vSAN のプランニングとデプロイ

Update 3
2019 年 8 月 20 日
VMware vSphere 6.7
VMware vSAN 6.7

vmware®

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

ヴイエムウェア株式会社
〒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

目次

vSAN のプランニングとデプロイ

「vSAN のプランニングとデプロイ」では、vSphere 環境で vSAN クラスタを設計およびデプロイする方法について説明します。これには、システム要件、サイジングのガイドラインおよび推奨されるベスト プラクティスの情報が含まれています。

対象読者

本書は、VMware vSphere 環境で vSAN クラスタを設計およびデプロイするユーザーを対象としています。ここには、仮想マシン テクノロジーおよび仮想データセンター運用に精通した、経験の豊富なシステム管理者向けの情報が含まれます。また、読者が VMware ESXi、vCenter Server、および vSphere Client などを含む、VMware vSphere に精通していることを前提としています。

vSAN の機能の詳細および vSAN クラスタの構成方法については、『VMware vSAN の管理』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。

vSphere Client および vSphere Web Client

本書の説明は、vSphere Client（HTML5 ベースの GUI）に対応しています。ここに記載のガイダンスは、vSphere Web Client（Flex ベースの GUI）を使用したタスクで使用できます。

vSphere Client と vSphere Web Client でワークフローが大きく異なるタスクでは、各クライアント インターフェイスに応じたステップが提供され、手順が重複しています。vSphere Web Client に関連する手順は、タイトルに vSphere Web Client が含まれています。

注： vSphere 6.7 Update 1 では、vSphere Web Client 機能のほぼすべてが vSphere Client に実装されています。サポート対象外の残りの機能を記載した最新のリストについては、「vSphere Client の機能の更新」を参照してください。

vSAN の概要

1

VMware vSAN は ESXi ハイパーバイザーの一部としてネイティブに実行されるソフトウェアの分散レイヤーです。vSAN はホスト クラスタのローカル ディスクまたは直接接続されたキャパシティ デバイスを統合し、vSAN クラスタのすべてのホストで共有される単一のストレージ プールを作成します。

HA、vMotion、DRS といった共有ストレージを必要とする VMware 機能をサポートすることで、vSAN では外部共有ストレージの必要性がなくなり、ストレージ構成や仮想マシンのプロビジョニング操作を簡素化できます。

この章には、次のトピックが含まれています。

vSAN の概念

VMware vSAN では、仮想マシンの共有ストレージをソフトウェア ベースで作成する方法を使用します。ESXi ホストのローカルの物理ストレージ リソースを仮想化し、サービス品質要件に沿って仮想マシンとアプリケーションに分割して割り当てることができる、ストレージのプールに変換します。vSAN は ESXi ハイパーバイザーに直接実装されます。

vSAN は、ハイブリッドのクラスタまたはオールフラッシュのクラスタのいずれかに構成できます。ハイブリッドのクラスタでは、キャッシュ レイヤーにフラッシュ デバイスが使用され、ストレージ キャパシティ レイヤーに磁気ディスクが使用されます。 オールフラッシュのクラスタでは、キャッシュとキャパシティの両方でフラッシュ デバイスが使用されます。

vSAN は、既存のホスト クラスタで、または新しく作成するクラスタで、有効にできます。vSAN は、すべてのローカル キャパシティ デバイスを、vSAN クラスタのすべてのホストによって共有される単一のデータストアに集約します。データストアは、キャパシティ デバイスまたはキャパシティ デバイスが搭載されているホストをクラスタに追加することにより、拡張することができます。 vSAN のベスト プラクティスとして、クラスタのすべての ESXi

ホストが、すべてのクラスタ メンバーと同様または同一の構成にすることをお勧めします。これにはストレージ構成も含まれます。この一貫した構成により、クラスタ内のすべてのデバイスおよびホストで、仮想マシンのストレージ コンポーネントが分散されます。ローカル デバイスを持たないホストでも、vSAN データストアに仮想マシンを参加させて実行することができます。

ホストがローカル ストレージ デバイスを vSAN データストアに提供する場合、フラッシュ キャッシュ用に少なくとも 1 個のデバイスを提供し、キャパシティ用に少なくとも 1 個のデバイスを提供する必要があります。キャパシティ デバイスはデータ ディスクとも呼ばれます。

提供元のホスト上のデバイスは、1 つ以上のディスク グループを形成します。各ディスク グループには、1 つのフラッシュ キャッシュ デバイスと、恒久的ストレージ用の 1 つまたは複数のキャパシティ デバイスが含まれています。各ホストは、複数のディスク グループを使用するように構成できます。

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

vSAN の特性

このトピックでは、vSAN とそのクラスタ、およびデータストアに適用される特性を概説します。

vSAN は、お使いの環境に数多くののメリットを提供します。

表 1-1. vSAN の機能

サポートされている機能	説明
共有ストレージ サポート	vSAN は、HA、vMotion、および DRS など、共有ストレージが必要な VMware 機能をサポートしています。たとえば、ホストの負荷が高くなると、DRS はクラスタ内の他のホストに仮想マシンを移行できます。
オンディスク フォーマット	vSAN 6.7.3 は、vSAN クラスタごとに拡張性の高いスナップショットとクローン管理のサポートを提供する、オンディスク仮想ファイル フォーマット 10.0 をサポートしています。vSAN クラスタごとにサポートされる仮想マシン スナップショットとクローンの数については、『構成の上限』ドキュメントを参照してください。
オールフラッシュ構成とハイブリッド構成	vSAN は、オールフラッシュまたはハイブリッド クラスタで構成できます。
フォールト ドメイン	vSAN は、vSAN クラスタがデータセンターの複数のラックまたはブレード サーバ シャーシにまたがる場合に、ラックまたはシャーシの障害からホストを保護するフォールト ドメイン構成をサポートしています。
iSCSI ターゲット サービス	vSAN iSCSI ターゲット サービスを使用すると、vSAN クラスタ外のホストおよび物理ワークロードが vSAN データストアにアクセスできます。
ストレッチ クラスタ	vSAN は 2 つの地理的な場所にまたがるストレッチ クラスタをサポートします。

表 1-1. vSAN の機能 （続き）

サポートされている機能	説明
Windows Server Failover Clustering (WSFC) のサポート	vSAN 6.7 Update 3 以降のリリースでは、共有ディスクへのアクセスをノード間で調停するために、Windows Server Failover Clustering (WSFC) で要求される仮想ディスク レベルでの SCSI-3 Persistent Reservations (SCSI3-PR) がサポートされます。SCSI-3 PR がサポートされることにより、vSAN データストアでネイティブに仮想マシン間で共有されているディスク リソースを使用して WSFC を構成できます。 現在、以下の構成がサポートされています。 ■ クラスタあたり最大 6 個のアプリケーション ノード。 ■ ノードあたり最大 64 台の共有仮想ディスク。 **注：** vSAN では、Microsoft Windows Server 2012 以降で実行される Microsoft SQL Server 2012 以降の動作が確認済みです。
vSAN Health Service	vSAN Health Service には、クラスタ コンポーネントの問題の原因を監視、トラブルシューティング、診断し、潜在的なリスクを識別する事前構成済みの健全性チェック テストが含まれています。
vSAN パフォーマンス サービス	vSAN パフォーマンス サービスには、IOPS、スループット、遅延、および輻輳の監視に使用される統計チャートが含まれています。vSAN クラスタ、ホスト、ディスク グループ、ディスク、および仮想マシンのパフォーマンスを監視できます。
組み込みの vSphere ストレージ機能	vSAN は、従来から VMFS および NFS ストレージとともに使用されている vSphere のデータ管理機能が組み込まれています。これらの機能には、スナップショット、リンク クローン、vSphere Replication が含まれます。
仮想マシン ストレージ ポリシー	vSAN では、仮想マシン ストレージ ポリシーと連携して、仮想マシン中心のストレージ管理をサポートしています。 仮想マシンのデプロイ中にストレージ ポリシーを割り当てない場合は、vSAN のデフォルト ストレージ ポリシーが自動的に仮想マシンに割り当てられます。
迅速なプロビジョニング	vSAN では、仮想マシンの作成中およびデプロイ中に、vCenter Server® で迅速にストレージをプロビジョニングできます。
デデュープおよび圧縮	vSAN はブロックレベルの重複排除および圧縮を実行してストレージ容量を節約します。vSAN オールフラッシュ クラスタで重複排除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。デデュープおよび圧縮はクラスタ全体の設定として有効にできますが、ディスク グループ単位で適用されます。
保存データの暗号化	vSAN では、保存データの暗号化が提供されます。データの暗号化は、デデュープなどの他のすべての処理が実行された後に行われます。保存データの暗号化を行うと、クラスタからデバイスが削除された場合に備えて、ストレージ デバイス上のデータが保護されます。
SDK サポート	VMware vSAN SDK for Java は、VMware vSphere Management SDK の拡張機能です。これには、開発者が vSAN のインストール、構成、監視、およびトラブルシューティングを自動化する際にに役立つドキュメント、ライブラリ、およびコード サンプルが含まれています。

vSAN の用語および定義

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

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

ディスク グループ

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

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

使用される容量

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

オブジェクト ベースのストレージ

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

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

- vSAN は、指定された仮想マシン ストレージ ポリシー設定に基づいて、仮想ディスク要件が適用されていることを確認します。
- vSAN はプロビジョニングの時点で、正しいクラスタ リソースが使用されていることを確認します。たとえば vSAN は、保護ポリシーに基づいて作成するレプリカの数を決定します。パフォーマンス ポリシーにより、各レプリカに割り当てられるフラッシュ リード キャッシュの量、各レプリカで作成されるストライプの数、およびそれらを配置するクラスタ内の場所が決まります。

- vSAN は、仮想ディスクのポリシーに準拠しているかどうかを継続的に監視してレポートします。ポリシーに準拠していない場合は、原因となっている問題のトラブルシューティングを行って解決する必要があります。

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

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

vSAN データストア

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

vSAN データストアでは、特定の特性について考慮する必要があります。

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

オブジェクトとコンポーネント

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

vSAN データストアには、次のオブジェクト タイプが含まれます。

VM Home 名前空間

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

VMDK

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

仮想マシン スワップ オブジェクト

仮想マシンのパワーオン時に作成されます。

スナップショット差分 VMDK

仮想マシンのスナップショットの作成時に作成されます。

メモリ オブジェクト

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

仮想マシンのコンプライアンス ステータス：準拠および非準拠

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

コンポーネントの状態：「低下」および「なし」

vSAN は、コンポーネントの次の障害状態を認識します。

- 低下 : vSAN で永続的なコンポーネント障害が検出され、障害が発生したコンポーネントが正常な状態に戻らないと判断される場合、コンポーネントのステータスは 「低下」 になります。vSAN は低下したコンポーネントの再構築をすぐに開始します。この状態は、障害の発生したデバイスにコンポーネントが存在する場合に発生することがあります。
- なし : vSAN で一時的なコンポーネント障害が検出され、そのすべてのデータを含むコンポーネントがリカバリされて vSAN が元の状態に戻るとみなされる場合、コンポーネントのステータスは 「なし」 になります。この状態は、ホストを再起動するとき、または vSAN ホストからデバイスを切り離す場合に発生する可能性があります。vSAN は 60 分待ってから、[なし] ステータスのコンポーネントの再構築を開始します。

オブジェクトの状態：[健全] および [非健全]

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

- 健全 : 少なくとも 1 つの完全な RAID 1 ミラーリングを使用できる場合、または最低限必要な数のデータ セグメントを使用できる場合、オブジェクトは健全であるとみなされます。

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

監視

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

vSAN 6.0 以降では、オブジェクトの可用性の判別に、各コンポーネントが 1 つ以上の票を持つ非対称投票システムを使用してクォーラムを維持します。票が 50 % を超えると、仮想マシンのストレージ オブジェクトはいつでもアクセス可能で、オブジェクトは利用可能とみなされます。票が 50 % 以下の場合、すべてのホストがオブジェクトにアクセス可能ですが、オブジェクトは vSAN データストアにアクセスできなくなります。アクセス不能なオブジェクトは、関連付けられた仮想マシンの可用性に影響を与えることがあります。

ストレージ ポリシーベースの管理 (SPBM)

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

Ruby vSphere Console (RVC)

Ruby vSphere Console (RVC) は、vSAN クラスタの管理およびトラブルシューティングに使用するコマンドライン インターフェイスです。RVC により、`esxcli` が提供するホスト中心のビューではなく、クラスタ全体のビューを表示できます。 RVC は vCenter Server Appliance および vCenter Server for Windows にバンドルされているため、個別にインストールする必要はありません。 RVC コマンドについては、『RVC Command Reference Guide』を参照してください。

vSphere PowerCLI

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

vSAN Observer

VMware vSAN Observer は、RVC で実行される Web ベースのツールで、vSAN クラスタの詳細なパフォーマンス分析と監視に使用されます。vSAN Observer を使用して、キャパシティ レイヤーのパフォーマンス統計、物理ディスク グループの統計情報、CPU の現在の負荷、vSAN メモリ プールの使用量、vSAN クラスタ全体の物理およびインメモリ オブジェクトの分散状況を表示します。

RVC と vSAN Observer の構成、起動、および使用方法の詳細については、『vSAN Troubleshooting Reference Manual』を参照してください。

vSAN と従来のストレージ

vSAN には従来のストレージ アレイと共通する特性が多数ありますが、vSAN の全体的な動作と機能は異なります。たとえば、vSAN は ESXi ホストのみの管理と処理が可能で、vSAN インスタンスごとに 1 つのクラスタのみがサポートされています。

vSAN と従来のストレージには、主に次のような違いがあります。

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

vSAN クラスタの構築

vSAN を考慮する場合、vSAN クラスタをデプロイするための複数の構成ソリューションから選択できます。

要件に応じて、次のいずれかの方法で vSAN をデプロイできます。

vSAN ReadyNode

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

ユーザー定義 vSAN クラスタ

vSAN クラスタを構築するには、vSAN 互換性ガイド (VCG) Web サイト (http://www.vmware.com/resources/compatibility/search.php) に記載されている個々のソフトウェアとハードウェア コンポーネント（ドライバ、ファームウェア、ストレージ I/O コントローラなど）を選択します。VCG Web サイトに記載されている認定された任意のサーバ、ストレージ I/O コントローラ、キャパシティ デバイスとフラッシュ キャッシュ デバイス、メモリ、CPU ごとに必要なコア数を選択できます。vSAN でサポートされているソフトウェアおよびハードウェア コンポーネント、ドライバ、ファームウェア、およびストレージ I/O コントローラを選択する前に、VCG Web サイトで互換性情報を確認します。vSAN クラスタを設計する場合は、VCG Web サイトに記載されているデバイス、ファームウェア、ドライバのみを使用します。VCG に記載されていないソフトウェアおよびハードウェア バージョンを使用すると、クラスタで障害や予期しないデータ損失が発生する可能性があります。vSAN クラスタの設計の詳細については、3 章 vSAN クラスタの設計とサイジングを参照してください。

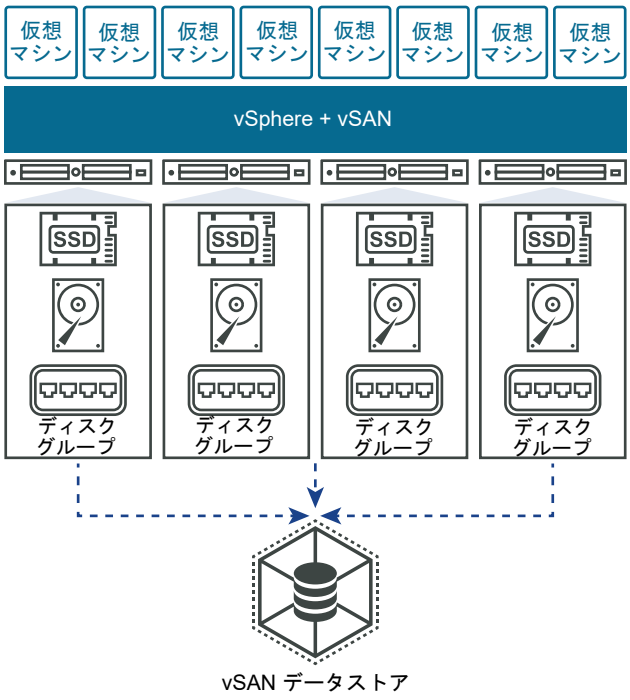
vSAN デプロイのオプション

このセクションでは、vSAN クラスタでサポートされているさまざまな展開オプションについて説明します。

標準 vSAN クラスタ

標準の vSAN クラスタは、3 台以上のホストで構成されます。通常、標準の vSAN クラスタ内のすべてのホストは同じ場所に配置され、同じレイヤー 2 ネットワークに接続されています。オールフラッシュ構成では 10Gb ネットワーク接続が必要です。これはハイブリッド構成の場合にも推奨されます。

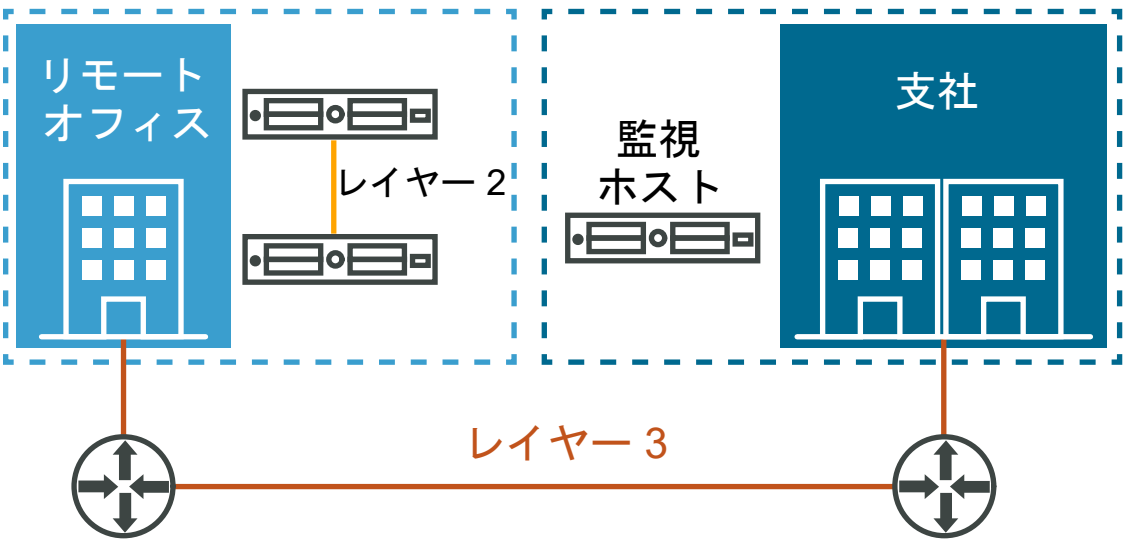
詳細については、5 章 vSAN クラスタの作成を参照してください。



2 ホスト vSAN クラスタ

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

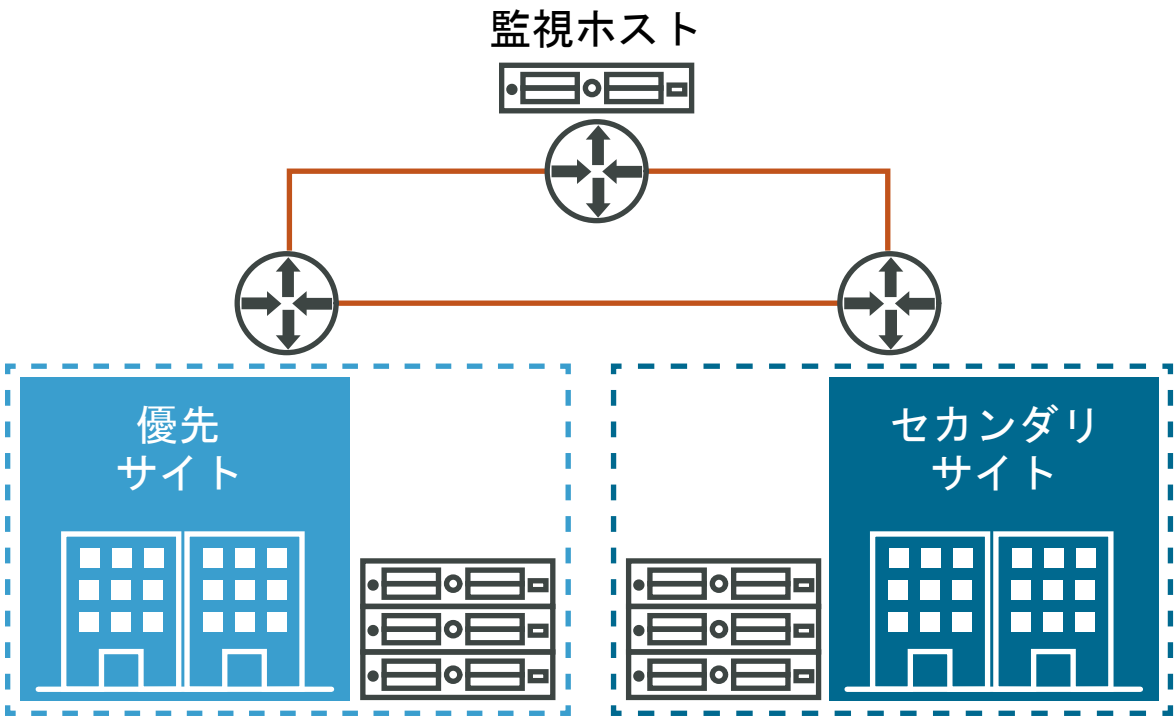
詳細については、ストレッチ クラスタの概要 を参照してください。



vSAN ストレッチ クラスタ

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

詳細については、ストレッチ クラスタの概要 を参照してください。



他の VMware ソフトウェアとの統合

vSAN を起動して実行すると、残りの VMware ソフトウェア スタックと統合されます。vSphere コンポーネントや、vSphere vMotion、スナップショット、クローン、Distributed Resource Scheduler (DRS)、vSphere High Availability、vCenter Site Recovery Manager などの機能を使用すると、従来のストレージで可能なほとんどの操作を実行できます。

vSphere HA との統合

vSphere HA と vSAN を同じクラスタで有効にできます。 従来のデータストアの場合と同様に、vSphere HA では vSAN データストアの仮想マシンに同じレベルの保護が提供されます。 このレベルの保護では、vSphere HA と vSAN がやり取りするときに、特定の制限が適用されます。 vSphere HA と vSAN の統合に関する特定の考慮事項については、 vSAN および vSphere HA の使用を参照してください。

VMware Horizon View との統合

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

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

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

vSAN の制限事項

このトピックでは、vSAN の制限事項について説明します。

vSAN を操作するときは、次の制限事項を考慮してください。

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

vSAN を有効にするための要件

2

vSAN を有効にする前に、ご使用の環境ですべての要件が満たされていることを確認してください。

この章には、次のトピックが含まれています。

- vSAN のハードウェア要件
- vSAN のクラスタ要件
- vSAN のソフトウェア要件
- vSAN のネットワーク要件
- ライセンス要件

vSAN のハードウェア要件

組織の ESXi ホストが vSAN のハードウェア要件を満たすことを確認します。

ストレージ デバイスの要件

vSAN 構成に含まれるすべてのキャパシティ デバイス、ドライバ、およびファームウェア バージョンが、『VMware 互換性ガイド』の「vSAN」セクションのリストに記載され、認定されている必要があります。

表 2-1. vSAN ホストでのストレージ デバイスの要件

ストレージ コンポーネント	要件
キャッシュ	■ 1 個の SAS または SATA 半導体ディスク (SSD) または PCIe フラッシュ デバイス。 ■ [許容されるプライマリ レベルの障害数] を計算する前に、各ディスク グループのフラッシュ キャッシュ デバイスのサイズを確認します。ハイブリッド クラスタの場合、キャパシティ デバイス上で使用する予定のストレージ容量の少なくとも 10%（ミラーなどのレプリカを含まない）を提供する必要があります。 ■ キャッシュ フラッシュ デバイスは、VMFS や別のファイル システムによってフォーマットしないようにする必要があります。
仮想マシンのデータ ストレージ	■ ハイブリッド グループ構成の場合は、SAS または NL-SAS 磁気ディスクが少なくとも 1 個使用できることを確認します。 ■ オールフラッシュ ディスク グループ構成の場合は、少なくとも 1 個の SAS または SATA 半導体ディスク (SSD) または PCIe フラッシュ デバイス利用できることを確認します。
ストレージ コントローラ	SAS または SATA ホスト バス アダプタ (HBA)、またはパススルー モードか RAID 0 モードの RAID コントローラ 1 個。 同じストレージ コントローラが vSAN ディスクと非 vSAN ディスクの両方をバッキングしている場合は、問題を回避するために次の点を考慮します。 vSAN ディスクと非 vSAN ディスクに異なるコントローラ モードを設定して、一貫しない方法でディスク処理を行うことは避けてください。vSAN の運用に悪影響となる場合があります。vSAN ディスクが RAID モードの場合は、非 vSAN ディスクも RAID モードにする必要があります。 VMFS に非 vSAN ディスクを使用する場合は、VMFS データストアをスクラッチ、ログ記録、およびコア ダンプ専用にします。 vSAN ディスクまたは RAID グループとコントローラを共有するディスクまたは RAID グループで仮想マシンを実行しないでください。 非 vSAN ディスクを Raw デバイス マッピング (RDM) として仮想マシンのゲストにパススルーしないでください。 詳細については、https://kb.vmware.com/s/article/2129050 を参照してください。 パススルーや RAID など、コントローラでサポートされている機能については、vSAN HCL (https://www.vmware.com/resources/compatibility/search.php?deviceCategory=vsan) を参照してください。

メモリ

vSAN のメモリ要件は、ESXi ハイパーバイザーが管理するディスク グループとデバイス数によって決まります。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/2113954 を参照してください。

フラッシュ起動デバイス

ESXi インストーラは、インストール中、起動デバイスにコア ダンプ パーティションを作成します。コア ダンプ パーティションのデフォルトのサイズは、ほとんどすべてのインストール環境の要件を満たすことができます。

- ESXi ホストのメモリが 512 GB 以下であれば、USB、SD、または SATADOM デバイスからホストを起動できます。vSAN を USB デバイスや SD カードから起動する場合、起動デバイスのサイズは少なくとも 4 GB にする必要があります。
- ESXi ホストのメモリが 512 GB を超える場合は、次のガイドラインを検討します。
  - 16 GB 以上のサイズの SATADOM またはディスク デバイスからホストを起動することができます。SATADOM デバイスを使用する場合は、シングル レベル セル (SLC) デバイスを使用します。
  - vSAN 6.5 以降を使用している場合、USB/SD デバイスから起動するには、ESXi ホストのコアダンプ パーティションのサイズを変更する必要があります。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。

ESXi 6.0 以降のホストを USB デバイスまたは SD カードから起動する場合、vSAN トレース ログは RAM ディスクに書き込まれます。シャットダウンやシステム クラッシュ（パニック）が発生すると、これらのログは永続メディアへ自動的にオフロードされます。これは、ESXi を USB スティックまたは SD カードから起動する際、vSAN トレースの処理にサポートされている唯一の方法です。電源障害が発生した場合、vSAN トレース ログは保存されません。

ESXi 6.0 以降のホストを SATADOM デバイスから起動する場合、vSAN トレース ログは直接 SATADOM デバイスに書き込まれます。したがって、SATADOM デバイスが、このガイドで説明している仕様を満たしていることが重要です。

vSAN のクラスタ要件

vSAN を有効にするための要件をホスト クラスタが満たしていることを確認します。

- vSAN 構成に含まれるすべてのキャパシティ デバイス、ドライバ、およびファームウェア バージョンが、『VMware 互換性ガイド』の「vSAN」セクションのリストに記載され、認定されている必要があります。
- vSAN クラスタには、クラスタの容量を構成する、最低 3 台のホストが必要です。3 台のホストからなるクラスタの考慮事項については、vSAN クラスタの設計に関する考慮事項を参照してください。
- vSAN クラスタ内のホストは他のクラスタに参加することはできません。

vSAN のソフトウェア要件

環境内の vSphere コンポーネントが vSAN を使用するためのソフトウェア バージョンの要件を満たしていることを確認します。

vSAN 機能のフル セットを使用するには、vSAN クラスタに参加する ESXi ホストをバージョン 6.7 Update 3 以降にする必要があります。vSAN の以前のバージョンからのアップグレード時に現在のオンディスク フォーマット バージョンを保持できますが、新しい機能の多くは使用できません。vSAN 6.7.3 以降のソフトウェアでは、すべてのオンディスク フォーマットがサポートされます。

vSAN のネットワーク要件

ESXi ホストでのネットワーク インフラストラクチャとネットワーク構成が、vSAN の最低限のネットワーク要件を満たしていることを確認します。

表 2-2. vSAN のネットワーク要件

ネットワーク コンポーネント	要件
ホストのバンド幅	各ホストには、vSAN 専用の最低限のバンド幅が必要です。 ■ ハイブリッド構成の場合は専用の 1 Gbps ■ オールフラッシュ構成の場合は専用または共有の 10 Gbps vSAN でのネットワークに関する考慮事項の詳細については、 vSAN ネットワークの設計を参照してください。
ホスト間の接続	vSAN クラスタの各ホストには、容量を提供するかどうかに関係なく、vSAN トラフィックに VMkernel ネットワーク アダプタが必要です。 vSAN の VMkernel ネットワークの設定を参照してください。
ホストのネットワーク	vSAN クラスタのすべてのホストは、vSAN レイヤー 2 またはレイヤー 3 ネットワークに接続されている必要があります。
IPv4 および IPv6 のサポート	vSAN ネットワークでは、IPv4 と IPv6 の両方がサポートされます。
ネットワーク遅延	■ クラスタ内のすべてのホスト間で標準（非ストレッチ）vSAN クラスタに対して最大 1 ミリ秒の RTT ■ ストレッチ クラスタの 2 つのメイン サイト間で最大 5 ミリ秒の RTT ■ メイン サイトから vSAN 監視ホストへ最大 200 ミリ秒の RTT

ライセンス要件

有効な vSAN のライセンスがあることを確認します。

本番環境で vSAN を使用するには、特別なライセンスを vSAN クラスタに割り当てる必要があります。

標準の vSAN ライセンスや、高度な機能をカバーするライセンスをクラスタに割り当てることができます。高度な機能には、RAID 5/6 イレイジャ コーディングと重複排除および圧縮が含まれます。エンタープライズ ライセンスが、暗号化とストレッチ クラスタに必要です。ライセンスの割り当ての詳細については、vSAN クラスタのライセンス設定を参照してください。

ライセンスの容量は、クラスタ内の CPU の合計数を満たしている必要があります。

vSAN クラスタの設計とサイジング

3

パフォーマンスと使用を最適にするには、vSphere 環境で vSAN をデプロイする前にホストおよびそのストレージ デバイスの機能および構成を計画します。vSAN クラスタ内での特定のホストおよびネットワーク構成について、慎重に検討してください。

『VMware vSAN の管理』ドキュメントでは、vSAN クラスタの設計およびサイジングに関する主要なポイントについて説明しています。vSAN クラスタの設計およびサイジングに関する詳細な手順については、『VMware vSAN 設計とサイジング ガイド』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 ストレージ コンポーネントの設計とサイジング
- vSAN ホストの設計とサイジング
- vSAN クラスタの設計に関する考慮事項
- vSAN ネットワークの設計
- vSAN ネットワークのベスト プラクティス
- vSAN フォルト ドメインの設計とサイジング
- 起動デバイスと vSAN の使用
- vSAN クラスタでの永続的なログ記録

vSAN ストレージ コンポーネントの設計とサイジング

予期される消費に基づいて、容量およびキャッシュを計画します。 可用性と耐久性に関する要件を考慮してください。

- vSAN でのキャパシティ プランニング

  vSAN データストアのキャパシティをサイジングして、クラスタ内の仮想マシン ファイルを調整し、障害およびメンテナンス処理に対応することができます。

- vSAN でのフラッシュ キャッシュ デバイスの設計上の考慮事項

  高パフォーマンスを実現して必要なストレージ容量を確保し、将来的な拡張に対応できるように、vSAN キャッシュ デバイスおよびオールフラッシュ キャパシティ デバイスとして使用するフラッシュ デバイス構成を計画します。

- vSAN のフラッシュ キャパシティ デバイスの設計に関する考慮事項

  高いパフォーマンスと必要なストレージ容量を提供し、将来の増加に対応できるように、vSAN オールフラッシュ構成に対するフラッシュ キャパシティ デバイスの構成を計画します。

- vSAN の磁気ディスクの設計に関する考慮事項

  ストレージ容量とパフォーマンスの要件に従って、ハイブリッド構成での磁気ディスクサイズと数について検討します。

- vSAN のストレージ コントローラの設計に関する考慮事項

  パフォーマンスと可用性の要件に最適な vSAN クラスタのホストにストレージ コントローラを含めます。

vSAN でのキャパシティ プランニング

vSAN データストアのキャパシティをサイジングして、クラスタ内の仮想マシン ファイルを調整し、障害およびメンテナンス処理に対応することができます。

Raw キャパシティ

この式を使用して、vSAN データストアの Raw キャパシティを決定します。これらのディスク グループ内のキャパシティ デバイスのサイズで、クラスタ内のディスク グループの合計数を乗算します。vSAN オンディスク フォーマットで必要なオーバーヘッドを減算します。

許容されるプライマリ レベルの障害数

vSAN データストアのキャパシティ（仮想マシン数と VMDK ファイルのサイズは含まない）をプランニングする場合、クラスタの仮想マシン ストレージ ポリシーの [許容されるプライマリ レベルの障害数] および [障害の許容方法] 属性を考慮する必要があります。

[許容されるプライマリ レベルの障害数] は、vSAN のストレージのキャパシティ プランでサイズを指定するときに重要な役割を果たします。仮想マシンの可用性の要件に基づいて設定する場合、仮想マシンとその個々のデバイスの使用量の 2 倍以上のサイズになる可能性があります。

たとえば、[障害の許容方法] が [RAID-1（ミラーリング）- パフォーマンス] に設定されていて、[許容されるプライマリ レベルの障害数] (PFTT) が 1 に設定されている場合、仮想マシンは Raw キャパシティの約 50% を使用できます。PFTT を 2 に設定すると、使用可能なキャパシティが約 33% になります。PFTT を 3 に設定すると、使用可能なキャパシティが約 25% になります。

ただし、[障害の許容方法] が [RAID-5/6（イレージャ コーディング）- キャパシティ] に設定されていて、FTT が 1 に設定されている場合、仮想マシンは Raw 容量の約 75% を使用できます。PFTT を 2 に設定すると、使用可能なキャパシティが約 67% になります。RAID 5/6 の詳細については、VMware vSAN の管理を参照してください。

vSAN ストレージ ポリシーの属性の詳細については、VMware vSAN の管理を参照してください。

必要なキャパシティの計算

次の基準に従って、RAID 1 ミラーリングが構成されているクラスタ内の仮想マシンのキャパシティ プランニングを行います。

1 vSAN クラスタ内の仮想マシンで使用されることが予想されるストレージ容量を計算します。

```
expected overall consumption = number of VMs in the cluster * expected percentage of
consumption per VMDK
```

2 クラスタ内の仮想マシンのストレージ ポリシーで構成される [許容されるプライマリ レベルの障害数] 属性を考慮します。この属性は、クラスタ内のホスト上の VMDK ファイルのレプリカ数に直接影響します。

```
datastore capacity = expected overall consumption * (PFTT + 1)
```

3 vSAN オンディスク フォーマットのオーバーヘッド要件を見積もります。

- オンディスク フォーマット バージョン 3.0 以降では、一般的にデバイスあたり 1 ～ 2% 未満の容量の追加のオーバーヘッドがかかります。ソフトウェア チェックサムが有効な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。
- オンディスク フォーマット バージョン 2.0 では、一般的にデバイスあたり 1 ～ 2% 未満の容量の追加のオーバーヘッドがかかります。
- 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 の追加のオーバーヘッドがかかります。

キャパシティ サイジング ガイドライン

- vSAN がストレージ負荷を再分散しないように、少なくとも 30% の容量を未使用のままにします。vSAN は、1 個のキャパシティ デバイスの使用量が 80% 以上に達するとクラスタ全体でコンポーネントの再分散を行います。再分散処理は、アプリケーションのパフォーマンスに影響する可能性があります。この問題を回避するには、ストレージ使用率を 70% 未満に維持します。
- キャパシティ デバイス、ディスク グループ、およびホストの障害発生時または置き換えの処理に使用するキャパシティを追加します。キャパシティ デバイスにアクセスできなると、vSAN はクラスタ内の別のデバイスからコンポーネントをリカバリします。フラッシュ キャッシュ デバイスで障害が発生するか削除された場合、vSAN はディスク グループ全体からコンポーネントをリカバリします。
- ホストに障害が発生した後またはメンテナンス モードになったときに、vSAN がコンポーネントを確実にリカバリできるように、追加のキャパシティを予約します。たとえば、ホストに十分なキャパシティをプロビジョニングして、ホスト障害が発生した後またはメンテナンス中のコンポーネントの再構築に必要なキャパシティが十分に残るようにします。障害が発生したコンポーネントの再構築に必要な空き容量を確保するため、4 台以上のホストを使用する場合、この追加キャパシティは非常に重要です。ホストで障害が発生した場合、新たな障害に対応できるように、別のホストの使用可能なストレージで再構築が行われます。ただし、3 台のホストで構成されたクラスタで [許容されるプライマリ レベルの障害数] が 1 に設定されている場合、1 台のホストで障害が発生するとクラスタ内には 2 台のホストのみが残されるため、vSAN は再構築操作を実行しません。障害発生後に再構築を行うには、少なくとも 3 台のホストが稼動している必要があります。

- vSAN 仮想マシン ストレージ ポリシーの変更に使用する十分な容量の一時ストレージを用意します。仮想マシン ストレージ ポリシーを動的に変更する場合、vSAN は、オブジェクトの新しい RAID ツリー レイアウトを作成する可能性があります。vSAN が新しいレイアウトをインスタンス化して同期する際、オブジェクトが使用する容量が一時的に増加することがあります。このような変化に対応するため、クラスタに一定の一時ストレージ容量を確保します。
- ソフトウェア チェックサムやデデュープおよび圧縮などの高度な機能を使用する場合、処理のオーバーヘッドに対応する追加のキャパシティを予約しておきます。

仮想マシン オブジェクトの考慮事項

vSAN データストアのストレージ キャパシティを検討する際は、データストアに必要な VM Home ネームスペース オブジェクト、スナップショット、およびスワップ ファイルの容量を考慮します。

- VM Home ネームスペース：VM Home ネームスペース オブジェクトに特定のストレージ ポリシーを割り当てることができます。キャパシティとキャッシュ ストレージの不要な割り当てを防ぐため、vSAN は VM Home 名前空間のポリシーから [許容されるプライマリ レベルの障害数] と [強制プロビジョニング] の設定のみを適用します。[許容されるプライマリ レベルの障害数] が 0 より大きい VM Home ネームスペースに割り当てられたストレージ ポリシーの要件を満たすように、ストレージ容量のプランニングを行ってください。
- スナップショット。差分デバイスは、ベースとなる VMDK ファイルのポリシーを継承します。スナップショットの想定されるサイズと数、および vSAN ストレージ ポリシーの設定に合わせて、追加容量を検討します。

  必要となる容量はさまざます。仮想マシンがデータを更新する頻度や、仮想マシンがスナップショットにアクセスする時間によって、サイズは異なります。
- スワップ ファイル。vSAN は、仮想マシンのスワップ ファイルに個別のストレージ ポリシーを使用します。このポリシーは単一障害を許容し、ストライピングおよび読み取りキャッシュ予約は定義せずに、強制プロビジョニングを有効にします。

vSAN でのフラッシュ キャッシュ デバイスの設計上の考慮事項

高パフォーマンスを実現して必要なストレージ容量を確保し、将来的な拡張に対応できるように、vSAN キャッシュ デバイスおよびオールフラッシュ キャパシティ デバイスとして使用するフラッシュ デバイス構成を計画します。

PCIe または SSD フラッシュ デバイスの選択

vSAN ストレージのパフォーマンス、容量、書き込み耐久性、およびコストの要件に応じて、PCIe または SSD フラッシュ デバイスを選択します。

- 互換性。 PCIe または SSD デバイスのモデルは、『VMware 互換性ガイド』の「vSAN」セクションのリストに含まれている必要があります。
- パフォーマンス。 一般に、PCIe デバイスのパフォーマンスは SSD デバイスよりも高速です。
- 容量。 PCIe デバイスで使用可能な最大容量は、『VMware 互換性ガイド』において現在 vSAN の互換 SSD デバイスとしてリストに含まれている最大容量よりも大きくなります。
- 書き込み耐久性。 PCIe または SSD デバイスの書き込み耐久性は、容量、オールフラッシュ構成のキャッシュ、およびハイブリッド構成でのキャッシュの要件を満たす必要があります。

オールフラッシュ構成とハイブリッド構成での書き込み耐久性要件の詳細については、『VMware vSAN 設計とサイジング ガイド』を参照してください。 PCIe および SSD デバイスの書き込み耐久性クラスの詳細については、『VMware 互換性ガイド』の「vSAN」セクションを参照してください。

- コスト。 一般に、PCIe デバイスのコストは SSD デバイスの場合よりも高くなります。

vSAN キャッシュとしてのフラッシュ デバイス

これらの考慮事項に基づき、書き込み耐久性、パフォーマンス、および潜在的な拡張性について、vSAN 用のフラッシュ キャッシュの構成を設計します。

表 3-1. vSAN キャッシュのサイジング

ストレージ構成	考慮事項
オールフラッシュ構成とハイブリッド構成	■ キャッシュ対容量比を高くすれば、将来的に容量を拡張しやすくなります。キャッシュのサイズを大きめに設定することにより、キャッシュのサイズを増やさずに、既存のディスク グループに容量を追加することができます。 ■ フラッシュ キャッシュ デバイスには、高い書き込み耐久性が必要です。 ■ フラッシュ キャッシュ デバイスの置き換えは、ディスク グループ全体に影響が及ぶ操作であるため、キャパシティ デバイスの置き換えよりも複雑になります。 ■ フラッシュ デバイスを追加してキャッシュのサイズを追加する場合は、ディスク グループをさらに作成する必要があります。フラッシュ キャッシュ デバイスとディスク グループの比率は、常に 1:1 です。 複数のディスク グループを構成することには、次の利点があります。 ■ 障害のリスクが低減されます。単一のキャッシュ デバイスに障害が発生した場合、影響を受けるキャパシティ デバイスの数が少なくなります。 ■ 小サイズのフラッシュ キャッシュ デバイスを含むディスク グループを複数デプロイすれば、潜在的にパフォーマンスが向上します。 ただし、複数のディスク グループを構成すると、ホストのメモリ消費量は増大します。
オールフラッシュ構成	オールフラッシュ構成の場合、vSAN は書き込みキャッシュでのみキャッシュ レイヤーを使用します。書き込みキャッシュには、大量の書き込み動作を処理する能力が必要です。このアプローチでは容量フラッシュの存続期間が延び、より廉価で、書き込み耐久性が低くなります。
ハイブリッド構成	フラッシュ キャッシュ デバイスは、仮想マシンの使用が想定される、予測されたストレージの少なくとも 10%（ミラーなどのレプリカを含まない）を提供する必要があります。仮想マシン ストレージ ポリシーの [許容されるプライマリ レベルの障害数] 属性は、キャッシュのサイズに影響しません。 アクティブな仮想マシン ストレージ ポリシーで読み取りキャッシュの予約が設定されている場合、vSAN クラスタのホストには、障害後の再構築またはメンテナンス操作の期間に予約の必要を満たす十分なキャッシュが必要です。 使用可能な読み取りキャッシュが予約の必要を満たすほど十分でない場合は、再構築またはメンテナンス操作に失敗します。読み取りキャッシュ予約は、特定のワークロードに対する明確で既知のパフォーマンス要件を満たす必要がある場合にのみ使用します。 スナップショットを使用する場合は、キャッシュ リソースが消費されます。いくつかのスナップショットを使用する場合は、キャッシュ対消費容量比 10 パーセントの従来量よりも多くのキャッシュを専用に使用することを考慮します。

vSAN のフラッシュ キャパシティ デバイスの設計に関する考慮事項

高いパフォーマンスと必要なストレージ容量を提供し、将来の増加に対応できるように、vSAN オールフラッシュ構成に対するフラッシュ キャパシティ デバイスの構成を計画します。

PCIe または SSD フラッシュ デバイスの選択

vSAN ストレージのパフォーマンス、容量、書き込み耐久性、およびコストの要件に応じて、PCIe または SSD フラッシュ デバイスを選択します。

- 互換性。 PCIe または SSD デバイスのモデルは、『VMware 互換性ガイド』の「vSAN」セクションのリストに含まれている必要があります。
- パフォーマンス。 一般に、PCIe デバイスのパフォーマンスは SSD デバイスよりも高速です。
- 容量。 PCIe デバイスで使用可能な最大容量は、『VMware 互換性ガイド』において現在 vSAN の互換 SSD デバイスとしてリストに含まれている最大容量よりも大きくなります。
- 書き込み耐久性。 PCIe または SSD デバイスの書き込み耐久性は、容量、オールフラッシュ構成のキャッシュ、およびハイブリッド構成でのキャッシュの要件を満たす必要があります。

  オールフラッシュ構成とハイブリッド構成での書き込み耐久性要件の詳細については、『VMware vSAN 設計とサイジング ガイド』を参照してください。 PCIe および SSD デバイスの書き込み耐久性クラスの詳細については、『VMware 互換性ガイド』の「vSAN」セクションを参照してください。
- コスト。 一般に、PCIe デバイスのコストは SSD デバイスの場合よりも高くなります。

vSAN キャパシティとしてのフラッシュ デバイス

オールフラッシュ構成では、vSAN は読み取り操作にキャッシュを使用せず、仮想マシン ストレージ ポリシーの読み取りキャッシュ予約設定を適用しません。キャッシュには、書き込み耐久性の高い、少量の高価なフラッシュを使用できます。 容量には、書き込み耐久性の低い安価なフラッシュを使用できます。

フラッシュ キャパシティ デバイスの構成は、次のガイドラインに従って計画します。

- vSAN のパフォーマンスを高めるには、小さいフラッシュ キャパシティ デバイスによるディスク グループをより多く使用します。
- バランスのとれたパフォーマンスと予測しやすい動作を実現するために、タイプとモデルが同じフラッシュ キャパシティ デバイスを使用します。

vSAN の磁気ディスクの設計に関する考慮事項

ストレージ容量とパフォーマンスの要件に従って、ハイブリッド構成での磁気ディスクサイズと数について検討します。

SAS および NL-SAS 磁気デバイス

vSAN ストレージのパフォーマンス、容量、コストの要件に沿って、SAS または NL-SAS 磁気デバイスを使用します。

- 互換性。 磁気ディスクのモデルは認証され、『VMware 互換性ガイド』の「vSAN」セクションに記載されている必要があります。

- パフォーマンス。 SAS および NL-SAS デバイスはパフォーマンスが高速です。
- キャパシティ。 vSAN の SAS または NL-SAS 磁気ディスクのキャパシティは、『VMware 互換性ガイド』の「vSAN」セクションで確認できます。容量が多いデバイスを少数使用するのではなく、容量が多いデバイスを多数使用することを検討してください。
- コスト。 SAS および NL-SAS デバイスは高価な場合があります。

vSAN キャパシティとしての磁気ディスク

次のガイドラインに従って、磁気ディスクの構成について検討します。

- vSAN のパフォーマンスを向上させるには、容量が少ない磁気ディスクを数多く使用します。

  キャッシュとキャパシティ デバイス間でのデータ転送全体で適切なパフォーマンスを得るには、十分な数の磁気ディスクを使用する必要があります。 容量が少ない磁気ディスクを数多く使用すると、容量が多いデバイスを少数使用する場合に比べてパフォーマンスが向上します。 複数の磁気ディスク スピンドルを使用すると、ステージング解除の処理時間を短縮できます。

  多くの仮想マシンが配置された環境では、読み取りキャッシュからデータを読み取れず、vSAN が磁気ディスクからデータを読み取る場合に、磁気ディスクの数が重要となります。仮想マシンの数が少ない環境では、アクティブな仮想マシン ストレージ ポリシーの [オブジェクトあたりのディスク ストライプの数] が 1 より大きければ、ディスク数が読み取り操作に影響します。
- 負荷を分散してパフォーマンスと予測しやすい動作を実現するには、タイプとモデルが同じ磁気ディスクを vSAN データストアで使用します。
- ストレージ ポリシーに設定された [許容されるプライマリ レベルの障害数] 属性と [オブジェクトあたりのディスク ストライプの数] 属性の値を満たすには、十分な数の専用の磁気ディスクを使用します。vSAN の仮想マシン ストレージ ポリシーの詳細については、「VMware vSAN の管理」を参照してください。

vSAN のストレージ コントローラの設計に関する考慮事項

パフォーマンスと可用性の要件に最適な vSAN クラスタのホストにストレージ コントローラを含めます。

- 『VMware 互換性ガイド』に記載されているストレージ コントローラ モデル、およびドライバとファームウェアのバージョンを使用します。 『VMware 互換性ガイド』で vSAN を検索します。
- 可能であれば複数のストレージ コントローラを使用して、パフォーマンスを高め、起こり得るコントローラの障害をディスク グループのサブセットのみに分離します。
- 『VMware 互換性ガイド』キュー深度が最も高いストレージ コントローラを使用します。 キュー深度が高いコントローラを使用すると、パフォーマンスが向上します。 たとえば vSAN が障害発生後にコンポーネントを再構築するときやホストがメンテナンス モードになったときです。
- vSAN のパフォーマンスを最適化するには、ストレージ コントローラをパススルー モードで使用します。 RAID 0 モードのストレージ コントローラは、パススルー モードのストレージ コントローラに比べて、より高度な構成とメンテナンス作業が必要になります。

vSAN ホストの設計とサイジング

パフォーマンスおよび可用性を最適にするには、vSAN クラスタのホストの構成を計画します。

メモリと CPU

次の考慮事項に基づいて、vSAN クラスタのホストのメモリと CPU のサイズを指定します。

表 3-2. vSAN ホストのメモリと CPU のサイジング

計算リソース	考慮事項
メモリ	■ 仮想マシンあたりのメモリ ■ 仮想マシンの予測数に基づいたホストあたりのメモリ ■ ホストあたりに 5 個のディスク グループ、ディスク グループあたりに 7 個のキャパシティ デバイスが搭載された、完全に動作可能な vSAN 用に 32 GB 以上のメモリ メモリが 512 GB 以下のホストは、USB、SD、または SATADOM デバイスから起動できます。ホストのメモリが 512 GB より大きい場合は、SATADOM またはディスク デバイスからホストを起動してください。 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/2113954 を参照してください
CPU	■ ホストあたりのソケット ■ ソケットごとのコア ■ 仮想マシンの予測数に基づいた vCPU 数 ■ vCPU とコアの比 ■ vSAN の 10% の CPU オーバーヘッド

ホストのネットワーク

パフォーマンス向上のため、vSAN トラフィックにさらに多くのバンド幅を提供します。

- 1 GbE のアダプタを備えたホストを使用する場合は、アダプタを vSAN 専用にします。オールフラッシュ構成の場合は、10 GbE の専用または共有アダプタを備えたホストを使用します。
- 10 GbE のアダプタを使用する場合は、ハイブリッド構成およびオールフラッシュ構成のどちらの場合も、アダプタを他のトラフィックと共有できます。
- 10 GbE のアダプタを他のトラフィック タイプと共有する場合は、vSAN トラフィックに vSphere Distributed Switch を使用し、Network I/O Control と VLAN を使用することによってトラフィックを分離します。
- 冗長性を持たせるため、vSAN トラフィックに物理アダプタのチームを作成します。

複数のディスク グループ

フラッシュ キャッシュまたはストレージ コントローラが応答を停止した場合、ディスク グループ全体に障害が発生する可能性があります。その結果、vSAN により、障害が発生したディスク グループのすべてのコンポーネントがクラスタ内の別の場所から再構築されます。

各ディスク グループの容量を少なくして、複数のディスク グループを使用した場合、次のメリットおよびデメリットがあります。

- メリット
  - データストアのキャッシュがさらに集約され I/O 操作が高速になるため、パフォーマンスが向上します。
  - 障害のリスクが複数のディスク グループに分散されます。
  - 1 個のディスク グループに障害が発生した場合に、vSAN が再構築するコンポーネントの数が少なくなるため、パフォーマンスが向上します。
- デメリット
  - 2 つ以上のキャッシュ デバイスが必要であるため、コストが高くなります。
  - 複数のディスク グループを処理するために、より多くのメモリが必要になります。
  - 単一障害点のリスクを軽減するために、複数のストレージ コントローラが必要になります。

ドライブ ベイ

メンテナンスを簡単にするには、ドライブ ベイと PCIe スロットがサーバ本体の前面にあるホストを検討してください。

デバイスのホット プラグとスワップ

ホット プラグ操作、または磁気ディスクとフラッシュ キャパシティ デバイスの置換をホストで簡単に行うには、ストレージ コントローラのパススルー モードのサポートを検討してください。 コントローラが RAID 0 モードで動作する場合は、追加の手順を実行してからでないとホストで新しいドライブを検出できません。

vSAN クラスタの設計に関する考慮事項

高い可用性を確保し、使用量の増大に対処できるように、ホストおよび管理ノード構成を設計します。

障害の許容に対応する vSAN クラスタのサイジング

仮想マシン ストレージ ポリシーで [許容されるプライマリ レベルの障害数] (PFTT) 属性を設定し、ホストの障害を処理します。クラスタに必要なホスト数は次のように計算されます： `2 * PFTT + 1`。 クラスタが許容する障害の数が多いほど、容量の大きいホストが必要になります。

クラスタのホストがラック サーバに接続されている場合は、ホストをフォールト ドメインに編成し、トップオブラックのスイッチの障害やサーバ ラック電源の損失などの問題に対して回復性を向上することができます。 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。

2 ホスト構成または 3 ホスト構成のクラスタの制限

3 台のホストで構成されるクラスタでは、許容する障害の数を 1 に設定することにより、ホスト障害を 1 つのみ許容することができます。vSAN は、仮想マシン データの 2 つのレプリカをそれぞれ異なるホストに保存します。監視オブジェクトは、3 つ目のホストに配置します。 クラスタのホスト数が少ないため、次の制限があります。

- 1 台のホストに障害が発生した場合、vSAN は、新たな障害に備えるために別のホストにデータを再構築することができません。
- ホストをメンテナンス モードに切り替える必要がある場合、vSAN はホストからデータを退避させてポリシーのコンプライアンスを維持することはできません。ホストがメンテナンス モードの場合、障害がさらに発生すると、データは潜在的な障害またはアクセス不可に対して無防備になります。

  [データのアクセシビリティの確保] のデータ退避オプションのみを使用できます。[データ アクセシビリティの確保] は、データの移行中でもオブジェクトが使用できるようにします。ただし、別の障害が発生した場合には、オブジェクトにリスクが発生する可能性があります。2 ホスト構成または 3 ホスト構成のクラスタの vSAN オブジェクトは、ポリシーに準拠しません。ホストがメンテナンス モードの場合は、オブジェクトが再構築され、ポリシーのコンプライアンスが確保されます。

  アクセスできないホストまたはディスク グループが 2 ホスト構成または 3 ホスト構成のクラスタに含まれていると、別の障害が発生した場合に vSAN オブジェクトがアクセス不能になるリスクがあります。

負荷分散と非負荷分散のクラスタ構成

vSAN は、ホストが同じ構成に統一されている環境で最適に機能します。

vSAN クラスタで構成が異なるホストを使用すると、次のようなデメリットがあります。

- vSAN は各ホストに同数のコンポーネントを格納できないため、ストレージ パフォーマンスの予測性が低下します。
- 各ホストのメンテナンス方法が異なります。
- キャッシュ デバイスの数が少ないか、タイプが異なる場合、クラスタ内のホストのパフォーマンスが低下します。

vSAN への vCenter Server のデプロイ

vCenter Server が使用できない場合でも、vSAN は正常に動作を続け、仮想マシンは継続して稼動します。

vCenter Server が vSAN データストアにデプロイされていて、vSAN クラスタに問題が発生した場合は、Web ブラウザを使用して各 ESXi ホストにアクセスし、vSphere Host Client 経由で vSAN を監視することができます。vSAN の健全性情報は、Host Client で、または esxcli コマンドを使用して表示できます。

注： vCenter Server を vSAN データストアに展開する場合は、vCenter vmdk のストレージ ポリシーをシック プロビジョニングに設定します。詳細については、『VMware vSAN の管理』の「vSAN ポリシーについて」を参照してください。

vSAN ネットワークの設計

可用性、セキュリティ、バンド幅の確保を vSAN クラスタで提供できるネットワーク機能を検討します。

vSAN ネットワークの構成の詳細については、『VMware vSAN 設計とサイジング ガイド』および『 vSAN ネットワーク設計ガイド』を参照してください。

ネットワークのフェイルオーバーと負荷分散

vSAN では、ネットワークの冗長性専用にバッキング仮想スイッチで構成されたチーミングおよびフェイルオーバー ポリシーが使用されます。vSAN では、ロード バランシングに NIC チーミングは使用されません。

可用性のために NIC チームを構成する場合は、次のフェイルオーバー構成を検討してください。

チーミング アルゴリズム	チームのアダプタのフェイルオーバー構成
発信元の仮想ポートに基づいたルート	アクティブ-パッシブ
IP ハッシュに基づいたルート	標準スイッチの固定 EtherChannel および Distributed Switch の LACP ポート チャネルでアクティブ-アクティブ
物理ネットワークのアダプタ負荷に基づいたルート	アクティブ-アクティブ

vSAN は、IP ハッシュに基づくロード バランシングをサポートしていますが、すべての設定についてパフォーマンスが向上されるわけではありません。vSAN が多くの受信者に使用されている場合は、IP ハッシュのメリットがあります。この場合、IP ハッシュが負荷分散を行います。vSAN が唯一の使用者である場合は、改善が見られない可能性があります。この動作は特に 1 GbE 環境に適用されます。たとえば、vSAN について 4 つの 1 GbE 物理アダプタと IP ハッシュを使用している場合、1 Gbps を超えて使用することはできない可能性があります。この動作は、VMware でサポートされるすべての NIC チーミング ポリシーにも適用されます。

vSAN では、同じサブネット上の複数の VMkernel アダプタはサポートされません。複数の VMkernel アダプタを、別の VLAN または別の物理ファブリックなどの異なるサブネットで使用できます。複数の VMkernel アダプタを使用して可用性を提供するには、vSphere やネットワーク インフラストラクチャを含む構成コストがかかります。 物理ネットワーク アダプタをチーミングすると、ネットワークの可用性を高めることができます。

vSAN ネットワークでのユニキャストの使用

vSAN 6.6 以降のリリースでは、vSAN クラスタをサポートする物理スイッチでマルチキャストは必要ありません。vSAN 用にシンプルなユニキャスト ネットワークを設計できます。以前のリリースの vSAN では、ハートビートを有効にし、クラスタ内のホスト間でメタデータをやり取りするには、マルチキャストが必要です。vSAN クラスタにそれ以前のバージョンのソフトウェアを実行しているホストがある場合は、マルチキャスト ネットワークが必要です。vSAN クラスタでマルチキャストを使用する方法の詳細については、旧バージョンの『VMware vSAN の管理』を参照してください。

注： vSAN 6.6 クラスタでデプロイされた vCenter Server では、予約機能のない DHCP から取得された IP アドレスを使用する構成はサポートされていません。予約機能付きの DHCP を使用する理由は、割り当てられた IP アドレスが VMkernel ポートの MAC アドレスにバインドされるためです。

Network I/O Control を使用した vSAN のバンド幅の割り当て

vSAN トラフィックは、vSphere vMotion トラフィック、vSphere HA トラフィック、および仮想マシン トラフィックなどの他のシステムのトラフィック タイプと、10 GbE 物理ネットワーク アダプタを共有できます。vSAN に必要なバンド幅を確保するには、vSphere Distributed Switch で vSphere Network I/O Control を使用します。

vSphere Network I/O Control では、vSAN 送信トラフィックの予約とシェアを構成できます。

- vSAN の物理アダプタで使用できる最低のバンド幅が Network I/O Control で確保されるように予約を設定します。
- vSAN に割り当てられた物理アダプタが飽和したときに特定のバンド幅を vSAN で使用できるようにシェアを設定して、再構築操作および同期操作の実行中に物理アダプタの容量全体が vSAN で使用されるのを回避します。たとえば、チームの別の物理アダプタに障害が発生し、ポート グループのすべてのトラフィックがチーム内の別のアダプタに転送されると、物理アダプタが飽和状態になる可能性があります。

たとえば、vSAN、vSphere vMotion、および仮想マシンのトラフィックを処理する 10 GbE の物理アダプタで、特定のバンド幅とシェアを構成できます。

表 3-3. vSAN を処理する物理アダプタの Network I/O Control の構成例

トラフィック タイプ	予約、Gbps	シェア
vSAN	1	100
vSphere vMotion	0.5	70
仮想マシン	0.5	30

10 GbE アダプタが飽和状態になると、Network I/O Control により物理アダプタの vSAN に 5 Gbps が割り当てられます。

vSphere Network I/O Control を使用して vSAN トラフィックのバンド幅の割り当てを構成する詳細については、『vSphere のネットワーク』ドキュメントを参照してください。

vSAN トラフィックのマーク

優先順位のタグ付けは、vSAN トラフィックの Quality of Service (QoS) の要求が高い接続済みネットワーク デバイスを示すためのメカニズムです。vSAN トラフィックを特定のクラスに割り当てて、0（優先順位が低い）～7（優先順位が高い）の Class of Service (CoS) 値をトラフィックに適切にマークにすることができます。vSphere Distributed Switch のトラフィック フィルタリングおよびマーキング ポリシーを使用して、優先順位レベルを設定します。

VLAN における vSAN トラフィックのセグメント化

セキュリティおよびパフォーマンスを強化するため、特に複数のトラフィック タイプ間でバッキング物理アダプタの容量を共有している場合は、VLAN で vSAN トラフィックを隔離することを検討します。

ジャンボ フレーム

CPU パフォーマンスを向上するために vSAN でジャンボ フレームを使用する場合は、クラスタ内のすべてのネットワーク デバイスとホストでジャンボ フレームが有効であることを確認します。

デフォルトでは、TCP セグメンテーション オフロード (TSO) および Large Receive Offload (LRO) 機能は、ESXi で有効になっています。 ジャンボ フレームを使用することにより、ネットワーク上のすべてのノードでジャンボ フレームを有効にするコストに見合うだけのパフォーマンス向上が可能かどうかを検討します。

vSAN ネットワークのスタティック ルートの作成

vSAN 環境にスタティック ルートの作成が必要になる場合があります。

vSphere が単一のデフォルト ゲートウェイを使用する従来の構成では、すべてのルーティング トラフィックがこのゲートウェイを通じて送信されます。

ただし、特定の vSAN 環境では、スタティック ルートが必要な場合があります。たとえば、別のネットワーク上に監視ホストを配置している環境や、データ サイトと監視ホストの両方を別々のサイトに配置するストレッチ クラスタ環境などです。

ESXi ホストでスタティック ルートを設定するには、esxcli コマンドを使用します。

`esxcli network ip route ipv4 add -g gateway-to-use -n remote-network`

remote-network は、ホストがアクセスするリモート ネットワークで、*gateway-to-use* は、リモート ネットワークへのトラフィックの送信に使用するインターフェイスです。

ストレッチ クラスタのネットワーク設計の詳細については、「VMware vSAN の管理」を参照してください。

vSAN ネットワークのベスト プラクティス

パフォーマンスおよびスループットの向上のために、vSAN のネットワークのベスト プラクティスを検討してください。

- ハイブリッド構成の場合は、少なくとも 1 GbE の物理ネットワーク アダプタを専用にします。ネットワークのパフォーマンスを最適にするには、10 GbE の専用または共有物理アダプタに vSAN トラフィックを配置します。
- オールフラッシュ構成の場合は、10 GbE の専用または共有物理ネットワーク アダプタを使用します。
- フェイルオーバー NIC として 1 つの追加物理 NIC をプロビジョニングします。
- 10 GbE の共有ネットワーク アダプタを使用する場合は、vSAN トラフィックを Distributed Switch に配置し、vSAN へのバンド幅が確保されるように Network I/O Control を構成します。

vSAN フォルト ドメインの設計とサイジング

vSAN フォルト ドメイン機能では、vSAN に対して、別個のコンピューティング ラックに収容されている各サーバに冗長コンポーネントを分散するよう指示します。この方法により、電源や接続が失われるなどのラックレベルの障害から使用環境を保護することができます。

フォルト ドメインの構成

vSAN では、PFTT=1 をサポートするため、少なくとも 3 つのフォルト ドメインが必要です。各フォルト ドメインは 1 台以上のホストで構成されます。フォルト ドメインの定義では、潜在的な障害ゾーン（たとえば、個々のコンピューティング ラック エンクロージャ）を表す物理ハードウェア構成について確認する必要があります。

可能であれば、少なくとも 4 つのフォルト ドメインを使用してください。3 つのフォルト ドメインは特定のデータ退避モードをサポートせず、vSAN は障害発生後にデータを再保護できません。この場合、再構築が可能な追加のフォルト ドメインが必要です。これは、3 つのフォルト ドメインだけでは提供できません。

フォルト ドメインが有効にされると、vSAN は、個々のホストではなくフォルト ドメインにアクティブな仮想マシン ストレージ ポリシーを適用します。

仮想マシンに割り当てるストレージ ポリシーの [許容されるプライマリ レベルの障害数] (PFTT) 属性に基づいて、クラスタ内のフォルト ドメインの数を計算します。

```
number of fault domains = 2 * PFTT + 1
```

ホストがフォルト ドメインのメンバーではない場合、vSAN はそのホストをスタンドアローンのフォルト ドメインと解釈します。

数台のホストの障害に対するフォルト ドメインの使用

それぞれ 2 台のホストが収容された 4 台のサーバ ラックで構成されるクラスタについて考慮します。[許容されるプライマリ レベルの障害数] が 1 に設定されていて、フォルト ドメインが有効になっていない場合、vSAN は、1 つのオブジェクトの両方のレプリカを同じラック エンクロージャに収容されているホストと一緒に保存することがあります。このためアプリケーションには、ラックレベルの障害が発生したときにデータが損失する潜在的な危険性があります。潜在的に障害が発生する可能性があるホストを別個のフォルト ドメインで一緒に構成する場合、vSAN では、各保護コンポーネント（レプリカおよび監視）が確実に別のフォルト ドメインに配置されるようにします。

ホストおよび容量を追加する場合は、既存のフォルト ドメイン構成を使用するか、またはフォルト ドメインを定義することができます。

フォルト ドメインを使用したときにストレージの負荷を分散し、Fault Tolerance を有効にする場合は、次のガイドラインを考慮します。

- ストレージ ポリシーで構成されている [許容されるプライマリ レベルの障害数] を満たす十分なフォルト ドメインを設定します。

  少なくとも 3 つのフォルト ドメインを定義します。 確実に保護するには、少なくとも 4 つのドメインを定義します。
- 各フォルト ドメインに同じ数のホストを割り当てます。
- 統一された構成のホストを使用します。
- 可能であれば、空き容量のある 1 つのフォルト ドメインを障害後のデータ再構築で専用に使用します。

起動デバイスと vSAN の使用

vSAN クラスタの一部である ESXi のインストールをフラッシュ デバイスから開始する場合、特定の制限が適用されます。

USB/SD デバイスから vSAN ホストを起動する際には、4 GB 以上の高品質の USB または SD フラッシュ ドライブを使用する必要があります。

SATADOM デバイスから vSAN ホストを起動する場合は、シングル レベル セル (SLC) デバイスを使用する必要があります。起動デバイスのサイズは少なくとも 16 GB にする必要があります。

インストール中に、ESXi インストーラによって起動デバイスにコアダンプ パーティションが作成されます。コア ダンプ パーティションのデフォルトのサイズは、大半のインストール要件を満たしています。

- ESXi ホストのメモリが 512 GB 以下である場合は、USB、SD、または SATADOM デバイスからホストを起動できます。
- ESXi ホストのメモリが 512 GB を超える場合は、次のガイドラインを検討します。
  - 16 GB 以上のサイズの SATADOM またはディスク デバイスからホストを起動することができます。SATADOM デバイスを使用する場合は、シングル レベル セル (SLC) デバイスを使用します。
  - vSAN 6.5 以降を使用している場合、USB/SD デバイスから起動するには、ESXi ホストのコアダンプ パーティションのサイズを変更する必要があります。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。

ディスクから起動するホストには、ローカル VMFS があります。仮想マシンを実行している VMFS を含むディスクがある場合は、vSAN 用でない ESXi 起動用のディスクを分離する必要があります。この場合は、コントローラも分離する必要があります。

vSAN のログ情報と起動デバイス

USB または SD デバイスから ESXi を起動すると、ホストの再起動時にログ情報やスタック トレースが失われます。これは、スクラッチ パーティションが RAM ドライブ上に存在するためです。ログ、スタック トレース、メモリ ダンプには、恒久的ストレージを使用します。

ログ情報は、vSAN データストアには保存しないでください。vSAN クラスタで障害が発生した場合に、ログ情報にアクセスできなくなる可能性があるため、この構成はサポートされていません。

恒久的なログ ストレージに関して、次のオプションを検討します。

- vSAN に使用されておらず、VMFS または NFS でフォーマットされたストレージ デバイスを使用します。
- メモリ ダンプとシステム ログを vCenter Server に送信するように、ホストで ESXi Dump Collector と vSphere Syslog Collector を構成します。

恒久的な場所を使用するスクラッチ パーティションの設定の詳細については、『vCenter Server のインストールとセットアップ』ドキュメントを参照してください。

vSAN クラスタでの永続的なログ記録

vSAN クラスタ内のホストからのログを保持するストレージを提供します。

USB または SD デバイスに ESXi をインストールし、ローカル ストレージを vSAN に割り当てると、永続的なログ記録に十分なローカル ストレージまたはデータストア容量が残らなくなる可能性があります。

ログ情報が失われることを避けるには、ESXi Dump Collector と vSphere Syslog Collector を構成して ESXi メモリ ダンプとシステム ログをネットワーク サーバにリダイレクトします。

vSphere Syslog Collector の構成の詳細については、http://kb.vmware.com/kb/2021652 を参照してください。

ESXi Dump Collector の構成の詳細については、https://kb.vmware.com/s/article/2002954 を参照してください。

vSAN の新規または既存クラスタの準備

4

クラスタで vSAN を有効にして仮想マシン ストレージとしての使用を開始する前に、vSAN が正しく動作するために必要なインフラストラクチャを提供します。

この章には、次のトピックが含まれています。

ストレージ デバイスの選択または互換性の確認

vSAN をデプロイする前の重要な手順は、『VMware 互換性ガイド』を参照して、ストレージ デバイス、ドライバ、およびファームウェアが vSAN と互換性があることを確認することです。

vSAN と互換性があるいくつかのオプションの中から選択できます。

- OEM ベンダーと VMware が vSAN との互換性について有効性を確認している物理サーバである、vSAN ReadyNode サーバを使用します。

- 検証済みのデバイス モデルの中から個々のコンポーネントを選択して、ノードを構築します。

VMware 互換性ガイド セクション	確認するコンポーネント タイプ
システム	ESXi を実行する物理サーバ。
vSAN	■ ハイブリッド構成の磁気ディスク SAS モデル。 ■ 『VMware 互換性ガイド』でのリストに含まれているフラッシュ デバイス モデル。PCIe フラッシュ デバイスのモデルによっては、vSAN と一緒に使用できるものもあります。書き込みの耐久性とパフォーマンス クラスも考慮してください。 ■ パススルーをサポートするストレージ コントローラ モデル。 vSAN は、各ストレージ デバイスが個々の RAID 0 グループとして表されている場合、RAID 0 モードに対応するように構成されているストレージ コントローラと連係動作することができます。

ストレージの準備

vSAN および vSAN データストアを使用する仮想ワークロードに対して十分なディスク容量を用意します。

ストレージ デバイスの準備

vSAN の要件に基づいて、フラッシュ デバイスおよび磁気ディスクを使用します。

予測される仮想マシンの使用に対応できるだけの十分な容量がクラスタにあることと、仮想マシンのストレージ ポリシーで定義された [許容されるプライマリ レベルの障害数] を確認します。

vSAN でストレージ デバイスを要求できるようにするため、ストレージ デバイスが次の要件を満たしている必要があります。

- ストレージ デバイスが ESXi ホストに対してローカルであること。vSAN ではリモート デバイスを要求できません。
- ストレージ デバイスに既存のパーティション情報が保存されていないこと。
- オールフラッシュとハイブリッドの両方のディスク グループを同じホストで使用していないこと。

ディスク グループのデバイスの準備

各ディスク グループには、1 つのフラッシュ キャッシュ デバイスと、1 つ以上の磁気ディスクまたは 1 つのフラッシュ キャパシティ デバイスがあります。ハイブリッド クラスタの場合、フラッシュ キャッシュ デバイスの容量は、キャパシティ デバイスでの予想ストレージ使用量の 10% 以上にする必要があります（保護コピーの容量を除く）。

vSAN では、3 台以上のホストで構成されるクラスタに対してストレージを提供するホストに、少なくとも 1 つのディスク グループが必要です。vSAN のパフォーマンスを最適にするには、統一された構成のホストを使用します。

Raw および使用可能な容量

特定の状況に対応するため、仮想マシンの容量を超える Raw ストレージ容量を用意します。

- 容量にはフラッシュ キャッシュ デバイスのサイズを含めないでください。ストレージのフラッシュ デバイスを追加しない限り、フラッシュ キャッシュ デバイスはストレージを提供せず、キャッシュとして使用されます。

- 仮想マシンのストレージ ポリシーで定義された [許容されるプライマリ レベルの障害数] (PFTT) の値に対応できる、十分な容量を用意します。PFTT が 0 より大きい場合は、デバイスの占有量が拡張されます。PFTT を 1 に設定すると、占有量が 2 倍になります。PFTT を 2 に設定すると、占有量が 3 倍になり、以下同様です。
- 統合された vSAN データストア オブジェクトではなく、個々のホストの容量を調べて、操作に十分な容量が vSAN データストアにあるかどうかを確認します。たとえば、ホストを退避させる場合、退避させるホストにデータストアのすべての空き容量があるために、別のホストへの退避をクラスタで処理できないことがあります。
- シン プロビジョニングされたワークロードで大量のストレージの消費を開始する場合は、データストアで容量不足になるのを回避できるだけの十分な容量を用意します。
- 物理ストレージで vSAN クラスタのホストの再保護モードとメンテナンス モードに対応できることを確認します。
- 使用可能なストレージ容量に対する vSAN のオーバーヘッドを検討します。
  - 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 の追加のオーバーヘッドがかかります。
  - オンディスク フォーマット バージョン 2.0 では、一般的にデバイスあたり 1 ～ 2% 未満の容量の追加のオーバーヘッドがかかります。
  - オンディスク フォーマット バージョン 3.0 以降では、一般的にデバイスあたり 1 ～ 2% 未満の容量の追加のオーバーヘッドがかかります。ソフトウェア チェックサムが有効な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。

vSAN データストアの容量の計画の詳細については、VMware vSAN 設計とサイジング ガイドを参照してください。

vSAN ポリシーのキャパシティ デバイスに与える影響

仮想マシンの vSAN ストレージ ポリシーは、さまざまな方法でキャパシティ デバイスに影響します。

表 4-1. vSAN の仮想マシン ポリシーと Raw 容量

ポリシーが影響する点	説明
ポリシーの変更	■ [許容されるプライマリ レベルの障害数] (PFTT) は、仮想マシンに提供する必要がある物理ストレージ容量に影響します。使用される PFTT の値が大きいほど可用性が高くなり、より多くの容量を用意する必要があります。 PFTT を 1 に設定すると、仮想マシンの VMDK ファイルのレプリカが 2 個作成されます。PFTT を 1 に設定すると、50 GB の VMDK ファイルが 1 個ある場合、異なるホストに 100 GB の容量が必要になります。PFTT が 2 に変更されると、クラスタ内のホスト全体で VMDK の 3 個のレプリカをサポートできる容量 (150 GB) が必要になります。 ■ オブジェクトあたりの新しいディスク ストライプ数など、一部のポリシー変更には一時リソースが必要です。vSAN では、変更によって影響を受けるオブジェクトを再作成します。一定の期間、物理ストレージで古いオブジェクトと新しいオブジェクトの両方に対応する必要があります。
再保護モードまたはメンテナンス モードの使用可能な容量	ホストをメンテナンス モードにするか、仮想マシンのクローンを作成する場合、vSAN データストアで十分な容量が利用可能であることが示されていても、データストアが仮想マシン オブジェクトを退避できないことがあります。空き容量がメンテナンス モードに設定されているホストにある場合、この容量不足が発生します。

ESXCLI でフラッシュ デバイスをキャパシティ デバイスとしてマーク

esxcli を使用して手動で各ホスト上のフラッシュ デバイスをキャパシティ デバイスとしてマークできます。

前提条件

vSAN 6.5 以降を使用していることを確認します。

手順

1 キャパシティ デバイスとしてマークするフラッシュ デバイスの名前を確認するには、各ホストで次のコマンドを実行します。

a ESXi Shell で、`esxcli storage core device list` コマンドを実行します。

b コマンド出力の上部でデバイス名を探し、その名前を書き留めます。

このコマンドには次のオプションがあります。

表 4-2. コマンド オプション

オプション	説明
`-d|--disk=str`	キャパシティ デバイスとしてタグ付けするデバイスの名前。 たとえば、`mpx.vmhba1:C0:T4:L0`。
`-t|--tag=str`	追加または削除するタグを指定します。 たとえば、`capacityFlash` タグは、フラッシュ デバイスをキャパシティ デバイスとしてマークするために使用します。

このコマンドでは、ESXi で識別されるすべてのデバイス情報が一覧表示されます。

2 出力で、デバイスの `Is SSD` 属性が `true` であることを確認します。

3 フラッシュ デバイスをキャパシティ デバイスとしてタグ付けするには、esxcli vsan storage tag add -d <device name> -t capacityFlash コマンドを実行します。

たとえば、esxcli vsan storage tag add -t capacityFlash -d mpx.vmhba1:C0:T4:L0 コマンドを使用することができます。ここで、mpx.vmhba1:C0:T4:L0 はデバイス名です。

4 フラッシュ デバイスがキャパシティ デバイスとしてマークされているかどうかを確認します。

a 出力で、デバイスの IsCapacityFlash 属性が 1 に設定されていることを確認します。

例： コマンド出力

vdq -q -d <device name> コマンドを実行して、IsCapacityFlash 属性を確認できます。 たとえば、vdq -q -d mpx.vmhba1:C0:T4:L0 コマンドでは、次の出力が返されます。

```
\{
"Name"     : "mpx.vmhba1:C0:T4:L0",
"VSANUUID" : "",
"State"    : "Eligible for use by VSAN",
"ChecksumSupport": "0",
"Reason"   : "None",
"IsSSD"    : "1",
"IsCapacityFlash": "1",
"IsPDL"    : "0",
    \},
```

ESXCLI を使用した、キャパシティ デバイスとして使用されるフラッシュ デバイスのタグの解除

キャパシティ デバイスとして使用されるフラッシュ デバイスのタグを解除し、キャッシュとして使用可能にすることができます。

手順

1 キャパシティ デバイスとしてマークされているフラッシュ デバイスのタグを解除するには、esxcli vsan storage tag remove -d <device name> -t capacityFlash コマンドを実行します。たとえば、esxcli vsan storage tag remove -t capacityFlash -d mpx.vmhba1:C0:T4:L0 コマンドを使用することができます。ここで、mpx.vmhba1:C0:T4:L0 はデバイス名です。

2 フラッシュ デバイスのタグが解除されたかどうかを確認します。

a 出力で、デバイスの IsCapacityFlash 属性が 0 に設定されていることを確認します。

例： コマンド出力

vdq -q -d <device name> コマンドを実行して、IsCapacityFlash 属性を確認できます。たとえば、vdq -q -d mpx.vmhba1:C0:T4:L0 コマンドでは、次の出力が返されます。

```
[
    \{
"Name"     : "mpx.vmhba1:C0:T4:L0",
"VSANUUID" : "",
```

```
"State"    : "Eligible for use by VSAN",
"ChecksumSupport": "0",
"Reason"   : "None",
"IsSSD"    : "1",
"IsCapacityFlash": "0",
"IsPDL"    : "0",
    \},
```

RVC を使用してフラッシュ デバイスをキャパシティ デバイスとしてマーク

`vsan.host_claim_disks_differently` RVC コマンドを実行して、ストレージ デバイスをフラッシュ、キャパシティ フラッシュ、または磁気ディスク (HDD) としてマークします。

RVC ツールを使用すると、フラッシュ デバイスをキャパシティ デバイスとしてタグ付けできます。このタグ付けは、個別に行うことも、デバイスのモデルを指定してバッチで行うこともできます。 フラッシュ デバイスにキャパシティ デバイスのタグを付ける場合、フラッシュ デバイスをオールフラッシュ ディスク グループに含めることができます。

注： `vsan.host_claim_disks_differently` コマンドでは、タグ付けの前にデバイス タイプは確認されません。このコマンドでは、使用中の磁気ディスクおよびデバイスを含め、`capacity_flash` コマンド オプションを使用して付加されたデバイスにタグが付けられます。タグ付けの前に、デバイスのステータスを必ず確認してください。

vSAN 管理のための 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。

前提条件

- vSAN バージョン 6.5 以降を使用していることを確認します。
- SSH が vCenter Server Appliance で有効であることを確認します。

手順

1. vCenter Server Appliance への SSH 接続を開きます。
2. 管理者権限を持つローカル アカウントを使用して、アプライアンスにログインします。
3. 次のコマンドを実行して、RVC を開始します。

   ```
   rvc local_user_name@target_vCenter_Server
   ```

   たとえば、同じ vCenter Server Appliance を使用してキャパシティ デバイスのフラッシュ デバイスを root ユーザーとしてマークするには、次のコマンドを実行します。

   ```
   rvc root@localhost
   ```

4. ユーザー名と対応するパスワードを入力します。
5. vSphere インフラストラクチャで、*vcenter_server*/*data_center*/computers/*cluster*/hosts ディレクトリに移動します。

6 `--claim-type capacity_flash --model` *model_ name* オプションを指定して `vsan.host_claim_disks_differently` コマンドを実行し、同じモデルのオールフラッシュ デバイスをクラスタ内のすべてのホストのキャパシティ デバイスとしてマークします。

```
vsan.host_claim_disks_differently --claim-type capacity_flash --model model_name *
```

次のステップ

クラスタで vSAN を有効にし、キャパシティ デバイスを要求します。

vSAN へのメモリの提供

vSAN にマッピングするデバイスおよびディスク グループの最大数に合わせて、ホストにメモリをプロビジョニングする必要があります。

デバイスおよびディスク グループの最大数の要件を満たすには、ホストのシステム操作に 32 GB のメモリをプロビジョニングする必要があります。最大デバイス構成の詳細については、『vSphere 構成の上限』ドキュメントを参照してください。

vSAN のホストの準備

vSAN を有効にする準備作業の一環として、クラスタのホストの構成に関する要件および推奨事項を確認します。

- ホストのストレージ デバイスと、そのドライバおよびファームウェアのバージョンが、『VMware 互換性ガイド』の「vSAN」セクションに記載されていることを確認します。
- vSAN データストアのストレージが少なくとも 3 台のホストで構成されていることを確認します。
- メンテナンスおよび障害時の修正用に、少なくとも 4 台のホストをクラスタに追加します。
- クラスタ内でストレージの負荷分散を最適にするため、同一構成のホストを指定します。
- ストレージを提供するホストに、ストレージ コンポーネントが集中することを回避するため、コンピューティング リソースのみを持つホストはクラスタに追加しないでください。コンピューティング専用ホストで実行される仮想マシンで大量のストレージ容量が必要な場合、キャパシティを提供する個々のホストに大量のコンポーネントが保存されることがあります。その結果、クラスタのストレージ パフォーマンスが低下する可能性があります。
- ホスト上で、積極的に電力を節約する CPU 電源管理ポリシーを構成しないでください。CPU 速度遅延に敏感な特定のアプリケーションでは、パフォーマンスが低下する可能性があります。CPU 電源管理ポリシーの詳細については、『vSphere のリソース管理』を参照してください。
- クラスタにブレード サーバが含まれる場合、ブレード サーバに接続されている外部ストレージ エンクロージャでデータストアの容量を拡張することを検討してください。ストレージ エンクロージャが VMware 互換性ガイド の vSAN に関するセクションに記載されていることを確認してください。
- ハイブリッド ディスク構成またはオールフラッシュ ディスク構成に配置するワークロードの構成を検討します。
  - 高レベルの予測可能なパフォーマンスを得るには、オールフラッシュ ディスク グループのクラスタを準備します。

- パフォーマンスとコストのバランスを取るには、ハイブリッド ディスク グループのクラスタを準備します。

vSAN と vCenter Server の互換性

vCenter Server と ESXi における vSAN サポートの違いが原因で障害が発生することを避けるには、vCenter Server と ESXi のバージョンを同期します。

vCenter Server と ESXi の vSAN コンポーネント間を最適に統合するには、2 つの最新バージョンの vSphere コンポーネントをデプロイします。『vCenter Server のインストールとセットアップ』および『vSphere のアップグレード』ドキュメントを参照してください。

ストレージ コントローラの準備

vSAN の要件に合わせて、ホストのストレージ コントローラを構成します。

vSAN のホストにあるストレージ コントローラが、モード、ドライバ、ファームウェア バージョン、キュー深度、キャッシュ、および高度な機能の特定の要件を満たしていることを確認します。

表 4-3. vSAN のストレージ コントローラ構成の確認

ストレージ コントローラの機能	ストレージ コントローラの要件
必須モード	■ 『VMware 互換性ガイド』で、コントローラが必須モード、パススルー、または RAID 0 の場合の vSAN の要件を確認します。 ■ パススルーと RAID 0 の両方のモードがサポートされている場合は、RAID 0 ではなくパススルー モードを構成します。RAID 0 にすると、ディスクの置換が複雑になります。
RAID モード	■ RAID 0 の場合は、物理ディスク デバイスごとに RAID ボリュームを 1 つ作成します。 ■ 『VMware 互換性ガイド』の一覧にあるモード以外の RAID モードは有効にしないでください。 ■ コントローラのスパニングを有効にしないでください。
ドライバおよびファームウェアのバージョン	■ コントローラでは、『VMware 互換性ガイド』の説明に従って、最新バージョンのドライバおよびファームウェアを使用してください。 ■ コントローラの筐体内ドライバを使用する場合は、そのドライバが vSAN 用に認定されていることを確認してください。 OEM の ESXi リリースには、認定されておらず、『VMware 互換性ガイド』のリストに含まれていないドライバがインストールされている場合があります。
キュー深度	コントローラのキュー深度が 256 以上であることを確認します。キュー深度が深いほどパフォーマンスが向上します。
キャッシュ	ストレージ コントローラのキャッシュを無効にするか、キャッシュを無効にすることができない場合は 100 パーセント読み取りに設定します。
高度な機能	HP SSD Smart Path などの高度な機能を無効にします。

vSAN ネットワークの構成

クラスタおよび ESXi ホストで vSAN を有効にする前に、vSAN 通信を行うために必要なネットワークを構築する必要があります。

vSAN は、クラスタに参加する ESXi ホスト全体でデータを交換する、分散ストレージ ソリューションを提供します。特定の構成項目を含む、vSAN をインストールするためのネットワークを準備します。

ネットワーク設計ガイドラインの詳細については、 vSAN ネットワークの設計を参照してください。

同じサブネット内へのホストの配置

最適なネットワーク パフォーマンスを得るには、ホストを同じサブネットに接続する必要があります。 vSAN 6.0 以降では、必要に応じてホストを同じレイヤー 3 ネットワークに接続することもできます。

物理アダプタのネットワーク バンド幅の専用化

少なくとも 1 Gbps のバンド幅を vSAN に割り当てます。次のいずれかの構成オプションを使用できます。

- 1-GbE 物理アダプタをハイブリッド ホスト構成専用にする。
- オールフラッシュ構成で専用または共有 10-GbE 物理アダプタを使用する。
- 可能であればハイブリッド構成で専用または共有 10-GbE 物理アダプタを使用する。
- 他のシステム トラフィックを処理する 10-GbE 物理アダプタで vSAN トラフィックを制御し、Distributed Switch の vSphere Network I/O Control を使用して vSAN のバンド幅を予約する。

仮想スイッチでのポート グループの構成

vSAN の仮想スイッチでポート グループを構成します。

- vSAN の物理アダプタをアクティブなアップリンクとしてポート グループに割り当てます。

  ネットワーク可用性について NIC チームが必要な場合は、スイッチへの物理アダプタの接続に基づいてチーミング アルゴリズムを選択します。
- 設計されている場合は、仮想スイッチでタギングを有効にして vSAN トラフィックを VLAN に割り当てます。

vSAN のホストでのファイアウォールの調査

vSAN は、クラスタ内の各ホストの特定のポートでメッセージを送信します。ホストのファイアウォールがこれらのポートでのトラフィックを許可していることを確認します。

表 4-4. vSAN 内のホスト上のポート

vSAN サービス	トラフィック方向	通信ノード	転送プロトコル	ポート
vSAN ベンダー プロバイダ (vsanvp)	受信および発信	vCenter Server および ESXi	TCP	8080
vSAN クラスタリング サービス		ESXi	UDP	12345、23451

表 4-4. vSAN 内のホスト上のポート （続き）

vSAN サービス	トラフィック方向	通信ノード	転送プロトコル	ポート
vSAN 転送		ESXi	TCP	2233
ユニキャスト エージェント		ESXi	UDP	12321
iSCSI		iSCSI イニシエータおよび ESXi	TCP	3260
vSAN パフォーマンス サービス		ESXi	TCP	80
vSAN Observer	入力	Web ブラウザおよび vCenter Server	TCP	8010

vSAN ライセンスに関する考慮事項

vSAN のクラスタを準備する場合は、vSAN ライセンスの要件を確認します。

- クラスタでホスト構成全体を管理するための有効なライセンスを取得していることを確認します。 そのライセンスは、評価プロセスで使用したライセンスとは異なります。

  vSAN のライセンス有効期間または評価期間が終了しても、vSAN のリソースの現在の構成を引き続き使用できます。ただし、ディスク グループに容量を追加したり、ディスク グループを作成したりすることはできません。
- クラスタがオールフラッシュのディスク グループで構成されている場合は、取得したライセンスでオールフラッシュ機能を使用できるかどうかを確認してください。
- vSAN クラスタがデデュープおよび圧縮やストレッチ クラスタなどの高度な機能を使用する場合は、ライセンスでこれらの機能を使用できるかどうかを確認してください。
- クラスタのホストを追加および削除する場合は、クラスタ全体での vSAN ライセンスの CPU 容量を考慮します。

  vSAN ライセンスには、CPU 容量単位です。vSAN ライセンスをクラスタに割り当てる場合、使用されるライセンス キャパシティの量は、クラスタに参加しているホストの CPU の総数に等しくなります。

  vSAN ライセンスのエディションおよびライセンスのシナリオの詳細については、『VMware vSAN 6.7 ライセンス ガイド』を参照してください。

vSAN クラスタの作成

5

クラスタを作成するときに vSAN を有効にすることも、既存のクラスタで vSAN を有効にすることもできます。

この章には、次のトピックが含まれています。

vSAN クラスタの特性

vSAN 環境で作業する前に、vSAN クラスタの特性を理解することが重要です。

vSAN クラスタの特性には、次のものが含まれます。

- vCenter Server インスタンスごとに複数の vSAN クラスタを使用できます。1 台の vCenter Server を使用して、複数の vSAN クラスタを管理できます。
- vSAN では、フラッシュ キャッシュ デバイスやキャパシティ デバイスを含むすべてのデバイスが使用され、他の機能とデバイスが共有されることはありません。
- vSAN クラスタには、キャパシティ デバイスを持つホストと持たないホストの両方を含めることができます。キャパシティ デバイスを持つホストが少なくとも 3 台必要です。ベスト プラクティスとして、vSAN クラスタ含めるホストは同一構成にします。
- ホストがキャパシティを提供する場合、そのホストには少なくとも 1 つのフラッシュ キャッシュ デバイスと 1 つのキャパシティ デバイスが必要です。

- ハイブリッド クラスタでは、磁気ディスクがキャパシティ デバイスとして使用され、フラッシュ デバイスが読み取り/書き込みキャッシュとして使用されます。vSAN では、使用可能なすべてのキャッシュの 70% が読み取りキャッシュとして使用され、30% が書き込みバッファとして使用されます。ハイブリッド構成では、フラッシュ デバイスは、読み取りキャッシュおよび書き込みバッファとしての役割を果たします。
- オールフラッシュ クラスタでは、指定された 1 つのフラッシュ デバイスが書き込みキャッシュとして使用され、追加のフラッシュ デバイスがキャパシティ デバイスとして使用されます。オールフラッシュ クラスタでは、直接フラッシュ プール キャパシティから読み取りが行われます。
- vSAN クラスタに入れることができるのは、ローカルまたは直接接続されたキャパシティ デバイスのみです。vSAN では、クラスタに接続された SAN や NAS などの他の外部ストレージは使用できません。

クイックスタートを利用して設定した vSAN クラスタの特性の詳細については、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。

vSAN クラスタの設計およびサイジングについては、3 章 vSAN クラスタの設計とサイジングを参照してください。

vSAN クラスタを作成する前に

このトピックでは、vSAN クラスタを作成するためのソフトウェアおよびハードウェア要件のチェックリストを提供します。また、このチェックリストを使用して、クラスタがガイドラインおよび基本的な要件を満たしていることを確認することもできます。

vSAN クラスタの要件

開始する前に、VMware 互換性ガイドの Web サイト (http://www.vmware.com/resources/compatibility/search.php) で、ハードウェア デバイスの特定のモデル、およびドライバとファームウェアの特定のバージョンを確認します。次の表に、vSAN でサポートされている主要なソフトウェアおよびハードウェアの要件を示します。

注意： 保証されていないソフトウェアおよびハードウェア コンポーネント、ドライバ、コントローラ、ファームウェアを使用すると、予期しないデータ損失やパフォーマンスの問題が発生する可能性があります。

表 5-1. vSAN クラスタの要件

要件	説明
ESXi ホスト	■ ホストで最新バージョンの ESXi を使用していることを確認します。 ■ vSAN クラスタに割り当て可能なサポートされているストレージ構成を持つ ESXi ホストが 3 台以上あることを確認します。最適な結果を得るには、4 台以上のホストで vSAN クラスタを構成します。
メモリ	■ 各ホストに 8 GB 以上のメモリがあることを確認します。 ■ 大規模な構成でパフォーマンスを高めるには、クラスタに 32 GB 以上のメモリが必要です。vSAN ホストの設計とサイジングを参照してください。

表 5-1. vSAN クラスタの要件 （続き）

要件	説明
ストレージ I/O コントローラ、ドライバ、ファームウェア	■ ストレージ I/O コントローラ、ドライバ、およびファームウェアのバージョンが 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。 ■ コントローラでパススルーまたは RAID 0 モードが構成されていることを確認します。 ■ コントローラ キャッシュおよび高度な機能が無効になっていることを確認します。キャッシュを無効にできない場合は、読み取りキャッシュを 100 パーセントに設定する必要があります。 ■ キューの深さが高いコントローラを使用していることを確認します。キューの深さが 256 未満のコントローラを使用すると、メンテナンス中や障害の発生時に仮想マシンのパフォーマンスに大きく影響する可能性があります。
キャッシュおよび容量	■ クラスタにストレージを提供する vSAN ホストに少なくとも 1 個のキャッシュ デバイスと 1 個のキャパシティ デバイスがあることを確認します。vSAN では、vSAN クラスタに含まれるホストのローカル キャッシュ デバイスとキャパシティ デバイスに対する排他的アクセスが必要です。これらのデバイスを、Virtual Flash File System (VFFS)、VMFS パーティション、ESXi 起動パーティションなどの他の用途で共有することはできません。 ■ 最適な結果を得るには、統一された構成のホストを持つ vSAN クラスタを作成します。
ネットワーク接続	■ 各ホストに少なくとも 1 つのネットワーク アダプタが構成されていることを確認します。 ■ ハイブリッド構成の場合、vSAN ホストで 1 GbE 以上の専用バンド幅を使用できることを確認します。 ■ オールフラッシュ構成の場合、vSAN ホストで 10 GbE 以上のバンド幅を使用できることを確認します。 vSAN ネットワークのベスト プラクティスと考慮事項については、 vSAN ネットワークの設計 および vSAN のネットワーク要件を参照してください。
vSAN と vCenter Server の互換性	vCenter Server の最新バージョンを使用していることを確認します。
ライセンス キー	■ 有効な vSAN ライセンス キーがあることを確認します。 ■ オールフラッシュ機能を使用するには、この機能をサポートするライセンスが必要です。 ■ ストレッチ クラスタ、あるいは重複排除および圧縮などの高度な機能を使用するには、これらの機能をサポートするライセンスが必要です。 ■ 使用する予定のライセンス数が、vSAN クラスタに参加しているホストの CPU 総数に等しいことを確認してください。クラスタに容量を提供するホストのみに、ライセンス数を設定しないでください。vSAN のライセンスの詳細については、『vCenter Server およびホスト管理』ドキュメントを参照してください。

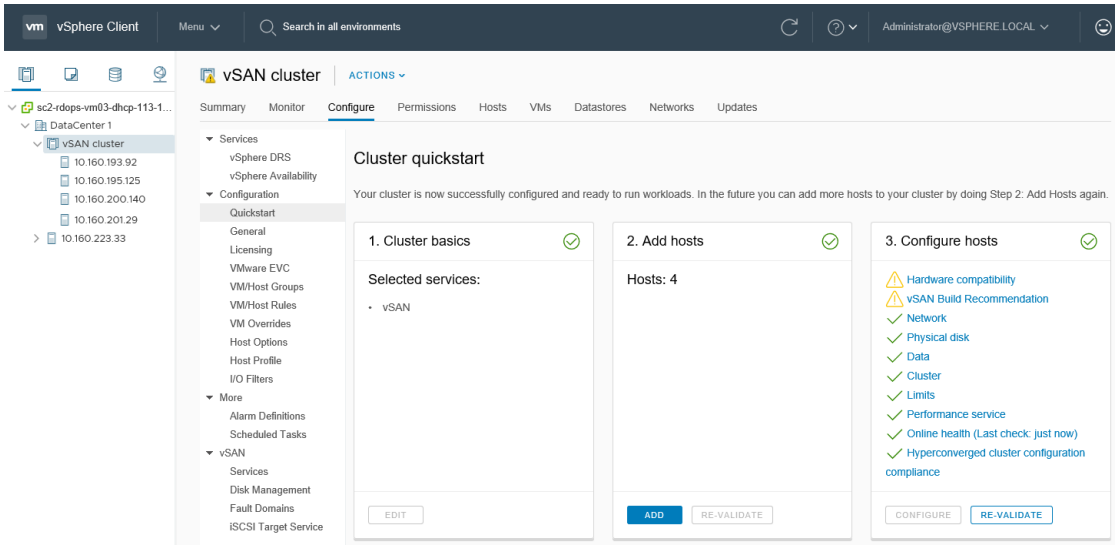
vSAN クラスタ要件の詳細については、2 章 vSAN を有効にするための要件を参照してください。

vSAN クラスタの設計とサイジングの詳細については、『VMware vSAN Design and Sizing Guide』を参照してください。

クイックスタートを使用した vSAN クラスタの構成および拡張

クイックスタート ワークフローを使用すると、vSAN クラスタを迅速に作成、構成、および展開できます。

クイックスタートはワークフローを統合し、ネットワーク、ストレージ、サービスなどの一般的な機能に推奨されるデフォルト設定を使用する新しい vSAN クラスタを迅速に作成することができます。クイックスタートは一般的なタスクをグループ化し、設定ウィザードを使用してプロセスをガイドします。クイックスタートの各ウィザードに必要な情報を入力すると、入力された情報に基づいてクラスタが構成されます。



クイック スタートでは vSAN Health Service を使用して構成を確認し、その結果に基づいて構成の問題を修正することができます。各クイック スタート カードには構成のチェックリストが表示されます。緑のメッセージ、黄色の警告、赤の障害をクリックすると詳細を表示できます。

クイックスタート クラスタに追加されるホストは、クラスタ設定に一致するように自動的に構成されます。新しいホストの ESXi ソフトウェアおよびパッチ レベルは、クラスタ内の ESXi ソフトウェアおよびパッチ レベルに一致する必要があります。クイックスタート ワークフローを使用してホストをクラスタに追加する際は、ホストにネットワークまたは vSAN を構成することはできません。ホストの追加の詳細については、『*VMware vSAN の管理*』の「vSAN クラスタの拡張」を参照してください。

クイックスタート クラスタの特性

クイックスタートを使用して構成された vSAN クラスタには次の特性があります。

- ホストに ESXi 6.0 Update 2 以降が必要です。
- すべてのホストはネットワーク設定を含み同じ構成になります。クイックスタートは、各ホストのネットワーク設定をクラスタ要件に合わせて変更します。
- クラスタ構成は、ネットワークとサービスで推奨されるデフォルトの設定に基づいています。
- クイックスタート ワークフローでは、ライセンスは割り当てられません。ライセンスは手動でクラスタに割り当てる必要があります。

クイックスタート クラスタの管理および拡張

クイックスタート ワークフローが完了したら、vSphere Client またはコマンドライン インターフェイスを使用して、vCenter Server からクラスタを管理できます。

クイックスタート ワークフローを使用して、クラスタにホストを追加し、追加ディスクを要求することができます。ただし、クイックスタートでクラスタを構成した後、クイックスタートを使用してクラスタ構成を変更することはできません。

クイックスタート ワークフローは、HTML5 ベースの vSphere Client を介してのみ使用できます。

クイックスタートのスキップ

[クイックスタートをスキップ] ボタンを使用して、クイックスタート ワークフローを終了し、引き続きクラスタとそのホストを手動で構成できます。新しいホストを個別に追加し、それらのホストを手動で構成することができます。スキップ後にクラスタのクイックスタート ワークフローをリストアすることはできません。

クイックスタート ワークフローは、新しいクラスタ向けに設計されています。既存の vSAN クラスタを 6.7 Update 1 以降にアップグレードする際、クイックスタート ワークフローが表示されます。クイックスタート ワークフローをスキップし、引き続き vCenter Server からクラスタを管理します。

クイックスタートを使用した vSAN クラスタの構成

クイックスタート ワークフローを使用すると、vSAN クラスタを迅速に構成できます。

前提条件

- ホストで ESXi 6.0 Update 2 以降が実行されていることを確認します。
- クラスタ内の ESXi ホストに既存の vSAN またはネットワーク構成がないことを確認します。

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. （オプション）[クラスタの基本] で [編集] をクリックして、クラスタの基本ウィザードを開きます。
   a. クラスタ名を入力します。
   b. DRS、vSphere HA、vSAN などの基本的なサービスを選択します。
   c. [終了] をクリックします。
4. [ホストの追加] で、[追加] 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。

選択したホストがメンテナンス モードになり、クラスタに追加されます。クイックスタート構成が完了したら、ホストはメンテナンス モードを終了します。

注： クラスタ内のホストで vCenter Server を実行している場合、ホストはクイックスタート 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 モードにする必要はありません。vCenter Server 仮想マシンが含まれているホストでは、ESXi 6.5 EP2 以降が実行されている必要があります。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。

5 [クラスタの構成] で、[構成] 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、Distributed Switch、ポート グループ、物理アダプタなどのネットワーク設定を入力します。

- [Distributed Switch] セクションで、ドロップダウン メニューから構成する Distributed Switch の数を入力します。各 Distributed Switch の名前を入力します。[既存の使用] をクリックし、既存の Distributed Switch を選択します。

  選択した物理アダプタが、ホスト全体で同じ名前を持つ標準仮想スイッチに接続されている場合、標準スイッチは Distributed Switch に移行されます。選択した物理アダプタが未使用の場合、標準スイッチから Distributed Switch への移行はありません。

  ネットワーク リソース コントロールを有効にして、バージョン 3 に設定します。Distributed Switch とネットワーク リソース コントロール バージョン 2 は併用できません。

- [ポート グループ] セクションで、vMotion に使用する Distributed Switch と、vSAN ネットワークに使用する Distributed Switch を選択します。

- [物理アダプタ] セクションで、各物理ネットワーク アダプタの Distributed Switch を選択します。各 Distributed Switch は、1 つ以上の物理アダプタに割り当てる必要があります。

  物理 NIC と Distributed Switch のこのマッピングは、クラスタ内のすべてのホストに適用されます。既存の Distributed Switch を使用する場合は、物理アダプタの選択内容が Distributed Switch のマッピングと一致することがあります。

b （オプション）[vMotion トラフィック] 画面で、vMotion トラフィックの IP アドレス情報を入力します。

c [ストレージ トラフィック] 画面で、ストレージ トラフィックの IP アドレス情報を入力します。

d [詳細オプション] ページで、DRS、HA、vSAN、ホスト オプション、EVC などのクラスタ設定情報を入力します。

[ホスト更新の設定] オプションでは、vSphere Update Manager の vSAN ビルドに関する推奨事項を構成します。詳細については、『*VMware vSAN の管理*』の「vSphere Update Manager に向けた vSAN ビルドの推奨事項」を参照してください。

e [ディスクの要求] ページで、キャッシュとキャパシティに使用する各ホスト上のディスクを選択します。

f （オプション）[プロキシ設定] 画面で、vSAN Support Insight データを VMware のカスタマ エクスペリエンス改善プログラム (CEIP) に送信するために使用されるプロキシ サーバを構成します。

g （オプション）[フォールト ドメインの作成] ページで、障害が発生する可能性のあるホストのフォールト ドメインを定義します。

フォールト ドメインの詳細については、『*VMware vSAN の管理*』の「vSAN クラスタのフォールト ドメインの管理」を参照してください。

h [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。

次のステップ

vCenter Server からクラスタを管理することができます。

クイックスタートを使用して、クラスタにホストを追加することができます。詳細については、『*VMware vSAN の管理*』の「vSAN クラスタの拡張」を参照してください。

vSAN の手動による有効化

vSAN クラスタを作成するには、ホスト クラスタを作成し、そのクラスタで vSAN を有効にします。

vSAN クラスタには、容量のあるホストと容量のないホストを含めることができます。vSAN クラスタを作成するときは、次のガイドラインに沿ってください。

- vSAN クラスタには、少なくとも 3 台の ESXi ホストを含める必要があります。vSAN クラスタでホストとデバイスの障害を許容する場合は、vSAN クラスタに参加する少なくとも 3 台のホストがクラスタに容量を提供する必要があります。最適な結果を得るには、4 つ以上のホストを追加してクラスタに容量を提供することを考慮してください。
- ESXi 5.5 Update 1 以降のホストだけが vSAN クラスタに参加できます。
- ホストを vSAN クラスタから別のクラスタに移動する前に、ターゲット クラスタで必ず vSAN を有効にしてください。
- vSAN データストアにアクセスできるようにするには、ESXi ホストは vSAN クラスタのメンバーであることが必要です。

vSAN を有効にすると、vSAN ストレージ プロバイダが自動的に vCenter Server に登録され、vSAN データストアが作成されます。ストレージ プロバイダについては、『vSphere のストレージ』ドキュメントを参照してください。

vSAN の VMkernel ネットワークの設定

vSAN クラスタ内でのデータの交換を有効にするには、各 ESXi ホストに vSAN トラフィック用の VMkernel ネットワーク アダプタを搭載する必要があります。

手順

1 ホストに移動します。

2 [設定] タブをクリックします。

3 [ネットワーク]で [VMkernel アダプタ] を選択します。

4 [ネットワークの追加] アイコン ( ) をクリックして、[ネットワークの追加] ウィザードを開きます。

5 [接続タイプの選択] ページで、[VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。

6 [ターゲット デバイスの選択] ページで、ターゲット スイッチング デバイスを設定します。

7 [ポートのプロパティ] ページで、[vSAN] サービスを選択します。

8 VMkernel アダプタの構成を完了します。

9 [設定内容の確認] ページで、vSAN の VMkernel アダプタのステータスが [有効] であることを確認し、[終了] をクリックします。

結果

ホストで vSAN ネットワークが有効になります。

次のステップ

ホスト クラスタで vSAN を有効にできます。

vSAN クラスタの作成

クラスタを作成してから、vSAN 用にクラスタを設定できます。

手順

1 データセンターを右クリックし、[新規クラスタ] を選択します。

2 [名前] テキスト ボックスに、クラスタの名前を入力します。

3 クラスタの DRS、vSphere HA、および EVC を設定します。

4 [OK] をクリックします。

インベントリにクラスタが表示されます。

5 vSAN クラスタにホストを追加します。

vSAN クラスタには、キャパシティ デバイスを持つホストと持たないホストの両方を含めることができます。ベスト プラクティスとして、キャパシティ デバイスを持つホストを追加します。

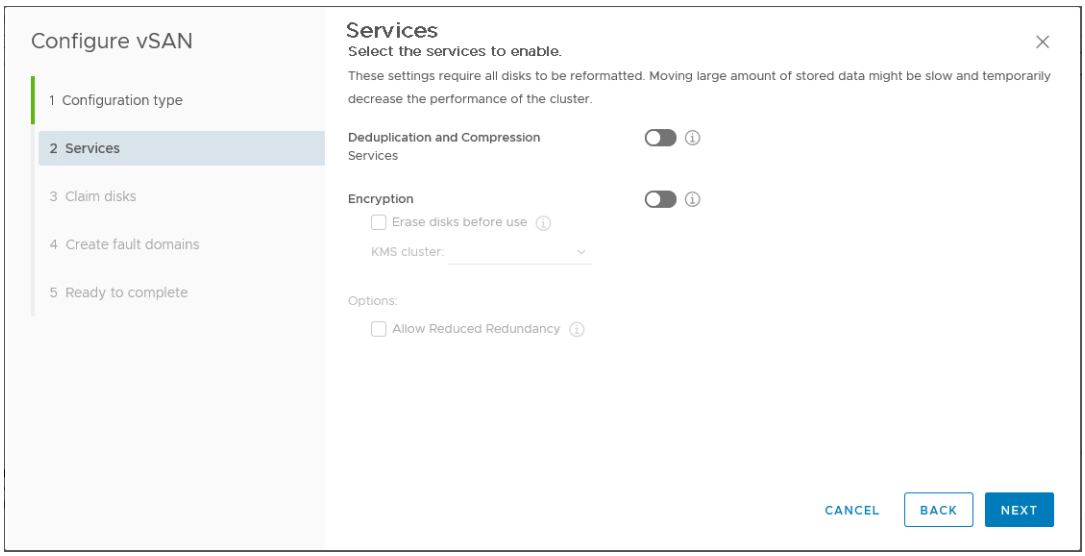
次のステップ

vSAN のクラスタを設定します。「VMware vSAN の管理」を参照してください。

vSphere Client を使用した vSAN クラスタの構成

HTML5 ベースの vSphere Client で vSAN の構成ウィザードを使用して、vSAN クラスタの基本構成を指定できます。

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、クイックスタートを使用した vSAN クラスタの構成および拡張を参照してください。



前提条件

vSAN の構成ウィザードを使用して基本構成を指定する前に、クラスタを作成してホストを追加する必要があります。

手順

1 vSphere Client で、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、[設定] ボタンをクリックします。

4 構成タイプを選択し、[次へ] をクリックします。

- 単一サイト クラスタ。すべてのホストを 1 つのサイトに配置して、監視機能を共有します。
- 2 ホスト構成の vSAN クラスタ。各サイトにホストを 1 台ずつ配置して、別のサイトに監視ホストを配置します。
- ストレッチ クラスタ。2 つのアクティブなデータ サイトに偶数個のホストとストレージ デバイスをそれぞれ配置し、3 番目のサイトに監視ホストを配置します。

5 [サービス] ページで、vSAN サービスを設定し、[次へ]をクリックします。

a （オプション）クラスタで [重複排除および圧縮] を有効にします。

b （オプション）[暗号化] を有効にし、KMS を選択します。

c リソースに制限のある vSAN クラスタで暗号化または重複排除および圧縮を有効にする場合は、[冗長性の低下を許可] チェック ボックスを選択できます。たとえば、3 台のホストで構成されたクラスタで [許容されるプライマリ レベルの障害数] が 1 に設定されているとします。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時に、データが失われるおそれがあります。

6 [ディスクの要求] ページで、クラスタで使用するディスクを選択して、[次へ] をクリックします。

ストレージを提供する各ホストで、キャッシュ層用にフラッシュ デバイスを 1 個選択し、キャパシティ層用に 1 個以上のデバイスを選択します。

7 フォルト トレランス モードに基づいて、ウィザードでクラスタを構成します。

a [2 ホストの vSAN クラスタの構成] を選択した場合は、クラスタの監視ホストを選択し、監視ホスト用にディスクを要求します。

b [ストレッチ クラスタの構成] を選択した場合は、クラスタのフォルト ドメインを定義し、監視ホストを選択して、監視ホストのディスクを要求します。

c [フォールト ドメインの構成] を選択した場合は、クラスタのフォルト ドメインを定義します。

フォルト ドメインとストレッチ クラスタの詳細については、「VMware vSAN の管理」を参照してください。

8 [[設定内容の確認]] ページで設定を確認し、[終了] をクリックします。

結果

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

次のステップ

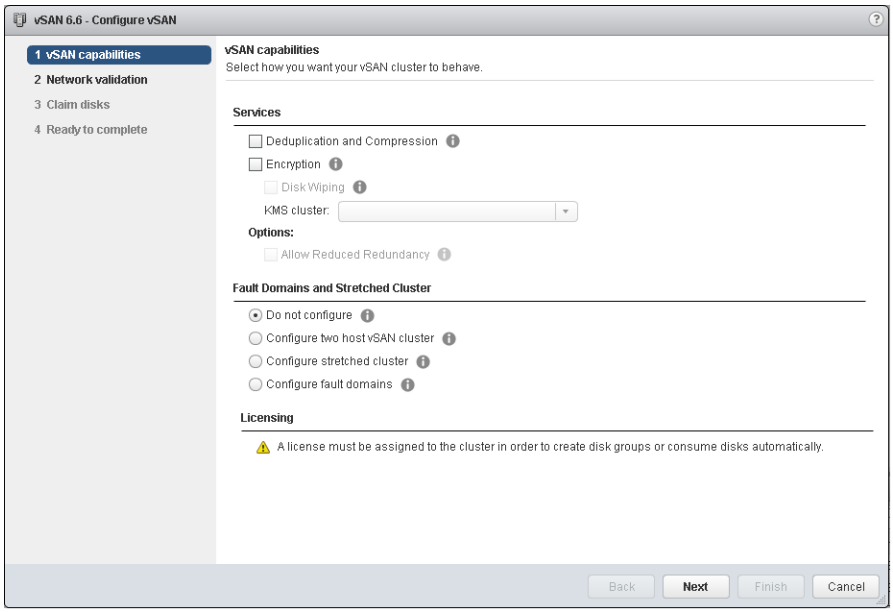
vSAN データストアが作成されたことを確認します。 vSAN データストアの表示 を参照してください。

vSAN ストレージ プロバイダが登録されていることを確認します。「VMware vSAN の管理」を参照してください。

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」を参照してください。

vSphere Web Client を使用した vSAN クラスタの構成

vSAN の構成ウィザードを使用して、vSAN クラスタの基本構成を指定できます。



前提条件

vSAN の構成ウィザードを使用して基本構成を指定する前に、クラスタを作成してホストを追加する必要があります。

手順

1 vSphere Web Client で、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、[全般] を選択し、[構成] ボタンをクリックします。

4 [vSAN 機能] を選択します。

a （オプション）クラスタで重複排除および圧縮を有効にする場合は、[デデュープおよび圧縮] チェック ボックスを選択します。

[冗長性の低下を許可] チェック ボックスを選択して、[許容されるプライマリ レベルの障害数] を 1 に設定した 3 台のホスト クラスタなど、リソースが制限された vSAN クラスタで重複排除および圧縮を有効にできます。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時に、データが失われるおそれがあります。

b （オプション）静止データの暗号化を有効にする場合は、[暗号化] チェック ボックスを選択して、KMS を選択します。

c クラスタのフォルト トレランス モードを選択します。

オプション	説明
構成しない	単一サイトの vSAN クラスタで使用されるデフォルト設定。
2 ホスト構成の vSAN クラスタ	リモート オフィスに 2 台のホストがあり、監視ホストがメイン オフィスにあるクラスタでフォルト トレランスを有効にします。[許容されるプライマリ レベルの障害数] ポリシーを 1 に設定します。
ストレッチ クラスタ	2 つのアクティブ サイトをサポートします。それぞれに偶数個のホストとストレージ デバイスがあり、監視ホストが 3 番目のサイトにあります。
フォルト ドメインの構成	障害が発生するおそれがある vSAN ホストをグループ化するために使用できるフォルト ドメインをサポートします。各フォルト ドメインに 1 台以上のホストを割り当てます。

d リソースに制限のある vSAN クラスタで暗号化または重複排除および圧縮を有効にする場合は、[冗長性の低下を許可] チェック ボックスを選択できます。たとえば、3 台のホストで構成されたクラスタで [許容されるプライマリ レベルの障害数] が 1 に設定されているとします。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時に、データが失われるおそれがあります。

5 [次へ] をクリックします。

6 [ネットワーク検証] ページで、vSAN VMkernel アダプタの設定を確認し、[次へ] をクリックします。

7 [ディスクの要求] ページで、クラスタで使用するディスクを選択して、[次へ] をクリックします。

ストレージを提供する各ホストで、キャッシュ層用にフラッシュ デバイスを 1 個選択し、キャパシティ層用に 1 個以上のデバイスを選択します。

8 ウィザードを使用して、フォルト トレランス モード ベースのクラスタを構成します。

a [2 ホストの vSAN クラスタの構成] を選択した場合、クラスタの監視ホストを選択し、監視ホストのディスクを要求します。

b [ストレッチ クラスタの構成] を選択した場合、クラスタのフォルト ドメインを定義し、監視ホストを選択して、監視ホストのディスクを要求します。

c [フォールト ドメインの構成] を選択した場合、クラスタのフォルト ドメインを定義します。

フォルト ドメインとストレッチ クラスタの詳細については、「VMware vSAN の管理」を参照してください。

9 [設定内容の確認] 画面で構成を確認し、[終了] をクリックします。

vSAN 設定の編集

vSAN クラスタの設定を編集して、ディスクを要求する方法を変更し、デデュープおよび圧縮を有効にできます。

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。

オプション	説明
vSphere Client	a [vSAN] の下で [サービス] を選択します。 b 設定するサービスの [編集] ボタンをクリックします。 ■ 重複排除および圧縮を有効または無効にします。 ■ vSAN 暗号化を設定します。 ■ vSAN パフォーマンス サービスを構成します。 ■ iSCSI ターゲット サービスを構成します。 ■ 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。
vSphere Web Client	a [vSAN] の下で [全般] を選択します。 b vSAN が有効になっているペインで、[編集] ボタンをクリックします。 c （オプション）クラスタで重複排除および圧縮を有効にする場合は、[デデュープおよび圧縮] チェック ボックスを選択します。vSAN は自動的にオンディスク フォーマットをアップグレードするため、クラスタ内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が行われます。 d （オプション）クラスタで暗号化を有効にする場合は、[暗号化] チェック ボックスをクリックしてから、KMS サーバを選択します。vSAN は自動的にオンディスク フォーマットをアップグレードするため、クラスタ内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が行われます。

3 [OK] または [適用] をクリックし、選択内容を確認します。

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。 『VMware vSAN の管理』の「vSAN を有効にするための要件」を参照してください。

手順

1 既存のホスト クラスタに移動します。

2 [設定] タブをクリックします。

オプション	説明
vSphere Client	a [vSAN] の下で [サービス] を選択します。 b （オプション）クラスタで重複排除と圧縮を有効にします。vSAN は自動的にオンディスク フォーマットをアップグレードするため、クラスタ内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が行われます。 c （オプション）クラスタで暗号化を有効にし、KMS サーバを選択します。vSAN は自動的にオンディスク フォーマットをアップグレードするため、クラスタ内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が行われます。 d （オプション）[冗長性の低下を許可] を選択します。vSAN は、必要に応じて重複排除と圧縮、または暗号化を有効にしながら、仮想マシンの保護を低いレベルに変更します。
vSphere Web Client	a [vSAN] の下で [全般] を選択します。 b vSAN が有効になっているペインで、[編集] ボタンをクリックします。 c （オプション）クラスタで重複排除および圧縮を有効にする場合は、[デデュープおよび圧縮] チェック ボックスを選択します。vSAN は自動的にオンディスク フォーマットをアップグレードするため、クラスタ内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が行われます。 d （オプション）クラスタで暗号化を有効にする場合は、[暗号化] チェック ボックスをクリックしてから、KMS サーバを選択します。vSAN は自動的にオンディスク フォーマットをアップグレードするため、クラスタ内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が行われます。

3 [OK] または [適用] をクリックし、選択内容を確認します。

次のステップ

ストレージ デバイスを要求するか、ディスク グループを作成します。「VMware vSAN の管理」を参照してください。

vSAN クラスタのライセンス設定

評価期間の終了前、または現在割り当てられているライセンスの有効期間の終了前に、vSAN クラスタにライセンスを割り当てる必要があります。

vSAN のライセンスをアップグレード、結合、または分割する場合は、新しいライセンスを vSAN クラスタに割り当てる必要があります。vSAN ライセンスをクラスタに割り当てる場合、使用されるライセンス キャパシティの量は、クラスタに参加しているホストの CPU の総数に等しくなります。vSAN クラスタのホストが追加または削除されるたびに、クラスタのライセンス使用量が再計算および更新されます。ライセンスの管理およびライセンスに関する用語と定義の詳細については、『vCenter Server およびホスト管理』ドキュメントを参照してください。

クラスタで vSAN を有効にすると、vSAN を評価モードで使用してその機能を調べることができます。評価期間は、vSAN が有効になると開始され、その 60 日後に期限切れになります。vSAN を使用する場合は、評価期間が期限切れになる前にクラスタのライセンス契約を行う必要があります。vSphere ライセンスと同様に、vSAN ライセンスにも CPU 単位のキャパシティがあります。オール フラッシュ構成やストレッチ クラスタなどの高度な機能を使用するには、その機能をサポートするライセンスが必要です。

前提条件

- vSAN のライセンスを表示および管理するには、vCenter Server システムに対する グローバル.ライセンス 権限を持っている必要があります。

手順

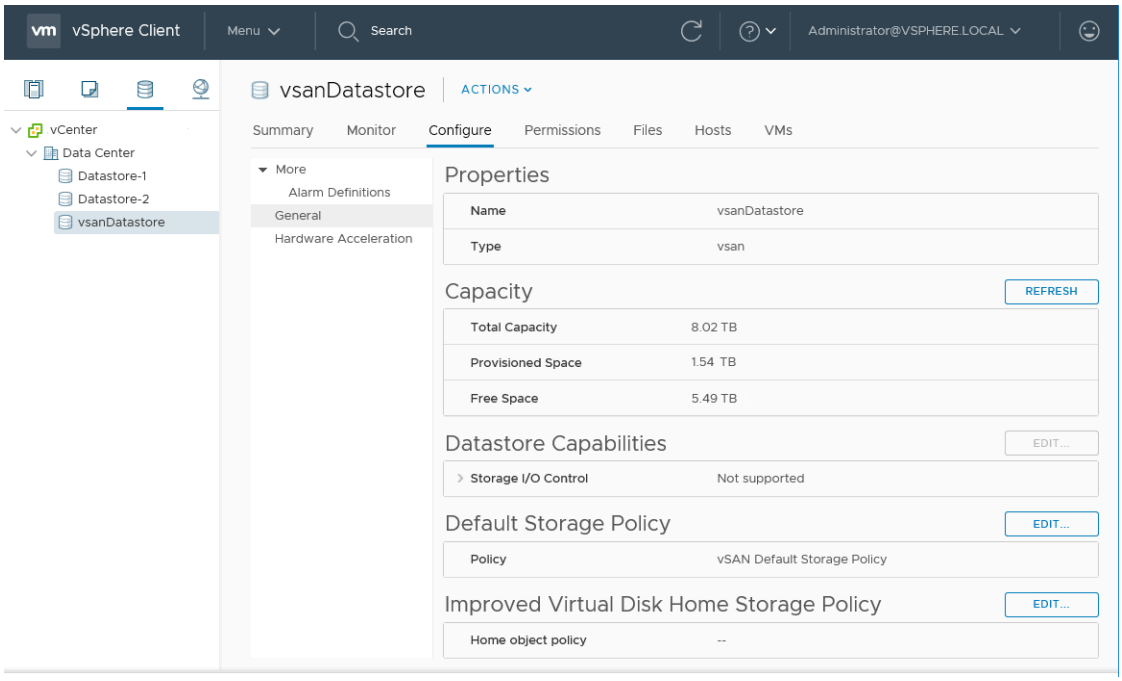
1 vSAN クラスタに移動します。

2 [設定] タブをクリックします。

オプション	説明
vSphere Client	a vSAN クラスタを右クリックし、[ライセンスの割り当て] メニューを選択します。 b ライセンス オプションを選択します。 ■ 既存のライセンスを選択し、[OK] をクリックします。
vSphere Web Client	a [構成] で、[ライセンス] を選択し、[ライセンスの割り当て] をクリックします。 b ライセンス オプションを選択します。 ■ 既存のライセンスを選択し、[OK] をクリックします。

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 [設定] 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 x 2 TB x 8 = 112 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重複排除および圧縮では、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』を参照してください。

vSAN および vSphere HA の使用

vSphere HA と vSAN を同じクラスタで有効にできます。vSphere HA では、vSAN データストアに従来のデータストアと同じレベルの仮想マシンの保護を提供します。このレベルの保護では、vSphere HA と vSAN がやり取りするときに、特定の制限が適用されます。

ESXi ホストの要件

vSAN は、次の条件を満たす場合にのみ vSphere HA クラスタと併用できます。

- クラスタの ESXi ホストはすべてバージョン 5.5 Update 1 以降である必要があります。
- クラスタには、3 台以上の ESXi ホストが必要です。最適な結果を得るには、4 台以上のホストで vSAN クラスタを構成します。

ネットワークの相違点

vSAN は独自の論理ネットワークを使用します。vSAN と vSphere HA が同じクラスタに対して有効にされていると、HA のエージェント間のトラフィックは管理ネットワークではなくこのストレージ ネットワークを通過します。vSphere HA は、vSAN が無効な場合にのみ管理ネットワークを使用します。vCenter Server は、ホストで vSphere HA が構成されている場合に適切なネットワークを選択します。

注： vSphere HA を無効にしてから、vSAN をクラスタで有効にする必要があります。その後、vSphere HA を再度有効にすることができます。

仮想マシンがすべてのネットワーク パーティションで部分的にのみアクセス可能な場合、仮想マシンをパワーオンしたり、すべてのパーティションで仮想マシンに完全にアクセスしたりすることはできません。たとえば、クラスタを P1 と P2 にパーティション分割した場合、仮想マシン名前空間オブジェクトはパーティション P1 にはアクセスできますが、P2 にはアクセスできません。VMDK はパーティション P2 にアクセスできますが、P1 にはアクセスできません。このような場合、仮想マシンはパワーオンできず、すべてのパーティションに完全にアクセスすることはできません。

次の表は、vSAN が使用されているときと使用されていないときの vSphere HA ネットワークの相違点を示しています。

表 5-2. vSphere HA ネットワークの相違点

	vSAN が有効	vSAN が無効
vSphere HA が使用するネットワーク	vSAN ストレージ ネットワーク	管理ネットワーク
ハートビート データストア	2 台以上のホストにマウントされる、vSAN データストア以外のデータストア	2 台以上のホストにマウントされるデータストア
ホストは 「隔離」 と宣言	隔離アドレスは ping 不可、vSAN ストレージ ネットワークはアクセス不可	隔離アドレスは ping 不可、管理ネットワークはアクセス不可

vSAN のネットワーク構成を変更すると、vSphere HA エージェントは新しいネットワーク設定を自動的に取得しません。vSAN ネットワークを変更するには、vSphere HA クラスタのホストの監視を有効に戻す必要があります。

1 vSphere HA クラスタの [ホストの監視] を無効にします。

2 vSAN ネットワークに変更を加えます。

3 クラスタのすべてのホストを選択して右クリックし、[HA の再構成] を選択します。

4 vSphere HA クラスタの [ホストの監視] を有効に戻します。

キャパシティの予約設定

アドミッション コントロール ポリシーで vSphere HA クラスタの容量を予約する場合は、この設定が vSAN ルール セットの対応する [許容されるプライマリ レベルの障害数] ポリシー設定と連携する必要があります。vSphere HA アドミッション コントロールの設定で予約されている容量よりも少なくすることはできません。たとえば、vSAN のルール セットが 2 つの障害しか許容していない場合、vSphere HA アドミッション コントロール ポリシーでは 1 つまたは 2 つのホスト障害に相当する容量を予約する必要があります。ホストが 8 台あるクラスタで [予約されたクラスタ リソースの割合] ポリシーを使用している場合、クラスタ リソースの 25 パーセントを超えて予約をしないでください。同じクラスタで、[許容されるプライマリ レベルの障害数] ポリシーを使用してホストの台数が

2 を超えないように設定します。vSphere HA によって予約される容量が少なすぎると、フェイルオーバーが期待されたとおりに動作しない可能性があります。過度に大きな容量が予約されると、仮想マシンのパワーオンとクラスタ間の vSphere vMotion 移行に大きな制約が生じることがあります。[予約されたクラスタ リソースの割合] ポリシーの詳細については、『vSphere 可用性』ドキュメントを参照してください。

複数のホストで障害が発生した状況での vSAN と vSphere HA の動作

vSAN クラスタで障害が発生し、仮想マシン オブジェクトのフェイルオーバー クォーラムが損失した場合、vSphere HA はそのクラスタ クォーラムがリストアされても仮想マシンを再起動できなくなる場合があります。vSphere HA では、クラスタ クォーラムがあり、仮想マシン オブジェクトの最新のコピーにアクセスできる場合にのみ、再起動が保証されています。最新のコピーとは、最後に書き込まれたコピーのことです。

1 台のホストの障害を許容するため、vSAN 仮想マシンをプロビジョニングする例を考えてみましょう。ホスト H1、H2、および H3 という 3 台のホストが含まれている vSAN クラスタで、仮想マシンを実行しています。3 台のすべてのホストに順番に障害が発生します。最後に障害が発生するホストは H3 です。

H1 と H2 が復旧した後、クラスタには 1 つのクォーラムがあります（1 台のホストの障害が許容される）。しかし、障害が発生した最後のホスト (H3) に仮想マシン オブジェクトの最新コピーが含まれており、そのコピーにはまだアクセスできないため、vSphere HA は仮想マシンを再起動できません。

この例では、3 台のすべてのホストを同時に復旧するか、2 台のホストのクォーラムに H3 が含まれている必要があります。どちらの条件も満たされない場合、HA はホスト H3 が再度オンラインになったら、仮想マシンの再起動を試行します。

vSAN と vCenter Server Appliance のデプロイ

vCenter Server Appliance をデプロイするときに vSAN クラスタを作成して、このクラスタでアプライアンスをホストすることができます。

vCenter Server Appliance は、Linux システムで VMware vCenter Server を実行するために使用される、事前構成された Linux 仮想マシンです。この機能を使用すると、vCenter Server を使用しなくても、新しい ESXi ホストに vSAN クラスタを構成することができます。

vCenter Server Appliance インストーラを使用して vCenter Server Appliance をデプロイする場合は、シングルホストの vSAN クラスタを作成して、このクラスタで vCenter Server Appliance をホストすることができます。デプロイのステージ 1 でデータストアを選択する場合は、[ターゲット ホストを含む新しい vSAN クラスタにインストール] をクリックします。インストーラ ウィザードの手順に従ってデプロイを完了します。

vCenter Server Appliance インストーラにより、ホストから要求されたディスクを含む、1 台のホストからなる vSAN クラスタが作成されます。vCenter Server Appliance は vSAN クラスタにデプロイされます。

デプロイが完了したら、vCenter Server Appliance を含むシングルホストの vSAN クラスタを管理できるようになります。vSAN クラスタの構成を完了する必要があります。

Platform Services Controller と vCenter Server を同じ vSAN クラスタにデプロイすることも、異なるクラスタにデプロイすることもできます。

- Platform Services Controller と vCenter Server を同じ vSAN クラスタにデプロイできます。PSC および vCenter Server を同じシングルホスト vSAN データストアにデプロイします。デプロイが完了したら、Platform Services Controller および vCenter Server が両方とも同じクラスタで実行されます。

- Platform Services Controller と vCenter Server を異なる vSAN クラスタにデプロイできます。Platform Services Controller および vCenter Server を異なるシングルホスト vSAN クラスタにデプロイします。デプロイが完了したら、各 vSAN クラスタの構成を個別に完了する必要があります。

vSAN を無効にする

ホスト クラスタの vSAN をオフにできます。

vSAN クラスタを無効にすると、共有 vSAN データストアのすべての仮想マシンにアクセスできなくなります。vSAN が無効であるときに仮想マシンを使用する場合は、必ず vSAN クラスタを無効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。

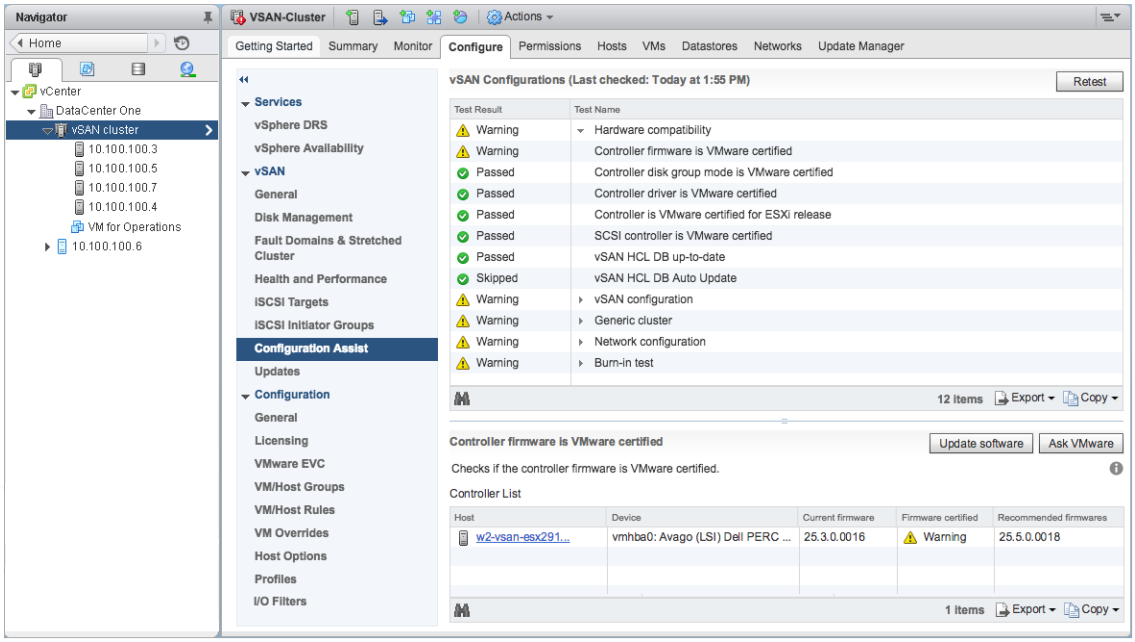
オプション	説明
vSphere Client	a [vSAN] の下で [サービス] を選択します。 b [vSAN をオフにする] をクリックします。 c [vSAN をオフにする] ダイアログで選択内容を確認します。
vSphere Web Client	a [vSAN] の下で [全般] を選択します。 b 有効になっている vSAN の[編集]ボタンをクリックします。 c vSAN を [オンにする] チェック ボックスを選択解除します。

vSAN Configuration Assist およびアップデートの使用

Configuration Assist を使用して vSAN クラスタの構成をチェックし、問題があれば解決することができます。

vSAN Configuration Assist では、クラスタ コンポーネントの構成を確認し、問題の解決とトラブルシューティングを行うことができます。構成チェックの対象となるのは、ハードウェアの互換性、ネットワーク、および vSAN 構成に関するオプションです。

注： vSAN 6.7 では、Configuration Assist および更新は vSphere Web Client でのみ使用できます。



Configuration Assist によるチェックは、次のカテゴリに分類されます。各カテゴリには、個別の構成チェックが含まれます。

表 5-3. Configuration Assist のカテゴリ

構成のカテゴリ	説明
ハードウェア互換性	vSAN クラスタのハードウェア コンポーネントをチェックして、サポート対象のハードウェア、ソフトウェア、およびドライバが使用されていることを確認します。
vSAN 構成	vSAN 構成オプションをチェックします。
汎用クラスタ	基本的なクラスタ構成オプションをチェックします。
ネットワークの構成	vSAN ネットワーク構成をチェックします。

ストレージ コントローラ ファームウェアまたはドライバが『VMware 互換性ガイド』に記載されている要件を満たさない場合は、[更新] ページを使用してコントローラを更新することができます。

vSAN 構成の確認

vSAN クラスタの構成ステータスを確認して、クラスタの動作に影響を及ぼす問題を解決できます。

手順

1 vSphere Web 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] の下にある [Configuration Assist] をクリックして、vSAN 構成のカテゴリを確認します。

[テスト結果] 列に警告アイコンが表示された場合、カテゴリを展開して各構成チェックの結果を確認します。

4 個々の構成チェックを選択し、ページ下部の詳細情報を確認します。

[AskVMware] ボタンをクリックすると、チェックの内容と、問題の解決方法に関する情報が記されたナレッジベース記事を開くことができます。

一部の構成チェックでは、構成を完了するために使用できる追加ボタンが用意されています。

vSAN 用の Distributed Switch の設定

[vSAN 用の新しい Distributed Switch の設定] ウィザードを使用して、vSAN トラフィックをサポートするように vSphere Distributed Switch を設定します。

クラスタで vSAN トラフィックをサポートするように vSphere Distributed Switch が設定されていない場合は、[Configuration Assist] ページの [ネットワーク構成] > [Distributed Switch を vSAN に使用する] を選択すると警告が表示されます。

手順

1 vSphere Web 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、[Configuration Assist] を選択し、[ネットワーク構成] カテゴリをクリックして展開します。

4 [vSAN 用に Distributed Switch を使用] をクリックします。ページの下半分で、[Distributed Switch の作成] をクリックします。

5 [名前] と [タイプ] で、新しい Distributed Switch の名前を入力し、新しいスイッチを作成するか、既存の標準スイッチを移行するかを選択します。

6 新しい Distributed Switch に移行する対象の未使用のアダプタを選択して、[次へ] をクリックします。

7 （オプション）[インフラストラクチャ仮想マシンの移行] で、既存の標準スイッチの移行中にインフラストラクチャ仮想マシンとして扱う仮想マシンを選択し、[次へ] をクリックします。

新しい Distributed Switch を作成する場合には、このステップは不要です。

8 [設定内容の確認] ページで設定を確認し、[終了] をクリックします。

vSAN 向けの VMkernel ネットワーク アダプタの作成

[新しい vSAN 用の VMkernel ネットワーク アダプタ] ウィザードを使用して、vSAN トラフィックをサポートするように vmknic を設定できます。

クラスタ内の ESXi ホストで vSAN トラフィックをサポートするように vmknic が設定されていない場合は、[Configuration Assist] ページで [ネットワーク構成] > [すべてのホストで vSAN vmknic が構成済み] を選択すると、警告が表示されます。

手順

1 vSphere Web 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、[Configuration Assist] を選択し、[ネットワーク構成] カテゴリをクリックして展開します。

4 [すべてのホストで vSAN vmknic が構成済み] をクリックします。ページの下半分で、[VMkernel ネットワーク アダプタの作成] をクリックします。

5 [ホストの選択] で、vSAN 用に vmknic が設定されていない各ホストのチェック ボックスを選択して、[次へ] をクリックします。

vSAN vmknic が設定されていないホストが、[Configuration Assist] ページに一覧表示されます。

6 [場所とサービス] で、Distributed Switch を選択し、[vSAN トラフィック] チェック ボックスを選択します。[次へ] をクリックします。

7 [vSAN アダプタ設定] で、ポート グループ、IP 設定、構成を選択して、[次へ] をクリックします。

8 [設定内容の確認] ページで設定を確認し、[終了] をクリックします。

ドライバおよびファームウェアのアップデート用に、コントローラ管理ツールをインストールする

vSAN では、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およびファームウェアを更新できます。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。

[更新] ページでは、一部のベンダーから提供される特定のストレージ コントローラ モデルのみをサポートしています。

前提条件

- [Configuration Assist] ページでハードウェア互換性を確認します。
- ソフトウェアの更新中に、仮想マシンを実行したままで維持するには、DRS を有効にする必要があります。

手順

1 vSphere Web 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 で [更新] をクリックして、欠けているコンポーネントまたは、インストール準備が完了したコンポーネントを確認します。

4 コントローラの管理 (Mgmt) ツールを選択して、[ダウンロード] アイコンをクリックします。

インターネット経由で管理ツールが vCenter Server にダウンロードされます。

5 [すべて更新] アイコンをクリックして、クラスタ内の ESXi ホストに管理ツールをインストールします。

すべてのホストを一度に更新するかどうか、またはローリング更新を使用するかどうかを確認します。

6 [更新] アイコンをクリックします。

[更新] ページに、更新の必要なコントローラ コンポーネントが表示されます。

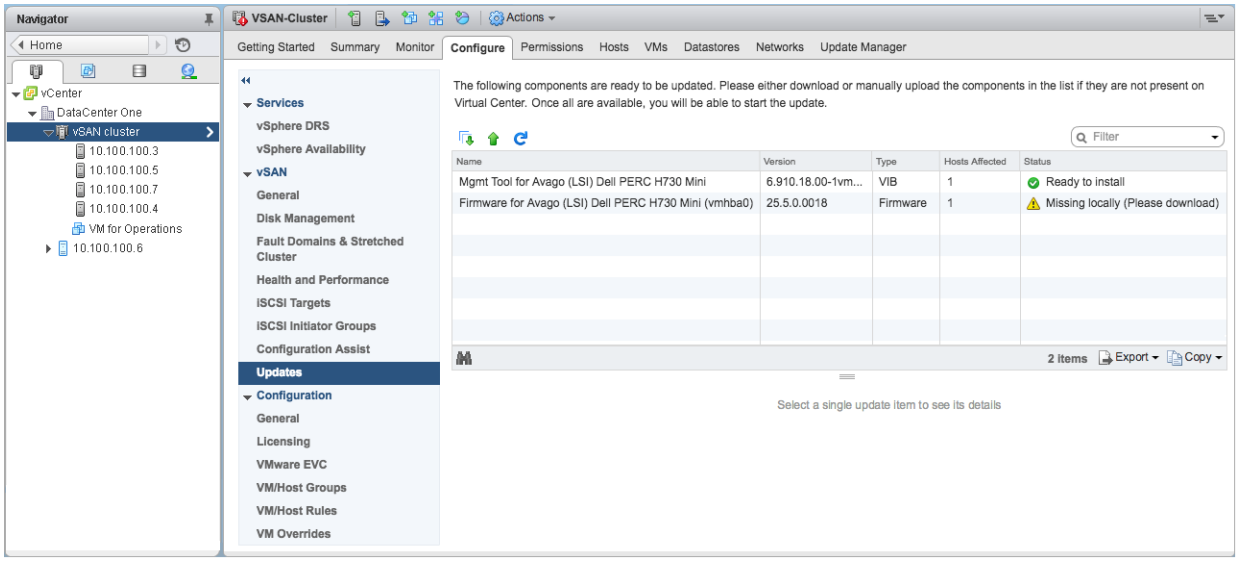
次のステップ

管理ツールがインストールされたら、[更新] ページに表示されるコントローラのドライバとファームウェアの更新に進むことができます。

ストレージ コントローラ デバイスおよびファームウェアの更新

vSAN を使用して、ストレージ コントローラの古いドライバやファームウェア、または正しくないドライバやファームウェアを更新することができます。

注： vSAN 6.7 以降のリリースでは、Configuration Assist および更新は vSphere Web Client でのみ使用できます。



Configuration Assist は、ストレージ コントローラが『VMware 互換性ガイド』に記載されている最新のドライバおよびファームウェア バージョンを使用していることを確認します。コントローラ ドライバまたはファームウェアが要件を満たさない場合は、[更新] ページを使用してドライバおよびファームウェアを更新します。

前提条件

ESXi ホスト上にストレージ デバイスのコントローラ管理ツールがなければなりません。

手順

1. vSphere Web 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 で [更新] をクリックして、欠けているコンポーネントまたは、インストール準備が完了したコンポーネントを確認します。

   [更新] ページに、見つからないファームウェアおよびドライバのコンポーネントがすべて表示されます。

   注： コントローラ管理 (Mgmt) ツールを使用できない場合は、管理ツールをダウンロードしてインストールするよう求められます。管理ツールを使用できる場合は、失われているすべてのドライバまたはファームウェアが表示されます。

4 更新するコンポーネントを選択し、[更新] アイコンをクリックして、クラスタ内の ESXi ホストのコンポーネントを更新します。また、[すべて更新] アイコンをクリックして、見つからないすべてのコンポーネントを更新することができます。

すべてのホストを一度に更新するかどうか、またはローリング更新を使用するかどうかを確認します。

注： 一部の管理ツールおよびドライバでは、更新プロセスでメンテナンス モードがバイパスされ、インストール結果に基づいて再起動されます。このような場合、[MM が必要です] および [再起動が必要です] テキスト ボックスは空になります。

5 [更新] アイコンをクリックします。

更新されたコンポーネントは画面から削除されます。

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 Validated Design Documentation』で、「vSphere with Tanzu ワークロード ドメインのシャットダウン」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
```

ストレッチ クラスタを使用して 2 つのサイトにデータストアを拡張する

6

2 つの地理的な場所（またはサイト）にわたるストレッチ クラスタを作成することができます。ストレッチ クラスタを使用すると、vSAN データストアを 2 つのサイトにわたって拡張し、これを拡張ストレージとして使用できます。ストレッチ クラスタは、1 つのサイトで障害が発生したり、スケジュール設定されたメンテナンスが実行されたりする場合にも、稼動し続けます。

この章には、次のトピックが含まれています。

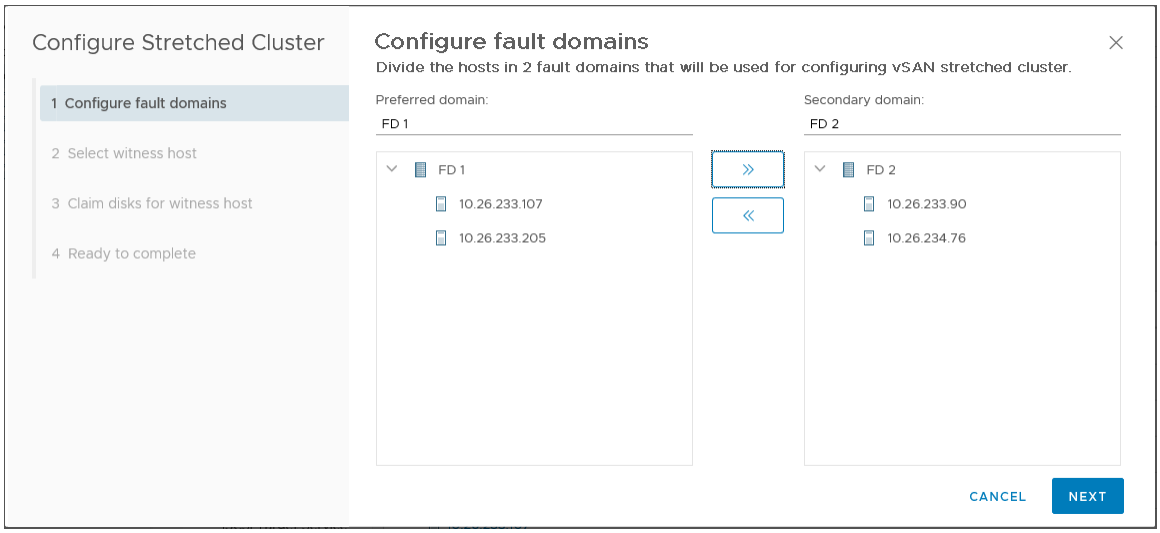
ストレッチ クラスタの概要

ストレッチ クラスタを使用すると、vSAN クラスタが 1 つのデータ サイトから 2 つのサイトに拡張され、より高度な可用性とサイト間の負荷分散を実現できます。通常、ストレッチ クラスタはデータセンター間の距離が限定されている環境（都市やキャンパスなど）に導入されます。

ストレッチ クラスタを使用すれば、一方のサイトでメンテナンスを実行したり、一方のサイトが切断したりしても、クラスタの全体的な運用には影響しないため、計画的なメンテナンスを管理して、災害シナリオを回避できます。 ストレッチ クラスタ構成では、両方のデータ サイトがアクティブになっています。いずれかのサイトで障害が派生すると、vSAN はもう一方のサイトのストレージを使用します。vSphere HA は、残りのアクティブ サイトで再起動する必要のある仮想マシンを再起動します。

1 つのサイトを優先サイトとして定義する必要があります。他のサイトは、セカンダリ サイトまたは非優先サイトになります。2 つのアクティブなサイト間でネットワーク接続が失われている場合、優先サイトのみ使用されます。優先として指定されているサイトとは、通常は、動作を継続しているサイトのことです。ただし、優先サイトが再同期している場合、または優先サイトに別の問題がある場合は除きます。サイトが運用を継続できれば、データの可用性は最大になります。

vSAN ストレッチ クラスタでは、一度に 1 つのリンク障害を許容でき、データを継続して使用できます。リンク障害とは、2 つのサイト間または 1 つのサイトと監視ホスト間でネットワーク接続が切断されることです。 サイト障害またはネットワーク接続の切断時に、vSAN は完全に機能するサイトに自動的に切り替わります。



ストレッチ クラスタの使用方法の詳細については、『vSAN ストレッチ クラスタ ガイド』を参照してください。

監視ホスト

各ストレッチ クラスタは、2 つのデータ サイトと 1 つの監視ホストで構成されます。監視ホストは 3 番目のサイトにあり、この監視ホストには仮想マシン オブジェクトの監視コンポーネントが含まれます。 メタデータのみが含まれ、ストレージ操作には関わりません。

監視ホストは、2 つのサイト間のネットワーク接続が切断されて、データストア コンポーネントの可用性に関して決定を下す必要がある場合のタイブレーカとして機能します。 この場合、通常、監視ホストは優先サイトを使用して vSAN クラスタを形成します。ただし、優先サイトがセカンダリ サイトと監視ホストから隔離された場合、監視ホストはセカンダリ サイトを使用してクラスタを形成します。 優先サイトが再度オンラインになると、両方のサイトにすべての最新データのコピーが含まれるようにデータが再同期されます。

監視ホストに障害が発生した場合、対応するすべてのオブジェクトがコンプライアンスに準拠しなくなりますが、完全にアクセスすることができます。

監視ホストには次の特性があります。

- 監視ホストは、バンド幅が狭い/待ち時間が長いリンクを使用できます。
- 監視ホストは、仮想マシンを実行できません。
- 1 台の監視ホストは、1 つの vSAN ストレッチ クラスタのみをサポートできます。

- 監視ホストには、vSAN トラフィックが有効で、クラスタ内のすべてのホストに接続できる VMkernel アダプタが 1 つ必要です。監視ホストは、管理用に 1 つの VMkernel アダプタを、vSAN データ トラフィック用に 1 つの VMkernel アダプタを使用します。監視ホストは、vSAN 専用に VMkernel アダプタを 1 つのみ使用できます。
- 監視ホストは、ストレッチ クラスタ専用のスタンドアロン ホストである必要があります。 vCenter Server を使用して、他のクラスタに追加したり、インベントリ内で移動したりできません。

監視ホストは、物理ホスト、または仮想マシン内で実行されている ESXi ホストになります。 仮想マシンの監視ホストでは、仮想マシンの保存や実行などの他のタイプの機能は提供されません。 1 つの物理サーバで複数の監視ホストを仮想マシンとして実行できます。 パッチの適用やネットワークおよび監視の基本構成の場合、仮想マシンの監視ホストは標準 ESXi ホストと同じように機能します。 監視ホストは、vCenter Server を使用して管理する、`esxcli` または vSphere Update Manager を使用してパッチの適用やアップデートを行う、および ESXi ホストと通信する標準ツールを使用して監視することができます。

ストレッチ クラスタの監視ホストとして監視仮想アプライアンスを使用できます。 監視仮想アプライアンスは仮想マシンの ESXi ホストで、OVF または OVA としてパッケージ化されています。 アプライアンスは、環境のサイズに基づいて各種オプションで使用できます。

ストレッチ クラスタおよびフォールト ドメイン

ストレッチ クラスタは、サイト間の冗長性を高めて障害から保護するためにフォールト ドメインを使用します。ストレッチ クラスタの各サイトは、個別のフォールト ドメインに存在します。

ストレッチ クラスタでは、優先サイト、セカンダリ サイト、および監視ホストの 3 つのフォールト ドメインが必要です。各フォールト ドメインは独立したサイトを表します。監視ホストに障害が発生するか、または監視ホストがメンテナンス モードになると、vSAN はサイトに障害があると見なします。

vSAN 6.6 以降のリリースでは、ストレッチ クラスタ内の仮想マシン オブジェクトに対して、ローカル障害からの保護レベルを一段と高めることができます。ストレッチ クラスタを構成する場合は、クラスタ内のオブジェクトに次のポリシー ルールを使用できます。

- [許容されるプライマリ レベルの障害数 (PFTT)] : ストレッチ クラスタでは、[PFTT] は 1 個の仮想マシン オブジェクトが許容できるサイトの障害の数を定義します。ストレッチ クラスタでサポートされている値は、0 または 1 のみです。
- [許容されるセカンダリ レベルの障害数 (SFTT)] : ストレッチ クラスタでは、SFTT は、[PFTT] で定義されたサイトの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。[PFTT] に 1、[SFTT] に 2 が指定され、1 つのサイトが利用できない場合、クラスタは 2 つの追加のホストの障害を許容できます。

  デフォルト値は 0 であり、最大値は 3 です。
- [データのローカリティ（局所性）] : このルールは、[PFTT] = 0 の場合のみ使用できます。[データのローカリティ] ルールは [なし]、[優先]、[セカンダリ] のいずれかに設定できます。このルールによって、ストレッチ クラスタ内の選択したサイトに仮想マシン オブジェクトを制限できます。デフォルト値は [なし] です。

注： ストレッチ クラスタに [SFTT] を設定すると、[耐障害性方式] ルールが [SFTT] に適用されます。[PFTT] に使用される耐障害性方式は、RAID 1 に設定されます。

ローカルでの障害からの保護が設定されたストレッチ クラスタでは、1 個のサイトが利用できない場合でも、クラスタ内の利用可能なサイトで、欠けているコンポーネントや障害のあるコンポーネントの修理を実行できます。

ストレッチ クラスタの設計に関する考慮事項

vSAN ストレッチ クラスタを使用する場合、次のガイドラインを考慮してください。

- ストレッチ クラスタの DRS 設定を構成します。
  - クラスタ上で DRS が有効になっている必要があります。DRS を一部自動化モードで設定すると、各サイトにどの仮想マシンを移行するかを制御できます。
  - 優先サイト用とセカンダリ サイト用に 2 つのホスト グループを作成します。
  - 優先サイト上に仮想マシンを保持するためのグループと、セカンダリ サイト上に仮想マシンを保持するためのグループの 2 つの仮想マシン グループを作成します。
  - 仮想マシンとホスト グループをマッピングする仮想マシンとホスト間のアフィニティ ルールを 2 つ作成し、どの仮想マシンとホストを優先サイト上に配置し、どの仮想マシンとホストをセカンダリ サイト上に配置するかを指定します。
  - クラスタ内の仮想マシンの初期配置を実行するように、仮想マシンとホスト間のアフィニティ ルールを構成します。
- ストレッチ クラスタの HA 設定を構成します。
  - クラスタ上で HA が有効になっている必要があります。
  - HA ルール設定はフェイルオーバー中に仮想マシンとホスト間のアフィニティ ルールを順守する必要があります。
  - HA データストア ハートビートを無効化します。
- ストレッチ クラスタにはオンディスク フォーマット 2.0 以降が必要です。必要に応じて、ストレッチ クラスタを構成する前にオンディスク フォーマットをアップグレードします。『*VMware vSAN の管理*』の「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。
- ストレッチ クラスタの [許容障害数] を 1 に構成します。
- vSAN ストレッチ クラスタでは、[PFFT] が 0 に設定され、[データのローカリティ] が「優先」または「セカンダリ」に設定されている場合、Symmetric Multiprocessing Fault Tolerance (SMP-FT) 仮想マシンの有効化がサポートされます。vSAN は、[PFFT] が 1 以上に設定されたストレッチ クラスタ上の SMP-FT 仮想マシンをサポートしていません。
- ホストが切断されたり応答しない場合は、監視ホストの追加または削除は実施できません。この制限により、再構成処理を開始する前に、vSAN が十分な情報をすべてのホストから収集できるようになります。
- `esxcli` を使用してホストの追加または削除を行うことは、ストレッチ クラスタではサポートされません。

ストレッチ クラスタを操作する場合のベスト プラクティス

vSAN ストレッチ クラスタを操作するときは、適切なパフォーマンスを得るために次の推奨事項に準拠してください。

- ストレッチ クラスタ内のサイト（フォルト ドメイン）の 1 つにアクセスできない場合でも、別の 2 つのサイトを含むサブクラスタに新しい仮想マシンをプロビジョニングすることができます。これらの新規仮想マシンは暗黙的に強制プロビジョニングされ、パーティション分割されたサイトがクラスタに再接続されるまでは非準拠状態になります。この暗黙的な強制プロビジョニングは、3 つのサイトのうちの 2 つが利用可能な場合にのみ実行されます。 この「サイト」とは、データ サイトまたは監視ホストのいずれかを指します。
- 停電やネットワーク接続が失われたことが原因でサイト全体がオフラインになった場合は、時間を置かずに、サイトを直ちに再起動します。 vSAN ホストを 1 台ずつ再起動する代わりに、すべてのホストをほぼ同時にオンラインに戻します。間隔は 10 分以内にするのが理想的です。このプロセスに従うと、サイト間で大量のデータが再同期されることを回避できます。
- ホストが永続的に使用不可の場合は、再構成タスクを実行する前に、クラスタからそのホストを削除します。
- 複数のストレッチ クラスタに対応するために仮想マシンの監視ホストのクローンを作成する場合、クローンを作成するまでは仮想マシンを監視ホストとして構成しないでください。 最初に OVF から仮想マシンを展開し、次に仮想マシンのクローンを作成して、各クローンを別のクラスタの監視ホストとして構成します。 または、OVF から必要な数の仮想マシンを展開し、それぞれを異なるクラスタ用の監視ホストとして構成できます。

ストレッチ クラスタのネットワーク設計

ストレッチ クラスタの 3 つのサイトはすべて、管理ネットワークと vSAN ネットワークを通じて通信を行います。両方のデータ サイトにある仮想マシンは、共通の仮想マシン ネットワークを通じて通信します。

vSAN ストレッチ クラスタは、特定の基本ネットワーク要件を満たす必要があります。

- 管理ネットワークは、レイヤー 2 拡張ネットワークまたはレイヤー 3 ネットワークを使用して、3 つのすべてのサイトに接続する必要があります。
- vSAN ネットワークは、3 つのすべてのサイトに接続する必要があります。データ サイトと監視ホスト間でルーティングと接続は独立している必要があります。2 つのデータ サイトの間にレイヤー 2 拡張ネットワークを使用し、データ サイトと監視ホストの間にレイヤー 3 ネットワークを使用します。vSAN ネットワークは、3 つのすべてのサイトに接続する必要があります。データ サイトと監視ホスト間でルーティングと接続は独立している必要があります。2 つのデータ サイトの間にレイヤー 2 拡張ネットワークを使用し、データ サイトと監視ホストの間にレイヤー 3 ネットワークを使用します。
- 仮想マシン ネットワークは、データ サイトと接続する必要がありますが、監視ホストと接続する必要はありません。データ サイト間ではレイヤー 2 拡張ネットワークまたはレイヤー 3 ネットワークを使用します。障害が発生した場合、仮想マシンにリモート サイトで機能する新しい IP アドレスは必要ありません。
- vMotion ネットワークは、データ サイトと接続する必要がありますが、監視ホストと接続する必要はありません。データ サイト間ではレイヤー 2 拡張またはレイヤー 3 ネットワークを使用します。

ESXi ホストでのスタティック ルートの使用

ESXi ホストで単一のデフォルト ゲートウェイを使用する場合、各 ESXi ホストに、単一のデフォルト ゲートウェイを持つデフォルト TCP/IP スタックが含まれます。デフォルト ルートは、通常、管理ネットワーク TCP/IP スタックに関連付けられます。

管理ネットワークと vSAN ネットワークは互いに隔離されている場合があります。たとえば、管理ネットワークは物理 NIC 0 の vmk0 を使用し、vSAN ネットワークは物理 NIC 1 の vmk2 を使用する場合があります。つまり、2 つの異なる TCP/IP スタックに対応する別々のネットワーク アダプタを使用します。この構成は、vSAN ネットワークにデフォルト ゲートウェイがないことを意味します。

vSAN ネットワークはレイヤー 2 ブロードキャスト ドメイン（たとえば 172.10.0.0）の 2 つのデータ サイトに拡張され、監視ホストは別のブロードキャスト ドメイン（たとえば 172.30.0.0）にあるとします。データ サイト上の VMkernel アダプタが監視ホスト上の vSAN ネットワークへ接続すると、ESXi ホストのデフォルト ゲートウェイが管理ネットワークと関連付けられているために、接続が失敗します。管理ネットワークから vSAN ネットワークへのルートはありません。

この問題を解決するために、スタティック ルートを使用できます。特定のネットワークに到達するためにどのパスをたどるのかを示す新しいルーティング エントリを定義します。ストレッチ クラスタの vSAN ネットワークについては、スタティック ルートを追加して、すべてのホストにわたって適切な通信を確保することができます。

たとえば、各データ サイトのホストにスタティック ルートを追加して、172.30.0.0 の監視ネットワークに到達する要求が、172.10.0.0 インターフェイスを通じてルーティングされるようにできます。また、データ サイトの 172.10.0.0 ネットワークに到達する要求が、172.30.0.0 インターフェイスを通じてルーティングできるように、スタティック ルートを監視ホストに追加します。

注： スタティック ルートを使用する場合は、新しく追加される ESXi ホストがクラスタ全体で通信できるようにする前に、それらのホストに対応するスタティック ルートをいずれかのサイトに手動で追加する必要があります。監視ホストを置き換える場合は、スタティック ルートの構成を更新する必要があります。

スタティック ルートを追加するには、`esxcli network ip route` コマンドを使用します。

クイックスタートを使用したストレッチ クラスタの構成

クイックスタート ワークフローを使用すると、ストレッチ クラスタを迅速に構成できます。

vSphere Client にクラスタを作成する際、クイックスタート ワークフローが表示されます。クイックスタートを使用して、ホストの追加やディスクの要求など、基本的な構成タスクを実行できます。

前提条件

- 監視ホストとして使用するクラスタ外部のホストをデプロイします。
- ホストで ESXi 6.0 Update 2 以降が実行されていることを確認します。
- クラスタ内の ESXi ホストに既存の vSAN またはネットワーク構成がないことを確認します。

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 [クラスタの基本] で、[編集] をクリックして、クラスタの基本ウィザードを開きます。

a クラスタ名を入力します。

b vSAN スライダを有効にします。

DRS または vSphere HA など、他の機能も有効にできます。

c [終了] をクリックします。

4 [ホストの追加] で、[追加] 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。

5 [クラスタの構成] で、[構成] 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、Distributed Switch、ポート グループ、物理アダプタなどのネットワーク設定を入力します。

- [Distributed Switch] セクションで、ドロップダウン メニューから構成する Distributed Switch の数を入力します。各 Distributed Switch の名前を入力します。[既存の使用] をクリックし、既存の Distributed Switch を選択します。

  選択した物理アダプタが、ホスト全体で同じ名前を持つ標準仮想スイッチに接続されている場合、標準スイッチは Distributed Switch に移行されます。選択した物理アダプタが未使用の場合、標準スイッチは Distributed Switch に移行されます。

  ネットワーク リソース コントロールを有効にして、バージョン 3 に設定します。Distributed Switch とネットワーク リソース コントロール バージョン 2 は併用できません。

- [ポート グループ] セクションで、vMotion に使用する Distributed Switch と、vSAN ネットワークに使用する Distributed Switch を選択します。

- [物理アダプタ] セクションで、各物理ネットワーク アダプタの Distributed Switch を選択します。各 Distributed Switch は、1 つ以上の物理アダプタに割り当てる必要があります。

  物理 NIC と Distributed Switch のこのマッピングは、クラスタ内のすべてのホストに適用されます。既存の Distributed Switch を使用する場合は、物理アダプタの選択内容が Distributed Switch のマッピングと一致することがあります。

b [vMotion トラフィック] ページで、vMotion トラフィックの IP アドレス情報を入力します。

c [ストレージ トラフィック] 画面で、ストレージ トラフィックの IP アドレス情報を入力します。

d [詳細オプション] ページで、DRS、HA、vSAN、ホスト オプション、EVC などのクラスタ設定情報を入力します。

[vSAN オプション] セクションで、[デプロイ タイプ] としてストレッチ クラスタを選択します。

e [ディスクの要求] ページで、キャッシュとキャパシティに使用する各ホスト上のディスクを選択します。

f [フォールト ドメインの作成] 画面で、優先サイトとセカンダリ サイト内のホストのフォールト ドメインを定義します。

フォルト ドメインの詳細については、『*VMware vSAN の管理*』の「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。

g [監視ホストの選択] ページで、監視ホストとして使用するホストを選択します。監視ホストはストレッチ クラスタに属することはできませんが、vSAN データ トラフィック用に構成された VMkernel アダプタを 1 つのみ配置することができます。

監視ホストを構成する前に、ホストが空でコンポーネントが含まれていないことを確認します。

h [監視ホストのディスクの要求] ページで、キャッシュとキャパシティに使用する監視ホスト上のディスクを選択します。

i [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。

次のステップ

vCenter Server からクラスタを管理することができます。

ホストをクラスタに追加し、クイックスタートを使用して構成を変更できます。また、vSphere Client を使用して構成を手動で変更することもできます。

vSAN ストレッチ クラスタの手動構成

2 つの地理的な場所またはサイトにまたがる vSAN ストレッチ クラスタを構成します。

前提条件

- 優先サイト用、セカンダリ サイト用、監視用と、少なくとも 3 つのホストがあることを確認します。
- ストレッチ クラスタの監視ホストとして機能するように 1 つのホストを構成していることを確認します。 監視ホストが vSAN クラスタの一部ではなく、vSAN データ トラフィックに対して 1 つの VMkernel アダプタのみが構成されていることを確認します。
- 監視ホストが空であり、コンポーネントが含まれていないことを確認します。 既存の vSAN ホストを監視ホストとして構成するには、最初にホストからすべてのデータを退避させて、ディスク グループを削除します。

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、[フォールト ドメイン] をクリックします。
4. ストレッチ クラスタの [構成] ボタンをクリックしてストレッチ クラスタの構成ウィザードを開始します。
5. セカンダリ ドメインに割り当てるホストまたはフォールト ドメインを選択し、[>>] をクリックします。

   [優先フォールト ドメイン] の下にリストされているホストは優先サイトにあります。
6. [次へ] をクリックします。
7. vSAN ストレッチ クラスタのメンバーでない監視ホストを選択し、[次へ] をクリックします。

8 監視ホストでストレージ デバイスを要求して、[次へ] をクリックします。

監視ホストでストレージ デバイスを要求します。キャッシュ層用にフラッシュ デバイスを 1 個選択し、キャパシティ層用に 1 個以上のデバイスを選択します。

9 [設定内容の確認] ページで構成を確認し、[終了] をクリックします。

優先フォールト ドメインの変更

セカンダリ サイトを優先サイトとして構成できます。現在の優先サイトはセカンダリ サイトになります。

注： [データのローカリティ] = [優先] のオブジェクトは常に優先フォールト ドメインに移動します。[データのローカリティ] = [セカンダリ] のオブジェクトは常にセカンダリ フォールト ドメインに移動します。優先ドメインをセカンダリに、セカンダリ ドメインを優先に変更すると、これらのオブジェクトはサイト間を移動します。このアクションにより、再同期アクティビティが増える可能性があります。不要な再同期を避けるには、優先ドメインとセカンダリ ドメインをスワップする前に、[データのローカリティ] の設定を [なし] に変更します。

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、[フォールト ドメイン] をクリックします。

オプション	説明
vSphere Client	a セカンダリ フォールト ドメインを選択し、[優先フォールト ドメインの変更] アイコンをクリックします。
vSphere Web Client	a セカンダリ フォールト ドメインを選択し、[フォールト ドメインをストレッチ クラスタ用に優先としてマーク] アイコンをクリックします。

4 [はい] または [適用] をクリックして確定します。

選択したフォールト ドメインが優先フォールト ドメインとしてマークされます。

監視ホストの変更

vSAN ストレッチ クラスタの監視ホストを変更できます。

vSAN ストレッチ クラスタで監視ホストとして使用される ESXi ホストを変更します。

前提条件

監視ホストが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 で [フォルート ドメイン] をクリックします。

オプション	説明
vSphere Client	a [変更] ボタンをクリックします。[監視ホストの変更] ウィザードが開きます。 b 監視ホストとして使用する新しいホストを選択して、[次へ] をクリックします。 c 新しい監視ホストでディスクを要求して、[次へ] をクリックします。
vSphere Web Client	a [監視ホストの変更] ボタンをクリックします。 b 監視ホストとして使用する新しいホストを選択して、[次へ] をクリックします。 c 新しい監視ホストでディスクを要求して、[次へ] をクリックします。

4 [設定内容の確認] ページで設定を確認し、[終了] をクリックします。

vSAN 監視アプライアンスのデプロイ

ストレッチ クラスタなどの特定の vSAN 構成には、監視ホストが必要です。監視ホストとして専用の物理 ESXi ホストを使用するのではなく、vSAN 監視アプライアンスをデプロイできます。アプライアンスは、ESXi を実行する事前構成された仮想マシンで、OVA ファイルとして配布されます。

汎用 ESXi ホストとは異なり、監視アプライアンスは仮想マシンを実行しません。監視アプライアンスは vSAN 監視として機能することのみを目的としています。

vSAN 監視アプライアンスをデプロイおよび構成するためのワークフローには、次のプロセスが含まれます。

vSAN 監視アプライアンスをデプロイする場合は、vSAN ストレッチ クラスタでサポートされている仮想マシンの予定台数を設定する必要があります。以下のいずれかのオプションを選択します。

- 極小（10 台以下の仮想マシン）
- 中規模（500 台までの仮想マシン）
- 大規模（500 台を超える仮想マシン）

また、vSAN 監視アプライアンス用のデータストアを選択する必要があります。監視アプライアンスには、vSAN ストレッチ クラスタのデータストアとは異なるデータストアを使用する必要があります。

1 VMware Web サイトからアプライアンスをダウンロードします。

2 アプライアンスを vSAN ホストまたはクラスタにデプロイします。詳細については、『vSphere の仮想マシン管理』ドキュメントの「OVF テンプレートのデプロイ」を参照してください。

3 監視アプライアンス上に vSAN ネットワークを構成します。

4 監視アプライアンス上に管理ネットワークを構成します。

5 アプライアンスを監視 ESXi ホストとして vCenter Server に追加します。必ずホスト上に vSAN VMkernel インターフェイスを構成してください。

監視アプライアンスの vSAN ネットワークの設定

vSAN 監視アプライアンスには、2 つの事前構成済みのネットワーク アダプタが含まれます。アプライアンスが vSAN ネットワークに接続できるようにするには、2 番目のアダプタの構成を変更する必要があります。

手順

1 監視ホストを含む仮想アプライアンスに移動します。

2 アプライアンスを右クリックして、[設定の編集] を選択します。

3 [仮想ハードウェア] タブで、2 番目のネットワーク アダプタを展開します。

4 ドロップダウン メニューから vSAN ポート グループを選択し、[OK] をクリックします。

管理ネットワークの構成

ネットワーク上で接続できるように、監視アプライアンスを構成します。

デフォルトでは、ネットワークに DHCP サーバが含まれている場合、アプライアンスはネットワーク パラメータを自動的に取得できます。含まれていない場合は、適切な設定を構成する必要があります。

手順

1 監視アプライアンスをパワーオンして、そのコンソールを開きます。

アプライアンスが ESXi ホストであるため、ダイレクト コンソール ユーザー インターフェイス (DCUI) が表示されます。

2 F2 キーを押して、[ネットワーク アダプタ] ページに移動します。

3 [ネットワーク アダプタ] ページで、転送用に少なくとも 1 つの vmnic が選択されていることを確認します。

4 管理ネットワーク用の IPv4 パラメータを構成します。

a [IPv4 構成] セクションに移動し、デフォルトの DHCP 設定を [固定] に変更します。

b 次の設定を入力します。

- IP アドレス
- サブネット マスク
- デフォルト ゲートウェイ

5 DNS パラメータを構成します。

- プライマリ DNS サーバ
- 代替 DNS サーバ
- ホスト名

監視トラフィック用のネットワーク インターフェイスの構成

2 ホスト構成の vSAN クラスタやストレッチ クラスタで、データ トラフィックと監視トラフィックを分離することができます。

vSAN のデータ トラフィックは、低遅延で高いバンド幅のリンクを必要とします。監視トラフィックの場合、高遅延、低バンド幅、かつルーティング可能なリンクを使用できます。データ トラフィックを監視トラフィックから分離するために、vSAN の監視トラフィック専用の VMkernel ネットワーク アダプタを構成できます。

vSAN ストレッチ クラスタで vSAN データ トラフィックを配信するために、直接ネットワーク交差接続のサポートを追加できます。監視トラフィック用に、別のネットワーク接続を構成できます。クラスタの各データ ホストで、管理 VMkernel ネットワーク アダプタを構成して、ここでも監視トラフィックを伝送できるようにします。監視ホスト上に監視トラフィック タイプを構成しないでください。

注： ネットワーク アドレス変換 (NAT) は、vSAN データ ホストと監視ホスト間ではサポートされていません。

前提条件

- データ サイトから監視トラフィックへの接続に、1,000 vSAN コンポーネントあたり 2 Mbps の最小バンド幅があることを確認します。
- 以下の遅延についての要件を確認します。
  - 2 ホスト構成の vSAN クラスタでは、RTT を 500 ミリ秒未満にする必要があります。
  - サイトあたりのホスト数が 11 台未満のストレッチ クラスタでは、RTT を 200 ミリ秒未満にする必要があります。
  - サイトあたりのホスト数が 11 台以上のストレッチ クラスタでは、RTT を 100 ミリ秒未満にする必要があります。
- vSAN データ接続が、次の要件を満たしていることを確認します。
  - 2 ホスト構成の vSAN クラスタで直接接続されているホストの場合、ホスト間で 10 Gbps の直接接続を使用します。ハイブリッド クラスタでは、ホスト間で 1 Gbps クロス接続も使用できます。
  - スイッチ インフラストラクチャに接続されたホストの場合、10 Gbps の共有の接続（オール フラッシュ クラスタには必須）か、1 Gbps の専用の接続を使用します。
- データ トラフィックと監視トラフィックで同じ IP バージョンが使用されていることを確認します。

手順

1. ESXi ホストへの SSH 接続を開きます。
2. `esxcli network ip interface list` コマンドを使用して、管理トラフィックに使用する VMkernel ネットワーク アダプタを決定します。

   例：

```
esxcli network  ip interface list
[vmk0]
   Name: vmk0
   MAC Address: e4:11:5b:11:8c:16
   Enabled: true
   Portset: vSwitch0
   Portgroup: [Management Network]
   Netstack Instance: defaultTcpipStack
   VDS Name: N/A
   VDS UUID: N/A
   VDS Port: N/A
   VDS Connection: -1
   Opaque Network ID: N/A
   Opaque Network Type: N/A
```

```
   External ID: N/A
   MTU: 1500
   TSO MSS: 65535
   Port ID: 33554437

[vmk1]
   Name: vmk1
   MAC Address: 00:50:56:6a:3a:74
   Enabled: true
   Portset: vSwitch1
   Portgroup: [vsandata]
   Netstack Instance: defaultTcpipStack
  VDS Name: N/A
   VDS UUID: N/A
   VDS Port: N/A
   VDS Connection: -1
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 9000
   TSO MSS: 65535
   Port ID: 50331660
```

注： 後方互換性のため、マルチキャスト情報が含まれます。vSAN 6.6 以降のリリースでは、マルチキャストは必要ありません。

3 `esxcli vsan network ip add` コマンドを使用して、監視トラフィックをサポートするように管理 VMkernel ネットワーク アダプタを構成します。

```
esxcli vsan network ip add -i vmkx -T witness
```

4 `esxcli vsan network list` コマンドを使用して、新しいネットワーク構成を確認します。

例：

```
esxcli vsan network list
Interface
   VmkNic Name: [vmk0]
   IP Protocol: IP
   Interface UUID: 8cf3ec57-c9ea-148b-56e1-a0369f56dcc0
   Agent Group Multicast Address: 224.2.3.4
   Agent Group IPv6 Multicast Address: ff19::2:3:4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group IPv6 Multicast Address: ff19::1:2:3
   Master Group Multicast Port: 12345
   Host Unicast Channel Bound Port: 12321
   Multicast TTL: 5
   Traffic Type: [witness]

Interface
   VmkNic Name: [vmk1]
   IP Protocol: IP
   Interface UUID: 6df3ec57-4fb6-5722-da3d-a0369f56dcc0
```

```
Agent Group Multicast Address: 224.2.3.4
Agent Group IPv6 Multicast Address: ff19::2:3:4
Agent Group Multicast Port: 23451
Master Group Multicast Address: 224.1.2.3
Master Group IPv6 Multicast Address: ff19::1:2:3
Master Group Multicast Port: 12345
Host Unicast Channel Bound Port: 12321
Multicast TTL: 5
Traffic Type: [vsan]
```

結果

vSphere Client で、vSAN トラフィック用に管理 VMkernel ネットワーク インターフェイスが選択されていません。vSphere Client でインターフェイスを再度有効にしないでください。

ストレッチ クラスタの標準の vSAN クラスタへの変換

ストレッチ クラスタを廃止し、標準の vSAN クラスタに変換できます。

ストレッチ クラスタを無効にすると、監視ホストは削除されますが、フォルト ドメインの構成はそのまま残ります。監視ホストは使用できないため、仮想マシンのすべての監視コンポーネントが見つかりません。仮想マシンの完全な可用性を確保するには、クラスタ オブジェクトをただちに修復します。

手順

1 vSAN ストレッチ 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、[フォルト ドメイン] をクリックします。

4 ストレッチ クラスタを無効にします。

オプション	説明
vSphere Client	a [無効化] をクリックします。[監視ホストの削除] ダイアログが開きます。 b [削除] をクリックして確認します。
vSphere Web Client	a ストレッチ クラスタの [設定] ボタンをクリックします。ストレッチ クラスタの構成ウィザードが開きます。 b [無効化] をクリックし、[はい] をクリックして確認します。

5 フォルト ドメインの構成を削除します。

オプション	説明
vSphere Client	a フォルト ドメインを選択し、[アクション] > [削除] の順に選択します。[はい] をクリックして確認します。 b ほかのフォルト ドメインを選択し、[アクション] > [削除] の順に選択します。[はい] をクリックして確認します。
vSphere Web Client	a フォルト ドメインを選択し、[選択したフォルト ドメインを削除します] アイコンをクリックします。[はい] をクリックして確認します。 b 他のフォルト ドメインを選択し、[選択したフォルト ドメインを削除します] アイコンをクリックします。[はい] をクリックして確認します。

6 クラスタ内のオブジェクトを修復します。

a [監視] タブをクリックします。

b [vSAN] の下で、[健全性] をクリックし、[vSAN オブジェクトの健全性] をクリックします。

c [オブジェクトをただちに修復] をクリックします。

vSAN によりクラスタ内に監視コンポーネントが再作成されます。