z/OS 3.1 IBM Education Assistant

Solution Name: Update security configuration REST API and One click to fix missing security authorizations in SCA

Solution Element(s): z/OSMF Security Configuration Assistant

July 2023

Agenda

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

Trademarks

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

Objectives

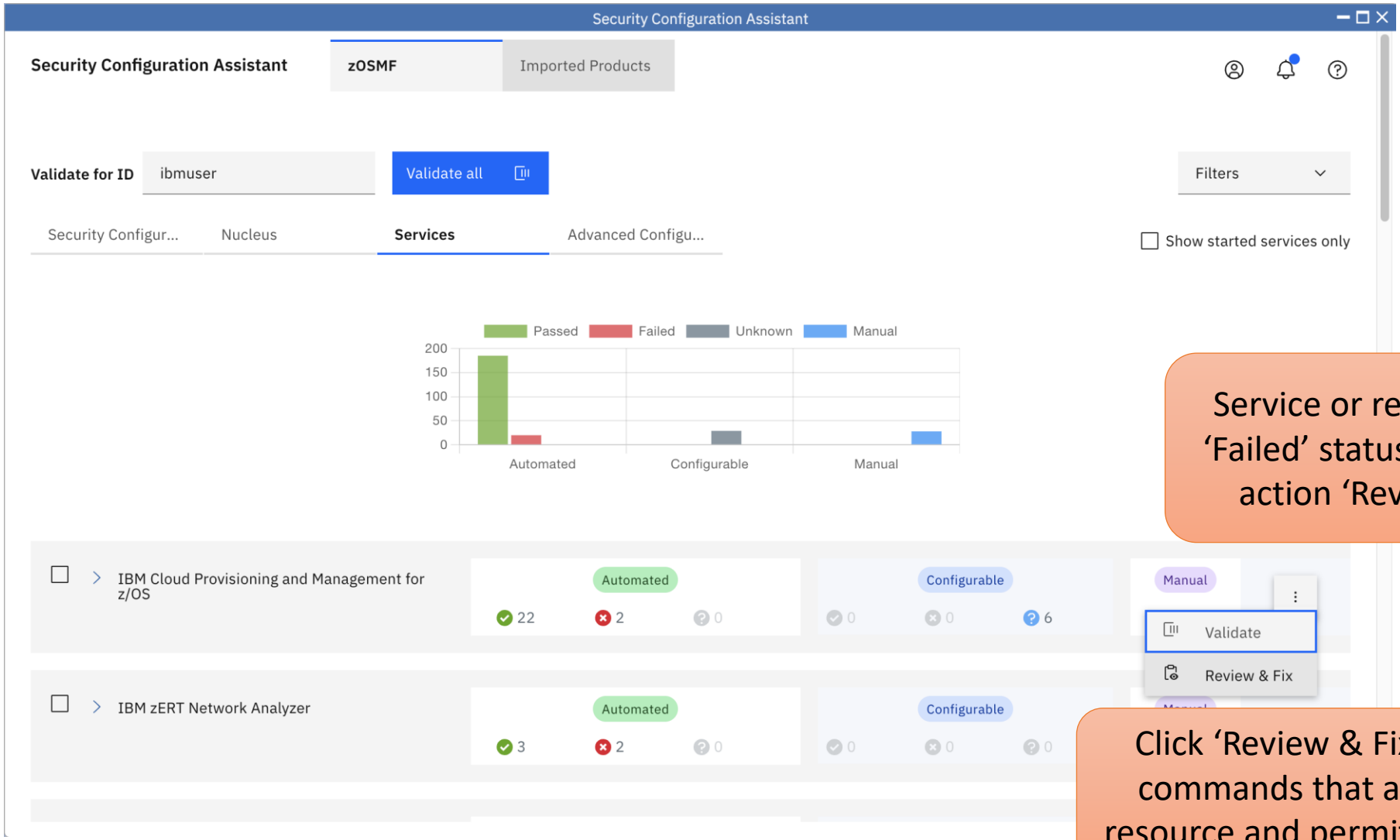
- SCA provides REST APIs for system programmer to call to provision security resources with required access for specified ID.
- *At current stage, new REST API do not support variables in security resources in JSON.*
- UI of SCA provides ways to fix missing security authorization.

Overview

- Who (Audience)
  - system programmer
- What (Solution)
  - REST APIs to provision security resources with required access.
  - SCA UI provides action to fix failure of security resource validation.
- Wow (Benefit / Value, Need Addressed)
  - Provision security authorization by programming (e.g. Ansible) without z/OSMF UI.
  - One-click to fix missing security authorization from UI of z/OSMF SCA.

Usage & Invocation

- Screenshot of UI changes

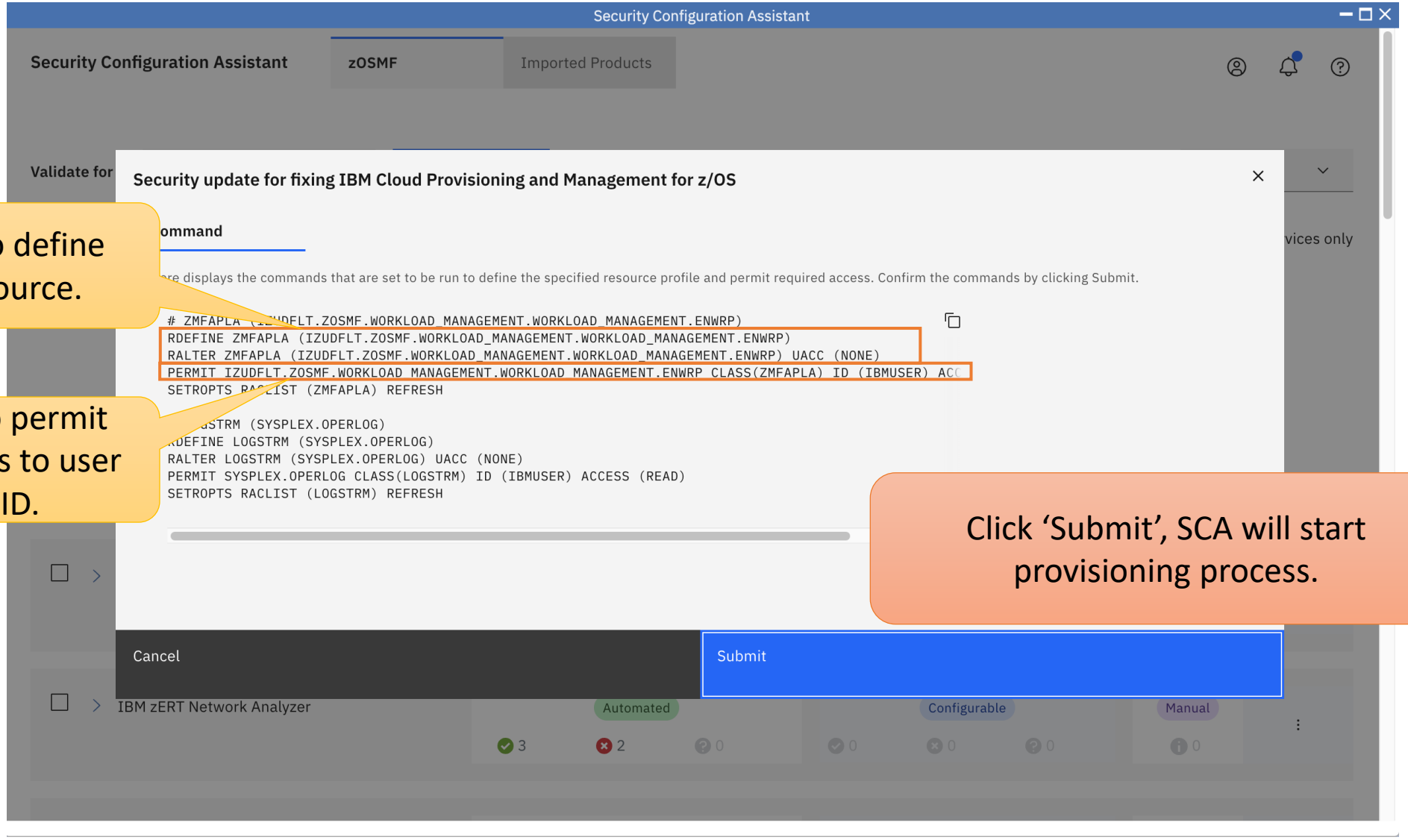


Service or resource with ‘Failed’ status have a new action ‘Review & Fix’

Click ‘Review & Fix’ to review the commands that are set to define resource and permit required access.

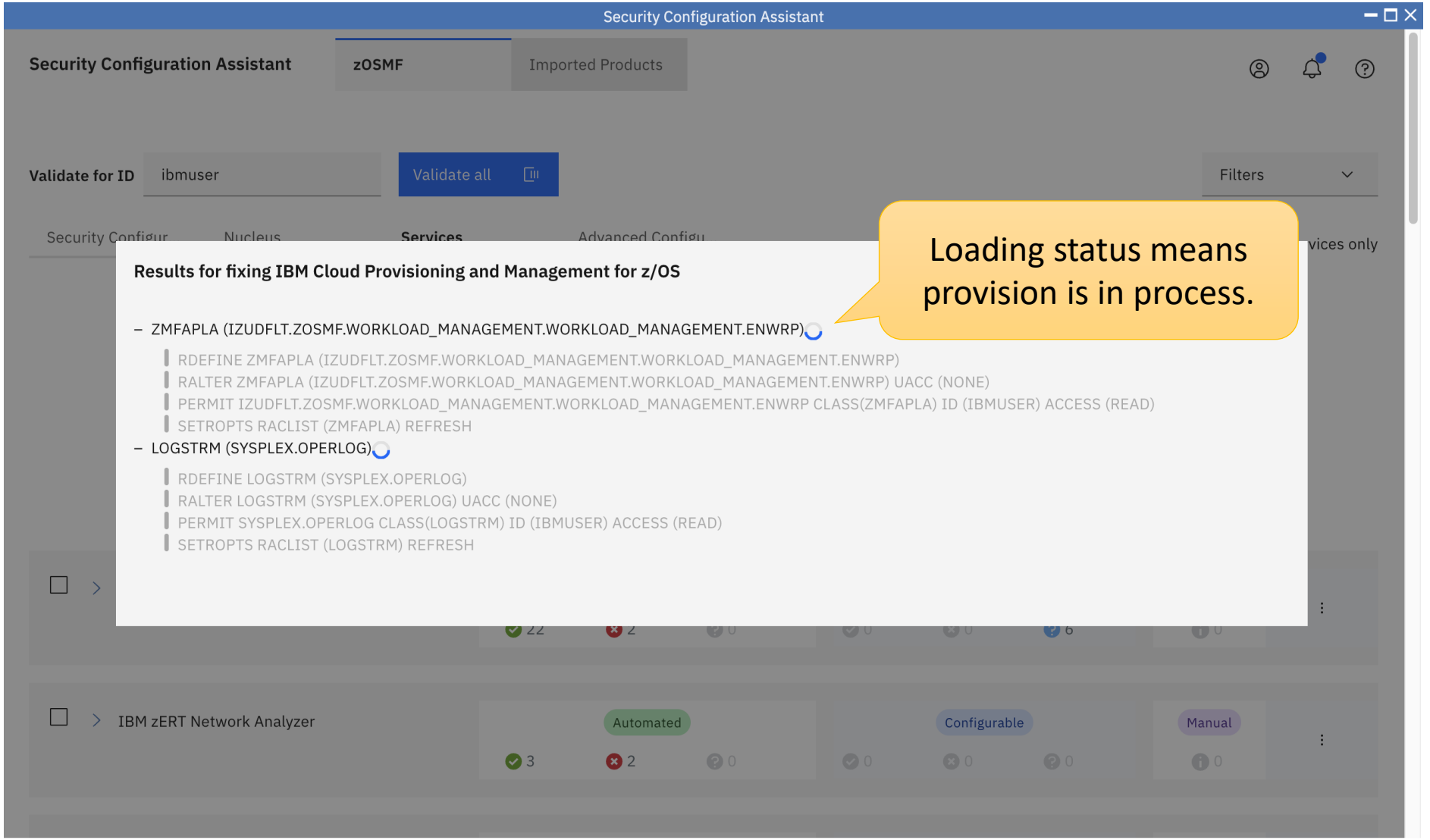
Usage & Invocation

- Screenshot of UI changes



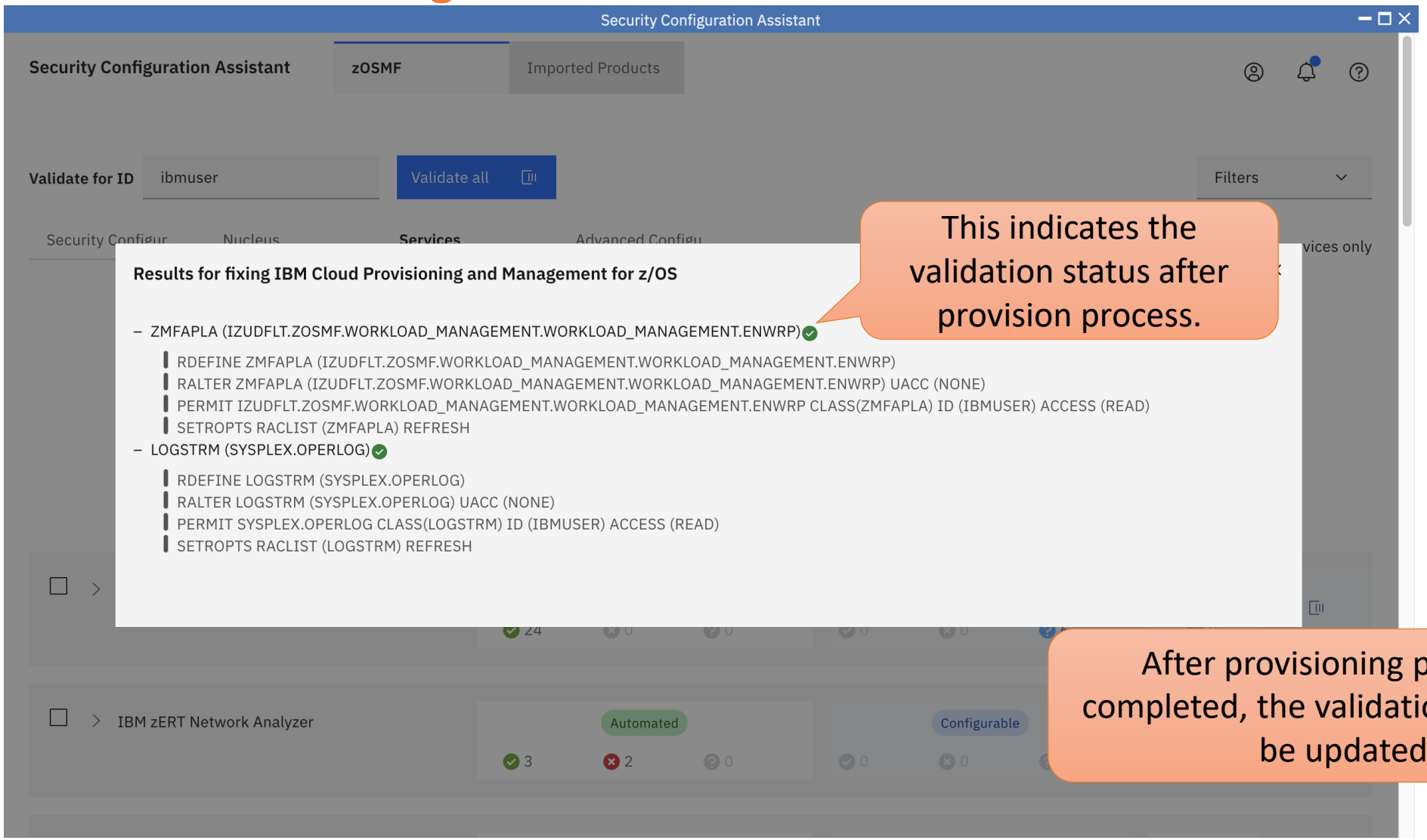
Usage & Invocation

- Screenshot of UI changes



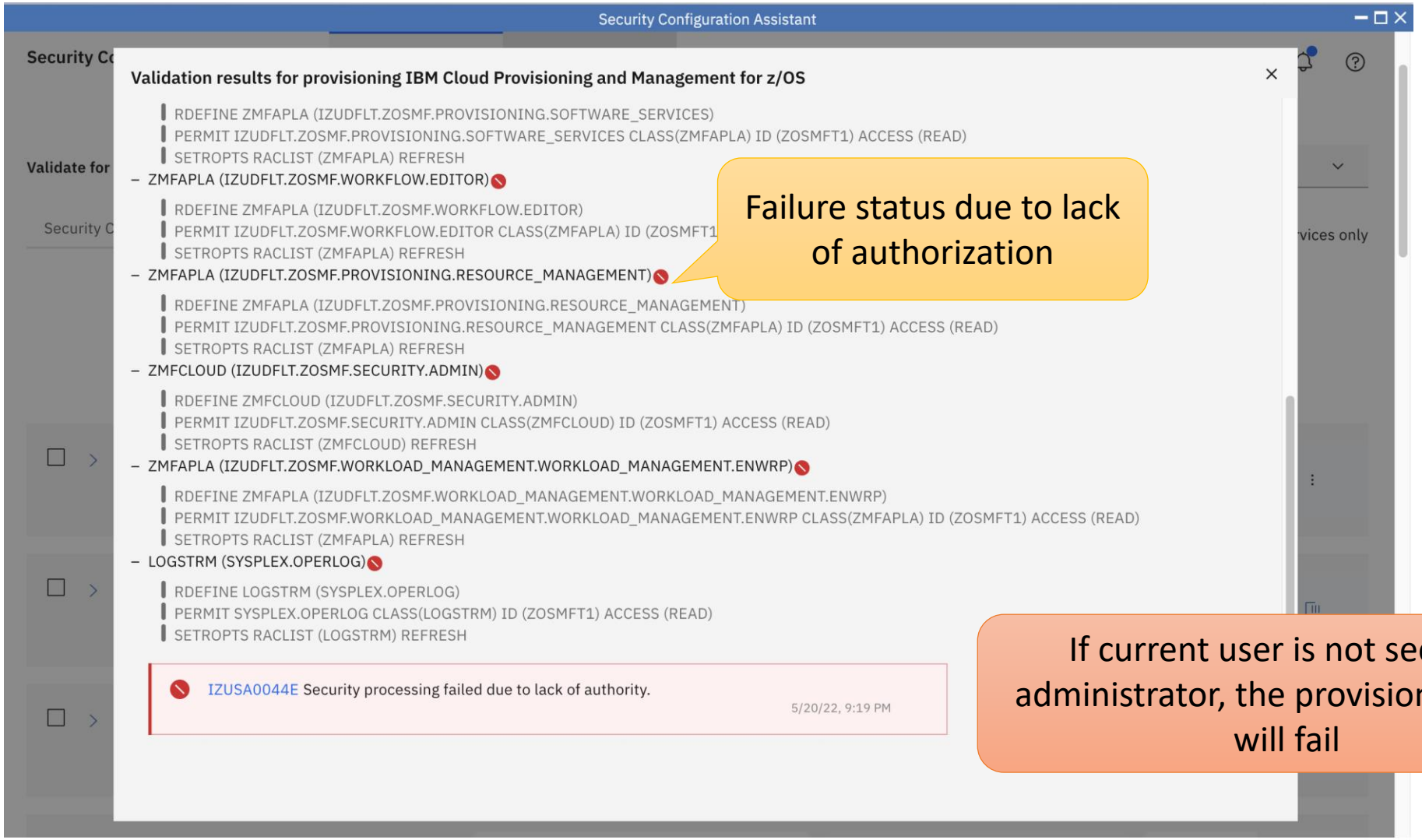
Usage & Invocation

- Screenshot of UI changes



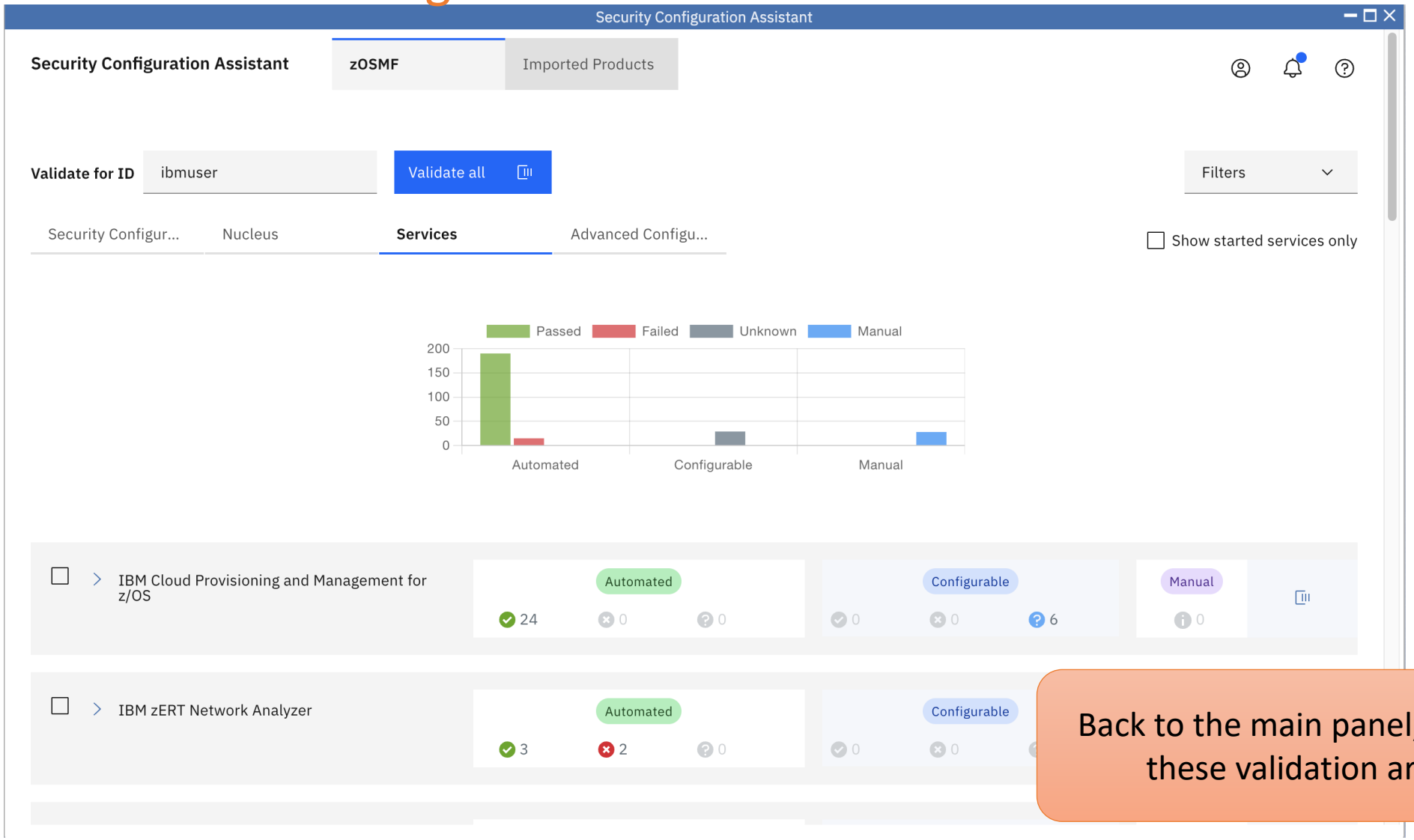
Usage & Invocation

- Screenshot of UI changes



Usage & Invocation

- Screenshot of UI changes



Usage & Invocation

- API: Provision resources specified in post body

POST */zosmf/config/security/v1/provision?userid={userid}*

Query parameter

Query Parameter	Required	Description
userid	no	User ID or group ID to be validated for the security resources specified in the request body. If the ID is not specified, the current logon user ID will be used to validate for the security resources in request body.

Request body

Json Request Body	Required	Description
object		
serviceId string alias ServiceId	no	Service ID
serviceName string alias ServiceName	no	Servcie name
version number alias MetaValidationItemVersion	no	version
vendor string alias Vendor	no	Vendor name
resourceItems object[ ] alias SecurityValidationItems	yes	Array of security resources to be validated for the specified user ID
itemId string alias ItemID alias ItemId	no	Item ID

Usage & Invocation

Json Request Body	Required	Description
itemType string alias ItemType	no	Item type More details: ○ If value not specified for this property, current resource will be used for validation. ○ If value specified for this property, in further versions, resource with any value other than 'PROGRAMMABLE' for this property will be ignored and be not used for validation. And the resource will not appear in the response list of the validated resources. So far, at current version, the value will not be validated.
itemCategory string alias ItemCategory	no	Item category
itemDescription string alias ItemDescription	no	Item description
whoNeedsAccess string alias WhoNeedsAccess	no	Users (security groups) who require access to this resource. The Security Configuration Assistant does not verify that security groups are defined; your security administrator must verify that the groups exist.

Usage & Invocation

Json Request Body	Required	Description
resourceProfile string alias ResourceProfile	yes	Name of security resource profile. At current stage, ○ Variable in the name is not supported. ○ Generic resource name is not supported.
resourceClass. string alias ResourceClass	yes	SAF resource class
access string alias LevelOfAccessRequired	yes	Level of access that is required to the security resource for the specified user ID or group ID. Value can be set with the following: ○ READ ○ UPDATE ○ CONTROL ○ ALTER
whoNeedsAccess string alias WhoNeedsAccess	no	Users (security groups) who require access to this resource. The Security Configuration Assistant does not verify that security groups are defined; your security administrator must verify that the groups exist.

Usage & Invocation

Response json

Json Response		Required	Description
object			
serviceId	string	no	Service ID
serviceName	string	no	Servcie name
version	number	no	version
vendor	string	no	Vendor name
resourceItems	object[ ]	yes	Array of security resources validated for the specified user ID
itemId	string	no	Item ID
itemType	string	no	Item type
itemCategory	string	no	Item category
itemDescription	string	no	Item description
resourceProfile	string	yes	Name of security resource profile. At current stage, ○ Variable in the name is not supported. ○ Generic resource name is not supported.
resourceClass	string	yes	SAF resource class
access	string	yes	Level of access that is required to the security resource for the specified user ID or group ID. Value can be the following: ○ READ ○ UPDATE ○ CONTROL ○ ALTER
action	string	yes	For validate action, the return value will be “validate”.

Usage & Invocation

Json Request Body		Required	Description
objectId	string	yes	the object ID of this action. For provision action, this ID is whom the required access is permitted to. This field can also be used for other action in further versions.
validatedId	string	yes	User ID or group ID that is used to validate for the resource
status	string	yes	Validation result Value can be the following: ○ Passed ○ Failed ○ Unknown
additionalInfo	string	no	Additional info
whoNeedsAccess	string	no	Users (security groups) who require access to this resource. The Security Configuration Assistant does not verify that security groups are defined; your security administrator must verify that the groups exist.
messageId	string	no	Message Id
messageText	string	no	Message text
httpStatus	integer	no	http status code if error
requestMethod	string	no	http request method if error
requestUri	string	no	Request uri if error

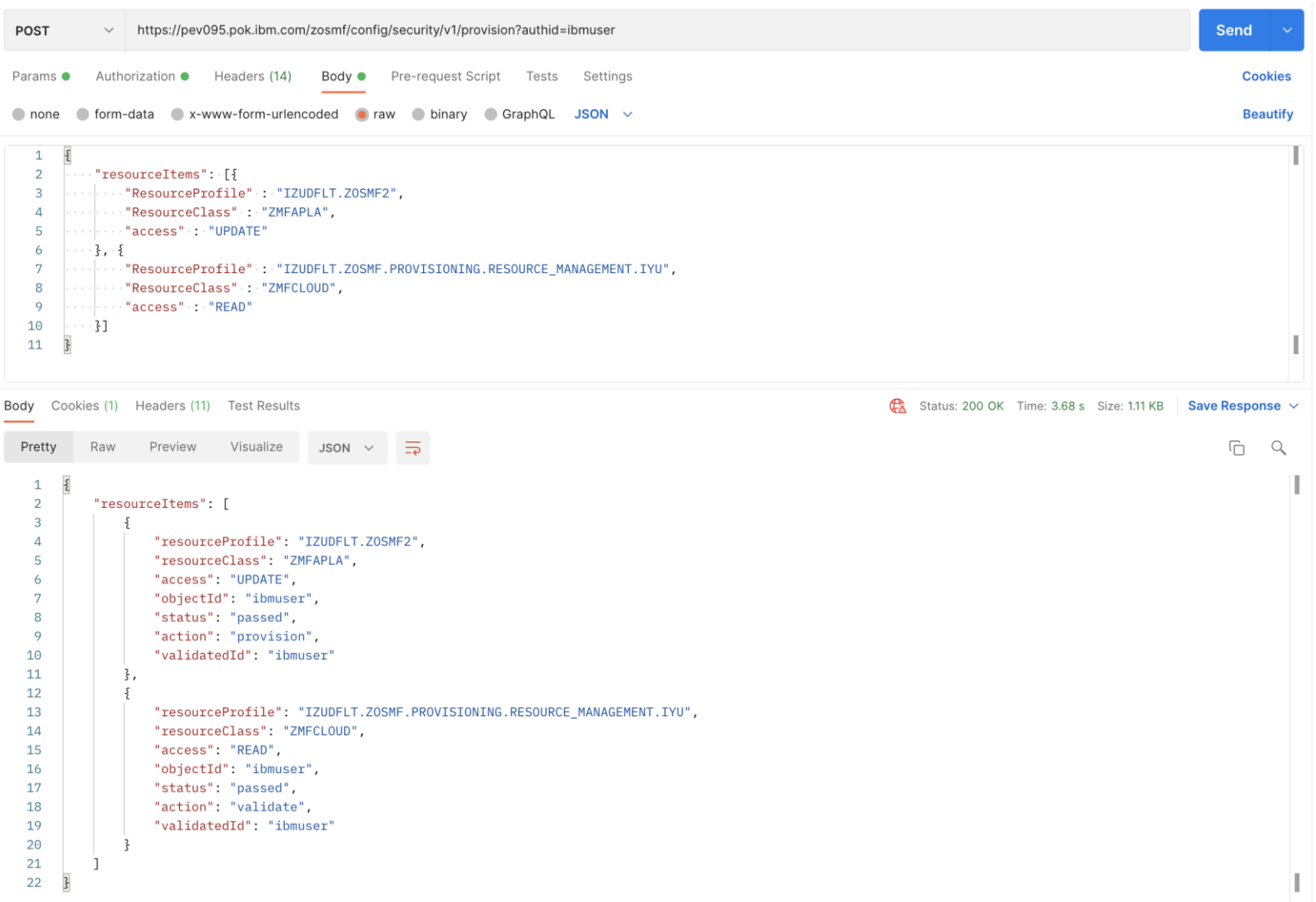
Usage & Invocation

Response code

Response Code	Description
200 OK	
400 Bad Request	Parameter error or missing
403 Forbidden	User is not logged on, or is not allowed to access z/OSMF Security Configuration Assistant
500 Internal Server Error	Internal Server Error

Mainline

- Provision API example



Usage & Invocation

- API: Provision resources specified in a json file

POST */zosmf/config/security/v1/provision/*descriptor*?userid={userid}*

Query parameter

Query Parameter	Required	Description
userid	no	User ID or group ID to be validated for the security resources specified in the request body. If the ID is not specified, the current logon user ID will be used to validate for the security resources in request body.

Request body

Json Request Body	Required	Description
object		
path string	yes	Absolute path of the existing security descriptor JSON file which contains resources to be validated against the id specified as the query parameter Current logged-on user ID will be used to read the specified JSON file. If current logged-on user has no access to the JSON file, an error will be return.

Usage & Invocation

JSON file content

Json Security Descriptor Content	Required	Description
object		
serviceId string alias ServiceId	no	Service ID
serviceName string alias ServiceName	no	Servcie name
version number alias MetaValidationItemVersion	no	version
vendor string alias Vendor	no	Vendor name
resourceItems object[ ] alias SecurityValidationItems	yes	Array of security resources to be validated for the specified user ID
itemId string alias ItemID alias ItemId	no	Item ID

Usage & Invocation

Json Request Body	Required	Description
itemType string alias ItemType	no	Item type More details: ○ If value not specified for this property, current resource will be used for validation. ○ If value specified for this property, in further versions, resource with any value other than 'PROGRAMMABLE' for this property will be ignored and be not used for validation. And the resource will not appear in the response list of the validated resources. So far, at current version, the value will not be validated.
itemCategory string alias ItemCategory	no	Item category
itemDescription string alias ItemDescription	no	Item description
whoNeedsAccess string alias WhoNeedsAccess	no	Users (security groups) who require access to this resource. The Security Configuration Assistant does not verify that security groups are defined; your security administrator must verify that the groups exist.

Usage & Invocation

Json Request Body	Required	Description
resourceProfile string alias ResourceProfile	yes	Name of security resource profile. At current stage, ○ Variable in the name is not supported. ○ Generic resource name is not supported.
resourceClass. string alias ResourceClass	yes	SAF resource class
access string alias LevelOfAccessRequired	yes	Level of access that is required to the security resource for the specified user ID or group ID. Value can be set with the following: ○ READ ○ UPDATE ○ CONTROL ○ ALTER
whoNeedsAccess string alias WhoNeedsAccess	no	Users (security groups) who require access to this resource. The Security Configuration Assistant does not verify that security groups are defined; your security administrator must verify that the groups exist.

Usage & Invocation

Response json

Json Response		Required	Description
object			
serviceId	string	no	Service ID
serviceName	string	no	Servcie name
version	number	no	version
vendor	string	no	Vendor name
resourceItems	object[ ]	yes	Array of security resources validated for the specified user ID
itemId	string	no	Item ID
itemType	string	no	Item type
itemCategory	string	no	Item category
itemDescription	string	no	Item description
resourceProfile	string	yes	Name of security resource profile. At current stage, ○ Variable in the name is not supported. ○ Generic resource name is not supported.
resourceClass	string	yes	SAF resource class
access	string	yes	Level of access that is required to the security resource for the specified user ID or group ID. Value can be the following: ○ READ ○ UPDATE ○ CONTROL ○ ALTER
action	string	yes	For validate action, the return value will be “validate”.

Usage & Invocation

Json Request Body		Required	Description
objectId	string	yes	the object ID of this action. For provision action, this ID is whom the required access is permitted to. This field can also be used for other action in further versions.
validatedId	string	yes	User ID or group ID that is used to validate for the resource
status	string	yes	Validation result Value can be the following: ○ Passed ○ Failed ○ Unknown
additionalInfo	string	no	Additional info
whoNeedsAccess	string	no	Users (security groups) who require access to this resource. The Security Configuration Assistant does not verify that security groups are defined; your security administrator must verify that the groups exist.
messageId	string	no	Message Id
messageText	string	no	Message text
httpStatus	integer	no	http status code if error
requestMethod	string	no	http request method if error
requestUri	string	no	Request uri if error

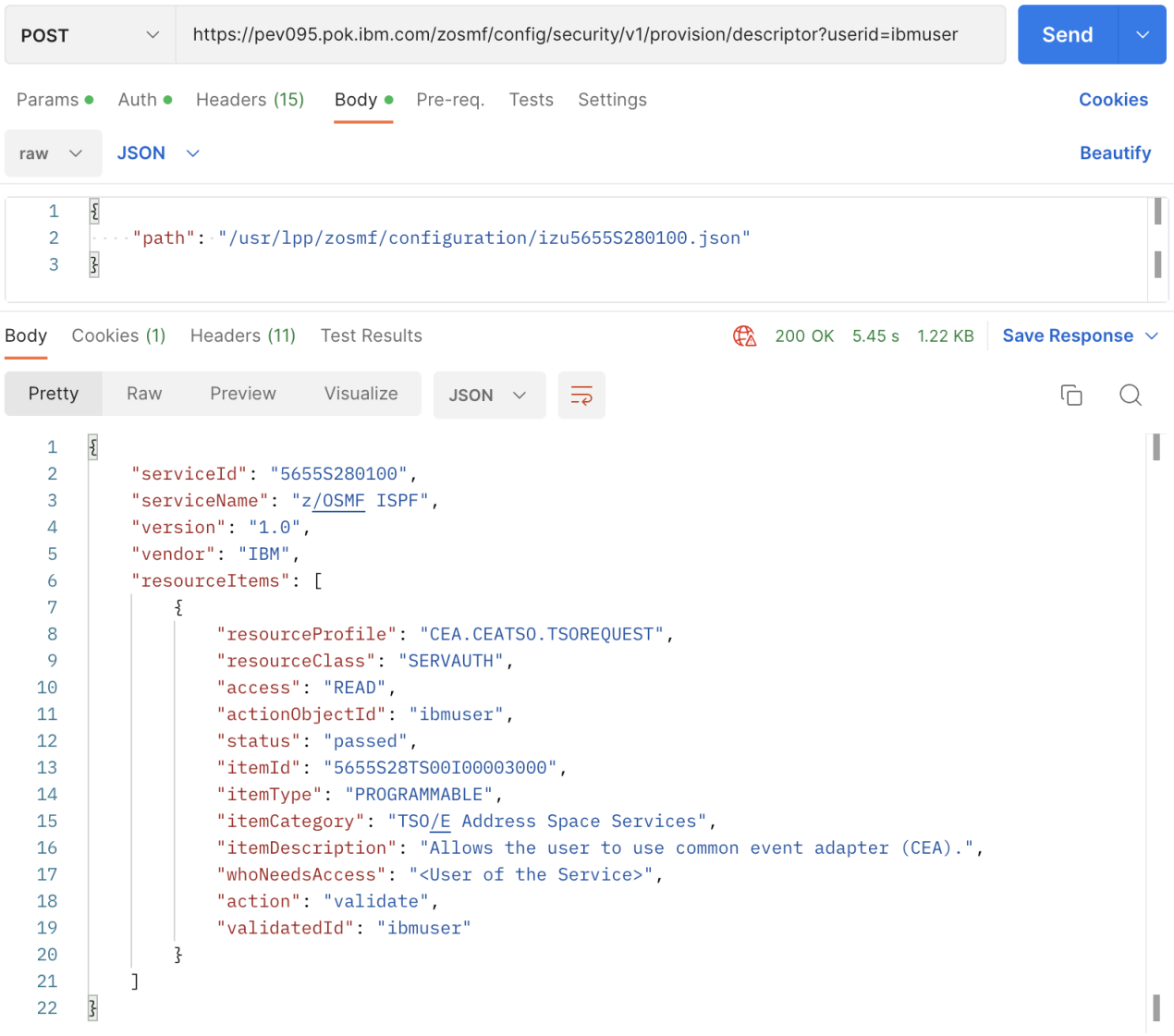
Usage & Invocation

Response code

Response Code	Description
200 OK	
400 Bad Request	Parameter error or missing
403 Forbidden	User is not logged on, or is not allowed to access z/OSMF Security Configuration Assistant
500 Internal Server Error	Internal Server Error

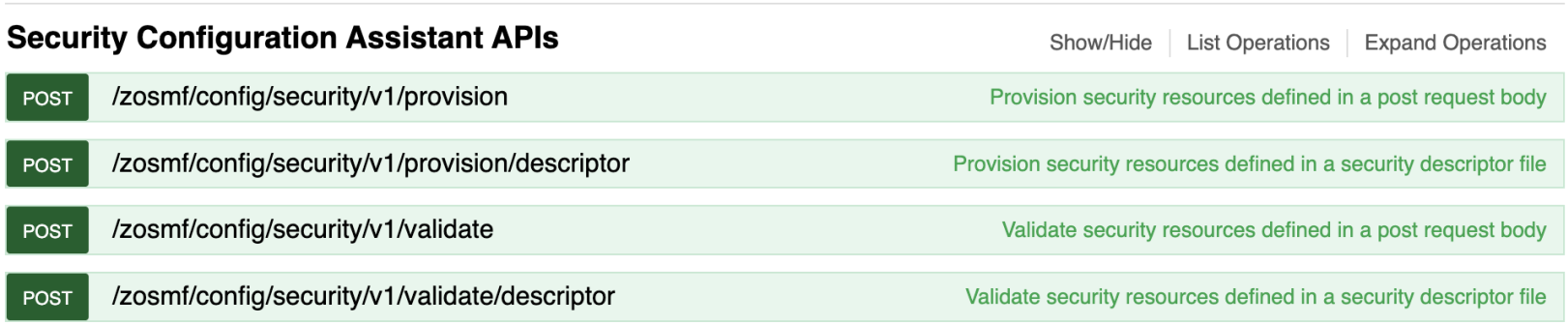
Usage & Invocation

- Provision API example



Usage & Invocation

- Reference on z/OSMF Swagger UI



Interactions & Dependencies

- Software Dependencies
  - No
- Hardware Dependencies
  - No
- Exploiters
  - System programmer
  - Security administrator

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: *No*
- List any toleration/coexistence APARs/PTFs. *PH47746*.
- List anything that doesn't work the same anymore. *None*.
- Upgrade involves only those actions required to make the new system behave as the old one did.
- Coexistence applies to lower level systems which coexist (share resources) with latest z/OS systems.

Installation & Configuration

- List anything that a client needs to be aware of during installation and include **examples** where appropriate - clients appreciate these:
  - Are any APARs or PTFs needed for enablement? *No*
  - What jobs need to be run? *No*
  - What hardware configuration is required? *No*
  - What PARMLIB statements or members are needed? *No*
  - Are any other system programmer procedures required? *No*
  - Are there any planning considerations? *No*
  - Are any special web deliverables needed? *No*
  - Does installation change any system defaults? *No*

Summary

- SCA provision REST APIs is convenient for system programmer to call to provision security resources by programming (e.g. ansible) without z/OSMF UI.
- The security resources to be provisioned in REST APIs can be defined in a post body or a JSON file in a format of JSON.
- Guide to use provision REST APIs can be found in z/OSMF Swagger UI or z/OSMF programming guide.
- One-click fix is provided in z/OSMF SCA UI to fix any security resources with validation failure.

Appendix

- IBM z/OS Management Facility Programming Guide(SC27-8420-50)
- IBM z/OS Management Facility Configuration Guide(SC27-8419-50)
- IBM z/OS Management Facility Online Help