SMPE & RACF

A Practical z/OS Software and Security Administration Workbook

Software lifecycle • SMP/E concepts • RACF access control • Audit and change readiness

Estimated time: 45–60 minutes | Audience: z/OS system programmers, security administrators and mainframe operations teams

What you will learn

Understand the roles of SMP/E and RACF in a z/OS environment, interpret key software maintenance and access-control concepts, investigate common operational symptoms, and structure controlled changes with validation and rollback. Follow the installed release documentation and organisation-specific procedures.

1. Two critical z/OS control domains

SMP/E manages the installation and maintenance of z/OS software products and service. RACF protects system resources by authenticating users and controlling access. They address different concerns but both require disciplined change management, evidence and validation.

Domain / concept	Purpose and operational focus
SMP/E CSI	Consolidated Software Inventory stores information about installed software, zones, elements and service.
Global, target and distribution zones	SMP/E zone structures support service tracking and maintenance processing; exact configuration varies by product and installation.
SYSMOD	A unit of software change such as a function, PTF, APAR or user modification.
HOLDDATA	Communicates actions or conditions that must be reviewed before applying service.
RACF user and group profiles	Define identities and group relationships used in access decisions.
RACF resource profiles	Protect datasets, general resources and other controlled objects.
RACF permissions and auditing	Access authorities and logging support least privilege, accountability and review.

Operating principle

Keep software maintenance and security administration distinct in purpose, but coordinate their impact. A maintenance action can affect system components or security controls; a permission change can affect installation jobs, started tasks and application availability.

2. SMP/E maintenance workflow: control points

Stage	Checks and evidence
Prepare	Confirm product, release, CSI, target zone, maintenance scope and approved change window.
Receive	Validate service package source and integrity; confirm required metadata and prerequisites.
Review	Inspect SYSMOD relationships, requisites, supersedes and HOLDDATA; resolve holds through approved process.
Apply	Use the approved SMP/E process and capture output, return codes and messages.
Accept	Accept service only after required validation and according to site policy.
Validate	Run product and system checks, verify affected functions and update service records.

Do not treat APPLY and ACCEPT as interchangeable. Their timing and implications must follow the organisation’s SMP/E standards and the applicable IBM documentation.

© Copyright protected

3. RACF access-control review workflow

Control area	Review questions
Identity	Is the user or started-task identity valid, owned and still required?
Group membership	Are group connections appropriate for current responsibilities?
Dataset access	Are dataset profile rules and access levels consistent with least privilege?
General resources	Are relevant class profiles active and protecting the intended resources?
Privileged access	Are SPECIAL, OPERATIONS, AUDITOR and other elevated authorities justified, approved and reviewed?
Logging and audit	Are access events, violations and administrative changes reviewed under policy?

RACF principle

Grant only the access required for the task, to the correct identity and resource, for the appropriate duration. Review the effective access path, including group authorities, generic profiles and elevated attributes, rather than relying on a single profile entry.

4. Troubleshooting playbook

Symptom	Investigation path	Avoid
SMP/E APPLY fails	Review SMP/E messages, return codes, requisites, zone definitions, dataset availability and HOLDDATA.	Blindly rerunning or bypassing unresolved holds.
Unexpected service level	Compare CSI inventory and service records; check zone scope, prior maintenance and accepted/applied status.	Assuming a job completion message proves the intended service is active.
User cannot access dataset	Confirm identity, group membership, dataset profile, effective access and relevant RACF messages.	Granting broad access as a quick workaround.
Started task fails after security change	Review task identity, required dataset/general-resource access, profile changes and job logs with system/security owners.	Changing the started-task identity or granting broad authority without analysis.
Unexpected privileged access	Review user/group attributes, approvals, change history and audit records; contain through approved security incident process.	Removing access without assessing operational dependencies or preserving evidence.

5. Scenario: maintenance job fails after a RACF change

Situation: A planned software maintenance job begins failing after a security profile update. The job previously ran successfully. The operations team suspects the maintenance package, while the security team reports that a dataset access rule was tightened.

Investigation sequence

Step	Action and evidence
1. Establish timeline	Record job, system, time of failure and exact messages; compare with the RACF change window.
2. Scope the failure	Identify the failing step and resource; determine whether other jobs or identities are affected.
3. Review SMP/E context	Check CSI/zone, service package, prerequisites and whether the same maintenance job ran before the security change.
4. Review RACF context	Inspect the relevant identity, group connections, dataset/general-resource profiles and access messages.
5. Confirm effective access	Determine the minimum access required and whether the profile change altered the job's effective permissions.
6. Remediate safely	Coordinate system programming and security owners; implement a narrowly scoped approved correction or rollback.
7. Validate and close	Rerun only when approved; verify maintenance results, access controls and audit evidence.

Decision prompts

- Which event occurred first: the software maintenance failure or the security profile update?
- Does the failure identify a dataset or general resource access denial?
- Can the minimum required access be restored without broadening privileges?
- What evidence proves both maintenance integrity and security control are preserved?

© Copyright protected

6. Combined change-control checklist

Control	Evidence required
Scope	Affected product, zones, identities, resources, systems and business impact documented.
Baseline	Current CSI/service state, security profiles, access paths and relevant logs captured.
Technical review	IBM release-specific guidance, prerequisites, HOLDDATA and security dependencies reviewed.
Testing	Maintenance and access changes validated in a representative non-production environment where possible.
Approvals	System programming, security, application and operations owners approve the plan.
Recovery	SMP/E recovery/rollback approach and RACF profile restoration plan defined.
Post-change	Software level, job execution, effective access and audit records validated.

7. Operational worksheet

Field	Record
System / environment	_____
SMP/E product, CSI and zone	_____
SYSMOD / service identifiers	_____
RACF identity and resource	_____
Observed messages and timestamps	_____
HOLDDATA / prerequisite review	_____
Effective access findings	_____
Action, approval and rollback owner	_____
Validation and closure evidence	_____

8. Knowledge check

1. What is the primary purpose of SMP/E? **A.** Manage z/OS software installation and service **B.** Route network traffic **C.** Schedule user leave **D.** Manage application screens

2. What should be reviewed before applying service? **A.** HOLDDATA, prerequisites and requisites **B.** Only the job name **C.** Printer settings **D.** User desktop settings

3. What is RACF primarily used for? **A.** Software compilation **B.** Identity and resource access control **C.** Database reorganisation **D.** Tape labelling

4. A started task loses access after a profile update. What is the best approach? **A.** Grant SPECIAL **B.** Review the task identity and effective access to the required resource **C.** Disable auditing **D.** Change all profiles

5. Why validate after maintenance and security changes? **A.** Confirm software function and intended access controls **B.** Skip change records **C.** Avoid rollback planning **D.** Remove logs

Answer key: 1-A, 2-A, 3-B, 4-B, 5-A

Key takeaway

Safe z/OS operations depend on controlled software service and disciplined access management. Review maintenance prerequisites and holds, understand effective RACF access, coordinate cross-team changes, and validate both system function and security posture.

Further learning: Consult IBM Documentation for SMP/E, z/OS and RACF at the installed release. Review CSI and zone management, SYSMOD processing, HOLDDATA, service application, RACF profiles, group connections, dataset and general-resource protection, privileged attributes and auditing. Follow local change and security standards.

Ez-Learn course resource: SMPE & RACF | Use alongside the official curriculum, instructor guidance and approved lab environment.

© Copyright protected