vSphere Availability

Update 3

VMware vSphere 8.0
VMware ESXi 8.0
vCenter 8.0

vmware
by Broadcom

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

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

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

目次

vSphere Availability

『vSphere Availability』は、vSphere® High Availability (HA) と vSphere Fault Tolerance の設定方法など、ビジネスに継続性を与えるソリューションについて説明します。

VMware では、多様性の受け入れを尊重しています。お客様、パートナー企業、社内コミュニティとともにこの原則を推進することを目的として、多様性に配慮した言葉遣いでコンテンツを作成します。

対象読者

この情報は、vSphere HA およびフォールト トレランスのソリューションを使用してビジネスに継続性を与える立場の方を対象としています。本書の情報は、仮想マシン テクノロジーおよびデータセンター運用に精通した、経験の豊富な Windows または Linux システムの管理者向けです。

vSphere によるダウンタイムの最小化 1

ダウンタイムは計画的であるか否かにかかわらず、多大なコストが生じます。一方、より高いレベルの可用性を実現するための従来のソリューションはコストがかかり、実装が複雑で、管理が困難でした。

VMware のソフトウェアを使用すると、より簡単で安価に、重要なアプリケーションに対する高いレベルの可用性を実現できます。vSphere を使用すると、より簡単で安価に、高いレベルの可用性を実現できるだけでなく、すべてのアプリケーションに提供される可用性の基準となるレベルが向上します。vSphere を使用すると、ユーザーは次のことが可能になります。

- ハードウェア、オペレーティング システム、およびアプリケーションに関わらず、高可用性を実現できます。
- 一般的なメンテナンス操作のための計画的ダウンタイムを減らすことができます。
- 障害が発生した場合に、自動的にリカバリできます。

vSphere では、計画的なダウンタイムを減らす、計画外のダウンタイムを回避する、停止状態から迅速に回復するなどが可能です。

次のトピックを参照してください。

- vSphere による計画的ダウンタイムの短縮
- vSphere による計画外のダウンタイムの防止
- vSphere HA が提供する、システム停止からの迅速なリカバリ
- vSphere Fault Tolerance が提供する継続的な可用性
- vCenter High Availability を使用した vCenter Server の保護
- VMware Service Lifecycle Manager での vCenter Server の保護

vSphere による計画的ダウンタイムの短縮

計画的ダウンタイムは一般に、データセンターのダウンタイムの 80% 以上を占めます。ハードウェアのメンテナンス、サーバの移行、ファームウェアの更新はすべて、物理サーバのダウンタイムを必要とします。このダウンタイムの影響を最小限にするために、組織は、不便でスケジュール設定が困難なダウンタイム用時間枠までメンテナンスを遅らせざるをえません。

vSphere では、組織は計画的ダウンタイムを大幅に短縮できます。vSphere 環境では、ダウンタイムやサービスの中断なしにワークロードを動的に別の物理サーバに移動できるため、アプリケーションとサービスのダウンタイムを必要とせずにサーバのメンテナンスを実行できます。vSphere を使用すると、組織は次のことができます。

- 一般的なメンテナンス操作のためのダウンタイムを排除できます。
- 計画的なメンテナンス用時間枠をなくすことができます。
- ユーザーの操作やサービスを中断せずに、いつでもメンテナンスを行うことができます。

vSphere における vSphere vMotion® 機能と Storage vMotion 機能により、組織は計画的ダウンタイムを短縮できます。VMware 環境ではサービスの中断なしに、ワークロードを別の物理サーバまたは別の基盤ストレージへ動的に移動できるからです。システム管理者は、不便なメンテナンス用時間枠のスケジュール設定を強制されずに、迅速かつ完全に透過的なメンテナンス操作を実行できます。

vSphere による計画外のダウンタイムの防止

実行中のアプリケーションに対して ESXi ホストが堅牢なプラットフォームを提供する一方で、組織も、ハードウェアやアプリケーションの障害により生じる計画外のダウンタイムから自分自身を守る必要があります。vSphere は、ユーザーが計画外のダウンタイムを防止する際に役立つ重要な機能を、データセンターのインフラストラクチャに組み込みます。

これらの vSphere の機能は仮想インフラストラクチャの一部であり、仮想マシン上で動作するオペレーティング システムやアプリケーションに対して透過的です。これらの機能は構成可能で、物理システム上のすべての仮想マシンで利用されるため、高可用性を提供する際のコストと複雑さが軽減されます。vSphere に組み込まれている可用性の主要な機能は、次のとおりです。

- 共有ストレージ。ファイバ チャネル SAN や iSCSI SAN、または NAS などの共有ストレージに仮想マシンのファイルを格納することで、単一点障害を除去します。SAN のミラーリングおよびレプリケーション機能を使用して、ディザスタ リカバリ サイトで仮想ディスクの更新コピーを維持できます。
- ネットワーク インターフェイス チーミング。個々のネットワーク カード障害に対応します。
- ストレージのマルチパス機能。ストレージのパス障害に対応します。

これらの機能に加え、vSphere HA 機能とフォールト トレランス機能は、システム停止からの迅速なリカバリと継続的な可用性をそれぞれが提供することで、計画外のダウンタイムを最小限にするか、排除することができます。

vSphere HA が提供する、システム停止からの迅速なリカバリ

vSphere HA は、クラスタとして構成されている複数の ESXi ホストを活用して、仮想マシンで実行中のアプリケーションに、システム停止からの迅速なリカバリと、費用対効果に優れた高可用性を提供します。

vSphere HA は、次の方法でアプリケーションの可用性が向上します。

- サーバ障害に対しては、仮想マシンをクラスタ内のほかのホストで再起動することで向上します。
- ゲスト OS 障害によるアプリケーション障害に対しては、仮想マシンを継続的に監視し、障害が検出された際に仮想マシンをリセットすることで向上します。
- まだデータストアにアクセスできる他のホストで、影響を受けている仮想マシンを再起動して、データストアのアクセシビリティ障害から保護します。

- 管理ネットワークまたは vSAN ネットワークでホストが隔離されると、再起動することによって仮想マシンをネットワーク隔離から保護します。この保護は、ネットワークがパーティション分割されている場合でも行われます。

ほかのクラスタリング ソリューションとは異なり、vSphere HA はインフラストラクチャを提供して、全ワークロードをそれにより保護できるようにします。

- アプリケーションまたは仮想マシンに特別なソフトウェアをインストールする必要はありません。vSphere HA が全ワークロードを保護するからです。vSphere HA を構成したあとは、新しい仮想マシンを保護するための操作は不要です。自動的に保護されます。
- vSphere HA を vSphere DRS（Distributed Resource Scheduler）と組み合わせると、障害に対する保護と、クラスタ内の複数のホストにわたるロード バランシング機能を提供できます。

vSphere HA には、従来のフェイルオーバー ソリューションと比べていくつかのメリットがあります。

最小限のセットアップ

vSphere HA クラスタのセットアップ後、追加の構成を行わずにクラスタ内のすべての仮想マシンがフェイルオーバーのサポートを受けます。

ハードウェアのコストとセットアップの削減

仮想マシンは、移動可能なアプリケーション用コンテナとして機能し、ホスト間で移動できます。システム管理者は、複数のマシン上の重複する構成を回避できます。vSphere HA を使用する場合は、vSphere HA で保護したい数のホストをフェイルオーバーするのに十分なリソースがなければなりません。ただし、VMware vCenter Server® システムは自動的にリソースを管理し、クラスタを構成します。

アプリケーションの可用性の向上

仮想マシン内で実行されるどのアプリケーションも、可用性が向上します。仮想マシンはハードウェア障害から復旧できるため、アプリケーション自体がクラスタリングされたアプリケーションでなくても、コンピューティング要件を加えることなく、ブート時に起動するすべてのアプリケーションの可用性が向上します。VMware Tools のハートビートを監視して応答し、応答しない仮想マシンを再起動することで、ゲスト OS のクラッシュから保護できます。

DRS と vMotion の統合

ホストに障害が起き、仮想マシンがほかのホスト上で再起動された場合、DRS は、バランスのとれたリソース割り当てを行うために、移行の推奨を提供するか、仮想マシンを移行できます。移行元ホストと移行先ホストのいずれか一方または両方に障害が起きた場合、vSphere HA が障害からの復旧に役立ちます。

vSphere Fault Tolerance が提供する継続的な可用性

vSphere HA は、ホスト障害時に仮想マシンを再起動することにより、仮想マシンに対して基本レベルの保護機能を提供します。vSphere フォールト トレランスは、より高度な可用性を提供します。ユーザーはデータ、トランザクション、または接続を失うことなくホスト障害から仮想マシンを保護できます。

フォールト トレランスは、仮想マシンの命令実行時のどの時点においても、プライマリおよびセカンダリ仮想マシンの状態を必ず同一にすることで継続的な可用性を実現します。

プライマリ仮想マシンを実行しているホスト、またはセカンダリ仮想マシンを実行しているホストのどちらかで障害が発生すると、直ちに透過的なフェイルオーバーが発生します。ネットワーク接続や処理中のトランザクションを失うことなく、正常機能している ESXi ホストがシームレスにプライマリ仮想マシンのホストになります。透過的なフェイルオーバーでは、データが失われず、ネットワーク接続が維持されます。透過的なフェイルオーバーの発生後は、新しいセカンダリ仮想マシンが再作成され、冗長性が再確立されます。プロセス全体は透過的で完全に自動的に行われ、vCenter Server が利用不可能な場合でも実行されます。

vCenter High Availability を使用した vCenter Server の保護

vCenter High Availability (vCenter HA) は、ホストとハードウェアの障害に加え、vCenter Server アプリケーションの障害からの保護にも対応します。vCenter HA は、アクティブからパッシブへの自動フェイルオーバーを使用することで、ダウンタイムを最小限に抑えた高可用性に対応します。

vCenter HA の構成は、vSphere Client から行います。構成ウィザードには、次のオプションが用意されています。

オプション	説明
自動	[自動] を選択した場合、パッシブ ノードと監視ノードにアクティブ ノードのクローンが作成され、それらのノードが自動的に構成されます。 ご利用の環境が次の要件を満たしている場合に、このオプションを選択できます。 ■ アクティブ ノードになる vCenter Server が、それ自身の ESXi ホストと仮想マシンを管理している。この構成は、自己管理型の vCenter Server と呼ばれることがあります。
手動	[手動] を選択した場合は、より柔軟な構成が可能になります。ご利用の環境がハードウェアとソフトウェアの要件を満たしていれば、このオプションを選択できます。 このオプションを選択した場合、パッシブ ノードと監視ノードに対し、手動でアクティブ ノードのクローンを作成する必要があります。一部のネットワーク構成についても自分で行う必要があります。

VMware Service Lifecycle Manager での vCenter Server の保護

VMware Service Lifecycle Manager によって vCenter Server の可用性が実現します。

vCenter サービスが失敗した場合、そのサービスは、VMware Service Lifecycle Manager によって再起動されます。VMware Service Lifecycle Manager は、サービスの健全性を監視し、障害検出時に事前構成された修正アクションを実行します。障害の修正が複数回試行された場合は、サービスが再起動されることはありません。

vSphere HA クラスタの作成と使用

2

vSphere HA クラスタによって、ESXi ホストの集合が 1 つのグループとして機能するようになるため、ESXi ホストがそれぞれ個別に機能する場合に比べて、仮想マシンの高い可用性を実現できます。新しい vSphere HA クラスタの作成と使用を計画する場合、選択したオプションによって、ホストまたは仮想マシンの障害に対するクラスタの対処方法が異なります。

vSphere HA クラスタを作成する前に、vSphere HA がホスト障害を確認して切り分け、対処する方法を知る必要があります。また、アドミッション コントロールの動作を知り、フェイルオーバーに関する実際のニーズに適したポリシーを選択できるようにします。クラスタの作成後は、詳細オプションを使用して動作をカスタマイズし、推奨ベスト プラクティスに従ってパフォーマンスを最適化できます。

注： vSphere HA を使用しようとしたとき、エラー メッセージが出ることがあります。vSphere HA に関するエラー メッセージについては、次の VMware ナレッジ ベースを参照してください。http://kb.vmware.com/kb/1033634

次のトピックを参照してください。

- vSphere HA の動作
- vSphere HA のアドミッション コントロール
- vSphere HA の相互運用性
- vSphere HA クラスタの作成
- vSphere の可用性設定の構成
- VMware vSphere® High Availability クラスタのベスト プラクティス
- HA VIB の動作の変更

vSphere HA の動作

vSphere HA は、仮想マシンとそれが配置されたホストをクラスタにプールすることで、仮想マシンに高可用性を提供します。クラスタ内のホストは監視され、障害発生時には、その故障したホスト上の仮想マシンが別のホスト上で再起動されます。

vSphere HA クラスタを作成すると、1 台のホストがプライマリ ホストとして自動的に選択されます。プライマリ ホストは vCenter Server と通信し、すべての保護された仮想マシンの状態とセカンダリ ホストの状態を監視します。ホスト障害には複数のタイプがあり、プライマリ ホストはその障害を検出して適切な処置を行う必要があります。プライマリ ホストは、障害のあるホストと、ネットワーク パーティションにあるホストやネットワークから隔離されたホストを区別できる必要があります。プライマリ ホストは、ネットワークとデータストア ハートビートを使用して障害の種類を確認します。

 (vSphere HA クラスタ)

プライマリ ホストとセカンダリ ホスト

ホストを vSphere HA クラスタに追加すると、そのホストにエージェントがアップロードされ、クラスタ内の他のエージェントと通信するように構成されます。クラスタ内の各ホストは、プライマリ ホストまたはセカンダリ ホストとして機能します。

クラスタ用に vSphere HA が有効にされると、アクティブなすべてのホスト（スタンバイでないか、メンテナンス モードでないか、切断されていないホスト）がクラスタのプライマリ ホスト候補になります。マウントしているデータストア数が最大のホストがマスタ候補として有利です。一般にクラスタごとにプライマリ ホストは 1 台だけで、残りはすべてセカンダリ ホストになります。プライマリ ホストは、障害が発生したり、シャットダウンされたり、スタンバイ モードになったり、クラスタから取り除かれたりした場合、選び直されます。

クラスタのプライマリ ホストには、いくつかの役割があります。

- セカンダリ ホストの状態を監視する。セカンダリ ホストに障害が発生した場合や接続できなくなった場合、プライマリ ホストはどの仮想マシンを再起動する必要があるかを特定します。
- 保護対象の仮想マシンの電源状態を監視する。ある仮想マシンに障害が発生した場合、プライマリ ホストはその仮想マシンを確実に再起動させます。ローカルの配置エンジンを使用して、どのホストで再起動するかもプライマリ ホストが決定します。
- クラスタ ホストと保護対象の仮想マシンのリストの管理。
- vCenter Server の管理インターフェイスとして機能し、クラスタの健全性状態をレポートします。

セカンダリ ホストは、主として仮想マシンをローカルに実行し、ランタイム状態を監視し、状態の更新をプライマリ ホストにレポートすることでクラスタに貢献します。プライマリ ホストも仮想マシンを実行し、監視できます。セカンダリ ホストとプライマリ ホストの両方とも、仮想マシンとアプリケーションの監視機能を実装しています。

プライマリ ホストにより実行される機能の 1 つは、保護された仮想マシンの組織的な再起動です。ユーザー アクションに対応して vCenter Server によって仮想マシンのパワー状態がパワーオフからパワーオンに変わったことが確認されると、仮想マシンはプライマリ ホストによって保護されます。プライマリ ホストは保護された仮想マシンのリストをクラスタのデータストアに保持します。新しく選択されたプライマリ ホストは、この情報を使用してどの仮想マシンを保護するか決定します。

注： ホストをクラスタから切断する場合、そのホストに登録されている仮想マシンは、vSphere HA の保護対象ではなくなります。

ホスト障害のタイプ

VMware vSphere® High Availability クラスタのプライマリ ホストは、セカンダリ ホストの障害検出を行います。検出された障害のタイプによっては、ホストで実行中の仮想マシンのフェイルオーバーが必要になる場合があります。

vSphere HA クラスタでは、3 種類のホスト障害が検出されます。

- 障害。ホストが機能を停止する。
- 隔離。ホストがネットワーク隔離される。
- パーティション。ホストがプライマリ ホストとの接続を失う。

プライマリ ホストは、クラスタ内のセカンダリ ホストの稼動状態を監視します。ネットワーク ハートビートを毎秒交換することで、通信を行います。セカンダリ ホストからのハートビートの受信が停止すると、プライマリ ホストはホストの稼動状態を確認してから障害を宣言します。プライマリ ホストは、セカンダリ ホストがデータストアの 1 つとハートビートを交換しているかどうかを調べて稼動状態を確認します。 データストア ハートビート を参照してください。また、ホストの管理 IP アドレスに送信された ICMP ping に反応するかどうかも確認します。

プライマリ ホストが、セカンダリ ホスト上のエージェントと直接通信できない場合、セカンダリ ホストは ICMP ping に応答しません。エージェントがハートビートを送信しないと、そのエージェントで障害が発生したと見なされます。このホストの仮想マシンは、代わりのホスト上で再起動されます。このようなセカンダリ ホストがデータストアとハートビートを交換している場合、プライマリ ホストは、セカンダリ ホストがネットワーク パーティション分割状態、またはネットワーク隔離の状態にあると見なします。このため、プライマリ ホストはホストとその仮想マシンの監視を続行します。 ネットワーク パーティション を参照してください。

ホストのネットワークが隔離されるのは、ホストがまだ実行中にも関わらず、管理ネットワーク上で vSphere HA エージェントからのトラフィックを確認できない場合です。ホストがこのトラフィックを確認できなくなった場合は、クラスタの隔離アドレスに ping を試みます。この ping も失敗した場合、ホストはネットワークからの隔離を宣言します。

プライマリ ホストは、隔離されているホスト上で実行中の仮想マシンを監視します。プライマリ ホストで仮想マシンのパワーオフが検出され、プライマリ ホストがその仮想マシンを管理している場合は、それらの仮想マシンを再起動します。

注： ネットワークのインフラストラクチャを冗長にして、少なくとも 1 つのネットワーク パスを常に使用できるようにしておくと、ホストのネットワーク隔離が発生する確率が少なくなります。

Proactive HA の障害

Proactive HA の障害は、ホスト コンポーネントに障害が発生し、その結果冗長性が失われたり、致命的ではない障害が発生した場合に起こります。ただし、ホスト上の仮想マシンの機能にはまだ影響が及んでいません。たとえば、ホストの電源で障害が発生したものの、その他の電源を利用できる場合などは、Proactive HA の障害と言えます。

Proactive HA の障害が発生した場合は、vSphere Client の [vSphere の可用性] セクションで、修正アクションを自動的に実行できます。影響を受けるホスト上の仮想マシンは、他のホストに退避させることが可能で、ホスト自体は検疫モードまたはメンテナンス モードになります。

注： Proactive HA の障害の監視を行うには、クラスタで vSphere DRS を使用する必要があります。

ホスト問題に対する対応の決定

ホストに障害が発生してホストの仮想マシンを再起動する必要がある場合、仮想マシン再起動の優先順位設定で、仮想マシンが起動する順序を制御できます。また、ホスト隔離時の対応設定を使用して、ホストがほかのホストとの管理ネットワークの接続が失われた場合の vSphere HA の対応を構成することもできます。障害発生後に vSphere HA が仮想マシンを再起動するとき、その他の要素も考慮されます。

ホストの障害または隔離時に、次の設定がクラスタ内のすべての仮想マシンに適用されます。特定の仮想マシンに対して例外を設定することも可能です。個々の仮想マシンのカスタマイズ を参照してください。

ホストの隔離時の対応

ホスト隔離時の対応で、vSphere HA クラスタ内のホストが管理ネットワークに接続できなくなったものの、実行が継続されている場合の対応を決定します。隔離時の対応を使用して、隔離状態にあるホストで実行されている仮想マシンを vSphere HA でパワーオフし、隔離状態にないホストで再起動することができます。ホスト隔離時の対応では、ホスト監視ステータスを有効にする必要があります。ホスト監視ステータスが無効になっていると、ホスト隔離時の対応もサスペンドされます。ホストは、他のホストで実行中のエージェントと通信できず、隔離アドレスに ping できないときに、自身が隔離されていると判断します。その後、ホストは隔離時の対応を実行します。仮想マシンをパワーオフして再起動、または仮想マシンをシャットダウンして再起動するという対応です。個々の仮想マシンのこのプロパティはカスタマイズできます。

注： 仮想マシンで再起動の優先順位設定が無効になっていると、ホスト隔離時の対応は行われません。

仮想マシンをシャットダウンして再起動する設定を使用するには、仮想マシンのゲスト OS に VMware Tools をインストールする必要があります。仮想マシンをシャットダウンすることには、仮想マシンの状態を保存できるというメリットがあります。ディスクへの最新の変更がフラッシュされず、トランザクションがコミットされないため、仮想マシンのシャットダウンはパワーオフよりも優れています。シャットダウン途中の仮想マシンは、シャットダウンが完了するまでフェイルオーバーに時間がかかります。300 秒以内または詳細オプション `das.isolationshutdowntimeout` で指定した時間以内にシャットダウンしない仮想マシンは、パワーオフされます。

vSphere HA クラスタを作成したあとで、特定の仮想マシンの再起動優先順位および隔離時の対応についてデフォルトのクラスタ設定をオーバーライドできます。このようなオーバーライドは、特別なタスクで使用される仮想マシンでは非常に便利です。たとえば、DNS や DHCP などのインフラストラクチャ サービスを提供する仮想マシンは、クラスタ内のほかの仮想マシンより前にパワーオンする必要があることがあります。

プライマリ ホストからホストが隔離されるかパーティション化され、プライマリ ホストがハートビート データストアを使用してホストと通信できなくなると、仮想マシンが「スプリット ブレイン」状態になることがあります。この場合、プライマリ ホストはホストが活動中かどうかを判断できないため、ホストが非活動であると宣言します。その後プライマリ ホストは、隔離されているホストまたはパーティション化されているホストで実行されている仮想マシンの再起動を試みます。仮想マシンが隔離/パーティション化されているホスト上で実行されていて、そのホストが隔離されたかパーティション化されたときにそのホストが仮想マシンのデータストアにアクセスできなくなった場合、この再起動の試行は成功します。この後、仮想マシンのインスタンスが 2 つ存在するため、スプリット ブレイン状態が発生します。ただし、1 つのインスタンスのみが仮想マシンの仮想ディスクを読み書きできます。仮想マシンのコンポーネント保護を使用することにより、このスプリット ブレイン状態を防ぐことができます。積極的設定で VMCP を有効にすると、VMCP は、パワーオンされた仮想マシンがデータストアにアクセスできるかどうかを監視し、データストアにアクセスできない仮想マシンをシャットダウンします。

この状況から回復するため、ESXi は、ディスク ロックを失った仮想マシンについて、ホストがいつ隔離状態から離脱してディスク ロックを再取得できなくなったかという問い合わせを生成します。vSphere HA は自動的にこの問い合わせに応答し、ディスク ロックを失った仮想マシンのインスタンスをパワーオフし、ディスク ロックを保持するインスタンスをそのままにします。

仮想マシンの依存関係

仮想マシンのグループ間で依存関係を作成できます。これを行うには、まず、vSphere Client でクラスタの [設定] タブに移動し、[仮想マシン/ホスト グループ] を選択して、仮想マシン グループを作成する必要があります。グループを作成したら、[仮想マシン/ホスト ルール] を表示し、[タイプ] ドロップダウン メニューで [仮想マシンから仮想マシン] を選択して、グループ間の再起動依存関係ルールを作成できます。これらのルールでは、指定した他の仮想マシン グループが先に準備完了の状態になるまで、特定の仮想マシン グループを再起動できないように指定できます。

仮想マシンの再起動に関して考慮される要素

障害発生後、クラスタのプライマリ ホストは障害の影響を受けた仮想マシンをパワーオンできるホストを特定して、障害の影響を受けた仮想マシンの再起動を試みます。このようなホストを選択する場合、プライマリ ホストはいくつもの要素を考慮します。

ファイルへのアクセス

仮想マシンが起動可能になるには、プライマリがネットワーク経由で通信できるアクティブなクラスタ ホストのいずれかから、仮想マシンのファイルにアクセスできる必要があります。

仮想マシンとホストとの互換性

アクセス可能なホストが複数存在する場合、仮想マシンは、そのうちの少なくとも 1 台と互換性を持っている必要があります。一連の仮想マシンの互換性には、必要となるすべての仮想マシンとホスト間のアフィニティ ルールの影響が反映されます。たとえばルールにより、2 台のホスト上でのみ仮想マシンの実行を許可している場合、それら 2 台のホストに仮想マシンを配置することが考慮されます。

リソースの予約

仮想マシンを実行可能なホストのうちの少なくとも 1 台には、仮想マシンのメモリ オーバーヘッドおよび任意のリソース予約に十分な、予約されていない容量が必要です。CPU、メモリ、vNIC、および仮想フラッシュの 4 種類の予約が考慮されます。また、仮想マシンをパワーオンするのに十分なネットワーク ポートも使用可能にする必要があります。

ホスト制限

リソース予約に加えて、許可される仮想マシン数または使用中の vCPU 数の最大数を超えない場合にのみ、仮想マシンをホストに配置できます。

機能の制約

vSphere HA の詳細オプションが、仮想マシンと仮想マシン間の非アフィニティ ルールを強制するように設定されている場合、vSphere HA はこのルールに違反しません。また vSphere HA は、Fault Tolerance 機能を持つ仮想マシンのホストごとに構成された制限のいずれにも違反しません。

上述の考慮事項を満たすホストが存在しない場合、プライマリ ホストは、vSphere HA が仮想マシンを起動するのに必要なリソースがないことを表すイベントを発行し、クラスタの状態が変更されたときに再試行します。たとえば、仮想マシンにアクセスできない場合、プライマリ ホストは、ファイルがアクセス可能になった後に再試行します。

仮想マシンとアプリケーションの監視

仮想マシンの監視では、VMware Tools のハートビートが設定した時間内に受信できなかった場合、その仮想マシンが個別に再起動されます。同様に、実行中のアプリケーションのハートビートが受信できない場合には、アプリケーションの監視によって仮想マシンが再起動されます。これらの機能を有効にし、vSphere HA が無応答を監視する感度を設定できます。

仮想マシンの監視を有効にすると、仮想マシンの監視サービスは （VMware Tools を使用）、ゲスト内で実行される VMware Tools プロセスからの定期的なハートビートおよび I/O アクティビティをチェックして、クラスタ内の各仮想マシンが稼動しているかどうかを判断します。ハートビートや I/O アクティビティが受信されない場合、ほとんどの原因は、ゲスト OS で障害が発生しているか、VMware Tools が割り当てられていないためにタスクが終了できないというものです。このような場合、仮想マシンの監視サービスは、仮想マシンで障害が発生したと判断し、仮想マシンを再起動してサービスを回復させます。

場合によっては、正常に機能している仮想マシンやアプリケーションが、ハートビートの送信を停止することがあります。不必要なリセットを防ぐため、仮想マシンの監視サービスは、仮想マシンの I/O アクティビティも監視しています。障害間隔内にハートビートが受信されなかった場合は、I/O 統計間隔 （クラスタ レベルの属性） がチェックされます。I/O 統計間隔では、過去 2 分間 （120 秒間） に、仮想マシンでディスクまたはネットワーク アクティビティが発生しているかどうかが確認されます。発生していない場合、その仮想マシンはリセットされます。このデフォルト値（120 秒）は、詳細オプション `das.iostatsinterval` を使用して変更できます。

アプリケーションの監視を有効にするには、まず適切な SDK を入手し （または VMware アプリケーションの監視をサポートするアプリケーションを使用中）、これを使用して監視対象となるアプリケーションの、カスタマイズされたハートビートを設定する必要があります。ハートビートを設定したら、アプリケーションの監視は仮想マシンの監視とほぼ同じように機能します。アプリケーションのハートビートが指定した期間受信できないと、仮想マシンは再起動されます。

監視感度のレベルは設定が可能です。監視感度を高度にすると、障害が発生したことが迅速に判断されます。ほとんど起こらないことですが、監視感度を高くすると、対象の仮想マシンまたはアプリケーションが実際には機能しているのに、リソースの制約などによってハートビートが受信されないため、障害であると誤って判断してしまうことがあります。監視感度を低くすると、実際に障害が発生してから仮想マシンがリセットされるまでの間、サービスが中断される時間が長くなります。ニーズに対して効果があるオプションを選択します。

[カスタム] チェック ボックスを選択すると、監視感度と I/O 統計間隔の両方に、カスタム値を指定することもできます。

表 2-1. 仮想マシンの監視設定

設定	障害間隔 （秒）	リセット間隔
高	30	1 時間
中	60	24 時間
低	120	7 日

障害が検出されると、vSphere HA は仮想マシンをリセットします。リセットすることで、確実にそのサービスが継続して利用可能になります。一時的ではないエラーに対して、仮想マシンが繰り返しリセットされないようにするため、デフォルトでは、仮想マシンは設定可能な特定の期間中に 3 回しかリセットされません。仮想マシンが 3 回リセットされると、vSphere HA は、これ以降に障害が発生しても、指定された時間が経過するまでは仮想マシンをリセットしようとしません。[仮想マシンごとの最大リセット回数] カスタム設定を使用することで、リセット回数を構成できます。

注： 仮想マシンをパワーオフしてからパワーオンした場合、または vMotion を使用して別のホストに移行した場合には、リセット統計がクリアされます。これによりゲスト OS が再起動しますが、仮想マシンの電源状態が変更された場合の再起動とは異なります。

仮想マシン コンポーネント保護

仮想マシンのコンポーネント保護 (VMCP) が有効な場合、vSphere HA はデータストアのアクセス障害を検出して、影響を受ける仮想マシンの自動リカバリを実行できます。

VMCP では、vSphere HA クラスタ内のホストで実行される仮想マシンに影響を与えることがある、データストアのアクセシビリティ障害に対する保護が提供されます。データストアのアクセシビリティ障害が発生すると、影響を受けるホストは、特定データストアのストレージ パスにアクセスできなくなります。このような障害に対して vSphere HA が実行する対応を決定できます。対応はイベント アラームの作成から、別のホスト上での仮想マシンの再起動までの多岐にわたります。

注： 仮想マシン コンポーネント保護機能を使用するには、ESXi ホストがバージョン 6.0 以降である必要があります。

障害の種類

次に 2 種類のデータストアのアクセシビリティ障害があります。

PDL

PDL (Permanent Device Loss)。データストアがホストからアクセスできないことをストレージ デバイスが報告するときに発生する、回復不可能なアクセシビリティの喪失です。仮想マシンをパワーオフせずにこの状態を元に戻すことはできません。

APD (All Path Down)

APD (All Paths Down)。一時的または不明なアクセシビリティの喪失、または I/O 処理に見られるその他の識別不可能な遅延です。この種類のアクセスの問題は回復可能です。

VMCP の構成

仮想マシン コンポーネント保護は vSphere Client で構成します。[構成] タブで、[vSphere の可用性]、[編集] の順にクリックします。[障害および対応] では、[PDL (Permanent Device Loss) 状態のデータストア] または [APD 状態のデータストア] を選択できます。選択可能なストレージ保護レベル、および使用可能な仮想マシンの修正操作は、データストアのアクセシビリティ障害の種類に応じて異なります。

PDL 障害

[PDL (Permanent Device Loss) 状態のデータストア] では、[イベントの発行] または [仮想マシンをパワーオフして再起動] を選択できます。

APD 障害

APD イベントへの対応はより複雑なため、それに合わせて構成もよりきめ細かくなります。[イベントの発行]、[仮想マシンをパワーオフして再起動: 標準的な再起動ポリシー]、または [仮想マシンをパワーオフして再起動: アグレッシブな再起動ポリシー] を選択できます。

注： ホストの監視または仮想マシン再起動の優先順位設定のいずれかが無効な場合、VMCP は仮想マシンの再起動を実行できません。ただし、ストレージの健全性を監視し、イベントを発行することができます。

ネットワーク パーティション

vSphere HA クラスタで管理ネットワークの障害が発生すると、そのクラスタのホストの一部は、管理ネットワーク越しに他のホストと通信できなくなる場合があります。クラスタ内に複数のパーティションが発生します。

クラスタがパーティション化されると、仮想マシンの保護やクラスタの管理機能が低下します。パーティション化したクラスタはできるだけ早く修復します。

- 仮想マシンの保護。vCenter Server を使用して仮想マシンをパワーオンできますが、仮想マシンを保護できるのは、その仮想マシンに責任のあるプライマリ ホストと同一パーティションで仮想マシンが実行されている場合のみです。プライマリ ホストは、vCenter Server と通信している必要があります。プライマリ ホストが仮想マシンに対して責任があるのは、その仮想マシンの構成ファイルを含むデータストア上のシステム定義ファイルを排他的にロックしている場合です。
- クラスタ管理。vCenter Server はプライマリ ホストと通信することができますが、セカンダリ ホストは一部のみです。結果的に、vSphere HA に影響する構成変更は、パーティション化が解決されるまで実行されない場合があります。この障害の結果、パーティションの 1 つは古い構成のまま運用され、他のパーティションでは新しい設定が使用されているということが起こり得ます。

データストア ハートビート

VMware vSphere® High Availability クラスタ内のプライマリ ホストが管理ネットワーク経由でセカンダリ ホストと通信できないとき、プライマリ ホストはデータストア ハートビートを使用して、セカンダリ ホストに障害があるのか、セカンダリホストがネットワーク パーティション内にあるのか、または隔離されたネットワークにあるのかを確認します。セカンダリ ホストがデータストア ハートビートを停止している場合は、障害が発生していて、仮想マシンはほかの場所で再起動されているとみなされます。

VMware vCenter Server® は、ハートビート用データストアの優先セットを選択します。この選択は、ハートビート データストアにアクセスするホスト数を最大に、データストアが同一 LUN または NFS サーバーにバッキングされる可能性が最小になるように行われます。

詳細オプションの `das.heartbeatdsperhost` を使用して、各ホストの vCenter Server により選択されるハートビート データストアの数を変更できます。デフォルトは 2 で、有効最大値は 5 です。

vSphere HA は各データストアのルートにディレクトリを作成します。このディレクトリは、データストア ハートビートおよび保護された仮想マシンのセット保持の両方に使用されます。ディレクトリ名は `.vSphere-HA` です。動作に影響することがあるので、このディレクトリに格納されたファイルを削除したり変更したりしないでください。複数のクラスタが 1 つのデータストアを使用している場合に備え、各クラスタ用にこのディレクトリのサブディレク

トリが作成されます。これらのディレクトリとファイルの所有者はルート （root） であり、これらのディレクトリやファイルを読み書きできるのはルートのみです。vSphere HA によって使用されるディスク スペースは、使用される VMFS のバージョンやハートビート用にデータストアを使用するホスト数など、いくつかの要因で決まります。vmfs3 では、最大使用量は 2GB で、通常の使用量は 3MB です。vmfs5 では、最大使用量と標準使用量は 3MB です。vSphere HA によるデータストアの使用は、無視できる程度のオーバーヘッドを追加するだけであり、ほかのデータストア操作に対するパフォーマンス上の影響はありません。

vSphere HA では、1 つのデータストアに構成ファイルを持つことのできる仮想マシンの数が制限されます。制限の更新については、『構成の上限』を参照してください。データストアにこの数を超える仮想マシンを配置してパワーオンした場合、vSphere HA によって保護されるのは制限数の仮想マシンまでです。

注： vSAN データストアは、データストア ハートビートには使用できません。したがって、他の共有ストレージがクラスタのすべてのホストにアクセスできない場合、使用中のハートビート データストアは存在しない可能性があります。ただし、vSAN ネットワークから独立している代替のネットワーク パスによってアクセスできるストレージがある場合、それを用いてハートビート データストアを設定できます。

vSphere HA セキュリティ

vSphere HA は、いくつかのセキュリティ機能により拡張されます。

開いているファイアウォールのポートを選択

vSphere HA は、TCP および UDP ポート 8182 をエージェント間の通信に使用します。ファイアウォールのポートの開閉は自動で、必要なときだけ開くようになっています。

ファイル システム権限を使用して保護された構成ファイル

vSphere HA は、ローカル データストアがない場合、構成情報をローカル ストレージまたは RAM ディスクに格納します。これらのファイルは、ファイル システム権限を使用して保護されており、root ユーザーだけがアクセス可能です。ローカル ストレージがないホストは、Auto Deploy で管理される場合にのみサポートされます。

詳細なログ

vSphere HA がログ ファイルを置く場所は、ホストのバージョンによって異なります。

- ESXi ホストでは、vSphere HA が Syslog に書き込むのはデフォルトの場合のみで、ログは、Syslog で構成された場所に置かれます。vSphere HA 用のログ ファイル名には、vSphere HA のサービスの 1 つであるフォールト ドメイン マネージャを表す `fdm` が前に付加されています。
- レガシー ESXi ホストでは、vSphere HA は、Syslog のほかにローカル ディスクの `/var/log/vmware/fdm` にも書き込みます（そのように構成されている場合）。

vSphere HA へのセキュアなログイン

vSphere HA は、vCenter Server により作成されたユーザー アカウントである vpxuser を使用して、vSphere HA エージェントにログオンします。このアカウントは、vCenter Server がホストを管理するために使用するのと同じアカウントです。vCenter Server はこのアカウント用にランダムなパスワードを作成し、定期的に変更します。その期間は、vCenter Server の `VirtualCenter.VimPasswordExpirationInDays`

設定で設定します。ホストのルート フォルダの管理権限を持つユーザーは、このエージェントにログインできます。

セキュアな通信

vCenter Server と vSphere HA エージェント間の通信は、すべて SSL 経由で行われます。エージェント間の通信も SSL を使用しますが、（マスター ホスト） 選択メッセージの通信だけは UDP 経由で行われます。選択メッセージは SSL で検証されるため、プライマリ ホストになることを不正なエージェントが妨害できるのは、そのエージェントが実行されているホストだけです。このケースでは、クラスタの構成に問題があることが通知され、ユーザーに注意を促します。

Host SSL 証明書の検証が必要

vSphere HA では、各ホストに検証済みの SSL 証明書があることが必要です。各ホストは、最初に起動したときに自己署名の証明書を生成します。次に、この証明書は再生成されるか、認証局が発行した証明書に置き換えられます。証明書が置き換えられた場合、ホスト上で vSphere HA を再構成する必要があります。証明書が更新されて ESXi または ESX ホスト エージェントが再起動した後にホストが vCenter Server から切断された場合は、vCenter Server に再接続されたときに vSphere HA は自動的に再構成されます。vCenter Server ホストの SSL 証明書の検証が無効なため切断されなかった場合は、新しい証明書を検証してホスト上の vSphere HA を再構成します。

vSphere HA のアドミッション コントロール

vSphere HA では、アドミッション コントロールを使用して、ホストで障害が発生した場合に仮想マシンをリカバリするのに十分なリソースが確保されるようにします。

アドミッション コントロールは、リソース使用量に制約を適用します。これらの制約に違反する可能性のあるアクションは許可されません。許可されない可能性のあるアクションには、次のものが挙げられます。

- 仮想マシンのパワーオン
- 仮想マシンの移行
- 仮想マシンの CPU またはメモリ予約の増加

vSphere HA アドミッション コントロールの基本は、クラスタでどれだけの数のホスト障害を許容しながら、フェイルオーバーを行うかにあります。ホストのフェイルオーバー キャパシティは、次の 3 つの方法で設定できます。

- クラスタ リソースの割合 (%)
- スロット ポリシー

- 専用のフェイルオーバー ホスト

注： vSphere HA アドミッション コントロールは無効にできます。ただし、アドミッション コントロールを有効にしておかないと、障害発生後に予想どおりの数の仮想マシンが再起動できるとは限りません。アドミッション コントロールは、無効のままにしないでください。

注： クラスタ内で vSphere vMotion を続行するには、HA アドミッション コントロールを一時的に無効にする必要があります。このアクションにより、修正するホスト上でのマシンのダウンタイムを防ぐことができます。2 ノード クラスタを修正する前に HA アドミッション コントロールを無効にすると、クラスタは実質的に高可用性に関するすべての保証を失います。これは、2 台のホストのうち 1 台がメンテナンス モードになると、vCenter Server が仮想マシンをそのホストにフェイルオーバーできなくなり、HA フェイルオーバーが正常に実行されなくなるためです。

注： vSphere HA アドミッション コントロールを使用するには、クラスタ内に 3 台以上のホストが必要です。

いずれのアドミッション コントロール オプションを選択した場合でも、仮想マシンのリソース削減のしきい値を設定できます。この設定では、許容するリソース削減の割合を指定できますが、vSphere DRS が有効でないと使用できません。

リソース削減の計算は、CPU とメモリの両方に対して行われます。パワーオン、移行、または予約の変更を許可するかどうか決定するため、計算には仮想マシンの予約済みメモリとメモリ オーバーロードが考慮されます。仮想マシンによって使用される実際のメモリは、計算に考慮されません。これは、メモリ予約量と仮想マシンの実際のメモリ使用量との間に相関関係があるとは限らないためです。実際の使用量が予約メモリ量を超えている場合、十分なフェイルオーバー キャパシティが確保されず、フェイルオーバー時にパフォーマンスが低下します。

パフォーマンス低下のしきい値を設定することで、構成に関する問題を指定できます。例：

- デフォルト値が 100% の場合、警告は生成されません。
- しきい値を 0% に引き下げた場合、クラスタ使用量が使用可能なキャパシティを超えると警告が生成されます。
- しきい値を 20% に引き下げた場合、許容されるパフォーマンスの低下は `performance reduction = current utilization * 20%` として計算されます。現在の使用量からパフォーマンスの低下を差し引いた結果が使用可能なキャパシティを超える場合、構成に関する注意が発行されます。

クラスタ リソースの割合アドミッション コントロール

ホスト障害からのリカバリ用にクラスタ CPU およびメモリ リソースの一定割合を予約することで、アドミッション コントロールが実行できるよう、vSphere HA を構成できます。

このタイプのアドミッション コントロールでは、vSphere HA によって、CPU とメモリのリソース総量のうち、指定した割合がフェイルオーバー用に予約されます。

クラスタ リソースの割合オプションでは、vSphere HA によって次のアドミッション コントロールが実行されます。

1 クラスタ内のパワーオン状態のすべての仮想マシンに対する、リソース要件の合計を計算します。

2 仮想マシンで使用できるホスト リソースの合計を計算します。

3 クラスタの現在の CPU フェイルオーバー キャパシティおよび現在のメモリ フェイルオーバー キャパシティを計算します。

4 現在の CPU フェイルオーバー キャパシティ、または現在のメモリ フェイルオーバー キャパシティのいずれかが、（ユーザーが定義した） 対応する構成済みフェイルオーバー キャパシティより小さいかどうかを判断します。

いずれかが小さい場合は、アドミッション コントロールにより操作が禁止されます。

vSphere HA では、仮想マシンの実際の予約が使用されます。仮想マシンに予約がない、つまり予約が 0 の場合は、デフォルトの 0MB のメモリおよび 32MHz の CPU が適用されます。

注： アドミッション コントロール用のクラスタ リソースの割合オプションでは、クラスタ内に少なくとも 2 台の vSphere HA 対応ホストがあることを確認します（メンテナンス モードに入っているホストを除く）。vSphere HA 対応のホストが 1 台しかない場合、利用可能なリソースの割合が十分であっても実行できません。この確認を追加するのは、クラスタ内にホストが 1 台しかない場合、vSphere HA はフェイルオーバーを実行できないからです。

現在のフェイルオーバー キャパシティの計算

パワーオン状態の仮想マシンに対するリソース要件の合計は、CPU とメモリの 2 つのコンポーネントで構成されます。vSphere HA は、これらの値を計算します。

- パワーオン状態の仮想マシンの CPU 予約量を合計することによる、CPU コンポーネントの値。仮想マシンの CPU 予約が指定されていない場合は、デフォルト値の 32MHz が割り当てられます（この値は、`das.vmcpuminmhz` 詳細オプションを使用して変更できます）。
- パワーオン状態の各仮想マシンのメモリ予約 （およびメモリ オーバーヘッド） を合計することによる、メモリ コンポーネントの値。

仮想マシンで使用できるホスト リソースの合計は、ホストの CPU リソースとメモリ リソースを合計して計算されます。これらの量は、ホストの物理リソースの合計ではなく、ホストのルート リソース プールに含まれています。仮想化のために使用中のリソースは除外されます。メンテナンス モードではない接続状態のホストで、vSphere HA のエラーがないホストのみが対象となります。

現在の CPU フェイルオーバー キャパシティは、ホスト CPU リソースの合計から、CPU リソース要件の合計を減算し、その結果の値を、ホスト CPU リソースの合計で除算した値になります。現在のメモリ フェイルオーバー キャパシティも同様に計算されます。

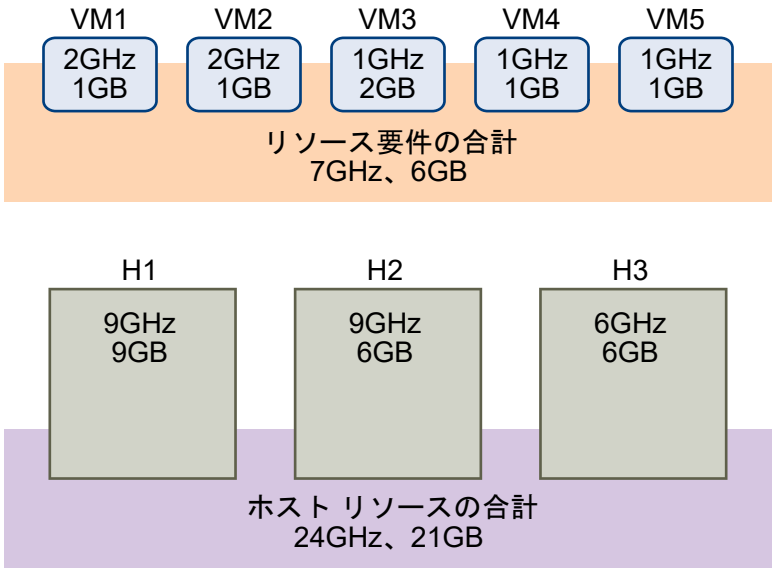
例： クラスタ リソースの割合を使用したアドミッション コントロール

この例では、現在のフェイルオーバー キャパシティがどのように計算され、このアドミッション コントロール ポリシーでどのように使用されるかを示します。クラスタについて次のように仮定します。

- クラスタは 3 台のホストで構成されており、それぞれ異なる量の、使用可能な CPU リソースとメモリ リソースがあります。最初のホスト （H1） は、使用可能な 9GHz の CPU リソースと 9GB のメモリがありますが、ホスト 2 （H2） には、9GHz の CPU リソースと 6GB のメモリ、ホスト 3 （H3） には 6GHz の CPU リソースと 6GB のメモリがあります。

- クラスタ内には、パワーオン状態の仮想マシンが 5 台あり、それぞれに異なる CPU 要件とメモリ要件があります。VM1 は 2GHz の CPU リソースと 1GB のメモリが必要ですが、VM2 は 2GHz の CPU リソースと 1GB のメモリ、VM3 は 1GHz の CPU リソースと 2GB のメモリ、VM4 は 1GHz の CPU リソースと 1GB のメモリ、VM5 は 1GHz の CPU リソースと 1GB のメモリが必要です。
- CPU とメモリの構成済みフェイルオーバー キャパシティはいずれも 25% に設定されています。

図 2-1. 予約されたクラスタ リソースの割合ポリシーを使用したアドミッション コントロールの例



パワーオン状態の仮想マシンに対するリソース要件の合計は、CPU リソースが 7GHz、メモリが 6GB です。仮想マシンで使用できるホスト リソースの合計は、CPU リソースが 24GHz、メモリが 21GB です。これに基づいて、現在の CPU フェイルオーバー キャパシティは 70% （(24GHz - 7GHz) / 24GHz） となります。同様に、現在のメモリ フェイルオーバー キャパシティは 71% （(21GB - 6GB) / 21GB） になります。

クラスタの構成済みフェイルオーバー キャパシティは 25% に設定されているため、クラスタの CPU リソースの合計の 45%、およびクラスタのメモリ リソースの 46% は、追加の仮想マシンをパワーオンするために使用できます。

スロット ポリシー アドミッション コントロール

スロット ポリシー オプションの場合、vSphere HA アドミッション コントロールにより、指定された数のホストで障害が発生しても、それらのホストからすべての仮想マシンにフェイルオーバーするのに十分なリソースがクラスタ内に残ります。

スロット ポリシーを使用する場合、vSphere HA は、次のようにアドミッション コントロールを実行します。

1 スロット サイズを計算します。

  スロットは、メモリおよび CPU リソースの論理的な表現方法です。デフォルトで、クラスタ内でパワーオンされている仮想マシンの要件を満たすよう、サイズが調整されます。

2 クラスタ内の各ホストが保持できるスロットの数を決定します。

3 クラスタの現在のフェイルオーバー キャパシティを決定します。

これは障害が発生し、パワーオン状態のすべての仮想マシンの要件を満たす十分なスロットが残っている可能性があるホストの数です。

4 現在のフェイルオーバー キャパシティが、（ユーザーが定義した）構成済みフェイルオーバー キャパシティよりも少ないかどうか判断します。

少ない場合、アドミッション コントロールにより操作が禁止されます。

注： vSphere Client の vSphere HA 設定のアドミッション コントロールのセクションで、CPU とメモリの両方について具体的なスロット サイズを設定できます。

スロット サイズの計算

(vSphere HA のスロット サイズとアドミッション コントロール)

スロット サイズは、CPU とメモリの 2 つのコンポーネントで構成されます。

- vSphere HA では、パワーオン状態の各仮想マシンの CPU 予約を取得し、最も大きな値を選択することによって、CPU コンポーネントを計算します。仮想マシンの CPU 予約を指定していない場合、デフォルト値である 32MHz が割り当てられます。`das.vmcpuminmhz` という詳細オプションで、この値を変更できます。
- vSphere HA では、パワーオン状態の各仮想マシンのメモリ予約 （にメモリ オーバーヘッドを加えた値） を取得し、最も大きな値を選択することによって、メモリ コンポーネントを計算します。メモリ予約には、デフォルト値はありません。

クラスタの中に、ほかよりもかなり多い予約が割り当てられている仮想マシンが含まれている場合は、スロット サイズの計算が正確になりません。このような問題を回避するために、`das.slotcpuinmhz` または `das.slotmeminmb` の詳細オプションを使用して、スロット サイズの CPU コンポーネントまたはメモリ コンポーネントに対する上限をそれぞれ指定できます。vSphere HA の詳細オプションを参照してください。

また、複数のスロットを必要とする仮想マシンの数を表示することで、クラスタ内のリソースの断片化のリスクを判断することもできます。これは、vSphere Client の vSphere HA 設定のアドミッション コントロールのセクションで計算できます。詳細オプションを使用して固定のスロット サイズや最大のスロット サイズを指定している場合、仮想マシンで複数のスロットが必要になる場合があります。

スロットを使用した現在のフェイルオーバー キャパシティの計算

スロット サイズが計算されると、vSphere HA は、仮想マシンで使用できる各ホストの CPU とメモリのリソースを決定します。これらの量は、ホストの物理リソースの合計ではなく、ホストのルート リソース プールに含まれています。vSphere HA で使用されるホストのリソース データは、vSphere Client のホストの [サマリ] タブにあります。クラスタ内のホストがすべて同一の場合、このデータは、クラスタレベルの数字をホスト数で割れば得られます。仮想化のために使用中のリソースは除外されます。接続されていてメンテナンス モードでなく、vSphere HA エラーがないホストのみが考慮されます。

次に、各ホストがサポートできるスロットの最大数が決定されます。そのためには、ホスト CPU のリソース量をスロット サイズの CPU コンポーネントで割り、結果を切り捨てます。ホストのメモリ リソース量に対して、同じ計算が行われます。これらの 2 つの値が比較され、小さい方が、ホストがサポートできるスロット数になります。

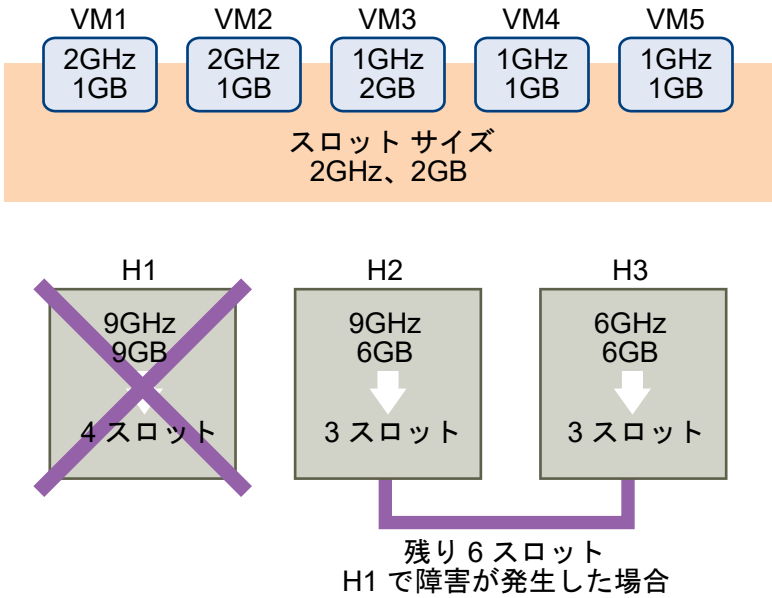
現在のフェイルオーバー キャパシティは、何台のホスト （最も大きいものから開始） で障害が発生する可能性があるか、およびパワーオン状態のすべての仮想マシンの要件を満たす十分なスロットが残っているかを判定することによって計算されます。

例： スロット ポリシーを使用したアドミッション コントロール

この例では、スロット サイズがどのように計算され、このアドミッション コントロール ポリシーでどのように使用されるかを示します。クラスタについて次のように仮定します。

- クラスタは 3 台のホストで構成されており、それぞれ異なる量の、使用可能な CPU リソースとメモリ リソースがあります。最初のホスト （H1） は、使用可能な 9GHz の CPU リソースと 9GB のメモリがありますが、ホスト 2 （H2） には、9GHz の CPU リソースと 6GB のメモリ、ホスト 3 （H3） には 6GHz の CPU リソースと 6GB のメモリがあります。
- クラスタ内には、パワーオン状態の仮想マシンが 5 台あり、それぞれに異なる CPU 要件とメモリ要件があります。VM1 は 2GHz の CPU リソースと 1GB のメモリが必要ですが、VM2 は 2GHz の CPU リソースと 1GB のメモリ、VM3 は 1GHz の CPU リソースと 2GB のメモリ、VM4 は 1GHz の CPU リソースと 1GB のメモリ、VM5 は 1GHz の CPU リソースと 1GB のメモリが必要です。
- クラスタで許容するホスト障害は 1 に設定されます。

図 2-2. クラスタで許容するホスト障害ポリシーによるアドミッション コントロールの例



1 仮想マシンの CPU 要件とメモリ要件の両方で比較を行なって最大の値を選択することにより、スロット サイズが計算されます。

   最大の CPU 要件は 2GHz （VM1 と VM2 で共通） で、最大のメモリ要件は 2GB （VM3 の） です。これらの値に基づいて、スロット サイズは 2GHz CPU および 2GB メモリになります。

2 各ホストでサポートできるスロットの最大数を決定します。

   H1 は 4 つのスロットをサポートできます。H2 は 3 スロット（9GHz/2GHz および 6GB/2GB の小さい方）、H3 も 3 スロットをサポートできます。

3 現在のフェイルオーバー キャパシティを計算します。

最も大きいホストは H1 で、H1 で障害が発生しても、クラスタでは 6 つのスロットを使用できます。これは、パワーオン状態の 5 台の仮想マシンすべてに対して十分なスロットです。H1 と H2 の両方で障害が発生すると、3 つのスロットしか使用できなくなり、これでは不十分です。したがって、現在のフェイルオーバー キャパシティは 1 になります。

クラスタには、使用できるスロットが 1 つあります （H2 と H3 の 6 つのスロットから、使用済みの 5 つのスロットを減算する）。

専用フェイルオーバー ホストのアドミッション コントロール

特定のホストをフェイルオーバー ホストとして指定するように vSphere HA を構成できます。

専用フェイルオーバー ホストのアドミッション コントロールでは、ホストで障害が発生したときに、vSphere HA が、指定されたフェイルオーバー ホストのいずれかで障害ホストの仮想マシンを再起動しようとします。フェイルオーバー ホスト自身で障害が発生している、または十分なリソースがない、などの理由で仮想マシンが再起動できない場合、vSphere HA はこれらの仮想マシンを、クラスタ内の別のホストで再起動しようとします。

フェイルオーバー ホストで予備のキャパシティを確実に使用できるようにするため、仮想マシンをパワーオンすること、または vMotion を使用して仮想マシンをフェイルオーバー ホストに移行することはできません。また、DRS はロード バランシング用としてフェイルオーバー ホストを使用しません。

注： 専用フェイルオーバー ホストのアドミッション コントロールを使用して複数のフェイルオーバー ホストを指定する場合、DRS は、フェイルオーバー ホストで実行されている仮想マシンについて仮想マシン間のアフィニティ ルールの強制適用を行いません。

vSphere HA の相互運用性

vSphere HA は、DRS や vSAN などの他の多くの機能と相互運用できます。

vSphere HA を構成する前に、これらの他の機能または製品との相互運用性の制限について理解しておく必要があります。

vSphere HA と vSAN の併用

vSAN を vSphere HA クラスタの共有ストレージとして使用できます。有効にすると、vSAN はホストの利用可能なローカル ストレージ ディスクの中で指定したものを、すべてのホストで共有される単一のデータストアに統合します。

vSphere HA を vSAN と併用するには、これらの両機能の相互運用性についていくつかの注意事項や制限事項を理解しておく必要があります。

vSAN の詳細については、「VMware vSAN の管理」を参照してください。

注： vSphere HA は vSAN ストレッチ クラスタと同時に利用できます。

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 以降である必要があります。
- クラスタには、3 つ以上の ESXi ホストが必要です。

ネットワークの相違点

vSAN には独自のネットワークがあります。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。vSphere HA がホストで構成されている場合、vCenter Server は適切なネットワークを選択します。

注： vSAN は、vSphere HA が無効な場合にのみ有効にできます。

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 のネットワークに変更を加えるには、vSphere Client で次の手順を実行する必要があります。

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右クリックし、[vSphere HA 用に再構成] 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。

表 2-2. vSphere HA ネットワークの相違点に、vSAN が使用されている場合と使用されていない場合の vSphere HA ネットワークの相違点を示します。

表 2-2. 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

キャパシティの予約設定

vSphere HA クラスタにアドミッション コントロール ポリシーでキャパシティを予約する場合、この設定は、障害時にデータのアクセシビリティを確保する vSAN の対応する設定と連係させる必要があります。特に、vSAN のルール セットの [許容する障害の数] の設定は、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キャパシティよりも低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% を超えて予約をしないでください。同じクラスタで、[ホスト障害のクラスタ許容] 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。

vSphere HA と DRS の併用

vSphere HA を DRS （Distributed Resource Scheduler） と組み合わせて使用すると、自動フェイルオーバーとロード バランシングの両方が実現されます。この組み合わせにより、vSphere HA が仮想マシンを別のホストに移行したあとのクラスタはバランスが向上します。

vSphere HA がフェイルオーバーを実行し、異なるホスト上で仮想マシンを再起動する場合、最優先事項は、すべての仮想マシンの当面の可用性にあります。仮想マシンが再起動されたあと、それらの仮想マシンがパワーオンされたホストは負荷が大きくなる場合があるのに対し、ほかのホストは負荷が比較的軽くなります。vSphere HA は、仮想マシンの CPU とメモリの予約とオーバーヘッド メモリを使用して、仮想マシンに対応できる十分なキャパシティがホストにあるかどうかを判断します。

DRS および vSphere HA を使用するクラスタでアドミッション コントロールがオンになっている場合、メンテナンス モードに入るホストから仮想マシンを退避できないことがあります。これは、障害時の仮想マシンの再起動用にリソースが予約されているために発生します。vMotion を使用して、手動でホストから仮想マシンを移行する必要があります。

いくつかのシナリオでは、リソースの制約が原因で、vSphere HA が仮想マシンをフェイルオーバーできない場合があります。これが生じる理由はいくつかあります。

- HA アドミッション コントロールが無効になっていて、DPM (Distributed Power Management) が有効になっている場合。これにより、DPM が少数のホストに仮想マシンを統合し、空のホストをスタンバイ モードにするため、パワーオン状態のキャパシティが不足してフェイルオーバーを行えなくなります。
- 仮想マシンとホスト間のアフィニティ （必須） ルールによって、特定の仮想マシンを配置できるホストが制限される場合がある。
- 十分な集約リソースはあっても、複数のホスト間で断片化される可能性があるため、仮想マシンでフェイルオーバーに使用できない場合。

このような場合、vSphere HA は DRS を使用してクラスタの調整を試み （ホストのスタンバイ モードを終了したり、仮想マシンを移行してクラスタ リソースを最適化したりするなど）、HA がフェイルオーバーを実行できるようにします。

DPM が手動モードの場合、ホストのパワーオンの推奨を確認する必要がある場合があります。同様に、DRS が手動モードの場合は、移行の推奨を確認する必要がある場合があります。

仮想マシンとホスト間の必須のアフィニティ ルールを使用している場合は、これらのルールに違反できないことを理解しておく必要があります。vSphere HA は、フェイルオーバーの実行がこのようなルールの違反につながる場合は、フェイルオーバーを行いません。

DRS の詳細については、『vSphere のリソース管理』ドキュメントを参照してください。

注： vSphere DRS は、vSphere の重要な機能で、vSphere クラスタ内で実行されるワークロードの健全性の維持に必要です。vSphere 7.0 Update 1 以降では、DRS は vCLS 仮想マシンの可用性に依存します。詳細については、『vSphere のリソース管理』の「vSphere クラスタ サービス (vCLS)」を参照してください。

vSphere HA および DRS のアフィニティ ルール

クラスタに DRS アフィニティ ルールを作成すると、仮想マシンのフェイルオーバー中に vSphere HA がそのルールをどのように適用するかを指定できます。

vSphere HA のフェイルーバーの動作に指定できる 2 種類のルールを以下に挙げます。

- フェイルオーバー アクション中、指定された仮想マシンをフェイルオーバーに参加させない、仮想マシン非アフィニティ ルール。
- フェイルオーバー アクション中、指定された仮想マシンを特定のホストまたは定義されたホスト グループのメンバーに配置する、仮想マシンとホスト間のアフィニティ ルール。

DRS アフィニティ ルールを編集するときに、vSphere HA の詳細オプションを使用して vSphere HA に必要なフェイル オーバーの動作を強制する必要があります。

- [HA はフェイルオーバー中に仮想マシン非アフィニティ ルールを順守する必要があります] -- 仮想マシン非アフィニティ ルールの詳細オプションが設定されていると、仮想マシンをフェイルオーバーするとルールに反する場合、vSphere HA はフェイルオーバーを実行しません。代わりに、vSphere HA はフェイルオーバーを実行するためのリソースが不足していることを報告するイベントを発行します。
- [HA 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]：vSphere HA は、このルールが指定された仮想マシンを、できる限り指定されたホストに配置するように試みます。

詳細については、vSphere HA の詳細オプションを参照してください。

注： ルールを設定した直後（デフォルトで 5 分以内）にホストの障害が発生した場合、vSphere HA は、仮想マシンとホスト間のアフィニティ ルールのマッピングを無視して、DRS が無効なクラスタ内の仮想マシンを再起動できます。

vSphere HA の相互運用性に関するその他の問題

vSphere HA を使用するには、次に示す、相互運用性に関するその他の問題について理解しておく必要があります。

仮想マシン コンポーネント保護

仮想マシン コンポーネント保護 (VMCP) には、次に示す相互運用性の問題と制限があります。

- VMCP は、vSAN データストアに配置されているファイルのアクセシビリティ問題を検出したり、それに応答したりしません。仮想マシンの構成ファイルと VMDK ファイルが vSAN データストアにのみ配置されている場合は、VMCP によって保護されません。
- VMCP は、Virtual Volumes データストアに配置されているファイルのアクセシビリティ問題を検出したり、それに応答したりしません。仮想マシンの構成ファイルと VMDK ファイルが Virtual Volumes データストアにのみ配置されている場合、それらのファイルは VMCP によって保護されません。

- VMCP は、アクセス不可の RAW デバイス マッピング (RDM) に対する保護は行いません。

IPv6

vSphere HA は IPv6 ネットワーク構成で使用することができ、次の考慮事項が守られている場合に完全にサポートされます。

- クラスタには、ESXi 6.0 以降のホストのみが含まれています。
- クラスタのすべてのホストの管理ネットワークは、同じ IP バージョン（IPv6 または IPv4 のどちらか）で構成されている必要があります。vSphere HA クラスタに両方のタイプのネットワーク構成を含めることはできません。
- vSphere HA によって使用されるネットワーク隔離アドレスは、管理ネットワークでクラスタによって使用される IP バージョンと一致する必要があります。
- IPv6 は、vSAN も使用されている vSphere HA クラスタで使用することはできません。

上記の制限事項に加えて、アドレス タイプがリンクローカル、ORCHID、および ゾーン インデックスのリンクローカルである IPv6 アドレスは、vSphere HA 隔離アドレスまたは管理ネットワークで使用するようにはサポートされていません。また、管理ネットワークでループバック アドレス タイプを使用することはできません。

注： 既存の IPv4 デプロイを IPv6 にアップグレードするには、まず vSphere HA を無効にする必要があります。

vSphere HA クラスタの作成

vSphere HA は、ESXi （または、レガシー ESX） ホストのクラスタのコンテキストで機能します。フェイルオーバーの保護を確立するには、事前にクラスタを作成し、そのクラスタにホストを配置して、vSphere HA の設定を構成しておく必要があります。

vSphere HA のクラスタを作成する場合には、機能がどのように作用するかを決定する多数の設定を構成する必要があります。これを実行する前に、クラスタのノードを確認します。これらのノードは、仮想マシンをサポートするリソースを提供する ESXi ホストで、vSphere HA は、これらのホストをフェイルオーバーの保護のために使用します。次に、これらのノードが互いにどのように接続されるか、および仮想マシンのデータが格納されている共有ストレージに対してどのように接続されるかを決定します。このネットワーク アーキテクチャが整備されると、クラスタにホストを追加し、vSphere HA の構成を完了できます。

クラスタにホスト ノードを追加する前に、vSphere HA を有効にして構成できます。ただし、クラスタにホストが追加されるまで、クラスタは十分に機能せず、クラスタの設定の中には使用できないものもあります。たとえば、フェイルオーバー ホストとして指定できるホストが存在しない場合は、フェイルオーバー ホストの指定アドミッション コントロール ポリシーは使用できません。

注： 仮想マシンの起動およびシャットダウン（自動起動）の機能は、vSphere HA クラスタ内にある（またはこのクラスタ内に移行された）ホスト上のすべての仮想マシンで無効になっています。vSphere HA とともに使用されるとき、自動起動はサポートされません。

vSphere HA のチェックリスト

vSphere HA のチェックリストでは、vSphere HA クラスタを作成および使用する前に理解しておく必要のある要件について説明しています。

vSphere HA クラスタをセットアップする前に、次の内容を確認してください。詳細については、該当するクロスリファレンスを参照してください。

- すべてのホストに vSphere HA のライセンスがある。
- クラスタには、ホストが少なくとも 2 つ含まれている必要があります。
- すべてのホストは、固定 IP アドレスで構成する必要があります。DHCP を使用している場合は、再起動しても各ホストのアドレスが変わらないことを確認する必要があります。
- すべてのホストに、少なくとも 1 つの共通の管理ネットワークが必要です。ベスト プラクティスでは、共通の管理ネットワークを 2 つ以上構成します。VMkernel ネットワークを、[管理トラフィック] チェックボックスが有効での状態で使用する必要があります。各ネットワークは相互にアクセス可能になっており、管理ネットワークで vCenter Server とホストが相互にアクセス可能になっている必要があります。ネットワークのベスト プラクティス を参照してください。
- クラスタ内の任意のホストで任意の仮想マシンを実行できるようにするために、すべてのホストから同じ仮想マシンのネットワークおよびデータストアにアクセスできるようになっている必要があります。同様に、仮想マシンはローカル以外の共有ストレージに配置する必要があります。共有できない場合は、ホストの障害時に仮想マシンはフェイルオーバーされません。

  注： vSphere HA は、データストア ハートビートを使用して、パーティション化されたホスト、隔離されたホスト、および障害のあるホストを区別します。したがって、使用環境で一部のデータストアの信頼性が高い場合は、それらを優先するように vSphere HA を構成します。

- 仮想マシンの監視が機能するために、VMware Tools がインストールされている。仮想マシンとアプリケーションの監視 を参照してください。
- vSphere HA は IPv4 および IPv6 の両方をサポートしています。IPv6 を使用する場合の考慮事項については、vSphere HA の相互運用性に関するその他の問題 を参照してください。
- 仮想マシン コンポーネント保護が正常に機能するには、ホストで全パスダウン (APD) タイムアウト機能を有効にする必要があります。
- 仮想マシン コンポーネント保護を使用するには、クラスタに ESXi 6.0 以降のホストが含まれている必要があります。
- VMCP を有効にするために使用できるのは、ESXi 6.0 以降のホストが含まれている vSphere HA クラスタのみです。以前のリリースのホストを含むクラスタでは VMCP を有効にできません。また、それらのホストは VMCP が有効なクラスタに追加できません。
- クラスタで仮想ボリューム データストアを使用する場合、vSphere HA が有効にされると、vCenter Server により各データストアで構成仮想ボリュームが作成されます。vSphere HA は、これらのコンテナに、仮想マシンの保護に使用するファイルを保存します。これらのコンテナを削除すると、vSphere HA が正常に機能しなくなります。コンテナは、仮想ボリューム データストアごとに 1 つだけ作成されます。

vSphere Client での vSphere HA クラスタの作成

vSphere HA 用にクラスタを有効にするには、最初に空のクラスタを作成する必要があります。クラスタのリソースおよびネットワーク アーキテクチャの計画後に、vSphere Client を使用してクラスタにホストを追加し、そのクラスタの vSphere HA 設定を指定します。

vSphere Fault Tolerance には vSphere HA 対応のクラスタが必須です。

前提条件

- すべての仮想マシンとその構成ファイルが共有ストレージに格納されていることを確認します。
- クラスタ内の別のホストを使用して仮想マシンをパワーオンできるようにするため、ホストが共有ストレージにアクセスするように構成されていることを確認します。
- ホストが仮想マシン ネットワークにアクセスできるよう構成されていることを確認します。
- vSphere HA 用に冗長な管理ネットワーク接続を使用していることを確認します。ネットワークの冗長性の設定に関する詳細は、ネットワークのベスト プラクティスを参照してください。
- vSphere HA データストア ハートビートに冗長性を持たせるため、少なくとも 2 つのデータストアを使用してホストが構成されていることを確認します。
- クラスタの管理者権限を持つアカウントを使用して、vSphere Client を vCenter Server に接続します。

手順

1. vSphere Client で、クラスタを配置するデータセンターを参照し、[新規クラスタ] をクリックします。
2. [新規クラスタ] ウィザードを最後まで実行します。

   vSphere HA (または DRS) を有効にしないでください。
3. [OK] をクリックしてウィザードを閉じ、空のクラスタを作成します。
4. クラスタのリソースおよびネットワーク アーキテクチャの計画に基づき、vSphere Client を使用してクラスタにホストを追加します。
5. クラスタを参照し、vSphere HA を有効にします。
   a [設定] タブをクリックします。
   b [vSphere の可用性] を選択し、[編集] をクリックします。
   c [vSphere HA] を選択します。
6. [障害および対応] で [ホスト監視の有効化] を選択します。

   ホスト監視を有効にすることにより、クラスタ内のホストはネットワークのハートビートを相互に送信でき、vSphere HA は障害を検出したときにアクションを実行できます。vSphere Fault Tolerance リカバリ プロセスが正常に機能するには、ホスト監視が必要です。
7. [仮想マシンの監視] の設定を選択します。

   [仮想マシンの監視のみ] を選択し、仮想マシンのハートビートを設定した時間内に受信できなくなった場合に、その仮想マシンを個別に再起動します。[仮想マシンとアプリケーションの監視] を選択してアプリケーションの監視を有効にすることもできます。
8. [OK] をクリックします。

結果

これで、ホストが組み込まれた vSphere HA クラスタは作成しました。

次のステップ

クラスタに適した vSphere HA 設定を構成します。

- 障害および対応
- アドミッション コントロール
- ハートビート データストア
- 詳細オプション

vSphere の可用性設定の構成を参照してください。

vSphere の可用性設定の構成

vSphere HA のクラスタを作成したり既存のクラスタを構成したりする場合は、機能の動作方法を決める設定を構成する必要があります。

vSphere Client では、次の vSphere HA の設定を構成できます。

障害および対応

ホストの障害応答、ホスト隔離、仮想マシンの監視、および仮想マシン コンポーネント保護の設定を指定します。

アドミッション コントロール

vSphere HA クラスタのアドミッション コントロールを有効または無効にしたり、アドミッション コントロールの適用方法を指定するポリシーを選択します。

ハートビート データストア

vSphere HA がデータストア ハートビートに使用するデータストアの環境設定を指定します。

詳細オプション

詳細オプションを設定して、vSphere HA の動作をカスタマイズします。

障害への応答の構成

vSphere HA 設定の [障害および対応] ペインでは、問題が発生したときにクラスタがどのように機能すべきかを構成できます。

vSphere Client のこの部分では、ホストの障害や隔離に対して vSphere HA が実施する特定の応答を決定できます。また、Permanent Device Loss (PDL) と All Paths Down (APD) が発生した場合の仮想マシン コンポーネント保護 (VMCP) アクションを構成し、仮想マシンの監視を有効にできます。

次のタスクを使用できます。

次に参照するドキュメント

手順

1 ホスト障害への応答

vSphere HA クラスタで発生するホスト障害への具体的な対応を設定できます。

2 ホスト隔離への応答

vSphere HA クラスタで発生するホスト隔離への応答を設定できます。

3 VMCP 応答の構成

データストアで PDL または APD の障害が発生したときに仮想マシン コンポーネント保護 (VMCP) が作成する応答を設定します。

4 仮想マシン監視の有効化

仮想マシンとアプリケーションの監視をオンにし、vSphere HA クラスタの監視感度も設定できます。

ホスト障害への応答

vSphere HA クラスタで発生するホスト障害への具体的な対応を設定できます。

このページは、vSphere HA を有効にしている場合のみ編集可能です。

手順

1 vSphere Client で、vSphere HA クラスタに移動して参照します。

2 [設定] タブをクリックします。

3 [vSphere の可用性] を選択し、[編集] をクリックします。

4 [障害および対応] をクリックし、[ホストの障害応答] を展開します。

5 次の構成オプションから選択します。

オプション	説明
障害応答	[無効] を選択すると、この設定によってホストの監視がオフになり、ホスト障害の発生時に仮想マシンは再起動しません。[仮想マシンの再起動] を選択すると、ホストの障害時に再起動の優先順位に従って、仮想マシンがフェイルオーバーされます。
仮想マシン再起動のデフォルトの優先順位	再起動の優先順位は、ホストの障害時に仮想マシンを再起動する順序を決定します。優先順位の高い仮想マシンが先に起動されます。複数のホストで障害が発生した場合、優先順位が 1 番目のホストのすべての仮想マシンを先に移行したあとで、優先順位に従って順次移行を行います。
仮想マシン再起動の優先順位の条件	vSphere HA が優先順位に従って仮想マシンの再起動を行うようにするには、特定の条件と、その条件に一致したあとの遅延を選択する必要があります。

6 [OK] をクリックします。

結果

ホスト障害応答の設定が有効になります。

ホスト隔離への応答

vSphere HA クラスタで発生するホスト隔離への応答を設定できます。

このページは、vSphere HA を有効にしている場合のみ編集可能です。

手順

1 vSphere Client で、vSphere HA クラスタに移動して参照します。

2 [設定] タブをクリックします。

3 [vSphere の可用性] を選択し、[編集] をクリックします。

4 [障害および対応] をクリックし、[ホスト隔離への対応] を展開します。

5 ホスト隔離への応答を設定するには、[無効]、[仮想マシンをシャットダウンして再起動]、または [仮想マシンをパワーオフして再起動] を選択します。

6 [OK] をクリックします。

結果

ホスト隔離への応答の設定が有効になります。

VMCP 応答の構成

データストアで PDL または APD の障害が発生したときに仮想マシン コンポーネント保護 (VMCP) が作成する応答を設定します。

このページは、vSphere HA を有効にしている場合のみ編集可能です。

手順

1 vSphere Client で、vSphere HA クラスタに移動して参照します。

2 [設定] タブをクリックします。

3 [vSphere の可用性] を選択し、[編集] をクリックします。

4 [障害および対応] をクリックし、[PDL (永続的なデバイスの損失) 状態のデータストア] または [APD 状態のデータストア] を展開します。

5 [PDL (永続的なデバイスの損失) 状態のデータストア] をクリックした場合は、このタイプの問題に対する VMCP 障害応答を [無効]、[イベントの発行]、または [仮想マシンをパワーオフして再起動] に設定できます。

6 [APD 状態のデータストア] をクリックした場合は、このタイプの問題に対する VMCP 障害応答を [無効]、[イベントの発行]、[仮想マシンをパワーオフして再起動: 標準的な再起動ポリシー]、または [仮想マシンをパワーオフして再起動: アグレッシブな再起動ポリシー] に設定できます。また、[応答復旧] も設定できます。これは、VMCP がアクションを実行するまで待機する時間（分）を指定します。

7 [OK] をクリックします。

結果

VMCP 障害応答の設定が有効になります。

仮想マシン監視の有効化

仮想マシンとアプリケーションの監視をオンにし、vSphere HA クラスタの監視感度も設定できます。

このページは、vSphere HA を有効にしている場合のみ編集可能です。

注： 仮想マシンの監視が無効になっている場合でも、vSphere HA によって健全でない仮想マシンが健全なホストにフェイルオーバーされることがあります。この場合のホストの選択は、DRS 推奨に基づいて行われるか、または使用可能なリソースが最も少ないホストに基づいて行われます。

手順

1 vSphere Client で、vSphere HA クラスタに移動して参照します。

2 [設定] タブをクリックします。

3 [vSphere の可用性] を選択し、[編集] をクリックします。

4 [障害および対応] をクリックし、[仮想マシンの監視] を展開します。

5 [仮想マシンの監視] および [アプリケーションの監視] を選択します。

これらの設定で、VMware Tools のハートビートとアプリケーションのハートビートがそれぞれ有効になります。

6 ハートビートの監視感度を設定するには、スライダを [低] と [高] の間で移動させるか、[カスタム] を選択してカスタム設定を指定します。

7 [OK] をクリックします。

結果

監視の設定が有効になります。

Proactive HA の構成

vCenter Server への健全性低下の通知によって、そのホストで部分的に障害が発生していることがプロバイダによって示されたときに、Proactive HA がどのように対応するかを構成できます。

このページは、vSphere DRS を有効にしている場合にのみ編集できます。

手順

1 vSphere Client で、Proactive HA クラスタに移動します。

2 [設定] タブをクリックします。

3 [vSphere の可用性] を選択し、[編集] をクリックします。

4 [Proactive HA をオンにする] チェック ボックスを選択します。

5 [Proactive HA の障害および対応] をクリックします。

6 次の構成オプションから選択します。

オプション	説明
自動化レベル	ホストを検疫モードまたはメンテナンス モードのどちらにするか、および仮想マシンの移行を推奨にするか、自動にするかについて決定します。 ■ [手動]。vCenter Server によって、仮想マシンの移行についての推奨が提案されます。 ■ [自動化]。仮想マシンは健全なホストに移行され、性能が低下したホストは、構成された Proactive HA 自動化レベルに応じて検疫モードまたはメンテナンス モードに移行します。
修正	部分的に性能が低下したホストへの対応を決定します。 ■ [すべての障害を対象とした検疫モード]。仮想マシンのパフォーマンスに影響がないかぎり、部分的に性能が低下したホストを使用せずに、パフォーマンスと可用性のバランスを調整します。 ■ [軽度の障害を対象とした検疫モードおよび重大な障害を対象としたメンテナンス モード (混合)]。仮想マシンのパフォーマンスに影響がないかぎり、性能がいくらか低下したホストを使用せずに、パフォーマンスと可用性のバランスを調整します。重大な障害が発生したホストで仮想マシンが実行されないようにします。 ■ [すべての障害を対象としたメンテナンス モード]。部分的に障害が発生したホストで仮想マシンが実行されないようにします。 ホストを検疫モードおよびメンテナンス モードにするには、`Host.Config.Quarantine` 権限と `Host.Config.Maintenance` 権限がそれぞれ必要です。

このクラスタの Proactive HA プロバイダを有効にするには、チェック ボックスを選択します。そのプロバイダに対応する vSphere Client プラグインがインストールされている場合は、プロバイダが表示されます。プロバイダは、クラスタ内のすべてのホストを監視します。プロバイダがサポートする障害状態を表示または編集するには、編集リンクをクリックします。

7 [OK] をクリックします。

アドミッション コントロールの構成

クラスタを作成したあとでアドミッション コントロールを構成して、仮想マシンが可用性の制約に違反した場合、その仮想マシンを開始できるかどうかを指定できます。指定した台数のホストに配置された実行中の仮想マシンすべてでフェイルオーバーができるように、クラスタはリソースを予約します。

アドミッション コントロール ページは、vSphere HA を有効にした場合のみ表示されます。

手順

1 vSphere Client で、vSphere HA クラスタに移動して参照します。

2 [設定] タブをクリックします。

3 [vSphere の可用性] を選択し、[編集] をクリックします。

4 [アドミッション コントロール] をクリックして構成オプションを表示します。

5 [クラスタで許容するホスト障害] で数値を選択します。これは、クラスタがリカバリできる、または確実にフェイルオーバーを行うホスト障害の最大数を示します。

6 [ホストのフェイルオーバー キャパシティの定義基準] のオプションを選択します。

オプション	説明
クラスタ リソースの割合 (%)	フェイルオーバーをサポートする予備キャパシティとして予約する、クラスタの CPU およびメモリ リソースの割合を指定します。
スロット ポリシー (パワーオン状態の仮想マシン)	パワーオンされたすべての仮想マシンに対応できる、または、固定サイズのスロット サイズ ポリシーを選択します。また、複数のスロットを必要とする仮想マシンの台数を計算することもできます。
専用フェイルオーバー ホスト	フェイルオーバー処理に使用するホストを選択します。デフォルトのフェイルオーバー ホストに十分なリソースがない場合でも、フェイルオーバー処理はクラスタ内の他のホストで実行できます。
無効	このオプションは、アドミッション コントロールを無効にして、可用性の制約に違反する仮想マシンのパワーオンを許可する場合に選択します。

7 [仮想マシンで許容するパフォーマンス低下] の割合を設定します。

この設定により、障害発生時にクラスタ内の仮想マシンに許容されるパフォーマンス低下の割合が決まります。

8 [OK] をクリックします。

結果

アドミッション コントロールの設定が有効になります。

ハートビート データストアの構成

vSphere HA は、データストア ハートビートを使用して、障害が発生したホストとネットワーク パーティションにあるホストを区別します。データストア ハートビートを使用すると、vSphere HA は、管理ネットワーク パーティションの発生時にホストを監視し、継続的に障害に対応できます。

データストア ハートビートに使用するデータストアを指定できます。

手順

1 vSphere Client で、vSphere HA クラスタに移動して参照します。

2 [設定] タブをクリックします。

3 [vSphere の可用性] を選択し、[編集] をクリックします。

4 [ハートビート データストア] をクリックして、データストア ハートビートの構成オプションを表示します。

5 データストアの選択方法と環境設定の処理方法について vSphere HA に指示するには、次のオプションから選択します。

表 2-3.

データストア ハートビートのオプション
[ホストからアクセス可能なデータストアを自動的に選択します]
[指定したリストからのデータストアのみを使用する]
[指定したリストからのデータストアを使用し、必要に応じて自動的に補足する]

6 [使用可能なハートビート データストア] ペインで、ハートビートに使用するデータストアを選択します。

一覧表示されるデータストアは、vSphere HA クラスタ内の複数のホストで共有されます。データストアを選択すると、そのデータストアにアクセスできる vSphere HA クラスタ内のホストがすべてペインの下部に表示されます。

7 [OK] をクリックします。

詳細オプションの設定

vSphere HA の動作をカスタマイズするには、vSphere HA の詳細オプションを設定します。

前提条件

クラスタの管理者権限があることを確認します。

注： これらのオプションは vSphere HA の機能に影響を与えるため、変更には注意が必要です。

手順

1 vSphere Client で、vSphere HA クラスタに移動して参照します。

2 [設定] タブをクリックします。

3 [vSphere の可用性] を選択し、[編集] をクリックします。

4 [詳細オプション] をクリックします。

5 [追加] をクリックし、詳細オプションの名前をテキスト ボックスに入力します。

値の列のテキスト ボックスでオプションの値を設定できます。

6 追加する新しい各オプションについてステップ 5 を繰り返し、[OK] をクリックします。

結果

クラスタはユーザーが追加または変更したオプションを使用します。

次のステップ

vSphere HA の詳細オプションを設定すると、次のいずれかの操作を実行するまでそのままになります。

- vSphere Client を使用することにより、その値をデフォルト値にリセットする。

- クラスタ内のすべてのホストの fdm.cfg ファイルで、オプションを手動で編集または削除する。

vSphere HA の詳細オプション

vSphere HA クラスタの動作を指定する詳細オプションを設定できます。

表 2-4. vSphere HA の詳細オプション

オプション	説明
das.isolationaddress[...]	ホストがネットワークから隔離されているかどうかを判断するため、ping を送信するアドレスを設定します。クラスタ内でほかのどのホストからもハートビートが受信されない場合にのみ、このアドレスに ping が送信されます。このアドレスが指定されていない場合は、管理ネットワークのデフォルト ゲートウェイが使用されます。このデフォルト ゲートウェイには、利用可能で信頼性の高いアドレスを指定します。これにより、ネットワークから隔離されているかどうかをホスト自身で判断することができます。クラスタには複数の隔離アドレス（10 個まで）を指定できます： das.isolationAddressX(X は 0 ～ 9)。通常は、管理ネットワークごとに 1 つ指定する必要があります。複数のアドレスを指定すると、隔離の検出に時間がかかります。
das.usedefaultisolationaddress	デフォルトでは、vSphere HA はコンソール ネットワークのデフォルト ゲートウェイを隔離アドレスとして使用します。デフォルトが使用されるかどうかをこのオプションで指定します（true または false）。
das.isolationshutdowntimeout	システムがパワーオフする前に、仮想マシンがシャットダウンするまで待機する時間を設定します。これはホストの隔離時の対応が、仮想マシンのシャットダウンの場合のみ適用されます。デフォルト値は 300 秒です。
das.slotmeminmb	メモリ スロット サイズの上限を定義します。このオプションが使用されると、スロット サイズは、この値、またはクラスタ内でパワーオン状態になっているあらゆる仮想マシンの最大メモリ予約にメモリ オーバーヘッドを加えた値よりも小さくなります。
das.slotcpuinmhz	CPU スロット サイズの上限を定義します。このオプションが使用されると、スロット サイズは、この値、またはクラスタ内でパワーオン状態になっているあらゆる仮想マシンの最大 CPU 予約よりも小さくなります。
das.vmmemoryminmb	メモリ予約が指定されていない、またはゼロの場合に、仮想マシンに割り当てるデフォルトのメモリ リソース値を定義します。これは、クラスタで許容するホスト障害アドミッション コントロール ポリシーで使用されます。値が指定されていない場合、デフォルトは 0 MB になります。
das.vmcpuminmhz	CPU 予約が指定されていない、またはゼロの場合に、仮想マシンに割り当てるデフォルトの CPU リソース値を定義します。これは、クラスタで許容するホスト障害アドミッション コントロール ポリシーで使用されます。値が指定されていない場合、デフォルトは 32MHz になります。

表 2-4. vSphere HA の詳細オプション （続き）

オプション	説明
das.iostatsinterval	仮想マシンの監視感度に対するデフォルトの I/O 統計間隔を変更します。デフォルトは 120（秒）です。0 以上の任意の値を設定できます。0 を設定すると、チェックが無効になります。 **注：** 50 未満の値は推奨されません。より小さい値を指定すると、vSphere HA が予期せずに仮想マシンをリセットする可能性があるためです。
das.ignoreinsufficienthbdatastore	ホストに vSphere HA 用の十分なハートビート データストアがない場合、作成された構成の問題を無効にします。デフォルト値は false です。
das.heartbeatdsperhost	データストアが必要とするハートビート数を変更します。有効な値は 2～5 の範囲で、デフォルトは 2 です。
das.config.fdm.isolationPolicyDelaySec	ホストが隔離されていると判断された場合に、隔離ポリシーを実行する前にシステムが待機する秒数。最小値は 30 です。30 未満の値に設定しても、遅延時間は 30 秒になります。
das.respectvmvmantiaffinityrules	vSphere HA によって、仮想マシン間の非アフィニティ ルールが強制されるかどうかを決定します。デフォルト値は「true」で、vSphere DRS が有効でない場合でもルールが適用されます。この場合、vSphere HA は仮想マシンをフェイルオーバーするとルールに反する場合はフェイルオーバーを実行しませんが、フェイルオーバーを実行するためのリソースが不足していることをレポートするイベントを発行します。このオプションは「false」にも設定でき、その場合ルールは適用されません。 非アフィニティ ルールの詳細については、『vSphere リソース管理ガイド』 を参照してください。
das.maxresets	VMCP が行うリセット試行回数の最大値です。APD (All Paths Down) 状態の影響を受ける仮想マシンでリセット操作が失敗すると、VMCP は処理を終了するまでにこの回数のリセットを試行します。
das.maxterminates	VMCP が行う仮想マシン終了の最大再試行回数です。
das.terminateretryintervalsec	VMCP が仮想マシンを終了できない場合に、システムが終了を再試行するまでに待機する時間（秒）です。
das.config.fdm.reportfailoverfailevent	1 に設定すると、vSphere HA が仮想マシンを再起動しようとして失敗したときに、仮想マシンごとの詳細なイベントを生成できます。デフォルト値は 0 です。vSphere 6.0 より前のバージョンでは、このイベントはデフォルトで生成されます。
vpxd.das.completemetadataupdateintervalsec	仮想マシンとホスト間のアフィニティ ルールが設定されてから、DRS が無効なクラスタで vSphere HA がルールを無視して仮想マシンを再起動できる時間（秒）。デフォルト値は 300 秒です。

表 2-4. vSphere HA の詳細オプション （続き）

オプション	説明
das.config.fdm.memReservationMB	デフォルトで vSphere HA エージェントは、メモリの上限 250 MB が構成された状態で実行されます。予約可能なキャパシティが不足している場合、ホストはこの予約を割り当てられないことがあります。この詳細オプションを使用してメモリの上限を減らすことで、この問題を回避できます。100 より大きい整数（最小値）のみを指定できます。反対に、(6,000 から 8,000 台の仮想マシンを含む）大規模なクラスタでプライマリ エージェントの選択中に発生する問題を回避するには、この制限を 325 MB に増やします。 **注：** この上限が変更されると、クラスタ内のすべてのホストに対して HA の再構成タスクを実行する必要があります。また、新しいホストがクラスタに追加されたり、既存のホストが再起動されるときに、そのホストに対してこのタスクを実行して、このメモリ設定を更新する必要があります。
das.reregisterrestartdisabledvms	vSphere HA が特定の仮想マシンで無効になっている場合、このオプションを使用することで、この仮想マシンが障害後に別のホストに登録されるようにします。これにより、この仮想マシンを手動で再登録せずにパワーオンできます。 **注：** このオプションを使用した場合、vSphere HA は、仮想マシンを登録するのみで、パワーオンは行いません。
das.respectvmhostsoftaffinityrules	同じ仮想マシン ホスト グループに属しているホスト上の各仮想マシンを vSphere HA が再起動するかどうかを決定します。そのような使用可能なホストがない場合、またはこのオプションの値が "false" に設定されている場合、vSphere HA はクラスタで使用可能なすべてのホスト上の仮想マシンを再起動します。vSphere 6.5 以降では、デフォルト値は「true」です。この値は、クラスタの詳細 HA オプションでは視覚的に定義されていない可能性があります。このオプションを無効にする場合は、クラスタの詳細 HA オプションで手動で「false」に設定する必要があります。

注： 次の詳細オプションのいずれかの値を変更する場合、変更を有効にするには vSphere HA を無効にしてから再度有効にする必要があります。

- das.isolationaddress[...]
- das.usedefaultisolationaddress
- das.isolationshutdowntimeout

個々の仮想マシンのカスタマイズ

vSphere HA クラスタ内の各仮想マシンには、仮想マシン再起動の優先順位、ホスト隔離時の対応、仮想マシンのコンポーネント保護、および仮想マシンの監視に対するクラスタのデフォルト設定が割り当てられます。これらのデフォルトを変更すると、仮想マシンごとに特定の動作を指定できます。仮想マシンがそのクラスタから離れると、これらの設定は失われます。

手順

1 vSphere Client で、vSphere HA クラスタに移動して参照します。

2 [設定] タブをクリックします。

3 [構成] の下で、[仮想マシンのオーバーライド] を選択して、[追加] をクリックします。

4 [+] ボタンを使用して、オーバーライドを適用する仮想マシンを選択します。

5 [OK] をクリックします。

6 （オプション）[自動化レベル]、[仮想マシン再起動の優先順位]、[ホスト隔離への対応]、VMCP 設定、[仮想マシンの監視]、または [仮想マシン監視の感度] などの設定を変更できます。

注： まず [関連するクラスタ設定] を展開してから [vSphere HA] を展開することで、これらの設定についてクラスタのデフォルトを表示できます。

7 [OK] をクリックします。

結果

これで、変更した各設定に関するこの仮想マシンの動作が、クラスタのデフォルトとは異なったものになります。

VMware vSphere® High Availability クラスタのベスト プラクティス

vSphere HA クラスタのパフォーマンスを最適化するには、特定のベスト プラクティスを実行する必要があります。このセクションでは特に、vSphere HA クラスタの主要なベスト プラクティスをいくつか取り上げます。

詳細については、発行ドキュメント『vSphere High Availability Deployment Best Practices』を参照することもできます。

ネットワークのベスト プラクティス

vSphere HA 用にホストの NIC とネットワーク トポロジを構成するには、次のベスト プラクティスを確認してください。ベスト プラクティスには、ESXi ホストや、配線、スイッチ、ルータ、ファイアウォールに対する推奨事項があります。

ネットワークの構成とメンテナンス

次のネットワーク メンテナンスに関する提案は、vSphere HA のハートビートが失われたためにホスト障害やネットワークの隔離を偶発的に検出するのを避けるのに役立ちます。

- クラスタリングされた ESXi ホストのあるネットワークを変更するときは、ホスト監視機能をサスペンドしてください。ネットワーク ハードウェアまたはネットワーク設定を変更すると、vSphere HA がホスト障害の検出に使用するハートビートが中断することがあり、仮想マシンの不要なフェイルオーバーが行われることがあります。

- ポート グループの追加、vSwitch の削除など、ESXi ホスト自体のネットワーク構成を変更するときは、ホスト監視をサスペンドしてください。ネットワーク構成を変更したあとには、クラスト内のすべてのホストで vSphere HA を再構成する必要があります。これにより、ネットワーク情報が再検査されます。次に、ホスト監視を再び有効にします。

注： ネットワークは vSphere HA の重要なコンポーネントであるため、ネットワークのメンテナンスを実行する必要がある場合は、vSphere HA の管理者に通知してください。

vSphere HA の通信に使用されるネットワーク

vSphere HA の動作に影響を与えるネットワーク操作を識別するには、ハートビートなどの vSphere HA の通信にどの管理ネットワークが使用されているかを知る必要があります。

- クラスタ内の レガシー ESX ホストでは、サービス コンソール ネットワークとして指定されたすべてのネットワークを、vSphere HA の通信が通過します。VMkernel ネットワークは、これらのホストで vSphere HA の通信に使用されません。ESX コンソール ネットワークのサブセットへの vSphere HA トラフィックを含めるには、`allowedNetworks` 詳細オプションを使用します。
- クラスタの ESXi ホストでは、vSphere HA の通信はデフォルトで VMkernel ネットワークを通過します。ESXi ホストで、vSphere HA のホストと通信するために、vCenter Server が使用するネットワーク以外のネットワークを使用する場合は、[管理トラフィック] チェック ボックスを明示的に有効にする必要があります。

vSphere HA エージェントのトラフィックを指定したネットワーク上にとどめるために、vSphere HA が使用する vmkNIC とほかの目的で使用される vmkNIC でサブネットを共有しないようにホストを設定します。vSphere HA エージェントは、vSphere HA 管理トラフィック用に構成された vmkNIC が 1 つ以上ある場合、指定されたサブネットに関連付けられている物理 NIC を使用してパケットを送信します。したがって、ネットワーク フローを確実に分離するには、vSphere HA が使用する vmkNIC と他の機能で使用される vmkNIC を、異なるサブネットに配置する必要があります。

ネットワーク隔離アドレス

ネットワーク隔離アドレスとは、ホストがネットワークから隔離されているかどうかを判断するために ping が行われる IP アドレスです。このアドレスに ping が行われるのは、ホストがクラスタ内のほかのすべてのホストからハートビートを受信しなくなった場合のみです。ホストがこのネットワーク隔離アドレスに ping 可能な場合、そのホストはネットワークから隔離されておらず、クラスタ内のほかのホストで障害が発生しているか、ネットワーク パーティション分割されています。一方、ホストが隔離アドレスに ping 不可能な場合、そのホストはネットワークから隔離されている可能性が高く、フェイルオーバー動作が行われません。

デフォルトでは、そのホストのデフォルト ゲートウェイがネットワーク隔離アドレスになります。管理ネットワークがいくつ定義されていても、デフォルトのゲートウェイとして指定されるのは 1 つだけです。追加ネットワーク用に隔離アドレスを追加するには、`das.isolationaddress[...]` 詳細オプションを使用します。vSphere HA の詳細オプションを参照してください。

ネットワーク パスの冗長性

クラスタ ノード間のネットワーク パスの冗長性は、vSphere HA の信頼性にとって重要です。単一の管理ネットワークの場合は単一点障害となるため、そのネットワークで障害が発生しただけで、フェイルオーバーが生じることがあります。管理ネットワークが 1 つしかない場合、ネットワーク障害時にハートビート データストア接続が保持されないと、ホストおよびクラスタ間で発生するすべての障害が、不要な （誤った） フェイルオーバーの原因となることがあります。そうした障害としては、NIC の故障、ネットワーク ケーブルの不良、ネットワーク ケーブルの外れ、スイッチのリセットなどがあります。このようなホスト間の障害の原因をよく検討し、ネットワークに冗長性を持たせるなどして、障害を最小限に抑制してください。

ネットワークの冗長性は、まず、NIC チーミングによって NIC レベルで実装できます。別々の物理スイッチに接続されている 2 つの NIC によるチームを使用すると、管理ネットワークの信頼性が向上します。2 つの NIC を介して（および別々のスイッチを介して） 接続されているサーバは、ハートビートを送受信する 2 つの独立したパスを持っているため、クラスタの信頼性が向上します。管理ネットワークに NIC チームを構成するには、有効またはスタンバイの構成の vSwitch 構成で vNIC を構成します。推奨される vNIC のパラメータ設定は、次のとおりです。

- デフォルトのロード バランシング = 発信元のポート ID に基づいたルート
- フェイルバック = なし

vSphere HA クラスタのホストに NIC を追加したあと、そのホストで vSphere HA を再構成する必要があります。

ほとんどの実装で、NIC チーミングは十分なハードビートの冗長性を確保しますが、別の方法として、別の仮想スイッチに接続する 2 番目の管理ネットワーク接続を作成することもできます。冗長な管理ネットワークでは、複数のネットワークを介してハートビートを送信できるため、信頼性の高い障害検出が可能になり、隔離状態またはパーティション状態の発生を防ぐことができます。元の管理ネットワーク接続は、ネットワークおよび管理の目的で使用します。2 番目の管理ネットワーク接続を作成すると、vSphere HA は両方の管理ネットワーク接続でハートビートを送信します。いずれかのパスに障害が発生しても、vSphere HA は、もう一方のパスでハートビートを送受信します。

注： クラスタ内のサーバ間で、できるだけ少ない数のハードウェア セグメントを構成します。これは、単一点障害を制限することが目的です。また、ルートのホップ数が多すぎる場合も、ハートビート用のネットワーク パケット遅延の原因となり、障害点が増加します。

IPv6 ネットワーク構成の使用

vSphere HA クラスタによって使用される所定のネットワーク インターフェイスに、1 つの IPv6 アドレスのみを割り当てることができます。複数の IP アドレスを割り当てても、クラスタのプライマリ ホストから送信されるハートビート メッセージ数が増えるだけで、それに伴う利点はありません。

相互運用性のベスト プラクティス

vSphere HA と他の機能との間で相互運用性を可能にするには、次のベスト プラクティスを確認してください。

バージョンが混在クラスタにおける vSphere HA および Storage vMotion の相互運用性

ESXi 5.x ホストおよび ESX/ESXi 4.1 以前のホストが含まれるクラスタにおいて、Storage vMotion が広範囲に使用されているか、Storage DRS が有効な場合は、vSphere HA をデプロイしないでください。vSphere HA は、ホスト障害に対応するために、障害の前に仮想マシンが稼動していたものとは ESXi のバージョンが異なるホスト上で、仮想マシンを再起動する場合があります。障害発生時に、仮想マシンが ESXi 5.x ホスト上で Storage vMotion のアクションに関わっており、vSphere HA が ESXi 5.0 より前のバージョンのホスト上で仮想マシンを再起動すると、問題が発生する可能性があります。仮想マシンはパワーオンする可能性がありますが、続くスナップショット処理で試みられる操作が vdisk の状態を破損し、仮想マシンが利用できないままになる恐れがあります。

vSphere HA を使用した Auto Deploy の使用

vSphere HA と Auto Deploy を合わせて使用し、仮想マシンの可用性を向上させることができます。Auto Deploy はホストがパワーオンする際にホストをプロビジョニングします。また、ブート時にホスト上に vSphere HA エージェントをインストールするよう設定することも可能です。詳細については、『vSphere Installation and Setup』 に含まれている Auto Deploy ドキュメントを参照してください。

vSAN を使用したクラスタでのホストのアップグレード

vSphere HA クラスタ内の ESXi ホストをバージョン 5.5 以降にアップグレードし、さらに vSAN も使用したい場合は、次のプロセスを実行します。

1 すべてのホストをアップグレードします。

2 vSphere HA を無効にします。

3 vSAN を有効にします。

4 vSphere HA を再度有効にします。

クラスタ監視のベスト プラクティス

vSphere HA クラスタのステータスと有効性を監視するには、次のベスト プラクティスを確認してください。

アラームの設定によるクラスタ変化の監視

vSphere HA または Fault Tolerance が、仮想マシンのフェイルオーバーなど、可用性維持のためのアクションを実行したときに通知を受けることができます。このようなアクションがトリガーとなるアラームを vCenter Server で設定し、指定した管理者グループにメールなどでアラートを通知できます。

デフォルトで、いくつかの vSphere HA アラームが利用できます。

- フェイルオーバーのリソース不足（クラスタのアラーム）
- プライマリが不明（クラスタのアラーム）
- フェイルオーバー処理中（クラスタのアラーム）
- ホスト HA ステータス（ホストのアラーム）
- 仮想マシン監視エラー（仮想マシンのアラーム）
- 仮想マシン監視アクション（仮想マシンのアラーム）

- フェイルオーバー失敗（仮想マシンのアラーム）

注： デフォルトのアラームには、vSphere HA の機能名が含まれています。

HA VIB の動作の変更

vSphere 7.0 以降では、Lifecycle Manager (vLCM) クラスタで HA が有効な場合に、HA VIB が削除されることがあります。以前のリリースでは、vCenter Server によって ESXi ホストからの HA VIB の削除が試行されることはありませんでした。

この状況は、vSphere HA が有効な vLCM クラスタでのみ発生します。クラスタで vSphere HA を無効にした後に、（ユーザーが開始した操作または API 呼び出しとして）vLCM の [修正] 処理が行われると、vSphere HA VIB が結果として削除されることがあります。

注： HA が再度有効になると、vCenter Server によって必要な vSphere HA VIB がプッシュされるため、この動作の変更による悪影響はありません。

仮想マシンの Fault Tolerance の準備 3

仮想マシンで vSphere Fault Tolerance を使用すると、高いレベルの可用性とデータ保護によって継続性を確保できます。

Fault Tolerance は、ESXi のホスト プラットフォームに構築され、別々のホストで同一の仮想マシンを実行することにより、可用性を提供します。

Fault Tolerance で最適化な結果を得るには、Fault Tolerance がどのように機能するのか、クラスタおよび仮想マシンに対して Fault Tolerance をどのように有効にするか、およびその使用法に対するベスト プラクティスについてよく理解しておく必要があります。

次のトピックを参照してください。

- Fault Tolerance の機能
- Fault Tolerance の使用事例
- Fault Tolerance の要件、制限、およびライセンス
- Fault Tolerance の相互運用性
- Fault Tolerance に向けたクラスタとホストの準備
- Fault Tolerance の使用
- Fault Tolerance 暗号化の有効化
- Fault Tolerance のベスト プラクティス
- Metro Cluster Fault Tolerance の有効化
- レガシー Fault Tolerance
- フォールト トレランス機能を持つ仮想マシンのトラブルシューティング

Fault Tolerance の機能

vSphere Fault Tolerance (FT) は、ほとんどのミッション クリティカルな仮想マシンで使用できます。FT では、継続的に使用できる同一の仮想マシンを別に作成して維持し、フェイルオーバーの発生時にそのマシンで置き換えることにより、ミッション クリティカルな仮想マシンに継続的な可用性を提供します。

保護された仮想マシンは、プライマリ仮想マシンと呼ばれます。複製された仮想マシンであるセカンダリ仮想マシンは、別のホストで作成されて実行されます。プライマリ仮想マシンがセカンダリ仮想マシンに絶えずレプリケートされ、セカンダリ仮想マシンがいつでも引き継ぐことができるため、Fault Tolerance 保護が確保されます。

プライマリ仮想マシンとセカンダリ仮想マシンは、相互にステータスを監視して Fault Tolerance が確保されるようにします。透過的フェイルオーバーは、プライマリ仮想マシンを実行しているホストで障害が発生した場合、またはプライマリ仮想マシンのメモリで修正不能なハードウェア エラーが発生した場合に発生します。この場合、セカンダリ仮想マシンがすぐに有効化され、プライマリ仮想マシンと置き換えられます。新しいセカンダリ仮想マシンが起動し、Fault Tolerance の冗長性が自動的に再確立されます。セカンダリ仮想マシンが稼動しているホストで障害が発生すると、その場合もすぐに置き換えられます。いずれの場合も、ユーザーはサービスの中断やデータの損失を意識しません。

フォールト トレランス対応の仮想マシン、およびそのセカンダリ コピーは、同じホスト上で実行することはできません。この制限により、ホストで障害が発生しても、仮想マシンが両方とも失われることがなくなります。

注： また、仮想マシンとホスト間のアフィニティ ルールを使用して、どのホストで仮想マシンを実行できるかを指定できます。これらのルールを使用する場合は、このようなルールの影響を受けるプライマリ仮想マシンすべてにおいて、関連付けられているセカンダリ仮想マシンも同じルールの影響を受けることを理解しておきます。アフィニティ ルールの詳細については、『vSphere リソース管理』ドキュメントを参照してください。

Fault Tolerance では、障害からのリカバリ後に 1 台の仮想マシンの 2 つのアクティブ コピーが存在する、「スプリット ブレーン」状態が防止されます。共有ストレージでアトミック ファイル ロックを使用してフェイルオーバーが調整され、一方のみがプライマリ仮想マシンとして稼動を続け、新しいセカンダリ仮想マシンが自動的に再作成されます。

vSphere Fault Tolerance は、最大で 8 つの vCPU を持つ対称型マルチプロセッサ (SMP) 仮想マシンに対応できます。

Fault Tolerance の使用事例

いくつかの典型的な状況で、vSphere Fault Tolerance を使用してメリットを得ることができます。

Fault Tolerance は、vSphere HA よりも高いレベルのビジネス継続性を実現します。対応するプライマリ仮想マシンを置き換えるためにセカンダリ仮想マシンが呼び出されると、セカンダリ仮想マシンは、仮想マシン全体の状態が保持されまま、すぐにプライマリ仮想マシンのロールを引き継ぎます。アプリケーションはすでに稼動し、メモリに格納されているデータを再入力または再ロードする必要はありません。vSphere HA によって提供されるフェイルオーバーは、障害により影響を受ける仮想マシンを再起動します。

より高度なレベルの継続性、および状態情報やデータ保護の強化により、Fault Tolerance をデプロイするタイミングのシナリオが通知されます。

- 常時使用可能である必要があるアプリケーション。特に、ユーザーがハードウェア障害中にも維持することを希望する長期クライアント接続を持つアプリケーション。
- カスタム アプリケーションで、これよりほかにクラスタリングを行う方法がない場合。
- カスタム クラスタリング ソリューションによって高可用性が提供されるが、これらのソリューションが複雑で構成および保持できない場合。

Fault Tolerance を使用して仮想マシンを保護するための、別の重要な使用事例として、オンデマンドの Fault Tolerance を挙げることができます。この場合、通常の操作では、仮想マシンは vSphere HA によって十分に保護されます。特定の重要な期間では、仮想マシンの保護を強化したいことがあります。たとえば、四半期の終わりにレポートを実行することがありますが、このレポートが中断されると、重要な情報の入手が遅延する可能性がありま

す。vSphere Fault Tolerance を使用すると、このレポートを実行する前にこの仮想マシンを保護し、レポートを生成した後で Fault Tolerance をオフまたはサスペンドすることができます。オンデマンドの Fault Tolerance を使用すると、重要な期間に仮想マシンを保護し、重要ではない操作のときには、リソースを通常の状態に戻すことができます。

Fault Tolerance の要件、制限、およびライセンス

vSphere Fault Tolerance (FT) を使用する前に、この機能に適用される要件、制限、およびライセンスについて検討します。

要件

次の CPU 要件とネットワーク要件が FT に適用されます。

フォルト トレランス対応仮想マシン用のホスト マシンに使用される CPU には、vSphere vMotion との互換性が必要です。また、ハードウェア MMU 仮想化（Intel EPT または AMD RVI）をサポートする CPU が必要です。次の CPU がサポートされています。

- Intel Sandy Bridge 以降。Avoton はサポートされていません。
- AMD Bulldozer 以降。

FT には 10 Gbit ログ記録ネットワークを使用し、ネットワークが低遅延であることを確認します。FT 専用のネットワークを使用することをお勧めします。

注： Fault Tolerance は現在、NSX-T で作成されたポートグループ（VLAN またはオーバーレイ セグメント）を使用している仮想マシンでは有効にできません。Fault Tolerance は、NSX-T Manager および Edge ノードでもサポートされていません。

制限

Fault Tolerance を使用するように構成されたクラスタでは、2 つの制限が個別に適用されます。

das.maxftvmsperhost

クラスタの 1 台のホストで許容されるフォールト トレランス対応仮想マシンの最大数。デフォルト値は 4 です。ホストあたりの FT 仮想マシン数に上限はありません。FT 仮想マシンでワークロードが適切に実行されている場合は、さらに大きな値を使用できます。値を 0 に設定すると、チェックを無効にできます。

das.maxftvcpusperhost

ホスト上のすべてのフォルト トレランス仮想マシンで集計される vCPU の最大数。デフォルト値は 8 です。ホストあたりの FT vCPU の数に上限はありません。ワークロードが適切に実行されている場合は、さらに大きな値を使用できます。値を 0 に設定すると、チェックを無効にできます。

ライセンス

1 台のフォールト トレランス対応仮想マシンによってサポートされる vCPU の数は、購入した vSphere のライセンスのレベルによって制限されます。Fault Tolerance は次のようにサポートされます。

- vSphere Standard と vSphere Enterprise。最大 2 つの vCPU を許可

- vSphere Enterprise Plus。最大 8 つの vCPU を許可

注： Fault Tolerance は、vSphere Standard、vSphere Enterprise、vSphere Enterprise Plus の各エディションでサポートされます。

Fault Tolerance の相互運用性

vSphere Fault Tolerance を構成する前に、Fault Tolerance と相互運用できない機能および製品について理解しておく必要があります。

Fault Tolerance でサポートされない vSphere の機能

クラスタを構成するときには、一部の vSphere 機能は Fault Tolerance に組み込むことができないことを理解しておく必要があります。

vSphere の次の機能は、フォールト トレランス対応の仮想マシンに対してサポートされていません。

注： vSphere 7.0 Update 2 より前のリリースでは、vSphere 仮想マシンの暗号化は FT でサポートされませんでした。

- スナップショット。仮想マシンで Fault Tolerance を有効にする前に、スナップショットを削除またはコミットしておく必要があります。また、Fault Tolerance が有効になっている仮想マシンでスナップショットを作成することはできません。

  注： vStorage APIs - Data Protection (VADP) のバックアップで作成されたディスク専用スナップショットは、Fault Tolerance によってサポートされています。ただし、レガシー FT は VADP をサポートしていません。

- Storage vMotion。Fault Tolerance がオンになった仮想マシンに対して、Storage vMotion を起動することはできません。ストレージを移行するには、Fault Tolerance を一時的にオフにして、ストレージの vMotion アクションを実行します。この処理が終了したら、Fault Tolerance をもう一度オンにすることができます。
- リンク クローン。リンク クローンの仮想マシンで Fault Tolerance を使用したり、Fault Tolerance が有効になっている仮想マシンからリンク クローンを作成したりすることはできません。
- Virtual Volumes データストア。
- ストレージベース ポリシー管理。ストレージ ポリシーは、vSAN ストレージにはサポートされます。
- I/O フィルタ。
- VBS が有効にされた仮想マシン。
- 仮想マシン名前空間 DB および仮想マシンの DataSet。

Fault Tolerance と互換性のない機能とデバイス

サード パーティのデバイス、機能、または製品の中には、Fault Tolerance と相互運用できないものもあります。

仮想マシンで Fault Tolerance を使用できるようにするには、仮想マシンで次の機能またはデバイスを使用しないでください。

表 3-1. Fault Tolerance と互換性のない機能とデバイス、および対策

互換性のない機能またはデバイス	対策
物理的な Raw ディスク マッピング （RDM）。	レガシー FT により、物理 RDM でバッキングされた仮想デバイスを使用している仮想マシンを、仮想 RDM を使用するように再構成することができます。
物理デバイスまたはリモート デバイスでバッキングされた CD-ROM またはフロッピー仮想デバイス。	CD-ROM またはフロッピー仮想デバイスを削除するか、共有ストレージにインストールされている ISO でバッキングを再構成します。
USB およびサウンド デバイス。	これらのデバイスを仮想マシンから削除します。
N_Port ID Virtualization （NPIV）。	仮想マシンの NPIV 構成を無効にします。
NIC パススルー。	この機能は Fault Tolerance でサポートされていないため、オフにする必要があります。
ホット プラギング デバイス。	Fault Tolerance 対応の仮想マシンに対して、ホット プラグ機能は自動的に無効になります。デバイスをホットプラグするには、取り付ける場合でも取り外す場合でも、少しの間 Fault Tolerance をオフにしてホットプラグを実行してから、Fault Tolerance をオンにします。 **注：** Fault Tolerance を使用するとき、仮想マシンを実行中に仮想ネットワーク カードの設定を変更するのはホットプラグ操作になります。それは、ネットワーク カードを「取り外して （アンプラギング）」から再度「取り付ける （プラギング）」必要があるからです。たとえば実行中の仮想マシンの仮想ネットワーク カード （仮想 NIC） が接続されているネットワークを変更する場合、Fault Tolerance を最初にオフにする必要があります。
シリアル ポートまたはパラレル ポート	これらのデバイスを仮想マシンから削除します。
3D を有効にしたビデオ デバイス。	Fault Tolerance は、3D を有効にしたビデオ デバイスをサポートしていません。
仮想マシン通信インターフェイス （VMCI）	Fault Tolerance によってサポートされていません。
2TB を超える VMDK	Fault Tolerance は、2TB を超える VMDK ではサポートされていません。

Fault Tolerance と DRS の併用

vSphere Fault Tolerance を vSphere Distributed Resource Scheduler (DRS) と併用できます。

Fault Tolerance 仮想マシンは EVC がなくても DRS をサポートできます。vSphere 6.7 以降の VC によって管理されている vSphere 6.5 および 6.0 ホストでは、Fault Tolerance と DRS を併用できます。

注： vSphere DRS は、vSphere の重要な機能で、vSphere クラスタ内で実行されるワークロードの健全性の維持に必要です。vSphere 7.0 Update 1 以降では、DRS は vCLS 仮想マシンの可用性に依存します。詳細については、『vSphere のリソース管理』の「vSphere クラスタ サービス (vCLS)」を参照してください。

Fault Tolerance に向けたクラスタとホストの準備

クラスタの vSphere Fault Tolerance を有効にするには、機能の前提条件を満たしてから、ホストでいくつかの構成手順を実行する必要があります。これらの手順が完了してクラスタが作成されたあと、構成が Fault Tolerance を有効にするための要件に準拠しているかどうかを確認することもできます。

クラスタの Fault Tolerance をセットアップにする前に、次のタスクを完了しておく必要があります。

- クラスタ、ホスト、および仮想マシンが、Fault Tolerance チェックリストで概説されている要件を確実に満たすようにする。
- 各ホストのネットワークを構成する。
- vSphere HA クラスタを作成し、ホストを追加して、コンプライアンスをチェックする。

クラスタとホストで Fault Tolerance の準備ができると、仮想マシンのフォールト トレランスをオンにできます。Fault Tolerance をオンを参照してください。

Fault Tolerance のチェックリスト

次のチェックリストに記載されているクラスタ、ホスト、仮想マシンの各要件は、vSphere Fault Tolerance を使用する前に確認しておく必要があります。

Fault Tolerance の設定前に、このリストを参照してください。

注： フォールト トレラント仮想マシンのフェイルオーバーは vCenter Server とは無関係ですが、Fault Tolerance クラスタは、vCenter Server を使用して設定する必要があります。

Fault Tolerance のクラスタ要件

Fault Tolerance を使用する前に、次のクラスタ要件を満たしている必要があります。

- Fault Tolerance のログおよび vMotion ネットワークが構成されている。ホスト マシンのネットワークの構成を参照してください。
- vSphere HA クラスタが作成され、有効となっています。vSphere HA クラスタの作成を参照してください。フォールト トレランス対応の仮想マシンをパワーオンする前、またはフォールト トレランス対応の仮想マシンがすでにサポートされているクラスタにホストを追加する前に、vSphere HA を有効にする必要があります。

Fault Tolerance でのホストの要件

Fault Tolerance を使用するには、次のホストの要件を満たしている必要があります。

- ホストではサポートされるプロセッサを使用する必要があります。
- ホストが Fault Tolerance 用にライセンスされている必要があります。
- ホストが Fault Tolerance 用に認定されている。http://www.vmware.com/resources/compatibility/search.php を参照して、[Search by Fault Tolerant Compatible Sets] を選択し、使用するホストが認定されているかどうかを確認します。

- 各ホストの構成で、BIOS のハードウェア仮想化 （HV） を有効にしている。

注： FT 仮想マシンをサポートするために使用するホストでは、BIOS 電源管理設定を「Maximum performance」または「OS-managed performance」に切り替えることをお勧めします。

フォールト トレランスをサポートするために、クラスタ内のホストの互換性を確認するには、#unique_60 に記載されているように、プロファイルのコンプライアンス チェックを実行します。

Fault Tolerance での仮想マシンの要件

Fault Tolerance を使用する前に、次の仮想マシンの要件を満たしている必要があります。

- サポートされていないデバイスが仮想マシンに接続されていない。Fault Tolerance の相互運用性を参照してください。
- フォールト トレランス対応の仮想マシンで、互換性のない機能が実行されていない。Fault Tolerance の相互運用性を参照してください。
- 仮想マシン ファイル（VMDK ファイルを除く）は、共有ストレージ上に保存する必要があります。使用できる共有ストレージのソリューションには、ファイバ チャネル、（ハードウェアおよびソフトウェア）iSCSI、vSAN、NFS、および NAS があります。

構成に関するその他の推奨事項

Fault Tolerance の構成時には、次のガイドラインにも従ってください。

- 共有ストレージにアクセスするために NFS を使用している場合は、Fault Tolerance が正しく機能するのに必要なネットワーク パフォーマンスを得るために、少なくとも 1Gbit NIC の専用 NAS ハードウェアを使用する必要があります。
- Fault Tolerance がオンになると、フォールト トレランス対応仮想マシンのメモリ予約は仮想マシンのメモリ サイズに設定されます。必ず、フォールト トレランス対応仮想マシンを含むリソース プールに仮想マシンのメモリ サイズより多くのメモリ リソースがあるように設定してください。リソース プールに余分なメモリがないと、オーバーヘッド メモリとして使用できるメモリがなくなる場合があります。
- 冗長性を確保し、Fault Tolerance による最大限の保護を得るためには、クラスタ内に 3 台以上のホストを用意する必要があります。そうすることで、フェイルオーバー時に作成された新しいセカンダリ仮想マシンを収容するホストを確保できます。

ホスト マシンのネットワークの構成

vSphere HA クラスタに追加する各ホスト上で、2 つの異なるネットワーク スイッチ（vMotion と FT ログ記録）を構成して、ホストが vSphere Fault Tolerance をサポートできるようにする必要があります。

1 台のホストに対して Fault Tolerance を設定にするには、この手順をポート グループ オプション（vMotion と FT ログ記録）ごとに実行して、Fault Tolerance のログ記録用に十分なバンド幅を確保する必要があります。一方のオプションを選択し、手順を実行してから、もう一方のポート グループ オプションを選択して再び同じ手順を繰り返します。

前提条件

ギガビットのネットワーク インターフェイス カード （NIC） が複数枚必要です。Fault Tolerance をサポートする各ホストについて、最低でも 2 つの物理 NIC を搭載することをお勧めします。たとえば、Fault Tolerance のログ専用に 1 つと、vMotion 専用に 1 つ必要です。可用性を確保するためには、3 つ以上の NIC を使用してください。Fault Tolerance の要件、制限、およびライセンスを参照してください。

手順

1 vSphere Client で、ホストに移動して参照します。

2 [構成] タブをクリックし、[ネットワーク] をクリックします。

3 [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ます。

5 接続タイプに該当する情報を入力します。

6 [終了] をクリックします。

結果

vMotion と Fault Tolerance のログの両方の仮想スイッチを作成したあとに、必要に応じてほかの仮想スイッチを作成できます。ホストをクラスタに追加し、Fault Tolerance をオンにするための手順を完了します。

次のステップ

注： FT をサポートするようネットワークを構成すると、その後 Fault Tolerance のログ用ポートをサスペンドしても、すでにパワーオンされている Fault Tolerance 対応の仮想マシンのペアはパワーオンされたままになります。フェイルオーバーの状況が発生した場合、プライマリ仮想マシンがそのセカンダリ仮想マシンで置き換えられると、新しいセカンダリ仮想マシンは起動されないため、新しいプライマリ仮想マシンは保護されていない状態で動作します。

Fault Tolerance の使用

クラスタ用の vSphere Fault Tolerance を有効にするために必要なすべての手順を行ったあと、個々の仮想マシンでフォールト トレランス機能をオンにすると、この機能を使用できます。

Fault Tolerance をオンにする前に、仮想マシンで検証が実行されます。

これらの検証に合格し、仮想マシンの vSphere Fault Tolerance をオンにすると、そのコンテキスト メニューの Fault Tolerance セクションに新しいオプションが追加されます。このオプションには、Fault Tolerance のオフまたは無効化、セカンダリ仮想マシンの移行、フェイルオーバーのテスト、セカンダリ仮想マシンの再起動テストがあります。

Fault Tolerance をオンにするときの検証

Fault Tolerance をオンにするオプションを利用できる場合であってもこのタスクは検証が必要であり、特定の要件が満たされない場合は失敗する可能性があります。

仮想マシンの Fault Tolerance をオンにするときは、いくつかの検証が行われます。

- vCenter Server 設定で SSL 証明書の確認が有効になっている。
- ホストが vSphere HA クラスタまたは vSphere HA と DRS の混合クラスタに属している。
- ホストに ESXi 6.x 以降がインストールされている。
- 仮想マシンにスナップショットがない。
- 仮想マシンがテンプレートではない。
- 仮想マシンで vSphere HA が無効になっていない。
- 仮想マシンが 3D 対応のビデオ デバイスを持っていない。

パワーオン状態の仮想マシンの確認

パワーオン済み （またはパワーオン処理中） の仮想マシンに対しては、これ以外の検証も行われます。

- Fault Tolerance 機能をオンにする仮想マシンが配置されているホストの BIOS で、ハードウェア仮想化 (HV) が有効になっている。
- プライマリ仮想マシンをサポートするホストのプロセッサが Fault Tolerance に対応している。
- 使用するハードウェアに、Fault Tolerance との互換性があることが認定されている。互換性があることを確認するには、http://www.vmware.com/resources/compatibility/search.php の VMware 互換性ガイドで、[Search by Fault Tolerant Compatible Sets] を選択します。
- 仮想マシンの構成で、Fault Tolerance の併用が有効である。たとえば、サポートしていないデバイスが構成に含まれていない必要があります。

セカンダリ仮想マシンの配置

仮想マシンの Fault Tolerance をオンにするための検証に合格すると、セカンダリ仮想マシンが作成されます。セカンダリ仮想マシンの配置と初期のステータスは、Fault Tolerance をオンにするときにプライマリ仮想マシンがパワーオンされているか、パワーオフされているかによって異なります。

プライマリ仮想マシンがパワーオンされている場合

- プライマリ仮想マシンの状態がすべてコピーされ、セカンダリ仮想マシンが作成されて、互換性のある別のホストに配置されます。そして、アドミッション コントロールで許可されるとパワーオンされます。
- 仮想マシンの表示される Fault Tolerance のステータスは、[保護済み] です。

プライマリ仮想マシンがパワーオフされている場合

- セカンダリ仮想マシンがすぐに作成され、クラスタ内のホストに登録されます （パワーオン時に、より適切なホストに再登録される場合があります）。
- セカンダリ仮想マシンは、プライマリ仮想マシンのパワーオン後にパワーオンされます。
- 仮想マシンに表示される Fault Tolerance のステータスは、[保護されていません]、[仮想マシンは実行されていません] です。
- Fault Tolerance がオンになったあとでプライマリ仮想マシンをパワーオンしようとすると、前述の検証が追加で実行されます。

前述の検証に合格すると、プライマリ仮想マシンとセカンダリ仮想マシンがパワーオンされ、互換性のあるホストに別々に配置されます。仮想マシンの Fault Tolerance のステータスには、[保護済み] というタグが付けられます。

Fault Tolerance をオン

vSphere Client を使用して vSphere Fault Tolerance をオンにすることができます。

Fault Tolerance がオンになると、vCenter Server は仮想マシンのメモリ制限の設定をリセットし、メモリ予約を仮想マシンのメモリ サイズに設定します。Fault Tolerance をオンのままにしていると、メモリの予約、サイズ、制限、vCPU 数、シェアを変更できません。また、仮想マシンのディスクを追加または削除することもできません。Fault Tolerance をオフにしても、変更されたパラメータは元の値に戻りません。

クラスタの管理者権限を持つアカウントを使用して、vSphere Client を vCenter Server に接続します。

前提条件

次のいずれかの条件に該当する場合、フォールト トレランスをオンにするオプションは利用できません （淡色で表示）。

- この機能のライセンスがないホストに仮想マシンが配置されている。
- メンテナンス モードまたはスタンバイ モードのホストに仮想マシンが配置されている。
- 仮想マシンが切断されているか実態なしの状態である （.vmx ファイルにアクセスできない）。
- この機能をオンにする権限がユーザーにない。

手順

1. vSphere Client で、Fault Tolerance をオンにする仮想マシンに移動して参照します。
2. 仮想マシンを右クリックし、[Fault Tolerance] - [Fault Tolerance をオンにする] を選択します。
3. [はい] をクリックします。
4. セカンダリ仮想マシンの構成ファイルを配置するデータストアを選択します。その後、[次へ] をクリックします。
5. セカンダリ仮想マシンを配置するホストを選択します。その後、[次へ] をクリックします。
6. 選択内容を確認し、[終了] をクリックします。

結果

指定した仮想マシンはプライマリ仮想マシンとして設定され、セカンダリ仮想マシンがほかのホスト上に作成されます。これで、プライマリ仮想マシンはフォールト トレランス対応になりました。

注： Fault Tolerance をオンにするプロセスでは、仮想マシンのデータストアとメモリがレプリケートされます。レプリケートされるデータのサイズによって、これには数分かかることがあります。レプリケーションが完了するまで、仮想マシンは保護されている状態と表示されません。

Fault Tolerance をオフ

vSphere Fault Tolerance をオフにすると、セカンダリ仮想マシンとその構成、およびすべての履歴が削除されます。

この機能を再び有効にする予定がない場合、[Fault Tolerance をオフにする] オプションを使用します。それ以外の場合は、[Fault Tolerance のサスペンド] オプションを使用します。

注： セカンダリ仮想マシンが配置されているホストの状態がメンテナンス モード、切断、または応答なしの場合、[Fault Tolerance をオフにする] オプションは使用できません。この場合は、Fault Tolerance をサスペンドして再開する必要があります。

手順

1 vSphere Client で、Fault Tolerance をオフにする仮想マシンに移動して参照します。

2 仮想マシンを右クリックし、[Fault Tolerance] - [Fault Tolerance をオフにする] を選択します。

3 [はい] をクリックします。

結果

選択した仮想マシンで Fault Tolerance がオフになります。選択した仮想マシンの履歴とセカンダリ仮想マシンが削除されます。

注： セカンダリ仮想マシンが起動プロセスの途中の場合、Fault Tolerance をオフにすることはできません。この状態ではプライマリ仮想マシンのすべての状態をセカンダリ仮想マシンに同期することが必要になるため、通常よりも長い時間がかかることがあります。

Fault Tolerance のサスペンド

仮想マシンの vSphere Fault Tolerance をサスペンドすると、Fault Tolerance の保護機能はサスペンドされますが、セカンダリ仮想マシンとその構成、およびすべての履歴は維持されます。Fault Tolerance の保護機能を今後再開する場合は、このオプションを使用します。

手順

1 vSphere Client で、Fault Tolerance をサスペンドする仮想マシンを参照します。

2 仮想マシンを右クリックし、[Fault Tolerance] - [Fault Tolerance のサスペンド] を選択します。

3 [はい] をクリックします。

結果

選択した仮想マシンで、Fault Tolerance がサスペンドされます。すべての履歴および選択した仮想マシンのセカンダリ仮想マシンは保存され、今後再開されたときに使用されます。

次のステップ

Fault Tolerance をサスペンドした後に、機能を再開する場合は、[Fault Tolerance の再開] を選択します。

セカンダリの移行

プライマリ仮想マシンの vSphere Fault Tolerance をオンにしたあと、関連付けられたセカンダリ仮想マシンを移行できます。

手順

1 vSphere Client で、セカンダリ仮想マシンを移行するプライマリ仮想マシンに移動して参照します。

2 仮想マシンを右クリックし、[Fault Tolerance] - [セカンダリの移行] を選択します。

3 [移行] ダイアログ ボックスでオプション設定を完了し、行った変更を確認します。

4 [完了] をクリックして変更内容を適用します。

結果

選択したフォールト トレランス機能を持つ仮想マシンに関連付けられているセカンダリ仮想マシンが、指定したホストに移行されます。

フェイルオーバーのテスト

選択したプライマリ仮想マシンにフェイルオーバーの状況を発生させ、Fault Tolerance による保護をテストできます。

仮想マシンがパワーオフ状態の場合、このオプションは利用できません （灰色で表示）。

手順

1 vSphere Client で、フェイルオーバーをテストするプライマリ仮想マシンに移動して参照します。

2 仮想マシンを右クリックし、[Fault Tolerance] - [フェイルオーバーのテスト] を選択します。

3 タスク コンソールにフェイルオーバーに関する詳細が表示されます。

結果

このタスクでは、プライマリ仮想マシンに障害を発生させて、セカンダリ仮想マシンへのフェイルオーバーが行われることを確認します。新規のセカンダリ仮想マシンも起動し、プライマリ仮想マシンが保護済みの状態に戻ります。

セカンダリの再起動テスト

セカンダリ仮想マシンに障害を発生させて、選択したプライマリ仮想マシンで提供される Fault Tolerance の保護をテストできます。

仮想マシンがパワーオフ状態の場合、このオプションは利用できません （灰色で表示）。

手順

1 vSphere Client で、テストを実行するプライマリ仮想マシンに移動して参照します。

2 仮想マシンを右クリックし、[Fault Tolerance] - [セカンダリの再起動テスト] を選択します。

3 タスク コンソールにテストに関する詳細が表示されます。

結果

このタスクによって、選択したプライマリ仮想マシンに Fault Tolerance の保護を提供するセカンダリ仮想マシンが停止します。新規のセカンダリ仮想マシンが起動し、プライマリ仮想マシンが保護済みの状態に戻ります。

Fault Tolerance で使用するホストのアップグレード

次の手順を使用して、Fault Tolerance に使用するホストをアップグレードします。

前提条件

クラスタの管理者権限があることを確認します。

パワーオンされたフォールト トレランス対応の仮想マシンをホストする、4 台以上の ESXi ホストのセットがあることを確認します。仮想マシンがパワーオフされている場合は、プライマリとセカンダリの仮想マシンを異なるビルドのホストに再配置できます。

注： このアップグレード手順は、最低 4 ノードのクラスタ用のものです。さらに小規模なクラスタでも同じ手順で実行できますが、保護されない期間が多少長くなります。

手順

1. vMotion を使用して、2 台のホストからフォールト トレランス対応の仮想マシンを移行します。
2. 退避した 2 台のホストを同じ ESXi ビルドにアップグレードします。
3. プライマリ仮想マシンで Fault Tolerance をサスペンドします。
4. VMotion を使用して、Fault Tolerance をサスペンドしたプライマリ仮想マシンを、アップグレードされたホストの 1 つに移動します。
5. 移動したプライマリ仮想マシンで Fault Tolerance を再開します。
6. アップグレード後のホストに格納可能なフォールト トレランス対応仮想マシン ペアの数だけ、手順 1 から手順 5 を繰り返します。
7. vMotion を使用して、フォールト トレランス対応の仮想マシンを再配分します。

結果

クラスタ内のすべての ESXi ホストがアップグレードされます。

Fault Tolerance 暗号化の有効化

Fault Tolerance ログ トラフィックを暗号化できます。

vSphere Fault Tolerance はプライマリ仮想マシンとセカンダリ仮想マシン間のチェックを頻繁に実行するため、最後に成功したチェックポイントからセカンダリ仮想マシンをすばやくレジュームできます。チェックポイントには、前のチェックポイント以降に変更された仮想マシンの状態が含まれます。Fault Tolerance ログ トラフィックを暗号化できます。

Fault Tolerance を有効にした場合、FT 暗号化はデフォルトで [任意] に設定されます。つまり、プライマリ ホストとセカンダリ ホストの両方で暗号化が可能な場合にのみ、暗号化が有効になります。FT 暗号化モードを手動で変更する必要がある場合は、次の手順を実行します。

注： Fault Tolerance は、vSphere 7.0 Update 2 以降での vSphere 仮想マシンの暗号化をサポートします。ゲスト内およびアレイベースの暗号化は、仮想マシンの暗号化に依存したり、仮想マシンの暗号化に干渉したりすることはありません。複数の暗号化レイヤーを使用すると、コンピューティング リソースが追加で使用され、仮想マシンのパフォーマンスに影響を与える可能性があります。この影響は、ハードウェアのほか、I/O の量とタイプによって異なりますが、全体的なパフォーマンスへの影響は多くのワークロードで無視できます。重複排除、圧縮、レプリケーションなどのバックエンド ストレージ機能の有効性と互換性も仮想マシンの暗号化の影響を受けることがあります。

前提条件

FT 暗号化には SMP-FT が必須です。レガシー FT（記録/再生 FT）での暗号化はサポートされていません。

手順

1 仮想マシンを選択し、[設定の編集] を選択します。

2 [仮想マシン オプション] で [暗号化された Fault Tolerance] ドロップダウン メニューを選択します。

3 以下のいずれかのオプションを選択します。

オプション	説明
無効	暗号化された Fault Tolerance のログを有効にしないでください。
任意	暗号化は、双方が対応している場合にのみ有効にします。Fault Tolerance 仮想マシンは、暗号化された Fault Tolerance ログをサポートしていない ESXi ホストに移動できます。
必須	暗号化された FT ログをサポートするホストの中から、Fault Tolerance のプライマリ ホストとセカンダリ ホストを選択します。

注： 仮想マシンの暗号化が有効になっている場合、FT 暗号化モードはデフォルトで [必須] に設定され、変更できません。

FT 暗号化モードが [必須] に設定されている場合は、次のようになります。

- FT が有効な場合、FT 暗号化がサポートされているホストのみが、FT セカンダリを配置するホストのリストに表示されます。
- FT フェイルオーバーは、FT 暗号化がサポートされているホストでのみ実行されます。

4 [OK] をクリックします。

Fault Tolerance のベスト プラクティス

Fault Tolerance の結果を最適化するには、特定のベスト プラクティスに従う必要があります。

ホストとネットワーク構成に関する以下の推奨事項を実行することで、クラスタの安定性とパフォーマンスを高めることができます。

ホスト設定

プライマリ仮想マシンとセカンダリ仮想マシンを実行しているホストは、ほぼ同じプロセッサ周波数で動作している必要があります。周波数が大きく異なると、セカンダリ仮想マシンが頻繁に再起動する場合があります。ワークロードに基づいて調整されないプラットフォームでは、電源管理機能（電力を節約するためのパワー キャッピングや強制的な低周波数モードなど）によって、プロセッサの周波数が大きく異なる可能性があります。セカンダリ仮想マシンが定期的に再起動する場合は、Fault Tolerance 対応の仮想マシンを実行するホストですべての電源管理モードを無効にするか、すべてのホストが同じ電源管理モードで動作するようにします。

ホスト ネットワーク構成

次のガイドラインで説明するように、トラフィック タイプ （たとえば NFS） と複数の物理 NIC をさまざまに組み合わせ、Fault Tolerance をサポートするホストのネットワークを構成できます。

- 各 NIC チームを 2 台の物理スイッチ経由で配布して、2 台の物理スイッチ間の各 VLAN の L2 ドメインの継続性を確保する。
- 明確なチーミング ポリシーを使用して、特定のトラフィック タイプが、特定の NIC （アクティブ/スタンバイ）または NIC のセット （たとえば送信元仮想ポート ID） に対してアフィニティを持つようにする。
- アクティブ/スタンバイ ポリシーを使用する場合は、2 つのトラフィック タイプを実装して、両方のトラフィック タイプが 1 枚の vmnic を共有することで、フェイルオーバーする前の影響を最小にする。
- アクティブ/スタンバイ ポリシーを使用する場合は、特定のトラフィック タイプ （たとえば FT ログ記録） 用のすべての有効なアダプタを、同一の物理スイッチに構成する。これにより、ネットワークのホップ数を最小限にし、スイッチ間のリンクが超過する可能性を減らすことができます。

注： プライマリ仮想マシンとセカンダリ仮想マシン間の FT ログ記録トラフィックは暗号化されず、ゲスト ネットワークおよびストレージ I/O データと、ゲスト OS のメモリの内容が含まれます。このトラフィックには、パスワードなどの機密情報がプレーンテキストで含まれる可能性があります。このようなデータの漏洩を回避するため、このネットワークは確実にセキュリティ保護し、特に中間者攻撃が防止されるように注意してください。たとえば、FT ログ記録トラフィック用にプライベート ネットワークを使用できます。

同種のクラスタ

vSphere Fault Tolerance は、異種ホストが含まれているクラスタでも機能しますが、互換性のあるノードを持つクラスタで最高の性能を発揮します。クラスタを構築するとき、すべてのホストが次の構成になっている必要があります。

- 仮想マシンで使用するデータストアへの共通アクセス。
- 同じ仮想マシンのネットワーク構成。
- すべてのホストで同じ BIOS 設定（電源管理とハイパースレッディング）。

[コンプライアンスの確認] を実行して互換性のないものを特定し、修正します。

パフォーマンス

プライマリ仮想マシンとセカンダリ仮想マシン間のトラフィックをログするために使用できるバンド幅を増やすには、10Gbit NIC を使用し、ジャンボ フレームの使用を有効にします。

FT ログ記録ネットワークに対しては複数の NIC を選択できます。複数の NIC を選択すると、それらがすべて FT の実行専用でない場合でも、複数の NIC のバンド幅を利用できるようになります。

共有ストレージ上の ISO による継続アクセス

Fault Tolerance が有効な仮想マシンがアクセスする ISO は、フォルト トレランス対応の仮想マシンの両方のインスタンスがアクセス可能な共有ストレージに格納します。この構成では、仮想マシンの CD-ROM はフェイルオーバーが発生しても正常に動作します。

ネットワーク パーティション分割の回避

ネットワーク パーティション分割が発生するのは、vSphere HA クラスタの管理ネットワークに障害が起こり、ホストの一部が vCenter Server や他のホストから分離されたときです。 ネットワーク パーティション を参照してください。パーティション分割が発生すると、Fault Tolerance による保護が脆弱になる場合があります。

Fault Tolerance を使用する vSphere HA クラスタがパーティション分割されると、プライマリ仮想マシン（またはそのセカンダリ仮想マシン）に対する責任のないプライマリ ホストによって管理されるパーティションに、これらの仮想マシンが配置される可能性があります。フェイルオーバーが必要な場合に、セカンダリ仮想マシンが再起動されるのは、プライマリ仮想マシンに責任のあるプライマリ ホストによって管理されるパーティションに、プライマリ仮想マシンが配置されている場合のみです。

管理ネットワークにネットワーク パーティション分割が生じるような障害が発生しないように、ネットワークのベスト プラクティスの推奨を実行してください

vSAN データストアの使用

vSphere Fault Tolerance （FT) vSAN データストアを使用できますが、次の制限に注意する必要があります。

- vSAN と他のタイプのデータストアの混在は、プライマリ仮想マシンでもセカンダリ仮想マシンでもサポートされません。

FT を vSAN と併用した環境でパフォーマンスと信頼性を向上させるには、次の構成が推奨されます。

- vSAN と FT には、別のネットワークを使用してください。
- プライマリ仮想マシンとセカンダリ仮想マシンを、個別の vSAN フォールト ドメインに配置する。

Metro Cluster Fault Tolerance の有効化

vSphere 8.0 U3 では、Fault Tolerance ウィザードで Metro Cluster Fault Tolerance を有効にできます。

Fault Tolerance ウィザードで、[Metro Cluster Fault Tolerance の有効化] というラベルの付いたチェックボックスをオンにすると、FT Metro Cluster 機能と、FT 仮想マシンの望ましい場所として HostGroup を選択するためのドロップダウン リストを有効にできます。デフォルトでは、このチェックボックスはオフになっており、ドロップダウン リストは無効になっています。これは、FT Metro Cluster が仮想マシンに対して無効であること（`ConfigInfo.metroFtEnabed` が「`FALSE`」）を示します。

チェックボックスをオンにすると、ドロップダウン リストが有効になって HostGroup を選択できます。仮想マシンに対して HostGroup が選択されていないと、ウィザードは次の手順に進めません。選択した HostGroup の正当性を確保するために、ウィザードは関数 `queryFaultToleranceCompatibleHosts` を呼び出し、返されたメッセージから結果を取得します。

[Metro Cluster Fault Tolerance の有効化] チェックボックスをオンにする前は、HostGroup のドロップダウン リストは無効になっています。**ホスト グループ** ラベルの横に、サインポスト ボタンが追加されます。このサインポストの内容は、「**選択したホスト グループに基づいて、FT はクラスタ内のホストを 2 つのグループに分割し、FT プライマリと FT セカンダリを異なるグループに配置できます。**」というものです。

[Metro Cluster Fault Tolerance の有効化] チェックボックスをオンにすると、ウィザード内で HostGroup を選択するためのドロップダウン リストが有効になります。FT は FT Metro Cluster フラグと HostGroup の検証チェックを処理します。これは [次へ] ボタンをクリックすることでトリガされます。ウィザードは [FaultToleranceConfigSpec.metroFtEnabled] を [TRUE] に設定し、[FaultToleranceConfigSpec.preferredLocation] を選択した HostGroup に設定します。次に、ウィザードは互換性のあるホストのリストを取得します。

[Metro Cluster Fault Tolerance の有効化] チェックボックスをオンにした後で HostGroup を選択しないと、[次へ] ボタンをクリックしてもウィザードは先に進めず、次のエラー メッセージが表示されます。`Metro Cluster` **を有効にする前に、フォルト トレランス仮想マシンにホスト グループを割り当ててください。**FT は FT Metro Cluster が有効になっている仮想マシンの HostGroup もチェックします。HostGroup が構成されていない場合、このタスクは失敗します。

構成済みのホスト グループは、FT 仮想マシンの実行中でも削除できます。この場合、FT Metro Cluster は無効になります。ただし、FT Metro Cluster はホスト グループを再度構成した後に再度有効にできるため、ホスト グループ名は FT 情報カードに表示されたままです。

実行中の FT 仮想マシン用の HostGroup を削除すると、FT Metro クラスタは無効になります。フェイルオーバーが発生した場合、「`Metro Cluster` **のステータスがありません。ホスト グループが見つかりません。**」と FT 情報カードに表示されます。ただし、HostGroup を追加し直すと、FT Metro クラスタは再度有効になります。

パワーオフ状態の FT 仮想マシン用の HostGroup を削除すると、Fault Tolerance 対応セカンダリ仮想マシンをパワーオンできません。

レガシー Fault Tolerance

レガシー FT 仮想マシンは、vSphere 6.5 より前のバージョンの ESXi ホストでのみ実行できます。

バージョン 6.5 より前の ESXi ホストでは、さまざまなテクノロジーに基づいて vSphere Fault Tolerance をサポートしていました。この形式の Fault Tolerance を使用していて、今後もこの形式を継続する必要がある場合は、これらの仮想マシンの実行に必要な 6.5 より前のホストのプールを管理するために vCenter Server 6.0 インスタンスを残しておくことをお勧めします。vCenter Server 6.0 は、レガシー Fault Tolerance で保護された仮想マシンを完全に管理できる最後のバージョンです。レガシー Fault Tolerance の詳細については、『vSphere の可用性 6.0』ドキュメントを参照してください。

フォールト トレランス機能を持つ仮想マシンのトラブルシューティング

フォールト トレランス対応の仮想マシンに対して高いレベルのパフォーマンスと安定性を保持し、フェイルオーバー率を最小にするには、いくつかのトラブルシューティングの問題について理解しておく必要があります。

ここで説明するトラブルシューティングの内容は、仮想マシンで vSphere フォールト トレランス機能を使用した場合に発生する可能性のある問題を中心にしています。また、問題の解決方法についても説明します。

また、フォールト トレランスのトラブルシューティングのために、当社のナレッジ ベースの記事を http://kb.vmware.com/kb/1033634 で参照することもできます。この記事には、フォールト トレランス機能を使用しようとしたときに発生するエラー メッセージのリストと、該当する場合は各エラーを解決するためのヒントも記載されています。

ハードウェア仮想化が有効化されていない

vSphere フォールト トレランスを使用する前に、ハードウェア仮想化 (HV) を有効にする必要があります。

問題

フォールト トレランスが有効になっている仮想マシンをパワーオンしようとしたときに、HV を有効化していないと、エラー メッセージが表示されることがあります。

原因

このエラーの多くの場合、仮想マシンをパワーオンしようとしている ESXi サーバで、HV が有効になっていない結果として示されるメッセージです。HV は、ESXi サーバ ハードウェアでサポートされていない、または BIOS で HV が有効になっていないという理由で使用できないことがあります。

解決方法

ESXi サーバ ハードウェアで HV をサポートしているのに、現在 HV が有効になっていない場合は、対象のサーバの BIOS で HV を有効にします。HV を有効にするプロセスは、BIOS によって異なります。HV を有効にする方法の詳細は、ホストの BIOS に関するドキュメントを参照してください。

ESXi サーバ ハードウェアで HV をサポートしていない場合は、フォールト トレランスをサポートするプロセッサを使用するハードウェアに切り替えます。

互換性のあるホストがセカンダリ仮想マシンで使用不可能

Fault Tolerance が有効になっている仮想マシンをパワーオンし、セカンダリ仮想マシンを格納可能な互換性のあるホストがない場合、エラー メッセージが表示されることがあります。

問題

次のエラー メッセージが表示されることがあります。

```
セカンダリ仮想マシンを格納可能な互換性のあるホストがないため、セカンダリ仮想マシンはパワーオンできませんでした。
```

原因

このメッセージは、クラスタ内にほかのホストがない、HV が有効なホストがほかにない、ハードウェア MMU 仮想化がホスト CPU でサポートされていない、データストアにアクセスできない、使用できるキャパシティがない、ホストがメンテナンス モードになっているなど、さまざまな理由で表示されます。

解決方法

ホストが不足している場合は、クラスタにホストを追加します。クラスタ内にホストがある場合は、それらのホストが HV をサポートしており、その HV が有効になっていることを確認します。HV を有効にするプロセスは、BIOS によって異なります。HV を有効にする方法の詳細は、ホストの BIOS に関するドキュメントを参照してください。ホストに十分なキャパシティがあること、およびホストがメンテナンス モードでないことを確認します。

オーバーコミットされたホスト上のセカンダリ仮想マシンによってプライマリ仮想マシンのパフォーマンスが低下する

ホストの負荷が少なく、アイドル状態の CPU 時間があるのに、プライマリ仮想マシンの実行が遅いと思われる場合は、セカンダリ仮想マシンが稼動しているホストをチェックして、負荷が高くないかを確認します。

問題

セカンダリ仮想マシンが格納されているホストの負荷が大きい場合、セカンダリ仮想マシンがプライマリ仮想マシンのパフォーマンスに影響することがあります。

原因

CPU リソースなどがオーバーコミットされたホスト上で稼動しているセカンダリ仮想マシンは、プライマリ仮想マシンと同じ量のリソースを得られないことがあります。このような場合には、セカンダリ仮想マシンを保持するために、プライマリ仮想マシンの実行速度をセカンダリ仮想マシンに合わせて遅くするため、プライマリ仮想マシンの処理が遅くなります。

解決方法

セカンダリ仮想マシンがオーバーコミットされたホスト上に存在する場合、リソースの競合の問題が存在しない別の場所に仮想マシンを移動できます。さらに具体的には、次の操作を実行します。

- FT ネットワークの競合については、vMotion テクノロジを使用して、セカンダリ仮想マシンを FT ネットワーク上にある、より競合する FT 仮想マシンが少ないホストに移動します。仮想マシンへのストレージ アクセスの品質が非対称ではないことを確認します。
- ストレージの競合の問題については、FT をオフにしてから再度オンにします。セカンダリ仮想マシンを再作成するときに、そのデータストアをよりリソースの競合が少なく、パフォーマンスの向上が望める場所に変更します。
- CPU リソースの問題を解決するには、プライマリ仮想マシンに、適切なパフォーマンス レベルでそのワークロードを実行するのに十分な CPU 予約を MHz 値で明示的に設定します。この予約は、プライマリ仮想マシンとセカンダリ仮想マシンの両方に対して適用され、これらの両方の仮想マシンが指定されたレートで確実に実行できるようにします。この予約を設定するためのガイダンスについては、（フォールト トレランスを有効にする前に）仮想マシンのパフォーマンス グラフを見て、通常の状態で CPU リソースがどのくらい使用されているかを確認します。

FT 仮想マシンでネットワーク遅延が長くなる

FT ネットワークが最適な構成になっていない場合、FT 仮想マシンで遅延問題が発生する可能性があります。

問題

FT 仮想マシンでは、パケット遅延（ミリ秒単位）が変動して長くなることがあります。また、ネットワークのパケット遅延またはジッターを非常に低く抑える必要があるアプリケーションでは、パフォーマンスが低下する場合があります。

原因

ネットワーク遅延は Fault Tolerance のオーバーヘッドでいくらか増加することが予期されますが、特定の要素によってもこの遅延が長くなる可能性があります。たとえば、FT ネットワークが特に高い遅延があるリンク上にある場合、この遅延がアプリケーションにも影響します。また、FT ネットワークのバンド幅が不十分な場合（10Gbps 未満）には、より大きな遅延が発生する可能性があります。

解決方法

FT ネットワークのバンド幅が十分であり（10 Gbps 以上）、プライマリ仮想マシンとセカンダリ仮想マシンの間で低遅延リンクが使用されていることを確認します。これらの対策を行ってもネットワーク遅延は解消されませんが、潜在的な影響を最小限に抑えることができます。

FT 仮想マシンの一部のホストが過負荷になる

クラスタのホストに FT 仮想マシンが不均衡に分散していると、パフォーマンスの問題が発生する可能性があります。

問題

クラスタ内のいくつかのホストに FT 仮想マシンにより過負荷がかかり、その一方で、その他のホストに未使用のリソースがあります。

原因

vSphere DRS は、（レガシー FT を使用しているのでない限り） FT 仮想マシンの負荷を分散しません。この制限により、クラスタ内のホストには、FT 仮想マシンの負荷が不均衡に分散されます。

解決方法

vSphere vMotion を使用することにより、クラスタ全体で FT 仮想マシンを手動でリバランスします。一般に、FT ネットワークのバンド幅および CPU リソースの競合が減少するため、ホスト上の FT 仮想マシンの数が少ないほどパフォーマンスが向上します。

FT メタデータ データストアにアクセスできない

Fault Tolerance メタデータ データストアへのアクセスは、FT 仮想マシンが正常に機能する上で不可欠です。このアクセスが失われると、さまざまな問題が発生する可能性があります。

問題

次のような問題があります。

- FT が予期せずに停止することがあります。
- プライマリ仮想マシンとセカンダリ仮想マシンの両方がメタデータ データストアにアクセスできなくなると、仮想マシンが予期せずに停止する場合があります。一般に、両方の仮想マシンで FT メタデータ データストアへのアクセスが失われると、関連のない障害が発生して FT が停止します。その後 vSphere HA は、メタデータ データストアにアクセスできるホストでプライマリ仮想マシンの再起動を試みます。
- その仮想マシンは、vCenter Server によって FT 仮想マシンとして認識されなくなります。認識されなくなると、スナップショットの取得などのサポートされていない操作が仮想マシンで実行され、問題のある動作の原因となる可能性があります。

原因

Fault Tolerance メタデータ データストアにアクセスできなくなると、上記のリストにある望ましくない結果になる場合があります。

解決方法

FT のデプロイを計画するとき、可用性の高いストレージにメタデータ データストアを配置してください。FT の実行中に、プライマリ仮想マシンまたはセカンダリ仮想マシンのどちらかでメタデータ データストアにアクセスできなくなった場合は、アクセスを失ったことで上記の問題のいずれかが発生する前に、すぐにそのストレージの問題を解決してください。FT 仮想マシンが vCenter Server によって認識されなくなったら、サポートされていない操作を仮想マシンで実行しないでください。メタデータ データストアへのアクセスをリストアします。FT 仮想マシンのアクセスが復元され、リフレッシュ期間が終了すると、仮想マシンが認識可能になります。

パワーオンされた仮想マシンで vSphere FT を有効にしようとすると失敗する

パワーオンされた仮想マシンで vSphere Fault Tolerance を有効にしようとすると失敗する可能性があります。

問題

パワーオンされた仮想マシンで [Fault Tolerance をオン] を選択すると、操作に失敗し、「不明なエラー」というメッセージが表示されます。

原因

仮想マシンが実行されているホストに、フォールト トレランスの保護を実現するだけの十分なメモリ リソースがないと、この操作に失敗する可能性があります。vSphere Fault Tolerance は、仮想マシンのホストに十分なメモリ予約を自動的に割り当てようとします。フォールト トレランス対応仮想マシンにはオーバーヘッド メモリが必要になり、場合によっては 1 ～ 2 GB まで拡張されます。予約分全体とオーバーヘッド メモリに対応するだけのメモリ リソースがないホストでパワーオンされた仮想マシンが実行されている場合、Fault Tolerance の有効化に失敗します。その後、「不明なエラー」というメッセージが返されます。

解決方法

次の解決策から選択します。

- 仮想マシンのメモリ予約と追加のオーバーヘッドに対応できるようにホストのメモリ リソースを解放する。

- 十分な空きメモリ リソースがあるホストに仮想マシンを移動し、やり直す。

vSphere DRS によって配置または退避させられない FT 仮想マシン

Enhanced vMotion Compatibility (EVC) が現在無効になっている場合、vSphere DRS が有効になっているクラスタ内の FT 仮想マシンは正常に機能しません。

問題

EVC は、DRS と FT 仮想マシンを組み合わせて使用するための前提条件であるため、EVC が無効になっていると（後で再度有効にしても）、DRS で FT 仮想マシンが配置または退避されません。

原因

DRS クラスタで EVC が無効になっている場合、FT 仮想マシンの DRS を無効にする仮想マシンのオーバーライドが追加される可能性があります。EVC を後で再度有効にしても、このオーバーライドはキャンセルされません。

解決方法

DRS で FT 仮想マシンがクラスタに配置または退避されない場合、仮想マシンをチェックして、DRS を無効にする仮想マシンのオーバーライドを確認してください。仮想マシンのオーバーライドがある場合、DRS. を無効にするオーバーライドを削除します。

注： 仮想マシンのオーバーライドを編集または削除する方法の詳細については、『vSphere リソース管理』を参照してください。

フォールト トレランス機能を持つ仮想マシンのフェイルオーバー

ESXi ホストがクラッシュしていなくても、プライマリ仮想マシンまたはセカンダリ仮想マシンでフェイルオーバーが発生する可能性があります。このような場合、仮想マシンの実行は中断されませんが、冗長性は一時的に失われます。このタイプのフェイルオーバーを回避するために、フェイルオーバーが発生する可能性のある状況について認識し、それらを回避するための手段を講じます。

ストレージに関連する部分的なハードウェア障害

いずれかのホストについて、ストレージへのアクセスが遅い、またはアクセスが停止した場合に、この問題が生じることがあります。この問題が発生した場合には、VMKernel ログに、多数のストレージ エラーが記録されます。この問題を解決するには、ストレージ関連の問題に対処する必要があります。

ネットワークに関連する部分的なハードウェア障害

ログ記録 NIC が機能しない、またはその NIC を介したほかのホストへの接続が停止した場合には、フォールト トレランス対応の仮想マシンのフェイルオーバーが起動され、冗長性が再確立されます。この問題を回避するには、vMotion 用と FT のログ トラフィック用にそれぞれ専用の独立した NIC を用意し、vMotion での移行は仮想マシンのアクティビティが少ないときのみに行うようにします。

ログ記録 NIC ネットワークのバンド幅が不十分

1 台のホスト上にあるフォールト トレランス対応の仮想マシンが多すぎる場合に、この問題が生じることがあります。この問題を解決するには、フォールト トレランス対応の仮想マシンのペアを、さまざまなホスト間でより広範に分散させます。

FT には 10 Gbit ログ記録ネットワークを使用し、ネットワークが低遅延であることを確認します。

仮想マシンのアクティビティ レベルによる vMotion の障害

フォールト トレランス対応の仮想マシンで vMotion での移行が失敗すると、仮想マシンのフェイルオーバーが必要になることがあります。通常、これはアクティビティが最小限に中断されるだけで完了する移行に対して、仮想マシンが過度にアクティブになっている場合に発生します。この問題を回避するには、仮想マシンがあまりアクティブになっていないときのみ、vMotion での移行を実行します。

VMFS ボリューム上のアクティビティが多すぎて仮想マシンでフェイルオーバーが発生することがある

ファイル システムのロッキング操作、仮想マシンのパワーオン、パワーオフ、または vMotion での移行が 1 つの VMFS ボリューム上で多数行われると、フォールト トレランス対応の仮想マシンのフェイルオーバーが起動されることがあります。このような問題が発生しそうな兆候として、VMKernel ログで SCSI の予約に関する多数の警告を受け取ります。この問題を解決するには、ファイル システムの操作数を減らすか、vMotion を使用して定期的にパワーオン、パワーオフ、または移行される仮想マシンがあまり多くない VMFS ボリューム上に、フォールト トレランス対応の仮想マシンを配置します。

ファイル システムの使用可能な容量がないためにセカンダリ仮想マシンを起動できない

/ （ルート） または /vmfs/*データソース* ファイル システムに使用可能な空き領域があるかどうか確認してください。これらのファイル システムはさまざまな理由でフルになることがあり、空き容量がないと、新しいセカンダリ仮想マシンを起動できなくなることがあります。

vCenter High Availability

4

vCenter High Availability (vCenter HA) は、ホストおよびハードウェアの障害から vCenter Server を保護します。また、ソリューションのアクティブ/パッシブ アーキテクチャは、vCenter Server にパッチを適用する際のダウンタイムを大幅に短縮することに役立ちます。

一定のネットワーク構成を行うと、アクティブ、パッシブ、監視の 3 つのノードを含むクラスタが作成されます。構成の手順にはいくつかの種類があります。どれを選ぶかは、既存の構成によって決まります。

手順

1 vCenter HA のデプロイ計画

vCenter HA の構成を行うには、いくつかの要素を事前に考慮しておく必要があります。異なるバージョンの vSphere を使用したコンポーネントが混在する環境では、vSphere 8.0 のコンポーネントのみを含む環境とは異なる考慮事項があります。またリソース要件とソフトウェア要件、ネットワークの設定も慎重に考慮しなければなりません。

2 ネットワークの構成

選択するデプロイ オプションとインベントリ階層に関係なく、構成を開始する前にネットワークをセットアップしておく必要があります。vCenter HA ネットワークの基盤を設定するには、各 ESXi ホストにポート グループを追加します。

3 vSphere Client による vCenter HA の構成

vSphere Client を使用した場合、[vCenter HA のセットアップ] ウィザードによって、2 番目のネットワーク アダプタが vCenter Server に作成されて構成され、アクティブ ノードのクローンが作成され、vCenter HA ネットワークが構成されます。

4 vCenter HA 構成の管理

vCenter HA クラスタの構成後、管理タスクを実行できます。たとえば、証明書や SSH キーの変更、SNMP のセットアップを実行できます。クラスタ構成を編集して、vCenter HA を無効または有効にするほか、メンテナンス モードへの切り替え、クラスタ構成の削除などの操作を行うこともできます。

5 vCenter HA 環境のトラブルシューティング

問題が発生した場合は、環境をトラブルシューティングします。実行する必要があるタスクは、障害の症状に応じて異なります。トラブルシューティングに関する詳しい情報については、VMware のナレッジベース システムを参照してください。

6 vCenter High Availability 環境へのパッチの適用

vCenter High Availability クラスタの vCenter Server にパッチを適用するには、vCenter Server シェルにある **software-packages** ユーティリティを使用します。

7 vCenter HA のダウンタイムの短縮アップグレード

vSphere 8.0 U3 では、ダウンタイムの短縮アップグレードが vCenter HA の自動デプロイと統合されています。

vCenter HA のデプロイ計画

vCenter HA の構成を行うには、いくつかの要素を事前に考慮しておく必要があります。異なるバージョンの vSphere を使用したコンポーネントが混在する環境では、vSphere 8.0 のコンポーネントのみを含む環境とは異なる考慮事項があります。またリソース要件とソフトウェア要件、ネットワークの設定も慎重に考慮しなければなりません。

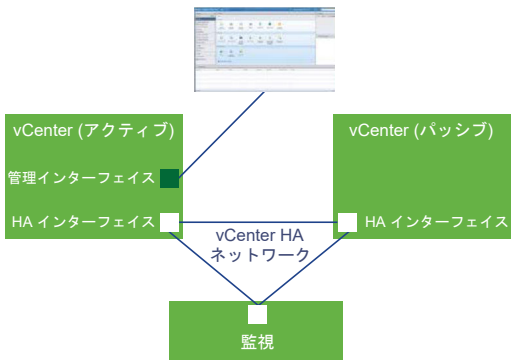
vCenter アーキテクチャの概要

vCenter HA クラスタは、3 つの vCenter Server インスタンスから成ります。1 つ目のインスタンスは、最初はアクティブ ノードとして使用され、パッシブ ノードと監視ノード用にそのクローンが 2 回作成されます。アクティブ-パッシブのフェイルオーバー ソリューションは、この 3 つのノードが一体となって実現されます。

ハードウェア障害からの保護は、それぞれ異なる ESXi インスタンスに各ノードをデプロイすることで得られます。3 つの ESXi ホストを DRS クラスタに追加すれば、より強力に環境を保護することができます。

vCenter HA の構成が完了した時点では、アクティブ ノードだけが、アクティブな管理インターフェイス（パブリック IP）を持ちます。3 つのノードは、vCenter HA ネットワークという、構成の過程でセットアップされたプライベート ネットワークを介して通信を行います。アクティブ ノードは、継続的にデータをパッシブ ノードに複製しています。

図 4-1. vCenter の 3 ノード クラスタ



この機能が動作するには、3 台のノードがすべて必要です。ノードの役割を比較します。

表 4-1. vCenter HA ノード

ノード	説明
アクティブ	■ アクティブ vCenter Server インスタンスを実行します。 ■ 管理インターフェイスにパブリック IP アドレスを使用します。 ■ vCenter HA ネットワークを使用して、パッシブ ノードへのデータのレプリケーションを行います。 ■ vCenter HA ネットワークを使用して、監視ノードとの通信を行います。
パッシブ	■ 元々はアクティブ ノードのクローンです。 ■ vCenter HA ネットワークを介して常時アクティブ ノードから更新を受信し、アクティブ ノードと状態を同期します。 ■ 障害が発生すると、自動的にアクティブ ノードの役割を引き継ぎます。
監視	■ アクティブ ノードの軽量クローンです。 ■ クォーラムを提供し、スプリットブレインの状態から保護します。

vCenter HA のハードウェア要件とソフトウェア要件

vCenter HA をセットアップする前に、必要なメモリと CPU、データストア リソースがあること、またご使用のバージョンの vCenter Server および ESXi が vCenter HA をサポートしていることを確認してください。

環境で、次の要件が満たされている必要があります。

表 4-2. vCenter HA の要件

コンポーネント	要件
ESXi	■ ESXi 6.0 以降が必要です。 ■ 3 台以上の ESXi ホストを推奨します。そうすれば各 vCenter HA ノードを異なるホストで実行して、より確実に保護することができます。
管理 vCenter Server (使用する場合)	ご利用の環境には、管理 vCenter Server システムを導入するか、動作環境となる ESXi ホストを自分自身で管理するように vCenter Server をセットアップすることができます（自己管理型の vCenter Server）。 ■ vCenter Server 6.0 以降が必要です。
vCenter Server	■ vCenter Server 6.5 以降が必要です。 ■ RTO を満たすためには、デプロイ サイズが小（4 つの CPU と 16 GB の RAM）かそれ以上であることが必要です。本番環境では極小を使用しないでください。 ■ VMFS、NFS、vSAN データストアで vCenter HA がサポートされ、テストされている必要があります。 ■ アクティブ ノードには、3 台すべてのノードに必要なサポート バンドルを収集して格納できるだけのディスク容量を確保してください。vCenter HA ノードのサポート バンドルの収集を参照してください。
ネットワーク接続	■ アクティブ、パッシブ、監視の各ノード間における vCenter HA ネットワークの遅延は 10 ミリ秒未満であることが必要です。 ■ vCenter HA ネットワークは、管理ネットワークとは異なるサブネットに配置する必要があります。
vCenter HA に必要なライセンス	■ vCenter HA には、1 つの vCenter Server ライセンスが必要です。 ■ vCenter HA には、標準ライセンスが必要です。

vSphere Client の構成ワークフロー

vSphere Client で [vCenter HA の設定] ウィザードを使用して、パッシブ ノードと監視ノードを構成することができます。[vCenter HA の設定] ウィザードを選択した場合は、vCenter HA の設定の一環としてパッシブ ノードと監視ノードが自動的に作成されます。手動オプションを選択した場合は、アクティブ ノードのクローンを手動で作成してパッシブ ノードと監視ノードを作成する必要があります。

vSphere Client での自動設定

自動設定を実行するには、次の要件を満たしている必要があります。

- アクティブ ノードになる vCenter Server が、それ自身の ESXi ホストと仮想マシンを管理している。この構成は、自己管理型の vCenter Server と呼ばれることがあります。

上記の要件を満たしている場合の自動ワークフローは次のようになります。

1 ユーザーが、アクティブ ノードとなる最初の vCenter Server をデプロイします。

2 ユーザーが各 ESXi ホストで vCenter HA トラフィック用の 2 つ目のネットワーク（ポート グループ）を追加します。

3 ユーザーが vCenter HA の設定を開始し、各クローンの IP アドレス、ターゲット ESXi ホストまたはクラスタ、およびデータストアを指定します。

4 システムがアクティブ ノードのクローンを作成し、ホスト名を含めて完全に同じ設定を使用してパッシブ ノードを作成します。

5 システムが再度アクティブ ノードのクローンを作成し、より軽量な監視ノードを作成します。

6 3 つのノードがハートビート情報の交換などの通信に使用する vCenter HA ネットワークがシステムによって設定されます。

vSphere Client での手動設定

デプロイをより細かく制御するには、手動による設定を行います。このオプションの場合、ユーザー自身が vCenter HA 設定の一環としてアクティブ ノードのクローンを作成する必要があります。また、このオプションを選択し、vCenter HA 設定を後で削除した場合、作成したノードを自分で削除する必要があります。

手動オプションを選択した場合のワークフローは次のようになります。

1 ユーザーが、アクティブ ノードとなる最初の vCenter Server をデプロイします。

2 ユーザーが各 ESXi ホストで vCenter HA トラフィック用の 2 つ目のネットワーク（ポート グループ）を追加します。

3 アクティブな管理 vCenter Server の認証情報が不明な場合、ユーザーはアクティブ ノードに 2 つ目のネットワーク アダプタ (NIC) を追加する必要があります。

4 ユーザーが vSphere Client を使用して vCenter Server（アクティブ ノード）にログインします。

5 ユーザーが vCenter HA の設定を開始し、手動設定のためのチェック ボックスを選択し、パッシブ ノードと監視ノードの IP アドレスとサブネット情報を指定します。オプションで、フェイルオーバー管理用 IP アドレスをオーバーライドすることもできます。

6 ユーザーが管理 vCenter Server にログインし、vCenter Server（アクティブ ノード）のクローンを 2 つ作成します。

7 3 つのノードがハートビート情報とレプリケーション情報を交換するために使用する vCenter HA ネットワークがシステムによって設定されます。

8 vCenter Server は vCenter HA によって保護されます。

詳細については、vSphere Client による vCenter HA の構成を参照してください。

ネットワークの構成

選択するデプロイ オプションとインベントリ階層に関係なく、構成を開始する前にネットワークをセットアップしておく必要があります。vCenter HA ネットワークの基盤を設定するには、各 ESXi ホストにポート グループを追加します。

構成が完了した後の vCenter HA クラスタには 2 つのネットワークが存在します。1 つ目の仮想 NIC 上の管理ネットワークと、2 つ目の仮想 NIC 上の vCenter HA ネットワークです。

管理ネットワーク

管理ネットワークは、クライアントの要求に対応します（パブリック IP）。管理ネットワーク IP アドレスは固定である必要があります。

vCenter HA ネットワーク

vCenter HA ネットワークはアクティブ、パッシブおよび監視ノードを接続し、サーバの状態をレプリケートします。また、ハートビートも監視します。

- アクティブ、パッシブおよび監視ノードの vCenter HA ネットワークの IP アドレスは固定である必要があります。
- vCenter HA ネットワークは、管理ネットワークとは異なるサブネットに配置する必要があります。3 台のノードの配置先は、同じサブネットでも異なるサブネットでもかまいません。
- アクティブ、パッシブおよび監視ノード間でのネットワークの遅延は、10 ミリ秒未満にする必要があります。
- クラスタ ネットワークのデフォルト ゲートウェイのエントリを追加しないでください。

前提条件

- 後でアクティブ ノードになる vCenter Server がデプロイされていること。
- その vCenter Server とそれが実行されている ESXi ホストにアクセスして変更するための権限があること。
- ネットワークのセットアップ時には管理ネットワークの固定 IP アドレスが必要となります。管理ネットワークおよびクラスタ ネットワークのアドレスは、IPv4 または IPv6 である必要があります。混合モードの IP アドレスにすることはできません。

手順

1 管理 vCenter Server にログインし、アクティブ ノードが実行されている ESXi ホストを見つけます。

2 ESXi ホストにポート グループを追加します。

既存の仮想スイッチ上のポート グループを使用できるほか、ネットワークの分離度を高めるために新しい仮想スイッチを作成することもできます。管理ネットワークとは別にする必要があります。

3 推奨される 3 台の ESXi ホストがご利用の環境に存在する場合、このポート グループを各ホストに追加します。

vSphere Client による vCenter HA の構成

vSphere Client を使用した場合、[vCenter HA のセットアップ] ウィザードによって、2 番目のネットワーク アダプタが vCenter Server に作成されて構成され、アクティブ ノードのクローンが作成され、vCenter HA ネットワークが構成されます。

前提条件

- 初期アクティブ ノードとして使用する vCenter Server をデプロイします。
  - vCenter Server には、固定 IP アドレスが必要です。
  - vCenter Server では、SSH を有効にする必要があります。
- 環境が次の要件を満たしていることを確認します。
  - アクティブ ノードになる vCenter Server が、それ自身の ESXi ホストと仮想マシンを管理している。この構成は、自己管理型の vCenter Server と呼ばれることがあります。
- vCenter HA ネットワークのインフラストラクチャを設定します。ネットワークの構成を参照してください。
- パッシブ ノードおよび監視ノードとなる 2 つの vCenter Server ノードに使用する固定 IP アドレスを決めます。

注： アクティブ ノードで NSX-T セグメントを使用するには、[仮想マシン設定の編集] を使用して NIC2/eth1 を作成し、NSX-T セグメントと一緒にこの 2 番目の NIC を追加する必要があります。パッシブ ノードまたは監視ノードのリソースを指定する必要はありません。これは、NIC1/eth0 と NIC2/eth1 および IP アドレスを含む、パッシブ ノードおよび監視ノードに必要なゲスト カスタマイズ仕様を追加した後に、[仮想マシンのクローン作成] を使用してクローンを作成する必要があるためです。vCenter Server で eth1 の VCHA IP アドレスを構成すると、アクティブ ノードの eth1 が自動的に入力されます。

手順

1 vSphere Client を使用してアクティブ ノードにログインします。

2 インベントリで vCenter Server オブジェクトを選択し、[構成] タブを選択します。

3 [設定] で [vCenter HA] を選択します。

4 [vCenter HA のセットアップ] ボタンをクリックして、設定ウィザードを開始します。
  - vCenter Server が自己管理型である場合は、[リソース設定] ページが表示されます。手順 7 に進みます。
  - vCenter Server が同じ SSO ドメイン内の別の vCenter Server によって管理されている場合は、手順 7 に進みます。

- vCenter Server が別の SSO ドメインの vCenter Server によって管理されている場合は、その管理 vCenter Server の場所と認証情報の詳細を入力します。

5 [管理 vCenter Server の認証情報] をクリックします。管理 vCenter Server の FQDN または IP アドレス、Single Sign-On のユーザー名とパスワードを指定し、[次へ] をクリックします。

Single Sign-On 管理者の認証情報がない場合は、2 つ目の項目を選択し、[次へ] をクリックします。

6 [証明書の警告] が表示される場合があります。SHA1 サムプリントを確認し、[はい] を選択して続行します。

7 [リソース設定] セクションのドロップダウン メニューで、アクティブ ノードの vCenter HA ネットワークを選択します。

注： NIC2/eth1 が作成されると、ネットワーク セレクタは表示されなくなります。

8 パッシブ ノードと監視ノードのクローンが自動的に作成されるようにする場合は、チェック ボックスをクリックします。

注： チェック ボックスを選択しない場合は、[終了] をクリックした後、パッシブ ノードと監視ノードのクローンを手動で作成する必要があります。

9 パッシブ ノードで、[編集] をクリックします。

a 一意の名前とターゲットの場所を指定します。

b 操作のターゲットのコンピューティング リソースを選択します。

c 構成とディスク ファイルを保存するデータストアを選択します。

d 仮想マシン管理 (NIC 0) と vCenter HA (NIC 1) ネットワークを選択します。

選択に問題があると、エラーまたは互換性の警告が表示されます。

e 選択内容を確認し、[終了] をクリックします。

10 監視ノードで、[編集] をクリックします。

a 一意の名前とターゲットの場所を指定します。

b 操作のターゲットのコンピューティング リソースを選択します。

c 構成とディスク ファイルを保存するデータストアを選択します。

d vCenter HA (NIC 1) ネットワークを選択します。

選択に問題があると、エラーまたは互換性の警告が表示されます。

e 選択内容を確認し、[終了] をクリックします。

11 [次へ] をクリックします。

12 [IP アドレス設定] セクションのドロップダウン メニューで、IP アドレスのバージョンを選択します。

13 IPv4 アドレス (NIC 1) と、アクティブ ノード、パッシブ ノード、および監視ノードのサブネット マスクまたはプリフィックス長の情報を入力します。

パッシブ ノードの管理ネットワーク設定は、編集することができます。これらの設定のカスタマイズはオプションです。デフォルトでは、アクティブ ノードの管理ネットワーク設定が適用されます。

14 [終了] をクリックします。

結果

パッシブ ノードと監視ノードが作成されます。[vCenter HA のセットアップ] が完了すると、vCenter Server に高可用性の保護が適用されます。vCenter HA が有効になったら、[編集] をクリックしてメンテナンス モードに入り、vCenter HA を有効または無効にすることができます。vCenter HA を削除するボタンと、vCenter HA フェイルオーバーを開始するボタンが個別にあります。

次のステップ

クラスタ管理タスクの一覧については、vCenter HA 構成の管理を参照してください。

vCenter HA と併用する際の vSphere Client の機能向上の概要については、以下を参照してください：

(vSphere Client と vCenter HA の併用に対する機能向上)

vCenter HA 構成の管理

vCenter HA クラスタの構成後、管理タスクを実行できます。たとえば、証明書や SSH キーの変更、SNMP のセットアップを実行できます。クラスタ構成を編集して、vCenter HA を無効または有効にするほか、メンテナンス モードへの切り替え、クラスタ構成の削除などの操作を行うこともできます。

- SNMP トラップの設定

  Simple Network Management Protocol (SNMP) トラップを設定すると、ご利用の vCenter HA クラスタについての SNMP 通知を受信することができます。

- ご利用の環境でカスタム証明書を使用するための設定

  クラスタの管理通信やレプリケーション トラフィックの暗号化には、各ノード上のマシン SSL 証明書が使用されます。カスタム証明書を使用するには、vCenter HA の構成を削除し、パッシブ ノードと監視ノードを削除して、カスタム証明書でアクティブ ノードをプロビジョニングしてから、クラスタを再構成する必要があります。

- vCenter HA SSH キーの管理

  vCenter HA では、アクティブ、パッシブ、監視の各ノード間でパスワードを使用しない認証を行うために SSH キーが使用されています。ハートビートのやり取りやファイルとデータのレプリケーションにこの認証が使用されます。vCenter HA クラスタのノードの SSH キーを置き換えるには、クラスタを無効にし、アクティブ ノード上に新しい SSH キーを生成して、そのキーをパッシブ ノードに転送してから、クラスタを有効にします。

- vCenter HA フェイルオーバーの開始

  フェイルオーバーを手動で開始し、パッシブ ノードをアクティブ ノードにできます。

- vCenter HA クラスタ構成の編集

  vCenter HA クラスタはその構成の編集を通じて、無効（または有効）にしたりメンテナンス モードにしたり削除したりすることができます。

- バックアップおよびリストア操作の実行

  セキュリティを強化するために、vCenter HA クラスタのアクティブ ノードをバックアップすることができます。バックアップしておくと、致命的な障害が発生した場合に、ノードをリストアできます。

- vCenter HA の構成の削除

  vCenter HA の構成は、vSphere Client から削除することができます。

- すべての vCenter HA ノードの再起動

  クラスタ内のすべてのノードをシャットダウンして再起動する必要がある場合は、パッシブ ノードがアクティブ ノードのロールを引き継がないように、所定の順序に従ってシャットダウンする必要があります。

- サーバ環境の変更

  vCenter Server のデプロイ時には、環境を選択します。vCenter HA では、運用環境用に小規模、中規模、大規模、超大規模の各環境がサポートされています。容量を拡大する必要があり環境を変更する場合は、構成の変更前にパッシブ ノードの仮想マシンを削除する必要があります。

- vCenter HA ノードのサポート バンドルの収集

  vCenter HA クラスタ内のすべてのノードからサポート バンドルを収集すると、トラブルシューティングに役立ちます。

SNMP トラップの設定

Simple Network Management Protocol (SNMP) トラップを設定すると、ご利用の vCenter HA クラスタについての SNMP 通知を受信することができます。

トラップのデフォルトは SNMP バージョン 1 です。

アクティブ ノードとパッシブ ノードに対して SNMP トラップを設定します。関連付けられているトラップの送信先をエージェントに指示するには、snmpd 構成にターゲット エントリを追加します。

手順

1 仮想マシン コンソールまたは SSH を使用してアクティブ ノードにログインします。

2 `vicfg-snmp` コマンドを実行します。以下にその例を示します。

```
vicfg-snmp -t 10.160.1.1@1166/public
```

この例の `10.160.1.1` はクライアントがリッスンしているアドレスを、`1166` はクライアントがリッスンしているポートを表します。`public` はコミュニティ文字列です。

3 次のコマンドを実行して SNMP エージェント (snmpd) を有効にします。

```
vicfg-snmp -e
```

次のステップ

次のコマンドも便利です。

- コマンドに関する詳しいヘルプを表示するには、**`vicfg-snmp -h`** を実行します。
- SNMP エージェントを無効にするには、**`vicfg-snmp -D`** を実行します。

- SNMP エージェントの構成を表示するには、**vicfg-snmp -s** を実行します。
- デフォルトの構成にリセットするには、**vicfg-snmp -r** を実行します。

ご利用の環境でカスタム証明書を使用するための設定

クラスタの管理通信やレプリケーション トラフィックの暗号化には、各ノード上のマシン SSL 証明書が使用されます。カスタム証明書を使用するには、vCenter HA の構成を削除し、パッシブ ノードと監視ノードを削除して、カスタム証明書でアクティブ ノードをプロビジョニングしてから、クラスタを再構成する必要があります。

可能であれば、アクティブ ノードになる vCenter Server の証明書を置き換えてから、ノードのクローンを作成してください。

手順

1 クラスタの構成を編集し、[削除] を選択します。

2 パッシブ ノードおよび監視ノードを削除します。

3 アクティブ ノード（この時点ではスタンドアロンの vCenter Server なっています）上のマシン SSL 証明書をカスタム証明書に置き換えます。

4 クラスタを再構成します。

vCenter HA SSH キーの管理

vCenter HA では、アクティブ、パッシブ、監視の各ノード間でパスワードを使用しない認証を行うために SSH キーが使用されています。ハートビートのやり取りやファイルとデータのレプリケーションにこの認証が使用されます。vCenter HA クラスタのノードの SSH キーを置き換えるには、クラスタを無効にし、アクティブ ノード上に新しい SSH キーを生成して、そのキーをパッシブ ノードに転送してから、クラスタを有効にします。

手順

1 クラスタを編集し、モードを [無効] に変更します。

2 仮想マシン コンソールまたは SSH を使用してアクティブ ノードにログインします。

3 bash シェルを有効にします。

```
bash
```

4 次のコマンドを実行して新しい SSH キーをアクティブ ノードに生成します。

```
/usr/lib/vmware-vcha/scripts/resetSshKeys.py
```

5 SCP を使用して、パッシブ ノードと監視ノードにキーをコピーします。

```
scp /vcha/.ssh/*
```

6 クラスタ構成を編集し、vCenter HA クラスタを [有効] に設定します。

vCenter HA フェイルオーバーの開始

フェイルオーバーを手動で開始し、パッシブ ノードをアクティブ ノードにできます。

vCenter HA クラスタは、2 種類のフェイルオーバーをサポートします。

自動フェイルオーバー

アクティブ ノードの障害時に、パッシブ ノードがアクティブの役割を引き継ぎます。

手動フェイルオーバー

フェイルオーバーの開始アクションを使用して、強制的にパッシブ ノードがアクティブの役割を引き継ぐことができます。

トラブルシューティングとテストのために手動フェイルオーバーを開始します。

手順

1. vSphere Client でアクティブ ノードの vCenter Server にログインし、フェイルオーバーを開始する必要がある vCenter Server の [構成] をクリックします。
2. [設定] で [vCenter HA] を選択し、[フェイルオーバー開始] をクリックします。
3. [はい] をクリックし、フェイルオーバーを開始します。

   同期なしでフェイルオーバーを強制的に実行するオプションがダイアログに表示されます。ほとんどの場合、最初に同期を実行しておくことをお勧めします。
4. フェイルオーバー後、vSphere Client で、パッシブ ノードにアクティブ ノードのロールが含まれていることを確認します。

vCenter HA クラスタ構成の編集

vCenter HA クラスタはその構成の編集を通じて、無効（または有効）にしたりメンテナンス モードにしたり削除したりすることができます。

vCenter Server の運用モードでは、vCenter HA クラスタでフェイルオーバー機能および状態のレプリケーションを制御します。

vCenter HA クラスタは、次のいずれかのモードで運用することができます。

表 4-3. vCenter HA クラスタの運用モード

モード	自動フェイルオーバー	手動フェイルオーバー	レプリケーション	
有効にする	はい	はい	はい	このデフォルトの運用モードでは、自動フェイルオーバーを実行して、ハードウェアおよびソフトウェア障害から vCenter Server を保護します。
メンテナンス	なし	はい	はい	一部のメンテナンス タスクで使用します。一方、vCenter HA を無効にしなければならないタスクもあります。
無効	いいえ	いいえ	いいえ	パッシブ ノードまたは監視ノードが失われた場合、または障害から回復中の場合に、vCenter HA の構成を無効にすることができます。アクティブ ノードはスタンドアローン vCenter Server として引き続き実行されます。

注： クラスタをメンテナンス モードまたは無効モードのいずれかで運用しているときは、パッシブ ノードおよび監視ノードが失われる場合、または到達不可能な場合でも、アクティブ ノードは引き続きクライアントの要求に対応できます。

前提条件

vCenter HA クラスタがデプロイされていて、アクティブ ノード、パッシブ ノード、および監視ノードが含まれていることを確認します。

手順

1 vSphere Client でアクティブ ノードの vCenter Server にログインし、[構成] をクリックします。

2 [設定] で [vCenter HA] を選択し、[編集] をクリックします。

3 次のオプションから 1 つ選択します。

オプション	結果
vCenter HA を有効にする	アクティブ ノードとパッシブ ノード間のレプリケーションが有効になります。クラスタが健全な状態の場合、アクティブ ノードは、パッシブ ノードからの自動フェイルオーバーによって保護されます。
メンテナンス モード	メンテナンス モードでも、アクティブ ノードとパッシブ ノード間のレプリケーションが実行されます。ただし、自動フェイルオーバーは無効になります。
vCenter HA を無効にする	レプリケーションとフェイルオーバーが無効になります。クラスタの構成が維持されます。後で再び vCenter HA を有効にすることができます。
vCenter HA クラスタの削除	クラスタを削除します。レプリケーションとフェイルオーバー機能は提供されなくなります。アクティブ ノードはスタンドアローンの vCenter Server として動作を継続します。詳細については、vCenter HA の構成の削除を参照してください。

4 OK をクリックします。

バックアップおよびリストア操作の実行

セキュリティを強化するために、vCenter HA クラスタのアクティブ ノードをバックアップすることができます。バックアップしておくと、致命的な障害が発生した場合に、ノードをリストアできます。

注： アクティブ ノードをリストアする前に、クラスタ構成を削除します。アクティブ ノードをリストアする際にパッシブ ノードが実行されているか、または他のクラスタ構成がまだ適用されている場合、予期できない結果が発生します。

前提条件

vCenter HA にバックアップおよびリストア ソリューションとの相互運用性があることを確認します。ソリューションの 1 つに、vCenter Server ファイルベースのリストアがあります。

手順

1 アクティブ ノードをバックアップします。

パッシブ ノードと監視ノードは、バックアップしないでください。

2 クラスタをリストアする前に、すべての vCenter HA ノードをパワーオフし、削除します。

3 アクティブ ノードをリストアします。

アクティブ ノードがスタンドアロン vCenter Server としてリストアされます。

vCenter HA の構成の削除

vCenter HA の構成は、vSphere Client から削除することができます。

手順

1 アクティブ ノードの vCenter Server にログインし、[構成] をクリックします。

2 [設定] で [vCenter HA] を選択し、[VCHA の削除] をクリックします。

- vCenter HA クラスタの構成がアクティブ、パッシブおよび監視ノードから削除されます。
- パッシブ ノードと監視ノードを削除することができます。
- アクティブ ノードはスタンドアローンの vCenter Server として稼働し続けます。
- 新しい vCenter HA の構成でパッシブ ノードと監視ノードを再利用することはできません。
- 手動構成を実施した場合や、パッシブ ノードと監視ノードが検出できない場合、それらのノードを明示的に削除する必要があります。
- この削除プロセスでは、構成プロセスで 2 つ目の仮想 NIC が追加されていたとしても、その仮想 NIC は削除されません。

すべての vCenter HA ノードの再起動

クラスタ内のすべてのノードをシャットダウンして再起動する必要がある場合は、パッシブ ノードがアクティブ ノードのロールを引き継がないように、所定の順序に従ってシャットダウンする必要があります。

手順

1 この順序でノードをシャットダウンします。

- パッシブ ノード
- アクティブ ノード
- 監視ノード

2 各ノードを再起動します。

任意の順序でノードを再起動できます。

3 すべてのノードがクラスタに正常に参加していること、また、前のアクティブ ノードがそのロールを再開していることを確認します。

サーバ環境の変更

vCenter Server のデプロイ時には、環境を選択します。vCenter HA では、運用環境用に小規模、中規模、大規模、超大規模の各環境がサポートされています。容量を拡大する必要があり環境を変更する場合は、構成の変更前にパッシブ ノードの仮想マシンを削除する必要があります。

手順

1 vSphere Client でアクティブ ノードにログインし、クラスタ構成を編集して、[無効にする] を選択します。

2 パッシブ ノードの仮想マシンを削除します。

3 アクティブ ノードの vCenter Server 構成を、たとえば小規模環境から中規模環境に変更します。

4 vCenter HA を再構成します。

vCenter HA ノードのサポート バンドルの収集

vCenter HA クラスタ内のすべてのノードからサポート バンドルを収集すると、トラブルシューティングに役立ちます。

vCenter HA クラスタのアクティブ ノードからサポート バンドルを収集するとき、システムによって次の処理が実行されます。

- アクティブ ノードそのものからサポート バンドル情報を収集します。
- パッシブ ノードと監視ノードからサポート バンドルを収集し、アクティブ ノードのサポート バンドルの `commands` ディレクトリに配置します。

注： パッシブ ノードと監視ノードからのサポート バンドルの収集は可能な場合に行われる処理であり、これらのノードに到達できる場合に実行されます。

vCenter HA 環境のトラブルシューティング

問題が発生した場合は、環境をトラブルシューティングします。実行する必要があるタスクは、障害の症状に応じて異なります。トラブルシューティングに関する詳しい情報については、VMware のナレッジベース システムを参照してください。

- デプロイ中に vCenter HA のクローン作成操作が失敗する

  vCenter HA の構成プロセスでクローンが正常に作成されない場合は、クローン作成エラーを解決する必要があります。

- パッシブ ノードまたは監視ノードの再デプロイ

  パッシブ ノードまたは監視ノードで障害が発生したとき、vCenter HA クラスタが自動クローン作成方法を使用して構成されていた場合は、[vCenter HA の設定] ページで再デプロイすることができます。

- エラーが発生して vCenter HA のデプロイが失敗する

  ネットワーク設定に関する問題など、構成の問題によってデプロイ エラーが発生することがあります。

- 低下状態の vCenter HA クラスタのトラブルシューティング

  vCenter HA クラスタが健全な状態であるためには、アクティブ ノード、パッシブ ノード、および監視ノードのそれぞれが完全に動作しており、vCenter HA クラスタ ネットワーク上でアクセスできる必要があります。いずれかのノードでエラーが発生すると、クラスタは低下した状態にあると見なされます。

- vCenter HA ノードの隔離状態からのリカバリ

  vCenter HA クラスタ内の一部のノードが互いに通信できなくなった場合、アクティブ ノードは、クライアントの要求に対する処理を中止します。

- フェイルオーバー障害の解決

  フェイルオーバー中にパッシブ ノードがアクティブ ノードにならなかった場合は、パッシブ ノードを強制的にアクティブ ノードにできます。

- VMware vCenter® HA アラームおよびイベント

  vCenter HA クラスタの状態が低下した場合、アラームおよびイベントにエラーが表示されます。

デプロイ中に vCenter HA のクローン作成操作が失敗する

vCenter HA の構成プロセスでクローンが正常に作成されない場合は、クローン作成エラーを解決する必要があります。

問題

クローン作成操作が失敗します。

注： ソースのアクティブ ノードの仮想マシンと同じ NFS 3.1 データストアへの VCHA 環境用のパッシブ仮想マシンまたは監視仮想マシンのクローン作成に失敗します。NFS 4 を使用するか、アクティブな仮想マシンとは異なるデータストアにパッシブ仮想マシンと監視仮想マシンをクローン作成する必要があります。

原因

クローン作成で例外が発生していないか確認してください。次のいずれかの問題が該当する可能性があります。

- DRS 対応のクラスタであるにもかかわらず、3 つのホストが存在しない。
- ホストまたはデータベース接続が失われた。
- ディスク容量が不足している。
- その他、[仮想マシンのクローン作成]に関するエラー。

解決方法

1 問題の原因になったエラーを解決します。

2 クラスタを削除してからもう一度最初から構成を行います。

パッシブ ノードまたは監視ノードの再デプロイ

パッシブ ノードまたは監視ノードで障害が発生したとき、vCenter HA クラスタが自動クローン作成方法を使用して構成されていた場合は、[vCenter HA の設定] ページで再デプロイすることができます。

手順

1 vSphere Client を使用してアクティブ ノードにログインします。

2 インベントリで vCenter Server オブジェクトを選択し、[構成] タブを選択します。

3 [設定] で [vCenter HA] を選択します。

4 再デプロイ ウィザードを起動するノードの横にある [再デプロイ] ボタンをクリックします。

5
   - vCenter Server が同じ SSO ドメイン内の別の vCenter Server によって管理されている場合は、手順 6 に進みます。
   - vCenter Server が別の SSO ドメインの vCenter Server によって管理されている場合は、その管理 vCenter Server の場所と認証情報の詳細を入力します。[管理 vCenter Server の FQDN または IP アドレス] と [Single Sign-On] 認証情報を入力します。

6 一意の名前とターゲットの場所を指定します。

7 操作のターゲットのコンピューティング リソースを選択します。

8 構成とディスク ファイルを保存するデータストアを選択します。

9 仮想マシン ネットワークを構成します。
   - パッシブ ノードを再デプロイしている場合は、仮想マシン管理 (NIC 0) ネットワークと vCenter HA (NIC 1) ネットワークを選択します。
   - 監視ノードを再デプロイしている場合は、vCenter HA (NIC 1) ネットワークを選択します。

   選択に問題があると、エラーまたは互換性の警告が表示されます。

10 選択内容を確認し、[完了] をクリックして、ノードを再デプロイします。

エラーが発生して vCenter HA のデプロイが失敗する

ネットワーク設定に関する問題など、構成の問題によってデプロイ エラーが発生することがあります。

問題

vCenter HA クラスタ構成を開始すると、エラーが発生して構成が失敗します。たとえば SSH 接続障害のメッセージなど、問題の原因が示されることがあります。

解決方法

デプロイが失敗する場合は、ネットワーク問題を解決するための手順を実行します。

1 アクティブ ノードからパッシブ ノードと監視ノードにアクセスできることを確認します。

2 ノード間のルーティングが正しく設定されていることを確認します。

3 ネットワーク遅延をチェックします。

低下状態の vCenter HA クラスタのトラブルシューティング

vCenter HA クラスタが健全な状態であるためには、アクティブ ノード、パッシブ ノード、および監視ノードのそれぞれが完全に動作しており、vCenter HA クラスタ ネットワーク上でアクセスできる必要があります。いずれかのノードでエラーが発生すると、クラスタは低下した状態にあると見なされます。

問題

クラスタが低下した状態にあると、フェイルオーバーを実行できません。クラスタが低下状態にある場合の障害シナリオの詳細については、フェイルオーバー障害の解決を参照してください。

原因

クラスタの低下状態には、さまざまな理由が考えられます。

いずれかのノードで障害が発生

- アクティブ ノードに障害が発生した場合、アクティブ ノードからパッシブ ノードへのフェイルオーバーが自動的に行われます。フェイルオーバー後は、パッシブ ノードがアクティブ ノードになります。

  この時点で、元のアクティブ ノードは使用できなくなるため、クラスタは低下した状態になります。

  障害の発生したノードが修復されるか、オンラインになると、このノードが新たにパッシブ ノードとなり、アクティブ ノードとパッシブ ノードの同期後にクラスタは健全な状態に戻ります。

- パッシブ ノードで障害が発生した場合、アクティブ ノードは引き続き機能しますが、フェイルオーバーは実行できず、クラスタは低下した状態になります。

  パッシブ ノードは、修復されるか、オンラインになると自動的に再びクラスタに参加し、クラスタは、アクティブ ノードとパッシブ ノードの同期後、健全な状態になります。

- 監視ノードで障害が発生した場合、アクティブ ノードは稼働し続け、アクティブ ノードとパッシブ ノードとの間でレプリケーションが続行されますが、フェイルオーバーは実行できなくなります。

監視ノードは修復されてオンラインになると自動的に再びクラスタに参加し、クラスタは健全な状態になります。

データベースのレプリケーションが失敗

アクティブ ノードとパッシブ ノード間のレプリケーションが失敗すると、クラスタは低下した状態と見なされます。その後もアクティブ ノードは、パッシブ ノードとの同期を実行します。それが成功すると、クラスタは健全な状態に戻ります。この状態は、ネットワーク バンド幅の問題やその他のリソース不足が原因である可能性があります。

構成ファイルのレプリケーションの問題

アクティブ ノードとパッシブ ノードとの間で構成ファイルのレプリケーションが適切に実行されなかった場合、クラスタは低下した状態になります。その後もアクティブ ノードは、パッシブ ノードとの同期を試みます。この状態は、ネットワーク バンド幅の問題やその他のリソース不足が原因である可能性があります。

解決方法

リカバリの方法は、クラスタの状態が低下した原因によって異なります。クラスタの状態が低下した場合、イベント、アラーム、SNMP トラップにエラーが表示されます。

いずれかのノードがダウンしている場合は、ハードウェアの障害またはネットワークの隔離をチェックしてください。障害の発生したノードがパワーオン状態であるかどうかを確認します。

レプリケーションに失敗する場合は、vCenter HA ネットワークの帯域幅が十分に確保されていることと、ネットワークの遅延が 10 ミリ秒以下であることを確認してください。

vCenter HA ノードの隔離状態からのリカバリ

vCenter HA クラスタ内の一部のノードが互いに通信できなくなった場合、アクティブ ノードは、クライアントの要求に対する処理を中止します。

問題

ノードの隔離は、ネットワーク接続の問題です。

解決方法

1. 接続の問題の解決を試みます。接続を復旧できる場合、隔離されたノードは自動的に再びクラスタに参加し、アクティブ ノードはクライアントの要求処理を開始します。
2. 接続の問題を解決できない場合、アクティブ ノードのコンソールに直接ログインする必要があります。
   a. パッシブ ノードと監視ノードの仮想マシンをパワーオフし、削除します。
   b. 仮想マシン コンソールまたは SSH を使用してアクティブ ノードにログインします。
   c. Bash シェルを有効にするには、`appliancesh` プロンプトで **`shell`** と入力します。
   d. 次のコマンドを実行して、vCenter HA の構成を削除します。

```
vcha-destroy -f
```

e アクティブ ノードを再起動します。

この時点でアクティブ ノードはスタンドアロン vCenter Server になります。

f vCenter HA クラスタの構成を再度実行します。

フェイルオーバー障害の解決

フェイルオーバー中にパッシブ ノードがアクティブ ノードにならなかった場合は、パッシブ ノードを強制的にアクティブ ノードにできます。

問題

パッシブ ノードがアクティブ ノードのロールの引き継ぎを試行している間に失敗します。

原因

vCenter HA フェイルオーバーが失敗する原因としては、次が考えられます。

- パッシブ ノードがアクティブ ノードのロールの引き継ぎを試行している間に、監視ノードが使用できなくなった。
- ノード間でのサーバ状態の同期に問題がある。

解決方法

この問題からは、次のように回復します。

1 アクティブ ノードが障害から回復した場合、そのノードは、再度アクティブ ノードになります。

2 監視ノードが障害から回復した場合は、次の手順を実行します。

a 仮想マシン コンソールで、パッシブ ノードにログインします。

b Bash シェルを有効にするには、`appliancesh` プロンプトで **`shell`** と入力します。

c 次のコマンドを実行します。

```
vcha-reset-primary
```

d パッシブ ノードを再起動します。

3 アクティブ ノードと監視ノードが両方ともリカバリできなかった場合は、パッシブ ノードを強制的にスタンドアローン vCenter Server にできます。

a アクティブ ノードと監視ノードの仮想マシンを削除します。

b 仮想マシン コンソールで、パッシブ ノードにログインします。

c Bash シェルを有効にするには、`appliancesh` プロンプトで **`shell`** と入力します。

d 次のコマンドを実行します。

```
vcha-destroy
```

e パッシブ ノードを再起動します。

VMware vCenter® HA アラームおよびイベント

vCenter HA クラスタの状態が低下した場合、アラームおよびイベントにエラーが表示されます。

問題

表 4-4. 次のイベントが vpxd に VCHA 健全性アラームを生成します。

イベント名	イベントの説明	イベント タイプ	カテゴリ
vCenter HA クラスタの状態は現在 [健全] です	vCenter HA クラスタの状態は現在 [健全] です	com.vmware.vcha.cluster.state.healthy	情報
vCenter HA クラスタの状態は現在 [低下しました] です	vCenter HA クラスタの状態は現在 [低下しました] です	com.vmware.vcha.cluster.state.degraded	警告
vCenter HA クラスタの状態は現在 [隔離] です	vCenter HA クラスタの状態は現在 [隔離] です	com.vmware.vcha.cluster.state.isolated	エラー
vCenter HA クラスタは破棄されます	vCenter HA クラスタは破棄されます	com.vmware.vcha.cluster.state.destroyed	情報

表 4-5. 次のイベントが vpxd に PSC HA 健全性アラームを生成します。

イベント名	イベントの説明	イベント タイプ	カテゴリ
PSC HA クラスタの状態は現在 [健全] です	PSC HA クラスタの状態は現在 [健全] です	com.vmware.vcha.psc.ha.health.healthy	情報
PSC HA クラスタの状態は現在 [低下しました] です	PSC HA クラスタの状態は現在 [低下しました] です	com.vmware.vcha.psc.ha.health.degraded	情報
vCenter HA クラスタの破棄後、PSC HA は監視されません	PSC HA の状態は監視されていません	com.vmware.vcha.psc.ha.health.unknown	情報

表 4-6. クラスタの状態関連のイベント

イベント名	イベントの説明	イベント タイプ	カテゴリ
ノード {nodeName} が再びクラスタに参加しました	あるノードが再びクラスタに参加しました	com.vmware.vcha.node.joined	情報
ノード {nodeName} がクラスタへの参加を解除しました	あるノードがクラスタへの参加を解除しました	com.vmware.vcha.node.left	警告
フェイルオーバーに成功しました	フェイルオーバーに成功しました	com.vmware.vcha.failover.succeeded	情報
クラスタが無効モードの場合、フェイルオーバーは続行できません	クラスタが無効モードの場合、フェイルオーバーは続行できません	com.vmware.vcha.failover.failed.disabled.mode	警告
クラスタに 3 台すべてのノードが接続されていない場合、フェイルオーバーは続行できません	クラスタに 3 台すべてのノードが接続されていない場合、フェイルオーバーは続行できません	com.vmware.vcha.failover.failed.node.lost	警告

表 4-6. クラスタの状態関連のイベント （続き）

イベント名	イベントの説明	イベント タイプ	カテゴリ
パッシブ ノードの vPostgres が引き継ぎの準備ができていない場合、フェイルオーバーは続行できません	パッシブ ノードが引き継ぎの準備ができていない場合、フェイルオーバーは続行できません	com.vmware.vcha.failover.failed.passive.not.ready	警告
vCenter HA クラスタ モードが {clusterMode} に変更されました	vCenter HA クラスタ モードが変更されました	com.vmware.vcha.cluster.mode.changed	情報

表 4-7. データベースのレプリケーションに関連するイベント

イベント名	イベントの説明	イベント タイプ	カテゴリ
データベースのレプリケーション モードが {newState} に変更されました	データベースのレプリケーション状態が変更されました：同期、非同期またはレプリケーションなし	com.vmware.vcha.DB.replication.state.changed	情報

表 4-8. ファイルのレプリケーションに関連するイベント

イベント名	イベントの説明	イベント タイプ	カテゴリ
アプライアンス {fileProviderType} は {state} です	アプライアンス ファイルのレプリケーション状態が変更されました	com.vmware.vcha.file.replication.state.changed	情報

vCenter High Availability 環境へのパッチの適用

vCenter High Availability クラスタの vCenter Server にパッチを適用するには、vCenter Server シェルにある **`software-packages`** ユーティリティを使用します。

詳細については、『vSphere のアップグレード』の「vCenter High Availability 環境へのパッチの適用」を参照してください。

vCenter HA のダウンタイムの短縮アップグレード

vSphere 8.0 U3 では、ダウンタイムの短縮アップグレードが vCenter HA の自動デプロイと統合されています。

ダウンタイムの短縮アップグレード (RDU) は、移行ベースの VCSA アップグレードであり、主な目的はアップグレードのダウンタイムを短縮することです。VCSA 構成の RDU アップグレード中に、VCDB データベースとネットワーク情報が古い VCSA から新しい VCSA バージョンにコピーされてから、ソース VCSA をシャットダウンしてターゲット VCSA に切り替えます。移行アップグレード中に、RDU の切り替え前のステージング フェーズでは、VCHA が自動的にデプロイ解除されます。アップグレード中は VCHA がありません。RDU の切り替えに成功すると、VCHA がターゲット ノードに再デプロイされます。

RDU アップグレードは、自己管理型の vCenter Server や自己管理型以外の vCenter Server を含む、vCenter HA の自動デプロイと統合されています。vCenter Server が自己管理型である場合は、vCenter Server の認証情報なしで vCenter Server をアップグレードできます。自己管理型以外の vCenter Server をアップグレードする場合は、サービス アカウントの認証情報を使用して、RDU フレームワークから提供される vCenter Server を管理する必要があります。アップグレードの前後に vCenter HA を削除またはセットアップしなくても、VCHA を含む vCenter Server Appliance をアップグレードできます。アップグレードをキャンセルすると、RDU ロールバックによって、vCenter HA のデプロイはアップグレード前と同様に機能します。