

Simple-FIM Proof of Concept Testing Plan

FIRM

**Dec/Jan 2013-2014**

**v.6**

**Table of Contents**

[1. Introduction 3](#_Toc421518303)

[2. To Do 3](#_Toc421518304)

[3. Appendix A: FIM Reports- Explanation and examples: 4](#_Toc421518305)

[4. Appendix B: List of monitored Files/(Registry Keys for Windows): 7](#_Toc421518306)

[5. Appendix C: FIM Fixlets/Analyses: 15](#_Toc421518307)

# Introduction

# To Do

The scope of this project will be to implement the FIM solution in a laboratory environment, using the BF Evaluation Software and execute the activities as defined below.

This will be done on Red Hat, Solaris, AIX, and Windows

The scope of this POC will include demonstrating the successful

|  |  |
| --- | --- |
| ∑ | File Integrity Monitoring proof-of-concept |

# Appendix A: FIM Reports- Explanation and examples:

So, the intent of this File Integrity Monitoring implementation is to monitor specific files and/or directories for changes, and to notify the administrator when this happens.

Initially, a fixlet is run on a scheduled basis, which creates a timestamped list of specific monitored files/directories, and which saves the checksum of this list. If one of the monitored files changes, the original list is saved with a *.bak* extension, and an updated list is generated

In the FIRM2 client folder.

When the system ‘notices’ a change in ‘checksum’, a report is triggered, and is sent to the administrator who must investigate and resolve the condition.

Note that additional directories could be added, by modifying the ‘create’ and ‘reset’ fixlets for each of the tested platforms. For each added directory, a line of the form must be added, substituting the directory’s full pathname where in the place of of the red /sbin, below

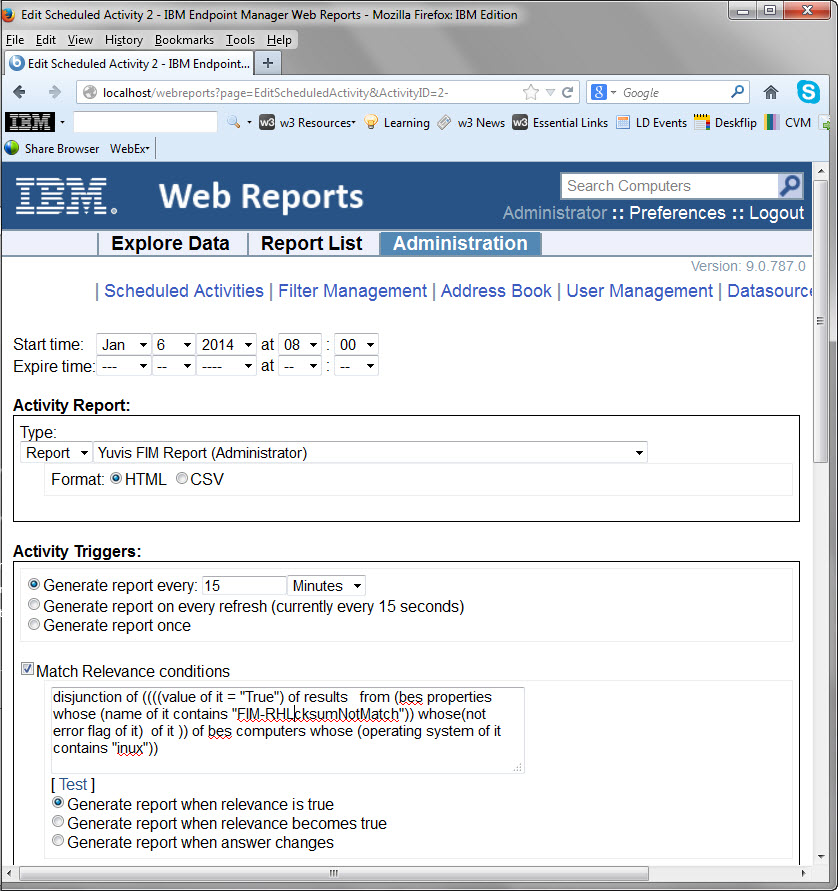
*{(if (exists it) then (pathname of it & " folder: " & modification time of it as string) else (it as string & "folder: <N/E>")) of folder "/sbin" | "/sbin folder: <N/E>"}*

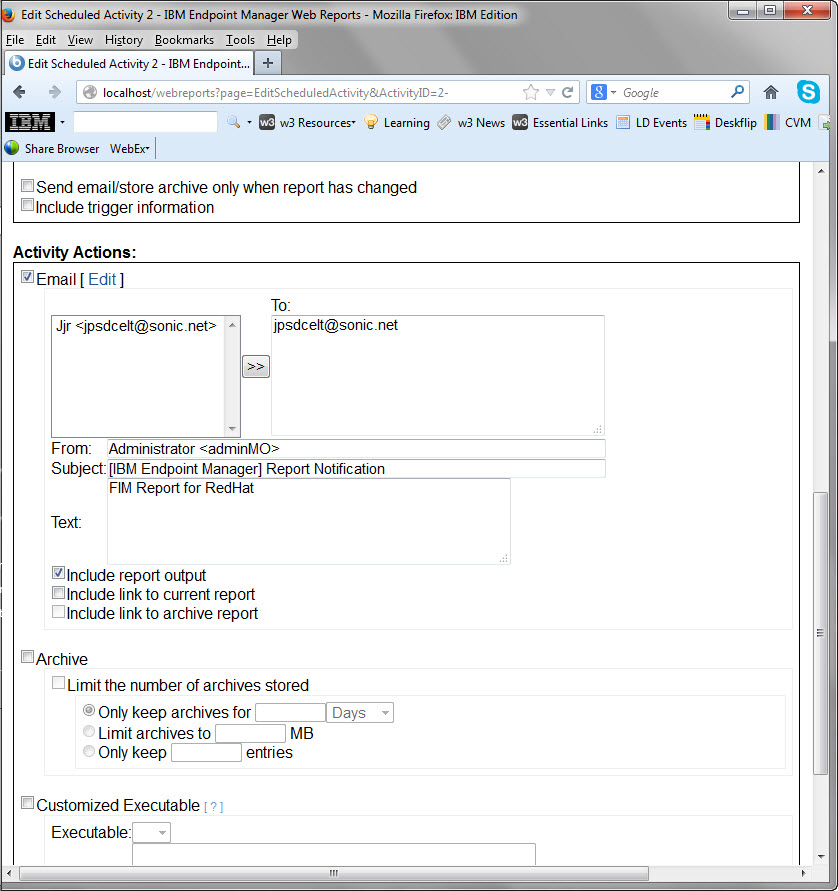
For each separate file, one would add a line (substituting the desired filename for the red

*/etc/passwd*, below

*{(if (exists it) then (pathname of it & ": " & modification time of it as string) else (it as string & ": <N/E>")) of file "/etc/passwd" | "/etc/passwd: <N/E>"}*

The report contains the names of each file and it’s timestamp (see the two screenshots, below, which show the ‘report-triggering’ section of the WebReports interface:





Then, after appropriate investigation of the file-change, the administrator executes a ‘reset’ fixlet, which returns the system to it’s monitoring state. See Appendix C, below, for an example report, received when one of the targeted files was modified:

# Appendix B: List of monitored Files/(Registry Keys for Windows):

**Red Hat:**

|  |
| --- |
| /etc/security/user |
| /etc/security/login.cfg |
| /etc/inetd.conf |
| /etc/rc.tcpip |
| /etc/inittab |
| /etc/inetd.conf |
| /etc/ftpusers |
| /etc/mail/sendmail.cf |
| /etc/security |
| /etc/passwd |
| /etc/group |
| /etc/motd |
| /etc/ntp.conf |
| /etc/hosts.equiv |
| /etc/tunables/nextboot |
| /etc/security/limits |
| /etc/security/audit/config |
| /etc/usr/lib/security/mkuser.default auditclasses |
| /etc/syslog.conf |
| /etc/ssh/sshd\_config |
| /etc/shosts.equiv |
| /etc/snmp.conf |
| /etc/ntp.conf |
| /sbin |
| /bin |
| /lib |
| /mnt |
| /mnt/floppy |
| /root |
| /boot |
| /etc |
| /etc/mtab |
| /etc/shadow |
| /etc/rc.d |
| /etc/pam.d |
| /etc/hosts |
| /etc/hosts.allow |
| /etc/hosts/deny |
| /var/spool |
| /var/spool/cron |
| /var/spool/mqueue |
| /var/spool/mail |

**Solaris:**

|  |
| --- |
| /etc/hosts.deny |
| /etc/hosts.allow |
| /etc/init.d |
| /etc/default/login |
| /etc/syslog.conf |
| /etc/default/init |
| /etc/hosts.equiv |
| /etc/ssh/sshd\_config |
| /etc/pam.conf |
| /etc/ftpd/ftpusers |
| /etc/default/passwd |
| /etc/passwd |
| /etc/profile |
| /etc/.login |
| /etc/ftpd/ftpaccess |
| /etc/motd |
| /etc/issue |
| /etc/ntp.conf |
| /etc/default/telnetd |
| /etc/group |
| /etc/ldap.conf |
| /var/ldap/ldap\_client\_file |
| /etc/snmp.conf |
| /sbin |
| /bin |
| /lib |
| /mnt |
| /mnt/floppy |
| /root |
| /boot |
| /etc |
| /etc/mtab |
| /etc/shadow |
| /etc/rc.d |
| /etc/pam.d |
| /etc/hosts |
| /etc/hosts.allow |
| /etc/hosts/deny |
| /var/spool |
| /var/spool/cron |
| /var/spool/mqueue |
| /var/spool/mail |
|  |

**AIX:**

|  |
| --- |
| /etc/security/user |
| /etc/security/login.cfg |
| /etc/inetd.conf |
| /etc/rc.tcpip |
| /etc/inittab |
| /etc/inetd.conf |
| /etc/ftpusers |
| /etc/mail/sendmail.cf |
| /etc/security |
| /etc/passwd |
| /etc/group |
| /etc/motd |
| /etc/ntp.conf |
| /etc/hosts.equiv |
| /etc/tunables/nextboot |
| /etc/security/limits |
| /etc/security/audit/config |
| /etc/usr/lib/security/mkuser.default auditclasses |
| /etc/syslog.conf |
| /etc/ssh/sshd\_config |
| /etc/shosts.equiv |
| /etc/snmp.conf |
| /etc/ntp.conf |
| /sbin |
| /bin |
| /lib |
| /mnt |
| /mnt/floppy |
| /root |
| /boot |
| /etc |
| /etc/mtab |
| /etc/shadow |
| /etc/rc.d |
| /etc/pam.d |
| /etc/hosts |
| /etc/hosts.allow |
| /etc/hosts/deny |
| /var/spool |
| /var/spool/cron |
| /var/spool/mqueue |
| /var/spool/mail |

**Windows:**

|  |
| --- |
| $(HKLM\_WNTCV)\Winlogon|ScreenSaverGracePeriod |
| $(HKLM\_WNTCV)\Winlogon|cachedlogonscount |
| $(HKLM\_WNTCV)\Winlogon|defaultpassword value |
| $(HKLM\_WCV)\policies\system|legalnoticecaption |
| $(HKLM\_WCV)\policies\system|legalnoticetext |
| $(HKLM\_WCV)\Policies\system|DisableBkGndGroupPolicy |
| $(HKLM\_CCS)\Control\Lsa|FIPSAlgorithmPolicy |
| $(HKLM\_CCS)\Control\Lsa|RestrictAnonymous |
| $(HKLM\_CCS)\Control\Lsa|RestrictAnonymousSAM |
| $(HKLM\_CCS)\Control\Lsa|auditbaseobjects |
| $(HKLM\_CCS)\Control\Lsa|everyoneincludesanonymous |
| $(HKLM\_CCS)\Control\Lsa|nolmhash |
| $(HKCU)\Control Panel\Desktop|ScreenSaveTimeOut |
| $(HKLM\_Services)\NetLogon\parameters|requirestrongkey |
| $(HKLM\_Services)\Netlogon\Parameters|DisablePasswordChange |
| $(HKLM\_Services)\Netlogon\Parameters|maximumpasswordage |
| $(HKLM\_Services)\Netlogon\Parameters|maxpasswordage |
| $(HKLM\_Services)\Netlogon\Parameters|refusepasswordchange |
| $(HKLM\_Services)\Netlogon\Parameters|requiresignorseal |
| $(HKLM\_Services)\Netlogon\Parameters|sealsecurechannel |
| $(HKLM\_Services)\Netlogon\Parameters|signsecurechannel |
| $(HKLM\_Services)\SNMP\Parameters\PermittedManagers |
| $(HKLM\_Services)\SNMP\Parameters\ValidCommunities |
| $(HKLM\_Services)\lanmanserver\parameters|enablesecuritysignature |
| $(HKLM\_Services)\lanmanworkstation\parameters|enableplaintextpassword |
| $(HKLM\_Services)\lanmanworkstation\parameters|requiresecuritysignature |
| $(HKLM\_Services)\lanmanserver\parameters|restrictnullsessaccess |
| $(HKLM\_Services)\lanmanworkstation\Parameters|enablesecuritysignature |
| $(HKLM\_Services)\LanmanWorkstation\Parameters|EnablePlainTestPassword |
| $(HKLM)\Software\Policies\Microsoft\W32time\Parameters|NTPServer |
| $(HKLM\_CCS)\Control\Lsa|limitblankpassworduse |
| $(HKLM\_Services)\Eventlog\Security|WarningLevel |
| $(HKLM)\SYSTEM\ControlSet001\Control\Terminal Server\WinStations\RDP-Tcp|MinEncryptionLevel |
| $(HKLM)\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp|MinEncryptionLevel |
| $(HKLM)\SECURITY\Policy\Secrets\SAC |
| $(HKLM)\SECURITY\Policy\Secrets\SAI |
| $(HKLM)\SECURITY\SAM\Domains\Account |
| $(HKLM)\SECURITY\SAM\Domains\Account\Users |
| $(HKLM\_CCS)\Control\LSA |
| $(HKLM\_CCS)\Control\LSA|LsaPid |
| HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa|restrictanonymoussam |
|  |

# Appendix C: FIM Fixlets/Analyses:

1. Properties corresponding to each operating system were created (like *FIM-WINcksumNotMatch*), the relevance for which was:

line 1 of file "FIMwindows\_dataChecksum.txt" of parent folder of regapp "BESClient.exe" != sha1 of file "FIMwindows\_data.txt" of parent folder of regapp "BESClient.exe"

The equivalent relevance for each system was used in triggering the reports (see step 2, below)

1. We created web reports of each of the analyses, above, and saved them as ‘public’, then ‘triggering’ them to be emailed, based on the following relevance (replace the names of the different operating systems where you see Win, below). For example, the ‘saved Windows analysis’ report was triggered by the following relevance:

**disjunction of ((((value of it = "True") of results   from (bes properties whose (name of it contains "FIM-WINcksumNotMatch")) whose(not error flag of it)  of it )) of bes computers whose (operating system of it contains "Win"))**

[the ‘translation’ of the above relevance is: ‘evaluate as true if any of the machines with the Windows operating system show the *FIM-WINcksumNotMatch* flag as ‘true’ (and do not indicate any errors)]

(See github repository <\*.bes> for fixlets).