# 仮想マシン対応 SAN

## 概要

データセンター（サーバ、ストレージ、およびネットワークを含む）を仮想化することで、統合、スペースの制約、電力消費の増大、冷却要件などに関連する課題のいくつかに対処できます。エンドツーエンドの仮想化により、効率が向上し、全体的な総所有コスト（TCO）が削減されます。仮想マシンでは、複数のアプリケーションとオペレーティング システムを 1 台のマシンで実行できます。ただし、仮想マシンが増えると、SAN には新たな課題が発生します。具体的には、可視性の低下、セキュリティ、アプリケーションごとのトラフィックの切り分け、Quality of Service（QoS）、パフォーマンス モニタリング、管理の複雑性などが挙げられます。

Cisco® MDS 9000 ファミリの VN-Link ストレージ サービスは、Data Center 3.0 構想をサポートします。ファブリックのスケーラビリティとパフォーマンス、パフォーマンス モニタリングと傾向分析、QoS、障害の隔離が可能な仮想 SAN（VSAN）、および仮想マシンのモビリティを実現することで、IT 部門はビジネスの要望の変化に動的に対応できます。

このドキュメントでは、Cisco MDS 9000 ファミリによって導入された革新的アプローチを説明します。このアプローチは、柔軟性が高く、セキュアでスケーラビリティとモビリティを備えた、エンドツーエンドの仮想 SAN 環境をサポートします。

## 仮想化された環境の課題

サーバ仮想化テクノロジーによって、ハイパーバイザを実行する少数の物理サーバに、多数のアプリケーション サーバを統合することが可能です。ハイパーバイザとは、複数のゲスト システム イメージをホスティングできる特殊なオペレーティング システムです。このソリューションを採用すると、各アプリケーション サーバの展開と管理に要する管理手順は大幅に軽減されますが、ネットワーク インフラストラクチャの課題はきわめて重くなります。

ネットワーク インフラストラクチャの課題としては、次のようなものがあります。

- 多対 1 モデルの通信パターンから多対少（メッシュ）モデルへの変化
- 仮想マシンの物理サーバ間におけるダイナミックな移動による、予測不可能なトラフィックの生成
- 複雑な管理手順を伴わず、セキュリティに影響を及ぼさない、仮想マシンの迅速な展開

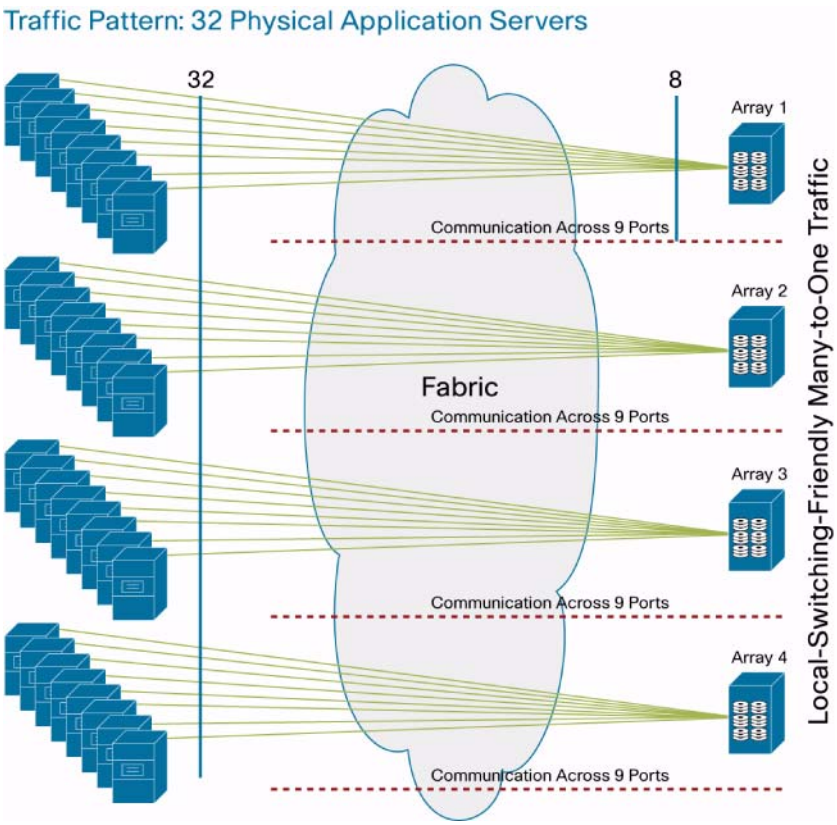
このドキュメントでは、これらの課題について詳細に分析します。

### 複雑な通信パターン

仮想化されたデータセンターの基本的なコンポーネントは、個々のサーバではなく、大量のストレージへのアクセスを共有する可能性があるサーバのクラスタです。最も広く導入されているハイパーバイザでは、32 台のサーバで構成されるクラスタを使用するのが一般的です。

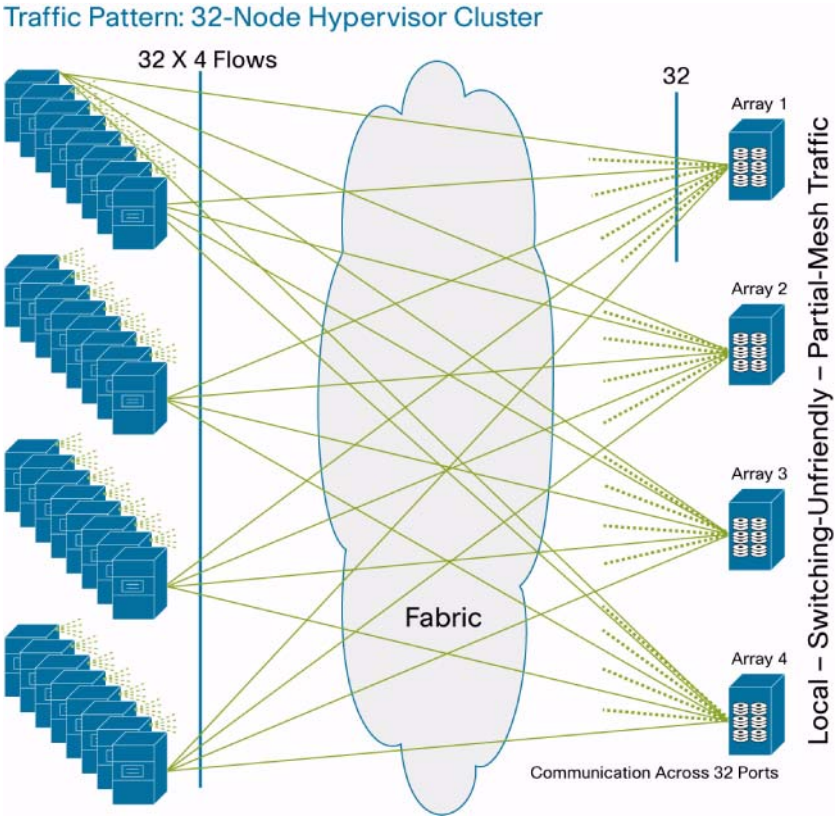
従来の構成では、少数のサーバのグループが 1 つのストレージ ポートにアクセスしますが、ハイパーバイザ クラスタでは、すべてのサーバがすべてのストレージ ポートを共有します。その結果、トラフィック パターンは多対 1 構成（図 1）から、多対少のメッシュ構成（図 2）へと変化しました。図 1 の物理サーバはそれぞれがアプリケーション サーバであるのに対して、図 2 の物理サーバはそれぞれが多数の仮想アプリケーション サーバをホスティングしていることに注目してください。

**図 1**　従来の多対 1 のストレージ アクセス




メッシュ構成に必要なのは、一貫したパフォーマンスで任意のトラフィック パターンを提供できるスイッチング インフラストラクチャです。

**図 2**　メッシュ ストレージ アクセス




仮想化された環境では、それぞれの物理サーバが多数のアプリケーション サーバをホスティングします。ホスティング元の物理サーバによって生成されるストレージ トラフィックの総数は、仮想化された各アプリケーション サーバで実行されるアプリケーション トランザクションの数に依存します。アプリケーション トランザクションの数は、個別の物理サーバから統合仮想環境に渡されるトランザクションの数と同じです。ストレージ トラフィックの総数は基本的に変化しません。

展開するファブリックがシンプルであっても、その設計から多対多の通信と予測不可能なトラフィック バーストが伴う厳しいトラフィック状況がもたらされ、スイッチング インフラストラクチャの機能は限界に達します。

**予測不可能で動的なトラフィック**

物理サーバ間での仮想マシンの透過的なモビリティは、サーバ仮想化ソリューションの魅力の 1 つです。しかし、静的な定義済みのトラフィック関係を基本としてストレージ ネットワークを設計することはできません。

フル装備のクラスタでは、仮想マシンのモビリティは、物理サーバの負荷やアプリケーション アベイラビリティの状況に基づいて自動的に発生し、クラスタの全メンバおよび関連する全ストレージ ポートの間で完全にランダムなトラフィック パターンが作成されます。

仮想マシンのモビリティを実現するには、大きな展開の中のすべての部分でスイッチング インフラストラクチャが均質なパフォーマンスを提供する必要があります。局所性に基づくトラフィック エンジニアリングは、アプリケーション サーバとストレージ ポートの静的な関

連付けを前提としていますが、そのようなエンジニアリングの価値はなくなります。この状況では、安定したスイッチング ファブリック アーキテクチャの潜在力が示され、ハードウェア コンポーネントに組み込まれた機能が最大限に発揮されます。

**仮想リソースの迅速な展開と管理**

数百の異種アプリケーション サーバの統合を目的とした仮想マシンのエンタープライズクラスの展開は、複数のクラスタで構成されます。当然、それらのセキュリティ要件とスコープは多様になります。この状況では、密なファブリック セグメントを作成し、短時間で柔軟にサーバをセグメントに割り当てることが求められます。

クラスタは、特定のネットワーク セグメントと管理グループに関連付けられます。通常、ファブリックにはスペアのサーバがあらかじめ接続されています。スペア サーバがクラスタに関連付けられたら、ファブリック自体が直ちにスペア サーバのインターフェイスを、宛先クラスタが属するネットワーク セグメントに関連付ける必要があります。

ユーザ コミュニティにはそれぞれに仮想マシンが必要であり、その仮想マシンは、元の物理アプリケーション サーバと同じように管理および保護される必要があります。この要件を満たすために、ファブリック管理はロールに基づいて、仮想マシン管理インフラストラクチャの機能に合わせて詳細な制御を行う必要があります。

## 競合ソリューション

小さなスイッチング要素を多数使用することで、大きなファイバ チャネル スイッチを開発することができます。これらの要素を接続して ASIC ラティスを作成します。これは、個別のスイッチのネットワークに似ていますが、単一の大きな筐体として組み立てられています。

この方法では研究開発コストが大幅に削減されるにもかかわらず、できあがったデバイスは、目的の宛先ポートに対してさまざまなソース ポートから多様なパスを提供することができます。同じライン カードまたはポート グループで送受信されるフレームは、経由するスイッチング要素が 1 つだけで済む可能性があり、多くの場合、発生する遅延は平均よりも短くなりますが、多くのスイッチング要素を経由するフレームでは、平均よりも長く変動の大きい遅延が発生します。トラフィック パターンが複雑な場合は、ASIC ラティス内部の輻輳により、大幅なパフォーマンス ジッタが発生したり、アプリケーションが実際に利用できる帯域幅が大幅に縮小される可能性があります。

ファイバ チャネル市場に参入している一部のベンダーは、アプリケーション サーバを、対応するストレージ ポートのローカル スイッチ ポートに接続することを提案してきました。この方法の目的は、ローカルなスイッチング要素から大量のトラフィックが送信されて予測不可能なパフォーマンスが発生するのを回避することです。

しかし、この設計要件は、ハイパーバイザ クラスタのメンバである物理サーバには当てはまりません。理由の 1 つは、関係するポートの数が多すぎてすべてをローカルに接続できないからですが、より本質的な理由は、多数のクラスタ サーバを同じ ASIC に接続することでクラスタ全体のアベイラビリティが大幅に低下し、クラスタを展開する一番の目的が果たされなくなることです。同様の理由から、また効果的なロード シェアリングのために、ストレージ ポートは、複数のライン カードまたはスイッチング ASIC に分散させる必要があります。局所性を重視しない場合、クラスタ内の物理サーバのパスは多様になり、パフォーマンスの幅も広がります。

セキュリティも重要な要因です。さまざまなビジネス機能を 1 つの物理インフラストラクチャに統合する際は、個別のサーバと分散ネットワークによって提供されていたときと同レベルの分離状態を提供する必要があります。

ハイパーバイザ ベンダーは仮想マシン間の理想的な分離状態を実現しようと努力していますが、この目標を追求する力がすべてのストレージ ネットワーキング ベンダーの間で同じであるとは言えません。分離は、所定の管理者の特権をファブリック内のゾーンのサブセットに限定することにより、ゾーニングのインフラストラクチャおよび機能のアドオンに委任されます。

このソリューションはベンダー固有であり、標準に基づいたものではないので、個別のファブリック サービスやハードウェアの分離を実現することはできません。すべてのデータが同じファブリック トポロジを共有し、同じ悪意ある攻撃にさらされ、設定エラーやプロトコル違反による同じサービスの中断を受けます。

## Cisco MDS 9000 ファミリの利点

シスコはネットワーキング企業として、複雑で予測不可能なトラフィック プロファイルを持つ大規模ネットワークに関し、豊富な経験を持っています。ファイバ チャネル スイッチとディレクタを備える Cisco MDS 9000 ファミリの設計には、シスコの幅広い視点が反映されています。

Cisco MDS 9000 ファミリは、任意のポート間で最適なパフォーマンスを提供するように設計されており、仮想化されたデータセンターの需要に対応できます。さらに、Cisco MDS 9000 ファミリには最初から仮想化が組み込まれており、仮想 SAN（VSAN）などの革新的な機能やロールベースの管理が導入されています。

Cisco MDS 9000 ファミリには、次のような利点があります。

- ハイパフォーマンス スイッチ アーキテクチャ
- クラスタ展開を簡素化する仮想 SAN インフラストラクチャ
- 仮想インフラストラクチャ管理の SAN への拡張
- 統合環境でのセキュリティ
- NPIV の使用による SAN での仮想マシン アイデンティティの提供
- QoS
- 仮想マシンごとのパフォーマンス モニタリング
- トラブルシューティング ツール
- ブレード サーバ上での仮想マシン展開
- F ポート トランキング機能
- 大規模な iSCSI（Small Computer System Interface over IP）展開のサポート

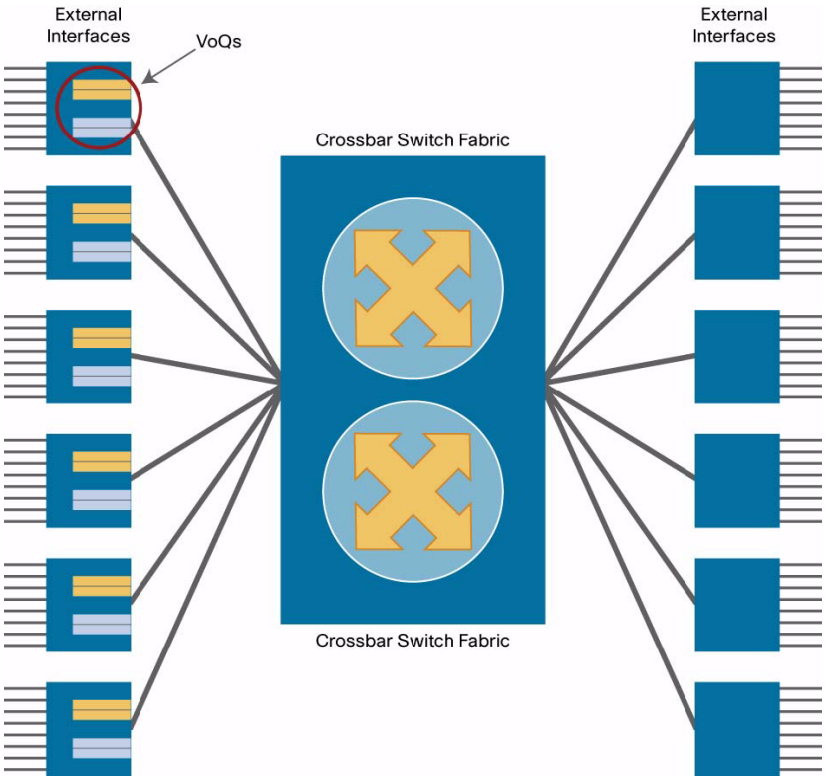
### ハイパフォーマンス スイッチ アーキテクチャ

Cisco MDS 9000 ファミリのスイッチとディレクタは、中央集中化されたクロスバー アーキテクチャ（図 3）に基づいており、多くの困難なトラフィック状況で最適なパフォーマンスを提供するように設計されています。クロスバーの入力での仮想出力キュー（VOQ）によってヘッドオブライン ブロッキングを回避することにより、トラフィック パターンに関係なく各ポートでラインレート パフォーマンスが確保されます。このアーキテクチャにより、多

対 1、多対少、およびメッシュ化された予測不可能な動的トラフィック パターンが存在する場合に、大きいフレームと小さいフレームの両方に対して、均質で予測可能なパフォーマンスが提供されます。

**図 3**　Cisco MDS 9000 ファミリの中央集中型クロスバー アーキテクチャ




**クラスタ展開を簡素化する仮想 SAN インフラストラクチャ**

仮想 SAN（VSAN）テクノロジーは、ANSI T11 標準で扱われており、単一の物理 SAN ファブリックまたはスイッチ内でハードウェア ベースのセキュアなネットワーク セグメントを実現します。

各 VSAN は、それぞれが独立したファブリック サービス（ゾーン サーバ、ネーム サーバ、ドメイン マネージャ、FSPS [Fabric Shortest Path First] ルーティング サービス）の制約を受けます。各 VSAN には任意の設定作業や選択を含めることができるので、これによって別の VSAN で発生する管理、設定、およびプロトコル エラーから保護できます。

たとえば、ゾーニングは VSAN インフラストラクチャを基礎として、その上で実行されるファブリック サービスです。設定エラーやプロトコル違反によってゾーニングに壊滅的な設定ミスが発生しても、問題が発生した VSAN 以外の場所にはまったく影響がありません。

Cisco MDS 9000 ファブリック全体から任意のインターフェイスを選び、簡単な設定コマンドですぐに任意の VSAN に割り当てることができます。

仮想マシン インフラストラクチャ内では、個別の物理サーバがクラスタとしてグループ化されます。仮想マシンは、クラスタ内の任意のサーバに簡単に移動できます。クラスタは、さらに上位の「データセンター」と呼ばれる管理エンティティにまとめることができます。このドキュメントではこれ以降、この管理エンティティを仮想データセンターと呼びます。

仮想マシンは、物理サーバ間を移動することで物理サーバ間のロード バランシングを行います。また、ホスティング元の物理サーバに障害が発生した場合は、他のサーバに移動することで仮想マシン自体のアベイラビリティを維持します。

最適なレベルのアベイラビリティを実現するために、同じクラスタのメンバである物理サーバは、ファブリック内の複数の SAN スイッチに分散させるか、スイッチが 1 つだけの場合でも少なくとも複数のライン カードに分散させる必要があります。

Cisco MDS 9000 ファミリ インフラストラクチャを使用すると、同じクラスタに属する物理サーバ、およびそれに対応するストレージ デバイスを同じ VSAN 内に展開しつつ、任意のスイッチの任意のポートに分散させることができます。このように構成すると、厳格な分離が維持されると同時に、事前に計画を立てなくても物理ネットワーク インフラストラクチャを共有できます。

仮想データセンターまたはクラスタの物理サーバの追加または削除は、仮想インフラストラクチャ管理インターフェイスでサーバのプロパティを変更し、スイッチ ポートを別の VSAN に再割り当てすることで簡単に実行できます。この方法は、分離された物理ファブリックから別のファブリックにファイバ チャネル ケーブルを配線し直すのと機能的には同じですが、VSAN を導入することで完全に仮想化されています。どのファブリック ポートも任意の VSAN に属することができるため、物理サーバから仮想データセンターまたはクラスタへの割り当てを指定するために事前の計画を作成する必要はありません。配線が適切に行われた後は、必要に応じてソフトウェアで割り当てを実行できます。

F ポート トランキングという新機能を適切なハイパーバイザ ドライバと組み合わせて使用すると、さらに柔軟性が高まり、同じ物理サーバ上にある複数の仮想マシンを複数の VSAN に接続できるようになります。この機能については、後で詳しく説明します。

**仮想マシン、SAN、およびストレージの仮想インフラストラクチャ管理**

仮想インフラストラクチャ管理には、複数のレベルのロールベース アクセス コントロール（RBAC）を利用できます。たとえば、1 人の管理者の担当範囲を 1 つ以上の仮想データセンターにすることも、1 つ以上のクラスタ、または 1 つ以上の物理サーバにすることもできます。

Cisco MDS 9000 ファミリの管理アーキテクチャでも、同じ程度に高度な RBAC インフラストラクチャを利用できます。管理者はグループや個人に対する管理権限を簡単に割り当てたり、適用範囲を仮想データセンターまたは物理サーバ クラスタにマッピングすることができます。

考えられる管理方法を図 4 に示します。ここでは、仮想データセンター内のすべての物理サーバが同じ VSAN に割り当てられていて、管理は VSAN 単位と仮想データセンター単位で行われるように構成されています。

別の構成として、同じクラスタに属するすべての物理サーバを同じ VSAN に割り当てて、管理は VSAN 単位とクラスタ単位で行うことが考えられます。

**図 4**　VSAN と仮想データセンターに基づいた管理

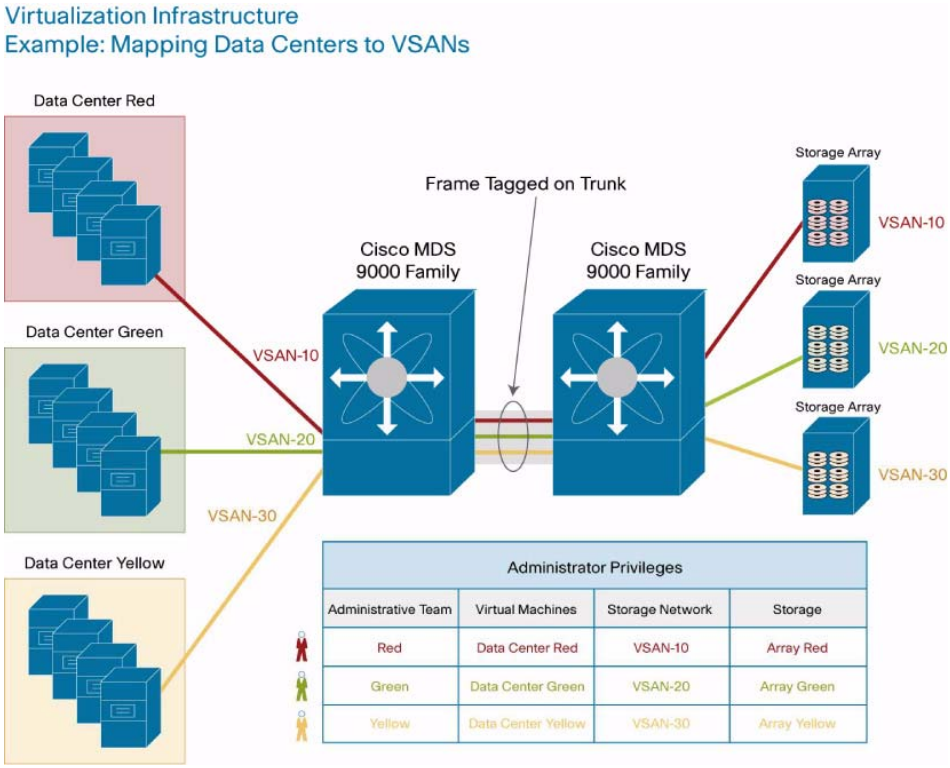



図 4 に、1 つの物理データセンターに 3 つの仮想データセンター（Red、Green、Yellow）が存在する運用環境を示します。たとえば、管理チーム Red は、仮想データセンター Red と VSAN-10 のリソースを設定する権限と、ストレージ アレイ Red のストレージ ボリュームを設定する権限があるとします。物理ネットワーク リソース、スイッチ、スイッチ間リンクが統合されていても、管理チーム Red と仮想リソースは完全に分離されています。

**統合環境でのセキュリティ**

さまざまなビジネス機能を 1 つの物理インフラストラクチャに統合する際は、個別のサーバまたは接続されていないネットワークによって提供されていたのと同レベルのセキュリティ分離状態を確保する必要があります。

基本的なファブリック セキュリティは VSAN 機能を持つハードウェアに組み込まれていますが、Cisco MDS 9000 ファミリによって提供される全体的なセキュリティへのアプローチがあれば、緊密に統合された環境でも安心です。

Cisco MDS 9000 ファミリの主なセキュリティ機能は次のとおりです。

- HTTPS、SNMPv3（Simple Network Management Protocol Version 3）、SSH（Secure Shell）、SFTP（Secure File Transfer Protocol）などのセキュア プロトコルを介して実行される管理。コマンドライン インターフェイス（CLI）と Cisco Fabric Manager 管理ツールの両方でセキュア プロトコルが使用され、どちらも完全に RBAC インフラストラクチャに組み込まれています。

- AAA（認証、許可、アカウンティング）。標準プロトコル（RADIUS および TACACS+）を使用してエンタープライズ インフラストラクチャに組み込むことができます。Cisco Secure Access Control Server（ACS）などの外部 AAA サーバを使用すると、ユーザ認証交換によっても RBAC をサポートするロール情報が提供されます。
- 設定の管理、配布、および一貫性分析。
- ファブリック アクセス セキュリティ（ファブリック バインディングとポート セキュリティ）。ポート セキュリティは物理ハイパーバイザ サーバに対応できます。また、NPIV テクノロジーと共に使用すると、後で説明するように個別の仮想マシンにも対応できます。
- ファイバ チャネル セキュリティ プロトコル（FC-SP、シスコが大半を開発した標準）のサポート。
- ゾーニングの拡張サポート（論理ユニット番号 [LUN] ゾーニングと読み取り専用ゾーン）。
- 転送中（IP 上の SAN 拡張、具体的には FCIP [Fibre Channel over IP] と iSCSI は IPsec [IP Security] を使用可能）および保管中（Cisco Storage Media Encryption [SME] を使用）のデータを保護する統合的な高パフォーマンス ネットワーク サービス。
- データ トラフィックを分離し、ファブリック サービスとプロトコルを保護する、ハードウェアによる標準ベースの VSAN セグメンテーション。

Cisco MDS 9000 ファミリには、エンタープライズクラスの仮想マシン展開に必要なレベルのセキュリティを実装するためのあらゆるツールが用意されています。

**NPIV の使用による SAN での仮想マシン アイデンティティの提供**

N ポート ID バーチャライゼーション（NPIV）は、個別の仮想マシンを SAN 上の完全なアイデンティティを持つものとして扱うことができるファイバ チャネル プロトコル機能です。NPIV を使用すると、ハイパーバイザは仮想マシンごとに仮想 HBA を作成できます。仮想 HBA は、物理 HBA と同じようにファイバ チャネルのポート pWWN（port World Wide Name）によって識別されます。このアイデンティティはその仮想マシンの属性であり、仮想マシンが物理サーバ間で移動されても維持されます。Cisco MDS 9000 ファミリは、NPIV 仮想マシンを完全かつスケーラブルにサポートします。物理サーバで利用可能な各機能は、NPIV で識別される個別の仮想マシンで利用できます。たとえば、ゾーニングなどの基本的なファイバ チャネル サービスや、トラブルシューティング ツール、QoS、パフォーマンス モニタリングなどの高度な機能を利用できます。

Cisco MDS 9000 ファミリは、現在のハイパーバイザの NPIV 機能を使用して、任意のエンタープライズクラスの仮想マシン展開をサポートできます。また、ハイパーバイザ ベンダーによって将来実用化されると見込まれる NPIV ベースの追加機能にも対応できます。

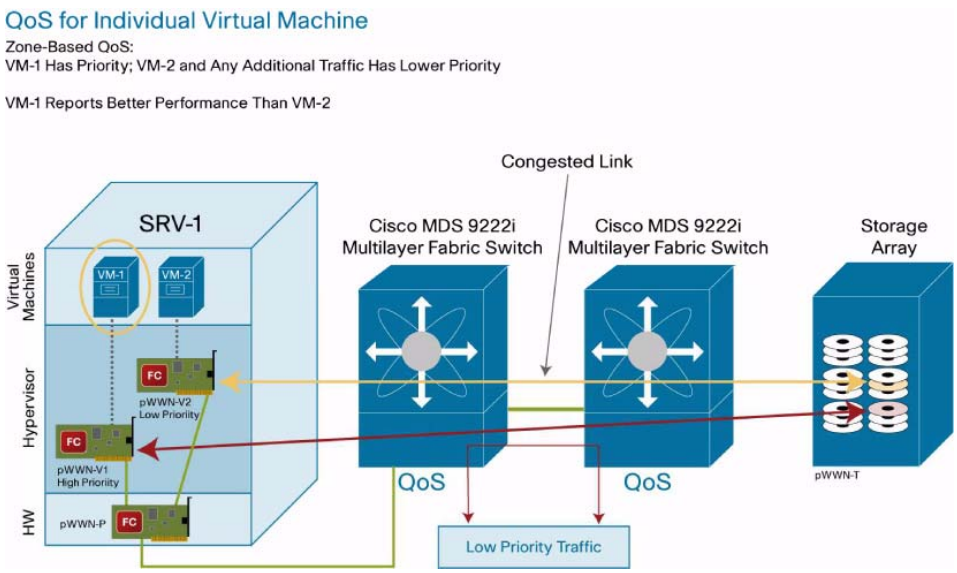
## QoS

Cisco MDS 9000 ファミリは、VSAN ベースやゾーンベースの QoS など、QoS 管理のためのオプションを多数備えています。

VSAN ベースの QoS は、仮想データセンター全体やクラスタ全体が 1 つの VSAN にマッピングされる場合に便利です。ゾーンベースの QoS を使用することにより、特定の物理サーバまたは物理サーバ グループのパフォーマンスを強化できます。NPIV と共に使用した場合、個別の仮想マシンに対しても効果が得られるということが実証されています（図 5）。

**図 5**　QoS レベルを個別の NPIV 仮想 HBA に割り当て可能




### トラブルシューティング ツール

Cisco MDS 9000 ファミリは、接続の問題を切り分けるためのトラブルシューティング ツールを備えています。ファイバ チャネル エコー パケットに基づくファイバ チャネル ping（FC-ping）を使用すると、デバイスがファブリックに接続されているかどうかを確認でき、FC-traceroute を使用すると、2 つのデバイス間のネットワーク ルートを追跡できます。これらのツールを使用して、物理サーバ、ハイパーバイザを実行している物理サーバ、および NPIV に対応した仮想マシンのトラブルシューティングを同じ方法で行うことができます。

仮想化環境で便利なトラブルシューティング ツールとしては、このほかに、ローカルおよびリモートの組み込みプロトコル分析や、ネットワーク アナライザ ポートへのミラーリングなどがあります。

### パフォーマンス モニタリング

Cisco Fabric Manager は、Cisco MDS 9000 ファミリ SAN 向けの GUI ベースの管理インフラストラクチャです。Cisco Fabric Manager には、ファブリックの設定とパフォーマンス モニタリングのためのツールが揃っています。

物理デバイスで利用できるものと同じパフォーマンス モニタリング機能を使用して、個々の NPIV 対応仮想マシンの統計データを収集できます。これにより、エンドツーエンド ストレージ インフラストラクチャの一元的なモニタリングが可能です（図 6）。

**図 6**　NPIV を使用する個々の仮想マシンのパフォーマンス モニタリング

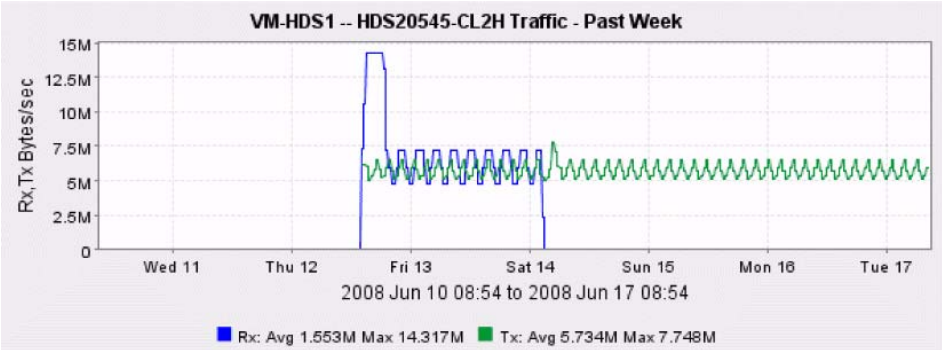



図 6 に、個々の NPIV 対応仮想マシンの傾向を示す統計情報と、読み書き操作に関する詳細情報を示します。

## ブレード サーバ上での仮想マシン

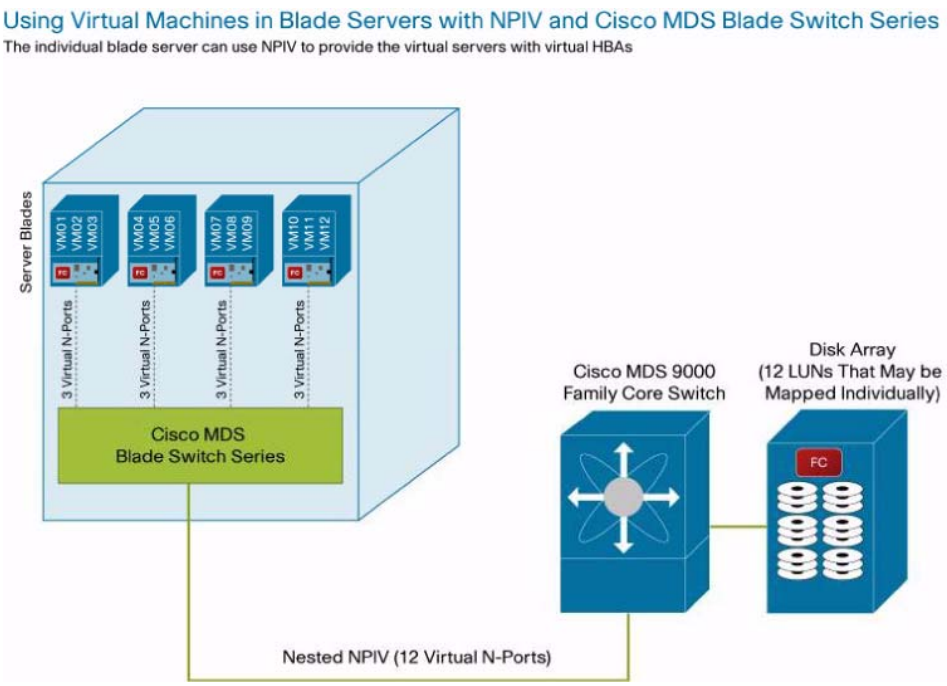
SAN 内で仮想マシンを識別するための NPIV は、ブレード サーバ フォーム ファクタで利用できる Cisco MDS 9000 ファミリ スイッチでもフル サポートされます。

シスコの N ポート バーチャライザ（NPV）機能により、ハードウェアやソフトウェアを追加しなくても、ブレード スイッチを大規模 SAN 内に容易に展開できるほか、任意のベンダーのコア スイッチと組み合わせた運用も容易になります。NPV を設定すると、ブレード スイッチはスイッチではなくホスト バス アダプタ（HBA）アグリゲータと見なされます。

すべてのサーバ ブレードは、それぞれの物理アイデンティティを使用して、ブレード スイッチに対してファブリック ログインを実行します。このブレード スイッチは各サーバ ブレードのプロキシとして機能し、各ブレードの物理アイデンティティを NPIV 仮想アイデンティティとして使用します。

NPIV を使用するハイパーバイザをサーバ ブレードが実行している場合、各仮想マシンの個々の仮想 HBA アイデンティティは Cisco MDS ブレード スイッチ シリーズによって守られ、Cisco MDS ブレード スイッチ シリーズはコアに対するプロキシとして機能します（図 7）。この機能は、ネスト状態の NPIV とも呼ばれ、ラックマウント サーバまたはブレード サーバのどちらかでインスタンス化された仮想マシンに対して同じ機能を提供するために不可欠な機能です。

**図 7**　Cisco MDS ブレード スイッチ シリーズ



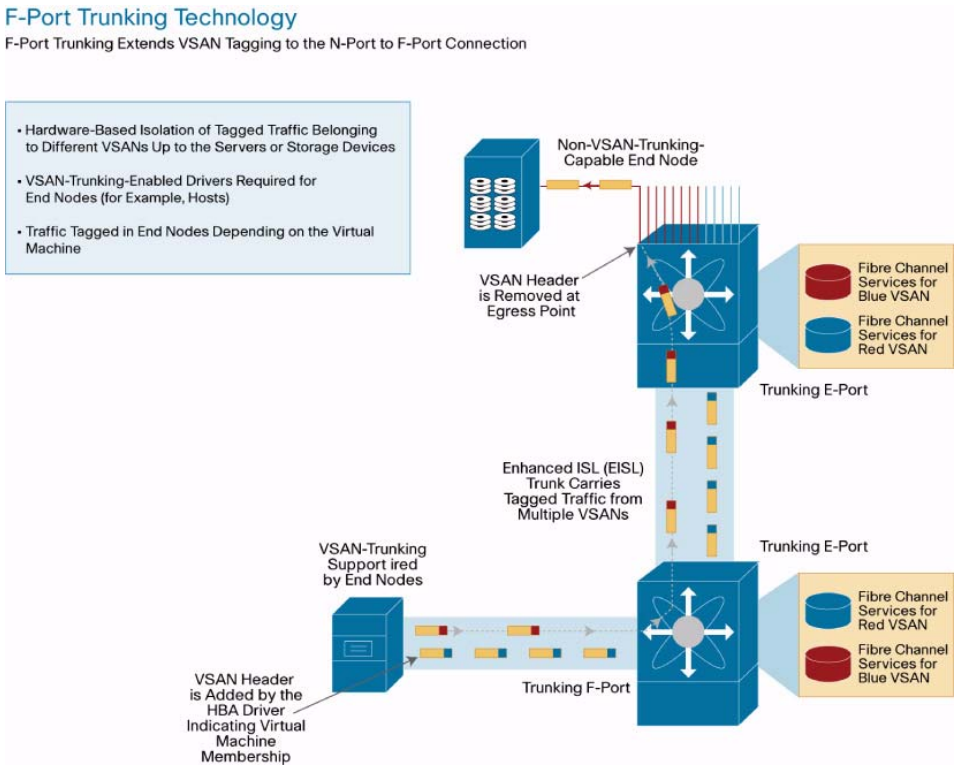

シスコは最近、ブレード シャーシ向けの FlexAttach 機能を発表しました。FlexAttach 機能を使用すると、サーバを移動、追加、変更する際の SAN スイッチやストレージ アレイの再構成が不要になります。FlexAttach を使用すると、サーバの SAN アイデンティティを仮想化できます。このアイデンティティは、ブレード サーバ シャーシ内で、またはシャーシから外にサーバを移動したり、サーバを交換する場合でも維持されるので、SAN の再構成を行う必要がなく、サーバ管理者はこれまでよりも柔軟に作業を行うことができます。

Cisco MDS ブレード スイッチ シリーズを NPV モードで使用すると、F ポート PortChanneling 機能が有効になり、コア スイッチとの複数の接続をまとめることができます。この機能では、複数のポートが結合されて 1 つの論理リンクが作成されます。これにより、帯域が増加し、ファブリック接続のアベイラビリティと復元性が高まります。F ポート PortChanneling を使用すると、仮想マシン展開の全体的な堅牢性が大幅に強化されます。

### F ポート トランキング

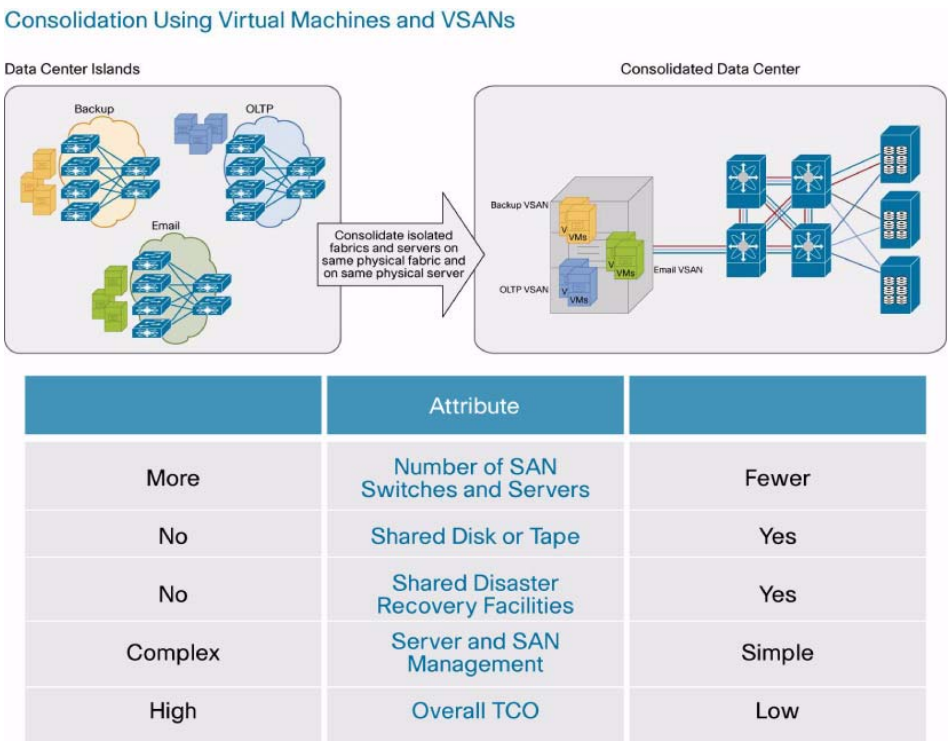
F ポート トランキング機能を使用すると、仮想マシンは同じ物理サーバ HBA を共有しながら複数の仮想 SAN に属することが可能になります（図 8）。このテクノロジーは ANSI T11 ファイバ チャネル規格に完全準拠しており、HBA ドライバが同様のサポートを行っていることが必要です。

**図 8**　F ポート トランキング テクノロジー




F ポート トランキング機能を使用すると、サーバとストレージの統合が促進されます。同じ物理サーバと同じ HBA で、さまざまなユーザ グループに属する仮想マシンをホスティングしながら、ストレージ リソース間の分離レベルを厳重に維持することが可能です（図 9）。

**図 9**　仮想マシンと VSAN による統合




ファイバ チャネル サービスのインスタンス化は VSAN 単位で行われるので、このソリューションでは各ユーザ グループがそれぞれのゾーンとゾーン セットを管理できます。

F ポート トランキングと NPIV を組み合わせて使用すると、VSAN 単位の独立したゾーン セットと、VSAN 内の個々の仮想マシン単位の独立したゾーン セットの両方を作成できます。

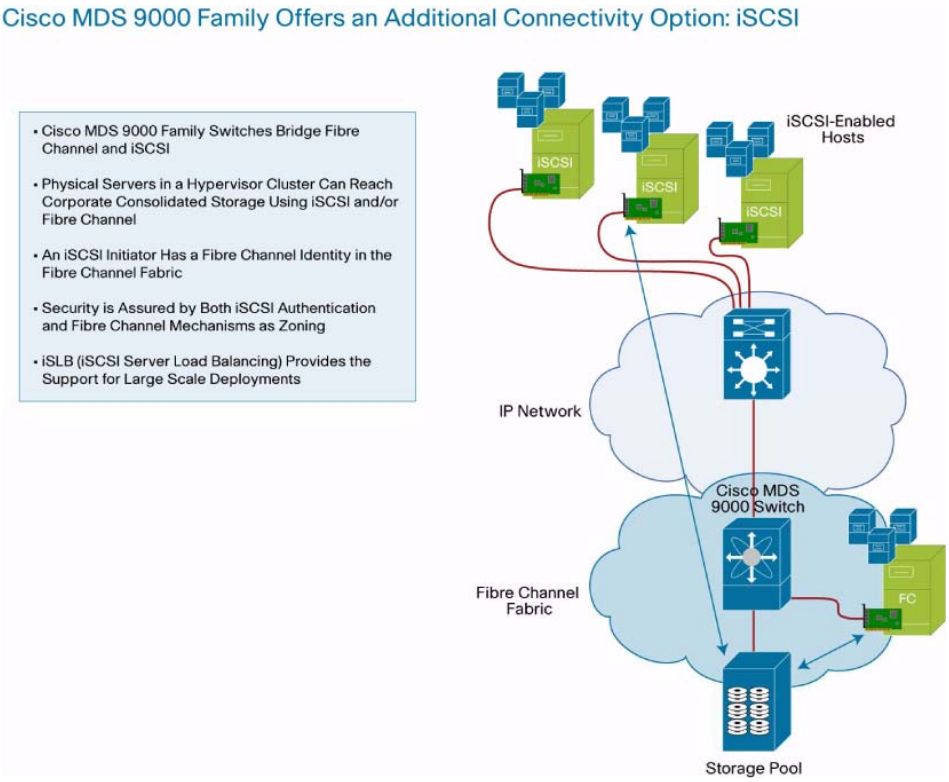
**大規模な iSCSI 展開のサポート**

ハイパーバイザの主要ベンダーは、高パフォーマンス ファイバ チャネル ハードウェアを展開することなく仮想マシンがストレージ ボリュームにブロックレベルでアクセスするための接続オプションとして、iSCSI を提供しています。

iSCSI は、目的とするレベルのパフォーマンスとスケーラビリティを特定のソリューションで達成でき、管理が容易で TCO に悪影響がなければ、エンタープライズクラスのアプリケーションをサポートできることが実証されています。

Cisco MDS 9000 ファミリは、ファイバ チャネルを iSCSI ゲートウェイに完全統合するソリューションを提供します。これにより iSCSI クライアントは、統合されたファイバ チャネル ストレージにアクセスできます。Cisco MDS 9000 ファミリの iSCSI 実装では、ファイバ チャネル イニシエータ（VSAN、高度セキュリティ、ゾーニングを含む）で利用可能なすべての機能が iSCSI イニシエータに提供されます。これにより、移行が容易になり、混在環境が実現します（図 10）。

**図 10**　iSCSI による仮想マシンの展開




エンタープライズクラスの仮想マシン展開では必要なことですが、多数のイニシエータの展開を合理化するために、Cisco MDS 9000 ファミリには iSCSI サーバ ロード バランシング（iSLB）と呼ばれる独自機能があります。

iSLB には次の 3 つの主要機能があります。

- イニシエータ指向のウィザードベース GUIにより、多数（数百）のイニシエータの展開が簡素化されます。
- iSLB ポータルはアベイラビリティに優れています。1 つの iSCSI ポータルを設定することで、イニシエータは多数のイーサネット インターフェイス、複数のラインカード、および複数の Cisco MDS 9000 ファミリ スイッチとディレクタに自動的に分散されます。
- iSCSI 設定がファブリック内の全スイッチに自動的に分散されることで、設定ポイントが一元化され、ファブリック内で設定に矛盾が生じるのを避けることができます。

これらの機能を備えた Cisco MDS 9000 ファミリは、大規模 iSCSI、エンタープライズクラス、仮想マシン展開にとっての理想的な選択肢です。

## まとめ

エンタープライズ クラスの仮想マシン展開が増えることで、ストレージ ネットワーキングには新たな課題が発生しました。

大半の展開は比較的大きなクラスタとして編成され、多数のストレージ デバイスを共有するので、一般的なファイバ チャネル トラフィックのプロファイルは、多対 1（10:1 など）から多対少またはメッシュ型（32:8 など）へと変化しています。また、仮想マシンのモビリティによって、物理サーバとストレージ デバイス間のトラフィック パターンはランダム化しています。

その結果、トラフィックは複雑に分散し、スイッチング インフラストラクチャは限界に達しつつあります。サーバとストレージの局所性に基づいた従来型の SAN 設計は通用しなくなっており、どのような予測不可能なトラフィック分散状況にあってもファブリック自体が最適なパフォーマンスを発揮する必要があります。

少数のスイッチング要素から成るネットワークに基づいたシンプルなスイッチング アーキテクチャとスイッチは、より高度なアーキテクチャに取って代わられています。たとえば、Cisco MDS 9000 ファミリのファイバ チャネル スイッチとディレクタは、最初から、予測不可能な多対多のネットワーク トラフィックを処理する設計になっています。

複数のユーザ コミュニティをホスティングし、そのそれぞれが少なくとも 1 つのハイパーバイザ クラスタを制御している大規模な物理データセンターは、物理サーバ、ネットワーク セグメンテーション、障害の分離、およびセキュリティに関して厳しい要件を課しています。

仮想マシンのエンタープライズ クラスの展開では、スペアの物理サーバを適切なネットワーク セグメントに接続し、クラスタに参加できる状態にするまでの時間を、最小限に抑える必要があります。Cisco MDS 9000 ファミリに実装されるファイバ チャネルの標準の VSAN テクノロジーでは、スペアのサーバをファブリック インターフェイスのいずれかの場所にあらかじめ接続しておきます。設定コマンドを実行すると、そのインターフェイスはただちに適切なネットワーク セグメントおよびクラスタに割り当てられます。

同時に、厳重なセキュリティと障害分離を実現するハードウェア面の基盤が VSAN インフラストラクチャによって提供されます。ファイバ チャネルと iSCSI にも同じアプローチが適用されます。ファイバ チャネル ゾーニングへの管理アクセス制限に基づく競合テクノロジーは、巨視的な人為的ミスを防ぐことはできますが、真のネットワーク セグメンテーションや、ネットワーク セグメンテーションの動的管理を行う機能は備えていません。

Cisco MDS 9000 ファミリは、ネットワーク管理、設定管理、トラブルシューティング、トラフィック エンジニアリングを行うための包括的なツールセットを備えています。RBAC インフラストラクチャは、仮想マシン管理用のエンタープライズクラスのツールによって提供される強力な機能と、簡単に対応させることができます。管理とトラブルシューティングでは、ブレード サーバで実行されるハイパーバイザや、NPIV ベースの仮想 HBA を使用する仮想マシンもサポートされます。

## 関連情報

詳細については、http://www.cisco.com/jp/go/storage/ を参照してください。

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS 含む)
電話受付時間 : 平日 10:00 ~ 12:00、13:00 ~ 17:00
http://www.cisco.com/jp/go/contactcenter/

お問い合せ先

08.12