Getting Started PowerSC Trusted Logging

Release 1.1.1 from May 2012

Nigel Griffiths
IBM Power Systems
Advanced Technology Support, Europe

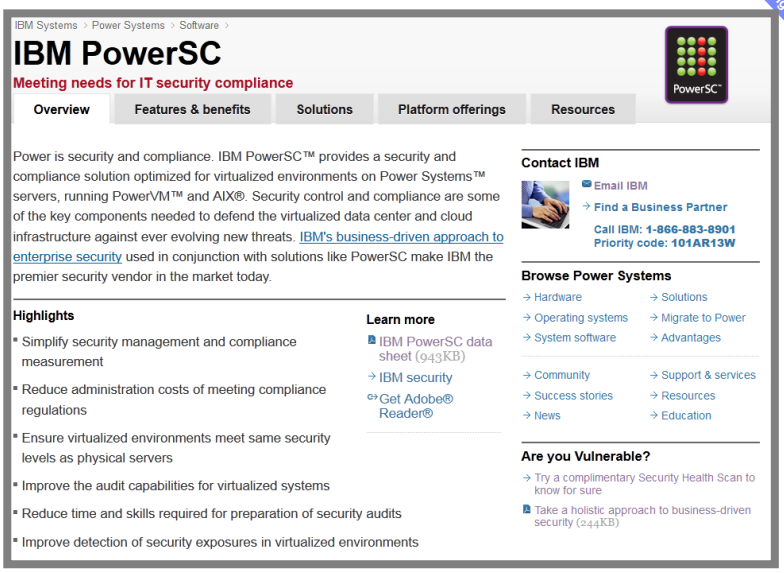
Presentation Version 5

Abstract

- To make sure we can track those nasty hackers/system crackers, we need to get the system logs off the machine to a safe place
  - So they can't hide their tracks or trash the system entirely
- PowerSC Trusted Logging does this without a network
  - That makes meddling impossible
- This session tells you
  - How to get started
  - Then more complex features like what happens with LPM
  - And how storing log on a Shared Storage Pool can help.
- This is NOT a general session of AIX error, syslog or audit logs
- But see Nigel's Notes at the end for a reminder

- Thanks to Morten Vagmo, IBM Norway and Geraint North one of the developers for information used in this presentation

10,000 feet overview but no "How To" details
http://www.ibm.com/systems/power/software/security/



IBM Systems › Power Systems › Software ›

IBM PowerSC

Meeting needs for IT security compliance

Overview | Features & benefits | Solutions | Platform offerings | Resources

Power is security and compliance. IBM PowerSC™ provides a security and compliance solution optimized for virtualized environments on Power Systems™ servers, running PowerVM™ and AIX®. Security control and compliance are some of the key components needed to defend the virtualized data center and cloud infrastructure against ever evolving new threats. IBM's business-driven approach to enterprise security used in conjunction with solutions like PowerSC make IBM the premier security vendor in the market today.

Highlights

- Simplify security management and compliance measurement
- Reduce administration costs of meeting compliance regulations
- Ensure virtualized environments meet same security levels as physical servers
- Improve the audit capabilities for virtualized systems
- Reduce time and skills required for preparation of security audits
- Improve detection of security exposures in virtualized environments

Learn more

- IBM PowerSC data sheet (943KB)
- IBM security
- Get Adobe® Reader®

Contact IBM

Email IBM
Find a Business Partner
Call IBM: 1-866-883-8901
Priority code: 101AR13W

Browse Power Systems

- Hardware
- Solutions
- Operating systems
- Migrate to Power
- System software
- Advantages
- Community
- Support & services
- Success stories
- Resources
- News
- Education

Are you Vulnerable?

- Try a complimentary Security Health Scan to know for sure
- Take a holistic approach to business-driven security (244KB)

Trusted Logging Pre-Requisites

- Virtual I/O Server 2.2.1.0
  - Latest = currently 2.2.1.4 recommended
- AIX 6 TL7+
- AIX 7 TL1+
  - With all service packs recommended
- Any hardware that runs the above

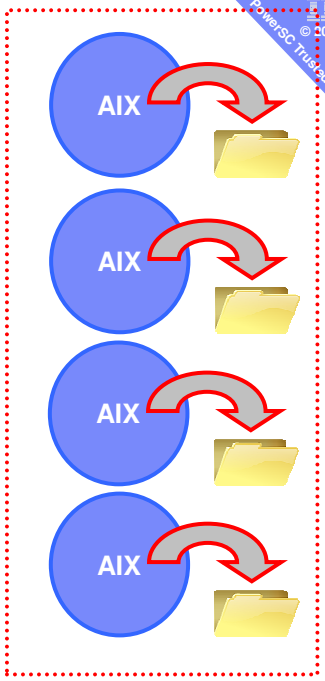
- PowerSC documentation page 22 -24
- http://pic.dhe.ibm.com/infocenter/aix/v6r1/topic/com.ibm.aix.powersc/powersc_pdf.pdf
- VIOS Documentation page 144 - 149
- http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/topic/p7hb1/p7hb1.pdf

Logging Alternatives

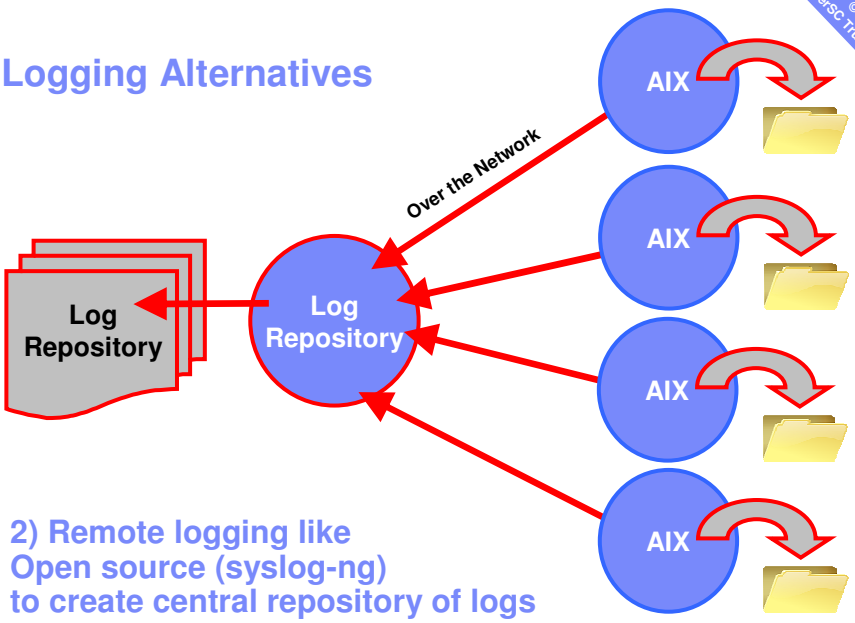
1) Local default AIX Logging

Risks: Your nasty hacker could
- shuts down logging
- removes log
- edits log
- destroys the LPAR and
  we will never work out how/why!

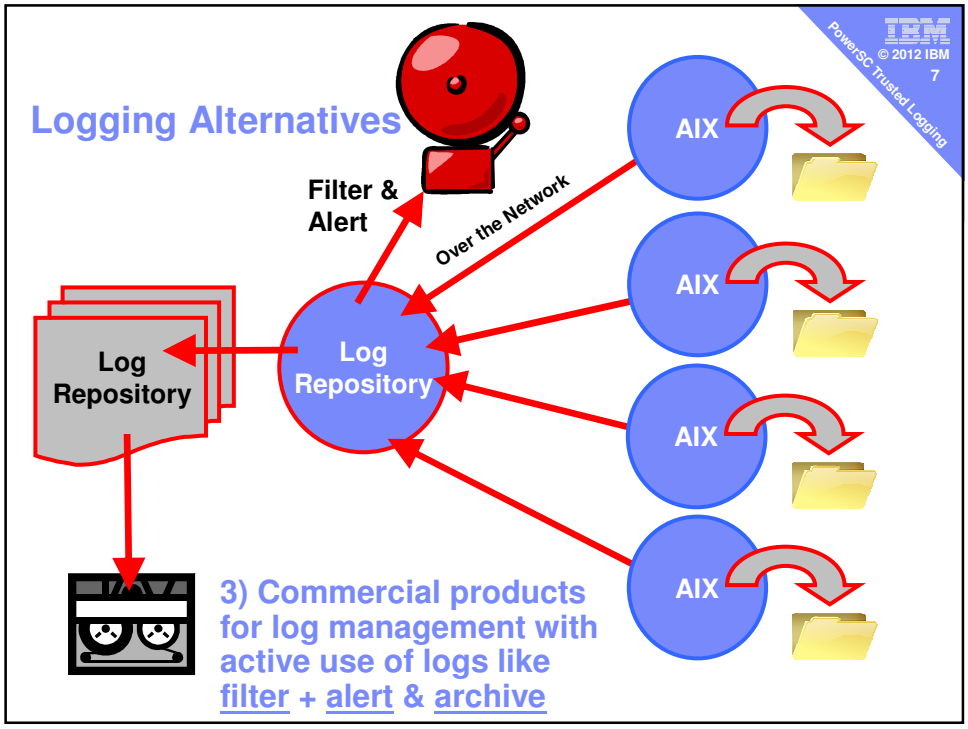
= No post-mortem analysis

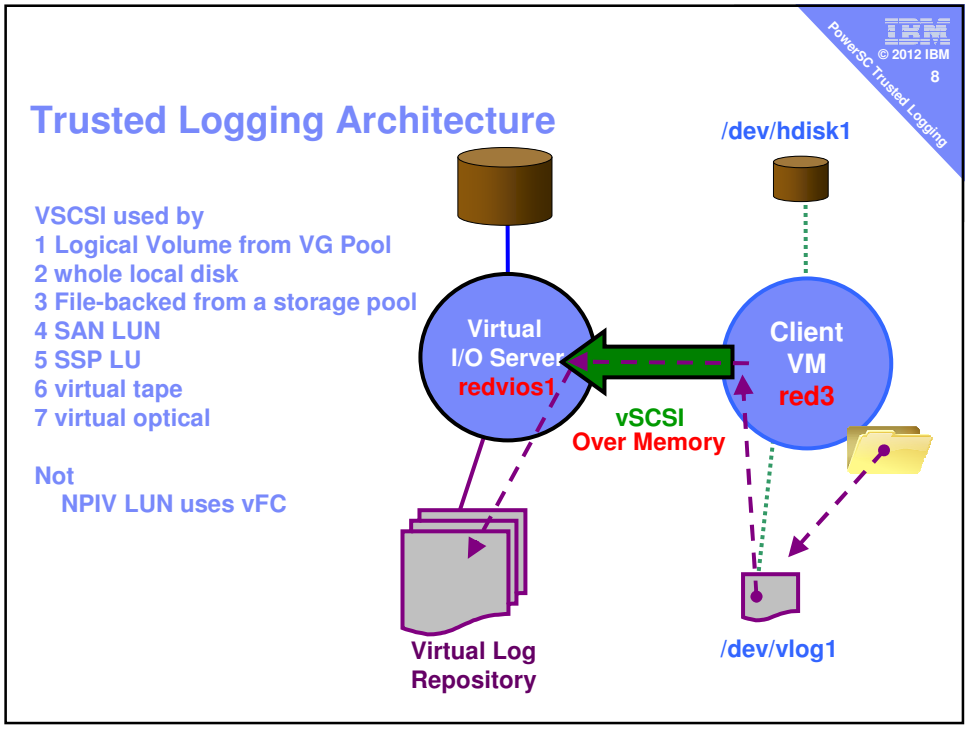


Logging Alternatives



2) Remote logging like
Open source (syslog-ng)
to create central repository of logs
- Now hacker can't hide initial intrusion


IBM
© 2012 IBM
7
PowerSC Trusted Logging
Logging Alternatives
Filter &
Alert
Over the Network
AIX
AIX
AIX
AIX
Log
Repository
Log
Repository
3) Commercial products
for log management with
active use of logs like
filter + alert & archive

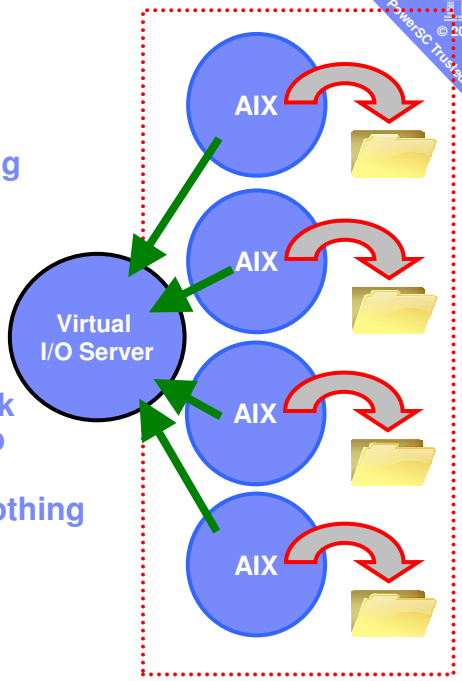

IBM
© 2012 IBM
8
PowerSC Trusted Logging
Trusted Logging Architecture
VSCSI used by
1 Logical Volume from VG Pool
2 whole local disk
3 File-backed from a storage pool
4 SAN LUN
5 SSP LU
6 virtual tape
7 virtual optical
Not
NPIV LUN uses vFC
/dev/hdisk1
Virtual
I/O Server
redvios1
Client
VM
red3
vSCSI
Over Memory
Virtual Log
Repository
/dev/vlog1

Logging Alternatives

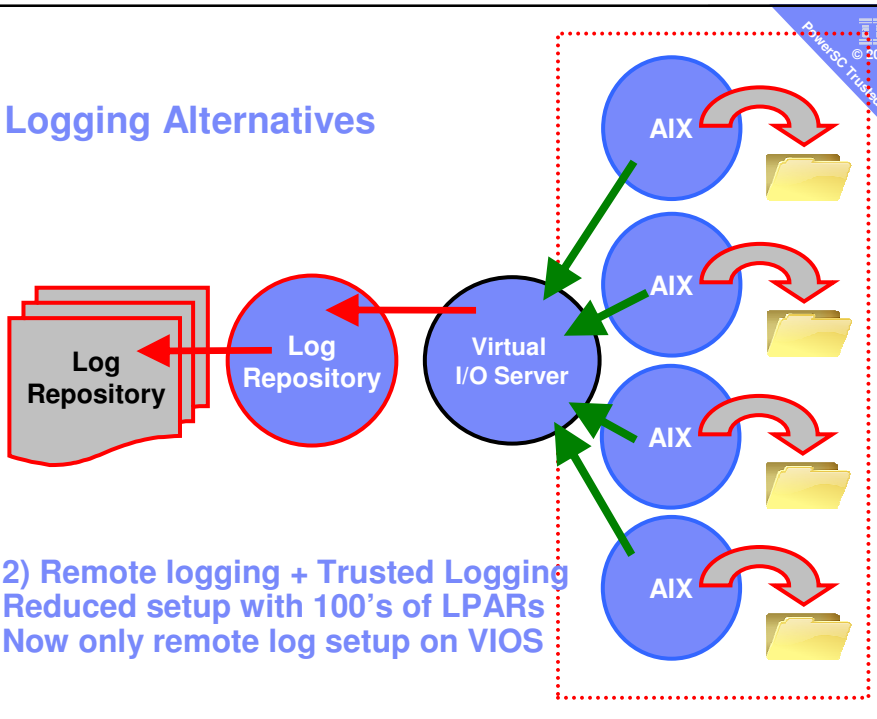
1) Local default AIX Logging
+ Trusted Logging

Risks
- Now hacker can't hide initial intrusion!
- Over memory = impossible network hack
- Simple "no brainer" setup

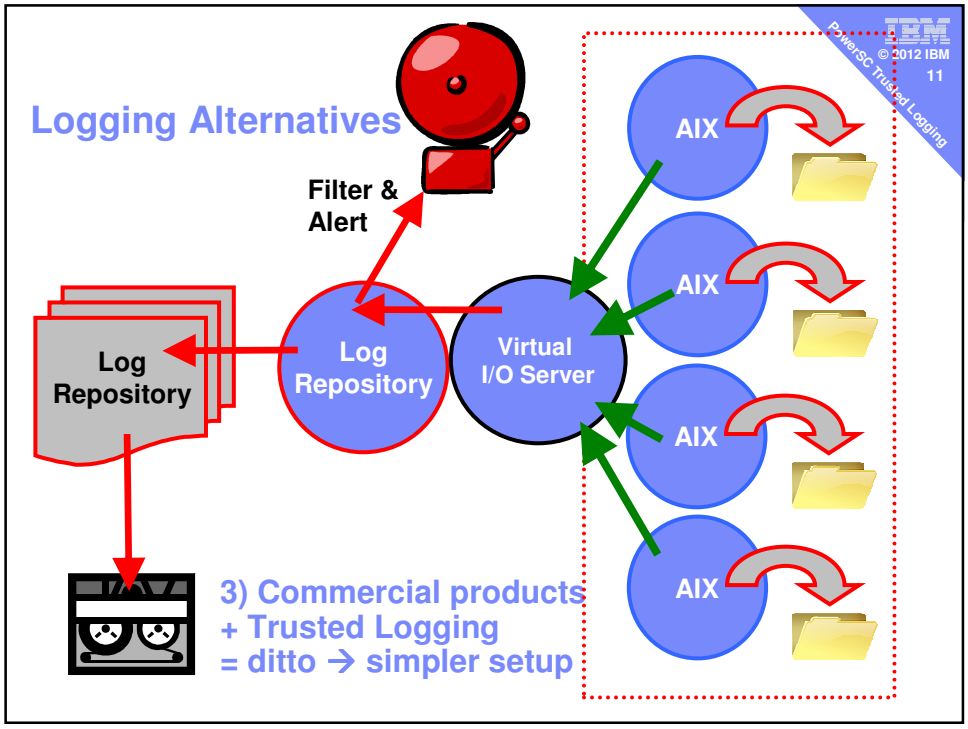
1000% better than doing nothing



Logging Alternatives



2) Remote logging + Trusted Logging
Reduced setup with 100's of LPARs
Now only remote log setup on VIOS



VIOS: mkvlog – make a simple virtual log

- mkvlog -name LogName log name like syslog mylog …
  [-client ClientName] LPAR name (will try to work this out)
  [-vadapter Adapter] vSCSI adapter like vhost33

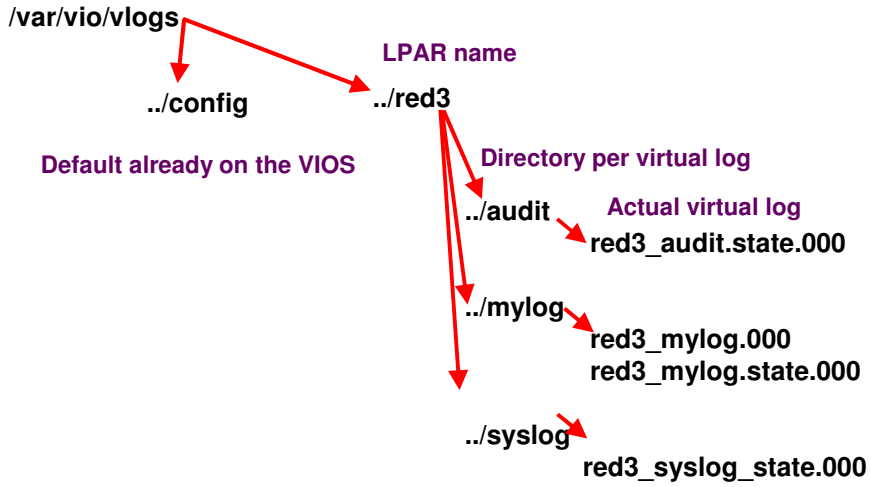
- Examples:
- mkvlog -name mylog -client red3 -vadapter vhost1
- mkvlog -name audit -client red3 -vadapter vhost1
- mkvlog -name syslog -client red3 -vadapter vhost1

```
As padmin on the VIOS:
$ mkvlog -name mylog -client red3 -vadapter vhost1
Virtual log 00000000000000f952c2fe4b205254 created
vtlog0 Available
$
```

mkvlog creates

```
$ ls -lR /var/vio/vlogs
total 0
drwxrwx---    2 root     system          256 Jul 31 18:00 config
drwxr-xr-x    5 root     staff           256 Jul 31 18:00 red3
/var/vio/vlogs/config:
ls: /var/vio/vlogs/config: The file access permissions do not allow the specified
  action.
total 0

/var/vio/vlogs/red3:
total 0
drwxr-xr-x    2 root     staff           256 Jul 31 18:00 audit
drwxr-xr-x    2 root     staff           256 Jul 31 17:58 mylog
drwxr-xr-x    2 root     staff           256 Jul 31 18:00 syslog

/var/vio/vlogs/red3/audit:
total 8
-rw-r-----    1 root     staff           164 Jul 31 18:00 red3_audit.state.000

/var/vio/vlogs/red3/mylog:
total 8
-rw-r-----    1 root     staff          1849 Jul 31 17:58 red3_mylog.000
-rw-r-----    1 root     staff           164 Jul 31 17:58 red3_mylog.state.000

/var/vio/vlogs/red3/syslog:
total 8
-rw-r-----    1 root     staff           166 Jul 31 18:00 red3_syslog.state.000
```


mkvlog creates



Log Files

- File names:
  - <LPAR-name>_<Log-name>.<generation-number>
- Example log file:
  - red3_mylog.000, red3_mylog.001 & red3_mylog.state.000
  - First two are the actual log files
    - Can be binary or text format but fixed size
    - Default is 10MB each and 2 of them
  - Third is the state file (normally small)
    - The .state. file is readable text with state changes, log switches, the processes connecting to the log
  - .000 to .999 the series of logs

VIOS: lsvlog -d for detailed

Note: this number from the VIOS

```
$ lsvlog
Client Name      Log Name  UUID              VTD
red3             syslog    31800e1837e15275  vhost1/vtlog2
red3             mylog     f952c2fe4b2f5254  vhost1/vtlog0
red3             audit     fee6038f67432bab  vhost1/vtlog1
$ lsvlog -d
Client Name: red3
  Log Name:                     syslog
  UUID:                         00000000000000031800e1837e15275
  Virtual Target Device:        vtlog2
  Parent Adapter:               vhost1
  Vlog State:                   enabled
  Device Status:                available
  Logical Unit Address:         8400000000000000
  Storage Pool:
  Log Directory:                /var/vio/vlogs/red3/syslog/
  Maximum Log Files:            2
  Maximum Log File Size:        1048576
  Maximum State Files:          2
  Maximum State File Size:      1048576
... One paragraph per virtual log
```

Note: UUID shortened to fit

VIOS: lsvlrepo -detail

```
$ lsvlrepo
Storage Pool      State     Path
                  enabled   /var/vio/vlogs
atlantic          enabled   /var/vio/SSP/galaxy/.../vlogs/
$ lsvlrepo -detail
Local Virtual Log Repository:
  Repository State:             enabled
  Path:                         /var/vio/vlogs
  Maximum Log Files:            2
  Maximum Log File Size:        1048576
  Maximum State Files:          2
  Maximum State File Size:      1048576

Virtual Log Repository for Shared Storage Pool atlantic:
  Repository State:             enabled
  Path:
  /var/vio/SSP/galaxy/D_E_F_A_U_L_T_061310/vlogs/
  Maximum Log Files:            2
  Maximum Log File Size:        1048576
  Maximum State Files:          2
  Maximum State File Size:      1048576
```


Note: This VIOS is also running Shared Storage Pool “atlantic”

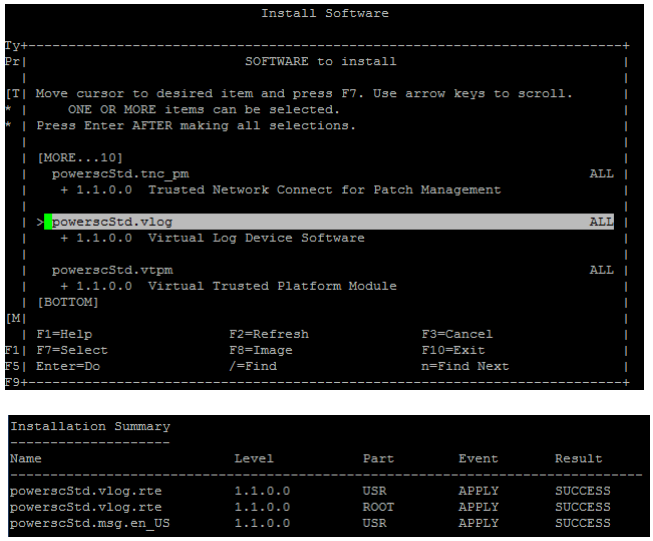
AIX Client VM: Find new devices

- New devices on the vSCSI → cfgmgr to find them
  - If VM just created found when booting/rebooting

```
As the root user

# cfgmgr
cfgmgr: 0514-621 WARNING: The following device packages are
  required for device support but are not currently installed.
devices.vscsi.tm
```

- Oops!! Forgot to add the PowerSC package for Virtual Logging to this AIX client VM

AIX: smitty installp with the PowerSC media



AIX: Find new devices

```
# lsconf >/tmp/a
# cfgmgr
# lsconf >/tmp/b
# diff /tmp/a /tmp/b
52a53,55
> * vlog2          U8203.E4A.10E0A41-V3-C3-T1-L8400000000000000  Virtual Log
> * vlog1          U8203.E4A.10E0A41-V3-C3-T1-L8300000000000000  Virtual Log
> * vlog0          U8203.E4A.10E0A41-V3-C3-T1-L8200000000000000  Virtual Log
```

But which is which one???

```
# lsattr -El vlog0
PCM                                 Path Control Module              False
UUID             f952c2fe4b2055254  Unique id for virtual log device False
client_name      red3               Client Name                      False
device_name      vlmylog0           Device Name                      False
log_name         mylog              Log Name                         False
max_log_size     2097152            Maximum Size of Log Data File    False
max_state_size   2097152            Maximum Size of Log State File   False
pvid             none               Physical Volume Identifier       False
```

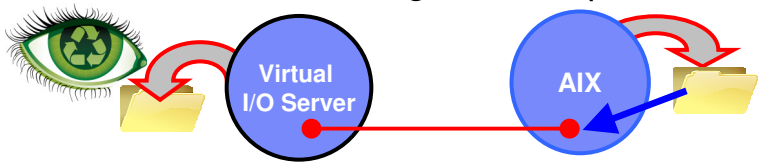
Will match VIOS lsvlog output command

Now we have a character device(s)

```
# ls -l /dev/vlog*
crw-rw----   1 root     system       35,  0 Aug 02 16:08 /dev/vlog0
crw-------   1 root     system       35,  1 Aug 01 12:05 /dev/vlog1
crw-------   1 root     system       35,  2 Aug 16 16:15 /dev/vlog2
```


All Done – phew!

- We have a virtual log & a transport mechanism



- But two gaps
  - A. AIX end: Setup AIX logs to use the virtual log
    - This is standard audit & log configuration
    - A bit scary if you have never done this before!
  - B. VIOS end: Prove we can read the virtual log
    - Easy but Undocumented!

AIX Audit log

AIX end: Setup audit logs to use the virtual log
Edit /etc/security/audit/config

```
start:
        binmode = on
        streammode = off

bin:
        trail = /audit/trail
        bin1 = /audit/bin1
        bin2 = /audit/bin2
        binsize = 10240
        cmds = /etc/security/audit/bincmds
        freespace = 65536
        backuppath = /audit
        backupsize = 0
        virtual_log = /dev/vlog0

stream:
        cmds = /etc/security/audit/streamcmds

classes:
        general = USER_SU,PASSWORD_Change,FILE_Unlink, ...
. . .
```

```
# audit shutdown
# audit start
```

Warning: does not by default restart on reboot

WARNING:

- The documents use /dev/vlog0 → all the time!
- Don't be FOOLED that will NEVER work!
- The 1st use will work OK
  Subsequent use will silently "log open" errors

If the log is already in use …

On the AIX client

```
# echo HELLO >/dev/vlog0
The requested resource is busy.
ksh: /dev/vlog0: 0403-005 Cannot create the specified file.
#
```

Which is doubly confusing as I already have a /dev/vlog0,
so why is it trying to create one.
It is failing to open the device not create it.

Simple test to prove the log is running

AIX end: Telnet failure then OK in Audit Log

```
# pwd
/audit
# ls -ltr
total 11976
-rw-------    1 root     system            0 Aug 07 12:17 auditb
-rw-r-----    1 root     system      6119558 Aug 07 12:22 trail
-rw-rw----    1 root     system            0 Aug 07 12:22 bin1
-rw-rw----    1 root     system         1522 Aug 07 12:22 bin2
# auditpr <bin2
. . .
event            login    status      time                     command       wpar
  name
---------------- -------- ----------- ------------------------ ------------- ------
  ___
S_PASSWD_READ    root     OK          Tue Aug 07 12:20:11 2012 telnetd       Global
S_PASSWD_READ    root     OK          Tue Aug 07 12:20:11 2012 telnetd       Global
TCPIP_connect    root     OK          Tue Aug 07 12:20:11 2012 telnetd       Global
. .
```


VIOS: Reading the virtual audit logs

Binary Audit Logs

```
# cd /var/vio/vlogs/red3/audit
# file *
red3_audit.000: data or International Language text
red3_audit.001: data or International Language text
red3_audit.state.000: commands text
# ls -ltr
total 2352
-rw-r-----    1 root start    4949 red3_audit.state.000
-rw-r-----    1 root staff 1048513 red3_audit.000
-rw-r-----    1 root staff  135852 red3_audit.001
```

Don’t use cat/tail/pg/vi
Use audit print → “auditpr”

```
# But which file? xxxx.000 or xxxx.001
```

VIOS end: Prove we can read the virtual log

$ tail /var//vio/vlogs//red3/audit/red3_audit.state.000

```
...
[1344602908] [redvois1.aixncc.uk.ibm.com] vtlog0 using /var/vio/vlogs/red3/audit//red3_audit.001
[1344613169] [redvois1.aixncc.uk.ibm.com] vtlog0 using /var/vio/vlogs/red3/audit//red3_audit.000
[1344632633] [redvois1.aixncc.uk.ibm.com] vtlog0 using /var/vio/vlogs/red3/audit//red3_audit.state.000
[1344632633] [redvois1.aixncc.uk.ibm.com] vtlog0 initialised
[1344869914] [redvois1.aixncc.uk.ibm.com] vtlog0 using /var/vio/vlogs/red3/audit//red3_audit.state.000
[1344869914] [redvois1.aixncc.uk.ibm.com] vtlog0 initialised
[1344874611] [redvois1.aixncc.uk.ibm.com] vtlog0 using /var/vio/vlogs/red3/audit//red3_audit.state.000
[1344874611] [redvois1.aixncc.uk.ibm.com] vtlog0 initialised
```

Last log file so currently in use

$ auditpr < /var//vio/vlogs//red3/audit/red3_audit.000 | more

```
event           login    status      time                     command   wpar name
--------------- -------- ----------- ------------------------ --------- ---------
FS_Rmdir        root     OK          Fri Aug 10 16:41:28 2012 java      Global
FS_Chdir        root     OK          Fri Aug 10 16:41:37 2012 ps        Global
FS_Mkdir        root     OK          Fri Aug 10 16:42:28 2012 java      Global
FILE_Unlink     root     OK          Fri Aug 10 16:42:28 2012 java      Global
FILE_Rename     root     OK          Fri Aug 10 16:42:28 2012 java      Global
FS_Rmdir        root     OK          Fri Aug 10 16:42:28 2012 java      Global
FS_Rmdir        root     OK          Fri Aug 10 16:42:28 2012 java      Global
FILE_Unlink     root     OK          Fri Aug 10 16:42:28 2012 java      Global
FS_Rmdir        root     OK          Fri Aug 10 16:42:28 2012 java      Global
FS_Chdir        root     OK          Fri Aug 10 16:42:37 2012 ps        Global
FS_Chdir        root     OK          Fri Aug 10 16:44:59 2012 ps        Global
S_PASSWD_READ   root     OK          Fri Aug 10 16:45:00 2012 cron      Global
S_PASSWD_READ   root     OK          Fri Aug 10 16:45:00 2012 cron      Global
CRON_Start      root     OK          Fri Aug 10 16:45:00 2012 cron      Global
FS_Chdir        root     OK          Fri Aug 10 16:45:00 2012 cron      Global
FS_Chdir        root     OK          Fri Aug 10 16:45:09 2012 ps        Global
```


AIX syslog

AIX: Setup UNIX syslogs to use the virtual log
Edit /etc/syslog.conf

```
. . .
# example:
# "mail messages, at debug or higher, go to Log file. File
  must exist."
# "all facilities, at debug and higher, go to console"
# "all facilities, at crit or higher, go to all users"
#  mail.debug           /usr/spool/mqueue/syslog
#  *.debug              /dev/console
#  *.crit                       *
#  *.debug              /var/log/syslog.debug100k.out  rotate
  size 100k files 4
#  *.crit               /var/log/syslog.dailycrit.out  rotate
  time 1d
# ASO log configuration
aso.notice /var/log/aso/aso.log rotate size 128k time 7d
aso.info /var/log/aso/aso_process.log rotate size 1024k
*.info /dev/vlog1
```

The means messages from all facilities at full detail gets sent to vlog0
Note rotation options are not allowed – that happens on then VIOS end

```
# refresh -s syslogd
```


Reading the virtual syslog logs

Plain Text Logs

```
# cd /var/vio/vlogs/red3/syslog
# file *
red3_syslog.000: commands text
red3_syslog.state.000: commands text
# ls
red3_syslog.000        red3_syslog.state.000
# ls -l
total 104
-rw-r-----    1 root     staff 47298 red3_syslog.000
-rw-r-----    1 root     staff  2564 red3_syslog.state.000
# tail -100 red3_syslog.000
. . .
```

Use cat/tail/pg/vi

UNIX syslog failed & then OK telnet passwd

```
Aug  7 12:17:06 red3 daemon:notice telnetd[7536838]: telnet from ::ffff:9.79.10.142 on /dev/pts/1
Aug  7 12:17:13 red3 auth|security:notice tsm: Login successful for root from 9.79.10.142 on /dev/pts/1
Aug  7 12:20:11 red3 daemon:notice telnetd[7536848]: telnet from ::ffff:9.79.10.142 on /dev/pts/1
Aug  7 12:20:17 red3 auth|security:info syslog: pts/1: failed login attempt for root from 9.79.10.142
Aug  7 12:20:23 red3 auth|security:notice tsm: Login successful for root from 9.79.10.142 on /dev/pts/1
```


Advanced Topics

- Virtual Log Control
  - mkvlog, lsvlog, chvlog, rmvlog
- Virtual Log Repository control
  - lsvlrepo, chvlrepo
- Advanced Related topics
  - Dual VIOS
  - Live Partition Mobility - LPM
  - Shared Storage Pool – SSP
- Note Taking Log - idea!

VIOS: Virtual Log control mkvlog

- mkvlog -name LogName log name like syslog or mylog …
  [-client ClientName] LPAR name (it will try to work this out)
  [-sp StoragePool] Advanced
  [-vadapter Adapter] vSCSI adapter like vhost3
  [-dev DeviceName] if not vtlogN assigned (confusing?)
  [-lf FileCount] [-lfs FileSize] # of Log files and sizes
  [-sf FileCount] [-sfs FileSize] # of State files and sizes

- Example (as padmin):
  mkvlog -name mylog -client LPAR42 -vdapter43 -lf 20 -lfs 20M

VIOS: mkvlog – make a virtual log

UUID shortened to fit

```
$ lsvlog
Client Name      Log Name  UUID              VTD
red3             syslog    31800e1837e15275  vhost1/vtlog2
red3             mylog     f952c2fe4b2052544 vhost1/vtlog0
red3             audit     fee6038f67432bab  vhost1/vtlog1
$ lsvlog -d
Client Name: red3
  Log Name:                     syslog
  UUID:                         00000000000000031800e1837e15275
  Virtual Target Device:        vtlog2
  Parent Adapter:               vhost1
  Vlog State:                   enabled
  Device Status:                available
  Logical Unit Address:         8400000000000000
  Storage Pool:
  Log Directory:                /var/vio/vlogs/red3/syslog/
  Maximum Log Files:            2
  Maximum Log File Size:        1048576
  Maximum State Files:          2
  Maximum State File Size:      1048576
. . . One paragraph per virtual log
```

Default values from the repository settings

VIOS: Virtual Log control chvlog - part 1 of 2

- Change name and/or logname
- chvlog -dev vtlog9 -client LPAR42 -name syslog

- State
  - Enabled, disabled, migrated (=LPM else where)

- chvlog -dev vtlog9 -state disabled
  - To change the state must not be connected to a device
  - Unclear why you would do this!

VIOS: Virtual Log control chvlog - part 2 of 2

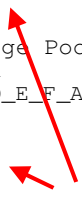
- Important not to fill up the filesystem
- So fixed number of files and sizes
  - For both the Log-file and Status-File
- List with lsvlog and changed with chvlog options
  - lf number of Log files default 2
  - lfs size of Log files default 1 MB
  - sf number of State files default 2
  - sfs size of State files default 1 MB
  - “l” –s lowercase L
- $ chvlog -dev vtlog9 -lfs 20M # as padmin user

VIOS: Virtual Log control rmvlog

- rmvlog -dev vtlog8
  - Unconfigure the virtual log device (disable) only
- rmvlog -dev vtlog8 -d
  - Remove the virtual log device
- rmvlog -dev vtlog8 -db
  - also remove the virtual log from the repository
- rmvlog -dev vtlog8 -dbdata
  - also remove the associated data from the repository

VIOS: Virtual Log Repository control

```
$ lsvlrepo
Storage Pool      State    Path
                  enabled  /var/vio/vlogs
atlantic          enabled
                  /var/vio/SSP/galaxy/D_E_F_A_U_L_T_061310/vlogs/

$ lsvlrepo -detail
Local Virtual Log Repository:
  Repository State:             enabled
  Path:                         /var/vio/vlogs
  Maximum Log Files:            2
  Maximum Log File Size:        1048576
  Maximum State Files:          2
  Maximum State File Size:      1048576

Virtual Log Repository for Shared Storage Pool atlantic:
  Repository State:             enabled
  Path:           /var/vio/SSP/galaxy/D_E_F_A_U_L_T_061310/vlogs/
  Maximum Log Files:            2
  Maximum Log File Size:        1048576
  Maximum State Files:          2
  Maximum State File Size:      1048576
```



Defaults for mkvlog

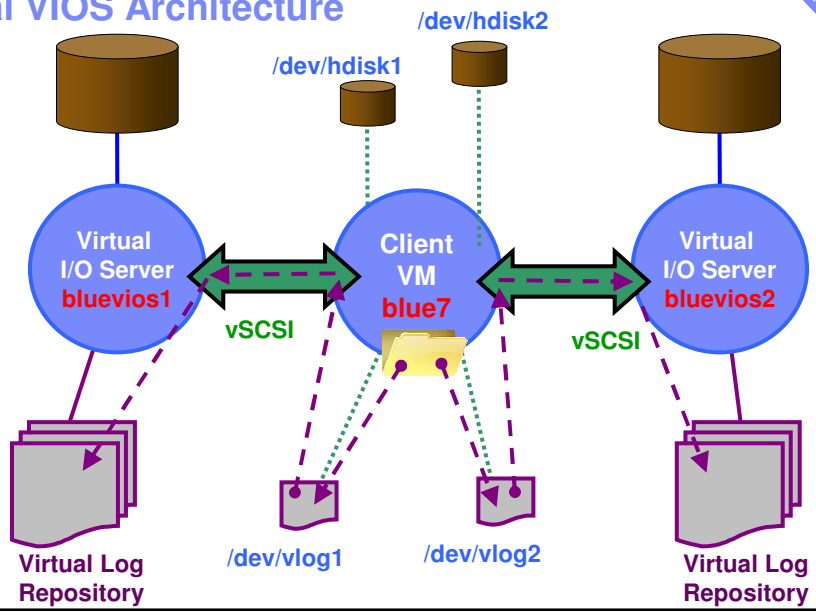
VIOS: Virtual Log Repository control

- chvlrepo -lf n -lfs m[KMG] -root *path*
- chvlrepo -lf n -lfs m[KMG] -sp *storagepool*
  - *Both also have -sf and –sfs for state-files*
- As padmin user
  $ chvlrepo -lf 20 -lfs 5M
  Updated repository.
- Other examples:
  - chvlrepo -p /home/virtuallogs
  - chvlrepo –sp my2nd_SSP
- Only changes defaults for next mkvlog

Advanced Related Topics

1. Dual VIOS
2. Live Partition Mobility (LPM)
3. Shared Storage Pools (SSP)

Dual VIOS Architecture



Dual Virtual I/O Server to dual path hdisk

AIX: Install powerscStd.vlogs
AIX: # lspath
Enabled hdisk0 vscsi0
Enabled hdisk0 vscsi1
VIOS1: $ mkvlog -name syslog -client diamond7 -vadapter vhost6
Virtual log 00000000000000063bb1cf5f3cd32e4 created
vtlog0 Available
AIX: cfgmgr
AIX: # lspath
Enabled hdisk0 vscsi0
Enabled hdisk0 vscsi1
Available vlog0 vscsi0
VIOS2: $ mkvlog -name syslog -client diamond7 -vadapter vhost6
Virtual log 0000000000000000a9f2a8d02ac57120 created
vtlog0 Available
AIX:# lspath
Enabled hdisk0 vscsi0
Enabled hdisk0 vscsi1
Available vlog0 vscsi0
Available vlog1 vscsi1
AIX: vi /etc/syslog.conf & refresh –s syslogd
BOTH VIOSs:
$ ls -l /var/vio/vlogs/diamond7/syslog
total 16
-rw-r----- 1 root staff 54 Aug 08 11:08 diamond7_syslog.000
-rw-r----- 1 root staff 421 Aug 08 11:08 diamond7_syslog.state.000
$ cat /var/vio/vlogs/diamond7/syslog/diamond7_syslog.000
Aug 8 11:07:12 diamond7 syslog:info syslogd: restart
AIX: # logger TESTING VLOGs
BOTH VIOSs:
$ cat /var/vio/vlogs/diamond7/syslog/diamond7_syslog.000
Aug 8 11:07:12 diamond7 syslog:info syslogd: restart
Aug 8 11:09:32 diamond7 user:notice root: TESTING VLOGs

vhost6 on both VIOSs is the VIOS vSCSI adapter ←→ LPAR client diamond7

vi /etc/syslog.conf
And added:
***.info /dev/vlog0**
***.info /dev/vlog1**

Dual Virtual I/O Server

- Note
  - The Client has double the number of logs
  - You need to configure twice the number of virtual logs on the client VM
  - Also double the data - one copy on each VIOS
- Using a Shared Storage Pool avoids this see next few slides

What about Live Partition Mobility?

- Worked fine on the first attempt ☺
- Virtual Logs are recreated on the target VIOS(s)
  - Initially containing the Migration DR log records
  - Same files = /var/vio/vlog/<LPAR-name>/<Log-name>
- AIX client is unaffected
- But now older logs still on original VIOS
  - They are not copied between VIOS's
  - May have to clean up or re-setup remote logging
- Using a VIOS Shared Storage Pool solves this ...→

What about Shared Storage Pools (SSP) + vlogs?

- All VIOS can access the same SSP based vlog
  - So same vlog before & after LPM = Cool!!
- When creating the VIOS side vlog add:
  - -sp poolname

- Example:

mkvlog -sp atlantic -name syslog -client red3 -vadapter vhost1

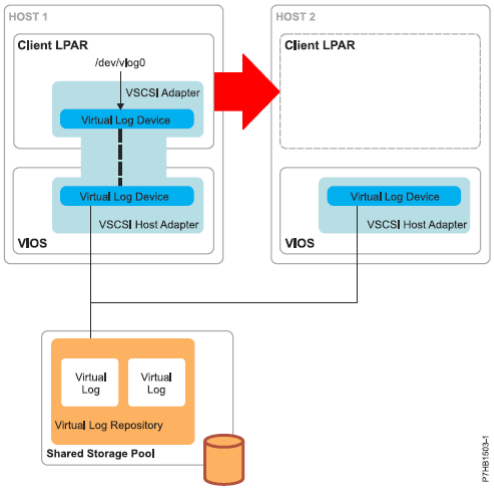
- That is it = very simple once you have a Shared Storage Pool setup

What about Shared Storage Pools (SSP) + vlogs

- Diagram from the PowerSC manuals
- Logical view

- So same vlog & NOT in 2 parts

Remotely Logging?
- Just set up on one VIOS
- LPM has no effect



Dual VIOS and Shared Storage Pools

- Assuming both VIOS in the Shared Storage Pool
- The two Virtual Logs have the same UUID, so multi-pathed over the two Virtual I/O Servers to the single SSP log file.

Note taking log?

- Don't connect a special log service (AIX client)
- Output just gets sent "as is"
- Example daily script to save config for DR

```
date >/dev/vlog5
echo About to start batch run 28 >/dev/vlog5
lsconf >/dev/vlog5
df -g >/dev/vlog5
lsdev >/dev/vlog5
lspv >/dev/vlog5
echo Hello Jim I found that /home was 100 percent full again I added 1 GB but
  we need to fix this >/dev/vlog5
```

etc.

- Good to save regular recovery data "off the LPAR"

Trusted Logging Summary

1. Simple to implement & understand
2. Flexible log naming
3. Piggy-backs vSCSI
4. Smaller sites it may be enough
5. Larger sites already shipping logs can localise setup to VIOS'
6. If using LPM further planning needed
7. If using SSP it adds further value

Pre-reqs: VIOS 2.2.1.4 and AIX 6 TL7+ or AIX 7 TL1+

PowerSC Trusted Logging - Cheat Sheet

- VIOS: mkvlog -name syslog -client red3 -vadapter vhost6
- VIOS: mkvlog -name mylog -client LPAR42 -lf 20 -lfs 20M -vdapter vhost8
- VIOS: logs in /var/vio/vlogs/LPAR/logname
- VIOS: lsvlog [-d]
- VIOS: lsvlrepo -detail [repository can be files or Shared Storage Pool]
- VIOS: chvlrepo -lf 33 -lfs 42M -root path [K=kilobytes M=Megabytes G=Gigabytes]
- VIOS: mkvlog -sp atlantic -name syslog -client red3 -vadapter vhost1
- VIOS: chvlog -dev vtlog9 -lfs 20M

-lf no. of log files **–lfs log file size**

- AIX: Install PowerscStd.vlog
- AIX: cfgmgr
- AIX: lspath
- AIX: lsattr -El vlog0 [match IDs with VIOS: lsvlog –d]

- AIX audit: /etc/security/audit/config add bin: virtual_log = /dev/vlog0
- AIX audit: activate with: audit shutdown; audit start
- AIX audit test: use auditpr <logfile

- AIX syslog: /etc/syslog.conf add *.info /dev/vlog1 then refresh –s syslogd
- AIX syslog: 1st time: startsrc –s syslogd and use: logger to inject messages

- AIX errpt to syslog: Create a small file called xxx contents below:

```
errnotify:
      en_name = "syslog1"
      en_persistenceflg = 1
      en_method = "/usr/bin/errpt -al $1 | /usr/bin/sed 's/^/AIX-errpt:-> /' | /usr/bin/logger -t errpt -p daemon.error"
```

- Setup: odmadd xxx Undo with: odmdelete -q"en_name='syslog1'" -o errnotify
- Testing: errlogger Testing Forty Two

Reference Material
Nigel's Notes starter pack on Logging

Things we should know but I had forgotten!

1. AIX error logging (i.e. errpt) = propriety
2. UNIX syslog
3. Getting AIX errpt output in to the syslog

AIX Errlog: – Reminder/Notes

- See AIX System Admin Redbook SG24-6191
- ERROR!! → /dev/error file → errdemon → /var/adm/ras/errlog
  - Also puts errors into NVRAM for first failure data capture
- AIX7 config: # **/usr/lib/errdemon -l**

```
Error Log Attributes
------------------------------------------
Log File                /var/adm/ras/errlog
Log Size                1048576 bytes
Memory Buffer Size      32768 bytes
Duplicate Removal       true
Duplicate Interval      10000 milliseconds
Duplicate Error Maximum 1000
PureScale Logging       off
PureScale Logstream     CentralizedRAS/Errlog
```

- List AIX Log errors: **errpt** or **errpt -a | pg**
- **errclear** Deletes entries → all but last 2 days: errclear 2
- Changing behaviour
- To change the maximum size of the error log file, enter:
  - /usr/lib/errdemon -s **2000000**
- To change the size of the error log device driver's internal buffer, enter:
  - **/usr/lib/errdemon -B 16384**

AIX errlog: errlogger to generate log entires

```
# errlogger Testing use of errlogger command

# errpt
IDENTIFIER TIMESTAMP T C RESOURCE_NAME DESCRIPTION
AA8AB241 0904103401 T O OPERATOR OPERATOR NOTIFICATION
1581762B 0831110701 T H cd0 DISK OPERATION ERROR
2BFA76F6 0828155301 T S SYSPROC SYSTEM SHUTDOWN BY USER

# errpt -a -j AA8AB241
---------------------------------------------------------------------------
LABEL: OPMSG
IDENTIFIER: AA8AB241
Date/Time: Tue Sep 4 10:34:17
Sequence Number: 6
Machine Id: 003826424C00
Node Id: mynode
Class: O
Type: TEMP
Resource Name: OPERATOR
Description
OPERATOR NOTIFICATION
User Causes
ERRLOGGER COMMAND
Recommended Actions
REVIEW DETAILED DATA
Detail Data
MESSAGE FROM ERRLOGGER COMMAND
Testing use of errlogger command
#
```

Now the bad news:
Errlog Can't be redirected to an additional file via a conf file but read on …

UNIX syslog on AIX

- AIX6 or later – Warning: syslog is off by default
- AIX7TL1 has ASO entries & syslog started
- ERROR!! →Network socket → syslogd demon → various
- Config: /etc/syslog.conf including filename for log(s)
  - This file has large detail comments/hints/examples
  - Facilities.Priority(detail-level) Destination Parameter
  - Warning: *.debug will generate a large volume of data
  - Destination can be
    1. file for appending,
    2. hostname for remote syslog feeding or
    3. username for email
  - You must create/touch the log file (or it fails to log)
  - Parameters can include: rotate size 1m files 10

UNIX syslog on AIX

- Testing: syslogd –d & watch for “errno warnings”
  - `# syslog -d`
  - `cfline(*.info /var/log/mysyslog_info  rotate size 1m files 10)`
  - `syslogd: /var/log/mysyslog_info: errno = 2`
  - `logmsg: pri 53, flags 8, from red3, msg syslogd`
    `/var/log/mysyslog_info: errno = 2`
    → **this failed to open the log file**
- First time: startsrc –s syslogd
- After config file change : refresh –s syslogd
- Use “logger” command to manual add entries
- To stop: stopsrc –s syslogd

AIX errpt log redirected to syslog

1. **vi /etc/syslog.conf** → see the many good comments in this file
   I added
   ***.info /var/log/mysyslog_info rotate size 1m files 10**
   Means everything except debug with 10 log files of 1 MB & for Trusted Logging:
   ***.info /dev/vlog2**
2. Start it up: **startsrc -s syslogd** or if running: **refresh -s syslogd**
3. Create a small file called xxx contents:

```
errnotify:
    en_name = "syslog1"
    en_persistenceflg = 1
    en_method = "/usr/bin/errpt -al $1 | /usr/bin/sed 's/^/AIX-errpt:-> /' | /usr/bin/logger -t errpt -p daemon.error"
```

Gets last errpt entry, formats it, uses logger to put in syslog

   - Note TAB characters to indent & “:-> ” to make it look nice in syslog output
4. Add to the ODM: **odmadd xxx**
5. Testing: as root: **errlogger Test Forty Two**
6. Remove this entry!!: odmdelete -q"en_name='syslog1'" -o errnotify

AIX errpt log to syslog - Sample test output

tail /var/log/mysyslog_info or what-ever you called your syslog
Give you

```
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> ---------------------------------------
   ---------------------------------
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> LABEL:          OPMSG
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> IDENTIFIER:     AA8AB241
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:->
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> Date/Time:       Tue Aug  7 13:32:56
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> Sequence Number: 64560
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> Machine Id:      000E0A41D900
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> Node Id:         red3
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> Class:           O
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> Type:            TEMP
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> WPAR:            Global
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> Resource Name:   OPERATOR
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:->
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> Description
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> OPERATOR NOTIFICATION
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:->
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> User Causes
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> ERRLOGGER COMMAND
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:->
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:->     Recommended Actions
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:->     REVIEW DETAILED DATA
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:->
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> Detail Data
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> MESSAGE FROM ERRLOGGER COMMAND
Aug  7 13:32:56 red3 daemon:err|error errpt:AIX-errpt:-> Test Forty Two
```


AIX errpt log to syslog – Real error output

```
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> ------------------------------------------------------------
   -----------
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> LABEL:          J2_FS_FULL
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> IDENTIFIER:     F7FA22C9
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:->
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> Date/Time:       Tue Aug  7 13:46:18
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> Sequence Number: 64561
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> Machine Id:      000E0A41D900
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> Node Id:         red3
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> Class:           O
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> Type:            INFO
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> WPAR:            Global
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> Resource Name:   SYSJ2
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:->
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> Description
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> UNABLE TO ALLOCATE SPACE IN FILE SYSTEM
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:->
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> Probable Causes
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> FILE SYSTEM FULL
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:->
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:->     Recommended Actions
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:->     INCREASE THE SIZE OF THE ASSOCIATED FILE SYSTEM
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:->     REMOVE UNNECESSARY DATA FROM FILE SYSTEM
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:->     USE FUSER UTILITY TO LOCATE UNLINKED FILES STILL REFERENCED
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:->
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> Detail Data
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> JFS2 MAJOR/MINOR DEVICE NUMBER
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> 000A 0008
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> FILE SYSTEM DEVICE AND MOUNT POINT
Aug  7 13:46:18 red3 user:notice root: AIX-errpt:-> /dev/hd1, /home
```