概要

実は、Active Directory へのログオン・ログオフの監査は、監査ポリシーでは正確に記録することができない。
そもそも、「アカウントログオン」のポリシーしかないし、しかもこれはログオンを監査するのではなく、Kerberos の認証チケット発行イベントなので、ドメインへの実際のログオンタイミングとは違うものである。

一方「ログオンイベント・ログオフイベント」の監査の方は、対話型ログオン・ログオフに関わらず、マシンへのアクセスの際に生じる認証イベントをローカルマシン上に記録するものなので、Active Directory 認証は関係ない。

そのため、正確にユーザーがドメインのコンピューターにログオン・ログオフしたことをイベントログに記録し集中管理するためには、ログオン・ログオフスクリプトを使うしかない、とのこと。
これはけっこう有名な話らしい。

前提条件

AD のアカウントユーザーは、イベントログへの書き込みを制限されている。

- セキュリティログに書き込みができるのは、管理者権限のあるユーザーのみ。かつ、デフォルトでは管理者も書き込みできない。管理者権限のないユーザーは、どうやっても書き込みができないようになっている。
- アプリケーションログとシステムログは、管理者はデフォルトで書き込みができる。一般ユーザーは、イベントログの権限設定を変更することで書き込みが可能となる。

一般ユーザーもログオン・ログオフスクリプトで監査する場合、上記のとおりセキュリティログは利用できない。一般的にはアプリケーションログを使用するという。

方法

アプリケーションログに対して Domain Users からの書き込みを許可する

監査ログを記録したいドメインコントローラー上にて、以下のコマンドをコマンドプロンプトで実行する（2008 以降のみ）。

```
wevtutil sl application /ca:O:BAG:SYD:(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;;;S-1-5-32-573)(A;;0x3;;;DU)
```

/ca オプション以降の意味のわからない文字列は、「SDDL 構文」と呼ばれるものだという。この書式に則って、アクセス権限が記述されているという。SDDL についての詳細は MS のサイトを参照のこと。

最後の (A;;0x3;;;DU) が、（「許可」;;「書き込み」;;;「Domain Users」）という意味になるといい、アプリケーションログのデフォルトのアクセス権に追加した部分。
つまり上記から (A;;0x3;;;DU) を除いた部分が、デフォルトのアクセス権。

このコマンドは、指定した SDDL 構文文字列を値として、HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\Application\CustomSD というレジストリキーを追加して有効にするだけ。したがって、このレジストリキーを直接いじることでも、アプリケーションログへのアクセス権をカスタマイズできる。
単にこのキーを削除すれば、デフォルトのアクセス権に戻る。

イベントログにログを記録するログオン・ログオフスクリプトを作る

VBScript on WSH のサンプルは添付の通り。

・
・

strEventLogDcName に、イベントログを記録する DC のホスト名を UNC で指定する。この DC 上で事前に、上記の wevtutil コマンドを実行しておかなければならない。
そうしないと一般ユーザーのログオン・ログオフがイベントログに書き込みできない。

このサンプルだと、ログオンしたユーザーが所属するグループの一覧がログに記録される。
ただし、MemberOf 属性にはプライマリグループが含まれない。AD ユーザーのデフォルトのプライマリグループは Domain Users なので、このスクリプトはそれを前提としている。
ADSI で、あるユーザーのプライマリグループを取得するためには、多少複雑な計算処理をしなければならない、とのこと。。。

一般的には WshShell オブジェクトの LogEvent メソッドを使用するスクリプト例が多いが、LogEvent メソッドだと、イベントログの「ユーザー」フィールドが記録されない。これは困る。

そこで代替として、EventCreate を呼び出して使うようにしている。
/T オプションにはわけあって INFORMATION を指定しているが、通常は SUCCESS とかの方がいいと思う。
/D オプションを指定した場合、空文字引数は許されないので注意。

WshShell.Run メソッドの第二引数には 7 を指定している。実行ウィンドウを最小化し、かつウィンドウフォーカスの操作をしない、という意味。ユーザーにスクリプトの実行を見せないようにするため。詳細は MS のサイトを見てくれ。

ログオフスクリプトだけ、WshShell.Run メソッドの第三引数に True を指定している。これは、実行コマンドの終了を待つ、という意味。ログオフスクリプトでは、ここは必ず True にしないとならない。さもないと、EventCreate が完了する前に即時にログオフしてしまい、ログが記録されない。
一方でログオンスクリプトではそのような心配はない。むしろ True にするとログオン時にユーザーが少し待たされるため、こちらは省いている。