

AUDITSTAR FOR IBM/MVS RACF

AUDITSTAR PERFORMS A THOROUGH SECURITY AND SYSTEM INTEGRITY AUDIT ON IBM MAINFRAMES RUNNING MVS AND RACF. AUDITSTAR ASSURES THAT PROBLEMS ARE FOUND WITHOUT DELAY AND CLOSED APPROPRIATELY. AUDIT POINTS ARE RESOLVED AND STAY RESOLVED.



AUDITSTAR WILL:

- ENFORCE INSTALLION SECURITY POLICIES AND STANDARDS.
- DETECT PROBLEMS BASED ON IBM BEST PRACTICE CRITERIA.
- EVALUATE COMPLIANCE WITH REGULATIONS.
- PERFORM CONTINUAL SELF-AUDITS.
- HELP PREPARE FOR AND PASS SECURITY AUDITS.
- IMPROVE DEPARTMENTAL EFFICIENCY.

Several years ago, Ford Motor Company and SunTrust Bank challenged us to help their IBM Mainframe security analysts track down and manage security and audit problems. Their security staff needed to find problems without spending hours sorting through volumes of data. They also needed to make sure that security problems and audit points that were fixed stayed fixed. We solved these problems by developing AuditStar.

AuditStar is a security status evaluation system that performs a thorough audit on IBM Mainframes running MVS and RACF, providing a fully automated security scorecard that reports deviations from installation specific security standards and IBM best practices. These standards cover all the important RACF security system parameters, profiles and privileges with reports. AuditStar also assures that MVS System integrity is maintained.

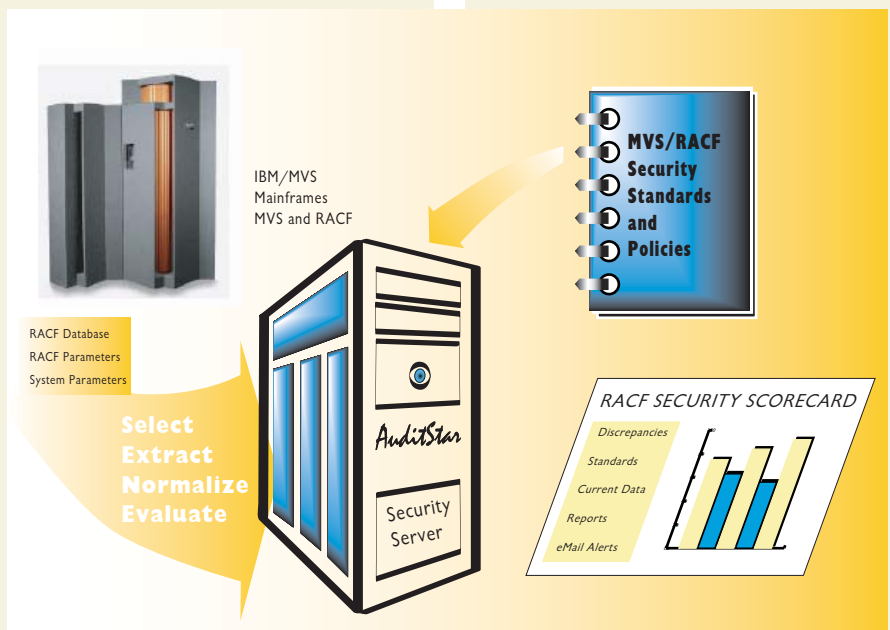
Finding Security Discrepancies

AuditStar is split into mainframe and server processes. The mainframe process periodically captures information regarding access protection and system integrity for each RACF database and each MVS image. This

information is sent from each mainframe to the AuditStar Server. The AuditStar Server stores the information and evaluates it based on a set of installation specific standards.

The AuditStar server triggers a discrepancy whenever there is a difference between the installation specific standard and the actual security parameter or privilege on the mainframe. AuditStar also reports on deviations from IBM best practices. The Windows based AuditStar client software makes discrepancies easy to review with all data easily available in Excel for custom analysis.

AuditStar is a proven solution that can handle the largest IBM Mainframe installations with multiple RACF databases and MVS systems.



AUDITSTAR FOR IBM/MVS RACF

Items Monitored by AuditStar

<u>Record ID</u>	<u>Information in record</u>	<u>What to look for</u>	<u>Examples of concerns</u>
O10	IPL volume and device unit address		
O30	SMF parameters	Global settings for SMF recording	Inactivating SMF
O41	SMF subsystem exit activity	SMF exits	New exits
O42	SMF subsystem recording inactivity	Suppressed SMF records	Suppressing audit trails (RACF 80 Dataset I/O)
O50	Supervisor Calls (SVCs)	New, altered or removed SVCs	Rogue SVCs
O51	Supervisor Calls (SVCs Details)	New, altered or removed SVCs	Rogue SVCs
O60	I/O Appendages	New, altered or removed appendages	Appendages that have been added or deleted
O61	I/O Appendages (Details)	New, altered or removed appendages	Appendages that have been added or deleted
O80	MVS Subsystem Appendages	New, altered or removed appendages	Appendages that have been added or deleted
O90	Modules with Scan Hits	Modules that have suspicious instructions	Programs that appear to be setting authorization bits: FakeSpecial, FakeOperations, FakePriv (flipping bit in ACEE).
O91	Monitored Load Modules	Changes in modules that have been specifically identified to be watched	Unexpected changes
O92	Monitored Text Members	Changes in text that have been specifically identified to be watched	Unexpected changes
P50	Sensitive Datasets - dsnames	See list of automatically detected system datasets	Unexpected changes
P51	Sensitive Datasets - details		
P60	RACF Segment Usage	Indicates number of profiles in the RACF database	For Information Only
P61	RACF Database Size	Indicates size of RACF database in terms of Bytes	For Information Only
R10	System software releases and status(RACF only)	RACF, DFP, HSM, JES, MVS, RMF, SMS, TSO, VTAM	An unexpected RACF upgrade / regression
R15	CONSOLES logon required	System consoles - security settings	Unexpected changes
R21	SETROPTS – part a	System wide RACF settings	Unexpected changes
R22	SETROPTS – part b	System wide RACF settings	
R23	SETROPTS – part c	System wide RACF settings	

AUDITSTAR FOR IBM/MVS RACF

Items Monitored by AuditStar (continued)

<u>Record ID</u>	<u>Information in record</u>	<u>What to look for</u>	<u>Examples of concerns</u>
R30	RACF Database Name Table	Names of your RACF datasets	Changes to table
R31	RACF Range Table	If you have multiple RACF datasets, table specifying which profiles go on which dataset	Changes to table
R40	RACF Authorized Caller Table	Programs that can run APF authorized within TSO	New programs
R50	RACF Class Descriptor Table	All RACF classes and their attributes	New classes; Deleted classes; Activation/inactivation of a class; modification to characteristics of a class
R70	SAF Router Table	MVS SAF table that routes SAF requests	
R80	Modules with PPT attributes	APF Modules, their library and access list for programs that are present in the PPT with BYPASS or a system key, or TSO authorizations (AuthCMD, AuthPGM, AuthTSF).	Any modules that can bypass RACF
RB2	System exits	See table of exits	RACF exits; SMF exits; Exits can modify expected security behavior; can modify SMF data
RC0	RACF Started Task Table (ICHRIN03)	Contents of table ICHRIN03	Started tasks with TRUSTED or PRIVILEGED
P10	RACF dataset profiles to be monitored	Monitor dataset profiles that do not comply with standards or policy; Monitor dataset profiles of identified "sensitive" datasets	Installation specific violations of standards for profiles.
P11	RACF dataset profiles to be monitored – Access lists	Access lists of above profiles.	
P20	RACF general resource profiles to be monitored	Monitor protection of system wide general resources, e.g. MVS operator commands; JES commands; CICS / IMS transactions.	
P21	RACF general resource profiles to be monitored – Access lists		
P22	RACF general resource profiles to be monitored – Members		
P30	RACF dataset profiles for Sensitive Datasets	Dataset profiles for datasets that are critical to the integrity of the operating system	Unexpected changes
P31	RACF dataset profiles for Sensitive Datasets – Access lists		UPDATE access (or higher)
P40	RACF STDATA segments for STARTED class	All STDATA segments in STARTED class	Started tasks with TRUSTED or PRIVILEGED

AUDITSTAR FOR IBM/MVS RACF

Items Monitored by AuditStar (continued)

<u>Record ID</u>	<u>Information in record</u>	<u>What to look for</u>	<u>Examples of concerns</u>
R60	RACF Global access table (GLOBAL class)	GLOBAL class entries have no SMF auditing	Unexpected changes
U10	RACF Userids with system attributes/privileges	Special attributes: SPECIAL allows you to make any change on RACF	Verify any new users. OPERATIONS is like a "back door" to dataset access; AUDITOR allows you to look at any RACF profile, and change global auditing settings
U11	RACF Userids that are being Audited	Userids being audited	Verify list
U12	RACF Userids that are Protected	Protected userids can not be used to logon	Verify list
U13	RACF Userids that are Restricted	Restricted userids can not access resources via UACC or GLOBAL	Verify list
U21	RACF Userids with Class Authorizations	Users who have class authorizations (CLAUTH)	Verify any new users
U31	RACF Groups to be monitored	Groups that have access to sensitive data and/or commands	Verify any new members in these groups are OK
U40	RACF Userids with non-conforming password interval	Users with password interval other than 30	Verify any user who has NOINTERVAL
U50	RACF 'Critical' userids that are revoked	"Hot ids", CA7 ids, AutoOps ids etc	Could cause outages
U60	RACF Userids that have never been used, Created > nn days ago	Userid probably not needed	Cleanup / housekeeping
U70	RACF Userids that are inactive, Last Use > mm days ago	"Stale" userids, probably not needed any more	Cleanup / housekeeping
U81	RACF Userids with Group attributes/privileges	All users with either GROUP SPECIAL, OPERATIONS, AUDITOR	Verify any new users - allows administrative capabilities within RACF
U90	Sensitive Unix UIDs	Sensitive UIDs that should or should not exist. (UID of 0 is superuser in OMVS)	Verify that sensitive UIDs exist. (Users can also get via access to BPX.SUPERUSER)
U91	Users with Sensitive Unix UIDs	UID of 0 is superuser in OMVS (Can also get via access to BPX.SUPERUSER)	Verify that Users with sensitive UIDs are restricted to those authorized
U95	Sensitive Unix GIDs	Some GIDs may be restricted	Verify that restricted GIDs exist are not used by unauthorized groups
U96	Groups with Sensitive Unix GIDs	Groups with sensitive GIDs may be restricted	Verify that Groups with sensitive GIDs are restricted to those authorized
U97	Users in Groups with Sensitive Unix GIDs	Users in Groups with sensitive GIDs may be restricted	Verify that Users in Groups with sensitive GIDs are restricted to those authorized
G10	Shared DASD	DASD should have same VOLSER across systems	Data access permissions should be the same across all systems

AUDITSTAR FOR IBM/MVS RACF

AUDITSTAR SECURITY STANDARDS CAN BE CREATED AND CUSTOMIZED FOR YOUR SYSTEMS IN ONLY A FEW HOURS. EVEN IN THE MOST COMPLEX ENVIRONMENTS ONLY A DAY OR TWO IS USUALLY REQUIRED TO PUT A COMPLETE SET OF STANDARDS IN PLACE.

THIS MEANS AUDITSTAR IS WORKING RIGHT AWAY TO KEEP YOUR IBM MVS/RACF SYSTEMS SECURE.

AuditStar gives you the tools to move beyond ad hoc methods for managing the quality of security on the IBM Mainframe. These tools support the security scorecard process by performing the following functions:

- The process of establishing installation specific standards for AuditStar usually takes no more than a day, even in complex environments. This is because AuditStar completely automates the process of loading, validating and managing security standards.
- AuditStar automatically gathers periodic extracts of all required RACF security and MVS integrity information from each monitored system. This can be done daily, weekly or on any custom schedule.
- As each periodic extract is transferred to the AuditStar server, a deviation analysis is automatically performed. The result is a series of summary and detailed discrepancy reports.
- AuditStar reports list all items that do not meet standards and all discrepancies that have been resolved.
- On each run, there is a report of deviations from IBM best practices. This helps catch items that are of concern before they create security or integrity problems.
- AuditStar manages the process of resolving discrepancies. The security administrator uses the program to view and close discrepancies, and to check historical trends.
- When discrepancies appear on multiple systems, they can be automatically closed on all systems at once. This makes the process of administering discrepancies and standards fast and efficient.
- AuditStar will automatically add, delete or modify standards based on the security administrator's input.
- AuditStar produces a summary security scorecard that lets you measure security quality. Daily reports show you see how systems programmers, application programmers and users are complying with security policies. Plus there are detail reports that provide thorough information on each discrepancy.
- AuditStar uses a familiar Windows interface. All reports can be transferred to Excel spreadsheets with the click of a mouse. You do not have to log on to the IBM Mainframe to use AuditStar.

MASE TECHNOLOGIES LLC
PO Box 1690
FLOWERY BRANCH GA 30542

SALES: 877.762.7300
TECHNICAL: 770.534.0611

WWW.MASE.COM

RELY ON AUDITSTAR TO IMPROVE YOUR ORGANIZATION'S IBM MVS/RACF SECURITY BOTTOM LINE.



SALES: 877-762-7300
SUPPORT: 770-534-0611