IBM SWG – Enterprise Networking Solutions

Configuring, operating, and monitoring Policy Agent

Alfred B Christensen – alfredch@us.ibm.com
Raleigh, NC, US

Configuring, operating, and monitoring Policy Agent

Date and time:	Thursday 5th November, 2009 from 10:30 to 11:30
Program:	Network Management working group
Speaker:	Alfred B Christensen, IBM
Abstract:	Many important functions provided by z/OS Communication Server, such as AT-TLS, IPSec filtering and VPNs, IDS, etc. - either require configuration through the policy agent, or can benefit from policy-based customization. However, if policy agent is new to you, or if you haven't taken a look at it recently, you may have concerns about implementing policy-based functions due to the anticipated learning curve. In this session we will try to flatten that curve by explaining how to configure the policy-related components using traditional MVS data sets and JCL procedures, how to operate, and how to monitor policy agent and related components. The session will also introduce significant networking policy infrastructure enhancements in z/OS V1R11, such as automated archive of Syslogd files to MVS data sets, an ISPF browse and search application for accessing the Syslogd files and archives, and new functions in Policy Agent to start, monitor, and stop the other related policy components.

One-day IBM ITSO workshop on how to assess, plan for, and implement the z/OS V1R11 Communications Server enhancements:

System z Networking Technologies Update, WRZ005GB
Starts 10th November 2009 for 1 day in Bedfont Lakes, U.K.
Contact Name: Khaled Ibrahim - Khaled_Ibrahim@uk.ibm.com

http://www.redbooks.ibm.com/projects.nsf/WorkshopIndex/

Trademarks, notices, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

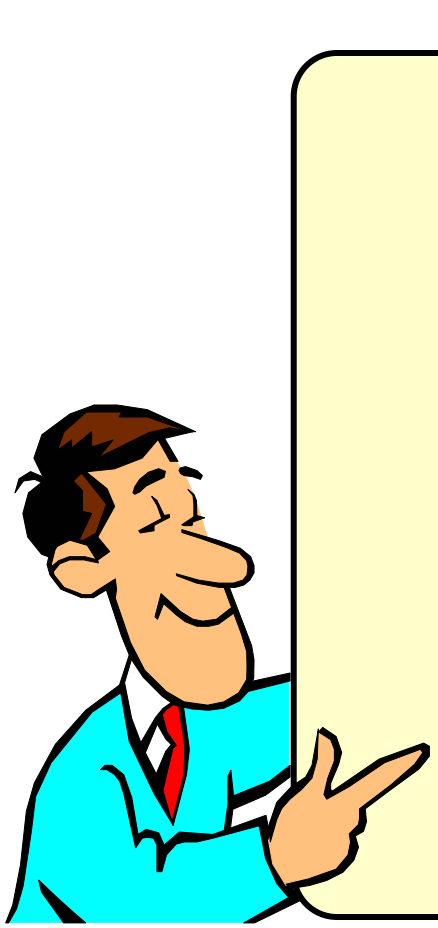
- Advanced Peer-to-Peer Networking®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e business(logo)®
- ESCON®
- FICON®
- GDDM®
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM (logo)®
- IBM®
- IMS
- IP PrintWay
- IPDS
- iSeries
- LANDP®
- Language Environment®
- MQSeries®
- MVS
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/400®
- OS/2®
- OS/390®
- OS/400®
- Parallel Sysplex®
- PR/SM
- pSeries®
- RACF®
- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x
- System z
- System z9
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat is a trademark of Red Hat, Inc.
- SUSE® LINUX Professional 9.2 from Novell®
- Other company, product, or service names may be trademarks or service marks of others.
- This information is for planning purposes only. The information herein is subject to change before the products described become generally available.
- Disclaimer: All statements regarding IBM future direction or intent, including current product plans, are subject to change or withdrawal without notice and represent goals and objectives only. All information is provided for informational purposes only, on an “as is” basis, without warranty of any kind.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

Refer to www.ibm.com/legal/us for further legal information.

Agenda



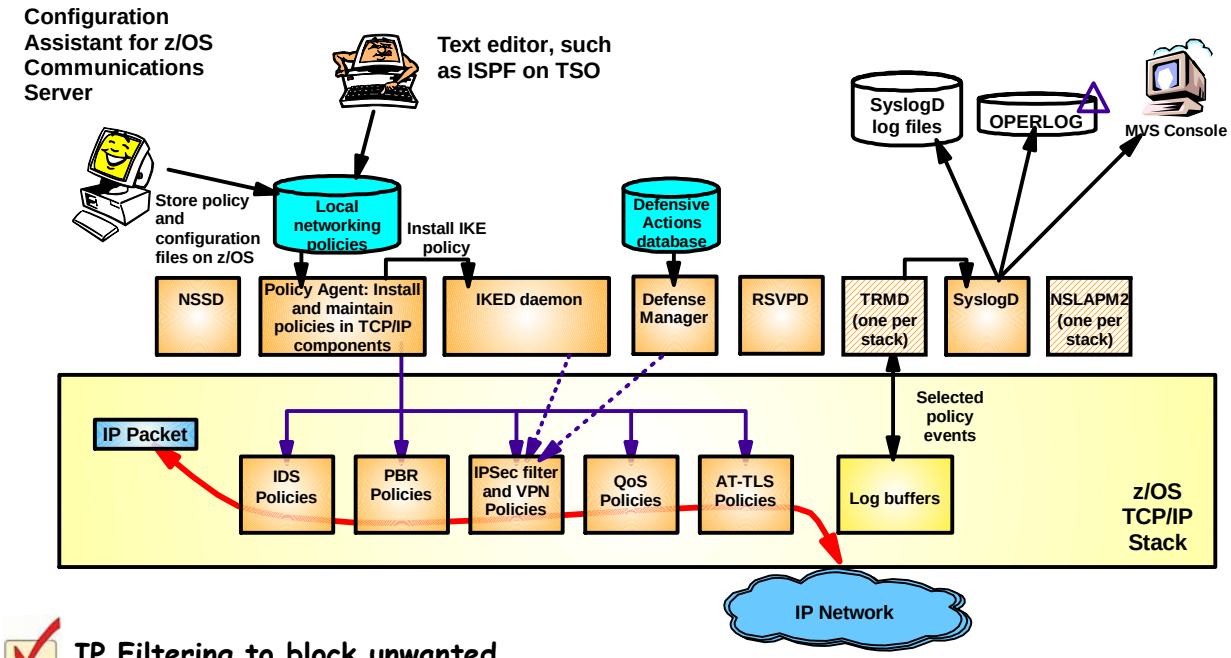
- z/OS networking policy infrastructure overview
- Setting up and managing Syslogd and TRMD
- Setting up and managing policy agent (PAGENT)
- Getting started with Configuration Assistant

Disclaimer: All statements regarding IBM future direction or intent, including current product plans, are subject to change or withdrawal without notice and represent goals and objectives only. All information is provided for informational purposes only, on an "as is" basis, without warranty of any kind.

Configuring, operating, and monitoring Policy Agent

z/OS networking policy infrastructure overview

z/OS Communications Server policy infrastructure overview



- **Perceived by some as a complex infrastructure**
  - Some initial cost to set up and enable the infrastructure
  - Difficult to manage and operate the infrastructure
  - But many valuable functions
- **z/OS V1R11 Communications Server simplifies the overall setup and operation of the networking policy infrastructure**
  - Making it simpler to gain the benefits of the networking policy-based functions on z/OS

IP Filtering to block unwanted traffic from entering or leaving your z/OS system

Connection-level security for TCP applications without application changes

Making sure high-priority applications also get high-priority processing by the network

Application-specific selection of outbound interface and route (Policy-based routing PBR)

Providing secure end-to-end IPSec VPN tunnels on z/OS

Protection against "bad guys" trying to attack your z/OS system

Which address spaces are needed for what?

- Sample LPAR configuration with common INET and two TCP/IP stacks (Stack1 and Stack2) that both need networking policy support

Policy Type	Shared by all stacks on the LPAR					Stack1		Stackn	
	PAGENT	NSSD (1)	IKED	RSVPD	SYSLOGD	TRMDA	SLAPA	TRMDn	SLAPn
QoS	Required			Optional			Optional		Optional
IDS	Required				Required	Required		Required	
AT-TLS	Required				Required				
IPSec filters	Required				Required	Required		Required	
IPSec static VPNs	Required				Required	Required		Required	
IPSec dynamic VPNs	Required	Optional	Required		Required	Required		Required	
PBR	Required								

Note 1: NSSD is really shared by all stacks in all LPARs in the NSSD domain (which could be a Sysplex or span multiple Sysplex environment)

Configuration files and policy definition files - overview

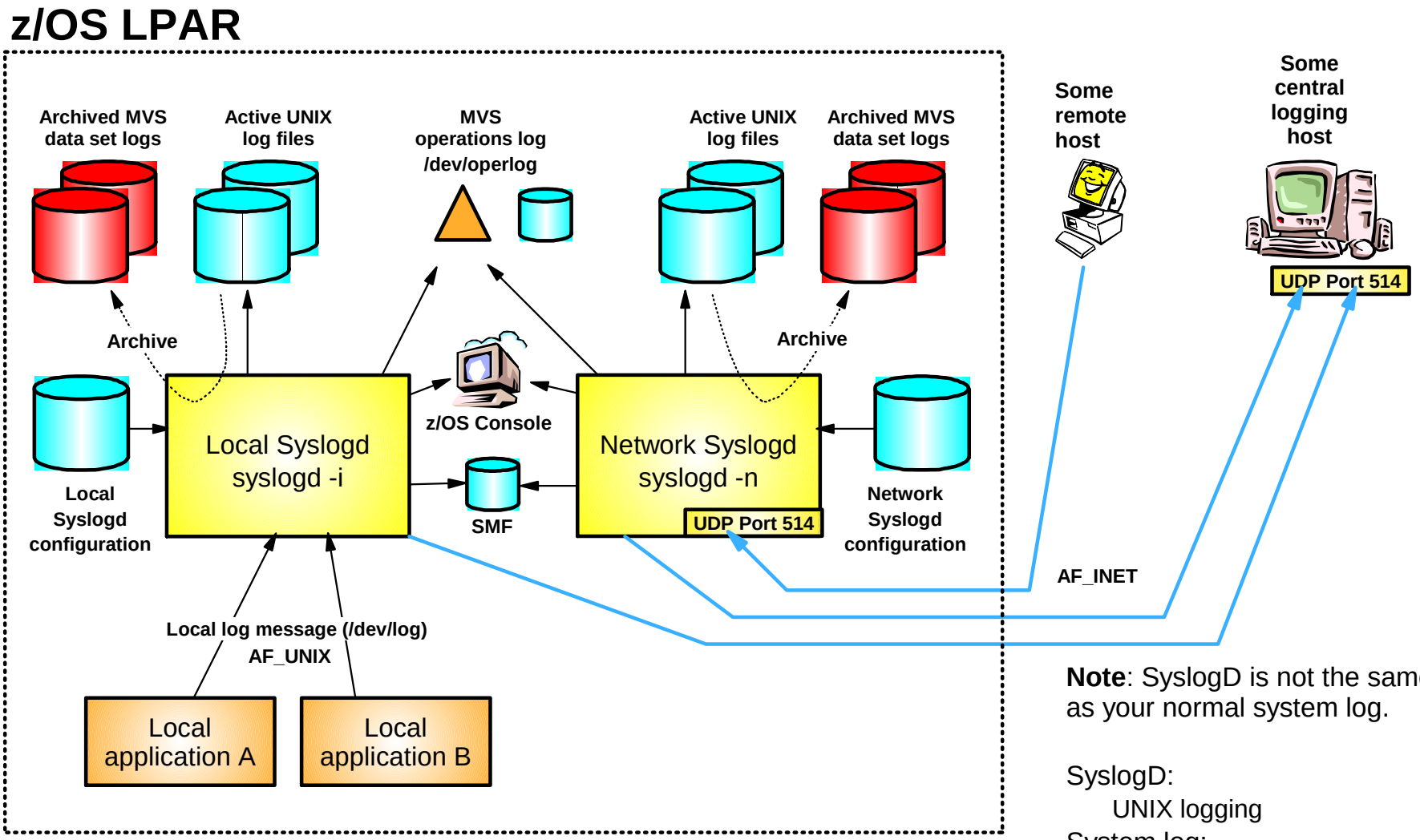
Configuration and policy definitions	Manual edit (ISPF)	Configu-ration Assistant	Configu-ration Assistant in z/OS V1R11
Configuration files			
Policy Agent configuration	Yes	No	Yes
Syslogd configuration	Yes	No	(partly)
IKED configuration	Yes	Yes	Yes
NSSD configuration	Yes	Yes	Yes
RSVPD configuration	Yes	No	No
DMD configuration	Yes	No	Yes
Policy definition files			
QoS policy	Yes	Yes	Yes
IDS policy	Yes	Yes	Yes
ATTLS policy	Yes	Yes	Yes
IPSec policy	Yes	Yes	Yes
PBR policy	Yes	Yes	Yes

- Most of the policy infrastructure components (address spaces you start) use a combination of configuration files, environment variables, and start options to control their start up processing
- Per stack and policy type that you want to use, you must define a policy definition and store that in a file, which Policy Agent reads during policy activation

Configuring, operating, and monitoring Policy Agent

Setting up and managing Syslogd and TRMD

z/OS Syslogd overview



Note: SyslogD is not the same as your normal system log.

SyslogD:
- UNIX logging

System log:
- JES-based system logging

Syslogd performance, management, and usability improvements in z/OS V1R11

New

Syslogd changed to be multi-threaded for improved scalability and message logging reliability

New

MVS Console command support

P SYSLOGD
F SYSLOGD,RESTART
F SYSLOGD,ARCHIVE
F SYSLOGD,DISPLAY

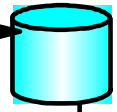
New

Automated archival support

Archival initiated by:

1. **Time of day (example: midnight)**
2. **File system utilization above threshold**
3. **Operator command**

Configuration Assistant



SyslogD Configuration file

SyslogD

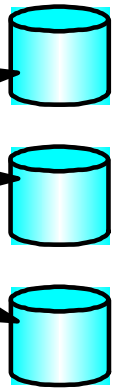
Main thread

Destination thread

Destination thread

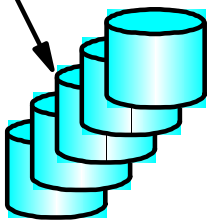
Destination thread

Archive control thread



Active log files

SyslogD file ARCHIVE jobs



Archived log files (GDG data sets or data sets with date/time info as LLQ)

ISPF-based search and browse support application

New

The Syslogd configuration file – the basics

- All messages to Syslogd are sent from local applications (using an AF_UNIX socket: /dev/log) along with information about facility name, priority, jobname, and user ID
  - Syslogd configuration rules use this information to determine where to send the message that is being logged.
  - A rule uses one of three formats:

```
Simple rule:     Facility.priority                destination
z/OS local rule: Userid.jobname.facility.priority destination
From remote:     (hostspace).facility.priority    destination
```

Facility name	Description
User	User process
Mail	Mail system
News	News system
Uucp	UUCP sustem
Daemon	Various server processes (FTPD, RSHD,SNMPD, etc.)
Auth / authpriv	Authorization system
Cron	cron system
Lpr	USS lp command
Local0-7	Local usage (local4 is used by IPsec)
Mark	Mark messages
Kernel	Kernel log messages (no such messages are generated on z/OS)

Priority name	Description
emerg / panic	A panic condition was reported to all processes
alert	A condition that needs immediate attention
crit	A critical condition
err(or)	An error message
warn(ing)	A warning message
notice	A condition requiring some special handling
info	A general information message
debug	A message useful for debugging
none	No messages logged for this priority
*******	Placeholder representing all priorities

Destination	Description
/UNIX file name	Name of z/OS UNIX active log file
@host	IP address or host name of Syslogd to forward messages to
User1, user2, ..	A list of local shell users
/dev/console	The MVS console
/dev/operlog	The MVS operlog log stream
$SMF	SMF record 109

Syslogd UNIX file location and naming

- **Location:**
  - Suggest you put them into one or more separate UNIX file systems
    - Reduce impact of Syslogd message flooding on other file systems and applications
    - Simplifies monitoring for file system full-conditions (or approaching file system full)
- **File names:**
  - Two options
    - Fixed names
      - /var/syslog/logs/syslog.log
    - Variable names with symbol substitution, such as day, month, year being part of the directory and/or file name (requires that you implement some kind of automation that makes Syslogd re-initialize every midnight)
      - /var/syslog/%Y/%m/%d/syslog.log
  - My (personal) preference is fixed names
    - Easier to know which file to look into for the most current messages - always the same directory and file names
    - I find it easier to implement an archival process that works both at regularly scheduled intervals (such as every midnight) and that works at unscheduled points in time (such as when file system approaches full-condition during the middle of the day)

Sample Syslogd configuration file with z/OS V1R11 archive options

```
#
# Syslogd configuration file
#
# USER1.TCPCS.TCPPARMS(SYSLOGT)
#
ArchiveThreshold       75
ArchiveCheckInterval   30
ArchiveTimeOfDay       00:01
#
BeginArchiveParms
 DSNPrefix    USER1.SYSLOGT
 Volume       DB2ABC
 MgmtClas     STANDARD
EndArchiveParms
#
*.*                        /var/syslog/logs/syslog.log -N SYSLOG(+1)
*.INETD*.*.*               /var/syslog/logs/inetd.log -X
*.OSNMP*.*.*               /var/syslog/logs/osnmpd.log -X
*.PAGENT*.*.*              /var/syslog/logs/pagent.log -N PAGENT(+1)
*.FTP*.*.*                 /var/syslog/logs/ftp.log -N FTP(+1)
*.TCPCS.daemon.*           /var/syslog/logs/ATTLS.log -N ATTLS(+1)
*.TRMD*.local4.*           /var/syslog/logs/FILT.log -N TRMD(+1)
*.IKED*.local4.*           /var/syslog/logs/IKED.log -N IKED(+1)
*.TRMD*.daemon.*           /var/syslog/logs/IDS.log -N IDS(+1)
```

DSNPrefix indicates the archive data set high level qualifier(s). You may use MVS System symbols in this value. You may have more ArchiveParms blocks in your Syslogd configuration file if you need to use different HLQs.

-N LLQ – indicates low level qualifier of archive data set name. If the LLQ end in (+1), it is a GDG. Otherwise Syslogd adds date and time LLQs after the LLQ you specify and allocates a plain sequential data set.

-X indicates that Syslogd may clear this file when archival processing is being performed.

These are the Syslogd rule criteria that govern where messages received by Syslogd are being logged. In this example only UNIX files are used to log messages to:

Userid.jobname.facility.priority

Starting, operating, and stopping Syslogd

```
//SYSLOGD PROC
//*
//* Start Syslogd
//*
//SYSLOGD EXEC PGM=SYSLOGD,REGION=0K,TIME=NOLIMIT,
//       PARM=('POSIX(ON) ENVAR("_CEE_ENVFILE=DD:MYENV")',
//             '/ -c -u -i -f //''USER1.TCPCS.TCPPARMS(SYSLOGT)''')
//SYSPRINT DD SYSOUT=*
//MYENV    DD DSN=USER1.TCPCS.TCPPARMS(SYSLOGEV),DISP=SHR
//SYSERR   DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//CEEDUMP  DD SYSOUT=*
```

-c
- Create log files and directories

-u
- Include userID and job name

-l
- Local-only mode

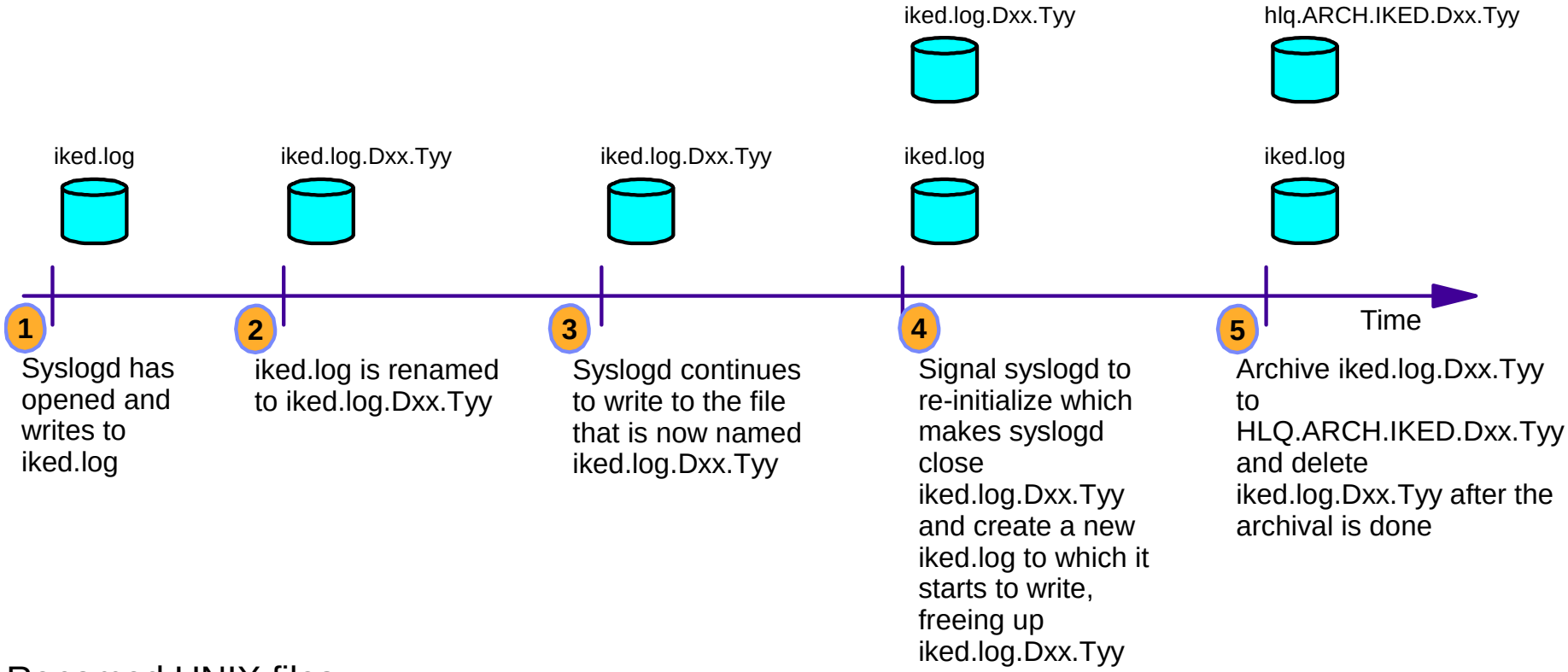
-f
- Configuration file

If you start Syslogd from the UNIX shell, you must include a trailing ampersand character (&) to run it as a background process. Especially important if you start Syslogd from a shell script such as /etc/rc

Action	Prior to z/OS V1R11	z/OS V1R11
S SYSLOGD	Resulting address space name became SYSLOGD1	Resulting address space name becomes SYSLOGD
F SYSLOGD	Not supported	F SYSLOGD,RESTART F SYSLOGD,ARCHIVE F SYSLOGD,DISPLAY
P SYSLOGD	Not supported	SYSLOGD will terminate

Syslogd in z/OS V1R11 no longer "forks" after start-up!

z/OS V1R11 Syslogd file archival process timeline



Renamed UNIX files:

filename`.Dyymmdd.Thhmmss`

Contains all records for current and previously failed archives

Sequential target data sets:

prefix.qualifier`.Dyymmdd.Thhmmss`

GDG target data sets:

prefix.qualifier`.GnnnnVnn`

Preparing for using the Syslogd browser ISPF tool

- **ISPF setup**
  - hlq.SEZAPENU - ISPF panel library
  - hlq.SEZAMENU - ISPF message library
  - hlq.SEZAEXEC - REXX program library (all REXX programs, except EZABROWS, are compiled REXX programs)
  - hlq.SEZALOAD - load module library (in your LNKLST or on TSO STEPLIB)

- **Note the following limitations if the REXX Alternate runtime Library is used (hlq.SEAGALT instead of hlq.SEAGLPA):**
  - No performance benefits as compared to interpreted REXX

- **Two ways to start the Syslogd browser:**
  - If TCPIP ISPF and REXX libraries are pre-allocated:
    - Start the EZASYRGO REXX program
  - If TCPIP ISPF and REXX libraries are not pre-allocated:
    - Copy EZABROWS to your REXX library and make local modifications
      - This REXX program is delivered in source form
    - Start the customized EZABROWS REXX program

```
/* ------------------------------------------------------------------ */
/* Change the value in the following statement---------------------- */
/* ------------------------------------------------------------------ */
hlq = 'TCPIP'
/* ------------------------------------------------------------------ */
/* No customization is needed below this point in this REXX---------- */
/* ------------------------------------------------------------------ */
```

Syslogd browser entry panel

In z/OS V1R11, a TSO/ISPF interface to browse and search messages captured by Syslogd is also introduced.

The Syslogd browser works with active UNIX files and archived MVS data sets.

The panel shown here is the initial panel when you start the Syslogd browser. This panel is used to set general options and to select the Syslogd configuration file representing the syslog daemon you want to work with.

```
*------------------------- z/OS CS Syslogd Browser ----------- Row 1 to 7 of 7
Command ===>                                                   Scroll ===> PAGE

Enter Syslogd browser options
  Recall migrated data sets ==> NO     (Yes/No) Recall data sets or not
  Maximum hits to display   ==> 5      (1-99999) Search results to display
  Maximum file archives     ==> 10     (0-400) Days to look for file archives
  Display start date/time   ==> YES    (Yes/No) Retrieve start date/time
  Display active files only ==> NO     (Yes/No) Active files only, no archives
  DSN Prefix override value ==>

Enter file or data set name of Syslogd configuration, or select one from below:

  File/DS Name ==> 'user1.tcpcs.tcpparms(syslogt)'

Press ENTER to continue, press END to exit without a selection

Line commands: S Select, R Remove from list, B Browse content, E Edit content

Cmd Recently used Syslogd configuration file or data set name
--- ---------------------------------------------------------------------------
    'user1.tcpcs.tcpparms(syslogt)'
    'user1.tcpcs.tcpparms(syslogn)'
    'user1.tcpcs.tcpparms(sysltom)'
    tcpcs.tcpparms(test)
    tcpcs.tcpparms(syslogt)
    /etc/syslog.test
    /etc/syslog.alfred.conf
****************************** Bottom of data ***
```

```
*---- z/OS CS Syslogd Browser ----*

   Collecting information about
     active Syslogd files and
             archives

        Please be patient.
```

Syslogd destination view

This panel lists all the rules in the specified Syslogd configuration file that writes to UNIX files.

Both primary and line commands are available on this panel to browse, search, etc.

```
*------------------------- z/OS CS Syslogd Browser ---------- Row 1 to 7 of 12
OPTION ===>                                                   Scroll ===> PAGE

  1 Change current Syslogd configuration file and/or options
  2 Guide me to a possible Syslogd destination
  3 Clear guide-me hits (indicated by ==> in the Cmd column)
  4 Search across all active Syslogd files

Current config file ==> 'user1.tcpcs.tcpparms(syslogt)'

Press ENTER to select an entry, press END to exit the Syslogd browser

Line commands: B Browse, A List archives, S Search active file and archives,
               SF Search active file, SA Search archives, I File/DSN info
                                                                  Archive
Cmd Rule/Active UNIX file name                    Start Time      Type Avail.
--- ---------------------------------------------- ---------------- ---- ------
    *.*                                           09 Dec 2008 00:00 GDG  3
    /var/syslog/logs/syslog.log
    - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    *.TCPCS*.*.*                                  09 Dec 2008 13:47 SEQ  9
    /var/syslog/logs/tcpcs.log
    - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    *.INETD*.*.*                                  Empty       N/A   None 0
    /var/syslog/logs/inetd.log
    - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    *.OSNMP*.*.*                                  09 Dec 2008 13:47 CLR  0
    /var/syslog/logs/osnmpd.log
    - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    *.PAGENT*.*.*                                 09 Dec 2008 00:01 SEQ  13
    /var/syslog/logs/pagent.log
    - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    *.FTP*.*.*                                    08 Dec 2008 15:22 FILE 2
    /var/syslog/logs/ftp.08.12.08.log
    - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
    *.FTP*.*.*                                    08 Dec 2008 15:22 FILE 2
    /var/syslog/logs/ftp.08.12.2008.log
```

Browse an active Syslogd file

```
 BROWSE    /var/syslog/logs/pagent.log                Line 00000000 Col 001 080
 Command ===>                                                  Scroll ===> PAGE
********************************* Top of Data **********************************
00000001 Dec  9 00:01:10 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :006:
         policy_perf_get_sampling_data(): Obtained 2 policy performance data
         entries from the stack
00000002 Dec  9 00:01:10 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :006:
         pqos_refresh_perf_cache: Refreshing cache with 2 performance entries
00000003 Dec  9 00:01:10 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :006:
         pqos_refresh_perf_cache: Refresh complete: #sla=2, #cache=1, #SL=1,
         #cacheSL=1
00000004 Dec  9 00:01:10 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :006:
         policy_perf_send_msg_to_SD(): Sending 1 default fractions to the stack
00000005 Dec  9 00:01:10 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :008:
         pqos_send_frns_to_SD: Sending fractions to the stack, 1 headers, 1
         entries
00000006 Dec  9 00:02:09 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :001:
         check_main_config_file: Main configuration file updated
00000007 Dec  9 00:02:09 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :001:
         check_main_config_file: pagentRefresh = NO
00000008 Dec  9 00:02:09 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :005:
         check_config_files: Thread cleanup completed
00000009 Dec  9 00:02:09 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :007:
         qosListener: Thread cleanup completed
00000010 Dec  9 00:02:09 MVS098/TCPCS    PAGENT   Pagent[13]:  SYSERR :008:
         pqos_recv_msg_from_listener: recv with peek failed, errno EDC8121I
         Connection reset., errno2 76650446
00000011 Dec  9 00:02:09 MVS098/TCPCS    PAGENT   Pagent[13]:  OBJERR :008:
         pqos_get_info_from_listeners: pqos_recv_msg_from_listener failed
00000012 Dec  9 00:02:09 MVS098/TCPCS    PAGENT   Pagent[13]:  LOG    :008:
         pqos_get_info_from_listeners: EZZ8775I PAGENT ON TCPCS CONNECTION NO
         LONGER ACTIVE TO 192.168.5.1..1700
00000013 Dec  9 00:02:09 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :008:
         pqos_get_info_from_listeners: Thread cleanup completed
00000014 Dec  9 00:02:09 MVS098/TCPCS    PAGENT   Pagent[13]:  EVENT  :006:
         policy_perf_monitor: Thread cleanup completed
```

A normal ISPF browser interface.

Search argument panel

```
*------------------------- z/OS CS Syslogd Browser --------------------------*
OPTION ===>

Enter your search options.

  Case sensitive  ==> NO         (Yes/No) Are string arguments case sensitive?
  Maximum hits    ==> 5          (1-99999) Max number of hits to display
  Result DSN name ==> 'USER1.SYSLOGD.LIST'
  Result DSN UNIT ==> SYSALLDA   Unit name for allocating new result DSN
  Result DSN disp ==> 1          1:Keep, 2:Delete, 3:Display print menu

Enter your search arguments.  All arguments will be logically ANDed.

  From date  . . .==> 2008/12/07 (yyyy/mm/dd) Search from date
  - and time . . .==> 10:50:00   (hh:mm:ss) - and time (24-hour clock)
  To date  . . . .==> 2008/12/08 (yyyy/mm/dd) Search to date
  - and time . . .==> 02:00:00   (hh:mm:ss) - and time (24-hour clock)
  User ID  . . . .==>            z/OS user ID of logging process
  Job name . . . .==>            z/OS jobname of logging process
  Rem. host name .==>
  Rem. IP address ==>
  Message tag  . .==> Syslogd         Enter ? for list
  Process ID . . .==>            z/OS UNIX process ID
  String 1 . . . .==>
  String 2 . . . .==>
  String 3 . . . .==>
  String 4 . . . .==>

Message tags are typically component names.
options set by the logging application.  User
for local messages if Syslogd is started with

UserID, jobname, message tag, and remote host
case insensitive.

Press ENTER to start search, press END to ret
```

```
*------ z/OS CS Syslogd Browser ------*

       *** S E A R C H I N G ***

  1 of 4 files/dsn processed so far
    150000 lines processed so far

      24% |****................|

           Please be patient.

  Halt by pressing ATTN and enter HI
```

The search data entry panel is used to initiate a search across one or more Syslogd files and data sets.

The anatomy of a message logged by Syslogd

- A message logged by a local application
- Syslogd started with the –u option
  - To have user ID and job name included in each logged message

```
Jun 25 09:52:08 MVS098/TCPCS    PAGENT   Pagent[15]: text
--timestamp---- -host- -userID- Jobname- -Tag-- PID -message-->
```

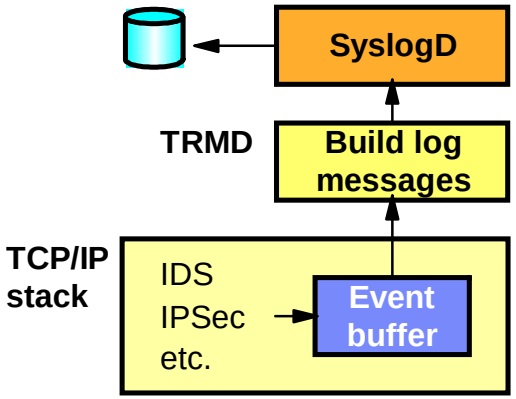
- Timestamp
  - Month is always 3-character English month name followed by the day in the month.
  - Note that Syslogd never includes the year
  - Time of day is always in 24-hour clock format (hh:mm:ss – where hh goes from 00 to 24)
  - Time value can be controlled by way of the TZ environment variable
    - As it is set for the logging application, not Syslogd itself!
    - Sample CEEPRMxx member in SYS1.PARMLIB:

```
CEEDOPT(
        ENVAR(NLSPATH=/COPY/%N:/USR/LIB/NLS/MSG/%L/%N,TZ=EST5EDT),
        )
CEECOPT(
        ENVAR(NLSPATH=/COPY/%N:/USR/LIB/NLS/MSG/%L/%N,TZ=EST5EDT),
        )
CELQDOPT(
        ENVAR(NLSPATH=/COPY/%N:/USR/LIB/NLS/MSG/%L/%N,TZ=EST5EDT),
        )
```

Managing TRMD

- **TRMD is stack-specific**
  - It determines which stack to use based on the TCPIPJOBNAME in its resolver configuration file
  - z/OS V1R11 adds a start option to specify the stack name in the EXEC PARM field
    - -p stackname

```
//TRMDA     PROC
//*
//TRMD   EXEC PGM=EZATRMD,REGION=4096K,TIME=NOLIMIT,
//  PARM=('POSIX(ON) ALL31(ON)',
//  'ENVAR("_CEE_ENVFILE=DD:MYENV")/')
//MYENV    DD DSN=USER1.TCPCS.TCPPARMS(TRMDENV),DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSERR   DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//CEEDUMP  DD SYSOUT=*
```

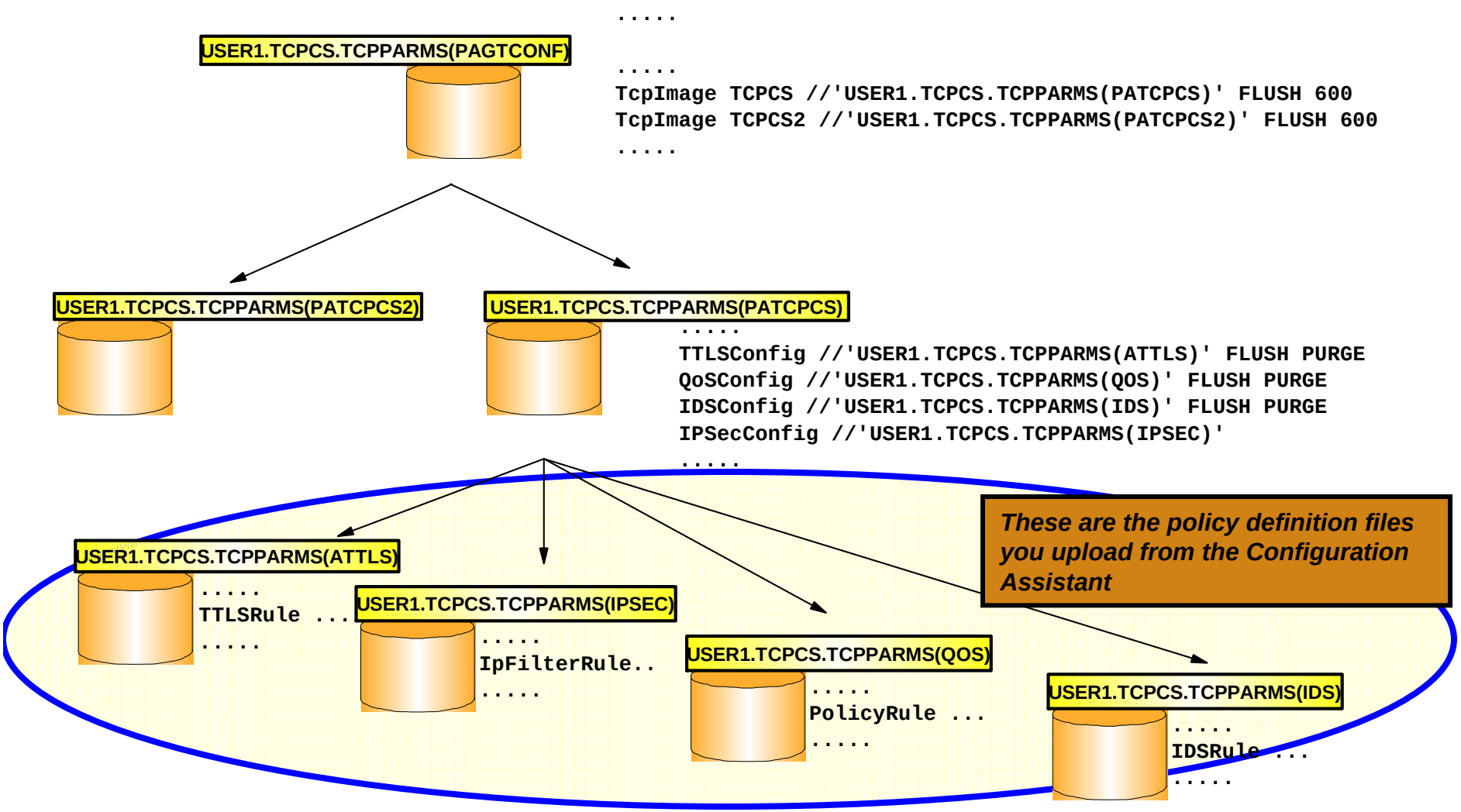


- **TRMD environment variables in my USER1.TCPCS.TCPPARMS(TRMDENV) member:**
  - RESOLVER_CONFIG=//'USER1.TCPCS.TCPPARMS(TCPDATA)'
- **TRMD forks, so the resulting address space becomes TRMDA1 in this example**
  - TRMD does support a STOP command
    - P TRMDA1
  - TRMD can also be stopped via a UNIX kill command, but it doesn't store its PID in any specific file (you can still determine it by using a "ps -ef | grep TRMD" command)

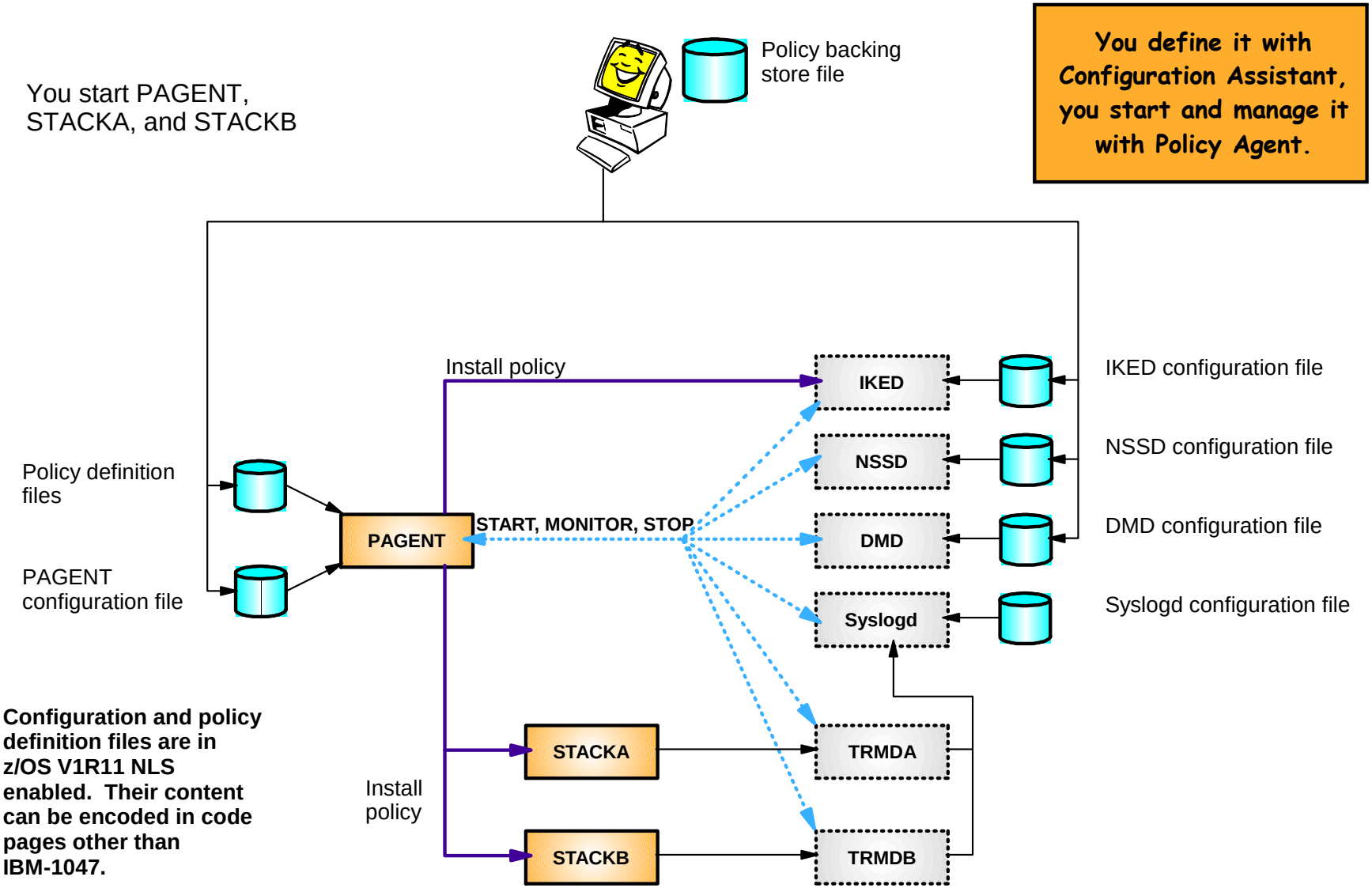
Configuring, operating, and monitoring Policy Agent

Setting up and managing policy agent (PAGENT)

A sample policy agent configuration file and policy definition file structure



z/OS V1R11 policy infrastructure management overview



Configuration and policy definition files are in z/OS V1R11 NLS enabled. Their content can be encoded in code pages other than IBM-1047.

Sample Policy Agent configuration for monitoring dependent functions

```
AutoMonitorParms
{
  MonitorInterval        10
  RetryLimitCount        5
  RetryLimitPeriod       600
}

AutoMonitorApps
{
  AppName         IKED
  {
    ProcName      IKED
    JobName       IKED
    EnvVar        IKED_FILE=//'USER1.POLICY.PROD.MVS098(IKEDCONF)'
  }
  AppName         SYSLOGD
  {
    ProcName      SYSLOGD
    JobName       SYSLOGD
    EnvVar        SYSLOGD_CONFIG_FILE=//'USER1.TCPCS.TCPPARMS(SYSLOGT)'
    StartParms    -c -u -i
  }
  AppName         TRMD
  {
    TcpImageName  TCPCS
    {
      ProcName    TRMD
      JobName     TRMD1
      StartParms  -p TCPCS
    }
  }
}
```

The Configuration Assistant will generate the initial set of definitions. You may want to update file locations, etc.

Simplified JCL procedures for the policy infrastructure components

The cataloged procedure specified on the AutoMonitorApps statement must accept the following JCL keyword parameters:

Parameter	Description	Value Passed by Pagent
PROG	Name of the executable program	DMD, IKED, NSSD, SYSLOGD, or TRMD
VARS	Name of environment variable file	Temporary file name generated by pagent
PARMS	Start parameter string	String configured on **AutoMonitorApps**, or a null string

```
//POLPROC  PROC PROG='',
//          VARS='',
//          PARMS=''
//POLPROC  EXEC PGM=&PROG.,REGION=0K,TIME=NOLIMIT,
// PARM=('POSIX(ON) ALL31(ON)',
// 'ENVAR("_CEE_ENVFILE=DD:VARS")',
// '/&PARMS.')
//VARS     DD PATH='&VARS.',PATHOPTS=(ORDONLY)
//STDENV   DD DUMMY
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=F,LRECL=80,BLKSIZE=80)
//SYSIN    DD DUMMY
//SYSERR   DD SYSOUT=*
//SYSOUT   DD SYSOUT=*,DCB=(RECFM=F,LRECL=80,BLKSIZE=80)
//CEEDUMP  DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
```

Sample JCL procedure in hlq.SEZAINST(POLPROC)

Remember: started task user IDs are assigned based on the proc name (not the job name). If you need different started task user IDs, you need to copy POLPROC into multiple members with different names.

New Policy Agent console commands

- You must use new operator commands to start, stop, or restart monitored applications, so status can be maintained
  - For example if you monitor IKED, and issue a P IKED command, Policy Agent automatically restarts IKED
- Format of Policy Agent operator command for applications:

  F pagproc,MON,operation,application[,P=image]
  - operation is START, STOP, RESTART
  - application is DMD, IKED, NSSD, SYSLOGD, TRMD, ALL
  - image is TCP/IP stack name for TRMD
- Example: F PAGENT,MON,STOP,IKED
- Tip: Stop all monitored applications before stopping Policy Agent if you want to shut down the whole policy infrastructure

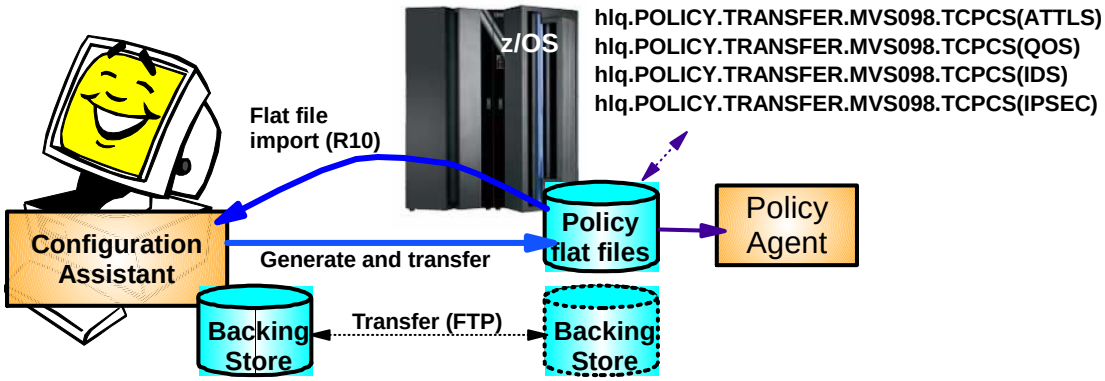
```
F PAGENT,MON,DISPLAY
EZD1588I PAGENT MONITOR INFORMATION 142
APPLICATION  MONITORED  JOBNAME  STATUS      TCP/IP STACK
DMD          NO         N/A      N/A         N/A
IKED         YES        IKED     ACTIVE      N/A
NSSD         NO         N/A      N/A         N/A
SYSLOGD      YES        SYSLOGD  ACTIVE      N/A
TRMD         YES        TRMD1    ACTIVE      TCPCS
```

Configuring, operating, and monitoring Policy Agent

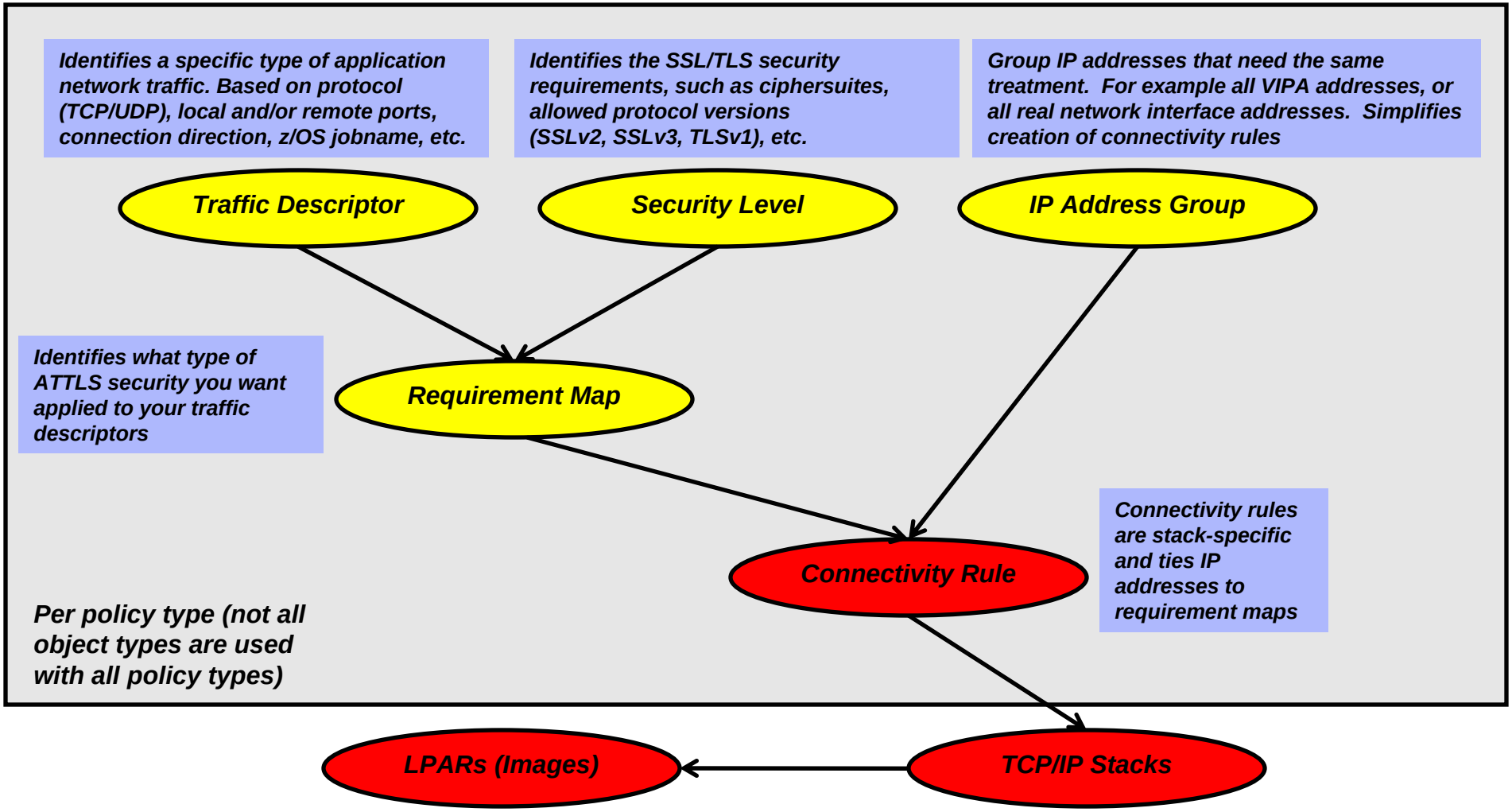
Getting started with the Configuration Assistant

Configuration Assistant files - overview

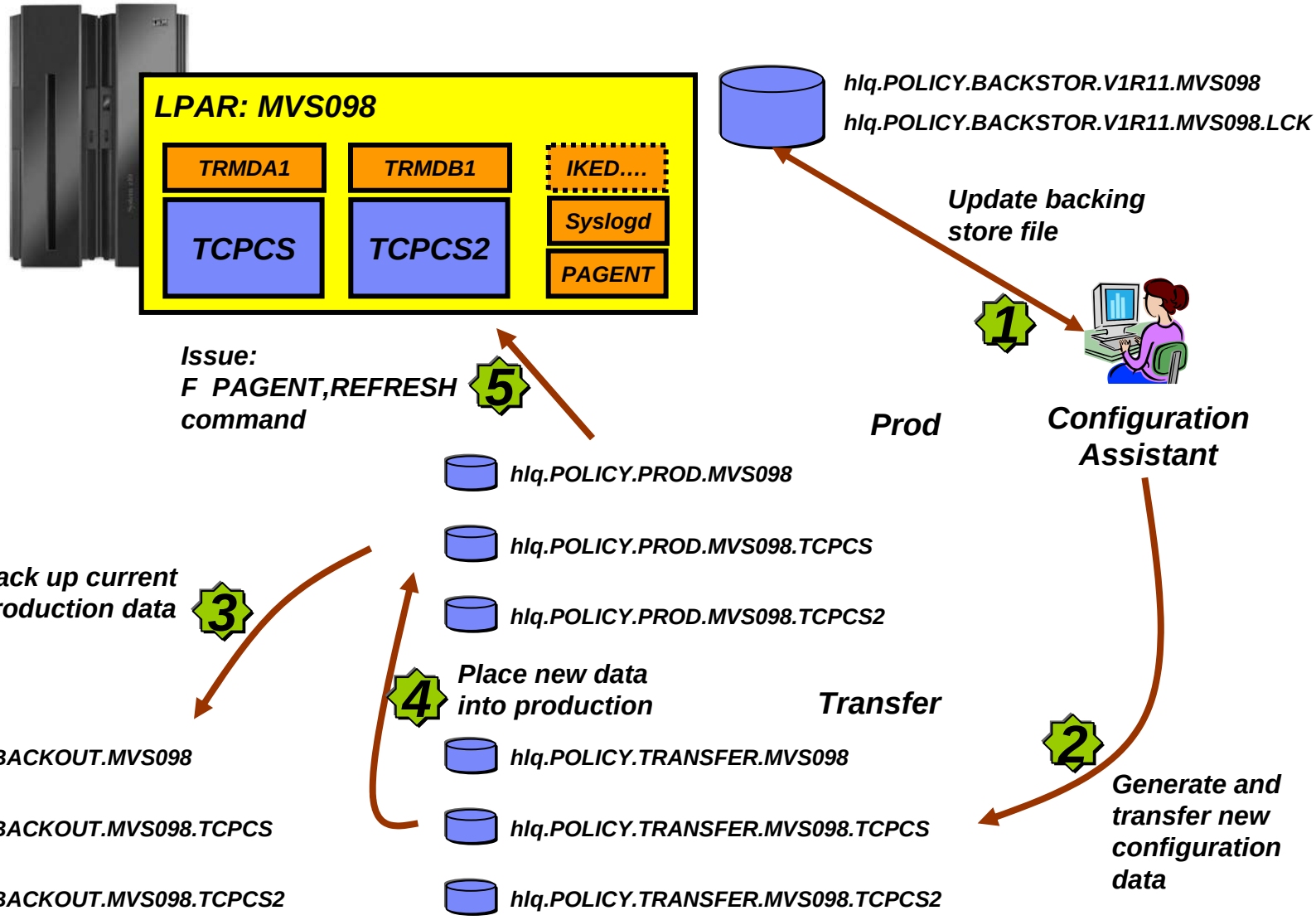
- **The configuration assistant reads and stores all information in binary form in the backing store file:**
  - Think of it as a binary version of all your z/OS CS networking policy definitions
  - You can maintain policies for many LPARs, stacks, and policy types in a single backing store file
  - If all policies are maintained by the same people, then I use a single backing store file per sysplex
    - Allows me to reuse some of the definitions, such as traffic descriptors across stacks
- **The backing store file may reside on your Windows workstation, on a LAN server (SMB server), or on z/OS in a z/OS UNIX file or MVS data set**
  - z/OS backing store files supported from z/OS V1R9
  - If on z/OS, open/save of the backing store file results in an FTP transfer to/from z/OS
  - The backing store file is protected against updates by more than one user at a time
    - Locking technology allows one user to update, others to access in read-only mode
- **When a discipline has been updated, the configuration assistant can generate the policy flat file that can be read by Policy Agent - and transfer it to z/OS using FTP**
- **In z/OS V1R10, Configuration Assistant can read and import an existing policy flat file**
  - Start from manually created policy definition files
  - Import into the Configuration Assistant after manual edit of a policy definition file



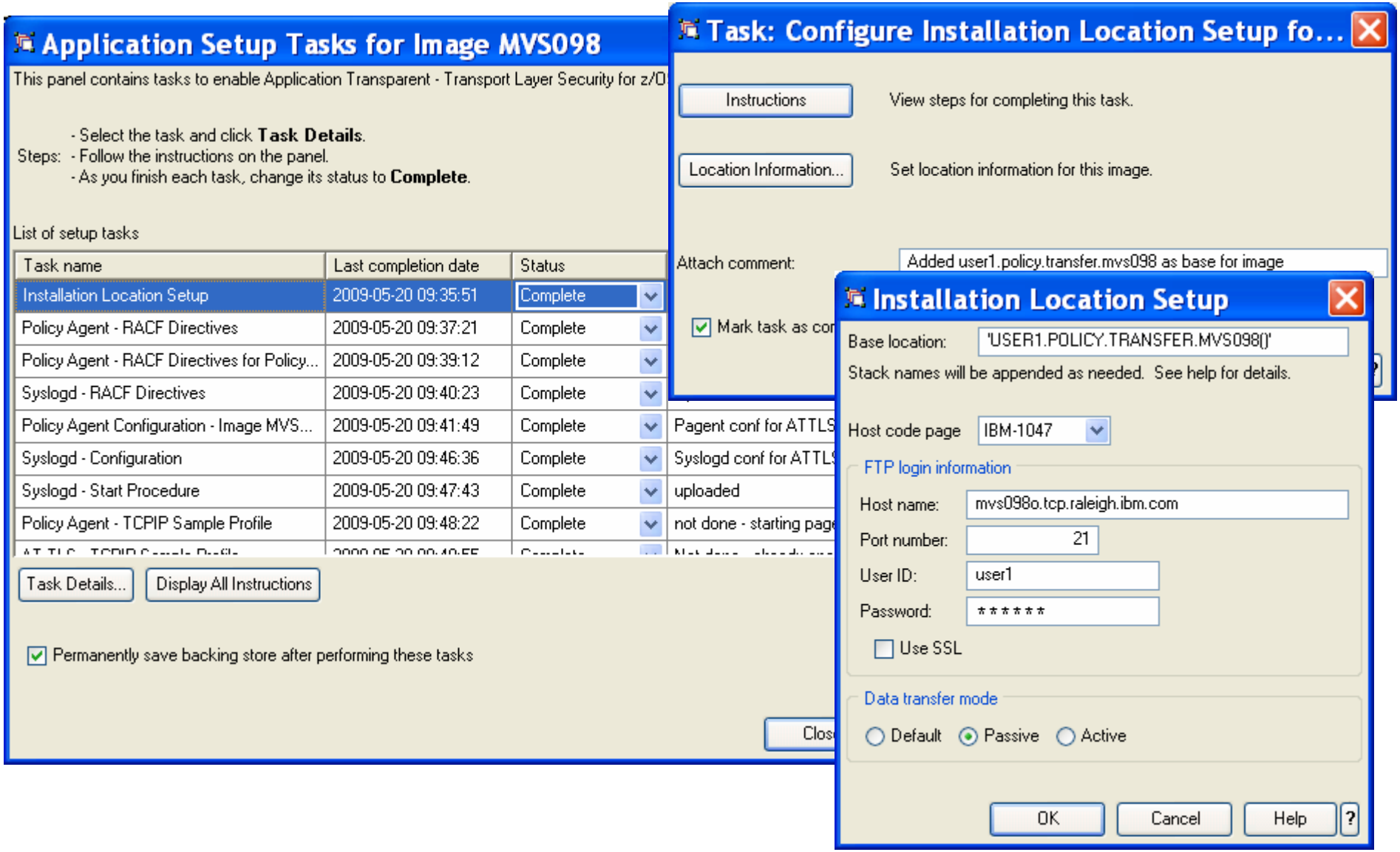
Quick guide to working with the Configuration Assistant objects - ATTLS example



Sample policy configuration environment



Application setup tasks - base location



Content of base locations after application setup tasks performed

Image PDS(E) library members

Component	Description
DMDCONF	DM configuration file
DMDPROC	DM JCL start procedure
DMDPROF	TCP/IP Profile sample IPSECURITY stmts.
IKEDCONF	IKE configuration file
IKEDPROC	IKE JCL start procedure
IMGPAG`	Image PAGENT configuration file
IPSPROF	TCP/IP Profile sample IPSECURITY stmts.
PAGPROC	Pagent JCL start procedure
RDMD	DM RACF setup commands
RIKED	IKE RACF setup commands
RIPSEC	RACF setup commands for ipsec cmd.
RPAGENT	Pagent RACF setup commands
RPOLICY	RACF setup commands for Policy data import
RSYSLOGD	Syslogd RACF setup commands
RTRMD	TRMD RACF setup commands
SYSLOCONF	Snippets for Syslogd configuration file
SYSLOGD	Syslogd JCL start procedure

Stack PDS(E) library members

Component	Description
IDSPOL	IDS policy
IPSPOL	IPSec policy
QOSPOL	QoS policy
STKPAG	Stack Pagent configuration
TLSPOL	ATTLS policy
TRMDPROC	TRMD JCL procedure

- ***Start PAGENT before any stacks are started***
  - ***Pagent will start Syslogd and other LPAR-wide components, such as IKED***
- ***When a stack is started, PAGENT notices it***
  - ***Pagent will then start the stack-specific TRMD***
  - ***Pagent will load all the relevant policies into that stack***

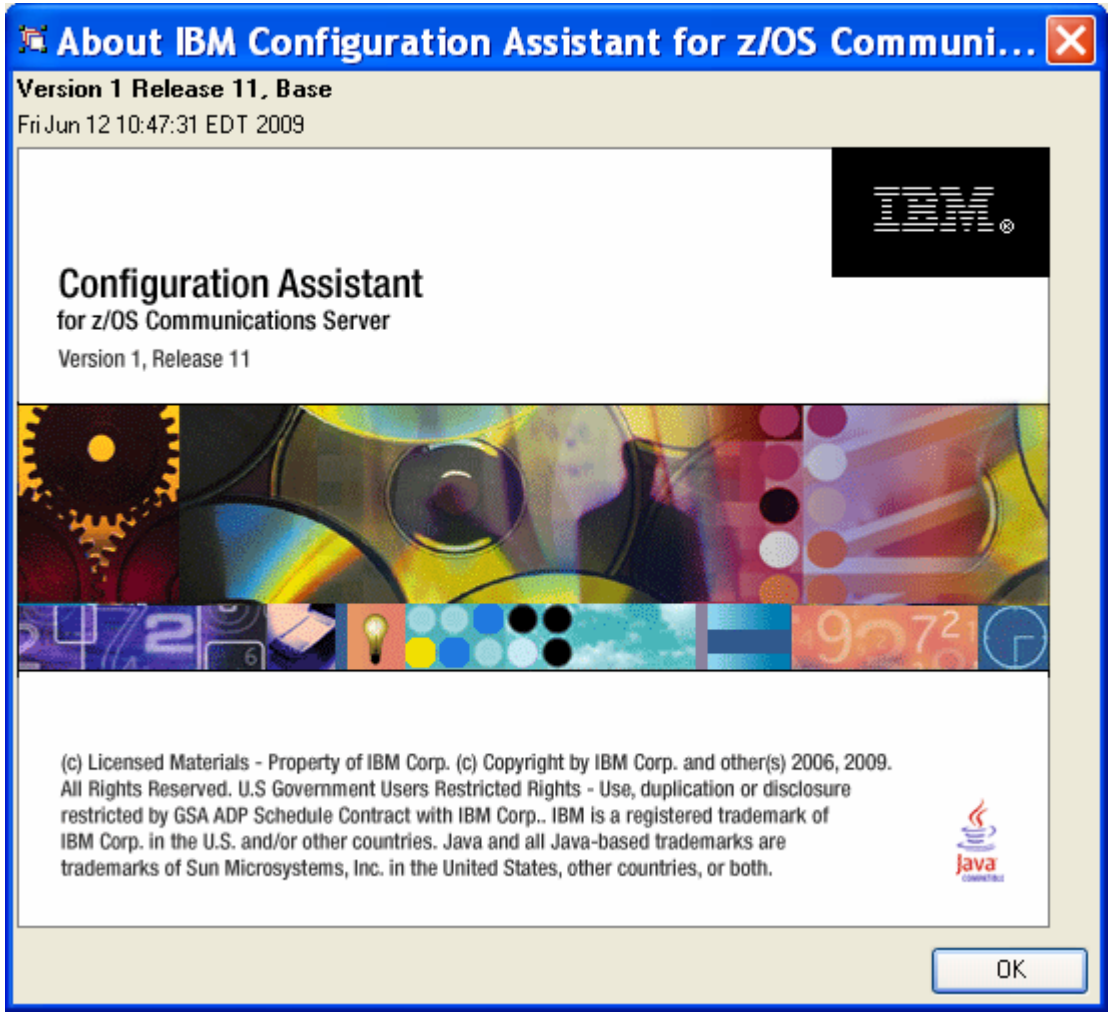
Sample JCL Log from PAGENT startup:

```
EZZ8431I PAGENT STARTING
EZZ8432I PAGENT INITIALIZATION COMPLETE

S IKED,JOBNAME=IKED,PROG=IKED,VARS='/var/tmp/IKED_AFfHxQ'
S
SYSLOGD,JOBNAME=SYSLOGD,PROG=SYSLOGD,VARS='/var/tmp/SYSLOGD_FgCdxQ',PARMS='-c
-u -i'

EZD1578I PAGENT IS UNABLE TO PROCESS REQUESTS FROM SERVICES REQUESTORS
EZD1581I PAGENT IS UNABLE TO START TCPCS/TRMD
EZD1581I PAGENT IS UNABLE TO START TCPCS2/TRMD
EZD1578I PAGENT IS UNABLE TO PROCESS REQUESTS FROM SERVICES REQUESTORS

EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : IDS
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : IPSEC
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : QOS
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : TTLS
EZD1586I PAGENT HAS INSTALLED ALL LOCAL POLICIES FOR TCPCS
S TRMD,JOBNAME=TRMD1,PROG=TRMD,VARS='/var/tmp/TRMD_TCPCS_fEegxQ',PARMS='-
pTCPCS'

EZD1576I PAGENT IS READY FOR SERVICES CONNECTION REQUESTS
```

The TCPCS stack is started

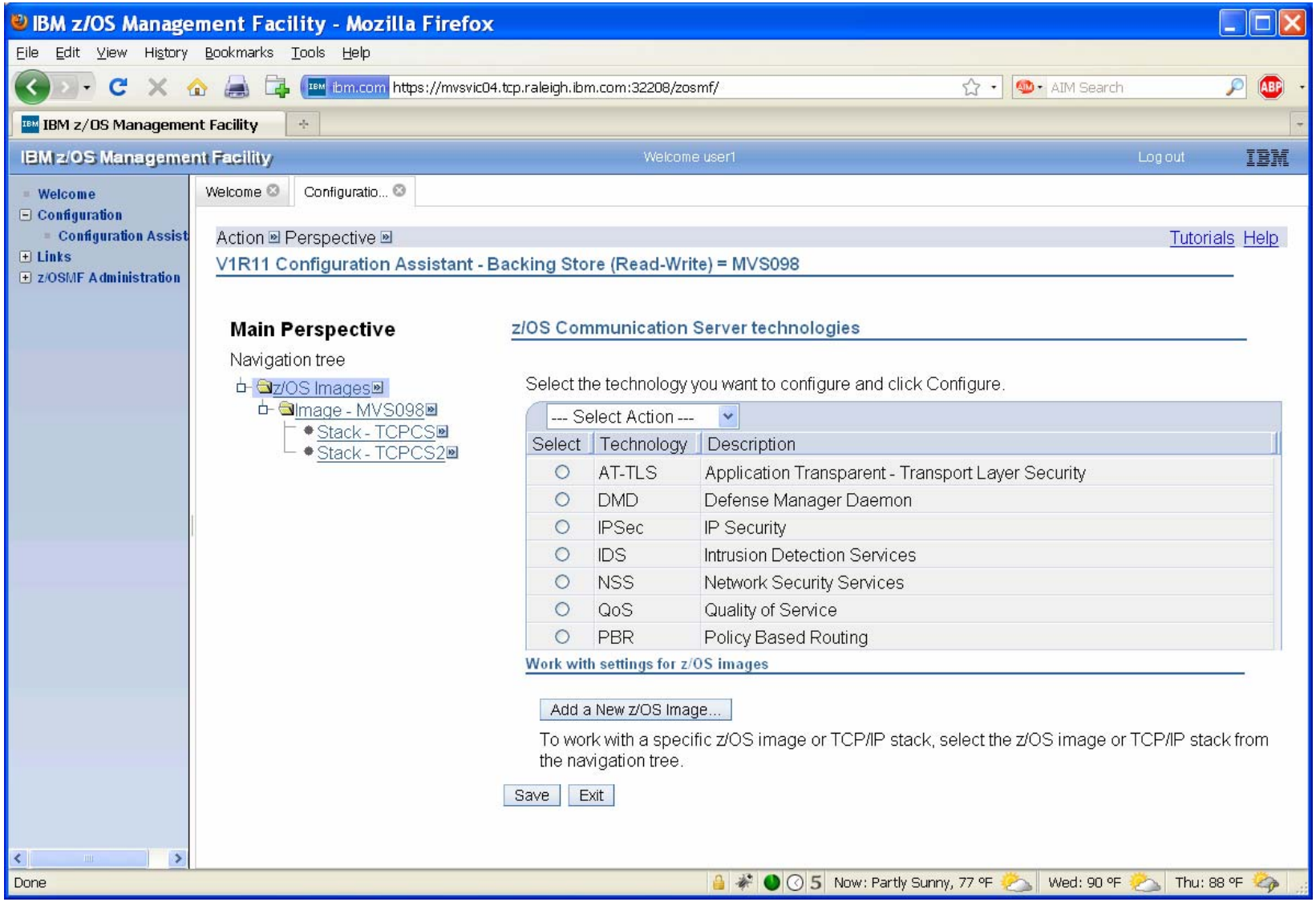
Configuration Assistant for z/OS Communications Server

- **Configuration Assistant for z/OS V1R11 Communications Server is shipped with the z/OSMF product**
  - Runs on z/OS
  - Accessed from a Web browser
  - Support is via normal IBM support channels
  - Same basic functions as the Windows-based version
- **The Windows-based standalone version remains available for z/OS V1R11, and can be downloaded from the web:**
  - Versions for z/OS V1R7, V1R8, V1R9, V1R10, and V1R11 are available for download
  - http://www.ibm.com/support/docview.wss?rs=852&context=SSSN3L&dc=D400&uid=swg24013160&loc=en_US&cs=UTF-8&lang=en&rss=ct852other
  - Support is "informal" via a forum



Tired of that long URL above – try this one instead: http://tinyurl.com/cgoqsa

Configuration Assistant in z/OSMF



For more information

URL	Content
http://www.twitter.com/IBM_Commserver	IBM Communications Server Twitter Feed
http://www.facebook.com/IBMCommserver	IBM Communications Server Facebook Fan Page
http://www.ibm.com/systems/z/	IBM System z in general
http://www.ibm.com/systems/z/hardware/networking/	IBM Mainframe System z networking
http://www.ibm.com/software/network/commserver/	IBM Software Communications Server products
http://www.ibm.com/software/network/commserver/zos/	IBM z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/	IBM Communications Server for Linux on System z
http://www.ibm.com/software/network/ccl/	IBM Communication Controller for Linux on System z
http://www.ibm.com/software/network/commserver/library/	IBM Communications Server library
http://www.redbooks.ibm.com	ITSO Redbooks
http://www.ibm.com/software/network/commserver/zos/support/	IBM z/OS Communications Server technical Support – including TechNotes from service
http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs	Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFC)
http://www.ibm.com/systems/z/os/zos/bkserv/	IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server

For pleasant reading ….