z/OS V2.5 IBM Education Assistant

Solution Element(s): Communications Server

July 2021

Agenda

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

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

Provide a high-level overview of the Communications Server functions in z/OS V2.5

- AT-TLS currency with System SSL
- AT-TLS and IPsec certificate diagnostics
- IPsec certificate reporting enhancements
- Shared Memory Communications multiple subnet support (SMCv2)
- z/OS Encryption Readiness Technology (zERT) policy-based enforcement
- zERT Aggregation recording interval
- zERT Network Analyzer database administration enhancements
- Notification of Availability of TCP/IP Extended Services
- Sysplex Autonomics for IPsec
- Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions
- SMTPD compatibility enhancements for CSSMTP
- Support Considerations for z/OS V2.5

AT-TLS currency with System SSL

Overview

- Background
  - AT-TLS provides TLS/SSL protection to TCP traffic
    - Acts as a System SSL wrapper
    - Applied based on policy, no need to change application source code
    - Stays current with new System SSL features
  - System SSL implemented support for RFC 7627
    - Extended Master Secret (EMS) extension
    - Applicable only to TLSv1.0 – TLSv1.2

Overview

- Who (Audience)
  - Network Security administrator
  - Software developer

- What (Solution)
  - AT-TLS enhanced to support new EMS extension

- Wow (Benefit / Value, Need Addressed)
  - New EMS extension is exploited (RFC 7627)

Usage & Invocation

- In AT-TLS policy

- RFC 7627
  - TTLSEnvironmentAdvancedParms
  - TTLSConnectionAdvancedParms

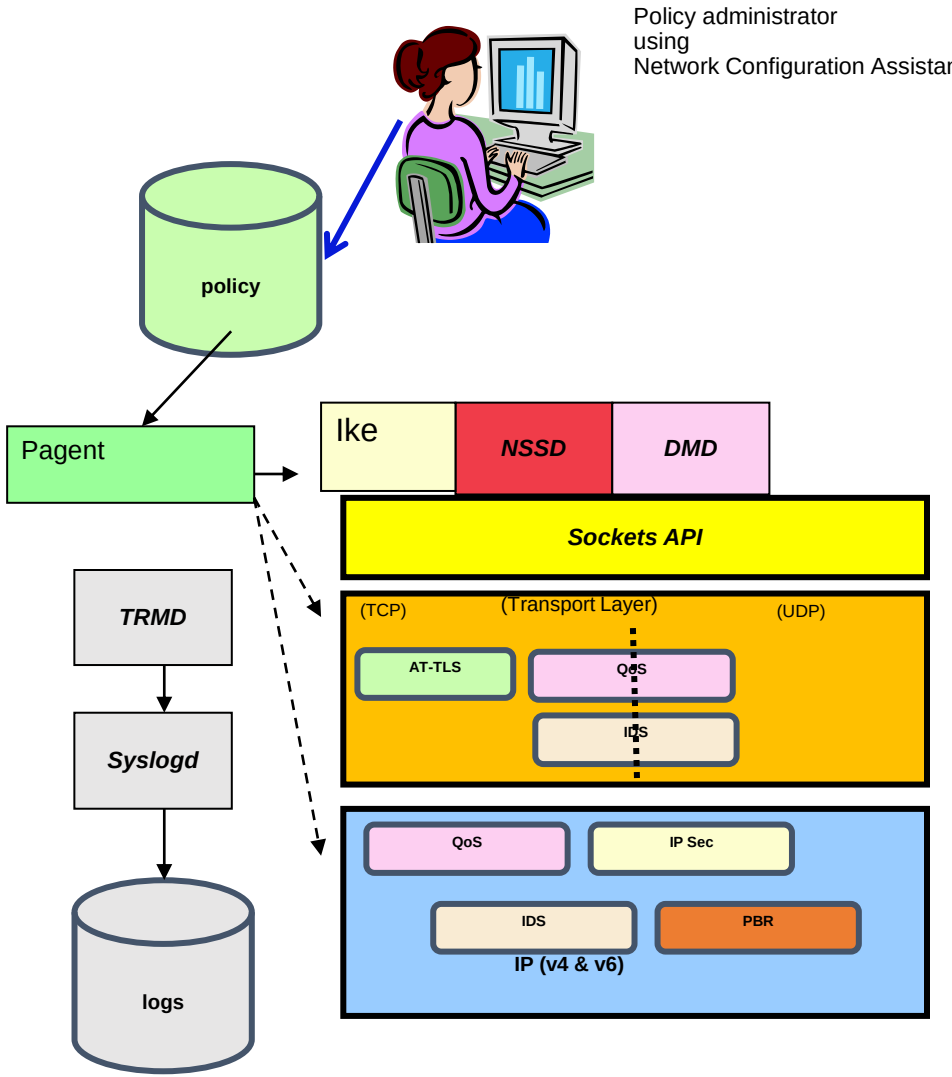
- Enabled by default

- No support added for z/OS V2R3 and V2R4

Usage & Invocation – Network Configuration Assistant

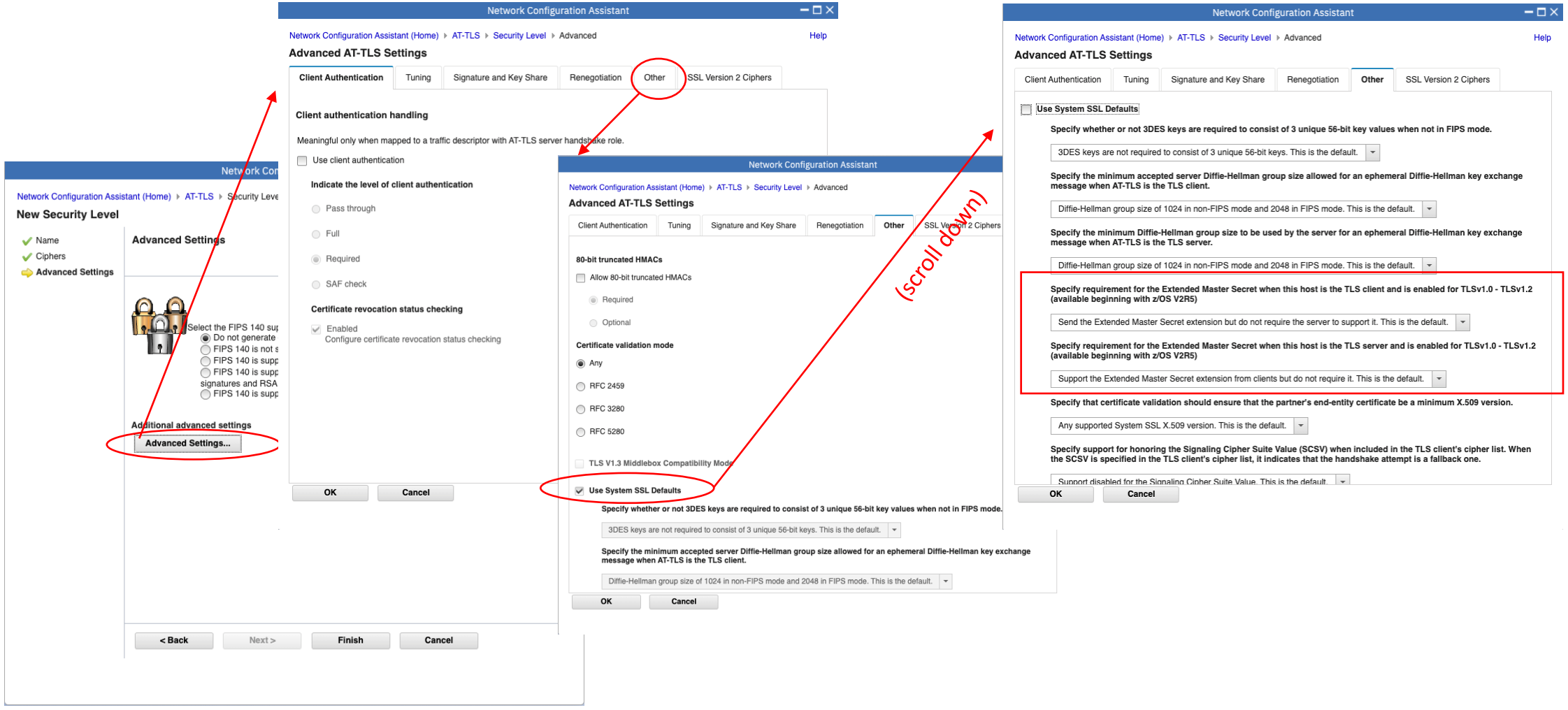
- Network Configuration Assistant (NCA) is updated to support the new AT-TLS policy parameters

- NCA is a z/OSMF plug-in to simplify configuration of z/OS Communications Server
  - TCP/IP profile
  - Policy-based networking technologies
    - IP Security – IP Filter rules and VPN tunnels
    - Application Transport TLS (AT-TLS)
    - Intrusion Detection Services (IDS)
    - Policy-based Routing (PBR)
    - Quality of Service (Qos)



Usage & Invocation - NCA

- NCA Security Level's Advanced Settings



Interactions, Dependencies, Upgrade & Installation

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies: None
- Hardware Dependencies: None
- Exploiters: None
- Coexistence:
  - V2R3 and V2R4
    - See System SSL presentation for more enablement information of their support for RFC 7627
      - *IEAV2R5 Certificate failure diagnostics and Extended master secret System SSL*
- Installation: None

AT-TLS and IPsec certificate diagnostics

Overview – AT-TLS certificate diagnostics

- Background
  - AT-TLS negotiation failures are reported in EZD1286I/ EZD1287I messages with return code

```
EZD1286I TTLS Error GRPID: 00000001 ENVID: 00000001 CONNID: 0000001F LOCAL: 9.42.104.171..1025 REMOTE: 9.42.104.171..6003
JOBNAME: USER603 USERID: USER60 RULE: tnsaso_clnt6 RC: 5006 Initial Handshake 00000000 00000000
```

  - When failure is due to an issue with the peer certificate or certificate chain the return code alone might not be sufficient for a diagnostic investigation

- Who (Audience)
  - z/OS Network Security administrator

- What (Solution)
  - Exploiting new System SSL API to provide new messages containing diagnostic data related to secure handshake failures caused by peer certificate validation issues for AT-TLS protected connections

Overview – AT-TLS certificate diagnostics continued

- What (Solution) continued
  - New messages written to syslogd
    - EZD2052I – additional information on failing certificate

```
EZD2052I TTLS Certificate Diagnostics GRPID: 00000001 ENVID: 00000009 CONNID: 00000066 SSLRetCode= 8 CMSRetCode= 0x0335302f
Description= Self-signed certificate is not found in the trusted key source
SubjectDN= <CN=TEST ROOT CA,OU=MYDEPT,O=MYCOMPANY,L=Raleigh,ST=NC,C=US>
IssuerDN= <CN=TEST ROOT CA,OU=MYDEPT,O=MYCOMPANY,L=Raleigh,ST=NC,C=US> SerialNumber= 111111
CertificateSource= Handshake TrustedSource= CLIENTRING
```

    - EZD2053I – information on each certificate in certificate chain used for validation

```
EZD2053I TTLS Certificate Diagnostics Details GRPID: 00000001 ENVID: 00000009 CONNID: 00000066
Certificate= 1 of 3 FailingCert= NO
SubjectDN= <CN=TEST Server,OU=MYDEPT,O=MYCOMPANY,L=Raleigh,ST=NC,C=US>
IssuerDN= <CN=TEST INTERMEDIARY CA,OU=MYDEPT,O=MYCOMPANY,L=Raleigh,ST=NC,C=US> SerialNumber= 333333
CertificateSource= Handshake
```

    - EZD2054I – information on data sources used for failed validation of the peer's certificate

```
EZD2054I TTLS Certificate Diagnostics Data Sources GRPID: 00000001 ENVID: 00000009 CONNID: 00000066
Count= 2 CLIENTRING , Handshake
```

- Wow (Benefit / Value, Need Addressed)
  - Mitigates need for collecting System SSL trace as part of diagnostic investigation

Usage & Invocation – AT-TLS certificate diagnostics

- In AT-TLS policy

- TTLSGroupAction, TTLSEnvironmentAction, and TTLSConnectionAction statements

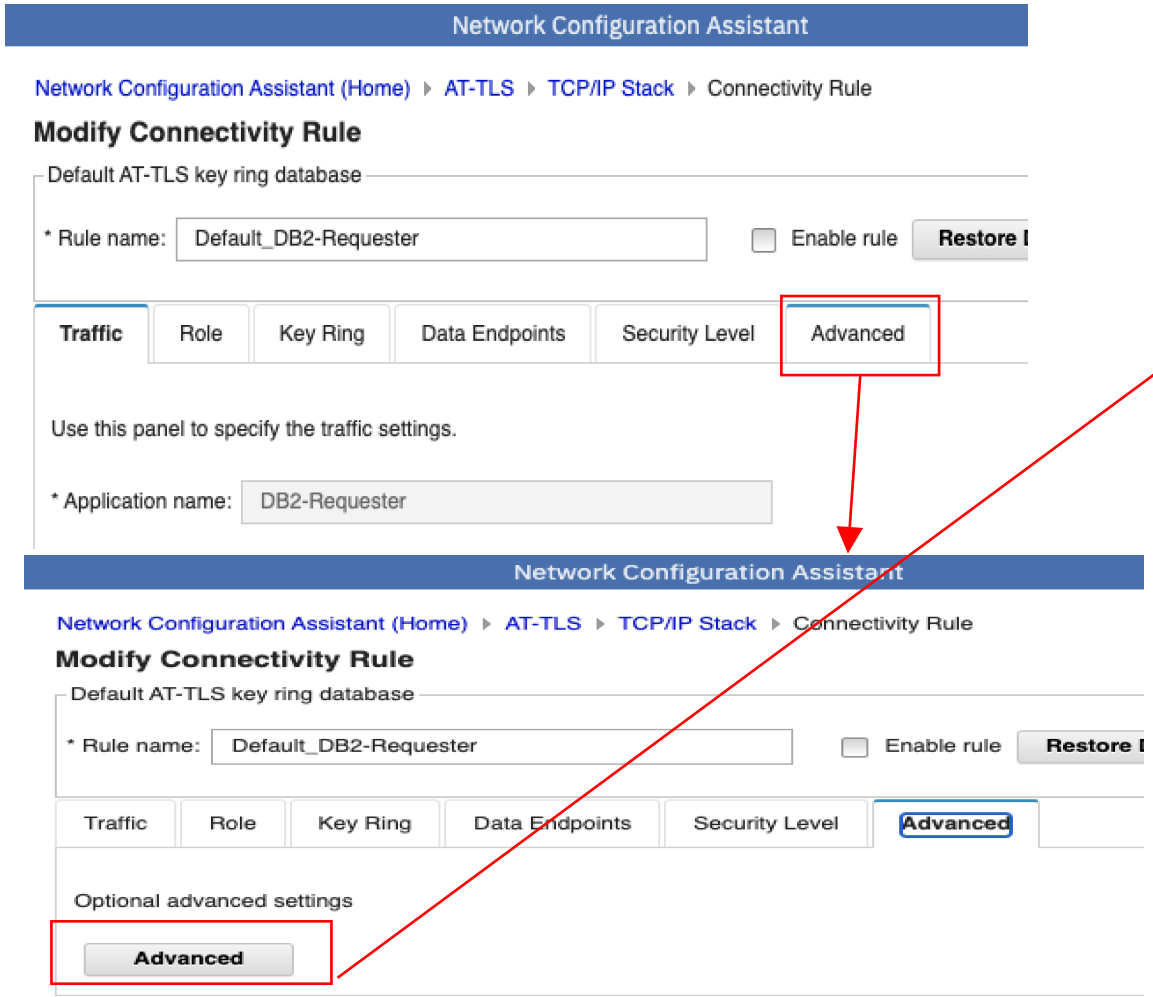
- Specifying an AT-TLS Trace level that includes Trace level 2 (error) (which is also the default Trace level) will provide information about the certificate in error (EZD2052I)
  - Typically, identifying the certificate in error is sufficient for the diagnostic investigation
  - However, if the certificate chain is needed then the additional new messages will be needed for the investigation
- Specifying an AT-TLS Trace level that includes Trace level 8 (event) will provide information about the chain of certificates and data sources used for the certificate validation (EZD2053I and EZD2054I)

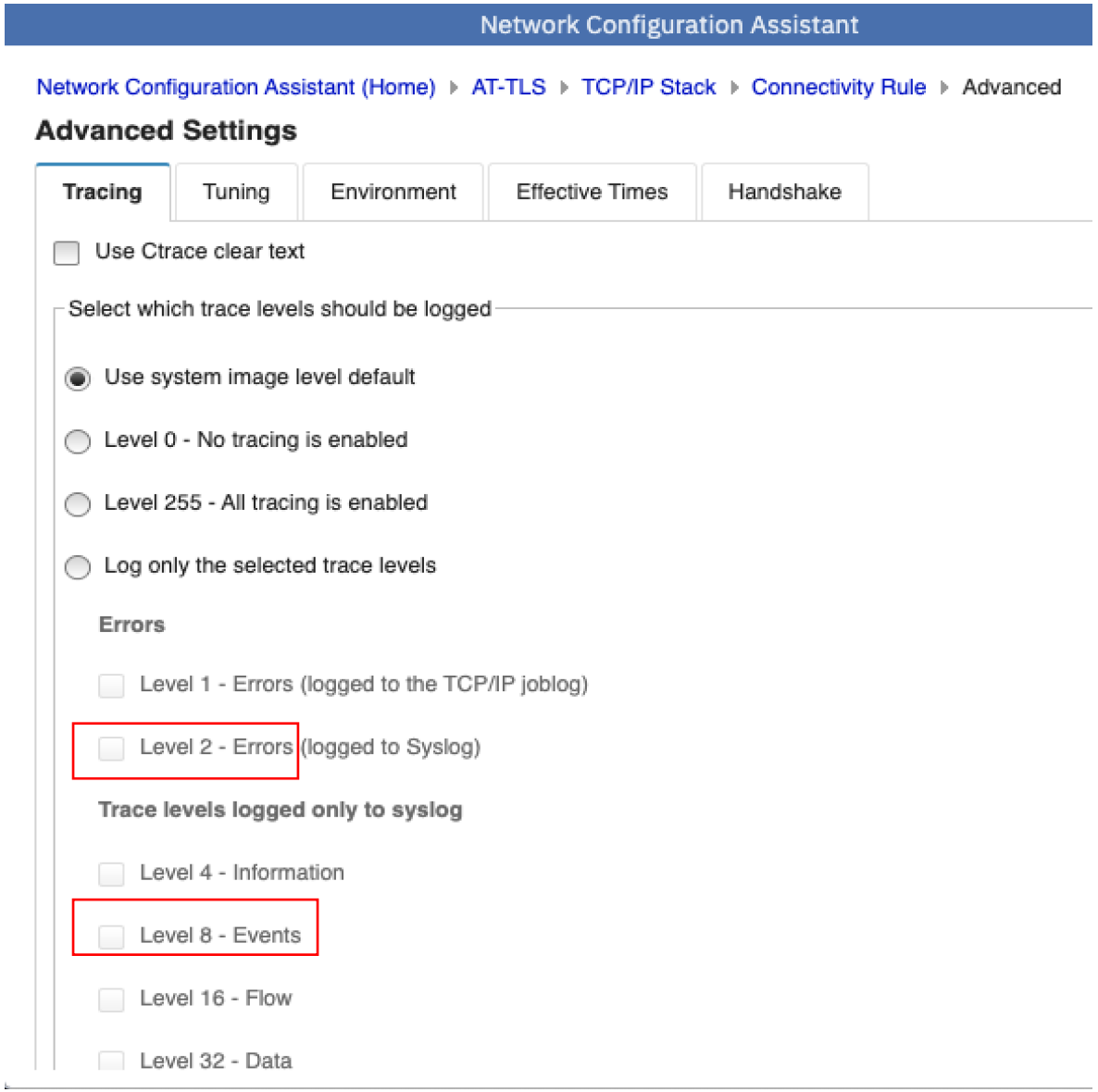
- Example: Trace 2 # Trace level 2 (error) enabled only

- Example: Trace 255 # All Trace levels enabled

Usage & Invocation – AT-TLS certificate diagnostics using NCA

- Update the AT-TLS rule trace level





Overview – IPsec certificate diagnostics 1 of 3

- Background
  - For IPsec protection IKED typically relies on NSS daemon for certificate services
    - Message EZD1139I issued when NSS daemon detects a certificate validation failure

```
EZD1139I Request type NSS_VerifySignatureReqToSrv with correlator ID 00000000000001DE0000000000000000
for stack TCPSVT failed - return code EGSKVAL reason code CMSERR_CERT_CHAIN_NOT_TRUSTED
```

  - IKED can also provide certificate services in some cases
    - Message EZD0902I issued when IKED detects a certificate validation failure

```
EZD0902I Peer certificate failed validation - System SSL CMS error : 03353024 Issuer certificate not found
```

  - Both NSSD and IKED exploit System SSL certificate management services (CMS) APIs for certificate validation
  - When failure is due to an issue with the peer certificate or certificate chain the return code or CMS error code alone may not be sufficient for diagnostic investigation

Overview – IPsec certificate diagnostics 2 of 3

- Who (Audience)
  - z/OS Network Security administrator
- What (Solution)
  - Exploiting new System SSL API to provide new messages containing diagnostic data related to secure handshake failures caused by peer certificate validation issues for IPsec protected connections
  - New messages written to syslogd
    - EZD2055I - additional information on failing certificate

```
EZD2055I Certificate Diagnostics RetCode= EGSKVAL ReasonCode= 0x0335302F
Description= Certificate is expired
SubjectDN= <CN=BO EXPCA,OU=SVT,O=IBM,C=US> IssuerDN= <CN=BO EXPCA,OU=SVT,O=IBM,C=US>
SerialNumber= 001111 CertSource= NSSD/NSSDRING TrustSource= NSSD/NSSDRING
```

    - IKE DEBUGSA Certificate Diagnostics Details - information on each certificate in certificate chain used for validation

```
IKE DEBUGSA : Certificate Diagnostics Details Certificate 1 of 2 FailingCert= No
SubjectDN= <CN=BOVIPA8_EXPCA,OU=SVT,O=IBM,C=US> IssuerDN= <CN=BO EXPCA,OU=SVT,O=IBM,C=US>
SerialNumber= 022222 CertSource= IKEPayload
```

Overview – IPsec certificate diagnostics 3 of 3

- What (Solution) continued
  - New messages written to syslogd
    - IKE DEBUGSA Certificate Diagnostics Data Sources - information on data sources used for failed validation of the peer's certificate

```
IKE DEBUGSA : Certificate Diagnostics Data Sources Count= 2 NSSD/NSSDRING , IKEPayload
```

- Wow (Benefit / Value, Need Addressed)
  - Mitigates need for collecting System SSL trace as part of diagnostic investigation

Usage & Invocation – IPsec certificate diagnostics

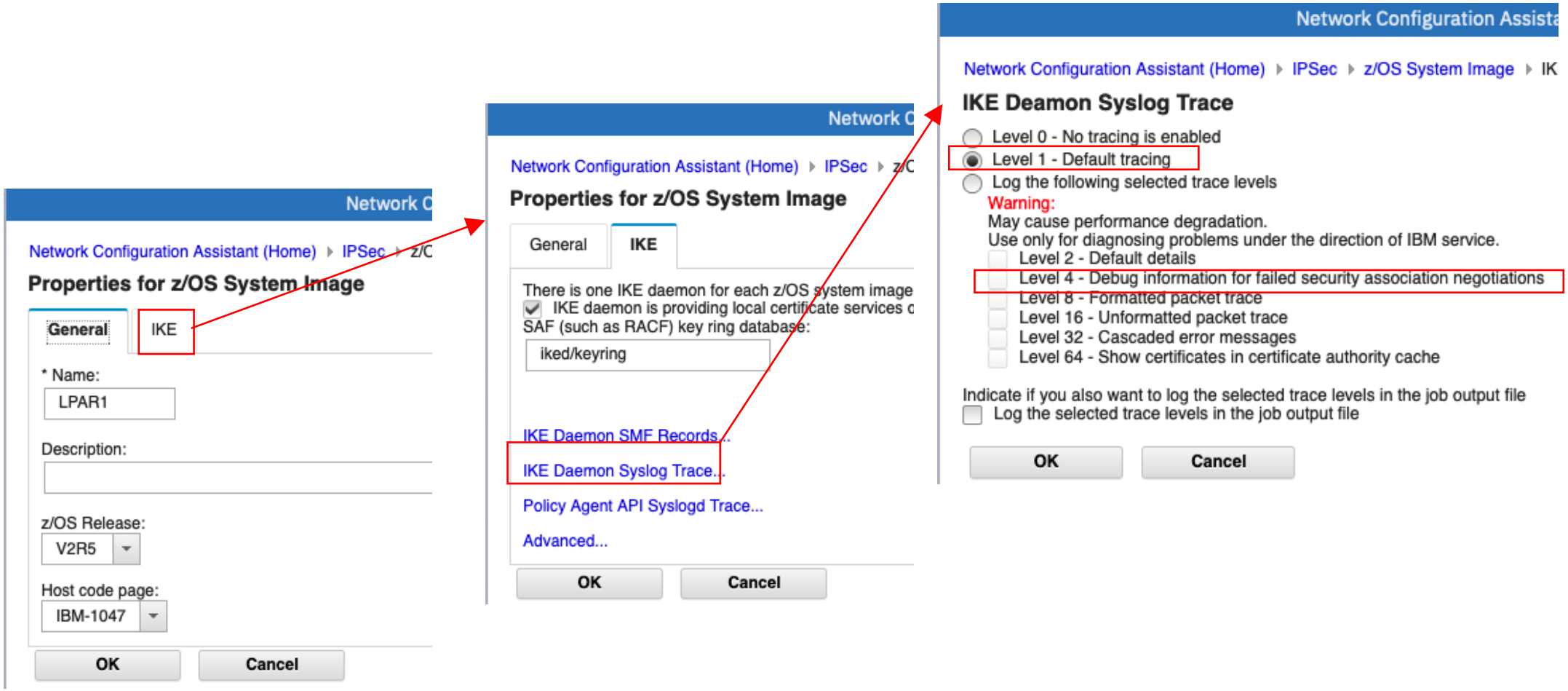
- In IKED configuration file

- Existing IkeSyslogLevel statement
  - Any value greater than 0 will provide information about the certificate in error (EZD2055I) along with existing message EZD1139I or EZD0902I
  - Any value including 4 (IKE_SYSLOG_LEVEL_DEBUGSA) will provide the chain of certificates and data sources used for the certificate validation (IKE DEBUGSA Certificate Diagnostics Details and IKE DEBUGSA Certificate Diagnostics Data Sources)

- Example: IkeSyslogLevel 7

Usage & Invocation – IPsec certificate diagnostics using NCA

- If you use NCA to create your IKED configuration file, update the syslog trace level



Interactions, Dependencies, Upgrade & Installation

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies: System SSL
- Hardware Dependencies: None
- Exploiters: None
- Coexistence:
  - When NSS Daemon (NSSD) is providing certificate services both IKED and NSSD must be at release z/OS V2R5 for new certificate diagnostic messages to be generated for IPsec
- Installation: None

IPsec certificate reporting enhancements

Overview – IPsec certificate reporting enhancements

- Who (Audience)
  - z/OS Network Security administrator

- What (Solution)
  - z/OS UNIX ipsec command enhanced to provide information about end entity certificates used during successful IKE phase 1 negotiations
    - No certificate information available in failed negotiation attempts
  - Enhanced associated SMF and NMI records to provide the same end entity certificate information

- Wow (Benefit / Value, Need Addressed)
  - Provides clarity on specific certificates used for IKE phase 1 negotiations

Usage & Invocation – IPsec certificate reporting enhancements

- ipsec –k display command

```
TunnelID:                    K13
Generation:                  1
IKEVersion:                  2.0
KeyExchangeRuleName:         KER-19-IPv4-IKEv2-bundl
KeyExchangeActionName:       KEA-6-IPv4-IKEv2-bundl
LocalEndPoint:               10.84.8.9
LocalIDType:                 ID_IPV4_ADDR
LocalID:                     10.84.8.4
RemoteEndPoint:              10.84.2.9
RemoteIDType:                ID_IPV4_ADDR
RemoteID:                    10.84.2.4
ExchangeMode:                n/a
State:                       DONE
AuthenticationAlgorithm:     HMAC-SHA2-512-256
EncryptionAlgorithm:         3DES-CBC
 KeyLength:                  n/a
PseudoRandomFunction:        AES128-XCBC
DiffieHellmanGroup:          20
LocalAuthenticationMethod:   RsaSignature
RemoteAuthenticationMethod:  RsaSignature
InitiatorCookie:             0xEECE213C56B8EAC0
...
RmtNAPTDetected:             No
RmtUdpEncapPort:             n/a
LocalCertExpires:            2046/04/29 20:38:50
LocalSerialNumber:           48AC547CF4A5A11B
LocalIssuerDNLength:         48
LocalIssuerDN:               CN=FVT Domain1 CA3,OU=FVT,O=IBM,L=RTP,ST=NC,C=US
LocalSubjectDNLength:        69
LocalSubjectDN:              CN=FVT.V1RDDomain1 Chain MVSB RSA Cert4,OU=FVT,O=IBM,L=RTP,ST=NC,C=US
RemoteCertExpires:           2046/04/29 20:38:33
RemoteSerialNumber:          48AC547CF4A5A119
RemoteIssuerDNLength:        48
RemoteIssuerDN:              CN=FVT Domain1 CA3,OU=FVT,O=IBM,L=RTP,ST=NC,C=US
RemoteSubjectDNLength:       69
RemoteSubjectDN:             CN=FVT.V1RDDomain1 Chain MVSA RSA Cert4,OU=FVT,O=IBM,L=RTP,ST=NC,C=US
*************************************************************************
```

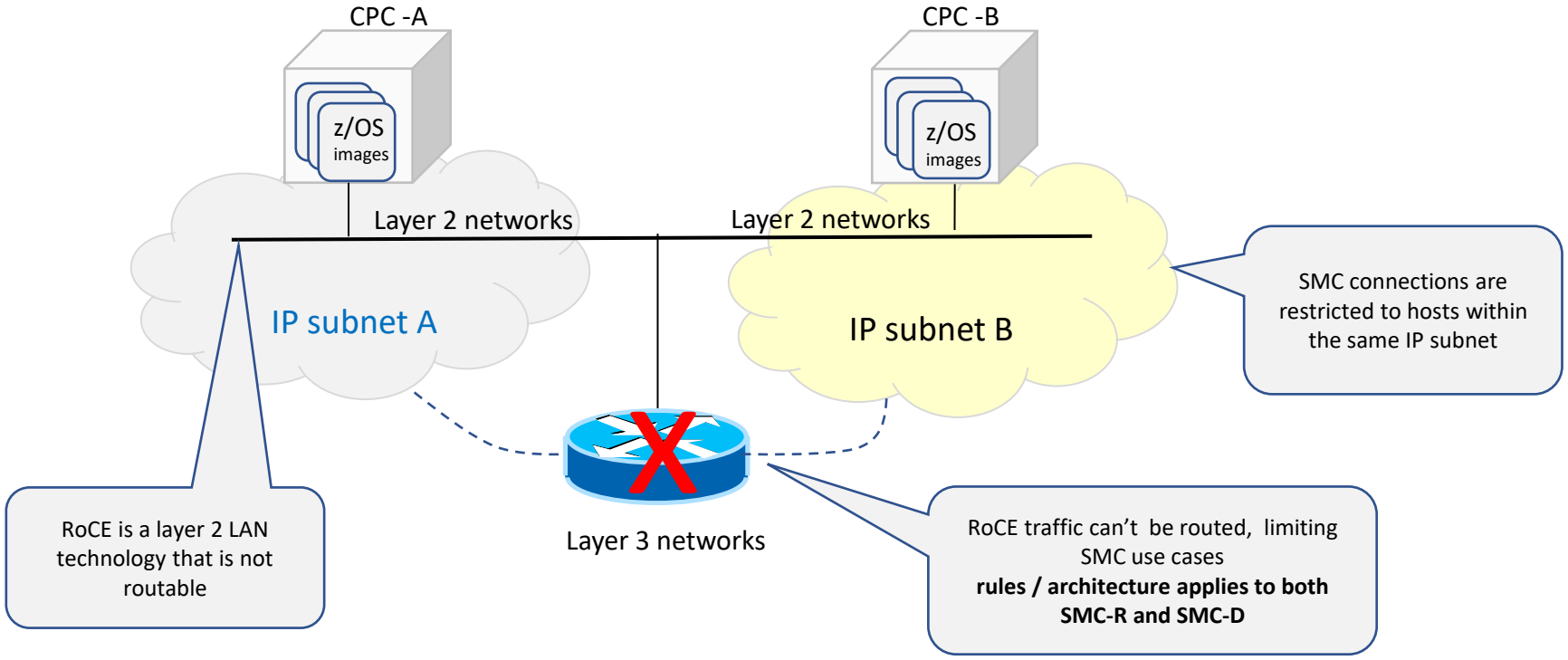
Interactions, Dependencies, Upgrade & Installation

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies: None
- Hardware Dependencies: None
- Exploiters: None
- Coexistence:
  - -z option can direct ipsec command to an NSS client on a different LPAR
    - New certificate related information is only available if both the system issuing the ipsec command and the system which the NSS client exists are at V2R5+
- Installation: None

Shared Memory Communications multiple subnet support (SMCv2)

Overview

- Background
  - Originally, SMC-R is limited to communications for hosts attached to a common IP subnet (physical or VLAN).



Note.
SMC-R (RoCE) and SMC-D (ISM) follow the same base SMC protocol and rules. The single subnet connection eligibility (limitation) applies to both forms of SMC.

28

Overview

- Background continued
- SMC-R requires both hosts to be on the ***same layer 2 network*** (physical LAN or VLAN) and in the ***same IP subnet*** when communicating via TCP/IP (i.e. have a direct communication path without the need to traverse IP routers)
  - SMC-R is based on RoCE v1 which depends on layer 2 network connectivity across all peers (RoCE v1 supported in original RoCE Express adapters on Z)
  - SMC-D designed as an extension of SMC-R and has the same layer 2 network connectivity requirements (via OSA or HiperSockets)
- This restriction prohibited many interested in adopting SMC because of this network topology requirement
  - Many have z/OS, Linux on Z and Power/AIX systems that reside in different subnets in their data center networks

Overview

- Who (Audience)
  - Solution Architect, Systems Programmer

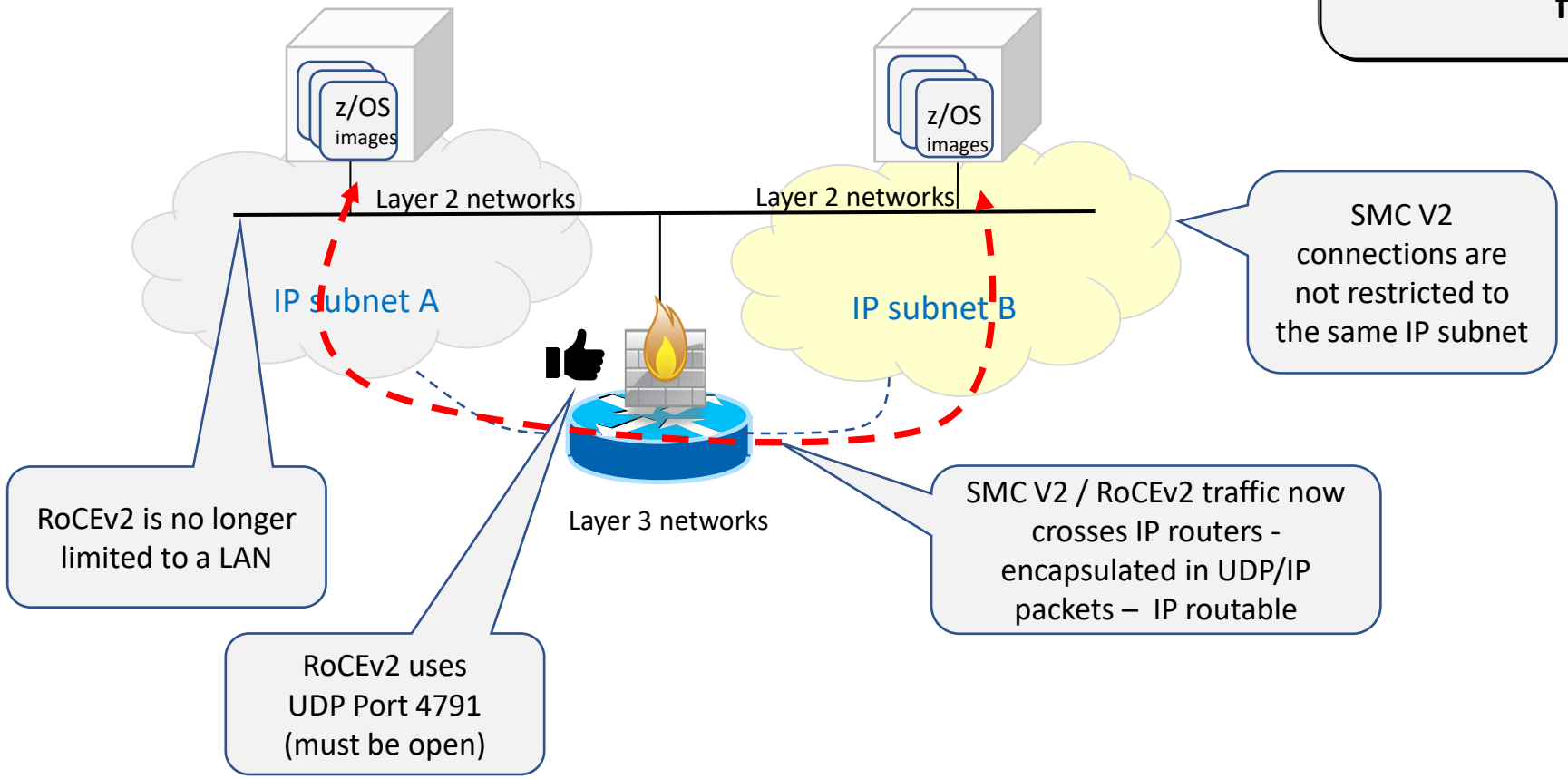
- What (Solution)
  - Shared Memory Communication Version 2 protocol - multiple IP subnet support for both SMC-D and SMC-R.
  - SMC-Dv2 for z/OS V2R5 to z/OS V2R5 TCP communications (co-located on the same CPC) and SMC-Rv2 for z/OS V2R5 to z/OS V2R5 TCP communications (across CPCs)[1]
  - SMC-Dv2 requires an update to the ISM firmware provided on the IBM z15.
  - SMC-Rv2 requires RoCEv2 (aka “routable RoCE”) supported with the IBM RoCE Express2 feature on the IBM z15.
  - New (optional) SMC Global filters that controls (permits and excludes) all four forms of SMC using the peer’s TCP/IP address/subnet

1. Although SMCv2 applies to both SMC-R and SMC-D, this program is primarily focused on feedback for SMC-Rv2. SMC-Dv2 (multiple IP subnet support with ISMv2) was previously shipped in z/OS V2R4 (APARs PH22695/OA59152)

Overview

- What (Solution) continued

SMC-Rv2 eliminates the Single-subnet restriction for SMC-R



Overview

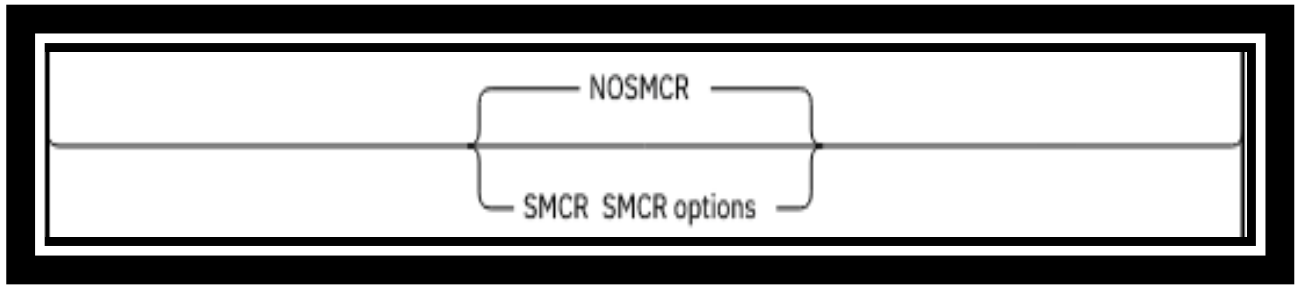
- Wow (Benefit / Value, Need Addressed)
  - SMC-R is a powerful IBM Z enterprise data center network communications solution that has the potential to offer savings in latency reduction, network related CPU costs and increased throughput.
  - SMC-R(RoCE) vs. TCP(OSA) savings[2] are up to:
    - 80% reduction in latency (transactional workloads)
    - 60% CPU savings (streaming workloads)
    - 60% increase in throughput (streaming workloads)
  - The SMC-Rv2 multiple IP subnet support extends the SMC-R capability and benefits to additional TCP application workloads that were previously ineligible for SMC without making any configuration changes to the network IP topology (IP subnets)

2. Performance information included here is based on internal IBM benchmarks in a controlled environment of modeled z/OS TCP sockets-based workloads using SMC-R (10GbE RoCE Express feature) vs TCP/IP (10GbE OSA Express feature). The actual response times and CPU savings any user will experience will vary.

Usage & Invocation – Enabling SMC-Rv2

- In the TCPIP Profile

- To enable SMC-Rv2:
  1. Configure existing GLOBALCONFIG SMCR statement

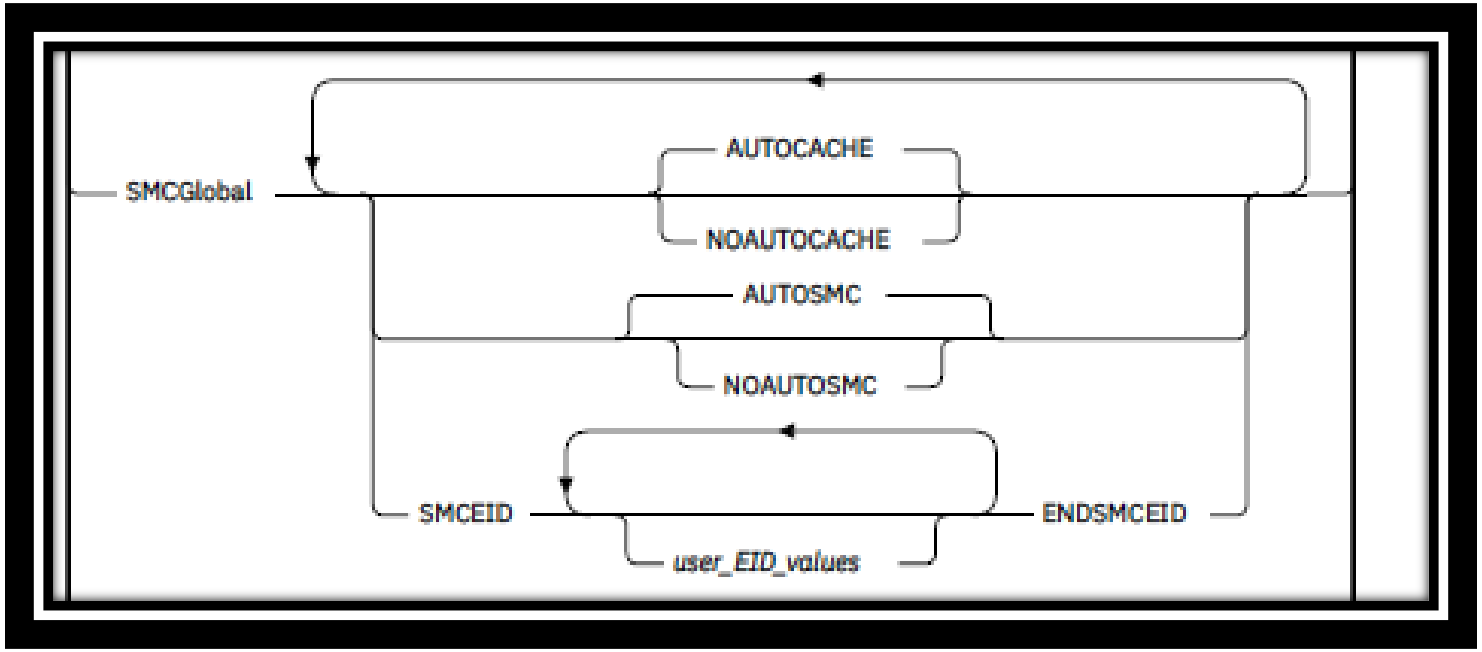


Usage & Invocation – Enabling SMC-Rv2

- In the TCPIP Profile

- To enable SMC-Rv2 (continued):
  2. New SMCEID/ENDSMCEID block on the SMCGLOBAL statement that specifies up to four user-defined Enterprise IDs

Example:
SMCEID MY.SYS1.EID ENDSMCEID



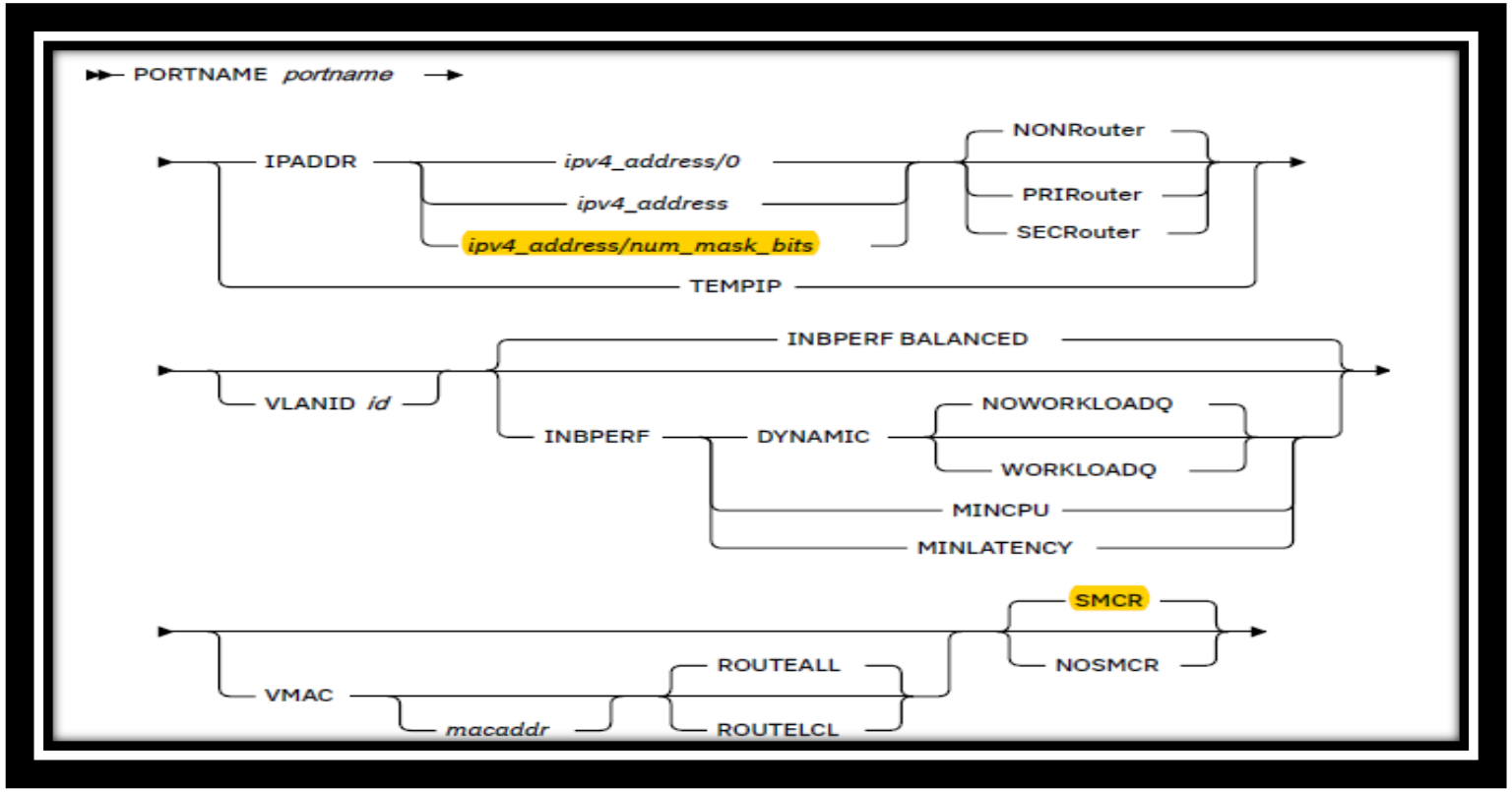
Usage & Invocation – Enabling SMC-Rv2

- In the TCPIP Profile

- To enable SMC-Rv2 (continued):
  3. Specify non-zero subnet mask specified on the IPADDR parameter of the IPAQENET INTERFACE statement

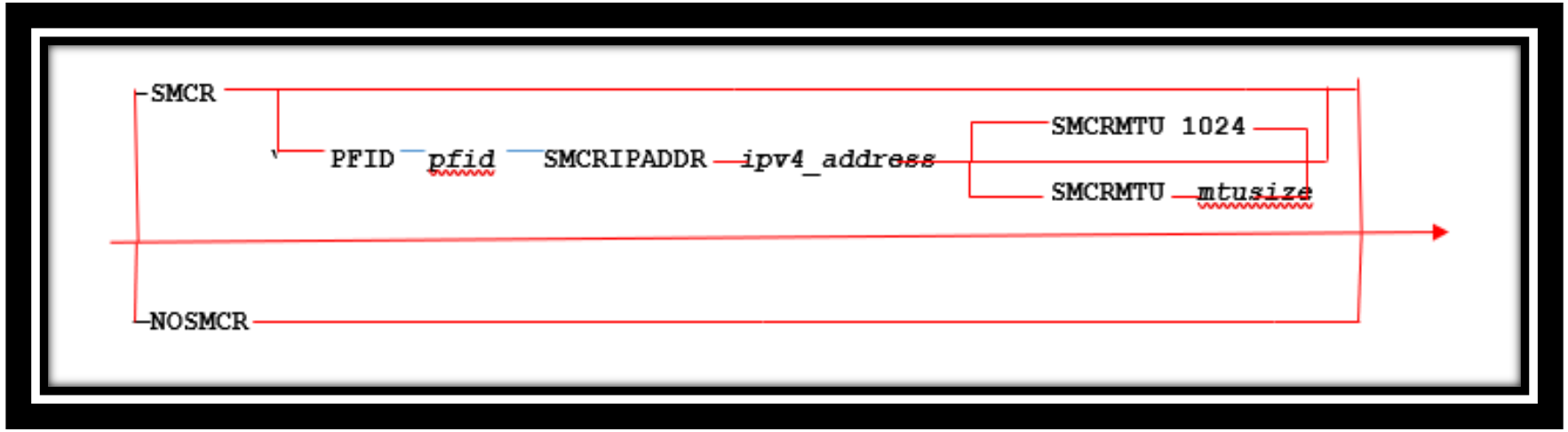
     Example:
     IPADDR 9.102.1.10/10

  4. Specify new sub parameters on the SMCR parameter of the IPAQENET INTERFACE statement
     - See next slide



Usage & Invocation – Enabling SMC-Rv2

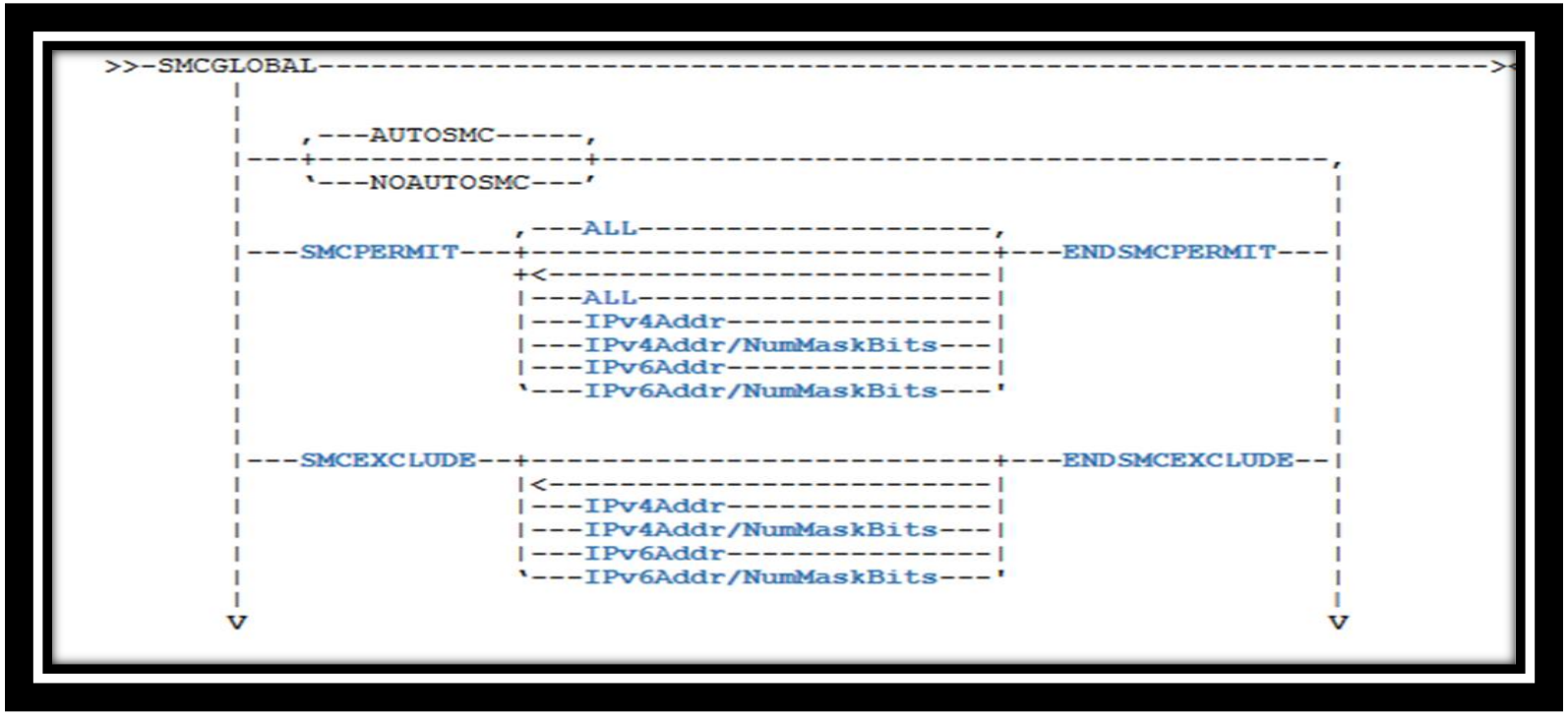
- In the TCPIP Profile



- To enable SMC-Rv2 (continued):
  - SMCR sub-parameters:
    - PFID *pfid*
    - Example PFID 0F
  - SMCRIPADDR *ipv4_address*
    - Example: SMCRIPADDR 9.102.1.11
  - SMCRMTU *1024* | *2048* | *4096*
    - Example: SMCRMTU 2048
    - Default value: 1024

Usage & Invocation – Enabling SMC Filters (optional)

- In the TCPIP Profile



- SMC Filters
  - SMCPERMIT/ENDSMCPERMIT block on SMCGLOBAL statement
    - Example

SMCGLOBAL SMCPERMIT 9.1.1.2 ENDSMCPERMIT

    - Default value:

SMCPERMIT ALL ENDSMCPERMIT

  - SMCEXCLUDE/ENDSMCEXLUDE block on SMCGLOBAL statement

    - Example:

SMCGLOBAL SMCEXCLUDE 9.1.1.5 ENDSMCELUDE

Interactions & Dependencies

- Software Dependencies: None

- Hardware Dependencies
  - IBM RoCE Express2 adapters (applies to both 10GbE and 25GbE)
  - ISMv2 (ISM firmware update)
  - IBM z15 (ISM and RoCE Express2)

- Exploiters: N/A

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No

- When enabling SMCv2 for either SMC-Rv2 or SMC-Dv2 a toleration update is required on peer SMC hosts:
  - z/OS toleration:
    - APAR PH17556
  - Linux toleration:
    - https://linux-on-z.blogspot.com/p/smc-for-linux-on-ibm-z.html
  - AIX toleration:
    - https://www.ibm.com/support/knowledgecenter/en/ssw_aix_72/rdma/s

Installation & Configuration – SMC-Rv2

- Considerations:
  - SMC-Rv2 support for IPv4 only
  - When a PFID is defined on an OSA INTERFACE, the RoCEv2 port must have the same Layer 2 (VLAN) and Layer 3 (IP subnet) attributes (definitions) as the associated OSA port (ports are “logically bonded”).
  - RoCEv2 is designed for the “Enterprise Data Center” – not for the WAN
  - Verify your firewalls are opened up for port 4791 UDP traffic
  - If enabling SMC-Rv2, for high-availability and load balancing
    - Verify you have multiple equal cost routes to the target SMC host
    - Verify your routes use OSA-Express interfaces configured for SMC-Rv2
    - Provision unique RoCE Express2 RNIC adapters to each LPAR to prevent a single point of failure

Installation & Configuration – SMC-Rv2 continued

- Hardware configuration:
  - Before using SMC-Rv2, you must take these actions:
    - Configure these values using HCD:
      - PCIe function ID (PFID) for RoCE Express2 features (IBM z15)
        - RNIC must support “Routable RoCE”
          - RoCE Express features only support SMC-Rv1 (RoCEv1)
        - Configure a type of ROC2
        - Configure associated port number
        - Configure two PFIDs, from unique RoCE Express2 features, per physical network, per LPAR for redundancy
      - Physical network ID (PNetID) for OSA and RNIC interfaces
        - PNetID still required for SMC-Rv2
    - Configure Ethernet switches appropriately
      - Optionally define VLAN ID values to be used
      - Enable jumbo frames if configuring SMC MTU larger than 1K

z/OS Encryption Readiness Technology (zERT) policy-based enforcement

Overview

- Background

- zERT Discovery
  - Attributes are collected and recorded at the connection level
  - SMF 119 subtype 11 “zERT Connection Detail” records and SYSTCPER NMI service
  - These records **describe the cryptographic protection history of each TCP and EE connection**
  - Measures are in place to minimize the number of subtype 11 records, but they could still be very voluminous
- zERT Aggregation
  - Discovery data aggregated by security session and written at each interval
  - SMF 119 subtype 12 “zERT Summary” records and SYSTCPES NMI service
  - These records **describe the repeated use of security sessions over time**
  - Aggregation can greatly reduce the volume of SMF records while maintaining the fidelity of the information – well suited for reporting applications
- zERT Network Analyzer
  - Web-based (z/OSMF) UI to query and analyze zERT Summary (subtype 12) records
  - Intended for z/OS network security administrators (typically systems programmers)

Overview

- Who (Audience)
  - z/OS systems programmer, z/OS network security administrator
- What (Solution)
  - TCP/IP stack takes specific actions when a user-defined security policy is met for a TCP connection
- Wow (Benefit / Value, Need Addressed)
  - Customers can codify and enforce their enterprise network encryption standards on z/OS to achieve a new level of compliance and auditability in their z/OS environments.

Usage & Invocation

- In the TCP/IP Profile

- Existing GLOBALCONFIG ZERT parameter enables monitoring of TCP and EE traffic

- New parameter on SMFCONFIG TYPE119 statement allows the generation of SMF 119 subtype 11 records with a new zERT Enforcement event type (0x07):

  SMFCONFIG TYPE119 ZERTDETAILBYPOLICY | NOZERTDETAILBYPOLICY

  Example: SMFCONFIG TYPE119 ZERTDETAILBYPOLICY
  Default value: NOZERTDETAILBYPOLICY

- New parameter on NETMONITOR statement allows the writing of SMF 119 subtype 11 records with a new zERT Enforcement event type (0x07) to the existing SYSTCPER NMI service:

  NETMONITOR ZERTSERVICEBYPOLICY | NOZERTSERVICEBYPOLICY

  Example: NETMONITOR ZERTSERVICEBYPOLICY
  Default value: NOZERTSERVICEBYPOLICY

Usage & Invocation

- In the Policy Agent configuration file

- New statement to specify path to the stack-specific ZERT policy file to be installed
  - ZERTConfig *path*

- If configuring Policy Agent as a policy client
  - New value for PolicyType parameter on the PolicyServer statement
    - ZERT

- If configuring Policy Agent as a policy server
  - New value for PolicyType parameter on the DynamicConfigPolicyLoad statement
    - ZERT
  - The policy client's user ID must be granted access to the following SERVAUTH class SAF profile: **EZB.PAGENT.*sysname.image.*ZERT**
    - *sysname* - System name defined in sysplex
    - *image* – Policy client's client name
  - The user ID is defined on the Userid parameter of the PolicyServer statement

Usage & Invocation

- New Policy Agent policy discipline and NCA technology perspective: zERT
- Policy is made up of ”zERT rules” that associate a set of connection and cryptographic conditions with a set of actions to be executed for traffic that maps to these conditions.
- Up to 4 “sets” of zERT Rules
  - TLS/SSL
  - IPsec
  - SSH
  - No recognized protection (NONE)
- Network Configuration Assistant is recommended to generate the “zERT rules”

Usage & Invocation

- Types of actions:
  - Log a message about the connection to the syslog daemon

EZZ8583I Connection logged by ZERT Policy Enforcement: timestamp connid= *connid* localipaddr= *localipaddr* localport= *localport* remoteipaddr= *remoteipaddr* remoteport= *remoteport* transproto= *transproto* jobname= *jobname* userid= *userid* conndir= *conndir* secproto= *secproto* secprotoversion= *secprotoversion* symenc1= *symenc1* symenc2= *symenc2* msgauth1= *msgauth1* msgauth2= *msgauth2* kex= *kex* rule= *rulename* action= *actionname*

  - Requires Traffic Regulation Manager daemon (TRMD) to be running

Usage & Invocation

- Types of actions:
  - Log a message about the connection to the console (TCP/IP joblog)

EZZ8551I CONN LOGGED BY ZERT POLICY
EZZ8552I STACK= *stackname* CONNID= *connid* CONNDIR= *conndir*
EZZ8553I LOCALIPADDR= *localipaddr* LOCALPORT= *localport*
EZZ8554I REMOTEIPADDR= *remoteipaddr* REMOTEPORT= *remoteport*
EZZ8555I TRANSPROTO= *transproto* JOBNAME= *jobname* USERID= *userid*
EZZ8556I SECPROTO= *secproto* SECPROTOVERSION= *secprotoversion*
[EZZ8557I SYMENC1= *symenc1* MSGAUTH1= *msgauth1*]
[EZZ8558I SYMENC2= *symenc2* MSGAUTH2= *msgauth2*]
[EZZ8559I KEX= *kex*]
EZZ8560I RULE= *rulename*
EZZ8561I ACTION= *actionname*

Usage & Invocation

- Types of actions:
  - Reset TCP connection
  - If LogSyslogd action is also specified, EZZ8584I message issued instead of EZZ8583I

EZZ8584I Connection reset by ZERT Policy Enforcement: timestamp connid= *connid* localipaddr= *localipaddr* localport= *localport* remoteipaddr= *remoteipaddr* remoteport= *remoteport* transproto= *transproto* jobname= *jobname* userid= *userid* conndir= *conndir* secproto= *secproto* secprotoversion= *secprotoversion* symenc1= *symenc1* symenc2= *symenc2* msgauth1= *msgauth1* msgauth2= *msgauth2* kex= *kex* rule= *rulename* action= *actionname*

  - If LogConsole action is also specified, EZZ8562I message is issued instead of EZZ8551I

EZZ8562I CONN RESET BY ZERT POLICY
EZZ8552I STACK= *stackname* CONNID= *connid* CONNDIR= *conndir*
EZZ8553I LOCALIPADDR= *localipaddr* LOCALPORT= *localport*
EZZ8554I REMOTEIPADDR= *remoteipaddr* REMOTEPORT= *remoteport*
EZZ8555I TRANSPROTO= *transproto* JOBNAME= *jobname* USERID= *userid*
EZZ8556I SECPROTO= *secproto* SECPROTOVERSION= *secprotoversion*
[EZZ8557I SYMENC1= *symenc1* MSGAUTH1= *msgauth1*]
[EZZ8558I SYMENC2= *symenc2* MSGAUTH2= *msgauth2*]
[EZZ8559I KEX= *kex*]
EZZ8560I RULE= *rulename*
EZZ8561I ACTION= *actionname*

Usage & Invocation

- Types of actions:
  - Create an audit record
    - Writes a SMF 119 subtype 11 record with new event type “zERT Enforcement” (x’07’)
    - New zERT policy-based enforcement section with the matching policy rule name
    - To write zERT enforcement audit records to SMF:
      - Audit enabled for the zERT policy rule
      - SMFCONFIG TYPE119 ZERTDETAILBYPOLICY in the TCP/IP profile
    - To write zERT enforcement audit records to real-time SMF NMI service SYSTCPER:
      - Audit enabled for the zERT policy rule
      - NETMONITOR ZERTSERVICEBYPOLICY in the TCP/IP profile

Interactions, Dependencies, Upgrade & Installation

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies:
  - TRMD (if zERT policy contains action to log messages about connections to the syslog daemon)
- Hardware Dependencies: None
- Exploiters: None
- Installation: None

zERT Aggregation recording interval

Overview

- Background
  - Originally, zERT Aggregation recording was tied directly to the z/OS system's SMF interval
  - Maximum z/OS system's SMF interval is 60 minutes

- Who (Audience)
  - Network Security Administrator

- What (Solution)
  - Support to configure larger recording intervals that is not associated with the z/OS system's SMF interval which allows for less frequent generation of zERT Summary SMF 119-12 records

- Wow (Benefit / Value, Need Addressed)
  - Dramatically reduce the number of zERT SMF 119-12 records
  - Improves the associated overhead and elapsed time when using zERT Network Analyzer for storing (importing) and querying the data using Db2
  - Reduced number of records still provides the same level of cryptographically significant information

Usage & Invocation

- In the TCP/IP Profile

- New sub-parameter INTVAL for the AGGREGATION sub-parameter to specify the interval zERT Aggregation will generate SMF 119-12 (zERT Summary) records:

  AGGREGATION INTVAL SMF | intval

  Example: GLOBALCONFIG ZERT AGGREGATION INTVAL 12
  Default value: SMF

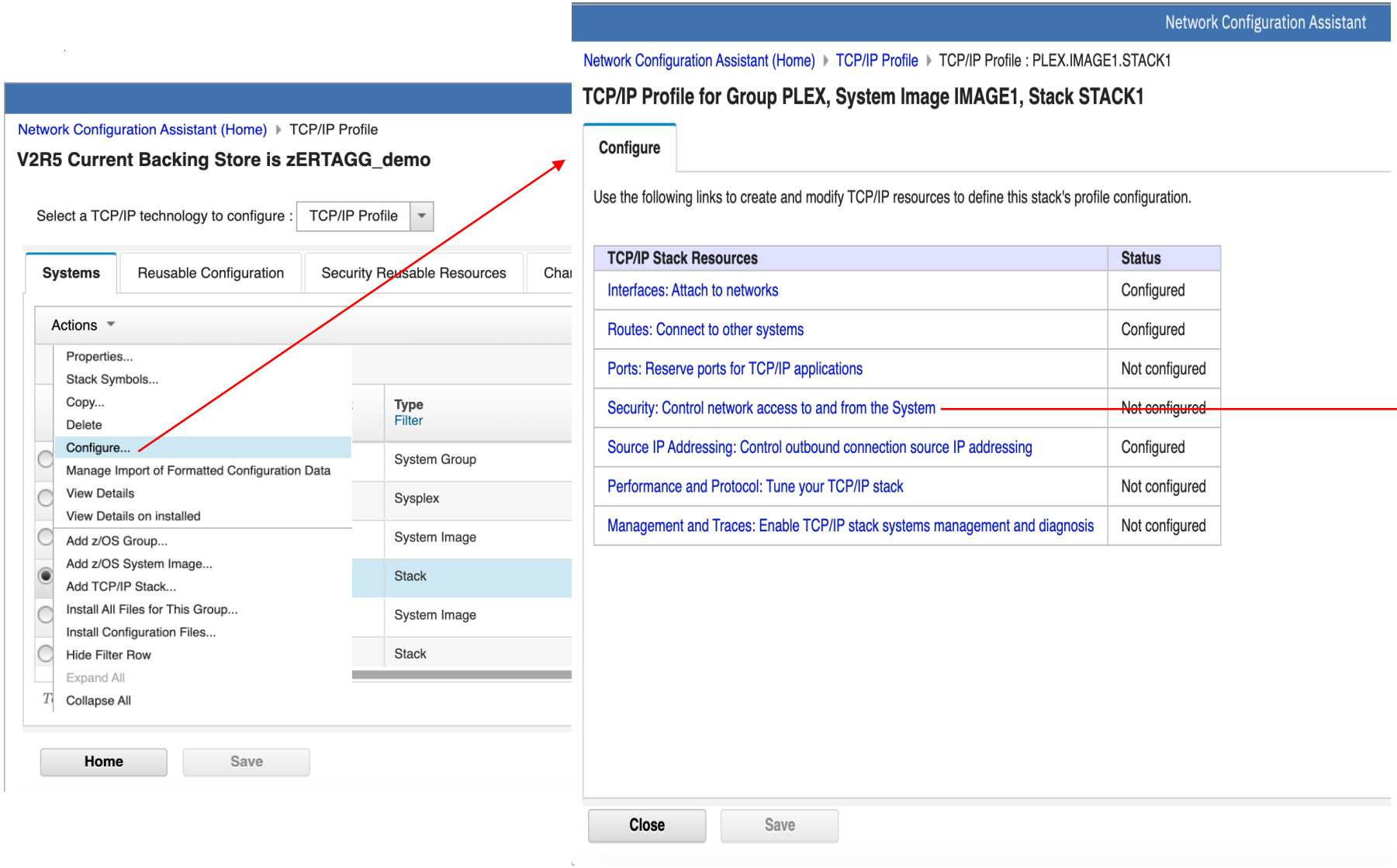
- New sub-parameter SYNCVAL for new INTVAL sub-parameter to indicate a reference time for which zERT Summary records will be recorded:

  INTVAL intval SYNCVAL hh:mm

  Example: INTVAL 4 SYNCVAL 08:00
  Default value: 00:00 (midnight)

- Support also provided for z/OS V2R3 and V2R4 (in 2Q 2020) with APAR PH25049 and NCA APAR PH24543

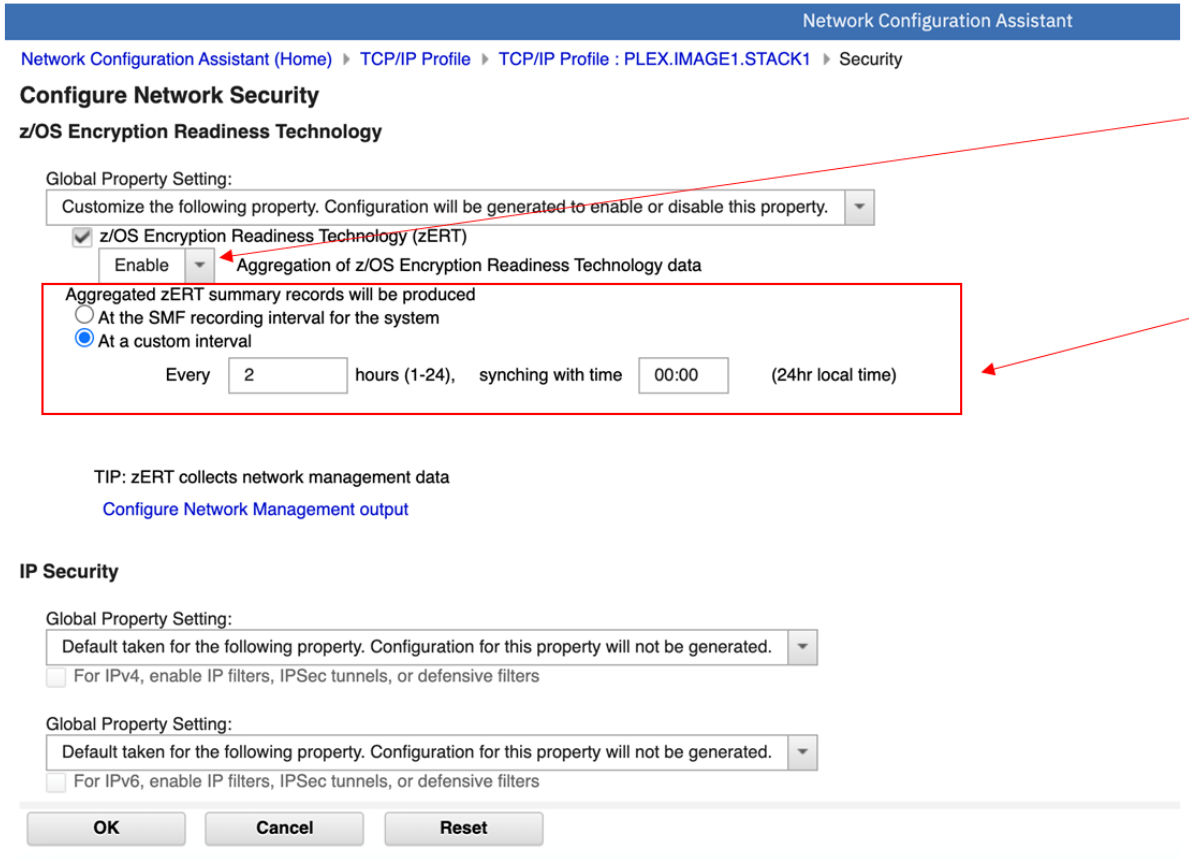
Usage & Invocation - NCA



Next slide

Usage & Invocation – NCA continued

zERT settings



zERT Aggregation must be enabled to use this function

Customize the zERT aggregation interval here.

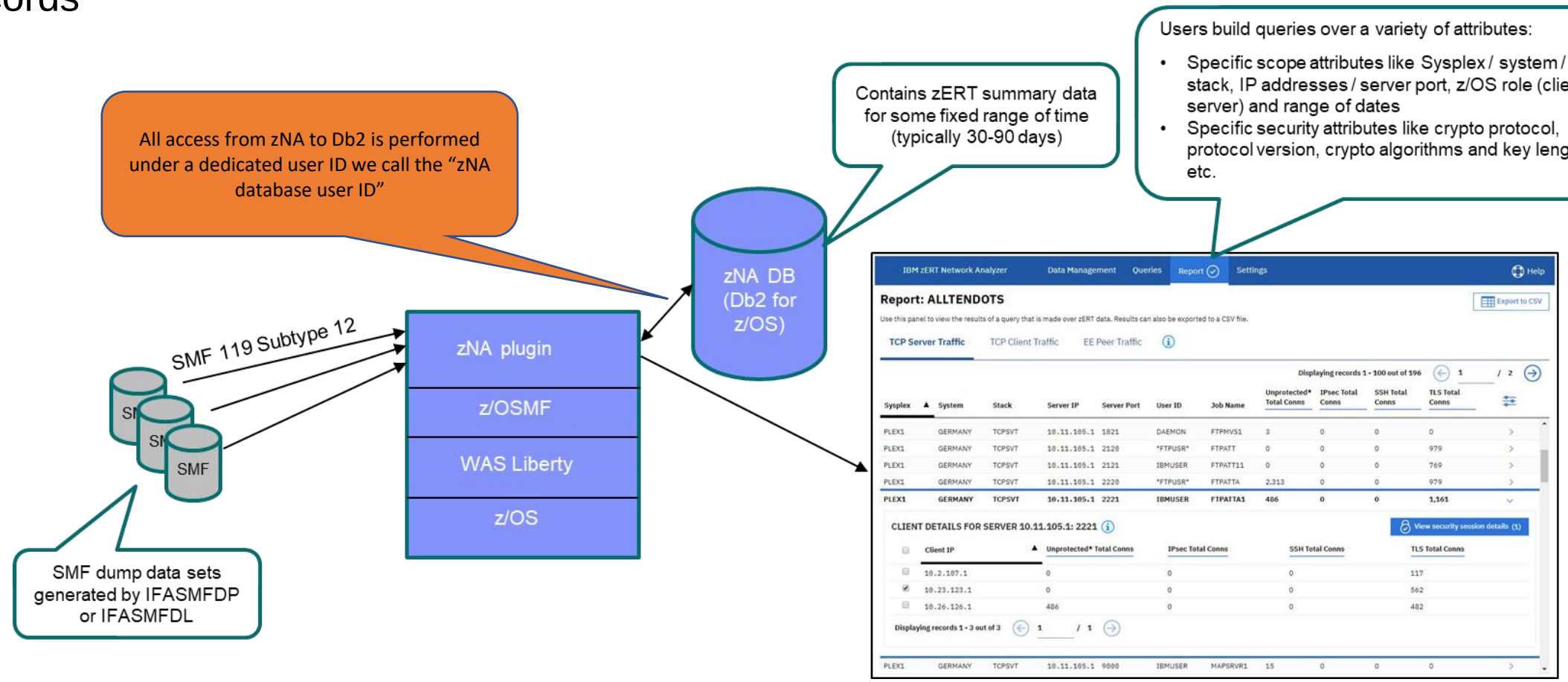
Interactions, Dependencies, Upgrade & Installation

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies: None
- Hardware Dependencies: None
- Exploiters: None
- Installation: None

zERT Network Analyzer database administration enhancements

Overview

- Background
  - z/OSMF plug-in using Db2 for z/OS to store and query data from SMF 119-12 (zERT Summary) records



Overview

- Background continued
  - Database schema consisted of a set of statically defined tables (through supplied templates) to store the persistent data imported from the SMF 119-12 (zERT Summary) records
  - zERT Network Analyzer also dynamically creates up to 17 database tables to temporarily store query results that only needs to persist across several transactions
    - Allows for a subset of potentially large query results to be sent to client UI while providing ability to sort across entire result set
  - Dynamically creating database tables requires executing Data Definition Language (DDL) commands which privileges are generally reserved for database administrators only
    - CREATE, ALTER, DROP
  - Applications are generally granted authority to execute Data Manipulation Language (DML) commands
    - SELECT, INSERT, UPDATE, MERGE

Overview

- Who (Audience)
  - Database administrator, z/OS Network security administrator
- What (Solution)
  - Statically pre-defined set of partition-by-range query result tables (though newly supplied database schema templates)
  - Introduced new set of “aliasing” database schema templates providing more flexibility with the naming conventions for various database schema definitions
  - Provided guidance on upgrading zERT Network Analyzer to a new z/OS release
- Wow (Benefit / Value, Need Addressed)
  - Reduced the database privileges required by zERT Network Analyzer to operate to no longer require the execution of any DDL commands
  - Provide additional flexibility in how database schema definitions are named allowing customers to utilize zERT Network Analyzer while adhering to their individual corporate naming conventions

Usage & Invocation

- New/updated database schema templates
  - Updated:
    - IZUZNADT – Added definitions for partition-by-range tables to store query results
  - New:
    - IZUZNADA – Same as IZUZNADT template but with enhanced flexibility for naming database schema definitions
    - IZUZNAPT – Template to alter the number of partition-by-range tables defined
    - IZUZNAPA – Same as IZUZNAPT but with enhanced flexibility for naming database schema definitions
  - Support available with APAR PH24492 for z/OS V2R3 and APAR PH24494 for z/OS V2R4

Interactions, Dependencies, Upgrade & Installation

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level: No
- Software Dependencies: None
- Hardware Dependencies: None
- Exploiters: None
- Upgrade considerations:
  - Follow steps in z/OS Upgrade Workflow to configure new database schema for z/OS V2R5
- Installation: None

Notification of Availability of TCP/IP Extended Services

Overview – TCP/IP complete initialization

- Background
  - Existing automation needs to rely on multiple messages to determine when TCP/IP and its extended services have completed initialization
    - Examples

```
EZZ4202I Z/OS UNIX - TCP/IP CONNECTION ESTABLISHED FOR TCPIP
EZB6473I TCP/IP STACK FUNCTIONS INITIALIZATION COMPLETE.
EZAIN11I ALL TCPIP SERVICES FOR PROC TCPIP ARE AVAILABLE.
```

- Who (Audience)
  - Systems programmer
  - Application developer

Overview – TCP/IP complete initialization

- What (Solution)
  - The following new notifications will indicate that TCP/IP and its required services (determined by user configuration) are initialized:
    - New console messages
      - TCP/IP and extended services have been fully initialized

```
EZD1314I TCP/IP AND EXTENDED SERVICES ARE NOW INITIALIZED
FOR STACK: tcpstackname
```

      - Delete Operator messages (DOM) to indicate required extended services have not initialized yet

```
EZD1315E NOTIFICATION OF TCP/IP EXTENDED SERVICES AVAILABILITY
IS DELAYED FOR tcpstackname DUE TO extended_service
```

        - extended_service could be one of the following:
          - SYSPLEX – The TCP/IP stack not in sysplex group and/or DVIPA profile definitions not completed processing (VIPADYNAMIC etc)
          - PAGENT – Policy Agent not completed installation of policy
          - IPSEC INFRASTRUCTURE – IKED heartbeat not detected

Overview – TCP/IP complete initialization

- What (Solution) continued
  - New Event Notification Facility (ENF) signal
  - New Name/Token Pair

- Wow (Benefit / Value, Need Addressed)
  - Provides automation more reliable message to indicate all necessary services are fully initialized
  - A software developer can programmatically determine when TCP/IP and its required services have fully initialized

Usage & Invocation - TCP/IP complete initialization

- In the TCP/IP Profile

- New parameter on GLOBALCONFIG statement to indicate to wait for policies to be installed from the Policy Agent before sending notification:
  POLICYREQUIRED YESIFTTLS | YES | NO

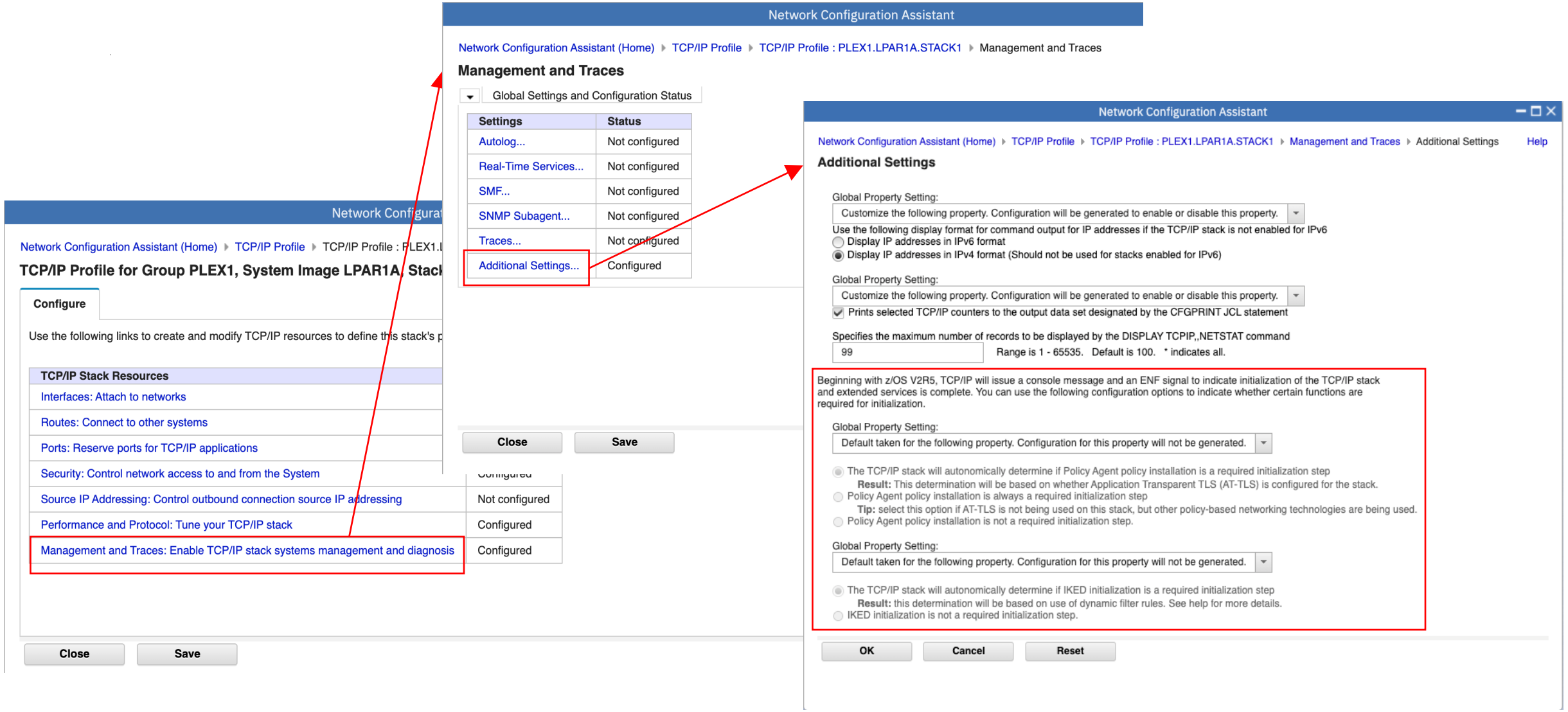
  Example: POLICYREQUIRED NO
  Default Value: YESIFTTLS

- New parameter on GLOBALCONFIG statement to indicate to wait for IPSec infrastructure (IKED) to be initialized before sending notification:
  IKEDREQUIRED YESIFDYNIPSEC | NO

  Example: IKEDREQUIRED NO
  Default value: YESIFDYNIPSEC

- Default values should be sufficient for most environments

Usage & Invocation – Network Configuration Assistant (continued)



Usage & Invocation – ENF signal

- Create an ENF 80 exit in order to listen for the new signal when the TCP/IP stack and its extended services have initialized

- To listen for ENF event code 80, specify the qualifying events (x'20000000') on the QUAL parameter

  Example: ENFREQ ACTION=LISTEN
  CODE(80)
  QUAL(X'20000000')

- The ENF signal contains
  - Flag bits representing the TCP/IP stack and extended services being fully initialized
  - The job name of the TCPIP stack that initialized

Usage & Invocation – Name/Token Pair

- Create a Name/Token Pair query using IEAN4RT or IEANTRT to check if the TCP/IP stack and extended services have initialized
- The generated Name/Token Pair is 16 bytes where the leftmost 8 bytes is a constant (EZBSTKUP) and the rightmost 8 bytes is the TCP/IP stack jobname

Example: (Assume TCP/IP jobname is TCPIP)

```
          LOAD EP=IEANTRT
          LR R15,R0
          Call (15),(LEVEL,NAME,TOKEN,RETCODE)
          LA R15,IEANT_OK              Get successful retcode value
          C R15,RETCODE                Was TOKEN Returned?
          BE STOPENF                   Yes, Stop ENF Listen
          EJECT
LEVEL     DC A(IEANT_SYSTEM_LEVEL)     SYSTEM LEVEL
NAME      DC CL16'EZBSTKUPTCPIP    '   Name for Name/Token pair
TOKEN     DS XL16                      Token for Name/Token Pair
RETCODE   DS F                         Return code from IEANTRT
```

- The Token value is IBM reserved for future use

Overview – TCP/IP availability for PAGENT

- Background
  - Prior to V2R5, Policy Agent utilized a registered file in the /tmp directory to detect when a TCP/IP stack was restarted and needed policies installed.
  - Registration of the file failed if the /tmp directory was located in a read/write sysplex-aware zFS file system.
  - It was necessary to create a symbolic link to a file in a z/OS UNIX file system or in a read-only zFS file system.
- Who (Audience)
  - Systems programmer
- What (Solution)
  - New mechanism is implemented for Policy Agent to detect when a TCP/IP stack is restarted.
- Wow (Benefit / Value, Need Addressed)
  - Provides reliable notification for Policy Agent in all scenarios/environments

Usage & Invocation - TCP/IP availability for PAGENT

- N/A – internal use only

Interactions, Dependencies, Upgrade & Installation

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level: No
- Software Dependencies: None
- Hardware Dependencies: None
- Exploiters: None
- Installation: None

Sysplex Autonomics for IPsec

Overview

- Background
  - Sysplex autonomics includes monitoring system health indicators such as:
    - Program execution time and storage usage
    - Abends
    - Availability of key network functions, such as OMPROUTE and VTAM
  - Stack could delay joining a sysplex group if conditions not met
  - Stack monitors resources and can leave the sysplex group if a problem is detected
  - For customers that have significant IPsec-protected sysplex workloads, the IPsec components are an essential requirement (critical resource) in the health of the TCP/IP stack. For example, if IKED is not available, it can impact the ability to send traffic for the sysplex distributor workload.

Overview

- Who (Audience)
  - Systems programmer, Network security administrator

- What (Solution)
  - Sysplex autonomics enhanced to monitor the health of the IPsec infrastructure
    - Includes Policy Agent, Internet Key Exchange (IKE) Daemon, and the Network Security Server (NSS) Daemon

- Wow (Benefit / Value, Need Addressed)
  - Alleviates the need for customers to implement automation in their environment to monitor and ensure the IPsec infrastructure is active and operational for a stack in the sysplex

Usage & Invocation

- In the TCP/IP Profile

- New parameter on SYSPLEXMONITOR statement to enable IPsec monitoring :
  SYSPLEXMONITOR DELAYJOINIPSEC | NODELAYJOINIPSEC

  Example SYSPLEXMONITOR DELAYJOINIPSEC
  Default value: NODELAYJOINIPSEC

- New sub-parameter on the DELAYJOINIPSEC parameter to control whether the IPsec infrastructure is monitored after the stack joins the sysplex:
  DELAYJOINIPSEC MONIPSEC | NOMONIPSEC

  Example: DELAYJOINIPSEC NOMONIPSEC
  Default Value: MONIPSEC

- Support available on z/OS V2R4 with APAR PH12788

Interactions, Dependencies, Upgrade & Installation

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level: No
- Software Dependencies: None
- Hardware Dependencies: None
- Exploiters: None
- Installation: None

Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions

Overview

- Who (Audience)
  - z/OS network administrators
- What (Solution)
  - With OSA-Express6S, inbound traffic separation for z/CX traffic is supported using a new ancillary input queue
- Wow (Benefit / Value, Need Addressed)
  - Finer tuning of read-side interrupt frequency to match the latency demands of the various workloads that are serviced
  - Improved multiprocessor scalability, because the multiple OSA-Express input queues are now efficiently serviced in parallel

Usage & Invocation

- No additional action required to enable IWQ for zCX
  - Existing WORKLOADQ parameter on the INTERFACE statements enables IWQ for all supported traffic types

- Support also provided for z/OS V2R4 (in 4Q 2019) with APARs PH16581 and OA58300

Interactions & Dependencies

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies: None
- Hardware Dependencies
    - OSA-Express6S or above
    - See the 3906DEVICE or 3907DEVICE Preventive Service Planning (PSP) bucket
- Exploiters: None

Upgrade & Coexistence Considerations

- Upgrade
  - If you have enabled QDIO inbound workload queuing (WORKLOADQ) and you have zCX traffic, the IWQ zCX function (input queue) will automatically be enabled
  - Each Ancillary Input Queue increases storage utilization in the following two areas:
    - Approximately 36 KB of fixed ECSA and
    - 4MB of fixed CSM HVCOMMON for READSTORAGE
  - The new input queue will not be used (and will not be backed by 4MB of storage) until the first zCX dynamic VIPA is activated
  - There are no configuration options for controlling each input queue type

Installation & Configuration

- Planning considerations
  - Verify that sufficient ECSA is available
  - Verify that sufficient real (fixed) storage is available
    - See z/OS Migration book for details
  - IWQ is not supported:
    - for DEVICE/LINK definitions
    - when z/OS is running as a z/VM guest with simulated devices (VSWITCH or guest LAN)

SMTPD compatibility enhancements for CSSMTP

Overview - CSSMTP default MAIL FROM parametrization

- Who (Audience)
  - System administrators

- What (Solution)
  - CSSMTP can define a default mail sender to be used in the MAIL FROM field

- Wow (Benefit / Value, Need Addressed)
  - Mitigates restriction of Microsoft Exchange Server requiring the MAIL FROM field to be specified for mail to be accepted and delivered
  - CSSMTP error reports can be sent to mail administrator even when the MAIL FROM field in the original mail is blank

Usage & Invocation - CSSMTP default MAIL FROM parametrization

- In the CSSMTP configuration file

- New statement: ReportMailFrom *mailbox*

  Example: ReportMailFrom user@company.com

  No default value

- Support also provided for z/OS V2R3 and V2R4 (in 4Q 2019) with APAR PH18237

Overview - CSSMTP SYSOUT class specification for error reports

- Who (Audience)
  - System administrators

- What (Solution)
  - CSSMTP can specify SYSOUT class for generated error reports to be sent

- Wow (Benefit / Value, Need Addressed)
  - Mitigates limitation of only sending error report to SYSOUT class of originating invalid spool file when Report SYSOUT was specified in CSSMTP configuration file

Usage & Invocation - CSSMTP SYSOUT class specification for error reports

- In the CSSMTP configuration file

- New statement: ReportSysoutClass *SysoutClass*

  Example: ReportSysoutClass B

  No default value

- Support also provided for z/OS V2R3 and V2R4 (in 4Q 2019) with APAR PH18237

Overview - Support of 256 characters long usernames in CSSMTP

- Who (Audience)
  - System administrators

- What (Solution)
  - CSSMTP supports email addresses with username up to 256 characters in length

- Wow (Benefit / Value, Need Addressed)
  - Improved compatibility with SMTPD which allow usernames up to 256 characters in length

Usage & Invocation - Support of 256 characters long usernames in CSSMTP

- In the CSSMTP configuration file

- New statement: MailBoxCompatibility Standard | Long

  Example: MailBoxCompatibility Long

  Default value: Standard

- Support also provided for z/OS V2R3 and V2R4 (in 4Q 2019) with APAR PH18237

Interactions, Dependencies, Upgrade & Installation

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level: No
- Software Dependencies: None
- Hardware Dependencies: None
- Exploiters: None
- Installation: None

Support considerations for z/OS V2.5:

- Ping output enhanced to provide microsecond precision

Overview

- Who (Audience)
  - Network Administrator

- What (Solution)
  - Ping response time provides additional millisecond display with microsecond precision

- Wow (Benefit / Value, Need Addressed)
  - Display accurate diagnostic data for low latency traffic (for instance localhost)

Usage & Invocation

- Existing ping command – no syntax changes
- Example: ping 127.0.0.1

```
# ping 127.0.0.1
CS V2R5: Pinging host 127.0.0.1
Ping #1 response took 0.000 seconds. (0.207 milliseconds)
```

- Verbose example: ping –v 127.0.0.1

```
# ping -v 127.0.0.1
CS V2R5: Pinging host 127.0.0.1
with 256 bytes of ICMP data
Ping #1 from 127.0.0.1: bytes=264 seq=1 ttl=64 time=0.202 ms
Ping #2 from 127.0.0.1: bytes=264 seq=2 ttl=64 time=0.092 ms
Ping #3 from 127.0.0.1: bytes=264 seq=3 ttl=64 time=0.098 ms
Ping statistics for 127.0.0.1
  Packets: Sent=3, Received=3, Lost=0 (0% loss)
  Approximate round trip times in milliseconds:
   Minimum=0.092 ms, Maximum=0.202 ms, Average=0.131 ms, StdDev=0.062 ms
```

Interactions, Dependencies, Upgrade & Installation

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies: None
- Hardware Dependencies: None
- Exploiters: None
- Installation: None

Support considerations for z/OS V2.5:

- Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS

Overview - DCAS

- Who (Audience)
  - Systems programmer

- What (Solution)
  - Remove native TLS/SSL support from DCAS
  - DCAS server migration health check
    - ZOSMIGV2R4_NEXT_CS_DCAS_NTVSSL
    - Available on z/OS V2R3 and V2R4 with APARs PH16144 and OA58255
    - By default, the health check will be INACTIVE
    - ISTM043I message – indicates DCAS profile is not configured with TLSMECHANISM DCAS
    - ISTM044E message – indicates DCAS profile is configured with TLSMECHANISM DCAS
      - Generated report will contain table updated with the identified server's jobname as ASID

- Wow (Benefit / Value, Need Addressed)
  - Fulfillment of Statement of Direction

Usage & Invocation - DCAS

- The following DCAS configuration statements are no longer supported:
  - KEYRING
  - LDAPPORT
  - LDAPSERVER
  - SAFKEYRING
  - STASHFILE
  - TLSV1ONLY
  - V3CIPHER
- The following DCAS configuration parameter is no longer supported:
  - TLSMECHANISM DCAS
- For DCAS, if TLSMECHANISM is not specified the default is taken
  - Prior to V2R5, the default was TLSMECHANISM DCAS
  - In V2R5 the default is now TLSMECHANISM ATTLS

Overview – TN3270E Telnet server

- Who (Audience)
  - Systems Programmer

- What (Solution)
  - Remove native TLS/SSL support from TN3270E Telnet server
  - TN3270 server migration health check
    - ZOSMIGV2R4_NEXT_CS_TN3270_NTVSSL
    - Available on z/OS V2R3 and V2R4 with APARs PH16144 and OA58255
    - By default, the health check will be inactive
    - ISTM041I message – indicates TN3270 server profile is not configured with SECUREPORT
    - ISTM042E message – indicates at least one TN3270 server profile is configured with SECUREPORT
      - Generated report will contain table updated with the identified server's jobname as ASID

- Wow (Benefit / Value, Need Addressed)
  - Fulfillment of Statement of Direction

Usage & Invocation - TN3270E Telnet server

- The following TN3270 profile statements are no longer supported:
  - SECUREPORT
  - CLIENTAUTH
  - CRLLDAPSERVER
  - ENCRYPTION
  - KEYRING
  - SSLV2 and NOSSLV2
  - SSLV3 and NOSSLV3
  - SSLTIMEOUT

- In addition, the PARMSGROUP and PARMSMAP statements will no longer support mapping security parameters to connections based on client hostname.

Overview – FTP server

- Who (Audience)
  - Systems Programmer

- What (Solution)
  - Remove native TLS/SSL support from FTP server
  - FTP server migration health check
    - ZOSMIGV2R4_NEXT_CS_FTPSRV_NTVSSL
    - Available on z/OS V2R3 and V2R4 with APARs PH21573 and OA59022
    - By default, the health check will be INACTIVE
    - ISTM045I message – indicates FTP server profile is not configured with TLSMECHANISM FTP and EXTENSIONS AUTH_TLS
    - ISTM046E message – indicates at least one FTP server profile is configured with TLSMECHANISM FTP and EXTENSIONS AUTH_TLS
      - Generated report will contain table updated with the identified server's jobname as ASID

- Wow (Benefit / Value, Need Addressed)
  - Fulfillment of Statement of Direction

Usage & Invocation – FTP server

- The following FTP.DATA configuration statements are no longer supported:
  - KEYRING
  - CIPHERSUITE
  - SSLV3
  - TLSTIMEOUT

- The following FTP.DATA configuration parameter is no longer supported for FTP server:
  - TLSMECHANISM FTP
  - TLSRFCLEVEL CCCNONOTIFY (more details in next section)

- For FTP server, if TLSMECHANISM is not specified the default is taken
  - Prior to V2R5, the default was TLSMECHANISM FTP
  - In V2R5 the default is now TLSMECHANISM ATTLS

- NOTE: Native TLS/SSL support for the FTP client remains unchanged. Both AT-TLS and native TLS/SSL are supported

Overview – FTP, CCCNONOTIFY and AT-TLS

- Background - TLSRFCLEVEL
  - The Clear Command Channel (CCC) subcommand is sent by an FTP client to request that the FTP server change the transmission mode in a control connection from encrypted mode to clear text mode

  - Both the FTP client and the FTP server utilize the TLSRFCLEVEL statement in their configuration to specify the RFC level which FTP supports for securing FTP with TLS. The three possible parameters are:
    - TLSRFCLEVEL DRAFT (Default)
      - CCC command is not supported
    - TLSRFCLEVEL RFC4217
      - CCC command causes the FTP server to shutdown the secure connection using TLSshutdown alert
    - TLSRFCLEVEL CCCNONOTIFY
      - CCC command causes the FTP server to “set aside” the security connection (TLSshutdown alert NOT issued)

Overview – FTP, CCCNONOTIFY and AT-TLS

- Background - CCCNONOTIFY and AT-TLS
  - When AT-TLS is used for an FTP server or client, TLSRFCLEVEL CCCNONOTIFY is not valid
    - Results are unexpected as there is no mechanism for AT-TLS to “set aside” the secure connection and begin sending data in the clear over the control connection based on the receipt of the CCC subcommand
    - IP Configuration Reference warns that configuration of TLSRFCLEVEL CCCNONOTIFY with AT-TLS is not valid
  - Prior to V2R5, CCCNONOTIFY configuration allowed

Overview – FTP, CCCNONOTIFY and AT-TLS

- Who (Audience)
  - Systems Programmer

- What (Solution)
  - Enforce configuration restriction that CCCNONOTIFY is not supported with AT-TLS
  - FTP server migration health check for TLSRFCLEVEL CCCNONOTIFY
    - ZOSMIGV2R4_NEXT_CS_FTPSRV_RFCLVL
    - Available on z/OS V2R3 and V2R4 with APARs PH24732 and OA59490
    - By default, the health check will be inactive
    - ISTM047I message – indicates no active FTP server profile is not configured with TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS, and EXTENSIONS AUTH_TLS
    - ISTM048E message – indicates at least one active FTP server profile is configured with TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS, and EXTENSIONS AUTH_TLS
      - Generated report will contain table updated with the identified FTP server's jobname as ASID

Overview – FTP, CCCNONOTIFY and AT-TLS

- What (Solution) continued
  - FTP client migration health check for TLSRFCLEVEL CCCNONOTIFY
    - ZOSMIGV2R4_NEXT_CS_FTPCLI_RFCLVL
    - Available on z/OS V2R3 and V2R4 with APARs PH24732 and OA59490
    - By default, the health check will be inactive
    - When active, the health check is done every “configured interval”
      - When an FTP client with TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS, and SECURE_MECHANISM TLS is identified:
        - Health check report will indicate message ISTM050E
          - ISTM050E also written to the console when the interval is processed
        - Syslogd message EZYFT79I issued to identify the FTP client’s userid, jobname, and local site configuration
        - FTP client debug message issued to job log when DEBUG PAR enabled
      - When no FTP client during the current IPL has been identified with the combination of TLSRFCLEVEL CCCNONOTIFY, TLSMECHANISM ATTLS, and SECURE_MECHANISM TLS:
        - Health check report will indicate message ISTM049I

Overview – FTP, CCCNONOTIFY and AT-TLS

- Wow (Benefit / Value, Need Addressed)
  - Fulfillment of Statement of Direction

Usage & Invocation – FTP, CCCNONOTIFY and AT-TLS

- N/A

Interactions, Dependencies, Upgrade & Installation

- Upgrade considerations:
  - DCAS
    - Use DCAS server migration health checks to determine if TLSMECHANISM DCAS is configured
    - Must migrate DCAS using native TLS/SSL to AT-TLS by z/OS V2R5
    - See "Migrating the DCAS server to use AT-TLS policies" in z/OS Communications Server: IP Configuration Guide for more information.

  - TN3270E Telnet server
    - Use TN3270 server migration health checks to determine If SECUREPORT is configured
    - Must migrate TN3270 servers using native TLS/SSL to AT-TLS by V2R5
      - In addition, the PARMSGROUP and PARMSMAP statements will no longer support mapping security parameters to connections based on client hostname.
    - See "Converting Telnet profile statements to equivalent AT-TLS policy statements" in z/OS Communications Server: IP Configuration Guide for more information.

Interactions, Dependencies, Upgrade & Installation

- Upgrade considerations continued:
  - FTP server
    - Use FTP server migration health checks to determine if TLSMECHANISM FTP and EXTENSIONS AUTH_TLS is configured
    - Must migrate FTP servers using native TLS/SSL to AT-TLS by V2R5
    - See "Steps for migrating the FTP server and client to use AT-TLS" in the IP Configuration Guide for additional information.
  - FTP client and server
    - The configuration for FTP servers and clients using TLSRFCLEVEL CCCNONOTIFY with AT-TLS should be updated to TLSRFCLEVEL RFC4217 or TLSRFCLEVEL DRAFT by V2R5
      - If AT-TLS and TLSRFCLEVEL CCCNONOTIFY are configured, CCCNONOTIFY is rejected and TLSRFCLEVEL is set to the default level of “DRAFT”

Support considerations for z/OS V2.5:

- Removal of support for load balancing to Data Power
- Removal of Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB)
- Removal of CMIP from VTAM
- Removal of support for NCA policy import

Overview

- Who (Audience)
  - System Programmer

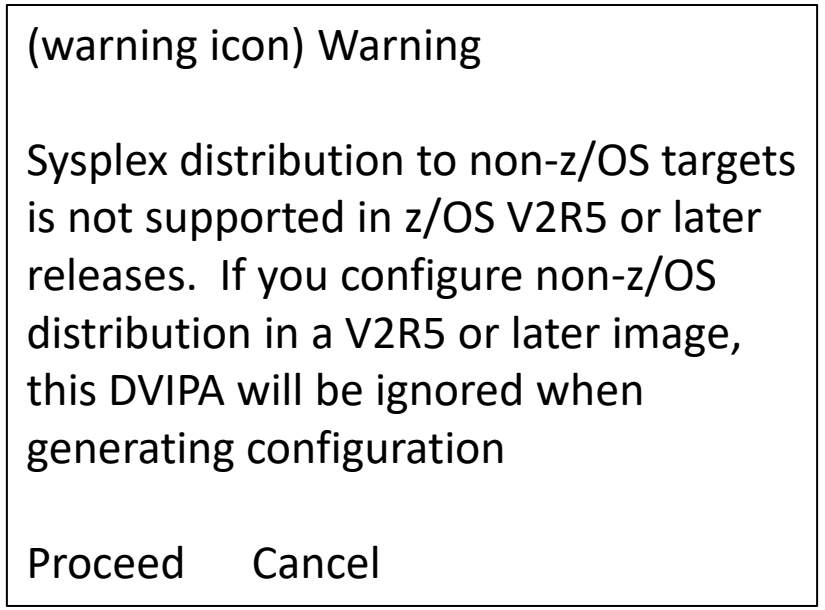
- What (Solution)
  - Remove support of workload balancing to DataPower® Gateway
  - Remove Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB)
  - Removed CMIP from VTAM
  - Removed Import Policy Data option from Actions menu in associated technology perspectives

- Wow (Benefit / Value, Need Addressed)
  - Fulfillment of Statement of Direction

Usage & Invocation

- Removal of support for load balancing to Data Power
  - The following parameters of the VIPADISTRIBUTE statement in the TCPIP profile is no longer valid:
    - GRE
    - ENCAP
    - DISTMETHOD
    - TARGCONTROLLED
    - CONTROLPORT

  - NCA Support
    - NCA can generate TCP/IP profiles for n-2 down-level systems
    - Therefore, the parameters will not be removed from the panels
    - However, NCA will not generate configuration for stack-managed DVIPAs that use the invalid parameters in TCP/IP profiles for stacks that run on images at z/OS V2R5 or later
    - Starting in z/OS V2R5, the following pop-up warning appears when selecting or modifying a non-z/OS distribution DVIPA



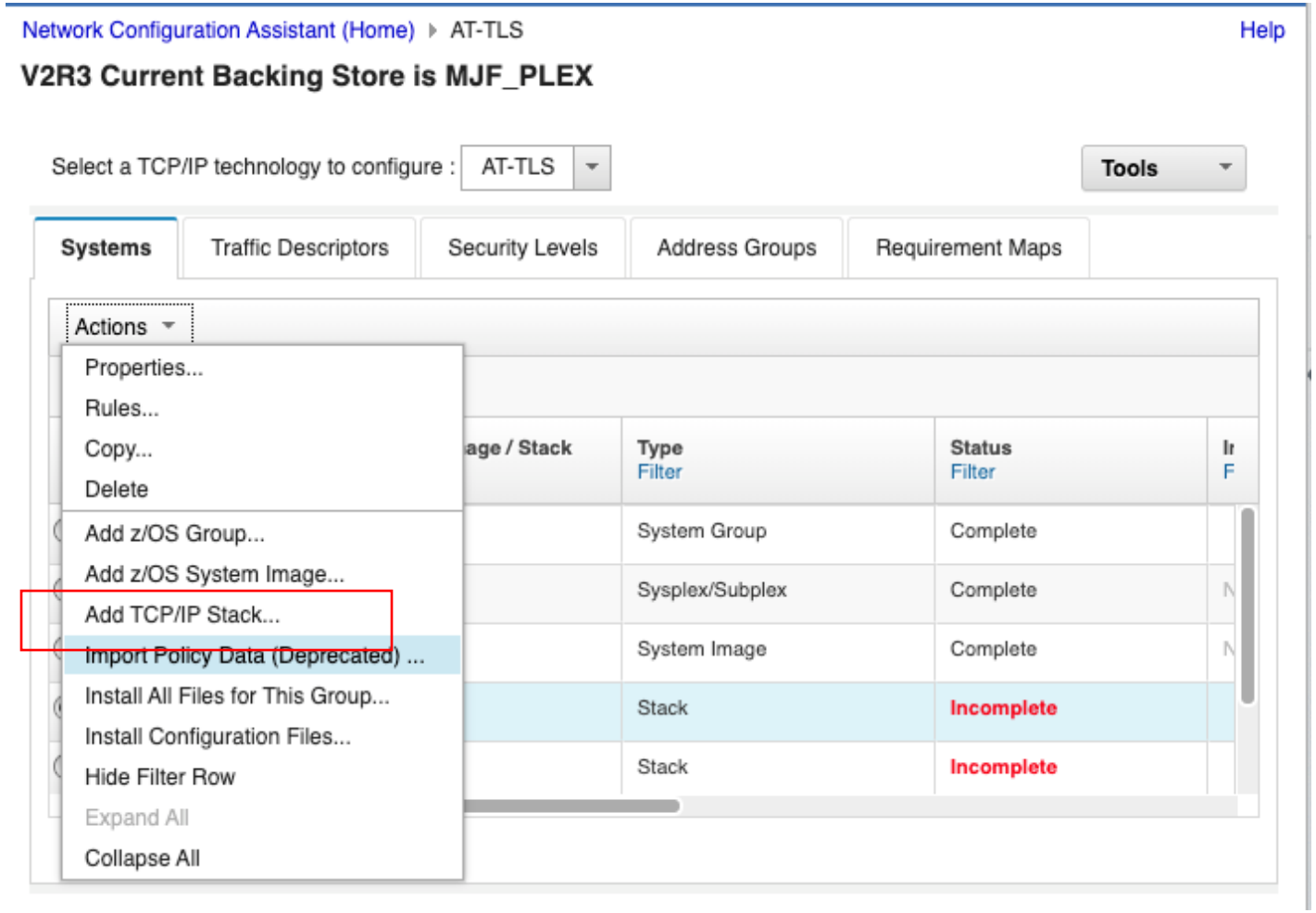
Usage & Invocation

- Removal of Sysplex Distributor support for Cisco Multi-Node Load Balancing (MNLB)
  - The SERVICEMGR parameter of the VIPADEFINE statement in the TCPIP profile will be ignored
    - Warning message will be issued on console during configuration processing
    - VIPASMPARMS configuration has no impact without SERVICEMGR
    - Prevents configuration bits from being passed down to externals (netstat, export profile, and NMI)

- Removal of CMIP from VTAM
  - The following VTAM start options are no longer valid:
    - OSIMGMT
    - OSIEVENT
    - OSITOPO
    - UPDDELAY

Usage & Invocation

- Removal of support for NCA policy import
  - The following “Import Policy Data (Deprecated)” option is no longer available



Upgrade planning considerations

- Removal of support for load balancing to Data Power
  - Verify none of the parameters are specified on the VIPADISTRIBUTE statement
  - If relying on an out of support DataPower Gateway target for load balancing consider implementing another solution for workload balancing that might be through an external load balancer as outlined in the Statement of Direction.

- Removal CMIP from VTAM
  - VTAM Migration Health Check of OSIMGMT function detects if CMIP is configured
    - ZOSMIGV2R4_Next_CS_OSIMGMT
    - Detected the use of OSIMGMT function
    - Available for z/OS V2R2 and V2R3 with APAR OA57227
    - Available in base of z/OS V2R4
  - If utilizing CMIP services today, consider using SNA network monitoring network management interface (NMI) as outlined in the Statement of Direction

Upgrade planning considerations

- Removal of support for NCA policy import
  - Policy import has been deprecated since z/OS V2R2
  - Customers who want to import policy data need to do so on z/OS V2R4 or earlier systems, but they need to understand that it will only import at the V2R2 level
  - Anything added since z/OS V2R2, like TLS 1.3 support, will not be imported
  - TCP/IP profile import is not affected and continues to be fully supported with regular updates as new parameters are added to the TCP/IP profile
    - This removal only applies to policy data import

Interactions, Dependencies, & Installation

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies: None
- Hardware Dependencies: None
- Exploiters: None
- Installation: None

Summary

- Security
  - AT-TLS currency with System SSL
  - AT-TLS and IPsec certificate diagnostics
  - IPsec certificate reporting enhancements
  - Sysplex Autonomics for IPsec
  - z/OS Encryption Readiness Technology (zERT) policy-based enforcement
  - zERT Network Analyzer database administration enhancements
  - Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
- Usability and skills
  - Removal of support for load balancing to Data Power
  - Removal of Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB)
  - Removal of CMIP from VTAM
  - Removal of support for NCA policy import
- Systems management
  - Notification of Availability of TCP/IP Extended Services
  - Ping output enhanced to provide microsecond precision
- Scalability and Performance
  - zERT Aggregation recording interval
  - Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions
- Application enhancement
  - SMTPD compatibility enhancements for CSSMTP
- Hardware
  - Shared Memory Communications multiple subnet support (SMCv2)

Appendix 1 of 3

Statement of Direction for V2.5: zERT policy-based enforcement (Issued March 2, 2021)

In the future, IBM intends to extend zERT to support policy-based rules that describe different levels of cryptographic protection along with optional actions to take when TCP connections match those rules. Since z/OS V2.3, zERT has provided a detailed view of the cryptographic protection attributes used on connections that terminate on the z/OS TCP/IP stack. The zERT policy-based enforcement feature would enable immediate notification through messages, auditing through SMF records, and even automatic connection termination when questionable or unacceptable cryptographic protection is used. IBM plans to enable z/OS network security administrators to create and manage zERT enforcement rules and actions through the z/OSMF Network Configuration Assistant and the z/OS Communications Server policy agent.

Appendix 2 of 3

z/OS Communications Server Publications

- z/OS Communications Server: IP and SNA Codes SC27-3648
- z/OS Communications Server: IP CICS Sockets Guide SC27-3649
- z/OS Communications Server: IP Configuration Guide SC27-3650
- z/OS Communications Server: IP Configuration Reference SC27-3651
- z/OS Communications Server: IP Diagnosis Guide GC27-3652
- z/OS Communications Server: IP IMS Sockets Guide SC27-3653
- z/OS Communications Server: IP Programmer's Guide and Reference SC31-8787
- z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference SC27-3660
- z/OS Communications Server: IP System Administrator's Commands SC31-8781
- z/OS Communications Server: IP User's Guide and Commands SC27-3662
- z/OS Communications Server: IPv6 Network and Application Design Guide SC27-3663
- z/OS Communications Server: New Function Summary GC31-8771
- z/OS Communications Server: SNA Network Implementation Guide SC27-3672
- z/OS Communications Server: SNA Operation SC31-8779
- z/OS Communications Server: SNA Resource Definition Reference SC27-3675

Appendix 3 of 3

- Other Publications
  - z/OS UNIX System Services Programming: Assembler Callable Services Reference SA23-2281
  - z/OS XL C/C++ Runtime Library Reference SC14-7314
  - z/OS Unicode Services User's Guide and Reference SA38-0680