Voting neue IBM Ideas

GSE Kassel 03/2023

Volkmar Langer, Dataport, Stand 15.3.2023

Hinweise vorweg…

Die auf den folgenden Seiten gezeigten Ideas stehen in Kassel zur Abstimmung (“high”, “medium” oder “low” Priority) an.

Falls ein Idea-Verfasser in Kassel seine Idea vor der Abstimmung kurz erläutern möchte, wird dafür Gelegenheit sein (bitte ganz kurz, max. 1-2 Minuten).

Unabhängig davon könnt Ihr natürlich GERNE auch direkt Votes für die Ideas abgeben. Dafür dann anmelden auf https://ideas.ibm.com

Links unten unter “My shared Groups” wechseln zu “GSE z/OS Germany”. Dort finden sich alle aufgeführten Ideas.

Alternativ gibt es auf den Folgeseiten in jedem Titel einen Direktlink zur beschriebenen Idea.

ZOS-I-3551 (high) (link)
zERT - Show a hint when zOSMF NCA will generate multiple policy agent rules

As there is no 1:n mapping from the zERT rules to the implementable policy, zERT will generate as many rules as required and append a suffix like ~1, ~2, ~n. However when coding those rules in the zOSMF NCA GUI there is not hint that the resulting policy will be created in a different way. Hence a warning message would be great in the GUI that makes a user aware that the coded zOSMF NCA zERT Rules will result in more than one entry in the policy agent rule that will be activated.

This is a follow up requirement from ZOS-I-3500 and defines only a subset of that requirement.

ZAUDIT-I-371 (?) (link)
zSecure Audit - Enhance Audit Trail data insert

When a RACF command fails to update a User, Group or any other profile in RACF an entry for this attempted and failed command is logged as expected in the Audit Trail.

This sample represents the removal of the password interval from a user that failed:

C4R739I Attrib: INTERV Removed on 22.252/07:53 by C2PSUSER CMD-RC=04

When this situation needs to be corrected, another password nointerval command is executed. As this has the same meaning of 'removal' the Audit Trail is not updated as zSecure Audit does not verify the return code from another command that should have removed the flag. This leads to inadequate data in the Audit Trail.

Hence zSecure Audit must be updated to not only check if another 'remove' item is already present in the Audit Trail but also check on the RC from the previous command and if the currently executed one has a lower RC it must overwrite the existing entry.

ZOS-I-3534 (high) (link)
zOSMF Network Analyzer allow cancellation

When having a big list of datasets being imported, it is not possible to cancel/stop a task. The only way to stop a task is to restart the full zOSMF instance which is very bad as other services rely on zOSMF. A full Server restart just because the option is not available to stop an import is very unhandy. Hence the option must be implemented to stop/cancel an import of a Dataset!

ZL1S-I-408 (medium) (link)
HMC with autoscaling windows in all 'screens'

Currently there is no HMC/SE internal alignment that windows do auto scale. As nowadays when working with large screens but the HMC window does not auto scale and works with fixed height of 30 lines, that's not very user-friendly. Hence all windows that are loaded in HMC/SE must support auto scale and do not work with fixed height anymore. As this is already in place for many windows there is still a lack of alignment within HMC overall.

ZOS-I-3497 (medium) (link)
zERT Report as well the timestamp

As all records that are loaded into zERT to analyze in the zOSMF Plugin do contain a timestamp, it must be possible to report on the time as requested here as well ZOS-I-3473 but additionally when running a report over few days or a single day, zERT must show the timestamp as when an improvement is implemented on day1 but days 1-4 are reported, it should be visible (on a timeline or similar) that on day 2,3,4 that record did not appear anymore.

ZL1S-I-407 (medium) (link)
Simplify Crypto Cipher Management in HMC

Currently HMC just offers a list (in a not auto scaling window) of available ciphers without any further details to which TLS version they might belong. It would be a great simplification if I can just select that I want to use TLS1.3 and TLS1.2 and then if required further narrow down the ciphers for only those two TLS versions and not go through the whole extensive list of all ciphers most probably not even applicable for the TLS versions I want to use.

Additionally: This feature must then be applicable for all TLS connections from the HMC hence it's then applicable for HTTPS traffic via Web-GUI, LDAPS as well as for OSA-ICC and the connection between HMC and SE.

This would be greatly aligned with IBM's target towards crypto agility.

ZOS-I-3473 (high) (link)
zERT - Time range scope filter

zERT Network Analyzer only offers the possibility to create queries for specific days or a daterange (scope filter). It would be very usefull to specify not only a daterange but also a timerange within a day. This is needed to analyze situations that occur within a specific timerange and makes analyzing a lot easier.

ZOS-I-3397 (high) (link)
zOSMF Network Analyzer must support SMF 119(11)

Currently zOSMF Network Analyzer does only support analyzing the zERT Discovery Records from SMF 119(12). However with the introduction of zERT Policy enforcement there must be the option to analyze the SMF 119(11) records too. It makes not sense to only support subtype 12 when both are closely related. Currently only users of zSecure Suite have a support out of the box option to analyze the records via zSecure EV.I panels. All other users must create their own SMF reports to analyze the behavior/results of the defined zERT Policy Enforcement. It would be a huge win for all customers using zERT Policy enforcement when zOSMF Network Analyzer supports as well SMF 119(11) record analysis!

ZOS-I-3407 (high) (link)
Use of PROTECTED userid on zERT access to DB2
→ZOS-I-504 (medium) (link) zERT plugin to use Certificate for Authentication

Currently in the DB settings panel of the zERT it is necessary to specify the user and password with which the zERT will access DB2

In order to avoid conflicts of password, expiration of the same by security policies, ... we would like to be able to use a user with the attribute PROTECTED (and therefore without password) to access the DB2

ZOS-I-3400 (high) (link)
Reuse of address groups in zOSMF Configuration Assistant

As more and more policies can be managed by zOSMF Configuration Assistant it would be very beneficial if the address groups can be re-used in the policies to:

- Speed up creation of new Policies
- Prevent duplication of data
- Simplify Management of addresses applying to all policies

ZOS-I-3384 (medium) (link)
Provide more granularity for control access to different paths under /global/zosmf

There is a need to distinguish between zOSMF ADMIN GROUP (IZUADMIN) and the USS OWNER GROUP of z/OSMF's USER_DIR path.

Users defined in the z/OSMF administrator's group (IZUADMIN) should NOT necessarily have access to all the USS directories under /global/zosmf.

ZOS-I-3346 (high) (link)
Software installation: Dataset restore w/o CB.** RACF dataset profile

Today, the use of z/OSMF software management for the installation of z/OS requires, that CB.** RACF data set profiles are defined. Our RACF rules only allow RACF userids with corresponding dataset profiles that are actively used. For a successful z/OS installation, we suggest the following ways to circumvent this issue: 1.) Use of ADRDSSUwith addition parameter ADMINISTRATOR 2.) Similar to CPAC dialogue: ALLOCATE zFS, MOUNT zFS, UNIX PAX

ZALERT-I-128 (?) (link)
Use sysplex wide SMF logstream as input to zSecure Alert

As a user of sysplex technologie (e.g. VTAM generic ressources) in our environments, we see that the functionality of some alerts is limited, if zAlert only analyzes data of one single lpar.

The biggest problem we see is in standard alert 1125 (Password spraying attack). It does only work, if the record 119 of telnet and 80 of the password violations occur on the same lpar. But one of the basic ideas of parallel sysplex is, that the user is automatically routed to one lpar of the sysplex.

Also other alerts (e.g. 1124 Logon from a not allowed IP address) can only work if all SMF records are produced on the same lpar.

ZL1S-I-394 (high) (link)
add TLS1.3 to OSA-ICC

In OSA-ICC we know that in the panel configuration option when you edit server configuration, when you check the TLS version it only goes to TLS 1.2. We have a requirement to go to TLS 1.3 or above

JSDK4Z-I-22 (high) (link)
Add support for HWIREST to JZOS

BCPii is an important z/OS specific API that currently supports several languages but NOT Java. Having this support within JZOS would make java applications relying on HWI communications (such as monitoring applications or system automation tasks) independent of complex multi-tier solutions.

ZOS-I-2855 (medium) (link)
Define KEYRING_OWNER in PARMLIB instead of local_override.cfg

If you use a shared KeyRing (one certificate for all services on one LPAR) you have currently to alter /global/zosmf/configuration/local_override.cfg inserting a line "KEYRING_OWNER_USERID=certOwnerID"
The KEYRING_NAME is configured in IZUPRM00.
This seems strange.