

SDS IronSphere for z/OS

Automate z/OS STIG Compliance through Continuous Security Monitoring

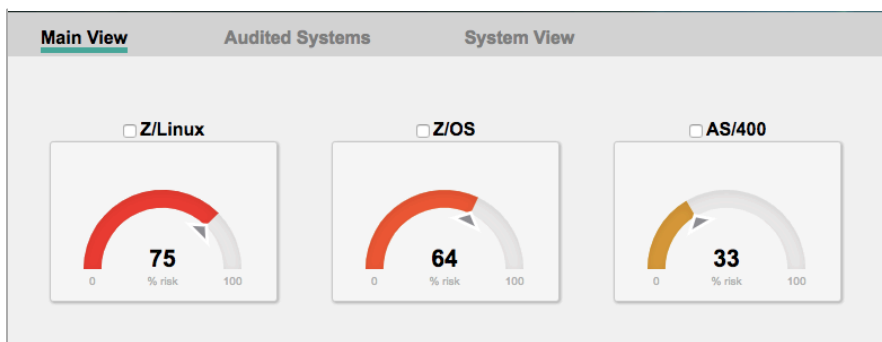
Mainframes are heavily used by high-volume businesses required to comply with stringent federal regulations and rigorous industry standards. They are also often run by outdated enterprise clients that rely on costly manual processing. For a system with numerous servers or LPARs, security scans can be an ongoing chore of enormous time and effort.

IronSphere conquers the task. It continuously monitors the mainframe, automatically performing security checks and looking for system vulnerabilities, altered system settings, and modified operands. What could take months to examine manually, IronSphere can automate in a few minutes, with low overhead and real-time results. If a change is detected, IronSphere launches automatic diagnostic routines to determine:

- Security problems and errors
- Root cause of problems
- Which components are affected
- Which issues are the highest risk

Security scans are based on IBM z/OS RACF® or CA Top Secret® STIGs (Security Technical Information Guides) which contain optimized policy and configuration information. IronSphere automatically compares each application to its STIG to detect discrepancies. The resulting real-time report identifies errors, assigns risk levels, and charts the findings. It even describes how to resolve the problem.

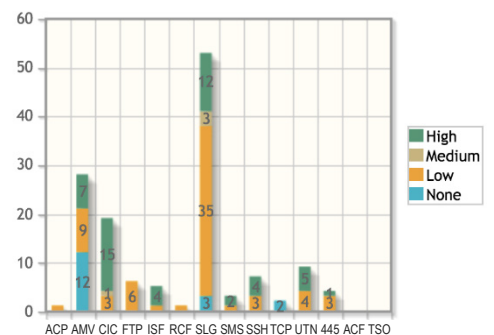
A dashboard reports the health of each system with intuitive, color-coded graphs.



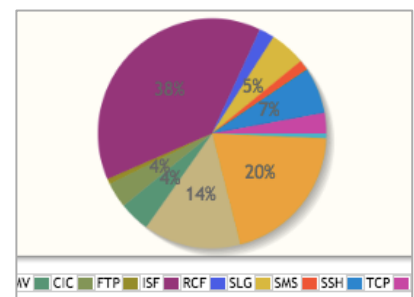
Compliance, Continuous Monitoring, and Data Protection

IronSphere helps comply with GDPR, NIST ISCM, and DoD requirements.

- Real-time vulnerability reporting.
- Mainframe STIG monitoring.
- Risk resolution sent to your inbox.
- Simplifies complicated mandates.
- Easy z/OS security audits.



Risk levels within each group.



Distribution of a risk level across groups.

Data is displayed graphically in easy-to-understand charts and tables. Results can be sorted and filtered per system, LPAR, group, severity level, or other criteria.

Simplify mainframe security! Intuitive GUI gives you the problem resolution.

Name	Severity	Description
MVS-AMV-040-00	Low	Inaccessible APF libraries defined.
MVS-AMV-150-00	Medium	Inapplicable PPT entries have not been
MVS-AMV-325-00	None	AMVU does not exist or inaccessible Link Pa
MVS-AMV-350-00	None	AMVU does not exist or inaccessible LINKL
MVS-AMV-410-00	None	AMVU database is not on separate p
MVS-AMV-440-00	None	AMVU database is not on separate p
MVS-ACP-010-00	Medium	AMVU database is not on separate p
MVS-ACP-020-00	None	AMVU database is not on separate p
MVS-ACP-030-00	None	AMVU database is not on separate p
MVS-ACP-040-00	High	AMVU database is not on separate p

Security and GRC teams are z/OS risk-aware:

Automatic assessments detect changes in the status of system components, identify risk levels, and report all results from a single graphical interface.

IronSphere can conclusively prove an application is error-free and in compliance with security standards.

IronSphere can validate that an application or group meets security standards.

When run regularly over time, a history is created that can confirm system integrity for compliance reporting.

Results can be shown in a variety of comparison and history charts to suit the needs of any management or security team.

Each IronSphere agent reports results to the server over HTTPS. Messages and trace data are not stored on the mainframe.

Name	Severity	Time	Control ID	Description
MVR-RCF-480-00	High	6 Feb 2018 8:13:12	RACF0480	The PROTECTALL SETROPTS value specified is improperly set.

Information

Name	MVSA
Type	z/OS 02.02.00 HBB77A0
Class	Data Integrity
Description	When PROTECTALL processing is active and set to FAIL, the system automatically rejects any request to create or access a data set that is not RACF protected. Temporary data sets that comply with standard MVS temporary data set naming conventions are excluded from PROTECTALL processing. PROTECTALL requires that data sets be RACF protected. In order for PROTECTALL to work effectively, you must specify GENERIC to activate generic profile checking. Otherwise, RACF would allow users to create or access only data sets protected by discrete profiles. The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any of these fields, individually or in combination with another, can compromise the security of the processing environment. In

Fix

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the example below. The RACF Command SETR LIST will show the status of RACF Controls including the value for the PROTECTALL is ACTIVATED and set to FAIL by issuing the command SETR PROTECTALL(FAIL).

Detailed STIG information is displayed in one location, including the fix.

About SDS

Founded in 1982, SDS supports over 25 products for z/OS, MVS, VSE, VM, AIX, Linux, and Windows. SDS has licensed more than 1,000 enterprise clients worldwide with quality mainframe software and offers award-winning technical support. Comprehensive solutions focus on security, encryption, data compression, and network monitoring. To learn more, please visit our web site.

©SDS 2018