z/OS 3.1 IBM Education Assistant

Solution Name: zERT Network Analyzer Enhanced Upgrade Support

Solution Name: zERT Network Analyzer enhancements for database connection authentication

Solution Element: HSMA31E (IBM zERT Network Analyzer)

July 2023

Agenda

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

Trademarks

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

Objectives

In 3.1, IBM zERT Network Analyzer addresses these customer requirements

Requirement 1: To support passphrases to authenticate with Db2® for z/OS®

- AS-IS: IBM zERT Network Analyzer only accepts passwords up to 8 characters

Requirement 2: To improve switching between multiple database users

- AS-IS: For clients using their own user IDs as the database user ID, it is cumbersome to clear and switch users

Requirement 3: To streamline release-to-release migration

- AS-IS: Database connection and application settings needs to be manually copied from one release to another
- AS-IS: Previous releases required the creation of a new IBM zERT Network Analyzer database instead of reusing existing database.

Overview (1)

IBM zERT Network Analyzer

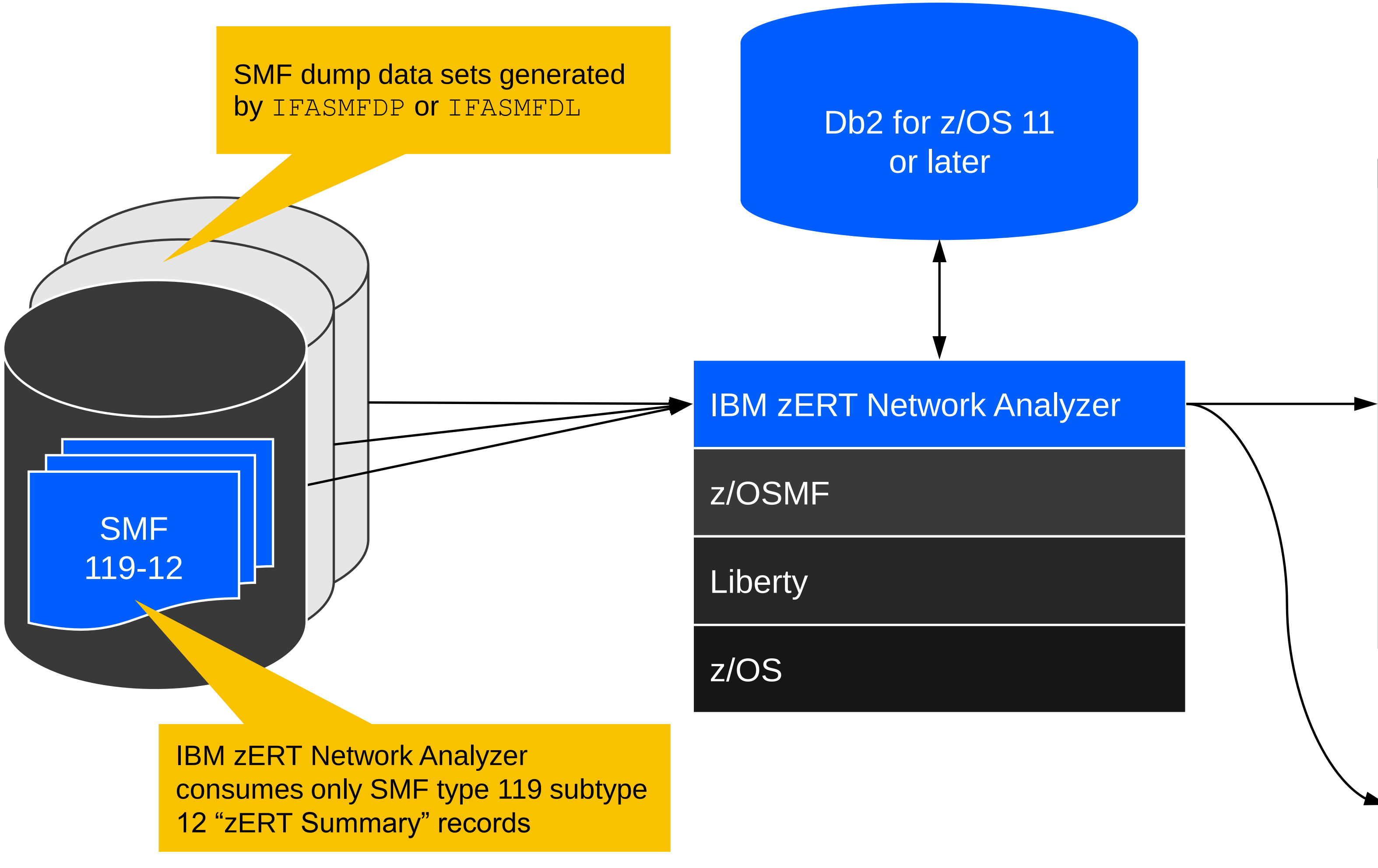
Overview (2)

- IBM zERT Network Analyzer is a standalone, optional z/OSMF plug-in
  - Web UI makes SMF Type 119 Subtype 12 (“zERT Summary”) data consumable for z/OS network security administrators
  - Used primarily to investigate cryptographic attributes of a network
    - Users can formulate their own queries using *scope* (date, system name, TCP/Enterprise Extender (EE) endpoints, etc.) and *security* filters (unprotected/no recognized protection, TLS, IPsec, SSH session attributes)
    - Running a query returns summary level results that can be drilled down to view:
      - TCP client and EE peer details
      - Security session details for matching sessions
    - Query results can also be exported as CSV files to z/OS UNIX® file path

- Uses a dedicated z/OS user ID to communicate with Db2 for z/OS
  - Stores imported SMF Type 119 Subtype 12 data in a specialized schema
- Shipped with z/OS Communications Server since V2R4

Overview (3)

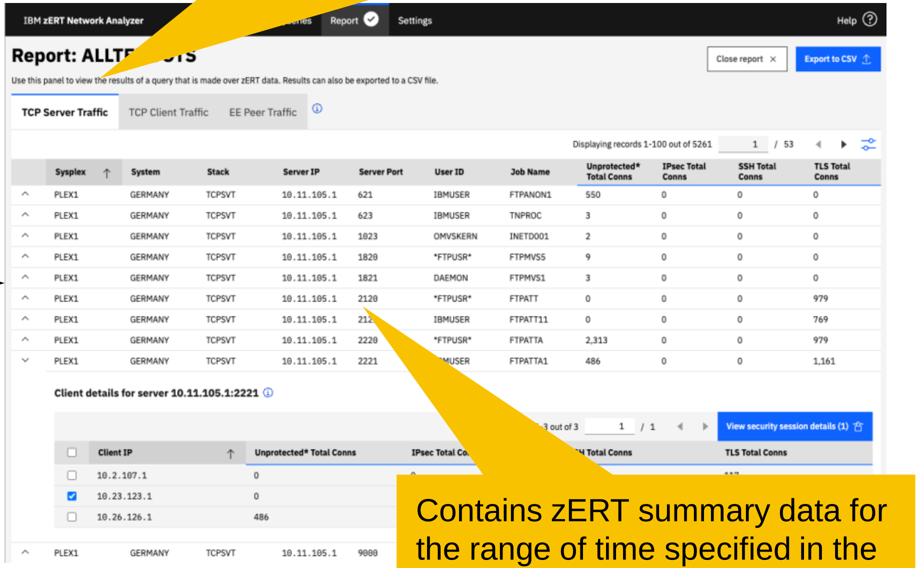
SMF dump data sets generated by `IFASMFDP` or `IFASMFDL`



IBM zERT Network Analyzer consumes only SMF type 119 subtype 12 "zERT Summary" records

Users can build queries with scope and security filters:

- **Scope** filters: Sysplex / system / stack, IP addresses / server port, z/OS role (client or server) and range of dates
- **Security** filters: crypto protocol, protocol version, crypto algorithms and key lengths, etc.



Report: ALLTE

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 5261 1 / 53

	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	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
^	PLEX1	GERMANY	TCPSVT	10.11.105.1	2120	*FTPUSR*	FTPATT	0	0	0	979
^	PLEX1	GERMANY	TCPSVT	10.11.105.1	212	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	MUSER	FTPATTA1	486	0	0	1,161

Client details for server 10.11.105.1:2221

3 out of 3 1 / 1

□	Client IP	Unprotected* Total Conns	IPsec Total Co	H Total Conns	TLS Total Conns
□	10.2.107.1	0			
☑	10.23.123.1	0			
□	10.26.126.1	486			

^	PLEX1	GERMANY	TCPSVT	10.11.105.1	9000

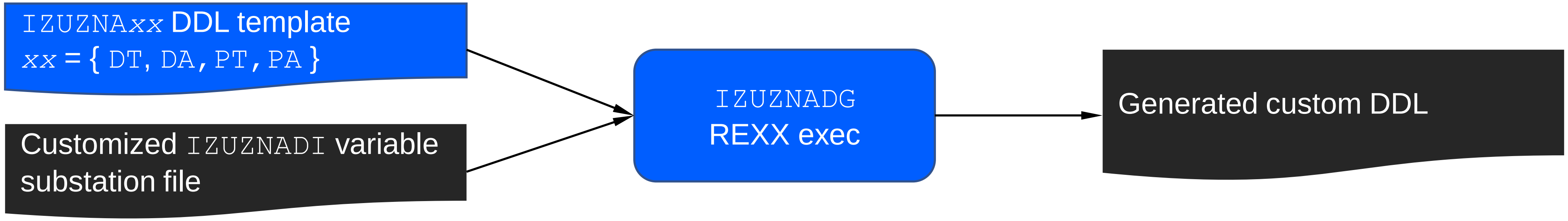
Contains zERT summary data for the range of time specified in the query

.csv file

Query results can be exported as a CSV file to z/OS UNIX file system

Overview (4)

- IBM zERT Network Analyzer comes with existing database schema tooling for creating custom Data Definition Language (DDL) when setting up a new database or making updates when needed
  - DDL templates:
    - `IZUZNA`**`DT`** creates or applies PTF-related updates to a network analyzer database using a fixed naming scheme for all the tables
    - `IZUZNA`**`DA`** creates or applies PTF-related updates to a network analyzer database using aliases for the tables. This is intended for use by customers that have internal table naming standards that the fixed table names would not conform to.
    - `IZUZNA`**`PT`** and `IZUZNA`**`PA`** modify the number of partitions in a set of partition by range tables in the network analyzer database. These use the fixed and aliased naming schemes, respectively.
  - `IZUZNA`**`DI`**: Sample variable substitution file (provides values for each variable in the `IZUZNADT` and `IZUZNADA` templates – your DBA specifies customized values in this file
  - `IZUZNA`**`DG`**: REXX exec that produces executable DDL using a specified template and variable substitution file as input


IZUZNA*xx* DDL template
xx = { DT, DA, PT, PA }
Customized IZUZNADI variable substation file
IZUZNADG
REXX exec
Generated custom DDL

Overview (5)

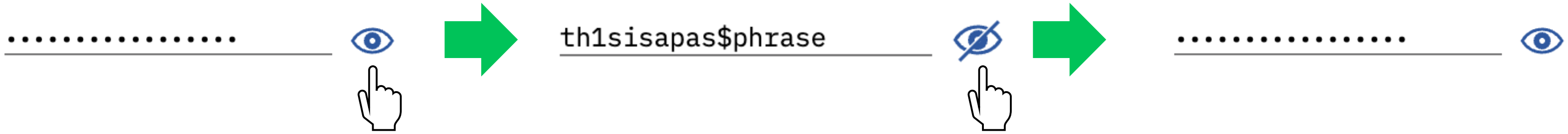
- Who
  - Users of IBM zERT Network Analyzer (z/OS network security administrators)
  - z/OSMF administrators
  - Db2 for z/OS database administrator (DBAs)
- What
  - **IBM zERT Network Analyzer enhancements for database connection authentication**
    - New passphrase support, ability to clear database user ID credentials
  - **IBM zERT Network Analyzer enhanced upgrade support**
    - New panel to reset or import IBM zERT Network Analyzer application settings from a prior release
    - New panel to import IBM zERT Network Analyzer database connection settings from a prior release
    - New DDL templates to facilitate migrating IBM zERT Network Analyzer database from to current schema level
- Wow
  - Connection to IBM zERT Network Analyzer database no longer tied to 8-character passwords and now easier to switch between different database users.
  - Easier migration of IBM zERT Network Analyzer settings and database to 3.1

Usage & Invocation (1)

IBM zERT Network Analyzer enhancements for database connection authentication

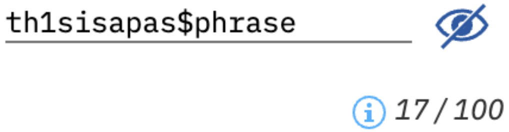
Usage & Invocation (2)

- **New:** Database Settings panel updated to add passphrase support of up to 100 characters for the IBM zERT Network Analyzer database user ID
- **New:** The following ease-of-use features are added to assist with long passphrases:
  - Password field Hide/Show button – this gives users an option to display passphrases in cleartext as it's being entered



th1sisapas$phrase

  - Password field character counter – this displays a ratio of the current characters used and the total character limit of 100



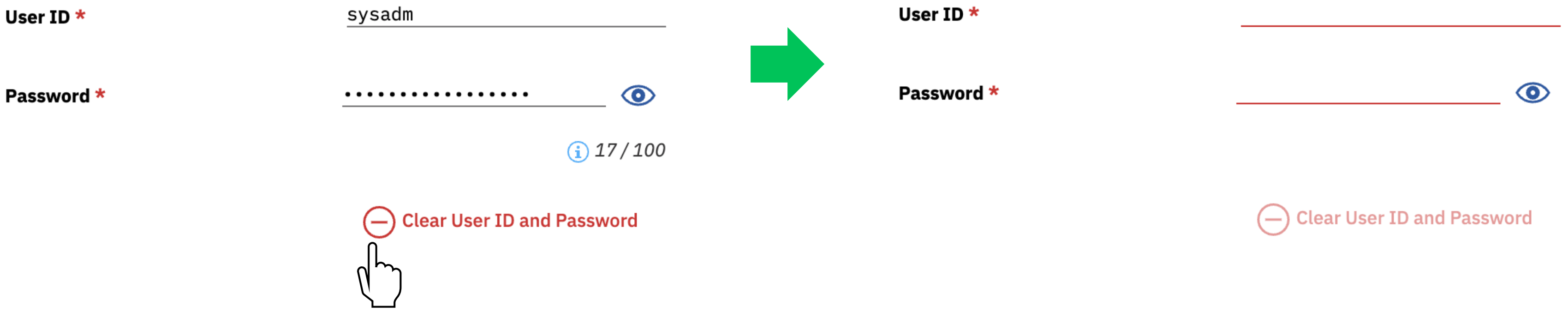
th1sisapas$phrase

17 / 100

- **Enhancement:** When invalid database credentials are used a unique error message is returned:
  - IZUET0056E: Database User ID or Password not accepted. Please reenter and save your database settings.
- **Enhancement:** The IBM zERT Network Analyzer will not attempt to connect to database again under new credentials are entered.

Usage & Invocation (3)

- **New:** Allow users to clear out their user ID and password from the Database Settings panel.
  - Users have 2 options to clear out their credentials:
    - Option 1 - Click a dedicated button that clears out the user ID and password
    - Option 2 - Clear out the User ID and Password fields manually and click the ‘Save settings’ button
  - Once the empty credentials are saved, IBM zERT Network Analyzer returns to the *Database Settings* panel and locks the user in that panel until the database connection settings are updated with the appropriate values.



User ID * sysadm

Password * •••••••••••••••••

17 / 100

User ID *

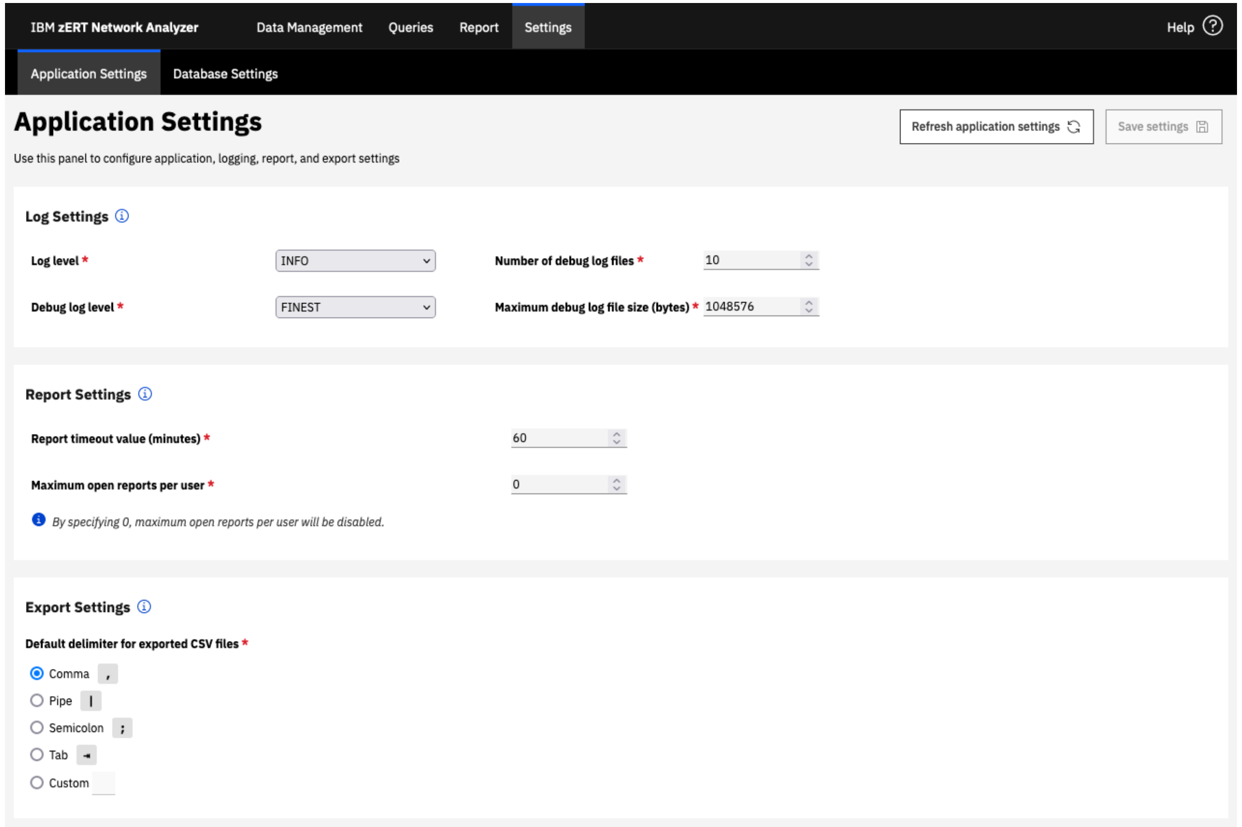
Password *

Usage & Invocation (4)

IBM zERT Network Analyzer enhanced upgrade support

Usage & Invocation (5)

- **Settings / Application Settings panel:**
    - Allows an end-user to modify the Log, Report, and Export settings.
    - There is no requirement for the user to enter application settings during IBM zERT Network Analyzer setup – a set of default values are provided for any settings that are not modified by the user.
    - Prior to 3.1, application settings needed to be manually copied from one release to another.



Application Settings

Use this panel to configure application, logging, report, and export settings

Log Settings

Log level * INFO

Debug log level * FINEST

Number of debug log files * 10

Maximum debug log file size (bytes) * 1048576

Report Settings

Report timeout value (minutes) * 60

Maximum open reports per user * 0

By specifying 0, maximum open reports per user will be disabled.

Export Settings

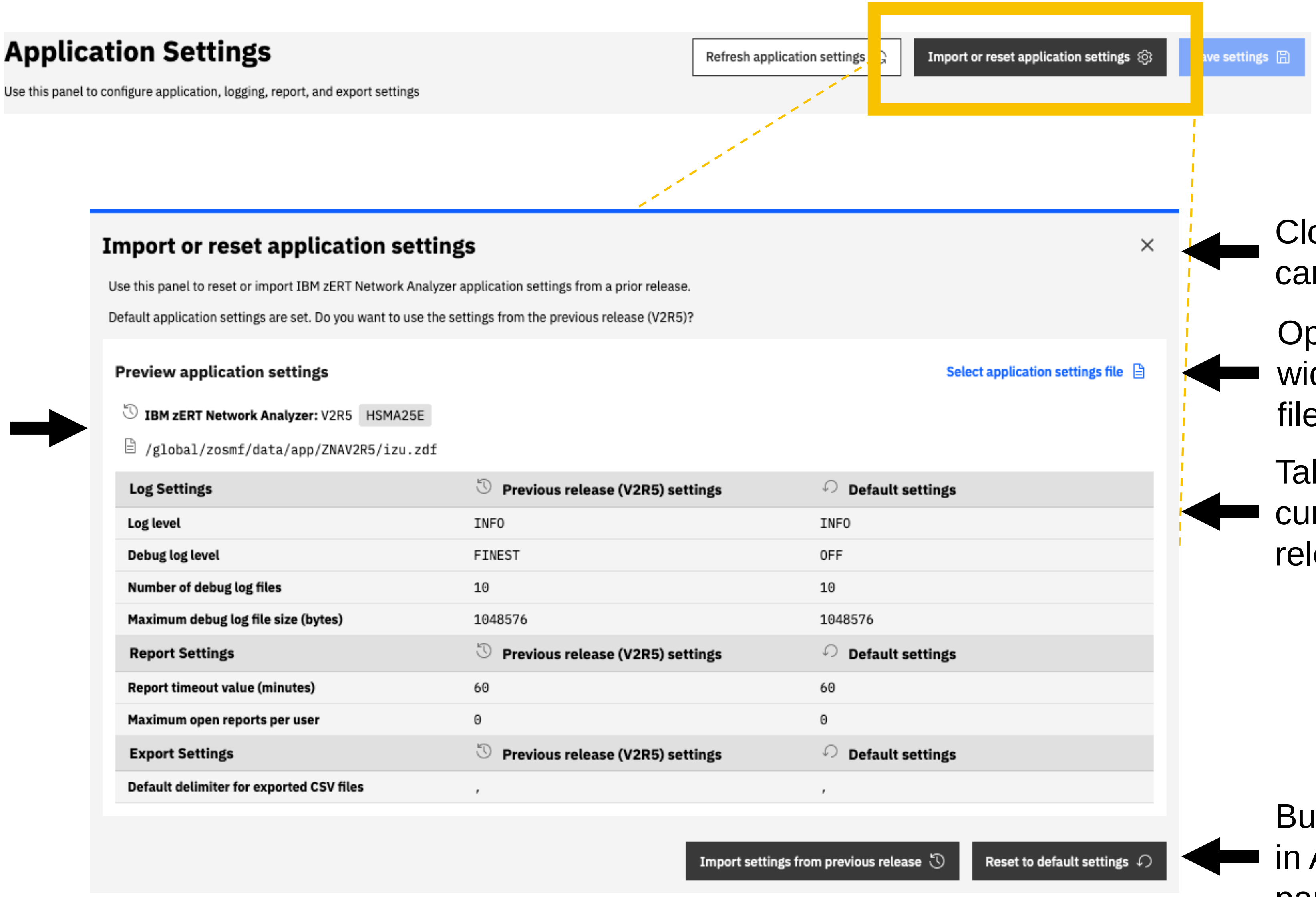
Default delimiter for exported CSV files *

● Comma ,
○ Pipe |
○ Semicolon ;
○ Tab ⇥
○ Custom

Usage & Invocation (6)

- **New:** “Import or reset application settings” modal
  - *Settings* / *Database Settings* / **Import or reset application settings**
  - A new modal appears on top of *Application Settings* panel (screenshot on next slide).
- If application settings are not configured, the panel will attempt to automatically locate a prior release’s application settings within current z/OSMF file system.
  - Automatic search order: *n*-1 (V2R5), *n*-2 (V2R4)
  - Alternatively, an application settings file (`izu.zdf`) can be manually selected using a file widget. The file must be selected from a z/OS UNIX file path.
- Importing application settings updates fields within *Application Settings* panel, requires clicking Save settings to apply.

Usage & Invocation (7)


Refresh application settings
Import or reset application settings
ave settings
Select application settings file
Import settings from previous release
Reset to default settings

Application Settings

Use this panel to configure application, logging, report, and export settings

Import or reset application settings

Use this panel to reset or import IBM zERT Network Analyzer application settings from a prior release.

Default application settings are set. Do you want to use the settings from the previous release (V2R5)?

Preview application settings

IBM zERT Network Analyzer: V2R5 HSMA25E

/global/zosmf/data/app/ZNAV2R5/izu.zdf

Log Settings	Previous release (V2R5) settings	Default settings
Log level	INFO	INFO
Debug log level	FINEST	OFF
Number of debug log files	10	10
Maximum debug log file size (bytes)	1048576	1048576
Report Settings	**Previous release (V2R5) settings**	**Default settings**
Report timeout value (minutes)	60	60
Maximum open reports per user	0	0
Export Settings	**Previous release (V2R5) settings**	**Default settings**
Default delimiter for exported CSV files	,	,

Close modal and cancel import

Opens z/OSMF file widget for manual file select

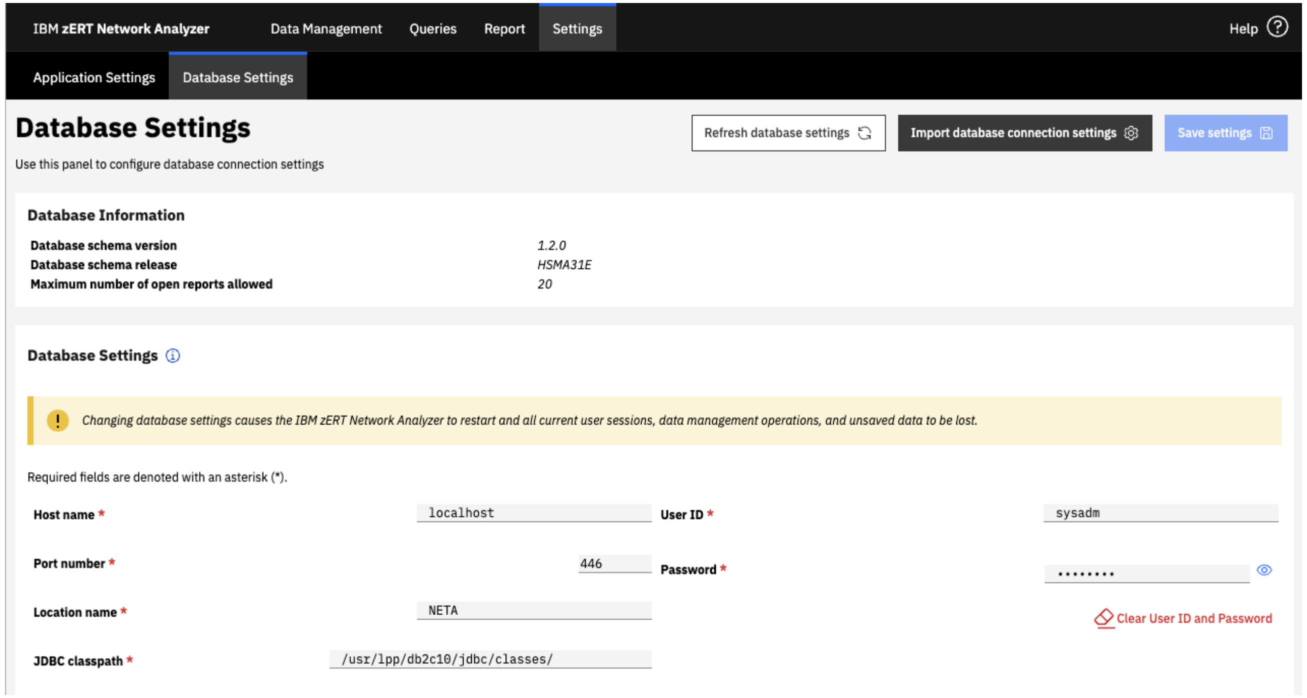
Table comparing current and previous release settings

Button to update fields in Application Settings panel

Release/FMID and path of application settings file

Usage & Invocation (8)

- **Settings / Database Settings panel:**
  - Allows an end-user to view database information and modify the connection parameters used to connect to Db2 for z/OS.
  - Users are locked to this settings panel until valid database settings are set.
  - Prior to 3.1, database connection settings needed to be manually copied from one release to another.



Database Settings

Use this panel to configure database connection settings

Database Information

Database schema version	*1.2.0*
Database schema release	*HSMA31E*
Maximum number of open reports allowed	*20*

Database Settings

Changing database settings causes the IBM zERT Network Analyzer to restart and all current user sessions, data management operations, and unsaved data to be lost.

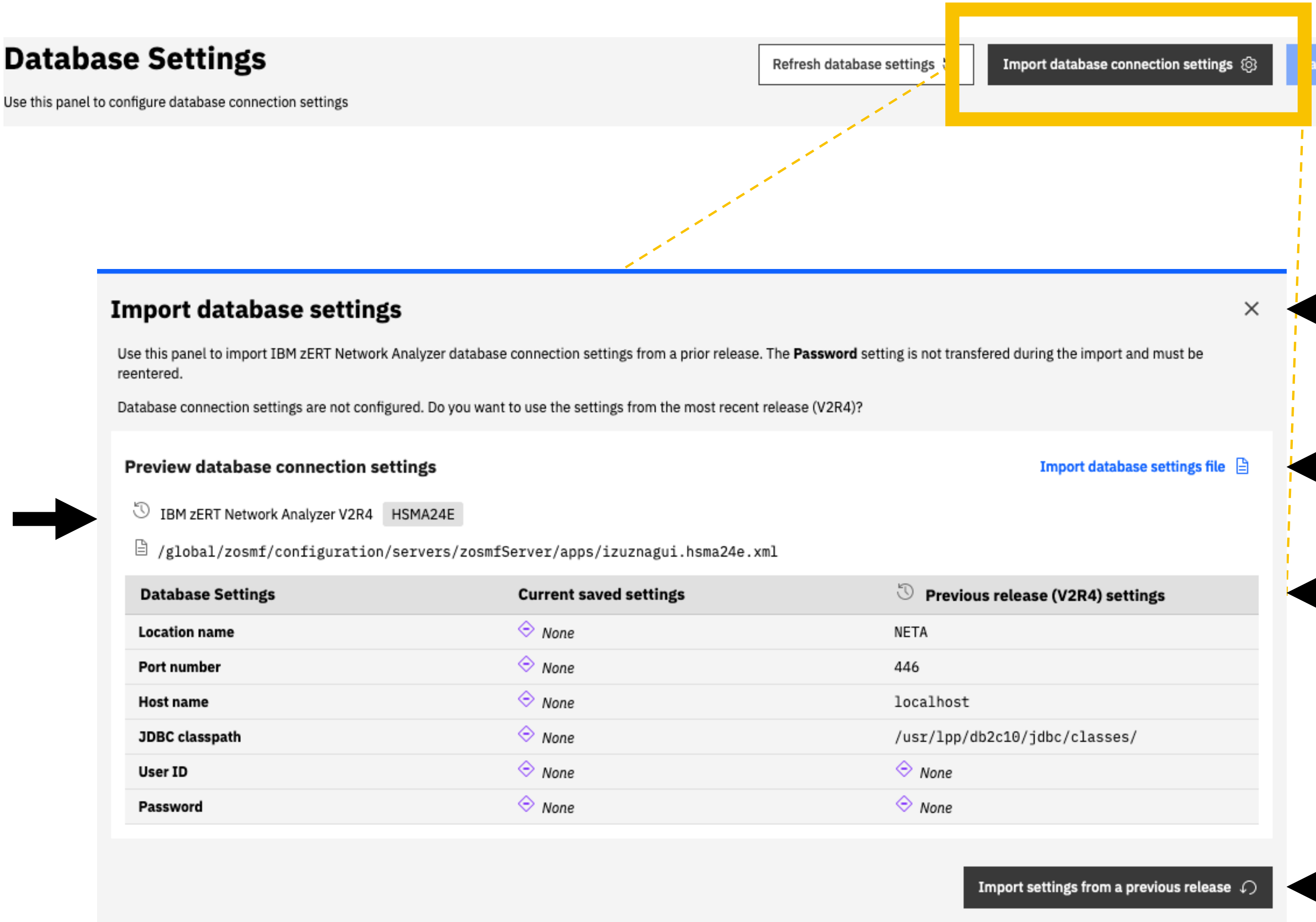
Required fields are denoted with an asterisk (*).

Host name *	localhost	**User ID** *	sysadm
Port number *	446	**Password** *	••••••••
Location name *	NETA		Clear User ID and Password
JDBC classpath *	/usr/lpp/db2c10/jdbc/classes/		

Usage & Invocation (9)

- **New:** “Import database connection settings” modal
  - *Settings* / *Database Settings* / **Import database connection settings**
  - A new modal appears on top of ***Database Settings*** panel (screenshot on next slide)
- If database (DB) settings are not configured, the panel will attempt to automatically locate a prior release DB connection settings within current z/OSMF file system.
  - Automatic search order: current release’s backup file (*n*), *n*-1, *n*-2
  - Alternatively, a DB connection settings file (`izuznagui.<fmid>.xml`) can be manually selected using a file widget. The file must be selected from a z/OS UNIX file path.
- Importing DB connection settings updates fields within *Database Settings* panel, requires clicking Save settings to apply.
  - Restriction: Database credentials are not copied over during the import
  - Restriction: In order to save and apply settings, new configuration must be different from current configuration.

Usage & Invocation (10)



Refresh database settings
Import database connection settings
ave settings
Import database settings file
Import settings from a previous release

Database Settings

Use this panel to configure database connection settings

Import database settings

Use this panel to import IBM zERT Network Analyzer database connection settings from a prior release. The **Password** setting is not transfered during the import and must be reentered.

Database connection settings are not configured. Do you want to use the settings from the most recent release (V2R4)?

Preview database connection settings

IBM zERT Network Analyzer V2R4 HSMA24E

/global/zosmf/configuration/servers/zosmfServer/apps/izuznagui.hsma24e.xml

Database Settings	Current saved settings	Previous release (V2R4) settings
Location name	*None*	NETA
Port number	*None*	446
Host name	*None*	localhost
JDBC classpath	*None*	/usr/lpp/db2c10/jdbc/classes/
User ID	*None*	*None*
Password	*None*	*None*

Release/FMID and path of database connection settings file

Close modal and cancel import

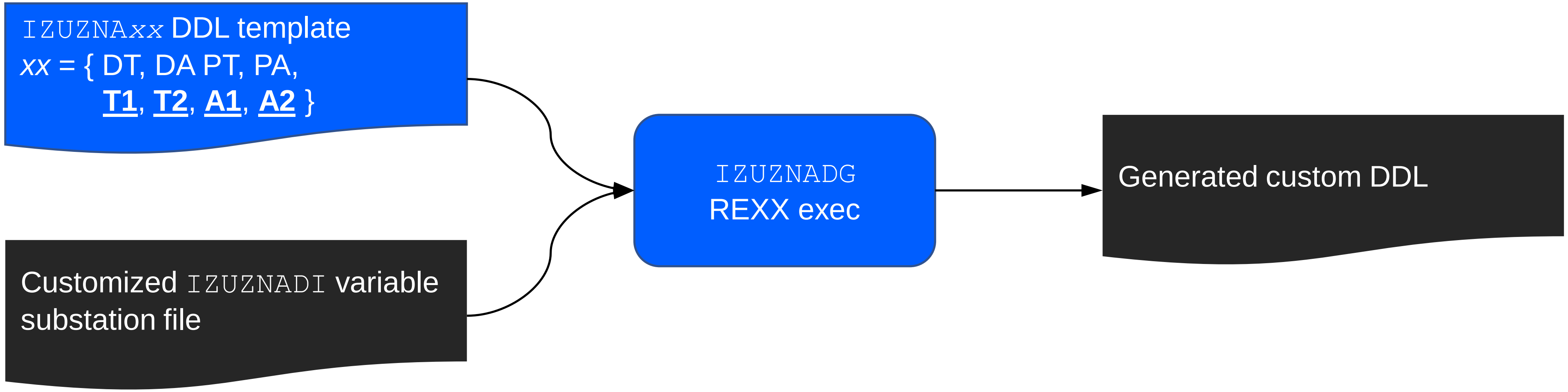
Opens z/OSMF file widget

Table comparing current and previous release settings

Button to update fields in Database Settings panel

Usage & Invocation (11)

- **New:** Schema generation tooling to support upgrading IBM zERT Network Analyzer to 3.1 from an existing database.
  - New DDL templates to support upgrades from back-level releases
    - `IZUZNA`**`T1`** – Upgrades fixed-schema template from V2R5 (*n*-1) to 3.1
    - `IZUZNA`**`T2`** – Upgrades fixed-schema template from V2R4 (*n*-2) to 3.1
    - `IZUZNA`**`A1`** – Upgrades aliased-schema template from V2R5 (*n*-1) to 3.1
    - `IZUZNA`**`A2`** – Upgrades aliased-schema template from V2R4 (*n*-2) to 3.1
  - Updated `IZUZNADG` REXX exec to produce DDL used to modify an existing zERT Network Analyzer database schema to the latest 3.1 schema version.



Usage & Invocation (12)

- The new templates will take an existing database at any PTF level and apply all changes to update the database to the latest level of the old release, then up to the latest 3.1 level.

- Examples
  - To generate DDL in a dataset named V25T120 that upgrades a fixed name V2R5 (n-1) database at schema version 1.2.0 to a 3.1 schema, issue the following:

    ```
    ex 'user1.izuznadg' 'IZUZNADI V25T120 IZUZNAT1 dbvers(1.2.0)’
    ```

  - To generate DDL in a dataset named V24A110 that upgrades an aliased V2R4 (n-2) database at schema version 1.1.0 to a 3.1 schema, issue the following:

    ```
    ex 'user1.izuznadg' 'IZUZNADI V24A110 IZUZNAA2 dbvers(1.1.0)'
    ```

Interactions & Dependencies

- Software Dependencies
  - Db2 for z/OS v11 or newer
    - IBM zERT Network Analyzer requires its own database
    - Consult with your database administrator
- Hardware Dependencies
  - No hardware dependencies
- Exploiters
  - No exploiters

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: **No**
- No upgrade and coexistence items to note

Installation & Configuration

- Please verify you met the requirements for running z/OSMF:
  - Correct IBM SDK for z/OS (Java) and WebSphere Liberty profile are applicable.
  - See “Software prerequisites for z/OSMF” for more information including browser requirements.
  - Enable the plugin by adding `ZERT_ANALYZER` to the `PLUGINS` statement in `IZUPRMxx`
  - See “Updating z/OS for the IBM zERT Network Analyzer plug-in” in IBM z/OS Management Facility Configuration Guide.

Diagnosis: General recommendations

- Recommended: z/OSMF diagnostic bundle (zip of `USER_DIR` file structure)
  - z/OSMF creates via the z/OSMF Diagnostic Assistant
  - File structure containing all z/OSMF and IBM zERT Network Analyzer logs in addition to some other configuration that may be valuable.

- Alternative: Manually collect the following set of documentation
  - IBM zERT Network Analyzer debug log (ensure log level is set to `FINEST`)
  - z/OSMF logs (`IZUG0.log`)
  - z/OSMF joblog (`IZUSVR1`)
  - Liberty logs (`messages.log`/`trace.log`)

Summary

- For z/OS 3.1, IBM zERT Network Analyzer introduces enhancements to streamline migration and address customer requirements with database connectivity.
  - Passphrases are now supported to authenticate with the IBM zERT Network Analyzer database
  - New function to clear saved database credentials
  - New function to import application and database connection settings from a previous release
  - New database schema upgrade tooling

Appendix

- Publications
  - IBM z/OS Management Facility Configuration Guide
    - **Updating z/OS for the IBM zERT Network Analyzer Plug-in**
    - IZUPRMxx reference information
- IBM zERT “all-in-one” page
  - http://ibm.biz/thingsaboutzert