

# 楽しい EVENT LOG

山岸 真人@Admintechnology.jp

# 講師紹介

- 山岸真人と申します
- Microsoft MVP
  - ▣ Windows Server – Management Infrastructure
- Admintechn.jp 副代表
  - ▣ 主に勉強会の司会やコミュニティ紹介などを担当
- エイケア・システムズ勤務
  - ▣ こないだ転職しました
  - ▣ Windows 系のエンジニアとして活動
    - Active Directory 関連の教育・R&D などをやっています
    - インフラ設計もやります

# Agenda

- イベント ログを把握する
- 運用の Hint&Tips
- Vista の Event Log に触れる

# Agenda

- イベント ログを把握する
- 運用の Hint&Tips
- Vista の Event Log に触れる

# Event Log とは何か

- Windows の健康状態を一発確認する
  - ▣ できる/できないではなく、そういう発想のもとに提供されている
  - ▣ 実際使い物になるかどうかは、このセッションを聞いた後で個人で判断してほしい
- Windows OS の基本的な情報を収集する
  - ▣ どんな情報かは後で説明する
- アプリケーションに関する情報も出力できる
  - ▣ 詳しい話は後で説明する

# 本題に入る前に言葉の定義

## □ 「ログ」

### □ イベント ビューアの左側ペインに表示される各項目

- アプリケーション・システム・セキュリティ・DNS・FRS・Office・OneCare などなど

### □ 全部をひっくるめると、Log"s" となる

- 英語だと表現できるが、日本語で「ログズ」って書くとダサイ
- ログ群とでも書けばいいのかな?

## □ 「イベント」

### □ 日時、ソース、分類、種類、イベント ID、ユーザー、コンピュータ、説明、データの記録された一つのレコード

- 複数形のジレンマはここにも顕在

# Windows の基本的なログとは

- アプリケーション ログ
  - 各サービスの動作結果
  - アプリケーションのインストール結果
  - 各ソフトウェア のログ (対応していれば)
- システム ログ
  - ログ サービスとサービス管理
    - Event Logging Service, Service Control Manager, Process Controller (WinLogon)
  - ドライバ回りにかかわる一部サービス, TCP/IP, Print Spooler
  - インストーラそのものの動作 (Windows Installer, Windows Update)
  - Microsoft 製のセキュリティ ソフト (Defender, OneCare) も
- セキュリティ ログ
  - 監査ログ

# ログの保存先はどこか

- %SystemRoot%\system32\config\
  - AppEvent.Evt (Application Log)
  - SecEvent.Evt (Security Log)
  - SysEvent.Evt (System Log)
  - DNS、FRS などなどもここに保存される
- Tips: 保存する先を変更することもできる
  - HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\%LogName%\File をいじる
  - 詳しくは KB315417 をどうぞ

# アプリケーションも独自イベントを出力できる

- .NET Framework 2.0 の場合
  - EventLogInstaller Class で新しいログやソースを定義・削除できる
  - EventLogEntry Class でイベントを読める・定義できる
  - EventLog Class でイベントを書き込み・削除ができる
- 要は新しいログを作るのもソースを作るのもイベントを書くのも、もちろん読むのもAPIを使えば自由自在ということ
- アプリ屋さんはずいぶんイベント ログを活用して!

# Event Log の保存形式

- 保存形式は独自 (.evt 形式)
  - ビューアとして「イベントビューア」が提供される
  - そのままでは再利用できない
- テキスト形式 (.txt/.csv 形式) で出力するためのインターフェイスは充実していないため、再利用は難しい
  - GUI から手動で Output する
  - Eventquery.vbs コマンドを実行する
  - MPS Reports の力を借りる
  - 先ほどの API を直接使用する (AP を開発する)

# イベント ログ データに説明は記録されない

- 文字列はイベント ログ データには保存しない
  - イベントの軽量化を図るため、イベント ログ データには番号 (イベント ID) を保存する
  - 別途「説明」が保存された DLL (メッセージ ソース DLL) を用意し、閲覧するときにはイベント ID からそれを呼び出す
- IP アドレスのような固有の情報はやむを得ない
  - 引数を用いることで、「説明」に固有の情報を組み込める
- メッセージ ソース DLL には他の情報もある
  - 「説明」のほか、「分類」も分類 ID が保存されている
  - 「分類」が数字化けするのはソース DLL の不具合

# Agenda

- イベント ログを把握する
- 運用の Hint&Tips
- Vista の Event Log に触れる

# 昔の Event Log の臨界点

- 昔の Event Log って?
  - Windows NT version 5.2 までのこと
  - ただし x64 Edition は含みません
- Tips: 全ての Event Log の容量が 200～300 MB 程度を超過した時点で動作異常をきたす
  - ログを相当量 (ほとんど全部) 取りこぼす
    - デモ見る?
  - この臨界点だけは突破させないでちょうだい

# Demo – 臨界点突破 -

# 1 Event あたりの容量はどのくらい?

- 1 Event あたりの容量 (Ave. 300 Bytes 程度)
  - DateTime ▪ Event ID、種類、分類の合計は 152 Bytes
  - Source (UNICODE)
  - Computer Name (UNICODE)
  - USER SID (SID Format, about 20 Bytes)
  - 引数、Data (イベントによってまちまち)
- Tips: 300 MB ÷ 300 Bytes/件 ≒ 100 万件
  - 監査ログ・印刷成功のログあたりを取得しているとあっさり超えそう

# 臨界点を突破するための裏ワザ

- できればツールを使いたくない
  - Tips: 最大容量に達した時点で自動ローテーションさせる
    - HKEY\_LOCAL\_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥%LogName%¥AutoBackupLogFiles を 1 にする
    - 詳しくは KB312571 の後半をどうぞ
    - デモ見る?
- ツール買うよ/使うよ?
  - OK、何でも好きなもん使ってください
    - 安価にするなら Eventquery.vbs や MPS Reports でテキスト化
    - お金をかけるなら Operation Manager や AppManager で集約



# Demo – Event Log Rotation -

# トラッシューに使えるイベント ログにするには

- 誰かに尋ねるときはこんな情報があると Good
  - ログ (System/Security/Application/anything...)
  - 出た日付・時刻
  - ソース
  - 分類
  - 種類 (情報/警告/エラー/成功の監査/失敗の監査)
  - イベント ID
  - 引数 (メッセージのコピペでも OK)
  - データ

# Agenda

- イベント ログを把握する
- 運用の Hint&Tips
- Vista の Event Log に触れる

# Vista で強化された点

- 保存形式が .evt から .evtx になった
  - フォーマットが変化した
    - カラムがいくつか追加された
  - イベント ビューアも拡張された
    - “Windows ログ” と “アプリケーションとサービス ログ”
    - カスタム ビュー
- 保存形式に .xml が選べるようになった
  - 再利用がしやすくなった
- 他のマシンのイベント ログを読みやすくなった
  - サブスクリプション機能

# フォーマットはどう変化した?

レガシ Windows	Windows Vista	値
N/A	ログの名前	アプリケーション/システム/etc...
ソース	ソース	Winlogon/EventLog/etc...
イベント ID	イベント ID	数字 [0-65535]
種類	レベル	重大/エラー/警告/情報/詳細
ユーザー	ユーザー	ユーザー SID
N/A	オペコード	おそらく数字 [0-65535]
日付 + 時刻	ログの日付	日付・時刻
分類	タスクのカテゴリ	数字 [0-65535]
N/A	キーワード	おそらく数字 [0-65535]
コンピュータ	コンピュータ	コンピュータ SID
説明	名称なし	イベント ID に従ったメッセージ
データ	非表示 (XML で見れる)	追加のバイナリ値

# 追加された情報の意味は?

- 「重大」というレベルができた
  - エラーより重い
  - ハングアップなど直接対応が求められるイベントに付与
- 「オペコード」と「キーワード」ができた
  - 古いイベントでは
    - オペコード: 空白
    - キーワード: クラシック
  - こんな内容を書くべき?
    - オペコード: 即時対応、現状維持、など
    - キーワード: 具体的な対応内容やインフォメーションなど
  - イベント ソース DLL から引っ張ってくるようだ
    - おそらくソース DLL 作成時に一緒に埋め込まないと表示できない

# Demo – Vista の Event Viewer -

- ・サマリビューの紹介
- ・Windows ログ/アプリとサービス ログ
- ・カスタム ビューの作成
- ・サブスクリプション