VANGUARD
Integrity Professionals
Information Security Experts

# Implementing SERVAUTH Class Profiles

Jim McNeill

IBM Server Proven
Business Partner IBM



## TRADEMARKS

VANGUARD
Integrity Professionals
Information Security Experts

- The following are trademarks or registered trademarks of the International Business Machines Corporation:
  - IBM
  - z/OS
  - MVS/ESA
  - SecureWay
  - S/390
  - z/OS
  - MVS/DFP
  - RACF
  - VTAM
- UNIX is a registered trademark of The Open Group in the United States and other countries.

## Unit Topics

VANGUARD Integrity Professionals Information Security Experts

1. Basic OSI models
2. IP sub-netting basics
3. Stacks
4. Ports
5. Networks
6. Misc controls
7. SERVAUTH Profiles



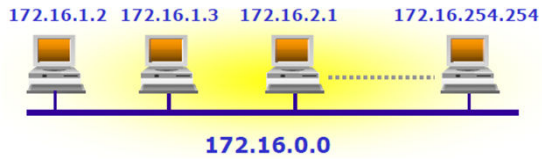
## Open Systems Interconnection Model

VANGUARD Integrity Professionals Information Security Experts

| | OSI Layers | TCP/IP Layers |
|---|---|---|
| Layer 7 | Application | Application Programs and Protocols for file transfer, electronic mail, etc. (Telnet, FTP,SMTP, etc.) |
| Layer 6 | Presentation | |
| Layer 5 | Session | |
| Layer 4 | Transport | Internet Protocol (IP) |
| Layer 3 | Network | |
| Layer 2 | Data Link | Network Interface Cards: Ethernet, Token-Ring, etc NIC Drivers: Open Datalink Interface (ODI), Network Independent Interface Specification (NDIS) |
| Layer 1 | Physical | Transmission Media: Twisted Pair, Coax, Fiber Optic, Wireless Media, etc. |

## Addressing without Subnets

VANGUARD Integrity Professionals Information Security Experts

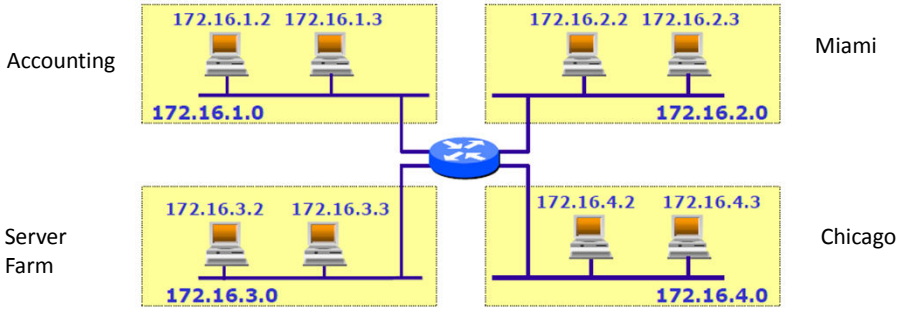



- **A class B "Flat Network", has one network and 65534 hosts (Computing Devices) available**
  - **How to manage that number of devices?**
  - **Performance?**



## Addressing with Subnets

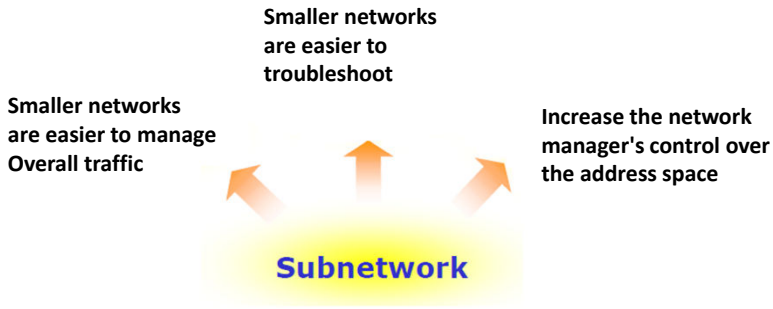
VANGUARD Integrity Professionals Information Security Experts




- **A class B ""Subdivided Network", has Smaller Manageable number of devices and can be controlled (routed, firewalled, etc. )**

## Subnetwork Benefits

VANGUARD Integrity Professionals Information Security Experts




- Subdivide on IP network number is an important initial task of network managers
- Understanding how your System Z is connected and what is connected to is important to knowing how to protect it.



## Default Subnet Masking

VANGUARD Integrity Professionals Information Security Experts

| Class A | 255.0.0.0 | 1.0.0.0 – 127.0.0.0 |
|---|---|---|

| 1111 1111 | 0000 0000 | 0000 0000 | 0000 0000 |
|---|---|---|---|

| Class B | 255.255.0.0 | 128.0.0.1 – 191.255.0.0 |
|---|---|---|

| 1111 1111 | 1111 1111 | 0000 0000 | 0000 0000 |
|---|---|---|---|

| Class C | 255.255.255.0 | 192.0.0.0- 223.255.255.0 |
|---|---|---|

| 1111 1111 | 1111 1111 | 1111 1111 | 0000 0000 |
|---|---|---|---|

## Changing the Range

VANGUARD Integrity Professionals Information Security Experts

| 172 | 16 | 0 | 0 |
|---|---|---|---|

**Default Subnet**

**255.255.0.0**

| 1111 1111 | 1111 1111 | 0000 0000 | 0000 0000 |
|---|---|---|---|

**Our Subnet**

**255.255.255.0**

| 1111 1111 | 1111 1111 | 1111 1111 | 0000 0000 |
|---|---|---|---|

**Define a subnet mask by extending the network portion to the right, 8 bits in this example**

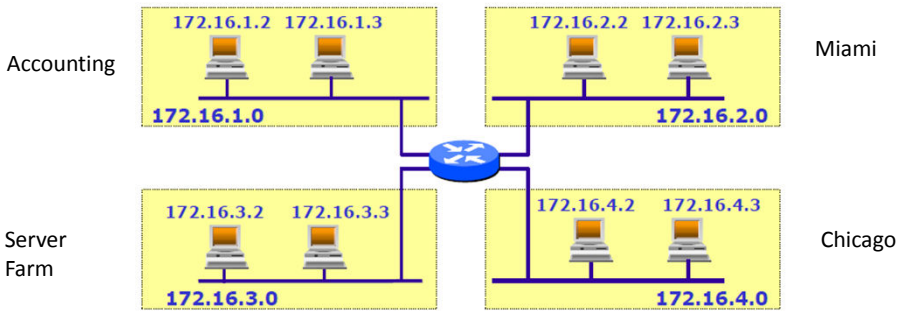
Server Proven

9

Business Partner IBM

## Our subnet

VANGUARD Integrity Professionals Information Security Experts




**Class B** **255.255.0.0** **172.16.0.0– 172.16.255.255**

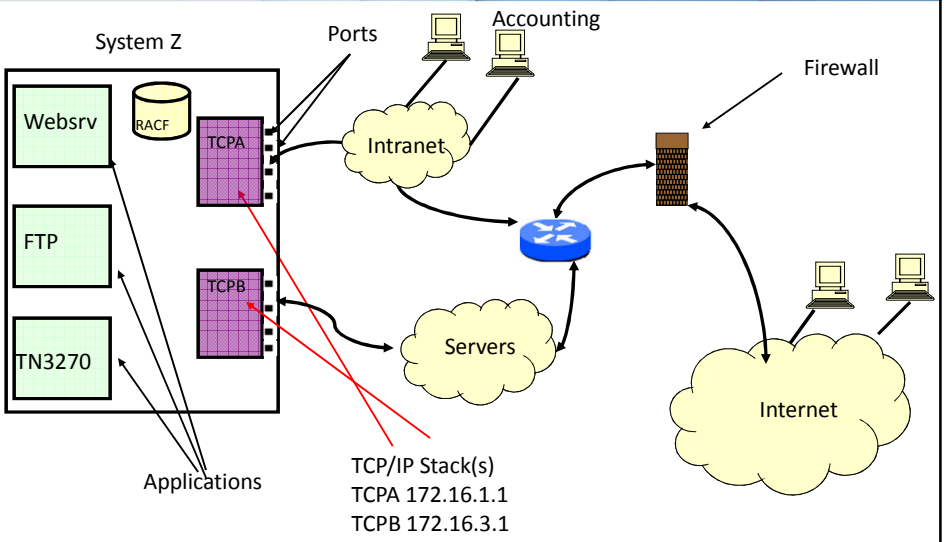
| 1111 1111 | 1111 1111 | 0000 0000 | 0000 0000 |
|---|---|---|---|

Server Proven

10

Business Partner IBM

## Simple Network Overview






## Type of Controls

- **STACK access**
- **PORT access**
- **Network access**

- **For outbound requests use above order**
- **For inbound request, reverse order**

## Controlling Stack Access

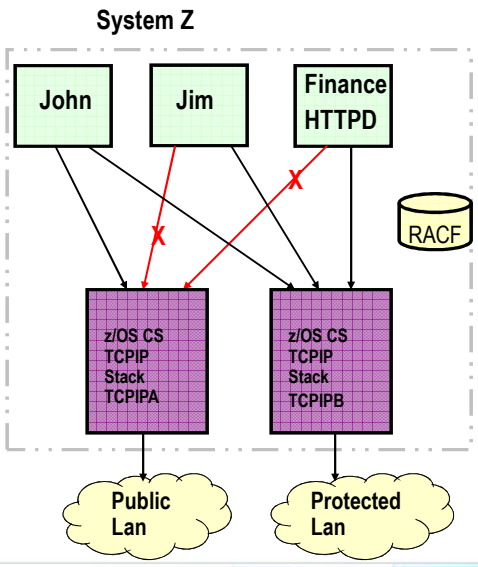
VANGUARD Integrity Professionals — Information Security Experts

- **Purpose to control who can access what from where.**
- **Applies to USERS on z/OS**
- **HOW?**
  - **Profiles in the SERVAUTH Class**



## Controlling Stack Access

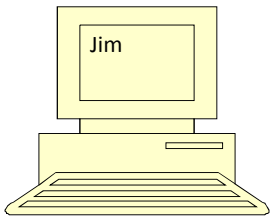
VANGUARD Integrity Professionals — Information Security Experts




### Stack access

- Define the stack resources with UACC(NONE) and permit groups or individual users to allow them to use the TCP/IP stack (open ANY socket on the stack).

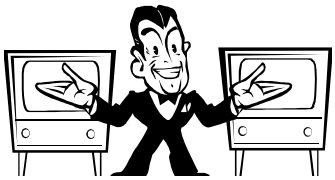
{ RACF Profiles Protecting TCP/IP Stacks
EZB.STACKACCESS.*sysname.tcpname.* }



## What are ports

VANGUARD Integrity Professionals Information Security Experts

- An easy way to understand ports is to imagine your IP address is a cable box and the ports are the different channels on that cable box.
- The cable company knows how to send cable to your cable box based upon a unique serial number associated with that box (IP address), and then you receive the individual shows on different channels (Ports).





## Controlling Port Access

VANGUARD Integrity Professionals Information Security Experts

- Purpose to control who can access what from where.
- Applies to USERS on z/OS
- HOW?
  - Profiles in the SERVAUTH Class
- Resource name format:
  - EZB.PORTACCESS.sysname.tcpname.portname

## Defining Reserved Ports

```
20 TCP * SAF FTPCTL          ; FTP SERVER
21 TCP * SAF FTPDATA         ; FTP SERVER
23 TCP * SAF TELNET          ; TELNET SERVER
25 TCP * SAF SMTP            ; SMTP SERVER
53 TCP NAMESRV               ; Domain Name Server
53 UDP NAMESRV               ; Domain Name Server
69 UDP OMVS                  ; OE TFTP SERVER
80 TCP OMVS                  ; OE WEB SERVER
81 TCP * SAF JIMWEB          ; OE WEB SERVER
```

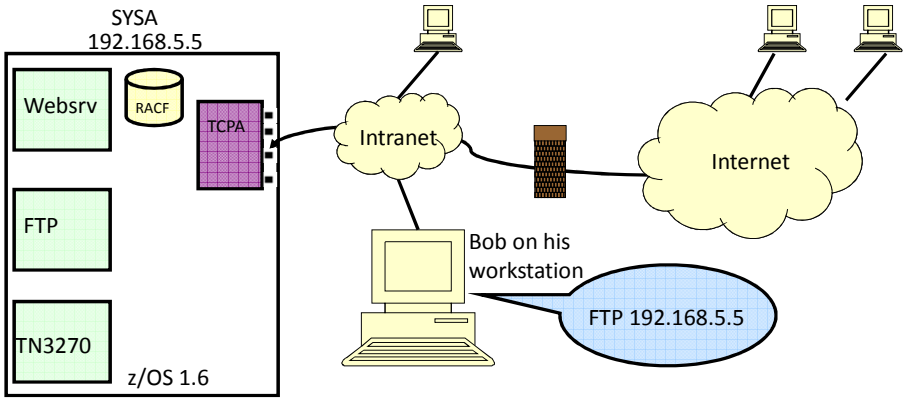
Partial listing of TCPIP PROFILE Data

**UDP=User Datagram Protocol**
**TCP=Transmission Control Protocol**

TCP ports: 0-65535 UDP ports 0-65534
Low ports 0-1024 High ports 1025 -65535

17

## Controlling port access (FTP)



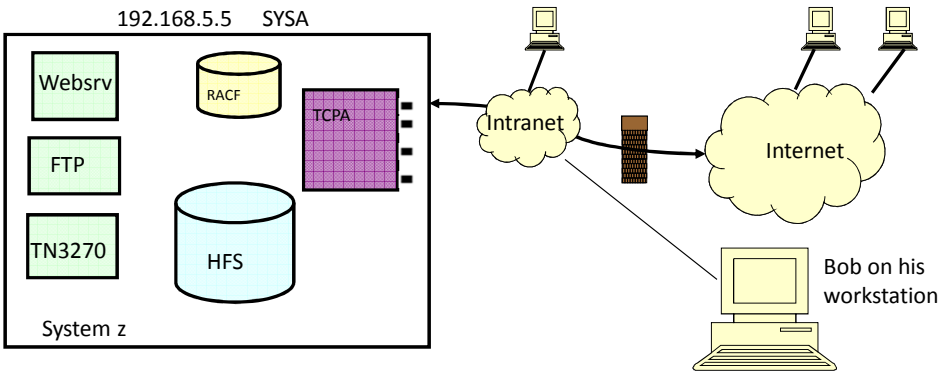

FTP calls RACF and asks:
Does BOB have READ access To
**EZB.PORTACCESS.SYSA.TCPA.FTPCTL**

***NOTE: Passive FTP bypasses PORTACCESS Because it uses dynamic PORTS***

18

## Controlling Access to HFS file System

VANGUARD Integrity Professionals — Information Security Experts




FTP calls RACF and asks:
Does BOB have READ access To
**EZB.FTP.SYSA.FTPD%.ACCESS.HFS**



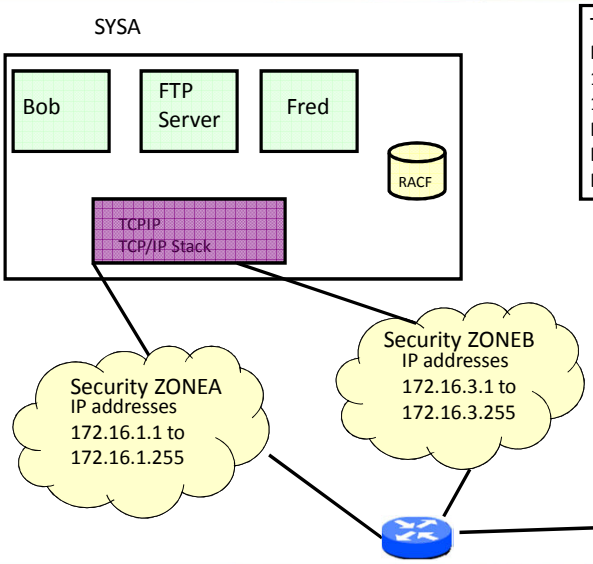
## Controlling Network Access

VANGUARD Integrity Professionals — Information Security Experts

- Purpose to control who can access what from where.
- Applies to USERS on z/OS
- HOW?
  - Profiles in the SERVAUTH Class
- Resource name format:
  - EZB.NETACCESS.sysname.tcpname.zone

## Security Zones

VANGUARD Integrity Professionals — Information Security Experts




TCP/IP PROFILE:
NETACCESS INBOUND OUTBOUND
172.16.1.0 255.255.255.0 ZONEA
172.16.3.0 255.255.255.0 ZONEB
DEFAULTHOME HOME
DEFAULT WORLD
ENDNETACCESS

Fred wants to FTP to 172.16.1.30
TCPIP calls RACF and asks:
Does FRED have READ access To
**EZB.NETACCESS.SYSA.TCPIP.ZONEA**

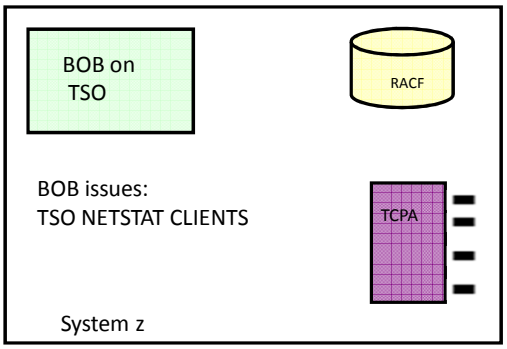
Firewall

Server Proven — 21 — Business Partner IBM

## Controlling The NETSTAT Command

VANGUARD Integrity Professionals — Information Security Experts

192.168.5.5 SYSA



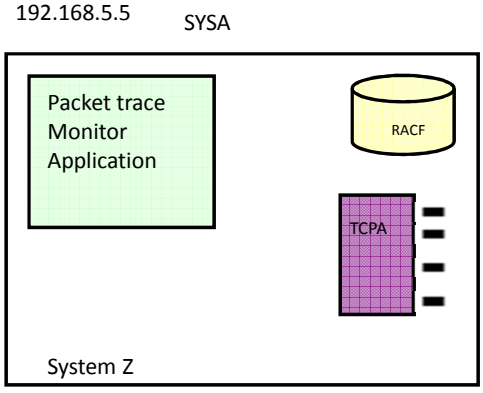

TCP/IP calls RACF and asks:
Does BOB have READ access To
**EZB.NETSTAT.SYSA.TCPA.CLIENTS**

**NETSTAT** Command for troubleshooting and gathering TCPIP information.

Server Proven — 22 — Business Partner IBM

## Controlling TCP/IP Packet Trace

VANGUARD Integrity Professionals — Information Security Experts




Bob is running the packet trace monitor application.
TCP/IP calls RACF and asks:
Does BOB have READ access To

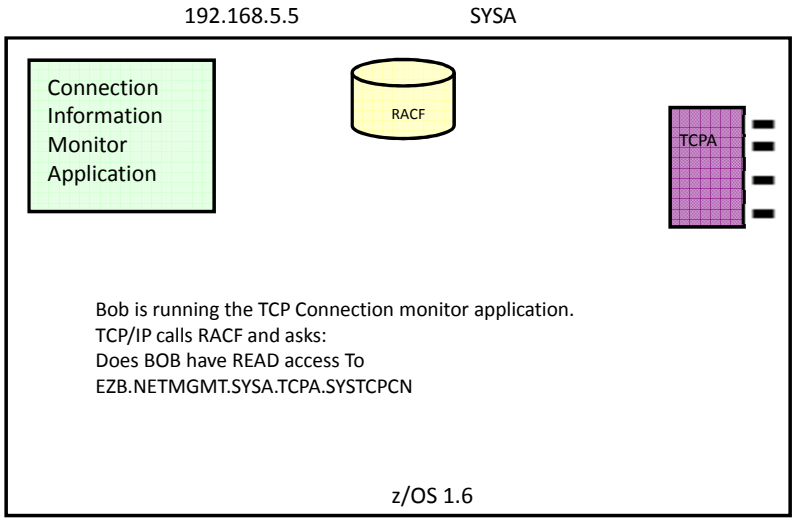
**EZB.NETMGMT.SYSA.TCPA.SYSTCPDA**

**Note: this can be applied system wide or stack wide.**



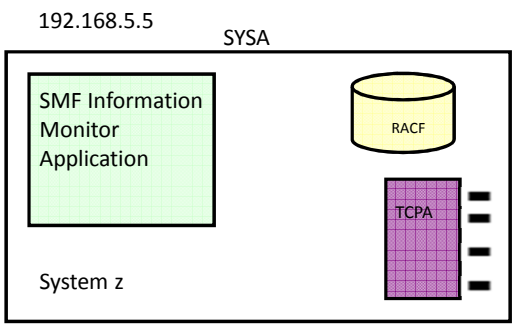
## Controlling TCP Connection Information

VANGUARD Integrity Professionals — Information Security Experts




Bob is running the TCP Connection monitor application.
TCP/IP calls RACF and asks:
Does BOB have READ access To
EZB.NETMGMT.SYSA.TCPA.SYSTCPCN

# Controlling Real-Time SMF Information




Bob is running the SMF Information monitor application.
TCP/IP calls RACF and asks:
Does BOB have READ access To
**EZB.NETMGMT.SYSA.TCPA.SYSTCPSM**

25

# SERVAUTH Profiles

| Function | Description | SERVAUTH profile |
|---|---|---|
| TN3270 server access control | Controls ability to access TN3270 server based on SAF user ID associated with TLS-authenticated X.509 client certificate | EZB.TN3270.sysname.tcpname.PORTxxxxx |
| FTP server access control | Controls ability to access FTP server based on SAF user ID associated with TLS-authenticated X.509 client certificate | EZB.FTP.sysname.ftpdaemonname.PORTxxxxx |
| DCAS server access control | Controls ability to access DCAS server based on SAF user ID associated with TLS-authenticated X.509 client certificate | EZB.DCAS.cvtsysname |
| TCP stack access control | Controls user ability to open a socket and get host name or host ID | EZB.STACKACCESS.sysname.tcpname |
| TCP local port access control | Controls user ability to bind to a non-ephemeral TCP or UDP port | EZB.PORTACCESS.sysname.tcpname.port_safname |
| TCP netaccess access control | Controls local user inbound and outbound access to network resources, and local user access to local IP address when explicitly binding to local interface (or using job-specific source IP addresses) | EZB.NETACCESS.sysname.tcpname.security_zonename |
| Netstat command access control | Provides ability to restrict Netstat usage | EZB.NETSTAT.sysname.tcpname.netstat_option |
| Policy Agent command control | Provides ability to restrict pasearch command usage by policy type | EZB.PAGENT.sysname.tcpname.policy_type |
| FTP SITE command control | Provides ability to restrict usage of SITE DUMP and DEBUG commands (commands generate large amount of output) | EZB.FTP.sysname.ftpdname.SITE.DUMP<br>EZB.FTP.sysname.ftpdname.SITE.DEBUG |
| SNMP agent control | Provides ability to control usage of SNMP subagents that connect to the TCP/IP SNMP agent | EZB.SNMPAGENT.sysname.tcpname |
| MODDVIPA utility program control | Provides ability to restrict usage of MODDVIPA utility program (creates new DVIPA on system) | EZB.MODDVIPA.sysname.tcpname |
| Fast Response Cache Accelerator (FRCA) Access Control | Provides ability of user to create FRCA cache (FRCA used by Web servers for caching static Web pages in the stack) | EZB.FRCAACCESS.sysname.tcpname |
| TCP connection information service access control | Provides ability to restrict access to the TCP connection information using TCP connection information service; intended for network management applications | EZB.NETMGMT.sysname.tcpname.SYSTCPCN |

26

# SERVAUTH Profiles

VANGUARD Integrity Professionals — Information Security Experts

| Function | Description | SERVAUTH profile |
|---|---|---|
| Real-time SMF information service access control | Provides ability to restrict access to select real-time SMF records accessible using the SMF information service; intended for network management applications | EZB.NETMGMT.sysname.tcpname.SYSTCPSM |
| TCP/IP packet trace service access control | Provides ability to restrict access to select real-time packet trace records accessible using the TCP/IP packet trace service; intended for network management applications | EZB.NETMGMT.sysname.tcpname.SYSTCPDA |
| FTP HFS access control | Provides ability to generally restrict FTP user access to HFS | EZB.FTP.sysname.ftpdaemonname.ACCESS.HFS |
| Broadcast access control | Provides ability to control whether an application is permitted to set the SO_BROADCAST socket option needed to send broadcast datagrams | EZB.SOCKOPT.sysname.tcpname.SO_BROADCAST |
| IPv6 Advanced Socket API access control | Provides ability to control whether an application is permitted to set IPv6 advanced socket API options:<br>IPv6_NEXTHOP IPv6_TCLASS<br>IPv6_RTHDR IPV6_HOPOPTS<br>IPV6_DSPOPTS IPV6_RTHDRDSTOPT<br>IPV6_PKTINFO IPV6_HOPLIMIT | EZB.SOCKOPT.sysname.tcpname.IPV6_NEXTHOP<br>EZB.SOCKOPT.sysname.tcpname.IPV6_TCLASS<br>EZB.SOCKOPT.sysname.tcpname.IPV6_RTHDR<br>EZB.SOCKOPT.sysname.tcpname.IPV6_HOPOPTS<br>EZB.SOCKOPT.sysname.tcpname.IPV6_DSTOPTS<br>EZB.SOCKOPT.sysname.tcpname.IPV6_RTHDRDSTOPTS<br>EZB.SOCKOPT.sysname.tcpname.IPV6_PKTINFO<br>EZB.SOCKOPT.sysname.tcpname.IPV6_HOPLIMIT |
| TCP/IP stack initialization access control | Controls ability of applications to open a socket before AT-TLS policy is loaded into the TCP/IP stack | EZB.INITSTACK.sysname.tcpname |
| CIM provider access control | Provides ability to restrict access to CIM data | EZB.CIMPROV.sysname.tcpname |
| ipsec command access control | Provides ability to control ipsec command usage | EZB.IPSECCMD.sysname.tcpname.command_rule |

IBM Server Proven — 27 — IBM Business Partner

# Reference Manuals

VANGUARD Integrity Professionals — Information Security Experts

| | |
|---|---|
| z/OS V1R1.13 CS: IP CONFIGURATION GUIDE | SC31-8775-5 |
| z/OS V1R1.13 CS: IP CONFIGURATION REFERENCE | SC31-8776-6 |

IBM Server Proven — 28 — IBM Business Partner