

IBM Education Assistance for z/OS V2R2

Element/Component: Communications Server



Agenda

- Trademarks
- Presentation Objectives
- For each function
 - Overview
 - Usage & Invocation
 - Interactions & Dependencies
 - Migration & Coexistence Considerations
 - Installation
- Presentation Summary
- Appendix



Trademarks

- See url <http://www.ibm.com/legal/copytrade.shtml> for a list of trademarks.



Presentation Objectives

- Provide a high-level overview of the Communications Server functions in z/OS V2R2
 - Remove GATEWAY statement from TCP/IP profile
 - Disable legacy DLC configuration
 - Sendmail security update
 - Policy Agent security update
 - SNMP security update
 - DCAS AT-TLS enhancements
 - Increase single stack DVIPA limit to 4096
 - VIPAROUTE fragmentation avoidance
 - Enhanced Enterprise Extender scalability
 - 64 bit enablement of the TCP/IP stack
 - Enhanced IKED scalability

■



Presentation Objectives continued

- Simplified access permissions to ICSF cryptographic functions for IPSec
- AT-TLS currency with System SSL features
- TLS session reuse support for FTP and AT-TLS applications
- TCP autonomic tuning enhancements
- Shared Memory Communications over RDMA enhancements
- Shared Memory Communications over RDMA adapter (RoCE) virtualization
- Reordering of cached Resolver results
- Activate Resolver trace without restarting applications
- CICS transaction tracking support for CICS TCP/IP IBM Listener
- Configuration Assistant – TCP/IP Profile Configuration

■



Remove GATEWAY statement from TCP/IP profile



Overview

- Problem Statement / Need Addressed
 - Two methods of configuring static routes
 - GATEWAY
 - BEGINROUTES
 - GATEWAY statement syntax is confusing
 - GATEWAY statement does not support IPV6
- Solution
 - Remove support for the GATEWAY profile statement
- Benefit / Value
 - Single method of configuring static routes
 - BEGINROUTES statement is easier to configure
 - BEGINROUTES provides full support for IPV6

▪



Usage & Invocation

- Support for the GATEWAY profile statement has been removed.
- Static route definitions must be defined using the BEGINROUTES statement
-



Migration & Coexistence Considerations

- Convert existing static route definitions using GATEWAY profile statement to BEGINROUTES statement
 - TCPIP PROFILE command formats static route definitions in the BEGINROUTES format

■



Disable legacy DLC configuration



Overview

- Problem Statement / Need Addressed
 - Legacy devices present testing problems
 - Physical devices not present in test environment
 - Some devices not supported without channel emulation
- Solution
 - Remove support for selected legacy devices
 - Associated address spaces are also removed
- Benefit / Value
 - Simplified configuration
 - Modern devices provide
 - Improved throughput
 - Lower CPU utilization

▪



Usage & Invocation

- Support for the following devices defined with DEVICE and LINK profile statements have been removed
 - Asynchronous Transfer Mode (ATM)
 - Channel Data Link Control (CDLC)
 - Common Link Access To Workstation (CLAW)
 - HYPERChannel
 - SNALINK (both LU0 and LU6.2)
 - X.25
- Support for address spaces associated with these devices has been removed
- Ancillary profile statements supporting these devices has been removed
-



Migration & Coexistence Considerations

- Remove any TCP/IP profile configuration statement supporting removed devices
- Do not start server applications supporting removed devices
-



Sendmail security update



Overview

- Problem Statement / Need Addressed
 - NIST mandate SP800-131a states that by the end of 2013, U.S. Government systems support TLSv1.2, SHA-2 hashes encryption key strengths of 112 bits or more
 - Sendmail client and server do not meet this NIST requirement
- Solution
 - Enhance Sendmail client and server to support TLSv1.1 and TLSv1.2 with a new set of ciphers
- Benefit / Value
 - Sendmail client and server conform to this NIST requirement
 -
 -



Usage & Invocation

- Update configuration of z/OS UNIX sendmail in z/OS specific file
 - CipherLevel
 - Specifies the list of TLSv1.0, TLSv1.1, or TLSv1.2 ciphers in the order of preference
 - Example
 - CipherLevel 6B50040A0306090201
- Default configuration file /etc/mail/zOS.cf
- Some TLSv1.2 ciphers require z/OS Integrated Cryptographic Services Facility
-
-



Interactions & Dependencies

- z/OS Integrated Cryptographic Services Facility (ICSF) may be required



Policy Agent security update



Overview

- Problem Statement / Need Addressed
 - NIST mandate SP800-131a states that by the end of 2013, U.S. Government systems support TLSv1.2, SHA-2 hashes encryption key strengths of 112 bits or more
 - Centralized Policy Agent policy client does not meet this NIST requirement
- Solution
 - Enhance policy client to support TLSv1.1 and TLSv1.2 with a new set of ciphers
- Benefit / Value
 - Policy Agent conforms to this NIST requirement
 -

▪



Usage & Invocation

- Centralized Policy Agent client function uses System SSL to secure connection to Centralized Policy Agent server
- Update Policy Agent main configuration file
 - ServerConnection ServerSSLV3CipherSuites
 - Specifies the list of TLSv1.0, TLSv1.1, or TLSv1.2 ciphers in the order of preference
 - Example

```
ServerConnection
  ServerSSLV3CipherSuites 6B50040A0306090201
```
- Centralized Policy Agent server requires matching AT-TLS policy
- Some TLSv1.2 ciphers require z/OS Integrated Cryptographic Services Facility

▪

▪



Interactions & Dependencies

- z/OS Integrated Cryptographic Services Facility (ICSF) may be required



SNMP security update



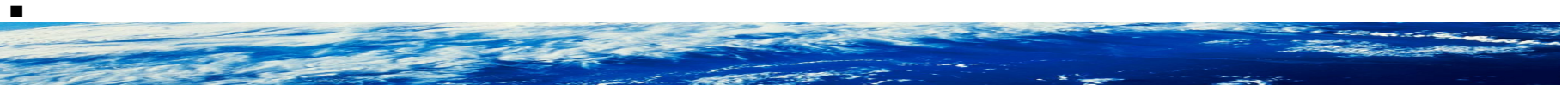
Overview

- Problem Statement / Need Addressed

- NIST mandate SP800-131a states that by the end of 2013, U.S. Government systems support TLSv1.2, SHA-2 hashes encryption key strengths of 112 bits or more
- Simple Network Management Protocol (SNMP) Agent, the z/OS UNIX snmp command, and the SNMP manager API functions do not meet this NIST requirement

- Solution

- Enhance the SNMP Agent, the z/OS UNIX snmp command, and the SNMP manager API to support the Advanced Encryption Standard (AES) 128-bit cipher algorithm as an SNMPv3 privacy protocol for encryption
 - The AES SNMP implementation is described in RFC 3826
 - SNMP uses AES encryption in Cipher FeedBack Mode (CFB)



Overview continued

- Benefit / Value
 - SNMP functions conform to this NIST requirement

-



Usage & Invocation

- SNMP Agent

- Update snmpd.conf
- Configure an SNMPv3 user to use AES 128-bit encryption by specifying a USM_USER entry with the privProto field set to AESCFB128

- Example

USM_USER u7 engineId HMAC-MD5

5fbd3ad2fa6569d6c1e9ab4b83728b87 AESCFB128

bf686267600ff8f4b1354b857d186b55 L nonVolatile



Usage & Invocation continued

- z/OS UNIX snmp command
 - Update osnmp.conf
 - Configure an SNMPv3 user to use AES 128-bit encryption by specifying a configuration statement with the privProto field set to AESCFB128
 - Example:
v3mpka 127.0.0.1 snmpv3 u7 u7password context AuthPriv
HMACMD5 15549009e2401748e8077fa17bf64c9b AESCFB128
90009683501c78a6f87575bdad5455bc
 -



Usage & Invocation continued

- SNMP manager API

- Update the SNMP manager API configuration file
- Configure an SNMPv3 user to use AES 128-bit encryption by specifying a configuration statement with the privProto field set to AESCFB128

- Example

```
127.0.0.1 161 snmpv3 u7 u7password AuthPriv HMAC-MD5  
15549009e2401748e8077fa17bf64c9b AESCFB128  
90009683501c78a6f87575bdad5455bc  
000000020000000000943714F
```



Interactions & Dependencies

- z/OS Integrated Cryptographic Services Facility (ICSF) is required for Advanced Encryption Standard (AES) 128-bit cipher



DCAS AT-TLS enhancements



Overview

- Problem Statement / Need Addressed
 - NIST mandate SP800-131a states that by the end of 2013, U.S. Government systems support TLSv1.2, SHA-2 hashes encryption key strengths of 112 bits or more
 - Digital Certificate Access Server (DCAS) does not meet this NIST requirement
- Solution
 - Enhance DCAS to be an AT-TLS aware server application
- Benefit / Value
 - DCAS conforms to this NIST requirement
-



Usage & Invocation

- New keyword TLSMECHANISM to specify whether to use AT-TLS policies or IBM System SSL directly
 - DCAS (default)
 - IBM System SSL is used directly for TLS/SSL
 - No changes are required to client connection
 - Does not meet this NIST requirement
 - ATTLS
 - AT-TLS policies are used for TLS/SSL
 - Client connection TLS/SSL must be updated to match configured AT-TLS policies

▪

▪



Interactions & Dependencies

- z/OS Integrated Cryptographic Services Facility (ICSF) may be required



Increase single stack DVIPA limit to 4096



Overview

- Problem Statement / Need Addressed
 - Horizontal workload growth is increasing the demand for application instance dynamic virtual IP addresses
 - Existing limit of 1024 application instance dynamic virtual IP addresses is an inhibitor to workload consolidation
- Solution
 - Application instance dynamic virtual IP addresses limit increased to 4096
 - Dynamic virtual IP addresses defined with VIPADEFINE and VIPABACKUP limit remains unchanged at 1024
 -
- Benefit / Value
 - Increased application workload consolidation
-



Usage & Invocation

- Dynamic virtual IP address creation
 - VIPADEFINE and VIPABACKUP configuration statements
 - VIPARANGE to define a range of IP addresses
 - Application binds to an IP address
 - Application issues an SIOCVIPA ioctl()
- Configuration defined dynamic virtual IP addresses
 - Created with profile statements
 - Associated with multiple applications
- Application instance dynamic virtual IP addresses
 - Dynamically created with bind() or ioctl()
 - Associated with a particular application

▪



Migration & Coexistence Considerations

- Coexistence in the same sysplex with pre V2R2 TCPIP limit of 1024 dynamic virtual IP addresses may limit the backup options
 - Providing VIPABACKUP definitions on down level systems may not be possible
 -
-



VIPAROUTE fragmentation avoidance



Overview

- Problem Statement / Need Addressed
 - VIPARROUTE is used by Sysplex Distributor to forward packets
 - Generic Routing Encapsulation routes packet to alternate address
 - Encapsulation increases the size of the packet
 - Larger packet may require fragmentation
 - Path MTU discovery does not always work
 - Path MTU discovery configured on every host
 - Routers block Internet Control Message Protocol packets
- Solution
 - Reduce TCP maximum segment size
 - Configurable global TCPIP option
- Benefit / Value
 - Avoid fragmentation due to Generic Routing Encapsulation by Sysplex Distributor



Usage & Invocation

- New TCPIP configuration parameter on the GLOBALCONFIG profile statement
 - ADJUSTDVIPAMSS
 - AUTO (default)
 - ALL
 - NONE
- Controls the adjustment of the maximum segment size
- Configured on the target TCPIP
- Example:
GLOBALCONFIG ADJUSTDVIPAMSS AUTO



Usage & Invocation continued

- AUTO

- Inbound connections
 - Local stack is a target and VIPAROUTE is being used
 - Local stack is a distributor and a target and VIPAROUTE is defined
- Outbound connections
 - Source IP address is a distributed dynamic virtual IP address

- ALL

- Inbound and outbound connections
 - Source IP address is a dynamic virtual IP address

- NONE

- Disable maximum segment size adjustment



Migration & Coexistence Considerations

- Disable maximum segment size adjustment to retain pre V2R2 behavior
- Example:
GLOBALCONFIG ADJUSTDVIPAMSS NONE

▪



Enhanced Enterprise Extender scalability



Overview

- Problem Statement / Need Addressed
 - Enterprise Extender (EE) traffic is serialized at the port level
 - Outbound traffic is serialized using the UCB lock
 - Inbound traffic is serialized using the EE policy lock
 - Large number of EE partners can cause queueing of traffic
 - Routes to all EE partners maintained in IPMAIN based route cache
- Solution
 - Create a remote UCB structure per port for each active EE partner
 - Serialization moved to remote UCB
 - EE partner route moved to remote UCB
- Benefit / Value
 - Serialization is reduced to a port and EE partner basis
 - Reduced overhead for maintaining IPMAIN based route cache

▪



64 bit enablement of the TCP/IP stack



Overview

- Problem Statement / Need Addressed
 - Workload growth limited by storage utilization
 - ECSA storage constrained
 - TCPIP private storage constrained
 - Performance penalty for AMODE switching
 - Performance penalty for accessing network data in CSM dataspace
- Solution
 - Move high usage control structures from ECSA to HVCOMMON
 - Move high usage TCPIP control blocks from private to HVPRIVATE
 - Enable the TCP/IP stack to run in AMODE 64
 - Enable 64 bit CSM HVCOMMON storage
 - Convert data buffers for OSA Express and Hypersocket DLCs from CSM dataspace to CSM HVCOMMON

▪



Overview continued

- Benefit / Value
 - Reduced ECSA usage
 - Reduced TCPIP private below the bar usage
 - Performance benefits of avoiding AMODE switching
 - Performance benefits of avoiding CSM dataspace access
 -
-



Usage & Invocation

- Define CSM HVCOMMON storage limit in IVTPRM00 member of SYS1.PARMLIB

- Sample IVTPRM00

- FIXED MAX(240M)

- ECSA MAX(120M)

- HVCOMM MAX(2000M)

- Default HVCOMM MAX value is 1000M
 - Modify proc,CSM supports new HVCOMM parameter
 - Example

- F VTAM,CSM,ECSA=120M,FIXED=240M,HVCOMM=2000M



Migration & Coexistence Considerations

- Display NET,CSM output includes new HVCOMM information
 - Sample output

D NET,CSM

IVT5530I BUFFER BUFFER

IVT5531I SIZE SOURCE INUSE FREE

TOTAL

...

IVT5532I

IVT5533I 4K HVCOMM 24K 1000K

1M

IVT5533I 16K HVCOMM 96K 928K

1M

IVT5533I 32K HVCOMM 192K 832K

1M

IVT5533I 60K HVCOMM 360K 660K

1020K

IVT5533I 180K HVCOMM 720K 1080K

1800K

IVT5535I TOTAL HVCOMM 1392K 4500K

5892K

IVT5532I

Migration & Coexistence Considerations continued

- Changed VIT entry
 - ODPK (inbound/outbound QDIO)
- New VIT entries
 - IUT6 (outbound QDIO)
 - XB61 (inbound/outbound QDIO)
 - XB62 (inbound/outbound QDIO)
 - XB63 (inbound/outbound QDIO)
 - QAP6 (QDIO accelerator)
 - GCE6 (64 bit CSM)



Migration & Coexistence Considerations continued

- Use the Inbound Workload Queueing function for OSA-Express QDIO to optimize Enterprise Extender network flows
 - Enterprise Extender does not fully exploit 64 bit storage
 - Inbound Workload Queueing allows OSA to stage inbound Enterprise Extender data into 31 bit storage
 - Sample interface statement

```
INTERFACE OSAQDIO24 DEFINE IPAQENET
          PORTNAME OSAQDIO2
          SOURCEVIP AINT VIPAV4
          IPADDR 100.1.1.1/24
          INBPERF DYNAMIC WORKLOADQ
```



Installation

- Update IVTPRM00

-



Enhanced IKED scalability



Overview

- Problem Statement / Need Addressed
 - Internet Key Exchange Daemon (IKED) dynamically negotiates IPSec Security Associations (SAs) between two hosts.
 - The negotiation process requires several network flows and CPU intensive processing.
 - Most IKED processing occurs in a single threaded model
 - Large number of concurrent negotiations overwhelm IKED
- Solution
 - Message prioritization and pruning
 - Use a multi-threading model where possible
- Benefit / Value
 - IKED is able to perform large numbers of concurrent negotiations without significant delays

▪



Usage & Invocation

- No action is required to enable the scalability enhancements
- Those with multiple thousands of IKE peers might need to adjust specific resources
 - Virtual storage available to IKED
 - Maximum number of messages allowed on z/OS message queues
 - Limitations on number of messages allowed on inbound UDP queues
- IKED messages written to syslogd now contain a thread id
- -
-



Migration & Coexistence Considerations

- Automated processing of IKED messages

-



Simplified access permissions to ICSF cryptographic functions for IPSec



Overview

- Problem Statement / Need Addressed
 - TCP/IP stack's IPSec support uses ICSF callable services
 - ICSF callable services can be SAF protected
 - CHECKAUTH=YES
 - Access required for TCPIP and application user ids
- Solution
 - Exploit new CSFACEE function
 - IPSec processing uses TCPIP user id for all ICSF services
- Benefit / Value
 - Access to ICSF services only required for TCPIP user id
 - Simplified access management

▪



Usage & Invocation

- No action for existing IPSec implementation with ICSF protected services
- New IPSec implementations with protected ICSF services access permissions limited to TCPIP user id



Migration & Coexistence Considerations

- Consider removing SAF access granted to application user ids for the purpose of IPSec

-



AT-TLS currency with System SSL features



Overview

- Problem Statement / Need Addressed
 - AT-TLS does not support RFC5280 certificate validation
 - Certificate revocation list (CRL) support limited to Lightweight Directory Access Protocol (LDAP)
 - Entire cache flushed on cache timeout
- Solution
 - AT-TLS is enhanced to support RFC5280 certificate validation
 - Enhanced CRL support
 - Online Certificate Status Protocol (OCSP)
 - HTTP retrieval of CRLs
 - LDAP with cache management enhancements
- Benefit / Value
 - System SSL support for RFC5280 certificate validation exploited
 - Enhanced certificate revocation exploited



Usage & Invocation

- RFC5280
 - TTLSEnvironmentAdvancedParms
- LDAP enhancements
 - TTLSGskLdapParms
- OCSP and HTTP support
 - TTLSGskAdvancedParms
-



TLS session reuse support for FTP and AT-TLS applications



Overview

- Problem Statement / Need Addressed
 - z/OS FTP does not support TLS session reuse on different ports
 - RFC 4217 (Securing FTP with TLS) refers to TLS session reuse to validate the data connection
 - Prior to V2R2 System SSL did not support session reuse on different ports
- Solution
 - System SSL support for session reuse on different ports
 - AT-TLS support for TLS session reuse
 - Enhance SIOCTTLSCTL ioctl interface
 - FTP client and server secure session reuse for SSL and AT-TLS
- Benefit / Value
 - FTP secure session reuse provides an enhanced level of security for the data connection



Usage & Invocation

- AT-TLS exploitation using SIOCTTLSCTL
 - GET TTLSK_GetSessionToken
 - GET TTLSK_GetSessionId
 - SET TTLSK_SetSessionToken
- FTP server
 - Configure SECURE_SESSION_REUSE in FTP.DATA file
 - ALLOWED to allow session reuse
 - REQUIRED to require session reuse
- FTP client
 - Configure SECURE_SESSION_REUSE in FTP.DATA file
 - NONE to prevent session reuse
 - ALLOWED to allow session reuse
 - REQUIRED to require session reuse



Migration & Coexistence Considerations

- FTP client user exit EZAFCCMD
- SMF type 119 records
 - Subtype 2, 3, 70, 71, 72
 - Subtype 100, 101, 102, 103, 104
- Netstat TTLS / -x
 -



TCP autonomic tuning enhancements



Overview

- Problem Statement / Need Addressed
 - Dynamic Right Sizing (DRS) disables if receiving application is not able to read data fast enough
 - Current storage conditions are not taken into account
 - Never re-enables
 - Outbound Right Sizing (ORS)
 - Send buffer size grows without regard for send window
- Solution
 - DRS
 - Can be re-enabled on a connection
 - Takes into account the CSM storage status
 - ORS
 - Takes into account the CSM storage status
 - Send buffer grows and shrinks as needed



Overview continued

- Benefit / Value
 - DRS does not unnecessarily disable
 - DRS is capable of re-enabling
 - ORS efficiently manages the send buffer size

▪



Overview continued

- Problem Statement / Need Addressed
 - Fast Recovery and Retransmit (FRR) impairs the connections ability to grow the congestion window
 - Out of order packets can trigger FRR
 - FRR ambiguity attempts to detect out of order packets
 - Increases FRR threshold
 - Requires timestamps to be present
- Solution
 - Detect out of order packets using timestamps or internal timing
 - Restore connection status to pre-FRR status if no packets are lost
- Benefit / Value
 - FRR uses a consistent threshold
 - Connection throughput is minimally effected by out of order packets

▪



Overview continued

- Problem Statement / Need Addressed
 - Delayed Acknowledgement (ACK) can impair certain workloads
 - Can be disabled by configuration
 - Difficult to identify impaired workloads
- Solution
 - Autonomic management of delayed ACK
 - Monitors effectiveness of delayed ACK
 - Enables or disables for optimal results
- Benefit / Value
 - Optimizes performance without managing configuration
-



Usage & Invocation

- DRS requires an initial receive buffer size of 64K or larger
- ORS requires an initial send buffer size of 64K or larger
- Delayed ACK autonomics must be enabled on TCPCONFIG profile statement

- AUTODELAYACKS

- Example

- ```
TCPCONFIG AUTODELAYACKS
```

- 

- 





## Migration & Coexistence Considerations

- Netstat ALL / -a modified
- Netstat CONFIG / -f modified
- SMF 119 subtype 4

–



# Shared Memory Communications over RDMA enhancements



## Overview

- V2R2 provides three enhancements to Shared Memory Communications over RDMA (SMC-R)
  - Problem Statement / Need Addressed
    - SMC-R supports a Maximum Transmission Unit (MTU) of 1K and 2K
    - RDMA over Converged Ethernet (RoCE) feature supports 1K ,2K, and 4K
    - Large data transfers over SMC-R using smaller MTUs require more data flows which reduce network performance
  - Solution
    - Add configuration option to enable 4K MTU on RoCE feature
  - Benefit / Value
    - Large data transfers using 4K MTU on RoCE feature can provide improved network performance



## Overview continued

- Problem Statement / Need Addressed
  - SMC-R eligible TCP connections may not be able to use SMC-R
    - IPSec
    - Mismatching subnets (two peers not in same subnet or vlan)
    - Link layer issues prevent connectivity over RoCE fabric
  - Attempts to use SMC-R that fail fall back to TCP or reset the connection
- Solution
  - Cache SMC-R failures on a peer IP address basis
  - Avoid using SMC-R for a peer when cache threshold reached
- Benefit / Value
  - SMC-R eligible TCP connections avoid the overhead of attempting to use SMC-R



## Overview continued

- Problem Statement / Need Addressed
  - SMC-R eligible TCP connections may not benefit from SMC-R
    - Short lived connections transferring small amounts of data
- Solution
  - Monitor incoming connections on a SMC-R eligible server basis
  - Analyze the monitoring results on an interval basis
  - Avoid using SMC-R for a server when connection behavior pattern deemed not well suited
- Benefit / Value
  - Connections to a local SMC-R eligible server use the most appropriate protocol, TCP or SMC-R



## Usage & Invocation

- Requires SMC-R base configuration
- 4K MTU
  - Configure 4096 on GLOBALCONFIG SMCR MTU profile statement
- SMC-R peer caching
  - Configure AUTOCACHE on the GLOBALCONFIG SMCGLOBAL profile statement
- SMC-R server suitability monitoring
  - Configure AUTOSMC on the GLOBALCONFIG SMCGLOBAL profile statement

- Example

```
GLOBALCONFIG SMCR PFID 01 MTU 4096
 SMCGLOBAL AUTOCACHE AUTOSMC
```

- 



## Migration & Coexistence Considerations

- Configure NOAUTOCACHE to prevent peer caching
- Configure NOAUTOSMC to prevent server suitability monitoring
- Netstat output contains new fields

- **Netstat CONFIG / -f**

SMCGLOBAL:

AUTOCACHE: YES AUTOSMC: YES

- **Netstat ALL / -a**

SMC INFORMATION:

SMCRCURRCONNS: 0000000025  
0000000100

SMCRTOTALCONNS:

UseSMC: Yes

Source: AutoSMC

AutoSMC%: 090

- **Netstat PORTLIST / -o**

| Port# | Prot  | User    | Flags | Range       | SAF Name |
|-------|-------|---------|-------|-------------|----------|
| ----- | ----- | -----   | ----- | -----       | -----    |
| 04020 | TCP   | DCICSTS | DAN   |             |          |
| 05000 | TCP   | *       | DARN  | 05000-05001 |          |



# Shared Memory Communications over RDMA adapter (RoCE) virtualization





## Overview

- Problem Statement / Need Addressed
  - No sharing of RoCE Express feature across LPARs
  - Single LPAR sharing supported
    - Up to eight TCP/IP stacks
  - Limit of 16 RoCE Express features per Central Processor Complex (CPC)
    - Redundant configuration reduces LPARs that can access RoCE Express features
    - Limited to using a single port
- Solution
  - Share RoCE Express feature across LPARs
  - Up to 31 operating system instances can share one feature
  - Both RoCE Express ports can be used simultaneously



## Overview continued

- Solution continued
  - z/OS V2R2 supports both dedicated and shared RoCE environments
    - Shared mode
      - IBM z13
    - Dedicated mode
      - IBM zEnterprise EC12 (zEC12) with driver 15
      - IBM zEnterprise BC12 (zBC12)
  - z/OS V2R1 supports both environments with APARs OA44576 and PI12223 installed
- Benefit / Value
  - Sharing across LPARs and dual port usage increases basic redundant access from 8 to 248

▪



## Usage & Invocation

- Sharing is determined automatically based on the CPC
- Sharing requires a Virtual Function (VF) to be defined for each access path
- Example

Command ==> \_\_\_\_\_ Scroll ==> CSR

Select one or more PCIe functions, then press Enter. To add, use F11.

|                            |       |     |       |             |
|----------------------------|-------|-----|-------|-------------|
| Processor ID . . . . : S88 |       |     |       | z13 S88     |
| / FID                      | PCHID | VF+ | Type+ | Description |
| _ 028                      | 108   | 28  | ROCE  | S3E         |
| _ 029                      | 108   | 29  | ROCE  | S3E         |
| _ 030                      | 108   | 30  | ROCE  | S3E         |
| _ 031                      | 108   | 31  | ROCE  | S3E         |



## Interactions & Dependencies

- 10Gbe RoCE Express feature
- z13 for SR-IOV support



## Migration & Coexistence Considerations

- Dedicated mode uses one feature access path per LPAR
- Shared mode uses one VF per feature access path
  - Each TCPIP instance on an LPAR must have a unique VF
  - GLOBALCONFIG PFID value in TCPIP profile identifies the VF
- Netstat DEvlinks/-d report
- 



## Installation

- z13 requires VF defined for each access path in HCD
- 



# Reordering of cached Resolver results



## Overview

- Problem Statement / Need Addressed
  - Resolver cache results remain static for the viable life time of a cached result
  - Domain Name System (DNS) round robin result sets not effective
- Solution
  - System Resolver is enhanced to support returning cache results in round robin fashion.
- Benefit / Value
  - Resolver caching performance benefits can be achieved when DSN round robin results are desired for simple load balancing
  -
- 





## Usage & Invocation

- New Resolver setup statements
  - CACHEREORDER to activate cache reordering
  - NOCACHEREORDER to stop cache reordering
    - Default value
- Reordering can be dynamically modified
  - Update Resolver setup
  - Modify Resolver
    - Example  
MODIFY <resolver>,REFRESH,SETUP=<setup file name>
- New TCPIP.DATA statement
  - NOCACHEREORDER to stop cache reordering
- Reordering effects Hostname to IP address lookup results



# Activate Resolver trace without restarting applications



## Overview

- Problem Statement / Need Addressed
  - Trace Resolver can be enabled using one of these methods:
    - z/OS UNIX RESOLVER\_TRACE environment variable
    - SYSTCPT DD allocation in the MVS batch job or TSO environment
    - TRACE RESOLVER or OPTIONS DEBUG statement in the TCPIP.DATA file
    - Debug option (resDebug) in an application \$\_\_res\_state structure
  - Dynamically starting or stopping Trace Resolver can be problematic for long running applications like Started Task Control (STC) servers
    - SYSTCPD DD usage requires stopping and restarting the server
    - resDebug requires special application logic
  - Diagnostic results not readily available to system administrator



## Overview continued

- Solution

- Collect Trace Resolver using Resolver Component Trace
  - New RESTRACE trace option

- Benefit / Value

- Allows Trace Resolver information to be collected without stopping and restarting the server
- Allows Trace Resolver information to still be collected on an individual application basis
  - Supports ASID and JOBNAME filtering
- Component Trace results are available for the system administrator review
  - Use Interactive Problem Control System (IPCS) CTRACE subcommand processing to view the formatted component trace data



## Usage & Invocation

- Use TRACE CT,ON command to enable the collection of Trace Resolver output as Resolver CTRACE records
  - TRACE CT,ON,COMP=SYSTCPRE,SUB=(resolver jobname)
  - R xx,OPTION=(TRACERES) in response text plus any filters
  - Example command and response:  
TRACE CT,ON,COMP=SYSTCPRE,SUB=(RESOLVER)  
\*05 ITT006A SPECIFY OPERAND(S) FOR TRACE CT  
COMMAND.  
R 05,OPTIONS=(TRACERES),JOBNAME=(SERVER1),END

▪



## Usage & Invocation continued

- Use TRACE CT,ON command to disable the collection of Trace Resolver output as Resolver CTRACE records
  - TRACE CT,ON,COMP=SYSTCPRE,SUB=(resolver jobname)
  - R xx,OPTION=() in response text plus any filters

- Example command and response:

```
TRACE CT,ON,COMP=SYSTCPRE,SUB=(RESOLVER)
*05 ITT006A SPECIFY OPERAND(S) FOR TRACE CT
COMMAND.
```

```
R 05,OPTIONS=(),JOBNAME=(SERVER1),END
```

▪



## Usage & Invocation continued

- Use the Interactive Problem Control System CTRACE subcommand to view the formatted component trace data from a dump or an external writer data set

- Example with filtering:

```
CTRACE COMP(SYSTCPRE) SUB((RESOLVER)) LOCAL FULL
JOBLIST(SERVER1) OPTIONS((TYPE(TRACERES))
```

–

–



# CICS transaction tracking support for CICS TCP/IP IBM Listener





## Overview

- Problem Statement / Need Addressed
  - CICS Transaction Server V4R2 introduced transaction tracking
  - Point of Origin information is useful for problem determination
  - CICS TCP/IP sockets interface does not register Point of Origin information
- Solution
  - Enhance CICS TCP/IP sockets to register Point of Origin information
  - Restricted to IBM supplied listener program (EZACIC02)
- Benefit / Value
  - Point of Origin information available for transactions started by IBM supplied listener (EZACIC02)
  - Improves problem diagnosis

▪



## Usage & Invocation

- No action required to enable Point of Origin registration
- Use the CICS TCP/IP IBM Listener program, EZACIC02
  - No Point of Origin information for non-IBM listener and client programs
- Transaction tracking Point of Origin fields updated by the zOS Communications Server CICS TCP/IP sockets TRUE are:
  - Origin Adapter Data 1
    - TCPIP Jobname
  - Origin Adapter Data 2
    - Local IP address and local port (Listener)
  - Origin Adapter Data 3
    - Remote IP address and remote port
  - Origin Adapter ID
    - IBM zOS CommServer CICS TCP/IP sockets supplied listener name



## Interactions & Dependencies

- Point of Origin information available for
  - CICS Explorer
  - SMF type 110
- Requires CICS Transaction Server 4.2 or later



# Configuration Assistant – TCP/IP Profile Configuration



## Overview

- Problem Statement / Need Addressed
  - TCP/IP profile configuration contained in an MVS data set.
  - Manual editing to define each statement
  - Defaults rarely change and differ from best practice
  - Reusable configuration limited to a sysplex scope
- Solution
  - Enhance Configuration Assistant for TCP/IP Profile configuration
- Benefit / Value
  - Web based user interface to simplify configuration process
  - Best practices configuration preselected
  - Default settings and migration addressed by workflow
  - Consolidated configuration at the enterprise level increase reusability

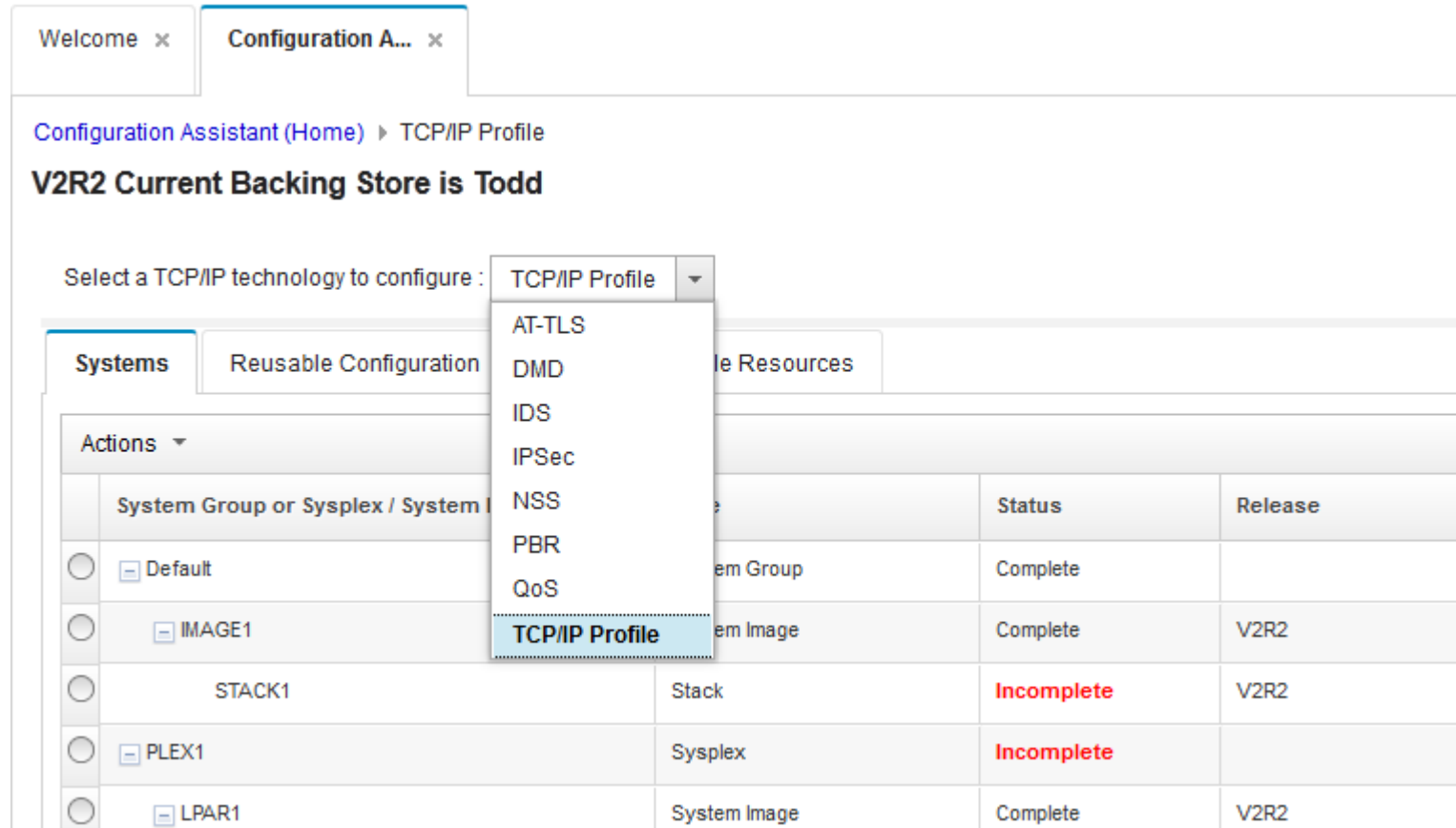
▪



## Usage & Invocation

- Select new “TCP/IP Profile” technology perspective within Configuration Assistant

■



The screenshot shows the Configuration Assistant interface with the 'Configuration Assistant (Home)' tab selected. The breadcrumb path is 'Configuration Assistant (Home) > TCP/IP Profile'. The main heading is 'V2R2 Current Backing Store is Todd'. Below this, there is a dropdown menu labeled 'Select a TCP/IP technology to configure :'. The dropdown is open, showing a list of options: TCP/IP Profile, AT-TLS, DMD, IDS, IPSec, NSS, PBR, and QoS. The 'TCP/IP Profile' option is highlighted. In the background, there is a table with columns 'System Group or Sysplex / System Image', 'Status', and 'Release'. The table contains several rows, including 'Default', 'IMAGE1', 'STACK1', 'PLEX1', and 'LPAR1'. The 'Status' column shows 'Complete' for 'Default', 'IMAGE1', and 'LPAR1', and 'Incomplete' for 'STACK1' and 'PLEX1'. The 'Release' column shows 'V2R2' for 'IMAGE1' and 'LPAR1'.

| System Group or Sysplex / System Image | Status     | Release |
|----------------------------------------|------------|---------|
| Default                                | Complete   |         |
| IMAGE1                                 | Complete   | V2R2    |
| STACK1                                 | Incomplete | V2R2    |
| PLEX1                                  | Incomplete |         |
| LPAR1                                  | Complete   | V2R2    |



## Interactions & Dependencies

- zOS Management Facility (zOSMF) must be installed
- Configuration Assistant plugin must be installed



## Presentation Summary

- Simplification
  - Removal of GATEWAY statement
  - Removal of Legacy devices and associated address spaces
  - Configuration Assistance support of TCP/IP Profile
- Security
  - NIST compliance
  - Simplified access to ICSF
  - AT-TLS currency
  - FTP and AT-TLS session reuse
  - 
  -





## Presentation Summary continued

- Economics / Platform Efficiency
  - TCP autonomies
  - Dynamic VIPA limit
  - Enterprise Extender scalability
  - 64 bit TCP/IP stack
  - IKED scalability
  - SMC-R enhancements and virtualization
  - VIPAROUTE MTU
- Availability / Business Resilience
  - Dynamic Resolver trace
  - Resolver cache reordering
- Applications / Middleware / Workload Enablement
  - CICS transaction tracking



## Appendix

### ▪ z/OS Communications Server Publications

- z/OS Communications Server: IP CICS Sockets Guide SC27-3649
- z/OS Communications Server: IP Configuration Reference SC27-3651
- z/OS Communications Server: IP Diagnosis Guide GC27-3652
- z/OS Communications Server: IP Programmer's Guide and Reference SC31-8787
- z/OS Communications Server: IP System Administrator's Commands SC31-8781
- z/OS Communications Server: New Function Summary GC31-8771
- z/OS Communications Server: SNA Diagnosis Vol 2, FFST Dumps and the VIT GC31-6851
- z/OS Communications Server: SNA Network Implementation Guide SC27-3672
- z/OS Communications Server: SNA Operation SC31-8779



## Appendix continued

- Publications

- z/OS Cryptographic Services ICSF Administrator's Guide SA22-7521
- z/OS Cryptographic Services System SSL Programming SC14-7495
- z/OS HCD User's Guide SC34-2669
- z/OS MVS Initialization and Tuning Reference SA22-7592

- IBM CICS Explorer

- <http://www-03.ibm.com/software/products/en/cics-explorer>

