、ディスク障害、ホスト障害などがあります。計画的な障害としては、メンテナンス モードへの切り替え (EMM) などがあります。たとえば、RAID 6 オブジェクトを持つ 6 個のホスト クラスターでホスト障害が発生すると、持続性コンポーネントを作成できません。

vSAN は、ストレージ ポリシーで指定された FTT に基づいてコンポーネントがオフラインになり、予期せずオンラインに戻ると、オブジェクトのデータ可用性が維持されます。障害発生時に、障害が発生したコンポーネントの書き込みは、持続性コンポーネントにリダイレクトされます。コンポーネントが一時的な障害から復旧し、オンラインに戻ると、持続性コンポーネントが消え、その結果、コンポーネントが再同期されます。

持続性コンポーネントが設定されることなく、クラスター内に 2 度目の永続的な障害が発生し、ミラー オブジェクトが影響を受けると、障害が解決してもオブジェクト データが完全に失われます。

vSAN Data Protection の使用

vSAN データ保護を使用すると、vSAN クラスターのローカルに保存されたネイティブ スナップショットを使用して、システム障害やランサムウェア攻撃から仮想マシンをすばやくリカバリできます。

vSAN データ保護は、vSAN ESA を搭載した vSAN HCI クラスターでサポートされます。ネイティブ vSAN スナップショットを使用して、仮想マシンの現在の状態をキャプチャします。vSAN スナップショットを使用して仮想マシンを以前の状態にリストアしたり、開発やテスト用に仮想マシンのクローンを作成したりできます。

The screenshot shows the vSAN Data Protection configuration page in vSphere Client. The left sidebar shows the navigation tree with 'vSAN-FVT-Cluster' selected. The main content area is divided into several sections:

- Services:** vSAN Data Protection
- Configuration:** Use vSAN Data Protection to create recurring snapshots for VMs within protection groups, and restore or clone VMs from snapshots.
- Licensing:** PROTECTION GROUPS > PRIORITY PG (with buttons for TAKE SNAPSHOT, EDIT, and PAUSE SCHEDULE)
- Overview:** Priority PG (Active)
- Summary:** Immutability mode: Disabled; VMs: 4; Snapshots: 27; Latest snapshot: 04/12/2024, 10:59:18 AM; Oldest snapshot: 04/11/2024, 10:04:35 AM
- Membership:** Lists Application VM 1, Application VM 2, Application VM 3, and Application VM 4.
- Schedules:**
 - Every 1 day, keep for 1 week: Take snapshot every 1 day, Keep snapshot for 1 week
 - Every 1 hour, keep for 1 day: Take snapshot every 1 hour, Keep snapshot for 1 day

vSAN データ保護では、vSAN スナップショットを管理するために VMware Snapshot Service が必要です。Snapshot Service アプライアンスを展開して、vSphere Client で vSAN データ保護を有効にします。

次のタブを使用して、[vSAN データ保護] ページに移動します。

タブ	説明
サマリ	保護グループの数、保護されている仮想マシンの割合、仮想マシンのスナップショットの数、スナップショットに使用されるストレージ容量など、vSAN データ保護に関する一般的な情報が表示されます。
保護グループ	vSAN データ保護グループとそのステータスのリストが表示されます。保護グループを選択して、その保護グループのスナップショットを表示します。また、構成を編集することもできます。
仮想マシン	vSAN クラスタ内の仮想マシンのリストと、そのデータ保護ステータスに関する詳細が表示されます。使用可能なスナップショットがある削除済みの仮想マシンがここに表示されます。 仮想マシンを選択してクリックし、仮想マシンをリストアまたはクローン作成できます。

vSAN スナップショット

vSAN スナップショットには、スナップショット作成時の仮想マシンの状態とデータが保存されます。このローカルアーカイブには、その時点で仮想マシンに存在するデータが保持されます。スナップショットの作成時の状態に仮想マシンをリストアできます。また、スナップショットに保持されている状態に一致する、新しいリンク クローン仮想マシンを作成することもできます。

スナップショットを作成すると、特定の時点での仮想マシンの状態がキャプチャされます。vSAN スナップショットは静止ではなく、仮想マシンの現在の実行状態をキャプチャします。

スナップショットは個々の仮想マシンで操作されます。仮想マシンごとに個別のスナップショットが必要です。仮想マシンを保護グループに配置することで、仮想マシンのスナップショットを手動またはスケジュールで作成できます。

各 vSAN スナップショットには、仮想マシンの名前空間オブジェクトと仮想ディスク オブジェクトの状態が含まれます。vSAN は、スケジュールリングされた間隔で保護グループ内の仮想マシンのスナップショットを作成します。これらの vSAN スナップショットは、vSAN データストアのローカルに保存されます。

保護グループ

保護グループを使用すると、1 台または複数の仮想マシンのスナップショットをスケジュールリングし、管理することができます。仮想マシンを保護グループに追加したり、スナップショットのスケジュールを構成したり、スナップショットの情報を確認できます。

保護グループを選択し、次のタブを使用してグループを管理します。

タブ	説明
概要	メンバー仮想マシンのリスト、スナップショット スケジュール、作成されたスナップショットの数など、保護グループに関する一般的な情報が表示されます。
スナップショット	保護グループに関連付けられているスナップショット シリーズが表示されます。個々のスナップショットを選択して、シリーズから削除できます。
仮想マシン	保護グループのメンバーである仮想マシンのリストと、各仮想マシンで使用可能なスナップショットの数が表示されます。

保護グループを作成する場合は、メンバー仮想マシンを追加し、1 つ以上のスナップショット スケジュールを構成します。仮想マシンは個別に追加することも、仮想マシン名のパターンを入力して、そのパターンに一致するすべての仮想マシンを追加することもできます。両方の方法で仮想マシンを保護グループに追加できます。

複数のスナップショット スケジュールを定義して、保護グループ内の仮想マシンの状態を定期的にキャプチャできません。新しいスナップショットがキャプチャされると、保持設定に基づいて vSAN は古いスナップショットをシリーズから削除します。また、手動でスナップショットを作成して、保護グループ内の仮想マシンの現在の状態をキャプチャすることもできます。

セキュリティを強化するため、保護グループで [不変モード] を有効にします。不変モードが有効になっている場合、その保護グループの編集または削除、仮想マシンのメンバーシップの変更、スナップショットの編集または削除を行うことはできません。不変モードのスナップショットは、管理者権限を持つ攻撃者でも変更または削除できない、データの読み取り専用コピーです。

注： 保護グループで不変モードが有効になっている場合、管理者がこのモードを無効にすることはできません。

[保護グループ] タブから保護グループの監視と変更を行うことができます。詳細を表示する保護グループをクリックします。

- [概要] には、仮想マシンのメンバーシップ、スナップショット スケジュール、スナップショットの数など、保護グループに関する全般的な情報が表示されます。
- [スナップショット] には、保護グループで使用可能なスナップショットのリストが表示されます。スナップショットを選択して [>>] をクリックすると、各仮想マシンの個々のスナップショットを表示して、アクションを実行できます。
- [仮想マシン] には、保護グループ内の仮想マシンのリストと、使用可能なスナップショットの詳細が表示されます。仮想マシンのラジオ ボタンを選択し、[仮想マシンをリストア] または [仮想マシンのクローン作成] をクリックして、スナップショットを選択します。

次のいずれかのボタンをクリックして、保護グループに対してアクションを実行します。

操作	説明
スナップショットの作成	スナップショットのデフォルト名を変更し、保持期間を定義できます。vSAN は、保護グループ内の仮想マシンごとに個別のスナップショットを作成します。
編集	仮想マシンを追加または削除したり、仮想マシン名のパターンを変更したり、スナップショット スケジュールの追加や変更を行うことができます。
スケジュールの一時停止/スケジュールの再開	保護グループに定義されているスナップショット スケジュールを一時停止できます。スケジュールが一時停止している間、スナップショットの作成または削除は実行されません。

保護グループを削除するには、[詳細..] アイコンをクリックして、メニューから [削除] を選択します。保護グループを削除する場合は、そのスナップショットの管理方法を決定する必要があります。

- [有効期限までスナップショットを保持]。既存のすべてのスナップショットの有効期限が切れると、保護グループが削除されます。
- [スナップショットの削除]。保護グループとその既存のスナップショットはすぐに削除されます。

vSAN と VMware Live Cyber Recovery

VMware Live Cyber Recovery は、保護サイトの vSAN スナップショットを利用して、クラウド内でランサムウェアに感染した仮想マシンを迅速にリカバリします。VLCR は、vSAN スナップショットを使用して、本番環境サイトで仮想マシンの差分のみを更新することで、リストア時間を短縮します。

詳細については、「VMware Live Cyber Recovery」の「VMware vSAN ローカル スナップショットを使用した高速リストア」を参照してください。

Snapshot Service アプライアンスの展開

vSAN データ保護では、vSAN スナップショットを管理するために VMware Snapshot Service アプライアンスが必要です。

Snapshot Service アプライアンスを vCenter Server と同じサイトに展開して、ネットワーク接続の遅延を低減します。

OVA ファイルをダウンロードして展開し、VMware Snapshot Service アプライアンスを追加します。アプライアンス OVA の展開は、テンプレートから仮想マシンを展開することに似ています。

このアプライアンスには、信頼できる vCenter Server 証明書が必要です。vCenter Server のホーム ページで、[信頼できるルート CA 証明書をダウンロード] をクリックします。証明書ファイルを展開し、[Certs > lin] を開き、拡張子が .0 のファイルからテキストをコピーします。詳細な手順については、次のナレッジベースの記事を参照してください：<https://knowledge.broadcom.com/external/article/330833/how-to-download-and-install-vcenter-serv.html>

手順

- 1 Broadcom の Web サイト (<https://support.broadcom.com/group/ecx/downloads>) から VMware Snapshot Service アプライアンスをダウンロードします。
- 2 vSphere Client で vSAN クラスタを右クリックし、[OVF テンプレートの展開] を選択してウィザードを開きます。
- 3 [OVF テンプレートの選択] ページで、アプライアンスの OVA ファイルの場所を指定し、[次へ] をクリックします。
- 4 [名前とフォルダの選択] ページで、アプライアンスの一意の名前を入力し、展開場所としてデータセンターを選択します。
- 5 [コンピューティング リソースの選択] ページで、コンピューティング リソースとして vSAN クラスタを選択します。
- 6 [ストレージの選択] 画面で、データストアを選択します。
- 7 [ネットワークの選択] ページで、vCenter Server と同じネットワークを選択し、[次へ] をクリックします。
- 8 [テンプレートのカスタマイズ] ページで、アプライアンス仮想マシンの root パスワードを入力し、アプライアンスを展開する vCenter Server を指定します。[vCenter Server 証明書] フィールドに証明書のテキストを入力します。

結果

VMware Snapshot Service が、指定された vCenter Server に展開され、vSphere Client で vSAN データ保護のページが使用できるようになります。

vSAN Data Protection グループの作成

仮想マシンをデータ保護グループに配置し、一貫した方法でグループのすべての仮想マシンメンバーのスナップショットをスケジューリングして管理します。

保護グループを使用すると、1台または複数の仮想マシンの vSAN スナップショットをスケジューリングし、管理することができます。リンク クローン仮想マシンまたは vSphere スナップショットのある仮想マシンを vSAN データ保護グループに追加することはできません。

Create Protection Group

- 1 General
- 2 Add VM name patterns
- 3 Select individual VMs
- 4 Add snapshot schedules
- 5 Review

Add snapshot schedules ✕

Schedule name	Every 1 hour, keep for 2 weeks	✕ REMOVE
Take snapshot every	1 hour(s) ▾	
Keep snapshot for	2 week(s) ▾	
<hr/>		
Schedule name	Every 1 day, keep for 1 month	✕ REMOVE
Take snapshot every	1 day(s) ▾	
Keep snapshot for	1 month(s) ▾	
<hr/>		
+ ADD SCHEDULE		

CANCEL
BACK
NEXT

前提条件

vSAN クラスタが次の要件を満たしていることを確認します。

- vSAN Express Storage Architecture
- vSAN 8.0 Update 3 以降
- vCenter Server に展開された VMware Snapshot Service アプライアンス

手順

- 1 vSphere Client で、vSAN クラスタに移動します。
- 2 [構成] タブをクリックして、[vSAN] > [データ保護] の順に選択します。

3 [保護グループ] を選択し、[保護グループの作成] をクリックしてウィザードを開きます。

a [全般] ページで、保護グループの名前を入力し、仮想マシンのメンバーシップの定義方法を選択します。

注： 管理者権限を持つ攻撃者が変更または削除できない読み取り専用スナップショットを作成するには、不変モードを有効にします。不変モードが有効になっている場合、管理者がこのモードを無効にすることはできません。

b (オプション) [仮想マシン名のパターンの追加] ページで、一致する 1 つ以上の仮想マシン名パターンを入力します。

クラスタ内でパターンに一致する名前のすべての仮想マシンが保護グループに追加されます。特殊文字を使用して、各仮想マシン名のパターンを定義できます。

- 0 個以上の文字と一致させるには * を使用します。たとえば、仮想マシン名のパターン database* と prod-*-x は、databaseSQL、prod-1-x、prod-23-x という名前の仮想マシンと一致します。
- 1 個の文字と一致させるには ? を使用します。たとえば、仮想マシン名のパターン prod-? は prod-1 という名前の仮想マシンと一致しますが、prod-23 とは一致しません

c (オプション) [個々の仮想マシンの選択] ページで、保護グループのメンバーとして追加する仮想マシンをリストから選択します。

d [スナップショット スケジュールの追加] ページで、スナップショットのスケジュールと保持間隔を定義します。

最大 10 個のスナップショット スケジュールを追加できます。スケジュール名を入力し、vSAN が保護グループ内の仮想マシンのスナップショットを作成する頻度を選択します。スケジュールされたスナップショットの保持期間を選択します。

e [確認] ページで選択内容を確認し、[作成] をクリックします。

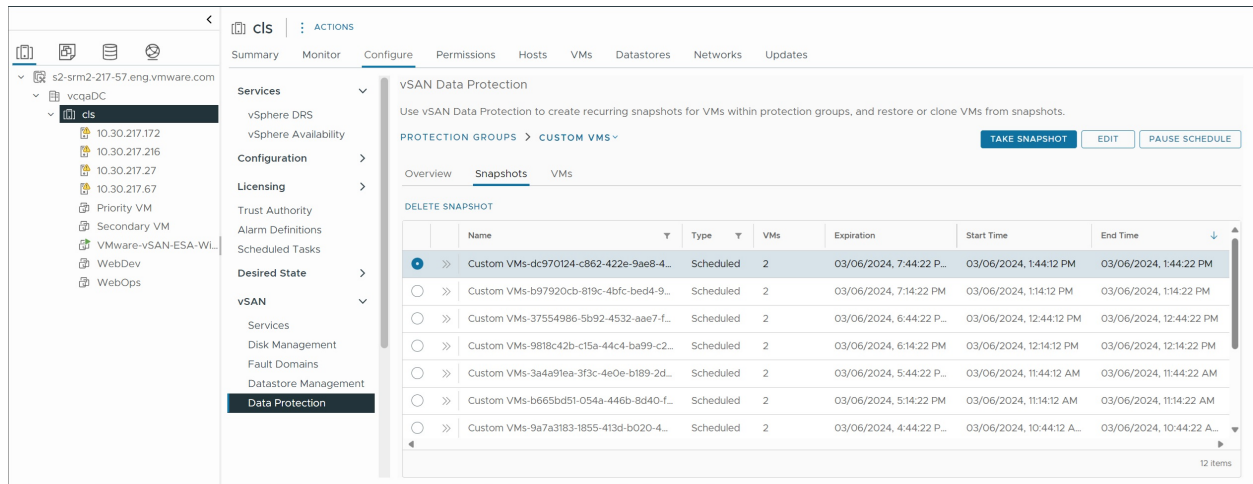
次のステップ

保護グループの設定を編集することができます。手動でスナップショットを作成して、保護グループ内の仮想マシンの現在の状態をキャプチャすることもできます。

vSAN スナップショットの削除

vSphere Client を使用して、保護グループから vSAN スナップショットを削除します。

保護グループの vSAN スナップショットを選択し、グループからスナップショットを削除します。



手順

- 1 vSphere Client で vSAN クラスタに移動し、[構成] > [vSAN] > [データ保護] の順に選択します。
- 2 [保護グループ] タブを選択して保護グループをクリックし、[スナップショット] タブを選択します。
- 3 スナップショットを選択して、[スナップショットの削除] をクリックします。
- 4 [削除] をクリックします。

vSAN スナップショットからの仮想マシンのリストア

vSAN スナップショットを使用すると、スナップショットによって保持された以前の状態に仮想マシンをリストアできます。

vSAN スナップショットから仮想マシンをリストアすると、vSAN は現在の仮想マシンをスナップショットの仮想マシンに置き換えます。スナップショットを使用できる削除済みの仮想マシンをリストアできます。

手順

- 1 vSphere Client で仮想マシンを右クリックし、メニューで [スナップショット] > [vSAN Data Protection] > [スナップショットの管理] の順に選択します。

削除された仮想マシンのスナップショットを検索するには、[構成] > [vSAN] > [データ保護] ページに移動し、[仮想マシン] タブをクリックし、[削除された仮想マシン] をクリックします。

- 2 リストからデバイスを選択して、[仮想マシンをリストア] をクリックします。
- 3 [リストア] ダイアログで [リストア] をクリックして、操作を実行します。

仮想マシンがパワーオフされます。新しいスナップショットが作成され、仮想マシンの現在の状態がキャプチャされるため、必要に応じてこの状態に戻すことができます。

結果

仮想マシンは、スナップショットで指定された以前の状態にリストアされます。

vSAN スナップショットからの仮想マシンのクローン作成

vSAN スナップショットを使用して、元の仮想マシンの状態と一致するリンク クローン仮想マシンを作成できます。

vSAN スナップショットから仮想マシンのクローンを作成する場合は、クローンの場所とコンピューティング リソースを指定する必要があります。

手順

- 1 vSphere Client で仮想マシンを右クリックし、メニューで [スナップショット] > [vSAN Data Protection] > [スナップショットの管理] の順に選択します。
- 2 リストからスナップショットを選択し、[仮想マシンのクローン作成] をクリックして、[仮想マシンのクローン作成] ダイアログを開きます。
- 3 クローンの名前を入力し、場所を選択して、[次へ] をクリックします。
- 4 コンピューティング リソースを選択して、[次へ] をクリックします。
- 5 情報を確認し、[クローン作成] をクリックします。

結果

リンク クローン仮想マシンが作成され、vCenter Server で使用できるようになります。

vSAN iSCSI ターゲット サービスの使用

iSCSI ターゲット サービスを使用すると、vSAN クラスターの外部にあるホストと物理ワークロードが vSAN データストアにアクセスできるようになります。

この機能を使用すると、リモート ホスト上の iSCSI イニシエータが、ブロックレベルのデータを vSAN クラスター内のストレージ デバイス上の iSCSI ターゲットに転送できます。vSAN 6.7 以降のリリースは Windows Server Failover Clustering (WSFC) をサポートしているため、WSFC ノードから vSAN iSCSI ターゲットにアクセスできます。

vSAN iSCSI ターゲット サービスを構成すると、vSAN iSCSI ターゲットをリモート ホストから見つけることができます。vSAN iSCSI ターゲットを見つけるには、vSAN クラスター内の任意のホストの IP アドレスと iSCSI ターゲットの TCP ポートを使用します。vSAN iSCSI ターゲットの高可用性を確保するには、iSCSI アプリケーションにマルチパス サポートを構成します。2 つ以上のホストの IP アドレスを使用して、マルチパスを構成できます。

注： vSAN iSCSI ターゲット サービスは、他の vSphere や ESXi クライアント、イニシエータ、サードパーティのハイパーバイザー、Raw Device Mapping (RDM) を使用した移行をサポートしません。

vSAN iSCSI ターゲット サービスは、次の CHAP 認証方法をサポートします。

CHAP

CHAP 認証では、ターゲットはイニシエータを認証しますが、イニシエータはターゲットを認証しません。

相互 CHAP

相互 CHAP 認証では、セキュリティのレベルが強化され、イニシエータからターゲットを認証できます。

vSAN iSCSI ターゲット サービスの使用の詳細については、『iSCSI Target Usage Guide』を参照してください。
<https://core.vmware.com/resource/vsan-iscsi-target-usage-guide>

iSCSI ターゲット

ストレージ ブロックを論理ユニット番号 (LUN) として提供する iSCSI ターゲットを 1 つまたは複数追加できます。vSAN は、一意の iSCSI 修飾名 (IQN) で各 iSCSI ターゲットを識別します。IQN を使用して iSCSI ターゲットをリモートの iSCSI イニシエータに提示し、イニシエータがターゲットの LUN にアクセスすることができます。

各 iSCSI ターゲットには 1 つまたは複数の LUN が含まれます。各 LUN のサイズを定義し、vSAN ストレージ ポリシーを各 LUN に割り当て、vSAN クラスタで iSCSI ターゲット サービスを有効にします。ストレージ ポリシーを設定して、vSAN iSCSI ターゲット サービスのホーム オブジェクトのデフォルト ポリシーとして使用することができます。

Virtual SAN iSCSI イニシエータ グループ

指定された iSCSI ターゲットにアクセスできる iSCSI イニシエータのグループを定義できます。iSCSI イニシエータ グループは、グループのメンバーであるイニシエータのみにアクセスを制限します。iSCSI イニシエータまたはイニシエータ グループを定義しない場合は、各ターゲットはすべての iSCSI イニシエータにアクセスできます。

各 iSCSI イニシエータ グループは、一意の名前で識別されます。1 つまたは複数の iSCSI イニシエータをグループのメンバーとして追加できます。イニシエータの IQN を、メンバー イニシエータ名として使用します。

vSAN iSCSI ターゲット サービスの有効化

iSCSI ターゲットと LUN を作成して iSCSI イニシエータ グループを定義する前に、vSAN クラスタで iSCSI ターゲット サービスを有効にする必要があります。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [サービス] の順にクリックします。
- 2 [vSAN iSCSI ターゲット サービス] 行で、[有効] をクリックします。
[vSAN iSCSI ターゲット サービスを編集] ウィザードが開きます。
- 3 vSAN iSCSI ターゲット サービスの構成を編集します。
この時点で、デフォルト ネットワーク、TCP ポート、認証方法を選択できます。vSAN ストレージ ポリシーを選択することもできます。
- 4 [vSAN iSCSI ターゲット サービスを有効化] スライダをクリックしてオンにし、[適用] をクリックします。

結果

vSAN iSCSI ターゲット サービスが有効になります。

次のステップ

iSCSI ターゲット サービスが有効になると、iSCSI ターゲット と LUN を作成して iSCSI イニシエータ グループを定義することができます。

vSAN iSCSI ターゲットの作成

iSCSI ターゲットとそれに関連付けられた LUN を作成または編集できます。

前提条件

vSAN iSCSI ターゲット サービスが有効になっていることを確認します。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
 - a vSAN で [iSCSI ターゲット サービス] をクリックします。
 - b [iSCSI ターゲット] タブをクリックします。
 - c [追加] をクリックします。[新しい iSCSI ターゲット] ダイアログ ボックスが表示されます。ターゲットの IQN フィールドを空白にしておくと、IQN が自動的に生成されます。
 - d ターゲットの [エイリアス] を入力します。
 - e [ストレージ ポリシー]、[ネットワーク]、[TCP ポート]、[認証方法] を選択します。
 - f [I/O 所有者の場所] を選択します。この機能は、ストレッチ クラスタとして vSAN クラスタを構成している場合にのみ使用できます。ターゲットの iSCSI ターゲット サービスをホストするサイトの場所を指定できます。これは、サイト間の iSCSI トラフィックを回避するのに役立ちます。ポリシーを HFT ≥ 1 に設定すると、サイトに障害が発生した場合に I/O 所有者の場所が別のサイトに変わります。サイト障害のリカバリ後、構成に従って自動的に I/O 所有者の場所が元の場所に戻ります。サイトの場所を設定するには、次のいずれかのオプションを選択します。
 - [いずれか]: iSCSI ターゲット サービスを優先サイトまたはセカンダリ サイトのいずれかにホストします。
 - [優先]: iSCSI ターゲット サービスを優先サイトにホストします。
 - [セカンダリ]: iSCSI ターゲット サービスをセカンダリ サイトにホストします。
- 3 [OK] をクリックします。

結果

iSCSI ターゲットが作成され、IQN、I/O 所有者ホストなどの情報と一緒に [vSAN iSCSI ターゲット] セクションに表示されます。

次のステップ

このターゲットにアクセスできる iSCSI イニシエータのリストを定義します。

vSAN iSCSI ターゲットへの LUN の追加

vSAN iSCSI ターゲットに 1 つ以上の LUN を追加したり、既存の LUN を編集したりできます。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
 - a vSAN で [iSCSI ターゲット サービス] をクリックします。
 - b [iSCSI ターゲット] タブをクリックし、ターゲットを選択します。
 - c [vSAN iSCSI LUN] セクションで、[追加] をクリックします。[LUN をターゲットに追加] ダイアログ ボックスが表示されます。
 - d LUN のサイズを入力します。iSCSI ターゲット サービス用に構成された vSAN ストレージ ポリシーが自動的に割り当てられます。各 LUN に異なるポリシーを割り当てることができます。
- 3 [追加] をクリックします。

vSAN iSCSI ターゲットでの LUN のサイズ変更

要件に応じて、オンライン LUN のサイズを増やすことができます。

LUN のオンライン サイズ変更は、クラスタ内のすべてのホストが vSAN 6.7 Update 3 以降にアップグレードされている場合にのみ有効となります。

手順

- 1 vSphere Client で vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] の下で [iSCSI ターゲット サービス] をクリックします。
- 4 [iSCSI ターゲット] タブをクリックして、ターゲットを選択します。
- 5 [vSAN iSCSI Lun] セクションで、LUN を選択し、[編集] をクリックします。[LUN の編集] ダイアログ ボックスが表示されます。
- 6 要件に応じて LUN のサイズを増やします。
- 7 [OK] をクリックします。

vSAN iSCSI イニシエータ グループの作成

vSAN iSCSI ターゲットに対するアクセス コントロールを提供する vSAN iSCSI イニシエータ グループを作成できます。

イニシエータ グループのメンバーである iSCSI イニシエータのみが vSAN iSCSI ターゲットにアクセスできます。

注： アクセスコントロールのイニシエータ グループが iSCSI ターゲットに作成されている場合、イニシエータ グループの外部のイニシエータはターゲットにアクセスできません。これらのイニシエータからの既存の接続は失われ、イニシエータ グループに追加されるまでリカバリできません。現在のイニシエータ接続を確認し、すべての認証済みイニシエータがイニシエータ グループに追加されているようにする必要があります。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
 - a vSAN で [iSCSI ターゲット サービス] をクリックします。
 - b [イニシエータ グループ] タブをクリックして、[追加] をクリックします。[新しいイニシエータ グループ] ダイアログ ボックスが表示されます。
 - c iSCSI イニシエータ グループの名前を入力します。
 - d (オプション) イニシエータ グループにメンバーを追加するには、各メンバーの IQN を入力します。次のフォーマットを使用して、メンバーの IQN を入力します。

iqn.YYYY-MM.domain:name

ここで、

- YYYY = 年 (2016 など)
- MM = 月 (09 など)
- domain = イニシエータが存在するドメイン
- name = メンバー名 (オプション)

- 3 [OK] または [作成] をクリックします。

次のステップ

iSCSI イニシエータ グループにメンバーを追加します。

vSAN iSCSI イニシエータ グループへのターゲットの割り当て

vSAN iSCSI ターゲットを iSCSI イニシエータ グループに割り当てることができます。

イニシエータ グループのメンバーであるイニシエータのみが割り当てられたターゲットにアクセスできます。

前提条件

既存の iSCSI イニシエータ グループがあることを確認します。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
 - a vSAN で [iSCSI ターゲット サービス] をクリックします。
 - b [イニシエータ グループ] タブを選択します。
 - c [アクセス可能なターゲット] セクションで [追加] をクリックします。[アクセス可能なターゲットの追加] ダイアログ ボックスが表示されます。
 - d 使用可能なターゲットのリストからターゲットを選択します。

3 [追加] をクリックします。

vSAN iSCSI ターゲット サービスをオフにする

vSAN iSCSI ターゲット サービスをオフにできます。

vSAN iSCSI ターゲット サービスをオフにしても、LUN/ターゲットは削除されません。領域を再利用する場合は、vSAN iSCSI ターゲット サービスをオフにする前に、LUN/ターゲットを手動で削除してください。

前提条件

iSCSI ターゲット サービスをオフにすると、iSCSI LUN で実行されているワークロードが停止します。オフにする前に、iSCSI LUN 上で実行されているワークロードがないことを確認します。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [サービス] の順にクリックします。
- 2 [vSAN iSCSI ターゲット サービス] 行で、[編集] をクリックします。
[vSAN iSCSI ターゲット サービスを編集] ウィザードが開きます。
- 3 [vSAN iSCSI ターゲット サービスを有効化] スライダをクリックしてオフにし、[適用] をクリックします。

結果

vSAN iSCSI ターゲット サービスが有効になっていません。

次のステップ

vSAN iSCSI ターゲット サービスの監視

iSCSI ターゲット サービスを監視して、iSCSI ターゲット コンポーネントの物理的な配置を表示し、障害が発生したコンポーネントを確認することができます。

iSCSI ターゲット サービスの健全性ステータスを監視することもできます。

前提条件

vSAN iSCSI ターゲット サービスを有効にしたことと、ターゲットと LUN を作成したことを確認します。

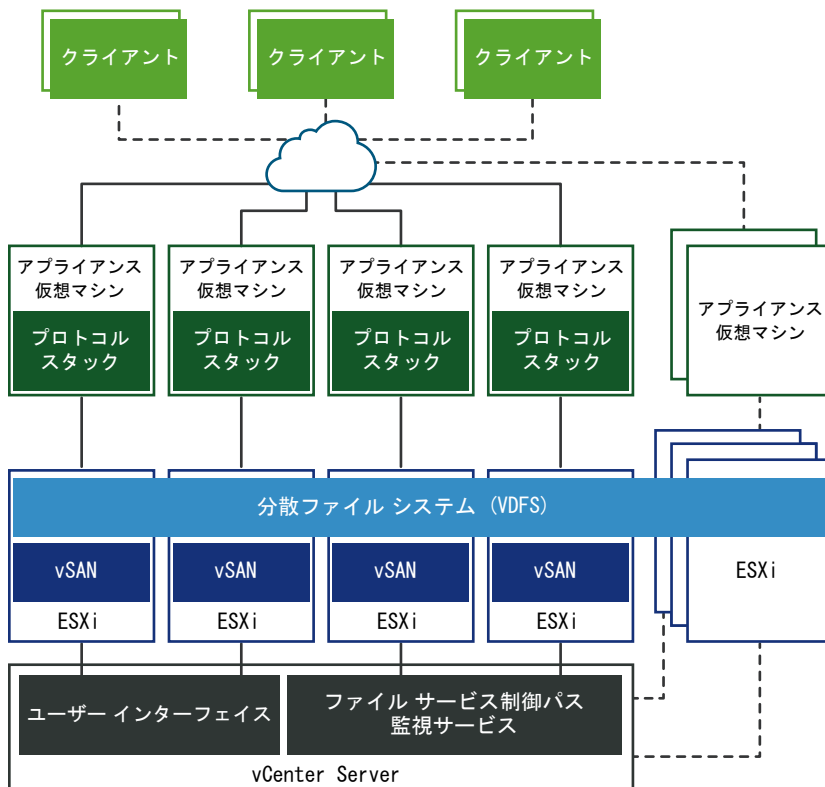
手順

- 1 vSAN クラスタを参照します。
- 2 [監視] をクリックして、[仮想オブジェクト] を選択します。ページに iSCSI ターゲットが一覧表示されます。
- 3 ターゲットを選択して、[配置の詳細の表示] をクリックします。[物理的な配置] に、ターゲットのデータ コンポーネントの配置場所が表示されます。
- 4 [ホスト配置別のグループ コンポーネント] をクリックして、iSCSI データ コンポーネントに関連付けられたホストを表示します。

vSAN ファイル サービス

vSAN ファイル サービスを使用して、クライアント ワークステーションまたは仮想マシンがアクセスできる vSAN データストアにファイル共有を作成します。

ファイル共有に保存されているデータには、アクセス権を持つ任意のデバイスからアクセスできます。vSAN ファイル サービスは vSAN の上にあるレイヤーで、ファイル共有を提供します。現在、SMB、NFSv3、NFSv4.1 ファイル共有をサポートしています。vSAN ファイル サービスは vSAN 分散ファイル システム (vDFS) とストレージ サービス プラットフォームで構成されています。vDFS は、vSAN オブジェクトを集約して基盤となるスケーラブルなファイル システムを提供します。ストレージ サービス プラットフォームは、回復力の高いファイル サーバ エンドポイントと展開、管理、監視を行う制御プレーンを提供します。ファイル共有は、シェアごとに既存の vSAN ストレージ ポリシー ベースの管理と統合されます。vSAN ファイル サービスでは、vSAN クラスタにファイル共有を直接ホストできます。



vSAN ファイル サービスを構成すると、vSAN は内部管理用として単一の VDFS 分散ファイル システムをクラスタに作成します。各ホストにファイル サービス仮想マシン (FSVM) が配置されます。FSVM は、vSAN データストアのファイル共有を管理します。各 FSVM には、NFS と SMB の両方のサービスを提供するファイル サーバが含まれています。

ファイル サービス ワークフローが有効になっている間、入力として固定 IP アドレス プールが提供されます。IP アドレスの1つがプライマリ IP アドレスとして使用されます。プライマリ IP アドレスは、SMB および NFSv4.1 リファラブルでファイル サービス クラスタ内のすべての共有にアクセスする場合に使用されます。IP アドレス プールで指定された IP アドレスごとにファイル サーバが起動します。ファイル共有は、1つのファイル サーバでのみエクスポートされます。ただし、ファイル共有は、すべてのファイル サーバ間で均等に分散されます。アクセス要求の管理に役立つコンピューティング リソースを提供するには、IP アドレスの数を vSAN クラスタ内のホストの数と同じにする必要があります。

vSAN ファイル サービスは、vSAN ストレッチ クラスタと 2 ノード vSAN クラスタをサポートします。2 ノード vSAN クラスタでは、2 台のデータ ノード サーバを同じ場所またはオフィスに配置し、リモートまたは共有の場所に監視ホストを配置する必要があります。

クラウド ネイティブ ストレージ (CNS) ファイル ポリユームの詳細については、VMware vSphere コンテナ ストレージ プラグインのドキュメントと『vSphere with Tanzu の構成と管理』を参照してください。

vSAN ファイル サービスの制限事項と考慮事項

vSAN ファイル サービスを構成するときは、次の点を考慮してください。

- vSAN 8.0 では、2 ノード構成とストレッチ クラスタがサポートされます。
- vSAN 8.0 では、64 台のホスト環境で 64 台のファイル サーバがサポートされます。
- vSAN 8.0 では、100 個のファイル共有がサポートされます。
- vSAN 8.0 Update 2 では、Express Storage Architecture (ESA) のファイル サービスがサポートされません。
- vSAN 8.0 Update 3 の ESA クラスタは 250 個のファイル共有をサポートします。250 個のファイル共有のうち、最大 100 個のファイル共有を SMB にできます。たとえば、100 個の SMB ファイル共有を作成した場合、クラスタでサポートされる追加の NFS ファイル共有は 150 個です。
- vSAN ファイル サービスは、次のものをサポートしていません。
 - ドメイン参加での読み取り専用ドメイン コントローラ (RODC)。RODC はマシン アカウントを作成できません。セキュリティのベスト プラクティスとして、専用の組織単位を Active Directory に事前に作成しておく必要があります。また、ここで説明しているユーザー名がこの組織を制御している必要があります。
 - 結合していない名前空間。
 - マルチ ドメインと単一 Active Directory フォレスト環境。
- ホストがメンテナンス モードに切り替わると、ファイル サーバが別の FSVM に移動します。メンテナンス モードに切り替わると、ホストの FSVM がパワーオフされます。ホストのメンテナンス モードを終了すると、FSVM がパワーオンされます。
- vSAN ファイル サービス仮想マシン (FSVM) Docker の内部ネットワークが、ユーザー ネットワークと重複していても、警告や再構成が行われないことがあります。

指定されたファイル サービス ネットワークが Docker の内部ネットワーク (172.17.0.0/16) と重複している場合、既知の競合問題が発生します。これにより、正しいエンドポイントに対するトラフィックでルーティングの問題が発生します。

回避策として、Docker 内部ネットワーク (172.17.0.0/16) と重複しないように、別のファイル サービス ネットワークを指定します。

vSAN ファイル サービスの有効化

vSAN ファイル サービスは、vSAN Original Storage Architecture (OSA) クラスタまたは vSAN Express Storage Architecture (ESA) クラスタで有効にできます。

前提条件

vSAN ファイル サービスを有効にする前に、次のものが構成されていることを確認します。

- vSAN クラスタは、通常の vSAN クラスタ、vSAN ストレッチ クラスタ、または vSAN ROBO クラスタである必要があります。
- vSAN クラスタ内のすべての ESXi ホストが、次の最小ハードウェア要件を満たしている必要があります。
 - 4 コア CPU
 - 16 GB の物理メモリ
- ネットワークを vSAN ファイル サービス ネットワークとして準備する必要があります。
 - 標準スイッチ ベースのネットワークを使用している場合、vSAN ファイル サービス有効化プロセスで無作為検出モードと偽装転送が有効になります。
 - DVS ベースのネットワークを使用している場合、vSAN ファイル サービスは DVS バージョン 6.6.0 以降でサポートされています。DVS で vSAN ファイル サービス用の専用ポート グループを作成します。MacLearning と偽装転送は、指定された DVS ポート グループの vSAN ファイル サービス有効化プロセスで有効になります。
- **重要:** NSX ベースのネットワークを使用している場合は、NSX 管理コンソールで指定のネットワーク エンティティで MacLearning が有効になっており、すべてのホストとファイル サービス ノードが目的の NSX-T ネットワークに接続していることを確認します。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [サービス] の順にクリックします。

2 [ファイル サービス] 行で [有効化] をクリックします。

[ファイル サービスを有効にする] ウィザードが開きます。

Enable File Service

i vSAN file service is supported on DVS version 6.6.0 or higher. Create a dedicated port group for vSAN file service in the DVS Promiscuous Mode and Forged Transmits are enabled as part of the vSAN file service enablement process for provided network entity. If NSX based networks are being used, ensure that similar settings are configured for the provided network entity from the NSX admin console.

Network

Network **VM NETWORK**

File service agent

Automatically load latest OVF

Let the system download the OVF from: http://buildweb.eng.vmware.com/sb/api/67089532/deliverable/?file=publish/vdfs-fsvm/VMware-vSAN-File-Services-Appliance-8.0.2.1000-67089532_OVF10.ovf

i The system will verify and download the OVF. You can monitor the process in the task panel.

Manually load OVF

Files: **BROWSE**

CANCEL **ENABLE**

3 [選択] ドロップダウンからネットワークを選択します。

- 4 [ファイル サービス エージェント] で、次のいずれかのオプションを選択し、OVF ファイルをダウンロードします。

オプション	説明
最新の OVF を自動的に読み込む	<p>このオプションを選択すると、システムによって OVF が検索され、ダウンロードされます。</p> <hr/> <p>注：</p> <ul style="list-style-type: none"> ■ vCenter Server が次の Web サイトにアクセスして適切な JSON ファイルをダウンロードできるようにプロキシとファイアウォールが構成されていることを確認します。 <p>https://download3.vmware.com/software/VSANOVF/FsOvfMapping.json</p> <p>vCenter Server の DNS、IP アドレス、プロキシ設定の構成の詳細については、『vCenter Server Appliance の構成』を参照してください。</p> <ul style="list-style-type: none"> ■ [現在の OVF を使用する]：すでに利用可能な OVF を使用できます。 ■ [最新の OVF を自動的に読み込む]：最新の OVF を自動的に検索し、ダウンロードできます。
OVF を手動で読み込む	<p>このオプションでは、ローカル システムで使用可能な OVF を検索して選択します。</p> <hr/> <p>注： このオプションを選択する場合は、次のすべてのファイルをアップロードする必要があります。</p> <ul style="list-style-type: none"> ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.mf ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x_OVF10.cert ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x-system.vmdk ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-cloud-components.vmdk ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-log.vmdk ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.ovf

- 5 [有効化] をクリックします。

結果

- OVF がダウンロードされ、展開されます。
- vSAN ファイル サービスが有効になります。
- 各ホストにファイル サービス仮想マシン (FSVM) が配置されます。

注： FSVM は、vSAN ファイル サービスによって管理されます。FSVM で操作を実行しないでください。

vSAN ファイル サービスの構成

ファイル サービスを構成すると、vSAN データストアにファイル共有を作成できます。

前提条件

vSAN ファイル サービスを構成する前に、次のことを確認してください。

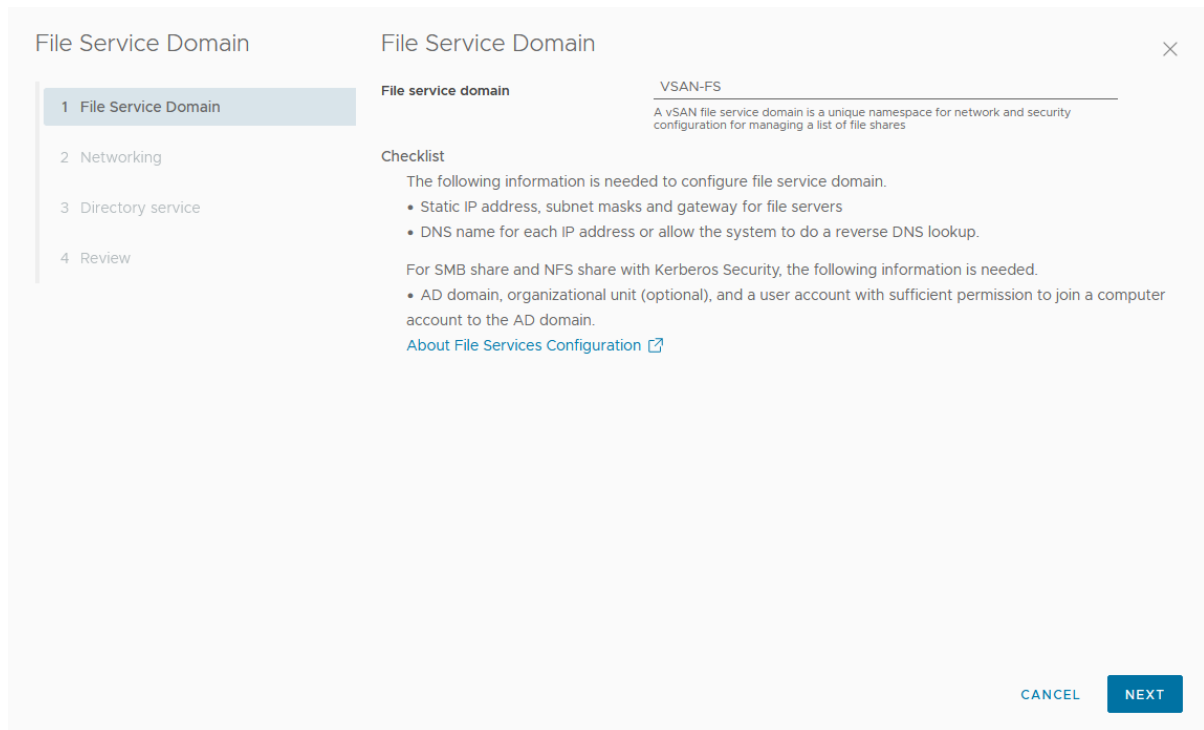
- vSAN ファイル サービスを有効にします。
- vSAN ファイル サービス ネットワークからファイル サーバの IP アドレスとして固定 IP アドレスを割り当てます。各 IP アドレスは、vSAN ファイル共有への単一のアクセス ポイントになります。
 - 最適なパフォーマンスを実現するには、IP アドレスの数は vSAN クラスタ内のホスト数と同じにする必要があります。
 - すべての固定 IP アドレスは、同じサブネットのアドレスにする必要があります。
 - 各固定 IP アドレスには FQDN が対応しています。これは、DNS サーバの正引き参照ゾーンと逆引きゾーンの一部にする必要があります。
- Kerberos ベースの SMB ファイル共有または Kerberos ベースの NFS ファイル共有を作成する場合は、次のものがが必要です。
 - Kerberos セキュリティで SMB ファイル共有または NFS ファイル共有を作成する場合は、認証を行う Active Directory (AD) ドメイン。
 - (オプション) すべてのファイル サーバ コンピュータ オブジェクトを作成する Active Directory 組織単位。
 - コンピュータ オブジェクトの作成および削除を行うために適切な権限を持つディレクトリ サービスのドメイン ユーザー。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [サービス] の順にクリックします。

2 [ファイル サービス] 行で [ドメインの構成] をクリックします。

[ファイル サービス ドメイン] ウィザードが開きます。



3 [ファイル サービス ドメイン] ページで、固有の名前空間を入力して、[次へ] をクリックします。ドメイン名は 2 文字以上にする必要があります。最初の文字は英字または数字にする必要があります。残りの文字には、英字、数字、アンダースコア (_)、ピリオド (.), ハイフン (-) を使用できます。

4 [ネットワーク] ページで次の情報を入力して、[次へ] をクリックします。

- [プロトコル]: IPv4 または IPv6 を選択できます。vSAN ファイル サービスは、IPv4 または IPv6 スタックのみをサポートします。IPv4 と IPv6 間の再構成はサポートされていません。
- [DNS サーバ]: ファイル サービスが適切に構成されるように、有効な DNS サーバを入力することを確認します。
- [DNS サフィックス]: ファイル サービスで使用される DNS サフィックスを指定します。これらのファイル サーバにアクセスするためにクライアントが使用する他の DNS サフィックスもすべて含める必要があります。ファイル サービスは、app、wiz、com など、単一ラベルの DNS ドメインをサポートしていません。ファイル サービスに指定するドメイン名は、thisdomain.registerdrootdnsname の形式にする必要があります。DNS 名とサフィックスは、[<https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/plan/selecting-the-forest-root-domain>] に記載されているベストプラクティスに準拠している必要があります。
- [サブネット マスク]: 有効なサブネット マスクを入力します。このテキスト ボックスは、IPv4 を選択すると表示されます。
- [プリフィックス長]: 1 ~ 128 の数値を入力します。このテキスト ボックスは、IPv6 を選択すると表示されます。
- [ゲートウェイ]: 有効なゲートウェイを入力します。

- [IP アドレス プール]: プライマリ IP アドレスと DNS 名を入力します。

vSAN 8.0 Update 3 では、vSAN ESA クラスタは 250 個のファイル共有をサポートします。250 個のファイル共有のうち、最大 100 個のファイル共有を SMB にできます。たとえば、100 個の SMB ファイル共有を作成した場合、クラスタでサポートされる追加の NFS ファイル共有は 150 個です。

vSAN ESA クラスタの各ファイル サーバは最大 25 個のファイル共有をサポートしますが、最大数である 250 個の共有を作成するには、少なくとも 10 個の IP アドレスが必要です。ホストあたりのファイル サーバまたはファイル共有の数が増えると、vSAN ファイル サービスのパフォーマンスに影響する可能性があります。最適なパフォーマンスを実現するには、IP アドレスの数を vSAN クラスタ内のホスト数と同じにする必要があります。

[アフィニティ サイト] オプションは、vSAN ストレッチ クラスタに vSAN ファイル サービスを構成する場合に使用できます。このオプションを使用すると、[優先] または [セカンダリ] サイト上にファイル サーバを配置できます。これは、サイト間トラフィックの遅延を低減する場合に役立ちます。デフォルト値 [いずれか] です。これは、ファイル サーバにサイト アフィニティ ルールが適用されていないことを示しています。

注: クラスタが ROBO クラスタの場合は、アフィニティ サイトの値を [いずれか] に設定されていることを確認します。

サイトの障害イベントが発生すると、そのサイトに関連するファイル サーバがもう一方のサイトにフェイルオーバーします。リカバリ時にファイル サーバが関連サイトにフェイルバックします。特定のサイトでより多くのワークロードが予想される場合は、1 つのサイトにより多くのファイル サーバを構成します。

注: ファイル サーバに SMB ファイル共有が含まれている場合、サイト障害から復旧しても自動的にフェイルバックされません。

IP アドレスと DNS 名を設定する場合は、次の点を考慮してください。

- ファイル サービスを適切に構成するには、[ネットワーク] ページで IP アドレスとして固定アドレスを入力し、これらの IP アドレスのレコードが DNS サーバに存在する必要があります。最適なパフォーマンスを実現するには、IP アドレスの数は vSAN クラスタ内のホスト数と同じにする必要があります。
- クラスタには最大 64 台のホストを含めることができます。大規模クラスタのサポートが構成されている場合は、最大 64 個の IP アドレスを入力できます。
- 次のオプションを使用すると、IP アドレスと DNS サーバ名のテキスト ボックスに自動的に入力することができます。

[自動入力]: このオプションは、[IP アドレス] テキスト ボックスに最初の IP アドレスを入力した後に表示されます。[自動入力] オプションをクリックすると、最初の行で指定した IP アドレスのサブネット マスクとゲートウェイアドレスに基づいて、残りのフィールドに一連の IP アドレスが自動的に入力されます。自動的に入力された IP アドレスを編集できます。

[ルックアップ DNS] : このオプションは、[IP アドレス] テキスト ボックスに最初の IP アドレスを入力した後に表示されます。[ルックアップ DNS] オプションをクリックすると、[IP アドレス] 列の IP アドレスに対応する FQDN が自動的に取得されます。

注 :

- FQDN には、すべての有効なルールが適用されます。詳細については、[<https://tools.ietf.org/html/rfc953>] を参照してください。
- FQDN の最初の部分 (NetBIOS 名) は 15 文字以内にする必要があります。

次の場合にのみ、FQDN が自動的に取得されます。

- [ドメイン] ページで有効な DNS サーバを入力している。
- [IP アドレス プール] ページで IP アドレスとして固定アドレスを入力し、これらの IP アドレスのレコードが DNS サーバに存在している。

5 [ディレクトリ サービス] ページで次の情報を入力して、[次へ] をクリックします。

オプション	説明
[ディレクトリ サービス]	認証用の Active Directory ドメインを vSAN ファイル サービスに構成します。Kerberos 認証を使用して SMB ファイル共有または NFSv4.1 ファイル共有を作成する場合は、vSAN ファイル サービスに Active Directory ドメインを構成する必要があります。
[Active Directory ドメイン]	ファイル サーバが参加している完全修飾ドメイン名。
[優先 Active Directory サーバ]	優先 Active Directory サーバの IP アドレスを入力します。IP アドレスが複数ある場合は、カンマで区切って入力する必要があります。
[組織単位 (オプション)]	vSAN ファイル サービスによって作成されるコンピュータ アカウントが含まれます。組織の階層が複雑な場合は、スラッシュで階層を表し、指定したコンテナにコンピュータ アカウントを作成します (例 : organizational_unit/inner_organizational_unit)。 注 : デフォルトでは、vSAN ファイル サービスはコンピュータ コンテナにコンピュータ アカウントを作成します。

オプション	説明
[Active Directory ユーザー名]	<p>Active Directory サービスの接続と構成に使用されるユーザー名。このユーザー名は、ドメインの Active Directory の認証を行います。ドメイン ユーザーは、ドメイン コントローラに対して認証を行い、vSAN ファイル サービスのコンピュータ アカウント、関連する SPN エントリ、DNS エントリ (Microsoft DNS を使用する場合) を作成します。ベスト プラクティスとして、ファイル サービスに専用のサービス アカウントを作成します。</p> <p>コンピュータ オブジェクトの作成および削除を行うために適切な以下の権限を持つディレクトリ サービスのドメイン ユーザー。</p> <ul style="list-style-type: none"> ■ (オプション) DNS エントリの追加/更新
[パスワード]	<p>ドメインの Active Directory のユーザー名のパスワード。vSAN ファイル サービスは、パスワードを使用して Active Directory に対する認証を行い、vSAN ファイル サービスのコンピュータ アカウントを作成します。</p>

注：

- vSAN ファイル サービスは、次のものをサポートしていません。
 - ドメイン参加での読み取り専用ドメイン コントローラ (RODC)。RODC はマシン アカウントを作成できません。セキュリティのベスト プラクティスとして、専用の組織単位を Active Directory に事前に作成しておく必要があります。また、ここで説明しているユーザー名がこの組織を制御している必要があります。
 - 結合していない名前空間。
 - マルチ ドメインと単一 Active Directory フォレスト環境。
- Active Directory のユーザー名には英字のみを使用できます。
- 単一の Active Directory ドメイン構成のみがサポートされています。ただし、有効な DNS サブドメインにファイル サーバを配置できます。たとえば、example.com という名前の Active Directory ドメインでは、ファイル サーバの FQDN を name1.eng.example.com として指定できます。
- ファイル サーバに事前作成されたコンピュータ オブジェクトはサポートされていません。ここで指定したユーザーに、組織単位に対する適切な権限があることを確認します。
- Active Directory が DNS サーバとしても使用され、DNS レコードの更新に十分な権限がユーザーにある場合、ファイル サーバの DNS レコードは vSAN ファイル サービスによって更新されます。vSAN ファイル サービスには、ファイルサーバの正引き/逆引き参照が正しく機能しているかどうかを確認できる健全性チェックがあります。ただし、DNS サーバとして独自のソリューションを使用している場合は、それらの DNS レコードを Vi 管理者が更新する必要があります。

6 設定内容を確認して、[終了] をクリックします。

結果

ファイル サービス ドメインが構成されます。ファイル サーバが、vSAN ファイル サービスの構成プロセスで割り当てられた IP アドレスを使用して起動します。

vSAN ファイル サービスの編集

vSAN ファイル サービスの設定を編集したり、再構成することができます。

前提条件

- vSAN 7.0 から 7.0 Update 1 にアップグレードする場合は、SMB および NFS の Kerberos ファイル共有を作成できます。これには、vSAN ファイル サービスに Active Directory ドメインを構成する必要があります。
- アクティブな共有がある場合、Active Directory ドメインの変更はできません。このアクションを実行すると、アクティブな共有のユーザー権限が損なわれる可能性があります。
- Active Directory のパスワードが変更されている場合は、Active Directory の設定を編集して、新しいパスワードを入力できます。

注： この操作により、ファイル共有で実行中の I/O が若干中断する可能性があります。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [サービス] の順にクリックします。
- 2 [ファイル サービス] 行で[編集]> [ドメインを編集] をクリックします。
[ファイル サービス ドメイン] ウィザードが開きます。
- 3 [ファイル サービス ドメイン] ページで、ファイル サービスのドメイン名を編集し、[次へ] をクリックします。
- 4 [ネットワーク] ページで、適切な構成変更を行い、[次へ] をクリックします。プライマリ IP アドレス、固定 IP アドレス、DNS 名を編集できます。プライマリ IP アドレスまたは固定 IP アドレスを追加または削除できます。IP アドレスを変更せずに DNS 名を変更することはできません。

注： ドメイン情報の変更は、中断操作です。ファイル共有に再接続する際に、すべてのクライアントで新しい URL の使用が必要になる場合があります。

- 5 [ディレクトリ サービス] ページで、ディレクトリに関連する適切な変更を行い、[次へ] をクリックします。

注： vSAN ファイル サービスを最初に構成した後、Active Directory ドメイン、組織単位、ユーザー名を変更することはできません。

- 6 [確認] ページで、必要な変更を行った後、[終了] をクリックします。

結果

変更が vSAN ファイル サービス構成に適用されます。

vSAN ファイル共有の作成

vSAN ファイル サービスが有効になっている場合、vSAN データストアに 1 つ以上のファイル共有を作成できます。

vSAN ファイル サービスでは、ESXi で NFS ファイル共有を使用できません。

前提条件

Kerberos セキュリティで SMB ファイル共有または NFSv4.1 ファイル共有を作成している場合は、Active Directory ドメインに vSAN ファイル サービスを構成していることを確認します。

[共有名と使用量に関する考慮事項]

- ASCII 以外の文字を含むユーザー名を使用して共有データにアクセスできます。
- 共有名は 80 文字以内にする必要があります。英字、数字、ハイフン文字を使用できます。ハイフンの前後には数字またはアルファベットが必要です。ハイフンを連続して使用することはできません。
- SMB タイプの共有の場合、ファイルとディレクトリに Unicode 対応の文字列を含めることができます。
- 純粋な NFSv4 タイプの共有の場合、ファイルとディレクトリに UTF-8 対応の文字列を含めることができます。
- 純粋な NFSv3 タイプと NFSv3+NFSv4 タイプの共有の場合、ファイルとディレクトリに ASCII 対応の文字列のみを含めることができます。
- 古い NFSv3 から NFSv4 のみの新しい vSAN ファイル サービス共有に移行するには、すべてのファイルとディレクトリの名前を UTF-8 エンコードに変換する必要があります。この操作は、別のサードパーティ ツールで行うこともできます。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [ファイル共有] の順にクリックします。

vSAN 8.0 Update 3 では、vSAN ESA クラスタは 250 個のファイル共有をサポートします。250 個のファイル共有のうち、最大 100 個のファイル共有を SMB にできます。たとえば、100 個の SMB ファイル共有を作成した場合、クラスタでサポートされる追加の NFS ファイル共有は 150 個です。

vSAN ESA クラスタの各ファイル サーバは最大 25 個のファイル共有をサポートしますが、最大数である 250 個の共有を作成するには、少なくとも 10 個の IP アドレスが必要です。ホストあたりのファイル サーバまたはファイル共有の数が増えると、vSAN ファイル サービスのパフォーマンスに影響する可能性があります。最適なパフォーマンスを実現するには、IP アドレスの数は vSAN クラスタ内のホスト数と同じにする必要があります。

- 2 [追加] をクリックします。

[ファイル共有の作成] ウィザードが開きます。

- 3 [全般] ページで次の情報を入力して、[次へ] をクリックします。

- [名前]: ファイル共有の名前を入力します。
- [プロトコル]: 適切なプロトコルを選択します。vSAN ファイル サービスでは、SMB および NFS ファイル システム プロトコルがサポートされています。

[SMB] プロトコルを選択した場合、[プロトコルの暗号化] オプションを使用して、暗号化されたデータのみを受け入れるように SMB ファイル共有を構成することもできます。

[NFS] プロトコルを選択した場合、[NFS 3]、[NFS 4]、または [NFS 3 と NFS 4] のいずれかをサポートするようにファイル共有を構成できます。[NFS 4] を選択すると、[AUTH_SYS] または [Kerberos] のいずれかのセキュリティを設定できます。

注： SMB プロトコルと NFS プロトコルの Kerberos セキュリティは、vSAN ファイル サービスが Active Directory で構成されている場合にのみ構成できます。詳細については、「[vSAN ファイル サービスの構成](#)」を参照してください。

- SMB プロトコルを使用している場合、共有クライアント ユーザーは、[アクセス ベースの列挙] オプションを使用して、権限のないファイルとフォルダを非表示にできます。
 - [ストレージ ポリシー]：適切なストレージ ポリシーを選択します。
 - [アフィニティ サイト]：vSAN ストレッチ クラスタにファイル共有を作成する場合は、このオプションを使用できます。このオプションは、選択したサイトに属するファイル サーバ上にファイル共有を配置する場合に役立ちます。このオプションは、ファイル共有へのアクセスで遅延を少なくしたい場合に使用します。デフォルト値は [いずれか] です。この場合、ファイル共有が優先サイトまたはセカンダリ サイトのいずれかで、トラフィックの少ないサイトに配置されます。
 - [ストレージ容量の割り当て]：次の値を設定できます。
 - [共有に関する警告しきい値]：共有がこのしきい値に到すると、警告メッセージが表示されます。
 - [ハードの割り当ての共有]：共有がこのしきい値に達すると、新しいブロックの割り当てが拒否されず。
 - [ラベル]：ラベルは、ファイル共有の整理に役立つキーと値のペアです。各ファイル共有にラベルを添付し、そのラベルに基づいてフィルタを適用できます。ラベル キーは 1 ～ 250 文字の文字列です。ラベル値は文字列で、ラベル値の長さは 1,000 文字未満にする必要があります。vSAN ファイル サービスでは、共有ごとに最大 5 個のラベルを使用できます。
- 4 [ネットのアクセス コントロール] ページには、ファイル共有へのアクセスを定義するオプションが表示されません。ネットワーク アクセス コントロール オプションは、NFS 共有でのみ使用できます。次のいずれかのオプションを選択し、[次へ] をクリックします。
- [アクセスなし]：任意の IP アドレスからファイル共有にアクセスできないようにするには、このオプションを選択します。
 - [任意の IP アドレスからのアクセスを許可]：すべての IP アドレスからファイル共有にアクセスできるようにするには、このオプションを選択します。
 - [ネット アクセスのカスタマイズ]：特定の IP アドレスの権限を定義するには、このオプションを選択します。このオプションを使用すると、ファイル共有に対する特定の IP アドレスの権限（アクセス、変更または読み取り専用）を指定できます。また、各 IP アドレスの [ルート スカッシュ] を有効にすることもできます。IP アドレスは次の形式で入力します。
 - 単一の IP アドレス。例：123.23.23.123
 - IP アドレスとサブネット マスク例：123.23.23.0/8
 - 範囲。開始 IP アドレスと終了 IP アドレスをハイフン (-) で区切って指定します。例：
123.23.23.123-123.23.23.128

- アスタリスク (*)。すべてのクライアントを表します。

5 [確認] ページで設定を確認し、[終了] をクリックします。

vSAN データストアに新しいファイル共有が作成されます。

vSAN ファイル共有の表示

vSAN ファイル共有のリストを表示できます。

vSAN ファイル共有のリストを表示するには、vSAN クラスタに移動し [構成] > [vSAN] > [ファイル サービスの共有] の順にクリックします。

vSAN ファイル共有のリストが表示されます。ファイル共有ごとに、ストレージ ポリシー、ハードの割り当て、割り当て超過、実際の使用量などの情報を確認できます。vSAN ESA クラスタには、既存のファイル共有の数と、クラスタで許可されているファイル共有の上限が表示されます。

vSAN ファイル共有へのアクセス

ホスト クライアントからファイル共有にアクセスできます。

NFS ファイル共有へのアクセス

NFS ファイル システムと通信するオペレーティング システムを使用して、ホスト クライアントからファイル共有にアクセスできます。RHEL ベースの Linux ディストリビューションの場合、NFS 4.1 のサポートは、カーネル 3.10.0-514 以降を実行している RHEL 7.3 と CentOS 7.3-1611 で利用できます。Debian ベースの Linux ディストリビューションの場合、NFS 4.1 サポートは Linux カーネル バージョン 4.0.0 以降で利用できます。

NFSv4.1 が動作するには、すべての NFS クライアントに一意的ホスト名が必要です。プライマリ IP アドレスを指定して Linux マウント コマンドを実行し、vSAN のファイル共有をクライアントにマウントできます。例 : `mount -t nfs4 -o minorversion=1,sec=sys <primary ip>:/vsanfs/<share name>` NFSv3 サポートは、RHEL ベースと Debian ベースの Linux ディストリビューションで使用できます。Linux の `mount` コマンドを実行し、vSAN のファイル共有をクライアントにマウントできます。例 : `mount -t nfs vers=3 <nfsv3_access_point> <localmount_point>`。

例

ホスト クライアントから NFS ファイル共有を検証するための v41 コマンドのサンプル :

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=sys <primary ip address>:/vsanfs/
TestShare-0 /mnt/TestShare-0
[root@localhost ~]# cd /mnt/TestShare-0/
[root@localhost TestShare-0]# mkdir bar
[root@localhost TestShare-0]# touch foo
[root@localhost TestShare-0]# ls -l
total 0
drwxr-xr-x. 1 root root 0 Feb 19 18:35 bar
-rw-r--r--. 1 root root 0 Feb 19 18:35 foo
```

NFS Kerberos ファイル共有へのアクセス

NFS Kerberos 共有にアクセスする Linux クライアントには、有効な Kerberos チケットが必要です。

[ホスト クライアントから NFS Kerberos ファイル共有を検証するための v41 コマンドのサンプル:]

NFS Kerberos 共有をマウントするには、次のマウント コマンドを使用します。

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=krb5/krb5i/krb5p <primary ip address>:/vsanfs/TestShare-0 /mnt/TestShare-0
[root@localhost ~]# cd /mnt/TestShare-0/
[root@localhost TestShare-0]# mkdir bar
[root@localhost TestShare-0]# touch foo
[root@localhost TestShare-0]# ls -l
total 0
drwxr-xr-x. 1 root root 0 Feb 19 18:35 bar
-rw-r--r--. 1 root root 0 Feb 19 18:35 foo
```

[NFS Kerberos 共有の所有権の変更]

共有の所有権を変更するには、Active Directory ドメインのユーザー名でログインする必要があります。ファイルサービスの構成で指定された Active Directory ドメインのユーザー名は、Kerberos ファイル共有の sudo ユーザーとして機能します。

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=sys <primary ip address>:/vsanfs/TestShare-0 /mnt/TestShare-0
[fsadmin@ocalhost ~]# chown user1 /mnt/TestShare-0
[user1@localhost ~]# ls -l /mnt/TestShare-0
total 0
drwxr-xr-x. 1 user1 domain users 0 Feb 19 18:35 bar
-rw-r--r--. 1 user1 domain users 0 Feb 19 18:35 foo
```

SMB ファイル共有へのアクセス

Windows クライアントから SMB ファイル共有にアクセスできます。

前提条件

Windows クライアントが vSAN ファイル サービスで構成されている Active Directory ドメインに参加していることを確認します。

手順

- 1 次の手順で SMB ファイル共有のパスをコピーします。
 - a vSAN クラスタに移動し、[構成] > [vSAN] > [ファイル サービスの共有] の順にクリックします。すべての vSAN ファイル共有のリストが表示されます。
 - b Windows クライアントからアクセスする SMB ファイル共有を選択します。
 - c [コピー パス] > [SMB] の順にクリックします。SMB ファイル共有のパスがクリップボードにコピーされます。
- 2 通常の Active Directory ドメイン ユーザーとして Windows クライアントにログインします。
- 3 コピーしたパスを使用して、SMB ファイル共有にアクセスします。

vSAN ファイル共有の編集

vSAN ファイル共有の設定を編集できます。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [ファイル サービスの共有] の順にクリックします。
すべての vSAN ファイル共有のリストが表示されます。
- 2 変更するファイル共有を選択し、[編集] をクリックします。
- 3 [ファイル共有の編集] ページで、ファイル共有の設定に適切な変更を行い、[終了] をクリックします。

結果

ファイル共有の設定が更新されます。

注： vSAN では、SMB と NFS 間のファイル共有プロトコルの変更はできません。

vSAN クラスタでの SMB ファイル共有の管理

vSAN ファイル サービスは、Microsoft 管理コンソール (MMC) の共有フォルダ スナップインをサポートし、vSAN クラスタの SMB 共有を管理します。

MMC ツールを使用して、vSAN ファイル システムの SMB 共有に次のタスクを実行できます。

- アクセス コントロール リスト (ACL) を管理します。
- 開いているファイルを閉じます。
- アクティブなセッションを表示します。
- 開いているファイルを表示します。
- クライアント接続を閉じます。

手順

- 1 次の手順で MMC コマンドをコピーします。
 - a vSAN クラスタに移動し、[構成] > [vSAN] > [ファイル サービスの共有] の順にクリックします。
すべての vSAN ファイル共有のリストが表示されます。
 - b MMC ツールを使用して、Windows クライアントから管理する SMB ファイル共有を選択します。
 - c [MMC コマンドのコピー] をクリックします。
クリップボードに MMC コマンドがコピーされます。
- 2 Windows クライアントにファイル サービス管理者ユーザーとしてログインします。ファイル サービス ドメインを作成すると、ファイル サービス管理者ユーザーが構成されます。ファイル サービス管理者ユーザーには、ファイル サーバに対するすべての権限が付与されます。
- 3 タスクバーの検索ボックスに「Run」と入力し、[ファイル名を指定して実行] を選択します。

- 4 [ファイル名を指定して実行] ボックスに、コピーした MMC コマンドを入力して、MMC ツールを開き、SMB 共有にアクセスして管理します。

vSAN ファイル共有の削除

不要になったファイル共有を削除できます。

ファイル共有を削除すると、そのファイル共有に関連付けられているスナップショットもすべて削除されます。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [ファイル サービスの共有] の順にクリックします。
すべての vSAN ファイル共有のリストが表示されます。
- 2 変更するファイル共有を選択し、[削除] をクリックします。
- 3 [ファイル共有の削除] ダイアログで、[削除] をクリックします。

vSAN 分散ファイル システムのスナップショット

スナップショットを使用すると、容量を効率的に使用し、時間ベースでデータをアーカイブできます。

ファイルを誤って削除した場合でも、ファイルまたはファイルのセットからデータを取得できます。ファイル システム レベルのスナップショットでは、変更されたファイルとファイルに対する変更の情報が提供されます。自動化されたファイル リカバリ サービスを使用できるので、従来のテープベースのバックアップよりも効率的に作業を行うことができます。このスナップショットだけでは完全なディザスタ リカバリを行うことはできませんが、サードパーティのバックアップ ベンダーが変更されたファイル (増分バックアップ) を別の物理的な場所にコピーするために使用できます。

vSAN ファイル サービスには、vSAN ファイル共有のポイントインタイム イメージを作成できる組み込み機能があります。vSAN ファイル サービスが有効になっている場合、共有ごとに最大で 32 個までのスナップショットを作成できます。vSAN ファイル共有スナップショットは、vSAN ファイル共有のポイントインタイム イメージを提供するファイル システム スナップショットです。

注: vSAN 分散ファイル システムのスナップショットは、バージョン 7.0 Update 2 以降でサポートされていません。

ファイル システムのスナップショットに関する考慮事項

- データを取得するスナップショットの名前として Default を使用します。
- スナップショット名は 100 文字以下にする必要があります。名前には、英字、数字、次のものを除く特殊文字を使用できません。
 - " (ASCII 34)
 - \$ (ASCII 36)
 - % (ASCII 37)
 - & (ASCII 38)
 - * (ASCII 42)

- / (ASCII 47)
- : (ASCII 58)
- < (ASCII 60)
- > (ASCII 62)
- ? (ASCII 63)
- \ (ASCII 92)
- ^ (ASCII 94)
- | (ASCII 124)
- ~ (ASCII 126)

スナップショットの作成

vSAN ファイル サービスを有効にすると、1つまたは複数のスナップショットを作成して、vSAN ファイル共有のポイントインタイム イメージを提供できます。ファイル共有ごとに最大で 32 個のスナップショットを作成できます。

前提条件

vSAN ファイル共有が作成されている必要があります。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [ファイル サービスの共有] の順にクリックします。
vSAN ファイル共有のリストが表示されます。
- 2 スナップショットを作成するファイル共有を選択して、[スナップショット] > [新規スナップショット] の順にクリックします。
[新しいスナップショットの作成] ダイアログが表示されます。
- 3 [新しいスナップショットの作成] ダイアログで、スナップショットの名前を入力して、[作成] をクリックします。

結果

選択したファイル共有のポイントインタイム スナップショットが作成されます。

スナップショットの表示

スナップショットのリストと、スナップショットの作成日時、サイズなどの情報を表示できます。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [ファイル サービスの共有] の順にクリックします。
vSAN ファイル共有のリストが表示されます。
- 2 ファイル共有を選択して、[スナップショット] をクリックします。

結果

そのファイル共有のスナップショットのリストが表示されます。スナップショットの作成日時、サイズなどの情報も表示できます。

スナップショットの削除

不要になったスナップショットを削除できます。

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [ファイル サービスの共有] の順にクリックします。
vSAN ファイル共有のリストが表示されます。
- 2 ファイル共有を選択して、[スナップショット] をクリックします。
選択したファイル共有に属するスナップショットのリストが表示されます。
- 3 削除するスナップショットを選択し、[削除] をクリックします。

vSAN ファイル サービス ホストでのワークロードのリバランス

Skyline Health には、vSAN ファイル サービス インフラストラクチャのすべてのホストについてワークロード バランスの健全性ステータスが表示されます。

ホストのワークロードに不均衡がある場合、ワークロードをリバランスすることで不均衡を修正できます。

前提条件

手順

- 1 vSAN クラスタに移動し、[監視] > [vSAN] > [Skyline Health] の順にクリックします。
- 2 [Skyline Health] で、[ファイル サービス] を展開し、[インフラストラクチャの健全性] をクリックします。
[インフラストラクチャの健全性] タブに、vSAN ファイル サービス インフラストラクチャに含まれるすべてのホストの一覧が表示されます。ホストごとに、ワークロード バランスのステータスが表示されます。ホストのワークロードに不均衡がある場合は、[説明] 列にアラートが表示されます。
- 3 不均衡を修正するには、[不均衡の修正] をクリックして、[リバランス] をクリックします。
リバランスを行う前に、次の点を考慮してください。
 - リバランスの実行中に、ワークロードが不均衡になっているホストのコンテナが別のホストに移動することがあります。リバランスにより、クラスタ内の他のホストに影響を及ぼす可能性があります。
 - リバランス プロセスの進行中、NFS 共有で実行されているワークロードは中断されません。ただし、移動したコンテナにある SMB 共有に対する I/O は中断されます。

結果

ホストのワークロードのバランスが調整されると、ワークロード バランスのステータスが緑色に変わります。

vSAN 分散ファイル システムのマッピング解除による容量の再利用

UNMAP コマンドを使用すると、ゲストが vSAN オブジェクトに作成し、vSAN 分散ファイル システム (VDFS) から削除されたファイルにマッピングされたストレージ容量を再利用できます。

vSAN 6.7 Update 2 以降では、UNMAP コマンドがサポートされます。ファイルとスナップショットを削除すると、ファイル システム内の容量が解放されます。この空き容量は、ファイル システムが解放またはマッピング解除するまで、ストレージ デバイスにマッピングされます。vSAN は、マッピング解除とも呼ばれる空き容量の再利用をサポートしています。ファイル共有とスナップショットの削除、ファイル共有とスナップショットの統合などを行うときに、VDFS のストレージ容量を解放できます。ファイルまたはスナップショットを削除するときに、ストレージ容量のマッピングを解除できます

マッピング解除機能は、デフォルトでは無効です。vSAN クラスタでマッピング解除を有効にするには、次の RVC コマンドを使用します。

```
vsan.unmap_support -enable
```

vSAN クラスタでマッピング解除を有効にするときは、すべての仮想マシンをパワーオフしてからパワーオンする必要があります。マッピング解除操作を実行するには、仮想マシンでバージョン 13 以降の仮想ハードウェアを使用する必要があります。

vSAN ファイル サービスのアップグレード

ファイル サービスのアップグレードは、ローリング ベースで実行されます。

アップグレードの実行中、アップグレード対象の仮想マシン上で実行されているファイル サーバ コンテナは、他の仮想マシンにフェイルオーバーされます。アップグレード中もファイル共有にはアクセスできます。アップグレード中に、ファイル共有へのアクセスが中断することがあります。

前提条件

次のものがアップグレードされていることを確認します。

- ESXi ホスト
- vCenter Server
- vSAN のディスク フォーマット

手順

- 1 vSAN クラスタに移動し、[構成] > [vSAN] > [サービス] の順にクリックします。
- 2 [vSAN サービス] の [ファイル サービス] 行で、[アップグレードの確認] をクリックします。

- 3 [ファイル サービスのアップグレード] ダイアログ ボックスで、次のいずれかの展開オプションを選択して、[アップグレード] をクリックします。

オプション	操作
[自動による方法]	<p>デフォルトのオプションです。このオプションを選択すると、システムによって OVF が検索され、ダウンロードされます。アップグレードを開始した後、このタスクをキャンセルすることはできません。</p> <p>注： vSAN を使用するには、このオプションのインターネット接続が必要です。</p>
[手動による方法]	<p>このオプションでは、ローカル システムで使用可能な OVF を検索して選択します。アップグレードを開始した後、このタスクをキャンセルすることはできません。</p> <p>注： このオプションを選択する場合は、次のすべてのファイルをアップロードする必要があります。</p> <ul style="list-style-type: none"> ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.mf ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.cert ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-system.vmdk ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-cloud-components.vmdk ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-log.vmdk ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.ovf

vSAN ファイル サービスのパフォーマンスの監視

NFS と SMB のファイル共有パフォーマンスを監視できます。

前提条件

vSAN パフォーマンス サービスが有効になっていることを確認します。vSAN パフォーマンス サービスを初めて使用するとき、このサービスを有効にするように警告するメッセージが表示されます。vSAN パフォーマンス サービスの詳細については、『vSAN の監視とトラブルシューティング』を参照してください。

手順

- 1 vSAN クラスタに移動し、[監視] > [vSAN] > [パフォーマンス] の順にクリックします。
- 2 [ファイル共有] タブをクリックします。
- 3 次のオプションのいずれかを選択します。

オプション	操作
[時間の範囲]	<ul style="list-style-type: none"> ■ パフォーマンス レポートを表示する時間数を選択する場合は、[直近] を選択します。 ■ パフォーマンス レポートを表示する日時を選択する場合は、[カスタム] を選択します。 ■ [保存] を選択して、現在の設定を [時間の範囲] リストにオプションとして追加します。
[ファイル共有]	パフォーマンス レポートを生成して表示するファイル共有を選択します。

- 4 [結果を表示] をクリックします。

結果

選択した期間の vSAN ファイル サービスのスループット、IOPS、遅延のメトリックが表示されます。

vSAN パフォーマンス グラフの詳細については、VMware のナレッジベースの記事「<https://kb.vmware.com/s/article/2144493>」を参照してください。

vSAN ファイル共有キャパシティの監視

ネイティブ ファイル共有と CNS で管理されるファイル共有の両方の容量を監視できます。

手順

- 1 vSAN クラスタに移動し、[監視] > [vSAN] > [容量] の順にクリックします。
- 2 [使用量] タブをクリックします。
- 3 [デデュープおよび圧縮前の使用量の内訳] セクションで、[ユーザー オブジェクト] を展開します。

結果

ファイル共有の容量情報が表示されます。

vSAN 容量の監視の詳細については、『vSAN の監視とトラブルシューティング』を参照してください。

vSAN ファイル サービスとファイル共有の健全性の監視

vSAN ファイル サービスとファイル共有オブジェクトの両方の健全性を監視できます。

vSAN ファイル サービスの健全性の表示

vSAN ファイル サービスの健全性を監視できます。

前提条件

vSAN パフォーマンス サービスが有効になっていることを確認します。

手順

- 1 vSAN クラスタに移動し、[監視] > [vSAN] の順にクリックします。
- 2 [Skyline 健全性] セクションで [ファイル サービス] を展開します。
- 3 次のファイル サービスの健全性パラメータをクリックして、ステータスを表示します。

オプション	操作
[インフラストラクチャの健全性]	ファイル サービス インフラストラクチャの健全性ステータスが ESXi ホストごとに表示されます。詳細については、[情報] タブをクリックしてください。
[ファイル サーバの健全性]	ファイル サーバの健全性ステータスが表示されます。詳細については、[情報] タブをクリックしてください。
[共有の健全性]	ファイル サービス共有の健全性が表示されます。詳細については、[情報] タブをクリックしてください。

vSAN ファイル共有オブジェクトの健全性の監視

ファイル共有オブジェクトの健全性を監視できます。

ファイル共有オブジェクトの健全性を表示するには、vSAN クラスタに移動し、[監視] > [vSAN] > [仮想オブジェクト] の順にクリックします。

[配置の詳細の表示] セクションに、名前、識別子または UUID、各仮想マシンで使用されるデバイスの数、ホスト全体でのミラー状況などのデバイス情報が表示されます。

ハイブリッド vSAN クラスタをオールフラッシュ クラスタに移行

ハイブリッド vSAN クラスタ内のディスク グループをオールフラッシュ ディスク グループに移行できます。

vSAN ハイブリッド クラスタは、容量レイヤーに磁気ディスクを、キャッシュ レイヤーにフラッシュ デバイスを使用します。キャッシュ レイヤーと容量レイヤーでフラッシュ デバイスを使用できるように、クラスタ内のディスク グループの構成を変更できます。

注： 手順に従って、ハイブリッド vSAN クラスタを ソリッド ステート ドライブ (Solid State Drive, SSD)、ハイブリッド vSAN クラスタを NVMe、または SSD を NVMe に移行します。

前提条件

- クラスタが使用するすべての vSAN ポリシーで、暗号化サービス、容量効率、およびストレージ階層に [環境設定なし] が指定されていることを確認します。
- すべてのディスク グループがオールフラッシュに変換されるまで、[許容される障害の数] に RAID 1 (ミラーリング) を使用する必要があります。

クラスタを SSD から NVMe または NVMe から SSD に移行する場合、これらの前提条件は適用されません。

手順

- 1 ホスト上のハイブリッド ディスク グループを削除します。
 - a vSphere Client で、vSAN クラスタに移動し、[構成] タブをクリックします。
 - b [vSAN] の下で、[ディスク管理] をクリックします。
 - c [ディスク グループ] の下で、削除するディスク グループを選択し、[...] をクリックしてから、[削除] をクリックします。

移行モードとして [全データの移行] を選択し、[はい] をクリックします。

注： vSAN クラスタ内の各ホストでディスク グループを移行します。

- 2 物理 HDD ディスクをホストから削除します。
- 3 フラッシュ デバイスをホストに追加します。

フラッシュ デバイスにパーティションがないことを確認します。
- 4 オールフラッシュ ディスク グループをホストに作成します。

- 5 すべてのハイブリッド ディスク グループがオールフラッシュ ディスク グループに変換されるまで、各ホストで手順 1 ~ 4 を繰り返します。

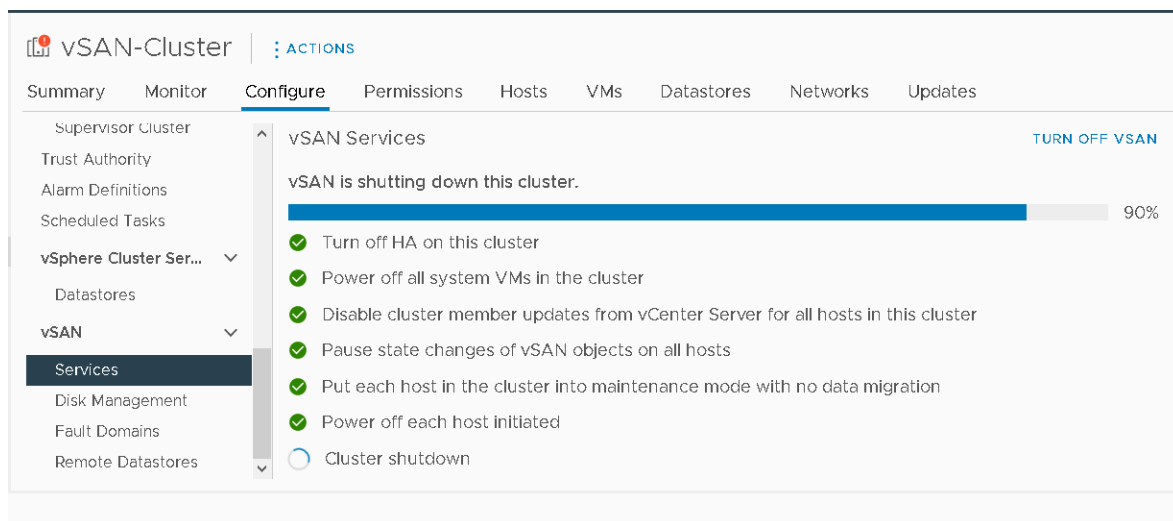
注： ホストでディスクをホットプラグできない場合は、ホストをメンテナンス モードに切り替えてから vSphere Client でディスクを削除します。ホストをシャットダウンして、ディスクをフラッシュ デバイスに置き換えます。次に、ホストをパワーオンしてメンテナンス モードを終了し、新しいディスク グループを作成します。

vSAN クラスタのシャットダウンと再起動

vSAN クラスタ全体をシャットダウンして、メンテナンスやトラブルシューティングを実行できます。

クラスタのシャットダウン ウィザードを使用して、vSAN クラスタをシャットダウンします。ウィザードが必要な手順を実行します。ユーザー アクションが必要な場合はアラートを表示します。必要に応じて、クラスタを手動でシャットダウンすることもできます。

注： vSAN ストレッチ クラスタをシャットダウンしても、監視ホストはアクティブなままになります。



The screenshot shows the vSAN Services configuration page. The left sidebar lists various vSAN components, with 'Services' selected. The main content area displays the 'vSAN Services' configuration, including a progress bar at 90% and a list of actions to be performed during the shutdown process. The actions are:

- Turn off HA on this cluster
- Power off all system VMs in the cluster
- Disable cluster member updates from vCenter Server for all hosts in this cluster
- Pause state changes of vSAN objects on all hosts
- Put each host in the cluster into maintenance mode with no data migration
- Power off each host initiated
- Cluster shutdown

クラスタのシャットダウン ウィザードを使用した vSAN クラスタのシャットダウン

クラスタのシャットダウン ウィザードを使用して、メンテナンスやトラブルシューティングで vSAN クラスタを正常にシャットダウンします。

クラスタのシャットダウン ウィザードは、vSAN 7.0 Update 3 以降のリリースで使用できます。

注： vSphere with Tanzu 環境では、コンポーネントのシャットダウンと起動を所定の順序で行う必要があります。詳細については、『VMware Cloud Foundation 運用ガイド』の「VMware Cloud Foundation のシャットダウンと起動」を参照してください。

手順

- 1 シャットダウンを行う vSAN クラスタを準備します。
 - a vSAN Skyline Health をチェックし、クラスタが良好な状態であることを確認します。
 - b vCenter Server 仮想マシン、vCLS 仮想マシン、ファイル サービス仮想マシンを除き、vSAN クラスタに格納されているすべての仮想マシンをパワーオフします。vCenter Server が vSAN クラスタでホストされている場合は、vCenter Server で使用される vCenter Server 仮想マシンまたはサービス仮想マシン (DNS、Active Directory など) をパワーオフしないでください。
 - c HCI メッシュ サーバ クラスタの場合は、クラスタ上に格納されているすべてのクライアント仮想マシンをパワーオフします。クライアント クラスタの vCenter Server 仮想マシンがこのクラスタに格納されている場合は、仮想マシンを移行またはパワーオフします。このサーバ クラスタがシャットダウンされると、クライアントは共有データストアにアクセスできなくなります。
 - d すべての再同期タスクが完了していることを確認します。
[監視] タブをクリックし、[vSAN] > [オブジェクトの再同期] の順に選択します。

注： ロックダウン モードのメンバー ホストがある場合は、ホストの root アカウントをセキュリティ プロファイルの例外ユーザー リストに追加します。詳細については、『vSphere セキュリティ』の「ロックダウン モード」を参照してください。

- 2 vSphere Client で vSAN クラスタを右クリックし、[クラスタのシャットダウン] を選択します。
[vSAN サービス] ページで [クラスタのシャットダウン] をクリックすることもできます。
- 3 クラスタのシャットダウン ウィザードで、シャットダウンの事前チェックが緑色になっていることを確認します。赤色の感嘆符の付いている問題を解決します。[次へ] をクリックします。

vCenter Server アプライアンスが vSAN クラスタに展開されている場合、クラスタのシャットダウン ウィザードに vCenter Server の通知が表示されます。クラスタの再起動中に必要になることがあるため、オーケストレーション ホストの IP アドレスをメモしておきます。vCenter Server が DNS や Active Directory などのサービス仮想マシンを使用している場合、これらの仮想マシンは、クラスタのシャットダウン ウィザードで例外的な仮想マシンとなります。
- 4 シャットダウンの実行理由を入力し、[シャットダウン] をクリックします。
[vSAN サービス] ページが変更され、シャットダウン プロセスに関する情報が表示されます。
- 5 シャットダウン プロセスを監視します。

vSAN は、クラスタのシャットダウン、システム仮想マシンのパワーオフ、ホストのパワーオフを実行します。

次のステップ

vSAN クラスタを再起動します。「[vSAN クラスタの再起動](#)」を参照してください。

vSAN クラスタの再起動

メンテナンスまたはトラブルシューティングでシャットダウンされた vSAN クラスタを再起動できます。

手順

- 1 クラスタ ホストをパワーオンします。

vCenter Server が vSAN クラスタでホストされている場合は、vCenter Server が再起動するまで待機します。

- 2 vSphere Client で vSAN クラスタを右クリックし、[クラスタの再起動] を選択します。

[vSAN サービス] ページで [クラスタの再起動] をクリックすることもできます。

- 3 [クラスタの再起動] ダイアログで、[再起動] をクリックします。

[vSAN サービス] ページが変更され、再起動プロセスに関する情報が表示されます。

- 4 クラスタが再起動したら、vSAN Skyline Health を確認し、未解決の問題を解決します。

手動による vSAN クラスタのシャットダウンと再起動

vSAN クラスタ全体を手動でシャットダウンして、メンテナンスやトラブルシューティングを実行できます。

ワークフローで手動シャットダウンが必要な場合を除き、クラスタのシャットダウン ウィザードを使用します。

vSAN クラスタを手動でシャットダウンする場合は、クラスタで vSAN を無効にしないでください。

注： vSphere with Tanzu 環境では、コンポーネントのシャットダウンと起動を所定の順序で行う必要があります。詳細については、『VMware Cloud Foundation 運用ガイド』の「VMware Cloud Foundation のシャットダウンと起動」を参照してください。

手順

- 1 vSAN クラスタをシャットダウンします。

- a vSAN Skyline Health をチェックし、クラスタが良好な状態であることを確認します。

- b vCenter Server が vSAN クラスタにホストされていない場合は、クラスタで実行されているすべての仮想マシンをパワーオフします。vCenter Server が vSAN クラスタでホストされている場合は、vCenter Server で使用される vCenter Server 仮想マシンまたはサービス仮想マシン (DNS、Active Directory など) をパワーオフしないでください。

- c vSAN クラスタで vSAN ファイル サービスが有効になっている場合は、ファイル サービスを無効にする必要があります。vSAN ファイル サービスを無効にすると、空のファイル サービス ドメインが削除されます。vSAN クラスタを再起動した後も空のファイル サービス ドメインを保持する場合は、vSAN ファイル サービスを無効にする前に、NFS または SMB ファイル共有を作成する必要があります。

- d [構成] タブをクリックし、HA を無効にします。これにより、クラスタはホストのシャットダウンを障害として登録しません。

vSphere 7.0 U1 以降の場合は、vCLS 退避モードを有効にします。詳細については、[<https://kb.vmware.com/s/article/80472>] にある VMware のナレッジベースの記事を参照してください。

- e すべての再同期タスクが完了していることを確認します。

[監視] タブをクリックし、[vSAN] > [オブジェクトの再同期] の順に選択します。

- f vCenter Server が vSAN クラスタにホストされている場合、vCenter Server 仮想マシンをパワーオフします。

vCenter Server 仮想マシンを実行するホストをメモします。これは、vCenter Server 仮想マシンを再起動する必要があるホストです。

- g クラスタの ESXi ホストで次のコマンドを実行して、vCenter Server からのクラスタ メンバーの更新を無効にします。すべてのホストで次のコマンドを実行します。

```
esxcfg-advcfg -s 1 /VSAN/IgnoreClusterMemberListUpdates
```

- h 監視ホスト以外のクラスタの任意のホストにログインします。

- i そのホストでのみ、次のコマンドを実行します。複数のホストで同時にコマンドを実行すると、競合状態が発生し、予期しない結果になる可能性があります。

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py prepare
```

コマンドを実行すると、次のメッセージが表示されます。

```
Cluster preparation is done.
```

注：

- コマンドが正常に完了すると、クラスタが完全にパーティション分割されます。
- エラーが発生した場合は、エラー メッセージに基づいて問題を解決し、vCLS 退避モードを再度有効にします。
- クラスタ内のホストが不良な状態か、切断されている場合は、ホストを削除してからコマンドを再度実行します。

- j すべてのホストをメンテナンス モードに切り替え、[アクションなし] にします。vCenter Server がパワーオフされている場合は、次のコマンドを使用して、ESXi ホストをメンテナンス モードに切り替え、[アクションなし] にします。

```
esxcli system maintenanceMode set -e true -m noAction
```

すべてのホストでこの手順を行います。

複数のホストで [アクションなし] を同時に使用する場合、複数のホストを再起動した後にデータが使用不能になるリスクを回避するには、[\[https://kb.vmware.com/s/article/60424\]](https://kb.vmware.com/s/article/60424) にある VMware ナレッジベースの記事を参照してください。組み込みツールを使用してクラスタ内のすべてのホストの同時再起動を行うには、[\[https://kb.vmware.com/s/article/70650\]](https://kb.vmware.com/s/article/70650) にある VMware ナレッジベースの記事を参照してください。

- k すべてのホストがメンテナンス モードに切り替わったら、必要なメンテナンス タスクを実行し、ホストをパワーオフします。

2 vSAN クラスタを再起動します。

- a ESXi ホストをパワーオンします。

ESXi がインストールされている物理ボックスをパワーオンします。ESXi ホストが起動して仮想マシンを検出し、正常に機能します。

いずれかのホストで再起動に失敗した場合は、手動でホストをリカバリするか、不良な状態のホストを vSAN クラスタから移動する必要があります。

- b パワーオンした後、すべてのホストが復帰したら、すべてのホストでメンテナンス モードを終了します。vCenter Server がパワーオフされている場合は、ESXi ホストで次のコマンドを使用して、メンテナンス モードを終了します。

```
esxcli system maintenanceMode set -e false
```

すべてのホストでこの手順を行います。

- c 監視ホスト以外のクラスタの任意のホストにログインします。

- d そのホストでのみ、次のコマンドを実行します。複数のホストで同時にコマンドを実行すると、競合状態が発生し、予期しない結果になる可能性があります。

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py recover
```

コマンドを実行すると、次のメッセージが表示されます。

```
Cluster reboot/power-on is completed successfully!
```

- e 各ホストで次のコマンドを実行して、すべてのホストがクラスタで使用可能であることを確認します。

```
esxcli vsan cluster get
```

- f クラスタの ESXi ホストで次のコマンドを実行して、vCenter Server からのクラスタ メンバーの更新を有効にします。すべてのホストで次のコマンドを実行します。

```
esxcfg-advcfg -s 0 /VSAN/IgnoreClusterMemberListUpdates
```

- g vCenter Server 仮想マシンがパワーオフされている場合は、再起動します。vCenter Server 仮想マシンがパワーオンされ、実行されるまで待機します。vCLS 退避モードを無効にする方法については、[\[https://kb.vmware.com/s/article/80472\]](https://kb.vmware.com/s/article/80472) にある VMware ナレッジベースの記事を参照してください。

- h 各ホストで次のコマンドを実行して、すべてのホストが vSAN クラスタに参加していることを確認します。

```
esxcli vsan cluster get
```

- i vCenter Server から残りの仮想マシンを再起動します。

- j vSAN Skyline Health を確認し、未解決の問題を解決します。

- k (オプション) vSAN ファイル サービスを有効にします。
- l (オプション) vSAN クラスタで vSphere 可用性が有効になっている場合は、「Cannot find vSphere HA master agent」というエラーが発生しないように、vSphere の可用性を手動で再起動する必要があります。

vSphere 可用性を手動で再起動するには、vSAN クラスタを選択して、次の場所に移動します。

- 1 [構成] > [サービス] > [vSphere 可用性] > [編集] > [vSphere HA を無効にする]
 - 2 [構成] > [サービス] > [vSphere 可用性] > [編集] > [vSphere HA を有効にする]
- 3 クラスタ内のホストが不良な状態か、切断されている場合は、ホストをリカバリするか、vSAN クラスタからホストを削除します。vCenter Server が DNS や Active Directory などのサービス仮想マシンを使用している場合、これらの仮想マシンは、クラスタのシャットダウン ウィザードで例外的な仮想マシンとなります。

vSAN Skyline Health で使用可能なすべてのホストが緑色で表示された場合にのみ、上記のコマンドを再試行してください。

3 ノード vSAN クラスタがある場合、1 台のホストで障害が発生すると、`reboot_helper.py recover` コマンドは機能しません。管理者として次の操作を行います。

- a ユニキャスト エージェント リストから障害ホスト情報を一時的に削除します。
- b 次のコマンドを実行した後、ホストを追加します。

```
reboot_helper.py recover
```

ホストを削除して vSAN クラスタに追加するには、次のコマンドを実行します。

```
#esxcli vsan cluster unicastagent remove -a <IP Address> -t node -u <NodeUuid>
```

```
#esxcli vsan cluster unicastagent add -t node -u <NodeUuid> -U true -a <IP Address> -p 12321
```

次のステップ

vSAN クラスタを再起動します。「[vSAN クラスタの再起動](#)」を参照してください。

vSAN クラスタでのデバイス管理

9

vSAN クラスタのさまざまなデバイス管理タスクを実行できます。

ハイブリッドまたはオールフラッシュ ディスク グループを作成する、vSAN がキャパシティおよびキャッシュ用のデバイスを要求できるようにする、LED インジケータをオンまたはオフにする、デバイスをフラッシュとしてマークする、あるいはリモート デバイスをローカルとしてマークする、などの処理が可能です。

注： vSAN Express Storage Architecture クラスタでは、デバイスをフラッシュとしてマークし、リモート デバイスをローカルとしてマークすることはできません。

次のトピックを参照してください。

- [vSAN クラスタのストレージ デバイスの管理](#)
- [vSAN クラスタの個々のデバイスの操作](#)

vSAN クラスタのストレージ デバイスの管理

クラスタで vSAN を構成するときに、各ホストのストレージ デバイスを要求して、vSAN データストアを作成します。

初期の段階では、vSAN クラスタには単一の vSAN データストアが含まれています。各ホストでディスク グループまたはストレージ プールのディスクを要求すると、これらのデバイスによって追加される物理容量に応じて、データストアのサイズが増大します。

vSAN では、どのシナリオでも統一されたワークフローを使用してディスクを要求できます。利用可能なすべてのディスクを、モデルとサイズ、またはホストごとに一覧表示できます。

ディスク グループの追加 (vSAN Original Storage Architecture)

ディスク グループを追加する場合は、要求するホストとデバイスを指定する必要があります。各ディスク グループには、1つのフラッシュ キャッシュ デバイスと1つ以上のキャパシティ デバイスが含まれます。各ホストに複数のディスク グループを作成して、各ディスク グループにキャッシュ デバイスを要求できます。

ディスク グループを追加する場合、フラッシュ キャッシュと使用容量の比率を考慮します。比率はクラスタの要件とワークロードによって異なります。ハイブリッド クラスタでは、使用容量に対するフラッシュ キャッシュの使用比率（ミラーなどのレプリカを含まない）が 10% を超えるように構成を検討してください。

注： vSAN クラスタに新しい ESXi ホストを追加した場合、そのホストのローカル ストレージは vSAN データストアに自動的に追加されません。新しいホストのストレージを使用するには、ディスク グループを追加する必要があります。

ストレージ プールの追加 (vSAN Express Storage Architecture)

ストレージを提供する各ホストには、フラッシュ デバイスの 1 つのストレージ プールがあります。各フラッシュ デバイスは、キャッシュとキャパシティをクラスタに提供します。互換性のあるデバイスを使用してストレージ プールを追加できます。vSAN は、ホストが接続されているストレージ ディスクの数に関係なく、ホストごとに 1 つのストレージ プールのみを作成します。

vSAN Direct 用ディスクの要求

vSAN Direct を使用すると、ステートフル サービスは直接バスを介して、未加工の非 vSAN ローカル ストレージにアクセスできます。

vSAN Direct にホストローカル デバイスを要求し、vSAN を使用してこれらのデバイスを管理し、監視できます。各ローカル デバイスで、vSAN Direct は独立した VMFS データストアを作成し、ステートフル アプリケーションで使用できるようにします。

ローカル vSAN Direct データストアは、vSAN-D データストアとして表示されます。

注： クラスタで vSAN Express Storage Architecture が有効になっている場合、vSAN Direct のディスクを要求することはできません。

vSAN クラスタのディスク グループまたはストレージ プールの作成

クラスタで使用するストレージ アーキテクチャに応じて、ディスク グループまたはストレージ プールを作成できます。

ホストでのディスク グループの作成 (vSAN Original Storage Architecture)

キャッシュ デバイスとキャパシティ デバイスを要求して、vSAN ホストのディスク グループを定義できます。ディスク グループを作成するには、1 つのキャッシュ デバイスと 1 つ以上のキャパシティ デバイスを選択します。

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] で、[ディスク管理] をクリックし、表からホストを選択して、[ディスクの表示] をクリックします。
- 4 [ディスク グループの作成] をクリックします。
- 5 要求するディスクを選択します。
 - a キャッシュ層に使用するフラッシュ デバイスを選択します。
 - b キャパシティ層に使用するディスクを選択します。

7. [作成] をクリックして、選択内容を確認します。

注： 新しいディスク グループがリストに表示されます。

ホストでのストレージ プールの作成 (vSAN Express Storage Architecture)

ディスクを要求して、vSAN ホストのストレージ プールを定義できます。ストレージを提供する各ホストには、フラッシュ デバイスの1つのストレージ プールがあります。各フラッシュ デバイスは、キャッシュとキャパシティをクラスタに提供します。ストレージ プールは、ESA と互換性のある任意のデバイスで作成できます。vSAN は、ホストごとにストレージ プールを1つだけ作成します。

ストレージ プールでは、各デバイスは単一の階層でキャッシュとキャパシティの両方を提供します。これは、キャッシュとキャパシティの異なる階層に専用デバイスがあるディスク グループとは異なります。

vSAN 管理対象ディスク要求を使用して、クラスタ ホスト上のすべての互換性のあるディスクを自動的に要求します。新しいホストを追加すると、vSAN は、それらのホスト上の互換性のあるディスクも要求します。手動で追加されたディスクは、この設定の影響を受けません。このようなディスクは、ストレージ プールに手動で追加できます。

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 [未使用のディスクの要求] をクリックします。

注： [vSAN 管理対象ディスクの要求] を使用するようにディスク要求モードを変更できます。vSAN は、クラスタ ホスト上のすべての互換性のあるデバイスを自動的に要求します。

- 5 ホストでグループ化します。
- 6 要求する互換性のあるディスクを選択します。
- 7 [作成] をクリックして、選択内容を確認します。

注： [ディスク管理] ページが表示され、ホストが一覧表示されます。ホストでディスクが要求されたことは、[使用中のディスク] 列で確認できます。ここには、更新後のホストあたりのディスク数が反映されます。ホストで要求されたディスクを確認するには、[ディスクの表示] ボタンをクリックします。

vSAN Original Storage Architecture クラスタのストレージ デバイスの要求

キャッシュ デバイスとキャパシティ デバイスのグループを選択して、vSAN でこれらをデフォルトのディスク グループに設定できます。

この方法では、デバイスを選択して、vSAN クラスタのディスク グループを作成します。各ディスク グループには、1個のキャッシュ デバイスと、少なくとも1個のキャパシティ デバイスが必要です。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。

- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 [未使用のディスクの要求] をクリックします。
- 5 ディスク グループに追加するデバイスを選択します。
 - ハイブリッド ディスク グループの場合は、ストレージを提供する各ホストが、1 個のフラッシュ キャッシュ デバイスおよび 1 個以上の HDD キャパシティ デバイスを提供する必要があります。ディスク グループごとに追加できるキャッシュ デバイスは 1 個のみです。
 - キャッシュとして使用するフラッシュ デバイスを選択して、[キャッシュ層を要求] をクリックします。
 - キャパシティとして使用する HDD デバイスを 1 つ以上選択して、デバイスごとに [キャパシティ層を要求] をクリックします。
 - [作成] または [OK] をクリックします。
 - オールフラッシュ ディスク グループの場合は、ストレージを提供する各ホストが、1 個のフラッシュ キャッシュ デバイスおよび 1 個以上のフラッシュ キャパシティ デバイスを提供する必要があります。ディスク グループごとに追加できるキャッシュ デバイスは 1 個のみです。
 - キャッシュとして使用するフラッシュ デバイスを 1 つ以上選択して、デバイスごとに [キャッシュ層を要求] をクリックします。
 - キャパシティとして使用するフラッシュ デバイスを選択して、[キャパシティ層を要求] をクリックします。
 - [作成] または [OK] をクリックします。

vSAN は選択したデバイスを要求し、それらを vSAN データストアを提供するデフォルトのディスク グループに編成します。

オールフラッシュ ディスク グループに追加する各デバイスのロールを確認するには、[ディスク管理] ページで指定ホストの [次として要求] 列に移動します。このテーブルには、デバイスとディスク グループにおける目的のリストが表示されます。オールフラッシュ ディスク グループとハイブリッド ディスク グループの場合、キャッシュ ディスクは常にディスク グループ グリッドの先頭に表示されます。

vSAN Express Storage Architecture クラスタのストレージ デバイスの要求

ホストからデバイスのグループを選択して、vSAN でストレージ プールに編成できます。

vSAN ESA を有効にすると、ディスクを手動または自動で要求できます。手動の場合は、要求するストレージ デバイスのグループを選択できます。

自動ディスク要求では、vSAN は、互換性のあるすべてのディスクをホストから自動的に選択します。新しいホストがクラスタに追加されると、vSAN は、それらのホストで使用可能な互換性のあるディスクを自動的に要求し、ストレージを vSAN データストアに追加します。

vSAN ESA 認定済みとして報告されていないデバイスを選択できます。これらのデバイスはストレージ プールで考慮されますが、そのような構成は推奨されず、パフォーマンスに影響を与える可能性があります。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 ディスクを手動で要求するには、[未使用のディスクの要求] をクリックします。
 - a 要求するデバイスを選択します。
 - b [作成] をクリックします。
- 5 ディスクを自動的に要求するには、[ディスク要求モードの変更] をクリックし、[vSAN 管理対象ディスクの要求] トグル ボタンをクリックします。

注： クラスタの構成時に vSAN 管理対象ディスクの要求を使用することを選択した場合、切り替えボタンはすでに有効になっています。

vSAN は、選択されたデバイスを要求し、それらを vSAN データストアをサポートするストレージ プールに編成します。デフォルトでは、vSAN は、クラスタにストレージを提供する ESXi ホストごとに 1 つのストレージ プールを作成します。選択したデバイスが vSAN ESA に認定されていない場合、それらのデバイスはストレージ プールの作成時に考慮されません。

vSAN Direct 用ディスクの要求

ローカルストレージ デバイスを vSAN Direct として要求し、vSAN Data Persistence プラットフォームで使用できます。

注： vSAN Direct ストレージを使用できるのは、vSAN Data Persistence プラットフォームのみです。vSAN Data Persistence プラットフォームは、ソフトウェアテクノロジー パートナーが VMware Infrastructure と統合するためのフレームワークを提供します。VMware のユーザーが vSAN Data Persistence プラットフォームのメリットを利用できるように、各パートナーが独自のプラグインを開発する必要があります。プラットフォーム上で実行されるパートナー ソリューションが稼働するまで、このプラットフォームは機能しません。詳細については、『vSphere with Tanzu の構成と管理』を参照してください。

手順

- 1 vSphere Client で vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 [未使用のディスクの要求] をクリックします。
- 5 [未使用のディスクの要求] ダイアログで、[vSAN Direct] タブを選択します。
- 6 [vSAN Direct の要求] 列のチェックボックスを選択して、要求するデバイスを選択します。

注： vSAN クラスタに要求したデバイスは、[vSAN Direct] タブに表示されません。

- 7 [作成] をクリックします。

結果

要求されるデバイスごとに、vSAN は新しい vSAN Direct データストアを作成します。

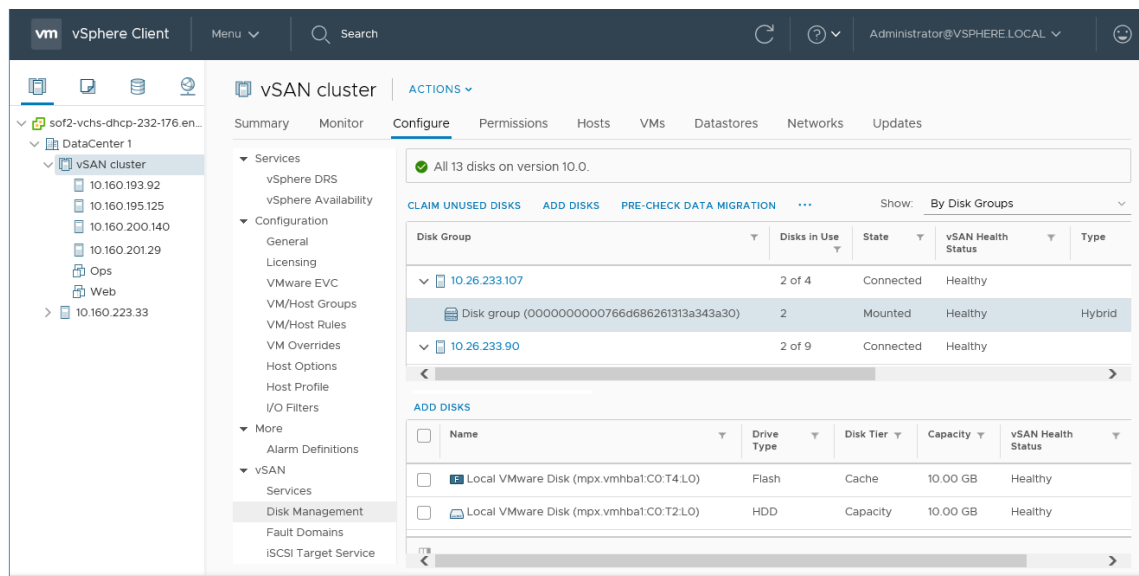
次のステップ

[データストア] タブをクリックすると、クラスタ内の vSAN Direct データストアが表示されます。

vSAN クラスタの個々のデバイスの操作

vSAN クラスタでさまざまなデバイス管理タスクを実行できます。

ディスク グループにデバイスを追加したり、ディスク グループからデバイスを削除したり、ロケータ LED を有効または無効にしたり、デバイスをマークしたりできます。また、vSAN Direct を使用して、要求されたディスクを追加または削除することもできます。



vSAN クラスタのディスク グループへのデバイスの追加

ディスクを要求するように vSAN を手動モードで構成している場合、追加のローカル デバイスを既存のディスク グループに追加できます。

デバイスは SSD や磁気ディスクなど、ディスク グループ内の既存のデバイスと同じタイプである必要があります。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 ディスク グループを選択し、[ディスクの追加] をクリックします。

5 追加するデバイスを選択し、[追加] をクリックします。

データまたはパーティション情報が残っている使用済みのデバイスを追加する場合は、最初にデバイスをクリーンアップする必要があります。デバイスからのパーティション情報の削除の詳細については、「[デバイスからのパーティションの削除](#)」を参照してください。RVC コマンド `host_wipe_vsan_disks` を実行してデバイスをフォーマットすることもできます。

次のステップ

vSAN ディスク バランス（ディスクの負荷分散）の健全性チェックが緑色であることを確認します。ディスク バランス健全性チェックが警告を示している場合は、オフピーク時に自動リバランス操作を実行します。詳細については、『vSAN の監視とトラブルシューティング』の「vSAN クラスタでの自動リバランスの構成」を参照してください。

vSAN クラスタからのディスクまたはディスク グループのデータ移行機能の確認

データ移行の事前チェックを使用して、ディスクまたはディスク グループをアンマウントしたり、vSAN クラスタから削除したりするときの移行オプションの影響を判断します。

vSAN クラスタからディスクまたはディスク グループをアンマウントまたは削除する前に、データ移行の事前チェックを実行します。テスト結果から得られる情報は、クラスタ キャパシティへの影響、予測される健全性チェック、コンプライアンスに準拠しなくなると予想されるオブジェクトを判断するのに役立ちます。操作が成功しないと予想される場合、事前チェックからは、必要なリソースに関する情報が提供されます。

手順

- 1 vSAN クラスタに移動します。
- 2 [監視] タブをクリックします。
- 3 [vSAN] の下で、[データ移行の事前チェック] をクリックします。
- 4 ディスクまたはディスク グループを選択し、データ移行オプションを選択して、[事前チェック] をクリックします。

vSAN によってデータ移行の事前チェック テストが実行されます。

5 テスト結果を確認します。

事前チェックの結果に、ディスクまたはディスク グループを安全にアンマウントまたは削除できるかどうかが表示されます。

- [オブジェクトのコンプライアンスおよびアクセシビリティ] タブには、データの移行後に問題が発生する可能性のあるオブジェクトが表示されます。
- [クラスタ キャパシティ] タブには、vSAN クラスタに対するデータ移行の影響が、操作を実行する前と後それぞれについて表示されます。
- [予測される健全性] タブには、データ移行によって影響を受ける可能性のある健全性チェックが表示されません。

次のステップ

事前チェックの結果でデバイスのアンマウントまたは削除が可能なが示されている場合は、オプションをクリックして操作を続行します。

vSAN からのディスク グループまたはデバイスの削除

選択したデバイスをディスク グループから削除したり、ディスク グループ全体を vSAN OSA クラスタから削除したりできます。

保護されていないデバイスを削除すると、vSAN データストアおよびデータストアの仮想マシンで問題が生じる場合があるため、デバイスまたはディスク グループの削除は回避してください。

通常、vSAN からのデバイスまたはディスク グループの削除は、デバイスをアップグレードする場合、障害の発生したデバイスを置き換える場合、またはキャッシュ デバイスを削除する必要がある場合に行います。他の vSphere ストレージ機能では、vSAN クラスタから削除するフラッシュベースの任意のデバイスを使用できます。

ディスク グループを永続的に削除すると、ディスクのメンバーシップおよびデバイスに保存されたデータが削除されます。

注： 1 台のフラッシュ キャッシュ デバイスまたはすべてのキャパシティ デバイスをディスク グループから削除すると、ディスク グループ全体が削除されます。

注： クラスタでデデュープおよび圧縮を使用している場合、ディスク グループから 1 つのディスクを削除することはできません。ディスク グループ全体を削除する必要があります。

デバイスまたはディスク グループのデータを退避すると、仮想マシンのストレージ ポリシーに一時的に準拠しなくなる可能性があります。

前提条件

クラスタから削除する前に、デバイスまたはディスク グループでデータ移行の事前チェックを実行します。詳細については、次を参照してください。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 ディスク グループまたは選択したデバイスを削除します。

オプション	説明
ディスク グループの削除	<ol style="list-style-type: none"> a [ディスク グループ] の下で、削除するディスク グループを選択し、[...] をクリックしてから [削除] をクリックします。 b データ退避モードを選択します。
選択したデバイスの削除	<ol style="list-style-type: none"> a [ディスク グループ] の下で、削除するデバイスを含むディスク グループを選択します。 b [ディスク] の下で、削除するデバイスを選択し、[ディスクの削除] をクリックします。 c データ退避モードを選択します。

- 5 [はい] または [削除] をクリックして確認します。

選択したデバイスまたはディスク グループからデータが退避されます。

vSAN クラスタでのディスク グループの再作成

vSAN クラスタ内のディスク グループを再作成すると、既存のディスクはディスク グループから削除され、ディスク グループが削除されます。

vSAN では、同一のディスクを使用してディスク グループを再作成します。vSAN クラスタでディスク グループを再作成するときのプロセスは vSAN によって管理されます。vSAN はディスク グループ内のすべてのディスクからデータを退避させて、ディスク グループを削除し、同一のディスクを使用してディスク グループを作成します。

手順

- 1 vSphere Client で vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 [ディスク グループ] の下で、再作成するディスク グループを選択します。
- 5 [...] をクリックしてから [再作成] をクリックします。

[ディスク グループの再作成] ダイアログ ボックスが表示されます。

- 6 データ移行モードを選択し、[再作成] をクリックします。

結果

ディスク上にあるすべてのデータが退避されます。ディスク グループがクラスタから削除され、再作成されます。

vSAN のロケータ LED の使用

ロケータ LED を使用して、ストレージ デバイスの場所を識別できます。

vSAN は障害が発生したデバイスでロケータ LED を点灯できるため、デバイスを簡単に識別できます。これは、複数のホット プラグおよびホスト スワップのシナリオで作業するときに特に役立ちます。

RAID 0 モードのコントローラはコントローラがロケータ LED を認識できるようにするには追加のステップが必要となるため、バススルー モードで I/O ストレージ コントローラを使用することを検討してください。

RAID 0 モードでのストレージ コントローラの構成に関する詳細については、ベンダーのドキュメントを参照してください。

ロケータ LED

vSAN ストレージ デバイスのロケータ LED をオンまたはオフにできます。ロケータ LED をオンにすると、特定のストレージ デバイスの場所を識別できます。

vSAN デバイスの視覚的アラートが不要になった場合は、選択したデバイスのロケータ LED をオフにできます。

前提条件

- この機能を有効にするストレージ I/O コントローラに、サポートされるドライバがインストールされていることを確認します。VMware によって認定されているドライバの詳細については、『VMware 互換性ガイド』(<http://www.vmware.com/resources/compatibility/search.php>) を参照してください。
- 場合によっては、ストレージ I/O コントローラのロケータ LED 機能を構成するにはサードパーティ ユーティリティの使用が必要な可能性があります。たとえば、HP を使用している場合、HP SSA CLI がインストールされていることを確認する必要があります。

サードパーティ VIB のインストールの詳細については、『vSphere のアップグレード』ドキュメントを参照してください。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 デバイスのリストを表示するホストを選択します。
- 5 画面の下部にあるリストからストレージ デバイスを 1 つ以上選択します。選択したデバイスのロケータ LED に対して必要な操作を実行します。

オプション	操作
[LED を点灯]	選択したストレージ デバイスのロケータ LED をオンにします。[管理] タブで、[ストレージ] > [ストレージ デバイス] をクリックすることもできます。
[LED を消灯]	選択したストレージ デバイスのロケータ LED をオフにします。[管理] タブで、[ストレージ] > [ストレージ デバイス] をクリックすることもできます。

vSAN でデバイスをフラッシュとしてマークする

フラッシュ デバイスが ESXi ホストによって自動的にフラッシュとして識別されない場合は、手動でローカル フラッシュ デバイスとしてマークできます。

パススルー モードではなく RAID 0 モードが有効なフラッシュ デバイスは、フラッシュとして認識されないことがあります。デバイスがローカル フラッシュとして認識されない場合、vSAN に提供されるデバイスのリストから除外され、vSAN クラスタでは使用できません。これらのデバイスにローカル フラッシュとしてマークを付けると、vSAN で使用可能になります。

前提条件

- デバイスがホストに対してローカルであることを確認します。
- デバイスが使用中ではないことを確認します。
- デバイスにアクセスする仮想マシンがパワーオフ状態であり、データストアがアンマウント済みであることを確認します。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 使用可能なデバイスのリストを表示するホストを選択します。
- 5 ページ下部の [表示] ドロップダウン メニューで、[未使用] を選択します。
- 6 リストから 1 個以上のフラッシュ デバイスを選択し、[フラッシュ ディスクとしてマーク] をクリックします。
- 7 [はい] をクリックして変更を保存します。

選択したデバイスのドライブ タイプがフラッシュとして表示されます。

vSAN でデバイスを HDD としてマークする

ローカル磁気ディスクが ESXi ホストによって自動的に HDD デバイスとして識別されない場合は、手動でローカル HDD デバイスとしてマークできます。

磁気ディスクをフラッシュ デバイスとしてマークした場合は、磁気ディスクとしてマークすることにより、デバイスのディスク タイプを変更できます。

前提条件

- 磁気ディスクがホストに対してローカルであることを確認します。
- 磁気ディスクが使用中でなく空であることを確認します。
- デバイスにアクセスする仮想マシンがパワーオフされていることを確認します。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 使用可能な磁気ディスクのリストを表示するホストを選択します。
- 5 ページ下部の [表示] ドロップダウン メニューで、[未使用] を選択します。
- 6 リストから 1 つ以上の磁気ディスクを選択し、[HDD ディスクとしてマーク] をクリックします。
- 7 [はい] をクリックして保存します。

選択した磁気ディスクの [ドライブ タイプ] に HDD と表示されます。

vSAN でデバイスをローカルとしてマークする

ホストが外部 SAS エンクロージャを使用している場合、vSAN で特定のデバイスがリモートとして認識され、自動的にローカルとして要求できない可能性があります。

そのような場合、デバイスをローカルとしてマークできます。

前提条件

ストレージ デバイスが共有されていないことを確認します。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 デバイスのリストを表示するホストを選択します。
- 5 ページ下部の [表示] ドロップダウン メニューで、[未使用] を選択します。
- 6 デバイスのリストから、ローカルとしてマークするリモート デバイスを 1 個以上選択し、[ローカル ディスクとしてマーク] をクリックします。
- 7 [はい] をクリックして変更を保存します。

vSAN でデバイスをリモートとしてマークする

外部 SAS コントローラを使用するホストは、デバイスを共有できます。

それらの共有デバイスをリモートとして手動でマークし、ディスク グループの作成時に vSAN がそれらのデバイスを要求しないようにすることができます。vSAN では、共有デバイスをディスク グループに追加できません。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 デバイスのリストを表示するホストを選択します。
- 5 ページ下部の [表示] ドロップダウン メニューで、[未使用] を選択します。
- 6 リモートとしてマークするデバイスを 1 個以上選択し、[リモートとしてマーク] をクリックします。
- 7 [はい] をクリックして確認します。

vSAN ディスク グループへのキャパシティ デバイスの追加

キャパシティ デバイスを既存の vSAN ディスク グループに追加できます。

共有デバイスはディスク グループに追加できません。

前提条件

デバイスがフォーマット済みで使用中にはないことを確認します。

手順

- 1 vSAN クラスタに移動します。

- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 ディスク グループを選択します。
- 5 画面の下部にある [ディスクの追加] をクリックします。
- 6 ディスク グループに追加するキャパシティ デバイスを選択します。
- 7 [OK] または [追加] をクリックします。

デバイスがディスク グループに追加されます。

デバイスからのパーティションの削除

vSAN が使用するデバイスを要求できるように、デバイスからパーティション情報を削除できます。

データまたはパーティション情報が残っているデバイスを追加した場合、デバイスから既存のパーティション情報を削除してからでないと、vSAN で使用するために要求できません。クリーンなデバイスをディスク グループに追加することをお勧めします。

デバイスからパーティション情報を削除すると、vSAN はディスク フォーマット情報と論理パーティションが含まれるプライマリ パーティションをデバイスから削除します。

前提条件

デバイスが起動ディスク、VMFS データストア、または vSAN として ESXi で使用されていないことを確認します。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。
- 4 使用可能なデバイスのリストを表示するホストを選択します。
- 5 [表示] ドロップダウン メニューで、[使用不可] を選択します。
- 6 リストからデバイスを選択し、[パーティションの消去] をクリックします。
- 7 [OK] をクリックして確認します。

デバイスはクリーンになり、パーティション情報が含まれなくなりました。

vSAN クラスターの容量効率の向上

10

容量効率の手法を使用すると、データを保存するための容量を削減できます。

これらの手法では、ニーズを満たすために必要な合計ストレージ容量を削減できます。

次のトピックを参照してください。

- vSAN の容量効率機能
- SCSI マッピング解除による vSAN のストレージ容量の再利用
- vSAN クラスターでのデデュープおよび圧縮の使用
- vSAN クラスターでの RAID 5 または RAID 6 イレージャ コーディングの使用
- vSAN クラスターの RAID 5 または RAID 6 の設計に関する考慮事項

vSAN の容量効率機能

容量効率の手法を使用すると、データを保存するための容量を削減できます。

これらの手法では、ニーズを満たすために必要な合計ストレージ容量を削減できます。vSAN 6.7 Update 1 以降では、削除された vSAN オブジェクトにマッピングされたストレージ容量を再利用するための SCSI unmap コマンドがサポートされています。

vSAN クラスターでデデュープと圧縮を使用すると、重複データを排除して、データを保存するために必要な容量を削減できます。また、圧縮のみの vSAN を使用すると、サーバのパフォーマンスを損なわずにストレージ要件を削減できます。

仮想マシンに [障害の許容方法] ポリシー属性を設定して、RAID 5 または RAID 6 イレージャ コーディングを使用できます。イレージャ コーディングでは、デフォルトの RAID 1 ミラーリングよりも少ないストレージ容量でデータを保護できます。

デデュープと圧縮および RAID 5 または RAID 6 イレージャ コーディングを使用することで、ストレージ容量をさらに節約できます。RAID 5 または RAID 6 ではそれぞれ、RAID 1 よりも明確に容量の節約を定義することが可能です。デデュープおよび圧縮を使用すれば、さらなる節約が期待できます。

SCSI マッピング解除による vSAN のストレージ容量の再利用

SCSI UNMAP コマンドを使用すると、ゲストが vSAN オブジェクトに作成し、ファイル システムから削除されたファイルにマッピングされたストレージ容量を再利用できます。

vSAN 6.7 Update 1 以降では、SCSI UNMAP がサポートされます。ファイルを削除すると、ファイル システム内の容量が解放されます。この空き容量は、ファイル システムが解放またはマッピング解除するまで、ストレージ デバイスにマッピングされます。vSAN は、マッピング解除操作とも呼ばれる空き容量の再利用をサポートしています。仮想マシンの削除または移行、スナップショットの統合などを行うときに、vSAN データストア内部のストレージ容量を解放することができます。

ストレージ容量を再利用すると、ホストとフラッシュ間の I/O スループットと、フラッシュのエンデュランス（書き換え回数）が向上します。

マッピング解除機能は、デフォルトでは無効です。vSAN サービスの [詳細オプション] タブで [ゲストのトリム/アンマップ] を有効にします。vSAN クラスタでマッピング解除を有効にするときは、すべての仮想マシンをパワーオフしてからパワーオンする必要があります。マッピング解除操作を実行するには、仮想マシンでバージョン 13 以降の仮想ハードウェアを使用する必要があります。

vSAN はまた、ストレージ容量を再利用するためにゲスト OS から直接発行される SCSI UNMAP コマンドをサポートしています。vSAN は、オフラインおよびインラインでのマッピング解除をサポートしています。Linux OS では、オフラインのマッピング解除は **fstrim(8)** コマンドで実行され、インラインのマッピング解除は **mount -o discard** コマンドの使用時に実行されます。Windows OS では、NTFS によってインラインのマッピング解除がデフォルトで実行されます。

vSAN クラスタでのデデュープおよび圧縮の使用

vSAN はブロックレベルのデデュープおよび圧縮を実行してストレージ容量を節約できます。

vSAN オールフラッシュ クラスタでデデュープと圧縮を有効にすると、各ディスク グループまたはストレージ プール内の冗長なデータが削減されます。デデュープでは冗長なデータ ブロックが削除されるのに対して、圧縮ではさらに各データ ブロック内で冗長なデータが削除されます。これらの技術は連携して機能し、データを保存するために必要な容量を減らすことができます。vSAN はデデュープを実行してから、データをキャッシュ層からキャパシティ層に移動するときに圧縮を実行します。オンライン トランザクション処理など、デデュープのメリットを得られないワークロードには、圧縮のみの vSAN を使用します。

デデュープは、キャッシュ層からキャパシティ層にデータが戻されるときにインラインで実行されます。デデュープ アルゴリズムは、固定ブロック サイズを使用し、各ディスク グループ内で適用されます。同じディスク グループ内のブロックの冗長コピーがデデュープされます。

vSAN Original Storage Architecture の場合、デデュープと圧縮は、クラスタ全体の設定として有効になりますが、ディスク グループ単位で適用されます。また、vSAN ポリシーを使用して設定を変更できないため、特定のワークロードで圧縮を有効にすることはできません。vSAN クラスタでデデュープおよび圧縮を有効にすると、特定のディスク グループ内の冗長なデータが単一のコピーに削減されます。

注： 圧縮のみの vSAN はディスク単位で適用されます。

vSAN Express Storage Architecture の場合、圧縮はクラスタで有効になっています（これがデフォルトです）。一部の仮想マシン ワークロードで圧縮を有効にしない場合は、カスタマイズされたストレージ ポリシーを作成し、そのポリシーを仮想マシンに適用します。また、vSAN Express Storage Architecture の圧縮は、新しい書き込みのみ適用されます。オブジェクトの圧縮を有効にしても、古いブロックは圧縮されません。

デデュープおよび圧縮は、vSAN オールフラッシュ クラスタを作成するとき、または既存の vSAN オールフラッシュ クラスタを編集するときに有効にできます。詳細については、「[既存の vSAN クラスタでデデュープと圧縮を有効にする](#)」を参照してください。

デデュープと圧縮を有効または無効にするときに、vSAN はすべてのホストのすべてのディスク グループまたはストレージ プールのローリング再フォーマットを実行します。vSAN データストアに保存されているデータによっては、このプロセスに長時間かかることがあります。これらの操作を頻繁に実行しないでください。デデュープおよび圧縮を無効にする予定の場合、最初にデータを配置するのに十分な物理容量があることを確認する必要があります。

注： 仮想マシンの暗号化では、ストレージに書き出す前にホストのデータを暗号化するため、デデュープおよび圧縮は暗号化された仮想マシンには効果的ではない場合があります。仮想マシンの暗号化を使用する場合は、ストレージのトレードオフについて検討してください。

デデュープおよび圧縮を使用したクラスタ内のディスクの管理方法

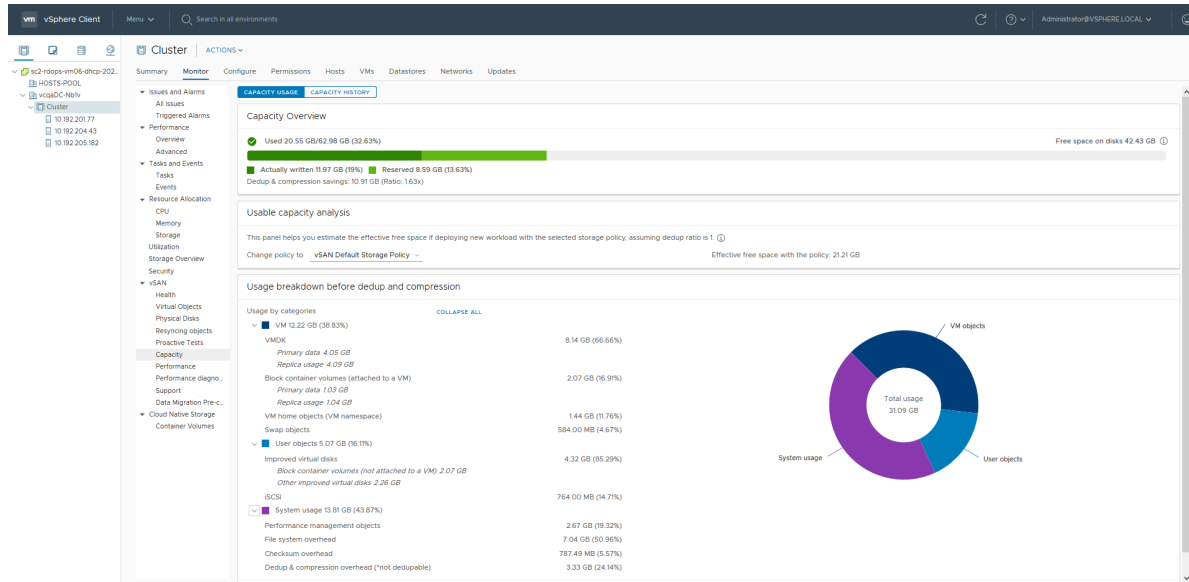
注： このトピックは、vSAN Original Storage Architecture クラスタにのみ適用されます。

デデュープおよび圧縮を有効にしてクラスタ内のディスクを管理する場合、次のガイドラインを考慮します。このガイドラインは、圧縮のみの vSAN には適用されません。

- ディスクを1つずつディスク グループに追加しないようにします。デデュープおよび圧縮の効率を高めるには、ディスク グループを追加してクラスタのストレージ容量を増やすことを検討してください。
- ディスク グループを手動で追加する場合は、すべてのキャパシティ ディスクを同時に追加します。
- 単一のディスクをディスク グループから削除することはできません。変更を行うには、ディスク グループ全体を削除する必要があります。
- 単一のディスクで障害が発生すると、ディスク グループ全体で障害が発生します。

デデュープおよび圧縮によって節約できる容量の確認

デデュープおよび圧縮によって削減できるストレージ量は、保存されているデータのタイプや重複するブロックの数など、多くの要因によって異なります。ディスク グループが大きくなると、デデュープ率が高くなる傾向があります。デデュープおよび圧縮の結果は、vSAN のキャパシティ モニターで [デデュープおよび圧縮前の使用量の内訳] を確認してチェックできます。



[デデュープおよび圧縮前の使用量の内訳]を確認できるのは、vSphere ClientでvSAN キャパシティを監視しているときです。デデュープおよび圧縮の結果に関する情報が表示されます。[有効化前に使用]容量はデデュープおよび圧縮を適用する前に必要な論理容量を示すのに対して、[有効化後に使用]容量はデデュープおよび圧縮を適用した後に使用される物理容量を示します。[有効化後に使用]容量には、節約される容量の量の概要と、デデュープおよび圧縮の比率も表示されます。

[デデュープおよび圧縮の比率]は、デデュープおよび圧縮を適用した後に必要となる物理（[有効化後に使用]）容量に対するデデュープおよび圧縮を適用する前にデータを保存するために必要な論理（[有効化前に使用]）容量に基づきます。具体的には、この比率は[有効化前に使用]容量を[有効化後に使用]容量で割ったものです。たとえば、[有効化前に使用]容量が3 GBだが物理的な[有効化後に使用]容量が1 GBの場合、デデュープおよび圧縮の比率は3倍です。

vSAN クラスタでデデュープおよび圧縮を有効にした場合、ディスク容量が要求されて再割り当てされるため、キャパシティの更新がキャパシティ モニターで反映されるまでに数分かかる場合があります。

vSAN クラスタのデデュープおよび圧縮の設計に関する考慮事項

vSAN クラスタでデデュープおよび圧縮を構成する場合、次のガイドラインを考慮してください。

- デデュープおよび圧縮は、オールフラッシュ ディスク グループでのみ使用できます。
- デデュープおよび圧縮をサポートするには、オンディスク フォーマット バージョン 3.0 以降が必要です。
- クラスタでデデュープおよび圧縮を有効にするには、有効なライセンスが必要です。
- vSAN クラスタでデデュープおよび圧縮を有効にすると、すべてのディスク グループのデータがデデュープおよび圧縮を使用して削減されます。
- vSAN は、各ディスク グループ内で重複するデータ ブロックを排除できますが、ディスク グループ間では排除できません（vSAN Original Storage Architecture にのみ適用可能）。
- デデュープおよび圧縮のための容量のオーバーヘッドは、合計 Raw 容量の約 5% です。

- ポリシーには、0% または 100% のいずれかのオブジェクト スペースの予約が必要です。100% のオブジェクト スペース予約のポリシーは常に順守されます。ただし、デデュープおよび圧縮の効率が低下する可能性があります。

新規の vSAN クラスタでデデュープおよび圧縮を有効にする

新規の vSAN オールフラッシュ クラスタを構成する際に、デデュープおよび圧縮を有効にすることができます。

手順

- 1 新規のオール フラッシュ vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] の下で [サービス] を選択します。
 - a [データ サービス] の下にある [編集] をクリックします。
 - b 容量効率オプション（デデュープと圧縮、または圧縮のみ）を選択します。
 - c [暗号化] で、切り替えボタンを使用して保存データの暗号化を有効にします。

注： vSAN Express Storage Architecture クラスタを使用する場合、ディスクの要求後にこの設定を変更することはできません。

- d (オプション) [冗長性の低下を許可] を選択します。デデュープおよび圧縮を有効にする間、vSAN は必要に応じて仮想マシンの保護レベルを低くします。詳細については、[vSAN クラスタにおける仮想マシンの冗長性の低下](#)を参照してください。
- 4 クラスタの構成を完了します。

既存の vSAN クラスタでデデュープと圧縮を有効にする

既存のオール フラッシュ vSAN クラスタで構成パラメータを編集して、デデュープおよび圧縮を有効にすることができます。

vSAN Original Storage Architecture クラスタで有効にするには：

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] の下で [サービス] を選択します。
 - a クリックして容量効率を編集します。
 - b 容量効率オプション（デデュープと圧縮、または圧縮のみ）を選択します。
 - c (オプション) [冗長性の低下を許可] を選択します。デデュープおよび圧縮を有効にする間、vSAN は必要に応じて仮想マシンの保護レベルを低くします。詳細については、[vSAN クラスタにおける仮想マシンの冗長性の低下](#)を参照してください。
- 4 [適用] をクリックして、構成の変更を保存します。

vSAN Express Storage Architecture クラスタで有効にするには：

- 1 クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] の下で [サービス] を選択します。
- 4 [データ サービス] で、[編集] をクリックします。
 - a [暗号化] で、切り替えボタンを使用して保存データの暗号化を有効にします。

注： ディスクの要求後にこの設定を変更することはできません。

- b [転送中データの暗号化] 切り替えボタンを使用して転送中データの暗号化を有効にし、再キー化間隔を指定します。
 - c (オプション) [冗長性の低下を許可] を選択します。デデュープおよび圧縮を有効にする間、vSAN は必要に応じて仮想マシンの保護レベルを低くします。詳細については、[vSAN クラスタにおける仮想マシンの冗長性の低下](#)を参照してください。
- 5 [適用] をクリックして、構成の変更を保存します。

デデュープおよび圧縮を有効にする間に、vSAN は、クラスタの各ディスク グループのディスク フォーマットを更新します。この変更を完了するために、vSAN はディスク グループからデータを退避させ、ディスク グループを削除してから、デデュープおよび圧縮をサポートする新しいフォーマットで再作成します。

この有効化処理には、仮想マシンの移行や DRS は必要ありません。この処理に必要な時間は、クラスタ内のホストの数とデータ量によって異なります。進捗は [タスクとイベント] タブで監視できます。

vSAN クラスタでデデュープおよび圧縮を無効にする

vSAN クラスタでデデュープおよび圧縮を無効にすることができます。

vSAN クラスタでデデュープおよび圧縮を無効にすると、クラスタで使用されるキャパシティのサイズが拡張可能になります (デデュープ率に基づきます)。デデュープおよび圧縮を無効にする前に、拡張されたデータのサイズを処理するのに十分な容量がクラスタにあることを確認します。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
 - a [vSAN] の下で [サービス] を選択します。
 - b [編集] をクリックします。
 - c デデュープおよび圧縮を無効にします。
 - d (オプション) [冗長性の低下を許可] を選択します。デデュープおよび圧縮を無効にする間、vSAN は必要に応じて仮想マシンの保護レベルを低くします。「[vSAN クラスタにおける仮想マシンの冗長性の低下](#)」を参照してください。
- 3 [適用] または [OK] をクリックして設定の変更を保存します。

結果

デデュープおよび圧縮を無効にすると、vSAN は、クラスタの各ディスク グループでディスク フォーマットを変更します。vSAN は、ディスク グループからデータを退避させ、ディスク グループを削除してから、デデュープおよび圧縮をサポートしないフォーマットでディスク グループを再作成します。

この処理に必要な時間は、クラスタ内のホストの数とデータ量によって異なります。進捗は [タスクとイベント] タブで監視できます。

vSAN クラスタにおける仮想マシンの冗長性の低下

デデュープおよび圧縮を有効にすると、特定の場合に仮想マシンの保護レベルを下げる必要があります。

デデュープおよび圧縮を有効にするには、ディスク グループのフォーマットを変更する必要があります。この変更を完了するために、vSAN はディスク グループからデータを退避させ、ディスク グループを削除してから、デデュープおよび圧縮をサポートする新しいフォーマットで再作成します。

特定の環境では、vSAN クラスタにディスク グループを完全に退避させるのに十分なリソースがない場合があります。そのような展開環境の例には、完全な保護を維持しながらレプリカの退避や監視をするリソースがない 3 ノード クラスタが含まれます。また、RAID-5 オブジェクトがすでに展開された 4 ノード クラスタも含まれます。後者の場合、RAID-5 オブジェクトは最低 4 ノードは必要のため、RAID-5 ストライプの一部を移動するための場所がありません。

それでも、デデュープおよび圧縮を有効にして、[冗長性の低下を許容] オプションを使用することはできます。このオプションでは、仮想マシンは引き続き実行されますが、その仮想マシンは、仮想マシン ストレージ ポリシーで定義された障害の最大数を許容できない可能性があります。結果として、デデュープおよび圧縮のためにフォーマットを変更する間、仮想マシンは一時的にデータ損失を経験するリスクにさらされる可能性があります。vSAN は、フォーマット変換の完了後に完全なコンプライアンスと冗長性をリストアします。

デデュープおよび圧縮が有効な場合のディスクの追加または削除

デデュープおよび圧縮が有効な vSAN クラスタにディスクを追加する場合は、特定の考慮事項が適用されます。

- デデュープおよび圧縮が有効なディスク グループにキャパシティ ディスクを追加できます。ただし、デデュープおよび圧縮の効率を高めるには、キャパシティ ディスクを追加するのではなく、新しいディスク グループを作成してクラスタのストレージ容量を増やします。
- キャッシュ層からディスクを削除すると、ディスク グループ全体が削除されます。デデュープおよび圧縮が有効な場合にキャッシュ層ディスクを削除すると、データの退避がトリガされます。
- デデュープおよび圧縮はディスク グループ レベルで実装されています。デデュープおよび圧縮が有効なクラスタからキャパシティ ディスクを削除することはできません。ディスク グループ全体を削除する必要があります。
- キャパシティ ディスクで障害が発生すると、ディスク グループ全体が使用できなくなります。この問題を解決するには、障害が発生しているコンポーネントをただちに識別して置き換えます。障害が発生したディスク グループを削除する際は、[データの移行なし] オプションを使用します。

vSAN クラスタでの RAID 5 または RAID 6 イレージャ コーディングの使用

RAID 5 または RAID 6 イレージャ コーディングを使用して、データ損失から保護してストレージの効率を高めることができます。

イレージャ コーディングでは、ミラーリング (RAID 1) と同じレベルのデータ保護が可能であるのに加えて、使用するストレージ容量が少なく済みます。RAID 5 または RAID 6 イレージャ コーディングにより、vSAN はデータストア内で最大 2 個のキャパシティ デバイスまで障害を許容できます。4 つ以上のフォルト ドメインがあるオールフラッシュ クラスタでは、RAID 5 を構成できます。6 つ以上のフォルト ドメインがあるオールフラッシュ クラスタでは、RAID 5 または RAID 6 を構成できます。

RAID 5 または RAID 6 イレージャ コーディングでは、RAID 1 ミラーリングよりデータを保護するために必要な追加の容量が少なく済みます。たとえば、RAID 1 での [許容される障害の数] 値 1 で保護される仮想マシンで必要となる仮想ディスク サイズは 2 倍ですが、RAID 5 で必要となる仮想ディスク サイズは 1.33 倍です。次の表に、RAID 1 と RAID 5 または RAID 6 の全般的な比較を示します。

表 10-1. 各 RAID レベルでデータを保存して保護するために必要な容量

RAID 構成	許容される障害の数	データ サイズ	必要な容量
RAID 1 (ミラーリング)	1	100 GB	200 GB
4 つのフォルト ドメインがある RAID 5 または RAID 6 (イレージャ コーディング)	1	100 GB	133 GB
RAID 1 (ミラーリング)	2	100 GB	300 GB
6 つのフォルト ドメインがある RAID 5 または RAID 6 (イレージャ コーディング)	2	100 GB	150 GB

RAID 5 または RAID 6 イレージャ コーディングは、仮想マシン コンポーネントに適用できるポリシー属性です。RAID 5 を使用するには、[障害の許容方法] を [RAID-5/6 (イレージャ コーディング)] に、[許容される障害の数] を 1 に設定します。RAID 6 を使用するには、[障害の許容方法] を [RAID-5/6 (イレージャ コーディング)] に、[許容される障害の数] を 2 に設定します。RAID 5 または RAID 6 イレージャ コーディングでは、[許容される障害の数] の値を 3 に設定することはできません。

RAID 1 を使用するには、[障害の許容方法] を [RAID-1 (ミラーリング)] に設定します。RAID 1 ミラーリングではストレージ デバイスに対して必要な I/O 操作が少なくなるため、パフォーマンスが向上します。たとえば、RAID 1 ではクラスタ再同期を完了するのにかかる時間が短くなります。

注： vSAN ストレッチ クラスタで、[RAID-5/6 (イレージャ コーディング)] の [障害の許容方法] は、[サイトの耐障害性] 設定にのみ適用されます。

注： vSAN Express Storage Architecture クラスタの場合、使用するフォルト ドメインの数に応じて、[RAID 5] ([監視] > [vSAN] > [仮想オブジェクト] > testVM > [配置の詳細の表示]) に表示されるコンポーネントの数が変わります。クラスタで 6 つ以上のフォルト ドメインが使用可能な場合は、5 つのコンポーネントが [RAID 5] に表示されます。使用可能なフォルト ドメインが 5 個以下の場合は、3 つのコンポーネントが表示されます。

ポリシーの構成の詳細については、「[7 章 vSAN ポリシーの使用](#)」を参照してください。

vSAN クラスターの RAID 5 または RAID 6 の設計に関する考慮事項

vSAN クラスターで RAID 5 または RAID 6 イレージャ コーディングを構成する場合、次のガイドラインを考慮してください。

- RAID 5 または RAID 6 イレージャ コーディングは、オールフラッシュ ディスク グループでのみ使用できません。
- RAID 5 または RAID 6 をサポートするには、オンディスク フォーマット バージョン 3.0 以降が必要です。
- クラスターで RAID 5/6 を有効にするには、有効なライセンスが必要です。
- vSAN クラスターでデデュープおよび圧縮を有効にすると、さらに容量を節約できます。

vSAN クラスタでの暗号化の使用

11

vSAN クラスタで転送中のデータを暗号化し、vSAN データストアで保存データを暗号化できます。

vSAN では、vSAN クラスタ内のホスト間で転送中のデータを暗号化できます。転送中データの暗号化では、vSAN クラスタ内を移動するデータが保護されます。

vSAN では、vSAN データストアに保存されているデータを暗号化できます。保存データの暗号化を行うと、クラスタからデバイスが削除された場合に備えて、ストレージ デバイス上のデータが保護されます。

次のトピックを参照してください。

- [vSAN による転送中データの暗号化](#)
- [vSAN による保存データの暗号化](#)

vSAN による転送中データの暗号化

vSAN では、vSAN クラスタ内のホスト間でデータを移動するときに、転送中のデータを暗号化できます。

vSAN では、クラスタ内のホスト間で転送されるデータを暗号化できます。転送中データの暗号化を有効にすると、vSAN は、ホスト間で転送されるすべてのデータとメタデータのトラフィックを暗号化します。

vSAN による転送中データの暗号化には次の特性があります。

- vSAN は転送中のデータに対して AES-256 ビットの暗号化を使用します。
- vSAN による転送中データの暗号化は、保存データの暗号化と関係ありません。それぞれを個別に有効または無効にすることができます。
- vSAN による転送中データの暗号化には前方秘匿性が適用されます。
- データ ホストと監視ホスト間のトラフィックが暗号化されます。
- VDFS プロキシと VDFS サーバ間のファイル サービス データ トラフィックが暗号化されます。
- vSAN ファイル サービスのホスト間接続が暗号化されます。

vSAN は、動的に生成され、ホスト間で共有される対称キーを使用します。ホストは、接続を確立するときに暗号化キーを動的に生成し、そのキーを使用してホスト間のすべてのトラフィックを暗号化します。キー管理サーバを使用して転送中データの暗号化を行う必要はありません。

各ホストは、クラスタに参加するときに認証され、信頼されたホストへの接続のみが許可されます。クラスタからホストを削除すると、そのホストの認証証明書が削除されます。

vSAN による転送中データの暗号化は、クラスタ全体の設定です。有効にすると、ホスト間で送信されるすべてのデータとメタデータのトラフィックが暗号化されます。

vSAN クラスタでの転送中データの暗号化の有効化

vSAN クラスタで構成パラメータを編集して、転送中データの暗号化を有効にすることができます。

手順

- 1 既存のクラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] の下で [サービス] を選択し、転送中データの暗号化の [編集] ボタンをクリックします。
- 4 クリックして、[転送中データの暗号化] を有効にし、再キー化間隔を選択します。
- 5 [適用] をクリックします。

結果

vSAN クラスタでは転送中データの暗号化が有効です。vSAN は、クラスタ内のホストとファイル サービスのホスト間接続で転送されるデータをすべて暗号化します。

vSAN による保存データの暗号化

vSAN では、vSAN データストアに保存されているデータを暗号化できます。

保存データの暗号化を有効にすると、vSAN は重複排除などの他のすべての処理が実行された後にデータを暗号化します。保存データの暗号化を行うと、クラスタからデバイスが削除された場合に備えて、ストレージ デバイス上のデータが保護されます。

vSAN データストアで暗号化を使用するには、いくつかの準備作業が必要です。環境が設定されたら、vSAN クラスタで保存データの暗号化を有効にすることができます。

保存データの暗号化を使用するには、外部のキー管理サーバ (KMS) または vSphere Native Key Provider が必要です。vSphere 暗号化の詳細については、『vSphere セキュリティ』を参照してください。

外部のキー管理サーバ (KMS)、vCenter Server システム、ESXi ホストを使用して、vSAN クラスタ内のデータを暗号化できます。vCenter Server は外部 KMS に暗号化キーを要求します。KMS はキーを生成して保存します。vCenter Server は KMS からキー ID を取得して、ESXi ホストに配布します。

vCenter Server は KMS キーを格納しませんが、キー ID のリストは保持します。

vSAN 保存データの暗号化の仕組み

保存データの暗号化を有効にすると、vSAN では、vSAN データストア内のすべてを暗号化します。

すべてのファイルが暗号化されるため、すべての仮想マシンとその対応するデータが保護されます。この暗号化および復号化タスクを実行できるのは、暗号化権限が付与されている管理者だけです。vSAN では、次のように暗号化キーを使用します。

- vCenter Server から KMS に AES-256 キー暗号化キー (KEK) が要求されます。vCenter Server では KEK の ID のみが保存されます。キー自体は保存されません。
- ESXi ホストでは、業界標準の AES-256 XTS モードを使用して、ディスクのデータを暗号化します。各ディスクでは、ランダムに生成された異なるデータ暗号化キー (DEK) が使用されます。
- 各 ESXi ホストでは、KEK を使用して、その DEK を暗号化し、暗号化された DEK をディスクに保存します。ホストでは KEK はディスクに保存されません。ホストは再起動すると、対応する ID を持つ KEK を KMS に要求します。その後、ホストは必要に応じて DEK を復号できます。
- ホスト キーは、データではなく、コア ダンプの暗号化に使用されます。同じクラスタに含まれるすべてのホストで、同じホスト キーが使用されます。サポート バンドルを収集する際に、コア ダンプの再暗号化のためにランダム キーが生成されます。パスワードを指定してランダム キーを暗号化することができます。

ホストが再起動すると、KEK を受け取るまで、ディスク グループをマウントしません。このプロセスが完了するには、数分以上かかることがあります。ディスク グループのステータスは、vSAN Health Service の [物理ディスク] > [ソフトウェア状態の健全性] で監視できます。

暗号化キーのパーシステンス

vSAN 7.0 Update 3 以降では、キー サーバが一時的にオフラインまたはアクセス不可の場合でも、保存データの暗号化は引き続き機能します。キーのパーシステンスを有効にすると、ESXi ホストは再起動後も暗号化キーを保持できます。

各 ESXi ホストは最初に暗号化キーを取得し、キー キャッシュに保持します。ESXi ホストに Trusted Platform Module (TPM) がある場合、暗号化キーは再起動後も TPM に保持されます。ホストは、暗号化キーを要求する必要がありません。暗号化キーは TPM に保持されているため、キー サーバに接続できない場合でも、暗号化操作を続行できます。

クラスタ ホストでキー パーシステンスを有効にするには、次のコマンドを使用します。

```
esxcli system settings encryption set --mode=TPM
```

```
esxcli system security keypersistence enable
```

暗号化キーのパーシステンスの詳細については、『vSphere セキュリティ』の「キー パーシステンスの概要」を参照してください。

vSphere Native Key Provider の使用

vSAN 7.0 Update 2 では、vSphere Native Key Provider がサポートされています。環境が vSphere Native Key Provider 用に設定されている場合、vSAN クラスタ内の仮想マシンを暗号化できます。詳細については、『vSphere セキュリティ』で「vSphere Native Key Provider の構成と管理」を参照してください。

vSphere Native Key Provider は、外部のキー管理サーバ (KMS) を必要としません。vCenter Server がキー暗号化キーを生成し、それを ESXi ホストに push します。次に、ESXi ホストがデータ暗号化キーを生成します。

注： vSphere Native Key Provider を使用する場合は、再構成タスクがスムーズに実行されるように、Native Key Provider のバックアップを作成してください。

vSphere Native Key Provider は、既存のキー サーバ インフラストラクチャと共存できます。

vSAN 保存データの暗号化を設計する際の考慮事項

保存データの暗号化を使用する場合、次のガイドラインを考慮してください。

- 暗号化する vSAN データストアと同じデータストアに、KMS サーバをデプロイしないでください。
- 暗号化は、CPU への負荷が高い処理です。AES-NI を使用すると、暗号化のパフォーマンスが大幅に向上します。BIOS で AES-NI を有効にします。
- vSAN ストレッチ クラスタ内の監視ホストは、vSAN 暗号化には関与しません。監視ホストは、vSAN オブジェクトとコンポーネントのサイズや UUID などのメタデータのみの顧客データを保存しません。

注： 監視ホストが別のクラスタで実行されているアプライアンスの場合は、そのホストに保存されているメタデータを暗号化できます。監視ホストを含むクラスタで保存データの暗号化を有効にします。

- コア ダンプに関するポリシーを確立します。コア ダンプは、機密情報を含む場合があるため、暗号化されています。コア ダンプを復号する場合は、このような機密情報を注意して扱ってください。ESXi のコア ダンプには、ESXi ホストのキーと、そこに保存されているデータのキーが含まれる場合があります。
 - vm-support バンドルを収集するときは、必ずパスワードを使用します。vSphere Client から、または vm-support コマンドを使用してサポート バンドルを生成するときに、パスワードを指定できます。パスワードを指定すると、内部キーを使用しているコア ダンプは、パスワードに基づくキーを使用するように再暗号化されます。暗号化されたコア ダンプがサポート バンドルに含まれている場合は、後でこのパスワードを使用して復号できます。暗号化されていないコア ダンプやログは、影響を受けません。
 - vm-support バンドルの作成時に指定するパスワードは、vSphere コンポーネント内で維持されません。サポート バンドルのパスワードは、記録しておく必要があります。

標準のキー プロバイダの設定

標準のキー プロバイダを使用して、vSAN データストアを暗号化するキーを配布します。

vSAN データストアを暗号化する前に、暗号化をサポートするように標準のキー プロバイダを設定する必要があります。そのタスクには、vCenter Server に KMS を追加したり、KMS との間で信頼関係を確立したりする作業が伴います。vCenter Server は、キー プロバイダから暗号化キーをプロビジョニングします。

KMS は、KMIP (Key Management Interoperability Protocol) 1.1 標準をサポートする必要があります。詳細については、『vSphere 互換性マトリックス』を参照してください。

vCenter Server への KMS の追加

vSphere Client からキー管理サーバ (KMS) を vCenter Server システムに追加します。

標準のキー プロバイダは、最初の KMS インスタンスを追加するときに vCenter Server によって作成されます。キー プロバイダを 2 台以上の vCenter Server で構成する場合は、同じキー プロバイダ名を使用するようにしてください。

注： 暗号化する vSAN クラスタに KMS サーバをデプロイしないでください。障害が発生した場合、vSAN クラスタ内のホストから KMS に通信する必要があります。

- KMS を追加するときに、このキー プロバイダをデフォルトとして設定するように求められます。デフォルトの設定は、後から明示的に変更することができます。
- vCenter Server によって 1 つ目のキー プロバイダが作成された後で、同じベンダーの KMS インスタンスをキー プロバイダに追加してすべての KMS インスタンスを構成すると、KMS インスタンス間でキーを同期させることができます。KMS ベンダーが定める方法を使用してください。
- キー プロバイダに設定できる KMS インスタンスは 1 個だけです。
- ご使用の環境がさまざまなベンダーの KMS ソリューションをサポートしている場合は、複数のキー プロバイダを追加することができます。

前提条件

- キー管理サーバが vSphere 互換性マトリックス にあり、KMIP 1.1 に準拠していることを確認してください。
- 必要な権限 Cryptographer.ManageKeyServers を有していることを確認してください。
- IPv6 アドレスのみを使用して KMS に接続することはできません。
- ユーザー名またはパスワードを要求するプロキシ サーバを介して KMS に接続することはできません。

手順

- 1 vCenter Server にログインします。
- 2 インベントリ リストを参照し、vCenter Server インスタンスを選択します。
- 3 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] をクリックします。
- 4 [標準のキー プロバイダの追加] をクリックしてキー プロバイダの情報を入力し、[キー プロバイダの追加] をクリックします。

[KMS の追加] をクリックすると、キー管理サーバを追加できます。

- 5 [信頼] をクリックします。

vCenter Server にキー プロバイダが追加され、ステータスは「接続済み」と表示されます。

証明書の交換による標準キー プロバイダの信頼された接続の確立

vCenter Server システムに標準キー プロバイダを追加した後に、信頼された接続を確立することができます。

実際のプロセスは、キー プロバイダが受け入れた証明書と企業ポリシーによって異なります。

前提条件

標準キー プロバイダを追加します。

手順

- 1 vCenter Server に移動します。
- 2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。
- 3 キー プロバイダを選択します。
キー プロバイダの KMS が表示されます。
- 4 KMS を選択します。
- 5 [信頼の確立] ドロップダウン メニューから [KMS が vCenter Server を信頼するようにします] を選択します。
- 6 ご使用のサーバに適したオプションを選択し、該当する手順を実行します。

オプション	詳細については、ドキュメントを参照してください。
vCenter Server ルート CA 証明書	[[ルート CA 証明書] オプションによる標準キー プロバイダの信頼済み接続の確立]。
vCenter Server 証明書	[[証明書] オプションによる標準キー プロバイダの信頼済み接続の確立]。
証明書およびプライベート キーのアップロード	[[証明書およびプライベート キーのアップロード] オプションによる標準キー プロバイダの信頼済み接続の確立]。
新規証明書署名要求	[[新規証明書署名リクエスト] オプションによる標準キー プロバイダの信頼済み接続の確立]。

[ルート CA 証明書] オプションによる標準キー プロバイダの信頼済み接続の確立

一部のキー管理サーバ (KMS) ベンダーでは、KMS にルート CA 証明書をアップロードすることが要求されます。

ルート CA によって署名されたすべての証明書は、この KMS によって信頼されます。vSphere 仮想マシンの暗号化で使用されるルート CA 証明書は、vCenter Server システムの VMware Endpoint Certificate Store (VECS) 内にある独立したストアに保存される自己署名証明書です。

注： ルート CA 証明書を生成するのは、既存の証明書を置き換える場合に限定してください。生成すると、そのルート CA によって署名された他の証明書は無効になります。新しいルート CA 証明書は、このワークフローの一部として生成できます。

手順

- 1 vCenter Server に移動します。
- 2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。
- 3 信頼された接続を確立するキー プロバイダを選択します。
キー プロバイダの KMS が表示されます。
- 4 [信頼の確立] ドロップダウン メニューから [KMS が vCenter Server を信頼するようにします] を選択します。
- 5 [vCenter Server ルート CA 証明書] を選択し、[次へ] をクリックします。
vCenter Server が暗号化に使用するルート証明書に基づいて、[ルート CA 証明書のダウンロード] ダイアログ ボックスが入力されます。この証明書は、VECS に保存されます。
- 6 証明書をクリップボードにコピーするか、ファイルとしてダウンロードします。

7 KMS ベンダーからの指示に従って証明書をベンダーのシステムにアップロードします。

注： 一部の KMS ベンダーでは、アップロードしたルート証明書を取得する際に、KMS の再起動が要求されます。

次のステップ

証明書の交換を完了します。「標準のキー プロバイダの信頼設定の完了」を参照してください。

[証明書] オプションによる標準キー プロバイダの信頼済み接続の確立

一部のキー管理サーバ (KMS) ベンダーでは、KMS に vCenter Server 証明書をアップロードすることが要求されます。

アップロード後、KMS はその証明書を使用しているシステムからのトラフィックを受け付けます。vCenter Server は、KMS との接続を保護するための証明書を生成します。証明書は、vCenter Server システムの VMware Endpoint Certificate Store (VECS) 内にある独立したキー ストアに保存されます。

手順

- 1 vCenter Server に移動します。
- 2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。
- 3 信頼された接続を確立するキー プロバイダを選択します。
キー プロバイダの KMS が表示されます。
- 4 [信頼の確立] ドロップダウン メニューから [KMS が vCenter Server を信頼するようにします] を選択します。
- 5 [vCenter Server 証明書] を選択し、[次へ] をクリックします。
vCenter Server が暗号化に使用するルート証明書に基づいて、[証明書のダウンロード] ダイアログ ボックスが入力されます。この証明書は、VECS に保存されます。

注： 既存の証明書を置き換える場合を除き、新しい証明書を生成しないでください。

- 6 証明書をクリップボードにコピーするか、ファイルとしてダウンロードします。
- 7 KMS ベンダーからの指示に従って証明書を KMS にアップロードします。

次のステップ

信頼関係を確立します。「標準のキー プロバイダの信頼設定の完了」を参照してください。

[新規証明書署名リクエスト] オプションによる標準キー プロバイダの信頼済み接続の確立

一部のキー管理サーバ (KMS) ベンダーでは、vCenter Server が証明書署名リクエスト (CSR) を生成して KMS に送信することが要求されます。

KMS は CSR に署名し、署名済み証明書を返します。この署名済み証明書を vCenter Server にアップロードしてください。[新規証明書署名リクエスト] オプションを使用するには、2 つのステップを実行します。まず、CSR を生成して KMS ベンダーに送信します。次に、KMS ベンダーから受け取った署名済み証明書を vCenter Server にアップロードします。

手順

- 1 vCenter Server に移動します。
- 2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。
- 3 信頼された接続を確立するキー プロバイダを選択します。
キー プロバイダの KMS が表示されます。
- 4 [信頼の確立] ドロップダウン メニューから [KMS が vCenter Server を信頼するようにします] を選択します。
- 5 [新規証明書署名リクエスト (CSR)] を選択し、[次へ] をクリックします。
- 6 ダイアログ ボックスで、テキスト ボックス内の証明書全体をクリップボードにコピーするか、ファイルとしてダウンロードします。
ダイアログ ボックスの [新規の証明書署名要求の生成] ボタンは、明示的に CSR を生成する場合にのみ使用します。
- 7 KMS ベンダーからの指示に従って CSR を送信します。
- 8 KMS ベンダーから署名付き証明書を受け取ったら、[キー プロバイダ] を再度クリックしてキー プロバイダを選択し、[信頼の確立] ドロップダウン メニューから、[署名済みの証明書署名要求の証明書のアップロード] を選択します。
- 9 一番下にあるテキスト ボックスに署名付き証明書を貼り付けるか、[ファイルのアップロード] をクリックしてファイルをアップロードし、[アップロード] をクリックします。

次のステップ

信頼関係を確立します。「[標準のキー プロバイダの信頼設定の完了](#)」を参照してください。

[証明書およびプライベート キーのアップロード] オプションによる標準キー プロバイダの信頼済み接続の確立
一部のキー管理サーバ (KMS) ベンダーでは、KMS サーバ証明書およびプライベート キーを vCenter Server システムにアップロードすることが要求されます。

一部の KMS ベンダーは、接続のための証明書およびプライベート キーを生成し、ユーザーが利用できるようにしています。ファイルをアップロードすると、KMS は vCenter Server インスタンスを信頼します。

前提条件

- 証明書およびプライベート キーを KMS ベンダーに要求します。ファイルは、PEM 形式の X509 ファイルです。

手順

- 1 vCenter Server に移動します。
- 2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。
- 3 信頼された接続を確立するキー プロバイダを選択します。
キー プロバイダの KMS が表示されます。

- 4 [信頼の確立] ドロップダウン メニューから [KMS が vCenter Server を信頼するようにします] を選択します。
- 5 [KMS 証明書およびプライベート キー] を選択し、[次へ] をクリックします。
- 6 一番上にあるテキスト ボックスに KMS ベンダーから受け取った証明書を貼り付けるか、[ファイルのアップロード] をクリックして証明書ファイルをアップロードします。
- 7 一番下にあるテキスト ボックスにキー ファイルを貼り付けるか、[ファイルのアップロード] をクリックしてキー ファイルをアップロードします。
- 8 [信頼の確立] をクリックします。

次のステップ

信頼関係を確立します。標準のキー プロバイダの信頼設定の完了を参照してください。

vSphere Client を使用したデフォルトのキー プロバイダの設定

vSphere Client を使用して、デフォルトのキー プロバイダを vCenter Server レベルで設定できます。

1 つ目のキー プロバイダをデフォルトにしない場合や、ご利用の環境で複数のキー プロバイダを使用していてデフォルトのプロバイダを削除した場合、デフォルトのキー プロバイダを設定する必要があります。

前提条件

ベスト プラクティスとして、[キー プロバイダ] タブの [接続状態] に [アクティブ] と表示され、緑色のチェック マークが表示されていることを確認します。

手順

- 1 vSphere Client を使用してログインします。
- 2 vCenter Server に移動します。
- 3 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。
- 4 キー プロバイダを選択します。
- 5 [デフォルトとして設定] をクリックします。
確認のダイアログ ボックスが表示されます。
- 6 [デフォルトとして設定] をクリックします。
キー プロバイダが現在のデフォルトとして表示されます。

標準のキー プロバイダの信頼設定の完了

[標準のキー プロバイダの追加] ダイアログで KMS を信頼するように促すメッセージが表示されなかった場合は、証明書の交換が完了した後で信頼を明示的に確立する必要があります。

KMS を信頼するか、KMS 証明書をアップロードすることにより vCenter Server が KMS を信頼するように設定すると、信頼関係の設定が完了します。これには次の 2 つのオプションがあります。

- [KMS 証明書のアップロード] オプションを使用して明示的に証明書を信頼します。

- [vCenter Server が KMS を信頼するようにします] オプションを使用して KMS リーフ証明書または KMS CA 証明書を vCenter Server にアップロードします。

注： ルート CA 証明書または中間 CA 証明書をアップロードすると、その CA で署名されたすべての証明書が vCenter Server で信頼されるようになります。セキュリティを強化するために、KMS ベンダーで管理されている リーフ証明書または中間 CA 証明書をアップロードするようにしてください。

手順

- 1 vCenter Server に移動します。
- 2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。
- 3 信頼された接続を確立するキー プロバイダを選択します。
キー プロバイダの KMS が表示されます。
- 4 KMS を選択します。
- 5 [信頼の確立] ドロップダウン メニューから次のいずれかのオプションを選択します。

オプション	操作
vCenter Server が KMS を信頼するようにします	表示されたダイアログ ボックスで、[信頼] をクリックします。
KMS 証明書のアップロード	a 表示されたダイアログ ボックスで、証明書を貼り付けるか、[ファイルのアップロード] をクリックして証明書ファイルを参照します。 b [アップロード] をクリックします。

新しい vSAN クラスタでの保存データの暗号化の有効化

新しい vSAN クラスタを構成する際に、保存データの暗号化を有効にすることができます。

前提条件

- 必要な権限：
 - Host.Inventory.EditCluster
 - Cryptographer.ManageEncryptionPolicy
 - Cryptographer.ManageKMS
 - Cryptographer.ManageKeys
- あらかじめ、標準のキー プロバイダを設定して、vCenter Server と KMS 間で信頼された接続を確立しておく必要があります。

手順

- 1 既存のクラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] の下で [サービス] を選択し、暗号化の [編集] ボタンをクリックします。

- 4 [vSAN サービス] ダイアログで [暗号化] を有効にし、KMS クラスタまたはキー プロバイダを選択します。

注： vSAN 暗号化を有効にする前にデバイスから残存データを消去するには、[残存データの消去] チェックボックスを使用します。仮想マシン データを含むクラスタを暗号化するときに、ストレージ デバイスから既存のデータを消去する場合を除き、このチェック ボックスはオフにしてください。これにより、vSAN 暗号化を有効にした後に、暗号化されていないデータがデバイスに保存されなくなります。ストレージ デバイスに仮想マシン データが存在しない新規インストールの場合、この設定は必要ありません。

- 5 クラスタの構成を完了します。

結果

vSAN クラスタでは保存データの暗号化が有効です。vSAN では、vSAN データストアに追加されたすべてのデータを暗号化します。

保存データの暗号化の新しいキーの生成

保存データの暗号化のキーの有効期限が切れたり、キーが漏えいしたりした場合は、新しいキーを生成できます。

vSAN クラスタの新しい暗号化キーを生成する際には、次のオプションを利用できます。

- 新しい KEK を生成すると、vSAN クラスタ内のすべてのホストが、新しい KEK を KMS から受け取ります。この新しい KEK を使用して、各ホストの DEK が再暗号化されます。
- 深い再キー化を実行し、新しいキーを使用してすべてのデータを再暗号化する場合は、新しい KEK と DEK が生成されます。データを再暗号化するには、ディスクのローリング再フォーマットが必要です。

前提条件

- 必要な権限：
 - Host.Inventory.EditCluster
 - Cryptographer.ManageKeys
- あらかじめ、キー プロバイダを設定して、vCenter Server と KMS 間で信頼された接続を確立しておく必要があります。

手順

- 1 vSAN ホスト クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] の下で [サービス] を選択します。
- 4 [新しい暗号化キーの生成] をクリックします。
- 5 新しい KEK を生成するには、[適用] をクリックします。この新しい KEK を使用して、DEK が再暗号化されません。
 - 新しい KEK と DEK を生成して、vSAN クラスタのすべてのデータを再暗号化するには、[新しいキーを使用してストレージのすべてのデータの再暗号化も行う] チェック ボックスを選択します。

- vSAN クラスタのリソースに制限がある場合は、[冗長性の低下を許可] チェック ボックスを選択します。冗長性の低下を許可した場合、ディスクの再フォーマット操作中にデータにリスクが及ぶおそれがあります。

既存の vSAN クラスタでの保存データの暗号化の有効化

既存の vSAN OSA および vSAN ESA クラスタで保存データの暗号化を有効にできます。

前提条件

- 必要な権限：
 - Host.Inventory.EditCluster
 - Cryptographer.ManageEncryptionPolicy
 - Cryptographer.ManageKMS
 - Cryptographer.ManageKeys
- あらかじめ、標準のキー プロバイダを設定して、vCenter Server と KMS 間で信頼された接続を確立しておく必要があります。
- クラスタのディスク要求モードは [手動] に設定する必要があります。

手順

- 1 vSAN ホスト クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 vSAN で [サービス] を選択します。
- 4 暗号化の [編集] ボタンをクリックします。
- 5 [vSAN サービス] ダイアログで [暗号化] を有効にし、KMS クラスタまたはキー プロバイダを選択します。
- 6 (オプション) クラスタのストレージ デバイスに秘密データが含まれる場合は、[残存データの消去] を選択します。

この設定により、暗号化の際にストレージ デバイスの既存データを消去するように vSAN に指示されます。このオプションでは各ディスクの処理に時間がかかることがあるため、ディスクに不要なデータがある場合を除き、選択しないでください。

- 7 [適用] をクリックします。

結果

vSAN によって vSAN データストアのすべてのデータが暗号化される際に、すべてのディスク グループのローリング再フォーマットが行われます。

次のステップ

クラスタの暗号化はいつでも無効にできます。vSAN はデータストア内のすべてのデータを復号するため、ディスクの再フォーマットが必要です。

vSAN の暗号化とコア ダンプ

vSAN クラスタで保存データの暗号化を使用している場合に ESXi ホストでエラーが発生すると、その結果として出力されるコア ダンプはデータを保護するために暗号化されます。

vm-support パッケージに含まれるコア ダンプも暗号化されます。

注： コア ダンプには機密情報が含まれることがあります。コア ダンプを使用する際は、組織のデータ セキュリティおよびプライバシーに関するポリシーに従ってください。

ESXi ホスト上のコア ダンプ

ESXi ホストがクラッシュすると、暗号化されたコア ダンプが生成され、ホストが再起動されます。このコア ダンプの暗号化には、ESXi キー キャッシュ内のホスト キーが使用されます。次に実行できることは、いくつかの要素によって決まります。

- ほとんどの場合、vCenter Server はホストのキーを KMS から取得し、そのキーを再起動後の ESXi ホストにプッシュしようと試みます。この操作が成功すると、vm-support パッケージを生成して、コア ダンプを復号化または再暗号化できるようになります。
- vCenter Server から ESXi ホストに接続できない場合、KMS からキーを取得できる可能性があります。
- ホストでカスタム キーを使用していて、そのキーが vCenter Server からホストにプッシュされたキーと異なる場合は、コア ダンプを操作できません。カスタム キーの使用は避けてください。

コア ダンプと vm-support パッケージ

深刻なエラーが発生して VMware テクニカル サポートに連絡すると、サポート担当者は通常、vm-support パッケージを生成するように要請します。このパッケージには、ログ ファイルのほか、コア ダンプなどの情報が含まれます。サポート担当者がログ ファイルやその他の情報を調べても問題を解決できない場合は、コア ダンプを復号化することで、関連情報を参照可能にできる可能性があります。組織のセキュリティ ポリシーとプライバシー ポリシーに基づき、ホスト キーなどの機密情報を保護してください。

vCenter Server システム上のコア ダンプ

vCenter Server システム上のコア ダンプは、暗号化されていません。vCenter Server にはすでに、機密である可能性のある情報が存在します。少なくとも、vCenter Server が保護されていることを確認します。また、vCenter Server システムのコア ダンプを無効にすることも考えられます。ログ ファイル内のその他の情報によって問題を特定できる可能性があります。

暗号化された vSAN データストアで ESXi ホストの vm-support パッケージを収集する

vSAN クラスタで保存データの暗号化が有効な場合は、vm-support パッケージに含まれるコア ダンプがすべて暗号化されます。

パッケージを収集し、後でコア ダンプを復号する必要がある場合は、パスワードを指定できます。vm-support パッケージにはログ ファイルやコア ダンプ ファイルなどが含まれています。

前提条件

vSAN データストアの保存データの暗号化が有効であることをサポート担当者に伝えてください。サポート担当者から、コア ダンプを復号して必要な情報を抽出するように依頼される場合がありますが、

注： コア ダンプには機密情報が含まれることがあります。組織のセキュリティ ポリシーとプライバシー ポリシーに基づき、ホスト キーなどの機密情報を保護してください。

手順

- 1 vSphere Client を使用して、vCenter Server にログインします。
- 2 [ホストおよびクラスタ] をクリックし、ESXi ホストを右クリックします。
- 3 [システム ログのエクスポート] を選択します。
- 4 ダイアログ ボックスで [暗号化されたコア ダンプ用のパスワード] を選択し、パスワードを入力して、確認のために再度パスワードを入力します。
- 5 その他のオプションはデフォルトのままにしておくか、VMware テクニカル サポートから依頼された場合は変更を加え、[完了] をクリックします。
- 6 ファイルの場所を指定します。
- 7 vm-support パッケージ内のコア ダンプを復号するようにサポート担当者から依頼された場合は、いずれかの ESXi ホストにログインして次の手順を実行します。

- a ESXi にログインし、vm-support パッケージが配置されているディレクトリに接続します。

ファイル名は **esx.date_and_time.tgz** という形式になっています。

- b パッケージ自体、解凍されたパッケージ、および再圧縮されたパッケージを格納できる空き容量がディレクトリにあることを確認し、空き容量がない場合はパッケージを移動します。
- c パッケージをローカル ディレクトリに解凍します。

```
vm-support -x *.tgz .
```

解凍されたファイル階層には、ESXi ホストのコア ダンプ ファイル（通常は /var/core にあります）と、仮想マシンの複数のコア ダンプ ファイルが含まれている場合があります。

- d 暗号化されたコア ダンプ ファイルを個別に復号します。

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

vm-support-incident-key-file の部分では、ディレクトリの最上位レベルにあるインシデント キー ファイルを指定します。

encryptedZdump の部分では、暗号化されたコア ダンプ ファイルの名前を指定します。

decryptedZdump の部分では、コマンド実行後に生成されるファイルの名前を指定します。
encryptedZdump で指定するファイル名に似た名前を使用してください。

- e `vm-support` パッケージの作成時に指定したパスワードを入力します。
- f 暗号化されたコア ダンプを削除し、パッケージを再び圧縮します。

```
vm-support --reconstruct
```

- 8 機密情報を含むファイルがある場合は、それらのファイルも削除します。

ESXi ホストで暗号化されたコア ダンプの復号と再暗号化

ESXi ホスト上で暗号化されているコア ダンプは `crypto-util` CLI を使用して復号または再暗号化できます。

`vm-support` パッケージに含まれるコア ダンプは手動で復号し、確認できます。コア ダンプには機密情報が含まれることがあります。組織のセキュリティ ポリシーとプライバシー ポリシーに基づき、ホスト キーなどの機密情報を保護してください。

コア ダンプの再暗号化と `crypto-util` のその他の機能の詳細については、コマンドライン ヘルプを参照してください。

注： `crypto-util` は上級ユーザー向けのコマンドです。

前提条件

コア ダンプの暗号化に使用された ESXi ホスト キーが、コア ダンプを生成した ESXi ホストで使用可能であることが必要です。

手順

- 1 コア ダンプが存在する ESXi ホストに直接ログインします。

ESXi ホストがロックダウン モードになっている場合や、SSH アクセスが有効になっていない場合は、最初にアクセスを有効にしなければならないことがあります。

- 2 コア ダンプが暗号化されているかどうかを確認します。

オプション	説明
コア ダンプの監視	<code>crypto-util envelope describe vmmcores.ve</code>
zdump ファイル	<code>crypto-util envelope describe --offset 4096 zdumpFile</code>

- 3 種類に応じてコア ダンプを復号します。

オプション	説明
コア ダンプの監視	<code>crypto-util envelope extract vmmcores.ve vmmcores</code>
zdump ファイル	<code>crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted</code>

vSAN クラスタのアップグレード

12

vSAN のアップグレード プロセスにはいくつかの段階があり、ここで説明する順序でアップグレード手順を実行する必要があります。

注： vSphere Client または Ruby vSphere Console (RVC) を使用して vSAN Original Architecture クラスタを vSAN Express Storage Architecture クラスタにアップグレードすることはできません。

アップグレードを開始する前に、アップグレード プロセス全体を明確に理解し、アップグレード作業を中断することなくスムーズに実行できるようにしてください。一般的な vSphere アップグレード手順に精通していない場合は、まず『vSphere のアップグレード』ドキュメントを読んでください。

注： ここで説明されているアップグレード タスクの順序どおりにできない場合、データ損失やクラスタの障害が発生する原因となります。

vSAN クラスタのアップグレード タスクは、次の順序で実行します。

- 1 vCenter Server をアップグレードします。『vSphere のアップグレード』のドキュメントを参照してください。
- 2 ESXi ホストをアップグレードします。ESXi ホストのアップグレードを参照してください。アップグレードに向けた ESXi ホストの移行および準備の詳細については、『vSphere のアップグレード』ドキュメントを参照してください。
- 3 vSAN ディスク フォーマットをアップグレードします。ディスク フォーマットのアップグレードは任意ですが、最適な結果を得るには、最新のバージョンを使用するようにオブジェクトをアップグレードします。オンディスク フォーマットでは、環境内で vSAN の完全な機能セットを使用できます。RVC を使用した vSAN のディスク フォーマットのアップグレードを参照してください。

次のトピックを参照してください。

- vSAN のアップグレードの準備
- vCenter Server のアップグレード
- ESXi ホストのアップグレード
- vSAN ディスク フォーマットについて
- vSAN オブジェクト フォーマットについて
- vSAN クラスタのアップグレードの確認
- vSAN クラスタのアップグレード中の RVC アップグレード コマンド オプションの使用

■ vSphere Lifecycle Manager の vSAN ビルドの推奨事項

vSAN のアップグレードの準備

フェイルセーフとなるようにアップグレードを計画および設計します。

vSAN をアップグレードする前に、ご使用の環境が vSphere のハードウェア要件とソフトウェア要件を満たしていることを確認してください。

アップグレードの前提条件

アップグレードプロセス全体の遅れにつながる要因について考慮します。ガイドラインおよびベストプラクティスについては、『vSphere のアップグレード』ドキュメントを参照してください。

クラスタをアップグレードする前に主な要件を確認します。

表 12-1. アップグレードの前提条件

アップグレードの前提条件	説明
ソフトウェア、ハードウェア、ドライバ、ファームウェア、およびストレージ I/O コントローラ	vSAN の新しいバージョンで、使用する予定のソフトウェアとハードウェアコンポーネント、ドライバ、ファームウェア、ストレージ I/O コントローラがサポートされていることを確認します。サポートされているアイテムは、VMware 互換性ガイドの Web サイト [http://www.vmware.com/resources/compatibility/search.php] に記載されています。
vSAN のバージョン	vSAN の最新バージョンを使用していることを確認します。ベータ版から新しい vSAN にはアップグレードできません。ベータ版からアップグレードする場合は、vSAN を新規に導入する必要があります。
ディスク容量	ソフトウェアバージョンのアップグレードを完了するのに十分な空き容量があることを確認します。vCenter Server のインストールに必要なディスクストレージ容量は、vCenter Server の構成によって異なります。vSphere のアップグレードに必要なディスク容量のガイドラインについては、『vSphere のアップグレード』ドキュメントを参照してください。
vSAN ディスクフォーマット	vSAN ディスクフォーマットは、データの退避や再構築を必要としないメタデータのアップグレードです。
vSAN ホスト	vSAN ホストがメンテナンスモードになっており、[データのアクセシビリティの確保] または [全データの退避] オプションが選択されていることを確認します。 アップグレードプロセスの自動化およびテストには、vSphere Lifecycle Manager を使用できます。vSphere Lifecycle Manager を使用して vSAN をアップグレードする場合、デフォルトの退避モードは [データのアクセシビリティの確保] になります。[データのアクセシビリティの確保] モードを使用する場合、データは保護されず、vSAN のアップグレード中に障害が発生した場合は、予期しないデータ消失が発生する可能性があります。ただし、[データのアクセシビリティの確保] モードでは、すべてのデータをクラスタ内の別のホストに移動する必要がないため、[全データの退避] モードの場合よりも短時間で処理されます。さまざまな退避モードの詳細については、『VMware vSAN の管理』ドキュメントを参照してください。
仮想マシン	仮想マシンがバックアップされていることを確認します。

推奨

vSAN で使用できるように ESXi ホストをデプロイする場合は、次の推奨事項について考慮してください。

- ESXi ホストが 512 GB 以下のメモリ容量で構成されている場合は、インストール メディアとして SATADOM、SD、USB、またはハード ディスク デバイスを使用します。
- ESXi ホストが 512 GB より大きいメモリ容量で構成されている場合は、インストール デバイスとして別個の磁気ディスクまたはフラッシュ デバイスを使用します。別個のデバイスを使用する場合は、vSAN がそのデバイスを使用しないことを確認します。
- vSAN ホストを SATADOM デバイスから起動する場合は、シングルレベル セル (SLC) デバイスを使用し、起動デバイスのサイズを少なくとも 16 GB にする必要があります。
- ハードウェアが vSAN の要件を満たしていることを確認するには、『vSAN のプランニングとデプロイ』を参照してください。

vSAN 6.5 以降では、vSAN クラスタに含まれる ESXi ホストの起動サイズの要件を調整できます。

2 ホスト構成のクラスタまたは vSAN ストレッチ クラスタ内の監視ホストのアップグレード

2 ホスト クラスタまたは vSAN ストレッチ クラスタの監視ホストは、vSAN クラスタの外部に配置されますが、同じ vCenter Server で管理されます。vSAN データ ホストと同じプロセスを使用して、監視ホストをアップグレードできます。

データ ホストをアップグレードする前に、監視ホストをアップグレードします。

vSphere Lifecycle Manager を使用して複数のホストを並行してアップグレードすると、データ ホストのいずれかと並行して、監視ホストがアップグレードされる場合があります。アップグレードの問題を回避するには、データ ホストと並行して監視ホストがアップグレードされないように、vSphere Lifecycle Manager を設定してください。

vCenter Server のアップグレード

vSAN のアップグレード処理において最初に実行するタスクは、vSphere の全般的なアップグレードです。これには、vCenter Server および ESXi ホストのアップグレードが含まれます。

VMware は、64 ビット システムにおいて、vCenter Server 4.x、vCenter Server 5.0.x、vCenter Server 5.1.x、および vCenter Server 5.5 から vCenter Server 6.0 以降へのインプレース アップグレードをサポートします。vCenter Server のアップグレードには、データベース スキーマのアップグレードと vCenter Server のアップグレードが含まれます。

ESXi 7.0 へのアップグレードの詳細とサポート レベルは、アップグレードするホストと使用するアップグレード方法によって異なります。ESXi の現在のバージョンからアップグレード予定バージョンへのアップグレードパスがサポートされていることを確認します。詳細については、http://www.vmware.com/resources/compatibility/sim/interop_matrix.php の「VMware 製品の相互運用性マトリックス」を参照してください。

vCenter Server へのインプレース アップグレードを行う代わりに、別のマシンを使用してアップグレードを行うことができます。詳細な手順とアップグレード オプションについては、『vCenter Server のアップグレード』を参照してください。

ESXi ホストのアップグレード

vCenter Server をアップグレードした後、vSAN クラスタのアップグレードの次のタスクとして、ESXi ホストを最新バージョンにアップグレードします。

次のものを使用して、vSAN クラスタの ESXi ホストをアップグレードできます。

- vSphere Lifecycle Manager : vSphere Lifecycle Manager では、イメージまたはベースラインを使用して、ESXi クラスタの vSAN ホストをアップグレードできます。デフォルトの退避モードは、[データ アクセシビリティの確保] です。このモードを使用しているときに、vSAN のアップグレード中に障害が発生すると、いずれかのホストがオンラインに戻るまでデータにアクセスできなくなる可能性があります。退避モードおよびメンテナンス モードの詳細については、「[メンテナンス モードでの vSAN クラスタのメンバーの操作](#)」を参照してください。アップグレードとアップデートの詳細については、『[ホストとクラスタのライフサイクルの管理](#)』を参照してください。
- Esxcli コマンド : 新しいソフトウェア配布としてコンポーネント、基本イメージ、アドオンを使用し、手動アップグレードで ESXi 7.0 ホストの更新またはパッチ適用を行うことができます。

フォルト ドメインが構成された vSAN クラスタをアップグレードすると、vSphere Lifecycle Manager は単一フォルト ドメイン内のホストをアップグレードし、その後、次のホストの処理に進みます。これにより、クラスタ内のすべてのホストで同じ vSphere バージョンが実行されます。vSAN ストレッチ クラスタをアップグレードする場合、vSphere Lifecycle Manager は優先サイトのすべてのホストをアップグレードし、その後、セカンダリ サイトのホストの処理に進みます。これにより、クラスタ内のすべてのホストで同じ vSphere バージョンが実行されます。vSAN ストレッチ クラスタのアップグレードの詳細については、『[ホストとクラスタのライフサイクルの管理](#)』を参照してください。

ESXi ホストをアップグレードする前に、『[vSphere のアップグレード](#)』に記載されているベスト プラクティスを確認してください。VMware は、いくつかの ESXi アップグレード オプションを提供しています。アップグレードするホストのタイプに応じて、最適なアップグレード オプションを選択してください。詳細な手順とアップグレード オプションについては、『[VMware ESXi のアップグレード](#)』を参照してください。

次のステップ

- 1 (オプション) vSAN ディスク フォーマットをアップグレードします。[RVC を使用した vSAN のディスク フォーマットのアップグレード](#) を参照してください。
- 2 ホストのライセンスを確認します。多くの場合、ホストのライセンスを再度適用する必要があります。ホストのライセンス適用の詳細については、『[vCenter Server およびホスト管理](#)』を参照してください。
- 3 (オプション) vSphere Client または vSphere Lifecycle Manager を使用して、ホスト上の仮想マシンをアップグレードします。

vSAN ディスク フォーマットについて

ESXi の更新が完了したら、vSAN の完全な機能セットにアクセスできるように vSAN オンディスク フォーマットをアップグレードします。

各 vSAN リリースでは、以前のリリースのオンディスク フォーマットがサポートされています。クラスタのすべてのホストが、同じオンディスク フォーマットになっている必要があります。一部の機能は、オンディスク フォーマット バージョンに関連付けられているため、vSAN オンディスク フォーマットを ESXi バージョンでサポートされている最新バージョンにアップグレードすることをお勧めします。詳細については、[<https://kb.vmware.com/s/article/2148493>] を参照してください。

vSAN オンディスク フォーマット バージョン 3 以降では、メタデータのアップグレードのみが必要です。この処理には数分かかります。オンディスク フォーマットのアップグレード中は、ディスクの退避や再構成は実行されません。

アップグレードをスムーズに実行できるように、vSAN オンディスク フォーマットをアップグレードする前に [アップグレードの事前チェック] を実行してください。事前チェックでは、障害のあるディスクや良好な状態でないオブジェクトなど、アップグレードの成功を妨げる可能性のある潜在的な問題を特定します。

注： オンディスク フォーマットをアップグレードすると、ホストへのソフトウェアのロールバックや、特定の古いホストをクラスタに追加することができなくなります。

vSphere Client を使用した vSAN ディスク フォーマットのアップグレード

vSAN ホストのアップグレードが完了したら、ディスク フォーマットのアップグレードを実行します。

注： 既存の vSAN クラスタで暗号化やデデュープと圧縮を有効にすると、オンディスク フォーマットが自動的に最新バージョンにアップグレードされます。この手順は必須ではありません。vSAN 設定の編集を参照してください。

前提条件

- vCenter Server のバージョンをアップデートしていることを確認します。
- ESXi ホストの最新バージョンを使用していることを確認します。
- ディスクが健全な状態であることを確認します。[ディスク管理] 画面に移動してオブジェクトのステータスを確認します。
- 使用するハードウェアとソフトウェアが『VMware 互換性ガイド』の Web サイト (<http://www.vmware.com/resources/compatibility/search.php>) に記載され、認証されていることを確認します。
- ディスク フォーマットのアップグレードに十分な空き容量があることを確認します。RVC コマンド `vsan.whatif_host_failures` を実行して、アップグレードを完了するため、またはアップグレード中に障害が発生した場合にコンポーネントを再構築するための十分な容量があることを確認します。
- ホストがメンテナンス モードではないことを確認します。ディスク フォーマットのアップグレード時には、ホストをメンテナンス モードにしないでください。vSAN クラスタのメンバー ホストのいずれかがメンテナンス モードになると、そのメンバー ホストのキャパシティはクラスタに含まれなくなります。そのため、クラスタのキャパシティが減少し、クラスタのアップグレードに失敗する場合があります。
- vSAN クラスタでコンポーネントの再構築タスクが進行していないことを確認します。vSAN の再同期の詳細については、『vSphere の監視とパフォーマンス』を参照してください。

The screenshot shows the VMware vSAN cluster configuration interface. The left sidebar lists various configuration options, with 'Disk Management' selected under the 'vSAN' section. The main area displays a warning about upgrading older disks and offers 'UPGRADE' and 'PRE-CHECK UPGRADE' buttons. Below this, there are options to 'CLAIM UNUSED DISKS', 'ADD DISKS', and 'PRE-CHECK DATA MIGRATION'. A table shows the current disk groups and their status.

Disk Group	Disks in Use	State	vSAN Health Status
10.26.235.157	9 of 9	Connected	Healthy
Disk group (0000000000766d686261313a353a30)	3	Mounted	Healthy
Disk group (0000000000766d686261313a343a30)	3	Mounted	Healthy
10.26.235.159	6 of 6	Connected	Healthy
Disk group (0000000000766d686261313a353a30)	3	Mounted	Healthy

Below the table, there is an 'ADD DISKS' section with a table of available disks:

Name	Drive Type	Disk Tier
Local VMware Disk (mpx.vmhba1:C0:T5:L0)	Flash	Cache
Local VMware Disk (mpx.vmhba1:C0:T1:L0)	Flash	Capacit
Local VMware Disk (mpx.vmhba1:C0:T9:L0)	Flash	Capacit

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] を選択します。
- 4 (オプション) [アップグレードの事前チェック] をクリックします。

アップグレードの事前チェックではクラスタを分析して、正常なアップグレードの妨げになる問題をすべて検出します。チェックされる項目には、ホスト ステータス、ディスク ステータス、ネットワーク ステータス、オブジェクト ステータスなどがあります。アップグレードの問題は、[ディスクの事前チェックのステータス] テキスト ボックスに表示されます。

- 5 [アップグレード] をクリックします。
- 6 [アップグレード] ダイアログ ボックスで [はい] をクリックし、オンディスク フォーマットのアップグレードを実行します。

結果

vSAN が、オンディスク フォーマットを正常にアップグレードします。[オンディスク フォーマットのバージョン] 列には、クラスタ内のストレージ デバイスのディスク フォーマットのバージョンが表示されます。

アップグレード中に障害が発生した場合、[オブジェクトの再同期] ページで確認できます。すべての再同期が完了するのを待ち、再びアップグレードを実行します。健全性サービスを使用してクラスタの健全性を確認することもできます。健全性チェックに表示された問題を解決した後で、アップグレードを再び実行できます。

RVC を使用した vSAN のディスク フォーマットのアップグレード

vSAN ホストのアップグレードを完了したら、Ruby vSphere Console (RVC) を使用してディスク フォーマットのアップグレードを続行できます。

前提条件

- vCenter Server のバージョンをアップデートしていることを確認します。
- vSAN クラスタで実行されている ESXi ホストのバージョンが 6.5 以降であることを確認します。
- [ディスク管理] ページで、ディスクが良好な状態であることを確認します。RVC コマンド `vsan.disks_stats` を実行してディスクのステータスを確認することもできます。
- 使用するハードウェアとソフトウェアが『VMware 互換性ガイド』の Web サイト (<http://www.vmware.com/resources/compatibility/search.php>) に記載され、認証されていることを確認します。
- ディスク フォーマットのアップグレードに十分な空き容量があることを確認します。RVC コマンド `vsan.whatif_host_failures` を実行して、アップグレードを完了するため、またはアップグレード中に障害が発生した場合にコンポーネントを再構築するための十分な容量があることを確認します。
- RVC にアクセスするために PuTTY または類似の SSH クライアントがインストールされていることを確認します。

RVC ツールのダウンロードと RVC コマンドの使用の詳細については、『RVC コマンド リファレンス ガイド』を参照してください。

- ホストがメンテナンス モードではないことを確認します。オンディスク フォーマットのアップグレード時には、ホストをメンテナンス モードにしないでください。vSAN クラスタのメンバー ホストのいずれかがメンテナンス モードになると、そのメンバー ホストがクラスタに容量を提供しなくなるため、クラスタ内で使用可能なリソース容量が減少します。クラスタのアップグレードに失敗することがあります。
- RVC コマンド `vsan.resync_dashboard` を実行して、vSAN クラスタで現在進行中のコンポーネント再構築タスクがないことを確認します。

手順

- 1 RVC を使用して vCenter Server にログインします。
- 2 次の RVC コマンドを実行して、ディスク ステータスを確認します。 `vsan.disks_stats /< vCenter IP address or hostname>/<data center name>/computers/<cluster name>`

例: `vsan.disks_stats /192.168.0.1/BetaDC/computers/VSANCluster`

このコマンドは、vSAN クラスタ内のすべてのデバイスとホストの名を一覧表示します。また、現在のディスク フォーマットとその健全性ステータスも表示します。デバイスの現在の健全性は、[ディスク管理] ページの [健全性ステータス] 列でも確認できます。たとえば、デバイス障害が発生したホストまたはディスク グループの [健全性ステータス] 列には、デバイス ステータスが [非健全] と表示されます。

- 3 次の RVC コマンドを実行します。 `vsan.ondisk_upgrade <path to vsan cluster>`

例: `vsan.ondisk_upgrade /192.168.0.1/BetaDC/computers/VSANCluster`

- 4 RVC で進行状況を監視します。

RVC は、一度に 1 つのディスク グループをアップグレードします。

ディスク フォーマットのアップグレードが正常に完了すると、次のようなメッセージが表示されます。

```
ディスク フォーマット アップグレード フェーズが終了しました
```

```
アップグレードの必要な n v1 オブジェクトがあります。オブジェクトのアップグレード進行:n アップグレード済み、0 残り
```

```
オブジェクトのアップグレードが完了しました:n アップグレード済み
```

```
vSAN アップグレードが終了しました
```

- 5 次の RVC コマンドを実行して、オブジェクトのバージョンが新しいオンディスク フォーマットにアップグレードされていることを確認します。 `vsan.obj_status_report`

vSAN ディスク フォーマットのアップグレードの確認

ディスク フォーマットのアップグレードが終了したら、vSAN クラスタが新しいオンディスク フォーマットを使用していることを確認する必要があります。

手順

- 1 vSAN クラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [vSAN] の下で、[ディスク管理] をクリックします。

現在のディスク フォーマットのバージョンが [ディスク フォーマットのバージョン] 列に表示されます。

vSAN オブジェクト フォーマットについて

vSAN がポリシーの変更を行う場合、または vSAN 7.0 以前で作成されたオブジェクトに対する操作を行う場合に必要になる操作領域は、クラスタ内で最大のオブジェクトで使用される容量となります。

これを事前に計画することは難しいため、以前は、クラスタ内の最大オブジェクトが容量の 25% 以上を使用する可能性が低いことを前提として、クラスタで 30% の空き容量を確保することが推奨されました。また、ポリシーの変更でクラスタがいっぱいにならないように、容量の 5% が予約されます。vSAN 7.0 U1 以降では、すべてのオブジェクトが新しいフォーマットで作成されます。オブジェクトのポリシー変更で vSAN が必要とする操作領域は、8 TB 未満のオブジェクトの場合、ホストあたり 255 GB、8 TB より大きいオブジェクトの場合はホストあたり 765 GB になります。

クラスタを vSAN 7.0 以前のリリースから vSAN 7.0 U1 以降にアップグレードした後、以前のリリースで作成されたオブジェクトが 255 GB を超えている場合は、オブジェクトを新しい形式で作成しなおす必要があります。これにより、vSAN は、新しい空き容量要件のオブジェクトに対して操作を実行できます。アップグレードを行った後に、新しいオブジェクト フォーマットへの変換が必要なオブジェクトが存在すると、新しいオブジェクト フォーマットに関する健全性アラートが表示されます。レイアウト変更タスクを開始すると、この健全性の状態を修正できません。健全性アラートには、修正が必要なオブジェクトの数と、書き換えられるデータ量に関する情報が表示されます。レイアウト変更タスクの進行中に、クラスタのパフォーマンスが 20% ほど低下することがあります。この操作が完了するまでの所要時間について、正確な情報が再同期ダッシュボードに表示されます。

vSAN クラスタのアップグレードの確認

vSAN クラスタのアップグレードは、最新バージョンの vSphere と vSAN を使用していることを確認するまで完了しません。

手順

- 1 vSAN クラスタに移動します。
- 2 [構成] タブをクリックして、vSAN がリストされていることを確認します。
 - ◆ ESXi ホストに移動して [サマリ] > [構成] を選択し、最新バージョンの ESXi ホストを使用していることを確認することもできます。

vSAN クラスタのアップグレード中の RVC アップグレード コマンド オプションの使用

`vsan.ondisk_upgrade` コマンドには、vSAN クラスタのアップグレードの制御と管理に使用できるさまざまなコマンド オプションがあります。

たとえば、使用可能な空き容量が少ない場合、アップグレードを実行する際に冗長性の低下を許可することができます。 `vsan.ondisk_upgrade --help` コマンドを実行して、RVC コマンド オプションのリストを表示します。

`vsan.ondisk_upgrade` コマンドでは、次のコマンド オプションを使用できます。

表 12-2. アップグレード コマンド オプション

オプション	説明
<code>--hosts_and_clusters</code>	クラスタまたはクラスタの計算リソース内のすべてのホスト システムへのパスを指定する場合に使用します。
<code>--ignore-objects, -i</code>	vSAN オブジェクトのアップグレードをスキップする場合に使用します。このコマンド オプションを使用して、オブジェクト バージョンのアップグレードを排除することもできます。このコマンド オプションを使用すると、オブジェクトは引き続き現在のオンディスク フォーマット バージョンを使用します。
<code>--allow-reduced-redundancy, -a</code>	ディスクのアップグレード中に 1 つのディスク グループに等しい空き容量が必要であるという要件を削除する場合に使用します。このオプションでは、アップグレード中に低下した冗長性モードで仮想マシンが動作します。つまり、特定の仮想マシンは一時的に障害を許容できない可能性があり、その結果データ損失が発生する可能性があります。vSAN は、アップグレードの完了後に完全なコンプライアンスと冗長性をリストアします。
<code>--force, -f</code>	強制続行を有効にし、すべての確認のための質問に自動的に回答する場合に使用します。
<code>--help, -h</code>	ヘルプ オプションを表示する場合に使用します。

RVC コマンドの使用の詳細については、『RVC コマンド リファレンス ガイド』を参照してください。

vSphere Lifecycle Manager の vSAN ビルドの推奨事項

vSAN は、vSphere Lifecycle Manager で使用するためのシステムのベースラインおよびベースライン グループを生成します。

vSphere 7.0 の vSphere Lifecycle Manager には、以前の vSphere リリースで提供され Update Manager システムのベースラインが含まれています。また、ESXi 7.0 以降を実行しているホスト用の新しいイメージ管理機能も含まれています。

vSAN 6.6.1 以降では、vSAN クラスタに対するビルドの推奨事項が自動生成されます。vSAN は、『VMware 互換性ガイド』および vSAN リリース カタログの情報とインストールされている ESXi リリースの情報を組み合わせます。これらの推奨更新は、ハードウェアのサポート状態を維持するために使用できる最適なリリースを提示します。

vSAN 6.7.1 から vSAN 7.0 のシステム ベースラインには、デバイス ドライバとファームウェア アップデートも含めることができます。これらのアップデートは、クラスタに推奨される ESXi ソフトウェアをサポートします。

vSAN 6.7.3 以降では、現在の ESXi リリースのみ、またはサポートされる最新の ESXi リリースについて、ビルドの推奨事項を提供するように選択できます。現在のリリースに対するビルドの推奨事項には、このリリースのすべてのパッチとドライバ アップデートが含まれています。

vSAN 7.0 以降では、パッチの更新や適用可能なドライバの更新などが vSAN ビルドの推奨事項が含まれています。vSAN 7.0 クラスタのファームウェアをアップデートするには、vSphere Lifecycle Manager を介してイメージを使用する必要があります。

vSAN のシステム ベースライン

vSAN ビルドの推奨事項は、vSphere Lifecycle Manager の vSAN システム ベースラインを介して提供されます。このシステム ベースラインは、vSAN によって管理されます。システム ベースラインは読み取り専用で、カスタマイズできません。

vSAN では、vSAN クラスタごとに 1 つのベースライン グループが生成されます。vSAN システム ベースラインは、[ベースラインおよびグループ] タブの [ベースライン] ペインに表示されます。ユーザーは引き続き独自のベースラインを作成して修正できます。

vSAN システム ベースラインには、認定ベンダーによって提供されるカスタム ISO イメージを含めることができます。vSAN クラスタ内のホストに OEM 固有のカスタム ISO がある場合、vSAN 推奨システム ベースラインには、同じベンダーによって提供されるカスタム ISO を含めることができます。vSphere Lifecycle Manager では、vSAN でサポートされていないカスタム ISO の推奨事項を生成できません。ホストのイメージ プロファイルでベンダー名をオーバーライドするカスタマイズされたソフトウェア イメージを実行している場合、vSphere Lifecycle Manager では推奨システム ベースラインを生成できません。

vSphere Lifecycle Manager は、各 vSAN クラスタを自動的にスキャンして、ベースライン グループに対するコンプライアンスを確認します。クラスタをアップグレードするには、vSphere Lifecycle Manager を使用してシステム ベースラインを手動で修正する必要があります。vSAN システム ベースラインは、1 台のホストまたはクラスタ全体に対して修正できます。

vSAN リリース カタログ

vSAN リリース カタログでは、使用可能なリリース、リリースの優先順位、各リリースに必要な重要パッチに関する情報が維持されます。vSAN リリース カタログは、VMware クラウドでホストされます。

vSAN では、リリース カタログにアクセスするためにインターネット接続が必要です。vSAN でリリース カタログにアクセスするためにカスタム エクスペリエンス改善プログラム (CEIP) への登録は必要ありません。

インターネット接続がない場合、vSAN リリース カタログは vCenter Server に直接アップロードできます。vSphere Client で、[構成] > [vSAN] > [更新] の順にクリックし、[リリース カタログ] セクションで [ファイルからアップロード] をクリックします。最新の vSAN [リリース カタログ] をダウンロードできます。

vSphere Lifecycle Manager を使用すると、vSAN クラスタに推奨されるストレージ コントローラのドライバをインポートできます。vSAN では、一部のストレージ コントローラのベンダーから提供されるソフトウェア管理ツールを使用して、コントローラのドライバを更新できます。ESXi ホストに管理ツールがない場合は、このツールをダウンロードできます。

vSAN ビルドの推奨事項の操作

vSphere Lifecycle Manager は、インストールされている ESXi リリースを VMware 互換性ガイドのハードウェア互換性リスト (HCL) の情報に照らして確認します。Upgrade Manager は、最新の vSAN リリース カタログに基づいて、vSAN クラスタごとに正しいアップグレード パスを決定します。vSAN には、システムベースラインの推奨リリースに対して必要なドライバおよびパッチ更新も含まれます。

vSAN ビルドの推奨事項により、各 vSAN クラスタを現在のハードウェア互換性のステータス以上に維持できます。vSAN クラスタ内のハードウェアが HCL に含まれていない場合、vSAN は、最新リリースへのアップグレードを推奨することがあります。これは、最新リリースであれば現在の状態を下回ることはないためです。

注： vSphere Lifecycle Manager は、vSAN クラスタ内のホストの修正事前チェックを実行するときに、vSAN Health Service を使用します。vSAN Health Service は、ESXi 6.0 Update 1 以前を実行するホストでは使用できません。vSphere Lifecycle Manager で ESXi 6.0 Update 1 以前を実行するホストがアップグレードされるとき、vSAN クラスタ内の最後のホストでアップグレードに失敗する場合があります。vSAN の健全性に関する問題が原因で修正に失敗した場合は、アップグレードを完了できます。vSAN Health Service を使用してホストの健全性に関する問題を解決し、そのホストのメンテナンス モードを終了してアップグレード ワークフローを完了します。

次の例では、vSAN ビルドの推奨事項のロジックについて説明します。

例 1：

vSAN クラスタが 6.0 Update 2 を実行し、そのハードウェアが 6.0 Update 2 の HCL に含まれています。HCL には、リリース 6.0 Update 3 までがサポートされるハードウェアとしてリストされていますが、6.5 以降はサポートされないハードウェアとしてリストされています。vSAN は、必要な重要パッチを含むリリース 6.0 Update 3 へのアップグレードを推奨します。

例 2：

vSAN クラスタが 6.7 Update 2 を実行し、そのハードウェアが 6.7 Update 2 の HCL に含まれています。このハードウェアはリリース 7.0 Update 3 の HCL でもサポートされています。vSAN は、リリース 7.0 Update 3 へのアップグレードを推奨します。

例 3：

vSAN クラスタが 6.7 Update 2 を実行し、そのハードウェアがこのリリースの HCL に含まれていません。vSAN は、ハードウェアが 7.0 Update 3 の HCL に記載されていない場合でも、7.0 Update 3 へのアップ

グレードを推奨します。vSAN は、新しい状態が現在の状態を下回ることはないため、アップグレードを推奨します。

例 4 :

vSAN クラスタが 6.7 Update 2 を実行し、そのハードウェアが 6.7 Update 2 の HCL に含まれています。このハードウェアは、リリース 7.0 Update 3 の HCL でもサポートされます。選択されたベースラインの設定は、パッチのみです。vSAN は、必要な重要パッチを含むリリース 7.0 Update 3 へのアップグレードを推奨します。

推奨エンジンは定期的に行われるか（1日に1回）、または次のイベントが発生した場合に行われます。

- クラスタのメンバーシップが変更された場合。たとえば、ホストを追加または削除した場合。
- vSAN 管理サービスが再起動した場合。
- ユーザーが Web ブラウザまたは RVC 経由で「[VMware Customer Connect](#)」にログインした場合。
- 更新は、『VMware 互換性ガイド』または vSAN リリース カタログに対して行われます。

vSAN ビルドの推奨事項の健全性チェックにより、vSAN クラスタに推奨される現在のビルドが表示されます。機能に関する問題がある場合は、それに対する警告も表示されます。

システム要件

vSphere Lifecycle Manager は、vCenter Server 7.0 以降の拡張サービスです。

vSAN には、リリース メタデータの更新、『VMware 互換性ガイド』の確認、「[VMware Customer Connect](#)」からの ISO イメージのダウンロードのためのインターネット アクセスが必要です。

vSAN は、「[VMware Customer Connect](#)」からアップグレードする場合に ISO イメージをダウンロードするための有効な認証情報を必要とします。6.0 Update 1 以前を実行するホストでは、RVC を使用して [VMware Customer Connect] の認証情報を入力する必要があります。それ以降のソフトウェアを実行するホストでは、ESX ビルドの推奨事項の健全性チェックからログインできます。

RVC から [VMware Customer Connect] の認証情報を入力するには、次のコマンドを実行します。

```
vsan.login_iso_depot -u <username> -p <password>
```