Swiss Re

Access Elevation

Marco Egli, October 2023

Table of Contents

Rational for Access Elevation

- Reduce Timeframe where user has highest privileges
- Automated Reporting over high privileged groups
- Remove high access for software installation in Production as only needed in Maintenance

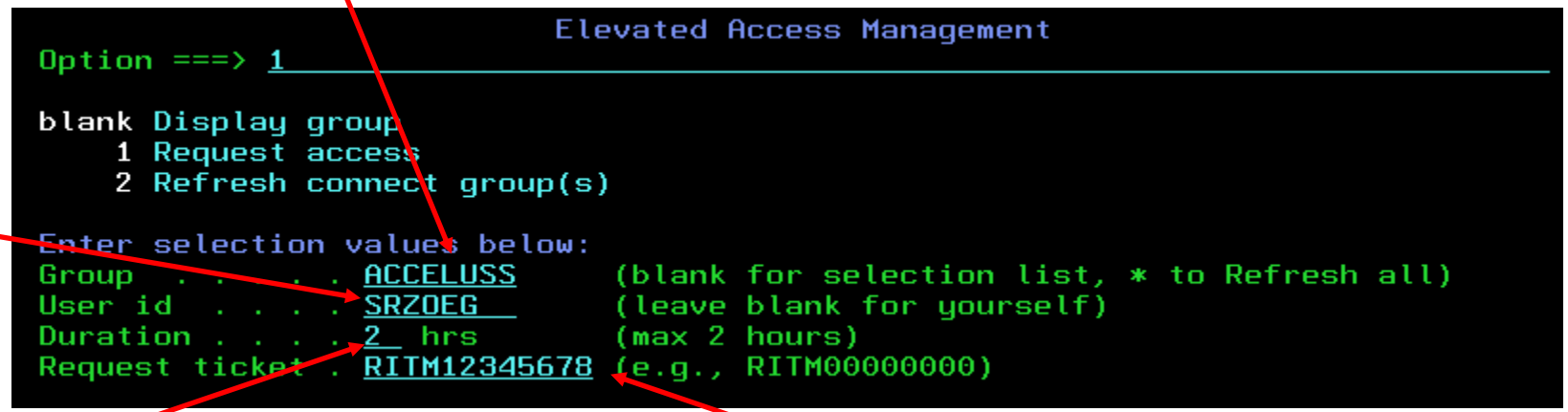
Elevated Access Management

- ISPF based
- Maximum elevation time is 2 hours
- RITM number required for elevation
- Automatic removal process every hour
- Per RACF environment (according to RRSF synch setup)

Elevated Access Management – ISPF application – request access

If this field is empty when one hits enter, if offers a list of available groups for elevation.

If this field is empty your userid will be used by default.



Maximum duration for the elevation is 2 hours.

RITM number must be provided as evidence that the elevation is used for a tasks that requires that elevated access.

Elevated Access Management – ISPF application – show current elevations

Add a group name or select one when the group name is empty.

```
                          Elevated Access Management
Option ===> ____________________________________________________________________

blank Display group
    1 Request access
    2 Refresh connect group(s)

Enter selection values below:
Group  . . . . . ACCELUSS     (blank for selection list, * to Refresh all)
User id  . . . . ________     (leave blank for yourself)
Duration . . . . __ hrs       (max 2 hours)
Request ticket . ____________ (e.g., RITM00000000)
```

Confirmation by hitting enter shows all current active elevations.

Displays the list of all current elevated users from the selected group.

```
                          Elevated Access Management
Option ===> ____________________________________________________________________

Group status for ACCELUSS

S User     Name                 Ticket       Hr Asked by Start           Status
_ SRZOEG   EGLI MARCO           RITM12345678 2  SRZOEG   02Sep2020 15:03 Active
****************************** Bottom of data ********************************
```

Elevated Access Management – zSecure – show current elevations

- zSecure shows the queued commands that triggered the RACF group connect (red box).
- zSecure shows the queued command that will be executed by the hourly scheduled Job (blue box).

```
 Identification                                          MAINT
_RACF group name              ACCELUSS
_Superior group               $RAK     STRUCTURAL    OWNER GROUP FOR APPLICATION RACF(STANDARD PREFIX RAK) - NO AUTHORIZATIONS PERMITTED FOR THIS GROUP
_Owner                        $RAK                    STRUCTURAL    OWNER GROUP FOR APPLICATION RACF(STANDARD PREFIX RAK) - NO AUTHORIZATIONS PERMITTE
 Security Class               PRIVILEGED
 Install Data                 ACCESS ELEVATION TESTING - USER

 User/Grp Auth    R SOA AG Uacc    Revokedt    Resumedt    Name                RI DfltGrp  InstData
_SRZOEG   USE     _ ___ __ NONE    ___________ ___________ EGLI MARCO           USRUSR   501333332



 Safeguards                        Statistics
 Terminal use authorization   No   Creation date               10Jun20
 Universal access authority   NONE Universal group             No
 Data set model profile name

 UsrNm    Flg UsrData
_$C4RAINS 00 A,20162/0552,SRZOEG,00
_$C4RAOWN 00 A,20162/0552,SRZOEG,00
_$C4RASPG 00 A,20162/0552,SRZOEG,00

 Timed commands waiting for execution
_Queued command (PR): CMD AT 03Sep2020 REASON('RITM12345678 HRS(2)') REMOVE   SRZOEG OWNER(ACCELUSS) GROUP(ACCELUSS); pending reverse by SRZOEG at  2 Sep 202

 Commands that have been executed
_Queued command (X): CMD AT 02Sep2020 FOR 1 REASON('RITM12345678 HRS(2)') CONNECT  SRZOEG GROUP(ACCELUSS); request by SRZOEG at  2 Sep 2020 15:03; executed b
```

Elevated Access Management – Successful access request

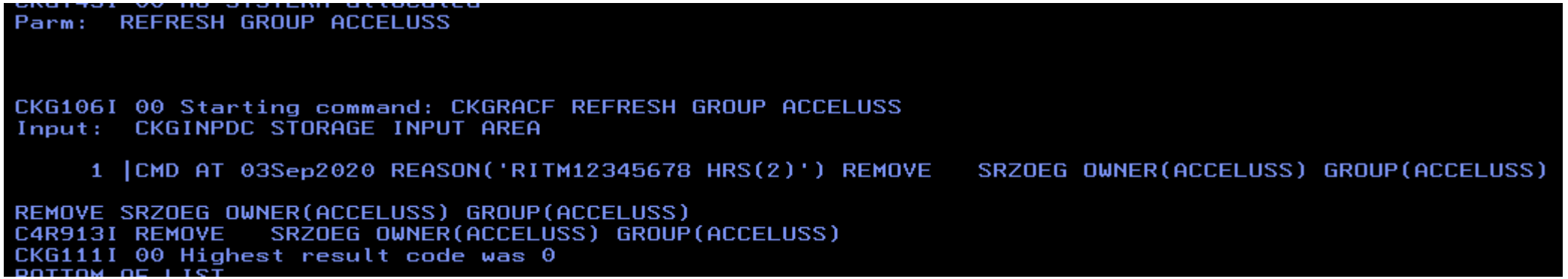
- A successful requests with the details from the previous slide will result
  - in a WTO

```
24000000 CH01MSYS 20246 15:03:44.89 T0788850 00000090  +SR-ACCESS-ELEVATION FOR SRZOEG TO ACCELUSS FOR 2H SRZOEG
```

  - in a E-Mail Alert

Elevated Access Management – Hourly Clean-up Job

- An hourly scheduled Job will execute all the queued commands as shown on the zSecure Panel for a selected elevation group.



Elevated Access Management – Important note

- Only Groups in the RACFVARS Profile &ACCELEV can be used for elevation.
- Elevation to such a privileged group can only be requested by specified groups.
- All based on zSecure (Command Verifier) with profiles in CL(XFACILIT)
  - CKG.CMD.CMD.REQ.CONNECT|REMOVE
  - CKG.SCP.G.INFRA.$RAK.RAKPUSSA
  - CKG.SCP.ID.RAKPUSSA.* -> only permit here the group that shall be able to elevate
  - C4R.CONNECT.ID.&ACCELEV.=RACUID
- Own written solution just because zSecure offers only calendar day elevations
  - Vote for idea to support hour granularity: ZSECURE-I-247

You do not loose access, you will have it for a limited time.

Any questions?

Legal notice