

z/OS Security Server (RACF)

für

- **Systemprogrammierer**
- **Systemorientierte Mitarbeiter**
- **Künftige Security Administratoren**

Version 1.8 vom Juli 2021

Autor: Wolfram Greis

European Mainframe Academy GmbH
Am Klostersgarten 3
D 78337 Öhningen
Tel. +49-7735-9388668
ann-chatrine.mueller@mainframe-academy.de

European Mainframe Academy AG
Obergass 23
CH 8260 Stein am Rhein
Tel. +41-52-558 20 40
wolfram.greis@mainframe-academy.de

Inhaltsverzeichnis

1	Ziele des Ausbildungsmoduls	3
2	Informationen zum "Blended Learning" der EMA.....	3
3	Inhaltsbeschreibung	3
3.1	Virtueller Kick-off	4
3.2	z/OS Security Server Basics (ca. 40 Stunden).....	5
3.3	z/OS Security Server Vertiefung (ca. 40 Stunden)	6
3.4	Abschluss (virtuell)	7

1 Ziele des Ausbildungsmoduls

Die Teilnehmer lernen, wie RACF als External Security Manager in eine z/OS Umgebung integriert ist. Sie kennen die diversen Profilarten von RACF und wie damit Ressourcen unterschiedlichster Art wirkungsvoll geschützt werden können. Nachdem die Basics bekannt sind, lernen die Teilnehmer – unterstützt durch viele praktische Übungen – wie RACF administriert und bzgl. Monitoring und Performance optimiert werden kann.

2 Informationen zum "Blended Learning" der EMA

Die Lehrgangsmodule der EMA sind eingeteilt in Pflichtstoff und Wahlstoff. Der Pflichtstoff ist prüfungsrelevant, d.h., dass die entsprechend vermittelten Kenntnisse in Tests, Prüfungen und praktischen Arbeiten vorhanden sein müssen und abgefragt werden, falls am Ende des Moduls ein Zertifikat erlangt werden soll.

Der Wahlstoff kann auf freiwilliger Basis durchgearbeitet werden. Selbstverständlich stehen für sämtliche Belange qualifizierte Fachkräfte für die Beantwortung von Fragen zur Verfügung. Der durchschnittliche Lernaufwand für den Pflichtstoff beträgt ca. 10 Stunden pro Woche.

Die Module bestehen aus:

- Virtueller Kick-off / Abschluss, ggf. mit Prüfung
- Virtuelle Klassenzimmer
- E-Learning
- Theoretische und praktische Übungen

3 Inhaltsbeschreibung

Im Folgenden werden die Module detailliert beschrieben. Die Zahl in Klammern bei den Inhalten gibt die geschätzte durchschnittliche Bearbeitungszeit in Stunden an.

3.1 Virtueller Kick-off

Mit diesem Kick-off wird die Basis einer erfolgreichen Zusammenarbeit während der gesamten Lernphase gelegt.

Dauer 2 halbe Tage virtuell

Datum Nächster Termin: s. Dokument Starttermine/Preisliste

Ort Virtuell

Ziele des Workshops

Mit diesem Präsenzworkshop sollen drei Dinge erreicht werden:

- Die Teilnehmer und die Key-Dozenten lernen sich gegenseitig kennen
- Die Teilnehmer lernen die wichtigsten E-Learning Werkzeuge kennen, vor allem das Virtuelle Klassenzimmer
- Die Teilnehmer bekommen einen ersten Überblick über die Seminarinhalte

Inhalt

Einführung

Vorstellungsrunde
Einführung in das Thema

Lerneffizienz

Lernen und Erkenntnisse der Neurobiologie
Effizientes Lernen

Security und Mainframes (Überblick)

Anforderungen an die Security
Worin unterscheidet sich Mainframe-Security von anderen Plattformen?
z/OS und z/OS UNIX System Services
Die Rolle des z/OS Security Servers
Gruppenarbeit

E-Learning & Blended Learning

Der Bedeutung von E-Learning
Die Vorteile des Blended Learning
E-Learning Werkzeuge im Überblick

Lernplattform Moodle

Übersicht über die Lernplattform
Aufbau der Lernplattform

Das Virtuelle Klassenzimmer

Ziele einer VC-Session
Unterschiede zum herkömmlichen Klassenzimmer
Einsatz des Virtuellen Klassenzimmers

Zugriff auf den Mainframe

Die Infrastruktur der EMA
Zugriff auf den IBM Rechner

3.2 z/OS Security Server Basics (ca. 40 Stunden)

Ziele dieses Untermoduls

Die Teilnehmer kennen den z/OS Security Server und insbesondere RACF. Sie können die diversen Profilarten von RACF beschreiben. Sie kennen die Befehle, um Profile einzurichten und zu verändern. Sie können abschätzen, wann welche Befehle sinnvoller Weise unter TSO/ISPF und wann als Batchjob abgesetzt werden.

Inhalt

RACF Überblick

Anforderungen an ein Security System
Sicherheit im Rechenzentrum
Physische Sicherheit
Sicherheit des Betriebssystems
RACF als Baustein eines Gesamtkonzepts
RACF Funktionsüberblick
RACF Profilarten
System Access Facility (SAF) und RACF

Reporting und Utilities

RACF Utilities
RACF Audit Funktionen

RACF Optionen

Display der Optionen
SETR Befehle

Verwaltung von RACF Benutzern

RACF Aufbau

Hierarchische Architektur
Gruppenkonzept
RACF Konzept & Konventionen
Generic Profiles
Schutz von Dateien
Schutz von General Resources

Komponenten von RACF

RACF Datenbank
RACF Befehle
Verwaltung mit Batchjobs
ISPF Schnittstelle

3.3 z/OS Security Server Vertiefung (ca. 40 Stunden)

Ziele dieses Untermoduls

Die Teilnehmer kennen erweiterte Möglichkeiten von RACF. Sie können z/OS Subsysteme wie DB2, CICS und weitere z/OS Komponenten aus Security-Sicht verwalten.

Inhalt

Erstellen und Migrieren einer RACF Umgebung

RACF Datenbank

RACF General Resources

Wie werden Klassen definiert?
Resource Typen und Klassen
Facility Class
Weitere Beispiele

RACF und UNIX System Services

UID und GID Verwaltung
Schutz von Prozessen
File Security Packet
SETUID/SETGID
BPX Profiles und UNIXPRIV Class

Security Labels

RACF Remote Sharing Facility (RRSF)

RACF und LDAP

Data Security Monitor (DSMON)

RACF und SMF

RACF Performance

3.4 Abschluss (virtuell)

Mit diesem virtuellen Abschluss werden die Ergebnisse zusammengefasst und offene Fragen beantwortet.

Dauer 1 Virtuelle Session

Ort Virtuell

Ziele des Workshops

- Die wichtigsten Themen und Schwerpunkte werden noch einmal zusammengefasst
- Die Teilnehmer beantworten Verständnisfragen der Coaches / Referenten um den Wissenstransfer sicher zu stellen.
- Die Teilnehmer stellen Fragen, die sich während der Ausbildung ergeben haben.
- Im Falle einer Zertifizierung wird eine Prüfung geschrieben.