The z Exchange – December 19, 2019

Getting a grip on your z/OS network encryption with zERT

Chris Meyer, CISSP (meyerchr@us.ibm.com)
z/OS network security architect

© 2019 IBM Corporation

Please note

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and 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 remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including 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 results similar to those stated here.

© 2019 IBM Corporation

Before we start

- Why does this topic sound so familiar?

- I presented the same topic at the zExchange just about 1 year ago, but…

- Interest and adoption continue to build, and many questions are being asked

- This is a chance to revisit the topic again, provide a bit of an update, and answer any questions you may have

© 2019 IBM Corporation

Agenda

- Background – why zERT?
- zERT overview
- Configuring zERT Discovery and Aggregation
- zERT Network Analyzer
- zERT support in other products
- Considerations
- Summary

Agenda

- **Background – why zERT?**
- zERT overview
- Configuring zERT Discovery and Aggregation
- zERT Network Analyzer
- zERT support in other products
- Considerations
- Summary

© 2019 IBM Corporation

Background: Cryptographic network protection on z/OS

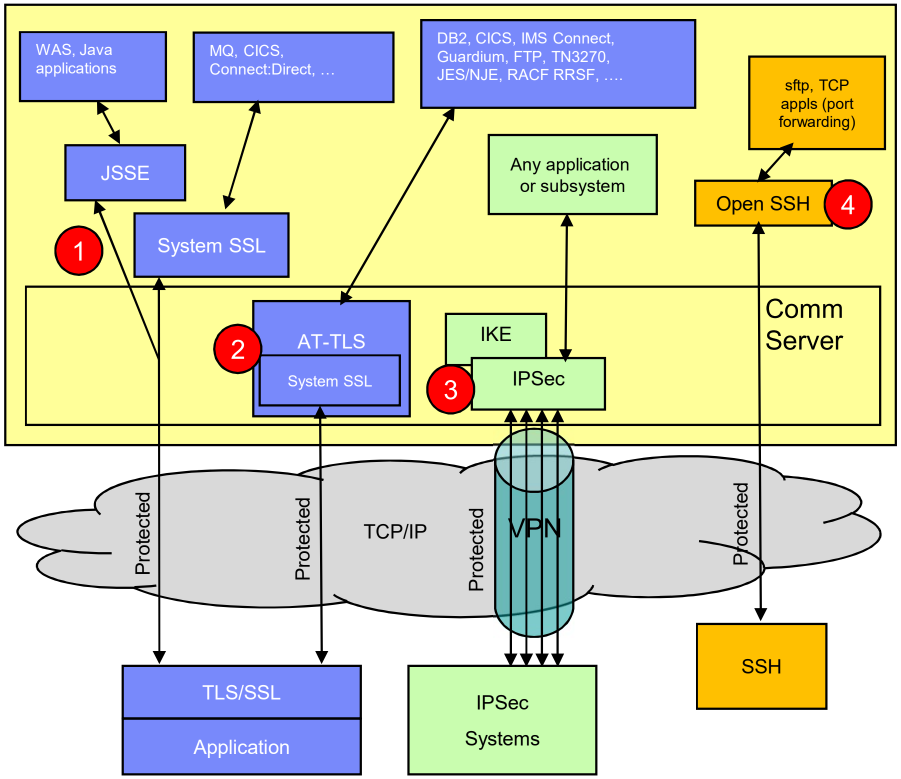
z/OS provides 4* main mechanisms to protect TCP/IP traffic:

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 through SMF 119 records – tunnel level only
- Completely transparent to application
- Wide variety (any to all) of traffic is protected
- Various topologies supported (host to host, host to gateway, etc.)
- 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



* - z/OS also provides Kerberos support, but that is not covered in this presentation

© 2019 IBM Corporation

Background: …so which traffic do I have and how is it protected?

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

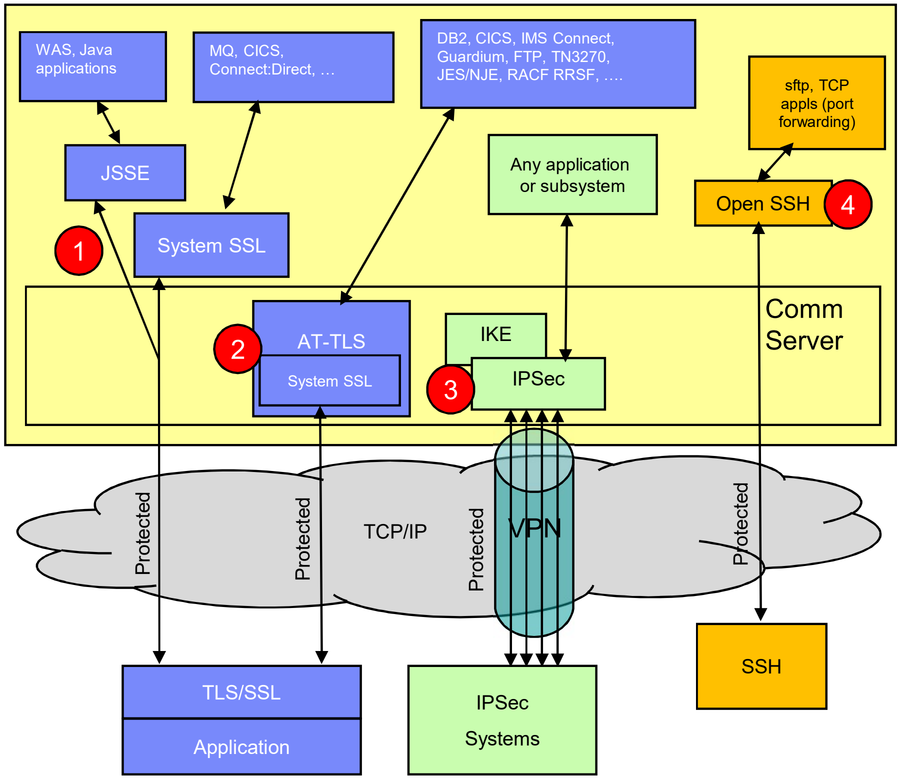
- ***How can I tell…***
  - ***Which traffic*** is being protected (and which is not)?
  - ***How*** is that traffic being protected?
    - Security protocol?
    - Protocol version?
    - Cryptographic algorithms?
    - Key lengths?
    - …and so on
  - ***Who*** does on the traffic belong to in case 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 are driving these questions:

- Regulatory compliance (corporate, industry, government)
- Vulnerabilities in protocols and algorithms
- Internal audits
- …and so forth



© 2019 IBM Corporation

Agenda

- Background – why zERT?
- **zERT overview**
- Configuring zERT Discovery and Aggregation
- zERT Network Analyzer
- zERT support in other products
- Considerations
- Summary

© 2019 IBM Corporation

Overview: z/OS Encryption Readiness Technology (zERT – 1 of 2)

- zERT positions the TCP/IP stack as a central collection point and repository for cryptographic protection attributes for:
  - **TCP** connections that are protected by **TLS, SSL, SSH, IPsec or** have **no recognized cryptographic protection**
  - **Enterprise Extender** connections that are protected by **IPsec or** have **no recognized cryptographic protection**
    - Each peer-to-peer UDP port is considered a separate EE connection
    - In this presentation, we'll focus on TCP examples

- Two methods for discovering the security sessions and their attributes:
  - Stream observation (for TLS, SSL and SSH) – the TCP/IP stack observes the protocol handshakes as they flow over the TCP connection
  - Advice of the cryptographic protocol provider (System SSL, OpenSSH, TCP/IP's IPsec support)

- Reported through new SMF 119 records via:
  - SMF and/or
  - New real-time NMI services

© 2019 IBM Corporation

Overview: z/OS Encryption Readiness Technology (zERT – 2 of 2)

- zERT **Discovery** – part of z/OS V2R3 base
  - SMF 119 subtype 11 “zERT Connection Detail” records
  - These records **describe the cryptographic protection history of each TCP and EE connection***
  - Writes at **least one zERT Connection Detail record for every local TCP and EE connection***
  - **Well suited for real-time monitoring** applications
  - Depending on your z/OS network traffic, these could be generated in very high volumes

* See next page

- zERT **Aggregation –** available since V2R3 new function APAR PI83362
  - 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 SMF interval for each security session** that was active during the SMF 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 –** available since V2R3 new function APAR PH03137…
  - …but you can just install the latest network analyzer PTF – each one contains an up-to-date new install image
  - Web-based (z/OSMF) UI to query and analyze zERT Summary (subtype 12) records
  - Intended for z/OS network security administrators (typically systems programmers)

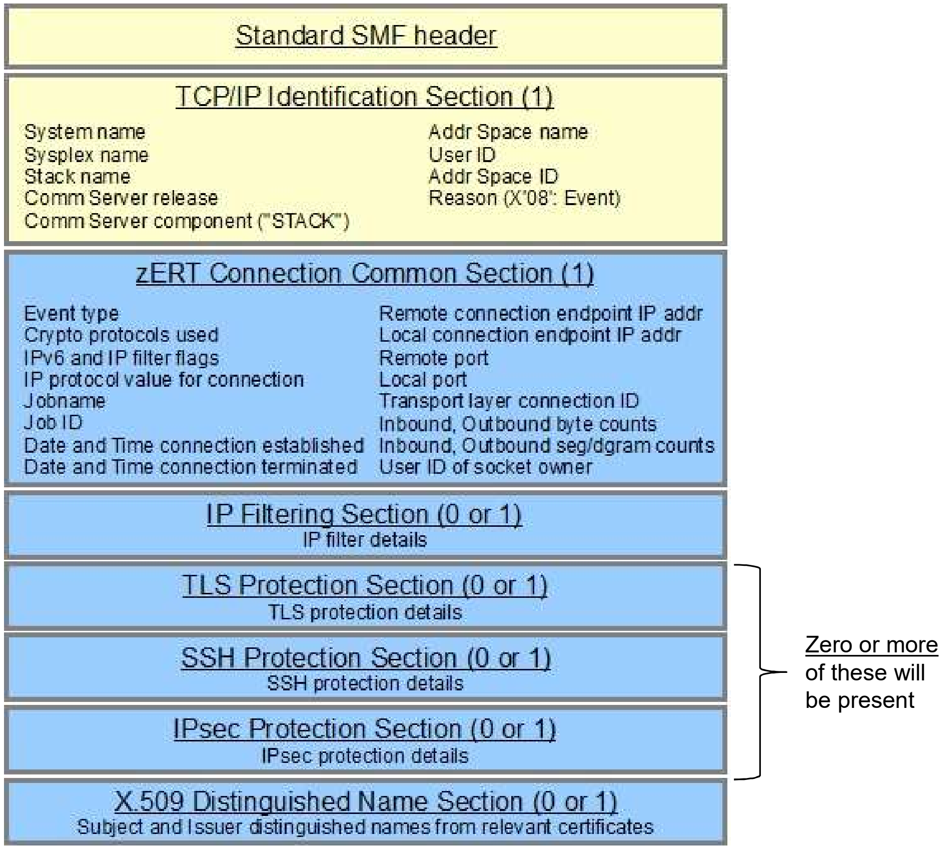
© 2019 IBM Corporation

Overview: zERT Discovery (1 of 2)

Written at various events in a TCP or EE connection’s life:

- **Connection Initiation** (event type 1)
  - Describes protection state when connection was created (for TCP, state as established within the first 10 seconds of the connection’s life)
  - Not usually written for short-lived TCP connections
- **Protection State Change** (event type 2)
  - Describes significant changes in protection state (security session added, deleted, or modified)
- **Connection Termination** (event type 3)
  - Describes protection state when connection terminated
  - Has an accompanying Connection Initiation record
- **Short Connection Termination** (event type 4)
  - Describes protection state when connection terminated
  - Written for short-lived TCP connections (less than 10 seconds long)

Also written when zERT is enabled (5) or disabled (6). Event type is the only zERT information in these records.



Standard SMF header

TCP/IP Identification Section (1)

System name
Sysplex name
Stack name
Comm Server release
Comm Server component ("STACK")

Addr Space name
User ID
Addr Space ID
Reason (X'08': Event)

zERT Connection Common Section (1)

Event type
Crypto protocols used
IPv6 and IP filter flags
IP protocol value for connection
Jobname
Job ID
Date and Time connection established
Date and Time connection terminated

Remote connection endpoint IP addr
Local connection endpoint IP addr
Remote port
Local port
Transport layer connection ID
Inbound, Outbound byte counts
Inbound, Outbound seg/dgram counts
User ID of socket owner

IP Filtering Section (0 or 1)
IP filter details

TLS Protection Section (0 or 1)
TLS protection details

SSH Protection Section (0 or 1)
SSH protection details

IPsec Protection Section (0 or 1)
IPsec protection details

Zero or more of these will be present

X.509 Distinguished Name Section (0 or 1)
Subject and Issuer distinguished names from relevant certificates

Overview: zERT Discovery (2 of 2)

What is collected and recorded?

- Attributes of the connection and its security sessions
  - **Significant attributes**
    - Identifying attributes like IP addresses, ports, jobname, userid, etc.
    - Protection attributes like protocol version, cryptographic algorithms, key lengths, etc. Changes in these cause a protection state change record to be written if they change
  - **Informational attributes** like protocol session identifiers, session or certificate expiry data and certificate serial numbers are recorded for informational purposes only. When recorded, the values of such attributes are taken at the time the SMF record is written. Changes in these attributes do not constitute a significant change and will not result in the creation of a change event record

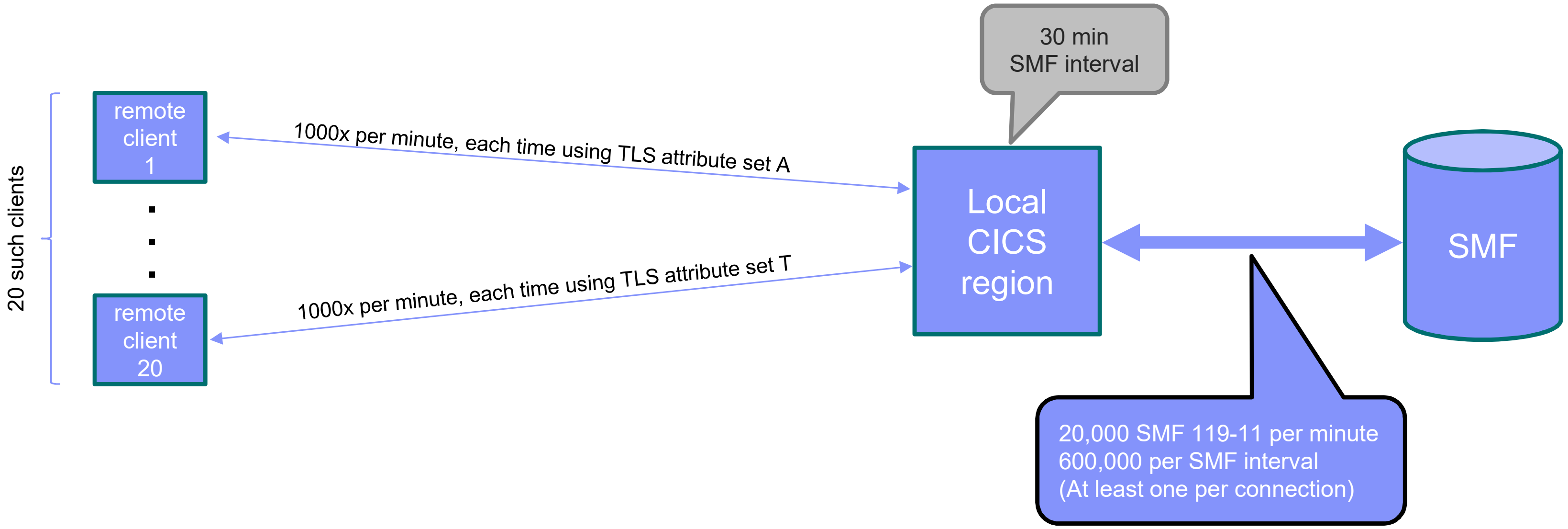
- **zERT does not collect, store or record the values of secret keys, initialization vectors, or any other secret values that are negotiated or derived during cryptographic protocol handshakes**

See the z/OS Communications Server IP Programmer's Guide for all the details

© 2019 IBM Corporation

Overview: zERT Aggregation (1 of 3)

Workloads that consist of large numbers of frequent short-lived connections could generate huge volumes of zERT subtype 11 records

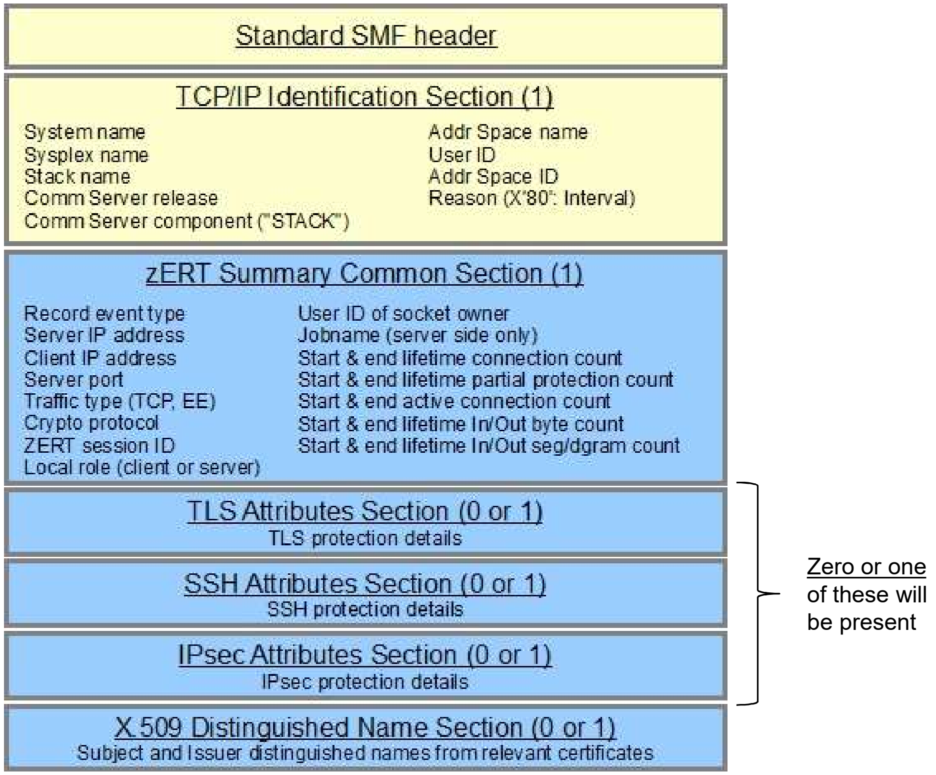

30 min
SMF interval
20 such clients
remote client 1
remote client 20
1000x per minute, each time using TLS attribute set A
1000x per minute, each time using TLS attribute set T
Local CICS region
SMF
20,000 SMF 119-11 per minute
600,000 per SMF interval
(At least one per connection)

Some measures are already taken in zERT Discovery to reduce the number of subtype 11 records (timers and “Short-lived Connection Termination” records), but in environments that manage thousands of connections per hour or minute, the number of subtype 11 records can still be very large

© 2019 IBM Corporation

Overview: zERT Aggregation (2 of 3)

- **zERT Aggregation summarizes the repetitive use of security sessions over time**
  - From the server’s perspective (based on server IP address, server port, & client IP address)
  - Regardless of whether z/OS is the client or the server
- Summaries are written at the end of each SMF interval through new SMF 119 zERT summary (subtype 12) records which contain:
  - Connection attributes (Server IP addr, server port, client IP addr, transport protocol)
  - Significant security attributes
  - Statistics (connection counts, byte counts, etc.)
- With aggregation, **the same example scenario from the previous page would result in 20 SMF 119 subtype 12 records per interval** – one per client TLS session



Standard SMF header

TCP/IP Identification Section (1)

System name
Sysplex name
Stack name
Comm Server release
Comm Server component ("STACK")

Addr Space name
User ID
Addr Space ID
Reason (X'80': Interval)

zERT Summary Common Section (1)

Record event type
Server IP address
Client IP address
Server port
Traffic type (TCP, EE)
Crypto protocol
ZERT session ID
Local role (client or server)

User ID of socket owner
Jobname (server side only)
Start & end lifetime connection count
Start & end lifetime partial protection count
Start & end active connection count
Start & end lifetime In/Out byte count
Start & end lifetime In/Out seg/dgram count

TLS Attributes Section (0 or 1)
TLS protection details

SSH Attributes Section (0 or 1)
SSH protection details

IPsec Attributes Section (0 or 1)
IPsec protection details

X.509 Distinguished Name Section (0 or 1)
Subject and Issuer distinguished names from relevant certificates

Zero or one of these will be present

Overview: zERT APIs (1 of 2)

Real-time network monitoring services

- **Used by 3rd party Network Monitor products to collect SMF data in near real-time**
- Two new Network Monitoring Interfaces (NMIs):
  - New SYSTCPER service for collecting zERT Connection Detail (subtype 11) SMF records
  - New SYSTCPES service for collecting zERT Summary (subtype 12) SMF records

SIOCSHSNOTIFY IOCTL (for System SSL applications)

- **For System SSL application programs that initiate TLS session mid-stream**
- **Use this interface ONLY IF:**
- Your program calls the System SSL gsk_* APIs directly for TLS/SSL protection (i.e., it is NOT protected by AT-TLS or another TLS/SSL provider like JSSE)
- TLS session is initiated after one or more bytes of application-specific data flow over the TCP connection (this is not the typical case)
- **IBM Sterling Connect:Direct** APAR PI77316 uses this interface to achieve proper zERT monitoring

See the z/OS Communications Server IP Programmer's Guide for API details

© 2019 IBM Corporation

Agenda

- Background – why zERT?
- zERT overview
- **Configuring zERT Discovery and Aggregation**
- zERT Network Analyzer
- zERT support in other products
- Considerations
- Summary

Configuring: The steps

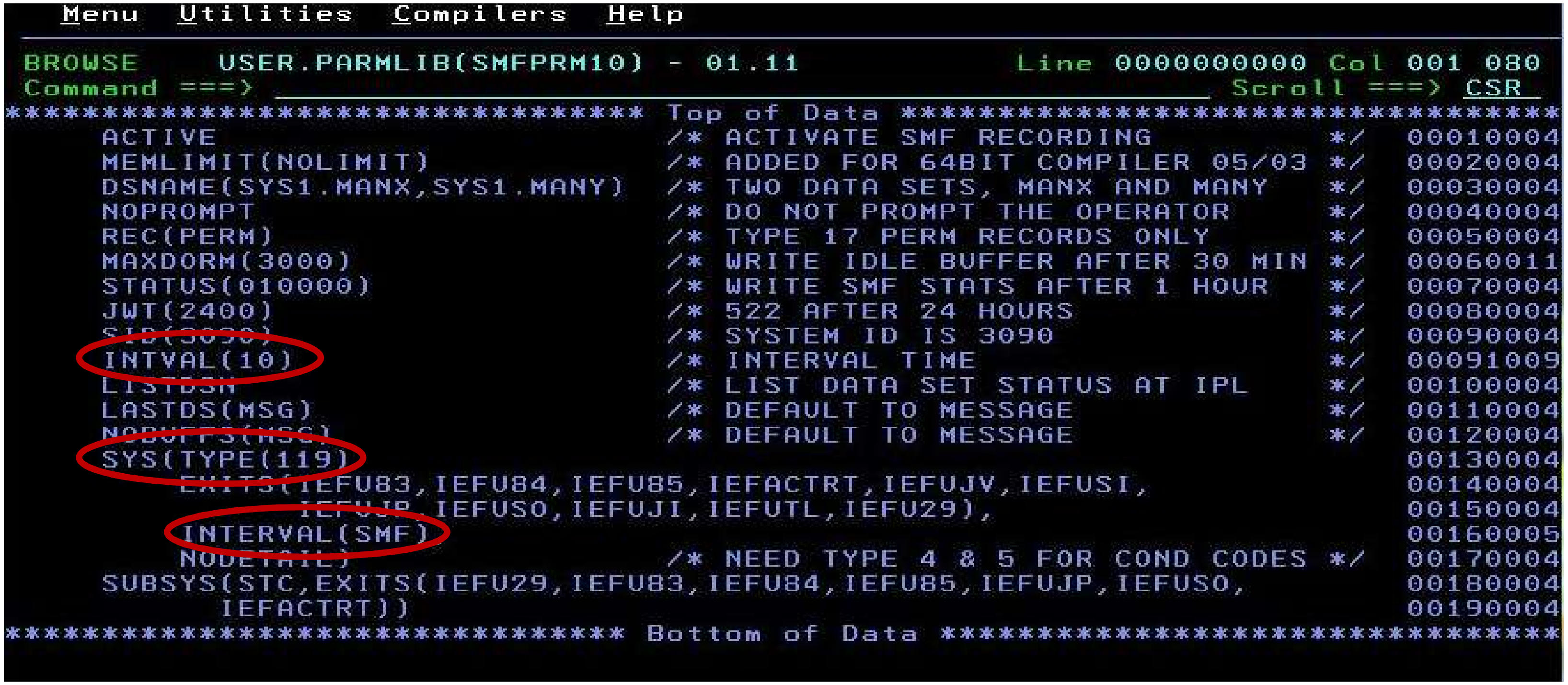
1. Enable SMF 119 records in SMF (PARMLIB)
2. Enable zERT monitoring (TCPIP profile)
3. Specify recording destinations (TCPIP profile)
4. Verification (NETSTAT and DISPLAY TCPIP commands)

© 2019 IBM Corporation

Configuring: 1. Enable SMF 119 records in SMF (PARMLIB)

In your PARMLIB(SMFPRMxx):

- Ensure that SMF 119 records are enabled (SYS(TYPE(119)…)
- If you plan to use Aggregation, ensure that your SMF interval is set appropriately (INTVAL and INTERVAL(SMF))



```
   Menu  Utilities  Compilers  Help
 BROWSE    USER.PARMLIB(SMFPRM10) - 01.11            Line 0000000000 Col 001 080
 Command ===> ________________________________________________ Scroll ===> CSR
********************************* Top of Data **********************************
     ACTIVE                       /* ACTIVATE SMF RECORDING         */  00010004
     MEMLIMIT(NOLIMIT)            /* ADDED FOR 64BIT COMPILER 05/03 */  00020004
     DSNAME(SYS1.MANX,SYS1.MANY)  /* TWO DATA SETS, MANX AND MANY   */  00030004
     NOPROMPT                     /* DO NOT PROMPT THE OPERATOR     */  00040004
     REC(PERM)                    /* TYPE 17 PERM RECORDS ONLY      */  00050004
     MAXDORM(3000)                /* WRITE IDLE BUFFER AFTER 30 MIN */  00060011
     STATUS(010000)               /* WRITE SMF STATS AFTER 1 HOUR   */  00070004
     JWT(2400)                    /* 522 AFTER 24 HOURS             */  00080004
     SID(3090)                    /* SYSTEM ID IS 3090              */  00090004
     INTVAL(10)                   /* INTERVAL TIME                  */  00091009
     LISTDSN                      /* LIST DATA SET STATUS AT IPL    */  00100004
     LASTDS(MSG)                  /* DEFAULT TO MESSAGE             */  00110004
     NOBUFFS(MSG)                 /* DEFAULT TO MESSAGE             */  00120004
     SYS(TYPE(119)                                                      00130004
         EXITS(IEFU83,IEFU84,IEFU85,IEFACTRT,IEFUJV,IEFUSI,             00140004
               IEFUJP,IEFUSO,IEFUJI,IEFUTL,IEFU29),                     00150004
         INTERVAL(SMF)                                                  00160005
         NODETAIL)                /* NEED TYPE 4 & 5 FOR COND CODES */  00170004
     SUBSYS(STC,EXITS(IEFU29,IEFU83,IEFU84,IEFU85,IEFUJP,IEFUSO,        00180004
           IEFACTRT))                                                   00190004
******************************** Bottom of Data ********************************
```

© 2019 IBM Corporation

Configuring: 2. Enable zERT monitoring (TCPIP profile)

In your TCPIP profile data set:

- GLOBALCONFIG ZERT controls zERT **in-memory** monitoring (default is NOZERT)
  - `GLOBALCONFIG ZERT [AGGRegation] | NOZERT`
  - `AGGRegation` subparameter enables aggregation function

- Note that the discovery and aggregation in-memory functions are enabled independently of the destinations to which records are written.
- Can be dynamically enabled or disabled
- Can be configured by hand or through the z/OSMF Configuration Assistant for z/OS Communications Server (see backup slides)

© 2019 IBM Corporation

Configuring: 3. Specify recording destinations (TCPIP profile)

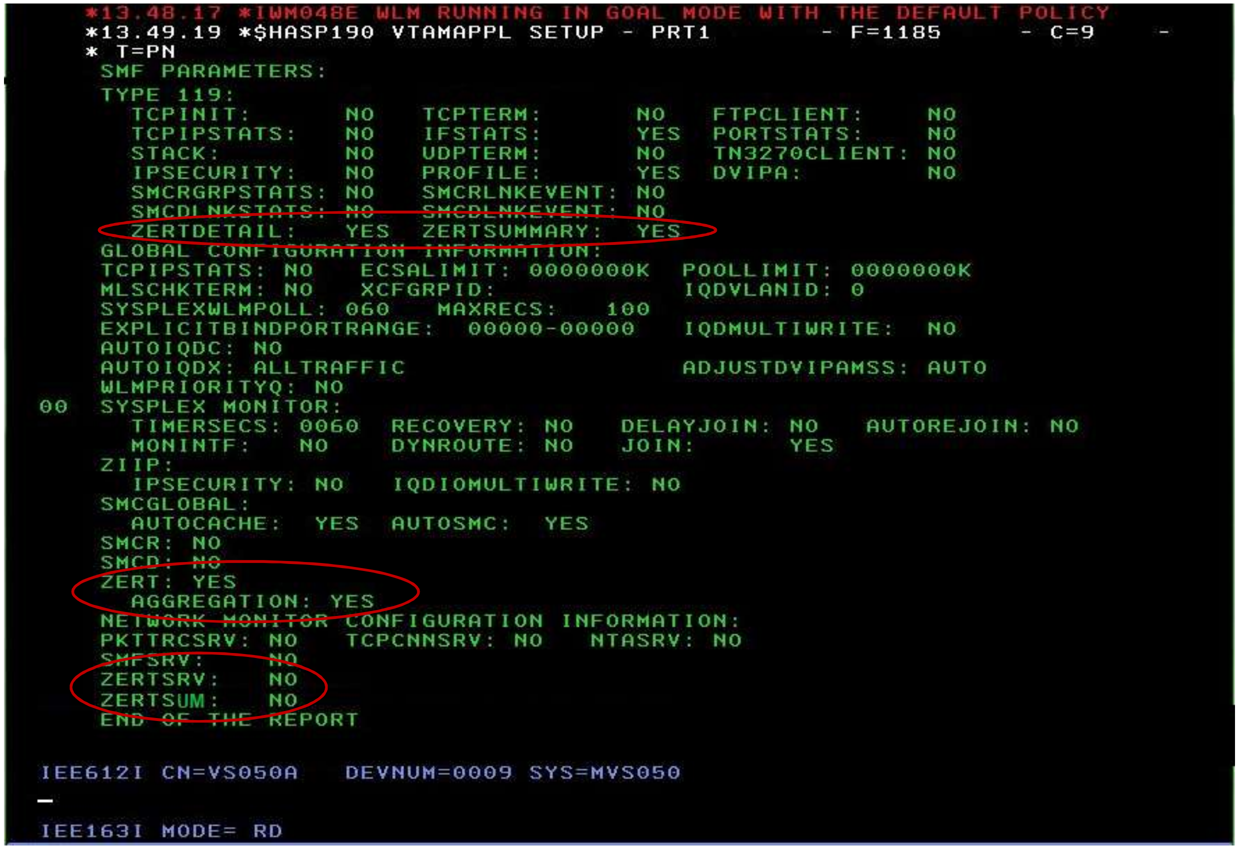
In your TCPIP profile data set:

- SMFCONFIG controls writing of zERT records to System Management Facility
  - `SMFCONFIG TYPE119 ZERTDetail | NOZERTDetail`
  - `SMFCONFIG TYPE119 ZERTSUMmary | NOZERTSUMmary`
  - Defaults are NOZERTDetail and NOZERTSUMmary
- NETMONITOR controls writing of zERT records to new real-time network monitoring services
  - `NETMONITOR ZERTService | NOZERTService`
  - `NETMONITOR ZERTSUMmary | NOZERTSUMmary`
  - Defaults are NOZERTService and NOZERTSUMmary
- Note that the discovery and aggregation in-memory functions are enabled independently of the destinations to which records are written.
- Can be dynamically enabled or disabled
- Can be configured by hand or through the z/OSMF Configuration Assistant for z/OS Communications Server (see backup slides)

© 2019 IBM Corporation

Configuring: 4. Verifying zERT configuration

NETSTAT CONFIG or DISPLAY TCPIP,*tcpipprocname*,NET,CONFIG command shows current configuration:



```
     *13.48.17 *IWM048E WLM RUNNING IN GOAL MODE WITH THE DEFAULT POLICY
     *13.49.19 *$HASP190 VTAMAPPL SETUP - PRT1         - F=1185      - C=9     -
     * T=PN
      SMF PARAMETERS:
      TYPE 119:
        TCPINIT:       NO    TCPTERM:       NO    FTPCLIENT:     NO
        TCPIPSTATS:    NO    IFSTATS:       YES   PORTSTATS:     NO
        STACK:         NO    UDPTERM:       NO    TN3270CLIENT:  NO
        IPSECURITY:    NO    PROFILE:       YES   DVIPA:         NO
        SMCRGRPSTATS:  NO    SMCRLNKEVENT:  NO
        SMCDLNKSTATS:  NO    SMCDLNKEVENT:  NO
        ZERTDETAIL:    YES   ZERTSUMMARY:   YES
      GLOBAL CONFIGURATION INFORMATION:
      TCPIPSTATS: NO    ECSALIMIT: 0000000K   POOLLIMIT: 0000000K
      MLSCHKTERM: NO    XCFGRPID:             IQDVLANID: 0
      SYSPLEXWLMPOLL: 060    MAXRECS:   100
      EXPLICITBINDPORTRANGE:  00000-00000     IQDMULTIWRITE:  NO
      AUTOIQDC: NO
      AUTOIQDX: ALLTRAFFIC                    ADJUSTDVIPAMSS: AUTO
      WLMPRIORITYQ: NO
  00  SYSPLEX MONITOR:
        TIMERSECS: 0060  RECOVERY: NO   DELAYJOIN: NO   AUTOREJOIN: NO
        MONINTF:   NO    DYNROUTE: NO   JOIN:      YES
      ZIIP:
        IPSECURITY: NO   IQDIOMULTIWRITE: NO
      SMCGLOBAL:
        AUTOCACHE:  YES  AUTOSMC:  YES
      SMCR: NO
      SMCD: NO
      ZERT: YES
        AGGREGATION: YES
      NETWORK MONITOR CONFIGURATION INFORMATION:
      PKTTRCSRV: NO    TCPCNNSRV: NO    NTASRV: NO
      SMFSRV:    NO
      ZERTSRV:   NO
      ZERTSUM:   NO
      END OF THE REPORT

  IEE612I CN=VS050A   DEVNUM=0009 SYS=MVS050
  _
  IEE163I MODE= RD
```

Agenda

- Background – why zERT?
- zERT overview
- Configuring zERT Discovery and Aggregation
- **zERT Network Analyzer**
- zERT support in other products
- Considerations
- Summary

© 2019 IBM Corporation

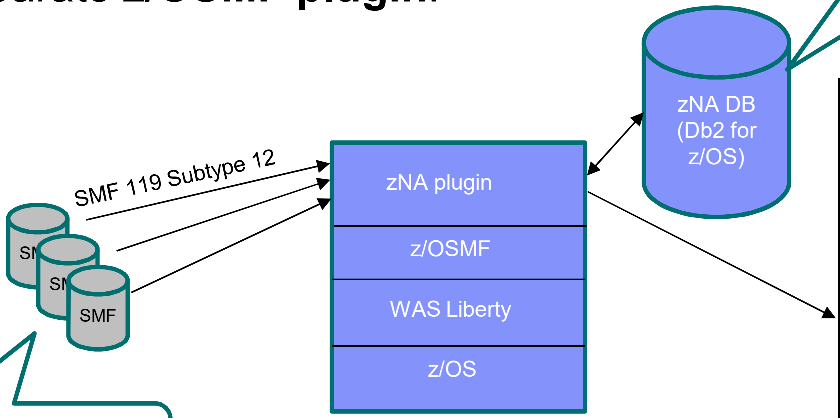
zERT Network Analyzer Overview

- A separate **z/OSMF plugin**:

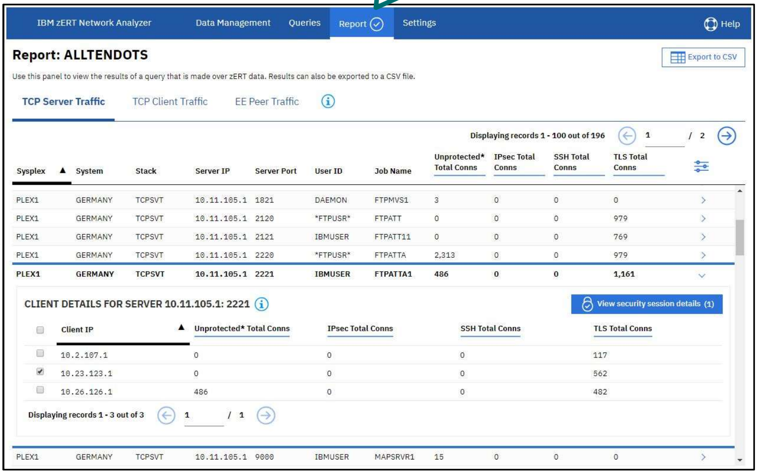
Contains zERT summary data for some fixed range of time

Users build queries over a variety of attributes:

- Specific scope attributes like Sysplex / system / stack, IP addresses / server port, z/OS role (client or server) and range of dates
- Specific security attributes like crypto protocol, protocol version, crypto algorithms and key lengths, etc.



SMF dump data sets generated by IFASMFDP or IFASMFDL



Report: ALLTENDOTS

Use this panel to view the results of a query that is made over zERT data. Results can also be exported to a CSV file.

Displaying records 1 - 100 out of 196 1 / 2

Sysplex ▲	System	Stack	Server IP	Server Port	User ID	Job Name	Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	GERMANY	TCPSVT	10.11.105.1	1821	DAEMON	FTPMVS1	3	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	2120	*FTPUSR*	FTPATT	0	0	0	979
PLEX1	GERMANY	TCPSVT	10.11.105.1	2121	IBMUSER	FTPATT11	0	0	0	769
PLEX1	GERMANY	TCPSVT	10.11.105.1	2220	*FTPUSR*	FTPATTA	2,313	0	0	979
PLEX1	**GERMANY**	**TCPSVT**	**10.11.105.1**	**2221**	**IBMUSER**	**FTPATTA1**	**486**	**0**	**0**	**1,161**

CLIENT DETAILS FOR SERVER 10.11.105.1: 2221

□	Client IP ▲	Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
□	10.2.107.1	0	0	0	117
☑	10.23.123.1	0	0	0	562
□	10.26.126.1	486	0	0	482

Displaying records 1 - 3 out of 3 1 / 1

Sysplex	System	Stack	Server IP	Server Port	User ID	Job Name	Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	GERMANY	TCPSVT	10.11.105.1	9000	IBMUSER	MAPSRVR1	15	0	0	0

- **Web UI** makes zERT data consumable for **z/OS network security administrators** (typically systems programmers)
- **Access to UI controlled through SAF** resource IZUDFLT.ZOSMF.ZERT_NETWORK_ANALYZER in the ZMFAPLA class
- Used primarily to investigate specific network encryption questions (but could also be used for periodic report generation)
- Available on **V2R3** via APAR PH03137 and in the **V2R4** base – for either, the **latest PTF always has a full install image**

© 2019 IBM Corporation

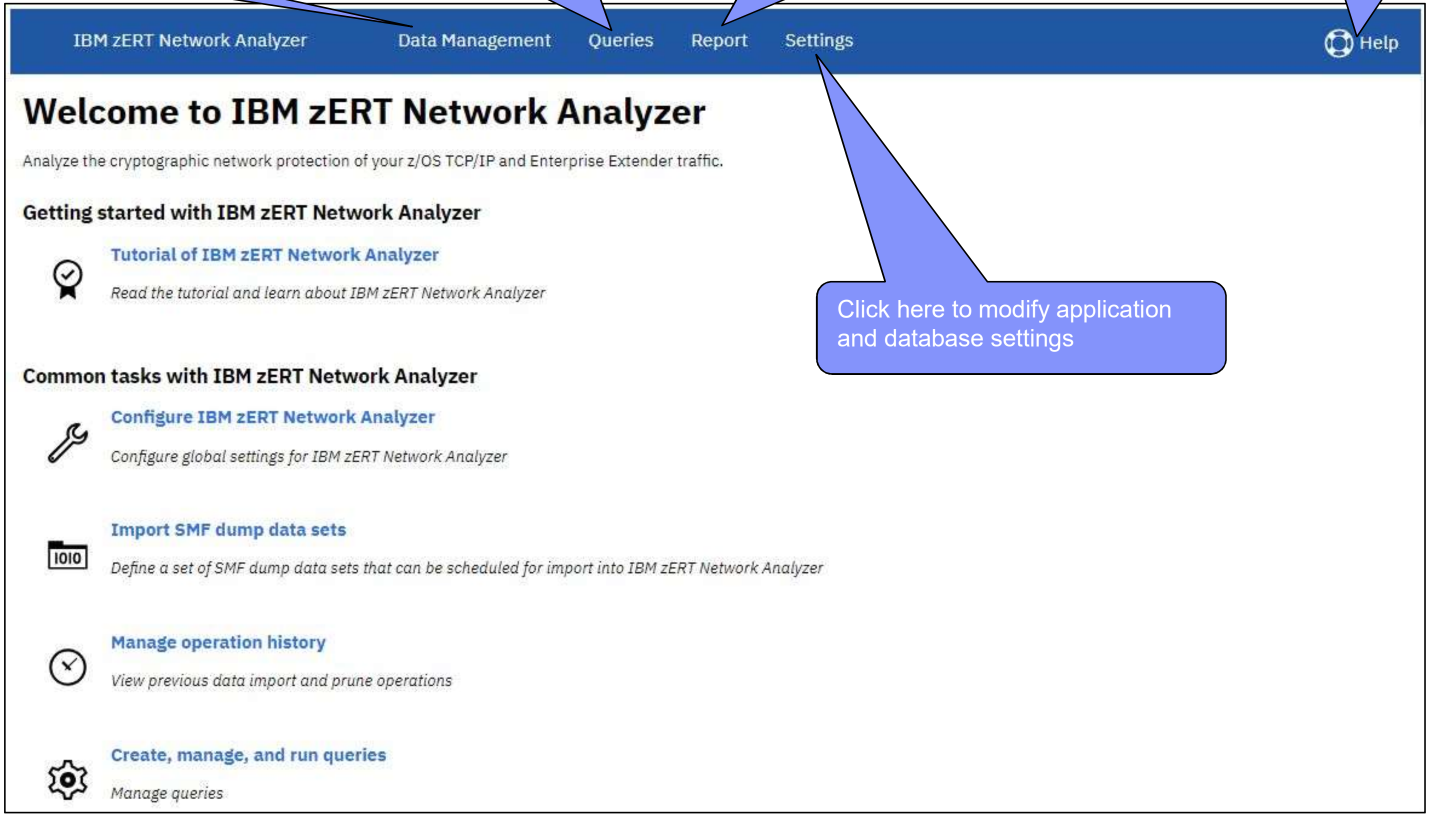
zERT Network Analyzer Overview: Welcome page and layout

Click here to import SMF dump data sets and to prune old data out of the database

Click here to create, modify, and run queries over the imported data

Click here to view the query results (more on this in the following slides)

Click here for topical help in the IBM Knowledge Center



Welcome to IBM zERT Network Analyzer

Analyze the cryptographic network protection of your z/OS TCP/IP and Enterprise Extender traffic.

Getting started with IBM zERT Network Analyzer

Tutorial of IBM zERT Network Analyzer

Read the tutorial and learn about IBM zERT Network Analyzer

Common tasks with IBM zERT Network Analyzer

Configure IBM zERT Network Analyzer

Configure global settings for IBM zERT Network Analyzer

Import SMF dump data sets

Define a set of SMF dump data sets that can be scheduled for import into IBM zERT Network Analyzer

Manage operation history

View previous data import and prune operations

Create, manage, and run queries

Manage queries

Click here to modify application and database settings

© 2019 IBM Corporation

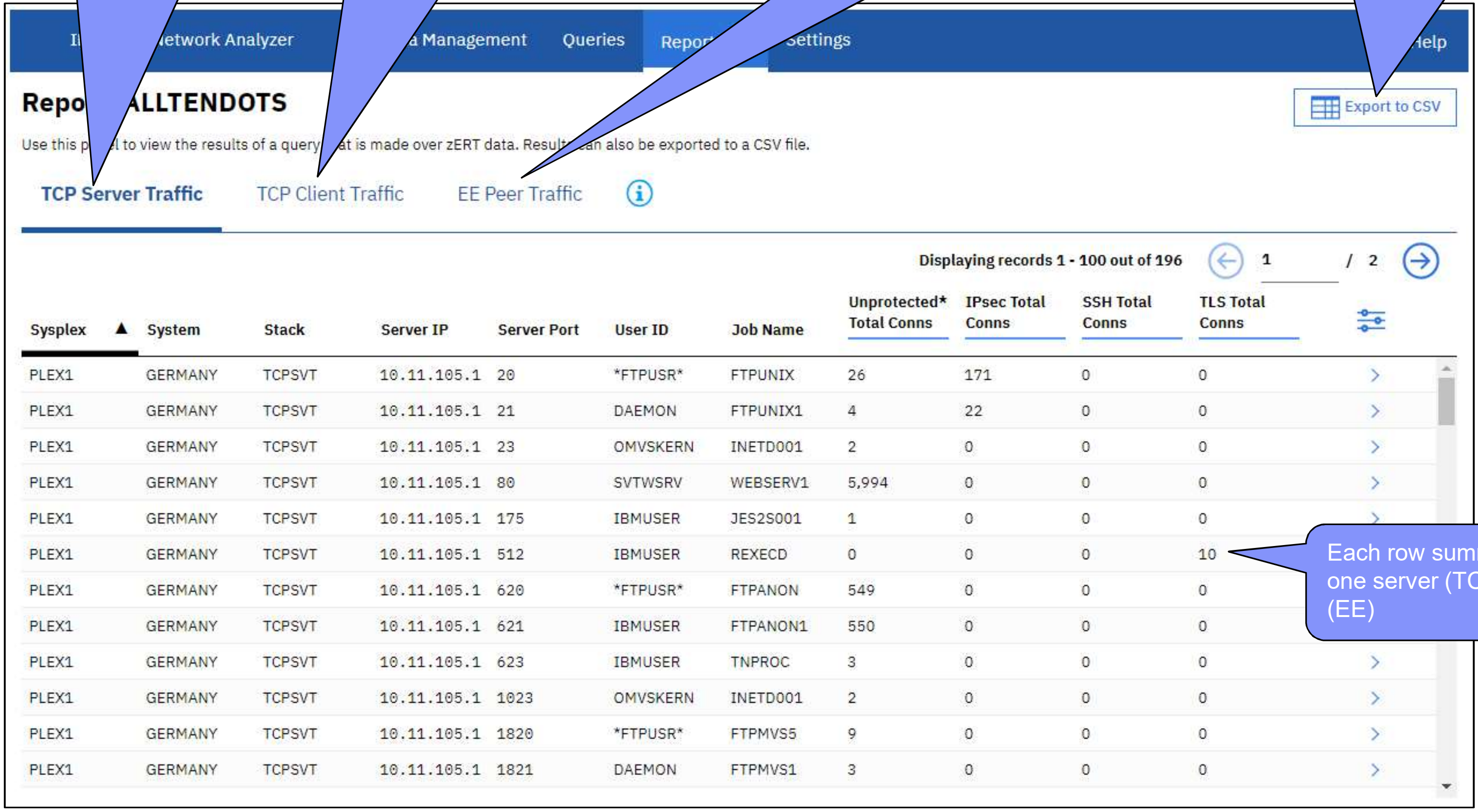
zERT Network Analyzer Overview: Report summary view (1 of 2)

TCP Server Traffic: Summary of all the traffic connecting in to servers running on local z/OS systems

TCP Client Traffic: Summary of all the traffic connecting out to servers running on other systems

EE Peer Traffic: Summary of all EE traffic connected to local z/OS systems

Exports the query results and all related details to a comma separated value file



Repo ALLTENDOTS

Use this p l to view the results of a query at is made over zERT data. Result an also be exported to a CSV file.

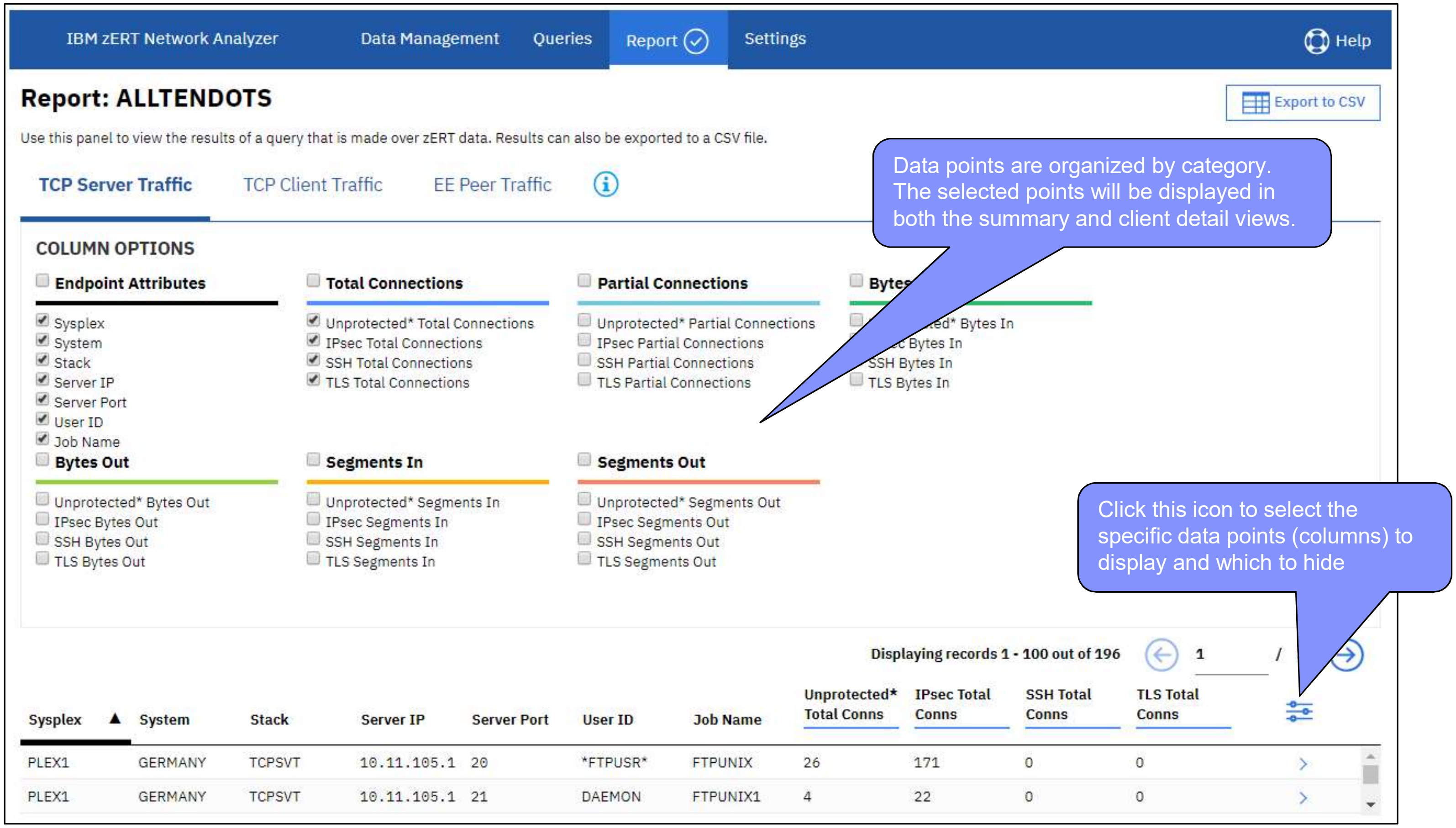
Displaying records 1 - 100 out of 196   1 / 2

Sysplex ▲	System	Stack	Server IP	Server Port	User ID	Job Name	Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	GERMANY	TCPSVT	10.11.105.1	20	*FTPUSR*	FTPUNIX	26	171	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	21	DAEMON	FTPUNIX1	4	22	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	23	OMVSKERN	INETD001	2	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	80	SVTWSRV	WEBSERV1	5,994	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	175	IBMUSER	JES2S001	1	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	512	IBMUSER	REXECD	0	0	0	10
PLEX1	GERMANY	TCPSVT	10.11.105.1	620	*FTPUSR*	FTPANON	549	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	621	IBMUSER	FTPANON1	550	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	623	IBMUSER	TNPROC	3	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	1023	OMVSKERN	INETD001	2	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	1820	*FTPUSR*	FTPMVS5	9	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	1821	DAEMON	FTPMVS1	3	0	0	0

Each row summarizes traffic for one server (TCP) or local peer (EE)

© 2019 IBM Corporation

zERT Network Analyzer Overview: Report summary view (2 of 2)



Report: ALLTENDOTS

Use this panel to view the results of a query that is made over zERT data. Results can also be exported to a CSV file.

COLUMN OPTIONS

□ **Endpoint Attributes**

- ☑ Sysplex
- ☑ System
- ☑ Stack
- ☑ Server IP
- ☑ Server Port
- ☑ User ID
- ☑ Job Name

□ **Bytes Out**

- □ Unprotected* Bytes Out
- □ IPsec Bytes Out
- □ SSH Bytes Out
- □ TLS Bytes Out

□ **Total Connections**

- ☑ Unprotected* Total Connections
- ☑ IPsec Total Connections
- ☑ SSH Total Connections
- ☑ TLS Total Connections

□ **Segments In**

- □ Unprotected* Segments In
- □ IPsec Segments In
- □ SSH Segments In
- □ TLS Segments In

□ **Partial Connections**

- □ Unprotected* Partial Connections
- □ IPsec Partial Connections
- □ SSH Partial Connections
- □ TLS Partial Connections

□ **Segments Out**

- □ Unprotected* Segments Out
- □ IPsec Segments Out
- □ SSH Segments Out
- □ TLS Segments Out

□ **Bytes**

- □ ted* Bytes In
- c Bytes In
- SSH Bytes In
- □ TLS Bytes In

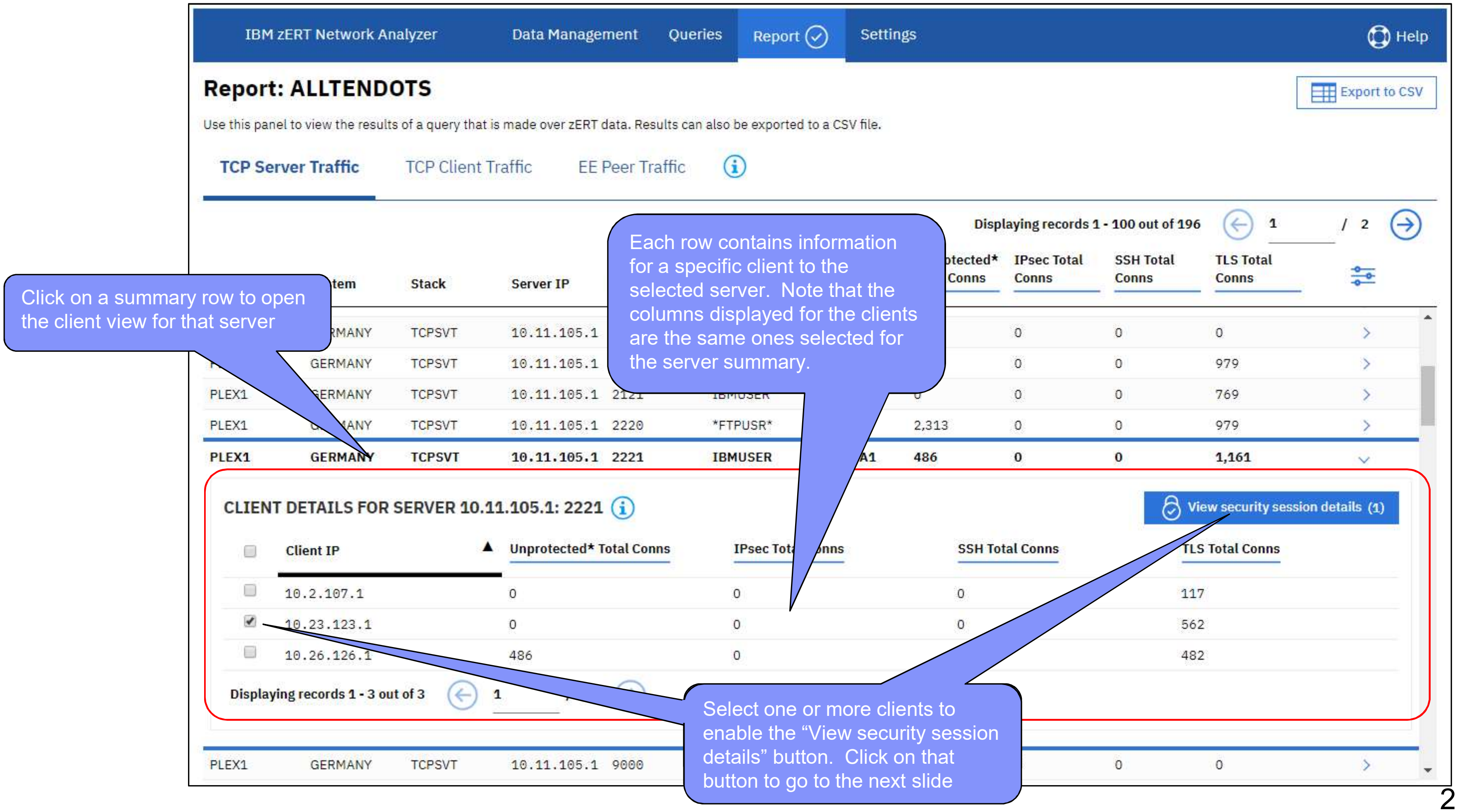
Displaying records 1 - 100 out of 196 1 /

Sysplex ▲	System	Stack	Server IP	Server Port	User ID	Job Name	Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	GERMANY	TCPSVT	10.11.105.1	20	*FTPUSR*	FTPUNIX	26	171	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	21	DAEMON	FTPUNIX1	4	22	0	0

Data points are organized by category. The selected points will be displayed in both the summary and client detail views.

Click this icon to select the specific data points (columns) to display and which to hide

zERT Network Analyzer Overview: Client detail view for a given server



Report: ALLTENDOTS

Use this panel to view the results of a query that is made over zERT data. Results can also be exported to a CSV file.

Displaying records 1 - 100 out of 196 ← 1 / 2 →

[illegible]	tem	Stack	Server IP	[illegible]	[illegible]	[illegible]	ptected* Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns	
[illegible]	RMANY	TCPSVT	10.11.105.1	[illegible]	[illegible]	[illegible]	[illegible]	0	0	0	>
[illegible]	GERMANY	TCPSVT	10.11.105.1	[illegible]	[illegible]	[illegible]	[illegible]	0	0	979	>
PLEX1	ERMANY	TCPSVT	10.11.105.1	2121	IBMUSER	[illegible]	0	0	0	769	>
PLEX1	G ANY	TCPSVT	10.11.105.1	2220	*FTPUSR*	[illegible]	2,313	0	0	979	>
PLEX1	**GERMANY**	**TCPSVT**	**10.11.105.1**	**2221**	**IBMUSER**	**A1**	**486**	**0**	**0**	**1,161**	⌄

CLIENT DETAILS FOR SERVER 10.11.105.1: 2221

□	Client IP ▲	Unprotected* Total Conns	IPsec Tota onns	SSH Total Conns	TLS Total Conns
□	10.2.107.1	0	0	0	117
☑	10.23.123.1	0	0	0	562
□	10.26.126.1	486	0	[illegible]	482

Displaying records 1 - 3 out of 3 ← 1

PLEX1	GERMANY	TCPSVT	10.11.105.1	9000	[illegible]	0	0	>

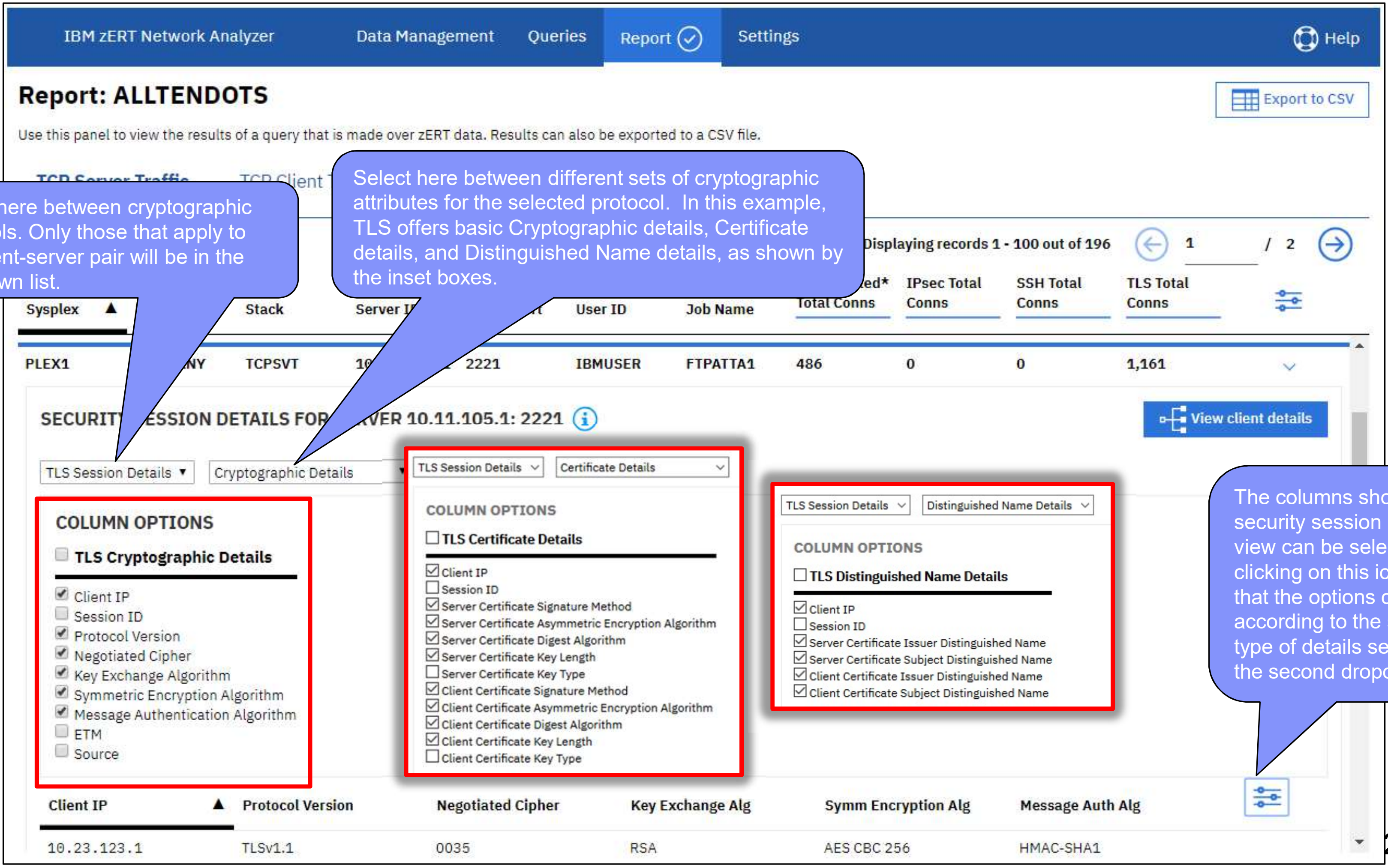
Click on a summary row to open the client view for that server

Each row contains information for a specific client to the selected server. Note that the columns displayed for the clients are the same ones selected for the server summary.

Select one or more clients to enable the “View security session details” button. Click on that button to go to the next slide

© 2019 IBM Corporation

zERT Network Analyzer Overview: Security session details view



Report: ALLTENDOTS

Use this panel to view the results of a query that is made over zERT data. Results can also be exported to a CSV file.

Displaying records 1 - 100 out of 196   1 / 2

Sysplex ▲		Stack	Server I		User ID	Job Name	…ed* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	…NY	TCPSVT	10…	2221	IBMUSER	FTPATTA1	486	0	0	1,161

SECURIT… …ESSION DETAILS FOR … …VER 10.11.105.1: 2221

TLS Session Details ▾   Cryptographic Details

COLUMN OPTIONS

□ **TLS Cryptographic Details**

- ☑ Client IP
- □ Session ID
- ☑ Protocol Version
- ☑ Negotiated Cipher
- ☑ Key Exchange Algorithm
- ☑ Symmetric Encryption Algorithm
- ☑ Message Authentication Algorithm
- □ ETM
- □ Source

TLS Session Details   Certificate Details

COLUMN OPTIONS

□ **TLS Certificate Details**

- ☑ Client IP
- □ Session ID
- ☑ Server Certificate Signature Method
- ☑ Server Certificate Asymmetric Encryption Algorithm
- ☑ Server Certificate Digest Algorithm
- ☑ Server Certificate Key Length
- □ Server Certificate Key Type
- ☑ Client Certificate Signature Method
- ☑ Client Certificate Asymmetric Encryption Algorithm
- ☑ Client Certificate Digest Algorithm
- ☑ Client Certificate Key Length
- □ Client Certificate Key Type

TLS Session Details   Distinguished Name Details

COLUMN OPTIONS

□ **TLS Distinguished Name Details**

- ☑ Client IP
- □ Session ID
- ☑ Server Certificate Issuer Distinguished Name
- ☑ Server Certificate Subject Distinguished Name
- ☑ Client Certificate Issuer Distinguished Name
- ☑ Client Certificate Subject Distinguished Name

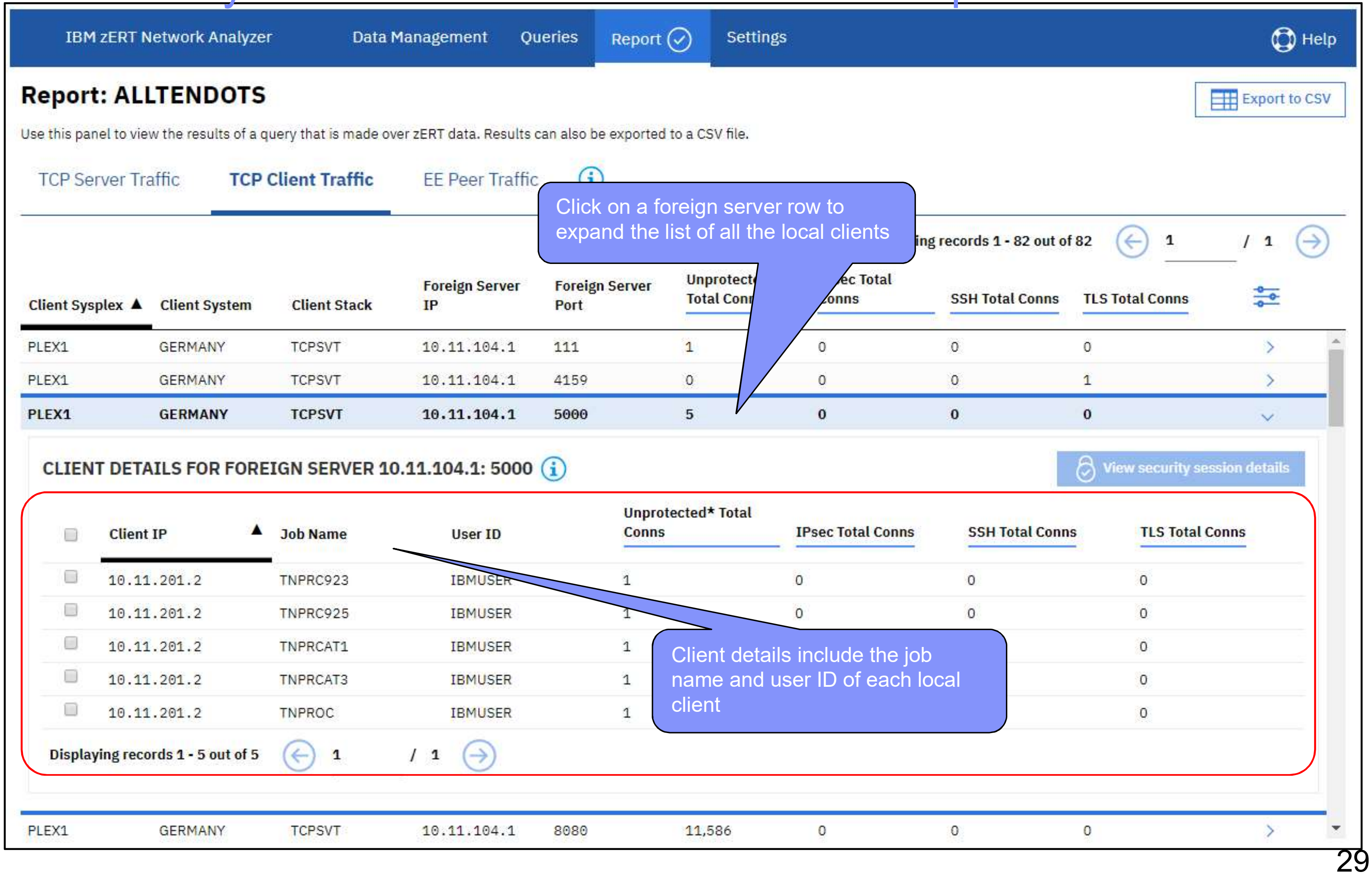
Client IP ▲	Protocol Version	Negotiated Cipher	Key Exchange Alg	Symm Encryption Alg	Message Auth Alg
10.23.123.1	TLSv1.1	0035	RSA	AES CBC 256	HMAC-SHA1

Select here between cryptographic protocols. Only those that apply to this client-server pair will be in the dropdown list.

Select here between different sets of cryptographic attributes for the selected protocol. In this example, TLS offers basic Cryptographic details, Certificate details, and Distinguished Name details, as shown by the inset boxes.

The columns shown in the security session details view can be selected by clicking on this icon. Note that the options change according to the specific type of details selected in the second dropdown.

zERT Network Analyzer Overview: TCP Client Traffic report



Report: ALLTENDOTS

Use this panel to view the results of a query that is made over zERT data. Results can also be exported to a CSV file.

Click on a foreign server row to expand the list of all the local clients

ing records 1 - 82 out of 82   1 / 1

Client Sysplex ▲	Client System	Client Stack	Foreign Server IP	Foreign Server Port	Unprotecte Total Conn	ec Total onns	SSH Total Conns	TLS Total Conns
PLEX1	GERMANY	TCPSVT	10.11.104.1	111	1	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.104.1	4159	0	0	0	1
PLEX1	**GERMANY**	**TCPSVT**	**10.11.104.1**	**5000**	**5**	**0**	**0**	**0**

CLIENT DETAILS FOR FOREIGN SERVER 10.11.104.1: 5000

□	Client IP ▲	Job Name	User ID	Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
□	10.11.201.2	TNPRC923	IBMUSER	1	0	0	0
□	10.11.201.2	TNPRC925	IBMUSER	1	0	0	0
□	10.11.201.2	TNPRCAT1	IBMUSER	1			0
□	10.11.201.2	TNPRCAT3	IBMUSER	1			0
□	10.11.201.2	TNPROC	IBMUSER	1			0

Displaying records 1 - 5 out of 5   1 / 1

Client details include the job name and user ID of each local client

Client Sysplex	Client System	Client Stack	Foreign Server IP	Foreign Server Port	Unprotected Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	GERMANY	TCPSVT	10.11.104.1	8080	11,586	0	0	0

© 2019 IBM Corporation

zERT Network Analyzer: Setup and configuration (1 of 4)

NOTE: In most shops, setting up the zERT Network Analyzer will require some **coordination between** your z/OS **networking team**, your z/OS **security team** and your **Db2 for z/OS team**. The steps that need to be accomplished are:

1. Enable the zERT Network Analyzer plugin in z/OSMF IZUPRMxx parmlib member. For example:

```
PLUGINS(COMMSERVER_CFG,SOFTWARE_MGMT,…,ZERT_ANALYZER)
```

2. Edit the IZUNASEC* sample JCL stream to add names of z/OS user IDs that are to be permitted access to the new plugin. For example:

```
/*  Connect the users of the zERT Network Analyzer to the     */
/*  zERT Network Analyzer group                               */
CONNECT USER1 GROUP(IZUZNA)
CONNECT USER2 GROUP(IZUZNA)
/*  End connect the users to zERT Network Analyzer group      */
```

3. Run the IZUNASEC job to create the appropriate SAF resources to control access to the plugin and grant the appropriate permissions for the appropriate z/OS user IDs
4. Create the zERT Network Analyzer database objects…

* - IZUNASEC works with RACF. Check with your vendor if you use a different security manager product.

© 2019 IBM Corporation

zERT Network Analyzer: Setup and configuration (2 of 4)

- Requires Db2 for z/OS 11 or higher
- Tooling is provided to allow DBAs to create zERT Network Analyzer database objects according to their own local conventions
  - IZUZNADT – DDL template with variables for appropriate names and resource identifiers
  - IZUZNADI – sample variable substitution file (provides values for each variable in the IZUZNADT template)
  - IZUZNADG – REXX exec that reads IZUZNADT and IZUZNADI and produces a customized DDL data set that your Db2 for z/OS DBAs can use to create the required database objects
- JDBC binding needs to be created on Db2 side (not done automatically)
- The zERT Network Analyzer performs all database operations under a single user ID that is configured via the database settings panel. This user ID must be granted the appropriate database privileges
- Once the zERT Network Analyzer database is created, the required JDBC connectivity parameters must be configured on the Database Settings panel of the UI
  - When a user logs into the UI, they will be forced to the Database Settings panel
  - Once the correct information is successfully configured, you can use the zERT Network Analyzer

© 2019 IBM Corporation

zERT Network Analyzer: Setup and configuration (3 of 4)

New!

Coming soon: APAR PH16222 (V2R3) / PH16223
Database administration enhancements

- CHANGES the way the zERT Network Analyzer manages query result tables
  - Significantly reduces the Db2 access privileges required by the network analyzer database user ID
  - Requires schema and Db2 resource allocation changes (all managed in database tooling)

- New IZUZNADA aliasing template that allows customization of schema and table names

- As with every zERT Network Analyzer PTF, the database tooling provided with the PTF will handle upgrading an existing database as well as creating a brand new database. Note that upgrade path does NOT handle switching an existing database to use the new IZUZNADA template.

© 2019 IBM Corporation

zERT Network Analyzer: Setup and configuration (4 of 4)

Some of the parameterized values in IZUZNADT template:

<authId>	z/OS auth ID for the Db2 objects
<database>	**DB name for persistent tables***
<QRTDatabase)	**DB name for query result (QR) tables***
<QRTParts>	**number of partitions for QR tables***
<tableStoGrp>	Storage group name - table spaces
<indexStoGrp>	Storage group name - indexes
<tablePriqty>	min primary space alloc - tables
<tableSecqty>	min secondary space alloc - tables
<indexPriqty>	min primary space alloc - indexes
<indexSecqty>	min secondary space alloc - indexes
<table4KbpName>	4K buffer pool name - tables
<table8KbpName>	8K buffer pool name - tables
<indexBpName>	Buffer pool name - indexes

*** - new with APAR PH16222 (V2R3) / PH16223 (V2R4) which also includes variables for index names and new IZUZNADA aliasing template that allows custom schema and table names**

	Table space names for...
<appSpace>	...application instance table
<dmhistSpace>	...data mgmt history table
<dsSpace>	...data set table
<topologySpace>	...topology table
<secsessSpace>	...security sessions table
<sessstatsSpace>	...session statistics table
<ipsecSpace>	...ipsec info table
<sshSpace>	...ssh info table
<tlsSpace>	...tls/ssl info table
<topoSpace>	...toplogy table
<querySpace>	...user-built query table
<scopeFltrSpace>	...scope filter table
<scopeFltrEndptSpace>	...scope filter table
<scopeFltrSysspecSpace>	...scope filter table
<secFltrSpace>	...security filter table
<secIpsecFltrSpace>	...IPsec security filter table
<secSshFltrSpace>	...SSH security filter table
<secTlsFltrSpace>	...TLS security filter table
<openjpaSpace>	...JPA sequence table

© 2019 IBM Corporation

Agenda

- Background – why zERT?
- zERT overview
- Configuring zERT Discovery and Aggregation
- zERT Network Analyzer
- **zERT support in other products**
- Considerations
- Summary

© 2019 IBM Corporation

Other products with zERT support (as of December, 2019)

IBM is aware of the following products that have shipped new support for zERT data. Note that this should not be considered to be a comprehensive list as **there may be others of which IBM is currently unaware**:

- IBM zSecure Audit V2.3 (supports subtype 11 and subtype 12 records)
- IBM QRadar SIEM (supports what zSecure feeds it)
- Merrill Technologies MXG (feeds subtype 11 and subtype 12 records into SAS)
- Broadcom (formerly CA Technologies) NetMaster Network Management for TCP/IP 12.2.03 (supports subtype 11 records through NMI)
- BMC Mainview for IP 3.6 (supports subtype 11 and subtype 12 records through NMI)
- Vanguard Advisor 2.3 (supports subtype 11 records)
- IntelliMagic Vision (supports subtype 12 records)
- IBM Z Common Data Provider 2.1.0 (supports subtype 11 and 12 records)
- IBM NetView Version 6.3 will be adding support for subtype 11 records through NMI in their connection views in 4Q2019

We hope this list will continue to grow over time

© 2019 IBM Corporation

Agenda

- Background – why zERT?
- zERT overview
- Configuring zERT Discovery and Aggregation
- zERT Network Analyzer
- zERT support in other products
- **Considerations**
- **Summary**

Considerations (1 of 2)

- zERT can generate very large volumes of subtype 11 records, depending on the number of connections supported by your z/OS system.
  - Please plan accordingly
  - Consider only capturing subtype 12 records on a regular basis and only capture subtype 11s for limited times when investigating specific traffic or if using a real-time monitoring application.

- zERT monitors TCP and Enterprise Extender traffic. All other IP protocols are unmonitored.

- zERT monitors traffic that terminates at the local TCP/IP stack. It does not monitor routed traffic

- zERT does not store or record the values of secret keys, initialization vectors, or any other secret values that are negotiated or derived during cryptographic protocol handshakes.

- Regardless of the prior point, the zERT data that is recorded provides a fairly complete picture of the z/OS system's network cryptographic protection profile. As such, you should take appropriate steps to protect the recorded SMF data as well as access to the zERT real-time network monitoring services.

© 2019 IBM Corporation

Considerations (2 of 2)

- zERT only monitors connections that are established after zERT is enabled (or re-enabled).
  - If you disable and later re-enable zERT, it will no longer monitor any of the connections that existed before re-enabling.
  - To ensure the most complete monitoring, enable zERT in your TCP/IP profile

- TCP traffic protected by other TLS/SSL implementations (JSSE, OpenSSL, other SSH, etc.) will only be reported through stream observation. Limitations:
  - Only reports initial handshake as long as it is the first thing to flow over the connection. zERT stream observation has no visibility to rehandshakes or early termination of security sessions
  - zERT stream observation has no visibility to attributes that are negotiated during the initial handshake using encrypted messages

- There are some limitations to the data that zERT stream observation can collect or that zERT will collect in mixed-release environments. For details, consult the z/OS Communications Server IP Configuration Guide.

Summary: Customer value

- zERT SMF 119 Connection Detail (subtype 11) records:
  - Provide ample opportunity for correlation to records (SMF or otherwise) from other applications, workloads and devices to help build an larger picture of individual network connections to z/OS
  - Can reveal traffic that is being double-protected
  - Can be used to verify use of refreshed digital certificates (when zERT-enabled CPPs are used)
  - Well-suited for realtime monitoring applications
- zERT SMF 119 Summary (subtype 12) records:
  - Provide the 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 for reporting and analysis applications
- Several network monitoring and audit-related products now support zERT data – some of them providing near real-time views based on Connection Detail records
- The zERT Network Analyzer:
  - Makes it easy for z/OS network security admins to consume, query and search zERT data
  - Great flexibility in creating queries that zero in on the specific systems, endpoints, time spans, and security attributes of interest. These queries can be built for regular compliance checks or for special purpose investigations
  - Query results can be viewed through a browser or exported to a CSV file for post-processing

© 2019 IBM Corporation

For more information

URL	Content
http://tinyurl.com/zoscsblog	IBM Communications Server blog
https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.cs3/cs3.htm	IBM Communications Server library

© 2019 IBM Corporation

Thank you!

© 2019 IBM Corporation

Notices and disclaimers (1 of 2)

© 2019 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 (2 of 2)

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.

.

© 2019 IBM Corporation

Backup

© 2019 IBM Corporation

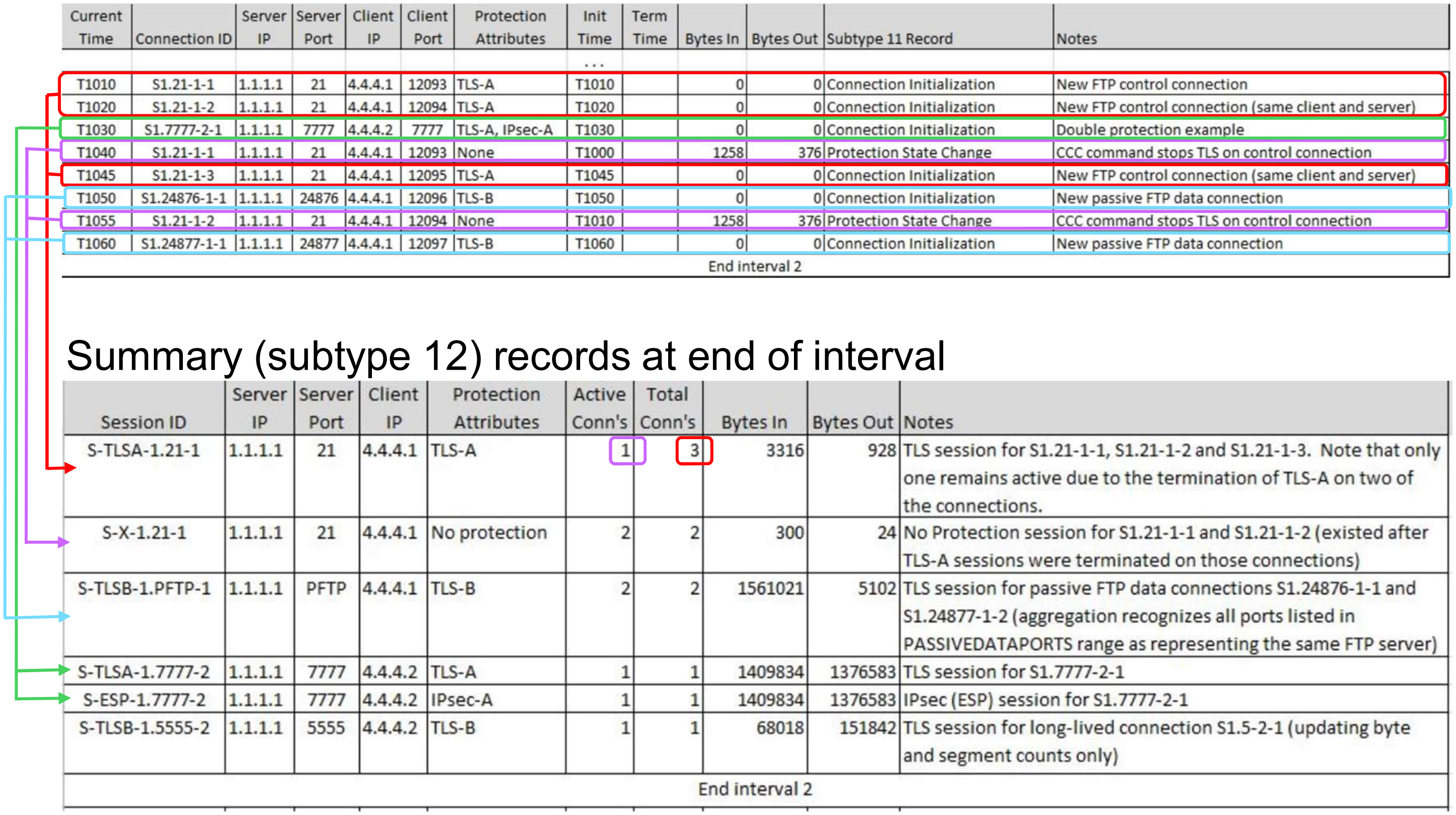
Important zERT terms

- *Cryptographic Protocol Provider (CPP):* A z/OS-resident component that processes a specific cryptographic network security protocol (i.e., TLS/SSL, IPSec or SSH).
  - IBM zERT-enabled CPPs:
    - System SSL, OpenSSH and IPSec
    - ZERTJSSE provider - shipped with IBM SDK, Java Technology Edition 8.0.0 Service Refresh 5, Fix Pack 25 – wraps the standard Java 8 JSSE
  - IBM non-zERT enabled CPPs: JSSE in any form other than ZERTJSSE
  - 3rd party non-zERT-enabled: Tectia SSH, OpenSSL, etc.
- *Protection state:* The cumulative state of cryptographic protection of a connection. There are numerous possible combinations here:
  - No cryptographic protection (connection is in cleartext mode)
  - Protection from a single cryptographic protocol (most common case)
  - Protection from multiple cryptographic protocols (for example, a TCP connection protected by both TLS and IPSec)
- *Application **connection**:* A sockets-based connection between two application programs. No security is implied or provided – just a cleartext path.
- *Security **session**:* The application (by a CPP) of an agreed-to set of security attributes (as defined by a cryptographic security protocol) to one or more application connections between the same client and server. Examples are TLS/SSL sessions, IPSec tunnels and SSH sessions.

© 2019 IBM Corporation

zERT Aggregation example (and eye test!)

Connection detail (subtype 11) records for one SMF interval



Current Time	Connection ID	Server IP	Server Port	Client IP	Client Port	Protection Attributes	Init Time	Term Time	Bytes In	Bytes Out	Subtype 11 Record	Notes
							. . .					
T1010	S1.21-1-1	1.1.1.1	21	4.4.4.1	12093	TLS-A	T1010		0	0	Connection Initialization	New FTP control connection
T1020	S1.21-1-2	1.1.1.1	21	4.4.4.1	12094	TLS-A	T1020		0	0	Connection Initialization	New FTP control connection (same client and server)
T1030	S1.7777-2-1	1.1.1.1	7777	4.4.4.2	7777	TLS-A, IPsec-A	T1030		0	0	Connection Initialization	Double protection example
T1040	S1.21-1-1	1.1.1.1	21	4.4.4.1	12093	None	T1000		1258	376	Protection State Change	CCC command stops TLS on control connection
T1045	S1.21-1-3	1.1.1.1	21	4.4.4.1	12095	TLS-A	T1045		0	0	Connection Initialization	New FTP control connection (same client and server)
T1050	S1.24876-1-1	1.1.1.1	24876	4.4.4.1	12096	TLS-B	T1050		0	0	Connection Initialization	New passive FTP data connection
T1055	S1.21-1-2	1.1.1.1	21	4.4.4.1	12094	None	T1010		1258	376	Protection State Change	CCC command stops TLS on control connection
T1060	S1.24877-1-1	1.1.1.1	24877	4.4.4.1	12097	TLS-B	T1060		0	0	Connection Initialization	New passive FTP data connection
									End interval 2			

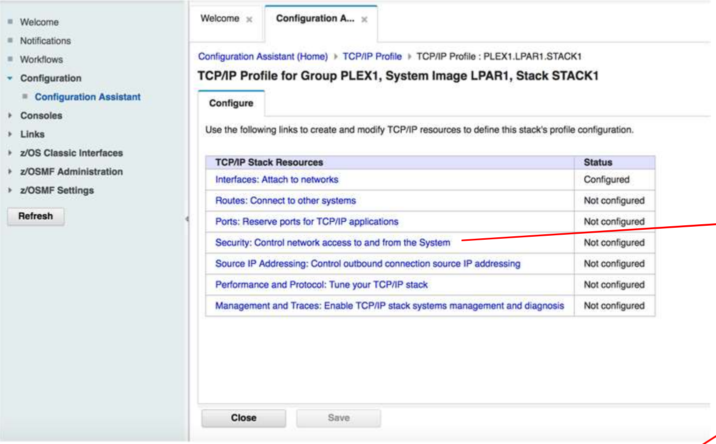
Summary (subtype 12) records at end of interval

Session ID	Server IP	Server Port	Client IP	Protection Attributes	Active Conn's	Total Conn's	Bytes In	Bytes Out	Notes
S-TLSA-1.21-1	1.1.1.1	21	4.4.4.1	TLS-A	1	3	3316	928	TLS session for S1.21-1-1, S1.21-1-2 and S1.21-1-3. Note that only one remains active due to the termination of TLS-A on two of the connections.
S-X-1.21-1	1.1.1.1	21	4.4.4.1	No protection	2	2	300	24	No Protection session for S1.21-1-1 and S1.21-1-2 (existed after TLS-A sessions were terminated on those connections)
S-TLSB-1.PFTP-1	1.1.1.1	PFTP	4.4.4.1	TLS-B	2	2	1561021	5102	TLS session for passive FTP data connections S1.24876-1-1 and S1.24877-1-2 (aggregation recognizes all ports listed in PASSIVEDATAPORTS range as representing the same FTP server)
S-TLSA-1.7777-2	1.1.1.1	7777	4.4.4.2	TLS-A	1	1	1409834	1376583	TLS session for S1.7777-2-1
S-ESP-1.7777-2	1.1.1.1	7777	4.4.4.2	IPsec-A	1	1	1409834	1376583	IPsec (ESP) session for S1.7777-2-1
S-TLSB-1.5555-2	1.1.1.1	5555	4.4.4.2	TLS-B	1	1	68018	151842	TLS session for long-lived connection S1.5-2-1 (updating byte and segment counts only)
							End interval 2		

© 2019 IBM Corporation

zERT Discovery and Aggregation config via Network Configuration Assistant (1 of 3)

TCP/IP profile configuration tasks



Configuration Assistant (Home) ▸ TCP/IP Profile ▸ TCP/IP Profile : PLEX1.LPAR1.STACK1

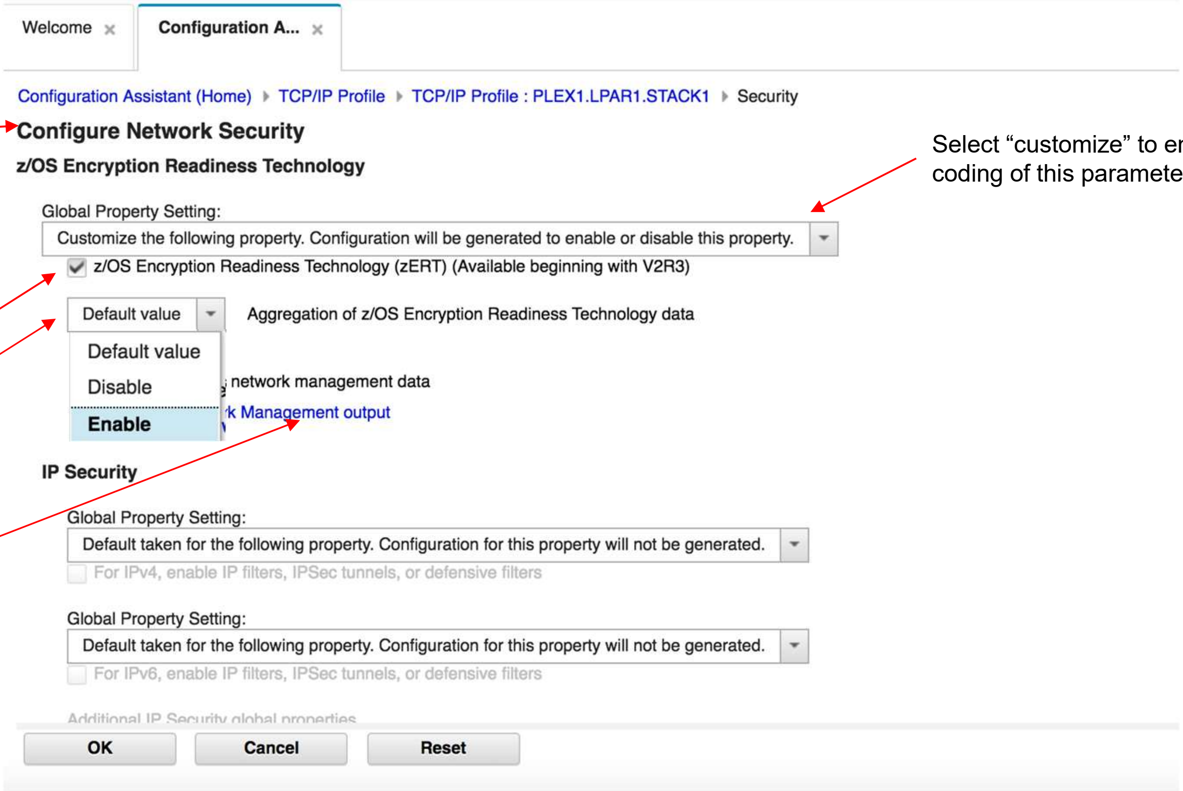
TCP/IP Profile for Group PLEX1, System Image LPAR1, Stack STACK1

Use the following links to create and modify TCP/IP resources to define this stack's profile configuration.

TCP/IP Stack Resources	Status
Interfaces: Attach to networks	Configured
Routes: Connect to other systems	Not configured
Ports: Reserve ports for TCP/IP applications	Not configured
Security: Control network access to and from the System	Not configured
Source IP Addressing: Control outbound connection source IP addressing	Not configured
Performance and Protocol: Tune your TCP/IP stack	Not configured
Management and Traces: Enable TCP/IP stack systems management and diagnosis	Not configured

Aggregation requires Configuration Assistant APAR **PI94208**

Configure Network Security



Configuration Assistant (Home) ▸ TCP/IP Profile ▸ TCP/IP Profile : PLEX1.LPAR1.STACK1 ▸ Security

Configure Network Security

z/OS Encryption Readiness Technology

Global Property Setting:
Customize the following property. Configuration will be generated to enable or disable this property.

☑ z/OS Encryption Readiness Technology (zERT) (Available beginning with V2R3)

Default value ▾ Aggregation of z/OS Encryption Readiness Technology data

network management data

k Management output

IP Security

Global Property Setting:
Default taken for the following property. Configuration for this property will not be generated.

□ For IPv4, enable IP filters, IPSec tunnels, or defensive filters

Global Property Setting:
Default taken for the following property. Configuration for this property will not be generated.

□ For IPv6, enable IP filters, IPSec tunnels, or defensive filters

Additional IP Security global properties

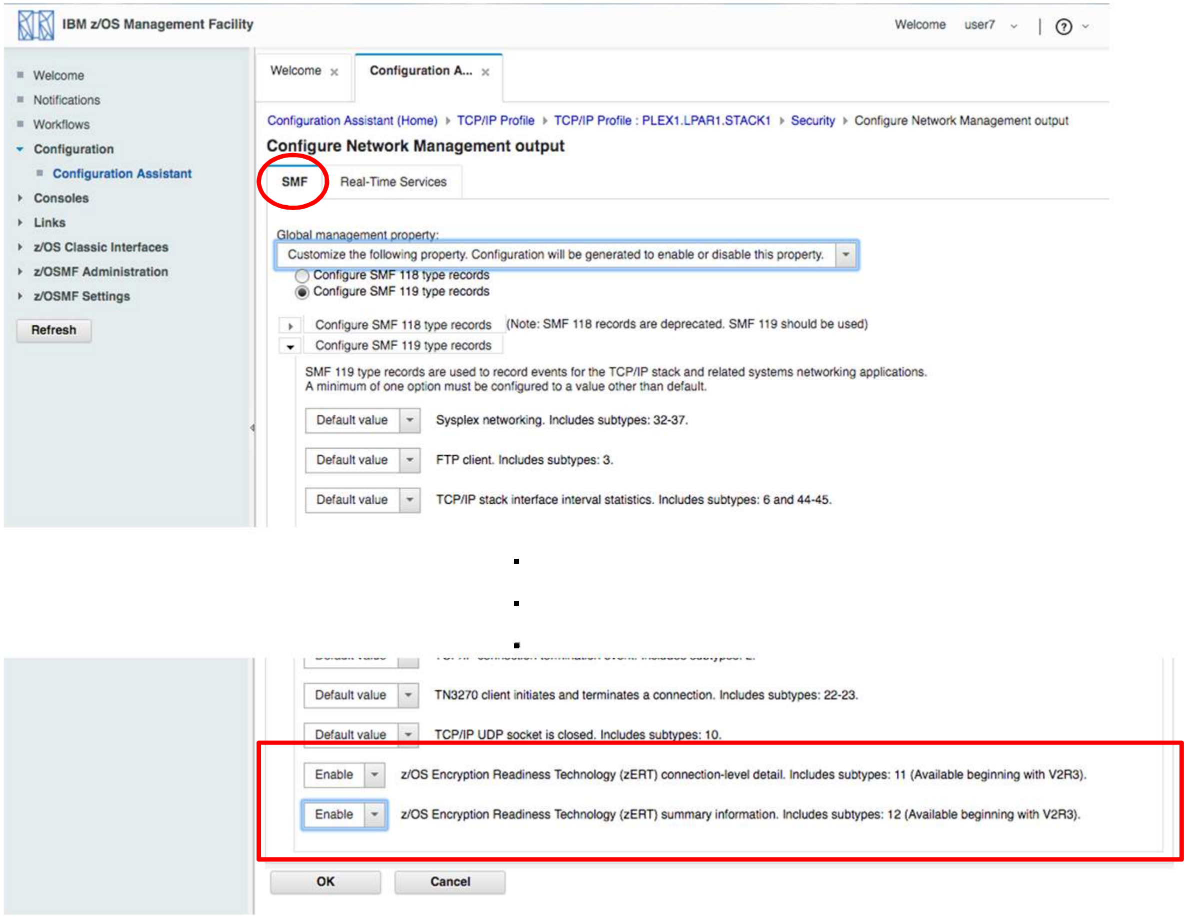
Select "customize" to enable coding of this parameter

Checkbox enables zERT in-memory montoring

Dropdown controls coding of AGGREGATION subparameter

Brings you to the next page

zERT Discovery and Aggregation config via Network Configuration Assistant (2 of 3)



Configuration Assistant (Home) ▸ TCP/IP Profile ▸ TCP/IP Profile : PLEX1.LPAR1.STACK1 ▸ Security ▸ Configure Network Management output

Configure Network Management output

Global management property:

Customize the following property. Configuration will be generated to enable or disable this property.

○ Configure SMF 118 type records
● Configure SMF 119 type records

▸ Configure SMF 118 type records (Note: SMF 118 records are deprecated. SMF 119 should be used)

▾ Configure SMF 119 type records

SMF 119 type records are used to record events for the TCP/IP stack and related systems networking applications.
A minimum of one option must be configured to a value other than default.

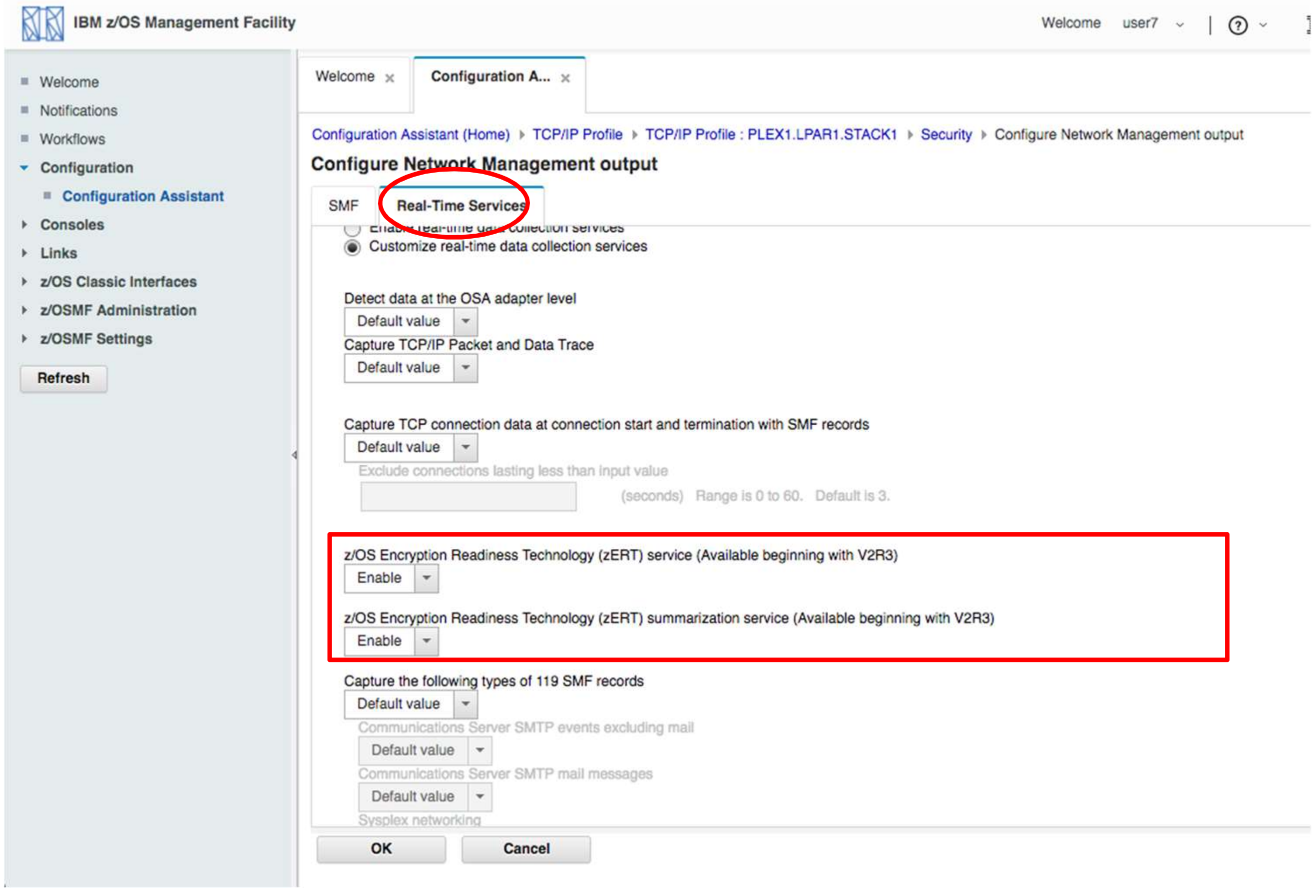
Default value	Sysplex networking. Includes subtypes: 32-37.
Default value	FTP client. Includes subtypes: 3.
Default value	TCP/IP stack interface interval statistics. Includes subtypes: 6 and 44-45.

.
.
.

Default value	TN3270 client initiates and terminates a connection. Includes subtypes: 22-23.
Default value	TCP/IP UDP socket is closed. Includes subtypes: 10.
Enable	z/OS Encryption Readiness Technology (zERT) connection-level detail. Includes subtypes: 11 (Available beginning with V2R3).
Enable	z/OS Encryption Readiness Technology (zERT) summary information. Includes subtypes: 12 (Available beginning with V2R3).

© 2019 IBM Corporation

zERT Discovery and Aggregation config via Network Configuration Assistant (3 of 3)



Configuration Assistant (Home) ▸ TCP/IP Profile ▸ TCP/IP Profile : PLEX1.LPAR1.STACK1 ▸ Security ▸ Configure Network Management output

Configure Network Management output

○ Enable real-time data collection services
● Customize real-time data collection services

Detect data at the OSA adapter level: Default value

Capture TCP/IP Packet and Data Trace: Default value

Capture TCP connection data at connection start and termination with SMF records: Default value

Exclude connections lasting less than input value: (seconds) Range is 0 to 60. Default is 3.

z/OS Encryption Readiness Technology (zERT) service (Available beginning with V2R3): Enable

z/OS Encryption Readiness Technology (zERT) summarization service (Available beginning with V2R3): Enable

Capture the following types of 119 SMF records: Default value

Communications Server SMTP events excluding mail: Default value

Communications Server SMTP mail messages: Default value

Sysplex networking