

vSphere 可用性

VMware vSphere 5.5

VMware ESXi 5.5

vCenter Server 5.5

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各製品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、<http://www.vmware.com/jp/support/pubs> を参照してください。

JA-001254-00

vmware[®]

最新の技術ドキュメントは VMware の Web サイト (<http://www.vmware.com/jp/support/>) にあります
VMware の Web サイトでは最新の製品アップデートも提供されています。

このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

Copyright © 2009–2013 VMware, Inc. 無断転載を禁ず。著作権および商標情報。

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

ヴァイムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

vSphere の可用性について	5
1 ビジネス継続性とダウンタイムの最小化	7
計画的ダウンタイムの短縮	7
計画外のダウンタイムの防止	8
vSphere HA が提供する、システム停止からの迅速なリカバリ	8
vSphere フェールトトレランスが提供する継続的な可用性	9
2 vSphere HA クラスタの作成と使用	11
vSphere HA の動作	11
vSphere HA のアドミッションコントロール	19
vSphere HA のチェックリスト	25
vSphere HA クラスタの作成	26
vSphere HA 動作のカスタマイズ	30
vSphere HA クラスタのベストプラクティス	33
3 仮想マシンのフェールトトレランスの準備	37
フェールトトレランスの機能	38
フェールトトレランスと DRS の併用	39
フェールトトレランスの使用事例	39
Fault Tolerance のチェックリスト	40
Fault Tolerance の相互運用性	41
Fault Tolerance に向けたクラスタとホストの準備	43
仮想マシンのフェールトトレランスの準備	45
vSphere Web Client でのフェールトトレランス機能を持つ仮想マシンの情報の表示	49
Fault Tolerance のベストプラクティス	50
推奨される vSphere Fault Tolerance の構成	52
インデックス	53

vSphere の可用性について

『vSphere 可用性ガイド』は、vSphere[®] High Availability (HA) と vSphere フォールトトレランスの設定方法など、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。

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。

ビジネス継続性とダウンタイムの最小化

計画的または計画外のいずれの場合でも、ダウンタイムによって多大なコストが生じます。一方、従来、高いレベルの可用性を実現するため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。

当社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、組織はより簡単で安価に、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対して提供される可用性の基準レベルを向上させることができます。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とは関係なく、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。

この章では次のトピックについて説明します。

- [計画的ダウンタイムの短縮 \(P. 7\)](#)
- [計画外のダウンタイムの防止 \(P. 8\)](#)
- [vSphere HA が提供する、システム停止からの迅速なリカバリ \(P. 8\)](#)
- [vSphere フォールト トレランスが提供する継続的な可用性 \(P. 9\)](#)

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。

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 チューニング。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。

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、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仮想マシン内で実行される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 フォールトトレランス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。これは、ESXi ホスト プラットホーム上の VMware vLockstep テクノロジーを使用して行われます。vLockstep は、プライマリおよびセカンダリ仮想マシンに同一の x86 命令シーケンスを実行させてこれを実現しています。プライマリ仮想マシンでは、プロセッサから仮想 I/O デバイスへのすべての入力とイベントが取得され、それがセカンダリ仮想マシンで再現されます。セカンダリ仮想マシンは、プライマリ仮想マシンと同一の一連の命令を実行しますが、単一の仮想マシン イメージ（プライマリ仮想マシン）のみがワークロードを実行します。

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。

vSphere HA クラスタの作成と使用

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、詳細な属性を使用して動作をカスタマイズし、次の推奨ベスト プラクティスによってパフォーマンスを最適化できます。

注意 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>

この章では次のトピックについて説明します。

- [vSphere HA の動作 \(P. 11\)](#)
- [vSphere HA のアドミッション コントロール \(P. 19\)](#)
- [vSphere HA のチェックリスト \(P. 25\)](#)
- [vSphere HA クラスタの作成 \(P. 26\)](#)
- [vSphere HA 動作のカスタマイズ \(P. 30\)](#)
- [vSphere HA クラスタのベスト プラクティス \(P. 33\)](#)

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 つのホストがマスター ホストとして自動的に選択されます。マスター 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スレーブ 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、マスター 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。マスター 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する必要があります。マスター 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。

マスター ホストとスレーブ 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、マスター ホストまたはスレーブ ホストとして機能します。

クラスタ用に vSphere HA が有効化されると、アクティブなすべてのホスト（スタンバイやメンテナンス モード以外の、切断されていないホスト）がクラスタのマスタ候補になります。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マスター ホストは 1 つだけで、残りはすべてスレーブ ホストになります。マスター ホストに障害が発生したり、シャットダウンしたり、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、選び直します。

クラスタのマスター ホストには多くの責任があります。

- スレーブ ホストの状態を監視する。スレーブ ホストに障害が発生したり接続できなくなったりした場合、マスター ホストは、どの仮想マシンを再起動する必要があるかを確認します。
- 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、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マスター 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。

スレーブ 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、状態の更新をマスター ホストにレポートすることでクラスタに貢献します。マスター ホストも仮想マシンを実行し、監視できます。スレーブ ホストとマスター 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。

マスター 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、仮想マシンはマスター ホストによって保護されます。マスター ホストはクラスタのデータストアに保護された仮想マシンのリストを保持します。新しく選択されたマスター 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。

注意 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すべて、vSphere HA の保護対象ではなくなります。

ホスト障害のタイプと検出

vSphere HA クラスタのマスター ホストは、スレーブ ホストの障害検出を行う責任があります。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をフェイルオーバーする必要があることがあります。

vSphere HA クラスタでは、3 種類のホスト障害が検出されます。

- ホストが機能を停止する（すなわち障害）。
- ホストがネットワーク隔離される。
- ホストがマスター ホストとの接続を失う。

マスター ホストは、クラスタ内のスレーブ ホストの稼動状態を監視します。この通信は、ネットワーク ハートビートを毎秒、交換することによって行われます。スレーブ ホストからのこのハートビートの受信が停止すると、マスター 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。マスター ホストは、スレーブ 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 \(P. 16\)」](#) 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。

マスター ホストがスレーブ ホストのエージェントと直接、通信できない場合は、スレーブ ホストは ICMP ping に応答せず、そのエージェントはハートビートを送出しないうので、障害とみなされます。このホストの仮想マシンは、代わりにホスト上で再起動されます。そのようなスレーブ 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、マスター ホストは、そのスレーブ ホストがネットワークパーティションにあるか、隔離されたネットワークにあると推測し、ホストと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 \(P. 15\)」](#) を参照してください。

ホストがネットワーク隔離されるのは、まだ実行中であっても、管理ネットワークの 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、クラスターの隔離アドレスに ping を試みます。ping にも応答がなかった場合、そのホストは自身をネットワークから隔離されたとみなします。

マスター ホストは、隔離されたホストで実行中の仮想マシンを監視します。仮想マシンがパワーオフし、マスター ホストが責任を負っている場合は、その仮想マシンを再起動します。

注意 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、ネットワークの隔離はほとんど発生しません。

ホスト問題に対する対応の判断

ホストで障害が発生してそ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の設定によって再起動を行う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。

これらの設定は、ホストで障害が発生した場合、またはホストが隔離された場合に、クラスタ内のすべての仮想マシンに対して適用されます。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。[「vSphere Web Client での個々の仮想マシンのカスタマイズ \(P. 33\)」](#) を参照してください。

仮想マシン再起動の優先順位

仮想マシン再起動の優先順位は、ホストで障害が発生したあとで仮想マシンが新しいホストに配置される相対的な順序を決定します。そうした仮想マシンは、優先順位の高い仮想マシンから優先順位の低い仮想マシンへと再起動され、すべての仮想マシンが再起動されるか、クラスタのリソースに余裕がなくなるまで試行されます。vSphere HA が優先順位の高い仮想マシンをパワーオンするのに失敗した場合、優先順位の低い仮想マシンのパワーオンを続行しようとする点に注意してください。そのため、仮想マシン再起動の優先順位を使用して、複数の仮想マシン アプリケーションの再起動の優先順位を強制的に実行することはできません。また、ホストの障害数がアドミッションコントロールで許可している値を超えた場合、再起動の優先順位が低い仮想マシンは、使用可能なリソースが増えるまで再起動されない可能性もあります。仮想マシンは、フェイルオーバー ホストが指定されている場合、そこで再起動されます。

この設定の値は、次のとおりです。無効、低、中 (デフォルト)、および高。無効を選択すると、仮想マシンに対して vSphere HA が無効になります。これは、ESXi ホストで障害が発生した場合に、仮想マシンがほかの ESXi ホストで再起動されないことを意味します。無効を選択しても、vSphere HA の仮想マシンとアプリケーションの監視機能で無視されます。これは、この機能により、仮想マシンの障害ではなくオペレーティングシステム レベルの障害に対して仮想マシンが保護されるからです。オペレーティングシステム レベルの障害が発生すると、vSphere HA によってオペレーティングシステムが再起動され、仮想マシンは同じホストで稼働したままになります。この設定は、仮想マシンごとに変更できます。

注意 仮想マシンをリセットすると、ゲスト OS が強制的に再起動されますが、仮想マシンは電源サイクルされません。

仮想マシン再起動の優先順位設定は、ユーザーのニーズによって異なります。最も重要なサービスを提供する仮想マシンに、最も高い再起動の優先順位を割り当てます。

たとえば、多重階層のアプリケーションでは、仮想マシン上にホストされている機能に応じて、割り当てをランク付けすることができます。

- 高：アプリケーションにデータを提供するデータベース サーバ。
- 中：データベースのデータを消費し、その結果を Web ページに提供するアプリケーション サーバ。
- 低：ユーザー要求を受け取り、問い合わせをアプリケーション サーバに渡して、その結果をユーザーに戻す Web サーバ。

ホストの隔離時の対応

ホスト隔離時の対応により、vSphere HA クラスタ内のホストの管理ネットワーク接続が切断されたときに実行が継続されている場合にどうするかが決まります。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。ホストが隔離されると、ホストは隔離時の対応を実行します。具体的には、パワーオンのままにする（デフォルト）、パワーオフ後フェイルオーバー、およびシャットダウン後フェイルオーバーという対応があります。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。

注意 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 秒以内または詳細属性 `das.isolationshutdowntimeout` で指定した秒数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。

注意 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。

ホスト隔離時の対応が無効（隔離時に仮想マシンをパワーオンにしたまま）で、管理ネットワークおよびストレージネットワークにアクセスできなくなった場合、「スプリット ブレーン」状態が発生することがあります。このケースでは、隔離されたホストはディスク ロックを失い、仮想マシンの元のインスタンスが隔離されたホストで実行中のままでも、仮想マシンは他のホストにフェイルオーバーされます。ホストが仮想マシンのデータストアに再びアクセスできるようになると、仮想マシンが 2 コピーあることになりませんが、元の隔離されたホスト上のコピーは `vmdk` ファイルにアクセスできず、データは破損しません。

この状態を修復するために、ESXi は、ディスク ロックを失った仮想マシンについて、ホストがいつ隔離から脱出してディスク ロックを再取得できないことに気づいたかという質問を作成します。vSphere HA は自動的にこの質問に回答し、ディスク ロックを失った仮想マシンのインスタンスはパワーオフし、ディスク ロックを所有するインスタンスはそのままにします。

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（クラスターレベルの属性）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を確認されます。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、詳細属性 `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。

監視感度のデフォルト設定は、表 2-1 に記載されています。[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。

注意 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した場合の再起動とは異なります。

ネットワークパーティション

vSphere HA クラスターで管理ネットワークの障害が発生すると、そのクラスターのホストの一部は、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。クラスター内に複数のパーティションが発生します。

クラスター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ー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ー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マスター 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。マスター ホストは、vCenter Server と通信する必要があります。マスター 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 が通信できるのは、クラスタ内の一部のホストとのみで、1 つのマスター ホストのみとしか接続できません。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。

vSphere HA クラスタに ESXi 5.0 より前のホストが含まれている状態でパーティションが発生した場合、vSphere HA は、ユーザーがパワーオフした仮想マシンを過ってパワーオンしたり、障害の発生した仮想マシンの再起動に失敗したりする恐れがあります。

データストア ハートビート

vSphere HA クラスタ内のマスター ホストが管理ネットワーク経由でスレーブ ホストと通信できないとき、マスター ホストはデータストア ハートビートを使用して、スレーブ ホストに障害があるかどうか、スレーブ ホストがネットワークパーティションにあるのか、分離されたネットワークにあるのかを確認します。スレーブ 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、障害が発生して仮想マシンはほかのところで再起動されているとみなします。

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 サーバーにバックアップされる可能性が最小になるように行われます。

詳細属性の `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せん。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、最大使用量は約 2GB で、通常の使用量は 3MB 程度です。vmfs5 では、最大使用量と通常の使用量は約 3MB です。vSphere HA がデータストアを使用することによるオーバーヘッドは無視できる程度で、他のデータストア処理のパフォーマンスには影響しません。

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、制限数の仮想マシンまでしか vSphere HA によって保護されません。

注意 Virtual SAN 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、Virtual SAN ネットワークとは独立した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、必要など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 5.x 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 4.x 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）。
- レガシー ESX 4.x ホストでは、vSphere HA は `/var/log/vmware/fdm` に書き込みます。

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インします。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、マスター 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中のホストだけです。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 と Virtual SAN の併用

Virtual SAN 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、Virtual SAN 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 Virtual SAN 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。

Virtual SAN の詳細については、『vSphere ストレージ』を参照してください。

ESXi ホストの要件

Virtual SAN 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

Virtual SAN には独自のネットワークがあります。Virtual SAN 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。Virtual SAN が無効のときだけ、vSphere HA は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とき、vCenter Server は適切なネットワークを選択します。

注意 vSphere HA が無効のときだけ、Virtual SAN を有効にできます。

Virtual SAN 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。したがって、Virtual SAN のネットワークに変更を加えるには、vSphere Web 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 Virtual SAN ネットワークに変更を加えます。
- 3 クラスタのすべてのホストを選択して右クリックし、[HA の再構成] を選択します。
- 4 vSphere HA クラスタの [ホストの監視] を有効に戻します。

表 2-2 に、Virtual SAN が使用されているときと使用されていないときの vSphere HA ネットワークの相違点を示します。

表 2-2. vSphere HA ネットワークの相違点

	Virtual SAN 有効時	Virtual SAN 無効時
vSphere HA が使用するネットワーク	Virtual SAN 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 つ以上のホストにマウントされる、Virtual SAN データストア以外のデータストア	2 つ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、Virtual SAN 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

容量の予約設定

vSphere HA クラスタにアドミッション コントロール ポリシーで容量を予約する場合、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 Virtual SAN の対応する設定と関係させる必要があります。特に、Virtual SAN 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容量よりも低くすることはできません。

たとえば、Virtual SAN 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。一方、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 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 リソース管理』ドキュメントを参照してください。

vSphere HA のアドミッション コントロール

vCenter Server はアドミッション コントロールを使用することで、フェイルオーバー保護を提供できるだけの十分なリソースをクラスタ内に確保し、仮想マシンのリソース予約が必ず順守されるようにします。

3 つのタイプのアドミッション コントロールを使用できます。

ホスト	ホスト上で実行されるすべての仮想マシンの予約を満たすのに十分なリソースを、そのホストに確保します。
リソース プール	リソース プールに関連付けられたすべての仮想マシンの予約、シェア、制限を満たすのに十分なリソースを、そのリソース プールに確保します。
vSphere HA	ホストで障害発生時に仮想マシンをリカバリするための、十分なリソースがクラスタ内で必ず予約されるようにします。

アドミッション コントロールでは、リソース使用率が制約され、その制約に違反するすべてのアクションが禁止されます。禁止されるアクションとしては、次のようなものがあります。

- 仮想マシンのパワーオン。
- ホスト、クラスタ、リソース プールへの仮想マシンの移行。
- 仮想マシンの CPU またはメモリ予約の増加。

3 つのタイプのアドミッション コントロールの中で、無効にできるのは vSphere HA アドミッション コントロールのみです。ただし、このアドミッション 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する保証が得られません。アドミッション コントロールを無効にしないでください。ただし、次のような場合は一時的に無効にする必要があることがあります。

- フェイルオーバーをサポートできるだけの十分なリソースがなく、フェイルオーバー制約に違反する必要がある場合 (ホストをスタンバイ モードにして DPM (Distributed Power Management) の使用をテストするときなど)。
- 自動プロセスで、一時的にフェイルオーバー制約に違反する可能性のあるアクションを実行する必要がある場合 (vSphere Update Manager の指示によるアップグレードの一部など)。

- テストまたはメンテナンス操作を実行する必要がある場合。

アドミッション コントロールは容量を別に確保しますが、障害が発生すると仮想マシンの再起動に利用できるすべての容量が vSphere HA で使用されます。たとえば、vSphere HA は、ユーザーが開始するパワーオンに対してアドミッション コントロールで許可されている以上の仮想マシンをホストに配置します。

注意 vSphere HA アドミッション コントロールが無効なとき、vSphere HA は、DPM が有効で仮想マシンすべてを 1 つのホストに統合できる場合でも、クラスタ内に少なくとも 2 つのパワーオン ホストが確実にあるようにします。これによって確実にフェイルオーバーが可能になります。

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

vSphere HA を構成して、指定した数のホスト障害を許容できます。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 ポリシーでは、vSphere HA 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。

クラスタで許容するホスト障害ポリシーでは、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 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。

注意 vSphere Web 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

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.vmcputminmhz という詳細属性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 の詳細属性を使用して、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 の詳細属性 \(P. 31\)\]](#) 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 Web 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 Web 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。

詳細ランタイム情報

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 ポリシーを選択すると、[詳細ランタイム情報] ペーンが、vSphere Web Client のクラスタの [監視] タブの vSphere HA セクションに表示されます。このペーンには、クラスタに関する次の情報が表示されます。

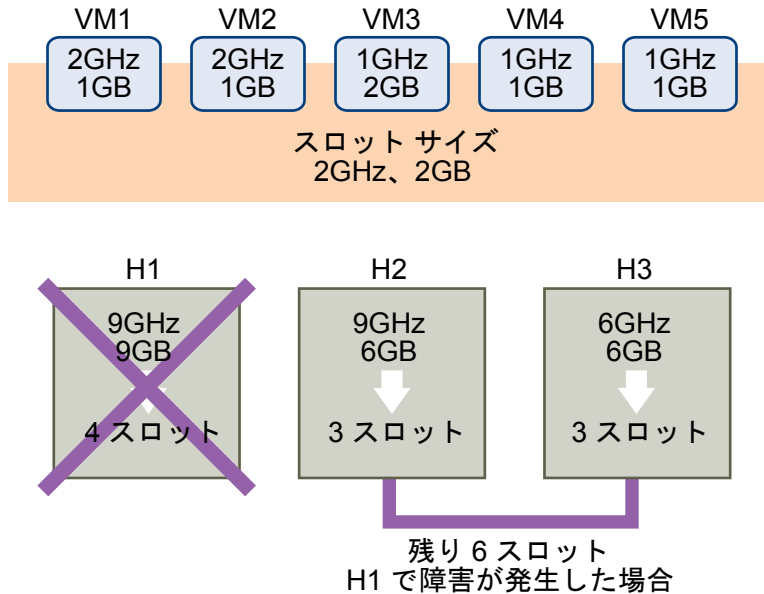
- スロット サイズ。
- クラスタ内のスロット総数。クラスタ内の正常ホストでサポートされるスロット総数。
- 使用済みスロット。パワーオン状態の仮想マシンに割り当てられているスロット数。詳細オプションを使用して、スロット サイズに上限を定義している場合は、パワーオン状態の仮想マシンの数を超えることがあります。これは、一部の仮想マシンが複数のスロットを占有しているからです。
- 使用可能なスロット。クラスタ内で追加の仮想マシンをパワーオンするのに使用できるスロット数。vSphere HA は、フェイルオーバーに必要な数のスロットを予約します。それ以外のスロットは、新しい仮想マシンのパワーオンに使用できます。
- フェイルオーバー スロット。使用済みのスロットや利用可能なスロットをカウントしない総スロット数。
- クラスタ内でパワーオン状態にある仮想マシンの総数。
- クラスタ内のホスト総数。
- クラスタ内の正常ホスト総数。接続されていて、メンテナンス モードでなく、vSphere HA エラーの生じていないホスト数。

例: クラスタで許容するホスト障害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 2-1. 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)。

予約されたクラスタ リソースの割合アドミッション コントロール ポリシー

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。

予約されたクラスタ リソースの割合アドミッション コントロール ポリシーでは、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。

予約されたクラスタ リソース ポリシーでは、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 OMB のメモリおよび 32MHz の CPU が適用されます。

注意 予約されたクラスタ リソースの割合アドミッション コントロール ポリシーでは、クラスタ内に少なくとも 2 つの 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 つしかない場合、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 つしかない場合、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。仮想マシンに対して 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` 詳細属性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。

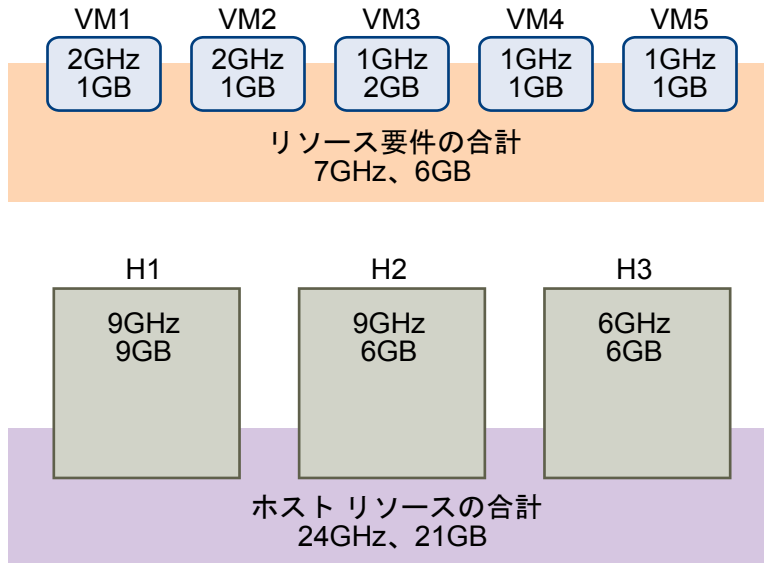
現在の CPU フェイルオーバー キャパシティは、ホスト CPU リソースの合計から、CPU リソース要件の合計を減算し、その結果の値を、ホスト CPU リソースの合計で除算した値になります。現在のメモリ フェイルオーバー キャパシティも同様に計算されます。

例: 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

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 2-2. 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% $((24\text{GHz} - 7\text{GHz}) / 24\text{GHz})$ 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% $((21\text{GB} - 6\text{GB}) / 21\text{GB})$ 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。

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

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。

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。

注意 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 ルールを強制的に実行しようとしません。

現在のフェイルオーバー ホストが、クラスタの [サマリ] タブにある vSphere HA セクションに表示されます。各ホストの隣のステータス アイコンは、緑、黄色、赤のいずれかになります。

- 緑：ホストが接続されている状態で、メンテナンス モードではなく、vSphere HA のエラーはありません。このホストには、パワーオン状態の仮想マシンは存在しません。
- 黄色：ホストが接続されている状態で、メンテナンス モードではなく、vSphere HA のエラーはありません。ただし、このホストには、パワーオン状態の仮想マシンが存在しています。
- 赤：ホストが切断されている状態で、メンテナンス モードであるか、vSphere HA のエラーがあります。

アドミッション コントロール ポリシーの選択

vSphere HA のアドミッション コントロール ポリシーは、可用性のニーズ、およびクラスタの特性に基づいて選択する必要があります。アドミッション コントロール ポリシーを選択する場合は、いくつかの事項を考慮する必要があります。

リソースの断片化の回避

リソースの断片化が発生するのは、フェイルオーバーの対象となる仮想マシンに対して、全体のリソースは十分であるものの、個々のリソースが複数のホストに分散しており、リソースを使用できない場合です。これは、1 台の仮想マシンは同時に 1 台の ESXi ホスト上でしか稼動できないためです。クラスタで許容するホスト障害ポリシーのデフォルト構成では、仮想マシンの最大予約量として 1 つのスロットを定義することにより、リソースの断片化を回避します。クラスタリソースの割合ポリシーは、リソースの断片化の問題について対処しません。フェイルオーバー ホストの指定ポリシーでは、フェイルオーバーに対してホストが予約されるため、リソースは断片化されません。

フェイルオーバー リソースの予約に関する柔軟性

それぞれのアドミッション コントロール ポリシーでは、フェイルオーバーの保護に対してクラスタ リソースを予約する場合のコントロールの細かさが異なります。クラスタで許容するホスト障害ポリシーでは、フェイルオーバー レベルをホストの数として設定できます。クラスタ リソースの割合ポリシーでは、フェイルオーバー に対し、クラスタの CPU またはメモリ リソースを最大 100% まで指定できます。フェイルオーバー ホストの指定ポリシーでは、フェイルオーバー ホストの組を指定できます。

クラスタの異種性

仮想マシンのリソース予約、およびホストのリソース キャパシティの合計については、クラスタは異種であってもかまいません。異種クラスタでは、クラスタで許容するホスト障害ポリシーにおいて、許容する程度がかなり低くなる場合があります。このポリシーでは、スロット サイズを定義する場合に仮想マシンの最大の予約量しか考慮せず、現在のフェイルオーバー キャパシティを計算する場合に、最大のホストで障害が発生することを仮定しているためです。ほかの 2 つのアドミッション コントロール ポリシーは、クラスタの異種性によって影響されません。

注意 vSphere HA は、アドミッション コントロールの計算を実行する場合に、Fault Tolerance のセカンダリ仮想マシンのリソース使用量を含めます。クラスタで許容するホスト障害ポリシーでは、セカンダリ仮想マシンにスロットが割り当てられ、クラスタ リソースの割合ポリシーでは、クラスタで使用可能なキャパシティを計算するときに、セカンダリ仮想マシンのリソース使用率が計上されます。

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 クラスタの要件

vSphere HA クラスタをセットアップする前に、このリストを参照してください。詳細については、該当するクロス リファレンス、または [「vSphere HA クラスタの作成 \(P. 26\)」](#) 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。
- クラスタ内に少なくとも 2 台のホストがある。
- すべてのホストが、固定 IP アドレスを使用して構成されている。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。
- ホスト全体で共通の管理ネットワークが少なくとも 1 つ必要で、ベスト プラクティスとしては、少なくとも 2 つの管理ネットワークを持っておきます。管理ネットワークは、使用しているホストのバージョンによって異なります。
 - ESX ホスト： サービス コンソール ネットワーク。
 - バージョン 4.0 よりも前の ESXi ホスト： VMkernel ネットワーク。

- ESXi ホストバージョン 4.0 およびそれ以降の ESXi ホスト：[管理トラフィック] チェック ボックスが有効になっている VMkernel ネットワーク。

「[ネットワークのベスト プラクティス \(P. 35\)](#)」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確実に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 ネットワークおよびデータストアにアクセスする必要があります。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。

注意 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、信頼性の高いデータストアが環境に存在する場合は、それを参照するように 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 \(P. 14\)](#)」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。ただし、両方のバージョンのプロトコルが混在しているクラスタでは、ネットワーク パーティションが生じる可能性が高まります。

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。

クラスタに対してホスト 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。

注意 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時、自動起動はサポートされません。

vSphere Web 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してください。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 Web 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。

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

開始する前に

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、ホストがその共有ストレージにアクセスでき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。

注意 vSphere HA には、冗長な管理ネットワーク接続を使用してください。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 パスの冗長性 \(P. 36\)」](#) 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提供するために、ホストに少なくとも 2 つのデータストアを構成する必要があります。

手順

- 1 vSphere Web Client で、クラスタを配置するデータ センターに移動して参照します。
- 2 [クラスタの作成] をクリックします。
- 3 [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。
- 4 [OK] をクリックしてウィザードを閉じ、クラスタを作成します。
空のクラスタが作成されました。
- 5 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 Web Client を使用してクラスタにホストを追加します。
- 6 クラスタに移動して参照します。
- 7 [管理] タブをクリックして、[設定] をクリックします。
- 8 [vSphere HA] を選択し、[編集] をクリックします。
- 9 [vSphere HA をオンにする] チェック ボックスを選択します。
- 10 クラスタについて、vSphere HA 設定を適切に構成します。
 - ホストの監視
 - アドミッション コントロール
 - 仮想マシンの監視
 - データストア ハートビート
 - 詳細オプション
- 11 [OK] をクリックします。

これで、ホストを集めた vSphere HA クラスタが構成されました。 [「vSphere Web Client での vSphere HA クラスタ設定の構成 \(P. 28\)」](#) を参照してください。

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

vSphere Web Client での vSphere HA クラスタ設定の構成

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

ホストの監視	ホスト監視を有効にして、クラスタのホストがネットワークのハートビートを相互に送信できるようにし、障害を検出した場合は vSphere HA が動作できるようにします。ここでは、仮想マシン再起動の優先順位とホスト隔離時の対応も設定できます。
<hr/>	
	注意 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。
<hr/>	
アドミッションコントロール	vSphere HA クラスタに対してアドミッション 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 コントロールをどのように実行するかポリシーを選択したりします。
仮想マシンの監視	仮想マシンの監視または仮想マシンとアプリケーションの監視を有効にします。
データストア ハートビート	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。

ホストの監視の構成

クラスタが作成されると、ホストの監視によって vSphere HA マスター ホストは、ホストまたは仮想マシンの障害および管理ネットワークの隔離に対応できるようになります。仮想マシン再起動の優先順位とホスト隔離時の対応によって、ホスト障害と隔離に対する vSphere HA の対応が決まります。

ホストの監視ページは、vSphere HA を有効にした場合のみ表示されます。

手順

- 1 vSphere Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [vSphere HA] を選択し、[編集] をクリックします。
- 4 [ホストの監視] を展開して、ホスト監視の構成オプションを表示します。
- 5 [ホストの監視] を選択してこの機能を有効にします。
- 6 クラスタ内の仮想マシンに対して、[仮想マシン再起動の優先順位] を選択します。

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特定します。優先順位の高い仮想マシンが先に起動されます。この優先順位はホスト単位でのみ適用されます。複数のホストで障害が発生した場合、優先順位が 1 位のホストからすべての仮想マシンを移行し、次に優先順位が 2 位のホストからすべての仮想マシンを移行するといったように、順次移行を行います。

- 7 [ホスト隔離時の対応] を選択します。

ホストの隔離時の対応は、vSphere HA クラスタ内のホストがコンソール ネットワーク接続を切断されても実行し続ける場合に、どのような処理を行うかを特定します。

- 8 [OK] をクリックします。

これで、ホスト監視機能が有効になり、仮想マシン再起動の優先順位とホスト隔離時の対応に関する設定が有効になります。

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 コントロールを使用して、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をフェイルオーバーできるように、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 Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [vSphere HA] 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] を展開して構成オプションを表示します。
- 5 アドミッション コントロールのポリシーを選択してクラスタに適用します。

オプション	説明
静的なホストの数によるフェイルオーバー キャパシティを定義	復旧可能なホスト障害またはフェイルオーバーを保証するホスト障害の最大数を選択します。また、スロット サイズ ポリシーも選択する必要があります。
クラスタ リソースの割合を予約することによるフェイルオーバー キャパシティの定義	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。
専用のフェイルオーバー ホストの使用	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ほかのホストで実行できます。
フェイルオーバー キャパシティを予約しない	このオプションを使用すると、可用性の制約に違反する仮想マシンのパワーオンが可能になります。

- 6 [OK] をクリックします。

アドミッション コントロールが有効になり、選択したポリシーが有効になります。

仮想マシンとアプリケーションの監視の構成

仮想マシンの監視機能は、VMware Tools がゲスト OS の可用性を確認するためにプロキシとして取得するハートビート情報を使用します。この機能によって、vSphere HA は、ハートビートを送信できなくなった個々の仮想マシンをリセットまたは再起動できます。

仮想マシンの監視ページは、vSphere HA を有効にした場合のみ表示されます。

手順

- 1 vSphere Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [vSphere HA] を選択し、[編集] ボタンをクリックします。
- 4 [仮想マシンの監視] を展開して構成オプションを表示します。
- 5 [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] を選択すると、アプリケーションの監視も有効にできます。
- 6 仮想マシンの監視感度は、[低] および [高] の間のスライダを移動して設定します。
- 7 (オプション) カスタム設定を行う場合は [カスタム] を選択します。
- 8 [OK] をクリックします。

データストア ハートビートの構成

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存在す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、管理ネットワークパーティションが発生したときに vSphere HA でホストを監視し、発生したエラーに継続的に応答できます。

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 Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [vSphere HA] を選択し、[編集] をクリックします。
- 4 [データストア ハートビート] を展開して、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。
一覧表示されるのは、vSphere HA クラスタ内の複数のホストで共有されるデータストアです。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。

vSphere HA 動作のカスタマイズ

クラスタを設定したあとで、vSphere HA の動作に影響を与える特定の属性を変更できます。各仮想マシンが継承するクラスタのデフォルト設定を変更することもできます。

使用できる詳細設定を確認して、使用環境内の vSphere HA クラスタを最適化します。これらの属性は 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。

vSphere Web Client での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。

開始する前に

クラスタの管理者権限があることを確認します。

手順

- 1 vSphere Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [vSphere HA] を選択し、[編集] をクリックします。
- 4 [詳細オプション] を展開します。

- 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。
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。

vSphere HA の詳細属性

vSphere HA クラスタの動作に影響を与える詳細属性を設定できます。

表 2-4. vSphere HA の詳細属性

属性	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に ping するアドレスを設定します。このアドレスは、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のみ ping 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。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できるように、このデフォルト ゲートウェイは、使用可能で信頼性の高いアドレスでなければなりません。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 つのアドレスを指定してください。アドレスを指定する数が多すぎると、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属性で指定します (true または false)。
das.isolationshutdowntimeout	システムは、この時間、仮想マシンがシャットダウンするのを待ってからパワーオフします。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.vmcpcuminmhz	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。
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 に設定した場合は、チェックが行われません。
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、作成された構成の発行を無効にします。デフォルト値は false です。

表 2-4. vSphere HA の詳細属性 (続き)

属性	説明
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。有効値は 2~5 の範囲で、デフォルトは 2 です。
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 VM-VM 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「false」であり、ルールは強制されません。「true」に設定して、(vSphere DRS が有効になっていない場合でも) ルールを強制させることもできます。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報告するイベントを発行します。 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。

注意 次の詳細属性のいずれかの値を変更する場合は、変更を有効にする前に、vSphere HA をいったん無効にして、もう一度有効化する必要があります。

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

サポートされなくなったオプション

vCenter Server 5.x では、vSphere HA 用の多数の詳細構成オプションがサポートされなくなりました。次のオプションは現在サポートされていません。

- das.consoleUser
- das.consoleNode
- das.consolePerm
- das.primaryCount
- das.checkVmStateDelay
- das.trace
- das.traceLevel
- das.traceOutput
- das.preferredPrimarys
- das.disableUWSwapRequirement
- das.sensorPollingFreq
- das.bypassNetCompatCheck
- das.defaultfailoverhost
- das.failureDetectionTime
- das.failureDetectionInterval

サポートされなくなったオプションのいずれかの設定を試みた場合、vCenter Server でオプションが無効であることを示すレポートが出力されます。また、これらのオプションが定義されている以前のバージョンから vCenter Server 5.x にアップグレードした場合、それらは削除され、有効ではなくなります。

vSphere Web Client での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、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 Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [仮想マシンのオーバーライド] を選択し、[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]、[ホスト隔離時の対応]、[仮想マシンの監視]、または [仮想マシンの監視感度] の設定を変更できます。

注意 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。

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。

vSphere HA 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 プラクティスに従う必要があります。このトピックでは特に、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。

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動作を行うときは、その変化に関する通知を受けられます。このような動作が行われたときに起動されるアラームを vCenter Server で構成し、指定された管理者グループにメールなどでアラートを送信させることができます。

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 リソース不足 (クラスタのアラーム)
- マスターが見つかりません (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)
- VM 監視エラー (仮想マシンのアラーム)
- VM 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)

注意 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。

クラスタの妥当性の監視

有効なクラスタとは、アドミSSION コントロール ポリシーに違反していないクラスタです。

vSphere HA が有効に設定されているクラスタが無効になるのは、パワーオンされた仮想マシンの数がフェイルオーバー要件を超えた場合、つまり、現在のフェイルオーバー キャパシティが、構成されたフェイルオーバー キャパシティよりも小さい場合です。アドミッション コントロールが無効な場合は、クラスタが無効になることはありません。

vSphere Web Client で、クラスタの [監視] タブから [vSphere HA] を選択し、[構成の問題] を選択します。vSphere HA の現在の問題が一覧で表示されます。

vSphere HA の問題でクラスタが赤になっても、DRS の動作に影響はありません。

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 ホストと ESX/ESXi 4.1 以前のホストが存在するクラスタ、および Storage vMotion が広範に使用されるかストレージ DRS が有効になっているクラスタの場合、vSphere HA をデプロイしないでください。vSphere HA がホストの障害に応答し、障害が発生する前に仮想マシンが実行されていたときと ESXi バージョンが異なるホストで仮想マシンを再起動する可能性があります。障害発生時に、仮想マシンが ESXi 5.x ホスト上での Storage vMotion アクションに関連していて、vSphere HA が ESXi 5.0 より前のバージョンのホストで仮想マシンを再起動した場合、問題が生じることがあります。仮想マシンはパワーオンする可能性があります。続くスナップショット処理で試みられる操作が vdisk 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。

アドミッション コントロールのベスト プラクティス

次に推奨するのは、vSphere HA アドミッション コントロールのベスト プラクティスです。

- 予約されたクラスタ リソースの割合アドミッション コントロール ポリシーを選択します。このポリシーは、ホストと仮想マシンのサイズについて最も柔軟です。このポリシーを構成する場合、サポートするホスト障害の回数を反映した CPU とメモリの割合を選択してください。たとえば、vSphere HA で 2 つのホスト障害に対してリソースを取ってにおいて、クラスタ内に同等のキャパシティのホストが 10 個ある場合には、20% (2/10) と指定します。
- 確実にすべてのクラスタ ホストが同じサイズになるように調節します。クラスタで許容するホスト障害ポリシーについては、クラスタのサイズが異なっていると、vSphere HA で最大のホストのためにキャパシティが予約されるため、障害を処理するために予約されているキャパシティを超過する原因になります。クラスタ リソースの割合ポリシーについては、クラスタのサイズが異なっていると、予期されるホスト障害の回数に対して十分なキャパシティを予約するために、クラスタのサイズが同じ場合よりも多くの割合を指定する必要があります。
- クラスタで許容するホスト障害ポリシーの使用を検討している場合、仮想マシンのサイズ要件が、構成された仮想マシン全体にわたってできるだけ同じになるようにしてください。このポリシーは、スロット サイズを使用して各仮想マシン用に予約する必要があるキャパシティを計算します。スロット サイズは、仮想マシンに必要な最大予約メモリと CPU に基づいています。CPU とメモリ要件の異なる仮想マシンが混在する場合、スロット サイズ計算のデフォルトは可能な最大値になり、統合の制約になります。
- フェイルオーバー ホストの指定ポリシーの使用を検討している場合、何個のホスト障害をサポートするかを決めて、ホストのこの数値をフェイルオーバー ホストとして指定します。クラスタのサイズが異なっている場合、指定されたフェイルオーバー ホストは少なくともクラスタ内の非フェイルオーバー ホストと同じサイズである必要があります。これにより、障害が発生した場合でも十分なキャパシティが確保されます。

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、ブート時にそのようなホスト上の vSphere HA エージェントをインストールするように構成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。

Virtual SAN を使用したクラスタ内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 以上にアップグレードし、さらに Virtual SAN も使用したい場合は、次のプロセスに従います。

- 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 Virtual SAN を有効にします。
- 4 vSphere HA を再度有効にします。

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 ホストが存在するネットワークに変更を加えるときは、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は、クラスタ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。

注意 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 の管理者に知らせます。

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調べるには、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。
- クラスタの ESXi ホストでは、vSphere HA の通信がデフォルトで VMkernel ネットワークを通過します。ただし、vMotion で使用することが指定されている場合を除きます。VMkernel ネットワークが 1 つのみの場合、vSphere HA は必要に応じてそのネットワークを vMotion と共有します。ESXi 4.x および ESXi では、[管理トラフィック] チェック ボックスを明示的にオンにして、vSphere HA がこのネットワークを使用できるようにする必要があります。

注意 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構成します。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 も 1 つ以上存在する場合、指定されたサブネットに関連付けられている pNIC 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ためには、`das.isolationaddress[...]` 詳細属性を使用する必要があります。[\[vSphere HA の詳細属性 \(P. 31\)\]](#) 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、NIC チーミングによって NIC レベル、または管理ネットワーク レベルで実装できます。ほとんどの実装では、NIC のチーミングで十分な冗長性が提供されますが、必要に応じて、管理ネットワークの冗長性を使用したり追加したりできます。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。

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。

NIC チーミングを使用したネットワーク冗長性

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。

2番目のネットワークを使用したネットワーク冗長性

NIC チーミングの代わりに、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して、ハートビートの冗長性を確保できます。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。

仮想マシンのフォールトトレランスの準備

仮想マシンの vSphere フォールトトレランスを有効にすると、vSphere HA を使用した場合よりも、高いレベルの可用性によるビジネス継続性、およびデータ保護を実現できます。

フォールトトレランスは、(VMware の vLockstep テクノロジーを使用して) ESXi ホスト プラットフォーム上に構築され、別のホスト上の仮想ロックステップで同一の仮想マシンを実行することによって、継続した可用性を提供します。

フォールトトレランスで最適化の結果を得るには、フォールトトレランス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フォールトトレランスをどのように有効にするか、および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。

注意 フォールトトレランスを使用しようとするときにエラーが表示されることがあります。フォールトトレランス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>

この章では次のトピックについて説明します。

- [フォールトトレランスの機能 \(P. 38\)](#)
- [フォールトトレランスと DRS の併用 \(P. 39\)](#)
- [フォールトトレランスの使用事例 \(P. 39\)](#)
- [Fault Tolerance のチェックリスト \(P. 40\)](#)
- [Fault Tolerance の相互運用性 \(P. 41\)](#)
- [Fault Tolerance に向けたクラスタとホストの準備 \(P. 43\)](#)
- [仮想マシンのフォールトトレランスの準備 \(P. 45\)](#)
- [vSphere Web Client でのフォールトトレランス機能を持つ仮想マシンの情報の表示 \(P. 49\)](#)
- [Fault Tolerance のベストプラクティス \(P. 50\)](#)
- [推奨される vSphere Fault Tolerance の構成 \(P. 52\)](#)

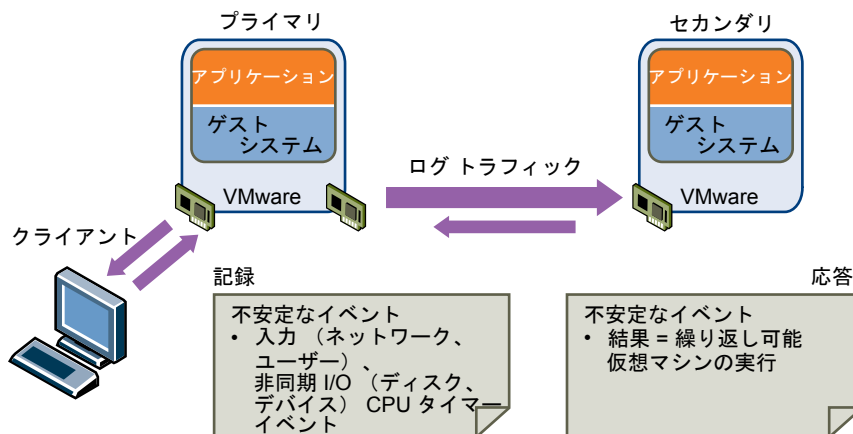
フォールトトレランスの機能

vSphere フォールトトレランスは、フェイルオーバーが発生したときに、プライマリ仮想マシンと同じセカンダリ仮想マシンを作成および保持し、継続してプライマリ仮想マシンの代わりに使用できるようにして、仮想マシンに対して継続的な可用性を実現します。

ミッションクリティカルなほとんどの仮想マシンに対して、フォールトトレランスを有効にすることができます。セカンダリ仮想マシンと呼ばれる複製仮想マシンが作成され、仮想ロックステップ方式でプライマリ仮想マシンとともに動作します。VMware vLockstep は、プライマリ仮想マシンで発生する入力とイベントを取得し、それを別のホストで稼働しているセカンダリ仮想マシンに送信します。この情報を使用することで、セカンダリ仮想マシンはプライマリ仮想マシンと同一の動作を行います。セカンダリ仮想マシンは仮想ロックステップ方式でプライマリ仮想マシンとともに動作するため、中断することなくいつでも実行を引き継ぐことができます。その結果、フォールトトレランスの保護を実現できます。

注意 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。

図 3-1. フォールトトレランス ペアのプライマリ仮想マシンとセカンダリ仮想マシン



プライマリ仮想マシンおよびセカンダリ仮想マシンは、常にハートビートを交換します。この交換により、仮想マシンのペアが互いのステータスを監視し、フォールトトレランスが継続して維持されます。プライマリ仮想マシンが稼働しているホストで障害が発生すると、透過的なフェイルオーバーが行われ、プライマリ仮想マシンの代わりにセカンダリ仮想マシンがすぐにアクティブになります。数秒間で新しいセカンダリ仮想マシンが起動し、フォールトトレランスの冗長性が再確立されます。セカンダリ仮想マシンが稼働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。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。

フォールトトレランスでは、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、「スプリットプレーン」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働を続け、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。

注意 プライマリ仮想マシンがパワーオンされるときに、非アフィニティチェックが行われます。プライマリ仮想マシンとセカンダリ仮想マシンが両方ともパワーオフの状態であれば、これらの2台の仮想マシンを同じホスト上に配置することが可能です。これは通常の動作であり、プライマリ仮想マシンがパワーオンされると同時に、セカンダリ仮想マシンは別のホスト上で起動されます。

フォールトトレランスとDRSの併用

EVC (Enhanced vMotion Compatibility) 機能を有効にすると、vSphere フォールトトレランスを vSphere DRS (Distributed Resource Scheduler) と併用できます。この処理により、フォールトトレランス対応の仮想マシンで、効率的な初期配置の利点を活かすことが可能になり、これらの仮想マシンをクラスタのロードバランシングの計算に含めることもできます。

クラスタで EVC が有効になっていると、DRS はフォールトトレランス対応の仮想マシンの初期配置を推奨し、クラスタのロードバランシングの際にそれらの仮想マシンを移動します。また、DRS の自動化レベルをプライマリ仮想マシンに割り当てることができます (セカンダリ仮想マシンは、対応するプライマリ仮想マシンの設定と常に同じであることを前提とします)。

DRS が初期配置またはロードバランシングの際にホストに配置するプライマリ仮想マシンまたはセカンダリ仮想マシンの数が、一定数を超えることはありません。この制限は、詳細オプション `das.maxftvmsperhost` で管理されます。このオプションのデフォルト値は4です。ただし、このオプションを0に設定すると、DRSはこの制限を無視します。

EVC が無効になっているクラスタ内の仮想マシンで vSphere フォールトトレランスを使用すると、フォールトトレランス対応の仮想マシンの DRS 自動化レベルが「無効」に設定されます。このようなクラスタでは、各プライマリ仮想マシンは登録されているホストでのみパワーオンされ、それぞれのセカンダリ仮想マシンが自動的に配置されますが、いずれのフォールトトレランス対応の仮想マシンもロードバランシングのために移動されません。

フォールトトレランス対応の仮想マシンのペアでアフィニティルールを使用する場合、仮想マシン間のアフィニティルールはプライマリ仮想マシンにのみ適用されますが、仮想マシンとホスト間のアフィニティルールは、プライマリ仮想マシンとそのセカンダリ仮想マシンの両方に適用されます。プライマリ仮想マシンに仮想マシン間のアフィニティルールが設定される場合、DRS は、フェイルオーバー後 (つまり、プライマリ仮想マシンが新規ホストに移行した後) に発生した違反を修正しようとします。

フォールトトレランスの使用事例

いくつかの典型的な状況で、vSphere フォールトトレランスを使用してメリットを得ることができます。

フォールトトレランスは、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働し、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 によるフェイルオーバーでは、障害による影響を受けた仮想マシンが再起動されるという違いがあります。

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、フォールトトレランスをデプロイするタイミングのシナリオが通知されます。

- アプリケーションを常に利用できるようにしておく必要がある場合 (特に、ユーザーがハードウェアの障害中も維持しておきたい、長期にわたるクライアント接続があるアプリケーション)。
- 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。

オンデマンドのフォールトトレランス

フォールトトレランス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、オンデマンドのフォールトトレランス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、ミッションクリティカルな可用性が妨げられる可能性があります。vSphere フォールトトレランスを使用すると、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あとでフォールトトレランスをオフまたは無効にすることができます。オンデマンドのフォールトトレランスを使用すると、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 を使用する前に認識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。また、vSphere FT に使用するクラスタ、ホスト、仮想マシンに関連する構成上の問題について理解を深めるために、VMware SiteSurvey ユーティリティ (http://www.vmware.com/download/shared_utilities.html からダウンロード可能) も使用できます。

注意 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 クラスタの設定には vCenter Server を使用する必要があります。

Fault Tolerance でのクラスタ要件

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。

- 同一の Fault Tolerance のバージョンまたはホストビルド番号を実行する、少なくとも 2 つの FT 認定ホスト。Fault Tolerance のバージョン番号は、vSphere Web Client のホストの [サマリ] タブに表示されます。

注意 ESX/ESXi 4.1 より前のレガシーホストに対しては、このタブには代わりにホストビルド番号が表示されます。パッチを適用すると、ホストのビルド番号に ESX と ESXi のインストール間で違いが出る場合があります。レガシーホストを確実に FT 互換にするには、FT ペアにレガシー ESX ホストと ESXi ホストを混在させないようにします。

- ESXi ホストから、同じ仮想マシンのデータストアおよびネットワークにアクセスできます。[[Fault Tolerance のベストプラクティス \(P. 50\)](#)] を参照してください。
- Fault Tolerance のログおよび vMotion ネットワークが構成されている。[[vSphere Web Client でのホストマシンのネットワークの構成 \(P. 43\)](#)] を参照してください。
- vSphere HA クラスタが作成され、有効です。[[vSphere HA クラスタの作成 \(P. 26\)](#)] 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 が有効になっている必要があります。

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。

- ホストは、FT 対応のプロセッサグループのプロセッサを装備している。また、ホストのプロセッサには相互互換性があることを推奨します。サポートされるプロセッサの詳細については、当社のナレッジベースの記事 (<http://kb.vmware.com/kb/1008027>) を参照してください。
- 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。

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、[\[vSphere Web Clientでのクラスタの作成とコンプライアンスの確認 \(P.45\)\]](#)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することもできます。

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 \(P.41\)\]](#)を参照してください。
- 仮想マシンが、仮想 RDM またはシック プロビジョニングされた仮想マシン ディスク (VMDK) ファイルに格納されている必要があります。仮想マシンが、シン プロビジョニングされた VMDK ファイルに格納されていて、Fault Tolerance を有効化しようとする、VMDK ファイルを変換する必要があるというメッセージが表示されます。変換を行うには、仮想マシンをパワーオフする必要があります。
- vSphere Fault Tolerance は 2TB を超える VMDK ではサポートされていません。
- 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 \(P.41\)\]](#)を参照してください。
- 仮想マシンファイルが共有ストレージに格納されている。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、NFS、および NAS があります。
- vCPU が 1 つの仮想マシンのみ、Fault Tolerance を使用できます。
- 仮想マシンがサポートされているゲスト OS のいずれかで実行されている。詳細については、当社のナレッジベースの記事 (<http://kb.vmware.com/kb/1008027>) を参照してください。

Fault Tolerance の相互運用性

vSphere Fault Tolerance を構成する前に、フォールトトレランス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

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。

- 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。
- 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、フォールトトレランス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は、Fault Tolerance を有効にできません。また、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することもできません。
- 仮想マシンのバックアップ。フォールトトレランスが有効になっている仮想マシンは、Storage API for Data Protection、vSphere Data Protection、または仮想マシンのスナップショットを使用する必要がある類似のバックアップ製品を使用して、ESXi で実行されるようにバックアップすることはできません。フォールトトレランス対応の仮想マシンをこの方法でバックアップするには、まずフォールトトレランスを無効にし、バックアップの実行後に再度有効にする必要があります。ストレージのアレイベースのスナップショットは、フォールトトレランスには影響しません。
- Virtual SAN。

Fault Tolerance と互換性のない機能とデバイス

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
対称型マルチプロセッサ (SMP) の仮想マシン。vCPU が 1 つの仮想マシンのみ、Fault Tolerance を使用できます。	仮想マシンを、1 つの vCPU として再構成してください。多数のワークロードが 1 つの vCPU として構成され、すぐれたパフォーマンスが保持されます。
物理的な Raw ディスク マッピング (RDM)。	物理 RDM でバックアップ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します。
物理デバイスまたはリモート デバイスでバックアップされた 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 でバックアップを再構成します。
準仮想化ゲスト。	準仮想化が必要ない場合は、VMI ROM を使用しないように仮想マシンを再構成します。
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。
vlance ネットワーク ドライバ。	Fault Tolerance では、vlance 仮想 NIC カードで構成されている仮想マシンはサポートされません。ただし、vmxnet2、vmxnet3、および e1000 は完全にサポートされています。
クラスタリング機能が有効になっていない、シン プロビジョニングされているストレージまたはシック プロビジョニングされているディスクでバックアップされた仮想ディスク。	Fault Tolerance をオンにすると、適切なディスク フォーマットへの変換がデフォルトで実行されます。この変換を動作させるには、仮想マシンをパワーオフする必要があります。
ホット プラグング デバイス。	<p>フォールトトレランス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、フォールトトレランスをオンにします。</p> <p>注意 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 (アンプラグング)」から再度「取り付ける (プラグング)」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、フォールトトレランスを最初にオフにする必要があります。</p>
EPT/RVI (Extended Page Tables/Rapid Virtualization Indexing)。	Fault Tolerance がオンになっている仮想マシンに対して、EPT/RVI は自動的に無効になります。
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。
IPv6	FT ログ記録 NIC では IPv4 アドレスを使用します。
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 EFI ファームウェア	ゲスト OS をインストールする前に、仮想マシンが BIOS ファームウェアを使用するように構成されていることを確認してください。

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 を有効にする前に、次のタスクを完了しておく必要があります。

- 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。[\[vSphere Web Client での仮想マシンの Fault Tolerance の有効化 \(P. 47\)\]](#) を参照してください。

vSphere Web Client でのホスト 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 スイッチを構成して、ホストが vSphere Fault Tolerance も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 を有効にするには、この手順を 2 回（ポート グループ オプションごとに 1 回ずつ）実行し、フォールトトレランスのログ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。

開始する前に

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 つの物理ギガビット NIC が必要です。たとえば、Fault Tolerance のログ用に 1 つと、vMotion 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。

注意 vMotion と FT ログ記録 NIC は異なるサブネットに配置する必要があります。IPv6 は FT ログ記録 NIC ではサポートされません。

手順

- 1 vSphere Web Client で、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[ネットワーク] をクリックします。
- 3 [アクション]-[すべての vCenter アクション]-[ネットワークの追加] をクリックします。
- 4 接続タイプの選択ページで [VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。
- 5 [新しい標準スイッチ] を選択して [次へ] をクリックします。
- 6 空いている物理ネットワーク アダプタをスイッチに割り当て、[次へ] をクリックします。
- 7 ネットワーク ラベルを入力し、目的のサービスを有効化して [次へ] をクリックします。
- 8 IP アドレスとサブネット マスクを指定し、設定内容を確認してから [完了] をクリックします。

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。

次に進む前に

注意 FT をサポートするようネットワークを構成したあとに Fault Tolerance のログ用ポートを無効にした場合、すでにパワーオンされているフォールトトレランス対応の仮想マシンのペアはパワーオンのままになります。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。

フォールトトレランスのホストのネットワーク構成の例

この例では、4つの1GB NICを使用する標準的な導入環境でフォールトトレランスを有効にするホストネットワーク構成について説明します。ここに挙げる導入環境の一例は、例の中で示す各トラフィックタイプに対して適切なサービスを提供できるようにしたもので、構成のベストプラクティスといえます。

フォールトトレランス機能は、停電、システムパニック、または類似の原因で物理ホストに障害が発生する過程で、継続的なアップタイムを提供します。セカンダリ仮想マシンへのフォールトトレランスのフェイルオーバーは、ネットワークまたはストレージのパス障害や、ホストの実行状態に影響を与えないその他の物理サーバコンポーネントによっては開始されません。したがって、仮想マシンからネットワークやストレージアレイなどのインフラストラクチャコンポーネントへの接続を失う可能性を減らすために、適切な冗長性（たとえば、NICチーミング）を使用することを強くお勧めします。

NICチーミングポリシーは、vSwitch (vSS) ポートグループ（またはvDSの分散仮想ポートグループ）で構成され、物理NIC (vmnics) を経由する、仮想マシンおよびvmkernelポートからのトラフィックをvSwitchで処理および配布する方法を管理します。一般的に、各トラフィックタイプに固有のポートグループが使用され、それぞれのトラフィックタイプは異なるVLANに割り当てられます。

ホストネットワークの構成ガイドライン

次のガイドラインに従って、トラフィックタイプ（たとえばNFS）と多数の物理NICの異なる組み合わせで、フォールトトレランスをサポートするようにホストのネットワークを構成できます。

- 各NICチームを2つの物理スイッチ経由で配布して、2つ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。
- 確定的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（アクティブまたはスタンバイ）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。
- アクティブまたはスタンバイのポリシーを使用する場合は、両方のトラフィックタイプでvmnicを共有するフェイルオーバー時の影響を最小限にするようなトラフィックタイプを組み合わせる。
- アクティブまたはスタンバイの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。

4つの1GB NICを使用する構成例

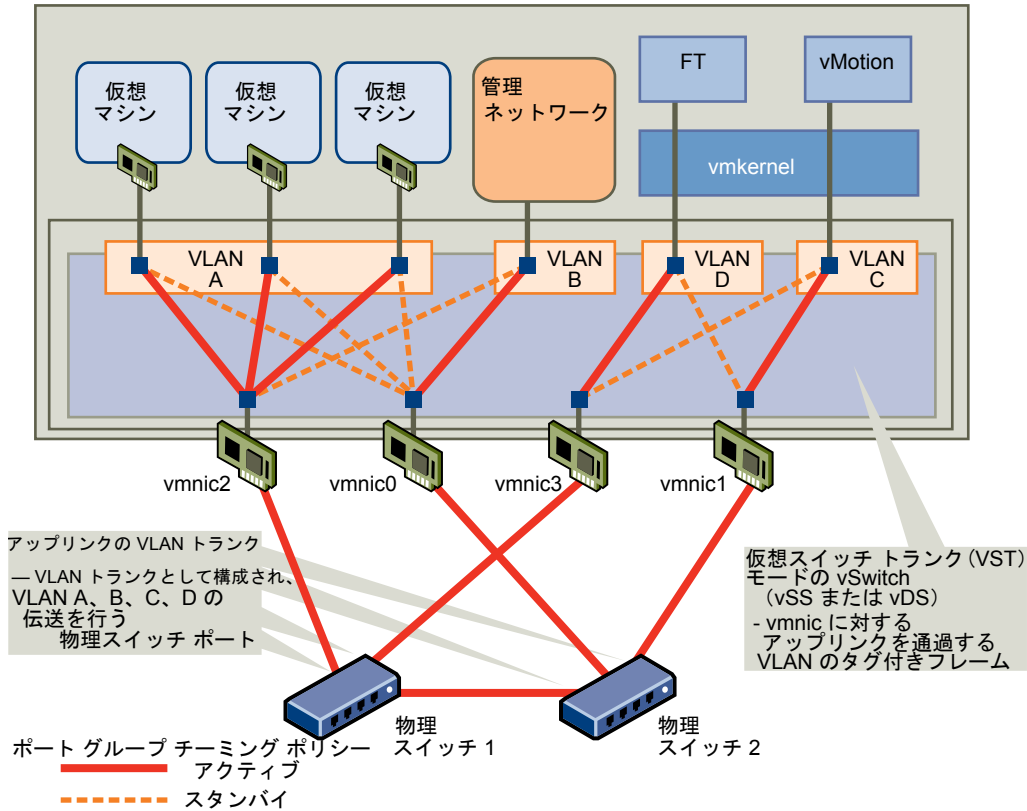
図3-2は、4つの1GB NICによってフォールトトレランスをサポートする、ESXiホストが1台のネットワーク構成を示しています。FTクラスタ内のほかのホストも同様に構成されます。

この例で使用する4つのポートグループは、次のように構成されます。

- VLAN A：仮想マシンネットワークポートグループ。vmnic2はアクティブ（物理スイッチ#1に接続）、vmnic0はスタンバイ（物理スイッチ#2に接続）。
- VLAN B：管理ネットワークポートグループ。vmnic0はアクティブ（物理スイッチ#2に接続）、vmnic2はスタンバイ（物理スイッチ#1に接続）。
- VLAN C：vMotionポートグループ。vmnic1はアクティブ（物理スイッチ#2に接続）、vmnic3はスタンバイ（物理スイッチ#1に接続）。
- VLAN D：FTログ用ポートグループ。vmnic3はアクティブ（物理スイッチ#1に接続）、vmnic1はスタンバイ（物理スイッチ#2に接続）。

vMotionとFTログ記録は、同じVLANを共有できますが（同じVLAN番号を両方のポートグループで構成）、異なるIPサブネットに配置されたそれぞれに固有のIPアドレスが必要です。ただし、QoS（Quality of Service）の制限が、VLANベースのQoSを使用した物理ネットワークで有効になっている場合は、別々のVLANを使用します。QoSは、たとえば、複数の物理スイッチのホップが使用される場合や、フェイルオーバーが発生して複数のトラフィックタイプがネットワークリソースを取り合う場合のように、競合するトラフィックが発生する場合に特に役立ちます。

図 3-2. フォールトトレランスのネットワーク構成の例



vSphere Web Client でのクラスタの作成とコンプライアンスの確認

vSphere Fault Tolerance は、vSphere HA クラスタ コンテキストで使用されます。各ホスト上でネットワークを構成したあと、vSphere HA クラスタを作成し、そこにホストを追加します。クラスタが正しく構成されているか、およびクラスタが Fault Tolerance の有効化のための要件に準拠しているかどうかを確認できます。

手順

- 1 vSphere Web Client で、クラスタに移動して参照します。
- 2 [監視] タブをクリックし、[プロファイルのコンプライアンス] をクリックします。
- 3 [コンプライアンスを今すぐ確認] をクリックしてコンプライアンス テストを実行します。

コンプライアンス テストの結果が表示され、各ホストのコンプライアンスまたはコンプライアンス違反が表示されます。

仮想マシンのフォールトトレランスの準備

クラスタ用の vSphere フォールトトレランスを有効にするために必要なすべての手順を行なったあと、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。

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。

フォールトトレランス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。

フォールトトレランスをオンにするときの検証

仮想マシンのフォールトトレランス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 ESX/ESXi 4.0 以降がインストールされている。
- 仮想マシンの vCPU が 1 つだけである。
- 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。

- フォールトトレランス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フォールトトレランスに対応している。
- セカンダリ仮想マシンをサポートするホストのプロセッサがフォールトトレランスに対応し、またプライマリ仮想マシンをサポートするホストと同じ CPU ファミリまたはモデルである。
- 使用するハードウェアに、フォールトトレランス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。
- 仮想マシンのゲスト OS とプロセッサとの組み合わせが、フォールトトレランスでサポートされている。たとえば、AMD ベースのプロセッサで動作する 32 ビット版の Solaris は現在サポートしていません。サポート対象のプロセッサとゲスト OS の組み合わせの詳細は、当社のナレッジベースの記事 (<http://kb.vmware.com/kb/1008027>) を参照してください。
- 仮想マシンの構成で、フォールトトレランス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。

仮想マシンのフォールトトレランス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、フォールトトレランス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フォールトトレランスのステータスは、[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（パワーオンされるときに、より適切なホストに再登録されることがあります）。
- 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。
- 仮想マシンの表示されるフォールトトレランスのステータスは、[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。

- フォールトトレランス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、上記の追加検証が実行されます。仮想マシンが適切にパワーオンされるようにするために、仮想マシンが準仮想化（VMI）を使用していないことを確認してください。

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。仮想マシンのフォールトトレランスのステータスには、[保護済み]というタグが付けられます。

vSphere Web Client での仮想マシンの Fault Tolerance の有効化

vSphere Web 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、シェアを変更できません。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。

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

手順

- 1 vSphere Web 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、[すべての vCenter アクション]-[フォールトトレランス]-[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。

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。

vSphere Web Client での Fault Tolerance 機能を持つ仮想マシンの設定オプション

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フォールトトレランスセクションに新しいオプションが追加されます。

vSphere Web Client のオプションには、Fault Tolerance のオフ設定または無効化、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。

vSphere Web Client での Fault Tolerance の無効化

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。この機能を今後使用する場合は、[Fault Tolerance の無効化]オプションを使用します。

注意 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 を無効にして有効にする必要があります。

手順

- 1 vSphere Web 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、[すべての vCenter アクション]-[フォールトトレランス]-[フォールトトレランスをオフ]を選択します。
- 3 [はい]をクリックします。

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。

vSphere Web Client でのセカンダリ仮想マシンの移行

プライマリ仮想マシンの vSphere フォールト トレランスをオンにしたあと、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 Web 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、[すべての vCenter アクション]-[フォールト トレランス]-[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。

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。

vSphere Web Client での Fault Tolerance の無効化

仮想マシンの vSphere Fault Tolerance の無効化と、フォールト トレランス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保存されます。Fault Tolerance の保護機能を今後有効にする場合は、このオプションを使用します。

手順

- 1 vSphere Web Client で、Fault Tolerance の無効化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、[すべての vCenter アクション]-[フォールト トレランス]-[フォールト トレランスの無効化] を選択します。
- 3 [はい] をクリックします。

選択した仮想マシンで Fault Tolerance が無効になります。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、今後再度有効になった場合に使用されます。

次に進む前に

Fault Tolerance の無効化と、メニュー オプションは [Fault Tolerance の有効化] になります。再度有効にする場合は、このオプションを選択します。

vSphere Web Client での Fault Tolerance 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 Web 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、[すべての vCenter アクション]-[フォールト トレランス]-[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。

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。

vSphere Web Client でのセカンダリ仮想マシンの再起動テスト

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 Web 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、[すべての vCenter アクション] - [フォールトトレランス] - [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。

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。

vSphere Web Client でのフォールトトレランス機能を持つ仮想マシンの情報の表示

vSphere Web Client を使用して、フォールトトレランス機能を持つ仮想マシンを vCenter Server インベントリに表示できます。

注意 セカンダリ仮想マシンから Fault Tolerance の無効化ことはできません。

vSphere Fault Tolerance セクション（ペイン）がプライマリ仮想マシンの [サマリ] タブに表示され、仮想マシンに関する次の情報が表示されます。

Fault Tolerance のステータス

仮想マシンの Fault Tolerance のステータスを示します。

- 保護済み：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、正常に実行されています。
- 保護されていません：セカンダリ仮想マシンが実行されていません。考えられる原因を次の表に示します。

表 3-2. プライマリ仮想マシンのステータスが「保護されていません」と表示される原因

「保護されていません」ステータスの原因	説明
起動	Fault Tolerance によってセカンダリ仮想マシンの起動処理を実行中です。このメッセージが表示されるのは短時間だけです。
セカンダリ仮想マシンが必要です	プライマリ仮想マシンがセカンダリ仮想マシンなしで実行されているため、現在保護されていません。これは、セカンダリ仮想マシンを実行するための互換ホストがクラスタ内にない場合に発生します。この問題を解決するには、互換ホストをオンラインにします。オンライン状態の互換ホストがクラスタ内にある場合は、さらに調査が必要な可能性があります。特定の状況下では、Fault Tolerance をいったん無効にして再度有効にすると、問題が解決することがあります。

表 3-2. プライマリ仮想マシンのステータスが「保護されていません」と表示される原因 (続き)

「保護されていません」ステータスの原因	説明
無効	Fault Tolerance は現在無効になっています (セカンダリ仮想マシンは実行されていません)。ユーザーが Fault Tolerance の無効化か、セカンダリ仮想マシンをパワーオンできないため vCenter Server によって Fault Tolerance の無効化と、このような状況になります。
VM は実行されていません	Fault Tolerance は有効になっていますが、仮想マシンがパワーオフされています。仮想マシンをパワーオンして、「保護済み」の状態にします。

セカンダリの場所	セカンダリ仮想マシンのホスト先の ESXi ホストを示します。
セカンダリ CPU の合計	セカンダリ仮想マシンの CPU 使用率 (MHz 単位)。
セカンダリ メモリの合計	セカンダリ仮想マシンのメモリ使用量 (MB 単位)。
vLockstep 間隔	セカンダリ仮想マシンがプライマリ仮想マシンの現在の実行状態と同じになるために必要な時間間隔 (秒単位) です。この間隔は通常は 0.5 秒未満です。vLockstep 間隔の値にかかわらず、フェイルオーバー中に状態が失われることはありません。
ログ バンド幅	プライマリ仮想マシンを実行しているホストからセカンダリ仮想マシンを実行しているホストに、vSphere Fault Tolerance のログ情報を送信するために使用されているネットワークの容量です。

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。

次の情報のほか、『VMware Fault Tolerance Recommendations and Considerations』ホワイトペーパー (<http://www.vmware.com/resources/techresources/10040>) も参照してください。

ホスト構成

ホストを構成する場合には、次のベスト プラクティスを考慮してください。

- 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されることがあります。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の電力管理機能 (電力を節約するための電源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は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されている場合は、フォールトトレランス対応の仮想マシンを実行するホストですべての電力管理モードを無効にするか、すべてのホストが同じ電力管理モードで動作するようにします。
- すべてのホストに対して、同じ命令セットの拡張構成 (有効または無効) を適用します。命令セットを有効または無効にするプロセスは、BIOS によって異なります。命令セットの構成方法については、ホストの BIOS のドキュメントを参照してください。

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。

- 同じ互換プロセッサ グループのプロセッサ。
- 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。
- 同じバージョンの ESXi。
- 同じ Fault Tolerance バージョン番号（または ESX/ESXi 4.1 以前のホストではホストのビルド番号）。
- すべてのホストで同じ BIOS 設定（電力管理とハイパースレッド）。

[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。

共有ストレージ上での ISO 格納による継続アクセス

Fault Tolerance が有効になっている仮想マシンによってアクセスされる ISO は、フォー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。この構成を使用する場合は、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。

Fault Tolerance が有効になっている仮想マシンでは、プライマリ仮想マシンへのみアクセス可能な ISO イメージを使用することもできます。このような場合、プライマリ仮想マシンは ISO にアクセスできますが、フェイルオーバーが生じると、CD-ROM はメディアがないことを示すエラーを報告します。インストールなどの一時的で重要性が低い操作に CD-ROM を使用する場合は、このような状況になっても問題ないことがあります。

ネットワークパーティションの回避

ネットワークパーティションが発生するのは、vSphere HA クラスター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 \(P. 15\)\]](#) を参照してください。パーティションが発生すると、Fault Tolerance の保護が低下する場合があります。

Fault Tolerance を使用する vSphere HA クラスターがパーティションされると、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）が、仮想マシンに対して責任のないマスターホストによって管理されるパーティションに入る恐れがあります。フェイルオーバーが必要なとき、セカンダリ仮想マシンが再起動するのは、仮想マシンに対して責任のあるマスター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ある場合のみです。

管理ネットワークにネットワークパーティションを生じるような障害ができるだけ発生しないようにするには、[\[ネットワークのベストプラクティス \(P. 35\)\]](#) の推奨に従ってください。

vSphere Web Client での Fault Tolerance エラーの表示

Fault Tolerance の実装に関連したタスクでエラーが発生した場合は、[最近のタスク] ペインでエラー情報を確認できます。

[最近のタスク] ペインの [失敗] タブに、各エラーのサマリが一覧表示されます。失敗したタスクの詳細については、[他のタスク] をクリックして [タスク コンソール] を開いてください。

[タスク コンソール] には、名前、ターゲット、ステータスなどの情報がタスクごとに表示されます。タスクが失敗した場合は、生成された障害のタイプが [ステータス] 列に示されます。タスクを選択すると、詳細がタスクリストの下にあるペインに表示されます。

Fault Tolerance で使用するホストのアップグレード

フォールトトレランス対応の仮想マシンを持つホストをアップグレードする際は、FT バージョン番号、または ESX/ESXi 4.1 以前のホストではホストのビルド番号が同じホスト上で、プライマリ仮想マシンとセカンダリ仮想マシンが必ず動作し続けるようにします。

開始する前に

クラスター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。

注意 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 を無効にします。
- 4 vMotion を使用して、アップグレードしたホストの一方に、無効化したプライマリ仮想マシンを移動します。
- 5 移動したプライマリ仮想マシンに対して Fault Tolerance を有効にします。
- 6 アップグレード後のホストに格納可能な Fault Tolerance 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。

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。

推奨される vSphere Fault Tolerance の構成

Fault Tolerance を構成するときは、特定のガイドラインに従ってください。

- フォールトトレランス非対応の仮想マシン以外に、1 台のホストに収容するフォールトトレランス対応の仮想マシン（プライマリまたはセカンダリ）は 4 台以下にしてください。各ホストで安全に稼働できるフォールトトレランス対応の仮想マシンの台数は、ESXi ホストおよび仮想マシンのサイズおよびワークロードに基づいており、それらは異なることがあります。
- 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。
- フォールトトレランス対応の仮想マシンを含むリソース プールでは、仮想マシンのメモリよりも多くのメモリを持つようにします。Fault Tolerance がオンになると、フォールトトレランス対応の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。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。
- フォールトトレランス対応の仮想マシンごとに、最大 16 個の仮想ディスクを使用します。
- 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。

インデックス

A

Auto Deploy 33

D

das.heartbeatdsperhost 16, 31
das.ignoreinsufficienthbdatastore 31
das.iostatsinterval 14, 31
das.isolationaddress 31, 35
das.isolationshutdowntimeout 13, 31
das.slotcpuinmhz 20, 31
das.slotmeminmb 20, 31
das.usedefaultisolationaddress 31
das.vmcputminmhz 20, 22, 31
das.vmmemoryminmb 31
das.respectvmmantiaffinityrules 31
das.maxftvmsperhost 39
DNS ルックアップ 25
DPM (Distributed Power Management) 18, 19
DRS (Distributed Resource Scheduler)
 vSphere HA との併用 18
 vSphere フォールト トレランスとの併用 39
 Fault Tolerance 41

E

Enhanced vMotion Compatibility 39
EPT (Extended Page Tables) 41
EVC 39

F

fdm.isolationpolicydelaysec 31
FT ログ記録 38

I

I/O 統計間隔 14
IPv4 25, 41
IPv6 25, 41, 43
iSCSI SAN 40
ISO イメージ 50

N

NIC チーミング 36, 44
NPIV (N_Port ID Virtualization) 41

P

PortFast 35

R

RDM 40, 41
RVI (Rapid Virtualization Indexing) 41

S

SSL 証明書 16
Storage vMotion 7, 33, 41

T

TCP ポート 16

U

UDP ポート 16

V

Virtual SAN 16, 17, 33, 41
VLAN 44
VMDK 40
VMFS 16, 35
VMware Tools 14
VMware vLockstep 9, 37, 38
vpxuser ユーザー アカウント 16
vSphere HA
 エラー メッセージ 11
 カスタマイズ 30
 仮想マシンのオプション 28
 仮想マシンの監視 29
 監視 33
 クラスタ設定 26
 クラスタ設定の構成 28
 サスペンド 33
 システム停止からのリカバリ 8
 詳細属性 30
 チェックリスト 25
 メリット 8
vSphere HA クラスタ
 アドミッション コントロール 19
 異種性 25
 計画 11
 作成 26, 45
 スレーブ ホスト 12
 ベスト プラクティス 33
 マスター ホスト 12, 15
vSphere HA アーキテクチャ 11
vSphere HA クラスタの計画 11

- vSphere HA クラスタの作成 26
- vSphere HA データストア ハートビート 30
- vSphere HA ネットワーク
 - バスの冗長性 36
 - ベスト プラクティス 35
- vSphere HA のカスタマイズ 30
- vSphere HA の監視 33
- vSphere HA の詳細オプションの構成 30

あ

- アドミッション コントロール
 - vSphere HA 19
 - 構成 29
 - タイプ 19
 - ポリシー 29
- アドミッション コントロールのポリシー
 - クラスタで許容するホスト障害 20
 - 選択 25
 - フェイルオーバー ホストの指定 24
 - 予約されたクラスタ リソースの割合 22
- アフィニティ ルール 38, 39
- アプリケーションの監視 12, 14

い

- イベントとアラーム、設定 33

え

- エラー、フォールト トレナランス 51
- エラー メッセージ
 - vSphere HA 11
 - フォールト トレナランス 37

お

- オフにする、フォールト トレナランス 47
- オンデマンドのフォールト トレナランス 39

か

- 隔離時の対応、ホスト 28
- 仮想マシン、再起動の優先順位 28
- 仮想マシン間のアフィニティ ルール 24
- 仮想マシンごとの最大リセット回数 14
- 仮想マシン再起動の優先順位の設定 13
- 仮想マシンのオーバーライド 13, 33
- 仮想マシンのオプション、vSphere HA 28
- 仮想マシンの監視 12, 14, 29
- 仮想マシンの起動およびシャットダウン機能 26
- 仮想マシンの保護 12, 15
- 監視感度 14
- 管理ネットワーク 25, 35

き

- 許容するホスト障害 20

く

- クラスタ設定 26
- クラスタ設定の変更 26
- クラスタで許容するホスト障害 20, 33
- クラスタの操作ステータス 33
- クラスタの妥当性 33

け

- 計画外のダウンタイム 8
- 計画的ダウンタイム 7
- 現在のフェイルオーバー キャパシティ 20, 22
- 現在のフェイルオーバー ホスト 24

こ

- 構成済みのフェイルオーバー キャパシティ 20, 22
- コンプライアンスのチェック、フォールト トレナランス 45

し

- 準仮想化 41
- 詳細属性、vSphere HA 30
- 詳細ランタイム情報 20
- 使用事例、フォールト トレナランス 39

す

- ストレージ
 - iSCSI 40
 - NAS 40, 52
 - NFS 40, 52
 - ストレージ DRS 33
 - スナップショット 41
 - スロット 20
 - スロット サイズの計算 20

せ

- セカンダリの移行、フォールト トレナランス 48
- セカンダリの再起動テスト、フォールト トレナランス 49
- 前提条件、フォールト トレナランス 40

そ

- 相互運用性、フォールト トレナランス 41

た

- 対称型マルチプロセッサ (SMP) 41
- 対象読者 5
- ダウンタイム
 - 計画外 8
 - 計画的 7
- ダウンタイムの最小化 7
- 妥当性チェック 45

て

データストア ハートビート 12, 16
デフォルト ゲートウェイ 35

と

透過的フェイルオーバー 9, 38

ね

ネットワーク隔離アドレス 35
ネットワークの構成
 フォールトトレランス 44
 フォールトトレランス 43
ネットワークパーティション 12, 15, 16, 50
ネットワークラベル 35

は

ハードウェア仮想化 (HV) 40, 45
ハートビート 30

ひ

非アフィニティルール 38
ビジネス継続性 7

ふ

ファイアウォールポート 16, 35
フェイルオーバーのテスト、フォールトトレランス 48
フェイルオーバーホスト 24
フェイルオーバーホストの指定 24
フォールトトレランス
 エラーメッセージ 37
 オンにするための制約 45
 概要 38
 継続的な可用性 9
 使用事例 39
 妥当性チェック 45
 ネットワークの構成 44
 非アフィニティルール 38
 ログ 44
フォールトトレランス
 vLockstep 間隔 49
 vSphere の構成 40
 エラー 51
 オプション 47
 オフにする 47
 オンにする 47
 構成の推奨 52
 コンプライアンスのチェック 45
 セカンダリ CPU の合計 49
 セカンダリの移行 48
 セカンダリの再起動テスト 49
 セカンダリの場所 49

セカンダリメモリの合計 49

前提条件 40
相互運用性 41
チェックリスト 40
ネットワークの構成 43
バージョン 40
フェイルオーバーのテスト 48
ベストプラクティス 50
無効化 48
有効化 43
ログ 43
ログバンド幅 49

フォールトトレランス対応の仮想マシンを持つホスト
 のアップグレード 51
Fault Tolerance のステータス
 VM は実行されていません 49
 起動 49
 セカンダリ仮想マシンが必要です 49
 無効 49

へ

ベストプラクティス
 vSphere HA クラスタ 33
 vSphere HA ネットワーク 35
 フォールトトレランス 50

ほ

ポートグループ名 35
ホスト
 ネットワークの隔離 12
 メンテナンスモード 12, 18
ホスト隔離時の対応の設定 13
ホスト監視機能 35
ホストの隔離時の対応 28
ホストの監視、有効化 28

ま

マスターホストの選択 12

む

無効化、フォールトトレランス 48

よ

予約されたクラスタリソースの割合 22, 33

り

リソースの断片化 25

ろ

ロードバランシング 39
ログファイル 16

