

Securing and Encrypting Network Traffic with z/OS Communications Server and Policy Agent

Security Workshop

SYSLOGD



IBM Washington System Center
IBM Technical Sales Support

Trademarks

- **The following are Registered Trademarks of the International Business Machines Corporation in the United States and/or other countries.**
 - IBM
 - z/OS
 - **The following are trademarks or registered trademarks of other companies.**
 - Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.
 - All other products may be trademarks or registered trademarks of their respective companies.
 - Refer to www.ibm.com/legal for further legal information.
-
- OSA-Express Features
 - There are many different types of OSA-Express features. In this document where OSA is mentioned it refers to an OSA port on any of the OSA-Express features unless a specific OSA-Express feature is mentioned.

Agenda

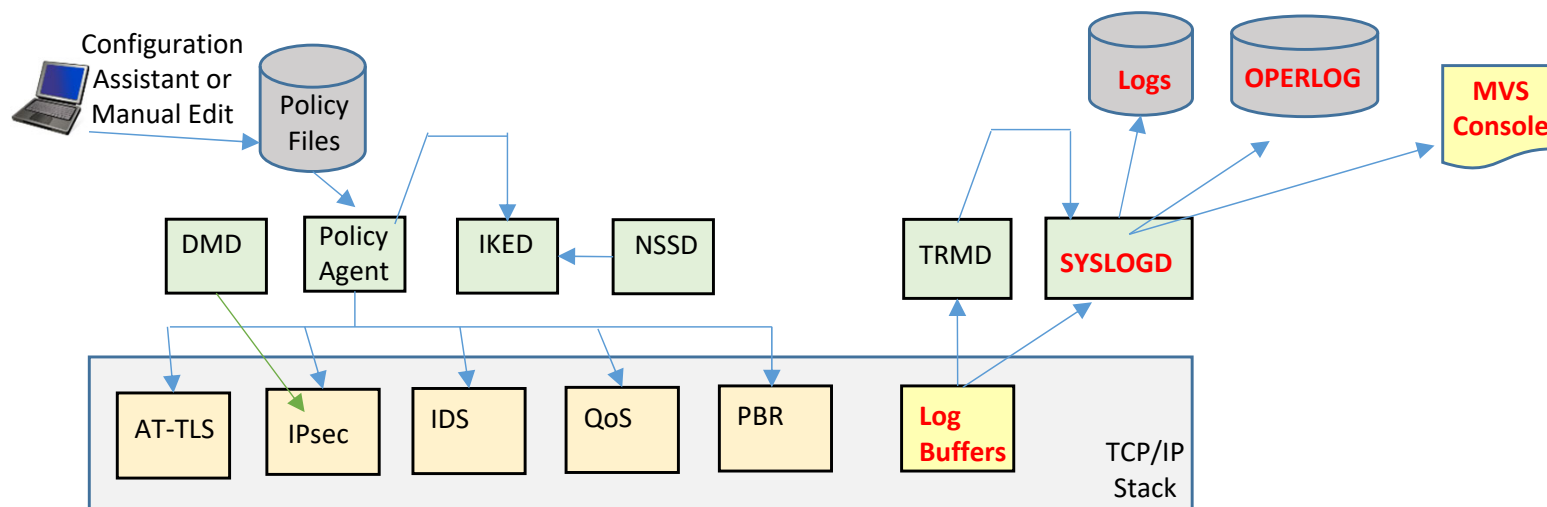
- SYSLOG Daemon Overview
- Defining SYSLOG Daemon
- SYSLOGD Configuration File
- Automatic Archiving
- SyslogD ISPF Browser
- Log File Management
- Time Stamps
- Appendices:
 - Cron Daemon
 - Cron Example

SYSLOG Daemon Overview

Security Implementation can greatly increase the volume of log messages. You must warn your SYSLOG Daemon and MVS implementers about the increased logging activity.



Lots of Different Policy Types and Started Tasks



- Policy Agent
 - Installs Policies into the TCP/IP stack
- TCP/IP Stack
 - Enforces the Policies
- DMD (Defense Manager Daemon)
 - ipsec command can be used to install temporary IP Filter rules.
- IKED (Internet Key Exchange Daemon)
 - Required for IPsec Dynamic VPN (Virtual Private Network) Tunnels
- NSSD (Network Security Server Daemon)
 - Required for IKEv2
 - Provides central RACF certificate repository for remote IKED applications
 - Provides DataPower access to RACF
- TRMD (Traffic Regulation Management Daemon)
 - Required for log messages to syslogd for IP Filter, IPsec, and IDS
- **SyslogD**
 - **Recommended for logging**

What Happened to My Messages?

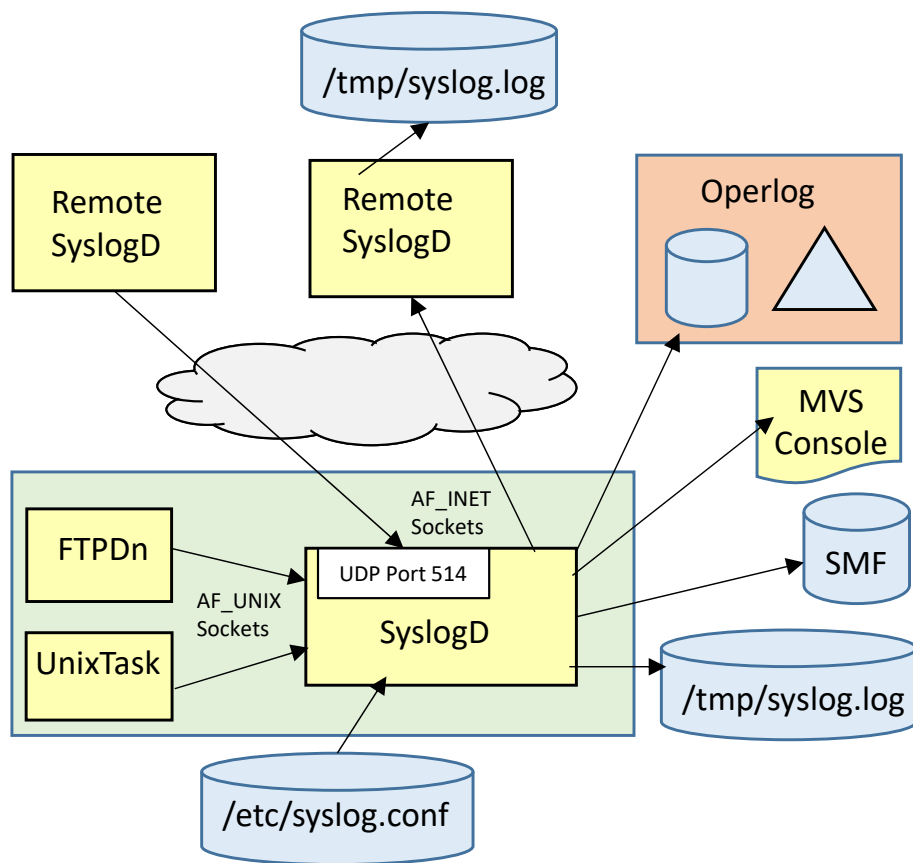


```
***** TOP OF DATA *****  
  
J E S 2   J O B   L O G   --   S Y S T E M   S 7 3  
  
--- TUESDAY,    20 JUL 1999  ----  
  
IEF695I START TCPIP1A  WITH JOBNAME TCPIP1A  IS  
$HASP373 TCPIP1A  STARTED  
  
IEE252I MEMBER CTIEZB01 FOUND IN SYS1.PARMLIB  
EZZ0300I OPENED PROFILE FILE DD:PROFILE  
EZZ0309I PROFILE PROCESSING BEGINNING FOR DD:PROF  
.....  
EZZ0334I IP FORWARDING IS ENABLED  
.....
```

- SYSLOG Daemon (SyslogD) is the traditional Unix log repository.
- Prior to Unix becoming part of z/OS (MVS) all messages were written to the MVS System Log.
- Now that Unix is part of z/OS not all the messages are automatically sent to the MVS System Log, some Unix application messages are sent to syslogd instead.
- Rather than looking in multiple Unix application job logs it is recommended to use syslogd as a central log repository.

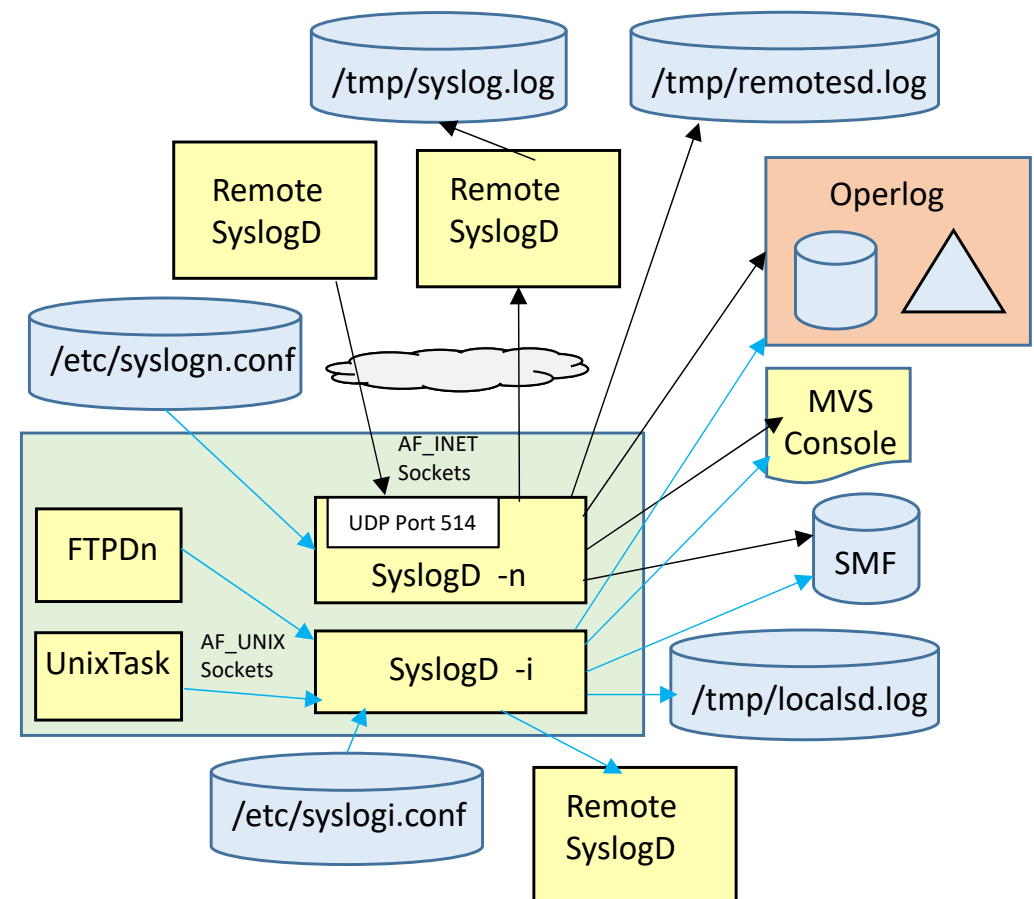
SYSLOGD Environment

- One Single SYSLOGD



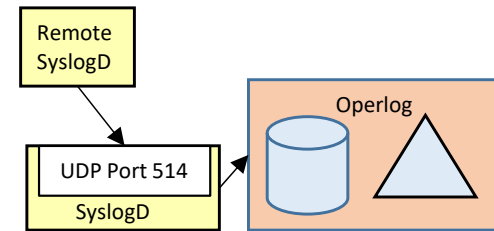
- Or Two SYSLOGD

- One for Logging from remote systems
- One for Local Logging



Central Log Repository

- Receive Messages from Remote SyslogD systems
 - Central Monitor Location
 - Messages from Multiple SYSLOGD Systems Logged in One Place
 - Filter messages based on remote Source IP Address or Hostname
- Sysplex Operlog configured as log stream in the Coupling Facility
 - Centralizes messages for entire SYSPLEX
 - Contains z/OS generated messages and syslogd messages
 - Better performance than having SYSLOGD write to /dev/console
- Two instances of SYSLOGD
 - Improved SYSLOGD Performance
 - Logging from Local applications only mode (-i option)
 - Logging from remote Network SYSLOGD only mode (-n option)
 - Multi-threaded syslogd for improved performance and message capturing reliability
- Best Practice:
 - If you use both local and network logging, use two instances of syslogd
 - Remote messages do not interfere with local logging performance



Defining SYSLOG Daemon



SyslogD Startup

- SyslogD start command

```
syslogd [-c] [-d] [-D value] [-f conffile] [-F value] [-i] [-m markinterval] [-n]
        [-p logpath] [-u] [-x] [-?]
*****
-c      CREATE the logfiles and directories automatically
-d      DEBUG mode
-D      Default DIRECTORY permissions when created (by -c)
-f <config filename> specify configuration file
-F      Default FILE permissions when created (by -c)
-i      RECEIVE only AF_UNIX messages (not from network)
-m      MINUTES between Mark Messages (used for syslogd testing)
-n      RECEIVE only AF_INET messages from network
-p      PATH (not recommended)
-u      INCLUDE userid and jobname
-x      Omits hostname lookup for messages received from remote SYSLOGD (performance
        improvement)
```

- Start SYSLOGD
 - /etc/rc
 - JCL Procedure and PROFILE.TCPIP AUTOLOG
 - COMMNDxx member in PARMLIB
- Both SYSLOG.CONF and SYSLOG.LOG can be created with permission bits of 644.
 - 6 = Owner can Read and Write
 - 4 = Group can Read
 - 4 = Other can Read

Unix Permission Bits for unix Files

| File Owner UID | File Owner GID | Ex- tended Attri- bute | Set UID | Set GID | Sticky | Owner | | | Group | | | Other | | | File Owner | Audit |
|-----------------------|----------------------|---------------------------------|------------|------------|--------|-------|-------|--------------|-------|-------|--------------|-------|-------|--------------|---------------|-------|
| | | | | | | Read | Write | Exec- ute | Read | Write | Exec- ute | Read | Write | Exec- ute | | |
| | | | | | | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | | |
| | | | | | | 2^2 | 2^1 | 2^0 | 2^2 | 2^1 | 2^0 | 2^2 | 2^1 | 2^0 | | |
| | | | | | | (4) | (2) | (1) | (4) | (2) | (1) | (4) | (2) | (1) | | |
| | | | | | | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | | |
| Permission of 755 is: | | | | | | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | | |
| Permission of 644 is: | | | | | | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | | |

For Log Files and Configuration Files, Permission bits of 644 are usually adequate.

For directories, Permission bits of 755 are usually adequate, unless a user needs to write to a directory he does not own.

/etc/rc

```
# Start the SYSLOG daemon for logging UNIX activity
_BPX_JOBNAME='NM2ASYSL' /usr/sbin/syslogd -f /etc/syslog.conf &
# /usr/sbin/syslogd -f /etc/syslog.conf &

.....

sleep 5

echo /etc/rc script executed, `date`
```

- Jobname "NM2ASYSL" if "_BPX_JOBNAME='NM2ASYSL'"
- Jobname "SYSLOGDn" if "_BPX_JOBNAME='SYSLOGD' "
- Jobname "ETCRCn" if started without "_BPX_JOBNAME="

JCL Procedure

Proc

```
//NM2ASYSL PROC MODULE='SYSLOGD',  
//          PARMS='-f /etc/syslog.conf'  
//*  
//*  
//SYSLOGD  EXEC  
PGM=&MODULE,REGION=4096K,TIME=NOLIMIT,  
//          PARM='POSIX(ON) ALL31(ON) /&PARMS'  
//SYSPRINT DD SYSOUT=*
```

PROFILE.TCPIP

```
AUTOLOG 5  
  NM2ASYSL          ; SYSLOG Daemon PROC  
ENDAUTOLOG  
  
PORT  
  514 UDP OMVS      ; SYSLOG Daemon
```

/etc/services

```
syslog          514/udp
```

Start

S proc_name
ie. S SYSLOGD

Display

D A,SYSLOGD*
IEE115I ...

| JOB | M/S | TS | USERS | SYSAS | ... |
|-----------------------------|-------|-------|-------|-------|-----|
| 00004 | 00011 | 00001 | 00035 | ... | |
| SYSLOGD1 STEP1 OMVSKERN ... | | | | | |

Stop

P proc_name
ie. P SYSLOGD1

SYSLOGD Configuration File



SYSLOGD Configuration File

- SYSLOGD configuration file contains two types of statements:
 - Logging Rules
 - Archive Configuration Statements
- Sample is located in the TCP/IP unix sample directory:
 - /usr/lpp/tcpip/samples/syslog.conf
- If you update syslog.conf, you can request SYSLOGD to re-read the configuration file without restarting SYSLOGD by sending a SIGHUP signal:
 - Modify syslogd
 - /F SYSLOGD,RESTART
 - kill -SIGHUP <pid number of syslogd>
 - kill -1 <pid> where -1 is the number 1

Logging Rules

- Logging rules in /etc/syslog.conf
- Each logging rule has an Identifier and a Destination
- SYSLOGD startup without -u

- Identifier consists of two parameters

| | |
|--------------------------------------|-----------------------|
| - IDENTIFIER | DESTINATION |
| - Facility_Name.Priority_Code | destination_path |
| ie. | |
| IDENTIFIER | DESTINATION |
| daemon.err | /tmplog/daemon.errlog |

- SYSLOGD startup with -u

- Identifier consists of four parameters

| | |
|---|-----------------------|
| - IDENTIFIER | DESTINATION |
| - User_ID.Job_Name.Facility_Name.Priority_Code | destination_path |
| ie. | |
| IDENTIFIER | DESTINATION |
| user9.ftpd1.daemon.err | /tmplog/daemon.errlog |

Both facility name and priority code are predefined. (That is, you cannot establish new facility names or priority codes.)

Facility Name

| | |
|----------|--|
| kern | Unix kernel messages |
| user | Default facility used when no other category applies |
| Mail | Mail system messages |
| news | Usenet system messages |
| uucp | uucp messages |
| daemon | Server messages |
| auth | Authorization messages |
| authpriv | Same as auth |
| cron | cron system messages |
| lpr | Printing system messages |
| local0-7 | Facility names meant for local use TelnetD uses local1 to log its messages IKE uses local4 |
| * | Placeholder used to represent any facility name |
| mark | Provides heartbeat messages |

Application usage of Facilities is documented in a table in the Syslog daemon chapter of the IP Config Ref manual.

Priority Codes

| | |
|---------|--|
| emerg | Emergency - system is becoming unusable |
| panic | Same as emerg |
| alert | Immediate action is required |
| crit | Critical condition - device or is becoming unusable |
| error | Error condition |
| warning | Warning condition |
| notice | Normal, but significant condition |
| info | Information message |
| debug | Debugging message |
| none | Placeholder used to represent none of the priorities |
| * | Placeholder used to represent all priority codes |

- NOTE: A priority code includes all above priorities.
 - Emerg is the highest priority.

Destination

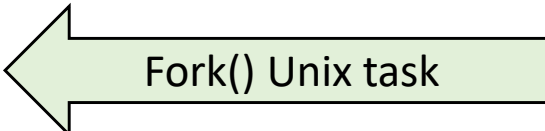
- A file in the hierarchical file system
 `auth.* /tmplog/syslogd/auth.log`
- One or more local shell users
 `facility_name.priority_code user1,user2`
 `facility_name.priority_code *`
- A SyslogD server on another host
 `facility_name.priority_code @myaixserver`
- Remote SYSLOGD messages can be separated by remote IP Address or Hostname
 `(host14.xyz.com).*. * /var/log/rslog14.log`
 `(10.42.15.0/24).*. * /var/log/rslog15.log`
- MVS Operlog (if it has been implemented)
 `*.* /dev/operlog`
- The MVS console
 `facility_name.priority_code /dev/console`
- Don't log the messages with Priority Code of ".none":
 `mail.err /var/log/mail.log`
 `*.err;mail.none; /var/log/err.log`

SYSLOGD -u and Symbols

- When SYSLOGD is started with -u the Identifier consists of four parameters

| IDENTIFIER | DESTINATION |
|--|------------------|
| User_ID.Job_Name.Facility_Name.Priority_Code | destination_path |

- User_ID and Job_Name enables separation of logged messages

| | | |
|---------------------|-----------------------------|---|
| - *.ftpd*.*.* | /var/log/ftpd.log |  |
| - user7*.*.* | /var/log/user7.log | |
| - user8.ftpserv1*.* | /var/log/user8_ftpserv1.log | |
| - user9.ftpserv2*.* | /var/log/user9_ftpserv2.log | |

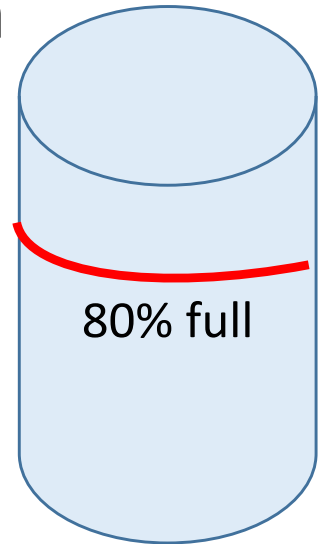
- File names can be created using symbols for date:
 - userx.job3*.* /var/%Y/%m/%d/userx_job3.log
 - %Y represents the current year
 - %m represents the current month
 - %d represents the current day
 - Path is created for symbols even without SYSLOGD startup with -c

Automatic Archiving



Archive Configuration Statements

- Also referred to as Global syslogd Configuration Statements
- Specified in SYSLOGD configuration file
- ArchiveThreshold
 - Define Archive due to the file system being a percentage in use (full)
- ArchiveTimeOfDay
 - Define Archive due to a time of day
- BeginArchiveParms/EndArchiveParms
 - Define a prefix to use for Archiving



Archive when Threshold is reached, or by Time of Day, or both.

Archive Destination

- IDENTIFIER DESTINATION -F *file_acc_per* -D *dir_acc_per* -N *archive_prefix* -X
 - *file_acc_per* defines the unix permissions for allocated file
 - *dir_acc_per* defines the unix permissions for allocated directory
 - *archive_prefix* is used with the BeginArchiveParms statement
 - -X causes the log file to be deleted and a new file created
- Archive sequential data set is created with name:
 - prefix.archive_prefix.data_suffix.time_suffix
 - prefix is defined on BeginArchiveParms
 - archive_prefix is defined by -N on Logging Rule
 - data_suffix is the date Dyymmdd
 - time_suffix is the time Thhmmss
- When Archive is Generation Data Group (GDG) data set:
 - prefix.archive_prefix.gdg_suffix
 - gdg_suffix is an automatic unique value, ie. G0007V00

Archive Threshold Examples

ArchiveThreshold 80

ArchiveTimeOfDay 00:01 (24 hour format)

BeginArchiveParms

DSNPrefix USER1.SYSTRACE

Unit SYSDA

EndArchiveParms

daemon.debug /var/log/daemon.trace -N DAEMON

Local1.debug /var/log/local1.trace -N LOCAL1

BeginArchiveParms

DSNPrefix USER1.SYSLOG

Unit SYSDA

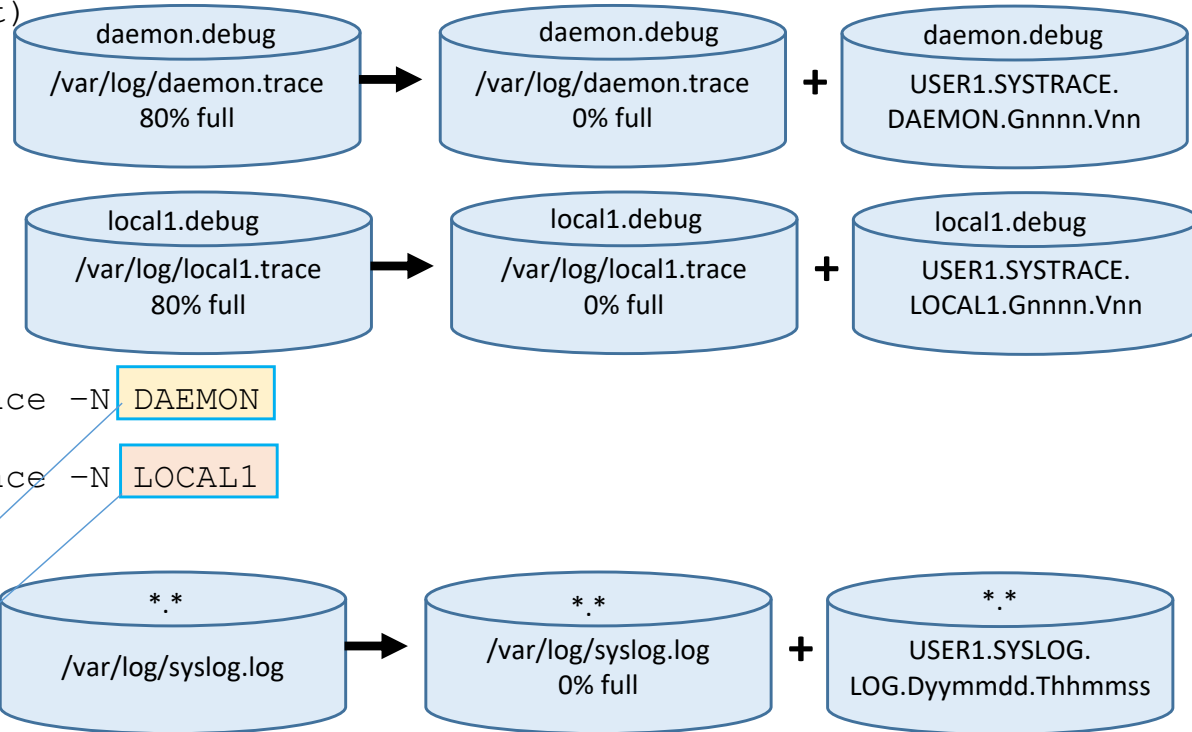
EndArchiveParms

. /var/log/syslog.log -N LOG

- The following archive data set names are created:

- USER1.SYSTRACE.DAEMON.GnnnnVnn
- USER1.SYSTRACE.LOCAL1.GnnnnVnn
- USER1.SYSLOG.LOG.Dyymmdd.Thhmmss

004_ZCS301_SYSLOGD



Note: Archiving requires -c on syslogd startup

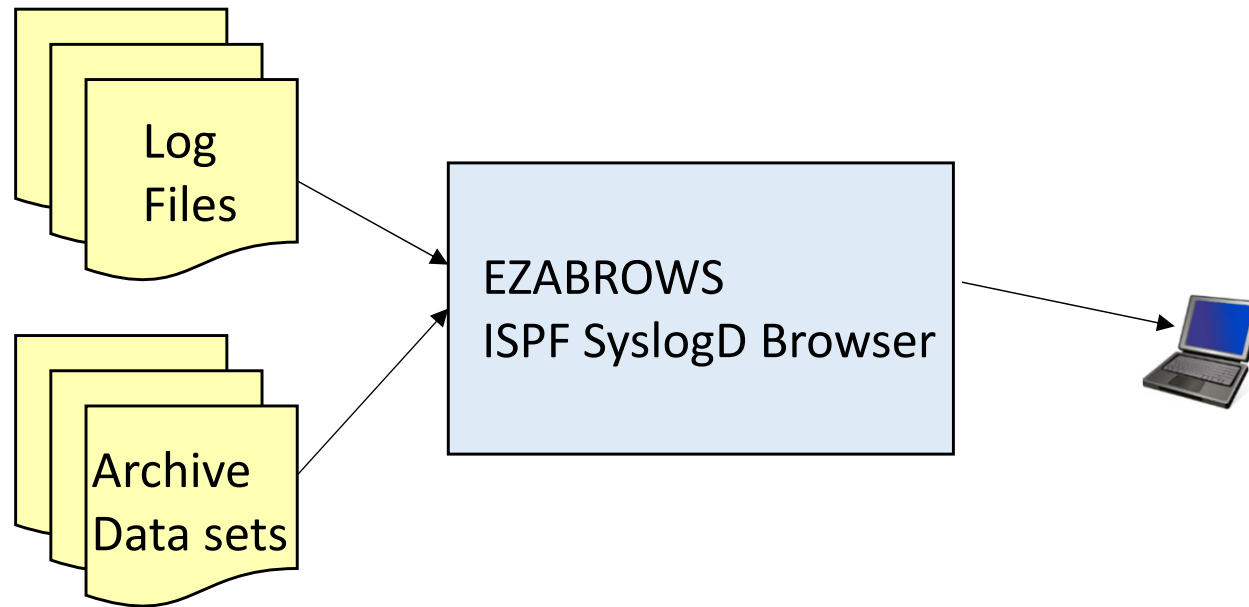
GDG data set

Sequential data set

SyslogD ISPF Browser



ISPF SyslogD Browser



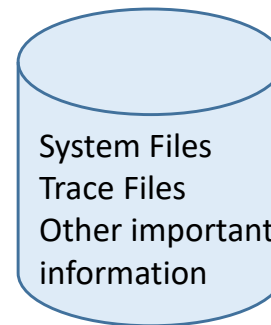
- EZABROWS

- Reads SYSLOGD configuration file to learn active log files and archive data sets
- Displays and Searches active log files and archive data sets

Log File Management



SyslogD File Location




Root unix at Mountpoint "/"
OMVS.HFS.TMP at Mountpoint "/tmp"

- Root unix Mountpoint "/"
 - Do not log to files that fill up the MVS dataset that is mounted at Root "/".
 - Root "/" is needed for System Files, Trace Files, and other important files.
- Mountpoint "/tmp"
 - Do not log to files that fill up the MVS dataset that is mounted at "/tmp".
 - "/tmp" may be needed for log data that cannot be rerouted to another path.
- Temporary Files System (TFS)
 - Do not use a TFS syslogd logging because you will lose important messages if the system crashes.
- Mountpoint "/var"
 - If you use "/var" for syslogd log files mount an MVS dataset at that mountpoint to avoid interfering with other paths.
- Mountpoint "/tmplog"
 - Create a directory like "/tmplog" and mount an MVS dataset at that mountpoint for syslogd log files.
- No matter what directory path you use, make sure you monitor it to be sure syslogd logging is not interrupted due to lack of space.
 - df (shows all usage)
 - df -P /tmp (shows usage for mount point /tmp)

Display Unix File Usage


- df

```
***** Top of Data *****
- Mounted on      Filesystem      Avail/Total      Files      Status
- /u/users        (OMVS.HOMEDIRS.HFS)  12904/12960      4294967292 Available
- /u/tf           (OMVS.TF.HFS)        1400/1440        4294967294 Available
- /u/rdm          (OMVS.RDM.HFS)       177032/177120    4294967293 Available
- /u/jc           (OMVS.JC.HFS)        1400/83520       4294967051 Available
- /u/harris1      (OMVS.HARRISL.HFS)   176976/177120    4294967288 Available
- /u/gdente       (OMVS.GDENTE.HFS)   161552/177120    4294967238 Available
- /usr/lpp/HOD    (OMVS.HOD40.HOM.HFS) 222968/1308960   4294918223 Available
- /tmp            (OMVS.NM2.TMP)       174152/182880    4294967208 Available
- /etc            (OMVS.V2R7.ETC.HFS)  6792/11520       4294966979 Available
- /               (OMVS.V2R7.PUT9904.BASE.HFS) 131696/1398240 4294953323 Available
- ***** Bottom of Data *****
```



- df -P /tmp

```
***** Top of Data *****
- Filesystem      512-blocks      Used Available Capacity Mounted on
- OMVS.NM2.TMP    182880          8736    174144      5% /tmp
- ***** Bottom of Data *****
```



SMS Managed Volume

Data Set Information

Command ===>

Data Set Name . . . : OMVS.NM2.TMP

General Data

Management class . . : STANDARD

Storage class . . . : SCOMVS

Volume serial . . . : NM27AF

Device type : 3390

Data class :

Organization . . . : PO

Record format . . . : U

Record length . . . : 0

Block size : 0

1st extent cylinders: 5

Secondary cylinders : 1

Data set name type : HFS

Current Allocation

Allocated cylinders : 127

Allocated extents . : 123

Maximum dir. blocks : NOLIMIT

Current Utilization

Used pages : 1,176

% Utilized : 5

Number of members . : 40

Creation date . . . : 1998/05/29

Referenced date . . : 1999/10/21

Expiration date . . : ***None***

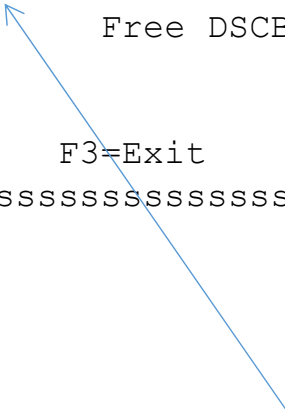
- Even though the usage percentage is not of concern, the limit of 123 extents has been reached.

SMS Managed Volume

```

Eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee VTOC Summary Information eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeN
e Volume . . : NM27AF e
e Command ==> e
e e
e Unit . . : 3390 e
e e
e Volume Data VTOC Data Free Space Tracks Cyls e
e Tracks . . : 50,085 Tracks . . : 29 Size . . : 717 47 e
e %Used . . : 98 %Used . . : 5 Largest . . : 285 19 e
e Trks/Cyls: 15 Free DSCBS: 1,379 e
e Free Extents . . : 8 e
e e
e F1=Help F2=Split F3=Exit F9=Swap F12=Cancel e
DeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeM

```



- Total Used = 98%

Time Stamps



Setting Time in z/OS

z/OS

MVS

SYS1.PARMLIB(IEASYS00)

CLOCK=00,
OMVS=07,

SYS1.PARMLIB(CLOCK00)

TIMEZONE W.05.00.00 EST

or

TIMEZONE W.04.00.00 EDT



Hardware Clock:
GMT (UTC)

Unix

/etc/init.options

-e TZ=EST5EDT

/etc/rc daemons

/etc/profile

TZ=EST5EDT

shell users

SYSLOGD Log (Time not Synchronized)

Jul 8 [15:24:03](#) WSC1 FSUM1220 syslogd: restart

Jul 8 19:25:53 WSC1 Config[67108868]: EZZ0300I OPENED PROFILE FILE

Jul 8 19:25:53 WSC1 Config[67108868]: EZZ0309I PROFILE PROCESSING

.....

Jul 8 19:28:11 WSC1 ftpd[369098755]: EZYFT18I Using catalog

Jul 8 19:28:11 WSC1 ftpd[369098755]: EZYFT08W Unable to get port

Jul 8 19:28:11 WSC1 ftpd[369098755]: EZY2697I IBM FTP CS V2R7

Jul 8 19:28:12 WSC1 ftpd[369098755]: EZY2640I Using

Jul 8 19:28:12 WSC1 ftpd[369098755]: EZYFT47I dd:SYSFTPD file,

.....

Jul 8 19:28:12 WSC1 ftpd[1577058316]: EZY2702I Server-FTP:

Jul 8 19:28:12 WSC1 ftpd[1577058316]: EZYFT41I Server-FTP: process

Jul 8 [15:36:15](#) WSC1 inetd[83886093]: FOMN0044 Unable to lock /etc/inetd.pid:
EDC5112I Resource temporarily unavailable., rsn=055501B7

Jul 8 [15:39:12](#) WSC1 inetd[134217741]: FOMN0026 otelnet/tcp: unknown service

Jul 8 [15:47:25](#) WSC1 telnetd[33554448]: IP address is 9.82.131.114

NETSTAT (Time not Synchronized)

==> netstat home

GMT or UDC Time



MVS TCP/IP NETSTAT CS V2R7 TCPIP NAME: NM2ATCP 21:49:42

Home address list:

| Address | Link | Flg |
|---------------|----------|-----|
| ----- | ---- | --- |
| 192.168.251.1 | VLINK1 | |
| 192.168.253.1 | VLINK2 | |
| 9.82.1.170 | TR1 | P |
| 9.82.67.170 | LNK2BTCP | |

Local (CLOCKnn=TIMEZONE W.04.00.00)



TIME-05:50:46 PM. CPU-00:00:05 SERVICE-663221 SESSION-01:49:17 JULY 14,2008

Synchronize Time Zones – Best Practice

- `SYS1.PARMLIB(CEEPRMxx)`
 - `CEEDOPT(ALL31(ON), ENVAR('TZ=EST5EDT'))`
 - `CEECOPT(ALL31(ON), ENVAR('TZ=EST5EDT'))`
 - `CELQDOPT(ALL31(ON), ENVAR('TZ=EST5EDT'))`
- Default Parmlib CEEPRMxx is found in CEE.SCEESAMP.

SYSLOGD Log (Time Synchronized)

Jul 8 08:31:34 LO0 FSUM1220 syslogd: restart

Jul 8 12:33:47 LO0 ConfigY16777218": EZZ0300I OPENED PROFILE FILE

Jul 8 12:33:48 LO0 ConfigY16777218": EZZ0316I PROFILE PROCESSING

Jul 8 12:33:48 LO0 ConfigY16777218": EZZ0334I IP FORWARDING IS

Jul 8 12:33:48 LO0 ConfigY16777218": EZZ0335I ICMP WILL IGNORE

Jul 8 12:33:48 LO0 ConfigY16777218": EZZ0352I VARIABLE SUBNETTING

Jul 8 12:33:48 LO0 ConfigY16777218": EZZ0345I STOPONCLAWERROR IS

Jul 8 12:34:03 LO0 ConfigY16777218": EZZ0403I TELNET/VTAM (SECOND

Jul 8 12:34:04 LO0 ftpdY13": EZYFT18I Using catalog '/usr/lib/nls

Jul 8 12:34:04 LO0 ftpdY13": EZY2697I IBM FTP CS V2R7 12:34:04

Jul 8 12:34:04 LO0 ftpdY13": EZY2640I Using dd:SYSFTPD=SYS1.TCPP

Jul 8 12:34:04 LO0 ftpdY13": GU0754 chkunit: unitname 3390

Jul 8 12:34:04 LO0 ftpdY13": EZYFT21I Using catalog '/usr/lib/nlst

Jul 8 12:34:06 LO0 snmpagentY16": EZZ6202I Using catalog 'snmpd

Jul 8 12:34:06 LO0 snmpagentY16": EZZ6232I The SNMP agent is run

Jul 8 12:34:06 LO0 snmpagentY16": EZZ6295I SNMP agent: Dynamic

.....

Jul 8 12:37:49 LO0 telnetdY167772177": EYZTE52E Couldn't resolve

Jul 8 12:37:49 LO0 telnetdY167772177": IP address is 9.82.1.107

NETSTAT (Time Synchronized)

==> netstat home

MVS TCP/IP NETSTAT CS V2R7

TCPIP NAME: NM2ATCP 18:04:34

Home address list:

| Address | Link | Flg |
|---------|------|-----|
|---------|------|-----|

| ----- | ---- | --- |
|-------|------|-----|
|-------|------|-----|

| | | |
|---------------|--------|--|
| 192.168.251.1 | VLINK1 | |
|---------------|--------|--|

| | | |
|---------------|--------|--|
| 192.168.253.1 | VLINK2 | |
|---------------|--------|--|

| | | |
|------------|-----|---|
| 9.82.1.170 | TR1 | P |
|------------|-----|---|

| | | |
|-------------|----------|--|
| 9.82.67.170 | LNK2BTCP | |
|-------------|----------|--|

TIME-06:05:30 PM. CPU-00:00:05 SERVICE-773160 SESSION-02:04:01 JULY 14,1999

Appendix: Cron Daemon

CRON was popular prior to Automatic Archive option.
Use Automatic Archive or CRON, not both!



CRON

- CRON Daemon is a work scheduler for Unix in z/OS.



Files used by CRON

- /etc/mailx.rc file
 - Only required for cron to send messages via sendmail.
- /usr/lib/cron directory contains:
 - at.allow – contains the list of users who have permission to use at command
 - at.deny - contains the list of users who do not have permission to use at command
 - cron.allow - contains the list of users who have permission to use crontab command
 - cron.deny - contains the list of users who do not have permission to use crontab command
- /usr/spool/cron directory contains:
 - log - file that maintains a history of the commands being run
 - pid - file that cron uses to ensure that only one version of cron is currently running
 - queuedefs – defines queue values
- /usr/spool/cron/atjobs directory contains:
 - at files
- /usr/spool/cron/crontabs directory contains:
 - crontab files (cron job files)

Start CRON Daemon

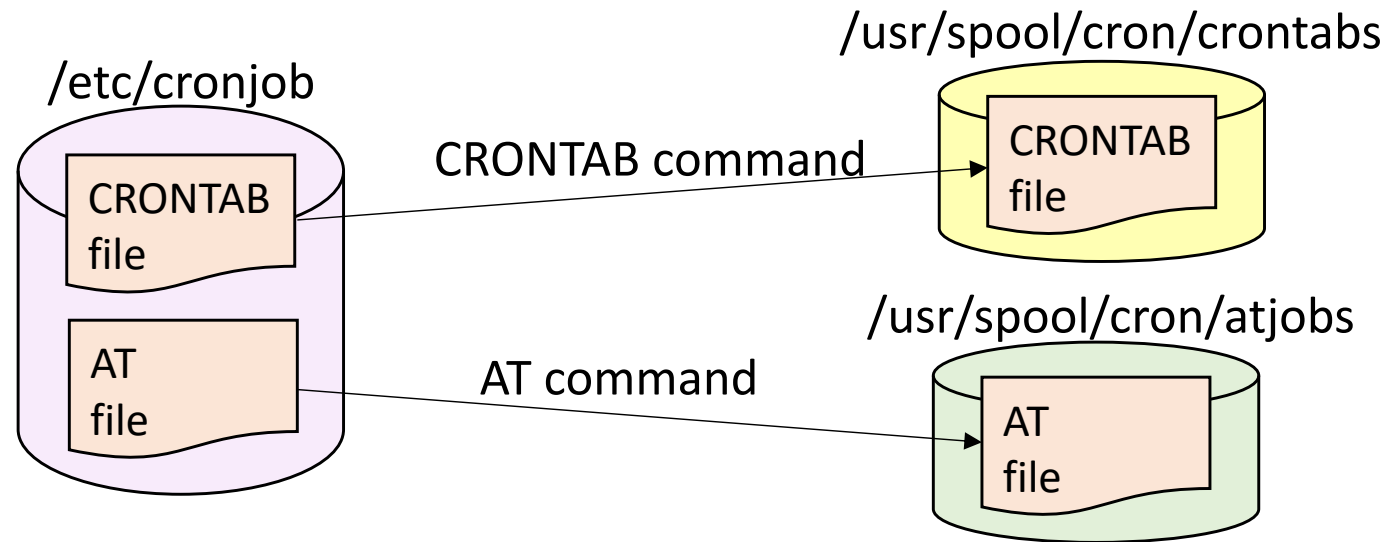
- /etc/rc

```
# Start the SYSLOG daemon for logging UNIX activity
_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf &
# Start the INET daemon for remote login activity
_BPX_JOBNAME='INETD' /usr/sbin/inetd /etc/inetd.conf &
# Start the CRON daemon for automated, timed operations
_BPX_JOBNAME='CRON' /usr/sbin/cron &
#
sleep 5
echo /etc/rc script executed, `date`
```

- D OMVS,A=ALL

```
OMVSKERN CRON7 0033 16777221 1 1KI 08.24.48 .053
LATCHWAITPID= 0 CMD=/usr/sbin/cron
```

CRON Commands



- Three different commands for submitting CRON Files:
 - CRONTAB – for CRON files defining repeating CRON jobs
 - AT – for CRON files defining one time CRON jobs
 - BATCH – for CRON files defining one time batch CRON jobs
- Implementation Steps
 - Create CRONTAB, AT, or BATCH file
 - Use CRONTAB, AT, or BATCH command to submit the file to CRON

CRONTAB Job File

CRONTAB file syntax:

Mininue Hour Day Month DayOfWeek command

Minute Day Day of Week
↓ ↓ ↓
53 23 * * 0 echo Now replacing log files with the A set
↑ ↑ ↑
Hour Month Execution string

```
# This is a sample crontab file stored
# in my maintenance directory
52 23 * * 0 echo Now replacing log files with the A set
53 23 * * 0 cp /etc/syslog.conf.a /etc/syslog.conf
54 23 * * 0 kill -SIGHUP $(cat /etc/syslog.pid)
55 23 * * 0 cp /tmp/syslog.log.b /tmpback/syslog.log.backb
58 23 * * 0 rm /tmp/syslog.log.b
59 23 * * 0 touch /tmp/syslog.log.b
```

CRONTAB Command

- `CRONTAB [-u user] [filename] --` highly recommended!
 - Copies file into CRON directory `/usr/spool/cron/crontabs` for use.
 - Superuser may define a specific user to associate the file with.
 - Recommended instead of `CRONTAB -e` which can inadvertently delete the crontab entry.
- `CRONTAB -l [-u user] --` to list your current crontab tasks
- `CRONTAB -r [-u user] --` to delete a file from crontab subdirectory
- `CRONTAB -e [-u user]` – lets you edit your crontab entry. Define editor environment variable or crontab defaults to `vi`. Not recommended - don't directly edit the file! You could inadvertently delete your entries.

AT Command

- `at [-m] [-f file] [-q queue] -t time`
- `at [-m] [-f file] [-q queue] timespec`
- `at -r [-q queue] at_job ...`
- `at -l [-q queue] [at_job ...]`
- `-f file` Reads commands from *file* rather than from standard input (stdin).
- `-l` Displays all jobs you have submitted with at command.
- `at_job` Filters display to only show jobs with matching job name.
- `-m` Sends you mail after your job has finished running.
- `-q queue` Specifies the queue your at job is to be recorded in or removed from.
- `-r at_job` Removes previously scheduled at jobs.
- `-t time` Specifies the time for the system to run the job.
- When you do not use the `-t` option, you can use a *timespec* argument to specify the time.
- A *timespec* argument consists of three parts: a time, a date, and an increment. You must always specify the time, but you can omit the date, the increment, or both.
 - For time specification see the z/OS UNIX System Services Command Reference, SA23-2280
- The **batch** command is equivalent to:
 - `at -q b -m now`

Using Cron Steps

- Start CRON in /etc/rc during OMVS startup:
Start Cron
_BPX_JOBNAME='CRON' /usr/sbin/cron &
- Create flat cron job file - such as /etc/cronjob which contains:
0 0 * * * kill -HUP `cat /etc/syslog.pid`
0 0 * * * /u/user1/rmoldlogs
- Execute crontab command to load cron job file:
crontab /etc/cronjob
- List cron jobs:
USER1:/u/user1: >crontab -l
0 0 * * * kill -HUP `cat /etc/syslog.pid`
0 0 * * * /u/user1/rmoldlogs

CRON Log

- This is the cron log stored in `/usr/spool/cron/log`.

```
>  CMD: echo Replace log files with A set and Copy B to MVS
>  OMVSKERN 184549386 c Tue Jul 13 23:51:03 1999
<  OMVSKERN 184549386 c Tue Jul 13 23:51:04 1999 rc=0
>  CMD: /etc/replaceb.sh
>  OMVSKERN 201326602 c Tue Jul 13 23:52:00 1999
<  OMVSKERN 201326602 c Tue Jul 13 23:52:08 1999 rc=0
>  CMD: echo If only the weekend could begin now!
>  OMVSKERN 939524108 c Wed Jul 14 12:15:01 1999
<  OMVSKERN 939524108 c Wed Jul 14 12:15:02 1999 rc=0
>  CMD: echo Commit random acts of kindness!
>  OMVSKERN 956301324 c Wed Jul 14 12:56:01 1999
<  OMVSKERN 956301324 c Wed Jul 14 12:56:01 1999 rc=0
```


Mail Log

- Activity also shows up in /usr/mail/(username), as identified by the CRONTAB entry names.

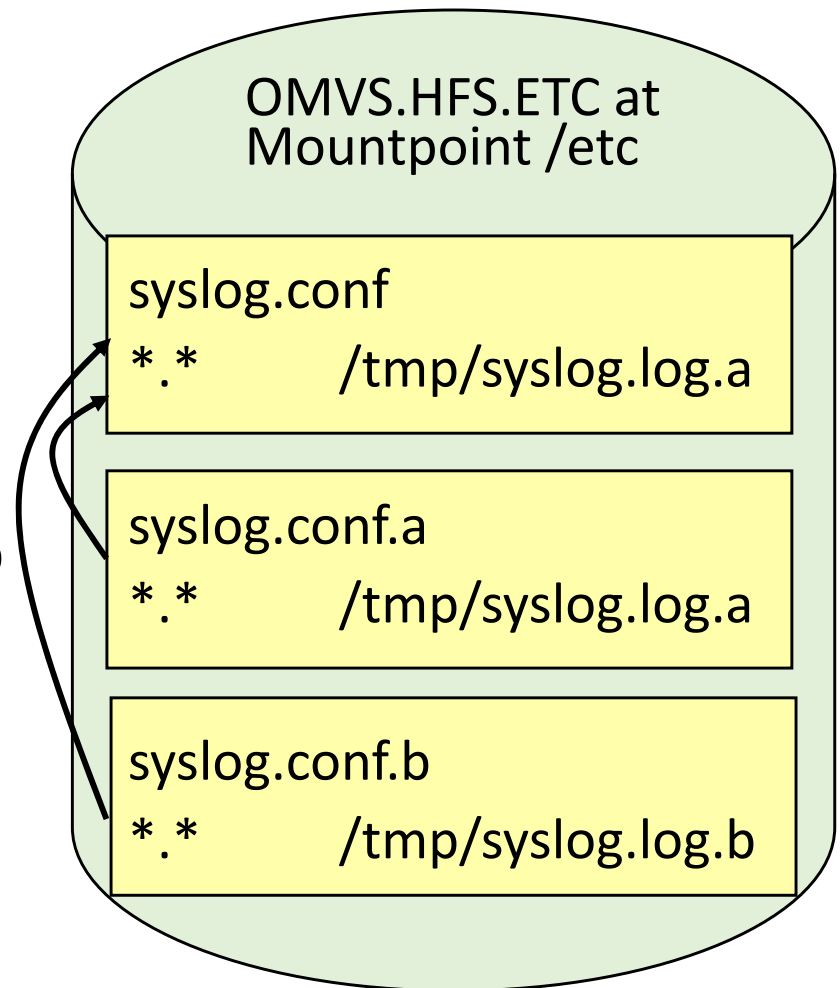
```
From OMVSKERN Tue Jul 13 23:52:10 1999
To: OMVSKERN

alloc da('gdente.syslog.log.b') dsorg(ps) space(3,1) cylinders 1
oget '/tmp/syslog.log.b' 'gdente.syslog.log.b'
BPXF112W THE RECORD SIZE IN THE OUTPUT DATA SET IS SMALLER THAN

*****
Cron: The previous message is the standard output
      and standard error of one of your cron commands.
```

Manage SYSLOGD with CRON

- Create “a” and “b” version of syslog configuration file.
- Day 1
 - cp syslog.conf.a syslog.conf
 - Messages are logged to /tmp/syslog.log.a
 - Optionally backup /tmp/syslog.log.b
 - Remove /tmp/syslog.b
- Day 2
 - cp syslog.conf.b syslog.conf
 - Messages are logged to /tmp/syslog.log.b
 - Optionally backup /tmp/syslog.log.a
 - Remove /tmp/syslog.log.a
- Repeat swapping files each day.



Sample CRONTAB File (unix to unix)

```
# Copies logs into HFS dataset
# ORIGINAL Crontab named OMVSKERN.hfs stored in
# /usr/spool/cron/crontabs
# Every night archive log except Saturday night
# Another process archives log files on /tmpback to tape or other
52 23 * * 0 echo Now replacing log files with the A set
53 23 * * 0 cp /etc/syslog.conf.a /etc/syslog.conf
54 23 * * 0 kill -SIGHUP $(cat /etc/syslog.pid)
55 23 * * 0 cp /tmp/syslog.log.b /tmpback/syslog.log.backb
58 23 * * 0 rm /tmp/syslog.log.b
59 23 * * 0 touch /tmp/syslog.log.b
#
52 23 * * 1 echo Now replacing log files with the B set
53 23 * * 1 cp /etc/syslog.conf.b /etc/syslog.conf
54 23 * * 1 kill -SIGHUP $(cat /etc/syslog.pid)
55 23 * * 1 cp /tmp/syslog.log.a /tmpback/syslog.log.backa
58 23 * * 1 rm /tmp/syslog.log.a
59 23 * * 1 touch /tmp/syslog.log.a
#
    AND SO ON THROUGH DAY 5!
```

Sample CRONTAB File (unix to MVS)

```
# Copies logs into MVS dataset
# Every night archive log except Saturday night
# Another process archives log files to tape or other from MVS
#
52 23 * * 0 echo Now replacing log files with the A set
53 23 * * 0 cp /etc/syslog.conf.a /etc/syslog.conf
54 23 * * 0 kill -SIGHUP $(cat /etc/syslog.pid)
55 23 * * 0 tso -t "OGET '/tmp/syslog.log.b' 'GDENTE.SUNLOG.MVS'"
58 23 * * 0 rm /tmp/syslog.log.b
59 23 * * 0 touch /tmp/syslog.log.b
#
52 23 * * 1 echo Now replacing log files with the B set
53 23 * * 1 cp /etc/syslog.conf.b /etc/syslog.conf
54 23 * * 1 kill -SIGHUP $(cat /etc/syslog.pid)
55 23 * * 1 tso -t "OGET '/tmp/syslog.log.b' 'GDENTE.MONLOG.MVS'"
58 23 * * 1 rm /tmp/syslog.log.a
59 23 * * 1 touch /tmp/syslog.log.a
#
#           AND SO ON THROUGH DAY 5!
```

Appendix: Cron Example



Sample CRONTAB File (unix to MVS)

```
# Copies logs into MVS dataset
# Every night archive log except Saturday night
# This CRONTAB = /etc/OMVSKERN.scr2
# Another process archives the log files from MVS to GDS and/or tape
#
51 23 * * 0 echo Replace log files with A set & Copy B to MVS
52 23 * * 0 /etc/replaceb.sh
#
51 23 * * 1 echo Replace log files with B set & Copy A to MVS
52 23 * * 1 /etc/replacea.sh
#
51 23 * * 2 echo Replace log files with A set & Copy B to MVS
52 23 * * 2 /etc/replaceb.sh
#
51 23 * * 3 echo Replace log files with B set & Copy A to MVS
52 23 * * 3 /etc/replacea.sh
#
#           AND SO ON THROUGH DAY 5!
```

CRONTAB Shell Script (unix to MVS)

```
# Step 1) Setting up Variables
# LOG_DIRECTORY is the path of the syslogs files. i.e. /tmp/syslog
LOG_DIRECTORY='/tmp'
# The following variables hold the names of the various log files
SYSLOG_LOGA='syslog.log.a'
# ERROR_LOG='error.log'
# DS_PREFIX is the Data Set Prefix. Files will be named with this hlq
# For example, HFS error.log becomes 'gdente.error.log' in MVS
DS_PREFIX='gdente'
# The following loop iterates through all the log files and executes
# the commands in the loop on each file.
#for LOGFILE in $SYSLOG_A $ERROR_LOG
for LOGFILE in $SYSLOG_LOGA
do
#
# Step 2) Allocating MVS Datasets
#
tso -t "alloc da('$DS_PREFIX.$LOGFILE')dsorg(ps)space(3,1) cylinders \
lrecl(132) blksize(13200) recfm(f,b) volume(csscat) unit(sysda) old"
#lrecl(132) blksize(13200) recfm(f,b) volume(csscat) unit(sysda) new"
#
```

CRONTAB Shell Script (unix to MVS)

```
# Step 3) Swap out syslogd.conf files (Copy B configuration file
#         into /etc/syslog.conf to record on B logs)
#
cp /etc/syslog.conf.b /etc/syslog.conf
#
# Step 4) Force SYSLOGD to reread the new configuration file
#
kill -SIGHUP $(cat /etc/syslog.pid)
# Step 5) Copy old A logs to an MVS Dataset and wait 1 minute
sleep 1
tso -t oget \'$LOG_DIRECTORY/$LOGFILE\' \'$DS_PREFIX.$LOGFILE\'
# Step 6) Delete and Recreate the A log file
#         We've copied the specified file if it exists,
#         so now we should delete and recreate the log file.
rm $LOG_DIRECTORY/$LOGFILE
touch $LOG_DIRECTORY/$LOGFILE
#
# DONE - files should now be in a MVS dataset for some other archiver
# to handle. Every night, with the exception of Saturday, the cron
# daemon uses the crontab entry to swap out the log files. Archiver
# program must run at least every two days; otherwise the data is
# overwritten with a new tso allocate command ("old").
done
```

End of Topic



End of Topic

