

VERITAS Storage Foundation™ *for Windows*

**VERITAS Storage Foundation™ *for Windows* による
ストレージ エリア ネットワーク (SAN) からの Windows のブート
(Windows OS の起動)**

目次

はじめに.....	3
SAN からブートすることの利点.....	3
SAN からブートすることの欠点.....	3
要件.....	3
推奨事項.....	4
制限事項.....	4
Windows ブート プロセス.....	4
プリブート.....	4
Windows のブート.....	4
IA-64.....	6
ブートタイプ.....	6
ローカル ブート.....	6
ネットワーク ブート.....	6
SAN からのブート.....	6
SAN からのブート.....	6
クラスタ環境でのブート.....	7
Dymamic Multi-Pathing (DMP).....	8
潜在的な問題と解決方法.....	9
まとめ.....	10
参考資料.....	10

はじめに

Microsoft は、Knowledge Base の文書 [305547](#) に指定された設定により、ストレージ エリア ネットワーク (SAN) からの Windows 2000 および Windows Server 2003 のブート (起動) をサポートしています。VERITAS Storage Foundation for Windows を使用すれば、Storage Area Network (SAN) から Windows をブートする際の、同じバスを共有するシステム/ブート ディスク リソースとクラスタ ディスク リソースのプロセスを簡単にすることができます。

SAN からブートすることによる利点

配備するのは複雑な作業ですが、SAN からブートすることにはいくつかの利点があります。次に、SAN からブートすることによる利点を示します。

- **サーバーの統合** - SAN 上にある OS イメージからブートできるようになると、安価なシン ディスクレス サーバーを採用しやすくなります。シン ディスクレス サーバーはスペースも電力もあまり必要とせず、ハードウェア コンポーネントも少なくすみます。
- **集中管理** - OS イメージを SAN ディスクに格納すると、OS のアップグレードや修正を集中管理することができます。
- **サーバー障害からの復旧が簡単にできる** - SAN からブートしたシステムに障害が発生した場合、代替用のシステムを容易に SAN からブートでき、しかも SAN 上に格納されたデータへのアクセスも容易にできるため、実稼働環境にすばやく復帰できます。また、SAN からブートすることにより、サーバーの障害からすばやく簡単に復旧することができます。
- **災害からすばやく復旧できる** - SAN 上にあるブート情報と実際に使うデータをリモートの SAN にミラーリングまたはレプリケーション (複製) して置くことにより、プライマリ サイトで災害が発生した場合でも、リモート サイトの実稼働環境に処理をすばやく移行することができます。
- **一時的なサーバーの負荷をすばやく分散できる** - 一時的に高い作業負荷がかかる実稼働環境では、SAN テクノロジーでブート イメージを複製し、複数のサーバーで分散して処理することにより迅速な分散処理を可能とします。このようにサーバーを必要に応じてすばやく実稼働環境に追加したり削除したりできるので、費用対効果の非常に高いソリューションとなります。

SAN からブートすることの欠点

SAN からのブートには数多くの利点がありますが、これを実行するユーザーは、SAN の配備に関する数多くの複雑な問題を熟知している必要があります。次に、SAN からのブートの欠点を示します。

- **ハードウェアの配備が複雑** - 特にヘテロジニアスな環境に当てはまりますが、すべてのハードウェア コンポーネントを正しく設定しなければなりません。誤った設定の場合には、SAN からのブートが失敗してしまいます。
- **ブートプロセスが複雑** - 効果的なトラブルシューティングを行うには、ブートプロセスを理解することが不可欠です。

要件

ストレージ エリア ネットワーク (SAN) から正常にブートするためには、次の条件を満たす必要があります。

上記の Knowledge Base 文書によると、次の設定要件に適合する必要があります。

1. SAN はスイッチの整った環境に設定するか、もしくは各ホストをストレージ サブシステムのファイバ チャンネルポートに直接接続する必要があります。
2. ホストはブート元のディスクへの排他アクセス権を持つ必要があります。これは、Microsoft の Windows では、ブート ディスクが一意かつ専用である必要があるためです。すなわち、SAN から Windows をブートするときには LUN マスキングが必要です。LUN マスキングは、ホストの HBA に関連付けした一意の World Wide Name (WWN) により、ディスク、アレイ、または LUN パーティションへの排他的なアクセス権をホストに与えます。
3. Windows 2000 の場合、Microsoft は MSCS でクラスタ化したサーバーのブート ディスクは、クラスタの共有ストレージで使用されるものとは別のストレージ パス上にある必要があるとしています。SAN からブートするとき、ブート用と共有ストレージ用にそれぞれ異なる専用パスが必要です。

注: Windows Server 2003 での Storport ドライバーの導入により、ブート ディスクとクラスタ ディスクは同じバスを共有できるようになりました。Microsoft の Storport ドライバーの詳細については、Microsoft のホワイトペーパー『Storport in Windows Server™ 2003: Improving Manageability and Performance in Hardware RAID and Storage Area Networks』を参照してください。

4. HBA は SAN ブートをサポートする必要があります。また、正しいバージョンの HBA BIOS ファームウェアと HBA ドライバーを使用する必要があります。さらに、HBA 設定も正しく設定する必要があります。
5. ブート BIOS は、サーバーごとに 1 つのアダプタのみ有効にする必要があります。
6. IA-64 の場合、ブート可能な HBA はハードウェアも含めてテストしておく必要があります。

推奨事項

SAN からブートするための多くの要件に加えて、次の推奨事項を適用すると、より柔軟性や冗長性が向上します。

- ブート ボリュームをローカルまたはリモートの別の LUN にミラーまたはコピーします。ディスクまたはアレイに障害が発生した場合、サーバーのブートデバイスをミラー側にマッピングしなおせば、すばやく回復できます。
- マルチパス機能を使用して、SAN ストレージへのパスの冗長化をします。これによって、単一 ポイント障害を回避できます。
- Windows Server 2003 に含まれる Microsoft の Storport ドライバーと HBA ベンダーから提供される適切なミニポート ドライバーを使用すると、SAN の設定がより柔軟になります。Storport ドライバーを使用することにより、ブート ディスクとクラスタ ディスクを同じファイバ チャンネルのパス上で共有することができます。
- ページファイルはローカル ディスク上に置きます。後述の「潜在的な問題と解決方法」を参照してください。

制限事項

SAN から Windows をブートする場合の制限事項としては、現在のところ、ブート イメージを共有できない (各サーバーが個々のブート イメージを持つ必要がある) ことと、複数のブート イメージを配置する簡単な方法がないことがあります。

Windows ブート プロセス

SAN からのブートの複雑さと利点を詳細に説明する前に、まず、ブート プロセスを説明する必要があります。ブート プロセス (「ブートストラップ」とも呼ぶ) とは、オペレーティング システムのコードをストレージ デバイスからコンピュータのメモリーにロードするプロセスのことです。ブートを行うことができるのは、直接接続されたディスク、LAN、または SAN からになります。ブートのプロセスはブートのタイプにかかわらず同じです。後述の節では、32 ビット アーキテクチャのブート プロセスについて説明します。Intel IA-64 アーキテクチャのブート プロセスでの違いについては、Microsoft の技術文書『Boot from SAN in Windows Server™ 2003 and Windows® 2000 Server』を参照してください。

プリブート

コンピュータの電源を投入すると、まず、コンピュータの最も基本的なコードである BIOS (Basic Input/Output System) がロードされます。BIOS は自己診断テスト (POST) を実行して、ハードウェアに問題がないかどうかをチェックします。何も問題がなければ、CPU は次の処理に移ります。BIOS はすべてのブート可能デバイス (NIC や HBA を含む) を見つけて初期化し、ブート デバイスを設定します。ブート デバイスには、最初に見つかったブート可能なデバイスが設定されるか (デフォルト)、あるいは、複数のブート デバイスが存在する場合は、ユーザーが設定したデバイスが設定されます。次に、ブート セクターがブート デバイスからメモリーにロードされます。Intel ベースのシステムでは、プライマリ ディスクの最初のセクターに MBR (Master Boot Record) が含まれていなければなりません。MBR には、Windows をブートするために必要なコードや設定ファイル (Ntldr、boot.ini、および Ntdetect.com) が格納されているシステム パーティションを含みます。このパーティションはアクティブ (ブート可能) に設定されている必要があります。

Windows のブート

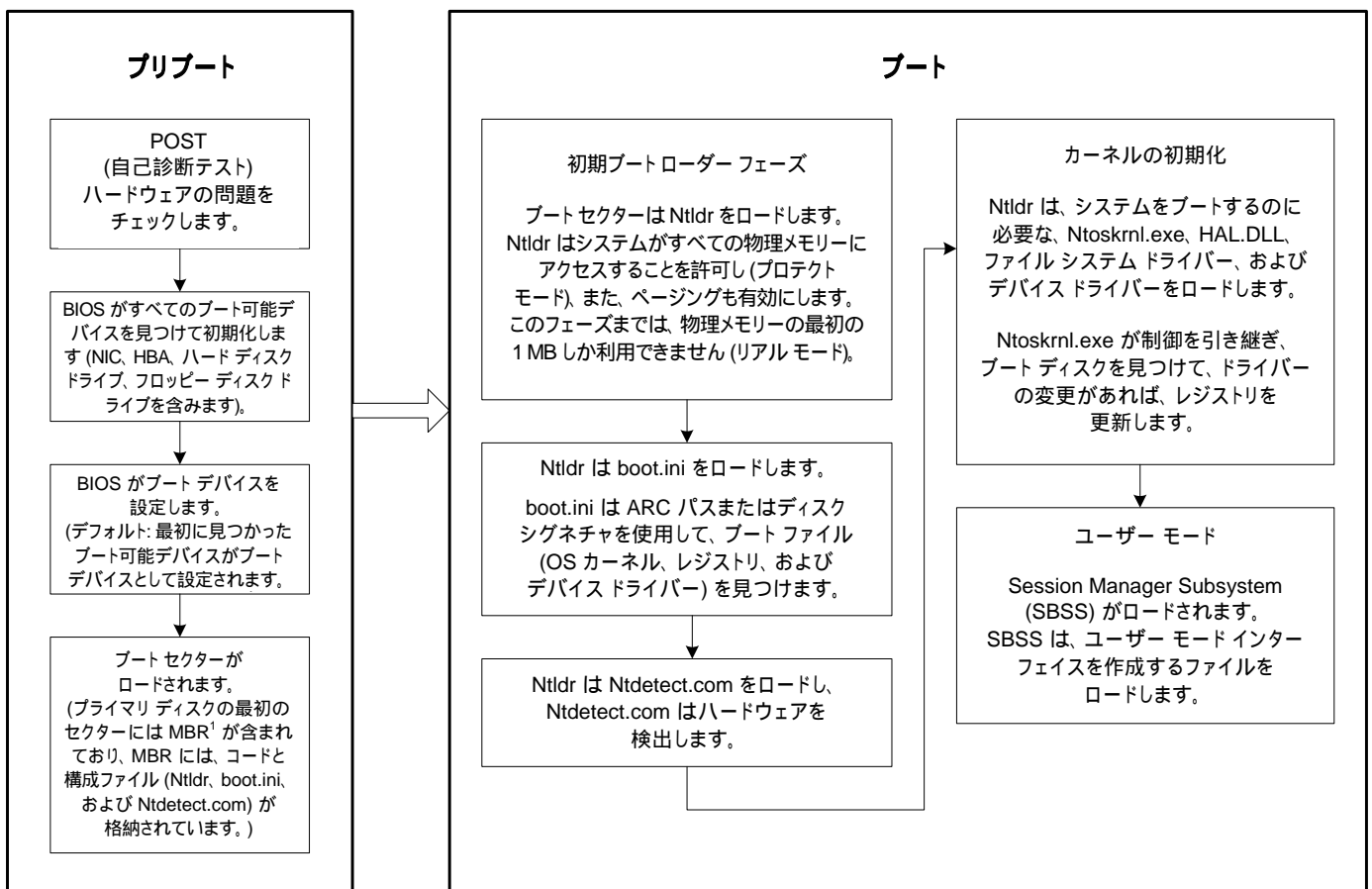
ブート セクターがロードされたら、残りのブート プロセスに進めます。Windows の場合、Ntldr がほとんどのブート プロセスを制御します。ブート セクターが Ntldr をロードすると、Ntldr は Windows オペレーティング システムをロードするプロセスを開始します。このプロセスは複数のフェーズから構成されます。

最初のフェーズは、初期ブート ロードー フェーズです。このフェーズでは、Ntldr によりシステムはすべてのシステム メモリー（物理メモリー）にアクセスできます。このフェーズのことを「プロテクト モード」と呼び、ページングも有効になります。なお、プロテクト モードに入る前のことを「リアル モード」と呼び、このとき、システムはシステム メモリーの最初の 1 MB にしかアクセスできません。

次のフェーズでは、Ntldr は boot.ini をロードします。このファイルには、オペレーティング システムのカーネル、レジストリ、およびデバイス ドライバーの場所についての情報が含まれます。boot.ini は ARC (Advanced RISC Computing) パスまたはディスク シグネチャ (32 ビットの一意的番号) を使用して、ブート ファイルを見つけます。次に、Ntldr は Ntdetect.com をロードします。Ntdetect.com は BIOS を使い、追加のハードウェア情報 (マシン ID、バス/アダプタのタイプ、ディスク ドライブの数とサイズ、およびポート) についてシステムに問い合わせます。これらの情報は後でレジストリに記録されます。次に、Ntldr は、カーネル初期化に必要なファイル、つまり、システムをブートするのに必要な、ntoskrnl.exe (カーネル)、HAL.DLL (Hardware Abstraction Layer)、ファイル システム ドライバー、およびデバイス ドライバーをブート パーティションからロードします。その後、ntoskrnl.exe が制御を引き継ぎ、ディスクを見つけたあと、ドライバの変更があればレジストリを更新します。

これらのフェーズが正常に終了すると、残りのシステム ドライバー ファイルおよび Session Manager Subsystem (SMSS) がロードされ、User モード インターフェイスを作成するのに必要なファイルがロードされます。この時点で、ユーザーはログインできます。図 1 に、ブート プロセスの概要を示します。

図 1: Windows のブート プロセス



¹ Master Boot Record の略

IA-64

Windows Server 2003 は Extensible Firmware Interface (EFI) BIOS によって 64 ビットのアドレス指定をサポートし、IA-32 の INIT13 メカニズムを使用しないので、どのデバイスからでもブートできます。IA-64 では、ドライブは新しいパーティション テーブルを使用します。つまり、GPT または GUID パーティション テーブルです。EFI loader は Ntldr の機能を置き換えます。ハードウェアの検出は、Ntdetect ではなく、ファームウェアが行います。また、ハードウェアの検出には、デバイス パス (WWN と 8 ビットの LUN 番号) とディスク シグネチャが使用されるので、以前よりも簡単にできます。

ブート タイプ

ローカル ブート

最も一般的なブート タイプは、直接接続されたディスクからのブートです。SCSI BIOS には、サーバーがブート ディスクを決定するときに使用される命令が含まれています。

ネットワーク ブート

ネットワーク ブートでは、システムは、ローカル エリア ネットワーク (LAN) 経由でリモート ブート サーバーからブートされます。ネットワーク アダプタ (NIC) には、ブートに必要な命令が含まれています。ネットワークからブートできるという利点がありますが、セキュリティのリスクについて十分な考慮する必要があります。

SAN からのブート

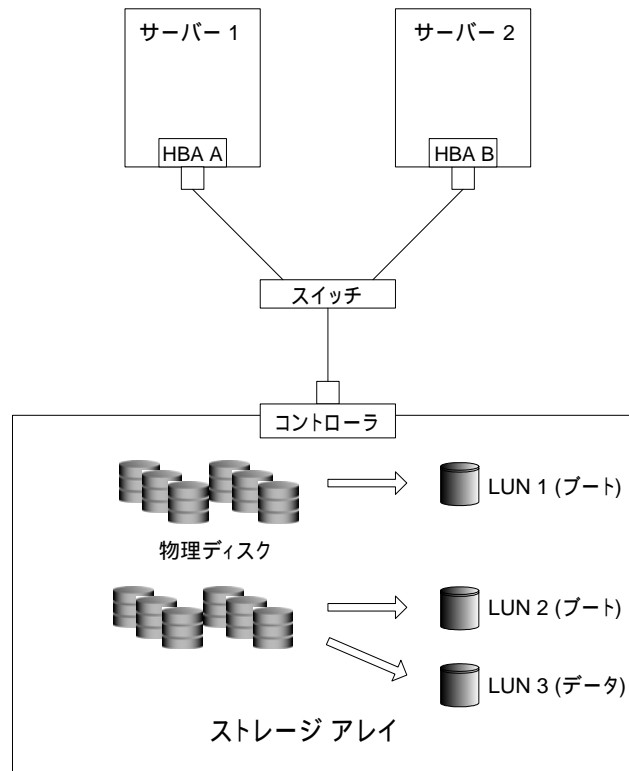
ストレージ エリア ネットワーク (SAN) からブートするとき、ブート ディスクは SAN 上にあります。サーバーと SAN 間の通信は、ホスト バス アダプタ (HBA) 経由で行われます。HBA BIOS には、サーバーが SAN 上にあるブート ディスクを見つけるために必要な命令が含まれています。

SAN からのブート

ブート プロセスとブート タイプについての説明は以上です。ここからは、SAN からの Windows のブートについて詳細に説明します。SAN からのブートは、2 つのサーバーを 1 つのスイッチに接続して、そのスイッチをファイバ チャネル アレイの単一のポートに接続するような簡単なものや、クラスタ環境に複数のシステムを複数のバス (HBA、スイッチ、アレイ コントローラ) 経由で SAN に接続する、マルチバス設定を導入した非常に複雑なものもあります。

図 2 に、2 つのサーバーを接続する基本的な SAN を示します。この SAN では、2 つのサーバーが同じポート (LUN 0) 経由で、同じストレージ アレイからブートします。LUN 1 と LUN 2 は、それぞれのサーバーのブート ディスクです。マスキングを使用して、各サーバーが必ず自分のブート LUN だけにアクセスするようにします。すなわち、サーバー 1 は LUN 1 だけにアクセスするなどです。

図 2: 基本的な SAN



クラスタ環境でのブート

Microsoft は、Windows 2000 (アップデートしたバージョン) と Windows Server 2003 での SAN からのブートをサポートします。しかし、Windows 2000 では、ストレージ デバイスは、クラスタ管理デバイス (ブート ディスク、システム ディスク、およびページファイル ディスク) とは異なるバス上にある必要があります。Windows Server 2003 の Storport ドライバーを導入すると、ブート ディスク、システム ディスク、およびページファイル ディスクは、その他のディスク (クラスタ ディスクを含む) と同じバスを共有することができます。これにより、クラスタ内で SAN からブートするときの必要なハードウェアが減るので、より安価で柔軟なソリューションになります。Windows 2000 で SCSIport ドライバーを使用するクラスタでは、ブート ディスクと共有クラスタ ディスクが同じバスを共有しないように、クラスタ ノードごとに少なくとも 2 つの HBA が必要になります。そして、他のクラスタ ノードが共有ディスクにはアクセスでき、別のサーバーのブート ディスクにはアクセスできないように、共有クラスタ ディスクをブート ディスクからマスクまたはゾーン化により隔離する必要があります。マルチバス機能を実装する場合には、システムごとに必要な HBA は最低 4 つ必要になります。2 つはシステム ディスクとブート ディスク用で、もう 2 つはクラスタ ディスク用です。このソリューションは価格もあがりますが、各サーバーで使用可能な HBA スロットの数によっても制限を受けます。Storport ドライバーを使用すれば、この制限が少なくなり、設定も楽になります。

Windows Server 2003 クラスタ サーバーには、クラスタ ディスクを含む任意のディスクと、システム ディスク、ブート ディスク、またはページファイル ディスクによる同じバスの共有をサポート可能にできる設定があります。これは実装を完全に理解していないユーザーが間違っても有効にしないように設けられました。この機能を有効にするには、レジストリキー (HKLM\SYSTEM\CurrentControlSet\Services\ClusSvc\Parameters\ManageDisksOnSystemBuses) を設定する必要があります。

VERITAS Storage Foundation for Windows では、Windows 2000 と Windows Server 2003 の両方で、この機能をユーザーが簡単に有効にできるようになります。つまり、コマンドライン ユーティリティ vxclus を使用して、システムま

たはブート ディスクとクラスタ ディスク グループのディスクが同じバスを共有できるように、レジストリの設定を変更します。Windows 2000 では正しい HBA ドライバーを使用する必要がありますので注意してください。Microsoft は、Windows 2000 でのブート ディスクとクラスタ ディスクの同じバスの共有をサポートしていませんが、この制限はユーザーの要望によってなくなりました。

VERITAS Storage Foundation for Windows では、32 ビットと 64 ビットの両方の環境において、コマンドライン ユーティリティを使用して SAN からのブートのサポートを有効または無効にできます。コマンドライン ユーティリティ、vxclus は次のように使用します。

vxclus UseSystemBus ON

クラスタ ディスクとシステム/ブート ディスクによる同じバスの共有のサポートを有効にします。

vxclus UseSystemBus OFF

クラスタ ディスクとシステム/ブート ディスクによる同じバスの共有のサポートを無効にします。

Dynamic Multi-Pathing (DMP)

SAN からのブートに関する文書 ([Q305547](#))において、Microsoft はマルチパス機能について次のように述べています。

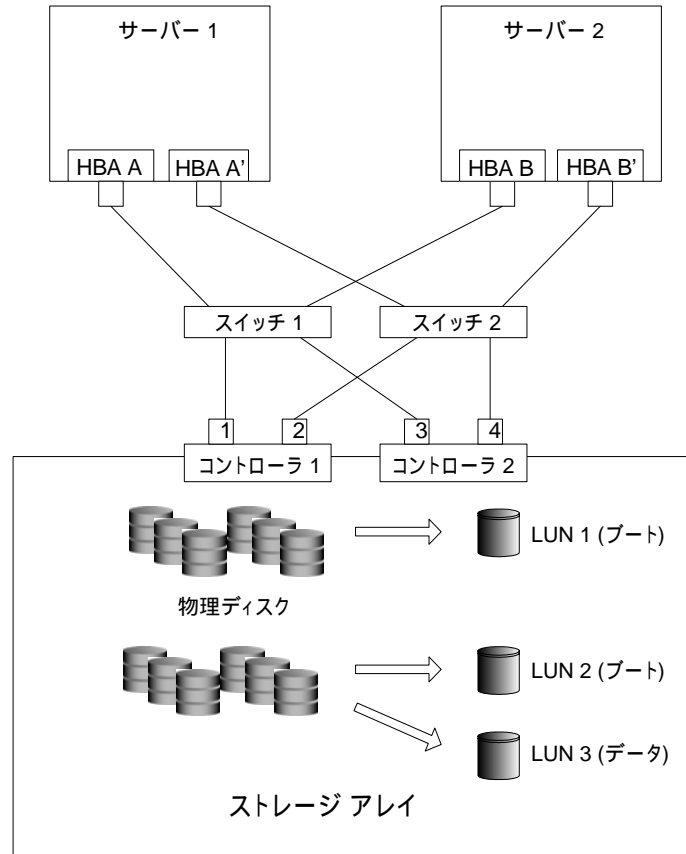
「マルチパス ソフトウェアと複数の HBA は、パス障害から復旧できる可能性を向上します。単一のホストで複数の HBA を持つ目的は、冗長性および、スループット向上の可能性のためです。」

VERITAS Storage Foundation for Windows のマルチパス機能は Dynamic Multi-Pathing (DMP) のオプションとして提供され、Volume Manager の機能の 1 つとして利用できます。DMP を使用すると、セカンダリ パス (冗長化した HBA、配線、スイッチ、アレイ コントローラ、および各コントローラのポート) を導入することによって、SAN 上のブート ディスクへのパスに冗長性を提供するとともに、スループットを向上させることができます。マルチパス設定では、適切なマスキングを実装して、各サーバーが、各 HBA を介して SAN 上にある自分のブート ディスクだけを認識できるようにする必要があります。1 つの LUN だけがブート LUN になるように、1 つの HBA だけでサーバーごとにその BIOS を有効にする必要があります。プライマリ HBA に障害が発生した場合、冗長化した HBA からブートするには、BIOS を手動でリセットする必要があります。図 3 では、HBA A はサーバー 1 のアクティブなアダプタで、HBA A' はスタンバイ (予備) のアダプタです。HBA A に障害が発生した場合、HBA A' がブート LUN を見つけて、そこからシステムを起動できるように、HBA A' 上の BIOS を有効にする必要があります。

VERITAS Storage Foundation 4.3 for Windows は Microsoft の MPIO と StorPort ドライバーを VERITAS Device Specific Module (DSM) 経由でサポートします。DMP 環境での SAN からのブートは MPIO によってのみサポートされます。VERITAS DSM と StorPort ドライバーは必須です。

マルチパス設定で SAN からブートする場合は、クラッシュ ダンプ ファイルの作成に関する問題があります。これは、ブート時に作成され、クラッシュ ダンプ ファイルよりも先に作成されるクラッシュ ダンプ スタックが、システムをブートする HBA パスに特有であるためです。マルチパス環境でのクラッシュ ダンプ ファイルの詳細については、Microsoft のホワイトペーパー「Boot from SAN in Windows Server 2003 and Windows 2000 Server」を参照してください。

図 3: SAN マルチパス設定からのブート



潜在的な問題と解決方法

SAN からの Windows のブートに関する潜在的な問題は、ページファイルへのアクセスです。OS はページファイルに高速で制限なくアクセス可能である必要があります。SAN 環境では、複数のシステムが同時にページングを行ったり、同じストレージポート経由でブートしたりするので、システムがハングしたり、パフォーマンスが落ちたりする場合があります。

ページファイルをローカルストレージに置くと、この問題を解決できます。しかし、Windows で STOP エラーが発生した際に、ページファイルがブートパーティション/ボリュームとは異なるパーティション/ボリュームにある場合には、メモリーダンプファイル (Memory.dmp) が作成されません。メモリーダンプは、Windows の STOP エラーを解析するときに使用します。Dell は、『[Disaster Recovery with the PowerVault 530F](#)』で、SAN からブートされるサーバーごとに SCSI ドライブをインストールして、そのドライブのページファイルだけが格納されるように設定することを推奨しています。

ストレージアレイ (ファームウェアなど) をアップグレードするときには、ストレージアレイを停止する必要がある場合があります。このような場合、アレイがホストするアプリケーションだけが停止するのではなく、ホストそのものが停止します。この状態を回避するには、ブートボリュームを別のアレイにミラーリングします。

もう一つの潜在的な問題は、今日では、障害を特定することにはそのトラブルシューティングも含まれることがあるということです。すなわち、このような環境では、ホストや OS だけではなく、SAN 自身が問題の原因である可能性もあります。

まとめ

SAN からのブートは、設定が複雑ですが、いくつかの利点があります。たとえば、ハードウェアの統合、集中管理、サーバー障害からの簡単な回復、そして災害からのすばやい復旧などがそうです。VERITAS Storage Foundation for Windows を使用すると、ブートディスクとクラスタディスクが同じバスを共有できるので、クラスタ環境での SAN ブート設定が簡単になります。これによって、ハードウェアの要件を減らし、具体的な設定するときの複雑さを緩和できます。Microsoft は、Windows 2000 でのブートディスクとクラスタディスクのバスの共有をサポートしていませんが、Windows Server 2003 では、Storport ドライバーを使用することでサポートしています。ブートディスクを別のアレイにレプリケーション（複製）/ミラーリングすれば、アレイに障害が発生した場合でも、ブートディスクの冗長性が確保されます。そして、Dynamic Multi-Pathing (DMP) を使用すると、ストレージバスの障害に対する保護レベルが向上します。

参考資料

このドキュメントは、次の資料を参考にして作成しています。

Boot from SAN in Windows Server™ 2003 and Windows® 2000 Server	Microsoft
Server Clusters : Storage Area Networks Windows 2000 and Windows Server 2003	Microsoft
Storport in Windows Server™ 2003: Improving Manageability and Performance in Hardware RAID and Storage Area Networks	Microsoft
Microsoft Knowledge Base 文書 - 305547 : Support for booting from a Storage Area Network	
Booting Windows from the SAN	Rick Cook
Disaster Recovery with the PowerVault 530F	Mike Kosacek と Juan Montuno (DELL)

詳細な製品情報につきましては、弊社の Web サイト (www.veritas.com/jp) をご覧ください。

Copyright © 2005 Symantec Corporation. All rights reserved. Symantec, Symantec ロゴ, VERITAS は米国における Symantec Corporation およびその関連会社の登録商標です。その他の会社名、製品名等は、それぞれ各社の商標または登録商標です。製品の仕様、性能等は予告なく変更する場合がありますので、ご了承ください。

株式会社シマンテック

〒150-0031 東京都渋谷区桜丘町 20-1 渋谷インフォスター
☎0120-402-665 (受付時間 平日 9:30 - 12:00, 13:00 - 18:00)
FAX.03-5532-0887
www.veritas.com/jp

お問い合わせ先