



Protecting SPOOL data sets with pervasive encryption and other recent JES2 security changes

Tom Wasik
Wasik@us.ibm.com
IBM
JES2 Development



2020 NY Tampa Bay RUG

October 22, 2020

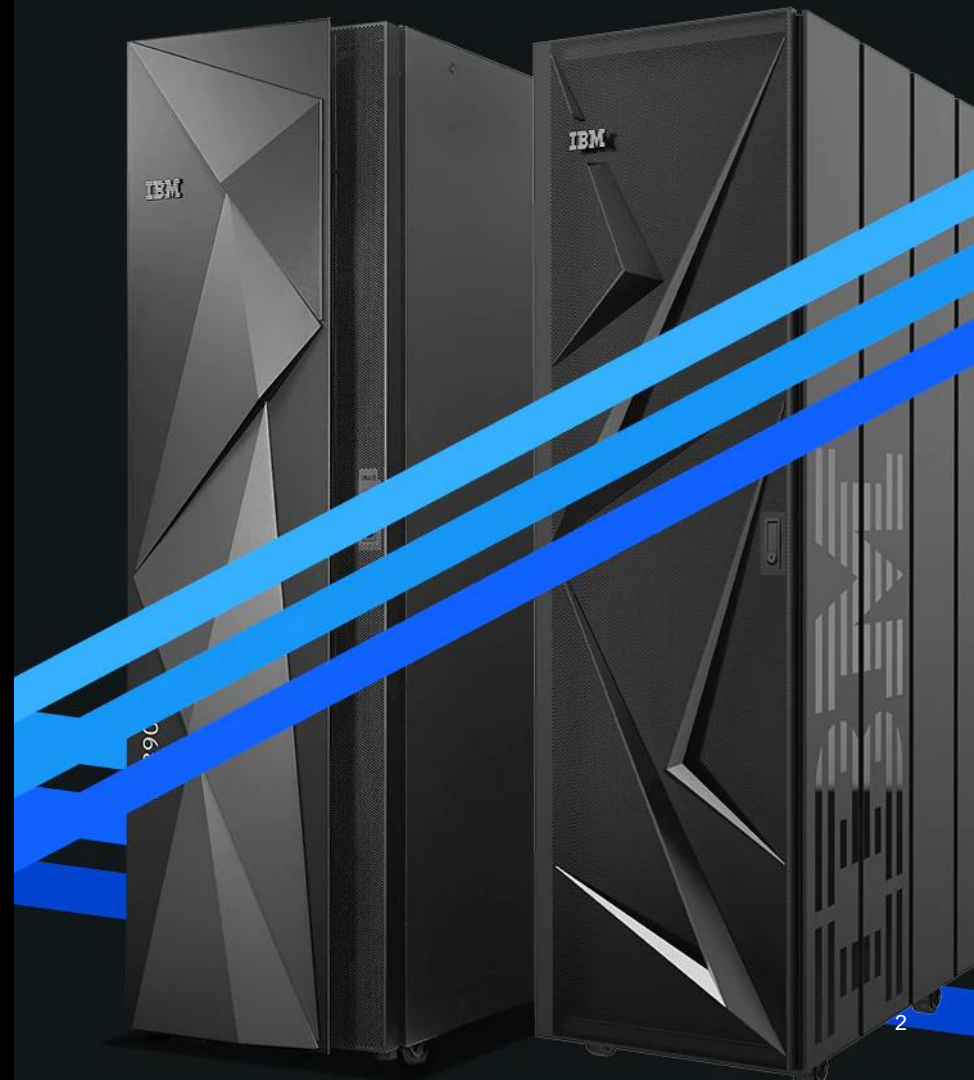


JES2 SPOOL will never be the same

Data protection using the power of pervasive encryption to keep prying eyes from your instream data and SYSOUT

Compression using the integrated features of the z15 processor to save you significant space

No changes needed to your batch jobs or applications accessing SPOOL



SPOOL encryption

Data protection and compliance issues are becoming business imperatives

SPOOL data could contain sensitive data that falls under various compliance regulations

Encryption protects application data at rest on the JES2 SPOOL

Extends Data Set encryption paradigm to job's instream data and SYSOUT data



Designed to take advantage of the processing power of the z14

By managing key label access you can control who can access data across both regular data sets and spool data sets in a consistent manner

Controlling who can read (decrypt) the data is separate from who can control what happens to the data set

Encrypting SPOOL data

Protection occurs on a JES2 spool data set level

Each SPOOL data set can have its own key label (and encryption key)

Usage of key labels is controlled through your security product

Applications access to data on SPOOL is unchanged

However, users must have access to the key label to decrypt the data

Uses same key labels concept as Data Set encryption to encrypt data before writing it

Accessing (decrypting) the data is done using the same key label


Encryption keys

The required key labels are defined in the ICSF Cryptographic Key Data Set (CKDS)

Actual keys are associated with the key labels

Same type of key label setup as Data Set encryption

- Labels are up to 64 characters in length
- AES-256 bit encryption data key associated with the key label
- Set as a protected key in CSFKEYS
- Uses XTS encryption mode



Loss of a key implies loss of access to the data the key encrypts

Key and key label management is critical for a robust security strategy

A consistent strategy should be developed across data set and spool encryption

However, JES2 data is generally short lived (days perhaps weeks) so processes like re-keying do not apply

Specifying a key label



To encrypt data, associate a key label with a data set

RACF JESJOBS profile `ENCRYPT.nodename.userid.jobname.dsname`

KEYLABEL field in the JES segment

Access list/UACC is not used

`DSKEYLBL=` keyword on the `DD *`, `DATA`, and `SYSOUT=` JCL statements, TSO ALLOC, or DYNALLOC

Job owner or submitter needs READ access to FACILITY class profile

`JES.ENCRYPT.OWNER`

or

`JES.ENCRYPT.SUBMITTER`

NJE SYSOUT receiver always uses the JESJOBS profile to assign key label to the SYSOUT

Other security checks

The following security check must pass to create or read data that is encrypted

Users of key labels must have read access to the label in the CSFKEYS class

Conditional access is supported using
`WHEN(CRITERIA(SMS(DSENCRYPTION)))`

Access is needed to the ICSF CKDS Key Record Read2 (CSNBKRR2) service

This is controlled by read access to the CSFKRR2 entity in the CSFSERV class

CSFSERV access is not needed if ICSF is configured with CHECKAUTH(NO)

Security checks are not performed for system access to encrypt or decrypt data

- NJE/OFFLOAD job transmitters, SYSOUT transmitters, and SYSOUT receivers
- Local (non-FSS) and RJE printers and punches

Encryption example

```
//PRINTJOB JOB '', 'Test print job', MSGLEVEL=(1,1), NOTIFY=IBMUSER,
//          USER=IBMUSER, MSGCLASS=A, PRTY=3, CLASS=A
//STEP1    EXEC  PGM=IEBDG
//SYSPRINT DD  SYSOUT=*, DSKEYLBL=ALPHA
//JOBOUT   DD  SYSOUT=*, DSN=&SECOUT
//SYSIN    DD  *, DSKEYLBL=INTERNAL
DSD OUTPUT=(JOBOUT)
FD NAME=A, STARTLOC=01, LENGTH=2,           X
          PICTURE=2, '1 '
FD NAME=B, STARTLOC=03, LENGTH=8, FORMAT=ZD, INDEX=1
FD NAME=C, STARTLOC=11, LENGTH=31,         X
          PICTURE=31, ' GENERATE MANY LINES '
FD NAME=D, STARTLOC=44, LENGTH=30,         X
          PICTURE=30, 'TEST CASE NAME = IBMUSERH '
CREATE FILL=' ', NAME=(A,B,C,D), QUANTITY=100
END
XX

RDEFINE JESJOBS ENCRYPT.ROCH.IBMUSER.PRINTJOB.SECOUT UACC(READ)
JES(KEYLABEL(OUTPUT))
```

SYSPRINT DD is encrypted with key label ALPHA

- Explicitly specified DSKEYLBL

JOBOUT DD is encrypted with key label OUTPUT

- JESJOBS ENCRYPT profile

SYSIN DD is encrypted with key label INTERNAL

- Explicitly specified DSKEYLBL

SPOOL data set compression

Significantly reduce the size of most SPOOL data sets

Stores more data on the same SPOOL volumes

Less data means less I/O to write and later read data

Less I/O means less CPU to write and later read the data

Designed to take advantage of the Integrated Accelerator for zEDC on the z15



Included feature of the z15 processor

No additional licensing fees

Setting up Compression

COMPRESS=YES on OUTCLASS statement

Always attempted for encrypted data set

Not available for instream data sets that are not encrypted

CPU costs are not noticeable in most environments

- In single digit percent increase

I/O reductions is significant

Compression ratios are VERY data dependent

Long LRECL data sets (CPDS) show largest benefits



Sample compression ratios

Assembler listing

517,887	82,696	84.03%
---------	--------	--------

Test tool log

9,024,000	648,519	92.81%
-----------	---------	--------

Ratios available in SDSF JDS display

Encryption and compression notes

JES system data sets not eligible

- JESJCLIN, JESMSG LG, JESJCL, JESYSMSG, \$INTTEXT, \$JOURNAL, \$SWABLKS, EVENTLOG

System jobs not eligible

- SYSLOG, Remote messages, EDS notify messages, \$TRCLOG

Data sets that use GET/PUT update not eligible

- Generic tracker to detect if you have any



Activation

Function shipped with OA57466 on JES2
z/OS 2.4

Not active by default

Can activate once all members completed
migration to z/OS 2.4

- **Once activated, pre-2.4 members cannot join the JESplex**

```
$T SPOOLDEF,ADVANCED_FORMAT=ENABLED
```

`$D SPOOLDEF`
displays current
setting



Can set `ADVANCED_FORMAT` to `DISABLED`
`ADVDF=` is shorthand for `ADVANCED_FORMAT=`
Stop new data set compression and encryption
No effect on existing data sets
Does **NOT** allow pre-2.4 members in the JESplex

Logging

No data set level SMF records for JES2 data sets

Section for compression and encryption in SMF 26 record at the job level



Compression statistics (job total compressed and uncompressed bytes)

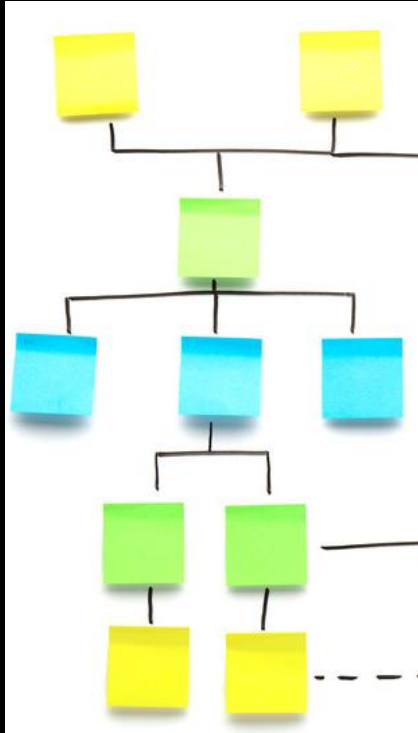


Count of compressed and encrypted data sets

SDSF (via SSI) reports on individual data sets on the JDS panel



Journey to SPOOL encryption



1. Migrate JESplex to z/OS 2.4 and install all needed service (OA57466 et al)
2. Once fall back to an earlier release is no longer needed, activate advanced format (`$T SPOOLDEF,ADVANCED_FORMAT=ENABLED`)
 - Enabling advanced format has no effect if no profiles exist
3. Develop (or extend existing) key label scheme for SPOOL encryption
 - Ensure needed RACF access to CSFKEYS and CSFSERV class profiles
4. Decide what data sets to encrypt and how you want to specify key labels
 - If using JCL, set up JES.ENCRYPT.OWNER and SUBMITTER profiles
5. Test encryption using JCL to ensure that all permissions are set up
6. Once ready, set up JESJOBS RACF policies to assign key labels as need

Something completely different

NJE

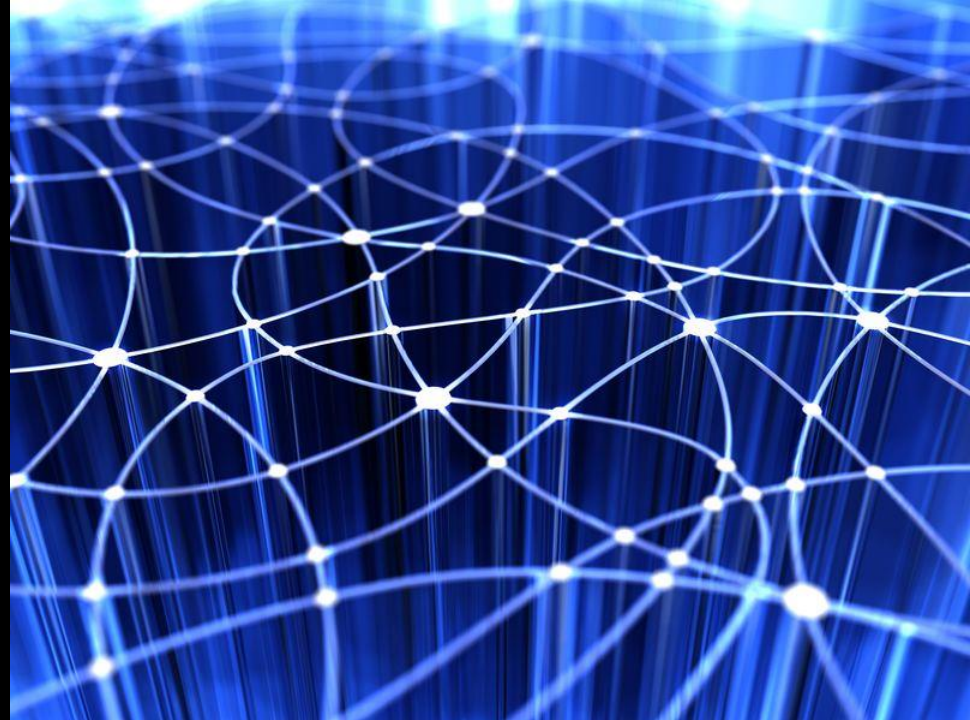
NJE security is based on clear text data in NJE headers

Based on assumption that the network is secure

Only properly authenticated NJE nodes can inject objects into the network

THIS IS NJE so this is the JES guys

This is not TCP/IP so not the network guys



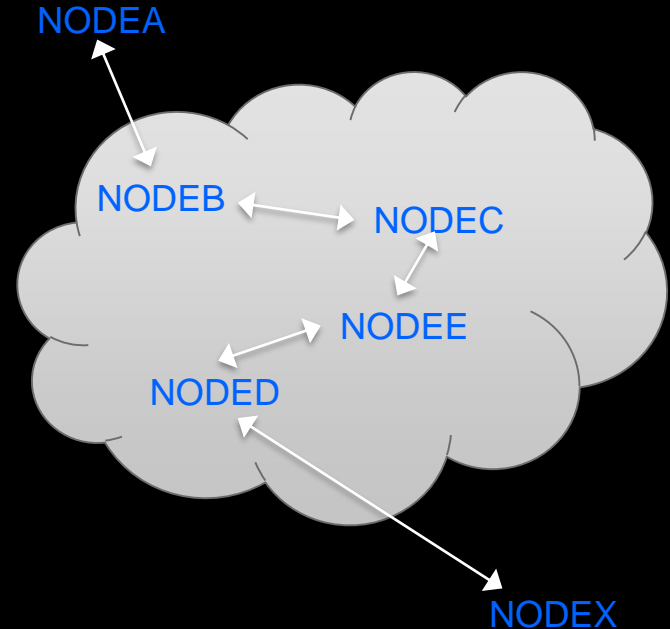
High level NJE concepts

Store and forward

NJE uses a concept of store and forward

Data moving from NODEA to NODEX can travel through intermediate nodes

At the intermediate nodes, the data is stored locally until it is time to move it to the next node in the path



Strange new node in the network

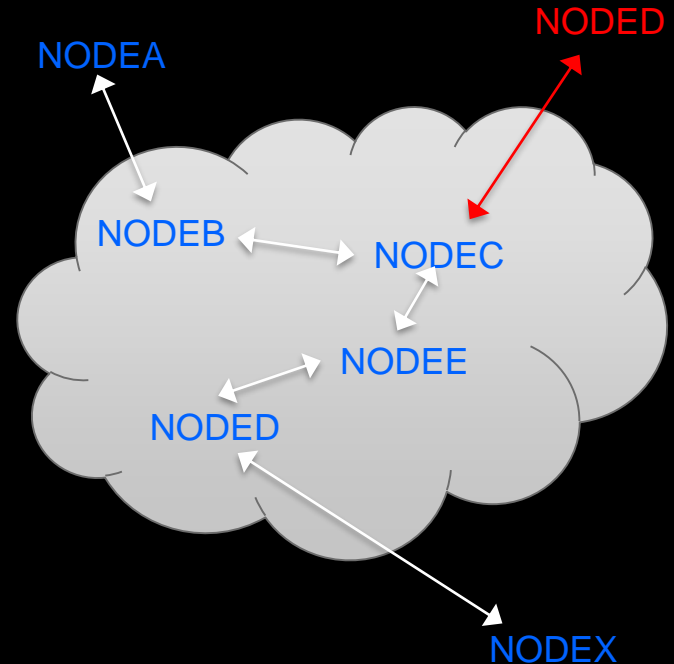
A new node has joined our network

Strange, it has the same name as another node in the network

This is an imposter, allowed in through a single unprotected node (perhaps it is that zVM guy)

So what harm can this imposter do?

Ever GOOGLE “NJE python”?



Imposter in the network

So our imposter has placed a job on the network

It claims to be from NODEX

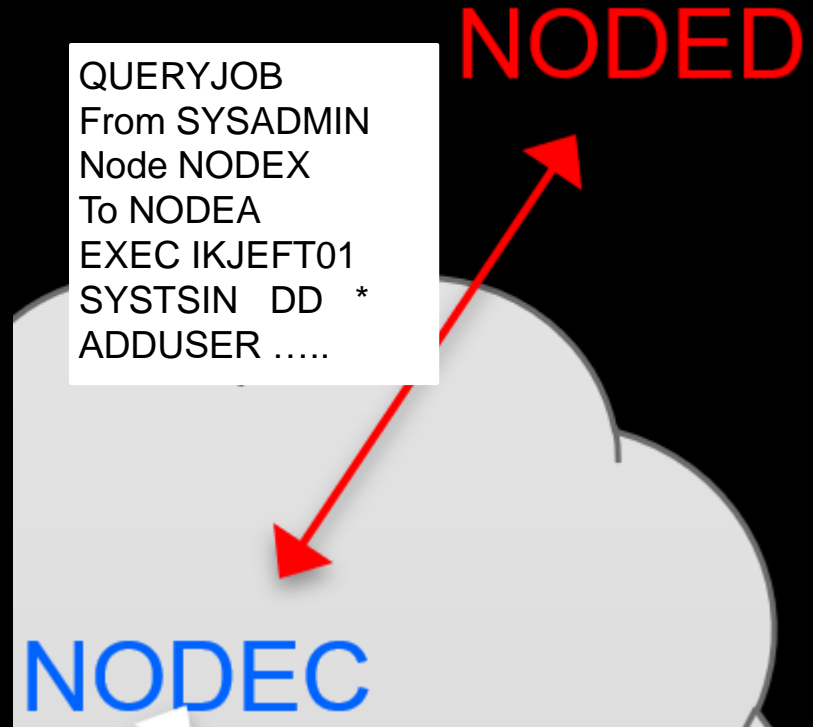
It is going to NODEA

Can NODEA detect that this is from the imposter?

NO

Does NODEA trust jobs from NODEX?

?



Routing based NJE security

Routing based security adds path to destination to the mix

Jobs that come from unexpected places are marked dubious

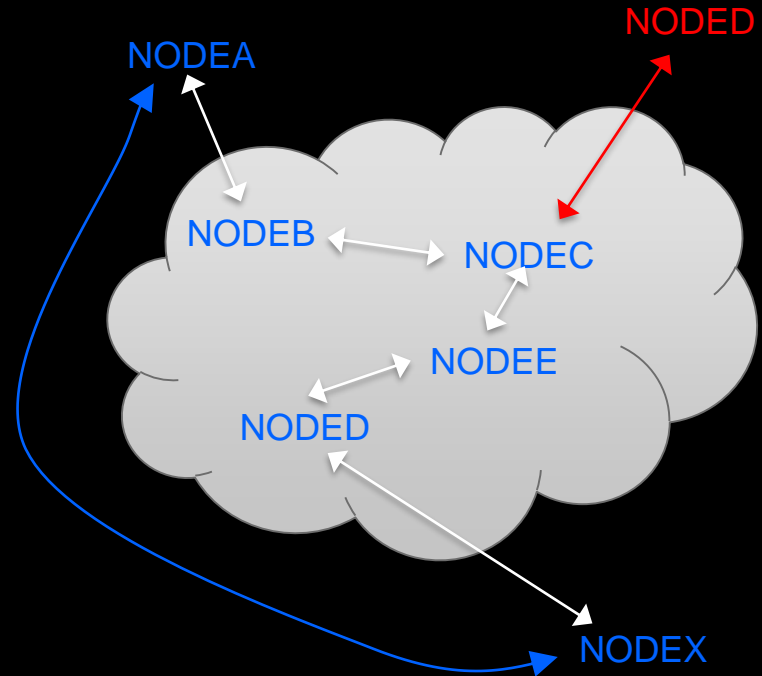
Dubious jobs are not to be trusted

Connect NODEA directly to NODEX via a TCP/IP connection

On NODEA define NODEX as DIRECT=YES and on
NODEX define NODEA as DIRECT=YES

Now NODEA and NODEX will only send data over the blue
direct connection

Anything arriving on NODEA that does not come on the
direct connection is dubious



Advanced routing based security (NJE SUBNETs)

NJE subnets are a way of defining a set of NJE nodes

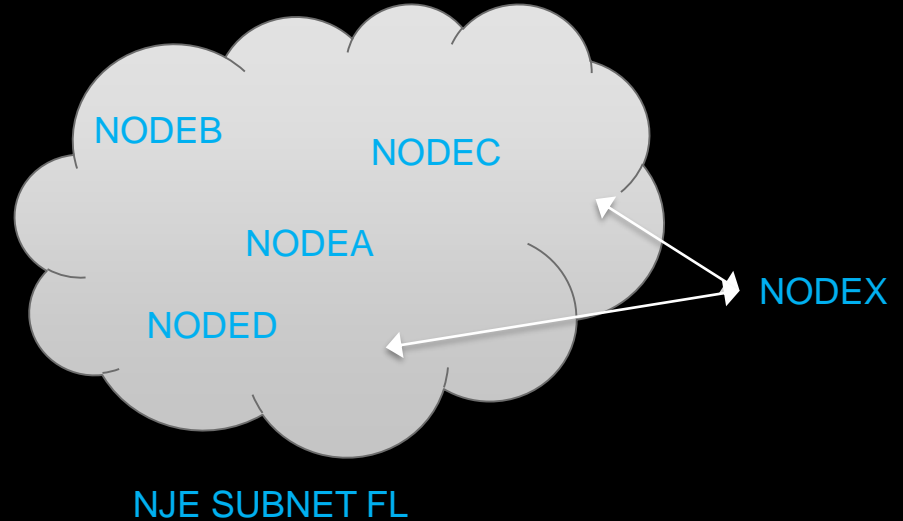
Typically an NJE subnet is a campus or perhaps a company

Rule is when sending an object to a node in the same NJE subnet as you, do not send it outside the NJE subnet

So an object going from NODED to NODEC would never be sent to NODEX

So if NODEX sends an object claiming to be from NODEA, NODEB, NODEC, or NODED, then something is wrong

This is another case when a job is marked dubious



A job is dubious if...

Arrives with origin being local node and destination is ...

- Local node
- A direct node

Destination is local node, origin is a direct node, but arrived via some other node

Job arrived via a node not in the local subnet but the origin and destination is within the local subnet

Marked dubious before it arrived

Once marked dubious, setting is forwarded with job

Special cases:

- Origin is unknown node
- Destination is node it arrived via
- Origin node in NJE header does not match RACF token

Dubious Jobs External

VFYPATH= on NODE for local and DIRECT=YES nodes

- Activates dubious check for nodes

VERIFY_SUBNET= (or VFYSUBNET=) on NJEDEF

- Activates subnet dubious check

PRECHECK= on NJEDEF

- Activates RACF non-NJE pre check for dubious jobs

DUBIOUS= on \$D JOB/JOBGROUP commands

- Displays dubious setting for job (pre and post execution)



NJE Security Health Check

Checks the following for trusted nodes:

- Ensure directly connected or in local subnet
- Ensure NJE password protection
- Ensure using TLS
- Ensure VFYPATH is set

Checks for the local node:

- Ensure VFYPATH set for the local node
- Ensure if local node is in a subnet, VERIFY_SUBNET set
- Ensure that PRECHECK is set

Checks for non-trusted nodes:

- If node can be connected, ensure password protection



Pervasive encryption survey

Please take a minutes to complete
the IBM Z pervasive encryption
survey at

[Pervasive Encryption Survey](#)

Thank You!



Thank you!

Questions?

Tom Wasik
JES Chief Product Owner

wasik@us.ibm.com
+1-507-253-3870
ibm.com

Notices and disclaimers

© 2020 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