Center for Internet Security (CIS®) Benchmarks

New York/Tampa/Dallas/Raleigh RACF® Users Group

15 May 2024

Mark Nelson, CISSP®, CSSLP®, markan@us.ibm.com

CIS Benchmarks

- **The Center for Internet Security, Inc. (CIS):**
  - Community-driven, not-for-profit (501 (c) 3) organization responsible for the CIS Controls® and CIS Benchmarks™, best practices for securing IT systems and data.
  - Mission: Help people, businesses, and governments protect themselves against pervasive cyber threats.

Available CIS Benchmarks

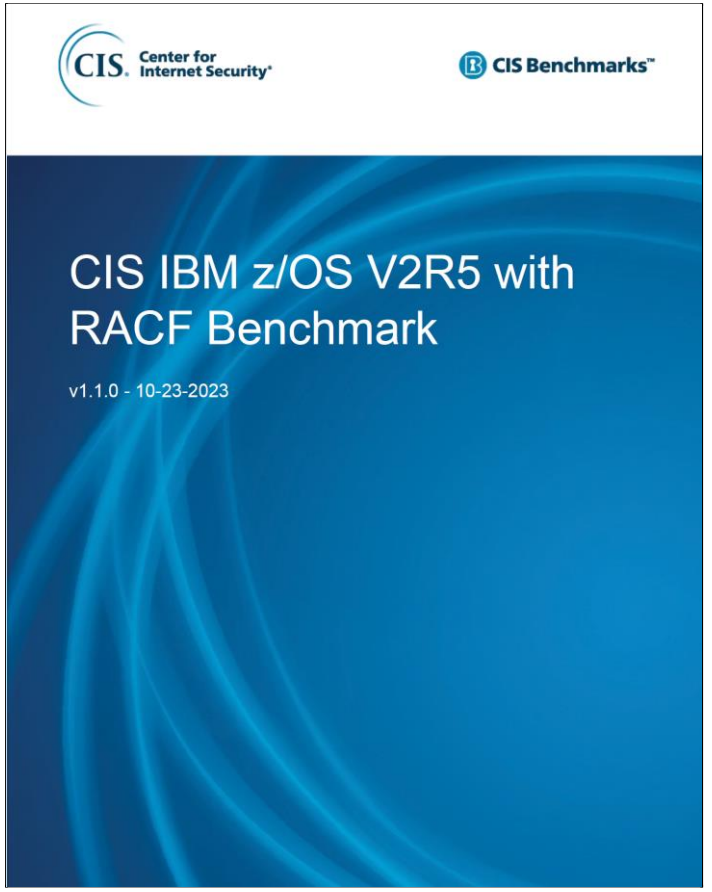
- Alibaba Cloud
- Aliyun Linux
- AlmaLinux OS
- Amazon Linux
- Amazon Web Services
- Apache Cassandra
- Apache HTTP Server
- Apache Tomcat
- Apple iOS
- Apple macOS
- Azure Linux
- BIND
- Bottlerocket
- CentOS Linux
- Check Point Firewall
- Cisco
- Debian Family Linux
- Debian Linux
- Distribution Independent Linux
- Docker
- F5
- Fedora Family Linux
- Fortinet
- Google Android
- Google Chrome
- Google Cloud Computing Platform
- Google Workspace
- **IBM AIX**
- **IBM Cloud Foundations**
- **IBM Db2**
- **IBM i**
- **IBM WebSphere**
- ***IBM Z System***
- Juniper
- Kubernetes
- LXD
- MariaDB
- Microsoft 365
- Microsoft Azure
- Microsoft Dynamics 365 Power Platform
- Microsoft Exchange Server
- Microsoft IIS
- Microsoft Intune for Microsoft Windows
- Microsoft Office
- Microsoft SharePoint
- Microsoft SQL Server
- Microsoft Web Browser
- Microsoft Windows Desktop
- Microsoft Windows Server
- MIT Kerberos
- MongoDB
- Mozilla Firefox
- NGINX
- Oracle Cloud Infrastructure
- Oracle Database
- Oracle Linux
- Oracle MySQL
- Oracle Solaris
- Palo Alto Networks
- pfSense Firewall
- PostgreSQL
- Print Devices
- Red Hat Enterprise Linux
- Robot Operating System (ROS)
- Rocky Linux
- Safari Browser
- Snowflake
- Software Supply Chain Security
- Sophos
- SUSE Linux Enterprise Server
- Ubuntu Linux
- VMware
- YugabyteDB
- Zoom

IBM Z System Benchmarks

- **Four IBM Z® System Benchmarks are available:**
  - IBM z/OS® V2R5 with RACF (1.1.0)
  - IBM Db2® 13 for z/OS (1.0.0)
  - IBM CICS Transaction Server 6.1 (1.0.0)
  - RHEL8 on IBM Z Linux (1.0.0)

CIS Benchmarks

- **The z/OS V2R5 with RACF Benchmark:**
  - ***Contains 219 recommendations across 9 domains:***
    - Identification and Authentication
    - Authorization and Access Control Management
    - Logging and Auditing
    - System Resilience
    - Storage Management
    - Networking
    - Cryptography and Encryption
    - Job Management
    - UNIX System Services
  - ***https://www.cisecurity.org/benchmark/ibm_z***
    - Provide contact information, link e-mailed



Control Documentation

Each control has a:

- **Title:** A Concise description for the recommendation's intended configuration.
- **Assessment Status:** Can the control be automated or must it be manual?
- **Profile Applicability:** Level 1 (applicable to all) or Level 2 (for special security needs)
- **Description:** Detailed information pertaining to the setting
- **Rationale:** Detailed reasoning for the recommendation
- **Impact Statement:** Any security, functionality, or operational consequences that can result from following the recommendation.
- **Audit Procedure:** Systematic instructions for determining if the target system complies with the recommendation
- **Remediation Procedure:** Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.
- **Default Value:** Default value for the given setting in this recommendation
- **References:** Additional documentation relative to the recommendation.

Sample Control

1.1.1 Ensure that the PASSWORD(INTERVAL) SETROPTS value is set to no longer than 90 days (Automated)

Profile Applicability:

- Level 1

Description:

When a user logs on to the system, RACF compares the system password interval value to the value specified in the user profile. RACF uses the lower of the two values to determine if the user's password has expired.

`PASSWORD(INTERVAL(n))` command sets the maximum age of a password. The `INTERVAL` suboperand specifies the system default for the maximum number "n" of days that each user's password and password phrase remain valid.

If you have the `SPECIAL` attribute, you can specify the `INTERVAL` of the `SETROPTS PASSWORD` command. The `INTERVAL` suboperand specifies the system default for the maximum number of days that each user's password and password phrase remain valid.

Rationale:

The improper setting of any of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for RACF control options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

To verify a password will expire within 90 days issue the TSO command:

```
SETROPTS LIST
```

and look for the interval value. The `PASSWORD(INTERVAL)` value is found in the return message "PASSWORD CHANGE INTERVAL IS xxx DAYS." xxx will be a value from 1 to 90.

Remediation:

Setting the password interval to 90 days is activated by issuing the TSO command:

```
SETROPTS PASSWORD(INTERVAL(90))
```

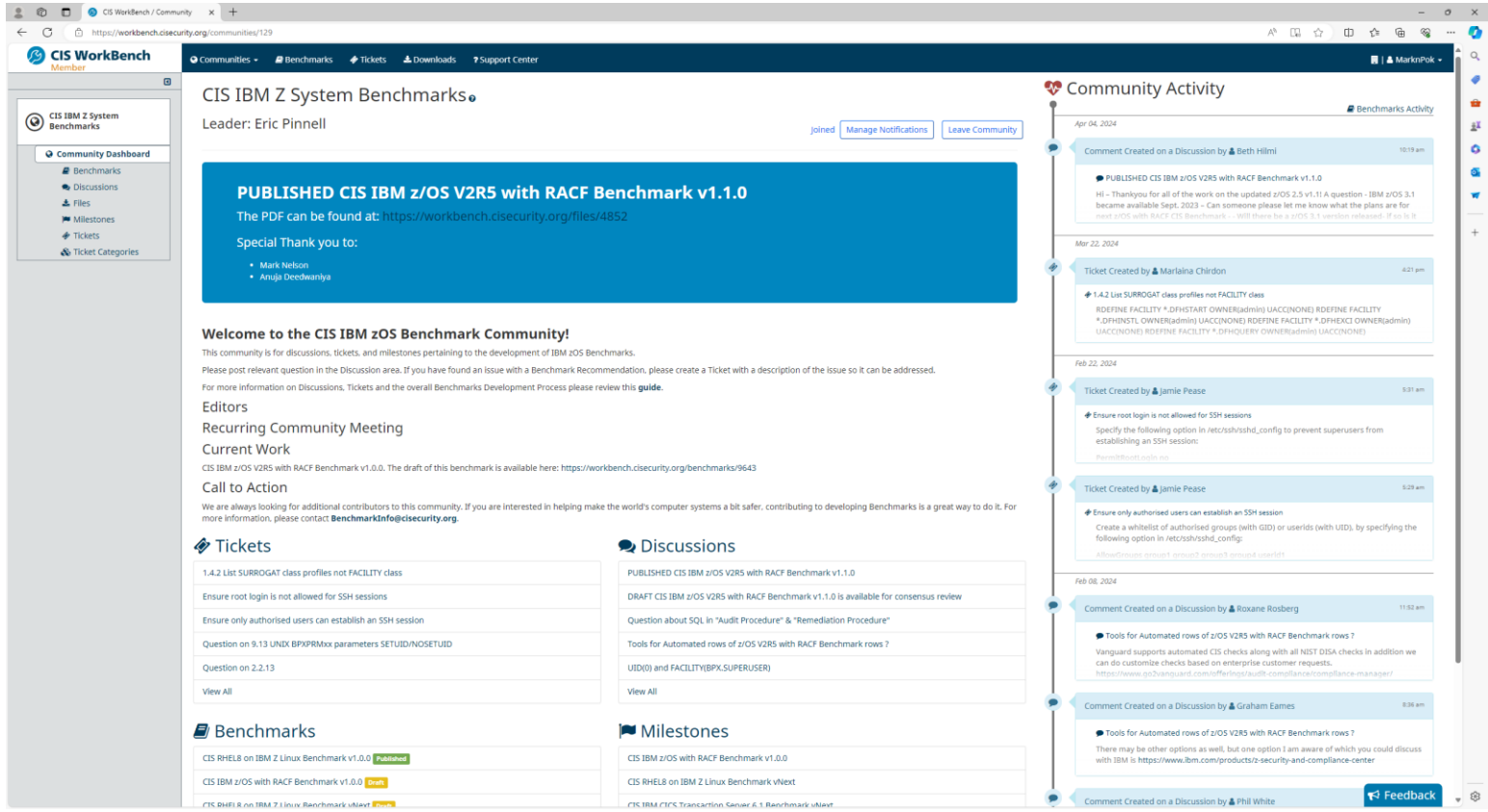
Default Value:

INTERVAL = 30

Page 18

CIS Workbench

- Website (https://workbench.cisecurity.org/community/129/files) for:
  - Discissions on controls
  - Downloading of benchmarks
  - Tracking of request “tickets” for controls
  - Tracking of milestones



Center for Internet Security (CIS®) Benchmarks

New York/Tampa/Dallas/Raleigh RACF® Users Group

15 May 2024

Mark Nelson, CISSP®, CSSLP®, markan@us.ibm.com