Microsoft | Desktop Virtualization

Windows Thin PC

Enhanced Write Filter

目次

Enhanced Write Filter 2
EWF の概要 2
EWF のシステム要件 3
EWF アーキテクチャ 4
EWF ボリュームの構成 4
EWF モード 5
EWF RAM モード 5
EWF RAM モードの構成 6
EWF RAM Reg モード 7
EWF RAM Reg モードの構成 8
EWF の設計に関する考慮事項 8
EWF の保守と管理 9
EWF Manager コマンド 9
EWF で保護されたランタイム イメージへの更新プログラムのインストール 13
書き込みフィルターと夏時間の自動調整 14
EWF のパフォーマンスに関する考慮事項 14
イベント ログの場所の変更 15
ページファイルの場所の変更 15
一時ファイル フォルダーの場所の変更 15
前回アクセス時のタイム スタンプの無効化 16
Prefetch の無効化 16
SuperFetch の無効化 17
EWF と File-Based Write Filtering 17

© 2011 Microsoft. All rights reserved.

Enhanced Write Filter

Enhanced Write Filter (EWF) では、ランタイム イメージを書き込み禁止にできる機能を提供します。すべての書き込み要求を RAM にリダイレクトすることで、EWF では書き込み可能なランタイム イメージの外観を保つことができます。

このセクションの内容

EWF の概要

Enhanced Write Filter の概要を示します。この概要では、EWF のアーキテクチャ、および EWF のサポートに必要なコンポーネントについて説明します。

EWF モード

EWF のさまざまなモード、および各種モードの実装方法について説明します。

EWF の設計に関する考慮事項

EWF で保護されたランタイム イメージを構成および展開する前の考慮事項について説明します。

EWF の概要

Enhanced Write Filter (EWF) は、書き込みアクセスからボリュームを保護します。EWF は、システムの 1 つまたは複数のパーティションを書き込み保護します。

また、多数のメディア タイプおよび構成に展開できます。

重要

EWF は、"リムーバブル" としてマークされているメディアを保護することはできません。EWF が保護できるのは、"固定" としてマークされているメディアのみです。

EWF の 2 つの主なコンポーネントは、EWF オーバーレイと EWF ボリュームです。

- EWF オーバーレイ: EWF はすべての書き込み操作を別の記憶域の場所にリダイレクトし、ボリュームの内容を保護します。この場所をオーバーレイと呼びます。EWF オーバーレイは RAM に配置されます。オーバーレイの概念は、オーバーヘッド プロジェクターの透明オーバーレイと似ています。オーバーレイに行う変更は集合体で表示される画像に影響を及ぼしますが、オーバーレイが削除されると、基本の画像は変更されないまま残ります。
- EWF ボリューム: EWF には、EWF ボリュームの構成に基づく 2 種類の EWF モードがあります。

EWF モード	EWF オーバーレイの場所	EWF ボリュームの場所	説明
RAM	RAM 内	ディスク上の非パーティション領域に作成	EWF はオーバーレイ情報を RAM に保存します。システムを再起動すると、オーバーレイのすべての情報が破棄されます。 再起動後に書き込み情報を破棄する場合、またはオーバーレイのメディアへの書き込みを遅らせる場合は、システムで EWF RAM の種類を使用します。 詳細については、「EWF RAM モード」を参照してください。

EWF モード	EWF オーバーレイの場所	EWF ボリュームの場所	説明
RAM Reg	RAM 内	システム レジストリ内	EWF RAM の種類と同様、RAM Reg オーバーレイでもオーバーレイ情報を RAM に保存します。ただし、EWF に関する構成情報は、別の EWF ボリュームではなく、レジストリ内に保存されます。 メディアのパーティション構造の変更をサポートしないメディアで EWF RAM Reg の種類を使用します。 詳細については、「EWF RAM Reg モード」を参照してください。

このセクションの内容

EWF のシステム要件

EWF で必要とされるシステム構成について説明します。

EWF アーキテクチャ

EWF ドライバー アーキテクチャについて説明します。

EWF ボリュームの構成

EWF ボリュームの処理と構成について説明します。

EWF のシステム要件

EWF で保護されたランタイム イメージを展開する前に、ご使用のシステムが次の要件を満たしていることを確認してください。

EWF セットアップのパーティション要件

- EWF RAM モードの場合は、Enhanced Write Filter (EWF) を構成するディスクのプライマリ パーティションの数が 3 つ以内であることを確認します。ディスクに作成できるプライマリ パーティションの数は合計 4 つです。論理パーティションを使用する場合は、拡張パーティション内に EWF 用の空き領域が確保されている必要があります。
  次のいずれかの領域で、最小 8 MB の容量が使用可能であることを確認してください。
  - プライマリ パーティションの直後
  - 拡張パーティション内

  メモ

  拡張パーティション外のディスクの最後に容量がある場合でも、EWF ボリュームは EWF によって拡張パーティション内に作成されます。

RAM REG モードを使用している場合、この容量は必要ありません。

EWF ボリュームの詳細については、「EWF ボリュームの構成」を参照してください。

- ディスク パーティション構成は簡素にしてください。複雑なディスク パーティションでは、EWF のセットアップが適切に行われないことがまれにあります。EWF を初めて構成する場合はなるべく、1 つのディスクで 1 つのプライマリ パーティションを使用してください。

EWF のメディア要件

- EWF では、ダイナミック ディスクは保護されません。保護されているすべてのボリュームをベーシック ディスクとして構成する必要があります。
- コンパクトフラッシュのように、リムーバブルとしてマークされているメディアでは、EWF ボリュームを作成することはできません。一部のコンパクトフラッシュ メーカーは、メディアを固定としてマークするためのユーティリティを提供しています。このユーティリティにより、EWF ボリュームを作成することが可能になります。また、必要に応じて、EWF RAM Reg モードを使用して、EWF ボリュームの要件をバイパスすることもできます。詳細については、「EWF RAM Reg モードの構成」を参照してください。

EWF アーキテクチャ

Enhanced Write Filter (EWF) は、ボリューム スタックの下位フィルター ドライバーです。ファイル システムと、物理ディスクとインターフェイスをとるクラス ドライバーの間にあります。

EWF Manager (EWFMGR) は、EWF を管理するコマンドライン インターフェイスを提供するコンソール アプリケーションです。

Enhanced Write Filter ドライバーの Ewf.sys は、EWF オーバーレイに書き込み I/O 要求パケット (IRP) をリダイレクトします。EWF オーバーレイは、RAM に保存できる書き込みキャッシュです。読み取り専用の IRP によって、EWF ドライバーが現在のオーバーレイ スタックの一致項目を検索します。オーバーレイでそのセクターが見つかると、オーバーレイからのデータが返されます。そうでない場合は、保護されているボリュームからのデータが返されます。

EWF ボリュームは、現在の EWF 構成に関するメタデータを保存します。オーバーレイについては、保護されているボリュームに関する情報も保存します。

EWF の種類とオーバーレイ構成の詳細については、「EWF モード」を参照してください。

EWF ボリュームの詳細については、「EWF ボリュームの構成」を参照してください。

EWF ボリュームの構成

EWF インストーラー プロセス中に EWF の構成を行う場合、メディア上に小さいパーティションが作成されます。このパーティションは、EWF ボリュームと呼ばれます。EWF ボリュームには、デバイス上の EWF で保護されているボリュームに関する構成情報が保存されます。その情報には、保護されているボリュームの数、サイズ、オーバーレイ レベルなどが含まれます。システム内のディスク数に関係なく、デバイスには 1 つの EWF ボリュームのみが作成されます。

次の一覧に、EWF ボリュームの構成要件を示します。

- EWF RAM モードの場合、EWF ボリュームは 64 KB 未満です。RAM ベース オーバーレイの EWF ボリュームには、システムの再起動時に適用される EWF enable や disable などの追加起動コマンドが保存されます。
- EWF RAM Reg モードの場合、EWF ボリューム内に保存される構成情報は、EWF ボリュームの代わりにレジストリ内に保存されます。RAM Reg モードは、EWF ボリュームの新しいパーティションを作成できない場合に便利です。

EWF インストーラー フェーズ中に、EWFcfg.dll は メディア上に EWF ボリュームを作成します。EWF ボリュームは、メディア上の次の 2 種類の領域のいずれかに作成されます。

- プライマリ パーティションの直後
- 拡張パーティション内の空き領域の中

メモ

システム上で拡張パーティションが利用可能な場合、EWF は、ディスクの終端に空き領域があったとしても、必ず拡張パーティション内の空き領域に EWF ボリュームを作成しようとします。拡張パーティションがある場合は、パーティション内に EWF ボリューム用の領域があることを確認してください。

メモ

ディスク オーバーレイは、ドライブ上に事前 EWF インストーラー ランタイムを再展開する前に、無効にする必要があります。無効にされていない場合、EWF は、EWF インストール フェーズ中にそれらの EWF ボリュームの削除および再作成を実行できなくなります。この手順を実行しないと、次のシステムの起動中に、エラー "missing or corrupted hal.dll" が返されます。

ご使用のメディアが、EWF ボリュームの作成をサポートできることを確認してください。コンパクトフラッシュ デバイスなど、リムーバブルとしてマークされている一部のメディアでは、新しいパーティションの作成が許可されていません。ただし、メディアが固定としてマークされている場合は、複数のパーティションを作成できます。一部のコンパクトフラッシュ メーカーは、メディアを固定としてマークするためのユーティリティを提供しています。

また、既存のボリュームに割り当てられているドライブ文字がオペレーティング システムによって変更されないようにするには、次の規則に従って EWF ボリュームを作成します。拡張ボリュームが十分な容量のあるドライブ上に存在する場合、EWF ボリュームは論理ボリュームとして作成されます。ドライブの容量が不十分な場合、EWF ボリュームはプライマリ ボリューム内に作成されます。

メディア上で新しいパーティションを作成できない場合、またはメディアのパーティション構造を変更できない場合は、EWF RAM Reg モードを実装することを検討してください。詳細については、「EWF RAM Reg モード」を参照してください。

以下に、EWF ボリュームの構成時に発生することの多い問題をいくつか示します。

- ディスク上に既に 4 つのプライマリ パーティションがある。ディスクには、5 つ以上のプライマリ パーティションを作成することはできません。
- プライマリ パーティションの直後に空き領域がない。
- 拡張パーティション内に空き領域がない。EWF ボリュームは、拡張パーティションの直後に作成することはできません。
- 削除されなかった既存の EWF ボリュームがある。

EWF モード

EWF には、EWF ボリュームの実装に基づく 2 種類の EWF モードがあります。EWF はオーバーレイ データを RAM に保存します。EWF ボリュームは、メディア上の非パーティション領域またはシステム レジストリ内に配置できます。詳細については、「EWF の概要」を参照してください。

HORM の設定で Enhanced Write Filter (EWF) を構成する際に、EWF オーバーレイのモードを選択します。また、EWF RAM Reg モードでは、ランタイム イメージの展開後に追加の構成設定が必要です。

このセクションの内容

EWF RAM モード

EWF RAM モードを使用するタイミングおよび構成方法について説明します。EWF RAM モードでは、RAM にオーバーレイ データが保存され、ディスク上の非パーティション領域に EWF ボリュームが保存されます。

EWF RAM Reg モード

EWF RAM Reg モード、EWF RAM モードとの相違、および追加の構成に関する詳細について説明します。EWF RAM Reg モードでは、RAM にオーバーレイ データが保存され、システムのレジストリに EWF ボリュームが保存されます。

EWF RAM モード

EWF RAM モードでは、次の構成が使用されます。

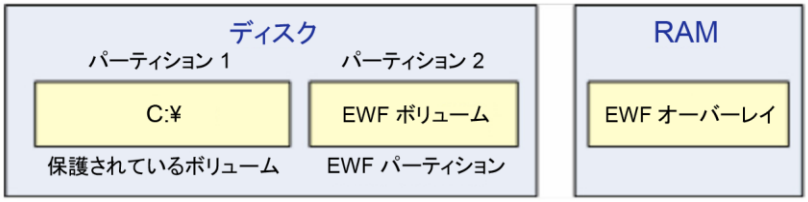
- EWF オーバーレイ タイプは RAM に保存されます。
- EWF ボリュームはディスクに保存されます。

EWF RAM オーバーレイは、書き込みキャッシュを RAM に保存します。EWF インストーラー フェーズ中に、EWF RAM モードが構成されると、EWF ボリュームがメディア上の利用可能な領域に作成されます。EWF ボリュームには、EWF マスター ボリューム テーブル、およびシステム メモリ内のオーバーレイ データをポイントするオーバーレイ スタックが保存されます。ターゲット システムをシャットダウンすると、システム メモリ内のオーバーレイ データは失われます。EWF RAM モードでは、1 つのオーバーレイ レベルのみがサポートされます。

EWF RAM モードは、次のようなシナリオで使用します。

- 読み取り/書き込みボリュームのデータを、変更または破損から保護する場合
- ステートレス デバイスにランタイム イメージを展開する場合
- 永続読み取り/書き込み領域のないデバイスにランタイム イメージを展開する場合

次の図に、EWF RAM モード構成の例を示します。



EWF RAM オーバーレイで書き込みキャッシュを保存するには、追加の RAM が必要です。EWF は RAM を事前に割り当てません。そのため、EWF は、システムがメモリ不足になるまで、RAM の空き領域を使用します。EWF RAM オーバーレイの RAM 要件はさまざまであり、オーバーレイに対する書き込み操作の量によって異なります。

詳細については、「EWF RAM モードの構成」を参照してください。

EWF RAM モードの構成

EWF RAM モードでは、オーバーレイ データがシステム メモリに保存されます。オーバーレイは RAM に保存されるため、システムに加えられた書き込み操作の数によっては、デバイスに追加の RAM が必要になる場合があります。また、データ キャッシュが揮発性メモリに保存されるため、データ キャッシュはシステム再起動時に失われます。

EWF RAM モードを構成するには

1. イメージを展開し、デバイスを起動します。EWF インストーラーによって、デバイスに EWF コンポーネントが追加されます。Ewfcfg.exe ツールは、EWF セットアップを処理する Ewfcfg.dll へのプロキシです。Ewfcfg.dll によって、応答ファイルからの構成設定が読み込まれ、適用されます。
2. インストール プロセスが完了したら、次のコマンドラインを入力して、EWF の状態を確認します。

   ```
   ewfmgr -all
   ```

   既定では、EWF によって、EWF がすべてのドライブで無効になっていることが報告されます。
3. 次のコマンドラインを入力して、EWF を有効にします。

   ```
   ewfmgr c: -enable
   ```
4. システムを再起動します。
5. コマンド プロンプトで次のコマンドを入力して、EWF が正しく構成されていることを確認します。

   ```
   ewfmgr c:
   ```

   Ewfmgr.exe によって、EWF が有効になっていることが報告され、EWF RAM オーバーレイの現在の状態が提供されます。

EWF RAM Reg モード

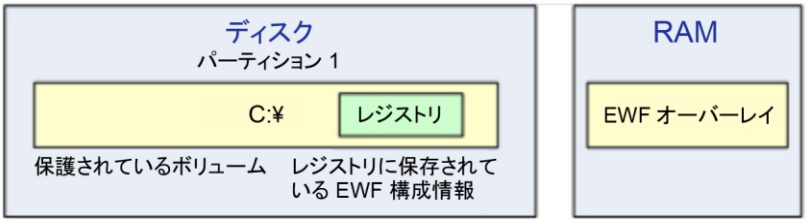
EWF RAM Reg モードは、EWF RAM モードに似ています。標準の EWF RAM モードと異なるのは、EWF ボリュームに保存される構成情報が、システムのレジストリに保存されるという点だけです。EWF RAM Reg モードでは、次の構成が使用されます。

- EWF オーバーレイは RAM に保存されます。
- EWF ボリュームはシステムのレジストリに保存されます。

RAM Reg モードは、次のようなシナリオで使用します。

- パーティションが 1 つしかないメディア、またはパーティション分割できないメディアを保護する場合
- コンパクトフラッシュ、USB、IEEE 1394 デバイスなどのリムーバブル メディアを保護する場合
- 標準の RAM オーバーレイがサポートされないメディアを保護する場合
- コンパクトフラッシュなど、書き込み回数の制限されているデバイスの書き込み操作回数を減らす場合

次の図に、デバイスでの EWF RAM Reg モードの構成例を示します。



EWF ボリューム情報はレジストリに保存されるため、レジストリが書き込み保護されていると、EWF を無効にしようとしても失敗します。EWF Ram Reg モードの EWF を無効にするには、次の 3 つの方法があります。

- EWF を無効にしてから、保護されているボリュームにオーバーレイをコミットします。
  例:
  ```
  ewfmgr c: -disable
  ewfmgr c: -commit
  ```

警告

上記のシナリオでは、システムを再起動する必要があります。これは、次のシステム再起動時にオーバーレイが保護されているボリュームに書き込まれるためです。

- または -

- CommitandDisable コマンドを使用して、EWF を無効にし、オーバーレイをコミットします。
  例:
  ```
  ewfmgr c: -commitanddisable
  ```

警告

上記のシナリオでは、システムを再起動する必要があります。これは、次のシステム再起動時にオーバーレイが保護されているボリュームに書き込まれるためです。

- または -

- CommitandDisable コマンドの -live オプションを使用して、システムを再起動せずに EWF を無効にし、オーバーレイを保護されているボリュームにコミットします。
  例:
  ```
  ewfmgr c: -commitanddisable -live
  ```

詳細については、「EWF Manager コマンド」を参照してください。

EWF RAM Reg モードの構成方法の詳細については、「EWF RAM Reg モードの構成」を参照してください。

また、EWF RAM Reg モードを使用して複数のボリュームを保護することもできます。

EWF RAM Reg モードの構成

EWF RAM Reg モードでは、RAM にオーバーレイ データが保存され、レジストリに EWF 構成情報が保存されます。EWF RAM オーバーレイでは、RAM にデータ キャッシュが保存されるため、デバイスに追加の RAM が必要になる場合があります。また、データ キャッシュが揮発性メモリに保存されるため、データ キャッシュはシステム再起動時に失われます。

さらに EWF 構成情報はレジストリに保存されますが、これは通常 EWF によって保護されています。そのため、ewfmgr -commitanddisable コマンドを使用して変更を EWF に適用する必要があります。

EWF RAM モードを構成するには

1. イメージを展開し、デバイスを起動します。EWF インストーラーによって、デバイスに EWF コンポーネントが追加されます。Ewfcfg.exe ツールは、EWF セットアップを処理する Ewfcfg.dll へのプロキシです。Ewfcfg.dll によって、応答ファイルからの構成設定が読み込まれ、適用されます。
2. インストール プロセスが完了したら、次のコマンドラインを入力して、EWF の状態を確認します。
   `ewfmgr -all`
   既定では、EWF によって、EWF がすべてのドライブで無効になっていることが報告されます。
3. 次のコマンドラインを入力して、EWF を有効にします。
   `ewfmgr c: -enable`
4. システムを再起動します。
5. コマンド プロンプトで次のコマンドを入力して、EWF が正しく構成されていることを確認します。
   `ewfmgr c:`
   Ewfmgr によって、EWF が有効になっていることが報告され、EWF RAM オーバーレイの現在の状態が提供されます。

メモ

中間のハード ディスクを使用している場合、EWF が正しく構成されていることを確認した後で、ランタイム イメージをコンパクトフラッシュ デバイスにコピーします。

EWF の設計に関する考慮事項

このセクションでは、Enhanced Write Filter (EWF) の一般的な設計に関する考慮事項を考察します。

このセクションの内容

EWF の保守と管理

EWFMGR コマンドを使用して EWF を管理する方法について説明します。このコマンドにより、EWF で保護されたランタイム イメージに更新プログラムをインストールできます。

EWF のパフォーマンスに関する考慮事項

EWF のパフォーマンスを向上させる方法について説明します。

EWF と File-Based Write Filtering

EWF と File-Based Write Filtering (FBWF) の関連性について説明します。

EWF の保守と管理

EWF Manager ツールを使用して、EWF を有効化/無効化したり、保護されているボリュームにオーバーレイをコミットしたりできます。EWF Manager コマンドを使用して、EWF を無効にし、ランタイム イメージに更新プログラムを適用することができます。

このセクションの内容

EWF Manager コマンド

EWF Manager コマンドのコマンド構文について説明します。

EWF で保護されたランタイム イメージへの更新プログラムのインストール

保護されたランタイム イメージにアプリケーションや QFE をインストールする際に従うプロセスや考慮すべき事柄について説明します。

書き込みフィルターと夏時間の自動調整

書き込みフィルターの使用時に夏時間を処理するための推奨方法について説明します。

EWF Manager コマンド

EWF Manager コンソール アプリケーションを使用して、Enhanced Write Filter (EWF) を制御します。EWF Manager は、次の構文を使用します。

構文

EWFMGR [`<volume-name>`*](optional) [`options`]

パラメーター

*<volume-name>**

ボリューム名には、ドライブ文字 (C: など)、デバイス名 (¥Device¥Harddiskvolume など)、または "¥¥?¥Volume{GUID}¥" 形式の (ここで、GUID はボリュームを識別するグローバル一意識別子を表す) ボリューム GUID パス (¥¥?¥Volume{26a21bda-a627-11d7-9931-806e6f6e6963}¥ など) のいずれかを指定できます。

GUID を使用したボリュームの参照は、ボリュームの識別を難しくする要素を回避できるので、より信頼性が高くなります。たとえば、同じラベルを持つ 2 つのボリューム、ドライブ文字やラベルを持たないボリューム、ボリュームに応じて変わるドライブ文字などが、コンピューターで追加されたり削除されたりする場合です。詳細については、「Naming a Volume」を参照してください。ボリュームの GUID ボリューム パスを取得する方法は、「GetVolumeNameForVolumeMountPoint Function」を参照してください。

この名前は、Windows エクスプローラーでドライブ文字の前に表示されるボリューム ラベルではないことに注意してください。

<volume-name> が指定されていない場合、既定の動作では、EWF ボリュームの構成に関する情報が表示されます。保護されているボリュームの状態を表示するには、ewfmgr c: のように、保護されているボリュームのドライブ文字を指定します。

```
ewfmgr ¥¥?¥GLOBALROOT¥Device¥HarddiskVolume1
```

メモ

複数のボリュームを指定することが可能です。volume-name は、デバイス名、GUID ボリューム パス、またはドライブ文字とコロンを使用して指定できます。

メモ

volume-name パラメーターの代わりに **-all** コマンドを使用して、指定した操作をすべてのボリュームに実行することもできます。たとえば、すべてのボリュームで EWF を有効にするには、次のように入力します: `ewfmgr -all -enable`

重要

ディスクにバックアップされたオーバーレイの操作はサポートされていません。

options

EWF ボリュームの起動オプションを指定します。

保護されているボリュームの構成を管理するには、**Disable**、**Enable**、**Commit**、**CommitandDisable**、**Persist**、**ActivateHORM**、**DeactivateHORM**、および **Nocmd** コマンドを使用します。

注釈

次の表に、Enhanced Write Filter (EWF) コンソール マネージャー アプリケーション ツールの起動コマンドを示します。

起動コマンド	説明
All	保護されているすべてのボリュームに指定されたコマンドを実行します。
Commit	オーバーレイの現在のレベルのすべてのデータを保護されているボリュームにコミットし、現在のオーバーレイ レベルを 1 にリセットします。**Commit** コマンドを **Disable** コマンドと組み合わせて、コミットしてから無効にすることもできます。 オーバーレイは、次のシステム起動時に保護されているボリュームに書き込まれます。オーバーレイをコミットすると、起動処理速度に影響を与える可能性があります。
CommitandDisable	オーバーレイの現在のレベルのすべてのデータを保護されているボリュームにコミットしてから、オーバーレイを無効にします。 オーバーレイは、次のシステム起動時に保護されているボリュームに書き込まれます。オーバーレイをコミットすると、起動処理速度に影響を与える可能性があります。 EWF RAM モードと EWF RAM Reg モードの両方に **-live** コマンドを使用すると、保護されているボリュームにすぐにオーバーレイをコミットし、システムを再起動せずにオーバーレイを無効にすることができます。 例: `ewfmgr c: -commitanddisable -live`
Disable	保護されている指定のボリュームでオーバーレイを無効にします。 **重要** RAM REG モードで Disable コマンドを使用すると、変更はレジストリまでは保持されません。RAM REG モードの場合は、**-CommitAndDisable** コマンドを使用する必要があります。
Enable	書き込みフィルターを有効にして、保護されているメディアに書き込まれるデータがオーバーレイでキャッシュされるようにします。EWF が起動するとすぐ現在のオーバーレイのレベルは 1 になり、新しいオーバーレイはレベル 1 で作成されます。
NoCmd	現在保留中のコマンドをクリアします。
Persist	保護された指定のボリュームのすべてのオーバーレイで永続する 64 バイトのフィールドを指定します。Persist コマンドを使用すると、EWF 固有の状態情報やアプリケーションの状態情報を保存することができ、デバイスを更新する際に便利です。永続的なデータは、EWF ボリューム ストアに保存されます。

起動コマンド	説明
ActivateHorm	HORM を有効にします。 **重要** HORM の要件として、すべてのボリュームが EWF で保護されているか、ハイバーネーション状態になるときにすべてのボリュームのマウントが解除された状態であることが必要です。これは、状態の同期に関する問題を回避するためです。ハイバーネーションから再開するたびに、システム全体がハイバーネーション状態になったときとまったく同じ状態になることが求められます。
DeactivateHorm	HORM を無効にします。

EWF Manager コマンドは次の起動時に実行されるため、コマンドを有効にするにはシステムを再起動する必要があります。

例

Microsoft.Win32.RegistryKey#4

次の例は、EWF RAM REG モードがドライブ C を保護するように構成されるシステムを参照しています。

次の例は、EWF の状態と形式を確認する方法を示しています。

```
ewfmgr c:
```

EWF Manager で次の結果が表示されます。

```
Protected Volume Configuration

    Type            RAM(REG)

    State           DISABLED

    Boot Command    NO_CMD

        Param1      0

        Param2      0

    Volume          D 58 55 BF A4 00 00 50 06 00 00 00 00 00 00 00 00

    Volume Name     "¥¥?¥GLOBALROOT¥Device¥HarddiskVolume2" [C:]

    Max Levels      1

    Clump Size      512

    Current Level   N/A

    Memory used for data 0 bytes

    Memory used for mapping 0 bytes
```

次の例は、ドライブ C の EWF を有効にする方法を示しています。

```
ewfmgr c: -enable
```

EWF Manager で、Enable コマンドが保留中と表示されます。コマンドは次の起動時まで実行されません。EWF Manager で次の結果が表示されます。

```
*** Enabling overlay

Protected Volume Configuration

    Type RAM      (REG)

    State         DISABLED

    Boot Command ENABLE

        Param1    0

        Param2    0

    Volume ID     58 55 BF A4 00 00 50 06 00 00 00 00 00 00 00 00

    Volume Name   "¥¥?¥GLOBALROOT¥Device¥HarddiskVolume2" [C:]

    Max Levels    1

    Clump Size    512

    Current LevelN/A

    Memory used for data 0 bytes

    Memory used for mapping 0 bytes
```

次の例は、EWF ボリュームの状態の種類を確認する方法を示しています。

```
ewfmgr -all
```

EWF Manager で次の結果が表示されます。

```
    Type RAM      (REG)

    State         ENABLE

    Boot Command NO_CMD

        Param1    0

        Param2    0

    Volume ID     58 55 BF A4 00 00 50 06 00 00 00 00 00 00 00 00

    Volume Name   "¥¥?¥GLOBALROOT¥Device¥HarddiskVolume2" [C:]

    Max Levels    1

    Clump Size    512

    Current Level1

    Memory used for data 9910272 bytes

    Memory used for mapping 12288 bytes
```

メモ

EWF が無効な場合、**Current Level** は **N/A** と表示されます。

EWF で保護されたランタイム イメージへの更新プログラムのインストール

ボリュームへの書き込みアクセスは Enhanced Write Filter (EWF) によって禁じられているため、アプリケーションをインストールしたり、ランタイム イメージを更新したりする場合には、さらに注意する必要があります。

現在の EWF オーバーレイを無効にするには、**ewfmgr disable** コマンドを使用します。EWF オーバーレイを無効にしたら、システムを再起動して、アプリケーションをインストールする必要があります。

メモ

EWF RAM Reg モードの場合、EWF を無効にするには、**ewfmgr commitanddisable** コマンドを使用する必要があります。**ewfmgr commitanddisable** コマンドにより、アプリケーションのインストールや更新に無関係なものを含めて、オーバーレイのすべての変更が保護されているボリュームに適用されます。ボリュームへの追加の書き込み操作を最小限に抑えるには、アプリケーションをインストールする前にデバイスを再起動することで、オーバーレイ キャッシュを消去します。詳細については、「EWF RAM Reg モード」を参照してください。

更新プログラムを適用するには、次の手順のいずれかを実行する必要があります。

EWF RAM モードで保護されているランタイム イメージを更新するには

1. EWF Manager で次のコマンドを入力して、オーバーレイを無効にします。
   ewfmgr c: -disable
2. システムを再起動します。
3. アプリケーションまたは更新プログラムをインストールします。
4. 必要に応じてインストールが完了し、コンピューターが再起動されるまで待機します。
5. 次のコマンドを使用して、EWF オーバーレイを再度有効にします。
   ewfmgr c: -enable
6. システムを再起動して、EWF オーバーレイを再度有効にします。

EWF RAM Reg モードで保護されているランタイム イメージを更新するには

1. デバイスを再起動して、RAM オーバーレイを消去します。
2. 次のコマンドを入力して、オーバーレイを保護されているボリュームにコミットし、EWF オーバーレイを無効にします。
   ewfmgr c: -commitanddisable
   RAM Reg モードでは、レジストリに EWF 構成データが保存されるので、無効化の変更を保護されているランタイム イメージにコミットする必要があります。詳細については、「EWF RAM Reg モードの構成」を参照してください。
3. システムを再起動して、オーバーレイを無効にします。
4. アプリケーションまたは更新プログラムをインストールします。
5. 必要に応じてインストールが完了し、コンピューターが再起動されるまで待機します。
6. 次のコマンドを入力して、EWF オーバーレイを有効にします。
   ewfmgr c: -enable
7. システムを再起動して、EWF オーバーレイを再度有効にします。

書き込みフィルターと夏時間の自動調整

夏時間 (DST) の自動調整には、File-Based Write Filter (FBWF) および HORM を使用する Enhanced Write Filter (EWF) との適合性がありません。FBWF または EWF が有効な場合に夏時間の自動調整を有効にすると、コンピューターが再起動されるたびに、システム クロックの時間が春には進み、秋には戻ります。

書き込みフィルター使用時の DST に関する問題を解決するための推奨方法は、CMOS クロックを UTC を使用するように変更する方法です。

CMOS クロックを UTC を使用するように変更するには

1. EWF および FBWF が無効になっていることを確認します。
2. Windows システムのタイム ゾーンを希望する値 (太平洋タイム ゾーンなど) に構成します。
3. 次の場所にあるレジストリに RealTimeIsUniversal キーの DWORD 値を追加します。
   HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥TimeZoneInformation¥.
4. RealTimeIsUniversal キーの値を 1 に変更します。
5. システムを再起動して、BIOS にアクセスします。
6. CMOS クロックを現在の UTC 日時に設定します。たとえば、太平洋標準タイムゾーンにいて、現在 11:00 AM の場合は、8 時間の時差があるため、CMOS クロックを 7:00 PM に設定します。
7. システムを再起動して、EWF または FBWF を有効にします。

EWF のパフォーマンスに関する考慮事項

このセクションには、Enhanced Write Filter (EWF) を有効にしてランタイム イメージのパフォーマンスを高める方法に関するトピックが含まれています。

このセクションの内容

イベント ログの場所の変更

システムのイベント ログの場所を保護されていないボリュームに変更する方法について説明します。

ページファイルの場所の変更

システムのページファイルの場所を保護されていないボリュームに変更する方法について説明します。

一時ファイル フォルダーの場所の変更

一時ファイルのディレクトリの場所を保護されていないボリュームに変更する方法について説明します。

前回アクセス時のタイム スタンプの無効化

NTFS の前回のアクセス時のタイム スタンプを無効にする方法について説明します。

Prefetch の無効化

Prefetch を無効にして EWF のパフォーマンスを高める方法について説明します。

SuperFetch の無効化

SuperFetch を無効にして EWF のパフォーマンスを高める方法について説明します。

イベント ログの場所の変更

イベント ログを使うシステムにおける Enhanced Write Filter (EWF) のパフォーマンスを改善するため、イベント ログの場所を EWF で保護されていない別のパーティションに変えることができます。これには、最低 2 つのパーティションが必要です。EWF で保護されたパーティションと、書き込み可能な別のパーティションです。

イベント ログの場所を変更するには

1. イベント ログの場所を保護されていないボリュームに変更するには、ランタイム イメージのレジストリを更新する必要があります。
   次の 3 つのレジストリ キーを変更し、イベント ログの場所を保護されていないボリュームに変更します。
   キー名: **HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥EventLog¥Application¥**
   値名: **File**
   種類: **REG_EXPAND_SZ**
   値: <ボリューム名とパス>**¥AppEvent.evt**

   キー名: **HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥EventLog¥Security¥**
   名前: **File**
   種類: **REG_EXPAND_SZ**
   値: <ボリューム名とパス>**¥SecEvent.evt**

   キー名: **HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥EventLog¥System¥**
   名前: **File**
   種類: **REG_EXPAND_SZ**
   値: <ボリューム名とパス>**¥SysEvent.evt**
2. [Value] フィールドで、イベント ファイルのパスを保護されていないボリュームに変更します。

ページファイルの場所の変更

ページファイルを使うシステムにおける Enhanced Write Filter (EWF) のパフォーマンスを改善するため、システムのページファイルの場所を EWF で保護されていない別のパーティションに変えることができます。これには、最低 2 つのパーティションが必要です。EWF で保護されたパーティションと、書き込み可能な別のパーティションです。

ページファイルの場所を変更するには

1. ランライム イメージを展開したら、次のレジストリ キーを編集します。
   キー名: **HKLM¥SYSTEM¥CurrentControlSet¥Control¥Session Manager¥Memory Management¥**
   値名: **PagingFiles**
   種類: **REG_MULT_SZ**
   データ: **C:¥Pagefile.sys 150 500**
2. [Data] フィールドでは、ページファイルのパスとファイル名、さらにファイル サイズの最小値と最大値 (MB) を変更します。

一時ファイル フォルダーの場所の変更

一時ファイルの場所を EWF で保護されていない別のパーティションに変更することで、ランタイム イメージにおける Enhanced Write Filter (EWF) のパフォーマンスを改善することができます。既定で、一時インターネット ファイルは %USERPROFILE%¥AppData¥Local¥Microsoft¥Windows フォルダーに保存されています。

一時ファイル フォルダーの場所を変更するには

1. ランタイム イメージで、次のレジストリ キーの 1 つまたは両方を変更します。
   - キー: **HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥Current Version¥Explorer¥User Shell Folders**
     名前: **Cache**
     種類: **REG_EXPAND_SZ**
     値: <保護されていないボリューム上のフォルダーのパス>
   - キー: **HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Shell Folders**
     名前: **Cache**
     種類: **REG_EXPAND_SZ**
     値: <保護されていないボリューム上のフォルダーのパス>
2. また、次のレジストリ設定を変更することで、TMP フォルダーおよび TEMP フォルダーを、保護されていないボリュームにリダイレクトすることもできます。
   - キー: **HKEY_CURRENT_USER¥Environment**
     名前: **TEMP**
     種類: **REG_SZ**
     値: <保護されていないボリューム上のフォルダーのパス>
   - キー: **HKEY_CURRENT_USER¥Environment**
     名前: **TMP**
     種類: **REG_SZ**
     値: <保護されていないボリューム上のフォルダーのパス>

前回アクセス時のタイム スタンプの無効化

NTFS ファイル システムを使用している場合、前回アクセス時の日時のタイム スタンプを無効にすることで、EWF のパフォーマンスを高めることができます。

前回アクセス時のタイム スタンプを無効にするには

- ランタイム イメージに次のレジストリ キーを作成します。
  キー名: **HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥FileSystem**
  名前: **NtfsDisableLastAccessUpdate**
  種類: **REG_DWORD**
  値: **1**

メモ

前回アクセス時のタイム スタンプを再度有効にする必要がある場合は、NtfsDisableLastAccessUpdate キーの値を 0 に変更するか、NtfsDisableLastAccessUpdate キーを削除します。詳細については、「NtfsDisableLastAccessUpdate」を参照してください。

Prefetch の無効化

Prefetch を無効にすることで、Enhanced Write Filter (EWF) のパフォーマンスが改善する場合があります。Prefetch は、オペレーティング システムとアプリケーションの起動パフォーマンスを改善するためのツールです。そのために、Prefetch はアプリケーション データを要求される前にメモリ内に読み込みます。

EWF を RAM オーバーレイと併用してブート ボリュームを保護する場合、Prefetch は起動から次の起動までの間、そのデータを保持することはできません。このような状況下で、Prefetch は EWF リソースを消費して、システムが起動するたびに新しいデータ ファイルを計算し、保存しようとしますが、成果はありません。

Prefetch を無効にするには

- ランタイム イメージで **EnablePrefetcher** レジストリ キーを更新します。
  キー: **HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Session Manager¥Memory Management¥PrefetchParameters**
  名前: **EnablePrefetcher**
  種類: **REG_DWORD**
  値: **0**

EnablePrefetcher キーには次の値があります。
0 = 無効化
1 = Prefetch を有効にしてアプリケーションを起動
2 = Prefetch を有効にしてブート
3 = Prefetch を有効にしてアプリケーションを起動およびブート
Prefetch を無効にするには、値を 0 に設定します。

SuperFetch の無効化

SuperFetch を無効にすることで、Enhanced Write Filter (EWF) のパフォーマンスが改善する場合があります。SuperFetch は、オペレーティング システムとアプリケーションの起動パフォーマンスを改善するためのツールです。そのために、SuperFetch はアプリケーション データを要求される前にメモリ内に読み込みます。SuperFetch は、最も使用されるアプリケーションを監視して、システム メモリに事前に読み込んでおき、必要なときにそれらのアプリケーションが準備できているようにすることで、Prefetch の機能を上回ります。

EWF を RAM オーバーレイと併用してブート ボリュームを保護する場合、SuperFetch は起動から次の起動までの間、そのデータを保持することはできません。このような状況下で、SuperFetch は EWF リソースを消費して、システムが起動するたびに新しいデータファイルを計算し、保存しようとしますが、成果はありません。

SuperFetch を無効にするには

- ランタイム イメージで **EnableSuperfetch** レジストリ キーを更新します。
  キー: **HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Session Manager¥Memory Management¥PrefetchParameters**
  名前: **EnableSuperfetch**
  種類: **REG_DWORD**
  値: **0**

EnableSuperfetch キーには次の値があります。
0 = 無効化
1 = SuperFetch を有効にしてアプリケーションを起動
2 = SuperFetch を有効にしてブート
3 = SuperFetch を有効にしてアプリケーションを起動およびブート
SuperFetch を無効にするには、値を 0 に設定します。

EWF と File-Based Write Filtering

Thin PC では、2 つの書き込みフィルターを提供します。File-Based Write Filtering (FBWF) はファイル レベルで動作し、Enhanced Write Filter (EWF) はセクター レベルで動作します。ほとんどの場合、FBWF の使用をお勧めしますが、NTFS を完全にサポートするには、EWF を使う必要があります。

EWF では、FBWF でサポートされない次の NTFS 機能がサポートされます。

- ファイルのロックとロック解除
- NTFS のファイル ID
- 再解析ポイント

- クォータ
- ハード リンク
- 便宜的ロック
- ファイルの圧縮と暗号化

FBWF では、次の EWF 機能はサポートされません。

- ライブ コミットと無効化

EWF と FWBF を同じ OS のイメージで併用するには、1 つのボリュームで EWF を有効にし、別のボリュームで FBWF を有効にします。

© 2011 Microsoft. All rights reserved.