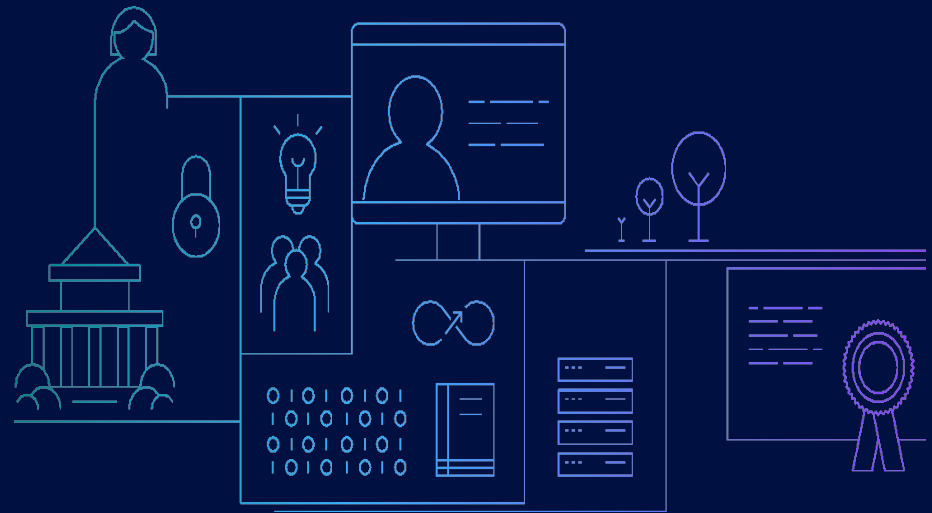


z/OS Communications Server

Technical Update: z/OS V2R5 Edition

—
Mike Fitzpatrick - mfitz@us.ibm.com
Sam Reynolds - samr@us.ibm.com

October 26, 2021



Agenda

- z/OS Encryption Readiness Technology (zERT)
- IPsec certificate reporting enhancements
- AT-TLS and IPsec certificate diagnostics
- Shared Memory Communications Version 2 (SMCv2)
- TCP/IP startup message and ENF notifications
- Function Removals
- Additional Information
- Appendix



z/OS Encryption Readiness Technology (zERT)

Background: Encrypting TCP/IP network traffic on z/OS

z/OS provides 4 mechanisms to cryptographically protect TCP/IP traffic:

1 TLS/SSL direct usage

- Application is explicitly coded to use these
- Configuration and auditing is unique to each application
- Per-session protection
- TCP only

2 Application Transparent TLS (AT-TLS)

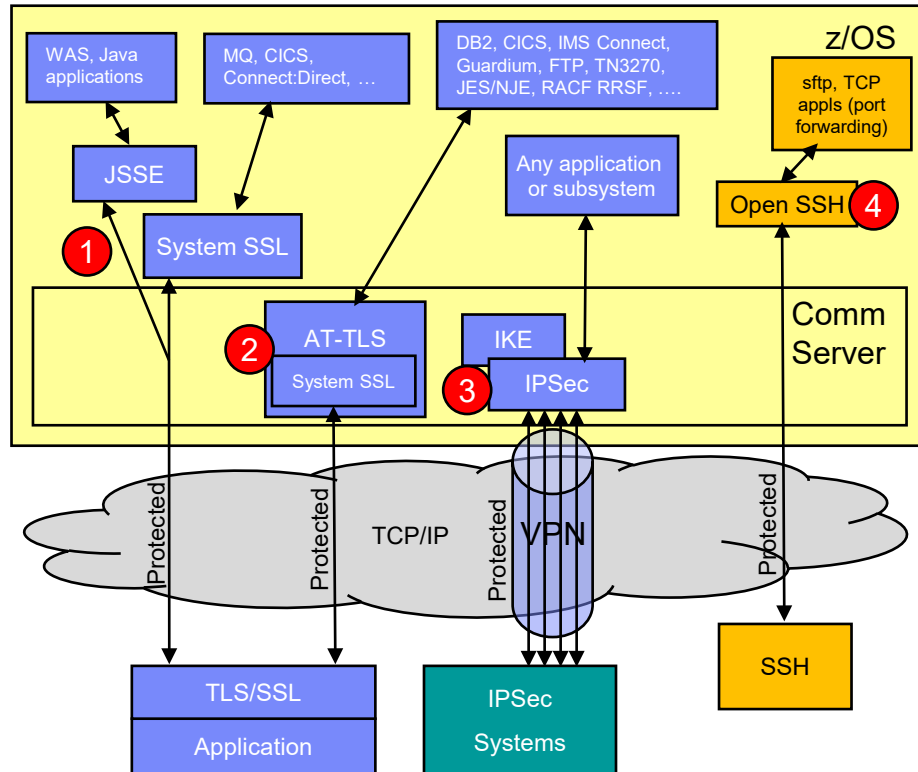
- TLS/SSL applied in TCP layer as defined by policy
- Configured in AT-TLS policy via Configuration Assistant
- Auditing through SMF 119 records
- Typically transparent to application
- TCP/IP stack is user of System SSL services

3 Virtual Private Networks using IPsec and IKE

- “Platform to platform” encryption
- IPsec implemented in IP layer as defined by policy
- Auditing via SMF 119 records at tunnel level only
- Completely transparent to application
- Wide variety (any to all) of traffic is protected
- IKE negotiates IPsec tunnels dynamically

4 Secure Shell using z/OS OpenSSH

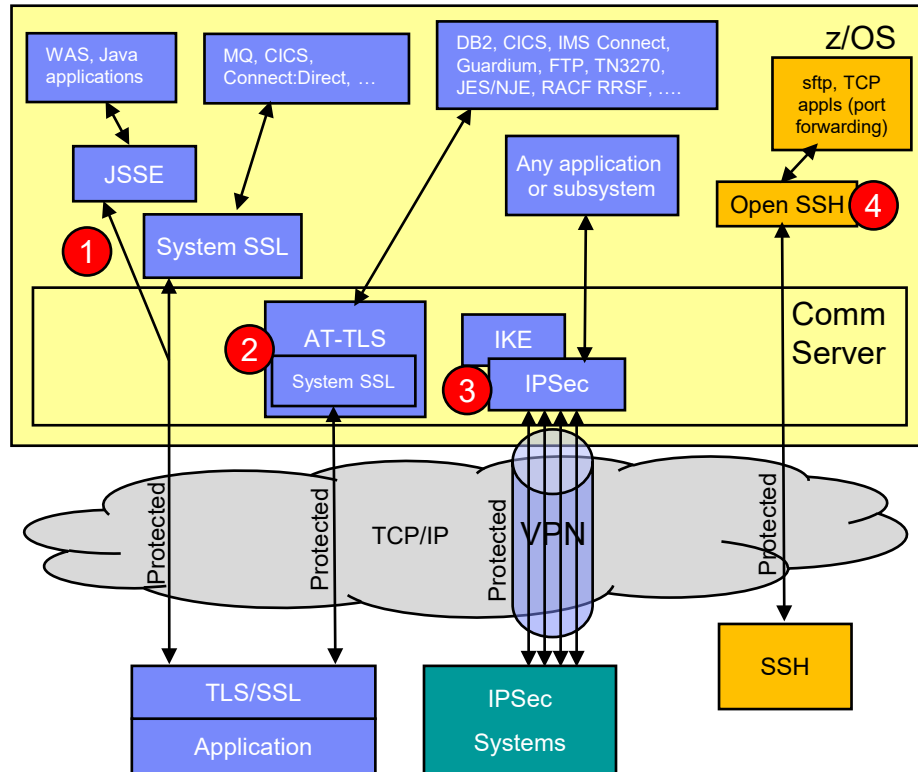
- Mainly used for sftp on z/OS, but also offers secure terminal access and TCP port forwarding
- Configured in ssh configuration file and on command line
- Auditing via SMF 119 records
- TCP only



Background (cont'd)

Given all these mechanisms, configuration methods and variation in audit detail...

- **How can I tell...**
 - **Which traffic** is being protected (and which is not)?
 - **How** is that traffic being protected?
 - Security protocol?
 - Protocol version?
 - Cryptographic algorithms?
 - Key lengths?
 - ...and so on
 - **Who** does the traffic belong to in case I need to follow up with them?
- How can I ensure that new configurations adhere to my company's security policies?
- Once I've answered the above questions, how can I provide the information to my auditors or compliance officers?
- Many factors driving these questions:
 - Regulatory compliance (corporate, industry, government)
 - Vulnerabilities in protocols and algorithms
 - Internal audits
 - ...and so on



Introducing z/OS Encryption Readiness Technology (zERT)

▪ zERT **Discovery**

- **SMF 119 subtype 11 “zERT Connection Detail” records**
- These records **describe the complete cryptographic protection history of each TCP and EE connection**
- **At least one record** is written **for each connection** - and each describes **all cryptographic protection** for that connection
- Well suited for **real-time monitoring** applications
- Depending on your z/OS network traffic, these could be generated in very high volume

▪ zERT **Aggregation**

- **SMF 119 subtype 12 “zERT Summary” records**
- These records **describe the repeated use of security sessions over time**
- Writes **one zERT Summary record at the end of each recording interval for each security session** active during the interval
- Well suited for reporting and analysis
- Can greatly reduce the volume of SMF records (over Discovery) while providing the same level of cryptographic detail

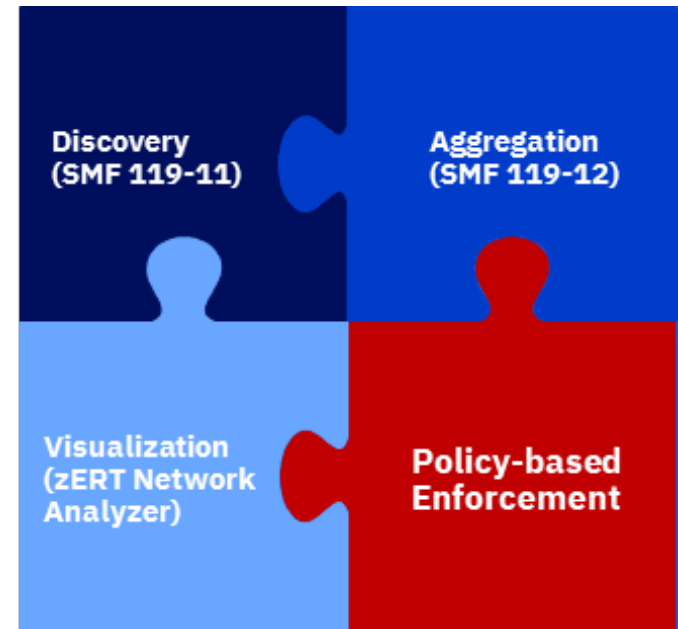
▪ zERT **Network Analyzer**

- **Web-based (z/OSMF) UI** to query and analyze zERT Summary (subtype 12) records
- **You can just install the latest network analyzer PTF – each one contains an up-to-date fresh install image**
- Intended for z/OS network security administrators (typically systems programmers)

Completing the zERT vision: Policy-based enforcement

Directs the TCP/IP stack to take specific actions when a user-defined security policy is or is not met for a new TCP/IP connection

- A new technology implemented through Network Configuration Assistant (NCA) and Policy Agent
- Rule conditions describe traffic (ports, addresses, etc.) along with acceptable or unacceptable protection attributes
- Rule actions determine what happens when a connection matches the rule conditions



Always on, real-time protection and alerting for TCP connection traffic to your z/OS systems that does not meet your enterprise network encryption standards

zERT policy-based enforcement overview

zERT policy administrator using Network Configuration Assistant

Rules are created and maintained through the z/OSMF Network Configuration Assistant (NCA) (generates the policy file)

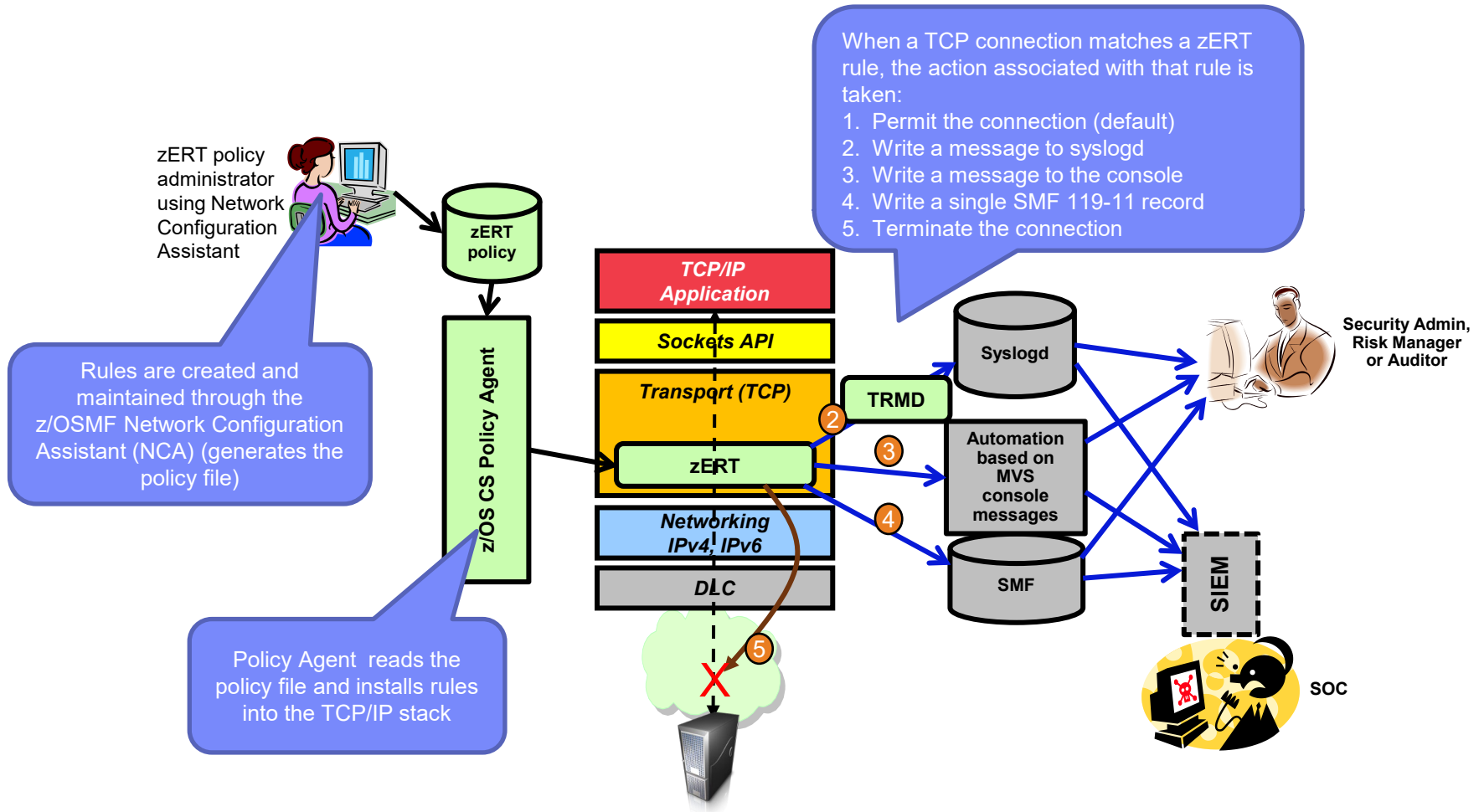
Policy Agent reads the policy file and installs rules into the TCP/IP stack

When a TCP connection matches a zERT rule, the action associated with that rule is taken:

1. Permit the connection (default)
2. Write a message to syslogd
3. Write a message to the console
4. Write a single SMF 119-11 record
5. Terminate the connection

Security Admin, Risk Manager or Auditor

SOC



Summary

- Phase 1: zERT Discovery - SMF 119 Connection Detail (subtype 11) records:
 - Per-connection: Well-suited for real-time monitoring applications
- Phase 2: zERT Aggregation - SMF 119 Summary (subtype 12) records:
 - Same level of cryptographic detail in a condensed format, typically with a great reduction in the volume of SMF records vs. Connection Detail records. Well suited to historical reporting applications.
- Phase 3: The zERT Network Analyzer:
 - z/OSMF UI for z/OS network security admins to query and search zERT summary data
 - Granular queries can be built for regular compliance checks or for special purpose investigations
- Phase 4: zERT policy-based Enforcement:
 - Rules configured through Network Configuration Assistant and installed through Policy Agent
 - Provides real-time monitoring, auditing and even defensive actions based on zERT data

z/OS Encryption Readiness Technology

Scan the QR code to visit
z/OS Communications Server product
page on IBM Community.




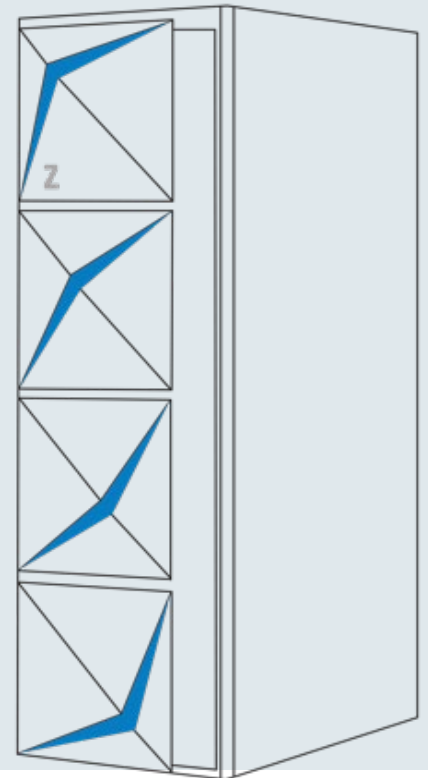
zERT policy-based enforcement – *new in z/OS V2R5*

- Enforce local network encryption standards for TCP traffic in real time.
- Policy-based rules you build in the Network Configuration Assistant describe acceptable or unacceptable levels of cryptographic protection along with the actions to take when TCP connections match those rules.

What are users saying about zERT?

- “Once we communicated to the our business what we're doing with zERT, they wanted to be able to do it across all our platforms!”
- “We use zERT data for compliance checks.”
- “zERT has given us the upper hand in monitoring mainframe connection security.”

 Visit [Things you should know about zERT](#) on IBM Community and discover blogs, product documentation, videos, event information, webinar, and presentations about zERT.



IPSec certificate reporting enhancements

IPSec certificate reporting enhancements

- Internet Key Exchange (IKE)
 - Communication between IKE-enabled peers begins with an initial exchange consisting of messages that negotiate Security Associations (SAs). This negotiation results in a phase 1 IKE tunnel.
 - During a phase 1 IKE tunnel negotiation, the following SA information is negotiated and/or exchanged:
 - Cryptographic algorithms
 - Nonces
 - Diffie-Hellman (DH)
 - Identities
 - **Certificates**
- The **ipsec -k display command** can be used to display **IKE tunnels**
- The **ipsec -k display command** can be issued to display IKE phase 1 tunnels, but the display output does not provide any information identifying which certificates were used for the IKE phase 1 negotiation
 - Customers have reported that when replacing an old certificate with a new certificate that there is no way of knowing which certificate IKE is using for authentication

IPSec certificate reporting enhancements ...

- In z/OS V2R5, the ipsec -k display is updated to display the following local and remote certificate information:
 - Expiration Date (yyyy/mm/dd HH:MM:SS)
 - Serial Number (hex string)
 - Issuer and Subject Distinguished Name
 - Length of the Issuer and Subject Distinguished Name
- Local and remote certificate information is also provided in the:
 - IPSec IKE tunnel activation and refresh SMF type 119, subtype 73 record
 - IPSec IKE tunnel deactivation and expire SMF type 119, subtype 74 record
- Local and remote certificate information is also provided in the:
 - Local IPSec NMI NMsec_GET_IKETUN response message
 - Local IPSec NMsec_GET_IKETUNCASCADE response message
- Updated response messages are also available for the Network security services (NSS) network management NMI

IPSec certificate reporting enhancements ...

- Example output from **the ipsec -k display command**:
 - New certificate-related fields in **bold**

```

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
*****

```

AT-TLS and IPsec certificate diagnostics

AT-TLS certificate diagnostics

- 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 the failure is due to an issue with the peer certificate or certificate chain the return code alone may not be sufficient for a diagnostic investigation
- In z/OS V2R5, Communication Server exploits a 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
- This capability is enabled by specifying an appropriate AT-TLS trace level in the AT-TLS policy
- This should reduce the need for collecting System SSL trace as part of diagnostic investigation

AT-TLS certificate diagnostics ...

- When enabled, new messages can be 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

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

IPsec certificate diagnostics

- For IPsec protection, IKED typically relies on NSS daemon for certificate services
 - IKED can also provide certificate services in some cases
- 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
- In z/OS V2R5, Communication Server exploits a 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
- This capability is enabled using the existing `IkeSyslogLevel` statement in the IKED configuration file
- This should reduce the need for collecting System SSL trace as part of diagnostic investigation

IPsec certificate diagnostics ...

- When enabled, new messages can be 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

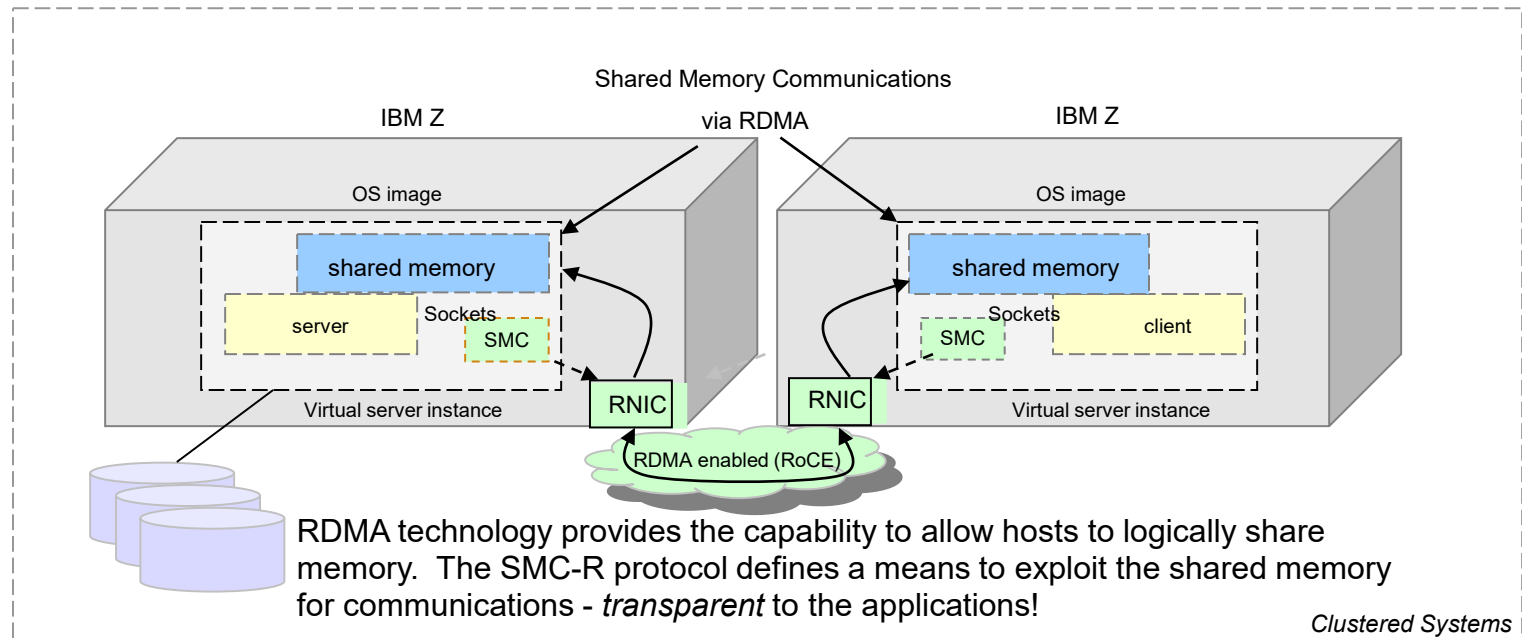
IKE DEBUGSA : Certificate Diagnostics Details **Certificate** 1 of 2 **FailingCert**= No
SubjectDN= <CN=BOVIPA8_EXPCA,OU=SVT,O=IBM,C=US> **IssuerDN**= <CN=BO EXPCA,OU=SVT,O=IBM,C=US>
SerialNumber= 022222 **CertSource**= IKEPayload

- 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**

Shared Memory Communications Version 2 (SMCv2)

Shared Memory Communications over RDMA (SMC-R)

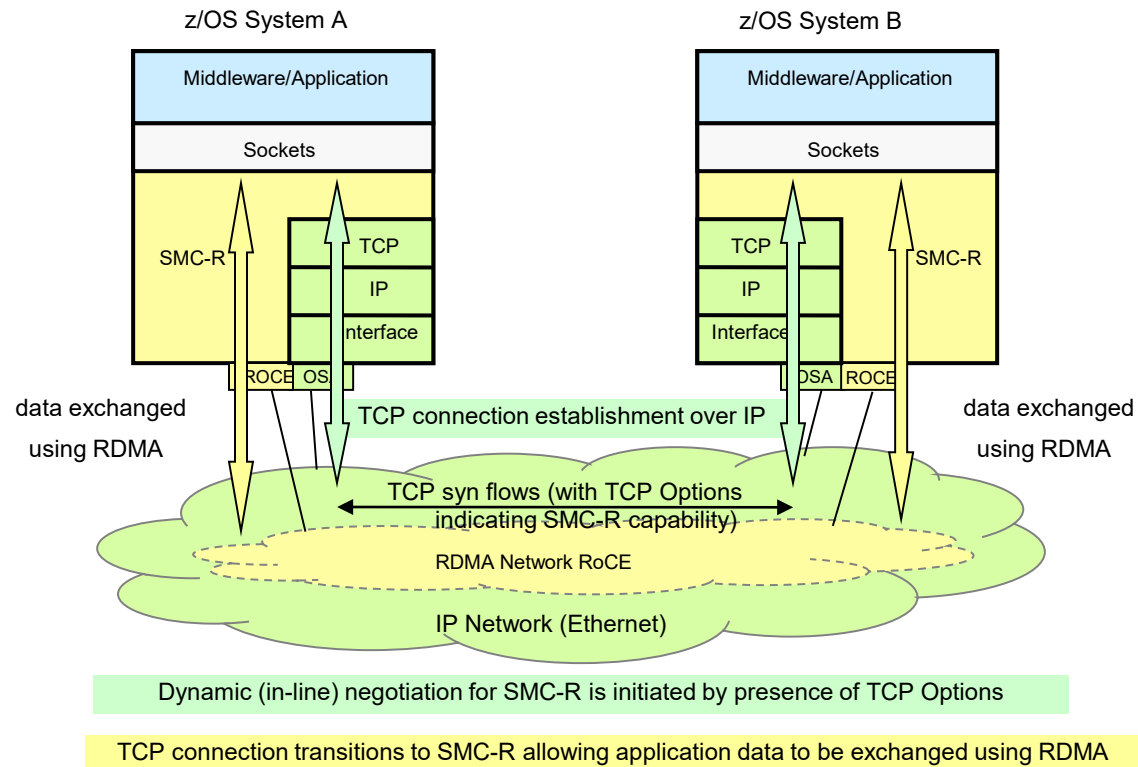


SMC-R is an *open* sockets over RDMA protocol that provides transparent exploitation of RDMA (for TCP based applications) while preserving key functions and qualities of service from the TCP/IP ecosystem that enterprise level servers/network depend on!

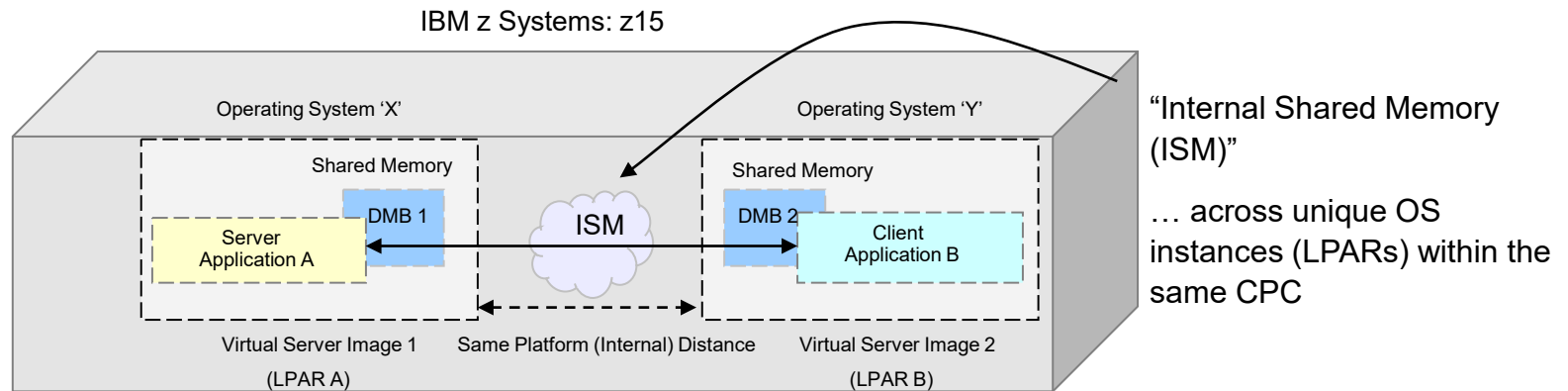
IETF RFC for SMC-R:

<http://www.rfc-editor.org/rfc/rfc7609.txt>

Dynamic Transition from TCP/IP to SMC-R



Shared Memory Communications-Direct Memory Access (SMC-D) over Internal Shared Memory (ISM)



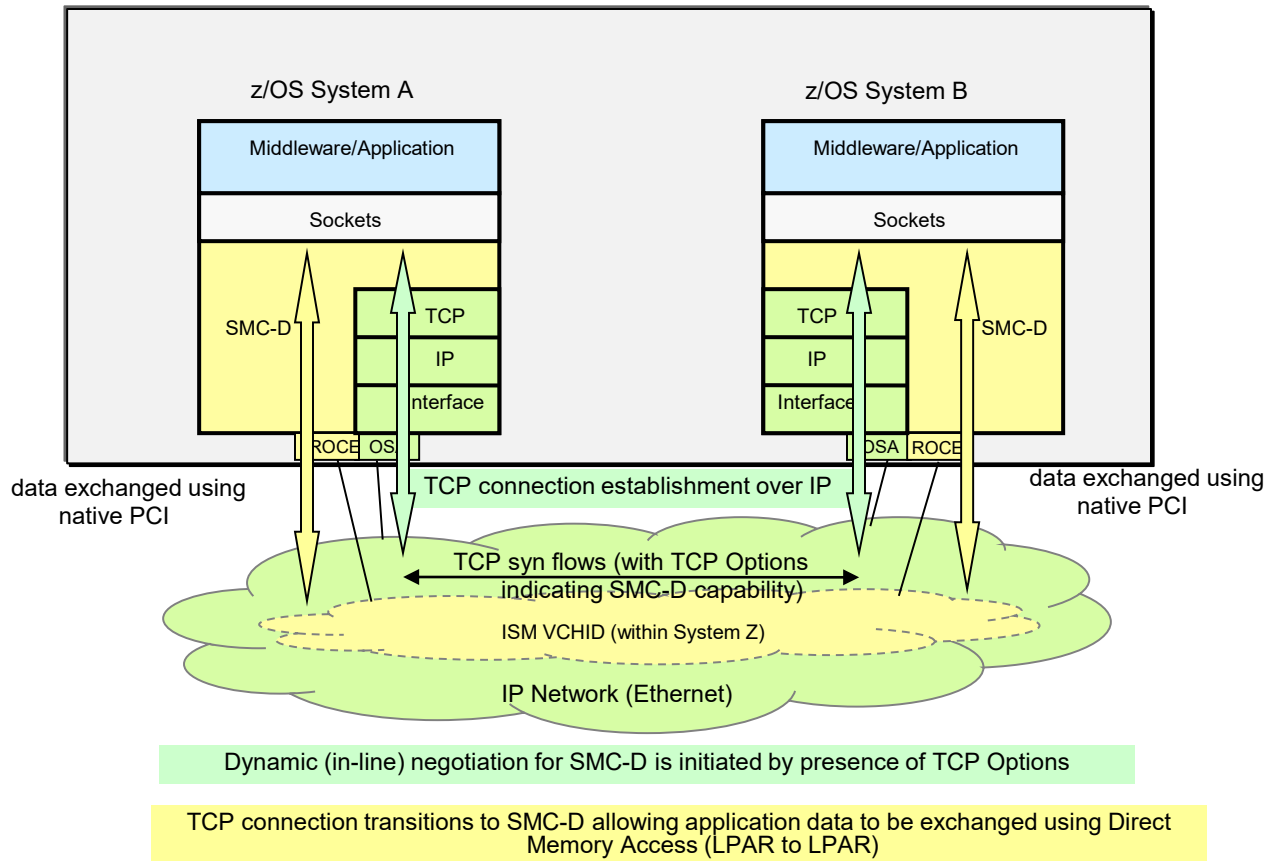
SMC-D (over ISM) extends the value of the Shared Memory Communications architecture by enabling SMC for direct LPAR to LPAR communications. SMC-D is very similar to SMC-R (over RoCE) extending the benefits of SMC-R to same CPC operating system instances without requiring physical resources (RoCE adapters, PCI bandwidth, NIC ports, I/O slots, network resources, 10GbE switches etc.).

Note 1. The performance benefits of SMC-R (cross CPC) and HiperSockets (within CPC) are similar to each other.

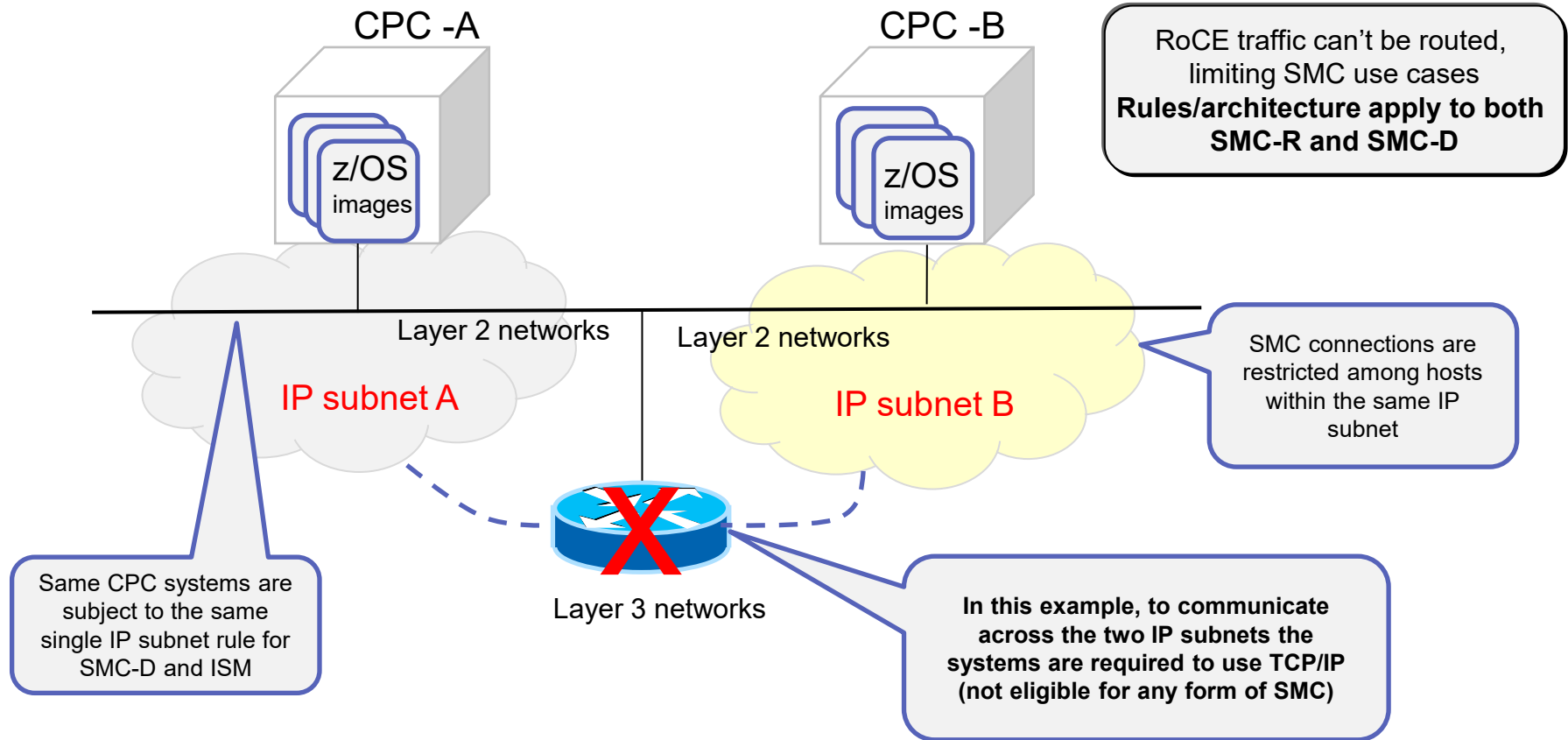
SMC-D / ISM provides significantly improved performance benefits above both within the CPC.

Reference performance information: <http://www-01.ibm.com/software/network/commserver/SMCR/>

Dynamic Transition from TCP/IP to SMC-D



SMC (SMC-R and SMC-D) is Limited to a Single IP Subnet



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.

IBM Shared Memory Communications (SMC)

A powerful IBM Z enterprise data center network communications solution that has the potential to offer you:

- Savings in network related CPU costs
- Reducing latency and increasing throughput

Originally, limited to TCP connections for hosts (client and server) that have direct access to the **same IP subnet**.

IBM SMC Version 2 (SMCv2)

announced in the IBM z/OS V2R4 3Q2020 new functions and enhancement RFA

SMC Version 2 (SMCv2) defines the specifications that enable SMC over **multiple IP subnets**. Extends the benefits of SMC to additional Z workloads.

- SMC-D Version 2 and IBM z15 with ISM Version 2 lift the single IP subnet limitation for communications **within an IBM Z system**¹.
- SMC-R Version 2 and IBM z15 with RoCE Express2 that introduces RoCEv2 will support "routable RoCE" connectivity over multiple IP subnets for communications **across IBM Z systems**¹.

Roadmap

3Q 2020, SMC-Dv2 release

Available with APARs [PH22695](#) and [OA59152](#)

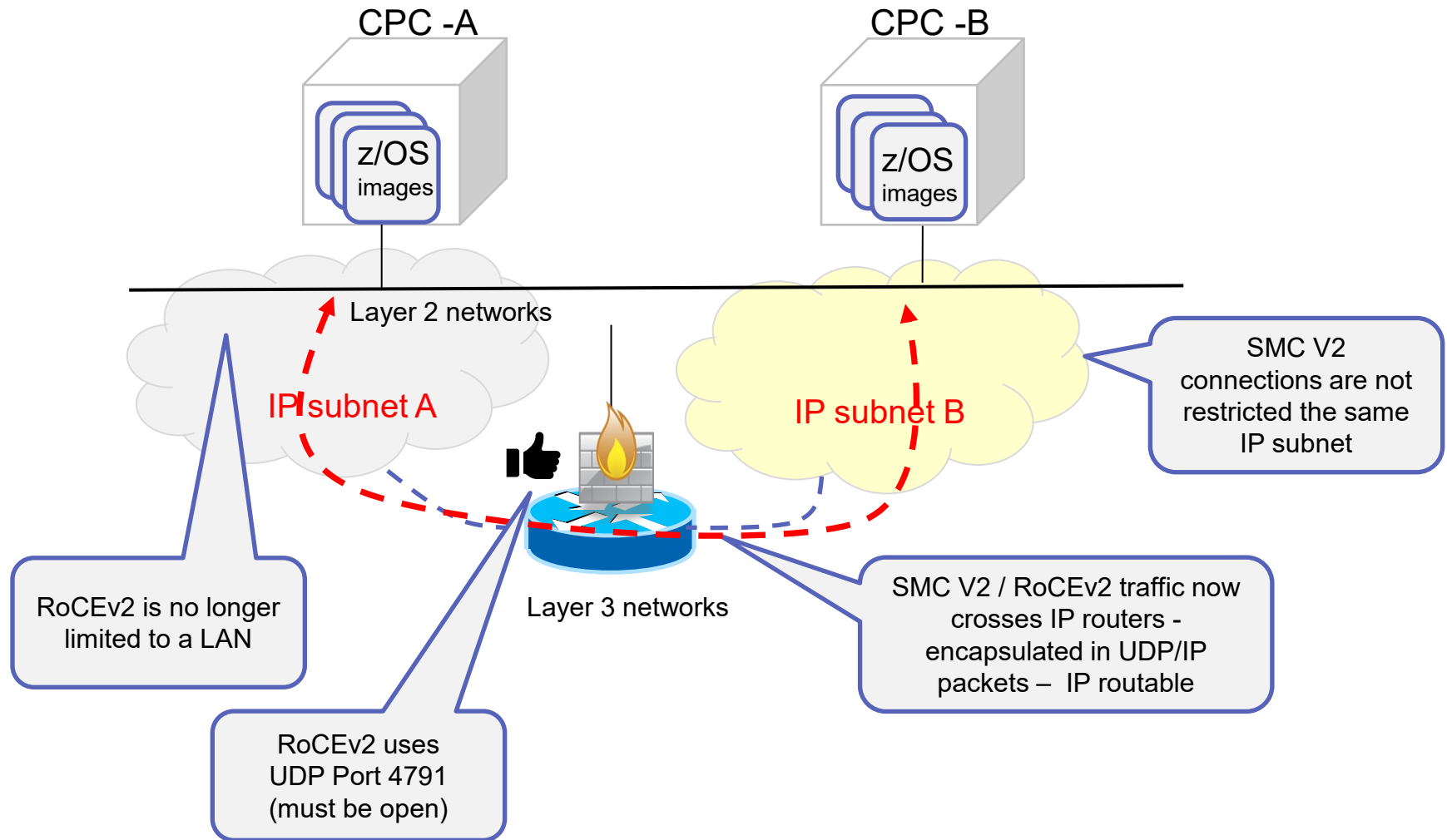
1. Refer to the SoD in [z/OS V2R4 3Q2020 RFA](#)

3Q 2021, SMC-Rv2 release

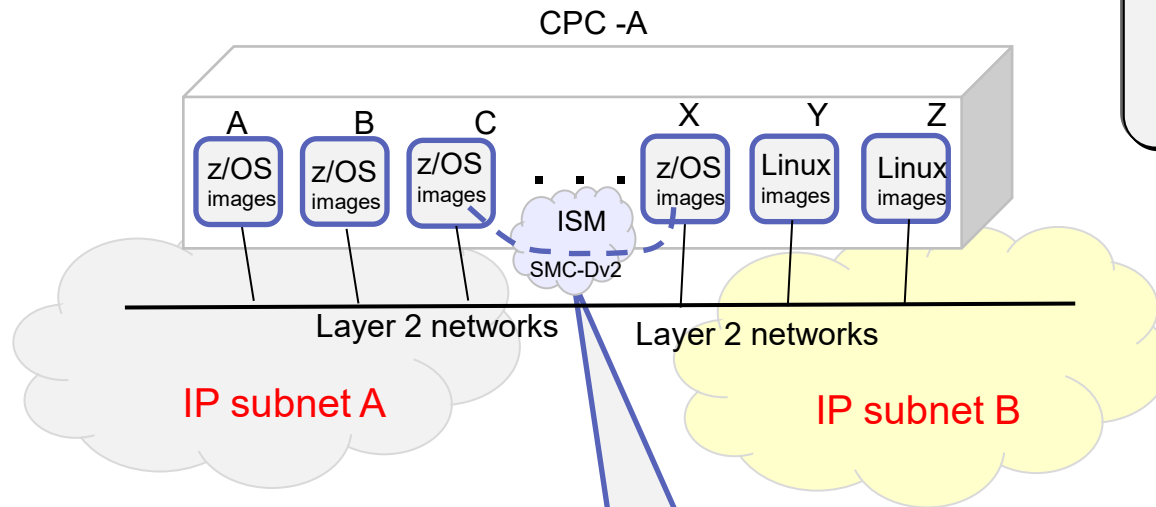
Available with z/OS V2R5

1. Refer to z/OS V2R5 RFA

SMC Version 2 for SMC-R: SMC-Rv2 (“Routable RoCE”)



SMC Version 2 for SMC-D: SMC-Dv2



SMC-Dv2 eliminates the single-subnet restriction for SMC-D

SMC-D supports IP connectivity over OSA or HS (no change for SMC-Dv2). TCP/IP connections over multiple IP subnets will typically be external connections over OSA.

SMC-Dv2 connections are not restricted the same IP subnet

SMC-Rv2 Performance:

How does SMC-Rv2 compare to TCP/IP?

Network Latency

Network latency for z/OS TCP/IP based OLTP workloads **reduced over 60%**

Network latency for z/OS TCP/IP based workloads with streaming data patterns **reduced by 45%**

Network-related CPU cost

Networking related CPU consumption for z/OS TCP/IP based OLTP workloads **reduced by up to 15%¹**

Networking related CPU consumption for z/OS TCP/IP based workloads with streaming data patterns **reduced by 85%**

1. OLTP workload – small message size used (4K); networking CPU savings increase with larger data sizes.

SMC-Dv2 Performance:

How does SMC-Dv2 compare to HiperSockets?

Network Latency

Network latency for z/OS TCP/IP based OLTP workloads ***reduced nearly 50%***

Network latency for z/OS TCP/IP based workloads with streaming data patterns ***reduced nearly 90%***

Network-related CPU cost

Networking related CPU consumption for z/OS TCP/IP based OLTP workloads ***reduced over 45%¹***

Networking related CPU consumption for z/OS TCP/IP based workloads with streaming data patterns ***reduced by 90%***

1. OLTP workload – small message size used (4K); networking CPU savings increase with larger data sizes.

Additional information on SMC V2

1. Presentation: Introduction to IBM Shared Memory Communications Version 2 (SMCv2) and SMC-Dv2
PDF available at: <http://ibm.biz/ibmsmcv2>
Screencast available at: <http://ibm.biz/ibmsmcv2vid>
2. IBM SMCv2 Overview: SMC-Dv2 / ISMv2 White Paper:

<https://www.ibm.com/docs/en/zos/2.5.0?topic=communications-shared-memory-reference-information>
3. NMI and SMF updates:
Reference the IP Programming Manual (minor updates)
4. SMC-AT: Using your existing output... The 2.4 APAR includes minor changes in the SMC-AT report to clarify what could be achieved with SMCv2.

TCP/IP startup message and ENF notifications

TCP/IP initialization complete - But is it really?

15:07:21.70 EZZ4202I Z/OS UNIX - TCP/IP CONNECTION ESTABLISHED FOR TCPIP
15:07:21.70 EZB6473I TCP/IP STACK FUNCTIONS INITIALIZATION COMPLETE.
15:07:21.70 EZAIN11I ALL TCPIP SERVICES FOR PROC TCPIP ARE AVAILABLE.

- So, what's the problem? Automation can use message EZAIN11I as a trigger that TCP/IP is initialized and can then trigger starting address spaces and workloads that depend on TCP/IP
 - Message EZAIN11I indicates that TCP/IP has progressed through initialization of all base services
 - However, after EZAIN11I is issued TCP/IP continues initialization of extended/optional functions
 - Joining the Sysplex and enabling Dynamic VIPAs and Sysplex Distributor
 - Enabling Policy Based Networking functions
 - AT-TLS, IPSec IDS, PBR, etc.
 - Currently, existing automation may need to examine multiple messages before declaring that TCP/IP and all extended services are available – for example, are DVIPAs available? Wait for this message:

EZD1214I INITIAL DYNAMIC VIPA PROCESSING HAS COMPLETED FOR TCPIP

- And this is critical because most workloads rely on the availability of many of these extended services
- But some of these extended functions may or may not be configured on all my z/OS systems. Do I need custom startup automation for these cases?

TCP/IP initialization complete – Can we simplify this?

- In z/OS V2R5, Communication Server adds new notifications to indicate that TCP/IP and its required services (determined by user configuration) are initialized. This includes:
 - New console messages
 - A new Event Notification Facility (ENF) signal
 - A new Name/Token Pair
- This provides more reliable message to indicate all necessary services are fully initialized, and allows a software developer to programmatically determine when TCP/IP and its required services have fully initialized

TCP/IP initialization complete - New console messages

- New console messages:

- TCP/IP and extended services have been fully initialized

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

- Eventual Action messages issues to indicate delays in initialization of required extended services:

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 policies
- IPSEC INFRASTRUCTURE – IKED heartbeat not detected
- This message gets deleted (DOM) when these services complete their initialization

10:08:10.99 IC015A 00000290 S TCPIP

10:08:11.66 STC00028 00000090 EZB6473I TCP/IP STACK FUNCTIONS INITIALIZATION COMPLETE

10:08:14.66 STC00028 00000090 EZAIN11I ALL TCPIP SERVICES FOR PROC TCPIP ARE AVAILABLE.

10:08:16.21 STC00028 00000090 *EZD1315E NOTIFICATION OF TCP/IP EXTENDED SERVICES AVAILABILITY IS DELAYED FOR TCPIP DUE TO SYSPLEX

10:08:16.73 STC00028 00000090 EZD1176I TCPIP HAS SUCCESSFULLY JOINED THE TCP/IP SYSPLEX GROUP

10:08:18.83 STC00028 00000090 EZD1314I TCP/IP AND EXTENDED SERVICES ARE NOW INITIALIZED FOR STACK: TCPIP

TCP/IP initialization complete - Configuration

- New configuration is provided in the TCP/IP Profile to indicate which services are required for initialization to be considered complete:
 - 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

Function Removals

Function removals in z/OS V2R5

- Several functions were removed from Communications Server in z/OS V2R5:
 - Removal of Sysplex Distributor support for Cisco Multi-Node Load Balancer (MNLB)
 - Removal of support for load balancing to DataPower® Gateway
 - Removal of CMIP from VTAM
 - Removal of support for NCA policy import
 - Removal of native TLS/SSL support from TN3270E Telnet Server, FTP Server, and DCAS
- Statements of direction (and some additional details) are in the appendix

Additional Information

Statement of Direction: Withdrawal of support for VTAM® Link Station Architecture (LSA) and TCP/ IP LAN Channel Station (LCS) devices (Issued July 27, 2021)

As stated in Hardware Announcement 121-029, dated May 4, 2021, many IBM Z clients continue to rely on Systems Network Architecture (SNA) applications for mission-critical workloads, and IBM has no plans to discontinue support of the SNA protocol, including the SNA APIs. However, IBM Z support for the SNA protocol being transported natively out of the server using OSA Express 1000BASE-T adapters configured as channel type “OSE” will be eliminated in a future hardware system family. With the support for OSE planned to be discontinued, support for the related VTAM and TCP/IP device drivers is also planned to be discontinued. IBM intends z/OS V2.5 to be the last z/OS release to provide support for LSA (SNA) and LCS (TCP/IP) devices. z/OS systems that have workloads that rely on the SNA protocol and utilize OSE networking channels as the transport should be updated to make use of some form of SNA over IP technology, where possible, such as Enterprise Extender.

Statement of Direction: Removal of OSA DEVICE/LINK/HOME configuration support (Issued July 27, 2021)

z/OS V2.5 is planned to be the last z/OS release to provide support for the TCP/IP profile statements DEVICE, LINK, and HOME for OSA connectivity. All z/OS users who currently use DEVICE, LINK, or HOME for OSA connectivity should migrate to the INTERFACE statement for defining OSA Express connectivity in their TCP/IP profile.

New function APAR summary web pages

⑩ We maintain web pages that provide a summary of the new function APARs available for each release:

- Includes a summary of the function, a link to the APAR, and a link to the function documentation
- V2R3: <https://www-01.ibm.com/software/support/systemsz/cs-v2r3-new-function-apars.html>
- V2R4: <https://www.ibm.com/support/pages/zos-v2r4-communication-server-new-function-apar-summary>

New function APAR summary web pages - Example



-
-

★ Inbound Workload Queueing (IWQ) support for IBM z/OS Container Extensions December 2019

z/OS V2R4 Communications Server, with VTAM APAR OA58300 and TCP/IP APAR PH16581, is enhanced to support inbound workload queueing for IBM z/OS Container Extensions (zCX) workloads for OSA-Express® in QDIO mode.

- [OA58300](#)
- [PH16581](#)
- [How to enable/use this function?](#)

Incompatibilities: This function does not support IPAQENET interfaces that are defined by using the DEVICE, LINK, and HOME statements. Convert your IPAQENET definitions to use the INTERFACE statement to enable this support.

Dependencies:

- This function is limited to OSA-Express6S Ethernet features or later in QDIO mode running on IBM z14.
- This function is supported only for interfaces that are configured to use a virtual MAC (VMAC) address.

V2R4: z/OS Communications Server Performance Summary Report

IBM Z Systems | **E**nterprise **N**etworking **S**olutions (**ENS**)

V2R4: Z/OS COMMUNICATIONS SERVER PERFORMANCE SUMMARY REPORT

<http://ibm.biz/zcsv2r4perfsummary>

Digital Badges & Online Courses



Networking on z/OS - Foundations

- **IBM Open Badge:**
<https://ibm.biz/zosnetworkingbadge>
- **Online course:**
<https://ibm.biz/zosnetworkingcourse>

Foundational understanding of networking on z/OS.



z/OS Network Security - Foundations

- **IBM Open Badge:**
<http://ibm.biz/zosnetsecuritybadge>
- **Online course:**
<http://ibm.biz/zosnetsecuritycourse>

Knowledge and foundational understanding of z/OS network security.



z/OS TCP/IP Configuration with NCA

- **IBM Open Badge:**
<http://ibm.biz/NCAbadge>
- **Online course:**
<http://ibm.biz/NCATCIPcourse>

Use the NCA to create and manage TCP/IP profiles.

Join z/OS Comm Server
on **IBM Community** !



<https://ibm.biz/cscommunity>

Rich and up-to-date technical content, including blogs, videos, and events.

Join Us on IBM Community!

IBM developerWorks platform is sunset.

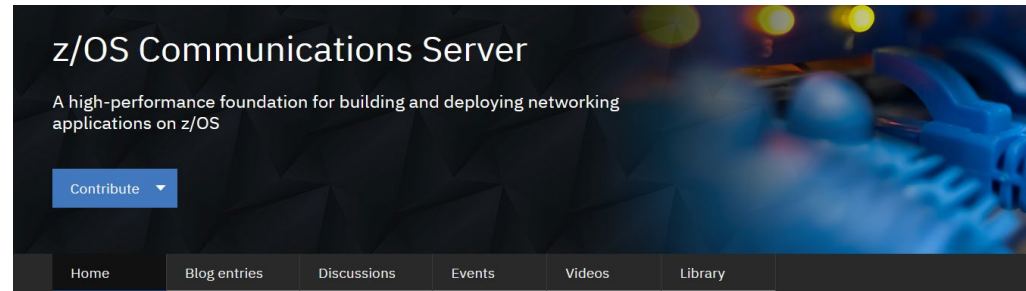
With **a new and improved platform**, we will continue to provide rich and up-to-date technical content on the IBM Community page, including blogs, videos, and events.

Join us at our new home:

<https://www.ibm.com/community/z/software/comm-server/>



Scan the QR code to visit the z/OS Communications Server home page on IBM Community.



Blog entries RSS

This group Related



z/OS Communications Server sessions at the SHARE Virtual August 2020

z/OS Communications Server | Posted by Erin ZHANG on 07/07/2020

Kicking off August 4, you will still be able to connect with peers, learn from the experts, and enjoy the same benefits of SHARE conferences wherever you are. There will be a good selection of content focused on z/OS Communications Server including the...

IBM Z IBM Z OS z/OS Software Solutions



zERT | Start your self-paced journey with IBM zERT Network Analyzer

IBM Z | Posted by Flora Gui on 04/21/2020

IBM zERT Network Analyzer, the web GUI of z/OS Encryption Readiness Technology (zERT), made its debut in December 2018. With IBM zERT Network Analyzer, z/OS network security administrators can analyze and report on data reported in zERT Summary records...

IBM Z Go IBM Z OS z/OS Software

zERT | Best practices: Sorting out the different z/OS user IDs involved with the zERT Network Analyzer

IBM Z | Posted by Erin ZHANG on 04/03/2020

With z/OS Encryption Readiness Technology (zERT), you are now able to discover and analyze the status of the network cryptographic protection of your z/OS TCP and Enterprise Extender workloads. If you have adopted zERT, you might already be familiar...

IBM Z IBM Z OS z/OS DB2 Software



Free webinar: Importing your existing TCP/IP profile into Network Configuration Assistant

z/OS | Posted by Alicia Mao on 04/03/2020

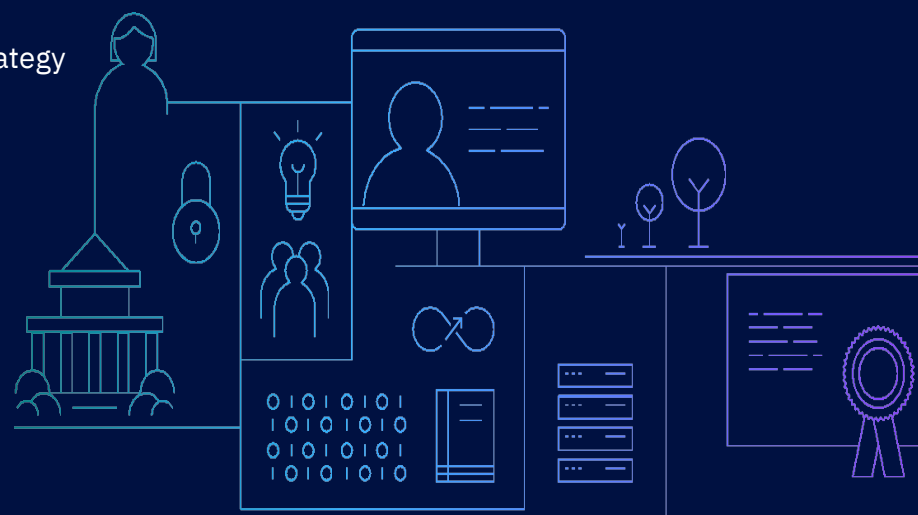
The Configuration Assistant for z/OS Communications Server (also known as Network Configuration Assistant or NCA) is a modern web application that plugs into IBM z/OS Management Facility. The NCA provides a guided interface to help you create and manage...

IBM Z IBM Z OS z/OS Software z/OSMF

Thank you



- Mike Fitzpatrick
- STSM, Lead Architect Multi-site Workload Lifeline. Performance & Design, z/OS Communications Server
- mfitz@us.ibm.com
- Sam Reynolds
- Enterprise Networking Solutions - Architecture, Design, and Strategy
- samr@us.ibm.com



- © 2021 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.
- **U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**
- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.
- IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”
- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**
- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml

