

VMware vSAN の管理

Update 3

VMware vSphere 7.0

VMware vSAN 7.0

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

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

VMware株式会社
〒108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

Copyright © 2015-2021 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

『VMware vSAN の管理』について 7

1 更新情報 8

2 vSAN の概要 9

3 vSAN クラスタの構成および管理 10

vSphere Client を使用した vSAN クラスタの構成 10

既存のクラスタで vSAN を有効にする 12

vSAN をオフにする 13

vSAN 設定の編集 14

vSAN データストアの表示 15

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 17

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 18

4 vSAN ポリシーの使用 19

vSAN ポリシーについて 19

vSAN ストレージ プロバイダの表示 22

vSAN のデフォルト ストレージ ポリシーについて 23

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 25

vSphere Client を使用した vSAN のストレージ ポリシーの定義 26

5 vSAN クラスタの拡張および管理 29

vSAN クラスタの拡張 29

vSAN クラスタの容量およびパフォーマンスの強化 30

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 30

vSAN クラスタへのホストの追加 31

ホスト プロファイルを使用したホストの構成 32

HCI メッシュとのリモート データストアの共有 34

リモート データストアの表示 36

リモート データストアのマウント 37

リモート データストアのアンマウント 37

HCI メッシュの監視 37

メンテナンス モードでの操作 39

ホストのデータ移行機能の確認 40

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 41

vSAN クラスタのフォルト ドメインの管理 43

vSAN クラスタのフォールト ドメインの新規作成 44

| | |
|---|-----------|
| 選択したフォールト ドメインへのホストの移動 | 45 |
| フォールト ドメインからのホストの移動 | 45 |
| フォールト ドメインの名前変更 | 45 |
| 選択したフォールト ドメインの削除 | 46 |
| フォールト ドメインによる追加障害の許容 | 46 |
| vSAN iSCSI ターゲット サービスの使用 | 47 |
| iSCSI ターゲット サービスの有効化 | 48 |
| iSCSI ターゲットの作成 | 48 |
| iSCSI ターゲットへの LUN の追加 | 49 |
| iSCSI ターゲットでの LUN の追加 | 49 |
| iSCSI イニシエータ グループの作成 | 50 |
| iSCSI イニシエータ グループへのターゲットの割り当て | 51 |
| iSCSI ターゲット サービスの無効化 | 51 |
| vSAN iSCSI ターゲット サービスの監視 | 52 |
| vSAN ファイル サービス | 52 |
| 制限事項と考慮事項 | 54 |
| ファイル サービスの構成 | 54 |
| vSAN ファイル サービスの編集 | 60 |
| ファイル共有の作成 | 61 |
| ファイル共有の表示 | 63 |
| ファイル共有へのアクセス | 63 |
| ファイル共有の編集 | 65 |
| SMB ファイル共有の管理 | 65 |
| ファイル共有の削除 | 66 |
| vSAN 分散ファイル システムのスナップショット | 66 |
| 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 | 68 |
| マッピング解除による容量の再利用 | 68 |
| ファイル サービスのアップグレード | 69 |
| パフォーマンスの監視 | 70 |
| 容量の監視 | 71 |
| 健全性の監視 | 71 |
| 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 | 72 |
| vSAN クラスタのシャットダウンと再起動 | 72 |
| 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 | 73 |
| vSAN クラスタの再起動 | 74 |
| 手動による vSAN クラスタのシャットダウンと再起動 | 74 |
| 6 vSAN クラスタでのデバイス管理 | 78 |
| ディスク グループおよびデバイスの管理 | 78 |
| vSAN ホストでディスク グループを作成する | 79 |
| vSAN クラスタでのストレージ デバイスの要求 | 80 |

| | |
|-----------------------------------|------------|
| vSAN Direct 用ディスクの要求 | 81 |
| 個々のデバイスの操作 | 81 |
| ディスク グループへのデバイスの追加 | 82 |
| 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 | 82 |
| vSAN からのディスク グループまたはデバイスの削除 | 83 |
| ディスク グループの再作成 | 84 |
| ロケータ LED の使用 | 85 |
| デバイスをフラッシュとしてマーク | 86 |
| デバイスを HDD としてマーク | 86 |
| デバイスをローカルとしてマーク | 87 |
| デバイスをリモートとしてマーク | 87 |
| キャパシティ デバイスの追加 | 88 |
| デバイスからのパーティションの削除 | 88 |
| 7 vSAN クラスターの領域効率の向上 | 90 |
| vSAN 容量効率化の概要 | 90 |
| SCSI マッピング解除による容量の再利用 | 90 |
| デデュープおよび圧縮の使用 | 91 |
| 重複排除および圧縮の設計に関する考慮事項 | 93 |
| 新規の vSAN クラスターでデデュープおよび圧縮を有効にする | 93 |
| 既存の vSAN クラスターでデデュープおよび圧縮を有効にする | 94 |
| デデュープおよび圧縮の無効化 | 94 |
| vSAN クラスターにおける仮想マシンの冗長性の低下 | 95 |
| 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 | 96 |
| RAID 5 または RAID 6 イレージャ コーディングの使用 | 96 |
| RAID 5 または RAID 6 の設計に関する考慮事項 | 97 |
| 8 vSAN クラスターでの暗号化の使用 | 98 |
| vSAN による転送中データの暗号化 | 98 |
| vSAN クラスターでの転送中データの暗号化の有効化 | 99 |
| vSAN による保存データの暗号化 | 99 |
| 保存データの暗号化の仕組み | 99 |
| 保存データの暗号化を設計する際の考慮事項 | 101 |
| 標準のキー プロバイダの設定 | 101 |
| 新しい vSAN クラスターでの保存データの暗号化の有効化 | 107 |
| 保存データの暗号化の新しいキーの生成 | 108 |
| 既存の vSAN クラスターでの保存データの暗号化の有効化 | 108 |
| vSAN の暗号化とコア ダンプ | 109 |
| 9 vSAN クラスターのアップグレード | 113 |
| vSAN のアップグレードの準備 | 114 |

| | |
|---|-----|
| vCenter Server のアップグレード | 116 |
| ESXi ホストのアップグレード | 116 |
| vSAN ディスク フォーマットについて | 117 |
| 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 | 119 |
| 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 | 120 |
| vSAN ディスク フォーマットのアップグレードの確認 | 122 |
| vSAN オブジェクト フォーマットについて | 122 |
| vSAN クラスターのアップグレードの確認 | 123 |
| RVC アップグレード コマンド オプションの使用 | 123 |
| vSphere Lifecycle Manager の vSAN ビルドの推奨事項 | 123 |

『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 |
|------------------|---|
| 2023 年 6 月 12 日 | <ul style="list-style-type: none">■ 「vSAN のアップグレードの準備」で、ストレッチ クラスタと 2 ホスト クラスタをアップグレードするためのガイダンスを更新しました。データ ホストの前に監視ホストがアップグレードされることを記載しました。■ マイナー更新を行いました。 |
| 2021 年 11 月 08 日 | <ul style="list-style-type: none">■ 「ファイル サービスの構成」で、vSAN ファイル サービスを構成するための前提条件を更新しました。■ 「vSAN ディスク フォーマットについて」で、ディスクのアップグレードに関する情報を追加しました。■ vSphere with Tanzu 環境でコンポーネントをシャットダウンまたは起動する方法については、『VMware Cloud Foundation Operations Guide』を参照してください。「手動による vSAN クラスタのシャットダウンと再起動」を更新しました。 |
| 2021 年 4 月 16 日 | <ul style="list-style-type: none">■ 「制限事項と考慮事項」で、vSAN ファイル サービスの制限と考慮事項を更新しました。■ 「ファイル サービスの構成」で、Active Directory サポートの制限を更新しました。■ VMware は、[My VMware] ポータルの名称を [VMware Customer Connect] に変更しました。この名称変更を反映するように「vSphere Lifecycle Manager の vSAN ビルドの推奨事項」のトピックを更新しました。 |
| 2020 年 11 月 12 日 | <ul style="list-style-type: none">■ 「HCI メッシュとのリモート データストアの共有」で、HCI メッシュの設計上の考慮事項を更新しました。■ 「ESXi ホストのアップグレード」で、ESXi のアップグレード情報を更新しました。 |
| 2020 年 10 月 06 日 | 初期リリース。 |

vSAN の概要

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 クラスターのローカル 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 クラスター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。

vSAN クラスタの構成および管理

3

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。

この章には、次のトピックが含まれています。

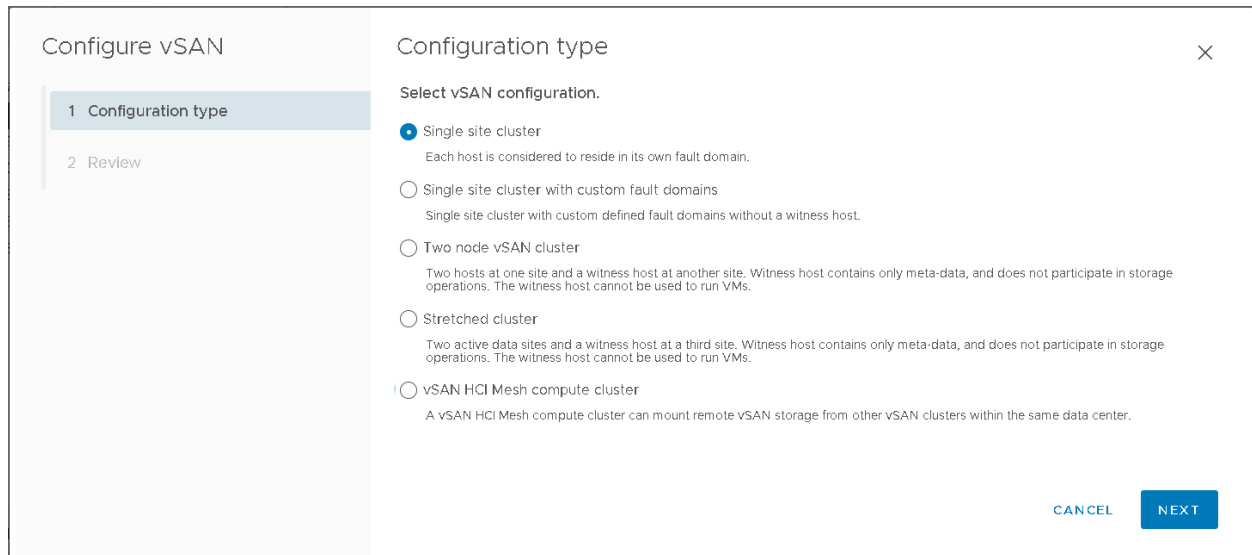
- vSphere Client を使用した vSAN クラスタの構成
- 既存のクラスタで vSAN を有効にする
- vSAN をオフにする
- vSAN 設定の編集
- vSAN データストアの表示
- vSAN データストアへのファイルまたはフォルダのアップロード
- vSAN データストアからのファイルまたはフォルダのダウンロード

vSphere Client を使用した vSAN クラスタの構成

HTML5 ベースの vSphere Client を使用して、vSAN クラスタを構成できます。

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。

注： vSAN HCI メッシュ コンピューティング クラスタの構成オプションには制限があります。



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。

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。

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。
- 4 [vSAN の構成] をクリックして、[vSAN の構成] ウィザードを開きます。
- 5 構成する vSAN クラスタのタイプを選択して、[次へ] をクリックします。
 - 単一サイト クラスタ。詳細については、『vSAN のプランニングとデプロイ』の「vSAN デプロイ オプション」を参照してください。
 - カスタム フォルト ドメインを持つ単一サイトのクラスタ。
 - 2 ノード構成の vSAN クラスタ。
 - ストレッチ クラスタ。
 - vSAN HCI メッシュ コンピューティング クラスタ。詳細については、『VMware vSAN の管理』の「HCI メッシュとのリモート データストアの共有」を参照してください。
- 6 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オプションを構成します。詳細については、[vSAN 設定の編集](#)を参照してください。

7 vSAN クラスタのディスクを要求し、[次へ] をクリックします。

各ホストで、キャッシュ層でフラッシュ デバイスを 1 個以上使用し、キャパシティ層で 1 個以上のデバイスを使用する必要があります。詳細については、『VMware vSAN の管理』の「ディスク グループとデバイスの管理」を参照してください。

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

ディスクを要求するか、ディスク グループを作成します。『VMware vSAN の管理』の「ディスク グループとデバイスの管理」を参照してください。

vSAN データストアが作成されたことを確認します。

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

クラスタのプロパティを編集して、既存のクラスタで vSAN を有効にできます。

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。

注： vSAN HCI メッシュ コンピューティング クラスタの構成オプションには制限があります。

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。
- 4 [vSAN の構成] をクリックします。
- 5 構成する vSAN クラスタのタイプを選択して、[次へ] をクリックします。
 - 単一サイト クラスタ。
 - カスタム フォルト ドメインを持つ単一サイトのクラスタ。
 - 2 ノード構成の vSAN クラスタ。
 - ストレッチ クラスタ。

- vSAN HCI メッシュ コンピューティング クラスタ。詳細については、『VMware vSAN の管理』の「HCI メッシュとのリモート データストアの共有」を参照してください。

6 使用する vSAN サービスを構成し、[次へ] をクリックします。

- 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 ネットワークの設計」を参照してください。
- vSAN Health Service の履歴を構成します。
- 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管理オプションを構成します。
- 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
 - 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

7 vSAN クラスタのディスクを要求し、[次へ] をクリックします。

各ホストで、キャッシュ層でフラッシュ デバイスを 1 個以上使用し、キャパシティ層で 1 個以上のデバイスを使用する必要があります。詳細については、『VMware vSAN の管理』の「ディスク グループとデバイスの管理」を参照してください。

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。

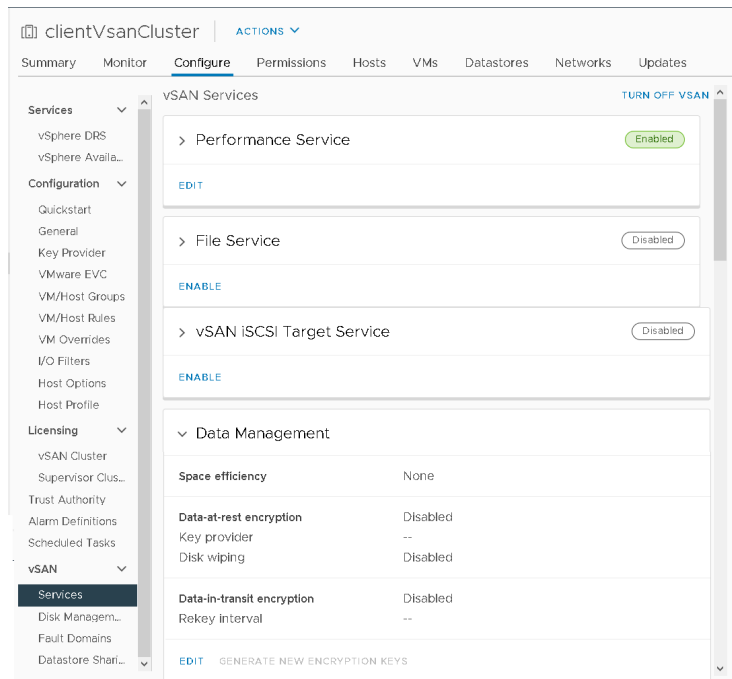
手順

- 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。



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。

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。

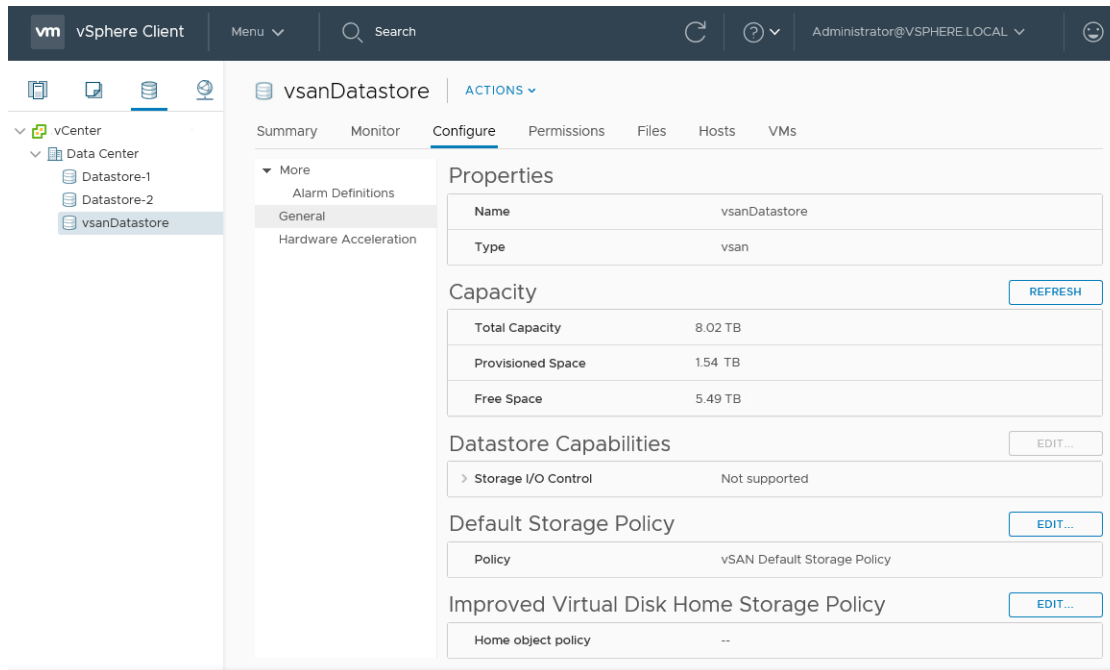
- vSAN パフォーマンス サービスを構成します。詳細については、『vSAN の監視とトラブルシューティング』の「vSAN のパフォーマンスの監視」を参照してください。
- ファイル サービスを有効にします。詳細については、『VMware vSAN の管理』の「vSAN ファイル サービス」を参照してください。
- vSAN ネットワーク オプションを構成します。詳細については、『vSAN のプランニングとデプロイ』の「vSAN ネットワークの構成」を参照してください。
- vSAN 健全性サービスの履歴を構成します。
- iSCSI ターゲット サービスを構成します。詳細については、『VMware 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管理オプションを構成します。
- 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
 - 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

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 を有効にして、ディスク グループを構成します。

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ープおよび圧縮では、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、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ース形式です。

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

4

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。

この章には、次のトピックが含まれています。

- vSAN ポリシーについて
- 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 オブジェクトおよび仮想マシン スナップショット メモリ オブジェクトでは、仮想マシンに割り当てられたストレージ ポリシーに準拠しません。これらのオブジェクトでは、[許容される障害の数] が 1 に設定されます。これらのオブジェクトの可用性は、[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。

表 4-1. ストレージ ポリシー ルール

| 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、RAID 5 または RAID 6 を使用している場合にはパリティ コピーを含めて、書き込まれる各データは n+1 個の場所に保存されます。</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。</p> <p>注： vSAN で仮想マシン オブジェクトの 1 つのミラー コピーを保護しない場合は、[データの冗長性なし] を指定できます。ただし、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退避させる必要があるため発生します。[データの冗長性なし] を設定すると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。</p> <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>ストレッチ クラスタでは、このルールによって、[FTT] で定義された障害数に達した後、そのオブジェクトが許容できる追加のホストの障害数が定義されます。</p> <p>なし - 標準クラスタがデフォルト値です。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> <p>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、各データ ホストに少なくとも 3 つのディスク グループが必要です。</p> <p>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。</p> |
| 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 デバイスに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> |

表 4-1. ストレージ ポリシー ルール (続き)

| 機能 | 説明 |
|-------------------|--|
| フラッシュ読み取りキャッシュの予約 | <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>フラッシュ読み取りキャッシュの予約のストレージ ポリシー属性は、ハイブリッド構成でのみサポートされます。オールフラッシュ クラスターの仮想マシン ストレージ ポリシーを定義する際には、この属性は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> |
| 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> |
| 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 4-1. ストレージ ポリシー ルール (続き)

| 機能 | 説明 |
|-------------------|--|
| オブジェクト チェックサムの無効化 | <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> |
| 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> |

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、『VMware vSAN の管理』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 ノードのクラスタ上で RAID5 ポリシーを RAID6 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する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>/vsanHealth/vsanvp/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。各ホストにストレージ プロバイダがありますが、アクティブなストレージ プロバイダは1つだけです。他のホストに属するストレージ プロバイダはスタンバイ状態です。現在アクティブなストレージ プロバイダがあるホストで障害が発生した場合、他のホストのストレージ プロバイダがアクティブになります。

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 ポリシーを仮想マシンに明示的に割り当てないと、vSAN のデフォルト ストレージ ポリシーが仮想マシンに割り当てられます。

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 4-2. 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 |

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] > [vSAN のデフォルト ストレージ ポリシー] > [管理] > [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。1つの仮想マシン ストレージ ポリシーのみ、vSAN データストアにデフォルト ポリシーとしていつでも割り当てることができます。

特性

vSAN のデフォルト ストレージ ポリシーの特性は、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 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、non-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。
- デフォルトの仮想マシン 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 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。

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。

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。

The screenshot shows the 'Create VM Storage Policy' dialog box with the 'vSAN' tab selected. The 'Advanced Policy Rules' section is active, displaying the following settings:

- Number of disk stripes per object: 1
- IOPS limit for object: 0
- Object space reservation: Thin provisioning (Initially reserved storage space for 100 GB VM disk would be 0 B)
- Flash read cache reservation (%): 0 (Reserved cache space for 100GB VM disk would be 0 B)
- Disable object checksum:
- Force provisioning:

Buttons at the bottom right include CANCEL, BACK, and NEXT.

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]

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 [新しい仮想マシン ストレージ ポリシーの作成] アイコン (📄) 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を [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、[重複排除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、[重複排除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

5

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。

この章には、次のトピックが含まれています。

- vSAN クラスタの拡張
- HCI メッシュとのリモート データストアの共有
- メンテナンス モードでの操作
- vSAN クラスタのフォルト ドメインの管理
- 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。デバイスを追加するか、または容量のあるホストを追加すると、vSAN は、新しく追加されたデバイスにデータを自動的に分散します。『vSAN の監視とトラブルシューティング』の「自動リバランスの設定」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 クラスタに移動します。ホスト プロファイルを使用したホストの構成を参照してください。新しいクラスタ メンバーによって、ストレージとコンピューティング能力が追加されます。新しく追加されたホストで、ローカルのキャパシティ デバイスからディスク グループのサブセットを手動で作成する必要があります。vSAN ホストでディスク グループを作成するを参照してください。

使用するハードウェア 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、『VMware 互換性ガイド』(<http://www.vmware.com/resources/compatibility/search.php>) に記載され、認定されていることを確認します。キャパシティ デバイスを追加する場合、デバイスがフォーマットおよびパーティション化されておらず、vSAN がデバイスを認識して要求できることを確認します。

- 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。ホスト上のディスク グループにデバイスを手動で追加する必要があります。[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、クラスタの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。

- 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、[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 がプロアクティブな再分散を完了すると、同様にパフォーマンスが向上します。

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。キャッシュおよびキャパシティ デバイスを持つホストを追加することでクラスタのキャパシティを拡張すると最適化が可能になります。ディスク グループ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。ホストとディスク グループ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 グループへのデバイスの追加の詳細については、[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。

クラスタのキャパシティを拡張してから手動で再調整し、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。

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) [フォールト ドメインの作成] 画面で、新しいホストを対応するフォールト ドメインに移動します。

フォールト 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 クラスタ内の残り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。


- a ホスト プロファイル ビューに移動します。
- b [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。
- c 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。

HCI メッシュとのリモート データストアの共有

vSAN クラスタは、他の vSAN 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。

データストア共有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、vCenter Server によって管理される同じデータセンター内のサーバ 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。

HCI メッシュを使用したリモート 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にマウントされます。

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。

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。

HCI メッシュ vSAN には、次のような設計上の注意事項があります。

- クラスタは同じ vCenter Server で管理し、同じデータセンター内に配置する必要があります。
- クラスタで 7.0 Update 1 以降が実行されている必要があります。
- vSAN クラスタは、ローカル データストアを最大 10 つのクライアント vSAN 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 つのリモート 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。vSAN サーバ クラスタにもホストをマウントできます。
- 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 HCI メッシュを機能させるには、APD を使用して、データストアの障害応答に「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。

次の機能は、HCI メッシュでサポートされません。

- vSAN 転送中データの暗号化
- vSAN ストレッチ クラスタ
- vSAN 2 ノード クラスタ

次の構成は、HCI メッシュでサポートされません。

- vSAN ファイル共有、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 vSAN 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。
- RDMA 経由の vSAN 通信。

HCI メッシュ コンピューティング専用クライアント

vSAN 7.0 Update 2 以降では、HCI メッシュ クライアントとして vSAN クラスタを構成できます。HCI メッシュ コンピューティング専用クライアント クラスタ内のホストには、ローカル ストレージは必要ありません。同じデータセンター内にあるクラスタ vSAN からリモート データストアをマウントできます。

HCI メッシュ コンピューティング専用クラスタには、次の設計上の考慮事項があります。

- vSAN ネットワークは、クライアント ホストで構成する必要があります。
- vSAN コンピューティング専用ホストにディスク グループを使用することはできません。
- コンピューティング専用クラスタで、vSAN データ管理機能を構成することはできません。

vSAN 用に vSphere クラスタを構成するときに、HCI メッシュ コンピューティング クラスタとして指定できません。リモート データストアをマウントし、リモート vSAN データストアのキャパシティ、健全性、パフォーマンスを監視できます。

リモート データストアの表示

[データストア共有] 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。

| 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、[データストア共有] 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
- データストアの容量
- 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 データストアのマウント

同じ vCenter Server によって管理されている他の 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、[データストア共有] をクリックします。
- 4 [リモート データストアのマウント] をクリックします。
- 5 データストアを選択して、[次へ] をクリックします。
- 6 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 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、[データストア共有] 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

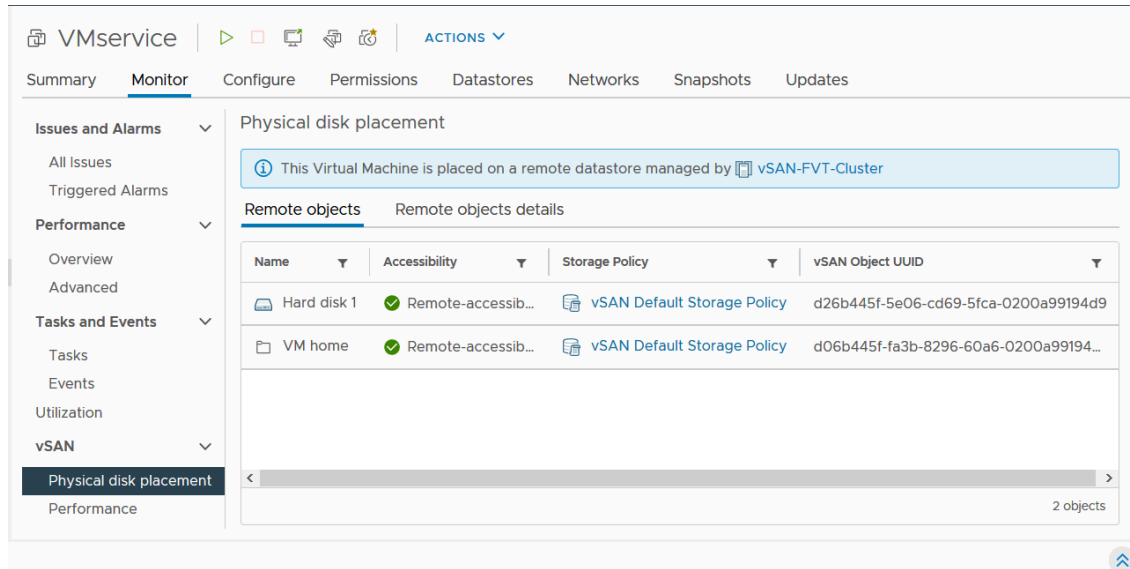
選択したデータストアがローカル クラスタからアンマウントされます。

HCI メッシュの監視

vSphere Client を使用して、HCI メッシュ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。

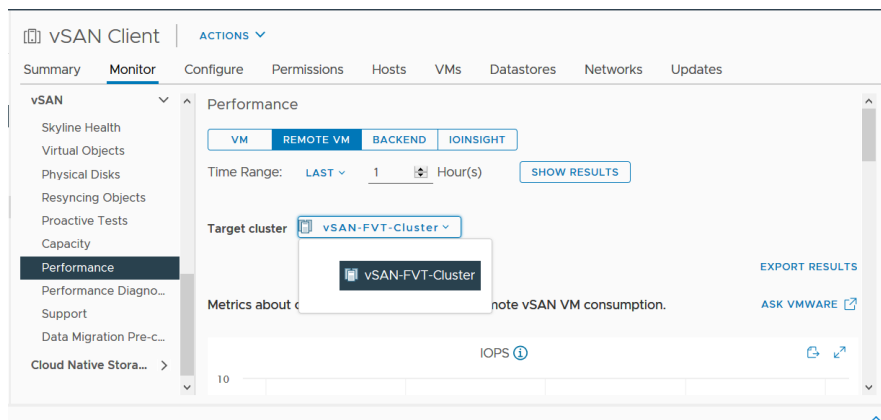
仮想オブジェクト ビューには、仮想オブジェクトが配置されているデータストアが表示されます。リモート データストアに配置されている仮想マシンの物理ディスク配置ビューには、リモートの場所に関する情報が表示されます。



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ず。
- [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。

メンテナンス モードでの操作

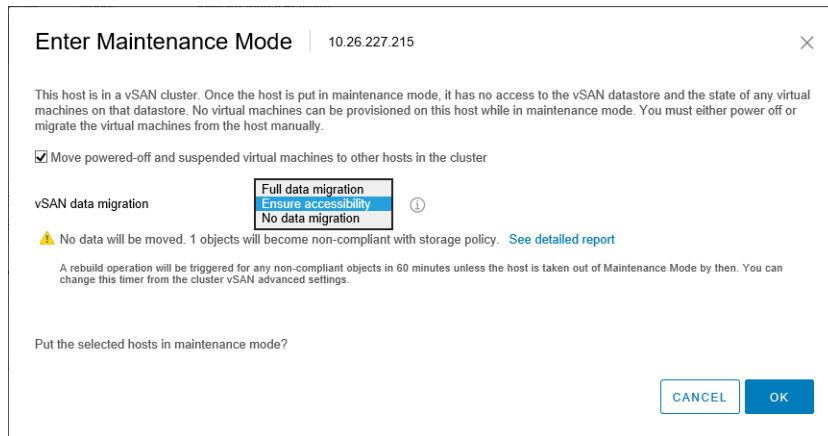
vSAN クラスタのメンバーであるホストは、シャットダウン、再起動または切断する前にメンテナンス モードにする必要があります。

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。



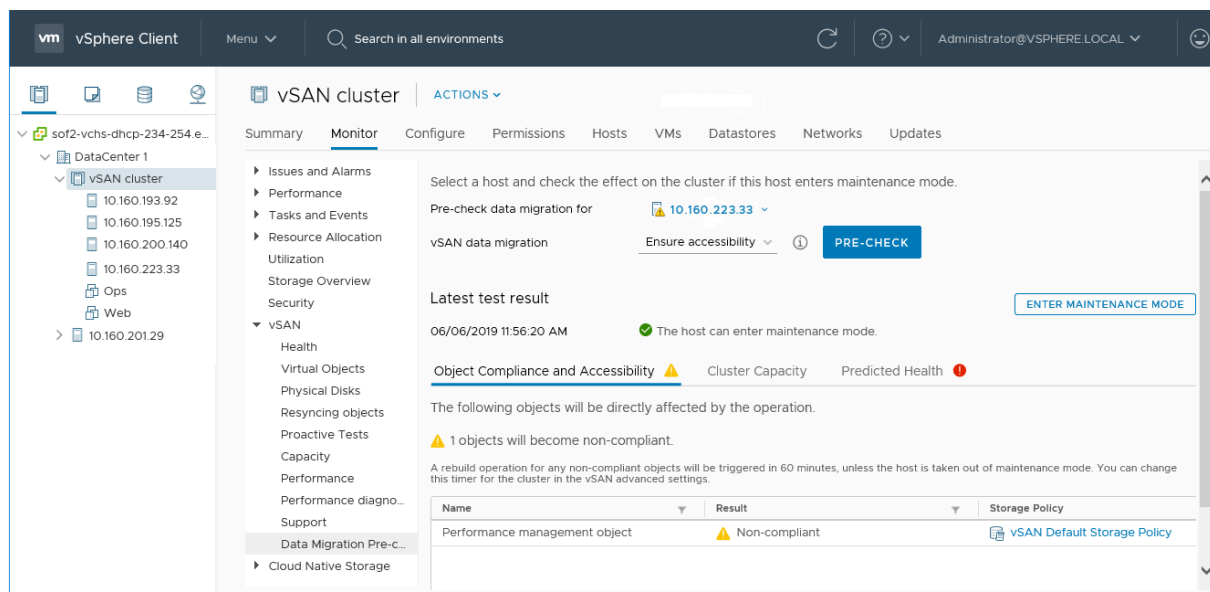
[メンテナンス モードの確認] ダイアログ ボックスは、メンテナンス作業のガイドとなる情報を提供します。ここでは、各データ退避オプションの影響を表示することができます。

- 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。

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データ移行オプションの影響を判断します。

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。

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。クラスタでホストをパワーオフまたは削除すると、vSAN によってこのホストのすべてのアクセス可能な仮想マシンはアクセス可能なままになります。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には、ホストで次のコマンドを実行します。

```
esxcli system maintenanceMode set --enable 1
```

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。

- フォールト 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 フォールト ドメインに存在しているとみなされます。
- すべての vSAN ホストをフォールト ドメインに割り当てる必要はありません。フォールト ドメインを使用して vSAN 環境を保護する場合は、サイズが同じフォールト 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、フォールト ドメインの割り当てを保持します。
- フォールト ドメインを設計する場合は、一定数のホストを各フォールト ドメインに配置します。
フォールト 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 フォールト ドメインの設計とサイジング」を参照してください。
- フォールト 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。各フォールト 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 クラスタのフォールト 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、異なるフォールト ドメインでホストをグループ化することができます。

フォールト 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 で異なるフォールト 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

- 一意のフォールト 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ールト 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。フォールト 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ールト 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 [フォールト 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。[新しいフォールト ドメイン] ウィザードが開きます。
- 5 フォールト ドメイン名を入力します。
- 6 フォールト ドメインに追加する 1 つ以上のホストを選択します。

フォールト ドメインは空にはできません。フォールト 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ールト ドメインに表示されます。各フォールト 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、フォールト ドメイン全体でのキャパシティ分布を確認できます。

選択したフォールト ドメインへのホストの移動

vSAN クラスタの選択したフォールト 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 [フォールト ドメイン] をクリックします。
- 4 既存のフォールト 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ールト ドメインに表示されます。

フォールト ドメインからのホストの移動

要件に応じて、フォールト 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ールト 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 [フォールト ドメイン] をクリックします。
 - a ホストをクリックして、フォールト 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、フォールト ドメインに属さなくなります。フォールト 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 フォールト ドメインに存在しているとみなされます。

次のステップ

フォールト ドメインにホストを追加できます。 [選択したフォールト ドメインへのホストの移動](#)を参照してください。

フォールト ドメインの名前変更

vSAN クラスタの既存のフォールト 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 [フォールト ドメイン] をクリックします。
 - a フォールト 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 フォールト 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、フォールト ドメインのリストに表示されます。

選択したフォールト ドメインの削除

フォールト 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 [フォールト ドメイン] をクリックします。
- 4 フォールト 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

フォールト ドメインのすべてのホストが削除され、選択したフォールト ドメインが vSAN クラスタから削除されます。フォールト 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 フォールト ドメインに存在しているとみなされます。

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 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。

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 にアクセスするようになります。

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。

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。

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

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。

iSCSI ターゲットへの LUN の追加

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。

iSCSI ターゲットでの LUN の追加

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。

iSCSI イニシエータ グループの作成

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 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 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。

iSCSI イニシエータ グループへのターゲットの割り当て

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。

iSCSI ターゲット サービスの無効化

vSAN iSCSI ターゲット サービスを無効にできます。vSAN iSCSI ターゲット サービスを無効にしても、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 サービスの無効にする前に、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 サービスを無効にすると、iSCSI LUN で実行されているワークロードが停止します。無効にする前に、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 サービスが無効になります。

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。

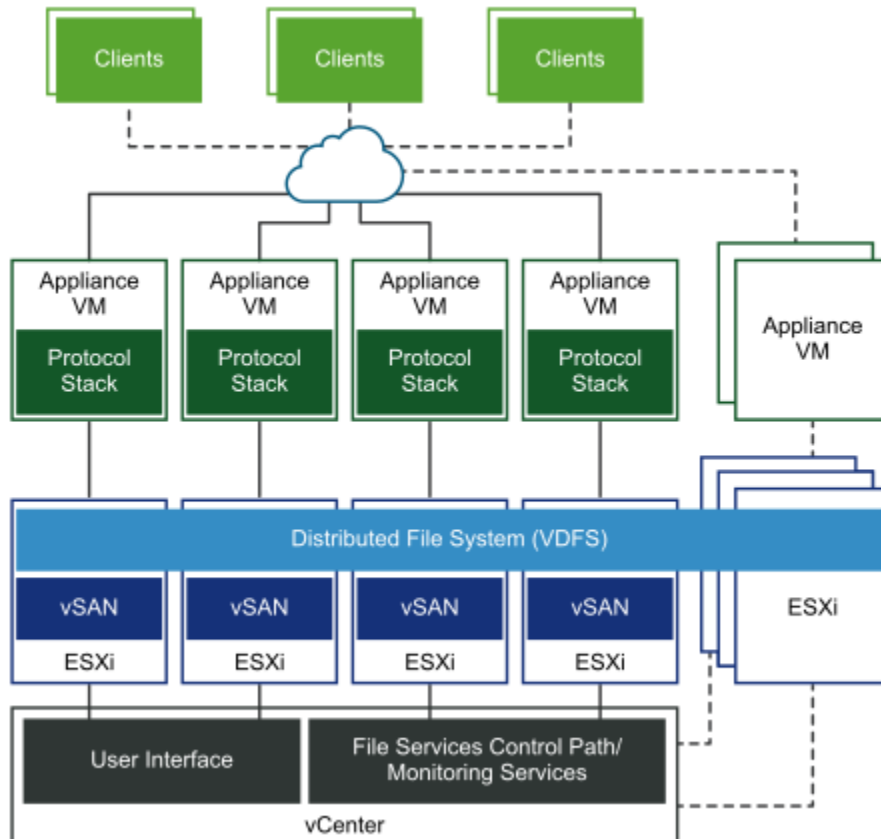
手順

- 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ーに作成します。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 リファラールでファイル 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、ストレッチ クラスタと 2 ノード構成のクラスターをサポートします。2 ノード構成のクラスターでは、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 (Cloud Native Storage, CNS) ファイル ボリュ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。

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 7.0 U3 では、vSAN クラスタがメンテナンス モードに切り替わると、ファイル サービス仮想マシンがパワーオフされますが、削除はされません。
- vSAN 7.0 Update 3 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 7.0 Update 3 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 7.0 Update 3 では、100 個のファイル共有がサポートされます。
- vSAN 7.0 Update 3 より前のリリースでは、ホストがメンテナンス モードに切り替わると、プロトコル スタック コンテナが別の 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 が削除されます。ホストのメンテナンス モードが終了すると、新しい FSVM がプロビジョニングされます。

vSAN クラスタがメンテナンス モードに切り替わると、ファイル サービス仮想マシンはパワーオフされ、削除されます。ホストのメンテナンス モードが終了すると、仮想マシンが再作成されます。

- 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。

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。vSAN ファイル サービスは、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
- 10 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。
-

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 [有効化] をクリックします。
[ファイル サービスの構成] ウィザードが開きます。
- 3 [概要] ページのチェックリストを確認し、[次へ] をクリックします。

- 4 [ファイル サービス エージェント] ページで、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 |
|-----------|---|
| [自動による方法] | <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"> ■ OVF がすでにダウンロードされ、使用可能な場合は、次のオプションを使用できます。 <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。 |
| [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。</p> <hr/> <p>注： このオプションを選択した場合は、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 [ドメイン] ページで次の情報を入力して、[次へ] をクリックします。
- [ファイル サービス ドメイン]：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。
 - [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.registerrootdnsname 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。

- [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。

次のテキスト ボックスに適切な値を入力して、vSAN ファイル サービスに Active Directory ドメインを構成します。

| オプション | 説明 |
|-------------------------|---|
| [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。 |
| [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。</p> <p>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。</p> <p>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。
 - 組織単位 (OU) 名のスペース。
 - 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 [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。

- ネットワーク
- プロトコル

- サブネット マスク
- ゲートウェイ

7 [IP アドレス プール] ページで、次の情報を入力し、[プライマリ IP] を選択して [次へ] をクリックします。

- [IP アドレス]
- [DNS 名]
- [アフィニティ サイト] : ストレッチ クラスタで vSAN ファイル サービスを構成する場合は、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、[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。
- 最大 32 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。

8 設定内容を確認して、[終了] 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。ファイル サービス ドメインが作成され、vSAN ファイル サービスが有効になります。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。

- OVF がダウンロードされ、展開されます。
- ファイル サービス ドメインが作成され、vSAN ファイル サービスが有効になります。
- 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。
- 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] をクリックします。
[ファイル サービスの構成] ウィザードが開きます。

3 構成に適切な変更を行います。vSAN ファイル サービスの構成では、次の項目を変更できます。

| ページ | 編集可能なフィールド |
|--------|---|
| ドメイン | <p>次のドメイン関連情報を編集できます。</p> <ul style="list-style-type: none"> ■ ファイル サービス ドメイン ■ DNS サーバ ■ DNS サフィックス ■ ディレクトリ サービス <p>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。</p> |
| ネットワーク | <p>次のネットワーク関連情報を編集できます。</p> <ul style="list-style-type: none"> ■ サブネット マスク ■ ゲートウェイ |
| IP プール | <p>プライマリ IP アドレスと DNS 名を除き、固定 IP アドレスと DNS 名を編集できます。</p> |

必要な変更を行ったら、[確認] ページで変更内容を確認し、[[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。

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、これらのファイル共有を ESXi のデータストアとして使用できません。

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。

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、[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]: 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ます。
- [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す。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 [Root squash] を有効または無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。

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。

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。

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。

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 サーバ管理者ユーザーとしてログインします。ファイル サービスを有効にするときに、ユーザーをファイル サーバ管理者ユーザーとして構成できます。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。

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。

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。

マッピング解除による容量の再利用

vSAN 6.7 Update 2 以降では、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のストレージ領域を再利用できます。

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

デフォルトではマッピング解除機能は無効です。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。

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せん。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 |

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。

容量の監視

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 [重複排除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。

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。 |

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 ディスクを使用します。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。

手順

- 1 vSAN クラスタに移動します。
- 2 クラスタ内の各ホストのハイブリッド ディスク グループを削除します。
 - a [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。
 - d 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。
- 3 物理 HDD ディスクをホストから削除します。
- 4 フラッシュ デバイスをホストに追加します。

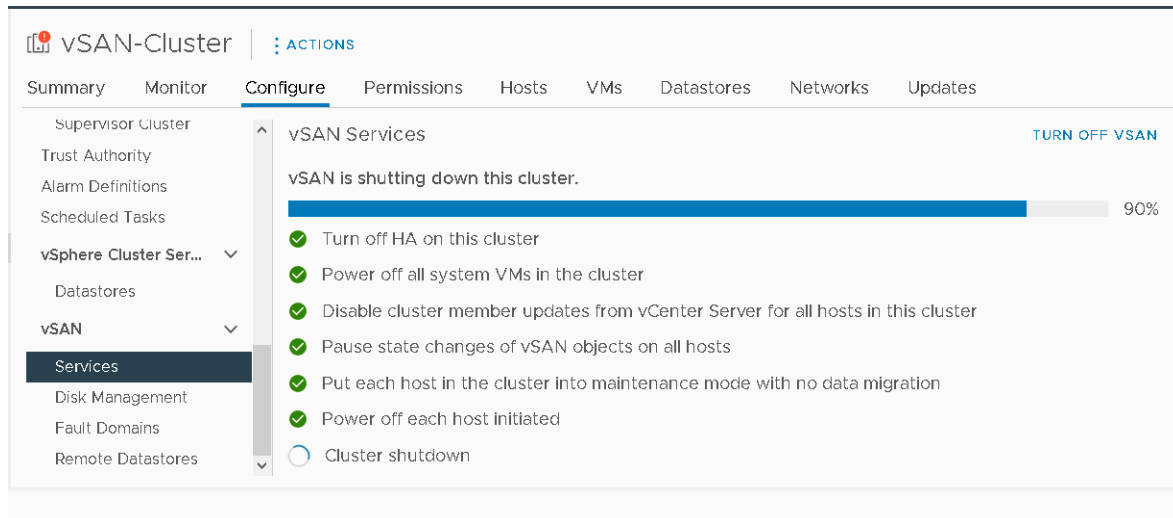
フラッシュ デバイスにパーティションがないことを確認します。
- 5 オールフラッシュ ディスク グループを各ホストに作成します。

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： 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。



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 Operations Guide』の「Shutdown and Startup of VMware Cloud Foundation」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 健全性サービスをチェックし、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、vCenter Server 仮想マシン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 Appliance が vSAN クラスタにデプロイされている場合、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。[次へ] をクリックします。
- 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。

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 健全性サービスを確認し、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 Operations Guide』の「Shutdown and Startup of VMware Cloud Foundation」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 健全性サービスをチェックし、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、vCenter Server 仮想マシンをパワーオフしないでください。
- c [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。

- 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。

- e 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。

- 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
```

- g 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。

- h 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。

- i 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> 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> にある VMware ナレッジベースの記事を参照してください。

- j 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> 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 健全性サービスを確認し、未解決の問題を解決します。
- k (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。vSAN の健全性サービス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
```

vSAN クラスタでのデバイス管理

6

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各デバイスを要求できるようにする、デバイスの LED インジケータを有効または無効にする、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。

この章には、次のトピックが含まれています。

- ディスク グループおよびデバイスの管理
- 個々のデバイスの操作

ディスク グループおよびデバイスの管理

クラスタで vSAN を有効にした場合、ディスク要求モードを選択して、デバイスをグループに編成します。

vSAN 6.6 以降のリリースでは、あらゆるシナリオに向けて統一されたディスク要求ワークフローが用意されています。このワークフローでは、利用可能なすべてのディスクが、モデルおよびサイズ、またはホストごとにグループ化されます。キャッシュ デバイスやキャパシティ デバイスとして使用するデバイスを選択する必要があります。

ホストでディスク グループを作成する

ディスク グループを作成するには、vSAN データストアで使用される各ホストおよび各デバイスを指定する必要があります。キャッシュ デバイスとキャパシティ デバイスをディスク グループに整理します。

ディスク グループを作成するには、ディスク グループを定義して、このディスク グループに含めるデバイスを個別に選択します。各ディスク グループには、1 個のフラッシュ キャッシュ デバイスと 1 個以上のキャパシティ デバイスが含まれます。

ディスク グループを作成する場合、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。

vSAN クラスタには当初、使用済みバイト数がゼロの単一の vSAN データストアが含まれています。

各ホストでディスク グループを作成し、キャッシュ デバイスとキャパシティ デバイスを追加すると、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、クラスタに追加されたホストで使用できるローカルの空のキャパシティ デバイスを使用して、1 つの分散 vSAN データストアが作成されます。

各ディスク グループには、1つのフラッシュ キャッシュ デバイスが含まれています。複数のディスク グループを手動で作成し、各グループのフラッシュ キャッシュ デバイスを要求できます。

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 ESXi ホストから新しいストレージを使用するには、ディスク グループを作成し、そのディスク グループにデバイスを追加する必要があります。

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。

vSAN ホストでディスク グループを作成する

特定のキャッシュ デバイスと特定のキャパシティ デバイスを手動で組み合わせて、特定のホスト上でディスク グループを定義することができます。

この方法では、デバイスを手動で選択して、ホストのディスク グループを作成します。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 デバイスを追加します。

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動するまで、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 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 ホストでグループ化します。
- 6 要求するディスクを選択します。
 - 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。
 - 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] または [OK] をクリックして、選択内容を確認します。

結果

新しいディスク グループがリストに表示されます。

vSAN クラスタでのストレージ 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。

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 インフラストラクチャ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動するまで、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 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。
 - 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。

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] ページ下部の [ディスク ロール] 列に移動します。この列には、リストとディスク グループにおける目的のリストが表示されます。

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

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 [未使用ディスクの要求] ウィザードで、[vSAN Direct] タブを選択します。
- 6 要求するデバイスを選択して、[vSAN Direct の要求] のチェックボックスを選択します。

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

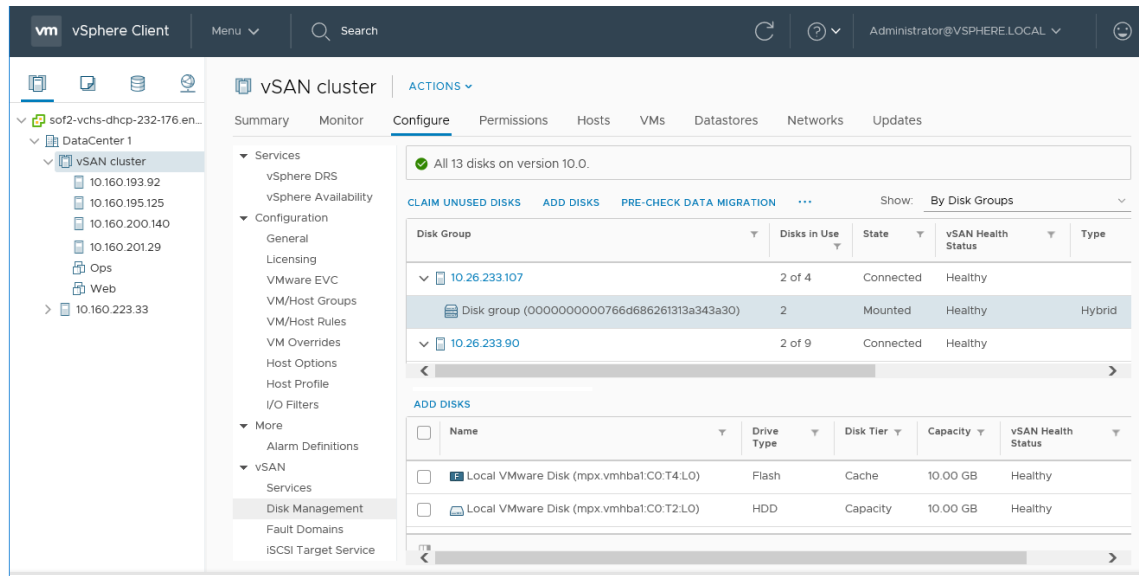
要求されるデバイスごとに、vSAN は新しい vSAN Direct データストアを作成します。

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。

個々のデバイスの操作

ディスク グループへのデバイスの追加、ディスク グループからのデバイスの削除、ロケータ LED の有効または無効の設定、デバイスのマークなど、さまざまなデバイス管理タスクを vSAN クラスタで実行できます。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。



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。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。

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。健全性チェックが警告を示している場合は、オフピーク時に再調整処理を手動で実行します。詳細については、『vSAN の監視とトラブルシューティング』の「手動リバランス」を参照してください。

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データ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す。

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 グループまたはディスク グループ全体から削除できます。

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。

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。

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。

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 の有効化および無効化

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 ページ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、選択したデバイスのロケータ LED を有効または無効にします。

| 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 を有効にします。ロケータ LED は、[管理] タブから有効にできます。[ストレージ] > [ストレージ デバイス] をクリックしてください。 |
| [LED を消灯] | 選択したストレージ デバイスのロケータ LED を無効にします。ロケータ LED は、[管理] タブから無効にできます。[ストレージ] > [ストレージ デバイス] をクリックしてください。 |

デバイスをフラッシュとしてマーク

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。

デバイスを HDD としてマーク

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。

デバイスをローカルとしてマーク

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。

デバイスをリモートとしてマーク

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。

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で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 クラスターの領域効率の向上

7

領域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。

この章には、次のトピックが含まれています。

- vSAN 容量効率化の概要
- SCSI マッピング解除による容量の再利用
- デデュープおよび圧縮の使用
- 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 の設計に関する考慮事項

vSAN 容量効率化の概要

容量効率化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容量の再利用

vSAN 6.7 Update 1 以降では、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のストレージ領域を再利用できます。

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。

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。

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

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。

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。

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。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。

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。vSAN クラスタの作成と編集については、『vSAN のプランニングとデプロイ』の「vSAN の有効化」を参照してください。

デデューブおよび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。デデューブ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、デデューブ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。

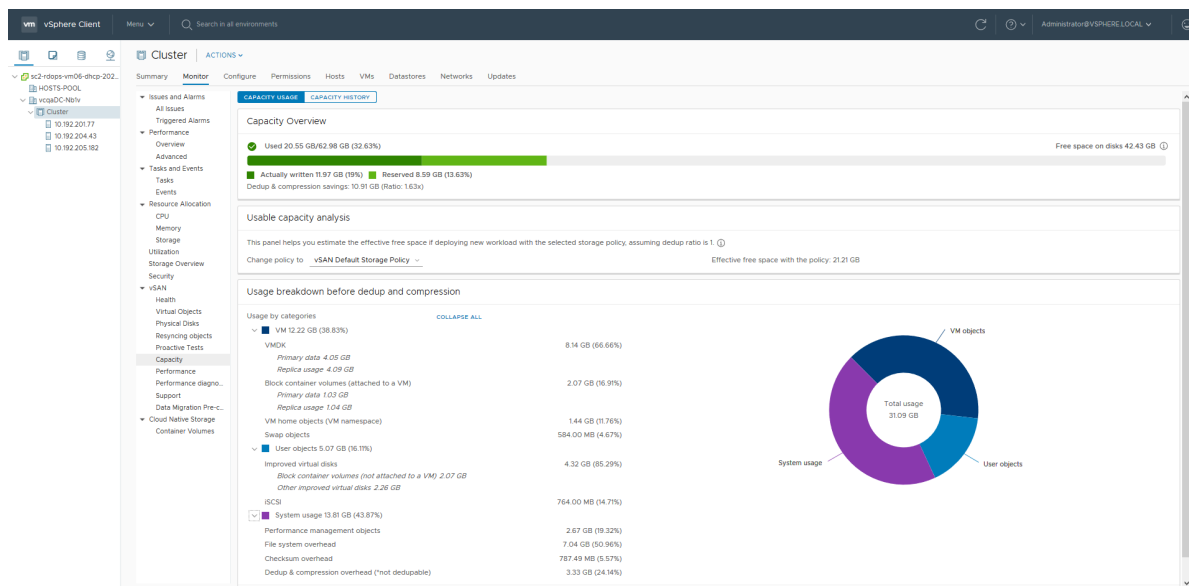
デデューブおよび圧縮を使用したクラスタ内のディスクの管理方法

デデューブ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。デデューブ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。

デデューブおよび圧縮によって節約できる容量の確認

デデューブ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、デデューブ率が高くなる傾向があります。デデューブおよび圧縮の結果は、vSAN のキャパシティ モニターで [デデューブ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。

重複排除および圧縮の設計に関する考慮事項

vSAN クラスタで重複排除 (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。

- 重複排除および圧縮は、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。
- 重複排除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。
- クラスタで重複排除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 クラスタで重複排除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重複排除および圧縮を使用して削減されます。
- vSAN は、各ディスク グループ内のデータ ブロックの重複を排除できますが、ディスク グループ間では排除できません。
- 重複排除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容量の予約が必要です。100% のオブジェクト容量の予約ポリシーは常に順守されます。ただし、重複排除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 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 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および圧縮を有効にする

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。

前提条件

オール フラッシュ vSAN クラスタを作成します。

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。
- 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。

結果

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。

デデュープおよび圧縮の無効化

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 重複排除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。重複排除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。

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て済みます。

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て済みます。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 7-1. 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) - キャパシティ] 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) - キャパシティ] 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) - パフォーマンス] 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) - キャパシティ] の [障害の許容方法] は、[サイトの耐障害性] にのみ適用されます。

ポリシーの構成の詳細については、[4 章 vSAN ポリシーの使用](#)を参照してください。

RAID 5 または RAID 6 の設計に関する考慮事項

vSAN クラスタで 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 クラスタで重複排除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

8

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。

この章には、次のトピックが含まれています。

- 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。

vSAN では、保存データの暗号化を実行できます。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。

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。

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。

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。
- 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を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、[キー管理サーバ] 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するルート 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、[キー管理サーバ] を選択します。
- 3 信頼された接続を確立する KMS インスタンスを選択します。
- 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、VMware Endpoint Certificate Store (VECS) に保存されません。
- 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、[キー管理サーバ] を選択します。
- 3 信頼された接続を確立する KMS インスタンスを選択します。
- 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、VMware Endpoint Certificate Store (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、[キー管理サーバ] を選択します。
- 3 信頼された接続を確立する KMS インスタンスを選択します。
- 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、[キー管理サーバ] を選択します。
- 3 信頼された接続を確立する KMS インスタンスを選択します。
- 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。

- 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。
- [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。

デフォルトのキー プロバイダの設定

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 [正常] 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

- vCenter Server に移動します。
- [構成] をクリックし、[キー管理サーバ] を選択します。
- キー プロバイダを選択します。
- [デフォルトにする] 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。
- [デフォルトにする] 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 ボックスで 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

- vCenter Server に移動します。

- 2 [構成] をクリックし、[キー管理サーバ] を選択します。
- 3 信頼された接続を確立する KMS インスタンスを選択します。
- 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 を信頼するようになります | 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 | <ol style="list-style-type: none"> 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。
- 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 クラスタで構成パラメータを編集して、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。
- 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。

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 ダンプはユーザーの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。

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 アクセスが無効な場合は、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

9

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。

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。オンデイスク 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。

この章には、次のトピックが含まれています。

- 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
- 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

フェイルセーフを念頭に、アップグレードのプランニングおよび設計を行います。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 9-1. 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 | ディスク フォーマットをアップグレードするのに十分な容量があることを確認します。最大のディスク グループが使用している容量と同じ空き容量はないが、変換されるディスク グループ以外のディスク グループに空き容量がある場合、データ移行オプションとして [冗長性の低下を許可] を選択する必要があります。 たとえば、クラスタ内の最大ディスク グループの物理容量が 10 TB で、使用量は 5 TB のみであるとします。この場合、移行中のディスク グループを除いたクラスタ内の別の場所に、追加で 5 TB の空き容量が必要になります。vSAN のディスク フォーマットのアップグレード時には、ホストがメンテナンス モードになっていないことを確認します。vSAN クラスタのいずれかのメンバー ホストをメンテナンス モードにすると、そのメンバー ホストはストレージをクラスタに提供しなくなり、ホストの容量をデータに使用できなくなるため、クラスタの容量が自動的に減少します。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。 |

表 9-1. アップグレードの前提条件（続き）

| アップグレードの前提条件 | 説明 |
|--------------|--|
| vSAN ホスト | <p>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。</p> <p>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。</p> |
| 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。詳細については、VMware のナレッジベースの記事 <http://kb.vmware.com/kb/2147881> を参照してください。

2 ホスト構成のクラスタまたはストレッチ 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行うタスクは、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 クラスター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 クラスターの 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 クラスターの 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、『ホストとクラスター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 クラスター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、クラスター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。ストレッチ クラスター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、クラスター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。ストレッチ クラスターのアップグレードの詳細については、『ホストとクラスター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

ディスク フォーマットのアップグレードはオプションです。以前のディスク フォーマットのバージョンを使用していても、vSAN クラスタは問題なく稼働し続けます。

ベスト プラクティスは、オブジェクトをアップグレードして最新のオンディスク フォーマットを使用します。最新のオンディスク フォーマットでは、vSAN の完全な機能セットを使用できます。

ディスク グループは一度に1つずつアップグレードされるため、ディスク グループのサイズによってはディスク フォーマットのアップグレードに時間がかかる場合があります。各ディスク グループのアップグレードでは、各デバイスにあるすべてのデータが退避し、vSAN クラスタからディスク グループが削除されます。その後、新しいオンディスク フォーマットの vSAN に、ディスク グループが再び追加されます。

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。

オンディスク フォーマットのアップグレードを開始すると、vSAN はいくつかの処理を実行します。これらの処理は [コンポーネントの再同期] ページで監視できます。次の表は、ディスク フォーマットのアップグレードの各プロセスを示したものです。

表 9-2. アップグレードの進行状況

| 進行状況 | 説明 |
|----------|--|
| 0% ~ 5% | <p>クラスタのチェック。クラスタ コンポーネントが確認され、アップグレードの準備が行われます。このプロセスには数分かかります。vSAN は、アップグレードの完了の妨げになるような未解決の問題がないことを確認します。</p> <ul style="list-style-type: none"> ■ すべてのホストが接続されている。 ■ すべてのホストが適切なバージョンのソフトウェアを使用している。 ■ すべてのディスクの健全性が良好である。 ■ すべてのオブジェクトにアクセスできる。 |
| 5% ~ 10% | <p>ディスク グループのアップグレード。vSAN はデータを移行せずに最初のディスク アップグレードを実行します。このプロセスには数分かかります。</p> |

表 9-2. アップグレードの進行状況（続き）

| 進行状況 | 説明 |
|------------|---|
| 10% ~ 15% | オブジェクトの再編成。vSAN はすべてのオブジェクトのレイアウトを変更し、正しく編成されるようにします。スナップショットがわずかしかない小規模なシステムの場合、このプロセスは数分で完了します。多数のスナップショット、多数の断片化された書き込み、および多数の整理されていないオブジェクトを含む大規模なシステムの場合は、数時間から数日間かかることがあります。 |
| 15% ~ 95% | バージョン 3.0 より前の vSAN をアップグレードする場合のディスク グループの削除と再フォーマット。各ディスク グループがクラスタから削除され、再フォーマット後、再びクラスタに追加されます。このプロセスにかかる時間は、割り当てられた容量とシステムの負荷によって異なります。I/O キャパシティの上限に達している、または近づいているシステムでは、転送速度が低下します。 |
| 95% ~ 100% | オブジェクト バージョンのアップグレードの完了。新しいオンディスク フォーマットへのオブジェクトの変換と再同期が完了します。このプロセスにかかる時間は、使用しているディスク容量、および [冗長性の低下を許可] オプションを選択しているかどうかによって異なります。 |

アップグレード中、[コンポーネントの再同期] ページから、アップグレード プロセスを監視できます。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。RVC コマンド `vsan.upgrade_status <cluster>` を実行してアップグレードを監視することもできます。オプションの `-r <seconds>` フラグを使用すると、Ctrl+C キーを押すまで、アップグレード ステータスを定期的に更新できます。指定できる最短の更新間隔は 60 秒です。

デバイスの削除やアップグレードなどのその他のアップグレード タスクは、ステータス バーの [最近のタスク] ペインから監視できます。

ディスク フォーマットをアップグレードするときは次のことを考慮します。

- 3 台のホストを含むクラスタをアップグレードして完全退避を行う場合、[許容される障害の数] がゼロ (0) よりも大きいと、オブジェクトの退避に失敗します。3 ホスト構成のクラスタでは、2 台のホストのリソースのみでは、完全退避が行われているディスク グループを再度保護することはできません。[許容される障害の数] が 1 に設定されている場合、vSAN に 3 つの保護コンポーネント (2 つのミラーと 1 つの監視) を設定し、各保護コンポーネントを独立したホストに配置する必要があります。

3 ホスト構成のクラスタでは、退避モードとして [データ アクセシビリティの確保] を選択する必要があります。このモードを選択すると、ハードウェア障害でデータが損失する可能性があります。

また、十分な空き容量も必要です。この容量は、最も大きいディスク グループの論理的な使用キャパシティと等しくする必要があります。移行されるディスク グループとは異なるディスク グループにこの容量がある必要があります。

- 3 台のホストからなるクラスタをアップグレードする場合、またはリソースが制限されているクラスタをアップグレードする場合は、仮想マシンの冗長性低下を許可します。オプション `vsan.ondisk_upgrade --allow-reduced-redundancy` を指定して RVC コマンドを実行します。

- `--allow-reduced-redundancy` コマンド オプションを使用すると、特定の仮想マシンが移行中の障害を許容できなくなる可能性があります。また、障害に対する許容性を低下させることが、データ損失を招く可能性もあります。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の維持と冗長性をリストアします。アップグレード中は、仮想マシンのコンプライアンスと冗長性は一時的に維持されなくなります。アップグレードを完了してすべての再構築タスクを完了すると、仮想マシンのコンプライアンスが維持されるようになります。
- アップグレードの進行中は、ホストを削除または切断したり、ホストをメンテナンス モードにしたりしないでください。これらの処理によって、アップグレードが失敗する場合があります。

RVC コマンドとコマンド オプションの詳細については、『RVC コマンド リファレンス ガイド』を参照してください。

vSphere 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。

The screenshot shows the vSAN cluster configuration page in vSphere Client. The left sidebar shows the navigation tree with 'vSAN' expanded to 'Disk Management'. The main content area displays a table of disk groups and a list of disks.

| 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 |

| 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 |

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。

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、ディスクが健全な状態であることを確認します。RVC コマンド `vsan.disk_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、認定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 コマンドの使用方法の詳細については、『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 ホストのキャパシティはクラスタで利用できないため、クラスタ内で使用可能なリソースのキャパシティが減少します。このため、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前を一覧表示します。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 での進行状況の監視
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 個がアップグレード済み、残り 0
```

```
オブジェクトのアップグレードが完了しました:n 個が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。

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 9-3. 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マ 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>
```