z/OS Communications Server Technical Update: Winter 2026 Edition

Paul Gartman – Paul.Gartman@ibm.com
Ed Seidl – eseidl@us.ibm.com
Upeksha Vidanapathirana - upekshavid@ibm.com

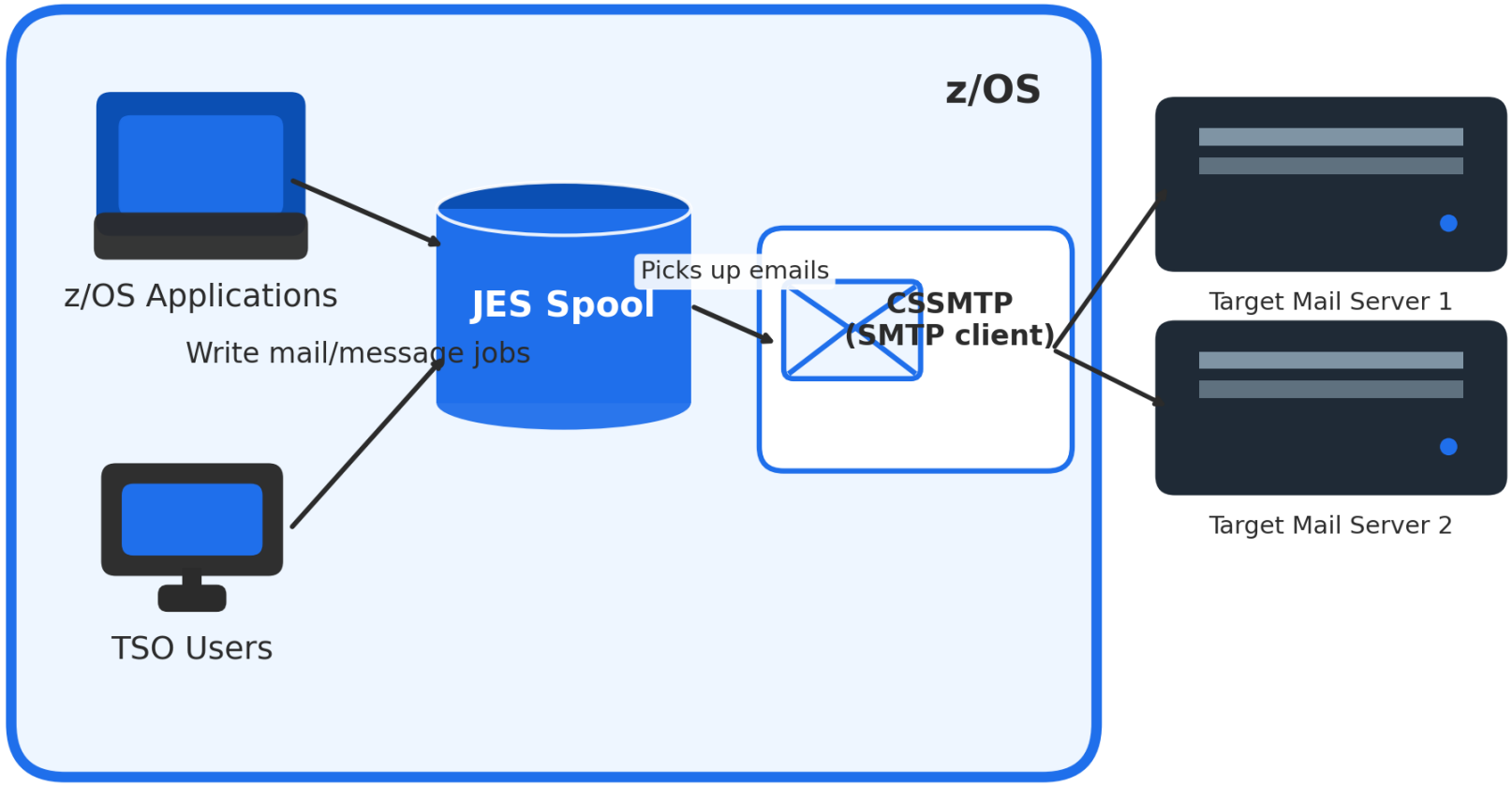
February 23, 2026

Agenda

- CSSMTP Enhancements
  - SMTP AUTH support for CSSMTP
  - Email Spoofing Prevention with CSSMTP
- EQDIO support for the IBM z17 Network Express feature
- AI-powered network outbound packet batching
- Networking support for z/OS Container Platform
- Increase VIPADISTRIBUTE Ports
- Network security enhancements
  - Support for AES-GCM for IKEv2 SA
  - zERT monitoring enhancements
- Additional Information
- Appendix
  - zNA database enhancements
  - Update to System SSL and AT-TLS default values in z/OS 3.2
  - Persistent Pause Support for Sysplex Distributor DVIPAs
  - Function Removals
  - Additional Information

SMTP AUTH support for CSSMTP

CSSMTP mail client for z/OS



SMTP AUTH support for CSSMTP

- SMTP AUTH is an Internet standard (RFC-4954) that provides a way for mail servers (like Exchange or Postfix) to authenticate the originator of an email.
- RFC-4954 specifies that the mail client will identify a SASL (Simple Authentication and Security Layer) mechanism to use for the authentication.
  - There are several SASL mechanisms, but the one that is required by the RFC is PLAIN. PLAIN is a simple username/password authentication mechanism.
  - Another SASL mechanism is AUTH LOGIN (which is equivalent to Microsoft Exchange “BasicAuth” support).
  - Either mechanism requires the use of TLS for the connection to the mail server to protect the username and password.
  - CSSMTP supports AUTH PLAIN and AUTH LOGIN.

SMTP AUTH support for CSSMTP …

- CSSMTP allows authentication for the CSSMTP client as a single entity, or authentication of the email addresses on individual emails.
  - The system administrator must configure the username and password pair (or pairs if authenticating at the email level) in RACF for secure storage. (Each of these is referred to as an AuthEntity.)
  - The CSSMTP configuration file will include a new parameter for the name of the AuthEntity. (“target.mail.server” or <MailFrom> in the examples on subsequent charts).
  - If the CSSMTP configuration file includes an AuthEntity for the target server, CSSMTP will know that Auth should be attempted (once the server requests it).
  - After a successful TLS connection, CSSMTP will retrieve the username and password from RACF and send it to the target server with the Auth Plain or Auth Login command. (This will happen for each email if authenticating at the email level.)
  - If the authentication is successful, CSSMTP can start forwarding the mails to that server. Otherwise, the connection will be terminated.

SMTP AUTH support for CSSMTP: Secure password storage

- The customer will need to define an encryption key in the LDAP.BINDPW.KEY profile (KEYSMSTR class) to allow the storage of an LDAP BIND password in the PROXY segment of the resource profile.
- Note that we are reusing the SAF LDAP BIND password storage for the CSSMTP password storage. However, CSSMTP has no dependency on LDAP, nor does it make use of it in any way.
- Previously, the LDAP.BINDPW.KEY profile storage could only be encrypted with DES encryption. RACF is enhancing this to allow for the storage to be AES-encrypted.

SMTP AUTH support for CSSMTP: Secure password storage …

The EZARACF sample provides instructions for storing the username/password pair(s) in RACF

```
//** The AUTHENTITY parameter on the TargetServer statement allows CSSMTP to retrieve the
//** username and the password from RACF to use for authentication with a mail server.

//**   Step 1
//** Activate the required classes:
//* SETROPTS CLASSACT(LDAPBIND)
//* SETROPTS CLASSACT(KEYSMSTR)
//* SETROPTS RACLIST(KEYSMSTR)

//** Step 2
//** For AES, define the key in ICSF and give it a label. Define this profile to reference the AES key:
//*  RDEFINE KEYSMSTR LDAP.BINDPW.KEY SSIGNON(KEYLABEL(mykey))
//** For DES, define this profile, using your own secret consisting of 16 hexadecimal chars
//** Note : If you already have LDAP.BINDPW.KEY profile, please skip this step and go to step 3
//*  RDEFINE KEYSMSTR LDAP.BINDPW.KEY SSIGNON(KEYENCRYPTED(0023528875DECFAC))
//*  SETROPTS RACLIST(KEYSMSTR) REFRESH

//* Step 3
//** Value defined for AuthEntity is defined as a profile in the LDAPBIND class. The username and
//** password are defined in the PROXY segment of the profile in BINDDN and BINDPW fields.
//*  RDEFINE LDAPBIND target.mail.server PROXY(BINDDN('username') BINDPW('password'))

//* Step 4
//** Give CSSMTP the authority to access the LDAPBIND profiles
//* RDEFINE FACILITY BPX.SERVER UACC(NONE)
//* PERMIT BPX.SERVER CLASS(FACILITY) ID(CSSMTP) ACCESS(READ)
//* SETROPTS RACLIST(FACILITY) REFRESH
```

SMTP AUTH support for CSSMTP: Configuration

- The CSSMTP Configuration file is updated with a new AuthEntity parameter in the target server statement.
  - The “Secure” parameter MUST be set to YES if configuring the AuthEntity.

```
TargetServer
    {
      TargetIp              10.1.1.1
      AuthEntity            target.mail.server
      Secure                Yes
    }
    Options
    {
      TLSEHLO YES
    }
```

- MODIFY procname,DISPLAY,CONFIG

```
TARGETSERVER:
  TARGETIP           : 10.1.1.1
  CONNECTPORT        : 25          CONNECTLIMIT    : 5
  MAXMSGSENT         : 0           MESSAGESIZE     : 524288
  SECURE             : YES         CHARSET         : ISO8859-1
  AUTHENTITY         : target.mail.server
```

SMTP AUTH support for CSSMTP: Configuration …

- If email level authentication is needed, <MAILFROM> can be specified for AuthEntity. CSSMTP will use the email address in the MAIL FROM field to retrieve the username and password from RACF.

```
TargetServer
    {
      TargetIp              10.1.1.1
      AuthEntity            <MAILFROM>
      Secure                Yes
    }
    Options
    {
      TLSEHLO YES
    }
```

- MODIFY procname,DISPLAY,CONFIG

```
TARGETSERVER:
  TARGETIP          : 10.1.1.1
  CONNECTPORT       : 25          CONNECTLIMIT    : 5
  MAXMSGSENT        : 0           MESSAGESIZE     : 524288
  SECURE            : YES         CHARSET         : ISO8859-1
  AUTHENTITY        : <MAILFROM>
```

SMTP AUTH support for CSSMTP: Viewing AUTH state

Modify procname, display, targets command shows the Auth State for the target servers

```
f cssmtp,d,targets
```

```
GLOBAL INFORMATION:
  MAIL SENT     : 0         TOTAL RETRY  : 0
  DEADLETTER    : 0         CURRENT RETRY: 0
  UNDELIVER     : 0
EXTENDED RETRY:
  CURRENT       : 0         TOTAL        : 0
TARGET SERVER 10.1.1.1
  STATE         : ACTIVE
  ESMTP         : YES       MESSAGE SIZE : 10240000
  STARTTLS      : YES       MAIL ATTEMPTS: 0
  AUTH STATE    : SUCCESSFUL
  MAIL SENT     : 0         CONNECT FAIL : 0
```

Auth states:

- NOT CONFIGURED - AUTH entity not configured
- CONFIGURED - AUTH entity configured
- SAF FAILURE - Failed to retrieve username or password from SAF
- SUCCESSFUL - AUTH connection successful
- REJECTED - AUTH command rejected from the server (Could be the wrong username password sent to the server or some other server problem)
- REQUESTED - AUTH support requested by the server, but AUTH entity is not configured in CSSMTP
- INVALID CERT - Failed server hostname check against the CA
- EMAIL LEVEL - Authentication is done by email address from the Mail From field

SMTP AUTH support for CSSMTP: V2R5 and 3.1

- The SMTP AUTH support for CSSMTP was developed as part of z/OS 3.2
- The support is available on z/OS V2R5 and 3.1 via APAR PH61015. (And the follow on APARs PH66815 and PH66548)
- RACF's support for AES encryption of the LDAPBIND storage is available on z/OS V2R5 and 3.1 via APAR OA66458.

Email Spoofing Prevention support for CSSMTP

Email Spoofing Prevention support for CSSMTP

- With enabling CSSMTP Auth support, mail servers can authenticate the originator of an email.
- However, CSSMTP did not have a way to verify whether a user was authorized to send an email using the address specified in the MAIL FROM field.
- Each email submitted to the JES spool has a mailfrom: field containing the sender's email address. CSSMTP allowed the mailfrom: address to be ANY email address. This is a security concern known as email spoofing.
- With email spoofing prevention support, CSSMTP will check if the user who submitted the email to the JES spool is allowed to use the email address specified in the mailfrom: field.
- CSSMTP will perform a check to see if the user has the email defined in the WAEMAIL in the WORKATTR segment of the user profile, or if the user has permission to use the matching email address profile in LDAPBIND profile.

Email Spoofing Prevention support for CSSMTP

- If the check fails, CSSMTP will treat the jespool file as a bad email and take an action based on the BadSpoolDisp setting (Hold or Delete).
- CSSMTP will not retry to process that mail file again.
- Instead, action will be taken depending on the Report statement setting (Admin, Sysout or None), and an error report will be generated with the reason why the validation failed.
- If the Report statement is set to Admin, the ReportMailFrom statement will be used to validate the error report along with the userid associated with CSSMTP.

Email Spoofing Prevention support for CSSMTP – RACF Configuration - The EZARACF sample updates

```
//* If the user can use only one email address, the email address can be configured in WAEMAIL in the WORKATTR
//* segment of the user profile.
//*
//* ALTUSER userid WORKATTR(WAEMAIL('test3@test.com'))
//*
//* Then permit the CSSMTP started procedure user, READ access to IRR.RUSERMAP.
//*
//* PERMIT IRR.RUSERMAP CLASS(FACILITY) ID(CSSMTP) ACCESS(READ)
//* SETROPTS RACLIST(FACILITY) REFRESH
//*
//* If the AuthEntity is already defined as <MAILFROM>, the email address in the same ldapbind profile is used for email
//* spoofing prevention.
//*
//* Then, permit the userid(s) read access for the profile.
//*
//* This example allows userid to submit an email to CSSMTP that is from test1@test.com:
//*
//* PERMIT test1@test.com CLASS(LDAPBIND) ID(userid) ACCESS(READ)
//*
//* If the CSSMTP Auth support has not been enabled, define the email address in the MailFrom as a profile in the LDAPBIND
//* class (one profile per email address).
//*
//* RDEFINE LDAPBIND test3@test.com UACC(NONE)
//*
//* Give the IDs userid and userid2 permission to submit an email to CSSMTP that is from test3@test.com:
//*
//* PERMIT test3@test.com CLASS(LDAPBIND) ID(userid) ACCESS(READ)
//* PERMIT test3@test.com CLASS(LDAPBIND) ID(userid2) ACCESS(READ)
```

- The CSSMTP configuration file will include a new parameter RestrictMailFrom to enable this function. (The default value for RestrictMailFrom is No)

```
Options
{
     RestrictMailFrom Yes
}
```

- MODIFY procname,DISPLAY,CONFIG

```
OPTIONS:
 NULLTRNC             : NO          DATALINETRUNC         : NO
 ATSIGN               : 7C          REPLACESUBJECTATSIGN  : YES
 TLSEHLO              : YES         TESTMODE              : NO
 RESTRICTMAILFROM     : YES
```

- If the Report option set to Admin, the ReportMailFrom email address must be defined in SAF, either as the WAEMAIL of the CSSMTP started procedure user or as an LDPBIND profile with READ access for the started procedure .

In addition to being planned for delivery in z/OS-Next, Email Spoofing Prevention support for CSSMTP is rolled back to z/OS 3.2 and z/OS 3.1 under APAR number PH68037

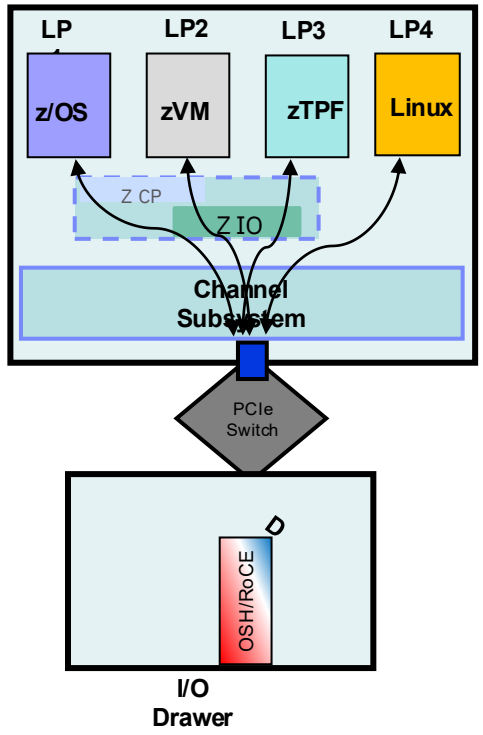
EQDIO support for the IBM z17 Network Express feature

The Network Express feature

- The Network Express feature combines the functionality of both the OSA-Express and RoCE Express features.
  - Can be viewed as the next generation “OSA” and “RoCE” adapter
- IBM Z customers will benefit from the increased I/O capacity, scale and density of the Network Express feature.
- Network Express allows RoCE and OSA networking features to converge into a single network feature reducing Z customers’ cost for physical networking resources (Z drawer I/O slots, adapters, ports, cables, switch ports).
- Network Express has been updated to support Enhanced QDIO (EQDIO) architecture allowing the updated z/OS Communications Server software to interact with the Network Express hardware using optimized operations required to meet the demand of the continuously growing I/O rates.
- EQDIO builds the foundation for the introduction of advanced Ethernet and networking capabilities for the future of IBM Z.

Network Express feature: Converged multi-function network adapter

- The Network Express provides Converged support for multiple networking protocols – provides ability to run existing functions on a single physical “appliance”
  - OSH – New Enhanced QDIO protocol capability
  - NETH – RoCE, RDMA, SMC-R & TCP/IP capabilities
- Characteristics
  - Multi-function networking adapter has 2 Ports per I/O Slot
    - Support for 10GbE and 25GbE
    - Each port on card is a unique CHPID (1 PCHID: 1 Port relationship)
    - Multiple protocols can share the same physical port
  - Each port can be configured to provide a single function or combination of functions
  - LPAR to LPAR traffic supported through the adapter



Network Express Feature: For more information at Summer SHARE

All Aboard the Network Express!
Tuesday, February 24, 2025: 10:30 AM - 11:30 AM
Salon 23
Speakers: Grant Mericle, Karthik Sundaresan

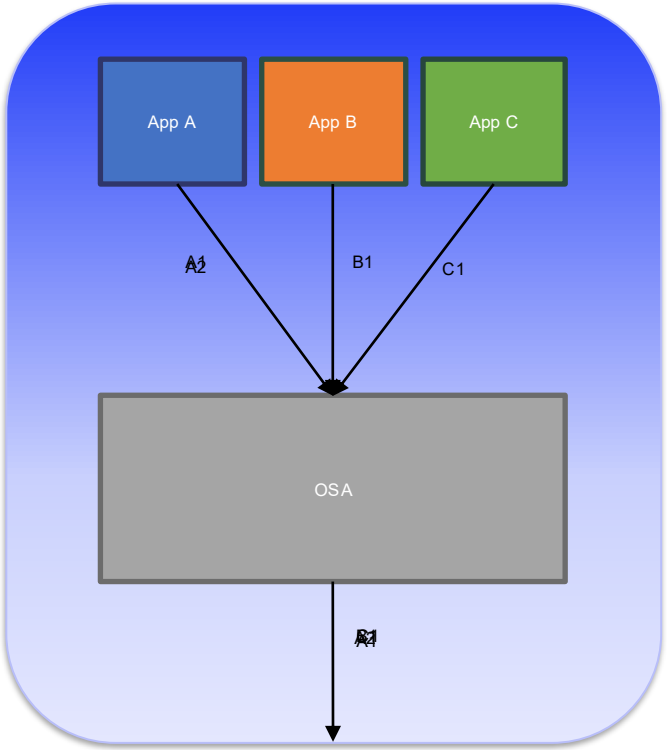
AI-powered network outbound packet batching

AI-powered network outbound packet batching: Background

What is standard processing of network outbound packets?

As data sent by applications is processed by TCP/IP stack, network interface is signaled

- Each interaction with network interface incurs some CPU consumption

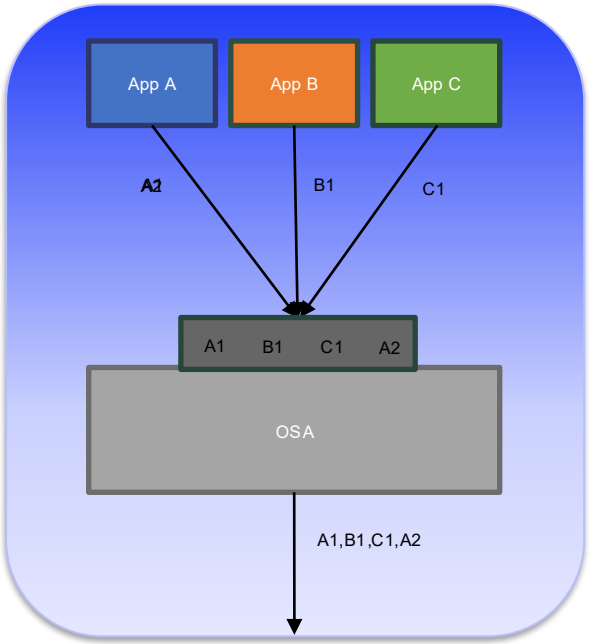


AI-powered network outbound packet batching: Background …

What is the goal of network outbound packet batching?

As data sent by applications is processed by TCP/IP stack, queue packets destined to same network interface and signal network interface with the batch

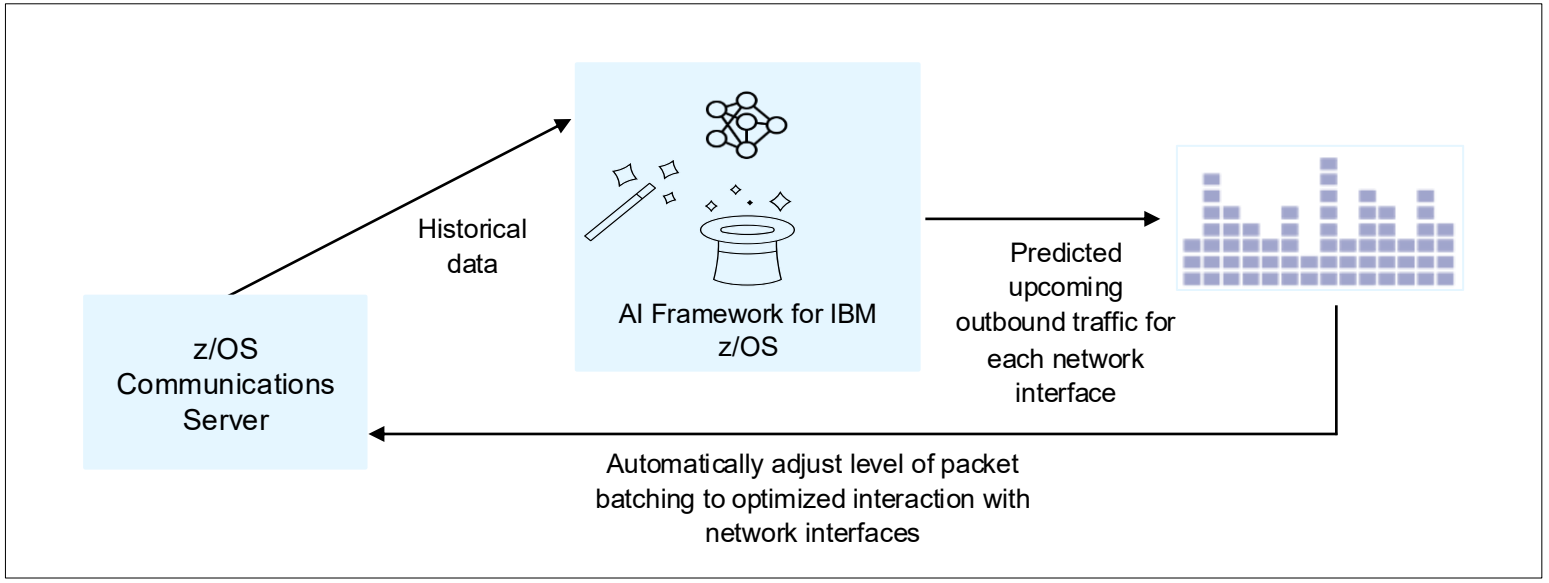
- Reducing the interactions with network interface should reduce network CPU consumption



AI-powered network outbound packet batching: Solution

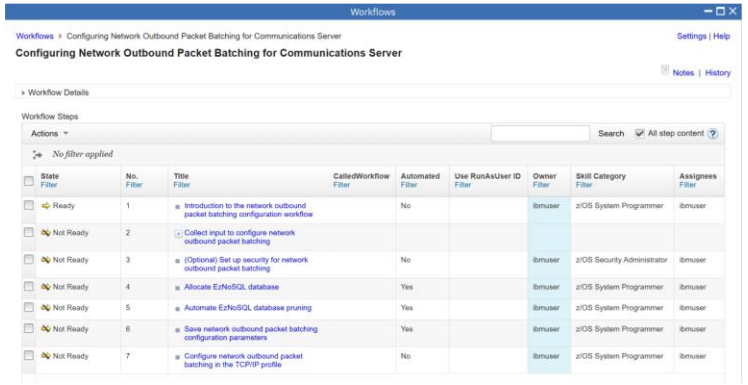
Leverage AI Framework for IBM z/OS

- Record historical data for changes in outbound network traffic patterns
- Train model to predict changes in outbound network traffic
- Use training results to predict when outbound network traffic changes will occur rather than react to network traffic changes
  - Should help to further reduce the interactions with network interfaces



AI-powered network outbound packet batching: Enablement

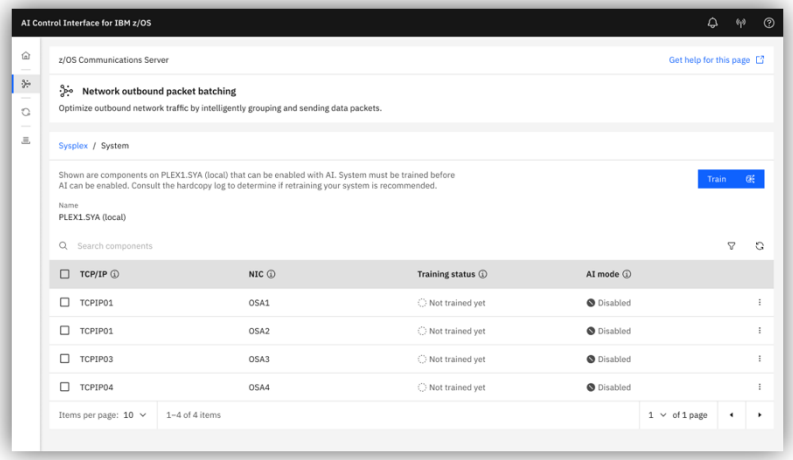
1. Configure AI Framework for IBM z/OS
   - New use case configured via z/OSMF workflows



2. Configure z/OS Communications Server
   - New TCP/IP profile statement
   - Optionally, use Network Configuration Assistant z/OSMF plugin

```
GLOBALCONFIG AIASSIST BATCHOUTbound
```

3. Enable AI Framework for IBM z/OS
   - Via AI Control Interface
   - Enable/Disable/Train network interface to use AI predictions



For more information at Winter SHARE

AI comes to z/OS networking
Monday , February 22, 2026: 3:45 PM – 4:45 PM
Salon 23
Speakers: Ben Hicks, Mary Julian

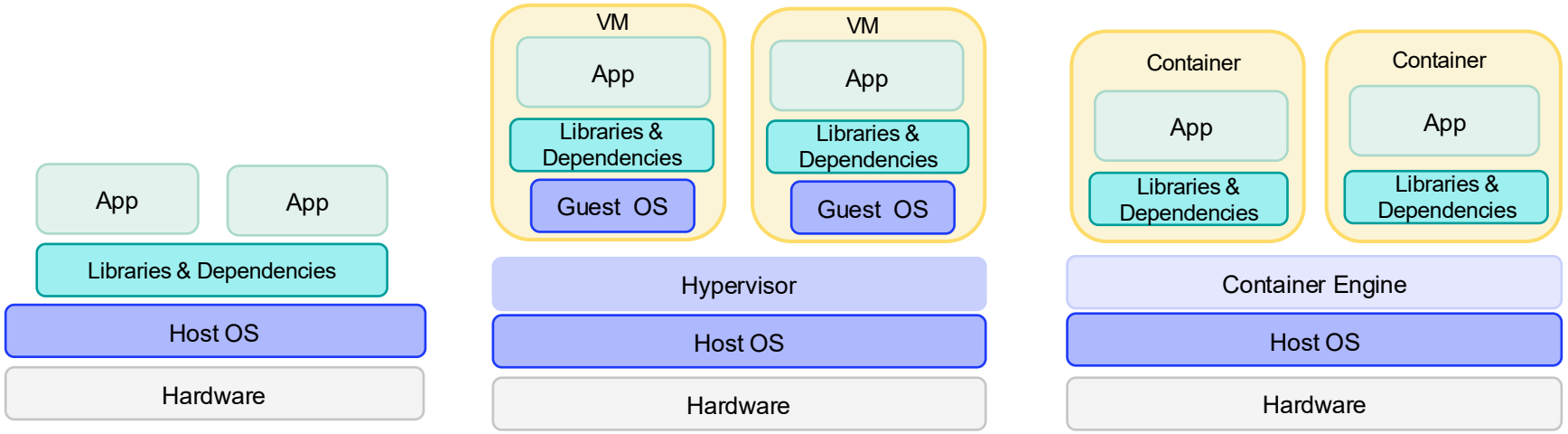
Deep Dive Into AI on IBM Z and LinuxONE
Tuesday, February 24, 2026: 9:15 AM – 10:15 AM
Salon 22
Speakers: Purvi Patel, Steve Warren

AI infused z/OS: Overview and Updates
Thursday, February 26, 2026: 9:15 AM – 10:15 AM
Salon 14
Speakers: Anastasiia Didkovska, Steve Partlow

Networking Support for z/OS Container Platform

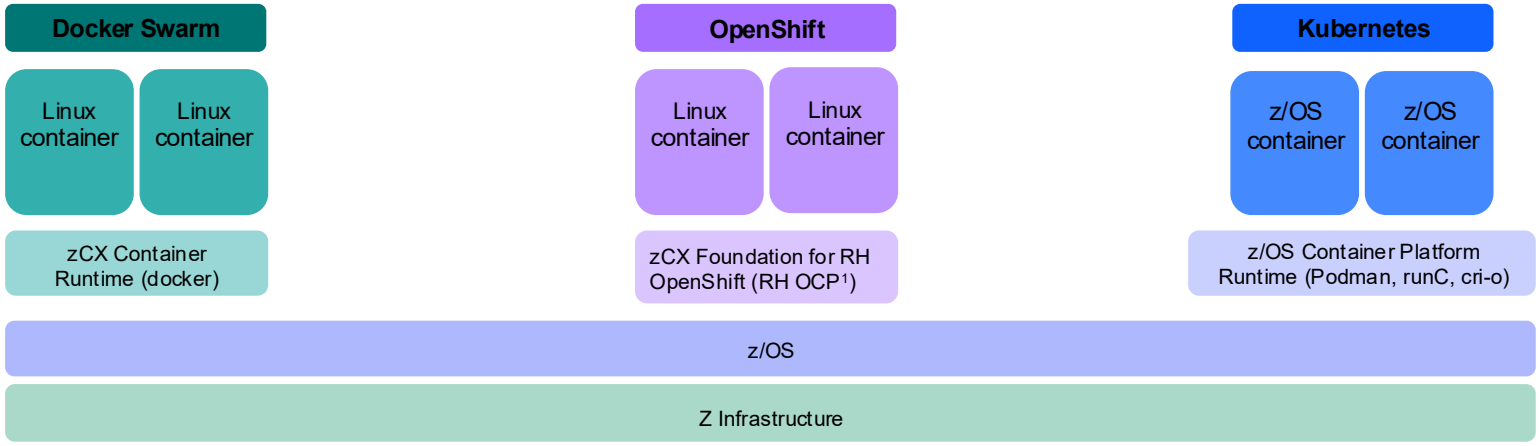
Evolution of Application Deployment

Personal Computer / Bare Metal	Virtual Machines	Containers
Dedicated hardware	Hardware virtualization	OS virtualization
Performance	Hardware utilization, different guest OSs	Fast deployment, scalability, portability
	Persistent, resource heavy apps, databases	Microservices, cloud native dev, DevOps



z/OS Container Platform positioning

z/OS Container Extension (zCX)	zCX Foundation for OpenShift	IBM z/OS Container Platform
• Containerized Linux on Z applications running on z/OS	• Containerized Linux on Z application running in Red Hat OpenShift on z/OS	• Containerized z/OS UNIX applications running on z/OS
• Linux applications requiring low latency access to z/OS apps/data	• Co-locating applications with non-containerized workloads/data on z/OS	• All cluster components run on z/OS
• Linux virtual appliance running as part of z/OS	• Red Hat CoreOS included with RH OpenShift	



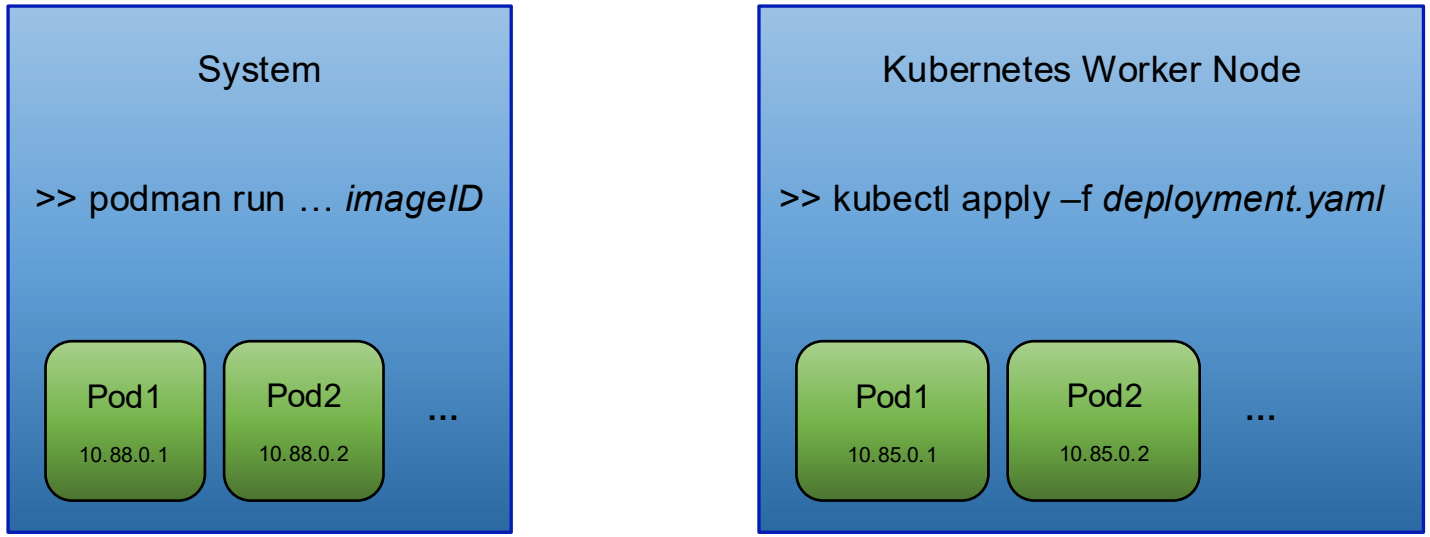
[1] OpenShift Container Platform includes Red Hat CoreOS, cri-o, Kubernetes, OpenShift

Container Network Interface (CNI)

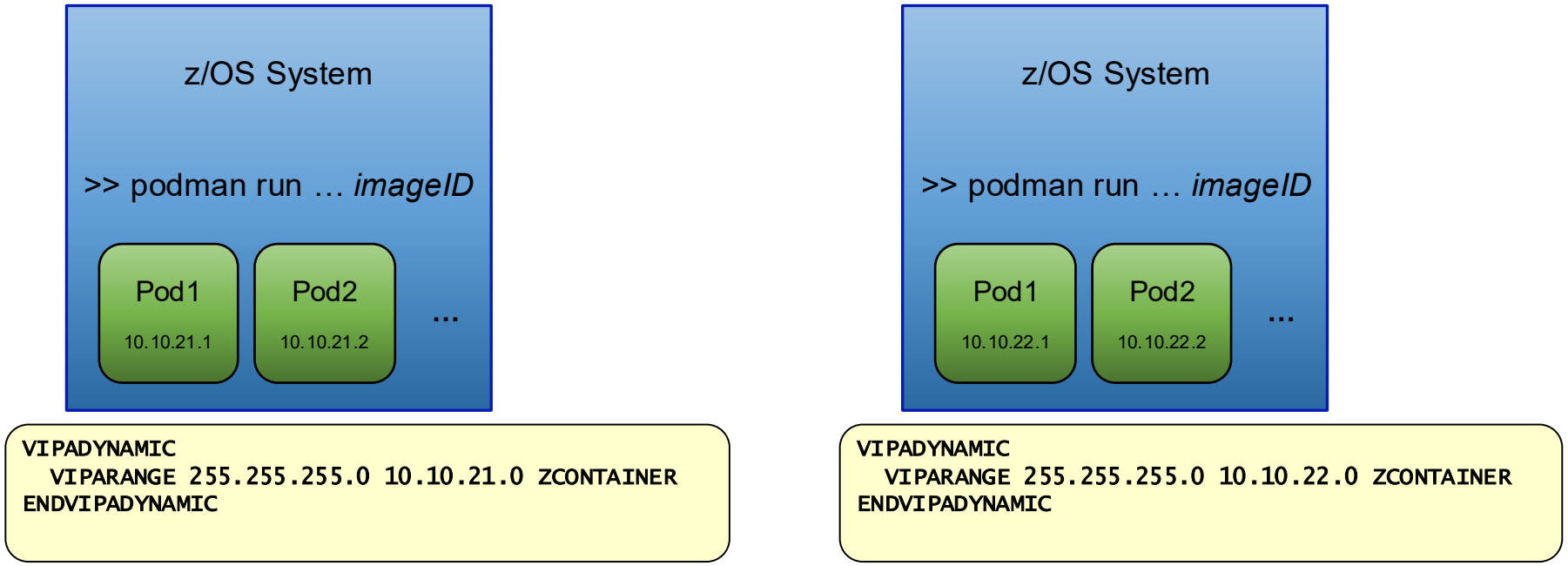
A **specification** to configure network interfaces in containers

- Concerned with adding, connecting and removing containers to/from networks via plugins
- Defines an interface for configuring the network, provisioning IP addresses, and maintaining connectivity with other containers and hosts
- https://github.com/containernetworking/cni/blob/main/SPEC.md

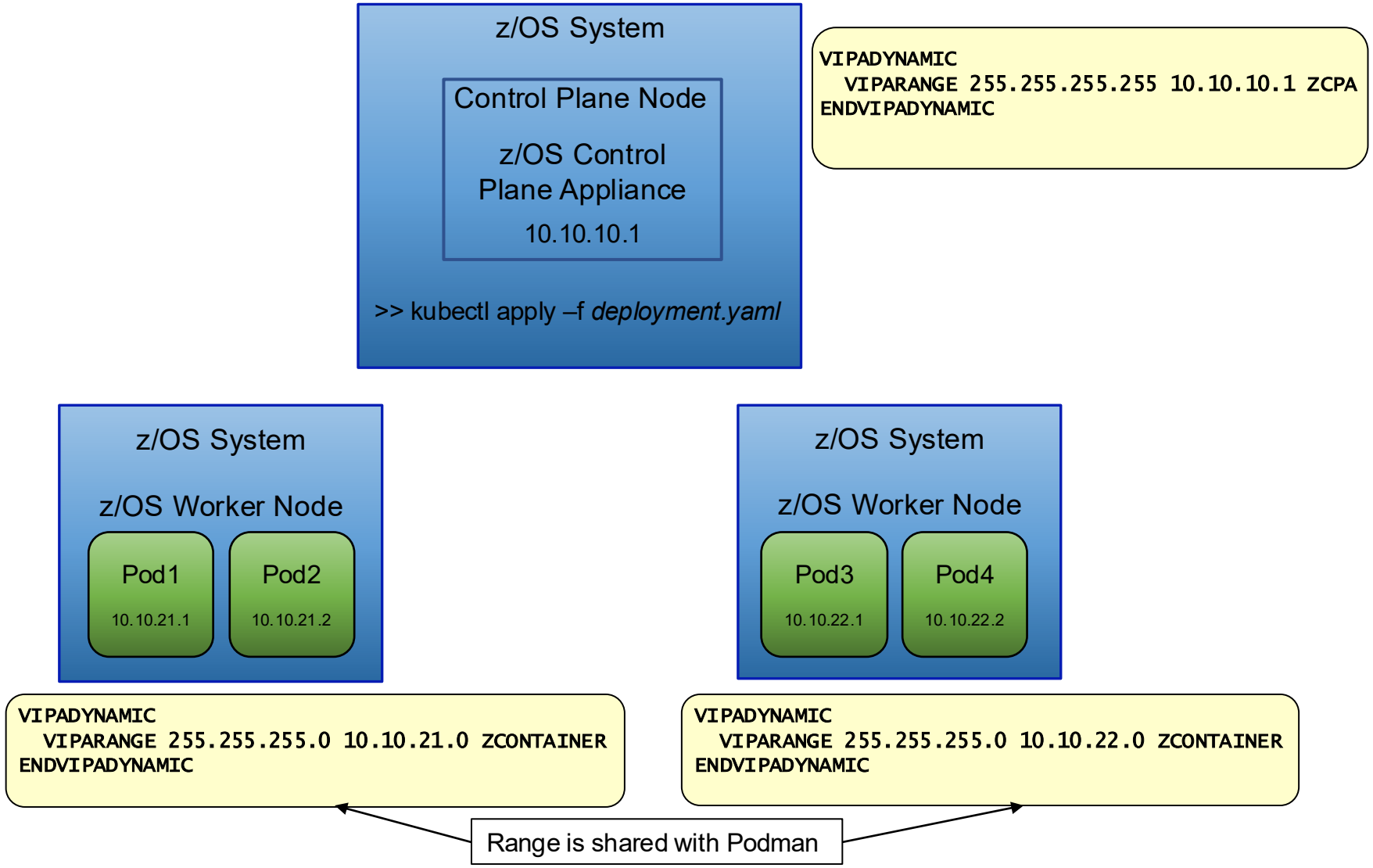
CNI plugins invoked by container runtimes such as Podman or cri-o (for Kubernetes)



z/OS Container Network Interface - Podman

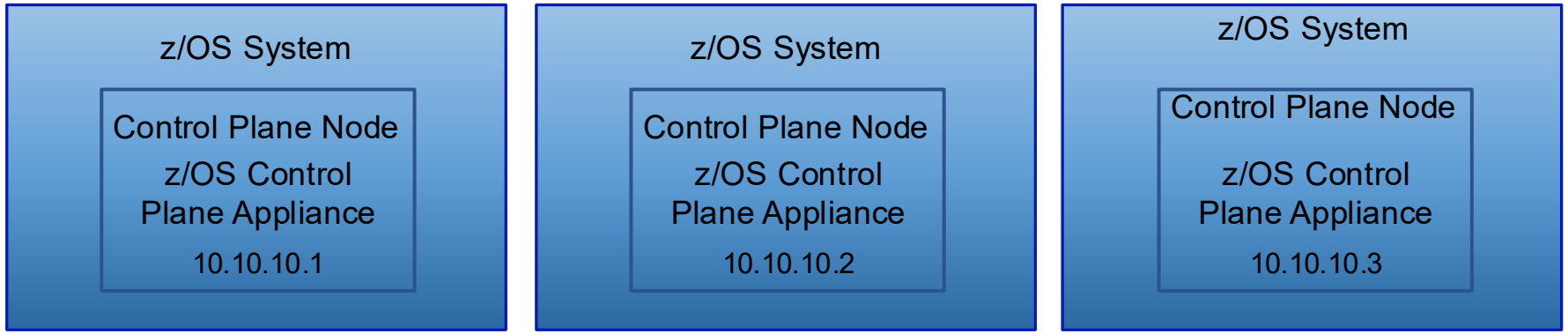


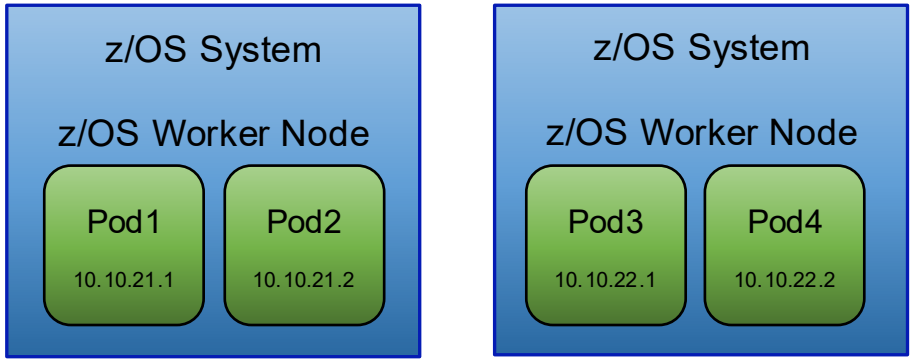
z/OS Container Network Interface - Kubernetes



z/OS Container Platform – HA Kubernetes clusters

```
VIPADYNAMIC
 VIPADISTRIBUTE DISTMETHOD ROUNDROBIN EXTTARG 10.1.1.1 DESTIP 10.10.10.1 10.10.10.2 10.10.10.3
ENDVIPADYNAMIC
```





...

Single ZCONTAINER VIPARANGE statement feedback

- A single subnet may not be sufficient for containers created for both Podman and Kubernetes users
  - Want the ability to combine multiple subnets into a “pool” of IP addresses for z/OS container use
- A single VIPARANGE statement does not allow for different “pools” to be defined for different classes of Podman users (i.e. development and test)
  - Want to permit different users access only to a specific “pool” of IP addresses
- A single VIPARANGE statement forces that sharing of the subnet between different use cases (Podman and Kubernetes)
  - Want to provide separate “pools” of IP addresses

Multiple ZCONTAINER VIPARANGE statements

- One or more VIPARANGE statements can be combined to form a larger “pool” of IP address for containers on z/OS
  - Applies to both IPv4 and IPv6 VIPARANGEs
- Utilize the SAF keyword on the VIPARANGE statement to permit specific use case(s) for a “pool” of IP addresses
  - Separate “pools” for different Podman users and/or Podman and Kubernetes users

Example of Multiple ZCONTAINER VIPARANGE statements

```
VIPARANGE DEFINE 255.255.255.248 10.10.17.216 SAF PODMAN1 ZCONTAINER
VIPARANGE DEFINE 255.255.255.248 10.10.10.232 SAF PODMAN2 ZCONTAINER
VIPARANGE DEFINE 255.255.255.255 10.10.10.225 SAF PODMAN1 ZCONTAINER
VIPARANGE DEFINE 255.255.255.248 10.10.10.240 SAF K8SGRP  ZCONTAINER
```

- The ordered list of available IP addresses for z/OS containers would be allocated as follows:
  - For Podman users with access to SAF resource PODMAN1:

    10.10.10.217, 10.10.10.218, 10.10.10.219, 10.10.10.220, 10.10.10.221, 10.10.10.222, 10.10.10.225
  - For Podman users with access to SAF resource PODMAN2:

    10.10.10.233, 10.10.10.234, 10.10.10.235, 10.10.10.236, 10.10.10.237, 10.10.10.238
  - For Kubernetes users with access to SAF resource K8SGRP:

    10.10.10.241, 10.10.10.242, 10.10.10.243, 10.10.10.244, 10.10.10.245, 10.10.10.246

z/OS Container Platform - Kubernetes dashboard

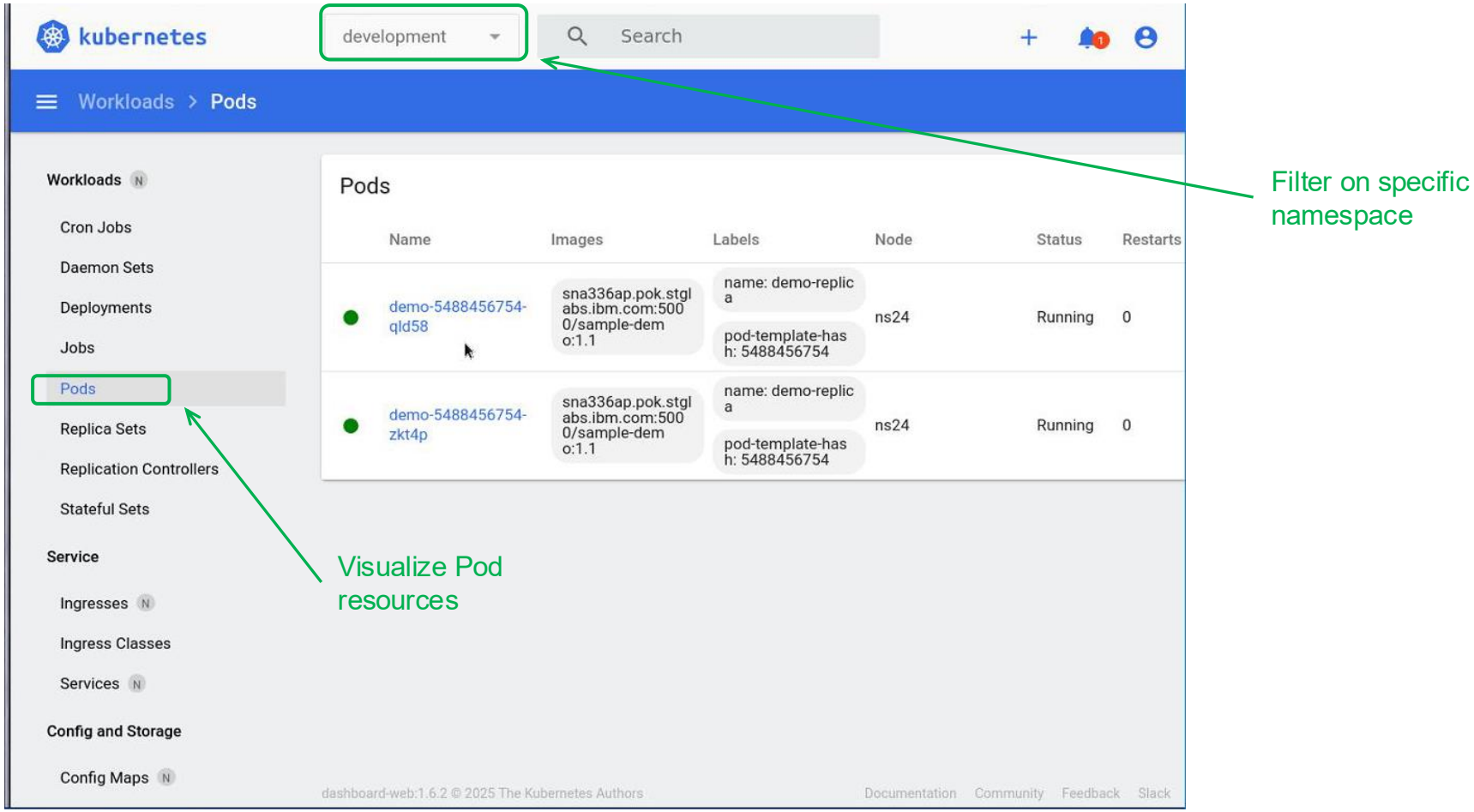
- Interacting with Kubernetes cluster requires familiarity with kubectl z/OS UNIX command line utility as well as with all combinations of command line options
  - How do I find which dynamic VIPA was assigned to a specific Kubernetes pod?

```
>> kubectl get pods -n development
NAME                  READY STATUS  RESTARTS AGE
demo-5488456754-qld58 1/1   Running 0        23m
demo-5488456754-zkt4p 1/1   Running 0        23m

>> kubectl get pod demo-5488456754-qld58 -n development -o=jsonpath='{.status.podIP}'
192.168.1.2
```

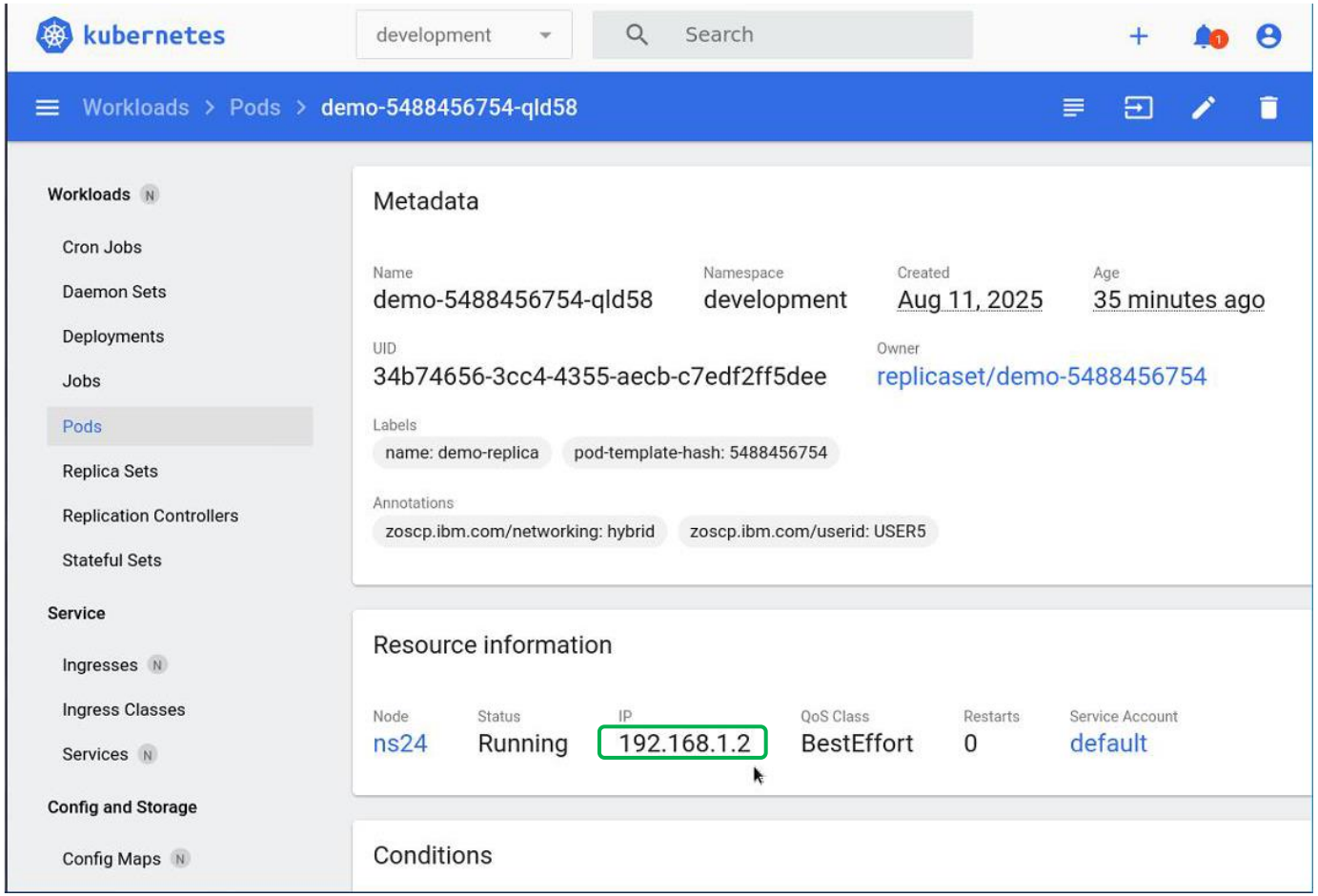
z/OS Container Platform - Kubernetes dashboard UI

- Using the Kubernetes dashboard simplifies monitoring of cluster resources



z/OS Container Platform - Kubernetes dashboard UI…

- Using the Kubernetes dashboard simplifies monitoring of cluster resources



More sessions about z/OS Container Platform at Summer SHARE

Introducing the z/OS Container Platform
Wednesday, Febraury 25, 2026: 9:15 AM - 10:15 AM
Salon 13
Speakers: Mary Julian, Ben Hicks

Configuring Networking for z/OS Container Platform
Wednesday, February 25, 2026: 2:30 PM - 3:30 PM
Salon 16
Speakers: Paul Gartman, Ben Hicks

Increase

VIPADISTRIBUTE

Ports

VIPADISTRIBUTE PORT keyword

- Used to specify one or more individual ports, ranges of ports, or a combination of individual ports and ranges
  - Servers that bind to the specified DVIPA, 0.0.0.0, or :: (IPv6 unspecified address) and one of the specified ports, cause the target stack to become eligible to receive connection requests
- The maximum number of ports that is specified, including all individual ports and all ports within ranges, could not exceed 64
  - Capped the size of XCF messages that could be sent between TCP/IP stacks in the Sysplex
  - But requires new VIPADISTRIBUTE IP addresses to be defined once the port limit is reached

VIPADISTRIBUTE PORT limit raised

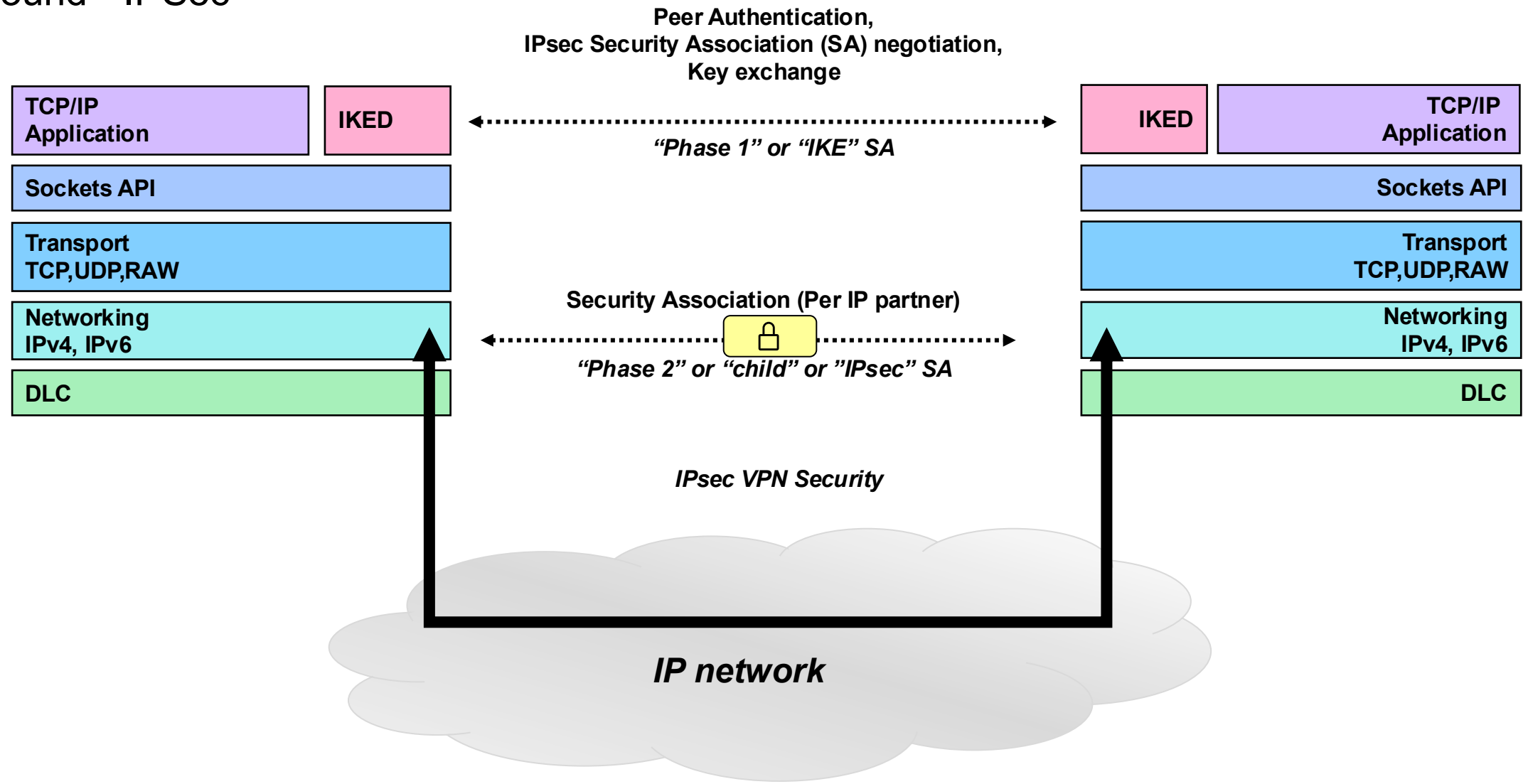
- The maximum number of ports that is specified, including all individual ports and all ports within ranges, has been raised to 256
  - Available on z/OS 3.1 via APAR PH63320

- Care should be taken to not combine large numbers of both ports (via the PORT keyword) and target TCP/IP stacks (via DESTIP statement)
  - Could result in very large XCF messages that could impact the performance of Sysplex Distributor
  - Recommendation is to use DESTIP ALL when configuring more than 64 ports on a VIPADISTRIBUTE statement

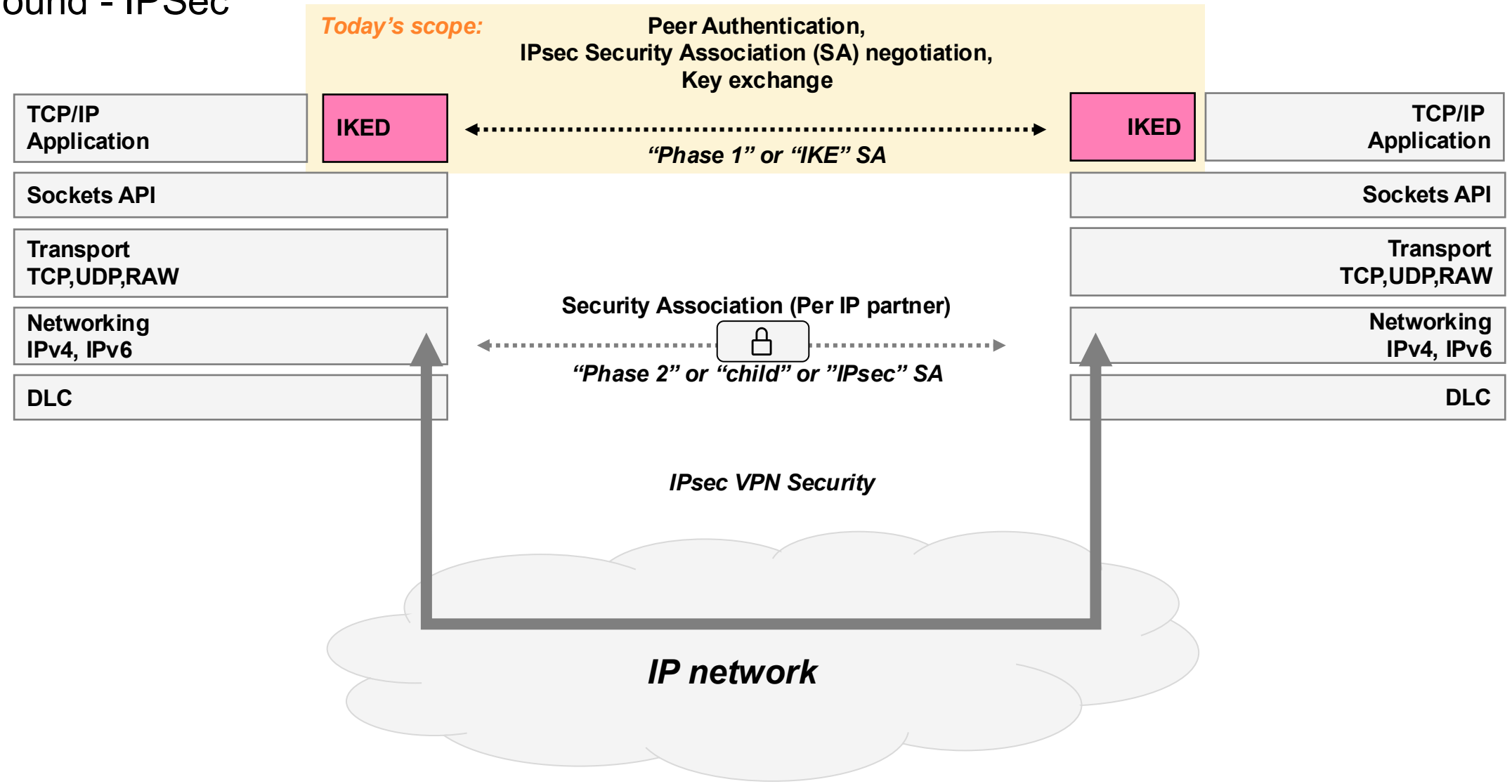
Network Security Enhancements

Support for AES-GCM for IKEv2 SA

Background - IPSec



Background - IPSec



Support for AES-GCM for IKEv2 SA

- With **z/OS 3.2 and 3.1 APAR PH68240**, you can use Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) to protect IPSec using IKEv2 key exchanges.
  - Implements RFC 5282 - *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol*
  - AES-GCM combines encryption and integrity into a single operation, referred to as a combined mode algorithm.
  - This algorithm has been long available as an option for IPsec/Child SA tunnels to protect TCP/IP data.
- **z/OSMF Network Configuration Assistant 3.2 and 3.1 APAR PH68902** provides new settings to configure use of AES-GCM for the IPSec discipline.

Restrictions:

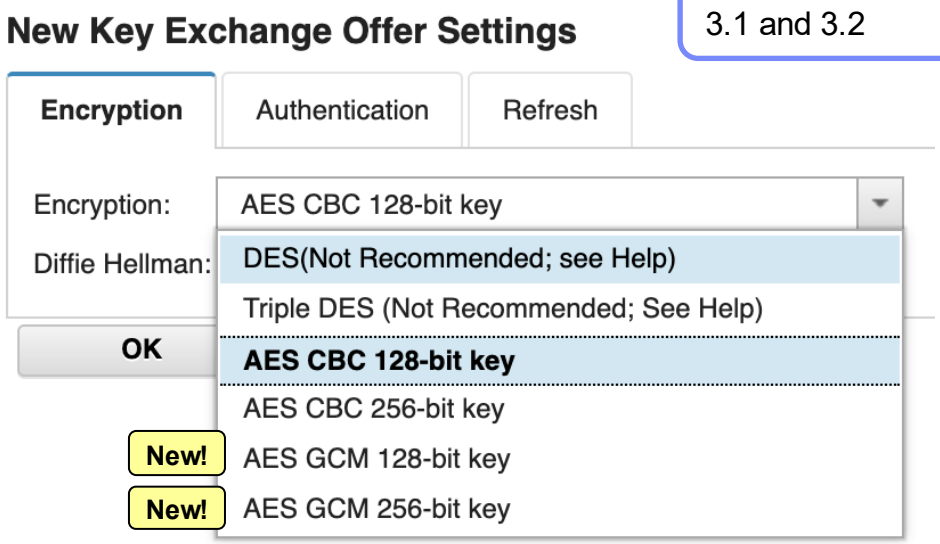
- **IKEv2 only** – IKEv1 has been deprecated by the IETF with no new support
- **Non-FIPS only** – When IKED is configured for FIPS-140, AES-GCM is not supported on the KeyExchangeOffer

- This addresses the following open requirement:
  - ZOS-I-4518 - IKE Data Offer to add GCM blocking ciphers

Support for AES-GCM for IKEv2 SA – Network Configuration Assistant changes

- New dropdown options are added to the **Advanced → Key Exchange Offer Settings** panel for the IPSec *Connectivity* or *Reusable Rule*:
  - Encryption: AES GCM 128-bit key
  - Encryption: AES GCM 256-bit key
- Use of AES-GCM in **Encryption** tab will carry over dropdown setting to the **Authentication** tab's *IKEv2 Message Authentication* field.
  - Remember, AES-GCM provide both encryption and message authentication function.

NCA APAR PH68902
3.1 and 3.2



IKEv2 Advanced Key Exchange Offer Settings must be configured on a rule-by-rule basis to use AES-GCM for the IKEv2 key exchange proposal.

This configuration is not to be confused with the Security Level configuration used for specifying "phase 2" or "Child"/"IPSec" SA use of AES-GCM to protect IP data.

Support for AES-GCM for IKEv2 SA – Policy configuration

`HowToEncrypt`, **`KeyExchangeOffer`** parameter

- Encryption algorithm for protecting key exchanges
- New value: `AES_GCM_16 KeyLength keylen`

```
    .-HowToEncrypt--DES----------------------------.
|--+-------------------------------------------------+-------->
   '-HowToEncrypt--+-DES-------------------------+-'
                   +-3DES------------------------+
                   +-AES-------------------------+
                   +-AES_CBC KeyLength keylen----+
                   '-AES_GCM_16 KeyLength keylen-'
```

Support for AES-GCM for IKEv2 SA – Policy configuration

`HowToVerifyMsgs`, **`KeyExchangeOffer`** parameter

- Authentication algorithm for verifying message integrity of IKE version 2 key exchanges
- New value: `Null`
  - Only valid when `HowToEncrypt AES_GCM_16`
  - Required when `HowToEncrypt AES_GCM_16`

```
   .-HowToVerifyMsgs--HMAC_SHA1_96----------.
>--+-------------------------------------+-----------------><
   '-HowToVerifyMsgs--+-Null--------------+-'
                      +-AES128_XCBC_96----+
                      +-HMAC_MD5_96-------+
                      +-HMAC_SHA1_96------+
                      +-HMAC_SHA2_256_128-+
                      +-HMAC_SHA2_384_192-+
                      '-HMAC_SHA2_512_256-'
```

Support for AES-GCM for IKEv2 SA – SMF and NMI updates

SMF:

SMF type 119 subtype type 73 (IPSec IKE tunnel activation and refresh record)

SMF type 119 subtype type 74 (IPSec IKE tunnel deactivation and expire record):

- `SMF119IS_IKETunEncryptAlg`: new value **`SMF119IS_ENCR_AES_GCM_16` (20)**
- `SMF119IS_IKETunAuthAlg`: new value **`SMF119IS_AUTH_NULL` (0)**

See `SMF119IS_IKETunEncryptKeyLength` to verify the AES-GCM key length.

NMI:

Local IPSec NMI and Network Security Services (NSS) NMI: `Nmsec_GET_IKETUN`

- `NMsIKETunEncryptAlg` new value **`NMsec_ENCR_AES_GCM_16` (20)**
- `NMsIKETunPeerAuthMethod`: new value **`NMsec_AUTH_NULL` (0)**

See `NMsIKETunEncryptKeyLength` to verify the AES-GCM key length.

Support for AES-GCM for IKEv2 SA – zERT SMF and NMI reporting

zERT SMF and NMI data can also be used to verify use of AES-GCM!

SMF:

- SMF 119, subtype 11 (zERT connection detail record)
  - zERT connection detail IPSec protocol attributes section:
    - `SMF119SC_IPSec_IKETunEncAlg`
    - `SMF119SC_IPSec_IKETunAuthAlg`
- SMF 119, subtype 12 (zERT summary record)
  - zERT summary record IPSec protocol attributes section
    - `SMF119SS_IPSec_IKETunEncAlg`
    - `SMF119SS_IPSec_IKETunAuthAlg`

NMI:

- Real-time TCP network monitoring interface (NMI) available through **`SYSTCPER`** & **`SYSTCPES`** services.

Support for AES-GCM for IKEv2 SA – Important bug fix reminder

Bug fix: Support of AES-GCM proposal in the IKEv2 key exchange, even if you are not exploiting it.

If AES-GCM is configured as one of several proposals for the IKEv2 key exchange, action is required for any z/OS IKE peer(s) that do not have support for AES-GCM:

The z/OS IKE peers must have the PTF for APAR PH69019 installed. APAR PH69019 resolves a problem that causes an IKEv2 negotiation with an AES-GCM proposal to fail even when there is also an acceptable proposal.

Available for z/OS 3.2, 3.1, and 2.5.

To enable and use AES-GCM for the IKEv2 key exchange

The z/OS IKE peer must have 3.2 and 3.1 PTF for APAR PH68240 must be installed.

Available for z/OS 3.2 and 3.1.

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remain at our sole discretion.

zERT monitoring enhancements

zERT monitoring and recording deficiencies

- The current z/OS Encryption Readiness Technology monitoring and recording implementation suffers from several deficiencies.
- z/OS 3.2 Communications Server has enhanced zERT to easily distinguish between TLS/SSH connections (successful and failed) and unprotected connections and provide all the information necessary to ensure that the network traffic is protected per network policy.
- This addressed several open requirements:
  - Idea ZOS-I-3371 – Enable zERT to Detect Partial/Failed Secure Handshakes
  - Idea ZOS-I-339 – Certificate details, particularly serial and expiry date, on SMF119-12
  - Idea ZOS-I-3963 – Add Client/Server role indicator into ZERT SMF 119 Subtype 11 Records
- The details are discussed on the next four charts.

zERT monitoring enhancements

- Currently, writing unprotected record when a TLS/SSL or SSH handshake fails with no indication of the attempt
  - zERT only reports on successful TLS/SSL and SSH handshakes. If a handshake fails, zERT reports it as an unprotected session – there is no indication that a handshake was attempted and failed
- In 3.2, when a TLS/SSH handshake fails zERT will not generate an unprotected record anymore
  - Subtype 11 detail record with a TLS/SSH section and a new indicator of ‘Failed handshake’
  - Subtype 12 summary record – new counts for the failed handshakes during that interval

zERT monitoring enhancements …

- Currently writing unprotected record when a TLS/SSL or SSH handshake is in progress (10 second timer pops)
  - When the init timer pops, we cut an unprotected record. An additional protection change record is written if the handshake completes and the cryptographic protocol provider tells us
- In 3.2, when a TLS/SSH handshake is in progress
  - zERT has detected the beginnings of a handshake, it will write a record for the connection only when the TLS/SSH handshake completes successful or fails. It will not write a record when the handshake is in progress.

zERT monitoring enhancements …

- Currently writing unprotected protection change record when a TLS session is terminated, and the TCP connection takes >1 second to terminate but no further application data flows
  - The TLS connection is explicitly terminated, causing System SSL to notify zERT of the change AND no additional data passes over the TCP connection after the TLS session is terminated by an inbound RST packet, BUT more than one second passes before the TCP connection is terminated
- In 3.2, When a TLS session is terminated, zERT will not write a record until the TCP connection is terminated (term or short-term record) or data flows on the TCP connection in the clear (protection state change record)

zERT monitoring enhancements …

- Currently, the client and server certificate information are only recorded in the subtype 11 records, not in subtype 12
- In 3.2, zERT aggregation will record the **certificate expiration dates and certificate serial** in subtype 12 records (similar to what we do in subtype 11).
  - SMF119SS_ proto_xCert_Serial_Len, SMF119SS_proto_xCert_Serial, SMF119SS_ proto_xCert_Time_Type and SMF119SS_ proto_xCert_Time (where x is S for server certificate information and C for client certificate information, Lcl for IKE Local certificate information and Rmt for IKE Peer certificate information; proto is TLS or IPsec)

- Currently, the flag to indicate whether the local socket is acting as the TCP client or server is only in subtype 12 records, not in subtype 11
- In 3.2, zERT discovery will record the indicator that tells whether the local socket is acting as the TCP client or server in subtype 11 records (similar to what we have in subtype 12)

zERT monitoring enhancements …

- The zERT monitoring enhancements are available on z/OS V2R5 and z/OS 3.1 via APAR PH65586.

z/OS Encryption Readiness Technology

Scan the QR code to visit z/OS Communications Server on IBM Community. (https://ibm.biz/cscommunity)

IBM zERT Network Analyzer enhancements - *new in z/OS 3.1*

- **reduce manual effort and optimize user experience** with IBM zERT Network Analyzer Upgrade Support
- **support passphrases and to allow clearing database user ID and password** with IBM zERT Network Analyzer enhancements for database connection authentication

What are users saying about zERT?

- "We're building self-serve capability for each business unit with zERT data as the basis for monitoring security of the mainframe"
- "We use zERT data for compliance checks."
- "zERT even provides real-time policy-based notifications when cryptographic usage doesn't match my expectations!."

Visit *Things you should know about zERT* on IBM Community and discover blogs, product documentation, videos, event information, webinar, and presentations about zERT.

zERT: For more information at Summer SHARE

TCP/IP Security Controls*
Wednesday, February 25, 2026: 9:15 AM - 10:15 AM
Salon 21
Speakers: Navya Ramanjulu, Ed Seidl

AT-TLS Hints and Tips*
Wednesday, February 25, 2026 : 3:45 PM - 4:45 PM
Salon 20
Speakers: Navya Ramanjulu, Ed Seidl

*** Qualifies towards Security Warrior Digital Badge**

Update to System SSL and AT-TLS default values in z/OS 3.2

- With the continued direction to improve the security of TLS connections, System SSL and AT-TLS will be updated to strengthen the defaults for protocols, ciphers, and signature algorithms for applications that rely on defaults.
  - This affects System SSL, AT-TLS, the z/OS FTP client, and the policy agent client.
- Details are included in the appendix.
- It is recommended to not rely on the defaults. Instead, configure the values required for your installation and use strong values.

Statement of Direction: Deprecated CMS, SSL APIs, SSLv2 and SSLv3 protocols (Issued July 22, 2025)

z/OS 3.2 is planned to be the last release to support the deprecated CMS, SSL APIs, SSLv2 and SSLv3 protocols. The Internet Engineering Task Force (IETF) deprecated SSL V2.0 in 2011 and SSL V3.0 in 2015. All z/OS System SSL and AT-TLS applications will need to change to use the newer protocols, and all z/OS System SSL applications that make use of the deprecated APIs will need to be changed to use the corresponding newer APIs. These APIs are documented in the z/OS Cryptographic Services within the Deprecated Secure Socket layer (SSL) APIs and the Certificate Management Services (CMS) API reference chapters.

Additional Information

z/OS 3.1 Communications Server Performance Summary Report

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

3.1: z/OS COMMUNICATIONS SERVER PERFORMANCE SUMMARY REPORT

https://ibm.biz/zcs31perfsummary

z/OS CS Performance Summary Reports for all releases are available, in the “z/OS Communications Server Performance Index” at:

https://www.ibm.com/support/pages/zos-communications-server-performance-index

z/OS Communications Server Performance Update
Tuesday, February 24, 2026: 3:45 PM – 4:45 PM
Salon 16
Speakers: Christopher Nyamful

The IBM Ideas Portal

A New Way to Submit Ideas

The IBM Ideas Portal provides a new way for customers, business partners and IBMers to suggest changes to our products and services, replacing the Request for Enhancements (RFE) process.

Why is it changing?

The IBM Ideas Portal is a single, company-wide portal, which will improve your experience by providing you with:

a single view into your ideas

an easier way to track them

the ability to collaborate with users, partners and IBMers around the world.

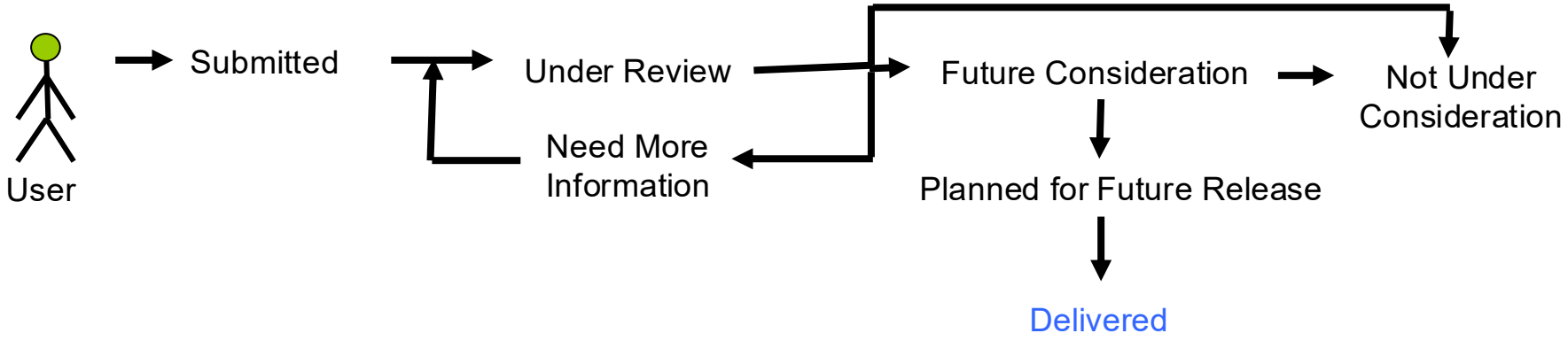
Use ideas.ibm.com to:

- Submit new ideas
- View the status of ideas you have previously submitted
- Vote, comment or subscribe to others' ideas
- View the status of ideas you have previously voted or commented on, or subscribed to

For more details about the migration, visit www.ibm.com/ideas

The new IBM Software Ideas portal for mainframe hardware and operating systems:
https://ibm-z-hardware-and-operating-systems.ideas.ibm.com/?project=ZOS

The IBM Ideas Portal …



- When you submit an Idea, please describe the problem you need to address, not just your suggested solution.
  - This helps us to better prioritize your Idea.
  - It also provides us with the opportunity to suggest alternate solutions or workarounds.
- Our responses to questions and comments cannot include unannounced delivery plans.

Digital Badges & Online Courses

Start your free IBM online learning and earn IBM open badges!

Networking on z/OS - Foundations

Foundational understanding of networking on z/OS.

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

z/OS TCP/IP Configuration with NCA

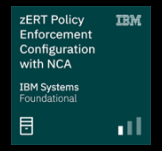
Use the IBM Configuration Assistant for z/OS Communications Server (NCA) to create and manage TCP/IP profiles.

- **IBM Open Badge:** http://ibm.biz/NCAbadge
- **Online course:** http://ibm.biz/NCATCPIPcourse

z/OS Network Security - Foundations

Knowledge and foundational understanding of z/OS network security.

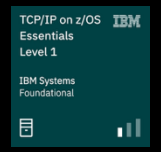
- **IBM Open Badge:** http://ibm.biz/zosnetsecuritybadge
- **Online course:** http://ibm.biz/zosnetsecuritycourse



zERT Policy Enforcement Configuration with NCA

Configure zERT Policy Enforcement using the IBM Configuration Assistant for z/OS Communications Server (NCA)

- **IBM Open Badge:** http://ibm.biz/NCA_zERTbadge
- **Online course:** http://ibm.biz/NCA_zERTcourse



TCP/IP on z/OS Essentials - Level 1

General knowledge and understanding of TCP/IP on z/OS, including network layers, protocols at each layer, and the hardware that facilitates the transport of data.

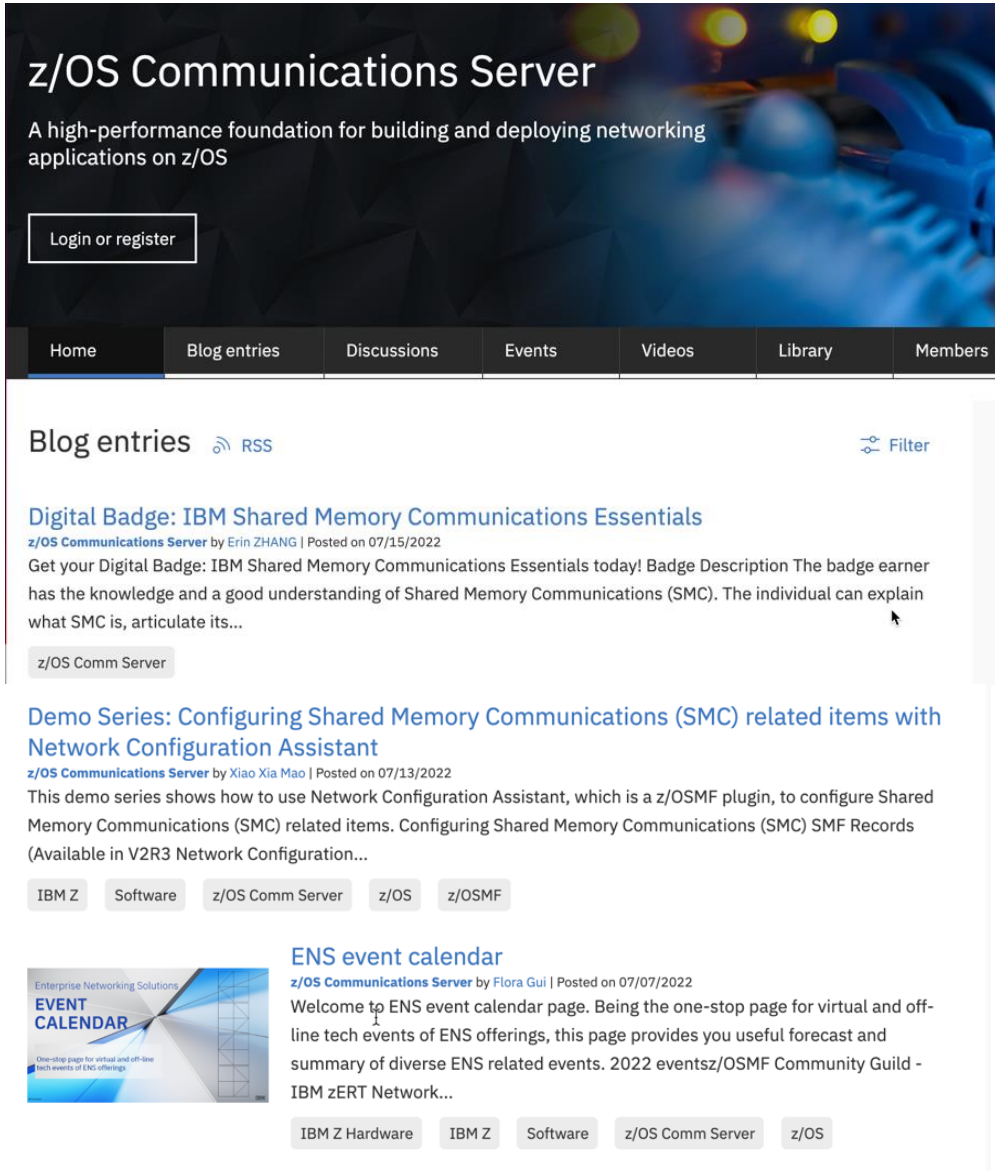
- **IBM Open Badge:** http://ibm.biz/tcpipl1badge
- **Online course:** https://ibm.biz/tcpipl1course

Join Us on the IBM Community!

The z/OS Communications Server page on the IBM Community provides rich and up-to-date technical content including blogs, videos, and event information.

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.



Additional z/OS Communications Server sessions at Summer SHARE

Rejoining the Tech Workforce: Strategies for a Successful Comeback
Tuesday, February 23, 2026: 2:30 PM - 3:30 PM
Salon 23
Speakers: Upeksha Vidanapathirana

Using IBM AI Generative Tooling to Assist with Code Development
Thursday, February 26, 2026: 10:30 AM - 11:30 AM
Salon 22
Speakers: Ben Hicks, Mary Julian

Sysplex Network Technologies and Considerations
Thursday, February 26, 2026: 2:30 PM - 3:30 PM
Salon 16
Speakers: Paul Gartman, Grant Mericle

*** Qualifies towards Security Warrior Digital Badge**

SHARE Security Warrior Digital Badge

- Explore all eligible sessions in the technical agenda
  - Filter ‘Digital Badge’ for ‘Security Warrior’
- Earn a Security Warrior digital badge
  - Attend **10** eligible sessions
  - Submit a Security Warrior badge form (link available on the Digital Badges page)
  - Claim your badge via email from SHARE HQ
- Session 117: z/OS Communications Server Technical Update: Winter 2026 Edition

Experience more with IBM

Visit us at the IBM Booth #113

After a full day of technical sessions, take a break with us!

Connect with our experts, snap a photo with the z17 Plexi or the latest Telum II, and get an up-close look at our Spyre Accelerator.

Come back each day for fresh topics and demos at our expert stations.

Think 2026

Join 5000+ senior business and technology leaders who are seizing the AI revolution to unlock unprecedented growth and productivity at Think 2026.

Find out more information using the QR code below.

IBM Digital Asset Haven

IBM Digital Asset Haven is the operational backbone for financial institutions and regulated enterprises entering the digital asset economy.

Find out more information using the QR code below.

Want to attend an in-person IBM z/OS Academy?

Learn, **Interact** and **Network** with IBMers and peers

May 5th- 7th, 2026	**Fall 2026**
IBM Tech Campus	**IBM US**
Ehningen, Germany	**New York, USA**

These **free** events are designed for early tenure z/OS system programmers (2-10 years), but all are welcome!

Training and presentations include topics on new z/OS capabilities, best practices, career tips, and **much more!**
Subscribe to the community page today to stay informed about future events!

Register now for Ehningen/ Germany:

Join our IBM Community: https://ibm.biz/zOSAcademy
Questions? Contact us at zOS.Academy.USA@us.ibm.com or zOS.Academy.Europe@de.ibm.com

Your feedback is important!

Submit a session evaluation for each session you attend:

www.share.org/evaluation

Thank You!

Any Questions?

Paul Gartman – Paul.Gartman@ibm.com
Enterprise Networking Solutions – Developer (Containers and AI)

Ed Seidl – eseidl@us.ibm.com
Enterprise Networking Solutions – Developer (Security)

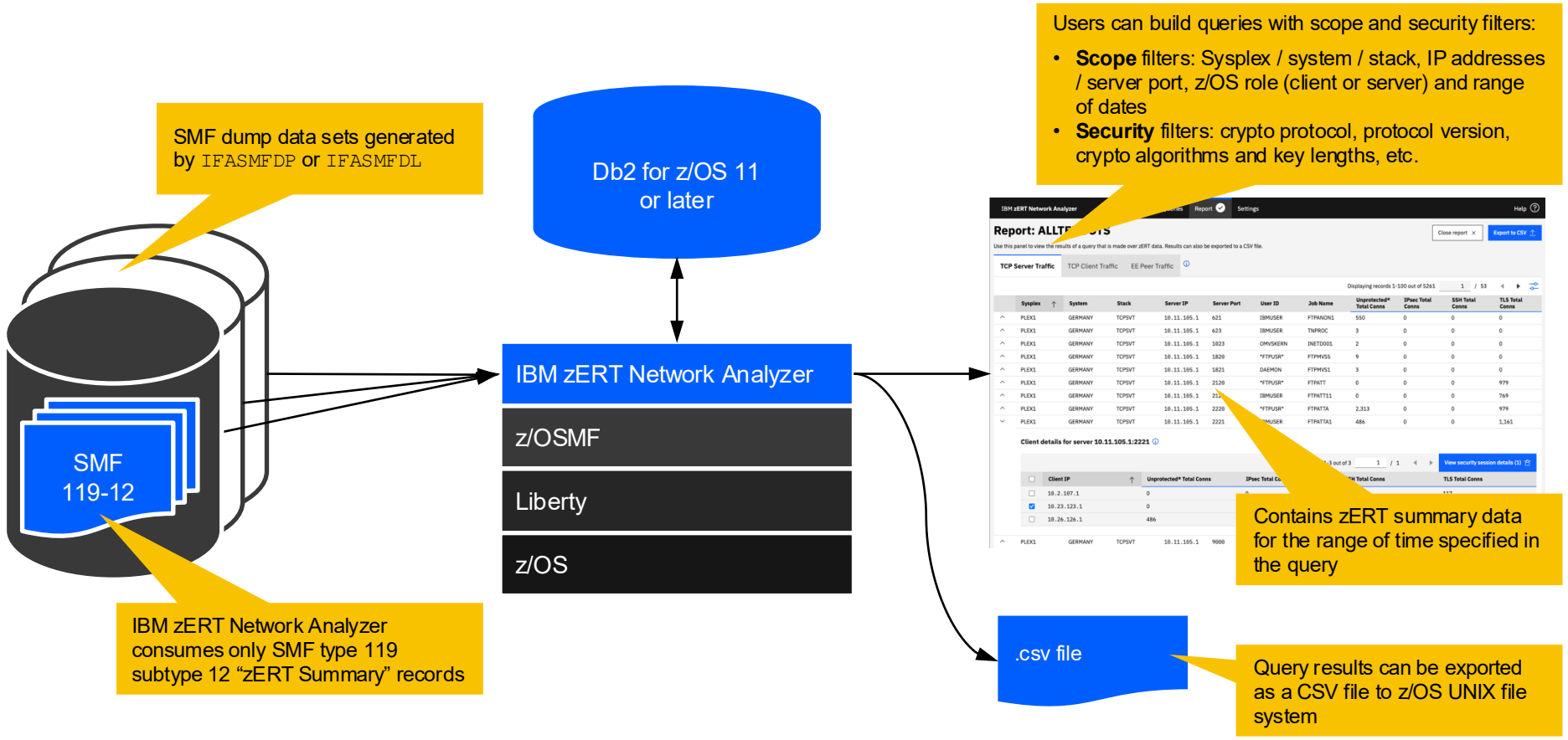
Upeksha Vidanapathirana - upekshavid@ibm.com
Enterprise Networking Solutions - Developer (Networking)

Appendix

- zNA database enhancements
- Update to System SSL and AT-TLS default values in z/OS 3.2
- Persistent Pause Support for Sysplex Distributor DVIPAs
- Function Removals
- Additional Information

zNA database enhancements

zERT Network Analyzer (zNA)



zNA DB enhancements

- zNA requires the use of the Db2 for z/OS NULLID collection that must be configured with the RELEASE(COMMIT) and KEEPDYNAMIC(NO) options.
  - In z/OS 3.2, zNA will be able to use a non-default collection ID for the JDBC connection.
  - This will provide more flexibility to configure the Db2 for z/OS environment for zNA.
  - The Settings / Database Settings panel will be updated with a new Collection ID field. The Settings / Database Settings / Import Database Settings modal will be updated to support the import of the Collection ID field.

zNA DB enhancements …

- Currently, the IBM zERT Network Analyzer's SMF import design uses a single database COMMIT once all SMF records are successfully processed from a data set, placing a heavy Db2 for z/OS resource strain.
  - In z/OS 3.2 zNA will support multiple database COMMIT points for import operations.
    - Imports will commit at regular intervals when SMF 119-12 records are read.
    - On an import failure, any committed records associated with the failed data set will be removed.
    - This is a transparent change in the import operation functionality.
  - This should provide a reduction of Db2 resource strain during intensive SMF data set import operations.
    - In our benchmark testing in a dedicated 3.2 environment, the import of 50M records had import times reduced by 70% with similar CPU savings.

Update to System SSL and AT-TLS default values in z/OS 3.2

Update System SSL and AT-TLS default values (1 of 3)

With the continued direction to improve the security of the TLS connections, System SSL and AT-TLS will be updated to strengthen the defaults for protocols, ciphers, and signature algorithms for applications that rely on defaults:

System SSL:

- Default TLSV1 setting will be changed from ON to OFF
- Default TLSV1.2 setting will be changed from OFF to ON (provided TLSV1.3 is not enabled)
- Default cipher suites list – excludes ciphers using SHA1
  - Only 4-character ciphers (C030, C02C, C02F and C02B)
  - Ciphers use elliptic curve Diffie-Helman ephemeral with AES-GCM SHA256 and SHA384
  - Require ICSF to be running and only are allowed with TLS 1.2
  - Will now need access to CSF1GKP, CSF1GAV and CSF1TRD profiles in the CSFSERV class with these new default ciphers
- Default hash and signature algorithms for X.509 certificates and handshake messages excludes SHA1, SHA224 and DSA
- Default hash and signature algorithms for OCSP, HTTP and LDAP CRL revocation checking excludes SHA1, SHA224 and DSA
  - New environment variable GSK_CRL_SIGALG_PAIRS and CMS APIs to control the allowed algorithms from CRLs retrieved from LDAP and HTTP servers
- Default client elliptic curves list order change: secp224r1 will be moved later in the order

Update System SSL and AT-TLS default values (2 of 3)

AT-TLS:

- With hand-coded AT-TLS policies
  - Default TLSv1 and TLSv1.1 setting on the TTLSEnvironmentAdvancedParms statement changed from ON to OFF
  - Default TLSv1.2 setting on the TTLSEnvironmentAdvancedParms statement changed from OFF to ON
  - Default list of SignaturePairs parameter on the TTLSSignatureParms updated to exclude SHA1, SHA-224 and DSA pairs
  - New parameter CrlSigAlgPairs on the TTLSGskAdvanceedParms statement to set allowed signature algorithms for CRLs retrieved from a LDAP or an HTTP server during revocation checking
  - Default order of the list of ClientEcurves parameter on the TTLSSignatureParms statement updated

- With the z/OSMF Network Configuration Assistant, when creating a new Security Level:
  - Default TLSv1.1 setting will be changed from ON to OFF. It already sets TLSv1.2 to ON by default
  - New "2025 Suggested Values" set of cipher suites that will be selected as the default (C02C, C028, C030, C02F and 1301, 1302 if TLSv1.3 is enabled)
  - New configuration to select hash and signature algorithms allowed in a CRL retrieved from LDAP and HTTP at System image level and new security level

Update System SSL and AT-TLS default values (3 of 3)

z/OS FTP client and policy agent client

- Support calling System SSL directly (instead of using AT-TLS)
- Updated defaults to disable weak protocol versions (TLSv1/TLSv1.1)
- Updated FTP client to use 4-char cipher suites
- When TLSv1.2 or TLSv1.3 is used, hash and signature algorithms for certificates and handshake messages come into play. System SSL's new defaults will be used

Notes:

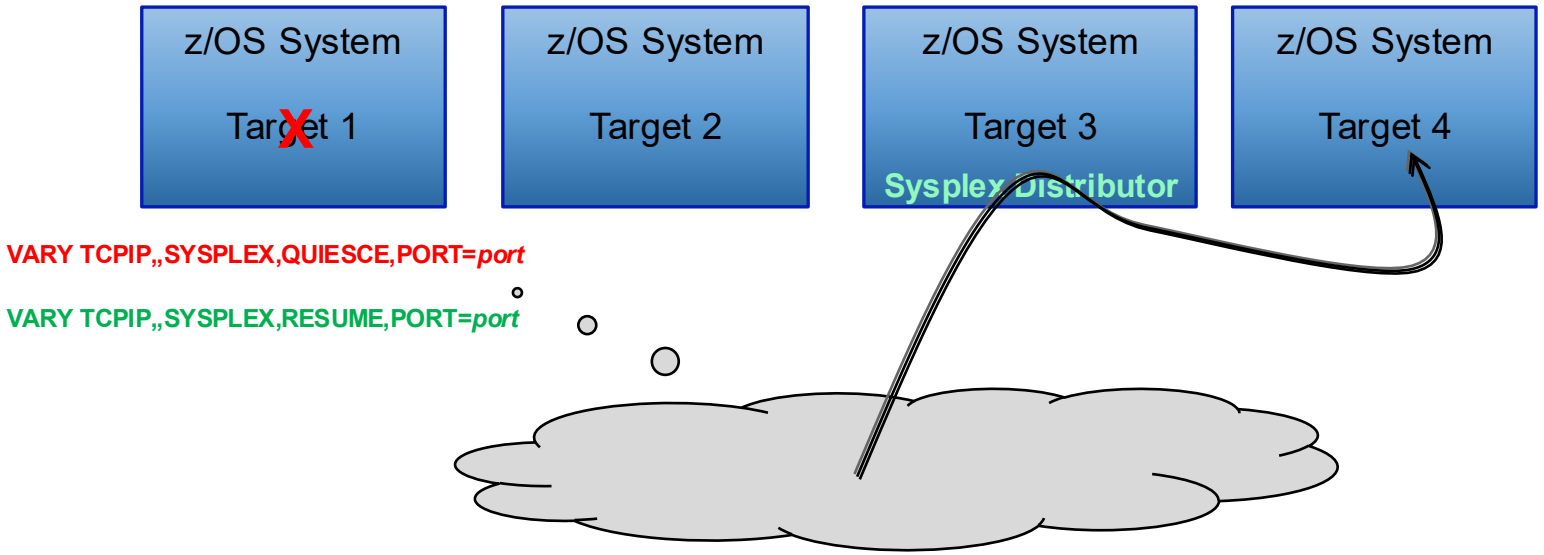
- **Recommendation: Do not rely on defaults, configure the values required for your installation, use strong values**
- We do NOT plan to add TLSv1.3 to the default list of protocol versions
  - You should be actively working on upgrading to TLSv1.3 (we will likely add it in the future, once adoption has leveled off)
- Potential migration issues and CPU increase – these would be documented
- zERT subtype 11 or subtype 12 records and zERT policy-based enforcement can be used to determine what is being used by your connections

Persistent Pause Support for Sysplex Distributor DVIPAs

Quiescing and Resuming Sysplex Distributor targets

On a target stack:

- A quiesce command to stop sysplex distribution of new connections to a specified port or application
  - Informs distributing stack that this application on this target stack should not receive new connections – existing connections are unaffected
- A resume command to reactivate the port or application for sysplex distribution



Quiescing a target is not persistent!

There exists no way to preserve a quiesced sysplex distribution status for a particular application workload over:

- All instances of a port or application across the sysplex
- An application stop and restart
- A target stack stop and restart

Persistent Quiesce of Sysplex Distributor targets

New in 3.1!

On Sysplex Distributor stack:

- A VIPADISTRIBUTE statement to define the dynamic VIPA in a paused state
- A pause command to stop sysplex distribution of new connections to a specified port or all ports across all targets
  - Informs distributing stack that this dynamic VIPA is not available to receive new connections for a specific port or all ports for any targets – existing connections are unaffected
  - Persists across application and target stack restarts
- A resume command to reactivate the dynamic VIPA and optional port for sysplex distribution across all targets


```
VIPADISTRIBUTE DISTMETHOD SERVERWLM PAUSE dvipa DESTIP ALL
```

600: Sysplex Network Technologies and Considerations
Thursday, August 21, 2025: 12:30 PM – 1:30 PM
Hope Ballroom B
Speakers: Mike Fitzpatrick, Paul Gartman

VARY TCPIP,,SYSPLEX,DISTPAUSE,DVIPA=*dvipa*
VARY TCPIP,,SYSPLEX,DISTRESUME,DVIPA=*dvipa*

Function Removals

Function removals in z/OS 3.1

- Several functions were removed from Communications Server in z/OS 3.1:
  - Withdrawal of support for VTAM® Link Station Architecture (LSA) and TCP/IP LAN Channel Station (LCS) devices
  - Removal of OSA DEVICE/LINK/HOME configuration support
- The statements of direction for these removals are included on the following charts

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 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 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.

- A migration health check is provided to identify if VTAM Link Station Architecture (LSA) devices are in use. These devices are configured with MEDIUM=CSMACD in the XCA major node PORT statement. This health check is available with SNA APAR OA62208 on z/OS V2R3, V2R4, and V2R5.

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.

- A migration health check is provided to identify if TCP/IP profile statements DEVICE, LINK, and HOME for OSA-Express connectivity are in use. This health check is available with SNA APAR OA62208 and TCP/IP APAR PH40875 on z/OS V2R3, V2R4, and V2R5.
- For guidance, refer to the z/OS Communications Server IP Configuration Guide topic *"Steps for converting from IPv4 IPAQENET DEVICE, LINK, and HOME definitions to the IPv4 IPAQENET INTERFACE statement".*

Additional Information

IBM z/OS Communications Server and OSA-Express Best Practices

This white paper is provided for the purpose of aiding IBM z/OS customers by providing a general set of considerations (a checklist) for guidance focused on configuring OSA-Express for optimizing network performance.

http://ibm.biz/OSACSBP

183: Getting the Most Out of OSA and HiperSockets with z/OS Communications Server
Wednesday, February 25, 2026: 8:00 AM - 9:00 AM
Salon 16
Speakers: Christopher Nyamful, Karthik Sundaresan

New function APAR summary web pages

- 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
  - V2R5: https://www.ibm.com/support/pages/zos-v2r5-communication-server-new-function-apar-summary
  - 3.1: https://www.ibm.com/support/pages/node/7031984

New function APAR summary web pages - Example

For more V2R5 new functions, see z/OS V2R5 Communications Server: New Function Summary.

Enhancing security

FTP server JES access control March 2022

z/OS V2R5 Communications Server, with APAR PH42618, supports a new SAF resource in the SERVAUTH class to control which users are allowed to access FTP JES mode. When the SERVAUTH class is active and a profile is defined for the EZB.FTP.sysname.ftpdaemonname.ACCESS.JES SAF resource, only users with permission to the profile are allowed to access FTP JES mode.

- PH42618
- How to enable/use this function?

Dependencies:

The SERVAUTH class must be active for the EZB.FTP.sysname.ftpdaemonname.ACCESS.JES SAF resource to provide access controls.

Notices and disclaimers

- © 2025 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.

Notices and disclaimers

- 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

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

IBM*
IBM Logo*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.
Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries. Docker, Inc. and other parties may also have trademark rights in other terms used herein.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.