z/OS 3.2 IBM Education Assistant

Solution Name: zERT Network Analyzer database-related enhancements

Solution Element(s): HSMA32E (IBM zERT Network Analyzer)

July 2025

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 z/OS 3.2, IBM zERT Network Analyzer addresses these customer requirements

Requirement 1: Support multiple database `COMMIT` points for IBM zERT Network Analyzer import operations.

- AS-IS: The SMF import design uses a single database `COMMIT` once all SMF records are successfully processed from a data set, placing a heavy Db2 for z/OS resource strain.

Requirement 2: Allow the IBM zERT Network Analyzer to use a non-default collection ID for the JDBC connection.

- AS-IS: The IBM zERT Network Analyzer requires the use of the Db2 for z/OS `NULLID` collection that must be configured with the `RELEASE(COMMIT)` and `KEEPDYNAMIC(NO)` options.

Overview (1)

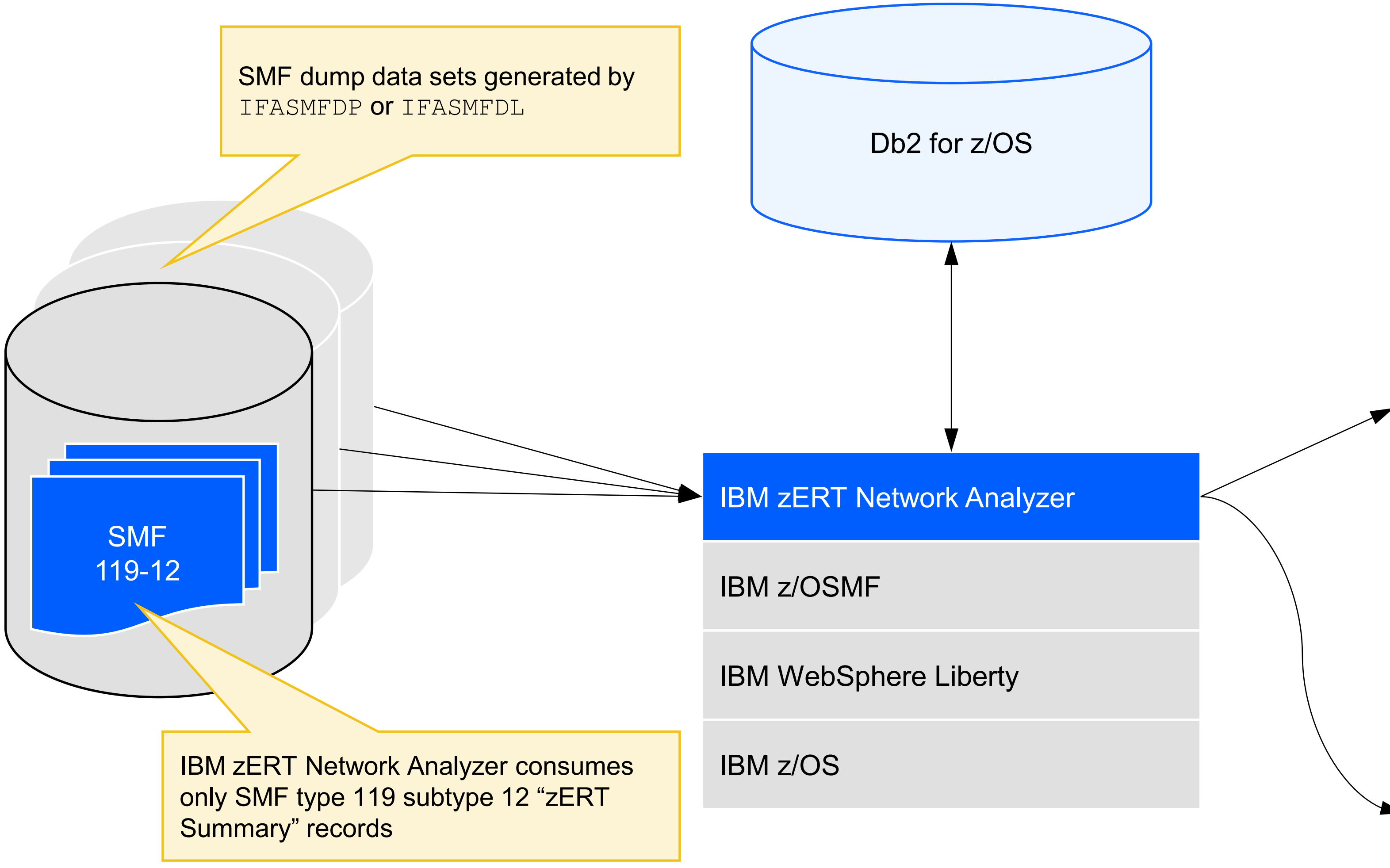
IBM zERT Network Analyzer

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

Overview (3)

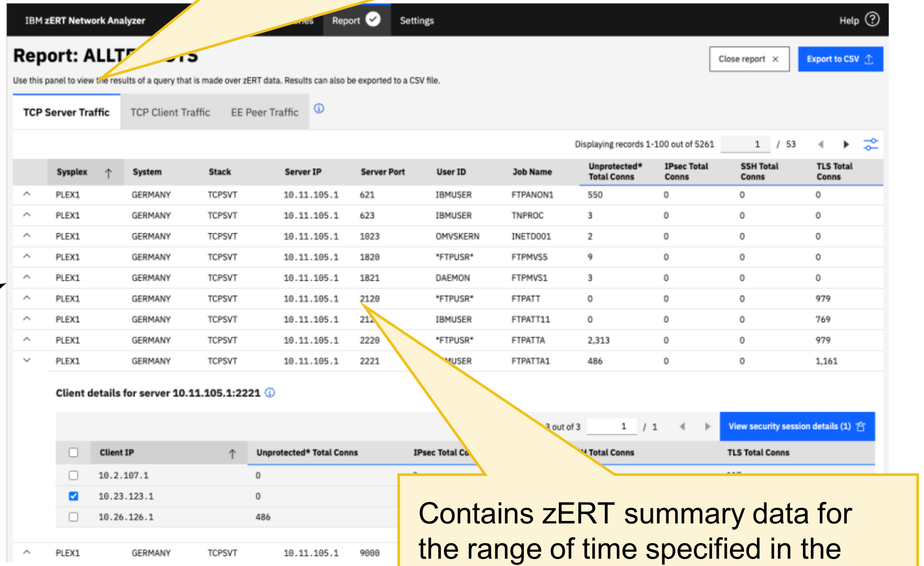


SMF dump data sets generated by `IFASMFDP` or `IFASMFDL`

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: ALLT

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	Total Conns	TLS Total Conns
□	10.2.107.1	0			
☑	10.23.123.1	0			
□	10.26.126.1	486			

	Sysplex	System	Stack	Server IP	Server Port
^	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)

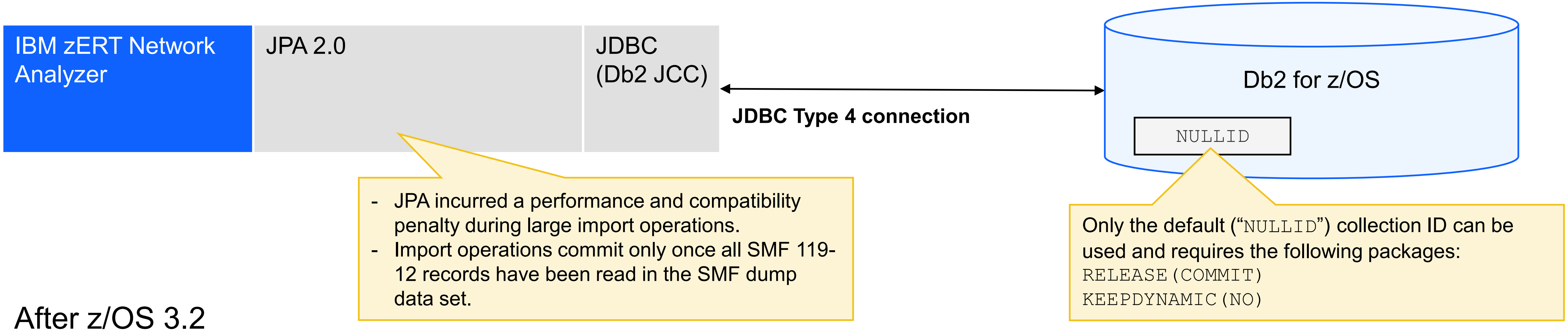
- Who
  - Users of IBM zERT Network Analyzer (z/OS network security administrators)
  - z/OSMF administrators
  - Db2 for z/OS database administrator (DBAs)
- What
  - IBM zERT Network Analyzer database-related enhancements
    - Configurable JDBC collection ID
    - Multiple commit points for import
- Wow
  - More flexibility to configure Db2 for z/OS environment for the IBM zERT Network Analyzer
  - Reduction of Db2 resource strain during intensive SMF data set import operations

Overview (5)

IBM zERT Network Analyzer database-related enhancements

Overview (6)

Before z/OS 3.2



IBM zERT Network Analyzer

JPA 2.0

JDBC (Db2 JCC)

JDBC Type 4 connection

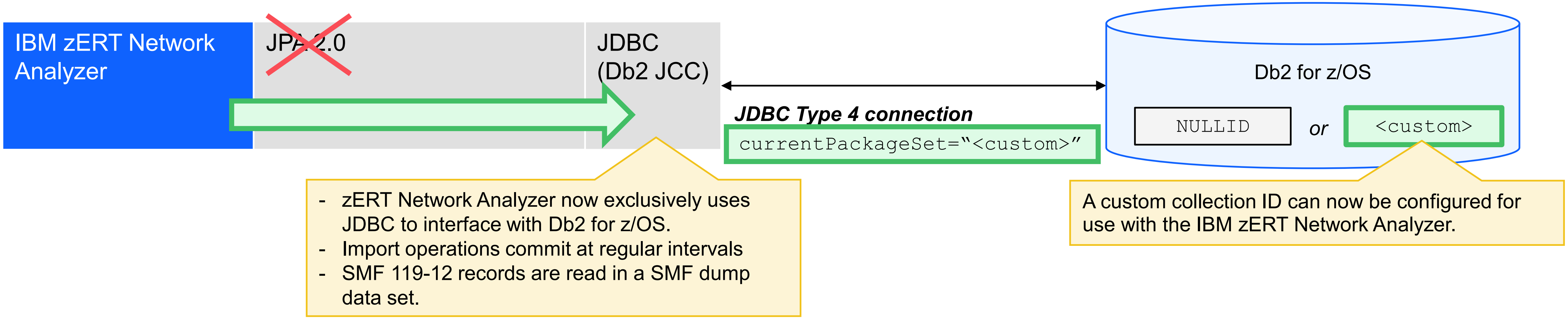
Db2 for z/OS

`NULLID`

- JPA incurred a performance and compatibility penalty during large import operations.
- Import operations commit only once all SMF 119-12 records have been read in the SMF dump data set.

Only the default (“`NULLID`”) collection ID can be used and requires the following packages:
`RELEASE(COMMIT)`
`KEEPDYNAMIC(NO)`

After z/OS 3.2



IBM zERT Network Analyzer

~~JPA 2.0~~

JDBC (Db2 JCC)

JDBC Type 4 connection

`currentPackageSet=“<custom>”`

Db2 for z/OS

`NULLID` *or* `<custom>`

- zERT Network Analyzer now exclusively uses JDBC to interface with Db2 for z/OS.
- Import operations commit at regular intervals
- SMF 119-12 records are read in a SMF dump data set.

A custom collection ID can now be configured for use with the IBM zERT Network Analyzer.

Usage & Invocation

- **New:** *Settings / Database Settings* panel updated with new **Collection ID** field
    - If no value is set, `NULLID` will be used

Collection ID NULLID

- **New:** If an invalid collection ID is used, a unique error message is returned.
    - IZUET0058E: Database current package set not accepted. Please re-enter and save your database settings.
- **New:** *Settings / Database Settings / Import Database Settings* modal is updated to support import of Collection ID field
    - If imported settings do not specify this value, `NULLID` will be preset as the value.
    - Importing database connection settings updates fields within *Database Settings* panel, requires clicking Save settings to apply.

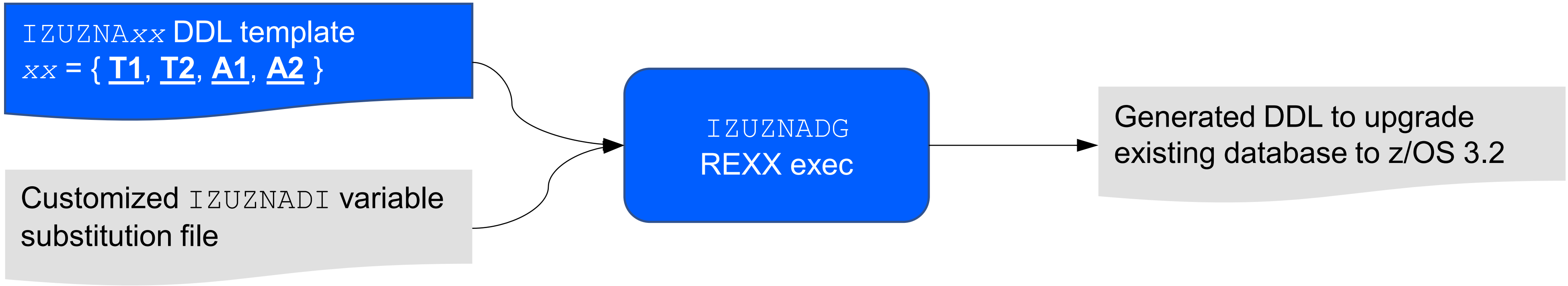
- **New:** Imports will commit at regular intervals when SMF 119-12 records are read
    - This is a transparent change in the import operation functionality
    - On an import failure, any committed records associated with the failed data set will be removed

Interactions & Dependencies

- Software Dependencies
  - Db2 for z/OS
    - IBM zERT Network Analyzer requires its own database (plug-in provides tooling to generate DDL)
    - Consult with your database administrator
- Hardware Dependencies
  - No hardware dependencies
- Exploiters
  - No exploiters

Upgrade & Coexistence Considerations (1)

- To exploit this solution, all systems in the Plex must be at the new z/OS level: **No**
- Upgrade action from previous release of IBM zERT Network Analyzer:
  - Use the schema generation tooling to upgrade an existing database to z/OS 3.2
  - Tooling provides DDL templates to upgrade old database:
    - `IZUZNA`**`T1`** – Upgrade DDL for fixed-schema database from 3.1 (*n*-1) to 3.2
    - `IZUZNA`**`T2`** – Upgrade DDL template for fixed-schema database from V2R5 (*n*-2) to 3.2
    - `IZUZNA`**`A1`** – Upgrade DDL template for aliased-schema database from 3.1 (*n*-1) to 3.2
    - `IZUZNA`**`A2`** – Upgrade DDL template for aliased-schema database from V2R5 (*n*-2) to 3.2
  - `IZUZNA`**`DI`**: Sample variable substitution file (provides values for each variable in the upgrade DDL 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` = { **T1**, **T2**, **A1**, **A2** }

Customized `IZUZNADI` variable substitution file

`IZUZNADG`
REXX exec

Generated DDL to upgrade existing database to z/OS 3.2

Upgrade & Coexistence Considerations (2)

- The upgrade 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 and then upgrade to the latest z/OS 3.2 level.

- Examples
  - To generate DDL in a dataset named `V31T120` that upgrades a fixed name IBM zERT Network Analyzer 3.1 (*n*-1) database at schema version 1.2.0 to a 3.2 schema, issue the following:

```
ex 'user1.izuznadg' 'IZUZNADI V31T120 IZUZNAT1 dbvers(1.2.0)’
```

  - To generate DDL in a dataset named `V25A110` that upgrades an aliased IBM zERT Network Analyzer V2R5 (*n*-2) database at schema version 1.1.0 to a 3.2 schema, issue the following:

```
ex 'user1.izuznadg' 'IZUZNADI V25A110 IZUZNAA2 dbvers(1.2.0)'
```

Installation & Configuration

- Please verify you’ve met the requirements for running z/OSMF:
  - See “*Software prerequisites for z/OSMF*” in IBM z/OS Management Facility Configuration Guide.
  - Enable the plugin
    - [Recommended] Enable the IBM zERT Network Analyzer plugin from the z/OSMF GUI (General Settings)
    - [Alternative] 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.
- If a custom Db2 collection is used, the following Db2 options must be set (Note: the plug-in does not enforce this configuration at runtime):
  - `RELEASE(COMMIT)`
  - `KEEPDYNAMIC(NO)`

Diagnosis: General recommendations

- Recommended: z/OSMF diagnostic bundle (zip of `USER_DIR` file structure)
  - z/OSMF creates this 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 3.2, IBM zERT Network Analyzer introduces database-related enhancements to address customer requirements for database connectivity and Db2 for z/OS resource usage during imports.
    - Configurable JDBC collection ID
    - Multiple commit points for import

Appendix

- Publications
  - IBM z/OS Management Facility Configuration Guide
    - **Updating z/OS for the IBM zERT Network Analyzer Plug-in**
    - **Db2 for z/OS customization for the IBM zERT Network Analyzer task**
    - IZUPRMxx reference information
- IBM zERT “all-in-one” page
  - http://ibm.biz/thingsaboutzert