

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

Security Workshop

Policy Agent (PAGENT)



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.

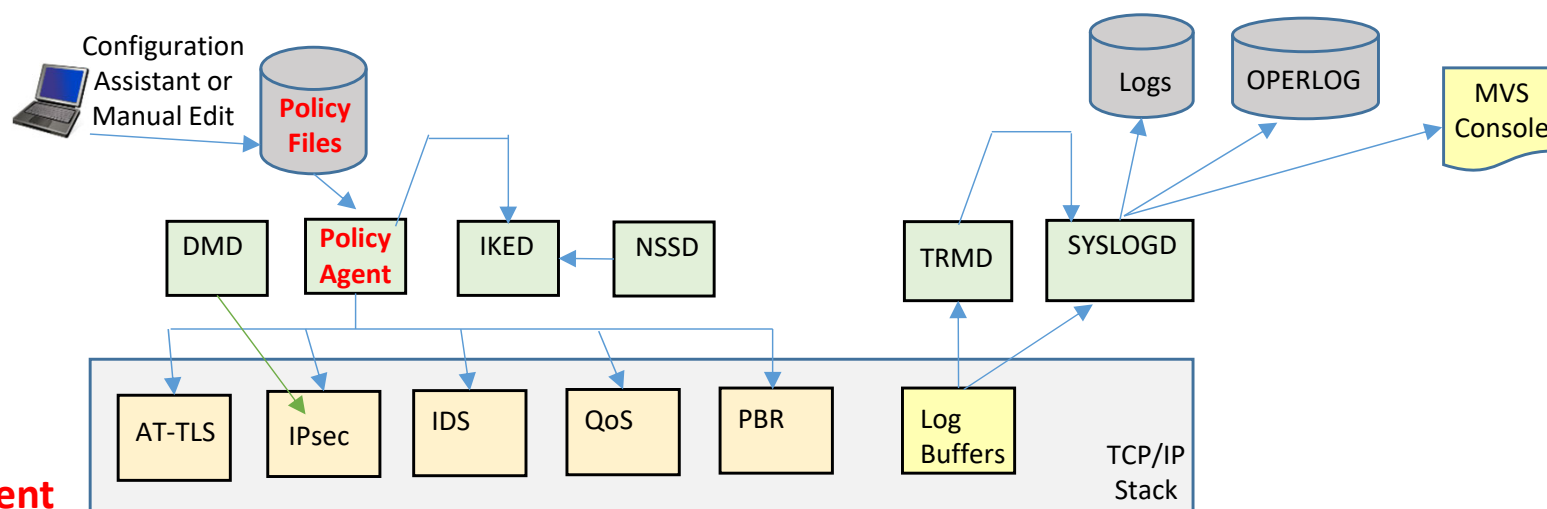
Agenda

- Structure of Policy Agent
- PAGENT Configuration Files
- Modify PAGENT and Monitor Applications
- Policy Views
- Configuration Assistant Tool
- Policy Server

Structure of Policy Agent



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) (One per TCP/IP stack)
 - Required for log messages to syslogd for IP Filter, IPsec, and IDS
- SyslogD
 - Recommended for logging

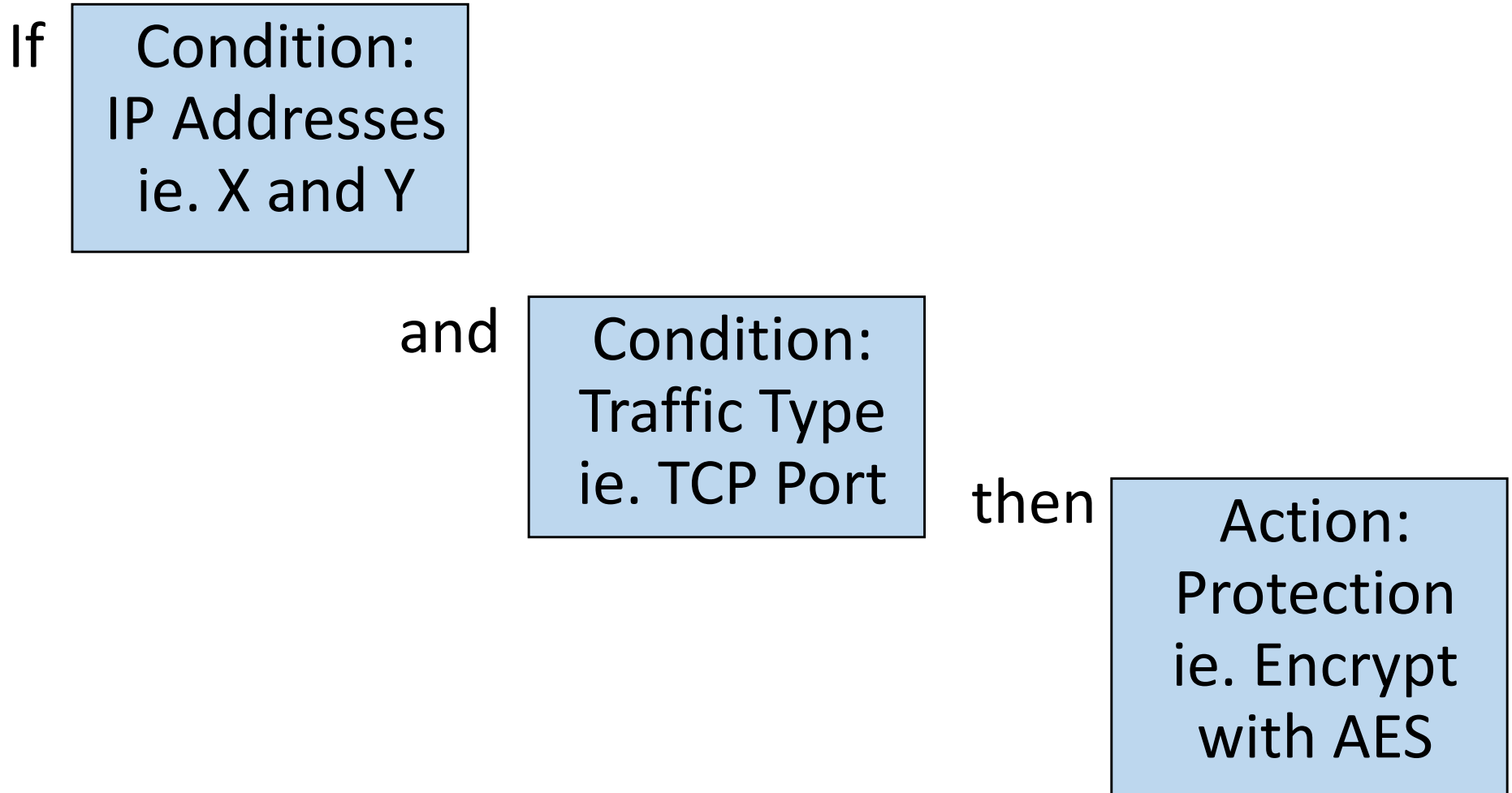
Policy Agent Prerequisites

- Syslogd for logging is recommended.
- Traffic Regulation Manager Daemon (TRMD) to collect information from the stack and send it to Syslogd or the console for policy types IP Filter, IPsec, and IDS
- RACF authorizations
 - PAGENT started Task OMVS segment with userid required
 - Commands that interoperate with PAGENT
 - psearch
 - ipsec
 - Some policies have additional access controls and definitions
 - AT-TLS
 - EZB.INITSTACK Servauth Class
 - IPsec
 - See details in the IPsec presentation
- How to configure the daemons?
 - z/OS Communications Server IP Configuration Guide SC31-8775
 - Communications Server for z/OS TCP/IP Implementation Volume 4: Security and Policy-based Networking SG24-7699, SG24-7801, SG24-7899

Policy Types

- IDSTConfig
 - Intrusion Detection Services (IDS) policies
 - Scan policies
 - Attack policies
 - Traffic Regulation policies
- IPSecConfig
 - IP Filtering policies
 - IPsec policies
 - Key exchange policies
 - Local dynamic VPN policies
 - Local manual VPN policies
- RoutingConfig
 - Policy-based Routing policies
- TTLSConfig
 - Application Transparent - Transport Layer Security (AT-TLS) policies
- QOSConfig
 - Quality of Service (QoS) policies
 - Differentiated Services (DS) policies or Data Traffic policies
 - Integrated Services policies or Resource Reservation Protocol (RSVP) policies
 - Sysplex distributor (SD) policies
- ZERTConfig
 - zERT Enforcement

Policy



If these conditions apply, then perform this action (or actions).

PAGENT Configuration Files



Main Configuration File

- Default is /etc/pagent.conf



```
LogLevel 31
TcplImage NM2ATCP /etc/nm2a.image FLUSH NOPURGE 600
#
PolicyPerfMonforSDR ...
#
SetSubnetPrioTosMask
#
PolicyRule....
#
PolicyAction...
#
```

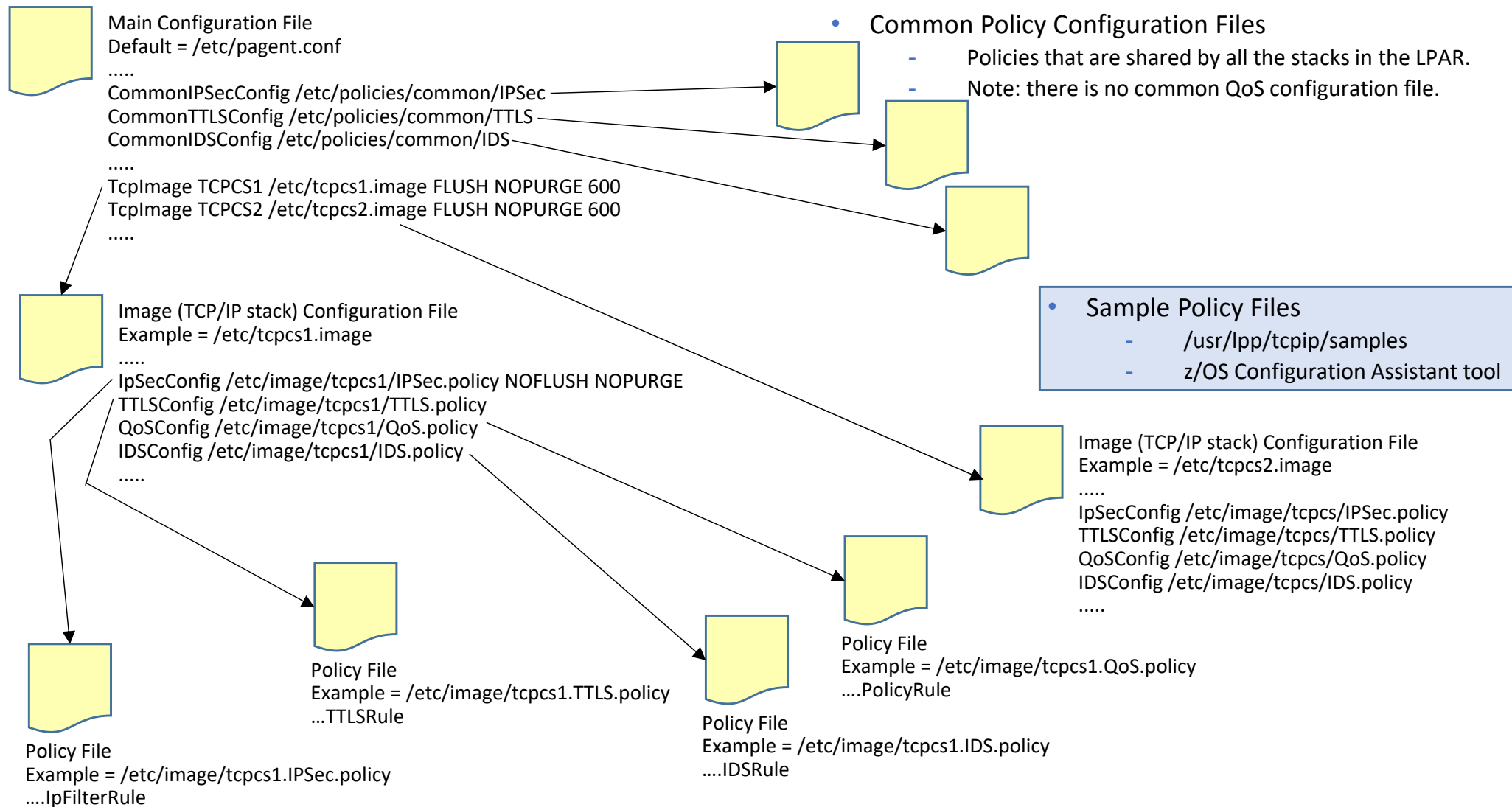
Image file with pointers to policy files

Some imbedded rules for QoS

How does Policy Agent find Policy Files?

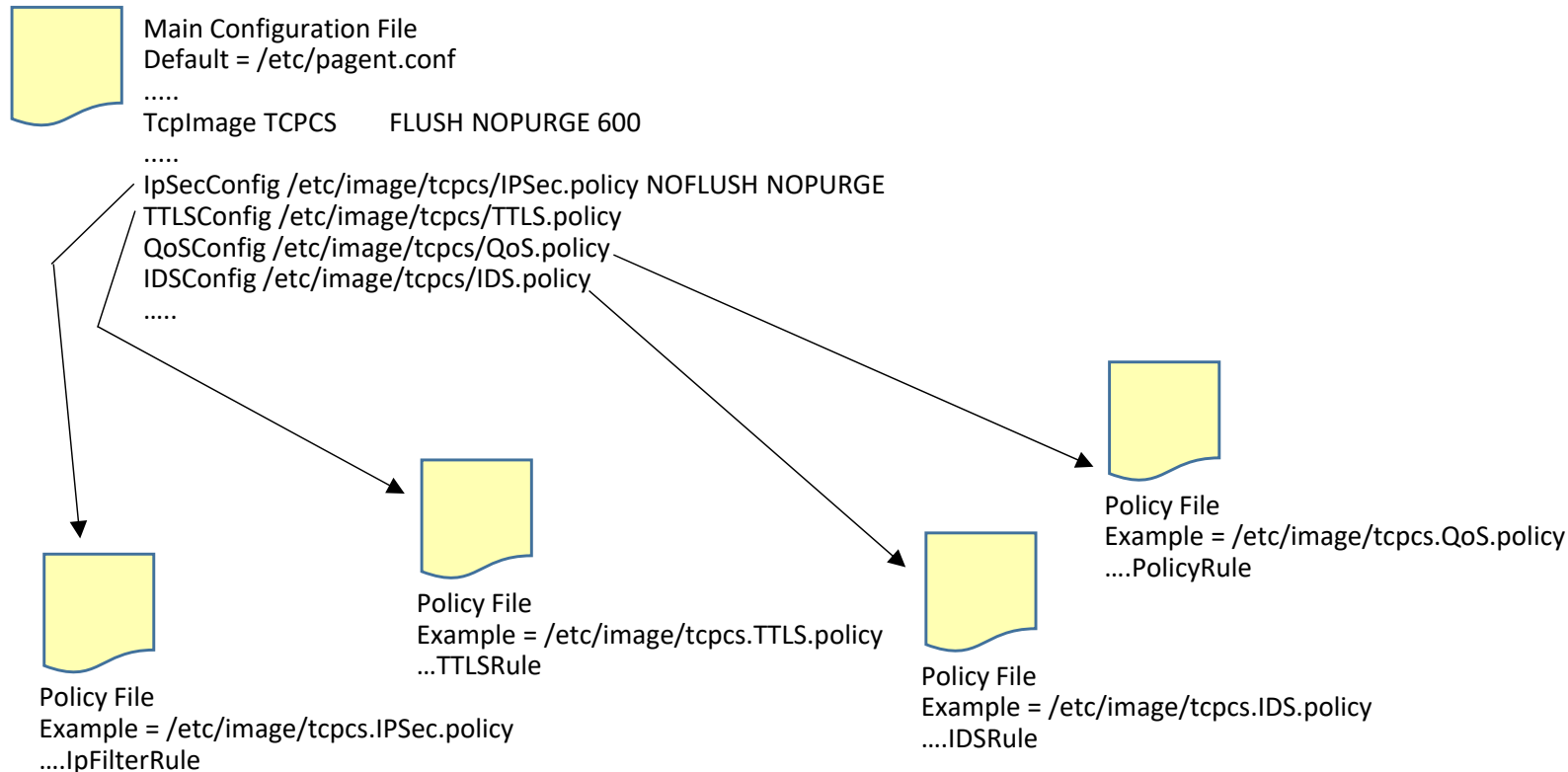
Main Policy file Option 1 – Image Files

- There is one Policy Agent per LPAR.
 - This one Policy Agent supports all stacks that run in that LPAR.



How does Policy Agent find Policy Files?

Main Policy file Option 2 – No Image Files



- Sample Policy Files
 - /usr/lpp/tcpip/samples
 - z/OS Configuration Assistant tool

Policy Agent JCL Procedure

Configuration file
may be a unix file or
an MVS data set.

```
//PAGENT PROC
//*
//* Status = CSV1R9
//*
//PAGENT EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
//          PARM='POSIX(ON) ALL31(ON) ENVAR("_CEE_ENVFILE=DD:STDENV")/-c/
//          etc/pagent2.conf -i -l SYSLOGD -d4 -t1'
// * Provide environment variables to run with the desired
// * configuration. As an example, the data set or file specified by
// * STDENV could contain:
// *
// * PAGENT_CONFIG_FILE=/etc/pagent2.conf
// * PAGENT_LOG_FILE=/tmp/pagent2.log
// *
//STDENV DD PATH='/etc/pagent2.env',PATHOPTS=(ORDONLY)
// *
// *STDENV DD DSN=TCPIP.PAGENT.ENV(PAGENT),DISP=SHR
// *
// *
//SYSPRINT DD SYSOUT=*
//SYSOUT DD SYSOUT=*
// *
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
```

```
TZ=EST5EDT
PAGENT_CONFIG_FILE=/etc/pagent2.conf
PAGENT_LOG_FILE=/tmp/pagent2.log
PAGENT_LOG_FILE_CONTROL=300,3
```

Fixed Block File Problem

- Standard Environment File (STDENV)

```
//PAGENT PROC
//PAGENT EXEC PGM=PAGENT,REGION=4096K,TIME=NOLIMIT,
//  PARM=('POSIX(ON) ALL31(ON)',
//  'ENVAR("_CEE_ENVFILE=DD:STDENV")',
//  '/ -c /etc/pagent2.conf -i -L SYSLOGD -d4 -t1')
//*
//STDENV DD PATH='/etc/pagent2.env',
//  PATHOPTS=(ORDONLY)
//*STDENV DD DSN=SYS1.TCPIP.STDENV,DISP=SHR
...
```

STDENV
Unix file

STDENV
VB or Other

Yes

```
//PAGENT PROC
//PAGENT EXEC PGM=PAGENT,REGION=4096K,TIME=NOLIMIT,
//  PARM=('POSIX(ON) ALL31(ON)',
//  'ENVAR("_CEE_ENVFILE=DD:STDENV")',
//  '/ -c /etc/pagent2.conf -i -L SYSLOGD -d4 -t1')
//*
//STDENV DD DSN=SYS1.TCPIP.TCPPARMS(PAGTENV),DISP=SHR
...
```

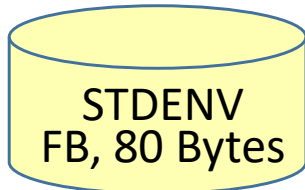
STDENV
FB, 80 Bytes

No

- Make sure your STDENV file is not in a fixed block dataset.

```
//PAGENT EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
//  PARM='POSIX(ON) ALL31(ON) ENVAR("_CEE_ENVFILE_S=DD:STDENV")/-
//  c/etc/pagent2.conf -i -l SYSLOGD -d4 -t1'
```

Fixed Block File Padded Blanks



0 10 20 30 40 80
+.....+.....+.....+.....+.....+.../ /..+

```
PAGENT_CONFIG_FILE=/etc/pagent2.conf  
TZ=EST5EDT
```



- EZZ7822 Could not find configuration file
- - or -
- Trailing blanks in directory names or filenames are not supported by edit or browse
- - or -
- EDC5129I No such file or directory.

- TRMD and PAGENT are UNIX applications.
- UNIX pads fixed-block file lines with blanks to the fixed-block size
- In UNIX, blanks are valid filename characters.
- So in this example PAGENT would be looking for files named:

```
"/etc/pagent2.conf
```

"

- Which probably isn't what you actually named it!

Modify PAGENT and Monitor Applications



FLUSH, PURGE, and Modify

- FLUSH or NOFLUSH and PURGE or NOPURGE are defined in policy configuration files:
 - TcpImage TCPIP /etc/tcpip_policy.config FLUSH PURGE
 - IpSecConfig /etc/IPSec.policy NOFLUSH NOPURGE
- Original design:
 - FLUSH – When PAGENT is started, if policies exist in the TCP/IP stack, policies are removed, and then reloaded.
 - NOFLUSH – When PAGENT is started, if policies exist in the TCP/IP stack, then they are not removed and reloaded.
 - PURGE – When PAGENT is stopped, policies are removed from the TCP/IP stack.
 - NOPURGE – When PAGENT is stopped, policies are not removed from the TCP/IP stack.
 - FLUSH effects Modify behavior as well.
- Modify Command
 - Refresh removes all policies from the TCP/IP stack and then reloads them.
 - F PAGENT,REFRESH
 - Update only changes the active policies that have been changed in the files.
 - F PAGENT,UPDATE
- Changes in configuration and policy files are installed:
 - Immediately when file is saved if –i is defined on startup – for unix files only

```
//PAGENT EXEC PGM=PAGENT,REGION=OK,TIME=NOLIMIT,  
//  PARM='POSIX(ON) ALL31(ON) ENVAR("_CEE_ENVFILE=DD:STDENV")/-c -i
```
 - At time interval if –i is defined on TcpImage statement (default 1800 seconds) – for all file types
 - TcpImage TCPIP /etc/tcp_policy.conf NOFLUSH NOPURGE –i
 - When Modify command is issued - for all file types
 - F PAGENT,REFRESH
 - F PAGENT,UPDATE
 - When SIGHUP is issued - for all file types
 - kill -1 3425

Behavior is Different for Policy Types

PAGENT start	FLUSH defined	IPsec and zERT Policies – All policies are replaced in the TCP/IP stack.
		PBR and All Other Policies – All policies are deleted, and then all policies are reloaded into the TCP/IP stack.
	NOFLUSH defined	IPsec and zERT Policies – All policies are replaced in the TCP/IP stack.
		PBR Policies – All policies are deleted, and then all policies are reloaded into the TCP/IP stack.
		All Other Policies – All changed policies are updated in the TCP/IP stack. No deleted policies are removed from the TCP/IP stack.
PAGENT Termination	PURGE defined	IPsec, zERT and PBR Policies – TCP/IP stack policies are unchanged.
		All Other Policies – All policies are removed from the TCP/IP stack.
	NOPURGE defined	IPsec, zERT, PBR, and All Other Policies – TCP/IP stack policies are unchanged.
PAGENT REFRESH	FLUSH defined	IPsec and zERT Policies – If there are any changed or deleted policies, then all policies are replaced in the TCP/IP stack.
		PBR and All Other Policies – If there are any changed or deleted policies, then all policies are deleted, and then all policies are reloaded into the TCP/IP stack.
	NOFLUSH defined	IPsec and zERT Policies – If there are any changed or deleted policies, then all policies are replaced in the TCP/IP stack.
		PBR Policies – If there are any changed or deleted policies, then all policies are deleted, and then all policies are reloaded into the TCP/IP stack.
		All Other Policies – If there are any changed policies, then they are replaced in the TCP/IP stack. No deleted policies are removed from the TCP/IP stack.
PAGENT UPDATE	FLUSH defined	IPsec and zERT Policies – If there are any changed or deleted policies, then all policies are replaced in the TCP/IP stack.
		PBR and All Other Policies – If there are any changed policies, then they are replaced in the TCP/IP stack, and then all deleted policies are removed from the TCP/IP stack.
	NOFLUSH defined	IPsec and zERT Policies – If there are any changed or deleted policies, then all policies are replaced in the TCP/IP stack.
		PBR Policies – If there are any changed policies, then they are replaced in the TCP/IP stack, and then all deleted policies are removed from the TCP/IP stack.
		All Other Policies – If there are any changed policies, then they are replaced in the TCP/IP stack. No deleted policies are removed from the TCP/IP stack.

Logging

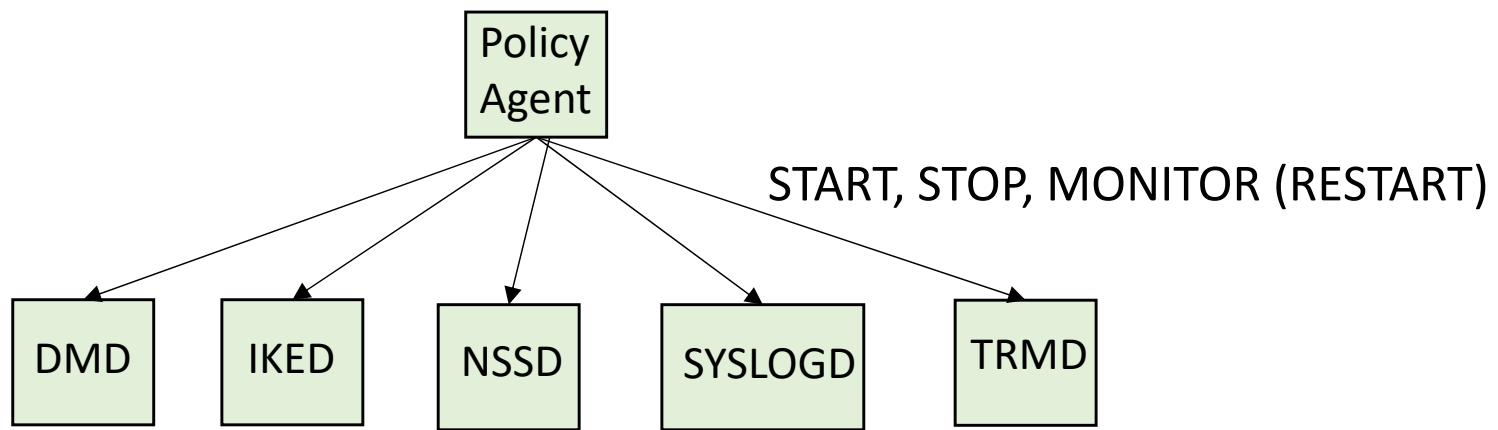
Log and Debug levels are not changed by updating the PAGENT configuration file and issuing Modify Update or Refresh!

- Log Level, Debug, and Trace
 - Log Level parameter is defined in the image Policy File.
 - Debug and Trace are specified on the Policy Agent start.
- Log Level
 - 1 - SYSERR - System error messages
 - 2 - OBJERR - Object error messages
 - 4 - PROTERR - Protocol error messages
 - 8 - WARNING - Warning messages
 - 16 - EVENT - Event messages
 - 32 - ACTION - Action messages
 - 64 - INFO - Informational messages
 - 128 - ACNTING - Accounting messages
 - 256 - TRACE - Trace messages
 - Log Level values are added together for a maximum Log Level value of 511.
 - 31 is the default
- Debug
 - 0 None. No debug messages are logged. This is the default.
 - 1 Base. The Policy Agent logs internal debug information.
 - When this level is selected, the Policy Agent also uses the maximum LogLevel value, regardless of what is configured.
 - 2 LDAP. The Policy Agent logs information about each LDAP object attribute that is processed.
 - 4 Sysplex summary. The Policy Agent logs summary information about performance monitor QoS fraction calculations at target stacks.
 - 8 Sysplex detail. The Policy Agent logs detailed information about performance monitor QoS fraction calculations at target stacks, and additional sysplex distributor information.
 - 16 Memory trace. The Policy Agent logs inline details of all memory allocation and free requests. This debug level is independent of the -m startup option.
 - 32 Policy install trace. The Policy Agent logs details of all policies as the policies are installed in the TCP/IP stack.
 - 64 Lock trace. The Policy Agent logs information about locks.
 - 128 Remote connection trace. The Policy Agent logs details about remote PAPI connections on the policy server and about connections to the policy server on the policy client.
 - 256 Discovery connection trace. The Policy Agent logs details about requests to discover TCP/IP profile information from import requestors.
 - Debug values are added together for a maximum Debug Level of 511.
- Trace
 - 0 No LDAP client debugging. This is the default.
 - 1 This level turns on LDAP client debugging.

- Set your loglevel and debug parameters with commands if you need more than the PAGENT defaults. Then disable the additional logging once no longer needed.
 - F PAGENT,LOGLEVEL,LEVEL=
 - F PAGENT,DEBUG,LEVEL=
 - F PAGENT,QUERY

Monitor Applications

- Policy Agent may be configured to automatically Start, Stop, and Monitor applications.
 - Configure with AutoMonitorApps statement.



Policy Views

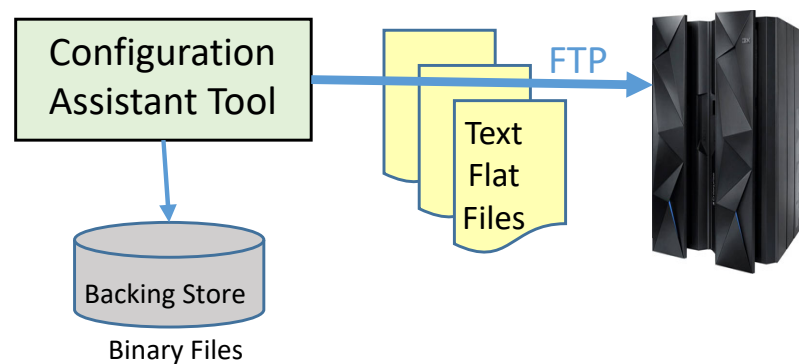


Example of Policy in Configuration Assistant Tool

```
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 1 Release 10
## Backing Store = C:\...\IBM\zCSConfigAssist\V1R10\files\ATTLSTEAM22_301
## FTP History:
##
## End of Configuration Assistant information
#####
# PolicyRule statements
#####

policyRule 0~1
{
  PolicyRulePriority    65000
  DestinationAddressRange 10.1.1.0-10.1.1.255
  SourcePortRange      1024-65535
  DestinationPortRange  21
  ProtocolNumberRange   6
  PolicyActionReference  action~1
}
#####
# PolicyAction Statements
#####

PolicyAction action~1
{
  PolicyScope      DataTraffic
  OutgoingTOS      01000000
  DiffServInProfileRate 256
  DiffServInProfileTokenBucket 512
  DiffServExcessTrafficTreatment Drop
}
```



Example of Policy on z/OS

- Stored as "flat file" in MVS dataset or in Unix file

```
PolicyRule                DiffServ_Rule1
{
  DestinationAddressRange  211.40.100.0-211.40.100.255
  SourcePortRange          20-21
  PolicyActionReference    DiffServ_Action1
  DayOfWeekMask            0111110
}
#
PolicyAction              DiffServ_Action1
{
  PolicyScope              DataTraffic
  OutgoingTOS              01000000
  DiffServInProfileRate    512    # 512 Kbps
  DiffServInProfileTokenBucket 64    # 64 Kbits
  DiffServInProfilePeakRate 1500   # 1.5 Mbps
  DiffServInProfileMaxPacketSize 120  # 120 Kbits
  DiffServOutProfileTransmittedTOSByte 00000000
  DiffServExcessTrafficTreatment BestEffort
}
```

QoS

- Beware of Duplicate Object Names
 - Sometimes a warning message is issued; sometimes it is not.
 - Sometimes the first entry is ignored; sometimes the last entry is ignored.

pasearch Example

policyRule: VIPAs2VIPAs~1
Rule Type: TTLS
Version: 3 Status: Active
Weight: 255 ForLoadDist: False
Priority: 255 Sequence Actions: Don't Care
No. Policy Action: 3
policyAction: gAct1
ActionType: TTLS Group
Action Sequence: 0
policyAction: eAct1~AllSecureFTPUsers
ActionType: TTLS Environment
Action Sequence: 0
policyAction: cAct1~AllSecureFTPUsers
ActionType: TTLS Connection
Action Sequence: 0
Time Periods:
Day of Month Mask:
First to Last: 11111111111111111111111111111111
Last to First: 11111111111111111111111111111111
Month of Yr Mask: 11111111111
Day of Week Mask: 1111111 (Sunday - Saturday)
Start Date Time: None
End Date Time: None
Fr TimeOfDay: 00:00 To TimeOfDay: 24:00
Fr TimeOfDay UTC: 05:00 To TimeOfDay UTC: 05:00
TimeZone: Local
TTLS Condition Summary: NegativeIndicator: Off

Local Address:
FromAddr: 192.168.20.101
ToAddr: 192.168.20.105
Remote Address:
FromAddr: 192.168.20.101
ToAddr: 192.168.20.105
LocalPortFrom: 1024 LocalPortTo: 65535
RemotePortFrom: 21 RemotePortTo: 21
JobName: UserId: USER*
ServiceDirection: Outbound
Policy created: Mon Nov 23 17:39:59 2009
Policy updated: Mon Nov 23 17:39:59 2009

TTLS Action: gAct1
Version: 3
Status: Active
Scope: Group
TTLSEnabled: On
CtraceClearText: Off
Trace: 2
TTLSGroupAdvancedParms:
SecondaryMap: Off
SyslogFacility: Daemon
Policy created: Mon Nov 23 17:39:59 2009
Policy updated: Mon Nov 23 17:39:59 2009
...

RACF Protection for pasearch

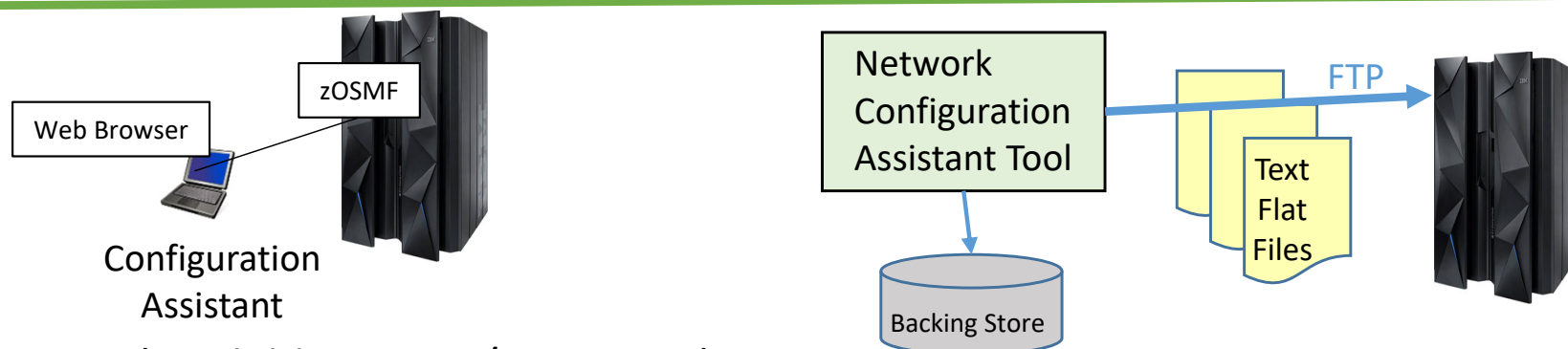
- pasearch command causes Policy Agent to display active policies.
 - pasearch -i IDS policies
 - pasearch -q QoS policies
 - pasearch -R PBR policies
 - pasearch -t AT-TLS policies
 - pasearch -v IPsec policies
- SERVAUTH class profile EZB.PAGENT.sysname.tcpimage.ptype
 - Where sysname is the z/OS system name,
 - tcpimage is the TCP/IP stack name,
 - ptype is either QOS or IDS.

EZB.PAGENT.SYSTEM1.TCPCS.QOS
EZB.PAGENT.SYSTEM1.*.IDS
EZB.PAGENT.SYSTEM1.*.*
- EZACMD command
 - REXX job that makes previous unix only commands available to TSO, NetView, and the z/OS console.
 - pasearch
 - ipsec
 - trmdstat
 - nssctl
 - ping

Network Configuration Assistant Tool



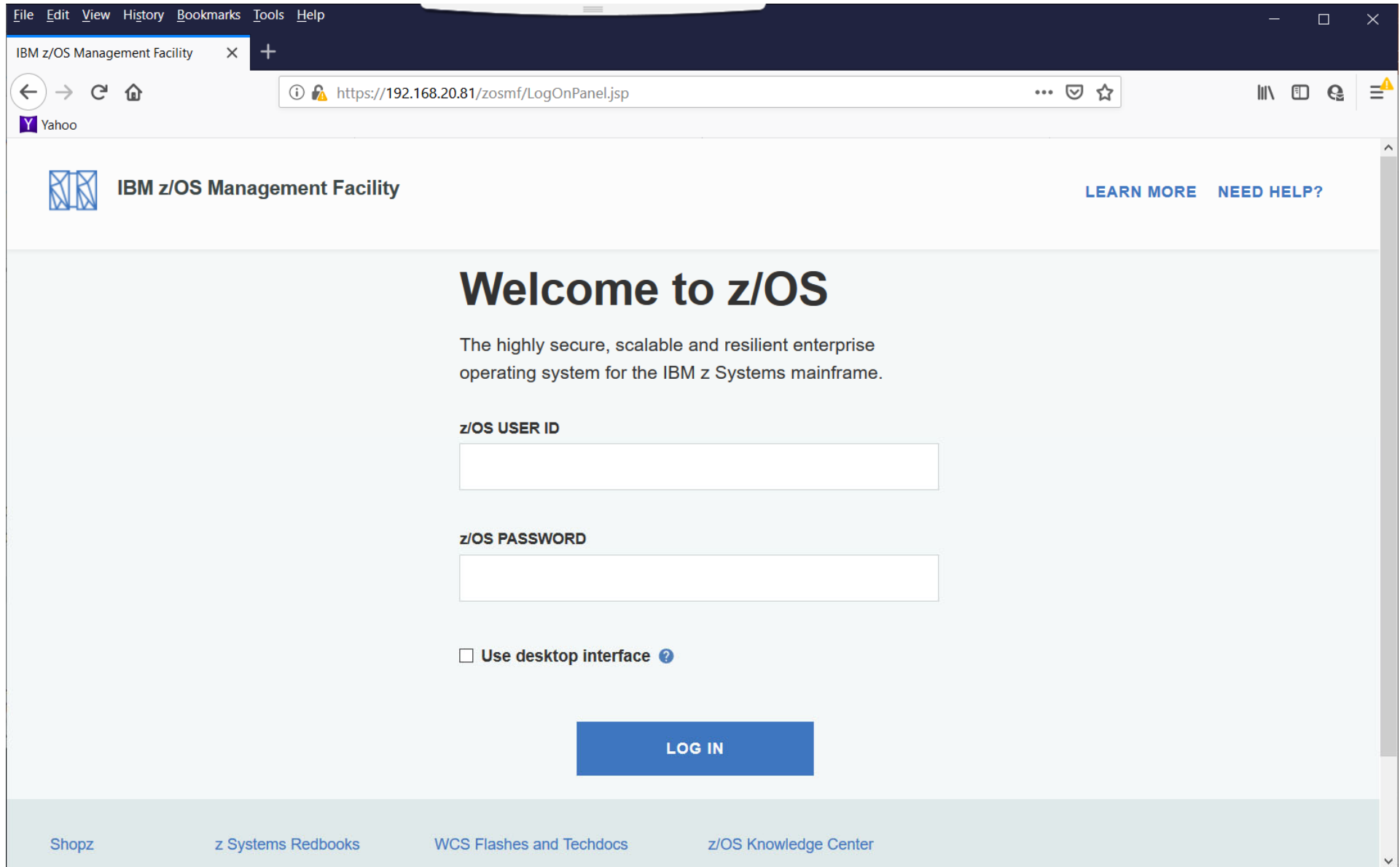
IBM Network Configuration Assistant for z/OS Communications Server



- Runs on zOSMF (available since z/OS V1R11)
- Network Configuration Assistant configurations are stored in binary files
 - Named “Backing Store” files (also referred to as Persistent Data Store)
 - Only Network Configuration Assistant for z/OS Communications Server can use Backing Store files!
 - zOSMF Tool saves Backing Store files on z/OS
 - Auto-backup to protect against loss of changes due to web browser session interruptions
- To use Network Configuration Assistant configurations the tool is used to send text files to z/OS
 - Network Configuration Assistant uses FTP to send the text files (FTP Server is required on z/OS)
 - Different text files can be generated by the Configuration Assistant
 - Separate policy file for each policy type (AT-TLS, IPsec, IDS, QoS, PBR)
 - Application setup files (IKED, NSSD, etc.)
- Older versions of Network Configuration Assistant Backing Store files may be upgraded to a later version.

Network Configuration Assistant Tool

Welcome screen



The screenshot shows a web browser window with the title "IBM z/OS Management Facility". The address bar displays the URL "https://192.168.20.81/zosmf/LogOnPanel.jsp". The page header includes the IBM logo and the text "IBM z/OS Management Facility", along with links for "LEARN MORE" and "NEED HELP?". The main content area features a large heading "Welcome to z/OS" followed by a description: "The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe." Below this, there are two input fields labeled "z/OS USER ID" and "z/OS PASSWORD". A checkbox labeled "Use desktop interface" with a help icon is positioned below the password field. A prominent blue "LOG IN" button is centered at the bottom of the main content area. The footer contains links to "Shopz", "z Systems Redbooks", "WCS Flashes and Techdocs", and "z/OS Knowledge Center".

File Edit View History Bookmarks Tools Help

IBM z/OS Management Facility

https://192.168.20.81/zosmf/LogOnPanel.jsp

IBM z/OS Management Facility

LEARN MORE NEED HELP?

Welcome to z/OS

The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe.

z/OS USER ID

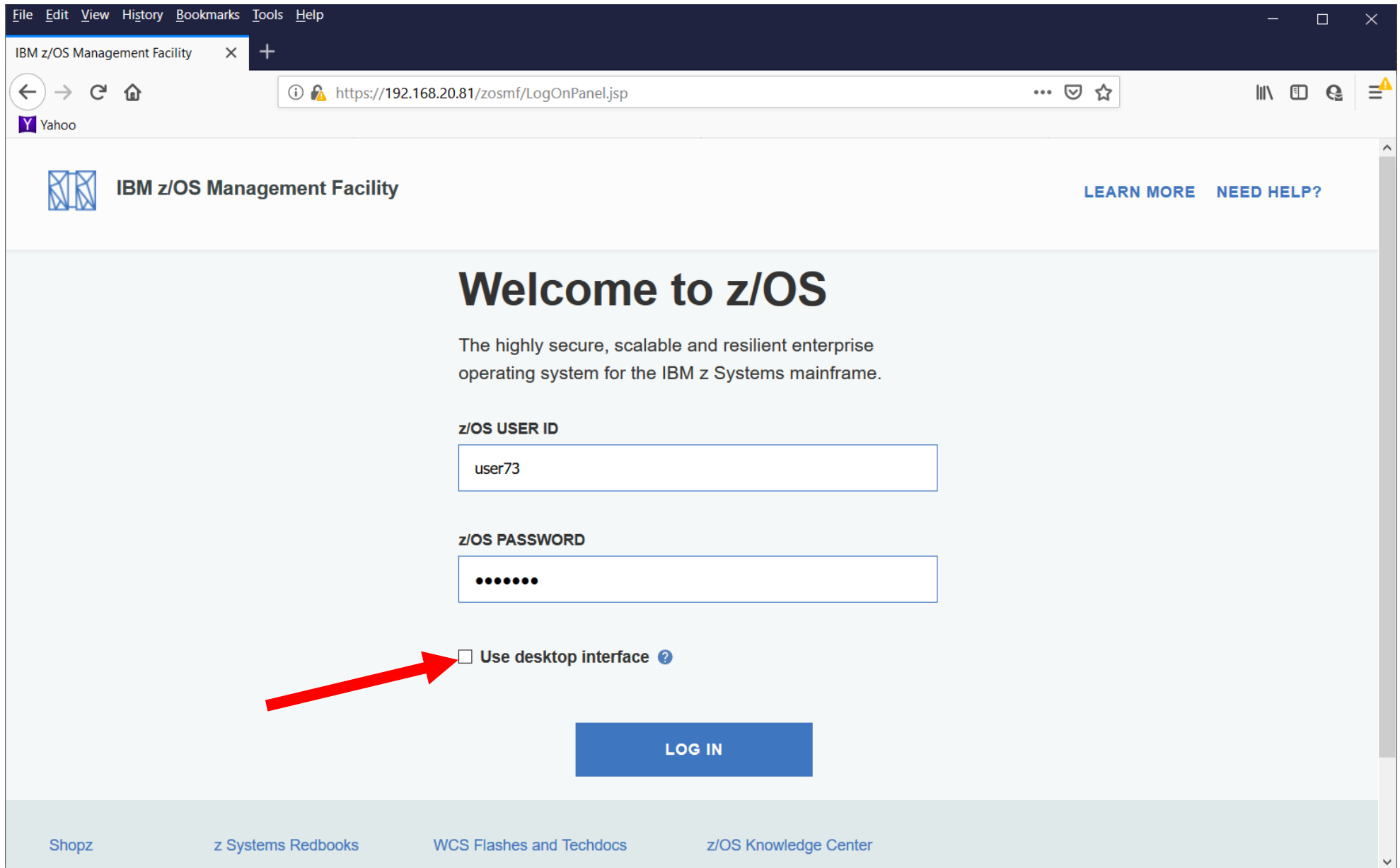
z/OS PASSWORD

☐ Use desktop interface ?

LOG IN

Shopz z Systems Redbooks WCS Flashes and Techdocs z/OS Knowledge Center

Logon Screen



The screenshot shows a web browser window with the title "IBM z/OS Management Facility". The address bar shows the URL "https://192.168.20.81/zosmf/LogOnPanel.jsp". The page header includes the IBM z/OS Management Facility logo and the text "LEARN MORE NEED HELP?". The main content area features a large heading "Welcome to z/OS" followed by a description: "The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe." Below this, there are two input fields: "z/OS USER ID" with the value "user73" and "z/OS PASSWORD" with masked characters "••••••". A checkbox labeled "Use desktop interface" with a question mark icon is located below the password field. A red arrow points to this checkbox. At the bottom of the form is a blue "LOG IN" button. The footer contains links to "Shopz", "z Systems Redbooks", "WCS Flashes and Techdocs", and "z/OS Knowledge Center".

File Edit View History Bookmarks Tools Help

IBM z/OS Management Facility

https://192.168.20.81/zosmf/LogOnPanel.jsp

Y Yahoo

IBM z/OS Management Facility

LEARN MORE NEED HELP?

Welcome to z/OS

The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe.

z/OS USER ID

user73

z/OS PASSWORD

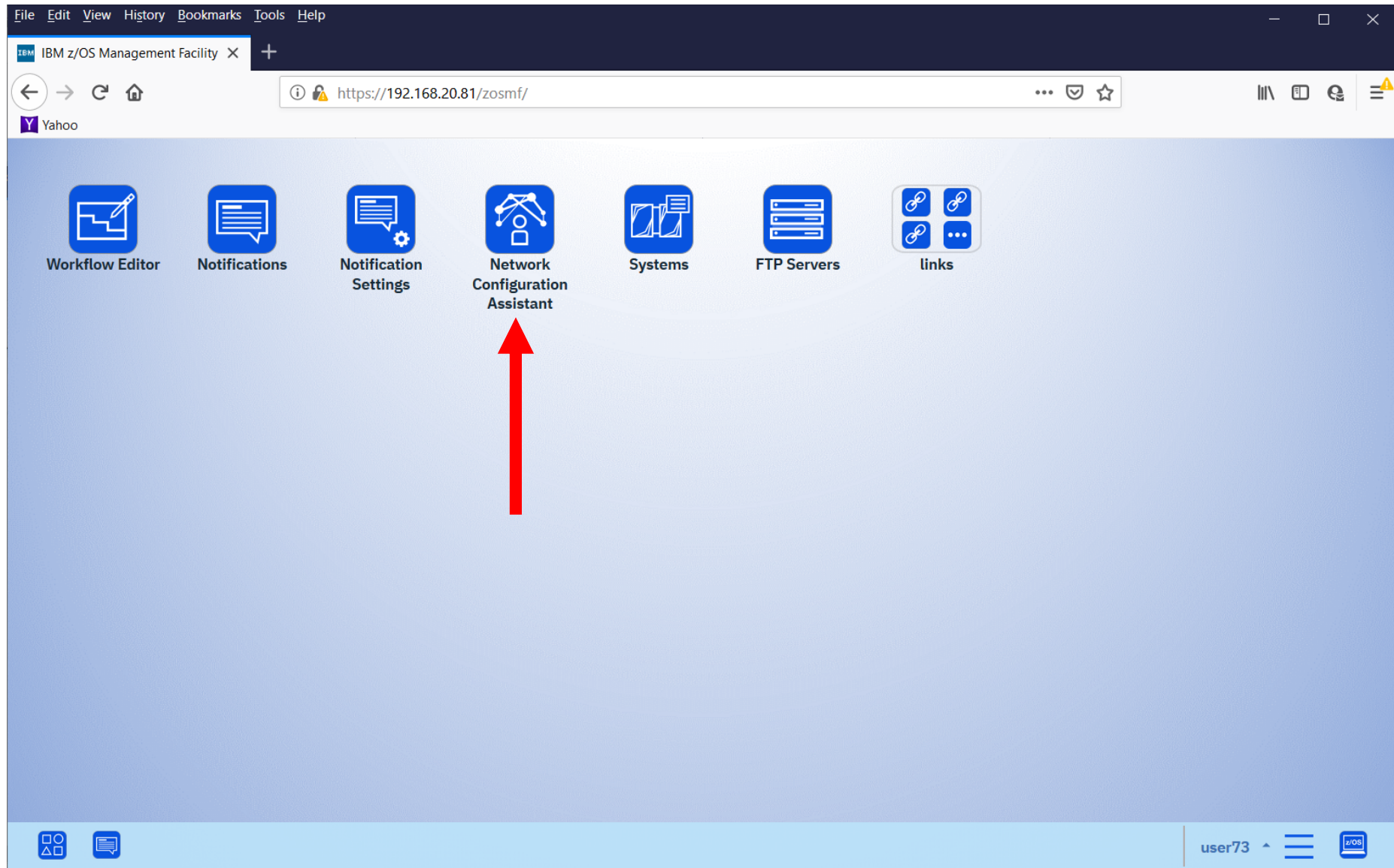
••••••

☐ Use desktop interface ?

LOG IN

Shopz z Systems Redbooks WCS Flashes and Techdocs z/OS Knowledge Center

Desktop Interface



Network Configuration Assistant

The screenshot displays the IBM z/OS Management Facility (z/OSMF) web interface. The browser window shows the URL `https://192.168.20.81/zosmf/NavigationTree.jsp`. The page title is "IBM z/OS Management Facility". The navigation pane on the left includes sections for "Welcome", "Notifications", "Workflow Editor", "Configuration" (which is expanded to show "Network Configuration Assistant"), "Links", and "z/OSMF Settings". A "Refresh" button is located below the navigation pane. The main content area displays a "Welcome" message with the following text:

Welcome to IBM z/OS Management Facility

IBM® z/OS® Management Facility (z/OSMF) provides a framework for managing various aspects of a z/OS system through a Web browser interface. By streamlining some traditional tasks and automating others, z/OSMF can help to simplify some areas of z/OS system management.

To learn more about z/OSMF, visit the links in the Learn More section.

To start managing your z/OS systems, select a task from the navigation area.

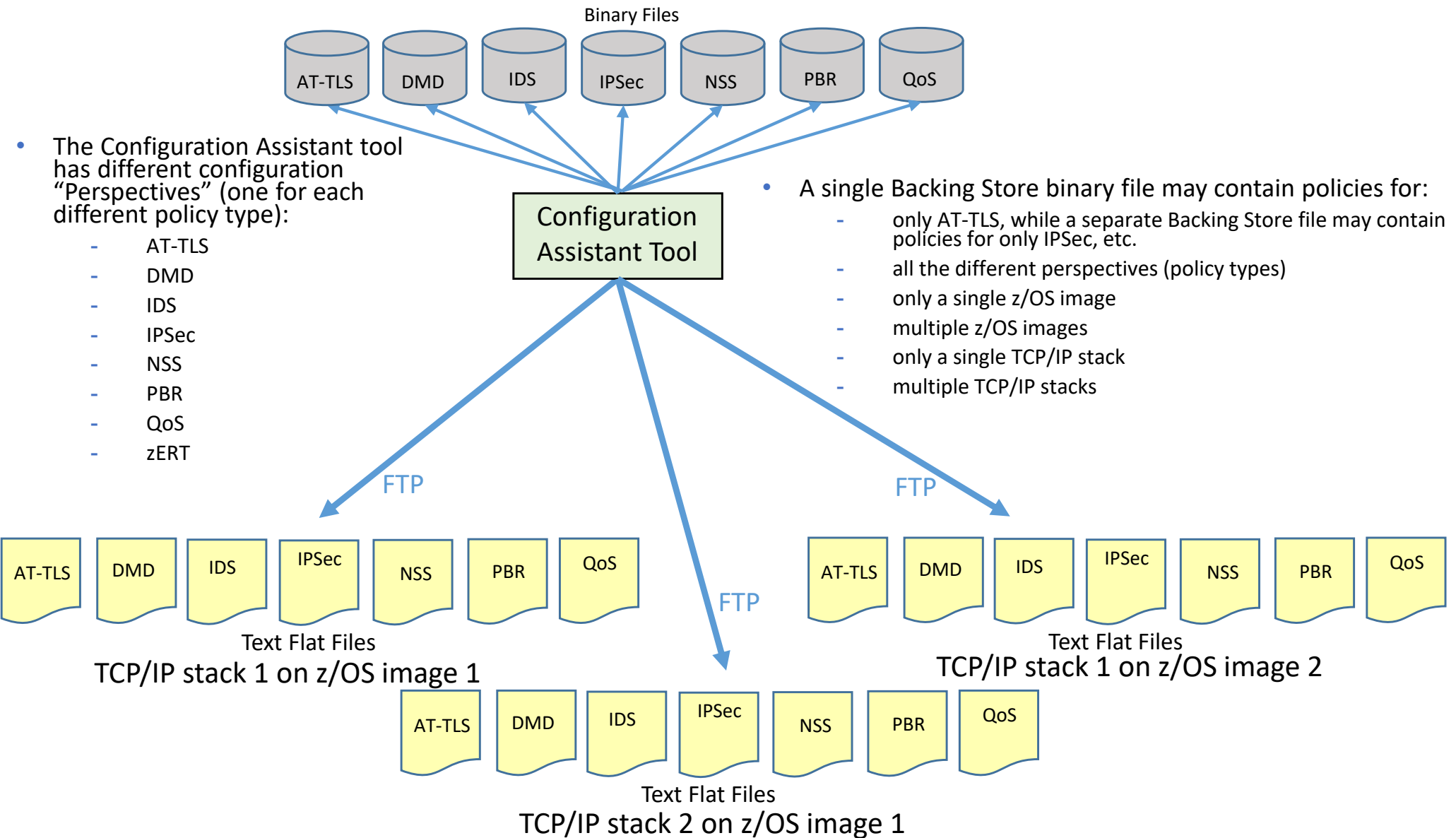
Learn More:

- [What's New](#)
- [z/OSMF tasks at a glance](#)
- [Getting started with z/OSMF](#)

Network Configuration Assistant Tool Usage

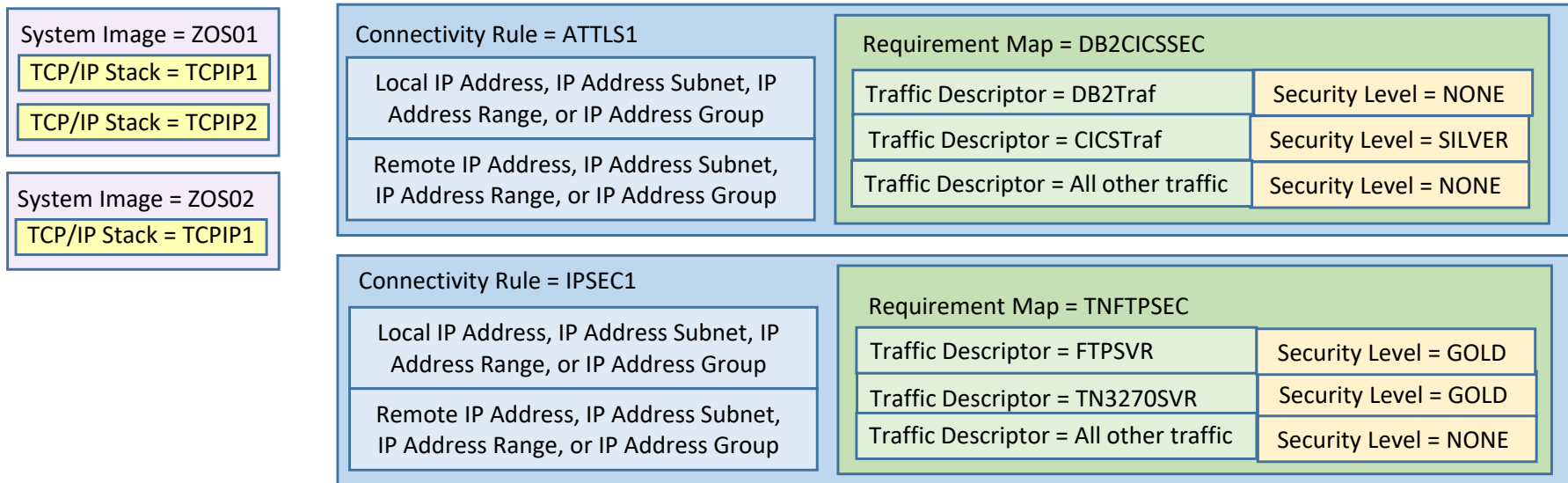
- As you can see on the previous foil, the Network Configuration Assistant (CA) tool may be used to configure:
 - z/OS Cloud – not covered in this class (see CA tutorial for more info)
 - AT-TLS
 - DMD
 - IDS
 - IPSec
 - NSS
 - PBR - not covered in this class
 - QoS - not covered in this class
 - zERT – not covered in this class
 - TCP/IP Profile – not covered in this class (may be used to customize a profile file for a TCP/IP stack)

Backing Store Files and Flat Files




z/OSMF V2.2 Backing Store files are stored in directory `/var/zosmf/data/app/CAV2R2/backingStore/`

AT-TLS and IPsec



- 1 Define Sysplex Group or use the “Default” group
- 2 Define system images (z/OS systems) and TCP/IP stacks
- 3 Select Type of Policy (AT-TLS or IPsec)
 - Define connectivity rules
 - Complete security policy for all traffic between two endpoints
- 6 Specify IP Addresses for data endpoints (IP Address Groups Reusable)
- 7 Define Requirements maps (reusable)
 - Maps a set of Traffic Descriptors to Security Levels
- 4 Define Traffic Descriptors (reusable)
- 5 Define Security Levels (reusable)

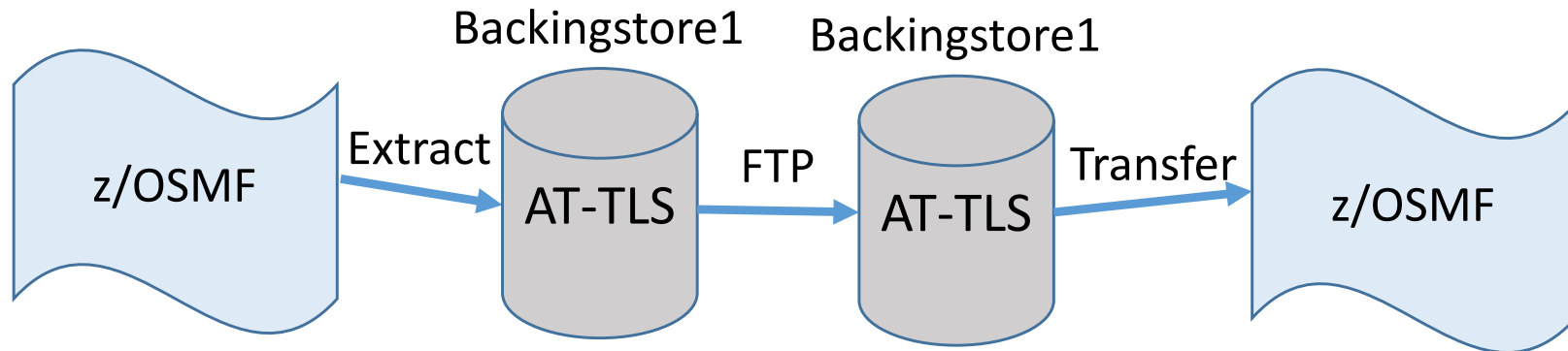
Network Configuration Assistant Data Model

- Define system images (z/OS systems) and TCP/IP stacks
- Select Type of Policy or Configuration Option 
- DMD
 - IP Address subnets (for exclusion)
- IP Filtering
 - Local IP Address, Subnet, Range, or Group
 - Remote IP Address, Subnet, Range, or Group
 - Traffic Descriptor
 - Permit or Deny
- IDS
 - Attack Types
 - Scans – Traffic Descriptors and Sensitivity
 - Traffic Regulation – Traffic Descriptors and Actions (Limit, Report, or both)
- NSS
 - Server or Client
- QoS
 - Local IP Address, Subnet, or Range
 - Remote IP Address, Subnet, or Range
 - Traffic Descriptors
 - Priority
 - Traffic Shaping Level
- PBR
 - Traffic Descriptors
 - Local IP Address, Subnet, Range, or Group
 - Remote IP Address, Subnet, Range, or Group
 - Routing Tables
 - Use Main Route Table?
- Type of Policy or Configuration Option
 - Application Transparent – Transport Layer Security (AT-TLS)
 - Defense Manager Daemon (DMD)
 - IP Filtering and IPsec
 - Intrusion Detection Services (IDS)
 - Network Security Services (NSS)
 - Quality of Service (QoS)
 - Policy Based Routing (PBR)
 - TCP/IP Profile
- zERT
 - Protocol
 - Port
 - Action

Samples, Samples, Samples

- Samples in the z/OS Communications Server
TCP/IP Unix sample directory:
 - /usr/lpp/tcpip/samples
- Samples in Network Configuration Assistant for z/OS
 - Connectivity Rules
 - Requirement Maps
 - Traffic Descriptors
 - Security Levels

Extract and Transfer

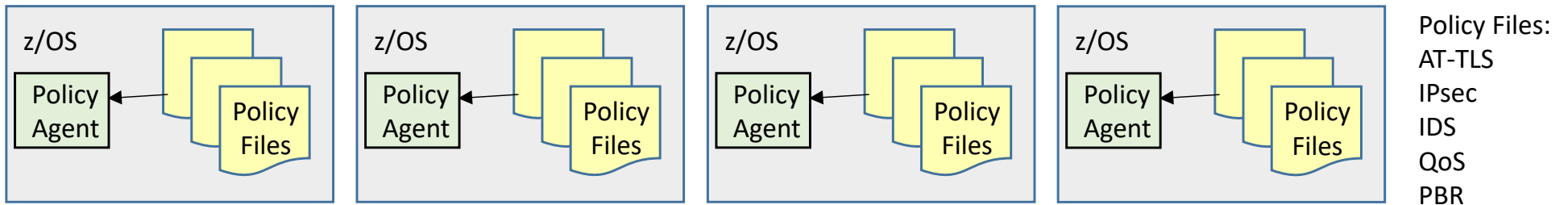


- From “Manage Backing Stores” panel
- Extract
 - Save Backing Store to a unix file.
- Transfer
 - Load Backing Store file from a unix file.

Policy Server

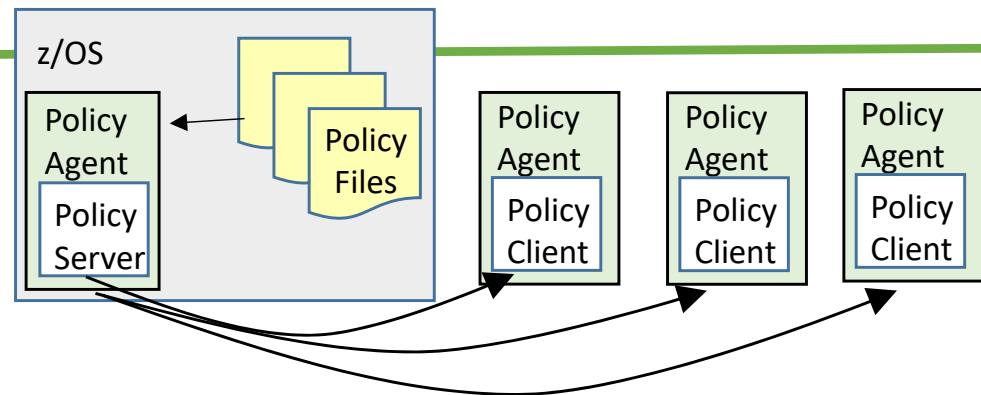


No Central Location for Policies



- Each z/OS system Policy Agent may have their own Policy files stored locally.
- Policy Administration may be from a single location
 - Configuration (Configuration Assistant or manual edits) and monitoring (pasearch) can be done from a single location (administrator computer).

Policy Server



- Centralized policy storage
 - Policy Server and Policy Clients can be non-sysplex, in sysplex, or cross-sysplex
 - IP connectivity required
- Policy Server provides policies to Policy Clients
 - Policy Client requests policies (ie. when client comes up or modify command)
 - When policies are changed on the server they are sent to clients
- Sysplex Not Required
 - Policy Server and Policy Clients can be non-sysplex, in sysplex, or cross-sysplex
- Availability
 - Backup Policy Server is supported
- Local Policies still supported
 - If Policy Client has policies locally stored, they will take precedence over policies from Policy Server.
- Administration may be from a single location (same as without Policy Server)
 - Configuration (Configuration Assistant or manual edits) and monitoring (pasearch) can be done from a single location (administrator computer).

Policy Files:
AT-TLS
IPsec
IDS
QoS
PBR

End of Topic



End of Topic

