RSH

CONSULTING

SERVAUTH Class

GSE UK
Security Working Group
June 2021

RSH Consulting – Robyn E. Gilchrist

RSH Consulting, Inc. is an IT security professional services firm established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050

Robyn E. Gilchrist is a Senior RACF and CA ACF2 Consultant. She assists clients with conducting penetration and vulnerability tests to evaluate z/OS controls and with enhancing access controls. As a systems programmer and network engineer, Ms. Gilchrist has installed, configured, and maintained the z/OS Communications Server and WebSphere Application Server (WAS) for z/OS in Network Deployment (ND) mode with associated ACF2 and RACF controls. She has converted CPF-connected ACF2 databases to RRSF-connected RACF databases.

- 617-977-9090
- R.Gilchrist@rshconsulting.com
- www.linkedin.com/in/robyn-e-gilchrist/

RACF and z/OS are Trademarks of the International Business Machines Corporation

SERVAUTH Protects TCP/IP

- SERVAUTH is the IBM supplied RACF class that protects z/OS Communication Server's TCP/IP base and applications
  - Use is optional but highly recommended
  - Supplements other z/OS Communication Server controls like Intrusion Detection Service (IDS), syslogd isolation, IP filtering

- CLASS Characteristics
  - RACLIST REQUIRED
  - DFTRETC=4

- Activation requires usual care and planning and is best done during maintenance window
  - SETR CLASSACT(SERVAUTH) RACLIST(SERVAUTH) GENERIC(SERVAUTH)

Terms and Variables Used

- Terms
  - endpoint
    - The termination point for a communication channel. A client and server each have an endpoint.
  - policy
    - A set of rules that govern the behavior of a managed user or resource
- Variables in SERVAUTH resource names
  - sysname
    - Value specified by MVS &SYSNAME. system symbol
    - sysname = SYSP in the following examples
  - tcpname
    - Name of the started procedure used to start TCPIP on z/OS
    - tcpname = TCPIP in the following examples
  - resname
    - A one to eight character value following the network specification in PROFILE.TCP
    - May not be a single “0” character
  - ftpdaemonname
    - Name of the started procedure used to start the FTP server on z/OS

TCP/IP on z/OS – “The Stack”

- The network stack or protocol stack (i.e. “The Stack”) is a set of network protocol layers and software that work together to allow communications between hosts

- Transmission Control Protocol / Internet Protocol (TCP/IP)
  - Most commonly used communication protocol suite
  - Non-proprietary – RFC 793
  - Implemented as z/OS Communications Server
    - z/OS Communications Server also handles SNA (VTAM)

- IP addresses for host identification

- Ports for network access

- Socket APIs for Pascal, REXX, CICS, Assembler, C, IMS program use

- Each TCP/IP address space is its own stack with its own IP addresses, ports and sockets
  - More than one stack on an LPAR is called a “multi-homed” LPAR

TCP/IP Components

- TCP/IP resources
  - Stack – A suite of protocols that allow packet-switched network communications regardless of network topology
  - Port – A stack access point for input or output to the network
  - Sockets – A unique communications endpoint within a port
  - NETSTAT command – display information about TCP/IP

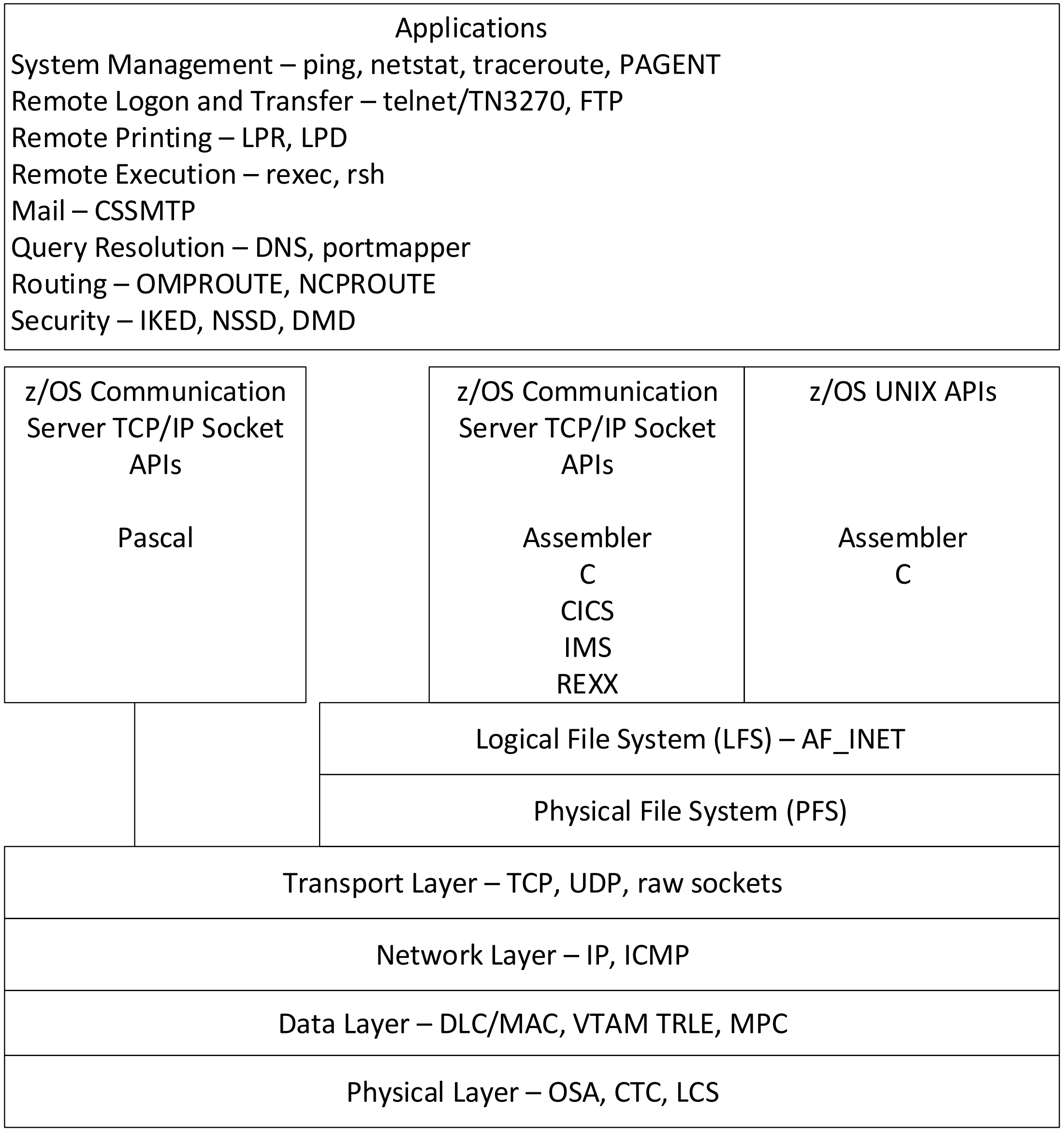
- TCP/IP services
  - Network Access Control (NAC)
  - Network management interfaces usage (NMI)
  - Fast Response Cache Accelerator (FRCA)
  - Miscellaneous (DCAS, rpcbind, CIM)

- TCP/IP applications including
  - TN3270/TN3270E Server (telnet)
  - FTP/FTPS Server
  - z/OS Policy Agent display (PAGENT)

The 7-Layer OSI Model on z/OS

Layer	OSI	z/OS	Description
7	Application	API	Application Programming Interface (API)
6	Presentation	LFS	Logical File System – AF_INET in BPXPRMxx
5	Session	PFS	Physical File System – ZFS, TFS, HFS
4	Transport	Transport	Transmission Control Protocol (TCP) User Datagram Protocol (UDP) Raw sockets
3	Network	Network	Internet Protocol (IP) Internet Control Message Protocol (ICMP)
2	Data	DLC/MAC VTAM MPC	Data Link Control/Media Access Control Transport Resource Link Entries (TRLE) Multipath Channel I/O
1	Physical	OSA CTC LCS	Open Systems Adapter Channel-to-Channel Adapter LAN Control Station

z/OS Communication Server Applications



Applications

System Management – ping, netstat, traceroute, PAGENT
Remote Logon and Transfer – telnet/TN3270, FTP
Remote Printing – LPR, LPD
Remote Execution – rexec, rsh
Mail – CSSMTP
Query Resolution – DNS, portmapper
Routing – OMPROUTE, NCPROUTE
Security – IKED, NSSD, DMD

z/OS Communication Server TCP/IP Socket APIs

Pascal

z/OS Communication Server TCP/IP Socket APIs

Assembler
C
CICS
IMS
REXX

z/OS UNIX APIs

Assembler
C

Logical File System (LFS) – AF_INET

Physical File System (PFS)

Transport Layer – TCP, UDP, raw sockets

Network Layer – IP, ICMP

Data Layer – DLC/MAC, VTAM TRLE, MPC

Physical Layer – OSA, CTC, LCS

SAF and SERVAUTH

- z/OS Communication Server TCP/IP is the resource manager that calls SAF for authorization to TCP/IP resources
  - Return Codes
    - 0 – Permit Access
    - 4 – No Decision (no profile)
    - 8 – Deny Access

- z/OS Communication Server action with a No Decision from SERVAUTH depends on function being requested

- UACC(NONE) is best practice

Protecting Stack Access

- EZB.INITSTACK.sysname.tcpname
  - Controls ability to open socket before security policy loads into the stack
    - SAF No Decision Action: DENY
    - SMF Type 80 record LOGSTR: TCPIP INIT STACK ACCESS CHECK
  - Do NOT allow daemons that require security policy control like FTP or TN3270
  - Permit USERIDs that start before TCP/IP and need a socket like z/OS Policy Agent

```
RDEF SERVAUTH EZB.INITSTACK.SYSP.TCPIP OWNER(RACFADM) UACC(NONE)
PERMIT EZB.INITSTACK.SYSP.TCPIP CLASS(SERVAUTH) ID(PAGENT) ACCESS(READ)
```

- EZB.STACKACCESS.sysname.tcpname
  - Allows access to the initialized TCP/IP stack, can open a socket, get hostname/hostid
    - SAF No Decision Action: PERMIT
    - SMF Type 80 record LOGSTR: TCPIP STACK ACCESS CHECK

```
PERMIT EZB.STACKACCESS.SYSP.TCPIP CLASS(SERVAUTH) ID(FTPSERVE) ACCESS(READ)
```

  - Permit servers and users of the servers
    - FTP Server
    - CICS Transaction Gateway / HTTP Server / WebSphere Application Server
    - Mail Server

TCP/IP Ports on z/OS

- Each port is a potential open door into z/OS and should be protected
  - Each TCP/IP stack has 65,536 ports
  - Each port represents a potential application process
  - A well-known port is a convention of which applications use which ports

- Low ports - 1 to 1023
  - Used by servers and system-level processes
  - Applications follow convention to use well-known ports
    - 21 used by FTP server (FTP)
    - 23 used by telnet server (TN3270)
    - 25 used by email server (CSSMTP)
    - 80/443 used by HTTP/HTTPS server (IBM HTTP Server)

- Ephemeral ports - z/OS default is 1024 to 65535
  - Some applications use ports above 1024 as their well-known port
    - 1414 used by MQSeries
    - 9080 used by WebSphere HTTP Transport
  - Used dynamically for temporary purposes like TN3270 or FTP endpoint

Protecting TCP/IP Low Ports in PROFILE.TCP

- PROFILE.TCP is the configuration file for TCP/IP
  - //PROFILE DD statement in TCP start deck
    - If no //PROFILE DD in TCP start deck, then search for file in
      - jobname.nodename.TCPIP
      - TCPIP.nodename.TCPIP
      - jobname.PROFILE.TCP
      - TCPIP.PROFILE.TCPIP

- Low port protection
  - TCPCONFIG RESTRICTLOWPORTS statement restricts TCP ports
  - UDPCONFIG RESTRICTLOWPORTS statement restricts UDP ports
  - UNRESTRICTLOWPORTS is default for TCP and UDP

- If RESTRICTLOWPORTS active, port bind permitted only if
    - JOBNAME matches PORT or PORTRANGE statement with optional SAF check, or
    - Application is APF authorized, or
    - Application is running as superuser/UID(0)

Reserved Ports

- RESERVED ports
  - Specified with PORT or PORTRANGE statement in PROFILE.TCP
    - Includes server JOBNAME (wildcards permitted)
    - May include the optional SAF keyword
  - RESERVED keyword in place of JOBNAME denies all access to the port

```
PORT
    21 TCP FTPD1     <- only JOBNAME FTPD1 can bind to port 21
    22 TCP RESERVED  <- port 22 is not available for use
    23 TCP TN3270*   <- JOBNAME starting with TN3270 can bind to port 23
    25 TCP *         <- any JOBNAME can bind to port 25
```

  - If JOBNAME doesn’t match
    - EDC5111I Permission denied. (errno2=0x744C7246)

Unreserved Ports

- Any port not specified on PORT or PORTRANGE statement is unreserved

- Can protect with PORT UNRSV statement
  - May include the optional SAF keyword

```
PORT UNRSV TCP *  <- Any JOBNAME can use an UNRESERVED port
```

- RESTRICTLOWPORTS
  - If RESTRICTLOWPORTS is active, PORT UNRSV applies to ports above 1023
  - If RESTRICTLOWPORTS is not active, PORT UNRSV applies to all ports

Protecting Ports with SERVAUTH

- EZB.PORTACCESS.sysname.tcpname.resname
  - Controls user ability to bind to non-ephemeral ports (i.e. low ports)
    - SAF No Decision Action: DENY
    - SMF Type 80 record LOGSTR: TCPIP PORT ACCESS CHECK PORT *portnum*

```
PE EZB.PORTACCESS.SYSP.TCPIP.FTPZONE1 CLASS(SERVAUTH)-
 ID(FTPSERVE) ACCESS(READ)
```

- PORT statement with SAF keyword allows SAF to control access to ports

```
PORT
       21    TCP FTPD1     SAF FTPZONE1
       UNRSV TCP *         SAF GENERIC
```

  - Only a batch, started task or TSO session with job name FTPD1 that runs with a USERID that has READ access to EZB.PORTACCESS.SYSP.TCPIP.FTPZONE1 can bind to port 21
  - Any batch, started task or TSO session with a USERID that has READ access to EZB.PORTACCESS.SYSP.TCPIP.GENERIC can bind to UNRESERVED ports above 1023

Protecting IPv4 Sockets

- A socket uniquely identifies a communication link between two endpoints
  - Allows multiple users to use the same port – e.g. browse web pages, use FTP
  - Identified by protocol, local-address and local-port

- EZB.SOCKOPT.sysname.tcpname.SO_BROADCAST
  - Limits use of “SO_BROADCAST” socket option needed to send broadcast datagrams
    - SAF No Decision Action: PERMIT
    - SMF Type 80 record LOGSTR: TCPIP SOCKOPT ACCESS CHECK
  - Determine use before locking with UACC(NONE)

```
RDEFINE SERVAUTH EZB.SOCKOPT.SYSP.TCPIP.SO_BROADCAST UACC(READ) AUDIT(ALL)
```

- Common TCP/IP applications that send broadcast datagrams
  - OMPROUTE – OSPF/RIP Router
  - SNTPD – Simple Network Time Protocol Daemon (Time Server)
  - RPCINFO – a z/OS UNIX synonym for ORPCINFO
  - ORPCINFO – Makes remote procedure calls (RPC) to an RPC server and displays the results

Protecting IPv6 Sockets

- EZB.SOCKOPT.sysname.tcpname.IPV6_option
  - Provides ability to control whether an application is permitted to set advanced socket API options
    - SAF No Decision Action: DENY unless USERID is APF authorized or superuser/UID(0)
    - SMF Type 80 record LOGSTR: TCPIP SOCKOPT ACCESS CHECK
  - Options are
    - NEXTHOP
    - TCLASS
    - RTHDR
    - HOPOPTS
    - DSTOPTS
    - RTHDRDSTOPTS
    - PKTINFO
    - HOPLIMIT
- IPv6 implementation on z/OS not particularly widespread

Layer 4 – Transport Layer

- Layer 4 of the OSI model is where the transport protocols for TCP and UDP and Raw sockets reside

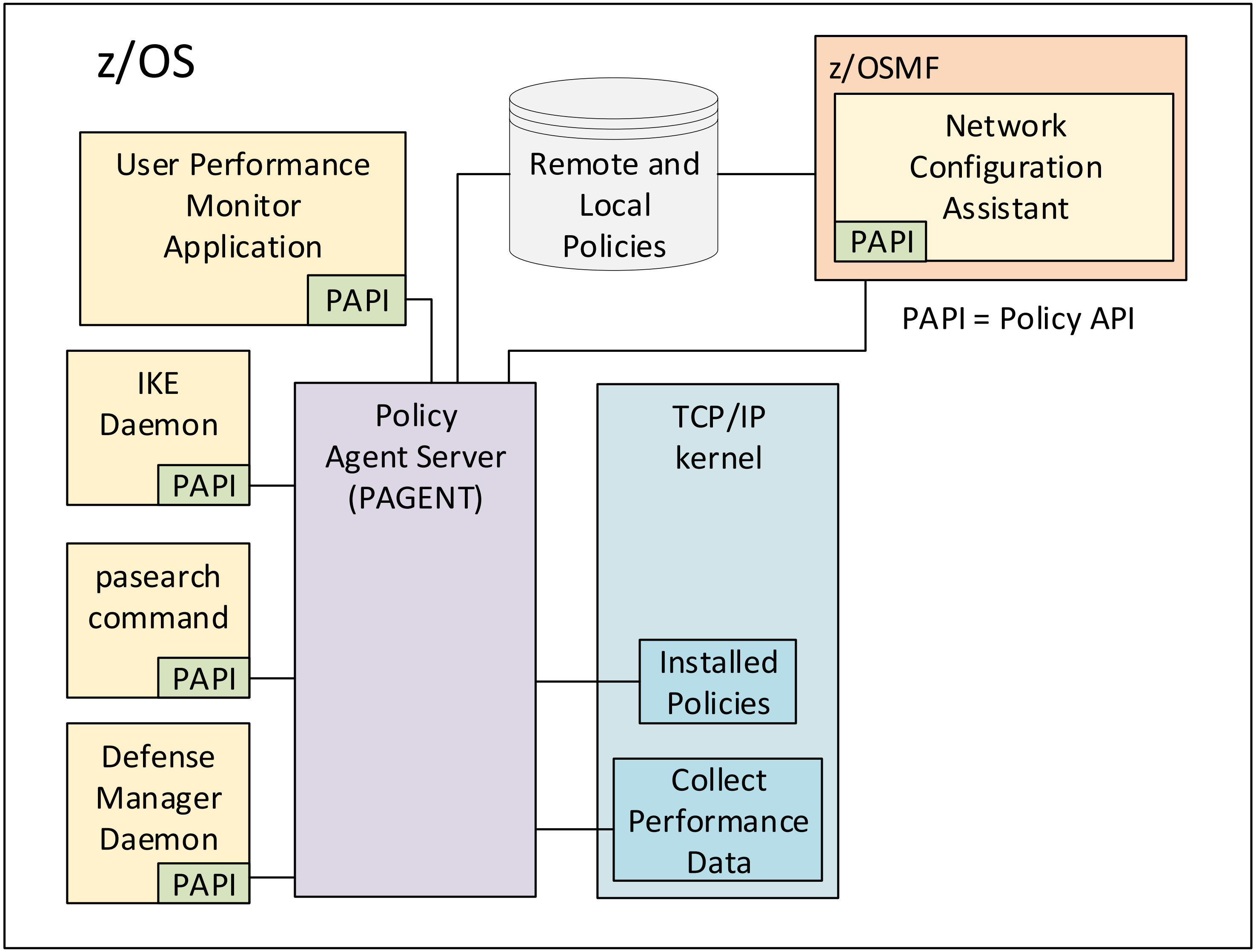
- In Policy-based networking, a policy type is configured into stack by the Policy Agent (PAGENT) policy component
  - Provides policy to TCP/IP stack at Transport Layer
  - Stack implements most policy types (ptype)
    - QOS – Quality of Service policy
    - IDS – Intrusion Detection Services policy
    - TTLS – Application Transparent/Transport Layer Security policy
    - IPSec – IPSec policy
    - Routing – Routing policy
    - CFGSERV – TCP/IP profile information

z/OS Policy Agent – PAGENT

- Configures network policy into stack
  - Policy may specify security, quality of service, routing, logging, etc.
  - Can view network policy with pasearch command
- Runs in its own address space - one per LPAR

- PAGENT is a required components of Policy-based networking
  - Stack - required
  - PAGENT address space - required
  - syslogd Daemon - required
  - Network Security Services Daemon (NSSD)
  - Defense Manager Daemon (DMD)
  - Traffic Regulation Management Daemon (TRMD)
    - required for IDS and IPSec policies
  - Internet Key Exchange Daemon (IKED)
  - Network Service Level Agreement Performance Monitor 2 (NSLAPM2)

PAGENT on z/OS



Protecting Policy Agent's pasearch Command

- EZB.PAGENT.sysname.image.ptype
  - Provides ability to restrict pasearch command for policy types
    - SAF No Decision Action: DENY
    - SMF Type 80 record LOGSTR: TCPIP EZACDRAU AUTH CHECK FOR EZB.PAGENT.*sysname.image.ptype*
    - Controls ability to display policy, not to update or activate policy
  - image is the tcpname, policy client name or import request name for policy information being requested
  - ptype is QOS, IDS, TTLS, IPSec, Routing or CFGSERV

- Restrict access to known Policy API (PAPI) clients
  - PAPI allows access to policy information by external user applications
  - Includes users of the pasearch command

```
RDEF SERVAUTH EZB.PAGENT.SYSP.TCPIP.TTLS UACC(NONE)
PE EZB.PAGENT.SYSP.TCPIP.TTLS CLASS(SERVAUTH) ID(RACFADM) ACCESS(READ)
```

Layer 3 – Network Layer

- Layer 3 of the OSI model is where IP addresses reside
- Can be protected by TERMINAL class, SERVAUTH class or both
- Private address do not route over the public internet, by default

Class	Address Range	Default Subnet Mask	Comments
A	0.0.0.0 – 127.255.255.255	255.0.0.0 (CIDR /8)	
	0.0.0.0		Reserved – all local
	10.0.0.0 – 10.255.255.255		Reserved private
	127.0.0.0 – 127.255.255.255		Reserved loopback
B	128.0.0.0 – 191.255.255.255	255.255.0.0 (CIDR /16)	
	169.254.0.0 – 169.254.255.255		Reserved – No IP
	172.16.0.0 – 172.31.255.255		Reserved private
C	192.0.0.0 – 223.255.255.255	255.255.255.0 (CIDR /24)	
	192.168.0.0 – 192.168.255.255		Reserved private
D	224.0.0.0 – 239.255.255.255	N/A	Multicast

IPv4 Address and Terminal Addresses

- When connected using IP applications like TN3270 or FTP, the IPv4 address is used as the terminal address

- SMF records IPv4 addresses in the header portion of the SMF Type 80 Unload
  - INIT_TERM field (offset 171) contains the hex representation of the 32-bit IPv4 address

	First Octet	**Second Octet**	**Third Octet**	**Fourth Octet**	**Result**
Decimal	10	100	21	112	10.100.21.112
Hex	0A	64	15	70	0A641570

TERMINAL Class

- TERMINAL class can be used to limit an IP host address to a USERID

```
RDEFINE TERMINAL 0A641570 UACC(NONE)
PERMIT 0A641570 CLASS(TERMINAL) ID(GOODUSR) ACCESS(READ)
```

  - NOTERMUACC on all connected groups hardens users to only logon at terminals with permitted access
  - Generics are overly broad and their use is discouraged

- GTERMINL grouping profile can be used to define sets of terminals

- Many shops do not run TERMINAL class

- TERMINAL does not distinguish between network entry points (Port of Entry)
  - If the user comes in on another IP address, this may not be desired
  - Difficult to manage on multi-homed systems (more than one TCP/IP started task on an LPAR)

Using SERVAUTH with NETACCESS Statement

- SERVAUTH class accepts resname as provided by the NETACCESS statement in PROFILE.TCP

- Provides one-to-one mapping between a network, subnetwork or host and a SAF resource name
  - Most specific network map is used

- Network/subnetwork/host assigned a security zone (resource name) with the NETACCESS statement in PROFILE.TCP
  - Controls INBOUND and/or OUTBOUND traffic
  - NOINBOUND OUTBOUND is default
  - CACHEALL indicates SAF results are stored in core regardless of permit or deny
    - All subsequent queries use cache
    - Limits audit reporting to first use of zone
    - This is the default
  - CACHEPERMIT and CACHESAME
    - variations of cache permits, do not cache denies

NETACCESS Statement and resname

```
NETACCESS INBOUND OUTBOUND                         ; check both directions
  10.1.100.0     255.255.255.0     DNGRZONE ; Network address
  10.1.100.64    255.255.255.192      ZONE1 ; SYSA PROD subnet
  10.1.100.113   255.255.255.255  FTPZONE1 ; ZONE1 FTP Server host
  10.1.100.128/26                     ZONE2 ; SYSB QA subnet
  10.1.100.192   255.255.255.192    TSTZONE ; SYSC DEV subnet
  10.1.100.224   255.255.255.252    DALZONE ; subnet - Dallas
  10.1.100.228/30                   BOIZONE ; subnet - Boise
  10.1.100.232/28                           ; unzoned
  DEFAULTHOME                       DEFHOME ; all local 0.0.0.0
  DEFAULT                            DEFNET ; everything else
ENDNETACCESS
```

- resname (in bold) is a parameter on the NETACCESS statement and is optional
- resname indicates the 1-8 character suffix sent to SAF
- Addresses can use “/” notation or “octets” to indicate the network subnet mask
- If no resname is provided, no SAF check is performed to SERVAUTH

NETACCESS Profile

- EZB.NETACCESS.sysname.tcpname.resname
  - Controls local user inbound and outbound access and local user access to local IP addresses when doing an explicit bind – i.e. Is the user authorized to use the network?
    - SAF No Decision Action: DENY
    - SMF Type 80 record LOGSTR: TCPIP NETWORK ACCESS CHECK *ipaddress*
  - resname is specified on the NETACCESS statement in PROFILE.TCP

```
RDEF SERVAUTH EZB.NETACCESS.SYSP.TCPIP.FTPZONE1 UACC(NONE)
```

  - READ access is required to use the network

```
PE EZB.NETACCESS.SYSP.TCPIP.FTPZONE1 CLASS(SERVAUTH) -
     ID(FTPSERVE) ACCESS(READ)
PE EZB.NETACCESS.SYSP.TCPIP.FTPZONE1 CLASS(SERVAUTH) -
     ID(GOODUSR) ACCESS(READ)
```

FTP PORTOFENTRY4 Statement

- The PORTOFENTRY4 statement is an FTP Server initialization statement in FTP.DATA that specifies the resource class name the FTP Server requests the Unix kernel pass to SAF for IPv4 client logins

- TERMINAL option - Default
  - READ access to TERMINAL required regardless of SERVAUTH specification
  - If the client comes in on a network not mapped with NETACCESS statement, TERMINAL class is called without a call to SERVAUTH

- SERVAUTH option
  - Tells FTP Server to use resname suffix from NETACCESS statement in PROFILE.TCP in call to SERVAUTH profile

```
PERMIT EZB.NETACCESS.SYSP.TCPIP.FTPZONE1 CLASS(SERVAUTH) -
     ID(GOODUSR) ACCESS(READ)
```

Restricting FTP Access with SERVAUTH

- EZB.FTP.sysname.ftpdaemonname.ACCESS.HFS
  - Provide ability to restrict FTP User access to z/OS Unix filesystem
    - SAF No Decision Action: PERMIT
    - SMF Type 80 record LOGSTR: (none)
- EZB.FTP.sysname.ftpdaemonname.PORTxxxxx
  - Controls user ability to access FTP Server based on logon USERID
  - VERIFYUSER must be set TRUE in FTP.DATA to use this profile
    - SAF No Decision Action: PERMIT
    - SMF Type 80 record LOGSTR: (none)
- EZB.FTP.sysname.ftpdaemonname.SITE.DEBUG
  - Restricts usage of DEBUG command which generates a large amount of output
    - SAF No Decision Action: PERMIT
    - SMF Type 80 record LOGSTR: (none)
- EZB.FTP.sysname.ftpdaemonname.SITE.DUMP
  - Restricts usage of DUMP command which generates a large amount of output
    - SAF No Decision Action: PERMIT
    - SMF Type 80 record LOGSTR: (none)

Securing the NETSTAT Command

- NETSTAT displays information about TCP/IP

- EZB.NETSTAT.sysname.tcpname.netstat_option
  - Provides ability to restrict NETSTAT command usage
    - SAF No Decision Action: PERMIT, except for DROP when access is denied
    - SMF Type 80 record LOGSTR: TCPIP EZACDNET AUTH CHECK FOR profile

```
RDEF SERVAUTH EZB.NETSTAT.SYSP.TCPIP.PORTL UACC(NONE)

PE EZB.NETSTAT.SYSP.TCPIP.PORTL CLASS(SERVAUTH) ID(RACFADM)-
ACCESS(READ)
```

  - Permit RACFADM to display NETSTAT command with PORTLIST option to see the resname associated with the PORT

TSO NETSTAT PORTList Command Output

```
netstat portl
 MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPIP           13:04:56
 Port# Prot User     Flags    Range       SAF Name
 ----- ---- ----     -----    -----       --------
    19  TCP MISCSERV DA
    20  TCP OMVS     DA
    21  TCP FTPSERVE DAF                  FTPZONE1
    23  TCP TN3270   DA
    25  TCP CSSMTP   DA
    53  TCP NAMESRV  DA
   111  TCP PORTMAP  DA
   512  TCP RXSERVE  DA
   515  TCP LPSERVE  DA
   750  TCP MVSKERB  DA
   751  TCP ADM@SRV  DA
  1414  TCP CSQPCHIN DA
  3000  TCP CICSTS54 DA
  9080  TCP ZOSCSRV* DAR      09080-09082
  9443  TCP ZOSCSRV* DAR      09443-09445
    53  UDP NAMESRV  DA
   111  UDP PORTMAP  DA
   135  UDP LLBD     DA
   161  UDP OSNMPD   DA
   162  UDP SNMPQE   DA
   520  UDP OROUTED  DA
   580  UDP NCPROUT  DA
   750  UDP MVSKERB  DA
  9080  UDP ZOSCSRV* DAR      09080-09082
  9443  UDP ZOSCSRV* DAR      09443-09445
READY
```

NETSTAT Options

NETSTAT option	Description
ACCess,NETwork	Displays information about the network access tree in TCP/IP.
ALL	Displays detailed information about TCP connections and UDP sockets, including some that were recently closed.
ALLConn	Displays information for all TCP/IP connections, including recently closed ones.
ARp	Displays ARP cache information.
BYTEinfo	Displays the byte-count information about each active TCP connection and UDP socket.
CACHinfo	Displays information about Fast Response Cache Accelerator statistics.
CONFIG	Displays TCP/IP configuration data.
COnn	Displays information about each active TCP/IP connection.
DEFADDRT	Displays the policy table for IPv6 default address selection.
DEvlinks	Displays information about interfaces in the TCP/IP address space.
HOme	Displays the home list.
IDS	Displays information about intrusion detection services.
ND	Displays IPv6 Neighbor Discovery cache information.
PORTList	Displays the list of reserved ports and the port access control configuration for unreserved port
RESCache	Displays information about the operation of the system-wide resolver cache.
ROUTe	Displays routing information.
SOCKets	Displays information for open TCP or UDP sockets that are associated with a client name.
SRCIP	Displays information for all job-specific and destination-specific source IP address associations on the TCP/IP address space.
STATS	Displays TCP/IP statistics for each protocol.
TTLS	Displays Application Transparent Transport Layer Security (AT-TLS) information for TCP protocol connections.
VCRT	Displays the dynamic VIPA Connection Routing Table information.
VDPT	Displays the dynamic VIPA Destination Port Table information.
VIPADCFG	Displays the current dynamic VIPA configuration information for a host.
VIPADyn	Displays the current dynamic VIPA and VIPAROUTE information for a local host.

Controlling Dynamic Virtual IP Addresses (DVIPA)

- Dynamic Virtual IP Address (DVIPA) is a function that allows the system to move IP addresses to other systems in the event of an application, system or stack failure

- EZB.BINDDVIPARANGE.sysname.tcpname
  - Control whether an application can create and bind to a DVIPA defined on PROFILE.TCP VIPARANGE statement
    - SAF No Decision Action: PERMIT
    - SMF Type 80 record LOGSTR: TCPIP BINDDVIPA ACCESS CHECK
- EZB.BINDDVIPARANGE.sysname.tcpname.resname
  - Control whether an application can create and bind to a DVIPA defined on PROFILE.TCP VIPARANGE statement that includes a SAF resname parameter
    - SAF No Decision Action: DENY
    - SMF Type 80 record LOGSTR: TCPIP BINDDVIPA SAF ACCESS CHECK
- EZB.MODDVIPA.sysname.tcpname
  - Control whether an application can create and bind to a DVIPA defined on PROFILE.TCP VIPARANGE statement using SIOCVIPA ioctl call
    - SAF No Decision Action: DENY unless user is APF authorized or superuser/UID(0)
    - SMF Type 80 record LOGSTR: TCPIP MODDVIPA or SIOCSVIPA(6) ACCESS CHECK
- EZB.MODDVIPA.sysname.tcpname.resname
  - Control whether an application can create and bind to a DVIPA defined on PROFILE.TCP VIPARANGE statement using SIOCVIPA ioctl call that includes a SAF resname parameter
    - SAF No Decision Action: DENY
    - SMF Type 80 record LOGSTR: TCPIP MODDVIPA or SIOCSVIPA(6) SAF ACCESS CHECK

Network Management Interfaces (NMI)

- A standardized interface that allows for applications to provide management and monitoring support of network services and applications
- Intended for network management applications
- Includes
  - SNMP
  - Packet traces
  - zERT
  - IPSec
  - Network Security Services (NSS) Servers and Clients
  - SNA
- See “Some Communication Server Resource Names” at end of presentation

SERVAUTH Protections For Other Resources

- z/OSMF
  - CEA.CEATSO.TSOREQUEST
    - Allows the HTTP client applications on your z/OS system to start and manage TSO/E address spaces. Allows the z/OSMF server to start and manage TSO/E address space services.
    - SAF No Decision Action: DENY
  - CEA.SIGNAL.ENF83
    - Allows the z/OSMF server to use ENF83 to indicate its status to other systems in the sysplex.
    - SAF No Decision Action: DENY
  - EZB.NETWORKUTILS.CLOUD.mvsname
    - Allows z/OS Configuration Assistant to issue operator commands for cloud provisioning and management
    - SAF No Decision Action: DENY

- RACF Callable Services
  - IRR.HOST.host-name
    - Controls access to initACEE service for ACEE creation and certificate queries
      - Also allows for certificate queries and registration/deregistration
      - host-name is specified in hostIdMappings certificate extension
      - Used by z/OS kernel on behalf of servers, for example
      - SAF No Decision Action: Program dependent
    - Can be used with Multi-Factor Authentication (MFA)

References

- z/OS Communications Server: IP Configuration Guide (SC27-3650-xx)
  https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.halz002/abstract.htm
- z/OS Communications Server: IP Configuration Reference (SC27-3651-xx)
  https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.halz001/abstract.htm
- z/OS Communications Server: IP Programmer's Guide and Reference (SC27-3659-xx)
  https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.halx001/abstract.htm
- z/OS Communications Server: IP System Administrator's Commands (SC27-3661-xx)
  https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R3SC273661/$file/halu101_v2r3.pdf
- z/OS Communications Server: SNA Resource Definition Reference (SC27-3675-xx)
  https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R3SC273675/$file/istrdr0_v2r3.pdf
- z/OS Management Facility Configuration Guide (SC27-8419-xx)
  https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R3SC278419/$file/izua300_v2r3.pdf
- RSH Consulting RACF Survey of RACF-L – March 2019
  https://www.rshconsulting.com/surveys/RSH_Consulting___RACF_Survey_090___SERVAUTH.pdf
- Internet Assigned Numbers Authority (IANA)
  https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Some Communication Server Resource Names

Function	SERVAUTH resource name	Description	No SAF DECISION	SMF Type 80 record LOGSTR
CIM Server Access Control	EZB.CIMPROV.sysname.tcpname	Provides ability to restrict access to Common Information Model (CIM) data	DENY	TCPIP CIM PROVIDER CHECK
Cloud	EZB.NETWORKUTILS.CLOUD.mvsname	Allows z/OS Configuration Assistant to issue operator commands for cloud provisioning and management		
DCAS Server Access Control	EZA.DCAS.cvtsysname	Controls ability to access Digital Certificate Access Server (DCAS) based on SAF user associated with a TLS-authenticated X.509 client certificate	PERMIT	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname> or DCAS SAFCERT CHECK FOR USER certuser
FRCA Access Control	EZB.FRCAACCESS.sysname.tcpname	Provides ability for user to create Fast Response Cache Accelerator (FRCA) cache	DENY2	TCPIP FRCA ACCESS CHECK
IPSec	EZB.IPSECCMD.sysname.tcpname.command_type	Controls ability to control ipsec command use	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
IPSec Command Access	EZB.IPSECCMD.sysname.DMD_GLOBAL.command_type	Controls ability to control ipsec command use	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NMI IPSec (remote)	EZB.NETMGMT.sysname.clientname.IPSEC.CONTROL	Controls whether a user issue NMI requests to manage IPSec NSS Clients and NSS Server clients	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NMI IPSec (remote)	EZB.NETMGMT.sysname.clientname.IPSEC.DISPLAY	Controls whether a user can issue NMI monitoring requests to IPSec and NSS Server for NSS clients	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>

DENY2 = unless user is WLM or Unix superuser

Some Communication Server Resource Names

Function	SERVAUTH resource name	Description	No SAF DECISION	SMF Type 80 record LOGSTR
NMI IPSec (local)	EZB.NETMGMT.sysname.tcpname.IPSEC.CONTROL	Controls whether a user issue NMI requests to manage IP filtering and IPSec function on local stack	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NMI IPSec (local)	EZB.NETMGMT.sysname.tcpname.IPSEC.DISPLAY	Controls whether a user can issue NMI requests to retrieve local IKE and IPSec monitoring data	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NMI IPSec Command Access Control	EZB.NETMGMT.sysname.sysname.IKED.DISPLAY	Controls whether a user can issue NMI requests to display IKE and IPSec NSS client information	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NSS NMI IPSec	EZB.NETMGMT.sysname.sysname.NSS.DISPLAY	Controls whether a user can issue NMI requests to display connections to NSS Server	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NMI Service Access Control	EZB.NETMGMT.sysname.tcpname.SYSTCPCN	Provides ability to restrict access to real time TCP connection information	DENY1	TCPIP NETWORK MANAGEMENT
NMI Service Access Control	EZB.NETMGMT.sysname.tcpname.SYSTCPDA	Provides ability to restrict access to real time TCP packet trace records	DENY1	TCPIP NETWORK MANAGEMENT
NMI Service Access Control	EZB.NETMGMT.sysname.tcpname.SYSTCPER	Provides ability to restrict access to z/OS Encryption Readiness Technology (zERT)	DENY1	TCPIP NETWORK MANAGEMENT
NMI Service Access Control	EZB.NETMGMT.sysname.tcpname.SYSTCPOT	Provides ability to restrict access to real time OSAENTA information	DENY1	TCPIP NETWORK MANAGEMENT
NMI Service Access Control	EZB.NETMGMT.sysname.tcpname.SYSTCPSM	Provides ability to restrict access to real time SMF records	DENY1	TCPIP NETWORK MANAGEMENT

DENY1 = unless user is superuser/UID(0) or has READ access to BPX.SUPERUSER

Some Communication Server Resource Names

Function	SERVAUTH resource name	Description	No SAF DECISION	SMF Type 80 record LOGSTR
NMI SNA	IST.NETMGMT.sysname.SNAMGMT	Controls access to VTAM ISTMGCEH subtask		
NMI TCP/IP trace	EZB.TRCCTL.sysname.tcpname.DATTRACE	Controls whether an application can invoke NMI to set filters for data trace	DENY	TCPIP NETWORK MANAGEMENT
NMI TCP/IP trace	EZB.TRCCTL.sysname.tcpname.OPEN	Controls whether an application can invoke NMI to open a packet trace	DENY	TCPIP NETWORK MANAGEMENT
NMI TCP/IP trace	EZB.TRCCTL.sysname.tcpname.PKTTRACE	Controls whether an application can invoke NMI to set filters for packet trace	DENY	TCPIP NETWORK MANAGEMENT
NMI TCP/IP trace	EZB.TRCSEC.sysname.tcpname.ATTLS	Controls whether an application request AT-TLS cleartext data on data trace filter	DENY	TCPIP NETWORK MANAGEMENT
NMI TCP/IP trace	EZB.TRCSEC.sysname.tcpname.IPSEC	Controls whether an application request IPSec cleartext data on packet trace filter	DENY	TCPIP NETWORK MANAGEMENT
NSS Server Access Control	EZB.NSS.sysname.clientname.IPSEC.CERT	Controls whether an NSS IPSec client can register with NSS Server for an IPSec certificate	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NSS Server Access Control	EZB.NSS.sysname.clientname.IPSEC.NETMGMT	Controls whether an NSS IPSec client can register with NSS Server IPSec remote server management	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NSS Server Access Control	EZB.NSS.sysname.clientname.XMLAPPLIANCE.PRIVKEY	Controls whether an NSS XMLAppliance client can register with NSS Server for keyring service	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NSS Server Access Control	EZB.NSS.sysname.clientname.XMLAPPLIANCE.SAFACCESS	Controls whether an NSS XMLAppliance client can register with NSS Server for SAF access	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>

Some Communication Server Resource Names

Function	SERVAUTH resource name	Description	No SAF DECISION	SMF Type 80 record LOGSTR
NSS Server Certificate Access Control	EZB.NSSCERT.sysname.mappedlabelname.CERTAUTH	Controls whether an NSS client can access a CERTAUTH on an NSS Server keyring	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NSS Server Certificate Access Control	EZB.NSSCERT.sysname.mappedlabelname.HOST	Controls whether an NSS client can access a PERSONAL or SITE certificate on an NSS Server keyring	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
NSS Server Certificate Access Control	EZB.NSSCERT.sysname.mappedlabelname.PRIVKEY	Controls whether an NSS client can access the private key on an NSS Server keyring	DENY	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
OSM Access Control	EZB.OSM.sysname.tcpname	Controls ability to access intranode management network using OSM interfaces	DENY	TCPIP OSM ACCESS CHECK
Partner Information ioctl Access Control	EZB.IOCTL.sysname.tcpname.PARTNERINFO	Controls whether an application can use SIOCPARTNERINFO ioctl to obtain partner security credentials over a plex over a trusted TCP connection	DENY	SIOCGPARTNERINFO
rpcbind Access Control	EZB.RPCBIND.sysname.rpcbindname.REGISTRY	Provides ability to control if user can register and unregister ports with rpcbind	DENY	(none)
SNMP Agent Control	EZB.SNMPAGENT.sysname.tcpname		PERMIT	TCPIP EZACDRAU AUTH CHECK FOR <SERVAUTH resname>
TN3270E Access Control	EZB.TN3270.sysname.tn3270name.PORTxxxxx	Controls ability to TN3270E Server based on SAF user associated with a TLS-authenticated X.509 client certificate	DENY	TN3270 SAFCERT CHECK FOR USER userid PORT portnum ON tn3270name