

UNCLASSIFIED



**z/OS
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG)
ADDENDUM**

Version 6, Release 62

24 October 2024

Developed by DISA for the DOD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

| | Page |
|---|------|
| 1. INTRODUCTION | 1 |
| 1.1 Executive Summary | 1 |
| 1.2 Authority..... | 1 |
| 1.3 Vulnerability Severity Category Code Definitions..... | 2 |
| 1.4 STIG Distribution..... | 2 |
| 1.5 Document Revisions | 2 |
| 1.6 Other Considerations | 2 |
| 1.7 Product Approval Disclaimer..... | 3 |
| 2. INTRODUCTION TO Z/OS | 4 |
| 2.1 z/OS Background | 4 |
| 2.2 z/OS Dataset Types..... | 5 |
| 2.3 z/OS Additional Access/Logging Restrictions..... | 5 |
| 3. Z/OS PRIVILEGED USERS..... | 6 |
| 4. Z/OS UNIX SYSTEM SERVICES | 9 |
| 4.1 z/OS UNIX System Services Background | 9 |
| 4.2 z/OS UNIX General Considerations | 9 |
| 4.3 z/OS UNIX User Identity | 14 |
| 4.4 z/OS UNIX User Identity | 14 |
| 4.5 z/OS UNIX Interactive Environment – The UNIX Shell..... | 21 |
| 4.6 z/OS UNIX Background Processes - Daemons and Servers..... | 25 |
| 4.7 z/OS UNIX Miscellaneous Considerations..... | 29 |
| 4.8 z/OS UNIX SMF Options | 30 |
| 4.9 z/OS UNIX Account Data Validation - IEFUJI..... | 30 |
| 4.10 z/OS UNIX RTLS | 31 |
| 5. EXTERNAL SECURITY MANAGER IMPLEMENTATION..... | 32 |
| 5.1 ESM General Considerations | 32 |
| 5.1.1 ESM Standard Global Options | 33 |
| 5.1.2 ESM Userid Controls | 33 |
| 5.1.3 Password Complexity | 36 |
| 6. TRUSTED STARTED TASKS | 37 |
| 7. Z/OS SYSTEM AND JES2 COMMANDS..... | 38 |
| 8. SENSITIVE UTILITY REQUIREMENT..... | 55 |
| 9. SMS PROGRAM REQUIREMENT..... | 57 |
| 10. Z/OS BASELINE REQUIREMENTS | 62 |
| 11. PRODUCT REQUIREMENTS..... | 71 |
| 11.1 General Installed Product Information..... | 71 |

| | | |
|---------|--|-----|
| 11.2 | BMC INCONTROL Resource Requirements | 71 |
| 11.3 | CA 1 Requirements | 92 |
| 11.3.1 | ACF2 Tables | 94 |
| 11.3.2 | RACF Tables | 95 |
| 11.3.3 | TSS Tables | 96 |
| 11.4 | CATALOG SOLUTIONS Requirements | 98 |
| 11.5 | CICS Requirements | 101 |
| 11.6 | WebSphere MQ Requirements | 122 |
| 11.7 | Web Application Server Requirements | 124 |
| 11.8 | SDSF Requirements | 125 |
| 11.9 | CL/SuperSession Requirements | 139 |
| 11.10 | CA ROSCOE Requirements | 140 |
| 11.10.1 | Access Attribute Translation | 140 |
| 11.11 | Vanguard Security Solutions Requirements | 143 |
| 11.12 | Compuware Abend-AID Requirements | 151 |
| 11.13 | BMC MAINVIEW Requirements | 152 |
| 11.14 | CA MIM Requirements | 158 |
| 11.15 | NetView Requirements | 160 |
| 11.16 | RACF Password Exit Settings | 166 |

LIST OF TABLES

| | Page |
|--|-------------|
| Table 1-1: Vulnerability Severity Category Code Definitions | 2 |
| Table 3-1: Authorized User Groups | 6 |
| Table 4-1: General FACILITY Class BPX Resources | 10 |
| Table 4-2: UNIXPRIV Class Resources..... | 11 |
| Table 4-3: MVS Data Sets with z/OS UNIX Components..... | 14 |
| Table 4-4: Permission Bits..... | 16 |
| Table 4-5: Special Permission Bits..... | 16 |
| Table 4-6: Extended Attributes..... | 18 |
| Table 4-7: Audit Bits..... | 18 |
| Table 4-8: System Directory Security Settings..... | 19 |
| Table 4-9: System File Security Settings | 20 |
| Table 4-10: Security Impact Shell Commands..... | 21 |
| Table 4-11: Security Impact Shell Variables..... | 24 |
| Table 4-12: Daemon Commands | 26 |
| Table 4-13: zOS Communications Server Daemons and Servers | 28 |
| Table 4-14: Restricted Network Services | 29 |
| Table 5-1: Interactive Users - ACF2..... | 33 |
| Table 5-2: Reserved Words and Prefixes..... | 36 |
| Table 6-1: Trusted Started Tasks | 37 |
| Table 7-1: Controls on z/OS System Commands | 38 |
| Table 7-2: Controls on JES2 System Commands | 48 |
| Table 8-1: Sensitive Utility Controls | 55 |
| Table 9-1: SMS Program Resources..... | 57 |
| Table 11-1: BMC IOA Resources | 71 |
| Table 11-2: BMC Control-D Resources..... | 73 |
| Table 11-3: BMC Control-M Resources..... | 80 |
| Table 11-4: BMC Control-O Resources..... | 82 |
| Table 11-5: BMC INCONTROL Resources Description..... | 87 |
| Table 11-6: CA 1 Command Resources | 92 |
| Table 11-7: CA 1 Function and Password Resources | 92 |
| Table 11-8: CA 1 Command Resources for ACF2..... | 94 |
| Table 11-9: CA 1 Function and Password Resources for ACF2..... | 94 |
| Table 11-10: CA 1 Command Resources for RACF..... | 95 |
| Table 11-11: CA 1 Function and Password Resources for RACF | 95 |
| Table 11-12: CA 1 Command Resources for TSS | 96 |
| Table 11-13: CA 1 Function and Password Resources for TSS | 97 |
| Table 11-14: CATALOG SOLUTIONS Resource List..... | 98 |
| Table 11-15: Category 1 Transactions for CICS TS 4.1 - 5.3..... | 101 |
| Table 11-16: Category 2 Transactions for CICS TS 4.1 - 5.3..... | 102 |
| Table 11-17: Category 3 Transactions for CICS TS 4.1 - 5.3..... | 106 |
| Table 11-18: CICS Category 4 COTS-Supplied Sensitive Transactions..... | 106 |
| Table 11-19: TSS FACILITY Initialization Parameters for CICS Region..... | 106 |
| Table 11-20: ACF2/CICS Parameters | 107 |

| | |
|--|-----|
| Table 11-21: CICS Systems Programmer's Worksheet..... | 108 |
| Table 11-22: CICS SPI Resources Table..... | 111 |
| Table 11-23: CICS SPI Resource Descriptions Table..... | 119 |
| Table 11-24: WebSphere MQ Command Security Controls..... | 122 |
| Table 11-25: WAS HFS Permission Bits..... | 124 |
| Table 11-26: SDSF SAF Resources..... | 125 |
| Table 11-27: SDSF SAF Resource Descriptions..... | 134 |
| Table 11-28: SDSF Server OPERCMDS Resources..... | 138 |
| Table 11-29: WebSphere MQ Queue Definition Authority SAF Resources..... | 139 |
| Table 11-30: Required GLOBAL Common Profile Segment Options..... | 139 |
| Table 11-31: Required SuperSess GLOBAL Profile Segment Options..... | 140 |
| Table 11-32: Advantage CA-Roscoe Access Attributes—External Security System..... | 140 |
| Table 11-33: CA ROSCOE Resources..... | 141 |
| Table 11-34: Vanguard Security Solutions Resources..... | 143 |
| Table 11-35: Vanguard Security Solutions Resources Description..... | 146 |
| Table 11-36: Compuware Abend-AID Resources..... | 151 |
| Table 11-37: BMC MAINVIEW Resources..... | 152 |
| Table 11-38: CA MIM Resource Sharing Resources..... | 158 |
| Table 11-39: NetView Resources..... | 160 |
| Table 11-40: Parameters for RACF IRRPWREX..... | 166 |

LIST OF FIGURES

| | Page |
|---|-------------|
| Figure 4-1: MVS HFS Datasets and Z/OS UNIX File Systems | 15 |

1. INTRODUCTION

1.1 Executive Summary

A core mission for the Defense Information Systems Agency (DISA) is to secure Department of Defense (DOD) Computing systems. The processes and procedures outlined in this Security Technical Information Guide (STIG) Checklist, when applied, will decrease the risk of unauthorized disclosure of sensitive information. Security is clearly still one of the biggest concerns for our DOD customers, for example, the war fighter.

This STIG Checklist was developed to enhance the confidentiality, integrity, and availability of sensitive DOD Automated Information Systems (AIS).

The requirements set forth in this document will assist Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), Network Security Officers (NSOs), and System Administrators (SAs) in support of protecting DOD Virtual Computing systems.

The Information Operations Condition (INFOCON) for the DOD recommends actions during periods when a heightened defensive posture is required to protect DOD computer networks from attack. The ISSO will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance. Password length and complexity given throughout this document must be adjusted as needed to comply with INFOCON guidance.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be [...] configured [...] consistent with applicable DOD cybersecurity policies, standards, and architectures.” The instruction tasks that DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

The use of the principles and guidelines in this STIG Checklist will provide an environment that meets or exceeds the security requirements of DOD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

It should be noted that DISA support for the STIG Checklists and Tools is only available to DOD Customers.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

| | DISA Category Code Guidelines |
|---------|--|
| CAT I | Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity. |
| CAT II | Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity. |
| CAT III | Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity. |

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at <https://cyber.mil/>. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from <https://public.cyber.mil/>.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA

implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<https://www.niap-ccevs.org/>) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/groups/STM/cmvp/>) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (<https://www.disa.mil/network-services/ucco>) IAW DODI 8100.04.

2. INTRODUCTION TO Z/OS

Addendum for z/OS-related update information - The purpose of this is to contain tables, etc., that the STIGs cannot accommodate at the current time.

Cross Ref Section:

- Use spreadsheet “Cross Ref of SRRAUDIT” during development, copy into addendum when complete.

Common Tables

2.1 z/OS Background

Operating System Security Design for most mainframe information systems deployed throughout DOD use the International Business Machines (IBM) z/OS operating system. Controls within z/OS have been developed and documented in IBM references to ensure operating system integrity is maintained.

Security mechanisms that provide MAC II Sensitive level controls for the z/OS operating environments are implemented by External Security Managers (ESMs). Previously these ESMs were known in the industry as Access Control Products (ACPs). In this document as well as the STIGs that are supported by this document the terms ESMs and ACPs will be referenced interchangeably.

ESMs currently in use throughout DOD are listed below:

- Access Control Facility 2 (ACF2) - Computer Associates (CA)
- Resource Access Control Facility (RACF) - IBM Corporation ¹
- TOP SECRET (TSS) - Computer Associates (CA)

To maintain the integrity of the site, the ESM must be properly installed and configured. Options specified during the installation and techniques involved in the administration of these products can reduce the assurance introduced into the individual operating environment. As a result, guidance is needed on how these products should be configured in the operational environment.

The System Authorization Facility (SAF) provides an installation with centralized control over system security processing through a system service called the MVS router. The MVS router provides a focal point for all products that provide resource management. Access to the MVS router is via the **RACROUTE** macro, which invokes the router program itself. The router in turn invokes the ESM to determine if authorization exists for the resource being tested.

¹ IBM has renamed RACF as the z/OS Security Server. In the interest of brevity, clarity, and continuity this document continues to refer to the product as RACF.

This concept provides a single interface that encourages the use of common functions across products and platforms. Products that interface via SAF calls can be protected with any of the three ESMs discussed in this document without modification of their interface code.

All new software acquired for or developed by DOD will fully utilize the SAF interface. Existing software that fails to utilize the SAF interface will be converted to do so where possible.

2.2 z/OS Dataset Types

z/OS operation data is held in many type of datasets that have a specific purpose in the system operation. Many of these dataset types require security protection to assure the confidentiality, integrity, and accessibility of the system. Major types are listed below:

Installation datasets primarily are system and product datasets that contain modules or data required to place a system/product into operation on the mainframe. The files are usually shipped with the operating system/product and for the most part are unmodified by the site. They are usually in one central location and are required for system/product maintenance. The datasets are generally the basis for the system/product.

Started Task (STC) datasets are read, controlled, created, and/or sustained by the STC. Since the system/application can require elevated access, it is important to protect these datasets from inappropriate use.

User datasets require some level of interaction with a user. Since there are differing levels of users in the z/OS arena, i.e., systems programmer users, production control users, end users, etc., security requirements should be defined according to those levels.

Program datasets are specific datasets necessary for application operation. These datasets can contain operation-sensitive information and should be appropriately protected.

2.3 z/OS Additional Access/Logging Restrictions

Data set and Resource access documented in the vulnerabilities establishes the basic access requirements. At the ISSO's discretion, additional control may be implemented to provide additional restrictions. An example of additional controls would be the use of program pathing to restrict access to a data set or resource when a specific program and/or program mask is used.

Data set and Resource logging requirements documented in the vulnerabilities specify where successful access logging starts. By default, all violations to access a data set and/or resource will require that logging be performed.

3. Z/OS PRIVILEGED USERS

Due to its architecture and its structure, the mainframe, definition of a Privileged user will refer to any users or tasks that require a level of access that provides for Control, monitoring, or administration of the Mainframe platform.

Roles commonly known as:

System Programmers
System Security Administrators
Operators
Tape Librarians
Storage Administrators
Automation Specialist
Schedulers
Application Support Teams (Domain level)
Any team member who has physical access to the data center and data storage

Members of these teams will be granted special privileges and special accesses that will be controlled by the Systems ESM. **For the purpose of references in the z/OS STIG Checklist, the individuals listed above will refer only to personal under the management and control of the Data Center.** These individuals will be assigned by and be the responsibility of the Site ISSM.

For example, references to System Programmers in the z/OS STIG Checklist will be as follows:

For the purpose of the z/OS STIG Checklist, a Systems Programmer will be defined as those individuals who are responsible for the z/OS systems software and z/OS systems products. They are the individuals who will have Level 1 responsibility to keep the z/OS Operating System software and its associated System Software Products functioning in a stable and well-maintained status and will be under management and control of the data center. These individuals will be assigned by the Site ISSM to perform these duties.

System programmers include such roles/functions as: OS System Programmer, DASD or Storage Administrators, CICS System Programmer, MQ Series System Programmer, Communications System Programmer, Database System Programmer (including not limited to IDMS, IMS, DB2, ADABAS, ORACLE, etc. - DBAs who install executive software on the Mainframe).

The following table identifies which users or types of users can be identified in the specified Authorized User group. These Authorized User groups are specified throughout this document.

Table 3-1: Authorized User Groups

Use this table to determine and/or define a site's user groups. These should be helpful when establishing site's specific user groups.

| User Group | Description |
|------------|---|
| APPBAUDT | Application Production Batch Userids. Userids that maintain and develop application programs for the customer base through batch submissions. |
| APPDAUDT | Application Development Programmers. Users that maintain and develop application programs for the customer base. |
| APPSAUDT | Application Production Support Team members. |
| AUDTAUDT | Auditors, whether they are System, Security, or other. This can be any user that performs any type of auditing on the system. These users can be an actual person, batch user, or STC. |
| AUTOAUDT | Automated Operation STCs/Batch Jobs. STC and/or Batch users that perform any type of automated operations control on the system. |
| BMCADMIN | INCONTROL Admins/Owners of CONTROL-D/M/O. Installers and system administrators for Control-D/M/O. |
| BMCUSER | INCONTROL Users of CONTROL-D/M/O. |
| CHGOWNER | Users authorized to issue the chown in UNIX. |
| CICBAUDT | CICS Batch Programs. |
| CICDAUDT | CICS Developers. Users who create and maintain CICS programs and routines. |
| CICSAUDT | CICS Started Task. |
| CICSDEF | CICS regions default user ids (DFLTUSER). |
| CICUAUDT | CICS Utils (CONTROLO, BatIDs via CONTROLM, MAINVIEW). |
| CONSOLES | The System Console user ids. |
| DABAAUDT | Database Administrators. Users that maintain and administer the databases and the database product software on the system. These users also perform backup and recovery of the databases. |
| DAEMAUDT | UNIX Daemon user ids. |
| DASBAUDT | DASD batch, jobs that perform DASD Backups, Migrate. Batch and/or STC users that perform DASD maintenance functions. |
| DASDAUDT | DASD Administrators. Users that administers DASD functions on the entire operating system. These users can perform a complete backup and recovery of the DASD farm. |
| DPCSAUDT | Decentralized Prod Cntl and Sched personnel. |
| DUMPAUDT | STCs/Batch ids that perform Dump processing. STC and/or Batch users that generate system-level dumps. |
| EMERAUDT | Emergency TSO logon ids. |
| FTPUSERS | FTP only interactive users. |
| MCATBAT | System Programmer batch ids that perform elevated system and user catalog functions not granted to regular users. |
| IOABAUDT | Special IOA user IDs, such as long-running started tasks, or specific system jobs. |
| MICSADM | MICS Administrators. |
| MICSUSER | MICS End Users. |

| User Group | Description |
|------------|--|
| MQSAAUDT | MQ Series Administrators. Users that define and administer the WebSphere MQ environment on the system. |
| MQSDAUDT | Decentralized MQ Series Administrators. Users that define and administer the WebSphere MQ environment on the system at customer site. |
| MVREAD | Mainview users that require read only mode. |
| MVUPDT | Mainview users that require some update functions. |
| OMVSAUDT | The OMVS started task kernel. |
| OPERAUDT | Operations personnel. Users that have direct access to the hardware components of the operating system. |
| PARMSTC | Users that have READ access justification via ISSO. These users are STCs and/or batch jobs that obtain their configuration settings from the Logical parmlib concatenation. |
| PCSPAUDT | Production Control and Scheduling personnel. Users that have domain-level control of all scheduling of batch processes on the system. Not users that schedule specific application batch jobs. |
| PRODAUDT | Production Started Tasks and batch logon ids. |
| ROSCAUTH | ROSCOE Master and Maintenance IDs. |
| SECAAUDT | Security Administrators. Domain Level I security administrators; these users have total control over the administration of the ESM. |
| SECBAUDT | Security batch, jobs that perform ESM maintenance. Batch and/or STC users that perform security maintenance. |
| SECDAUDT | Decentralized Security Administrators. |
| SERVAUDT | UNIX Server user ids. |
| SMFBAUDT | STCs/BATCH ids that perform SMF dump processing. |
| STCGAUDT | STCs ids that perform GTF processing. |
| SUPRAUDT | User ids that require BPX.SUPERUSER. |
| SYSCAUDT | CICS Systems Programmers. |
| SYSPAUDT | Systems Programmers or Systems Administrators. Users that perform installation and maintenance on the operating system and vendor software. |
| TAPEAUDT | Tape Librarians, CA1 Prod Batch Jobs, and CA1 STCs. Users that perform control, initialization, and maintenance of a systems tape library. |
| TSTCAUDT | Trusted Started Tasks users. See list in TRUSTED STARTED TASKS in the z/OS STIG Addendum. |
| WEBAAUDT | Web Server Administrators. |

4. Z/OS UNIX SYSTEM SERVICES

4.1 z/OS UNIX System Services Background

z/OS UNIX System Services, abbreviated by IBM as z/OS UNIX, provides a UNIX environment to z/OS users. It is now a base component of the z/OS operating system, conforms to the XPG4 UNIX 1995 standard (with UNIX 98 elements), and offers services designed to support applications written to open systems standards. z/OS UNIX also provides z/OS users the traditional UNIX structure for data storage through the Hierarchical File System (HFS)/zSeries File System (zFS). Finally, z/OS UNIX supports the UNIX User Identifier (UID) and Group Identifier (GID) concepts that establish identity in the UNIX environment.

In z/OS UNIX, security is handled, in part, through the UID and GID constructs that identify users and groups. This security impacts file access and process (e.g., z/OS task) control. While it is possible in some environments for multiple users to be assigned the same UID, this does not provide a desirable level of security.

z/OS UNIX provides an operating environment that can host many services such as File Transfer Protocol (FTP) and z/OS UNIX Telnet servers. In addition, z/OS components such as Communications Server provide support to z/OS UNIX. This section of this document is intended to describe the security considerations for the z/OS UNIX environment and does not cover these supporting and supported components in appropriate detail. Please check other sections of this document and the pertinent vendor documentation for security considerations for these other components.

4.2 z/OS UNIX General Considerations

Because of the scope of z/OS UNIX and its difference from the traditional MVS environment, there are a number of considerations that must be addressed to understand the security implications. In this section, security considerations for the following areas are discussed:

- User Identity - UID and GID Assignment
- Data Storage - HFS/zFS Directories and Files
- Interactive Environment - The UNIX Shell
- Background Processes - Daemons and Servers
- Miscellaneous Considerations

These considerations are discussed in general to explain the z/OS UNIX environment. This background is used when discussing the specific controls that are used to implement security policy.

Table 4-1: General FACILITY Class BPX Resources

Referenced by: ZUSS0021

| General FACILITY Class BPX Resources | |
|---|--|
| Resource Name | Description/Notes |
| BPX.DAEMON | Allows a daemon to use the seteuid, setuid, setreuid, and spawn services. |
| BPX.DEBUG | Allows a user to use ptrace (via dbx) to debug programs that run with APF authority or with BPX.SERVER authority. |
| BPX.FILEATTR.APF | Allows a user to set the APF-authorized attribute in an HFS file. |
| BPX.FILEATTR.PROGCTL | Allows a user to set the program-controlled attribute in a HFS file. This attribute is required, in most cases, for all programs executed by daemons or servers. |
| BPX.JOBNAME | Allows a user to set jobnames using the _BPX_JOBNAME environment variable or the inheritance structure on spawn. |
| BPX.SAFFASTPATH | Enables SAF fastpath support. This means that successful security checks are not audited. No access list is needed; the existence of the profile enables the function. |
| BPX.SERVER | <p>READ: Allows the server to establish a thread-level security environment for its clients. Access control decisions are based on the server's userid and the client's userid unless the server specifies a password on the service invocation.</p> <p>UPDATE: Allows the server to establish a thread-level security environment for its clients. Access control decisions are based only on the client's userid.</p> <p>The pthread_security_np (create/delete security environment) and the auth_check_resource_np (resource authorization checking) services are used. Also see the BPX.SRV.userid profile description.</p> |

| General FACILITY Class BPX Resources | |
|---|--|
| Resource Name | Description/Notes |
| BPX.SMF or BPX.SMF. <i>type.subtype</i> | <p>Allows permitted user access to write an SMF record or to test if an SMF type or subtype is being recorded.</p> <ul style="list-style-type: none"> • The BPX.SMF profile grants the permitted user the authority to write or test for any SMF record that is being recorded. The program-controlled attribute is not required if BPX.SMF is used • For more granular access to writing SMF records BPX.SMF.<i>type.subtype</i> allows a permitted user the authority to write or test only the SMF record of the specific type and subtype contained in the FACILITY class profile name. <p>Note: BPX.SMF must not be permitted to regular interactive usersids.</p> |
| BPX.STOR.SWAP | Allows a user to make address spaces non-swappable or swappable. |
| BPX.SUPERUSER | Allows a user to switch to superuser authority (i.e., effective UID of “0”). |
| BPX.WLMSEVER | <p>Allows a user to access Work Load Manager (WLM) server functions and C language WLM interfaces. These functions and interfaces are commonly used by server applications.</p> <p>Also see the BPX.SERVER profile description.</p> |

Table 4-2: UNIXPRIV Class Resources

Referenced by: ZUSS0023

| UNIXPRIV Class Resources | |
|----------------------------------|--|
| Resource Name | Description/Notes |
| CHOWN.UNRESTRICTED. ² | <p>Allows all z/OS UNIX users to transfer ownership for files they own to any UID or GID on the system.</p> <p>No access list is needed; the existence of the profile enables the function. Therefore, the resource will not be defined.</p> |

² The CHOWN.UNRESTRICTED profile defeats a basic file ownership protection, and must not be defined unless justified and documented to the ISSO.

| UNIXPRIV Class Resources | |
|-------------------------------|--|
| Resource Name | Description/Notes |
| SHARED.IDS (RACF only) | Allows users to assign UID and GID values that are not unique. To specify non-unique UID or GID users must specify the SHARED keyword in the RACF AG, AU, ALG, and ALU commands. These users must have the SPECIAL attribute or at least READ authority to the resource. Therefore, resource will be defined with no access given to users. |
| SUPERUSER.FILESYS | READ: Allows the user to read any HFS file and to read or search any HFS directory. UPDATE: Allows the user to write to any HFS file and includes <i>read</i> access. CONTROL: Allows user to write to any HFS directory and includes <i>update</i> access. Note: Allows access only to local HFS files, not to NFS files. |
| SUPERUSER.FILESYS.CHANGEPERMS | READ: Allows a user/group to do a CHMOD to any file. |
| SUPERUSER.FILESYS.CHOWN | READ: Allows the user to change the ownership of any file. |
| SUPERUSER.FILESYS.MOUNT | READ: Allows the user to mount a file system with the nosetuid option and to unmount a file system mounted with the nosetuid option. UPDATE: Allows the user to mount a file system with the setuid option and to unmount a file system mounted with the setuid option. |
| SUPERUSER.FILESYS.QUIESCE | READ: Allows the user to quiesce and unquiesce a file system mounted with the nosetuid option. UPDATE: Allows the user to quiesce and unquiesce a file system mounted with the setuid option. |
| SUPERUSER.FILESYS.PFSCtl | READ: Allows the user to use the pfscctl() (physical file system control) callable service. |
| SUPERUSER.FILESYS.VREGISTER | READ: Allows a server to use the v_reg() callable service to register as a virtual file system (VFS) file server. |
| SUPERUSER.IPC.RMID | READ: Allows the user to issue the ipcrm command to release IPC (Interprocess Communication) resources. |
| SUPERUSER.PROCESS.GETPSENT | READ: Allows the user to use the w_getpsent callable service to receive process status data for any process. |

| UNIXPRIV Class Resources | |
|--------------------------|---|
| Resource Name | Description/Notes |
| SUPERUSER.PROCESS.KILL | READ: Allows the user to use the kill() callable service to send signals to any process. |
| SUPERUSER.PROCESS.PTRACE | <p>READ: Allows the user to use the ptrace() function through the dbx debugger to trace any process. Also allows users of the ps command to output information on all processes.</p> <p>Note: Authorization to FACILITY class resource BPX.DEBUG is required to trace processes that run with APF authority or BPX.SERVER authority.</p> |
| SUPERUSER.SETPRIORITY | READ: Allows the user to increase that user's own priority. |

Table 4-3: MVS Data Sets with z/OS UNIX Components

Referenced by: ZUSS0032

| MVS Data Sets with z/OS UNIX Components | | |
|--|-------------------------|---|
| Data Set Name/Mask | Maintenance Type | Function |
| SYS1.ABPX* | Distribution | IBM z/OS UNIX ISPF panels, messages, tables, clists |
| SYS1.AFOM* | Distribution | IBM z/OS UNIX Application Services |
| SYS1.BPA.ABPA* | Distribution | IBM z/OS UNIX Connection Scaling Process Mgr. |
| SYS1.CMX.ACMX* | Distribution | IBM z/OS UNIX Connection Scaling Connection Mgr. |
| SYS1.SBPX* | Target | IBM z/OS UNIX ISPF panels, messages, tables, clists |
| SYS1.SFOM* | Target | IBM z/OS UNIX Application Services |
| SYS1.CMX.SCMX* | Target | IBM z/OS UNIX Connection Scaling Connection Mgr. |

4.3 z/OS UNIX User Identity

Within UNIX systems, users are assigned a user name and password that allow identification and authentication when the system is accessed. Each user is also assigned a numeric identifier that is known as the UID. Users are members of one or more groups; each of these groups has a name and a numeric identifier that is known as the GID. While it is possible in some environments to assign multiple users the same UID, this is not done where meaningful security is desired.

There are no software-specific UID or GID numbers, with one exception. If a user is assigned a UID value of 0 (zero), the user has *superuser* status and effectively bypasses all security checks. There are a limited number of instances where superuser status is actually needed, and z/OS UNIX provides some security resources that can be used to further limit the need to assign UID (0) to users.

During a UNIX shell session or during the execution of commands with certain attributes, it is possible for a user to temporarily use a different UID or GID value than what was assigned. The userid defined to the security system and used at system sign-on is referred to as the real ID. The temporary userid used for a specific period or process is referred to as the effective ID. For this reason, it is important to check the effective ID when researching access control issues.

4.4 z/OS UNIX User Identity

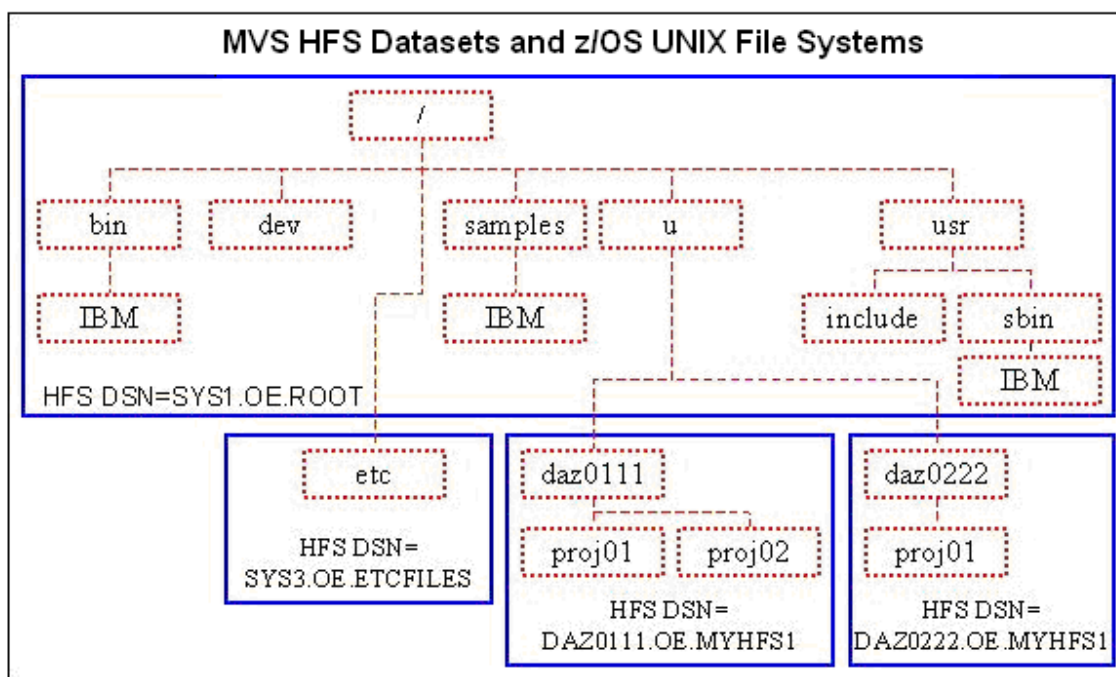
This section discusses the considerations related to data storage in the z/OS UNIX environment. These considerations include the logical and physical structures, file access permissions, extended attributes for executable files, and audit attributes. Understanding these considerations is important to setting and maintaining data and command security.

Hierarchical File System (HFS)/zSeries File System (zFS) is a tree structure consisting of multiple file systems. A file system is a logical collection of directories and files. The highest-level directory in the hierarchy is the root directory; it is often kept in a file system with only a few other directories. Each file system is made available by a process known as mounting the file system. It is mounted at a *mount point* that is actually just a directory in the higher-level file system.

The entire file hierarchy is made up of a collection of HFS/zFS data sets. Each physical HFS/zFS data set is actually a mountable file system. This means that it can be attached to the HFS/zFS tree at a mount point that is in the root directory or at a mount point further down in the hierarchy. Each HFS/zFS data set needs data set access rules defined to protect it.

The following diagram illustrates the relationship between MVS HFS/zFS data sets and z/OS UNIX File Systems. This is an example with four MVS data sets (SYS1.OE.ROOT, SYS3.OE.ETCFILES, DAZ0111.OE.MYHFS1, and DAZ0222.OE.MYHFS1) corresponding to four z/OS UNIX file systems (*root*, *etc*., *daz0111*, *daz0222*).

Figure 4-1: MVS HFS Datasets and Z/OS UNIX File Systems



To provide granularity in access control, there are three sets of permission bits to accommodate three categories of users whose access can be individually controlled:

- Owner** - The user whose UID matches the UID in the FSP
- Group** - A member of the group whose GID matches the GID in the FSP
- Other** - Anyone else

When permission bits are displayed in command output or used as command operands, they sometimes appear as a string of alphabetic characters and sometimes as a string of octal digits that correspond to these categories. For example, a file can have permissions set to “`rwX r-- ---`”, where “`rwX`” applies to the owner, “`r--`” to the group, and “`---`” to other. This would be expressed digitally as 740 where 7 applies to the owner, 4 to the group, and 0 to other.

The following tables show the permission bits, their alphabetic symbolic notation, their octal values, and their meaning:

Table 4-4: Permission Bits

| Permission Bits | | | |
|-----------------|-------------------|-------------|--|
| Permission | Symbolic Notation | Octal Value | Meaning for File or Directory |
| Read | r | 4 | Directory: Allows the user to read, but not search, contents. File: Allows the user to read or print contents. Note: Running shell scripts requires read and execute. |
| Write | w | 2 | Directory: Allows the user to change the directory, adding or deleting members. File: Allows the user to change the file, adding or deleting data. |
| Execute | x | 1 | Directory: Allows the user to search the directory. File: Allows the user to run the executable program. Note: Running shell scripts requires read and execute. |
| no access | - | 0 | No access allowed. |

There are additional permission bits that are used for special purposes. When in use, these bits may be displayed alphabetically in the *execute* position, with lower case indicating that the execute bit and special bit are both on. When displayed or used in a command in digital form, the value for these bits appears as an additional first digit in the string.

Table 4-5: Special Permission Bits

| Special Permission Bits | | | |
|-----------------------------|-------------------|-------------|--|
| Permission | Symbolic Notation | Octal Value | Meaning for file or Directory |
| set-user-ID set-group-ID | s/S | 4 2 | Used for an executable file, sets the effective userid and/or group ID of the user process executing the program to that of the file being executed. Allows a program to have temporary access to files (or potentially commands) that are not normally accessible. |
| sticky bit | t/T | 1 | Directory: Allows only the file owner, directory owner, or superuser to delete or rename files. File: Causes the search for an executable in the current STEPLIB, link pack area, or link list (the data in the HFS/zFS file is not loaded as the program). |

These permissions are combined as required to allow the desired access.

The chown, chgrp, and chmod shell commands are provided. Refer to *z/OS UNIX Interactive Environment - The UNIX Shell*, for information on these commands.

Note: The ACF2 and TOP SECRET ESMs offer an option called CA SAF HFS/zFS security. If this option is enabled, file mode checking is bypassed in favor of access rules written for the ESM. However, because CA SAF HFS/zFS can be disabled, the standard UNIX file permissions must be maintained for system sensitive directories and files.

z/OS UNIX adds the feature of *extended attributes* that are meaningful for executable files. These extended attributes include the following:

Table 4-6: Extended Attributes

| Extended Attributes | | |
|---------------------|-------------------|--|
| Extended Attribute | Symbolic Notation | Description |
| APF-authorized | a | Executable program acts as if loaded from an APF-authorized MVS library. |
| Program-controlled | p | Executable program acts as if defined to program control in the ESM. |
| Shared | s | Executable foreground program runs in the same MVS address space as the user's z/OS shell. Note: This bit is on as the default for all executable files. |

To maintain the extended attributes, the `extattr` shell command is provided. Refer to *Section z/OS UNIX Interactive Environment - The UNIX Shell*, in this document for information on this command.

z/OS UNIX adds a security extension in the form of audit attributes for files or directories. Audit attributes determine whether accesses to the object are audited by the System Authorization Facility (SAF) interface. The attributes can be set to audit successful access attempts (**s**), audit failed access attempts (**f**), audit all accesses (**a**), or do not audit access (**-**). To allow for both user and system auditing functions, there are two sets of audit attributes to accommodate two categories - user-requested and auditor-requested.

Within each category of audit attributes, the audit controls are as follows:

Table 4-7: Audit Bits

| Audit Bits | | |
|------------|----------------|--|
| Audit Flag | Alpha Notation | Description |
| Read | s/f/a/- | Audit attempts for <i>read</i> access |
| Write | s/f/a/- | Audit attempts for <i>write</i> access |
| Execute | s/f/a/- | Audit attempts for <i>execute</i> access |

To maintain the audit attributes, the **chaudit** shell command is provided. Refer to *z/OS UNIX Interactive Environment - The UNIX Shell*, in this document for information on this command.

Table 4-8: System Directory Security Settings

Note: Any Directory that uses AUTOMOUNT, does not require the specified settings.

Referenced by: ZUSS0016, ZUSS0034

| System Directory Security Settings | | | |
|------------------------------------|-----------------|-----------------|--|
| Directory | Permission Bits | User Audit Bits | Function |
| / [root] | 755 | faf | Root level of all file systems. Holds critical mount points. |
| /bin | 1755 | fff | Shell scripts and executables for basic functions |
| /dev | 1755 | fff | Character-special files used when logging into the OMVS shell and during C language program compilation. Files are created during system IPL and on a per-demand basis. |
| /etc | 1755 | faf | Configuration programs and files (usually with locally customized data) used by z/OS UNIX and other product initialization processes |
| /lib | 1755 | fff | System libraries including dynamic link libraries and files for static linking |
| /samples | 1755 | fff | Sample configuration and other files |
| /tmp | 1777 | fff | Temporary data used by daemons, servers, and users. Note: /tmp must have the sticky bit on to restrict file renames and deletions. |
| /u | 1755 | fff | Mount point for user home directories and optionally for third-party software and other local site files |
| /usr | 1755 | fff | Shell scripts, executables, help (man) files and other data. Contains sub-directories (e.g., lpp) and mount points used by program products that may be in separate file systems. |
| /var | 1775 | fff | Dynamic data used internally by products and by elements and features of z/OS UNIX. |

Note: The sticky bit is set on to restrict file renames and file deletions or subdirectory deletions.

In addition, the following guidelines must be followed:

All directories (such as `/tmp`) with the *write* permission set for the other group must also have the sticky bit set.

Any directory (such as `/tmp`) with the *write* permission set for the other group must not contain any files with the following bits set:

- set-user-ID permission
- set-group-ID permission
- APF-authorized extended attribute
- Program control extended attribute

Table 4-9: System File Security Settings

Referenced by: ZUSS0035, ZUSS0016

| System File Security Settings | | | |
|---|-----------------|-----------------|--|
| File | Permission Bits | User Audit Bits | Function |
| <code>/bin/sh</code> | 1755 | faf | z/OS UNIX shell Note: <code>/bin/sh</code> has the sticky bit on to improve performance. |
| <code>/dev/console</code> | 740 | fff | The system console file receives messages that may require System Administrator (SA) attention. |
| <code>/dev/null</code> | 666 | fff | A null file; data written to it is discarded. |
| <code>/etc/auto.master</code> and any <i>mapname</i> files | 740 | faf | Configuration files for automount facility |
| <code>/etc/inetd.conf</code> | 740 | faf | Configuration file for network services |
| <code>/etc/init.options</code> | 740 | faf | Kernel initialization options file for z/OS UNIX environment |
| <code>/etc/log</code> | 744 | fff | Kernel initialization output file |
| <code>/etc/profile</code> | 755 | faf | Environment setup script executed for each user |
| <code>/etc/rc</code> | 744 | faf | Kernel initialization script for z/OS UNIX environment |
| <code>/etc/steplib</code> | 740 | faf | List of MVS data sets valid for set-user-ID and set-group-ID executables |
| <code>/etc/tablename</code> | 740 | faf | List of z/OS userids and group names with corresponding alias names |

| System File Security Settings | | | |
|---|-----------------|-----------------|---|
| File | Permission Bits | User Audit Bits | Function |
| /usr/lib/cron/at.allow /usr/lib/cron/at.deny | 700 | faf | Configuration files for the at and batch commands |
| /usr/lib/cron/cron.allow /usr/lib/cron/cron.deny | 700 | faf | Configuration files for the crontab command |

Some of the files listed above (e.g., /etc/steplib) are not used in every configuration. While the absence of a file is generally not a security issue, the existence of a file that has not been properly customized can often be an issue. Therefore, all directories and files that do exist must have the specified permission and audit bit settings.

4.5 z/OS UNIX Interactive Environment – The UNIX Shell

The z/OS UNIX shell is a command processor that allows users to do the following:

- Invoke shell commands or utilities
- Write shell scripts using the shell programming language
- Run shell scripts and C-language programs in the foreground, in the background, or in batch

This section describes the security considerations for the z/OS UNIX shell, including shell commands, shell access, interoperability between the shell and TSO/E, and built-in shell variables.

As with other interactive environments, there are certain commands available in the z/OS shell that have security implications. Most of these commands impact data security by altering security attributes for a directory or file; others impact system operation and user privileges. The most important of these commands are as follows:

Table 4-10: Security Impact Shell Commands

| Security Impact Shell Commands | | |
|--------------------------------|--|--|
| Command | Description | User Restrictions |
| at ³ | Allows a user to run a series of commands at a specified later time, under control of the cron daemon. | Can be used by the superuser or users listed in the /usr/lib/cron/at.allow file. |
| automount | Configures the automount facility that mounts file systems at time of access. | Can only be used by a superuser. Started from /etc/rc. |

³ The at, batch, and crontab commands are used to manipulate the functions of the cron daemon. The default specified environment disables cron. The information is included here for the sake of completeness.

| Security Impact Shell Commands | | |
|--------------------------------|--|--|
| Command | Description | User Restrictions |
| batch | Allows a user to run a series of commands later when the system is not busy, under control of the cron daemon. | Same as at command. |
| chaudit | Changes the audit attributes of files or directories. Audit attributes determine whether accesses to a file are audited by SAF. | Can only be used by the file owner or a superuser for non-auditor-requested audit attributes. |
| chgrp | Changes the GID for the specified file or directory. | By default, can be used only by the file owner or a superuser. The file owner must be a member of the group the file or directory is being changed to. |
| chmod | Changes the file modes (permission bits) for the specified file or directory. | By default, can be used only by the file owner or a superuser. |
| chown | Changes the UID and optionally the GID for the specified file or directory. | By default, the UID can only be changed by a superuser. Changes to the GID follow the rules for the chgrp command. |
| chroot | Changes the root directory to that specified in the command. | Can only be used by a superuser or a user with access to the BPX.SUPERUSER resource. |
| crontab | Allows a user to schedule a series of commands to be run on a regular basis, under control of the cron daemon. | Can be used by the superuser or users listed in the /usr/lib/cron/cron.allow file. |
| extattr | Sets, resets, and displays the extended attributes of executable files. Extended attributes include APF authorization, program control, and shared address space use. | Can only be used by the file owner or a superuser. The APF attribute requires access to the BPX.FILEATTR.APF resource. The program control attribute requires access to the BPX.FILEATTR.PROGCTL resource. |

| Security Impact Shell Commands | | |
|--------------------------------|--|---|
| Command | Description | User Restrictions |
| su su userid | Starts a new shell with the security attributes of the superuser or a different user. When a different user is specified, the MVS identity is changed and MVS data set access is changed to that of the new MVS user. When issued as superuser (i.e., UID (0)) and BPX.DAEMON is defined, userid is switched to the value in BPXPRMxx SUPERUSER. | Access to superuser status requires access to the BPX.SUPERUSER resource. Access to a different user requires that user's password or access to the BPX.SRV.userid resource. |
| umask | Sets the file-creation permission mask. The mask specifies the default permissions that are not to be allowed when a file is created. | Not restricted |

As indicated, security for each command depends on resource privileges that are accessible to the user. The default restrictions for these commands can change according to options available with the installed ESM. If CA SAF HFS/zFS security is enabled, commands that may have required superuser authority or access to UNIXPRIV class resources are controlled by BPX.CAHFS resources instead.

Access to the z/OS shell is possible from multiple origins:

TSO/E OMVS command - TSO/E users can enter the OMVS command to access the shell via a 3270 terminal interface.

rlogin - Users from another system can use the rlogin command to access the shell via an asynchronous terminal interface. The use of rlogin access is not permitted.

telnet - Users from another system can use the telnet command to access the shell via an asynchronous terminal interface.

z/OS Communication Server with an RS/6000 system - Users of terminals attached to serial ports on an RS/6000 that is connected to the host can log on directly via an asynchronous terminal interface.

While there are no implicit security implications to the access origin point, control of these facilities in their own environment may be desirable. There is a high degree of interoperability between MVS TSO/E and the z/OS shell. The following capabilities are provided:

Data can be moved between MVS data sets and files in a z/OS UNIX HFS/zFS file system.

Some TSO/E commands manipulate the HFS/zFS environment to perform tasks such as creating directories and mounting file systems.

TSO/E commands can be issued from the shell command line, from a shell script, or from a program.

MVS job control language (JCL) can include shell commands. The BPXBATCH utility provides this capability. For examples, refer to *The BPXBATCH Utility* in IBM's *z/OS UNIX System Services User's Guide* document, and *Appendix C. Running Shell Scripts or Executable Files under MVS Environments* in IBM's *z/OS UNIX System Services Command Reference*.

HFS/zFS files can be edited in TSO/E through ISPF/PDF or in the z/OS shell through editors such as ed, sed, and vi.

Extensions to the REXX language allow REXX programs to access callable services in the TSO/E, batch, shell, or C program environments.

The primary security implication resulting from these capabilities is that file and command access is based on the value of the z/OS userid and/or the z/OS UNIX UID and GID that are in effect at the time of file access or command execution.

Behavior within the z/OS shell can be altered by the values of data from built-in shell variables. Variables that have security implications are as follows:

Table 4-11: Security Impact Shell Variables

| Security Impact Shell Variables | | |
|---------------------------------|--|---|
| Variable | Description | Implication |
| HOME | The user's home directory set from values specified by the security system. | The user's home directory contains that user's personal files and scripts that establish any unique environment settings. |
| LOGNAME | The user's logon name, set from values specified by the security system. | Child processes, by default, receive names based on LOGNAME. |
| SHELL | The full pathname of the shell program set from values specified by the security system. | An invalid shell program name would prevent system access. A compromised program could reduce system security. |
| PATH | The list of directories the system searches to find executable commands. | An improper sequence of directories could cause the wrong version of a program to be executed. |

| Security Impact Shell Variables | | |
|---------------------------------|--|--|
| Variable | Description | Implication |
| STEPLIB | For value = current: Currently, active TASKLIB, STEPLIB, or JOBLIB allocations are passed on. For value = none: No STEPLIB to be used in the search order. For value = <i>dsn1:dsn2:dsn3</i> : Use the specified, cataloged , user-accessible MVS load libraries. Default value = current. | Executables with the set-user-ID or set-group-ID bit set can only use STEPLIB data sets specified by the STEPLIBLIST parameter in BPXPRMxx. |
| _BPX_ACCT_DATA | The account data to be used for processes being created. | Could require additional access permissions if the use of account data is secured. |
| _BPX_JOBNAME | The MVS jobname to be used for processes being created. | Requires superuser authority or access to BPX.JOBNAME to be effective. Allows a user/process to start a child process that, by virtue of name, may have other security issues. Note: When the _BPX_JOBNAME variable is not set, processes created by fork or spawn are assigned jobnames consisting of the userid followed by a number (1-9). |
| _BPX_USERID | The z/OS user identity to be used for processes being created, effective only for users who have authority for the setuid() function. | Requires access to the BPX.DAEMON resource to be effective. Allows a user/process to start a child process using a different security context. |

4.6 z/OS UNIX Background Processes - Daemons and Servers

z/OS UNIX supports the execution of processes in the background. Daemons and servers are distinguished from other background processes by the duration of execution and the privileges used. z/OS UNIX daemons and servers correspond in function to MVS started tasks.

Note: z/OS UNIX supports two levels of security - UNIX and z/OS UNIX. UNIX-level security exists where the userids for daemons and servers are defined with a UID of "0" (i.e., superuser status) and the BPX.DAEMON and BPX.SERVER security resources are not defined. z/OS UNIX-level security exists where the BPX.DAEMON or BPX.SERVER security resources are

defined. This level provides a higher degree of security. z/OS UNIX-level security must be configured so that the enhanced security is available.

A daemon is a background process that operates continuously or periodically to provide a system service. Daemons may be started at system initialization or in response to some event. Daemons must be assigned a userid with a UID of “0” (i.e., superuser authority) and have the appropriate permission to the BPX.DAEMON security resource. A daemon can use the seteuid, setuid, setreuid, or spawn (with change in userid requested) service to execute work using the security context of a user.

A server is a background process that operates continuously or periodically to provide an application service required by a client. Servers are typically started when the service they provide is required. Servers must have the appropriate permission to the BPX.SERVER security resource. A server can use the pthread-security-np service to create task-level security environments. If the server processes user requests without the client (e.g., user) password, the server acts as a surrogate and must have the appropriate permission to the BPX.SRV.userid (where *userid* is the z/OS userid) security resource.

The security setup requirements for daemons and servers are as follows:

The daemon or server must be assigned a userid. For daemons, the userid must be assigned a UID of “0”.

The assigned userid must have the appropriate access to the BPX.DAEMON or BPX.SERVER security resource and to the BPX.SRV.userid resource(s) as required.

The ESM's Program Control feature must be active.

All programs to be loaded into the address space must be marked as controlled programs (i.e., defined to Program Control). Programs in HFS/zFS files must have the program-controlled extended attribute bit set.

Daemons are usually started in scripts executed at system initialization. These scripts contain commands that set up the environment and start the daemon. The commands used to start commonly used z/OS UNIX daemons include the following:

Table 4-12: Daemon Commands

| Daemon Commands | | |
|-----------------|--|--------------------------|
| Command | Description | Startup |
| cron | Runs commands scheduled through at, batch, and crontab at specified dates and times. | At system initialization |
| inetd | Provides Internet service management for a network. | At system initialization |

| Daemon Commands | | |
|-----------------|---|---|
| Command | Description | Startup |
| lm | Starts the logon monitor daemon that starts the logon process for logons initiated by Outboard Communications Server (OCS). | At system initialization |
| rlogind | Validates remote logon (rlogin) requests. | By inetd |
| uucico | Processes uucp and uux file transfer requests. | By other processes including cron, uucpd, uucp, and uux |
| uucpd | Invokes uucico for TCP/IP connections from remote uucp systems. | By inetd |
| uuxqt | Runs commands from remote systems. | By uucico or cron |

Unless justified and documented to the ISSO, all of the daemons on this list, except for the inetd daemon, must be disabled. This policy improves system security by reducing the number of common targets of system attacks.

There are daemons and servers that are specific to the z/OS Communications Server. These daemon/servers require additional resource access to start and stop. Several of these are listed below with their functions:

ADNR - The automated domain name registration (ADNR) application is a function that dynamically updates name servers with information about sysplex resources in near real time. As resources in the sysplex become available, Domain Name System (DNS) resource records are added to one or more name servers. As those resources become unavailable, the corresponding DNS resource records are removed from the name server. Clients that connect to sysplex resources using DNS names have a greater likelihood of connecting to an available resource in the sysplex. ADNR also removes the administrative burden of manually configuring and updating a name server to represent sysplex resources.

DCAS - The Digital Certificate Access Server (DCAS) (opens new browser) is a TCP/IP server application that runs on OS/390 V2R10 and later (z/OS included). It interfaces with a Security Access Facility (SAF)-compliant server product to assist with express logon services such as Web Express Logon. In this scenario, this SAF-compliant server product is IBM Resource Access Control Facility (RACF) (opens new browser).

LBADV - The z/OS® Load Balancing Advisor communicates with external load balancers and one or more Load Balancing Agents. The main function of the Load Balancing Advisor is to provide external TCP/IP load balancing solutions, such as the Cisco Content Switching Module (CSM), with recommendations on which TCP/IP applications and target z/OS systems within a z/OS sysplex are best equipped to handle new TCP/IP workload requests.

LBAGENT - Load Balancing Agents gather data on its own z/OS system about the TCP/IP stacks and applications running on that system. The Agent is configured with the information it needs to contact the Load Balancing Advisor.

OMPROUTE - OMPROUTE is a z/OS® UNIX application and it requires a z/OS UNIX file system to operate. It can be started from an MVS™ started procedure, from the z/OS shell, or from AUTOLOG (see step 2 for restrictions on using AUTOLOG to start OMPROUTE). OMPROUTE must be started by a RACF-authorized user ID, and it must be in an APF authorized library.

PAGENT - The Policy Agent (PAGENT) interacts with the sysplex distributor to assist with workload balancing. There will be one Policy Agent running on an LPAR regardless of how many stacks are configured. First, the Policy Agent can be configured to collect network performance statistics for applications being distributed on target stacks. These network performance statistics are then used to modify the overall WLM weight assigned to a target server.

RSVPD - Daemon to start and stop Resource ReSerVation Protocol (RSVP) is a protocol that provides a mechanism to reserve resources in support of Integrated Services.

Table 4-13: zOS Communications Server Daemons and Servers

Reference by ACP00282

| Daemon/Server | Resource Required to START/STOP | Authorization | Access |
|---------------|---------------------------------|---------------|--------|
| ADNR | MVS.SERVMMGR.ADNR | DAEMAUDT | ALTER |
| | | SERVAUDT | ALTER |
| | | TSTCAUDT | ALTER |
| | | | |
| DCAS | MVS.SERVMMGR.DCAS | DAEMAUDT | ALTER |
| | | SERVAUDT | ALTER |
| | | SYSPAUDT | ALTER |
| | | TSTCAUDT | ALTER |
| LBADV | MVS.SERVMMGR.LBADV | DAEMAUDT | ALTER |
| | | SERVAUDT | ALTER |
| | | SYSPAUDT | ALTER |
| | | TSTCAUDT | ALTER |
| LBAGENT | MVS.SERVMMGR.LBAGENT | DAEMAUDT | ALTER |
| | | SERVAUDT | ALTER |
| | | SYSPAUDT | ALTER |

| Daemon/Server | Resource Required to START/STOP | Authorization | Access |
|---------------|---------------------------------|---------------|--------|
| | | TSTCAUDT | ALTER |
| | | | |
| PAGENT | MVS.SERVMGR.PAGENT | DAEMAUDT | ALTER |
| | | SERVAUDT | ALTER |
| | | SYSPAUDT | ALTER |
| | | TSTCAUDT | ALTER |
| | | | |
| RSVPD | MVS.SERVMGR.RSVPD | DAEMAUDT | ALTER |
| | | SERVAUDT | ALTER |
| | | SYSPAUDT | ALTER |
| | | TSTCAUDT | ALTER |
| | | | |
| OMPROUTE | MVS.ROUTEMGR.OROUTED | AUTOAUDT | ALTER |
| | | DAEMAUDT | ALTER |
| | | SERVAUDT | ALTER |
| | | SYSPAUDT | ALTER |
| | | TSTCAUDT | ALTER |
| | | | |

4.7 z/OS UNIX Miscellaneous Considerations

This section discusses miscellaneous security considerations for the z/OS UNIX environment. These considerations include the following:

- SMF options
- Account data validation - IEFUJI
- Run-Time Library Services (RTLS)

Table 4-14: Restricted Network Services

Referenced by: ZUSS0014

| Restricted Network Services | | | | | |
|-----------------------------|------|------------|------|---------|------|
| Service | Port | Service | Port | Service | Port |
| Chargen | 19 | logon | 513 | systat | 11 |
| Daytime | 13 | nameserver | 42 | talk | 517 |
| Discard | 9 | netstat | 15 | tftp | 69 |
| Echo | 7 | qotd | 17 | time | 37 |
| Exec | 512 | shell | 514 | timed | 525 |
| finger | 79 | smtp | 25 | uucp | 540 |

4.8 z/OS UNIX SMF Options

In the z/OS environment, SMF data is collected to identify access to the system and to measure the use of resources. This data can be critical to auditors investigating security incidents. SMF data can also be created by authorized applications; this function is controlled to preserve system integrity. The z/OS UNIX environment is not exempt from SMF data collection.

For processes under z/OS UNIX, SMF record type 30 contains data on user identity, program name, and file system activity. SMF record type 92 provides information on the I/O activity of a user or application against a specific file. SMF record types 30 and 92 must be recorded. Due to the potential for very high volumes, subtypes 10 and 11 of the type 92 record may be suppressed at the site's discretion. Refer to IBM's *z/OS MVS System Management Facilities (SMF)* documentation for details and descriptions for these records.

SMF record types 34 and 35 are used to record TSO/E activity but are also written by default when a new address space is created for a fork or spawn in the z/OS UNIX environment. To eliminate errors in TSO/E accounting, IBM recommends that SYS1.PARMLIB(SMFPRMxx) be updated to suppress those records for z/OS UNIX processes (e.g., the OMVS subsystem). Therefore, SMF record types 34 and 35 for z/OS UNIX processes may be suppressed at the site's discretion.

User applications and non-IBM products that run under z/OS UNIX can generate SMF records or check if SMF records are being generated. This is done by using the smf_record callable service. To be able to do this, an application must be running under a userid that has access to the BPX.SMF security resource. When the application or product is installed, the ESM must be updated to allow the access.

4.9 z/OS UNIX Account Data Validation - IEFUJI

IEFUJI is a z/OS exit that validates job names and/or accounting information. If IEFUJI is being used, there are special considerations for z/OS UNIX:

- OMVS should be defined as a subsystem in SYS1.PARMLIB(IEFSSNxx).
- IEFUJI should be set as an exit for subsystem OMVS in SYS1.PARMLIB(SMFPRMxx).
- The IEFUJI code should be adapted to exclude the names of some jobs and daemons started from /etc/rc.
- Refer to IBM's *z/OS UNIX System Services Planning* document for details.

The use of IEFUJI has security implications when ACP rules are in use to validate job names or accounting data. The correct function of IEFUJI and the appropriate ESM access rules must be verified to ensure proper system operation and security.

4.10 z/OS UNIX RTLS

Members of IBM's Language Environment (LE) run-time library are used by z/OS UNIX components (including the shell and utilities) and optionally by user applications running in the z/OS UNIX environment. Access to the LE members can be made available through the system link list (LNKLSTxx) and LPA list (LPALSTxx), through STEPLIBs, or through a z/OS feature known as Run-Time Library Services (RTLS).

If RTLS is used for z/OS UNIX, the following three steps must be completed:

- The RUNOPTS parameter must be coded in SYS1.PARMLIB(BPXPRMxx).
- The RTLS feature must be configured in SYS1.PARMLIB(CSVRTLxx).
- Security resource profiles must be defined to the ESM:

CSVRTLS.LIBRARY.*library.version* for each logical RTLS library to enable security checking,

OR,

CSVRTLS.NOSECCONNECT.*library.version* for each logical RTLS library to disable checking

OR,

CSVRTLS.NOSECCONNECT.* to disable all RTLS security checking.

If the other methods of access (i.e., link list or STEPLIB) to the LE members are used, the CSVRTLS profiles are not needed.

5. EXTERNAL SECURITY MANAGER IMPLEMENTATION

5.1 ESM General Considerations

The ESM is the primary mechanism that controls access to data and resources in z/OS systems. Each ESM in use on the DOD platforms provides the flexibility to tailor the implementation to meet the needs of the local installation.

Many different implementations of various ESMs exist. These different implementations meet the needs of each local installation but make it difficult to coordinate and control the DOD Enterprise.

The installation and implementation of each ESM should be standardized across all DOD processing environments. z/OS STIG Checklist recommended implementation criteria are specified in the individual ESM installation sections of this document.

All deviations are to be specifically noted, with justification and approval documentation, in the system security plan and the accreditation package submitted to the Authorizing Official (AO).

To provide full compliance with the security support required by *DOD Directive 8500.1*, control all products within the operating system using the ESM. Use the following guidance in the acquisition of products to ensure that security-related issues are adequately addressed:

- (1) Products are to be on the National Information Assurance Partnership (NIAP) - Common Criteria Evaluation and Validation Scheme (CCEVS) Validated Products List before procurement and implementation.
- (2) At a minimum, evaluate products for sensitive functions and implement controls to protect these functions.
- (3) Restrict all data sets associated with a product to the access levels necessary for support and operation based upon the requirements. Only those authorized personnel who require the authority to modify or maintain the product are to have *update* and *alter* access.

Many products require special security considerations. Enforce the following considerations relating to compatibility and interfacing with the IBM System Authorization Facility (SAF):

- (1) Protect Commercial-Off-The-Shelf (COTS) products and associated data sets within the operating system using the ESM. Ensure that all COTS products being procured have, and utilize, the SAF interface to the ESM.C
- (2) Secure Government-Off-The-Shelf (GOTS) products and newly developed applications, along with associated data sets, using the ESM. Whenever possible, develop applications using the SAF interface. Safeguards enforced by the ESM are not to be duplicated by security mechanisms implemented within an application. Limit developed internal security mechanisms to those functions that augment the safeguards present in the ESM.
- (3) Internal Product Security Controls (IPSCs) are security mechanisms internal to COTS products and GOTS applications. Only use IPSCs when existing products or applications do not interface to the ESM through SAF, or to augment the protections provided by the existing interface. Reconfigure products using IPSCs, which are capable of taking advantage of the SAF interface, to take proper advantage of the SAF interface.

Whenever IPSCs are being used, develop and maintain security documentation. The documentation is to include descriptions of the IPSCs, the configuration, and the policy being enforced. The ISSO is to maintain the documentation and perform the administration of IPSCs where practical.

- (4) Modify all GOTS products and applications (if using ESM-specific interfaces) to interface with the ESM via standard SAF calls.

All applications are to eventually migrate from IPSCs to using the ESM. If this is unreasonable for any given application, the application is to be eventually phased out.

5.1.1 ESM Standard Global Options

Each ESM provides the capability for customization using global ESM configuration and processing options. These global options provide the flexibility to tailor the configuration and processing of the ESM to the needs of the local operating environment. These options also can pose the danger of compromising the operational environment when misused or when not properly applied.

In an organization as large as the DOD, the additional complication of diversity exists. Many different applications of the global options exist. These different applications meet the needs of each local installation but make it difficult to manage the organizational computing base as a whole. The task of optimizing the processing load of the enterprise across the myriad platforms becomes virtually impossible.

For the above reasons, and to mitigate the above risks and difficulties, all DOD processing environments are to implement the z/OS STIG Checklist required global options for each ESM installed. The z/OS STIG Checklist required options are specified in the individual Access Control Product installation sections of this document. The options specified are z/OS STIG Checklist requirements and each site can choose to be more restrictive.

5.1.2 ESM Userid Controls

Requires that each system user is uniquely identified to the operating environment, and that access to resources is limited to those needed to perform the function. In this case, a user is defined as either an individual accessing a computer resource, or as a task executing on the system that requires access to a resource. On z/OS systems a user is identified by means of a unique userid. This z/OS STIG Checklist requires that audit data record the identity of the user, time of access, interaction with the system, and sensitive functions that might permit a user or program to modify, bypass, or negate security safeguards.

It then follows that any userid (user) on the system must be associated with only one individual. However, any given individual may be assigned responsibility for multiple userids on a given system, depending on functional responsibilities, to ensure task segregation.

Table 5-1: Interactive Users - ACF2

Referenced by:ACF0570

| Interactive Users - ACF2 | | |
|--------------------------|--|--|
| Field | Description | Required Value |
| AUTHSUP1 | User Authorization Flag 1 | ON for highly privileged users controlled by NC-PASS. Note: Refer to Section 6.3.1, NC-PASS for ACF2, for further information. |
| GROUP(name) | This field is required for assigning <i>gids</i> to MVS OpenEdition users. Note: For sites running UNIX Systems Services, see Section 2.5.3.2, Defining Users and Groups, for GROUP(name) requirements. | Will be defined for OpenEdition users. |
| IDLE(time) | Specifies the maximum time permitted (in minutes) between terminal transactions for this user. If exceeded, ACF2 needs the logonid and password to be revalidated before another transaction is accepted. Zero (0) indicates no limit is enforced. This field is available for IMS and CICS on-line processing. | IDLE(15) |
| INTERCOM/ NOINTERCOM | Indicates this user is willing to accept messages from other users through the TSO SEND command. | INTERCOM |
| LGN-ACCT/ NOLGN-ACCT | Indicates permission to specify an account number at logon time. If a user has the PMT-ACCT field, ACF2 prompts the user for an account number unless an account number is specified before the prompt. If a user does not specify an account number at logon and PMT-ACCT is not specified in the user's logonid record, ACF2 uses the user's default account number (TSOACCT is the logonid field) or the system default account number. Specifies the default in the ACCOUNT field of the GSO TSO record. | LGN-ACCT |
| MAIL/NOMAIL | Indicates a user can receive mail messages from TSO at logon time. | MAIL |

| Interactive Users - ACF2 | | |
|--------------------------|--|--|
| Field | Description | Required Value |
| MAXDAYS(days) | Specifies the maximum number of days permitted between password changes before the password expires. Zero (0) indicates no limit. | MAXDAYS (60) |
| MINDAYS(days) | Specifies the minimum number of days that must elapse before a user can change a password. Zero (0) indicates no limit. | MINDAYS (1) |
| MSGID/NOMSGID | Indicates this user wants TSO messages to have message IDs prefixed. | MSGID |
| NO-STORE/ NONO-STORE | Specifies that a user cannot store or delete rule sets. This applies even if the value of the PREFIX field of the logonid record matches the \$KEY of the rule of the data set, if the user has the SECURITY privilege, or if the user has change authority through a %CHANGE or %RCHANGE control statement in the rule set. | NONO-STORE Note: The GSO RULEOPTS record must specify CENTRAL. |
| NOTICES/ NONOTICES | Indicates a user can receive TSO notices at logon time. | NOTICES |
| PASSWORD | The logon password for the user. | Must be completed. |
| PHONE | Specifies the 1- to 12-character telephone number of a user. | Optional |
| PMT-ACCT/ NOPMT-ACCT | Indicates that ACF2 requires a user to specify an account at logon time and to specify the LGN-ACCT field. ACF2 does not prompt for an account number if the FSRETAIN field is also specified. FSRETAIN obtains account values from the last session. | May be required for Fee-for-Service support. |
| PREFIX | User access to the user's own data sets without rule validation. | PREFIX() |
| PROMPT/ NOPROMPT | Indicates that ACF2 prompts a user for missing or incorrect parameters. | PROMPT |
| TSOACCT | Specifies the user's default TSO logon account. Used for all billing. | May be required for Fee-for-Service support. |
| TSOPROC | Specifies the user's default TSO logon procedure. | Optional, may be completed for TSO users. |
| VLD-ACCT/ NOVLD-ACCT | Indicates that ACF2 validates the TSO account number of a user. Creates a resource rule with a type code TAC and a \$KEY of the account number so that ACF2 will perform this validation. | VLD-ACCT May be required for Fee-for-Service support. |

| Interactive Users - ACF2 | | |
|--------------------------|---|--|
| Field | Description | Required Value |
| VLD-PROC/ NOVLD-PROC | Indicates that ACF2 validates the TSO logon procedure of a user. Creates a resource rule with a type code TPR and a \$KEY of the logon procedure so that ACF2 will perform this validation. | VLD-PROC Will be completed for all TSO users. |

5.1.3 Password Complexity

Password complexity is a measure to minimize guessing and brute-force attacks. The DOD has instituted the requirement that all passwords must be at least fifteen (15) characters in length. Currently the zOS operating system can only support a maximum password length of eight (8). As mitigation to this shortfall, each of the ESMs has introduced additional measures to assist in password complexity. One of these measures is a restriction of reserved words and prefixes. The following contains the default list of reserved words and prefixes for each ESM. For CA-ACF2 they are contained in RESWORD in the GSO record. In CA-TSS use the RPW control option to view and modify the restricted password list. For RACF the list is loaded in IRRPWREX.

Each site can make additions to this list to reflect regional common words and prefixes.

Table 5-2: Reserved Words and Prefixes

| | | | | |
|-------|-----|------|-----|-------|
| APPL | APR | ASDF | AUG | BASIC |
| CADAM | DEC | DEMO | FEB | FOCUS |
| GAME | IBM | JAN | JUL | JUN |
| LOG | MAR | MAY | NET | NEW |
| NOV | OCT | PASS | ROS | SEP |
| SIGN | SYS | TEST | TSO | VALID |
| VTAM | XXX | 1234 | | |

6. TRUSTED STARTED TASKS

Table 6-1: Trusted Started Tasks

Referenced by: RACF0660, TSS0810, ACF0640

| Trusted Started Tasks | | |
|-----------------------|------------------|----------|
| ACF2 | GSKSRVR | SMSRESTR |
| ACFBKUP | IEEVMPGR | SMSVSAM |
| APSWPROA | IOSAS | TCPIP |
| APSWPROB | IXGLOGR | TSS |
| APSWPROC | JES2 | TSSB |
| APSWPROM | JESXCF | TSSBKUP |
| APSWPROT | LLA | TSSRESTN |
| CATALOG | NFS | VLF |
| CEA | OMVS/OMVSKERN*** | VTAM |
| CONSOLE | RACF | XCFAS |
| DFHSM* | RMF | ZFS** |
| DFS | RMFGAT | |
| DUMPSRV | SMF | |
| GPMSERVE | SMSRESTN | |

The primary source for this Trusted Started Task Table is the MVS Init & Tuning Guide.

*=The name of the DFHSM Proc may be “DFSMSHSM”. Another consideration here is that IBM sometimes recommends that other Started Tasks be set up similar to DFHSM...reference SSO FIXDOC 1924. In this case, where IBM recommends either mapping a proc to the DFHSM userid or setting up additional DFHSM-like userids then the TRUSTED attribute would be justified.

**=This is not contained in the MVS Init & Tuning Guide. Reference Chapter 2 of z/OS V1R9.0 Distributed File Service zFS Administration z/OS V1R9.0 Distributed File Service zFS Administration.

*** = USS Planning Guide shows that the OMVS proc mapped to the OMVSKERN userid is OK to run as TRUSTED. This does not apply to the BPXOINIT proc.

Note: A Privileged user under ACF2 can have a logonid set up with Non Cancel attribute for special occasions. This logonid will not be used as an everyday logonid.

Note: Many of the Trusted Started tasks may be defined to the ESM with more stringent rules to restrict bypassing of security.

Note: “TRUSTED” Means any STC listed can have any level of access up to including complete bypassing of all security controls.

7. Z/OS SYSTEM AND JES2 COMMANDS

Table 7-1: Controls on z/OS System Commands

Referenced by: ACP00282, ZIOA0040

| Controls on z/OS System Commands | | | | |
|--|-------------|------------------------------------|------------|-----|
| Command/Keyword | Access | Resource-Name | Auth | Log |
| ACTIVATE | UPDATE | MVS.ACTIVATE | a o s t | Y |
| CANCEL device | UPDATE | MVS.CANCEL.DEV.device | a o s t | Y |
| CANCEL jobname (others) | UPDATE | MVS.CANCEL.JOB.jobname | a o s t | Y |
| CANCEL jobname (own jobs) | UPDATE | MVS.CANCEL.JOB.jobname | * | Y |
| The previous commands are for jobs that are not started tasks. | | | | |
| CANCEL jobname.id | UPDATE | MVS.CANCEL.STC.mbrname.id | a o s t | Y |
| CANCEL id | UPDATE | MVS.CANCEL.STC.mbrname.id | a o s t | Y |
| The previous command is for a started task for which an identifier is provided. | | | | |
| CANCEL jobname | UPDATE | MVS.CANCEL.STC.mbrname.job name | a o s t | Y |
| The previous command is for a started task for which an identifier was not provided. mbrname is the name of the member containing the JCL source. | | | | |
| CANCEL jobname | UPDATE | MVS.CANCEL.ATX.jobname | a o s t \$ | Y |
| The previous command is for APPC transaction programs. | | | | |
| CANCEL U=userid | UPDATE | MVS.CANCEL.TSU.userid | a o s t \$ | Y |
| CHNGDUMP | UPDATE | MVS.CHNGDUMP | a o s t | Y |
| CMDS DISPLAY | READ | MVS.CMDS.DISPLAY | * | Y |
| CMDS SHOW | READ | MVS.CMDS.SHOW | * | Y |
| CMDS REMOVE | CONTRO L | MVS.CMDS.REMOVE | a o s t | Y |
| CMDS ABEND | CONTRO L | MVS.CMDS.ABEND | a o s t | Y |
| CONFIG | CONTRO L | MVS.CONFIG | a o s t | Y |
| CONTROL | READ | MVS.CONTROL.A | * | |
| Note: The access authority for all CONTROL commands except CONTROL M is normally READ, but the <i>L=name</i> (console name) operand can change the access level. When <i>L=name</i> specifies a console that is not full-capability and is not the issuing console, the access authority is UPDATE. When <i>L=name</i> specifies a console that is full-capability and is not the issuing console, the access authority is CONTROL. | | | | |
| CONTROL C | READ | MVS.CONTROL.C | * | |
| Note: See the note for the CONTROL A command for exceptions. | | | | |
| CONTROL D | READ | MVS.CONTROL.D | * | |
| Note: See the note for the CONTROL A command for exceptions. | | | | |
| CONTROL E | READ | MVS.CONTROL.E | * | |
| Note: See the note for the CONTROL A command for exceptions. | | | | |
| CONTROL M | CONTRO L | MVS.CONTROL.M | a c o s t | |

| Controls on z/OS System Commands | | | | |
|---|--------|----------------------|------|-----|
| Command/Keyword | Access | Resource-Name | Auth | Log |
| CONTROL N | READ | MVS.CONTROL.N | * | |
| Note: See the note for the CONTROL A command for exceptions. | | | | |
| CONTROL Q | READ | MVS.CONTROL.Q | * | |
| Note: See the note for the CONTROL A command for exceptions. | | | | |
| CONTROL S | READ | MVS.CONTROLS.S | * | |
| Note: See the note for the CONTROL A command for exceptions. | | | | |
| CONTROL V | READ | MVS.CONTROL.V | * | |
| Note: See the note for the CONTROL A command for exceptions. | | | | |
| DEVSESV | READ | MVS.DEVSESV | * | |
| DISPLAY A | READ | MVS.DISPLAY.JOB | * | |
| DISPLAY ALLOC,GRPLOCKS | READ | MVS.DISPLAY.ALLOC | * | |
| DISPLAY ALLOC,OPTIONS | READ | MVS.DISPLAY.ALLOC | * | |
| DISPLAY APPC | READ | MVS.DISPLAY.APPC | * | |
| DISPLAY ASCH | READ | MVS.DISPLAY.ASCH | * | |
| DISPLAY ASM | READ | MVS.DISPLAY.ASM | * | |
| DISPLAY CEE | READ | MVS.DISPLAY.CEE | * | |
| DISPLAY CF | READ | MVS.DISPLAY.CF | * | |
| DISPLAY CNGRP | READ | MVS.DISPLAY.CNGRP | * | |
| DISPLAY CONSOLES | READ | MVS.DISPLAY.CONSOLES | * | |
| DISPLAY DIAG | READ | MVS.DISPLAY.DIAG | * | |
| DISPLAY DLF | READ | MVS.DISPLAY.DLF | * | |
| DISPLAY DMN | READ | MVS.DISPLAY.DMN | * | |
| DISPLAY DUMP | READ | MVS.DISPLAY.DUMP | * | |
| DISPLAY EMCS | READ | MVS.DISPLAY.EMCS | * | |
| DISPLAY ETR | READ | MVS.DISPLAY.ETR | * | |
| DISPLAY GRS | READ | MVS.DISPLAY.GRS | * | |
| DISPLAY GTZ | READ | MVS.DISPLAY.GTZ | * | |
| DISPLAY HIS | READ | MVS.DISPLAY.HIS | * | |
| DISPLAY HS | READ | MVS.DISPLAY.HS | * | |
| DISPLAY IEFOPZ | READ | MVS.DISPLAY.IEFOPZ | * | |
| DISPLAY IOS | READ | MVS.DISPLAY.IOS | * | |
| DISPLAY IPLINFO | READ | MVS.DISPLAY.IPLINFO | * | |
| DISPLAY IQP | READ | MVS.DISPLAY.IQP | * | |
| DISPLAY JOBS | READ | MVS.DISPLAY.JOB | * | |
| DISPLAY LOGGER | READ | MVS.DISPLAY.LOGGER | * | |
| DISPLAY LOGREC | READ | MVS.DISPLAY.LOGREC | * | |
| DISPLAY M | READ | MVS.DISPLAY.M | * | |
| DISPLAY MMS | READ | MVS.DISPLAY.MMS | * | |
| DISPLAY MPF | READ | MVS.DISPLAY.MPF | * | |
| DISPLAY MSGFLD | READ | MVS.DISPLAY.MSGFLD | * | |
| DISPLAY NET | READ | MVS.DISPLAY.NET | * | |

| Controls on z/OS System Commands | | | | |
|--|---------|-------------------------------|---------|-----|
| Command/Keyword | Access | Resource-Name | Auth | Log |
| DISPLAY OMVS | READ | MVS.DISPLAY.OMVS | * | |
| DISPLAY OPDATA | READ | MV S.DISPLAY.OPDATA | * | |
| DISPLAY PARMLIB | READ | MVS.DISPLAY.PARMLIB | * | |
| DISPLAY PCIE | READ | MVS.DISPLAY.PCIE | * | |
| DISPLAY PFK | READ | MVS.DISPLAY.PFK | * | |
| DISPLAY PPT | READ | MVS.DISPLAY.PPT | * | |
| DISPLAY PROD | READ | MVS.DISPLAY.PROD | * | |
| DISPLAY PROG | READ | MVS.DISPLAY.PROG | * | |
| For DISPLAY PROG,EXIT, if resource CSVDYNEX.LIST exists in the FACILITY class, READ authorization to CSVDYNEX.LIST is required. | | | | |
| DISPLAY R | READ | MVS.DISPLAY.R | * | |
| DISPLAY RRS | READ | MVS.DISPLAY.RRS | * | |
| DISPLAY RTLS | READ | MVS.DISPLAY.RTLS | * | |
| DISPLAY SLIP | READ | MVS.DISPLAY.SLIP | * | |
| DISPLAY SMF | READ | MVS.DISPLAY.SMF | * | |
| DISPLAY SMFLIM | READ | MVS.DISPLAY.SMFLIM | * | |
| DISPLAY SMS | READ | MVS.DISPLAY. SMS | * | |
| DISPLAY SSI | READ | MVS.DISPLAY.SSI | * | |
| DISPLAY SYMBOLS | READ | MVS.DISPLAY.SYMBOLS | * | |
| DISPLAY T | READ | MVS.DISPLAY.TIMEDATE | * | |
| DISPLAY TRACE | READ | MVS.DISPLAY.TRACE | * | |
| DISPLAY TS | READ | MVS.DISPLAY.JOB | * | |
| DISPLAY U | READ | MVS.DISPLAY.U | * | |
| DISPLAY WLM | READ | MVS.DISPLAY.WLM | * | |
| DISPLAY XCF | READ | MVS.DISPLAY.XCF | * | |
| DUMP | CONTROL | MVS.DUMP | a o s t | Y |
| DUMPDS | UPDATE | MVS.DUMPDS | a o s t | |
| FORCE device | CONTROL | MVS.FORCE.DEV.device | a o s t | Y |
| FORCE jobname | CONTROL | MVS.FORCE.JOB.jobname | a o s t | Y |
| The previous command is for a job that is not a started task. | | | | |
| FORCE jobname.id | CONTROL | MVS.FORCE.STC.mbrname.id | a o s t | Y |
| FORCE id | CONTROL | MVS.FORCE.STC.mbrname.id | a o s t | Y |
| The previous command is for a started task for which an identifier was provided. | | | | |
| FORCE jobname | CONTROL | MVS.FORCE.STC.mbrname.jobname | a o s t | Y |
| The previous command is for a started task for which an identifier was not provided. mbrname is the name of the member containing the JCL source. | | | | |
| FORCE U=userid | CONTROL | MVS.FORCE.TSU.userid | a o s t | Y |

| Controls on z/OS System Commands | | | | |
|--|---------|----------------------------------|---------|-----|
| Command/Keyword | Access | Resource-Name | Auth | Log |
| FORCE device,ARM | CONTROL | MVS.FORCEARM.DEV.device | a o s t | Y |
| FORCE jobname,ARM | CONTROL | MVS.FORCEARM.JOB.jobname | a o s t | Y |
| The previous command is for a job that is not a started task. | | | | |
| FORCE [jobname.] identifier,ARM | CONTROL | MVS.FORCEARM.STC.mbrname.id | a o s t | Y |
| The previous command is for a started task for which an identifier was provided. | | | | |
| FORCE jobname,ARM | CONTROL | MVS.FORCEARM.STC.mbrname.jobname | a o s t | Y |
| The previous command is for a started task for which an identifier was not provided. mbrname is the name of the member containing the JCL source. | | | | |
| FORCE U=userid,ARM | CONTROL | MVS.FORCEARM.TSU.userid | a o s t | Y |
| FORCE device,TCB=tcbaddr | CONTROL | MVS.FORCETCB.DEV.device | aost | Y |
| FORCE jobname,TCB=tcbaddr | CONTROL | MVS.FORCETCB.JOB.jobname | aost | Y |
| The previous command is for a job that is not a started task. | | | | |
| FORCE [jobname.]identifier.TCB=tcbaddr | CONTROL | MVS.FORCETCB.STC.mbrname.id | aost | Y |
| The previous command is for a started task for which an identifier was provided. | | | | |
| FORCE jobname,TCB=tcbaddr | CONTROL | MVS.FORCETCB.STC.mbrname.jobname | aost | Y |
| The previous command is for a started task for which an identifier was not provided. mbrname is the name of the member containing the JCL source. | | | | |
| FORCE U=userid.TCB=tcbaddr | CONTROL | MVS.FORCETCB.TSU.userid | aost | Y |
| HALT EOD | UPDATE | MVS.HALT.EOD | a o s t | Y |
| HALT NET | UPDATE | MVS.HALT.NET | a o s t | Y |
| IOACTION | CONTROL | MVS.IOACTION | a o s t | Y |
| LIBRARY | UPDATE | MVS.LIBRARY | a o s t | Y |
| LOG | READ | MVS.LOG | * | |
| MODE | UPDATE | MVS.MODE | a o s t | Y |
| MODIFY jobname | UPDATE | MVS.MODIFY.JOB.jobname | a o s t | Y |
| The previous command is for a job that is not a started task. | | | | |
| MODIFY userid | UPDATE | MVS.MODIFY.JOB.userid | a o s t | Y |

| Controls on z/OS System Commands | | | | |
|--|-------------|--|----------------------|-----|
| Command/Keyword | Access | Resource-Name | Auth | Log |
| MODIFY jobname | UPDATE | MVS.MODIFY.STC.mbrname.id | a o s t ⁴ | Y |
| MODIFY jobname.id | UPDATE | MVS.MODIFY.STC.mbrname.id | a o s t ⁴ | Y |
| MODIFY id | UPDATE | MVS.MODIFY.STC.mbrname.id | a o s t ⁴ | Y |
| The previous command is for a started task for which an identifier was provided. | | | | |
| MODIFY jobname | UPDATE | MVS.MODIFY.STC.mbrname.job name | a o s t ⁴ | Y |
| <p>The previous command is for a started task for which an identifier was not provided. mbrname is the name of the member containing the JCL source. Note: MODIFY might actually affect more than one job. For example: If START ABC.DEF and START ABC.GHI are issued, MODIFY ABC.* affects both jobs, and one authorization request is issued for each. If the START ABC command is issued twice, two started tasks named ABC start running on the system. MODIFY ABC affects both jobs, and one authorization request is issued for each.</p> <p>Note: The target of the MODIFY command may allow or require additional authorizations. Please be sure to examine all documentation regarding the target of the command to insure that the proper security is in place.</p> | | | | |
| MONITOR | READ | MVS.MONITOR | * | |
| MOUNT | UPDATE | MVS.MOUNT | a o s t | |
| PAGEADD | UPDATE | MVS.PAGEADD | a o s t | Y |
| PAGEDEL | UPDATE | MVS.PAGEDEL | a o s t | Y |
| QUIESCE | CONTRO L | MVS.QUIESCE | a o s t | Y |
| REPLY | READ | MVS.REPLY | * ⁴ | Y |
| RESET | UPDATE | MVS.RESET | a o s t | Y |
| RESET CN | CONTRO L | MVS.RESET.CN | a o s t | Y |
| ROUTE system | READ | MVS.ROUTE.CMD.system | * | |
| Note: When a system name is specified on the ROUTE command, <i>system</i> is the name of the system that is the target of the command. | | | | |
| ROUTE *ALL | READ | MVS.ROUTE.CMD.ALLSYSTEM S | * | |
| ROUTE *OTHER | READ | MVS.ROUTE.CMD.OTHERSYS TEMS | * | |
| ROUTE sysgrpname | READ | MVS.ROUTE.CMD.sysgrpname | * | |
| ROUTE (sys1,...,sysN) | READ | MVS.ROUTE.CMD.sys1 MVS.ROUTE.CMD.sysN | * | |
| ROUTE (group1,...,groupN) | READ | MVS.ROUTE.CMD.group1 MVS.ROUTE.CMD.groupN | * | |
| SEND | READ | MVS.SEND | * | |
| SET APPC | UPDATE | MVS.SET.APPC | a o s t | Y |
| SET ASCH | UPDATE | MVS.SET.ASCH | a o s t | Y |

⁴ For systems running TSS the Master SCA can have access to identified resources.

| Controls on z/OS System Commands | | | | |
|----------------------------------|-------------|---------------------|---------|-----|
| Command/Keyword | Access | Resource-Name | Auth | Log |
| SET CEE | UPDATE | MVS.SET.CEE | a o s t | Y |
| SET CLOCK | UPDATE | MVS.SET.TIMEDATE | a o s t | Y |
| SET CNGRP | UPDATE | MVS.SET.CNGRP | a o s t | Y |
| SET CNIDTR | UPDATE | MVS.SET.CNIDTR | a o s t | Y |
| SET CON | UPDATE | MVS.SET.CON | a o s t | Y |
| SET DAE | UPDATE | MVS.SET.DAE | a o s t | Y |
| SET DATE | UPDATE | MVS.SET.TIMEDATE | a o s t | Y |
| SET DEVSUP | UPDATE | MVS.SET.DEVSUP | a o s t | Y |
| SET GRSRNL | UPDATE | MVS.SET.GRSRNL | a o s t | Y |
| SET GTZ | UPDATE | MVS.SET.GTZ | a o s t | Y |
| SET IEFOPZ | UPDATE | MVS.SET.IEFOPZ | a o s t | Y |
| SET ICS | UPDATE | MVS.SET.ICS | a o s t | Y |
| SET IOS | UPDATE | MVS.SET.IOS | a o s t | Y |
| SET IQP | UPDATE | MVS.SET.IQP | a o s t | Y |
| SET IXGCNF | UPDATE | MVS.SET.IXGCNF | a o s t | Y |
| SET IPS | UPDATE | MVS.SET.IPS | a o s t | |
| SET MMS | UPDATE | MVS.SET.MMS | a o s t | Y |
| SET MPF | UPDATE | MVS.SET.MPF | a o s t | Y |
| SET MSGFLD | UPDATE | MVS.SET.MSGFLD | a o s t | Y |
| SET OPT | UPDATE | MVS.SET.OPT | a o s t | Y |
| SET PFK | UPDATE | MVS.SET.PFK | a o s t | Y |
| SET PROG | UPDATE | MVS.SET.PROG | a o s t | Y |
| SET RESET | UPDATE | MVS.SET.TIMEDATE | a o s t | |
| SET RTLS | UPDATE | MVS.SET.RTLS | a o s t | Y |
| SET SCH | UPDATE | MVS.SET.SCH | a o s t | Y |
| SET SLIP | UPDATE | MVS.SET.SLIP | a o s t | Y |
| SET SMF | UPDATE | MVS.SET.SMF | a o s t | Y |
| SET SMFLIM | UPDATE | MVS.SET.SMFLIM | a o s t | Y |
| SET SMS | UPDATE | MVS.SET.SMS | a o s t | Y |
| SET ALLOC | UPDATE | MVS.SETALLOC.ALLOC | d s t | Y |
| SETAPPC | UPDATE | MVS.SETAPPC.APPC | a o s t | Y |
| SETAUTOR | UPDATE | MVS.SETAUTOR.AUTOR | | |
| SETCEE | UPDATE | MVS.SETCEE.CEE | a o s t | Y |
| SETCON DELETE | UPDATE | MVS.SETCON.DELETE | a o s t | Y |
| SETCON MODE | CONTRO L | MVS.SETCON.MODE | a o s t | Y |
| SETCON MONITOR (MN) | CONTRO L | MVS.SETCON.MONITOR | a o s t | Y |
| SETCON TRACKING (TR) | CONTRO L | MVS.SETCON.TRACKING | a o s t | Y |
| SETDMN | UPDATE | MVS.SETDMN.DMN | a o s t | Y |
| SETETR | UPDATE | MVS.SETETR.ETR | a o s t | Y |
| SETGRS | UPDATE | MVS.SETGRS.AUTHQLVL | a o s t | Y |

| Controls on z/OS System Commands | | | | |
|---|---------|--|------------------------|------------|
| Command/Keyword | Access | Resource-Name | Auth | Log |
| SETGRS CNS | CONTROL | MVS.SETGRS.GRS | a o s t | Y |
| SETGRS MODE=STAR ENQMAXA ENQMAXU CNS MONITOR | UPDATE | MVS.SETGRS.TOLINT MVS.SETGRS.RESMIL MVS.SETGRS.MODE.STAR MVS.SETGRS.SYNCHRES MVS.SETGRS.GRSQ MVS.SETGRS.ENQMAXA MVS.SETGRS.ENQMAXU MVS.SETGRS.CNS MVS.SETGRS.MONITOR | a o s t a o s t | Y Y |
| SETGTZ | UPDATE | MVS.SETGTZ.GTZ | a o s t | Y |
| SETIOS | UPDATE | MVS.SETIOS.IOS | a o s t | Y |
| SETHS | UPDATE | MVS.SETHS | a o s t | Y |
| SETLOAD | UPDATE | MVS.SETLOAD.LOAD | a o s t | Y |
| SETLOAD xx,IEASYM | UPDATE | MVS.SETLOAD.IEASYM | a o s t | Y |
| SETLOAD xx,PARMLIB | UPDATE | MVS.SETLOAD.LOAD | a o s t | Y |
| SETLOGR | UPDATE | MVS.SETLOGR.LOGR | a o s t | Y |
| SETLOGRC | CONTROL | MVS.SETLOGRC.LOGRC | a o s t | Y |
| SETMF | UPDATE | MVS.SETMF.MF | a o s t | Y |
| SETPROG | UPDATE | MVS.SETPROG | s t | Y |
| SETRRS SHUTDOWN | UPDATE | MVS.SETRRS.SHUTDOWN | a o s t | Y |
| SETSMF | UPDATE | MVS.SETSMF.SMF | a o s t | Y |
| SETSMS | UPDATE | MVS.SETSMS.SMS | a o s t | Y |
| SETSSI ACTIVATE | CONTROL | MVS.SETSSI.ACTIVATE.subname | a o s t | Y |
| SETSSI ADD | CONTROL | MVS.SETSSI.ADD.subname | a o s t | Y |
| SETSSI DEACTIVATE | CONTROL | MVS.SETSSI.DEACTIVATE.subname | a o s t | Y |
| SETSSI DELETE | CONTROL | MVS.SETSSI.DELETE.subname | a o s t | Y |
| <p>Note: The following rules apply to the subsystem name (subname) value in the SETSSI commands:</p> <ul style="list-style-type: none"> Lower case characters in the subsystem name will be translated to upper case in the resource-name. The characters *, &, or % in the subsystem name will be translated to the _ character in the resource-name. | | | | |

| Controls on z/OS System Commands | | | | |
|--|--------|--|----------------------|-----|
| Command/Keyword | Access | Resource-Name | Auth | Log |
| <ul style="list-style-type: none"> Embedded blanks in the subsystem name will be translated to the _ character in the resource-name. Trailing blanks will not be translated. <p>No other characters are translated. IBM recommends defining generic profiles to match subsystem names with characters that cannot be specified using the RACF command interface.</p> | | | | |
| SETUNI | UPDATE | MVS.SETUNI.UNI | a o s t | Y |
| SETXCF | UPDATE | MVS.SETXCF.XCF | a o s t | Y |
| SLIP | UPDATE | MVS.SLIP | a o s t | Y |
| Note: When the IEASLIP.REFRESH FACILITY class profile is defined, the SLIP command issuer must have UPDATE access to that profile to use the REFAFTER and REFBEFOR keywords. | | | | |
| START mbrname[.identifier] | UPDATE | MVS.START.STC.mbrname[id] | a o s t | Y |
| The previous command is for a started task for which an identifier was provided. mbrname is the name of the member containing the JCL source. | | | | |
| START mbrname,JOBNAME =jobname | UPDATE | MVS.START.STC.mbrname.jobname | a o s t ⁵ | Y |
| The previous command is for a started task for which an identifier was not provided. mbrname is the name of the member containing the JCL source. | | | | |
| START commands that use one or more of the following keywords: DSN or DSNNAME DISP PROTECT | UPDATE | The resource name substitutes DDALERT for one or more of the keywords. MVS.START.jobname.qualifier.D DALER | a o s t | Y |
| An example of the previous MVS START command is as follows: START jobname.qualifier,DSN=dsname.qualifier,DISP=SHR | | | | |
| STOP jobname | UPDATE | MVS.STOP.JOB.jobname | a o s t ⁵ | Y |
| The previous command is for a job that is not a started task. | | | | |
| STOP userid | UPDATE | MVS.STOP.JOB.userid | a o s t | Y |
| STOP jobname STOP jobname.id STOP id | UPDATE | MVS.STOP.STC.mbrname.id | a o s t | Y |
| The previous command is for a started task for which an identifier was provided. mbrname is the name of the member containing the JCL source. | | | | |
| STOP jobname | UPDATE | MVS.STOP.STC.mbrname.jobname | a o s t | Y |
| The previous command is for a started task for which an identifier was not provided. mbrname is the name of the member containing the JCL source. | | | | |

⁵ The SDSF started task is authorized to Start and Stop the SDSF Aux server.

| Controls on z/OS System Commands | | | | |
|---|-----------------------|--|----------------------|--------|
| Command/Keyword | Access | Resource-Name | Auth | Log |
| Note: STOP might actually affect more than one started task if more than one unit of work with the same name is active at the same time. If so, there is one call to RACF for command authorization for each unit of work. | | | | |
| STOPMN | READ | MVS.STOPMN | * | |
| SWAP | UPDATE | MVS.SWAP | a o s t | Y |
| SWITCH SMF | UPDATE | MVS.SWITCH.SMF | a o s t | Y |
| TRACE CT | UPDATE | MVS.TRACE.CT | a o s t | Y |
| TRACE MT | CONTRO L | MVS.TRACE.MT | a o s t | Y |
| TRACE ST | UPDATE | MVS.TRACE.ST | a o s t | Y |
| TRACE STATUS | UPDATE | MVS.TRACE.STATUS | a o s t | Y |
| Unknown MVS commands | UPDATE | MVS.UNKNOWN | a o s t ⁴ | Y |
| UNLOAD | UPDATE | MVS.UNLOAD | a o s t | Y |
| VARY CN | UPDATE | MVS.VARY.CN | a o s t | Y |
| VARY CN,ACTIVATE | READ | MVS.VARY.CN | * | Y |
| Note: Issue VARY CN, ACTIVATE only from the system console. | | | | |
| VARY CN,AUTH | UPDATE CONTRO L | MVS.VARY.CN MVS.VARYAUTH.CN | a o s t a o s t | Y Y |
| Note: VARY CN, AUTH requires both profiles. | | | | |
| VARY CN,DEACTIVATE | READ UPDATE | MVS.VARY.CN | * a o s t | Y Y |
| Note: For the VARY CN, DEACTIVATE command, READ applies only when that command is issued from the system console; otherwise, UPDATE applies. | | | | |
| VARY CN,LOGON | UPDATE CONTRO L | MVS.VARY.CN MVS.VARYLOGON.CN | a o s t a o s t | Y Y |
| Note: VARY CN, LOGON requires both profiles. | | | | |
| VARY CN,LU | UPDATE CONTRO L | MVS.VARY.CN MVS.VARYLU.CN | a o s t a o s t | Y Y |
| Note: VARY CN, LU requires both profiles. | | | | |
| VARY CN,OFFLINE,FORC E | CONTRO L | MVS.VARYFORCE.CN | a o s t | Y |
| VARY CN(...),STANDBY | CONTRO L | MVS.VARYSTANDBY.CN | a o s t | Y |
| VARY CONSOLE | UPDATE | MVS.VARY.CONSOLE | a o s t | Y |
| VARY CONSOLE,AUTH | UPDATE CONTRO L | MVS.VARY.CONSOLE MVS.VARYAUTH.CONSOLE | a o s t a o s t | Y Y |

| Controls on z/OS System Commands | | | | |
|--|---------|-------------------|---------|-----|
| Command/Keyword | Access | Resource-Name | Auth | Log |
| Note: VARY CONSOLE, AUTH requires both profiles. | | | | |
| VARY GRS | CONTROL | MVS.VARY.GRS | a o s t | Y |
| VARY HARDCPY | CONTROL | MVS.VARY.HARDCPY | a o s t | Y |
| VARY NET | UPDATE | MVS.VARY.NET | a o s t | Y |
| VARY OFFLINE | UPDATE | MVS.VARY.DEV | a o s t | Y |
| Note: If VARY CN, OFFLINE is specified, the rules for VARY CN apply (the system checks for UPDATE access to MVS.VARY.CN, not MVS.VARY.DEV). | | | | |
| VARY OFFLINE, FORCE | CONTROL | MVS.VARYFORCE.DEV | a o s t | Y |
| VARY ONLINE | UPDATE | MVS.VARY.DEV | a o s t | Y |
| Note: If VARY CN, ONLINE is specified, the rules for VARY CN apply (the system checks for UPDATE access to MVS.VARY.CN, not MVS.VARY.DEV). | | | | |
| VARY PATH | UPDATE | MVS.VARY.PATH | a o s t | Y |
| VARY SMS | UPDATE | MVS.VARY.SMS | a o s t | Y |
| VARY TCPIP | UPDATE | MVS.VARY.TCPIP | a o s t | Y |
| VARY TCPIP cmd | CONTROL | MVS.VARY.TCPIP.* | a o s t | Y |
| VARY WLM | CONTROL | MVS.VARY.WLM | a o s t | Y |
| VARY XCF | CONTROL | MVS.VARY.XCF | a o s t | Y |
| WRITELOG | READ | MVS.WRITELOG | * | Y |

Auth column

a - AUTOAUDT, Automated operations.
c - CONSOLES, System consoles
d - DASDAUDT, Storage Management
o - OPERAUDT, Operations staff
s - SYSPAUDT, Systems Programming staff
t - TSTCAUDT, Trusted Started Tasks
* - All Users
\$ - May be given to All Users using SDSF, CA Roscoe, and similar products that interface with a user's input/output requiring the issuing of console commands.

Log

Y

Note: ALTER authority on RACF profiles: For discrete profiles, ALTER allows some RACF Administrative functions such as use of the RDELETE Command. However, this is not the preferred method for granting access for resource administration. Alter access for resource administration may be permitted but only to Security Administrators justified by the ISSO.

Resource access requirements are based on IBM minimal access requirements. Users that are authorized to have access to the resource can have the access specified or greater. The exceptions are those stated with the resource, resources that specify different accesses to users and above note.

Where multiple users have different accesses, an example is one user has READ and another has UPDATE the “access specified or greater” will be to the user with UPDATE.

When granted resource access utilize the highest level of granularity possible. Access at the MVS.** level must not be granted.

Table 7-2: Controls on JES2 System Commands

Referenced by: ZJES0052

| Controls on JES2 System Commands | | | | |
|----------------------------------|---------|------------------------|------------|-----|
| JES2 command | Access | Resource-Name | Auth | Log |
| \$ACTIVATE | CONTROL | Jesx.ACTIVATE.FUNCTION | a o s t | Y |
| \$ADD APPL | CONTROL | Jesx.ADD.APPL | a o s t | Y |
| \$ADD CONNECT | CONTROL | Jesx.ADD.CONNECT | a o s t | Y |
| \$ADD DESTID | CONTROL | Jesx.ADD.DESTID | a o s t | Y |
| \$ADD PRTnnnn | UPDATE | Jesx.ADD.DEV | a o s t | Y |
| \$ADD FSS | CONTROL | Jesx.ADD.FSS | a o s t | Y |
| \$ADD LINE | CONTROL | Jesx.ADD.LINE | a o s t | Y |
| \$ADD LOADMOD | CONTROL | Jesx.ADD.LOADMOD | a o s t | Y |
| \$ADD LOGON | CONTROL | Jesx.ADD.LOGON | a o s t | Y |
| \$ADD NETSRV | CONTROL | Jesx.ADD.NETSRV | a o s t | Y |
| \$ADD PROCLIB | CONTROL | Jesx.ADD.PROCLIB | a o s t | Y |
| \$ADD REDIRECT | CONTROL | Jesx.ADD.REDIRECT | a o s t | Y |
| \$ADD RMT | CONTROL | Jesx.ADD.RMT | a o s t | Y |
| \$ADD SOCKET | CONTROL | Jesx.ADD.SOCKET | a o s t | Y |
| \$ADD SRVCLASS | CONTROL | Jesx.ADD.SRVCLASS | a o s t | Y |
| \$B device | UPDATE | Jesx.BACKSP.DEV | a o s t | Y |
| \$C A** | CONTROL | Jesx.CANCEL.AUTOCMD | a o s t | Y |
| \$C J | UPDATE | Jesx.CANCEL.BAT | a o s t \$ | Y |
| \$C O J | UPDATE | Jesx.CANCEL.BATOUT | a o s t \$ | Y |
| \$C device | UPDATE | Jesx.CANCEL.DEV | a o s t \$ | Y |
| \$C Lx.yy | UPDATE | Jesx.CANCEL.DEV | a o s t | Y |
| \$C OFFn.JR | UPDATE | Jesx.CANCEL.DEV | a o s t | Y |
| \$C OFFn.JT | UPDATE | Jesx.CANCEL.DEV | a o s t | Y |
| \$C OFFn.SR | UPDATE | Jesx.CANCEL.DEV | a o s t | Y |
| \$C OFFn.ST | UPDATE | Jesx.CANCEL.DEV | a o s t | Y |
| \$C O JOBQ | UPDATE | Jesx.CANCEL.JSTOUT | a o s t | Y |
| \$C S | UPDATE | Jesx.CANCEL.STC | a o s t \$ | Y |
| \$C O S | UPDATE | Jesx.CANCEL.STCOUT | a o s t | Y |
| \$C T | UPDATE | Jesx.CANCEL.TSU | * | |
| \$C O T | UPDATE | Jesx.CANCEL.TSUOUT | * | |
| \$DEL CONNECT | CONTROL | Jesx.DEL.CONNECT | a o s t | Y |
| \$DEL DESTID | CONTROL | Jesx.DEL.DESTID | a o s t | Y |
| \$DEL LOADMOD | CONTROL | Jesx.DEL.LOADMOD | a o s t | Y |
| \$DEL PROCLIB | CONTROL | Jesx.DEL.PROCLIB | a o s t | Y |

| Controls on JES2 System Commands | | | | |
|----------------------------------|--------|------------------------|------|-----|
| JES2 command | Access | Resource-Name | Auth | Log |
| \$D ACTIVATE | READ | jesx.DISPLAY.ACTIVATE | * | |
| \$D ACTRMT | READ | jesx.DISPLAY.ACTRMT | * | |
| \$D J | READ | jesx.DISPLAY.BAT | * | |
| \$D O J | READ | jesx.DISPLAY.BATOUT | * | |
| \$L J | READ | jesx.DISPLAY.BATOUT | * | |
| \$D CKPTDEF | READ | jesx.DISPLAY.CKPTDEF | * | |
| \$D CONDEF | READ | jesx.DISPLAY.CONDEF | * | |
| \$D CONNECT | READ | jesx.DISPLAY.CONNECT | * | |
| \$D DESTDEF | READ | jesx.DISPLAY.DESTDEF | * | |
| \$D DEStid | READ | jesx.DISPLAY.DESTID | * | |
| \$D PRT | READ | jesx.DISPLAY.DEV | * | |
| \$D PRTnnnn | READ | jesx.DISPLAY.DEV | * | |
| \$D PUNnn | READ | jesx.DISPLAY.DEV | * | |
| \$D RDRnn | READ | jesx.DISPLAY.DEV | * | |
| \$D U | READ | jesx.DISPLAY.DEV | * | |
| \$D Rnnnnn.CON | READ | jesx.DISPLAY.DEV | * | |
| \$D Rnnnnn.PRm | READ | jesx.DISPLAY.DEV | * | |
| \$D Rnnnnn.PUm | READ | jesx.DISPLAY.DEV | * | |
| \$D Rnnnnn.RDm | READ | jesx.DISPLAY.DEV | * | |
| \$D I | READ | jesx.DISPLAY.INITIATOR | * | |
| \$D init stmt | READ | jesx.DISPLAY.initstmt | * | |
| \$D A | READ | jesx.DISPLAY.JOB | * | |
| \$D N | READ | jesx.DISPLAY.JOB | * | |
| \$D Q | READ | jesx.DISPLAY.JOB | * | |
| \$D JOBCLASS | READ | jesx.DISPLAY.JOBCLASS | * | |
| \$D JOBQ | READ | jesx.DISPLAY.JST | * | |
| \$D O JOBQ | READ | jesx.DISPLAY.JSTOUT | * | |
| \$L JOBQ | READ | jesx.DISPLAY.JSTOUT | * | |
| \$D L(nnnn).JR(n) | READ | jesx.DISPLAY.L | * | |
| \$D L(nnnn).JT(n) | READ | jesx.DISPLAY.L | * | |
| \$D L(nnnn).SR(n) | READ | jesx.DISPLAY.L | * | |
| \$D L(nnnn).ST(n) | READ | jesx.DISPLAY.L | * | |
| \$D LINE | READ | jesx.DISPLAY.LINE | * | |
| \$D LOADmod | READ | jesx.DISPLAY.LOADMOD | * | |
| \$D MASDEF | READ | jesx.DISPLAY.MASDEF | * | |
| \$D MODULE | READ | jesx.DISPLAY.MODULE | * | |
| \$D NETSRV | READ | jesx.DISPLAY.NETSRV | * | |
| \$D NJEDEF | READ | jesx.DISPLAY.NJEDEF | * | |
| \$D NODE | READ | jesx.DISPLAY.NODE | * | |
| \$D OPTSDEF | READ | jesx.DISPLAY.OPTSDEF | * | |
| \$D PATH | READ | jesx.DISPLAY.PATH | * | |
| \$D PCE | READ | jesx.DISPLAY.PCE | * | |
| \$D F | READ | jesx.DISPLAY.QUE | * | |

| Controls on JES2 System Commands | | | | |
|----------------------------------|---------|-------------------------|------------|-----|
| JES2 command | Access | Resource-Name | Auth | Log |
| \$D RDI | READ | jesx.DISPLAY.RDI | * | |
| \$D REBLD | READ | jesx.DISPLAY.REBLD | * | |
| \$D REDIRect | READ | jesx.DISPLAY.REDIRECT | * | |
| \$D SOCKET | READ | jesx.DISPLAY.SOCKET | * | |
| \$D SPOOL | READ | jesx.DISPLAY.SPOOL | * | |
| \$D SPOOLDEF | READ | jesx.DISPLAY.SPOOLDEF | * | |
| \$D SRVCLASS | READ | jesx.display.SRVCLASS | * | |
| \$D SSI | READ | jesx.DISPLAY.SSI | * | |
| \$D S | READ | jesx.DISPLAY.STC | * | |
| \$D O S | READ | jesx.DISPLAY.STCOUT | * | |
| \$L S | READ | jesx.DISPLAY.STCOUT | * | |
| \$D SUBNET | READ | jesx.DISPLAY.SUBNET | * | |
| \$D JES2 | READ | jesx.DISPLAY.SYS | * | |
| \$D MEMBer | READ | jesx.DISPLAY.SYS | * | |
| \$D TRACE(x) | READ | jesx.DISPLAY.TRACE | * | |
| \$D T | READ | jesx.DISPLAY.TSU | * | |
| \$D O T | READ | jesx.DISPLAY.TSUOUT | * | |
| \$L T | READ | jesx.DISPLAY.TSUOUT | * | |
| \$F device | UPDATE | jesx.FORWARD.DEV | a o s t | Y |
| \$G C | UPDATE | jesx.GCANCEL.JOB | a o s t | Y |
| \$G D | READ | jesx.GDISPLAY.JOB | * | |
| \$G H | UPDATE | jesx.GMODIFYHOLD.JOB | a o s t | Y |
| \$G A | UPDATE | jesx.GMODIFYRELEASE.JOB | a o s t | Y |
| \$G R | UPDATE | jesx.GROUTE.JOBOUT | a o s t | Y |
| \$G R (for execution) | UPDATE | jesx.GROUTE.JOBOUT | a o s t | Y |
| \$Z A | CONTROL | jesx.HALT.AUTOCMD | a o s t | Y |
| \$Z device | UPDATE | jesx.HALT.DEV | a o s t | Y |
| \$Z OFFLOADn | UPDATE | jesx.HALT.DEV | a o s t | Y |
| \$Z I | CONTROL | jesx.HALT.INITIATOR | a o s t | Y |
| \$Z SPOOL | CONTROL | jesx.HALT.SPOOL | a o s t | Y |
| \$I device | UPDATE | jesx.INTERRUPT.DEV | a o s t | Y |
| \$MSPL | CONTROL | jesx.MIGRATE | a t | Y |
| \$T APPL | CONTROL | jesx.MODIFY.APPL | a o s t | Y |
| \$T A(CREATE) | READ | jesx.MODIFY.AUTOCMD | * | Y |
| \$T A(NOT OWNER) | CONTROL | jesx.MODIFY.AUTOCMD | a o s t | Y |
| \$T A(OWNER) | READ | jesx.MODIFY.AUTOCMD | * | Y |
| \$T J | UPDATE | jesx.MODIFY.BAT | a o s t | Y |
| \$T O J | UPDATE | jesx.MODIFY.BATOUT | a o s t \$ | Y |
| \$T BUFDEF | CONTROL | jesx.MODIFY.BUFDEF | a o s t | Y |
| \$T CKPTDEF | CONTROL | jesx.MODIFY.CKPTDEF | a o s t | Y |
| \$T CONDEF | CONTROL | jesx.MODIFY.CONDEF | a o s t | Y |
| \$T CONNECT | CONTROL | jesx.MODIFY.CONNECT | a o s t | Y |
| \$T DEBUG | CONTROL | jesx.MODIFY.DEBUG | a o s t | Y |

| Controls on JES2 System Commands | | | | |
|----------------------------------|---------|-----------------------|---------|-----|
| JES2 command | Access | Resource-Name | Auth | Log |
| \$T DESTDEF | CONTROL | jesx.MODIFY.DESTDEF | a o s t | Y |
| \$T DESTid | CONTROL | jesx.MODIFY.DESTID | a o s t | Y |
| \$T device | UPDATE | jesx.MODIFY.DEV | a o s t | Y |
| \$T ESTBYTE | CONTROL | jesx.MODIFY.ESTBYTE | a o s t | Y |
| \$T ESTIME | CONTROL | jesx.MODIFY.ESTIME | a o s t | Y |
| \$T ESTLNCT | CONTROL | jesx.MODIFY.ESTLNCT | a o s t | Y |
| \$T ESTPAGE | CONTROL | jesx.MODIFY.ESTPAGE | a o s t | Y |
| \$T ESTPUN | CONTROL | jesx.MODIFY.ESTPUN | a o s t | Y |
| \$T EXIT | CONTROL | jesx.MODIFY.EXIT | a o s t | Y |
| \$T FSS | CONTROL | jesx.MODIFY.FSS | a o s t | Y |
| \$T I | CONTROL | jesx.MODIFY.INITIATOR | a o s t | Y |
| \$T init stmt | CONTROL | jesx.MODIFY.initstmt | a o s t | Y |
| \$T INTRDR | CONTROL | jesx.MODIFY.INTRDR | a o s t | Y |
| \$T JOBCLASS | CONTROL | jesx.MODIFY.JOBCLASS | a o s t | Y |
| \$T JOBDEF | CONTROL | jesx.MODIFY.JOBDEF | a o s t | Y |
| \$T JOBPRTY | CONTROL | jesx.MODIFY.JOBPRTY | a o s t | Y |
| \$T JOBQ | UPDATE | jesx.MODIFY.JST | a o s t | Y |
| \$T O JOBQ | UPDATE | jesx.MODIFY.JSTOUT | a o s t | Y |
| \$T LINE | CONTROL | jesx.MODIFY.LINE | a o s t | Y |
| \$T LOADMOD | CONTROL | jesx.MODIFY.LOADMOD | a o s t | Y |
| \$T LOGON | CONTROL | jesx.MODIFY.LOGON | a o s t | Y |
| \$T MASDEF | CONTROL | jesx.MODIFY.MASDEF | a o s t | Y |
| \$T NETSRV | CONTROL | jesx.MODIFY.NETSRV | a o s t | Y |
| \$T NJEDEF | CONTROL | jesx.MODIFY.NJEDEF | a o s t | Y |
| \$T NODE | CONTROL | jesx.MODIFY.NODE | a o s t | Y |
| \$T NUM | CONTROL | jesx.MODIFY.NUM | a o s t | Y |
| \$T OFFx.yy | CONTROL | jesx.MODIFY.OFF | a o s t | Y |
| \$T OFFLOADx | CONTROL | jesx.MODIFY.OFFLOAD | a o s t | Y |
| \$T OUTCLASS | CONTROL | jesx.MODIFY.OUTCLASS | a o s t | Y |
| \$T OUTDEF | CONTROL | jesx.MODIFY.OUTDEF | a o s t | Y |
| \$T OUTPRTY | CONTROL | jesx.MODIFY.OUTPRTY | a o s t | Y |
| \$T PCE | CONTROL | jesx.MODIFY.PCE | a o s t | Y |
| \$T PRINTDEF | CONTROL | jesx.MODIFY.PRINTDEF | a o s t | Y |
| \$T RECVopts | CONTROL | jesx.MODIFY.RECVOPTS | a o s t | Y |
| \$T REDIRect | CONTROL | jesx.MODIFY.REDIRECT | a o s t | Y |
| \$T RMT | CONTROL | jesx.MODIFY.RMT | a o s t | Y |
| \$T SMFDEF | CONTROL | jesx.MODIFY.SMFDEF | a o s t | Y |
| \$T SOCKET | CONTROL | jesx.MODIFY.SOCKET | a o s t | Y |
| \$T SPOOL | CONTROL | jesx.MODIFY.SPOOL | a o s t | Y |
| \$T SPOOLDEF | CONTROL | jesx.MODIFY.SPOOLDEF | a o s t | Y |
| \$T SRVCLASS | CONTROL | jesx.MODIFY.SRVCLASS | a o s t | Y |
| \$T SSI | CONTROL | jesx.MODIFY.SSI | a o s t | Y |
| \$T S | UPDATE | jesx.MODIFY.STC | a o s t | Y |

| Controls on JES2 System Commands | | | | |
|----------------------------------|---------|------------------------|------------|-----|
| JES2 command | Access | Resource-Name | Auth | Log |
| \$T STCCLASS | CONTROL | jesx.MODIFY.STCCLASS | a o s t | Y |
| \$T O S | UPDATE | jesx.MODIFY.STCOUT | a o s t \$ | Y |
| \$T MEMBER(x) | CONTROL | jesx.MODIFY.SYS | a o s t | Y |
| \$T TPDEF | CONTROL | jesx.MODIFY.TPDEF | a o s t | Y |
| \$T TRACEDEF | CONTROL | jesx.MODIFY.TRACEDEF | a o s t | Y |
| \$T | UPDATE | jesx.MODIFY.TSU | a o s t | Y |
| \$T TSUCLASS | CONTROL | jesx.MODIFY.TSUCLASS | a o s t | Y |
| \$T O T | UPDATE | jesx.MODIFY.TSUOUT | a o s t \$ | Y |
| \$H J | UPDATE | jesx.MODIFYHOLD.BAT | a o s t \$ | Y |
| \$H A | UPDATE | jesx.MODIFYHOLD.JOB | a o s t | Y |
| \$H JOBQ | UPDATE | jesx.MODIFYHOLD.JST | a o s t | Y |
| \$H S | UPDATE | jesx.MODIFYHOLD.STC | a o s t \$ | Y |
| \$H T | UPDATE | jesx.MODIFYHOLD.TSU | a o s t \$ | Y |
| \$A J | UPDATE | jesx.MODIFYRELEASE.BAT | a o s t \$ | Y |
| \$A A | UPDATE | jesx.MODIFYRELEASE.JOB | a o s t | Y |
| \$A JOBQ | UPDATE | jesx.MODIFYRELEASE.JST | a o s t | Y |
| \$A S | UPDATE | jesx.MODIFYRELEASE.STC | a o s t | Y |
| \$A T | UPDATE | jesx.MODIFYRELEASE.TSU | a o s t | Y |
| \$M | READ | jesx.MSEND.CMD | a o s t \$ | Y |
| \$N | READ | jesx.NSEND.CMD | a o s t | Y |
| \$O J | UPDATE | jesx.RELEASE.BATOUT | a o s t \$ | Y |
| \$O JOBQ | UPDATE | jesx.RELEASE.JSTOUT | a o s t | Y |
| \$O S | UPDATE | jesx.RELEASE.STCOUT | a o s t \$ | Y |
| \$O T | UPDATE | jesx.RELEASE.TSUOUT | a o s t \$ | Y |
| \$N device | UPDATE | jesx.REPEAT.DEV | a o s t | Y |
| \$E J | CONTROL | jesx.RESTART.BAT | a o s t \$ | Y |
| \$E device | UPDATE | jesx.RESTART.DEV | a o s t | Y |
| \$E OFFn.JT | UPDATE | jesx.RESTART.DEV | a o s t | Y |
| \$E OFFn.ST | UPDATE | jesx.RESTART.DEV | a o s t | Y |
| \$E LINE(x) | CONTROL | jesx.RESTART.LINE | a o s t | Y |
| \$E LOGON(x) | CONTROL | jesx.RESTART.LOGON | a o s t | Y |
| \$E NETSRV | CONTROL | jesx.RESTART.NETSRV | a o s t | Y |
| \$E CKPTLOCK | CONTROL | jesx.RESTART.SYS | a o s t | Y |
| \$E MEMBER() | CONTROL | jesx.RESTART.SYS | a o s t | Y |
| \$R ALL | UPDATE | jesx.ROUTE.JOBOUT | a o s t \$ | Y |
| \$R PRT | UPDATE | jesx.ROUTE.JOBOUT | a o s t \$ | Y |
| \$R PUN | UPDATE | jesx.ROUTE.JOBOUT | a o s t \$ | Y |
| \$R XEQ | UPDATE | jesx.ROUTE.JOBOUT | a o s t \$ | Y |
| \$D M | READ | jesx.SEND.MESSAGE | a o s t | Y |
| \$S A | CONTROL | jesx.START.AUTOCMD | a o s t | Y |
| \$S J | UPDATE | jesx.START.BAT | a o s t | Y |
| \$S device | UPDATE | jesx.START.DEV | a o s t | Y |
| \$S OFFLOADn | UPDATE | jesx.START.DEV | a o s t | Y |

| Controls on JES2 System Commands | | | | |
|----------------------------------|---------|----------------------|---------|-----|
| JES2 command | Access | Resource-Name | Auth | Log |
| \$S OFFn.JR | UPDATE | jesx.START.DEV | a o s t | Y |
| \$S OFFn.JT | UPDATE | jesx.START.DEV | a o s t | Y |
| \$S OFFn.SR | UPDATE | jesx.START.DEV | a o s t | Y |
| \$S OFFn.ST | UPDATE | jesx.START.DEV | a o s t | Y |
| \$S I | CONTROL | jesx.START.INITIATOR | a o s t | Y |
| \$S LINE(x) | CONTROL | jesx.START.LINE | a o s t | Y |
| \$S LOGON(x) | CONTROL | jesx.START.LOGON | a o s t | Y |
| \$S N | CONTROL | jesx.START.NET | a o s t | Y |
| \$S RMT(x) | CONTROL | jesx.START.RMT | a o s t | Y |
| \$S SPOOL | CONTROL | jesx.START.SPOOL | a o s t | Y |
| \$S SRVCLASS | CONTROL | jesx.START.SRVCLASS | a o s t | Y |
| \$S | CONTROL | jesx.START.SYS | a o s t | Y |
| \$S XEQ | CONTROL | jesx.START.SYS | a o s t | Y |
| \$S TRACE(x) | CONTROL | jesx.START.TRACE | a o s t | Y |
| \$P O J | UPDATE | jesx.STOP.BATOUT | a o s t | Y |
| \$PO JOB | UPDATE | jesx.STOP.BATOUT | a o s t | Y |
| \$P device | UPDATE | jesx.STOP.DEV | a o s t | Y |
| \$P OFFLOADn | UPDATE | jesx.STOP.DEV | a o s t | Y |
| \$P OFFn.JR | UPDATE | jesx.STOP.DEV | a o s t | Y |
| \$P OFFn.JT | UPDATE | jesx.STOP.DEV | a o s t | Y |
| \$P OFFn.SR | UPDATE | jesx.STOP.DEV | a o s t | Y |
| \$P OFFn.ST | UPDATE | jesx.STOP.DEV | a o s t | Y |
| \$P I | CONTROL | jesx.STOP.INITIATOR | a o s t | Y |
| \$P JOBQ | UPDATE | jesx.STOP.JST | a o s t | Y |
| \$P O JOBQ | UPDATE | jesx.STOP.JSTOUT | a o s t | Y |
| \$PO JOBQ | UPDATE | jesx.STOP.JSTOUT | a o s t | Y |
| \$P LINE(x) | CONTROL | jesx.STOP.LINE | a o s t | Y |
| \$P LOGON(x) | CONTROL | jesx.STOP.LOGON | a o s t | Y |
| \$P NETSRV | CONTROL | jesx.STOP.NETSRV | a o s t | Y |
| \$P RMT(x) | CONTROL | jesx.STOP.RMT | a o s t | Y |
| \$P SPOOL | CONTROL | jesx.STOP.SPOOL | a o s t | Y |
| \$P SRVCLASS | CONTROL | jesx.STOP.SRVCLASS | a o s t | Y |
| \$P S | UPDATE | jesx.STOP.STC | a o s t | Y |
| \$P O S | UPDATE | jesx.STOP.STCOUT | a o s t | Y |
| \$PO STC | UPDATE | jesx.STOP.STCOUT | a o s t | Y |
| \$P | CONTROL | jesx.STOP.SYS | a o s t | Y |
| \$P JES2 | CONTROL | jesx.STOP.SYS | a o s t | Y |
| \$P XEQ | CONTROL | jesx.STOP.SYS | a o s t | Y |
| \$P TRACE(x) | CONTROL | jesx.STOP.TRACE | a o s t | Y |
| \$P T | UPDATE | jesx.STOP.TSU | a o s t | Y |
| \$P O T | UPDATE | jesx.STOP.TSUOUT | a o s t | Y |
| \$PO TSU | UPDATE | jesx.STOP.TSUOUT | a o s t | Y |
| \$VS* | CONTROL | jesx.VS | a o s t | Y |

| Controls on JES2 System Commands | | | | |
|----------------------------------|---------|-------------------------|---------|-----|
| JES2 command | Access | Resource-Name | Auth | Log |
| \$ZAPJOB | CONTROL | jesx.ZAP.JOB | a o s t | Y |
| \$JD DETAILS | READ | jesxMON.DISPLAY.DETAIL | * | |
| \$JD HISTORY | READ | jesxMON.DISPLAY.HISTORY | * | |
| \$JD JES | READ | jesxMON.DISPLAY.JES | * | |
| \$JD MONITOR | READ | jesxMON.DISPLAY.MONITOR | * | |
| \$JD STATUS | READ | jesxMON.DISPLAY.STATUS | * | |
| \$J STOP | CONTROL | jesxMON.STOP.MONITOR | a o s t | Y |

Auth column

a - AUTOAUDT, Automated operations.

o - OPERAUDT, Operations staff

s - SYSPAUDT, Systems Programming staff

t - TSTCAUDT, Trusted Started Tasks

* - All Users

\$ - May be given to All Users using SDSF, CA Roscoe, and similar products that interface with a user's input/output requiring the issuing of console commands.

Log

Y

Note: ALTER authority on RACF profiles: For discrete profiles, ALTER allows some RACF Administrative functions such as use of the RDELETE Command. For this reason, access should be permitted based on the table above. ALTER should be flagged for all but Security Administrators or where justified by the ISSO.

Resource access requirements are based on IBM minimal access requirements. Users that are authorized to have access to the resource can have the access specified or greater. The exceptions are those stated with the resource, resources that specify different accesses to users and above note. Where multiple users have different accesses, an example is one user has READ and another has UPDATE the "access specified or greater" will be to the user with UPDATE.

8. SENSITIVE UTILITY REQUIREMENT**Table 8-1: Sensitive Utility Controls**

Referenced by: ACP00320, RACF0770, TSS1040, ACF0380, and ACF0870

| Sensitive Utility Controls | | | |
|---|--------------------|---|--|
| Program | Product | Function | Auth |
| AHLGTF HHLGTF IHLGTF | z/OS | System Activity Tracing | STCGAUDT (users can issue started task only) |
| ICPIOCP IOPIOCP IXPIOCP IYPIOCP IZPIOCP | z/OS | System Configuration | SYSPAUDT |
| BLSROPTR | z/OS | Data Management | DASBAUDT DASDAUDT SYSPAUDT |
| DEBE | OS/DEBE | Data Management | DASDAUDT TAPEAUDT |
| DITTO | OS/DITTO | Data Management | DASDAUDT TAPEAUDT |
| FDRZAPOP | FDR | Product Internal Modification | SYSPAUDT |
| GIMSMP | SMP/E | Change Management Product | AUDTAUDT DABAAUDT SYSPAUDT |
| ICKDSF | z/OS | DASD Management | DASDAUDT SYSPAUDT Userid assigned to DEVMAN STC |
| IDCSC01 | z/OS | IDCAMS Set Cache Module | SYSPAUDT |
| IEHINITT | z/OS | Tape Management | TAPEAUDT |
| IFASMFD | z/OS | SMF Data Dump Utility | AUDTAUDT PCSPAUDT SECAAUDT SMFBAUDT SYSPAUDT MICSADM* |
| IND\$FILE | z/OS | PC to Mainframe File Transfer (Applicable only for classified systems) | |
| CSQJU003 CSQJU004 CSQUCVX CSQ1LOGP | IBM WebSphereMQ | | MQSAAUDT |
| CSQUTIL | IBM WebSphereMQ | | AUDTAUDT MQSAAUDT |

| Sensitive Utility Controls | | | |
|----------------------------|---------|--|--|
| Program | Product | Function | Auth |
| WHOIS | z/OS | Share MOD to identify user name from USERID. Restricted to data center personnel only. | DASDAUDT OPERAUDT SYSPAUDT TAPEAUDT |

The following Sensitive Utilities will be checked or not checked for the reason specified.

AMDIOCP - May be in use on Fujitsu 5990, 5995a, and 5995m processors.

AMZIOCP - May be in use on Fujitsu Millennium and Omniflex processors.

DEBE - Check only if DEBE is installed on system.

DITTO - Check only if DITTO/ESA is installed on system.

FDRZAPOP - Check only if FDR from Innovation Data Processing is installed on system.

IND\$FILE - Check only on Classified systems.

CSQxxxx - Check only if WebSphere MQ is installed.

* This access is allowed at the discretion of the site ISSM/ISSO.

9. SMS PROGRAM REQUIREMENT

Items highlighted in yellow below should be authorized for User/Customer Community upon request.

DGTFMD01 module is the primary panel/initial entry into ISMF so that should be okay for all users.

Table 9-1: SMS Program Resources

Referenced by: ZSMS0012

| SMS Program Resources | |
|-----------------------|-----------|
| SMS Program | Authority |
| ACBFUTO2 | a d e s t |
| ACBFUTO3 | a d e s t |
| ACBFUTO4 | a d e s t |
| ACBFUTO6 | a d e s t |
| ACBFUTO7 | a d e s t |
| DFQFCND1 | * |
| DFQFHA01 | * |
| DFQFHB01 | * |
| DFQFHBD1 | * |
| DFQFHD01 | * |
| DFQFHM01 | * |
| DFQFHRC1 | * |
| DFQFHRL1 | * |
| DGTFACAT | d e s t |
| DGTFADAD | d e s t |
| DGTFAGAA | d e s t |
| DGTFAGCD | * |
| DGTFAGDA | d e s t |
| DGTFAGDI | * |
| DGTFAGLD | * |
| DGTFAL01 | * |
| DGTFAL11 | d e s t |
| DGTFALD1 | d e s t |
| DGTFALG1 | d e s t |
| DGTFALH1 | d e s t |
| DGTFALL1 | d e s t |
| DGTFALM1 | d e s t |
| DGTFALP1 | d e s t |
| DGTFALR1 | d e s t |
| DGTFALS1 | d e s t |
| DGTFALY1 | d e s t |
| DGTFAU01 | d e s t |
| DGTFAU02 | d e s t |
| DGTFAU04 | d e s t |

| SMS Program Resources | |
|-----------------------|-----------|
| SMS Program | Authority |
| DGTFAUL1 | d e s t |
| DGTFAZ01 | d e s t |
| DGTFBR01 | * |
| DGTFBX01 | d e s t |
| DGTFCAD1 | d e s t |
| DGTFCAG1 | d e s t |
| DGTFCAH1 | d e s t |
| DGTFCAL1 | d e s t |
| DGTFCAM1 | d e s t |
| DGTFCAP1 | d e s t |
| DGTFCAR1 | d e s t |
| DGTFCAS1 | d e s t |
| DGTFCAY1 | d e s t |
| DGTFCB01 | d e s t |
| DGTFCCL01 | * |
| DGTFCM01 | * |
| DGTFCN01 | d e s t |
| DGTFCO01 | * |
| DGTFCP01 | * |
| DGTFCPAA | d e s t |
| DGTFCPCD | d e s t |
| DGTFCPDA | d e s t |
| DGTFCPDI | d e s t |
| DGTFCPLD | d e s t |
| DGTFCR01 | * |
| DGTFCS01 | d e s t |
| DGTFACT01 | d e s t |
| DGTFCV01 | d e s t |
| DGTFCY01 | * |
| DGTFDCAA | d e s t |
| DGTFDCCD | * |
| DGTFDCCA | d e s t |
| DGTFDCDI | * |
| DGTFDCLD | * |
| DGTDFD01 | d e s t |
| DGTFDID1 | * |
| DGTFDIH1 | * |
| DGTFDIL1 | d e s t |
| DGTFDIM1 | * |
| DGTFDIP1 | d e s t |
| DGTFDIR1 | d e s t |
| DGTFDIS1 | * |
| DGTFDIY1 | d e s t |
| DGTFDL01 | * |

| SMS Program Resources | |
|-----------------------|-----------|
| SMS Program | Authority |
| DGTFTDM01 | dest |
| DGTFTDND1 | dest |
| DGTFTDNG1 | dest |
| DGTFTDNH1 | dest |
| DGTFTDNL1 | dest |
| DGTFTDNM1 | * |
| DGTFTDNP1 | dest |
| DGTFTDNR1 | dest |
| DGTFTDNS1 | dest |
| DGTFTDNY1 | dest |
| DGTFTDO01 | * |
| DGTFTDP01 | * |
| DGTFTDS00 | * |
| DGTFTDU01 | * |
| DGTFTED01 | * |
| DGTTFEF01 | dest |
| DGTTFEJ01 | dest |
| DGTTFEL01 | dest |
| DGTTFER02 | dest |
| DGTTFFI01 | * |
| DGTFFLAD | dest |
| DGTFFN01 | * |
| DGTFFU01 | * |
| DGTFFHI01 | * |
| DGTFFIL01 | dest |
| DGTFFIN01 | dest |
| DGTFFIV01 | dest |
| DGTFFJLCD | * |
| DGTFFLCAL | dest |
| DGTFFLCCD | dest |
| DGTFFLCDE | dest |
| DGTFFLCDI | dest |
| DGTFFLCLD | dest |
| DGTFFLE01 | * |
| DGTFFLIC1 | dest |
| DGTFFLL01 | * |
| DGTFFLMAL | dest |
| DGTFFLMCD | dest |
| DGTFFLMDE | dest |
| DGTFFLMDI | dest |
| DGTFFMLD | dest |
| DGTFFLVC1 | pdest |
| DGTFFLVL1 | dest |
| DGTFFMCAA | dest |

| SMS Program Resources | |
|-----------------------|-------------|
| SMS Program | Authority |
| DGTFMCCD | * |
| DGTFMCDA | d e s t |
| DGTFMCDI | * |
| DGTFMCLD | * |
| DGTFMD01 | * |
| DGTFMS00 | * |
| DGTFOVCD | d e s t |
| DGTFPF00 | * |
| DGTFPF01 | * |
| DGTFPF02 | * |
| DGTFPF03 | * |
| DGTFPF04 | * |
| DGTFPF05 | p d e s t |
| DGTFPF20 | d e s t |
| DGTFPF21 | * |
| DGTFPF22 | * |
| DGTFPR01 | * |
| DGTFRA01 | d e s t |
| DGTFRB01 | d e s t |
| DGTFRC01 | * |
| DGTFRCAL | d e s t |
| DGTFRCCD | d e s t |
| DGTFRCDE | d e s t |
| DGTFRCDI | d e s t |
| DGTFRCLD | d e s t |
| DGTFRE01 | * |
| DGTFRF01 | d e s t |
| DGTFRI01 | * |
| DGTFRL01 | * |
| DGTFRML1 | d e s t |
| DGTFRO01 | d e s t |
| DGTFRR00 | * |
| DGTFRT01 | * |
| DGTFRV01 | d e s t |
| DGTFRW01 | * |
| DGTF SACD | d e s t |
| DGTFSCAA | d e s t |
| DGTFSCCD | * |
| DGTFSCDA | d e s t |
| DGTFSCDI | * |
| DGTFSCLD | * |
| DGTFSGAR | d e s t |
| DGTFSGDR | p b d e s t |
| DGTFSGFR | d e s t |

| SMS Program Resources | |
|-----------------------|-------------|
| SMS Program | Authority |
| DGTFSGLD | p b d e s t |
| DGTFSGVR | d e s t |
| DGTFSLDS | * |
| DGTFSO01 | * |
| DGTFSRD1 | * |
| DGTFTVCD | d e s t |
| DGTFUP01 | * |
| DGTFUS01 | * |
| DGTFVA00 | p d e s t |
| DGTFVLVA | d e s t |
| DGTFVW01 | * |

a - AUDTAUDT
b - DASBAUDT
d - DASDAUDT
e - SECAAUDT
s - SYSPAUDT
t - TSTCAUDT
p - PCSPAUDT
* - All Users

10. Z/OS BASELINE REQUIREMENTS

Referenced by: ACP00340

DISA Requirement a. (SD) 527-1 dated 27 Jan 2006 b. INFOCON 3

Need to Baseline z/OS:

1. DISA has determined based upon references (a) and (b) that all 'servers' including z/OS Mainframes shall perform 'baseline' reporting.
2. DISA has acquired throughout the enterprise a product called CA-AUDITOR on z/OS Mainframes. The old and commonly known name of this product is CA-Examine. CA-Auditor provides a new feature available starting with R12 - called "baseline" which uses a started task called EXAMMON. Currently there are 15 functional areas that can be "baselined" and shall be implemented to meet the DOD requirement for "baseline" of "servers" (z/OS Mainframes). For ACP00340, we will only use **two** of these reports.

Basic process required per reference (a):

1. For INFOCON 5 - EXAMMON Policy control statements shall ensure the process run minimally every 180 days with responsible team members validating baseline analysis results (the delta as reported).
2. For INFOCON 4 - EXAMMON Policy control statements shall ensure the process run minimally every 90 days with responsible team members validating baseline analysis results (the delta as reported).
3. For INFOCON 3 - EXAMMON Policy control statements shall ensure the process run minimally every 60 days with responsible team members validating baseline analysis results (the delta as reported).
4. For INFOCON 2 - EXAMMON Policy control statements shall ensure the process run minimally every 30 days with responsible team members validating baseline analysis results (the delta as reported).

CA-Auditor Baseline Functions for ACP00340:

Note: These function codes (the numeric codes below) directly correspond to the CA-Auditor panels in such much that "221" is panel "2.2.1" and "243" would then be "2.4.3", just insert a "." between the numbers.

- 221** APF library stats (# of libraries in APF list, # duplicate libraries in APF list, # accessible of libraries in APF list, # of members in APF libraries, # of members linked with AC=1, # of APF libraries in LINKLIST/LPA, # duplicate of APF libraries in LINKLIST/APF, # of accessible APF libraries in LINKLIST/LPA, # of members in authorized LINKLIST/LPA, # of members links AC=1 in LINKLIST/LPA, total # of APF libraries, total # of unique APF libraries , total # of members with AC=1, total % of

members with AC=1, APF datasets. This functional name will correspond to the dataset report file name that ends in "CS221C".

- 243** LPA library display (LPA libraries added/removed, last accessed date for LPA libraries). This functional name will correspond to the dataset report file name that ends in "CS243C".

Basic Procedures to get started:

1. Procedures required to fully implement Baseline Functions on z/OS Mainframe domains that are licensed for CA-AUDITOR:

Software CA-Auditor R12SP00 or most current version must be installed. Validate that the EXAMMON policy control statements are set to run the baseline per the required schedule (weekly, monthly, every 60 days, etc.) Details as to the format of the policy control statements/records are found in the technical reference guide for CA-Auditor - Chapter 13. Ensure local procedures are in place to have the responsible team members' review the output of the Baseline reports (as stored in the specific GDG Datasets) and review/process of the online Alerts per each Mainframe domain.

Datasets that contain the actual baseline reports:

Note: These are merely examples, the actual dataset names depend upon the DISA Site and domain implementation and definition of the GDG bases. Regardless, all report dataset last qualifier will indicate the "report name" such as "2.2.1." CA-Auditor panel corresponds to the Policy Control Function name of "221" and corresponds to the report dataset that ends in "CS221C" as documented above. CA-Auditor dynamically builds the "mem" as part of the automated process which is used as input for the actual report dataset name. **The output data sets must be GDG data sets.**

SYSID = 'SYSID' of System Baseline is running on

ESM = 'ESM' running on Baseline System ex. (ACF2, RACF, TSS)

SYSID ESM.BASELINE.FUNCTION.CS221C

SYSID.ESM.BASELINE.FUNCTION.CS221C.G0001V00

SYSID ESM.BASELINE.FUNCTION.CS243C

SYSID ESM.BASELINE.FUNCTION.CS243C.G0001V00

See Sample output below:

Report CS221C:

PAGE

ETRUST CA EXAMINE BASELINE ANALYSIS INFORMATION

BASELINE ANALYSIS DATA

=====

BASELINE CHANGE DELTA DETAIL

FUNCTION: 2.2.1 APF STATS SUMMARY

BASELINE DATE: TUESDAY, 16 DECEMBER 2008 TIME: 11:10:46

CURRENT DATE: SUNDAY, 26 APRIL 2009 TIME: 05:23:01

SYSTEM SMFID: XXX

=====

- BASELINE: NUMBER OF LIBS IN APF LIST: 180
- CURRENT : NUMBER OF LIBS IN APF LIST: 181
- THE NUMBER OF APF LIBRARIES DIFFERS FROM THE SAVED BASELINE
- A CHANGE WAS MADE TO THE APF LIST
- IDENTIFY HOW CHANGE WAS MADE, WHETHER IT IS PROPER

- BASELINE: NUMBER OF ACCESSIBLE LIBS IN APF LIST: 180
- CURRENT : NUMBER OF ACCESSIBLE LIBS IN APF LIST: 180
- THE NUMBER OF ACCESSIBLE APF LIBS DIFFERS FROM SAVED BASELINE
- DATA SETS ARCHIVED/DELETED/MOVED/UNCATALOGED/RECATALOGED
- IDENTIFY WHY CHANGE OCCURRED, VERIFY IF IT IS PROPER

- BASELINE: NUMBER OF MEMBERS IN ACCESSIBLE APF LIBS: 56,679
 - CURRENT : NUMBER OF MEMBERS IN ACCESSIBLE APF LIBS: 56,679
 - THE # OF MEMBERS IN ACCESSIBLE APF LIBS DIFFERS FROM SAVED BASELINE
 - NUMEROUS METHODS
 - VALIDATE SPECIFIC CHANGE(S), VERIFY IF PROPER
-
- BASELINE: NUMBER OF MEMBERS LINKED AC=1 IN APF LIST: 4,295
 - CURRENT : NUMBER OF MEMBERS LINKED AC=1 IN APF LIST: 4,320
 - THE NUMBER OF AC=1 APF MEMBERS DIFFERS FROM SAVED BASELINE
 - NUMEROUS METHODS
 - VALIDATE SPECIFIC CHANGE(S), VERIFY IF PROPER
-
- BASELINE: NUMBER OF MEMBERS IN AUTHORIZED LINKLIST: 30,499
 - CURRENT : NUMBER OF MEMBERS IN AUTHORIZED LINKLIST: 30,499
 - NUMBER OF AUTHORIZED LINKLIST LIB MEMBERS DIFFERS FROM BASELINE
 - NUMEROUS METHODS
 - VALIDATE SPECIFIC CHANGE(S), VERIFY IF PROPER
-
- BASELINE: NUMBER LINKED WITH AC=1 IN LINKLIST: 1,876
 - CURRENT : NUMBER LINKED WITH AC=1 IN LINKLIST: 1,876
 - NUMBER AC=1 LINKLIST MEMBERS DIFFERS FROM BASELINE
 - NUMEROUS METHODS
 - VALIDATE SPECIFIC CHANGE(S), VERIFY IF PROPER
-
- BASELINE: TOTAL NUMBER OF APF LIBS: 266
 - CURRENT : TOTAL NUMBER OF APF LIBS: 266
 - NUMBER OF APF LIBRARIES DIFFERS FROM BASELINE
 - NUMEROUS METHODS
 - VALIDATE SPECIFIC CHANGE(S), VERIFY IF PROPER

xxx
14

PAGE

ETRUST CA EXAMINE BASELINE ANALYSIS INFORMATION

- BASELINE: TOTAL OF UNIQUE APF LIBS: 181
- CURRENT : TOTAL OF UNIQUE APF LIBS: 181
- NUMBER OF UNIQUE APF LIBS DIFFERS FROM BASELINE
- NUMEROUS METHODS
- VALIDATE SPECIFIC CHANGE(S), VERIFY IF PROPER
- BASELINE: TOTAL OF ACCESSIBLE APF LIBS: 181
- CURRENT : TOTAL OF ACCESSIBLE APF LIBS: 181
- NUMBER ACCESSIBLE APF LIBS DIFFERS FROM BASELINE
- NUMEROUS METHODS
- VALIDATE SPECIFIC CHANGE(S), VERIFY IF PROPER
- BASELINE: TOTAL OF UNIQUE MEMBERS IN APF LIBS: 56,825
- CURRENT : TOTAL OF UNIQUE MEMBERS IN APF LIBS: 56,825
- NUMBER UNIQUE APF MEMBERS DIFFERS FROM BASELINE
- NUMEROUS METHODS
- VALIDATE SPECIFIC CHANGE(S), VERIFY IF PROPER
- BASELINE: TOTAL MEMBERS WITH AC=1: 4,295
- CURRENT : TOTAL MEMBERS WITH AC=1: 4,295
- NUMBER AC=1 MEMBERS DIFFERS FROM BASELINE
- NUMEROUS METHODS
- VALIDATE SPECIFIC CHANGE(S), VERIFY IF PROPER
- BASELINE: PERCENTAGE OF AC=1: 7.56
- CURRENT : PERCENTAGE OF AC=1: 7.56
- AC=1 PERCENTAGE DIFFERS FROM BASELINE
- NUMEROUS METHODS
- USE AS GUIDE - AUDIT SPECIFIC MEMBERS IF IS OF CONCERN

=====

BASELINE CHANGE DELTA DETAIL

FUNCTION: 2.2.1 APF DATASETS

BASELINE DATE: TUESDAY, 16 DECEMBER 2008 TIME: 11:10:46

CURRENT DATE: SUNDAY, 26 APRIL 2009 TIME: 05:23:01

SYSTEM SMFID: XXX

=====

- BASELINE: APF DSN HAD THE FOLLOWING STATS:
- DSN: SYS2A.CADELIVE.V110701.CAILIB VOL: MYASS3
- NUMBER OF MEMBERS WITH AC=1: 124 TOTAL MEMBERS: 326
- CURRENT : APF DSN HAS THE FOLLOWING STATS:
- DSN: SYS2A.CADELIVE.V110701.CAILIB VOL: MYASS3
- NUMBER OF MEMBERS WITH AC=1: 124 TOTAL MEMBERS: 327

- BASELINE: APF DSN HAD THE FOLLOWING STATS:
- DSN: SYS2A.TSS.V12SP01.CAILIB VOL: MYASS1
- NUMBER OF MEMBERS WITH AC=1: 89 TOTAL MEMBERS: 382
- CURRENT : APF DSN HAS THE FOLLOWING STATS:
- DSN: SYS2A.TSS.V12SP01.CAILIB VOL: MYASS1
- NUMBER OF MEMBERS WITH AC=1: 90 TOTAL MEMBERS: 382

XXX

PAGE

15

ETRUST CA EXAMINE BASELINE ANALYSIS INFORMATION

- BASELINE: APF DSN HAD THE FOLLOWING STATS:
- DSN: SYS2A.VIEW.V110603.CAILIB VOL: MYASS3
- NUMBER OF MEMBERS WITH AC=1: 35 TOTAL MEMBERS: 281
- CURRENT : APF DSN HAS THE FOLLOWING STATS:
- DSN: SYS2A.VIEW.V110603.CAILIB VOL: MYASS3
- NUMBER OF MEMBERS WITH AC=1: 35 TOTAL MEMBERS: 282

xxx

PAGE

18

ETRUST CA EXAMINE AUDITING APF LIBRARY STATISTICS SUMMARY

PRESS ENTER FOR DETAILED DISPLAY.

```
+----- APF LIST INFORMATION -----+----- LINK LIST INFORMATION
+-----+
|                                     |
| LIBRARY NAMES SPECIFIED: 181      | APF LIBRARIES SPECIFIED: 86
| DUPLICATE LIBRARY NAMES: 0        | DUPLICATE LIBRARY NAMES: 0
| ACCESSIBLE LIBRARIES: 181         | ACCESSIBLE LIBRARIES: 86
| ACCESSED LIBRARY MEMBERS: 55,242 | ACCESSED LIBRARY MEMBERS:
30,505 |
| JOBSTEP APF AUTH MEMBERS: 4,320 | JOBSTEP APF AUTH MEMBERS:
1,877 |
|                                     |
|--- CONSOLIDATED LIST INFORMATION ----+----- LINK PACK AREA
-----|
|                                     |
| LIBRARY NAMES SPECIFIED: 267      | NUMBER OF UNIQUE MODULES:
2,362 |
| NET UNIQUE LIBRARY NAMES: 182     | JOBSTEP APF AUTH MODULES: 327
| NET ACCESSIBLE LIBRARIES: 182     | PERCENT AUTHORIZED:
13.84 |
| ACCESSED LIBRARY MEMBERS: 55,388 |
| JOBSTEP APF AUTH MEMBERS: 4,320 | MEMORY-BASED LPA IS AN
ADDITIONAL |
| PERCENT AUTHORIZED: 7.80         | SOURCE OF APF-AUTHORIZED
MODULES |
|                                     |
+-----+-----+-----+
-----+
```

Report: CS243C:

xxx PAGE
14 ETRUST CA EXAMINE BASELINE ANALYSIS INFORMATION

BASELINE ANALYSIS DATA

=====

BASELINE CHANGE DELTA DETAIL

FUNCTION: 2.4.1 KEY APF LIBRARIES

BASELINE DATE: TUESDAY, 16 DECEMBER 2008 TIME: 11:11:26

CURRENT DATE: SUNDAY, 26 APRIL 2009 TIME: 05:23:12

SYSTEM SMFID: xxx

=====

...

- THE FOLLOWING APF LIBS WERE ADDED:
- DSN: SYS2.CICSTS.V320807.CPSM.SEYUAUTH VOL: MYAS26
- DSN: SYS2.CICSTS.V320807.SDFHAUTH VOL: MYAS44
- DSN: SYS2.CICSTS.V320807.SDFJAUTH VOL: MYAS49
- DSN: SYS2.CICSTS.V320807.SDFJLPA VOL: MYAS2K
- DSN: SYS2.MICS.V120804.LOADLIB VOL: xxxxxx
- DSN: SYS2.MIMGR.V116SP02.APFLOAD VOL: xxxxxx
- DSN: SYS2.QUICKREF.V690.QWILINK VOL: xxxxxx
- DSN: SYS2.SYMUPDTE.V05325.LOAD VOL: xxxxxx
- DSN: SYS2A.CICSTS.V320807.CPSM.SEYULINK VOL: xxxxxx
- DSN: SYS2A.CICSTS.V320807.CPSM.SEYULPA VOL: xxxxxx
- DSN: SYS2A.CICSTS.V320807.SDFHEXCI VOL: xxxxxx
- DSN: SYS2A.CICSTS.V320807.SDFHLINK VOL: xxxxxx
- DSN: SYS2A.CICSTS.V320807.SDFHLPA VOL: xxxxxx

- THE FOLLOWING APF LIBS WERE REMOVED:

- DSN: SYS2.CICSTS.V310601.CPSM.SEYUAUTH VOL: xxxxxx

- DSN: SYS2.CICSTS.V310601.SDFHAUTH VOL: xxxxxx

- DSN: SYS2.CICSTS.V310601.SDFJLPA VOL: xxxxxx

- DSN: SYS2.CICSTS.V310611.SDFJAUTH VOL: xxxxxx

- DSN: SYS2.MIMGR.V116.APFLOAD VOL: xxxxxx

- DSN: SYS2.QUICKREF.V680.QWILINK VOL: xxxxxx

- DSN: SYS2.SYMUPDTE.V01271.LOAD VOL: xxxxxx

- DSN: SYS2A.CICSTS.V310601.CPSM.SEYULINK VOL: xxxxxx

- DSN: SYS2A.CICSTS.V310601.SDFHEXCI VOL: xxxxxx

- DSN: SYS2A.CICSTS.V310601.SDFHLINK VOL: xxxxxx

- DSN: SYS2A.CICSTS.V310611.CPSM.SEYULPA VOL: xxxxxx

- DSN: SYS2A.CICSTS.V310611.SDFHLPA VOL: xxxxxx

***** Bottom of Data *****

11. PRODUCT REQUIREMENTS

11.1 General Installed Product Information

Installed product will have checks for the protection of the installation datasets; privileged function datasets; datasets used by the product or product configuration datasets. To assist in the review, certain examples maybe identified for clarity of explanation of certain installation, STC, JCL, and user dataset categories.

Please note that the data sets and/or data set prefixes identified are only examples of a possible installation. The actual data sets and/or prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific. The site's Product System programmer will have the specific information for each installation.

11.2 BMC INCONTROL Resource Requirements

Table 11-1: BMC IOA Resources

Referenced by: ZIOA0020

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|--------|
| \$\$ADDCND | None | AUTOAUDT OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$ADDCTL | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$ADDRES | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CHARES | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CHKCND | None | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CHKCTL | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CHKRES | None | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$DELCND | None | AUTOAUDT | Read |

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|--------|
| | | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | |
| \$\$DELCTL | Read | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$DELRES | Read | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$ERACND | Read | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOAAS | Read | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOACMD | Read | AUTOAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOADEL | None | DPCSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOADIR | None | * | Read |
| \$\$IOAEDM | None | * | Read |
| \$\$IOAEDT | None | DPCSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOAGL | Read | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOAONLINE | None | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOARES | Read | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOASAV | None | DPCSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOAUTL | Read | AUTOAUDT OPERAUDT PCSPAUDT | Read |

| Resource Names | Logging | User Group | Access |
|------------------|---------|--|----------|
| | | SYSPAUDT | |
| \$\$IOAVD | Read | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOAVP | Read | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$IOAVIW | None | DPCSAUDT OPERAUDT PCSPAUDT SYSPAUDT IOABAUDT | Read |
| \$\$NEWCND | None | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$SECIOA.qname | None | * | ReadRead |

Table 11-2: BMC Control-D Resources

Referenced by: ZCTD0020

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|--------|
| \$\$ADDNOT | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Alter |
| \$\$ADNASR | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$BKPORD | None | APPSAUDT BMC STCs OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CDDSEL | None | APPSAUDT SYSPAUDT | Read |
| \$\$CHKRCL | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTDACT | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTDASR | Read | APPSAUDT | Read |

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|--------|
| | | OPERAUDT PCSPAUDT SYSPAUDT | |
| \$\$CTDCDD | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTDEDM | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTDJOB | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTDOBJ | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTDPNLA | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTDPNLF | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTDPREFIX | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTDPRF | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTDRRST | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$DELNOT | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$DLNASR | None | APPSAUDT OPERAUDT PCSPAUDT | Read |

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|--------|
| | | SYSPAUDT | |
| \$\$DPC1VIE | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$DPC2FRE | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$DPC2HLD | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$DPC3DEL | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$DPC3PRN | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$DPC4TRN | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$EDITNO | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$EDNASR | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$EXTENT | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$GIPASR | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$GIVETO | Read | APPSAUDT SYSPAUDT | Read |
| \$\$IPRASR | Read | APPSAUDT OPERAUDT PCSPAUDT | Read |

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|-----------|
| | | SYSPAUDT | |
| \$\$MIS1ZOO | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$MIS1LOG | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$MIS2FRE | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$MIS2HLD | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$MIS2RRN | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$MIS3CHA | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$MIS3DEL | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Alter |
| \$\$MIS3PPL | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | AlterRead |
| \$\$MIS3UPD | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$PAGI | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$PAGII | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$PAGIII | None | APPSAUDT | Read |

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|--------|
| | | OPERAUDT PCSPAUDT SYSPAUDT | |
| \$\$PGASRI | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$PGASRII | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$PGASRIII | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$PRTORD | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RCPASR | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RDLASR | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RECALL | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RECDEL | Read | APPSAUDT SYSPAUDT | Read |
| \$\$RECHEX | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RECINS | Read | APPSAUDT SYSPAUDT | Read |
| \$\$RECIPR | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RECRPR | None | APPSAUDT OPERAUDT PCSPAUDT | Read |

| Resource Names | Logging | User Group | Access |
|------------------|---------|--|--------|
| | | SYSPAUDT | |
| \$\$RECRST | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RECUPD | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$REPLST | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$REPORTD | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RMVASR | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RPRASR | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RSTASR | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RSTORD | None | APPSAUDT BMC STCs OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RULONF | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$RULSAV | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$SECCTD.qname | None | * | Read |
| \$\$SHNASR | None | APPSAUDT OPERAUDT PCSPAUDT | Read |

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|--------|
| | | SYSPAUDT | |
| \$\$TREE | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$UNRSTR | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$UPDASR | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$UPDNOT | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$UPNASR | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$UPRASR | Read | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$VEWUPD | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$VIEASR | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$VIEWCO | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$VIEWNO | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$VWNASR | None | APPSAUDT OPERAUDT PCSPAUDT SYSPAUDT | Read |

Table 11-3: BMC Control-M Resources

Referenced by: ZCTM0020

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|----------------------|
| \$\$CTMEDM | None | * | Read |
| \$\$CTMPNL3 | None | BMC STCs OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTMSTC | Read | BMC STCs PCSPAUDT SYSPAUDT | Read READ READ |
| \$\$JOB1ACT | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$JOB1AES | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$JOB1LOG | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$JOB1STA | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$JOB1SYS | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$JOB1ZOO | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$JOB2CHA | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$JOB2CNF | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$JOB2FOK | None | OPERAUDT PCSPAUDT PRODAUDT | Read |

| Resource Names | Logging | User Group | Access |
|-------------------------|---------|---|--------|
| | | SYSAUDT | |
| \$\$JOB2FRE | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |
| \$\$JOB2HLD | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |
| \$\$JOB2RRN | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |
| \$\$JOB3CHA | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |
| \$\$JOB3DEL | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |
| \$\$JOB3EDI | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |
| \$\$JOB3KIL | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |
| \$\$JOB3PRI. | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |
| \$\$JOBORD | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |
| \$\$JOBORD.qname.userid | None | APPBAUDT | Read |
| \$\$REFALL | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |
| \$\$REFDEAD | None | OPERAUDT PCSPAUDT PRODAUDT SYSAUDT | Read |

| Resource Names | Logging | User Group | Access |
|------------------|---------|--|--------|
| \$\$REFNET | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT DPCSAUDT | Read |
| \$\$REFPROP | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$REGSTR | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$SECCTM.qname | None | * | Read |
| \$\$STCORD | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$STRSTC | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |

Table 11-4: BMC Control-O Resources

Referenced by: ZCTO0020

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|--------|
| \$\$CTOAOP | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOASK | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOCMD | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOCMO | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTODOM | None | OPERAUDT PCSPAUDT PRODAUDT | Read |

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|--------|
| | | SYSPAUDT | |
| \$\$CTODRL | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTODSN | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTODSP | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOEDM | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOENV | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOJAR | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOJED | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOJSO | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOJST | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOKSL | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOMSG | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOONC | None | OPERAUDT | Read |

| Resource Names | Logging | User Group | Access |
|----------------|---------|--|--------|
| | | PCSPAUDT PRODAUDT SYSPAUDT | |
| \$\$CTOONM | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOONP | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOORD | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOORL | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOPCM | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOPKS | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOPNLOS | None | OPERAUDT PCSPAUDT SYSPAUDT | Read |
| \$\$CTOPRC | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOPTS | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTORES | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTORTS | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |

| Resource Names | Logging | User Group | Access |
|---------------------------|---------|--|--------|
| \$\$CTORUL | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOSET | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOSRL | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOSRQ | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOSTP | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOSUP | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOTSO | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOXAM | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOXAM.qname.TYPE1INI | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOXAM.qname.TYPE1RSL | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOXAM.qname.TYPE1TRM | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOXAM.qname.TYPE2LOC | Read | OPERAUDT PCSPAUDT | Read |

| Resource Names | Logging | User Group | Access |
|---------------------------|---------|--|--------|
| | | PRODAUDT SYSPAUDT | |
| \$\$CTOXAM.qname.TYPE3GLB | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOXAM.qname.TYPE3RUL | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$CTOXAMF | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$IOARES | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$RUL1LOG | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$RUL1ZOO | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$RUL2FRE | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$RUL2HLD | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$RUL2MOD | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$RUL2RES | None | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$RUL3CAN | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |

| Resource Names | Logging | User Group | Access |
|------------------|---------|--|--------|
| \$\$RUL3DEL | Read | OPERAUDT PCSPAUDT PRODAUDT SYSPAUDT | Read |
| \$\$SECCTO.qname | None | * | Read |

Table 11-5: BMC INCONTROL Resources Description

| Resource Names | Description |
|----------------|---|
| \$\$ADDCND | Add a condition name. |
| \$\$ADDCTL | Add a Control Resource. |
| \$\$ADDNOT | Add NOTES to a report. |
| \$\$ADDRES | Add a Quantitative resource name. |
| \$\$ADNASR | Add a note. |
| \$\$BKPORD | Order a Backup Mission. |
| \$\$CDDSEL | Select a record. |
| \$\$CHARES | Change a Quantitative resource name. |
| \$\$CHKCND | Check a condition name. |
| \$\$CHKCTL | Check a Control Resource. |
| \$\$CHKRCL | Perform a recall of a migrated CDAM file. |
| \$\$CHKRES | Check a Quantitative resource name. |
| \$\$CTDACT | Controlling Access to Reports. |
| \$\$CTDASR | Controlling Access to Reports by CONTROL-D. |
| \$\$CTDCDD | Controlling CONTROL-D Delivery functions. |
| \$\$CTDEDM | Extended Definition mode permits enhanced functionality. |
| \$\$CTDJOB | Controlling Access to Sysouts. |
| \$\$CTDOBJ | Entering to screen DO option 1 Report Clique. Entering to screen DO option 2 Resource Set. Saving a new or a modified report clique name. Deleting a report clique name or a resource set name. |
| \$\$CTDPNLA | Access to the Active Mission Status screen. |
| \$\$CTDPNLF | Access the Active Transfer screen. |
| \$\$CTDPREFIX | Controlling Access to PREFIX Parameter. |
| \$\$CTDPRF | Controlling Access to PREFIX Parameter. |
| \$\$CTDRRST | Access to the Active Mission Status screen. |
| \$\$CTMEDM | Extended Definition mode permits enhanced functionality. |
| \$\$CTMPNL3 | Access to the Active Environment Screen. |
| \$\$CTMSTC | Order a started task. |
| \$\$CTOAOP | Access or Use of Automated Options. |
| \$\$CTOASK | DO ASKOPER if a WTOR is issued. DO ASKOPER before a WTOR is issued. |
| \$\$CTOCMD | DO COMMAND. |
| \$\$CTOCMO | DO FORCEJOB. |
| \$\$CTODOM | DO DOM (delete operator message). |
| \$\$CTODRL | DO RULE. |

| Resource Names | Description |
|---------------------------|---|
| \$\$CTODSN | ON DSNEVENT. |
| \$\$CTODSP | DO DISPLAY with SUPPRESS set to NO. |
| \$\$CTOEDM | Extended Definition mode permits enhanced functionality when defining automation rules. |
| \$\$CTOENV | ON EVENT. |
| \$\$CTOJAR | ON JOBARRIV. |
| \$\$CTOJED | ON JOBEND. |
| \$\$CTOJSO | Jobname on Message |
| \$\$CTOJST | DO STOPJOB. |
| \$\$CTOKSL | DO KSL. |
| \$\$CTOMSG | DO DISPLAY. |
| \$\$CTOOMG | Exception Code on JOBSYSOUT. |
| \$\$CTOONC | Beginning of COMMAND TEXT. |
| \$\$CTOONM | ON MESSAGE. |
| \$\$CTOONP | ON CTOPCMMSG |
| \$\$CTOORD | Controlling Rule Ordering. |
| \$\$CTOORL | ON RULE. |
| \$\$CTOPCM | DO CTOPCMMSG. |
| \$\$CTOPKS | DO KLS. |
| \$\$CTOPNLOS | Initial access to Rule Status Screen. |
| \$\$CTOPRC | DO TSO or KLS. |
| \$\$CTOPTS | DO TSO. |
| \$\$CTORES | DO COND or DO RESOURCE. |
| \$\$CTORTS | Runtime security checking resource. Used to determine whether runtime security checks are performed, depending on the value set for the RUNTDFT global parameter (NONE, OWNER, or TRIGGER) in the CTOPARM member during CONTROL-O installation. |
| \$\$CTORUL | DO RULE and ON RULE. |
| \$\$CTOSET | DO SET for an IOA AutoEdit variable. |
| \$\$CTOSRL | Check if user is authorized to trigger a rule. |
| \$\$CTOSRQ | DO SYSREQ. |
| \$\$CTOSTP | ON STEP. |
| \$\$CTOSUP | DO DISPLAY with SUPPRESS set to YES. |
| \$\$CTOTSO | DO TSO. |
| \$\$CTOXAM | Controlling Access to Services Provided using the XAM (Extended Automation Mechanism). Security checking for XAM is more granular than the CTOXAMF basic automation mechanism mode of operation. |
| \$\$CTOXAM.qname.TYPE1INI | INIT action. |
| \$\$CTOXAM.qname.TYPE1RSL | RESOLVE action. |
| \$\$CTOXAM.qname.TYPE1TRM | TERM action. |
| \$\$CTOXAM.qname.TYPE2LOC | SETOLOC action. |
| \$\$CTOXAM.qname.TYPE3GLB | SETOGLB action. |

| Resource Names | Description |
|---------------------------|---|
| \$\$CTOXAM.qname.TYPE3RUL | DORULE action. |
| \$\$CTOXAMF | Performs a security check for authorization in basic automation mode. Security checking for XAM is less granular. |
| \$\$CTVINX | Use CONTROL-V Indexing features. |
| \$\$CTVQAC | Use CONTROL-V Quick Access features. |
| \$\$DELCND | Delete a condition name. |
| \$\$DELCTL | Delete a Control Resource. |
| \$\$DELNOT | Add NOTES. |
| \$\$DELRES | Delete a Quantitative resource name. |
| \$\$DLNASR | Delete a note. |
| \$\$DPC1VIE | Read the File Transfer facility. |
| \$\$DPC2FRE | Free the File Transfer facility. |
| \$\$DPC2HLD | Hold the File Transfer facility. |
| \$\$DPC3DEL | Delete the File Transfer facility. |
| \$\$DPC3PRN | Print the File Transfer facility. |
| \$\$DPC4TRN | Retransmit or Modify the File Transfer facility. |
| \$\$EDITNO | Add/Alter NOTES of a report. |
| \$\$EDNASR | Edit a note. |
| \$\$ERACND | Erase a manual condition name. |
| \$\$EXTENT | Define a Ruler. |
| \$\$GIPASR | Accessing the Global Index Path that is included in the list of paths in the CONTROL-D/WebAccess Index box or specified in the CONTROL-D/WebAccess filter manually by the user. |
| \$\$GIVETO | Copy a record. |
| \$\$IOAAS | Used by Control-D to interface with the IOAGATE address space. |
| \$\$IOACMD | Enter Operator Command. |
| \$\$IOADEL | Delete User Dataset. |
| \$\$IOADIR | Dir User Dataset. |
| \$\$IOAEDM | Extended Definition mode permits enhanced functionality. |
| \$\$IOAEDT | Edit User Dataset. |
| \$\$IOAGL | Accessing the Global Variable. |
| \$\$IOAONLINE | Access to the IOA Online facility. |
| \$\$IOARES | IOA Condition. CONTROL-M Quantitative Resource. CONTROL-M Control Resource. IOA Manual Condition. CONTROL-O DO COND or DO RESOURCE. |
| \$\$IOASAV | Save User Dataset. |
| \$\$IOAUTL | Access to Running Batch Utilities. |
| \$\$IOAVIW | View User Dataset. |
| \$\$IPRASR | Immediate printing of a report. |
| \$\$JOB1ACT | React in the Active Environment. |
| \$\$JOB1AES | AutoEdit simulation in the Active Environment. |

| Resource Names | Description |
|---------------------------|---|
| \$\$\$JOB1LOG | Log in the Active Environment. |
| \$\$\$JOB1STA | View statistics in the Active Environment. |
| \$\$\$JOB1SYS | View Sysout in the Active Environment. |
| \$\$\$JOB1ZOO | Zoom in the Active Environment. |
| \$\$\$JOB2CHA | Change in the Active Environment Screen. |
| \$\$\$JOB2CNF | Confirm in the Active Environment. |
| \$\$\$JOB2FOK | Force OK in the Active Environment. |
| \$\$\$JOB2FRE | Free in the Active Environment. |
| \$\$\$JOB2HLD | Hold in the Active Environment. |
| \$\$\$JOB2RRN | Rerun or Restore in the Active Environment. |
| \$\$\$JOB3CHA | Change in the Active Environment. |
| \$\$\$JOB3DEL | Delete or Undelete in the Active Environment. |
| \$\$\$JOB3EDI | Edit JCL in the Active Environment. |
| \$\$\$JOB3KIL | Kill an executing job in the Active Environment. |
| \$\$\$JOB3PRI. | Change priority in the Active Environment. |
| \$\$\$JOBORD | Order a job. |
| \$\$\$JOBORD.qname.userid | Order a job for a specific Environment |
| \$\$MIS1LOG | Log an Active Mission. |
| \$\$MIS1ZOO | Zoom an Active Mission. |
| \$\$MIS2FRE | Free an Active Mission. |
| \$\$MIS2HLD | Hold an Active Mission. |
| \$\$MIS2RRN | Rerun an Active Mission. |
| \$\$MIS3CHA | Change Active Mission. |
| \$\$MIS3DEL | Delete an Active Mission. |
| \$\$MIS3PPL | Print an Active Mission. |
| \$\$MIS3UPD | Alter an Active Mission. |
| \$\$NEWCND | Define a manual condition name. |
| \$\$PAGI | Printing a report of more than MAX number of pages. |
| \$\$PAGII | Printing a report within MIN-MAX number of pages. |
| \$\$PAGIII | Printing a report within MIN-MID number of pages. |
| \$\$PGASRI | Printing a report of more than MAX number of pages. |
| \$\$PGASRII | Printing a report within MIN-MAX number of pages. |
| \$\$PGASRIII | Printing a report within MIN-MID number of pages. |
| \$\$PRTORD | Order a Print mission. |
| \$\$RCPASR | Request to Copy a Report to another Recipient. |
| \$\$RDLASR | Delete a report record. |
| \$\$RECALL | Submit a job to perform recall of a migrated CDAM file. |
| \$\$RECDEL | Delete a record. |
| \$\$RECHEX | View the report in hexadecimal format. |
| \$\$RECINS | Insert a record. |
| \$\$RECIPR | Immediate print for a report. |
| \$\$RECRPR | Reprint a report. |
| \$\$RECRST | Restore a report. |
| \$\$RECUPD | Alter a record. |

| Resource Names | Description |
|----------------|---|
| \$\$REFALL | REFRESH ALL. Activates the processes described above (NET, DEADLINE and PROPAGATE) simultaneously in the CONTROL-M monitor. |
| \$\$REFDEAD | REFRESH DEADLINE. Adjust DUE OUT times, if necessary, for all job orders in the Active Jobs file that are not Held. |
| \$\$REFNET | REFRESH NET. Update the list of dependent jobs in the Job Dependency Network screen. |
| \$\$REFPROP | REFRESH PROPAGATE. Check and adjust the priority of predecessor jobs. |
| \$\$REGSTR | JOBDSN security check. |
| \$\$REPLST | Permit report access without Recipient Tree. |
| \$\$REPORTD | Decollating mission. |
| \$\$RMVASR | Request to Move a Report to another Recipient. |
| \$\$RPRASR | Request for a Deferred Print. |
| \$\$RSTASR | Restore a report or record. |
| \$\$RSTORD | Order a Restore Mission. |
| \$\$RUL1LOG | Log on rule definition. |
| \$\$RUL1ZOO | Zoom on rule definition. |
| \$\$RUL2FRE | Free on rule definition. |
| \$\$RUL2HLD | Hold on rule definition. |
| \$\$RUL2MOD | Mode on rule definition. |
| \$\$RUL2RES | Resume on rule definition. |
| \$\$RUL3CAN | Cancel on rule definition. |
| \$\$RUL3DEL | Delete on rule definition. |
| \$\$RULONF | Suppress or activate a ruler or use Global ruler. A ruler is a set of screen-editing rules that make a report look different when displayed or printed. |
| \$\$RULSAV | Save a ruler definition. |
| \$\$SECCTD | Security activate for CONTROL-D. |
| \$\$SECCTM | Security activate for CONTROL-M. |
| \$\$SECCTO | Security activate for CONTROL-O. |
| \$\$SECIOA | Security activate for IOA. |
| \$\$SHNASR | Show notes of a report. |
| \$\$STCORD | Order a started task. |
| \$\$STRSTC | Starting a started task. |
| \$\$TREE | Use of Recipient Tree Definitions by Online Users. |
| \$\$UNRSTR | Cancel Restore for History Report. |
| \$\$UPDASR | Alter report View Indicator. |
| \$\$UPDNOT | Alter NOTES to a report. |
| \$\$UPNASR | Alter a note. |
| \$\$UPRASR | Alter a Report Record. |
| \$\$VEWUPD | Alter Report View Indicator. |
| \$\$VIEASR | View Reports in Browse Mode. |

| Resource Names | Description |
|----------------|---------------------------|
| \$\$VIEWCO | View (browse) a report. |
| \$\$VIEWNO | Browse NOTES of a report. |
| \$\$VWNASR | View a note. |

11.3 CA 1 Requirements

The following table entries are guidelines regarding access authorizations to CA 1 resources:

Table 11-6: CA 1 Command Resources

Referenced by: ZCA10020

| CA 1 Command Resources | | | |
|------------------------|--|--------------|-----|
| Resource Name | Legitimate User | Access Level | Log |
| L0ADD | Tape librarian | READ | N |
| L0CLEAN | Tape librarian | READ | N |
| L0CHECKI | Tape librarian | READ | N |
| L0CHECKO | Tape librarian | READ | N |
| L0DELETE | Tape librarian | READ | N |
| L0ERASE | Tape librarian | READ | N |
| L0EXTEND | Tape librarian and users requiring the functionality of extending retention dates for tape data sets | READ | N |
| L0EXPIRE | Tape librarian | READ | N |
| L0PTRS | Tape librarian and System Programmer | READ | N |
| L0RETAIN | Tape librarian and users requiring the functionality of extending retention dates for tape data sets | READ | N |
| L0SCRATC | Tape librarian | READ | N |
| L0UPDTE | Tape librarian; users requiring update authority for command processing and System Programmer | READ | N |

Table 11-7: CA 1 Function and Password Resources

Referenced by: ZCA10021

| CA 1 Function and Password Resources | | | |
|--------------------------------------|---|--------------|-----|
| Resource Name | Legitimate User | Access Level | Log |
| NLRES | Tape librarian and technical support personnel | READ, UPDATE | N |
| NLNORES | Tape librarian and technical support personnel | READ, UPDATE | Y |
| NSLRES | Tape librarian and technical support personnel | READ, UPDATE | N |
| NSLNORES | Tape librarian and System Programmer | READ, UPDATE | Y |
| BLPRES | Tape librarian and System Programmer | READ, UPDATE | Y |
| BLPNORES | Tape librarian and technical System Programmer | READ, UPDATE | Y |
| FORRES | Tape librarian | READ, UPDATE | Y |
| FORNORES | Tape librarian and System Programmer | READ, UPDATE | Y |
| YSVCCOND | Users requiring tape data set processing | READ, UPDATE | N |
| YSVCUNCD | Tape librarian | READ, UPDATE | N |
| YSVCUNCD | System Programmer | READ | N |
| <i>Password</i> | Users requiring access to CA 1 on-line applications for tape data set processing Note: Multiple passwords are available providing different levels of CA 1 functionality ranging from general user to tape librarian. | READ | N |
| REINIT | Operations staff and systems personnel responsible for supporting CA 1 | READ | N |
| BATCH | Operations staff and systems personnel responsible for supporting CA 1 | READ | N |
| DEACT | Operations staff and systems personnel responsible for supporting CA 1 | READ | N |
| COPYCAT | Operations staff and systems personnel responsible for supporting CA 1 | READ | N |

Note: Tape librarian includes tape personnel, as well as STCs and Batch Users that perform CA 1 maintenance. The users for L0UPDTE may include off-siter personnel who require ability maintain applications.

11.3.1 ACF2 Tables**Table 11-8: CA 1 Command Resources for ACF2**

Used by: ZCA10020

| CA 1 Command Resources for ACF2 | | |
|---------------------------------|---------------|--------------------------|
| Resource Type | Resource Name | Description |
| CAC | L0ADD | On-line command ADD |
| CAC | L0CHECKI | On-line command CHECKIN |
| CAC | L0CHECKO | On-line command CHECKOUT |
| CAC | L0CLEAN | On-line command CLEAN |
| CAC | L0DELETE | On-line command DELETE |
| CAC | L0ERASE | On-line command ERASE |
| CAC | L0EXPIRE | On-line command EXPIRE |
| CAC | L0EXTEND | On-line command EXTEND |
| CAC | L0RETAIN | On-line command RETAIN |
| CAC | L0SCRATC | On-line command SCRATCH |
| CAC | L0UPDTE | On-line command UPDATE |

Table 11-9: CA 1 Function and Password Resources for ACF2

Used by: ZCA10021

| CA 1 Function and Password Resources for ACF2 | | |
|---|---------------|--|
| Resource Type | Resource Name | Description |
| CAT | BLPNORES | Bypass label processing for a tape undefined to CA 1 |
| CAT | BLPRES | Bypass label processing for a tape defined to CA 1 |
| CAT | FORNORES | Foreign tape undefined to CA 1 |
| CAT | FORRES | Foreign tape defined to CA 1 |
| CAT | NLNORES | Non-label tape undefined to CA 1 |
| CAT | NLRES | Non-label tape defined to CA 1 |
| CAT | NSLNORES | Non-standard label tape undefined to CA 1 |
| CAT | NSLRES | Non-standard label tape defined to CA 1 |
| CAT | YSVCCOND | Y SVC conditional access |

| CA 1 Function and Password Resources for ACF2 | | |
|---|-----------------|---|
| Resource Type | Resource Name | Description |
| CAT | YSVCUNCD | Y SVC unconditional access |
| CAT | <i>password</i> | CA 1 internal password used to access CA 1 on-line applications Note: A rule is written for each available password, including default passwords. |
| CAT | REINIT | TMSINIT re-initialization |
| CAT | BATCH | TMSINIT batch status |
| CAT | DEACT | TMSINIT deactivation |
| CAT | COPYCAT | TMSINIT file copy |

11.3.2 RACF Tables

Table 11-10: CA 1 Command Resources for RACF

Referenced by: ZCA10020

| CA 1 Command Resources for RACF | |
|-------------------------------------|--------------------------|
| RACF Command | Description |
| RDEFINE CA@MD (L0CLEAN) UACC(NONE) | On-line command CLEAN |
| RDEFINE CA@MD (L0EXTEND) UACC(NONE) | On-line command EXTEND |
| RDEFINE CA@MD (L0EXPIRE) UACC(NONE) | On-line command EXPIRE |
| RDEFINE CA@MD (L0RETAIN) UACC(NONE) | On-line command RETAIN |
| RDEFINE CA@MD (L0DELETE) UACC(NONE) | On-line command DELETE |
| RDEFINE CA@MD (L0ADD) UACC(NONE) | On-line command ADD |
| RDEFINE CA@MD (L0CHECKI) UACC(NONE) | On-line command CHECKIN |
| RDEFINE CA@MD (L0CHECKO) UACC(NONE) | On-line command CHECKOUT |
| RDEFINE CA@MD (L0ERASE) UACC(NONE) | On-line command ERASE |
| RDEFINE CA@MD (L0SCRATC) UACC(NONE) | On-line command SCRATCH |
| RDEFINE CA@MD (L0UPDTE) UACC(NONE) | On-line command UPDATE |

Table 11-11: CA 1 Function and Password Resources for RACF

Referenced by: ZCA10021

| CA 1 Function and Password Resources for RACF | |
|---|---|
| RACF Command | Description |
| RDEFINE CA@APE (YSVCCOND) UACC(NONE) | Y SVC conditional |
| RDEFINE CA@APE (YSVCUNCNCD) UACC(NONE) | Y SVC unconditional |
| RDEFINE CA@APE (NLRES) UACC(NONE) | Non-label tape defined to CA 1 |
| RDEFINE CA@APE (NLNORES) UACC(NONE) | Non-label tape undefined to CA 1 |
| RDEFINE CA@APE (NSLRES) UACC(NONE) | Non-standard label tape defined to CA 1 |
| RDEFINE CA@APE (NSLNORES) UACC(NONE) | Non-standard label tape undefined to CA 1 |
| RDEFINE CA@APE (BLPRES) UACC(NONE) | Bypass label processing for a tape defined to CA 1 |
| RDEFINE CA@APE (BLPNORES) UACC(NONE) | Bypass label processing for a tape undefined to CA 1 |
| RDEFINE CA@APE (FORRES) UACC(NONE) | Foreign tape defined to CA 1 |
| RDEFINE CA@APE (FORNORES) UACC(NONE) | Foreign tape undefined to CA 1 |
| RDEFINE CA@APE (<i>password</i>) UACC(NONE) | CA 1 internal password used to access CA 1 on-line applications Note: A rule is written for each available password, including default passwords. |
| RDEFINE CA@APE (REINIT) UACC(NONE) | TMSINIT re-initialization |
| RDEFINE CA@APE (BATCH) UACC(NONE) | TMSINIT batch status |
| RDEFINE CA@APE (DEACT) UACC(NONE) | TMSINIT deactivation |
| RDEFINE CA@APE (COPYCAT) UACC(NONE) | TMSINIT file copy |

11.3.3 TSS Tables

Table 11-12: CA 1 Command Resources for TSS

Used by: ZCA10020

| CA 1 Command Resources for TSS | |
|---|------------------------|
| Top Secret Command | Description |
| TSS ADD(<i>dept-acid</i>) CACMD(L0CLEAN) | On-line command CLEAN |
| TSS ADD(<i>dept-acid</i>) CACMD(L0EXTEND) | On-line command EXTEND |
| TSS ADD(<i>dept-acid</i>) CACMD(L0EXPIRE) | On-line command EXPIRE |

| CA 1 Command Resources for TSS | |
|---|--------------------------|
| Top Secret Command | Description |
| TSS ADD(<i>dept-acid</i>) CACMD(L0RETAIN) | On-line command RETAIN |
| TSS ADD(<i>dept-acid</i>) CACMD(L0DELETE) | On-line command DELETE |
| TSS ADD(<i>dept-acid</i>) CACMD(L0ADD) | On-line command ADD |
| TSS ADD(<i>dept-acid</i>) CACMD(L0CHECKI) | On-line command CHECKIN |
| TSS ADD(<i>dept-acid</i>) CACMD(L0CHECKO) | On-line command CHECKOUT |
| TSS ADD(<i>dept-acid</i>) CACMD(L0ERASE) | On-line command ERASE |
| TSS ADD(<i>dept-acid</i>) CACMD(L0SCRATC) | On-line command SCRATCH |
| TSS ADD(<i>dept-acid</i>) CACMD(L0UPDTE) | On-line command UPDATE |

Table 11-13: CA 1 Function and Password Resources for TSS

Used by: ZCA10021

| CA 1 Function and Password Resources for TSS | |
|---|--|
| Top Secret Command | Description |
| TSS ADD(<i>dept-acid</i>) CACMD(L0CLEAN) | On-line command CLEAN |
| TSS ADD(<i>dept-acid</i>) CATAPE(YSVCCOND) | Y SVC conditional access |
| TSS ADD(<i>dept-acid</i>) CATAPE(YSVCUNCD) | Y SVC unconditional access |
| TSS ADD(<i>dept-acid</i>) CATAPE(NLRES) | Non-label tape defined to CA 1 |
| TSS ADD(<i>dept-acid</i>) CATAPE(NLNORES) | Non-label tape undefined to CA 1 |
| TSS ADD(<i>dept-acid</i>) CATAPE(NSLRES) | Non-standard label tape defined to CA 1 |
| TSS ADD(<i>dept-acid</i>) CATAPE(NSLNORES) | Non-standard label tape undefined to CA 1 |
| TSS ADD(<i>dept-acid</i>) CATAPE(BLPRES) | Bypass label processing for a tape defined to CA 1 |
| TSS ADD(<i>dept-acid</i>) CATAPE(BLPNORES) | Bypass label processing for a tape undefined to CA 1 |
| TSS ADD(<i>dept-acid</i>) CATAPE(FORRES) | Foreign tape defined to CA 1 |
| TSS ADD(<i>dept-acid</i>) CATAPE(FORNORES) | Foreign tape undefined to CA 1 |
| TSS ADD(<i>dept-acid</i>) CATAPE(<i>password</i>) | CA 1 internal password used to access CA 1 on-line applications Note: A rule is written for each available password. |
| TSS ADD(<i>dept-acid</i>) CATAPE(REINIT) | TMSINIT re-initialization |

| CA 1 Function and Password Resources for TSS | |
|--|----------------------|
| Top Secret Command | Description |
| TSS ADD(<i>dept-acid</i>) CATAPE(BATCH) | TMSINIT batch status |
| TSS ADD(<i>dept-acid</i>) CATAPE(DEACT) | TMSINIT deactivation |
| TSS ADD(<i>dept-acid</i>) CATAPE(COPYCAT) | TMSINIT file copy |

11.4 CATALOG SOLUTIONS Requirements

Table 11-14: CATALOG SOLUTIONS Resource List

Referenced by: ZCSL0020

You can enable data set and catalog security verification by adding a FACILITY class profile with the resource name hlq1.hlq2.GLOBAL.DATASET. If the named FACILITY class resource has been defined to the security software, then Catalog Solution will determine if the current user is authorized to bypass data set security verification according to the following conditions:

- If the user has READ authorization for the named FACILITY class resource, data set security will be bypassed. This will allow for the existence of one or more “super users” that will not be subjected to data set and catalog security verification.
- If the current user is not authorized for the named FACILITY class resource, Catalog Solution will not bypass data set and catalog security verification. The security software currently executing in the user environment should cause OPEN processing to fail if the user is not authorized for the attempted access.

If the named FACILITY class resource has not been defined to the security software, Catalog Solution will bypass data security.

| Resource Names | Logging | User Groups | Access |
|--------------------------|---------|-------------|--------|
| hlq1 | | * | NONE |
| hlq1.hlq2.GLOBAL.DATASET | READ | * | NONE |
| | | DASDAUDT | READ |
| | | DASBAUDT | READ |
| | | SYSPAUDT | READ |
| hlq1.hlq2.READ.CATLIST | | * | READ |
| hlq1.hlq2.READ.LIST | | * | READ |
| hlq1.hlq2.READ.SCAN | | * | READ |
| hlq1.hlq2.READ.PRINT | | * | READ |
| hlq1.hlq2.READ.ALIASCHK | | * | READ |
| hlq1.hlq2.READ.DIAGNOSE | | * | READ |
| hlq1.hlq2.READ | | DASDAUDT | READ |
| | | DASBAUDT | READ |
| | | SYSPAUDT | READ |
| hlq1.hlq2.UPDATE | | DASDAUDT | READ |

| | | | |
|--|--|----------|------|
| | | DASBAUDT | READ |
| | | SYSBAUDT | READ |

* - All Users

hlq1 - The high-level qualifier for the resource. EMC for software version 9.00 and below and ROCKET for software version 9.10 and above.

hlq2 - The high-level qualifier for the resource. CSL for software version 9.00 and below and RCS for software version 9.10 and above.

| READ Resource Names | Related Command/Keyword |
|---------------------------------|--|
| hlq1.hlq2.READ.ALIASCHK | ALIASCHECK |
| hlq1.hlq2.READ.CATLIST | CATLIST |
| hlq1.hlq2.READ.DIAGNOSE.CSR | DIAGNOSE/TEST=CSR or DIAGNOSE/TEST=CHECK-SPANNED-RECS |
| hlq1.hlq2.READ.DIAGNOSE.CVB | DIAGNOSE/TEST=CVB or DIAGNOSE/TEST=CHECK-VVDS-BACKUP |
| hlq1.hlq2.READ.DIAGNOSE.CVC | DIAGNOSE/TEST=CVC or DIAGNOSE/TEST=CHECK-VVDS-CATALOGS |
| hlq1.hlq2.READ.DIAGNOSE.DDA | DIAGNOSE/TEST=DDA or DIAGNOSE/TEST=DELETE-DEAD-ALIAS |
| hlq1.hlq2.READ.DIAGNOSE.DS | DIAGNOSE/TEST=DS or DIAGNOSE/TEST=DATA-STRUCTURE |
| hlq1.hlq2.READ.DIAGNOSE.GADB | DIAGNOSE/TEST=GADB or DIAGNOSE/TEST=GENERATE-AMS-DIAG-BCS |
| hlq1.hlq2.READ.DIAGNOSE.GADV | DIAGNOSE/TEST=GADV or DIAGNOSE/TEST=GENERATE-AMS-DIAG-VVDS |
| hlq1.hlq2.READ.DIAGNOSE.GDC | DIAGNOSE/TEST=GDC or DIAGNOSE/TEST=GENERATE-DELETE-CARD |
| hlq1.hlq2.READ.DIAGNOSE.GDIAG3C | DIAGNOSE/TEST=GDIAG3C or DIAGNOSE/TEST=GENERATE-DIAG3-CARD |
| hlq1.hlq2.READ.DIAGNOSE.GDLN | DIAGNOSE/TEST=GDLN or DIAGNOSE/TEST=GENERATE-DELETE-NONVSAM |
| hlq1.hlq2.READ.DIAGNOSE.GDN | DIAGNOSE/TEST=GDN or DIAGNOSE/TEST=GENERATE-DEFINE-NONVSAM |
| hlq1.hlq2.READ.DIAGNOSE.GRC | DIAGNOSE/TEST=GRC or DIAGNOSE/TEST=GENERATE-RECATALOG-CARD |

| READ Resource Names | Related Command/Keyword |
|-----------------------------|--|
| hlq1.hlq2.READ.DIAGNOSE.GUL | DIAGNOSE/TEST=GUL or DIAGNOSE/TEST=GENERATE-UNCAT-LIST |
| hlq1.hlq2.READ.DIAGNOSE.GVC | DIAGNOSE/TEST=GVC or DIAGNOSE/TEST=GENERATE-VERIFY-CARD |
| hlq1.hlq2.READ.DIAGNOSE.IS | DIAGNOSE/TEST=IS or DIAGNOSE/TEST=INDEX-STRUCTURE |
| hlq1.hlq2.READ.DIAGNOSE.LA | DIAGNOSE/TEST=LA or DIAGNOSE/TEST=LIST-ASSOCIATIONS |
| hlq1.hlq2.READ.DIAGNOSE.VCE | DIAGNOSE/TEST=VCE or DIAGNOSE/TEST=VERIFY-CATALOG-ENTRIES |
| hlq1.hlq2.READ.DIAGNOSE.VV | DIAGNOSE/TEST=VV or DIAGNOSE/TEST=VTOC-VVDS |
| hlq1.hlq2.READ.DIAGNOSE.VVC | DIAGNOSE/TEST=VVC or DIAGNOSE/TEST=VVCN-CHECK |
| hlq1.hlq2.READ.DISPLAY | DISPLAY |
| hlq1.hlq2.READ.DUMP | DUMP |
| hlq1.hlq2.READ.LIST | LIST |
| hlq1.hlq2.READ.OELIST | OELIST |
| hlq1.hlq2.READ.PRINT | PRINT |
| hlq1.hlq2.READ.QUERY | QUERY |
| hlq1.hlq2.READ.SCAN | SCAN |
| hlq1.hlq2.READ.SCAVENGE | SCAVENGE |
| hlq1.hlq2.READ.SMFLIST | SMFLIST |
| hlq1.hlq2.READ.SYSCHECK | SYSTEMCHECK |

hlq1 - The high-level qualifier for the resource. EMC for software version 9.00 and below and
ROCKET for software version 9.10 and above.

hlq2 - The high-level qualifier for the resource. CSL for software version 9.00 and below and RCS
for software version 9.10 and above.

| UPDATE Resource Names | Related Command/Keyword |
|------------------------------|--|
| hlq1.hlq2.UPDATE.ALIASCHK | RESYNCH ALIASCHECK/RESYNCH |
| hlq1.hlq2.UPDATE.ALTER | ALTER |
| hlq1.hlq2.UPDATE.BCSRCVR | BCSRECOVER |
| hlq1.hlq2.UPDATE.DELETE | DELETE |
| hlq1.hlq2.UPDATE.DIAGNOSE | RVC DIAGNOSE/TEST=RVC or DIAGNOSE/TEST=REMOVE-VVDS- CATALOGS |
| hlq1.hlq2.UPDATE.EXTRACT | EXTRACT |
| hlq1.hlq2.UPDATE.LIST.VERREP | LIST/VER & REP |
| hlq1.hlq2.UPDATE.MODIFY | MODIFY |
| hlq1.hlq2.UPDATE.PURGE | PURGE |
| hlq1.hlq2.UPDATE.REBUILD | REBUILD |
| hlq1.hlq2.UPDATE.RECOVER | RECOVER |
| hlq1.hlq2.UPDATE.REPROMC | REPROMC |
| hlq1.hlq2.UPDATE.RESET | RESET |
| hlq1.hlq2.UPDATE.SCRATCH | SCRATCH |

hlq1 - The high level qualifier for the resource. EMC for software version 9.00 and below and ROCKET for software version 9.10 and above.

hlq2 - The high level qualifier for the resource. CSL for software version 9.00 and below and RCS for software version 9.10 and above.

11.5 CICS Requirements

Consult the current IBM CICS Transaction Server for z/OS RACF Security Guide for the latest information on categories of CICS-supplied transactions. This information found in that reference as well as the information in this Addendum specifies recommended security specifications. The Site Security plan should be the authorization for access.

Table 11-15: Category 1 Transactions for CICS TS 4.1 - 5.3

This transaction must be restricted to CICS regions only.

Referenced by: ZCIC0020

| | | | | | | | |
|------|------|------|------|------|------|------|------|
| CATA | CATD | CDBD | CDBF | CDBO | CDBQ | CDTS | CEPD |
| CEPF | CEPM | CESC | CEX2 | CFCL | CFCR | CFOR | CFQR |
| CFQS | CFTL | CFTS | CGRP | CHCK | CIS1 | CIS4 | CISB |
| CISC | CISD | CISE | CISM | CISP | CISQ | CISR | CISS |
| CIST | CISU | CISX | CITS | CJLR | CJSL | CJSP | CJSR |
| CJTR | CMPE | CMTS | COHT | COIE | COIR | COIO | CONA |
| COND | CONH | CONL | CONM | COVR | COWC | CPCT | CPIR |
| CPIS | CPLT | CRLR | CRMD | CRMF | CRSQ | CRST | CRSY |
| CRTP | CSFR | CSFU | CSHA | CSHQ | CSKP | CSNC | CSNE |
| CSOL | CSPQ | CSQC | CSSY | CSTE | CSTP | CSZI | CTSD |
| CWBG | CWXN | CWXU | CXCU | CXRE | | | |

Table 11-16: Category 2 Transactions for CICS TS 4.1 - 5.3

Referenced by: ZCIC0020

| Transaction | User Group | Access | Logging |
|-----------------------|----------------------------------|---------------|----------------|
| CADP | SYSPAUDT APPDAUDT | Read | Y |
| CBAM | SYSPAUDT OPERAUDT | Read | |
| CCRL | SYSPAUDT | Read | Y |
| CDBC | SYSPAUDT DABAAUDT | Read | Y |
| CDBI | SYSPAUDT DABAAUDT | Read | Y |
| CDBM | SYSPAUDT DABAAUDT INQUIRE | Read | Y |
| CDBT | SYSPAUDT APPDAUDT DABAAUDT | Read | Y |
| CDFS | SYSPAUDT INTERCOM | Read | |
| CDST | SYSPAUDT | Read | Y |
| CEBR | SYSPAUDT APPDAUDT | Read | Y |
| CEBT see Notes | SYSPAUDT | Read | Y |
| CECI | APPDAUDT SYSPAUDT | Read | Y |
| CECS | SYSPAUDT APPDAUDT | Read | Y |
| CEDA | SYSPAUDT | Read | Y |
| CEDB | SYSPAUDT | Read | Y |
| CEDC see Notes | SYSPAUDT INQUIRE APPDAUDT | Read | |
| CEDF | SYSPAUDT APPDAUDT | Read | Y |
| CEDX | SYSPAUDT APPDAUDT | Read | Y |
| CEHP | SYSPAUDT INTERCOM | Read | |
| CEHS | SYSPAUDT INTERCOM | Read | |
| CEKL | SYSPAUDT | Read | Y |
| CEMN | SYSPAUDT | Read | Y |
| CEMT see Notes | SYSPAUDT | Read | Y |

UNCLASSIFIED

z/OS STIG Addendum, V6R62
24 October 2024

DISA
Developed by DISA for the DOD

| Transaction | User Group | Access | Logging |
|--------------------------|-----------------------|--------|---------|
| CEOT | SYSPAUDT OPERAUDT | Read | |
| CEPH | SYSPAUDT EVENTUSER | Read | |
| CEPQ | SYSPAUDT EVENTUSER | Read | |
| CEPR | SYSPAUDT EVENTUSER | Read | |
| CEPS | SYSPAUDT EVENTUSER | Read | |
| CEPT | SYSPAUDT EVENTUSER | Read | |
| CESD see Notes | SYSPAUDT | Read | Y |
| CEST | SYSPAUDT OPERAUDT | Read | |
| CETR | SYSPAUDT APPAUDT | Read | Y |
| CHLP (alias for CMAC) | * | Read | |
| CIDP | SYSPAUDT OPERAUDT | Read | Y |
| CIND | SYSPAUDT | Read | Y |
| CIRP | IOPUSER | Read | |
| | | | |
| CJSA | WEBUSER CICSDEF | Read | |
| CJSU | WEBUSER CICSDEF | Read | |
| CLDM | SYSPAUDT PIPEUSER | Read | |
| | | | |
| CLDM | SYSPAUDT PIPEUSER | Read | |
| CMAC | * | Read | |
| CMSG | SYSPAUDT OPERAUDT | Read | |
| CPIA | SYSPAUDT PIPEUSER | Read | |
| CPIH | SYSPAUDT PIPEUSER | Read | |
| CPIL | SYSPAUDT PIPEUSER | Read | |
| CPIQ | SYSPAUDT PIPEUSER | Read | |
| CPMI | SYSPAUDT | Read | |

| Transaction | User Group | Access | Logging |
|-------------|----------------------------------|--------|---------|
| | INTERCOM | | |
| CREA | SYSPAUDT | Read | |
| CREC | SYSPAUDT INQUIRE | Read | |
| CRPA | SYSPAUDT RPCUSER | Read | |
| CRPC | SYSPAUDT RPCUSER | Read | |
| CRPM | SYSPAUDT RPCUSER | Read | |
| CRTE | SYSPAUDT APPDAUDT OPERAUDT | Read | |
| CRTX | * | Read | |
| CSFE | SYSPAUDT OPERAUDT | Read | |
| CSGM | * | Read | |
| CSHR | SYSPAUDT INTERCOM | Read | |
| CSM1 | SYSPAUDT INTERCOM | Read | |
| CSM2 | SYSPAUDT INTERCOM | Read | |
| CSM3 | SYSPAUDT INTERCOM | Read | |
| CSM5 | SYSPAUDT INTERCOM | Read | |
| CSMI | SYSPAUDT INTERCOM | Read | |
| CTIN | SYSPAUDT INTERCOM | Read | |
| CVMI | SYSPAUDT INTERCOM | Read | |
| CWBA | WEBUSER CICSDEF | Read | |
| CWWU | WEBUSER | Read | |
| CW2A | WEBUSER | Read | |
| CWTO | SYSPAUDT OPERAUDT | Read | |
| DSNC | SYSPAUDT OPERAUDT | Read | |
| CK** | SYSPAUDT MQSAAUDT | Read | |

Note:

- The CEMT and CEBT (Master for Alternate CICS) transactions can be secured at the command level allowing for a more inclusive authorization through the use of SPI and the user base can be expanded.
- These are IBM recommended users for these category 2 transactions, outside of SYSPAUDT, use of other transactions can be justified with the approval of the CICS Systems Programmer and the ISSO/ISSM.
- Give CICS default users access to the CESD shutdown-assist transaction. Users who can attach CICSplex SM transactions or define debugging transactions need access to CESD in case of CMAS failure.

CICS Users identified in the above table, detailed descriptions can be found in Section 3 z/OS Privileged Users.

| | |
|------------------|---|
| CICSDEF | The CICS regions default user ids, as specified in the DFLTUSER parameter. |
| PIPEUSER | These transactions are used when a CICS application is in the role of a Web service provider or requester. |
| IIOPUSER | These transactions use Java server applications that communicate with a client application using the IIOP protocol. |
| INTERCOM | <p>These transactions are used in function shipping. The mirror transactions must be available to remote users in a function shipping environment. When a database or file resides on another CICS region, CICS function ships the request to access the data, and this request runs under one of the CICS-supplied mirror transactions. This means:</p> <ul style="list-style-type: none"> • The terminal user running the application must be authorized to use the mirror transaction. • The terminal user must also be authorized to use the data that the mirror transaction accesses. |
| RPCUSER | These transactions are used with remote procedure calls. |
| INQUIRE | These transactions are available to inquire into CICS to obtain information. |
| EVENTUSER | These transactions are default EP adapter transaction IDs. |

Table 11-17: Category 3 Transactions for CICS TS 4.1 - 5.3

The following transactions are eligible for exemption from security checking.

Referenced by: ZCICA024

| | | | | | | | | |
|------|------|------|------|------|------|------|------|------|
| CATR | CCIN | CDBN | CEGN | CEKL | CESF | CESL | CESN | CIEP |
| CLQ2 | CLR1 | CLR2 | CLS1 | CLS2 | CLS3 | CLS4 | CMPX | CPCT |
| CPSS | CQPI | CQPO | CQRY | CRDR | CRSR | CSAC | CSCY | CSPG |
| CSPK | CSPP | CSPS | CSRK | CSRS | CSSF | CSXM | CXRT | |

Table 11-18: CICS Category 4 COTS-Supplied Sensitive Transactions

(COTS-supplied transactions are used to support and administer vendor products. Some of these transactions may offer the ability to bypass ESM controls for resources managed under CICS. These transactions are considered sensitive and are identified as Category 4 transactions. Category 4 transactions are restricted to systems programming personnel. The list is not all-inclusive.)

| Transaction | Description |
|-------------|----------------------------|
| ACFM | CA-ACF2 Master Transaction |
| ACFA | CA-ACF2 |
| ACFT | CA-ACF2 |
| ACUL | CA-ACF2 |
| DBOC | CA-DATACOM |
| LOOK | CA-LOOK |
| TMSU | CA 1 |
| TSEU | CA-TOP SECRET |
| TSSC | CA-TOP-SECRET |

Table 11-19: TSS FACILITY Initialization Parameters for CICS Region

Referenced by: ZCIC0030, ZCICT050

| | |
|-----------------|--|
| DEFACID(*NONE*) | No default ACID |
| NOABEND | For multi-user address space |
| RES | Allows storage of access authorizations for all resources within the online user region. |
| MODE(FAIL) | All unauthorized facility or resource access is denied unconditionally. |

Ensure that users cannot sign on more than once within the scope of a single CICS production region.

| | |
|--------------------|--|
| SIGN(S) | Single sign-on within the same CICS facility |
| SIGN(M) | Multiple sign-on within the same CICS facility (<i>use only with test or development regions</i>) |
| SHRPRF | Allows a copy of the profile to be shared by all users in the multiuser facility. |
| XDEF | Sets protection in place by default for all commands and transactions controlled by the facility. |
| PCTEXTSEC=OVERRIDE | CA-TOP SECRET does not honor the PCT EXTSEC= and RSLC= parameters and forces a security call. |
| EXTSEC=YES | CA-TOP SECRET security is invoked for this region |
| FACMATRX=YES | Controls for CICS security are specified in Facility Matrix. |
| LOCKTIME=0 | This parameter is set to zero since the OPTIME parameter (refer to <i>Section 8.2.3.4, CICS User Controls</i>) provides a more efficient method for managing idle time. |
| XTRAN=YES | Transaction checking is performed. |

Table 11-20: ACF2/CICS Parameters

Referenced by: ZCICA023

| Parameter | Keyword(s) | Description |
|-----------|---|--|
| CICSKEY* | OPTION=VALIDATE, TYPE= <i>ttt</i> ,** RESOURCE=TRANS | The CICSKEY parameter establishes CA-ACF2 CICS control over a CICS resource. |
| DEFAULT | Terminal= < <i>parameter</i> > Nonterminal=< <i>parameter</i> > | Ensures that every CICS task has a valid user identified. |
| EXIT | MROIN MROOUT | In normal operations, you would not use these exits. However if either of these exits are used they must follow the same guidelines as MVSEXIT described in AAMV0450. |
| OPTION | CONSOLE=VALIDATE DISCONNECT=YES MAXVIO=3 MODE=ABORT TIMEOUT=5 | Security controls are in effect for transactions being processed at the console. When the violation limit is reached, disconnects the terminal from CICS and returns it to VTAM. Maximum number of security violations allowed. Aborts the transaction if access is denied. Number of minutes between each scan for inactive terminals |
| INHERIT | TDJOB=YES | Batch jobs submitted to an internal reader through extra-partition transient data queues inherit the logonid of the submitting task |

| Parameter | Keyword(s) | Description |
|-----------|-------------------------------------|--|
| SIGNON | ENQSCOPE =NONE*** | Multiple sign-on within the same CICS region (<i>use only with test or development regions</i>) |
| | ENQSCOPE=CICS*** | Single sign-on within the same CICS region |
| | QUICK=NO | Disallows quick sign-on format, which enables the user to enter the password in clear text at the same time as the logonid is entered. |
| | REQUIRE=YES | Specifies that a user must sign-on before executing transactions. |
| SUSPEND | PASSWORD=YES | Suspends user during sign-on if the password violation count reaches the established threshold. |
| | RULE=YES | Suspends users during resource validation if the CA-ACF2 violation count reaches the established threshold. |
| VERIFY | IDLE=YES IDLE=NO See Note | Re-verify password after terminal idle time is exceeded. |
| MRO | TRANSMIT=YES RECEIVE=YES | This assures that logonid inheritance is performed. |

*At a minimum, enforce transaction-level protection.

**The default ACF2/CICS type for transactions is CKC, but is unique for each region, as specified above. An exception would be the situation where regions are grouped together in an MRO environment that may share a common transaction type with that unique MRO environment.

Note: IDLE=NO can be specified if mixed case passwords are being used.

Table 11-21: CICS Systems Programmer's Worksheet

Referenced by: ZCIC0010, ZCIC0020, ZCIC0030, ZCIC0040, ZCIC0041, ZCIC0042, ZCICA011, ZCICA022, ZCICA023, ZCICA024, ZCICA025, ZCICR021, ZCICR041, ZCICR042, ZCICT041, ZCICT050

1. CICS TABLES/RDO DEFINITIONS

- Provide information for all SITs:

| CICS JOBNAME | Data Set Name |
|--------------|---------------|
| | |
| | |
| | |
| | |

| CICS JOBNAME | Data Set Name |
|--------------|---------------|
| | |
| | |
| | |
| | |
| | |

Note: Add additional lines if required

b. Provide a list of all defined CICS transactions for product, test/development, and training regions.

| CICS JOBNAME | Data Set Name |
|--------------|---------------|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Note: Add additional lines if required.

2. CICS REGIONS

Complete the following with the JOB NAME, LOGONID/USERID/ACID, CICS REGION TYPE (TOR, AOR, other), CICS Version, and the Operational Function of the region, i.e., Production, Test, Development or Training.

DSN= _____

| JOB NAME | LOGONID/ACID USERID | REGION TYPE | CICS Version | Operational Function |
|----------|------------------------|----------------|--------------|-------------------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Table 11-22: CICS SPI Resources Table

Referenced by: ZCICA021, ZCICR021, ZCICT021

Note: For access levels in this table please consult individual external security management products to reconcile access syntax. Example. Alter access in CA-ACF2 would equate to Update in RACF. User and accesses in this table are recommendation only. Assessment of vulnerability should be determined by contents of the site security plan

Note: Final resource definitions should be governed by *Table 42. Resource and command check cross-reference* in the latest release of IBM CICS RACF Security Guide.

| Resource/TSS Resource | Command | Access | Users |
|-----------------------|-------------|--------|----------------------------------|
| ASSOCIATION/ASSOCIAT | ASSOCIATION | READ | SYSCAUDT CICSAUDT CICUAUDT |
| ATOMSERVICE/ATOMSERV | ATOMSERVICE | READ | CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| AUTINSTMODEL/AUTINSTM | AUTINSTM | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| AUTOINSTALL/AUTOINST | AUTOINST | READ | NONE |
| | | UPDATE | SYSCAUDT CICSAUDT |
| BEAN/BEAN | BEAN | READ | SYSCAUDT CICSAUDT CICUAUDT |
| BRFACILITY/BRFACILIT | BRFACILITY | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| BUNDLE/BUNDLE | BUNDLE | READ | CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| CAPTURESPEC/CAPTURES | CAPTURESPEC | READ | SYSCAUDT CICSAUDT CICUAUDT |
| CFDTPOOL/CFDTPOOL | CFDTPOOL | READ | SYSCAUDT CICSAUDT CICUAUDT |
| CLASSCACHE/CLASSCAC | CLASSCACHE | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| CONNECTION/CONNECTI | CONNECTION | READ | CICBAUDT CICDAUDT |
| | | UPDATE | OPERAUDT CICUAUDT |

| Resource/TSS Resource | Command | Access | Users |
|------------------------|---------------|--------|----------------------------------|
| | | ALTER | SYSCAUDT CICSAUDT |
| CORBASERVER/CORBASER | CORBASERVER | READ | CICUAUDT |
| | | UPDATE | NONE |
| | | ALTER | SYSCAUDT CICSAUDT |
| DB2CONN/DB2CONN | DB2CONN | Read | OPERAUDT CICUAUDT CICDAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| DB2ENTRY/DB2ENTRY | DB2ENTRY | READ | OPERAUDT CICUAUDT CICDAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| DB2TRAN/DB2TRAN | DB2TRAN | READ | OPERAUDT CICUAUDT CICDAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| DELETESHIPPED/DELETESH | DELETESHIPPED | READ | OPERAUDT CICUAUDT CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| DISPATCHER/DISPATCH | DISPATCHER | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| DJAR/DJAR | DJAR | READ | CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| DOCTEMPLATE/DOCTEMPL | DOCTEMPLATE | READ | CICUAUDT CICDAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| DSNAME/DSNAME | DSNAME | READ | OPERAUDT CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT CICUAUDT |
| DUMP/DUMP | DUMP | UPDATE | SYSCAUDT CICSAUDT CICUAUDT |
| DUMPDS/DUMPDS | DUMPDS | READ | CICDAUDT |
| | | UPDATE | SYSCAUDT |

| Resource/TSS Resource | Command | Access | Users |
|------------------------|--------------|--------|--|
| | | | CICSAUDT CICUAUDT |
| ENQMODEL/ENQMODEL | ENQMODEL | Read | CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| EVENTBINDING/EVENTBIN | EVENTBINDING | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| EVENTPROCESS/ EVENTPRO | EVENTPROCESS | Read | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| EXCI/EXCI | EXCI | READ | SYSCAUDT CICSAUDT CICUAUDT |
| EXITPROGRAM/EXITPROG | EXITPROGRAM | UPDATE | CICSAUDT CICUAUDT OPERAUDT SYSCAUDT |
| FECONNECTION/FEPIRESO | FECONNECTION | READ | NONE |
| | | UPDATE | SYSCAUDT CICSAUDT CICBAUDT OPERAUDT CICUAUDT |
| FENODE/FEPIRESO | FENODE | READ | NONE |
| | | UPDATE | SYSCAUDT CICSAUDT CICBAUDT OPERAUDT CICUAUDT |
| FEPOOL/FEPIRESO | FEPOOL | READ | NONE |
| | | UPDATE | SYSCAUDT CICSAUDT CICBAUDT OPERAUDT CICUAUDT |
| FEPROPSET/FEPIRESO | FEPROSET | READ | NONE |
| | | UPDATE | SYSCAUDT CICSAUDT CICBAUDT OPERAUDT CICUAUDT |
| FETARGET/FEPIRESO | FETARGET | READ | NONE |
| | | UPDATE | SYSCAUDT CICSAUDT CICBAUDT |

| Resource/TSS Resource | Command | Access | Users |
|-----------------------|--------------|--------|--|
| | | | OPERAUDT CICUAUDT |
| FILE/FILE | FILE | READ | ALL |
| | | UPDATE | CICBAUDT OPERAUDT CICUAUDT APPDAUDT* |
| | | ALTER | SYSCAUDT CICSAUDT |
| HOST/HOST | HOST | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| IPCONN/IPCONN | IPCONN | READ | OPERAUDT CICUAUDT CICDAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| IRC/IRC | IRC | READ | OPERAUDT CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT CICUAUDT |
| JOURNALMODEL/JOURNALM | JOURNALMODEL | READ | CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| JOURNALNAME/JOURNALN | JOURNALNAME | READ | NONE |
| | | UPDATE | SYSCAUDT CICSAUDT CICUAUDT |
| JVM/JVM | JVM | READ | SYSCAUDT CICSAUDT CICUAUDT |
| JVMPOOL/JVMPOOL | JVMPOOL | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| JVMPROFILE/JVMPROFI | JVMPROFILE | READ | SYSCAUDT CICSAUDT CICUAUDT |
| JVMSERVER/JVMSERVER | JVMSERVER | READ | NONE |
| | | ALTER | SYSCAUDT CICSAUDT |
| LIBRARY/LIBRARY | LIBRARY | READ | CICUAUDT CICDAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| LSRPOOL/LSRPOOL | LSRPOOL | ALTER | SYSCAUDT |

| Resource/TSS Resource | Command | Access | Users |
|-----------------------|--------------|--------|--|
| | | | CICSAUDT |
| MAPSET/MAPSET | MAPSET | ALTER | SYSCAUDT CICSAUDT |
| MODENAME/MODENAME | MODENAME | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| MONITOR/MONITOR | MONITOR | READ | CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT CICUAUDT |
| MQCONN/MQCONN | MQCONN | READ | OPERAUDT CICUAUDT CICDAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| MQINI/MQINI | MQINI | READ | SYSCAUDT CICSAUDT OPERAUDT CICDAUDT |
| MVSTCB/MVSTCB | MVSTCB | READ | SYSCAUDT CICSAUDT CICUAUDT |
| NETNAME/TERMINAL | NETNAME | READ | CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT CICBAUDT OPERAUDT CICUAUDT |
| PARTITIONSET/PARTITIO | PARTITIONSET | | |
| | | ALTER | SYSCAUDT CICSAUDT |
| PARTNER/PARTNER | PARTNER | READ | CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| PIPELINE/PIPELINE | PIPELINE | READ | CICUAUDT CICDAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| PROCESSTYPE/PROCESST | PROCESSTYPE | READ | CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| PROFILE/PROFILE | PROFILE | READ | CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| PROGRAM/PROGRAM | PROGRAM | READ | CICBAUDT CICDAUDT |

| Resource/TSS Resource | Command | Access | Users |
|------------------------|--------------|---------|--|
| | | UPDATE | OPERAUDT CICUAUDT APDAUDT* |
| | | ALTER | SYSCAUDT CICSAUDT |
| REQID/REQID | REQID | READ | SYSCAUDT CICSAUDT |
| REQUESTMODEL/ REQUESTM | REQUESTMODEL | READ | CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| RESETTIME | RESETTIME | UPDATE | SYSCAUDT CICSAUDT |
| RRMS/RRMS | RRMS | READ | SYSCAUDT CICSAUDT CICUAUDT |
| SECURITY/SECURITY | SECURITY | UPDATE | SYSCAUDT CICSAUDT |
| SESSIONS/SESSIONS | SESSIONS | ALTER | SYSCAUDT CICSAUDT |
| SHUTDOWN/SHUTDOWN | SHUTDOWN | UPDATE | SYSCAUDT CICSAUDT OPERAUDT CICUAUDT |
| STATISTICS/STATISTI | STATISTICS | READ | NONE |
| | | UPDATE | SYSCAUDT CICSAUDT CICUAUDT |
| STORAGE/STORAGE | STORAGE | READ | SYSCAUDT CICSAUDT CICUAUDT |
| STREAMNAME/STREAMNA | STREAMNAME | READ | SYSCAUDT CICSAUDT CICUAUDT |
| SUBPOOL/SUBPOOL | SUBPOOL | READ | SYSCAUDT CICSAUDT CICUAUDT |
| SYSDUMPCODE/SYSDUMPC | SYSDUMPCODE | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| | | CONTROL | SYSCAUDT CICSAUDT |
| SYSTEM/SYSTEM | SYSTEM | READ | CICBAUDT OPERAUDT CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |

| Resource/TSS Resource | Command | Access | Users |
|-----------------------|--------------|--------|-----------------------------------|
| TASK/TASK | TASK | READ | CICBAUDT OPERAUDT CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT CICUAUDT |
| TCLASS/TCLASS | TRANCLASS | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| TCPIP/TCPIP | TCPIP | READ | CICUAUDT CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| TCPIPSERVICE/TCPIPSER | TCPIPSERVICE | READ | CICUAUDT CICDAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| TDQUEUE/TDQUEUE | TDQUEUE | READ | OPERAUDT CICUAUDT CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| TEMPSTORAGE | TEMPSTORAGE | READ | CICUAUDT |
| | | UPDATE | CICSAUDT |
| | | | SYSCAUDT |
| TERMINAL/TERMINAL | TERMINAL | READ | CICDAUDT |
| | | UPDATE | CICBAUDT OPERAUDT CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| TRANDUMPCODE/TRANDUMP | TRANDUMPCODE | READ | CICUAUDT CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| TRANSACTION/TRANSACT | TRANSACTION | READ | CICDAUDT |
| | | UPDATE | OPERAUDT CICUAUDT APPDAUDT* |
| | | ALTER | SYSCAUDT CICSAUDT |
| TSMODEL/TSMODEL | TSMODEL | READ | CICUAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| TSPPOOL/TSPPOOL | TSPPOOL | READ | SYSCAUDT |

| Resource/TSS Resource | Command | Access | Users |
|-----------------------|------------|--------|--|
| | | | CICSAUDT CICUAUDT |
| TSQNAME/TSQNAME | TSQNAME | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| TSQUEUE/TSQUEUE | TSQUEUE | READ | CICUAUDT CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| TYPETERM/TYPETERM | TYPETERM | ALTER | SYSCAUDT CICSAUDT |
| UOW/UOW | UOW | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| UOWDSNFAIL/UOWDSNFA | UOWDSNFAIL | READ | SYSCAUDT CICSAUDT CICUAUDT |
| UOWENQ/UOWENQ | UOWENQ | READ | SYSCAUDT CICSAUDT CICUAUDT |
| UOWLINK/UOWLINK | UOWLINK | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| URIMAP/URIMAP | URIMAP | READ | CICUAUDT CICDAUDT |
| | | ALTER | SYSCAUDT CICSAUDT |
| VOLUME/VOLUME | VOLUME | UPDATE | SYSCAUDT CICSAUDT |
| VTAM/VTAM | VTAM | READ | CICDAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT OPERAUDT CICUAUDT |
| WEB/WEB | WEB | READ | CICUAUDT |
| | | UPDATE | SYSCAUDT CICSAUDT |
| WEBSERVICE/WEBSERVI | WEBSERVICE | READ | NONE |
| | | ALTER | SYSCAUDT CICSAUDT |

| Resource/TSS Resource | Command | Access | Users |
|-----------------------|--------------|--------|---------------------------------|
| WORKREQUEST/WORKREQU | WORKREQUEST | READ | SYSAUDT CICSAUDT CICUAUDT |
| XMLTRANSFORM/XMLTRANS | XMLTRANSFORM | READ | CICUAUDT |
| | | UPDATE | SYSAUDT CICSAUDT |

*Application Development Programmers can be granted this access ONLY on a Development or Test CICS region.

Each Command can take any combination of the following actions:

INQUIRE Retrieve information about
 SET To Change or Modify
 DISCARD To Remove
 CREATE To Define
 PERFORM Perform an action against (Initialize, Terminate, Delete, Request, Start, Reset, Refresh, Initiate)

| ACCESS | PERMISSIONS |
|-----------------|--|
| READ permits | INQUIRE |
| UPDATE permits | PERFORM, SET and DISCARD |
| ALTER permits | Create |
| CONTROL permits | Access to update the JOBLIST or DSPLIST option on SET SYSDUMPCODE . |

SRRAUDIT GROUPS

| | |
|----------|--|
| SYSAUDT | CICS Systems Programmers |
| CICSAUDT | CICS Started Task |
| CICBAUDT | CICS Batch Programs |
| CICUAUDT | CICS Utilities (Control O, Batch IDs submitted by Control M, MAINVIEW) |
| CICDAUDT | CICS Developers |
| OPERAUDT | OST CICS commands |
| APPDAUDT | Application Development Programmers |

Table 11-23: CICS SPI Resource Descriptions Table

Referenced by: ZCICA021, ZCICR021, ZCICT021

| Command | Description |
|-------------|---|
| ASSOCIATION | Association of information for a specified task |
| ATOMSERVICE | ATOMSERVICE resource definition |
| AUTINSTM | Terminal autoinstall model |
| AUTOINST | Terminal autoinstall values |
| BEAN | Information about an installed enterprise bean. |
| BRFACILITY | A virtual terminal (bridge facility) used by the 3270 bridge mechanism. |
| BUNDLE | A BUNDLE resource in the local CICS region |
| CAPTURESPEC | Information about a capture specification |
| CFDTPPOOL | Information about a coupling facility data table pool |

| Command | Description |
|--------------|--|
| CLASSCACHE | A shared class cache in the CICS® region |
| CONNECTION | A CICS Connection |
| CORBASERVER | A CorbaServer |
| DB2CONN | A CICS DB2 connection |
| DB2ENTRY | Used to define resources to be used by a specific transaction or by a group of transactions when accessing DB2 |
| DB2TRAN | A DB2TRAN associated with a DB2ENTRY |
| DELETSHPED | System settings that control automatic deletion of shipped terminal definitions |
| DISPATCHER | CICS dispatcher system information |
| DJAR | A definition of a specified deployed JAR file |
| DOCTEMPLATE | A document template |
| DSNAME | An external data set |
| DUMP | System dump of CICS |
| DUMPDS | CICS transaction dump data sets |
| ENQMODEL | An ENQMODEL definition |
| EVENTBINDING | A specified event binding |
| EVENTPROCESS | Event processing |
| EXCI | External CICS interface |
| EXITPROGRAM | A user exit |
| FECONNECTION | Information about the state of FEPI connections |
| FENODE | FEPI nodes |
| FEPOOL | FEPI pools of connections |
| FEPROPSET | FEPI property set |
| FETARGET | FEPI target |
| FILE | A FILE definition |
| HOST | A virtual host |
| IPCONN | An IPCONN resource is a Transport Control Protocol/Internet Protocol (TCP/IP) communication link from your local CICS® region to another CICS region or another system |
| IRC | An interregion communication |
| JOURNALMODEL | A journal model definition |
| JOURNALNAME | A journal name |
| JVM | JVMs in a CICS region |
| JVMPOOL | Pool of JVMs in the CICS address space |
| JVMPROFILE | JVM profiles that have been used in a CICS region |
| JVMSERVER | JVM server runtime environment in the CICS region |
| LIBRARY | LIBRARY resource in the local CICS region |
| LSRPOOL | Local shared resources (LSR) pool |
| MAPSET | The definition of a particular program, map set, or partition set |
| MODENAME | Sessions in an APPC session group |
| MONITOR | MONITOR command to find out whether CICS monitoring is active, which types of data are being recorded, and other recording options |
| MQCONN | The connection between CICS and WebSphere® MQ |

| Command | Description |
|--------------|---|
| MQINI | Initiation queue to be used for the connection between CICS and WebSphere MQ |
| MVSTCB | Addresses and storage usage information for MVS TCBs |
| NETNAME | Terminal or session |
| PARTITIONSET | Command installs a PARTITIONSET definition with the attribute specified on the command |
| PARTNER | The name assigned in its PARTNER resource definition |
| PIPELINE | PIPELINE in the local CICS region |
| PROCESSTYPE | A PROCESSTYPE in the local CICS region |
| PROFILE | A PROFILE definition |
| PROGRAM | A PROGRAM definition |
| REQUESTMODEL | A REQUESTMODEL resource definition maps an inbound request that is formatted using the Internet Inter-ORB PROTOCOL (IIOP) to a CICS transaction that is to be started to process the request |
| RESETTIME | Reset date and time |
| RRMS | Indicates whether inbound transactional EXCI work is currently being accepted |
| SECURITY | A request for CICS security information to be refreshed from its external security manager (ESM) source, so that it reflects any updates made since the information was last retrieved |
| SESSIONS | A SESSIONS definition |
| SHUTDOWN | Shuts down the CICS system |
| STATISTICS | Retrieve the current statistics for a single resource, or global statistics for a class of resources |
| STORAGE | You can use it to get a list of the task storage areas associated with a particular task (using the NUMELEMENTS option), or you can use it to find the length and starting address of a particular area of storage (using the ADDRESS option) |
| STREAMNAME | Retrieve information about a currently connected MVS log stream |
| SUBPOOL | Command returns information about a particular storage subpool |
| SYSDUMPCODE | System dump code table entry |
| SYSTEM | Returns information about the CICS system under which the task issuing the command is executing |
| TASK | Returns information about a specific user task. User tasks are those associated with user-defined transactions or with CICS-supplied transactions that are normally invoked by an operator |
| TCLASS | Transaction Class |
| TCPIP | CICS internal sockets support |
| TCPIPSERVICE | TCPIP ports on which CICS internal TCPIP support is currently |
| TDQUEUE | A transient data queue in the local CICS region |
| TERMINAL | Terminal Command |
| TRANDUMPCODE | A transaction dump code |
| TRANSACTION | A transaction installed in your CICS system |
| TSMODEL | A temporary Storage Table in the local CICS region |
| TSPool | A shared temporary storage pool |

| Command | Description |
|--------------|---|
| TSQNAME | A queue with a name up to 16 characters long |
| TYPETERM | A terminal type in the local CICS region |
| UOW | Information about a unit of work (UOW) |
| UOWDSNFAIL | The UOWDSNFAIL command returns UOWs that are shunted and also UOWs that are in the process of being retried. In the latter case, the only data sets returned are those that have not yet been processed as part of the retry. |
| UOWENQ | Retrieves information about enqueues. Enqueues are used by CICS to lock recoverable resources, such as file records or queues, to the UOW that is updating them. User enqueues obtained by the EXEC CICS ENQ command are also returned. |
| UOWLINK | Retrieves information about a connection involved in a unit of work. The connection can be to a remote system, to a task-related user exit, or to a CFDT server. |
| URIMAP | A URIMAP resource definition |
| VTAM | The connection between CICS and VTAM |
| WEB | CICS Web support |
| WEBSERVICE | A WEBSERVICE in the local CICS region |
| WORKREQUEST | Tasks that are started as a result of action by a request receiver |
| XMLTRANSFORM | Information about an installed XMLTRANSFORM resource. This information can include the state of the XMLTRANSFORM resource and details about the conditions under which the XMLTRANSFORM resource was installed, such as which mapping level was used. |

11.6 WebSphere MQ Requirements

Table 11-24: WebSphere MQ Command Security Controls

Referenced by: ZWMQ0059

| Command | Profile | Access Level | Authorized Users | Log |
|----------------|--|--------------|--|-----|
| ALTER xxxxxx | ssid.ALTER.xxxxxx | ALTER | MQ administrator Systems programmers Queue managers | Y |
| ALTER queue | Ssid.ALTER.queue Except ssid.SYSTEM.queue | ALTER | MQ administrator Decentralized MQ admin Systems Programmers Queue managers | Y |
| ARCHIVE LOG | ssid.ARCHIVE.LOG | CONTROL | MQ administrator Systems programmers Queue managers Operators Console automation software | Y |

| Command | Profile | Access Level | Authorized Users | Log |
|----------------|---|--------------|---|-----|
| CLEAR QLOCAL | ssid.CLEAR.QLOCAL | ALTER | MQ administrator Systems programmers Queue managers MQ System Admin Batch | Y |
| DEFINE xxxxxx | ssid.DEFINE.xxxxxx | ALTER | MQ administrator Systems programmers Queue managers | Y |
| DEFINE QUEUE | Ssid.DEFINE.QUEUE Except ssid.SYSTEM.queue | ALTER | MQ administrator Decentralized MQ admin Systems programmers Queue managers | Y |
| DELETE xxxxxx | ssid.DELETE.xxxxxx | ALTER | MQ administrator Systems programmers Queue managers | Y |
| DELETE queue | Ssid.DELETE.queue Except ssid.SYSTEM.queue | ALTER | MQ administrator Decentralized MQ admin Systems Programmers Queue managers | Y |
| DISPLAY xxxxxx | ssid.DISPLAY.xxxxxx | READ | Auditors Application programmers MQ administrator Systems programmers Queue manager Operators Console automation software MQ System Admin Batch | N |
| PING xxxxxx | ssid.PING.xxxxxx | CONTROL | Application programmers MQ administrator Systems programmers Queue managers Operators Console automation software | N |
| RECOVER BSDS | ssid.RECOVER.BSDS | CONTROL | MQ administrator Systems programmers Queue managers | Y |
| REFRESH xxxxxx | ssid.REFRESH.xxxxxx | ALTER | Security staff MQ administrator Systems programmers Queue managers | Y |

| Command | Profile | Access Level | Authorized Users | Log |
|---------------------|-----------------------|--------------|--|-----|
| RESET xxxxxx | ssid.RESET.xxxxxx | CONTROL | MQ administrator Systems programmers Queue managers | Y |
| RESOLVE xxxxxx | ssid.RESOLVE.xxxxxx | CONTROL | MQ administrator Systems programmers Queue managers Operators Console automation software | Y |
| RESUME QMGR | ssid.RESUME.QMGR | CONTROL | MQ administrator Systems programmers Queue managers Operators Console automation software | Y |
| RVERIFY SECURITY | ssid.RVERIFY.SECURITY | ALTER | Security staff MQ administrator | Y |
| START xxxxxx | ssid.START.xxxxxx | CONTROL | MQ administrator Systems programmers Queue managers Operators Console automation software | Y |
| STOP xxxxxx | ssid.STOP.xxxxxx | CONTROL | MQ administrator Systems programmers Queue managers Operators Console automation software | Y |
| SUSPEND QMGR | ssid.SUSPEND.QMGR | CONTROL | MQ administrator Systems programmers Queue managers Operators Console automation software | Y |

11.7 Web Application Server Requirements

Table 11-25: WAS HFS Permission Bits

Referenced by:ZWAS0020

| IHS Vendor Server Software HFS Object Security Settings | | | | |
|---|-----------------|-----------------|-------------|-------|
| Directory or File | Permission Bits | User Audit Bits | Owner | Group |
| /usr/lpp/internet | 755 | fff | UID(0) user | IMWEB |
| /usr/lpp/internet/bin | 755 | fff | UID(0) user | IMWEB |
| /usr/lpp/internet/sbin | 750 | fff | UID(0) user | IMWEB |

| IHS Local Server Standard HFS Object Security Settings | | | | |
|--|-----------------|-----------------|---------|----------|
| Directory or File | Permission Bits | User Audit Bits | Owner | Group |
| .../websrv1_root/ | 555 | fff | websrv1 | webadmgl |
| .../websrv1_root/Admin | 550 | fff | websrv1 | webadmgl |
| .../websrv1_root/admin-bin | 550 | fff | websrv1 | webadmgl |
| .../websrv1_root/cgi-bin | 551 | fff | websrv1 | webadmgl |
| .../websrv1_root/fcgi-bin | 550 | fff | websrv1 | webadmgl |
| .../websrv1_root/pub | 555 | fff | websrv1 | webadmgl |
| /etc/websrv1/httpd.conf | 460 | faf | websrv1 | webadmgl |
| /etc/websrv1/httpd.envvars | 564 | faf | websrv1 | webadmgl |
| /etc/websrv1/mvsds.conf | 460 | faf | websrv1 | webadmgl |

| IHS Local Server Log HFS Object Security Settings | | | | |
|---|-----------------|-----------------|---------|----------|
| Directory or File | Permission Bits | User Audit Bits | Owner | Group |
| .../websrv1_root/logs | 750 | fff | websrv1 | webadmgl |
| .../websrv1_root/logs/httpd-log | 750 | fff | websrv1 | webadmgl |
| .../websrv1_root/logs/httpd-errors | 750 | fff | websrv1 | webadmgl |
| .../websrv1_root/logs/cgi-error | 750 | fff | websrv1 | webadmgl |

11.8 SDSF Requirements

The following describes the definitions of the entries in the User Group column for all of the tables in the SDSF Requirements:

| User Group |
|--|
| APPDAUDT - Application Development Programmers |
| APPSAUDT - Application Support Programmers |
| AUDTAUDT - Auditors |
| OPERAUDT - Operations Personnel |
| SYSPAUDT - Systems Programming staff |
| * - All Users |

Table 11-26: SDSF SAF Resources

Referenced by: ZISF0020

| Resource Name | User Group | Access | Logging |
|----------------------------------|--|---------|---------|
| GROUP.** | * | NONE | |
| GROUP.group-name.server-name | Dependent on group | READ | |
| ISF.CONNECT. <i>sysname</i> | * | READ | |
| ISFAPF. <i>datasetname</i> | OPERAUDT SYSPAUDT | READ | |
| ISFAPPL. <i>device-name.jesx</i> | * | READ | |
| | OPERAUDT SYSPAUDT | CONTROL | |
| ISFAT*TR.** | * | NONE | |
| ISFAT*TR.CHECK.** | AUDTAUDT OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.ENCLAVE.** | AUDTAUDT OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.JOB.** | APPDAUDT APPSAUDT OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.JOB.PRTEST | * | UPDATE | |
| ISFAT*TR.JOBCL.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.LINE.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.MEMBER.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.MODIFY.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.NODE.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.OFFLOAD.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.OUTDESC.** | * | UPDATE | |
| ISFAT*TR.OUTPUT.** | AUDTAUDT APPDAUDT APPSAUDT OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.OUTPUT.BURST | * | UPDATE | |
| ISFAT*TR.OUTPUT.CLASS | * | UPDATE | |
| ISFAT*TR.OUTPUT.DEST | * | UPDATE | |
| ISFAT*TR.OUTPUT.FCB | * | UPDATE | |
| ISFAT*TR.OUTPUT.FLASH | * | UPDATE | |
| ISFAT*TR.OUTPUT.FORMS | * | UPDATE | |

| Resource Name | User Group | Access | Logging |
|--------------------------|--|--------|---------|
| ISFAT*TR.OUTPUT.PRMODE | * | UPDATE | |
| ISFAT*TR.OUTPUT.UCS | * | UPDATE | |
| ISFAT*TR.OUTPUT.WRITER | * | UPDATE | |
| ISFAT*TR.PROPTS.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.RDR.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.RESMON.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.RESOURCE.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.SELECT.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAT*TR.SPOOL.** | OPERAUDT SYSPAUDT | UPDATE | |
| ISFAUTH.** | * | NONE | |
| ISFAUTH.DEST.** | APPDAUDT APPSAUDT | READ | |
| | OPERAUDT SYSPAUDT | ALTER | |
| ISFCFC | OPERAUDT SYSPAUDT | READ | |
| ISFCFS | OPERAUDT SYSPAUDT | READ | |
| ISFCMD.** | * | NONE | |
| ISFCMD.DSP.ACTIVE.jesx | * | READ | |
| ISFCMD.DSP.HELD.jesx | * | READ | |
| ISFCMD.DSP.INPUT.jesx | * | READ | |
| ISFCMD.DSP.JGROUP.jesx | * | READ | |
| ISFCMD.DSP.OUTPUT.jesx | * | READ | |
| ISFCMD.DSP.SCHENV.system | * | READ | |
| ISFCMD.DSP.STATUS.jesx | * | READ | |
| ISFCMD.DSP.SYMBOL.system | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.FILTER.ACTION | APPDAUDT APPSAUDT OPERAUDT SYSPAUDT | READ | |
| ISFCMD.FILTER.DEST | * | READ | |
| ISFCMD.FILTER.FINDLIM | * | READ | |
| ISFCMD.FILTER.INPUT | * | READ | |
| | SYSPAUDT | | |
| ISFCMD.FILTER.OWNER | * | READ | |
| ISFCMD.FILTER.PREFIX | * | READ | |

| Resource Name | User Group | Access | Logging |
|------------------------------------|--|--------|---------|
| ISFCMD.FILTER.RSYS | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.FILTER.SYSID | * | READ | |
| ISFCMD.FILTER.SYSNAME | * | READ | |
| ISFCMD.MAINT.ABEND | SYSPAUDT | READ | |
| ISFCMD.MAINT.TRACE | APPDAUDT APPSAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.APF.system | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.AS | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.CFSTRUCT.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.COUPLE.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.CSR.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.DEVACT.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.ENCLAVE | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.ENQUEUE. <i>system</i> | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.DYNX | APPDAUDT APPSAUDT | READ | |

| Resource Name | User Group | Access | Logging |
|-----------------------------|--|--------|---------|
| | OPERAUDT SECAAUDT SYSPAUDT | | |
| ISFCMD.ODSP.FILESYS.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.HCHECKER.system | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.INITIATOR.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.JOB0.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.JOBCLASS.jesx | APPDAUDT APPSAUDT OPERAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.LINE.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.LNK.system | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.LPA.system | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.MAS.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |

| Resource Name | User Group | Access | Logging |
|----------------------------|--|--------|---------|
| ISFCMD.ODSP.NC.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.NETACT.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.NODE.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.NS.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.PAGE.system | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.PARMLIB.system | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.PRINTER.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.PROCESS | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.PROCLIB.JES2 | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.PUNCH.jesx | APPDAUDT APPSAUDT | READ | |

| Resource Name | User Group | Access | Logging |
|-----------------------------|--|--------|---------|
| | OPERAUDT SECAAUDT SYSPAUDT | | |
| ISFCMD.ODSP.READER.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.RESMON.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.RESOURCE.system | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.SO.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.SPOOL.jesx | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| SFCMD.ODSP.SMSVOL.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.SR.system | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.STORGRP.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.SUBSYS.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.SYSLOG.jesx | APPDAUDT APPSAUDT AUDTAUDT | READ | |

| Resource Name | User Group | Access | Logging |
|--------------------------------------|--|---------|---------|
| | OPERAUDT SECAAUDT SYSPAUDT | | |
| ISFCMD.ODSP.SYSTEM.system | APPDAUDT APPSAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.TRACKER.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.ULOG.jesx | APPDAUDT APPSAUDT AUDTAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.ODSP.VIRTSTOR.sysname | OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFCMD.OPT.SERVER | SYSPAUDT | READ | |
| ISFDEV. | OPERAUDT SYSPAUDT | READ | |
| ISFDISP. | * OPERAUDT SYSPAUDT | READ | |
| ISFDYNEX. | OPERAUDT SYSPAUDT | READ | |
| ISFENC.subsystem-type.subsystem-name | OPERAUDT SYSPAUDT | ALTER | |
| ISFENQ.majorname.sysname | OPERAUDT SYSPAUDT | READ | |
| ISFFS. | OPERAUDT SYSPAUDT | READ | |
| ISFGT. | OPERAUDT SYSPAUDT | READ | |
| ISFINIT.Ixx.jesx | * APPDAUDT APPSAUDT | READ | |
| | OPERAUDT SYSPAUDT | CONTROL | |
| ISFJDD. | * OPERAUDT SYSPAUDT | READ | |
| ISFJOBCL.class.jesx | * | READ | |

| Resource Name | User Group | Access | Logging |
|--------------------------|---|---------|---------|
| | OPERAUDT SYSPAUDT | CONTROL | |
| ISFLINE.device-name.jesx | * APFDAUDT APPSAUDT | READ | |
| | OPERAUDT SYSPAUDT | ALTER | |
| ISFLNK.datasetname | OPERAUDT SYSPAUDT | READ | |
| ISFLPA.datasetname | OPERAUDT SYSPAUDT | READ | |
| ISFMEMB.member-name.jesx | * | READ | |
| | OPERAUDT SYSPAUDT | ALTER | |
| ISFNETACT. | OPERAUDT SYSPAUDT | READ | |
| ISFNODE.node-name.jesx | * | READ | |
| | OPERAUDT SYSPAUDT | CONTROL | |
| ISFNS.device-name.jesx | OPERAUDT SYSPAUDT | CONTROL | |
| ISFOPER.ANYDEST.jesx | * APFDAUDT APPSAUDT OPERAUDT SYSPAUDT | READ | |
| ISFOPER.DEST.jesx | APFDAUDT APPSAUDT OPERAUDT SYSPAUDT | READ | |
| ISFOPER.SYSTEM | AUDTAUDT OPERAUDT SECAAUDT SYSPAUDT | READ | |
| ISFPAG.datasetname | OPERAUDT SYSPAUDT | READ | |
| ISFPARM.datasetname | OPERAUDT SYSPAUDT | READ | |
| ISFPLIB. | OPERAUDT SYSPAUDT | READ | |
| ISFPROC.owner.process | APFDAUDT APPSAUDT | READ | |
| | OPERAUDT SYSPAUDT | ALTER | |
| ISFRES.resource.system | * | READ | |

| Resource Name | User Group | Access | Logging |
|------------------------------------|----------------------|---------|---------|
| | OPERAUDT SYSPAUDT | ALTER | |
| ISFRM.resource.jesx | OPERAUDT SYSPAUDT | CONTROL | |
| ISFSE.sched-env.system | OPERAUDT SYSPAUDT | READ | |
| ISFSMFVOL. | OPERAUDT SYSPAUDT | READ | |
| ISFISO.device-name.jesx | * | READ | |
| | OPERAUDT SYSPAUDT | ALTER | |
| ISFSOCK.device-name.jesx | OPERAUDT SYSPAUDT | CONTROL | |
| ISFSP.volser.jesx | APPDAUDT APPSAUDT | READ | |
| | OPERAUDT SYSPAUDT | CONTROL | |
| ISFSR.ACTION.org-system.jobname | OPERAUDT SYSPAUDT | READ | |
| ISFSR.REPLY.org-system.jobname | OPERAUDT SYSPAUDT | READ | |
| ISFSR.type.org-system.jobname | OPERAUDT SYSPAUDT | READ | |
| ISFSTORGRP. | OPERAUDT SYSPAUDT | READ | |
| ISFSUBSYS. | OPERAUDT SYSPAUDT | READ | |
| ISFSYM. <i>symbolname.sysname</i> | OPERAUDT SYSPAUDT | READ | |
| ISFSYS. <i>sysplexname.sysname</i> | OPERAUDT SYSPAUDT | READ | |
| SERVER.NOPARM | SYSPAUDT | READ | READ |

Table 11-27: SDSF SAF Resource Descriptions

| Resource Name | Description |
|------------------------------|---|
| GROUP.group-name.server-name | Membership in group |
| ISFACCR.ENCLAVE.** | Modify fields on the Enclaves (ENC) panel |
| ISFAT*TR.CHECK.** | Modify fields on the Health checker (CK) panel |
| ISFAT*TR.JOB.** | Modify job fields on the Display Active (DA), Input (I), and Status (ST) panels |
| ISFAT*TR.JOB.PRTPDEST | Modify JES2 print destination name on ST and I panels |

| Resource Name | Description |
|--------------------------|--|
| ISFAT*TR.JOBCL.** | Modify Job Class panel fields |
| ISFAT*TR.LINE.** | Modify Line panel fields |
| ISFAT*TR.MEMBER.** | Modify Multi-Access Spool panel fields |
| ISFAT*TR.MODIFY.** | Modify Spool Offload panel fields |
| ISFAT*TR.NODE.** | Modify Node panel fields |
| ISFAT*TR.OFFLOAD.** | Modify Spool Offload panel fields |
| ISFAT*TR.OUTDESC.** | Modify output descriptor fields on the Job Data Set (JDS) and Output Descriptor (OD) panels |
| ISFAT*TR.OUTPUT.** | Modify output group fields on the Held Output (H) and Output Queue (O) panels |
| ISFAT*TR.OUTPUT.BURST | Modify burst indication field on H and O panels |
| ISFAT*TR.OUTPUT.CLASS | Modify JES2 output class on H and O panels |
| ISFAT*TR.OUTPUT.DEST | Modify JES2 print destination name on H and O panels |
| ISFAT*TR.OUTPUT.FCB | Modify output FCB ID on H and O panels |
| ISFAT*TR.OUTPUT.FLASH | Modify output flash ID on H and O panels |
| ISFAT*TR.OUTPUT.FORMS | Modify output form number on H and O panels |
| ISFAT*TR.OUTPUT.PRMODE | Modify printer process mode on H and O panels |
| ISFAT*TR.OUTPUT.UCS | Modify output UCS ID on H and O panels |
| ISFAT*TR.OUTPUT.WRITER | Modify output external writer name on H and O panels |
| ISFAT*TR.PROPTS.** | Modify Printer panel fields, lines and transmitter fields on the Lines panel, and Punch panel fields |
| ISFAT*TR.RDR.** | Modify fields on the Readers (RDR) panel |
| ISFAT*TR.RESMON.** | Modify fields on the Resource monitor (RM) panel |
| ISFAT*TR.RESOURCE.** | Modify WLM Resource panel fields |
| ISFAT*TR.SELECT.** | Modify selection criteria fields on the Initiator, Line, Printer, Punch, and Spool Offload panels |
| ISFAT*TR.SPOOL.** | Modify fields on the Spool volumes (SP) panel |
| ISFAUTH.DEST.destname | Specific destination name |
| ISFAUTH.DEST.destname | Display and list jobs |
| ISFAUTH.DEST.destname | All other functions such as cancel, purge, and release jobs |
| ISFCMD.DSP.ACTIVE.jesx | Display Active users (DA) panel command |
| ISFCMD.DSP.HELD.jesx | Held Output (H) panel command |
| ISFCMD.DSP.INPUT.jesx | Input Queue (I) panel command |
| ISFCMD.DSP.OUTPUT.jesx | Output Queue (O) panel command |
| ISFCMD.DSP.SCHENV.system | Scheduling Environment (SE) panel command |
| ISFCMD.DSP.STATUS.jesx | Status (ST) panel command |

| Resource Name | Description |
|--------------------------------------|---|
| ISFCMD.FILTER.ACTION | Gives user authority to issue the ACTION command. |
| ISFCMD.FILTER.DEST | Gives user authority to issue the DEST command. |
| ISFCMD.FILTER.FINDLIM | Gives user authority to issue the FINDLIM command. |
| ISFCMD.FILTER.INPUT | Gives user authority to issue the INPUT command. |
| ISFCMD.FILTER.OWNER | Gives user authority to issue the OWNER command. |
| ISFCMD.FILTER.PREFIX | Gives user authority to issue the PREFIX command. |
| ISFCMD.FILTER.RSYS | Gives user authority to issue the RSYS command. |
| ISFCMD.FILTER.SYSID | Gives user authority to issue the SYSID command. |
| ISFCMD.FILTER.SYSNAME | Gives user authority to issue the SYSNAME command. |
| ISFCMD.MAINT.ABEND | Cause SDSF to abend |
| ISFCMD.MAINT.TRACE | Create trace records with SDSF data |
| ISFCMD.ODSP.ENCLAVE | Enclave (ENC) panel command |
| ISFCMD.ODSP.INITIATOR.jesx | Initiator (INIT) panel command |
| ISFCMD.ODSP.JOBCLASS.jesx | Job Class (JC) panel command |
| ISFCMD.ODSP.LINE.jesx | Line (LI) panel command |
| ISFCMD.ODSP.MAS.jesx | Multi-Access Spool (MAS) panel command |
| ISFCMD.ODSP.NODE.jesx | Node (NO) panel command |
| ISFCMD.ODSP.PRINTER.jesx | Printer (PR) panel command |
| ISFCMD.ODSP.PROCESS | Process (PS) panel command |
| ISFCMD.ODSP.PUNCH.jesx | Punch (PUN) panel command |
| ISFCMD.ODSP.READER.jesx | Reader (RDR) panel command |
| ISFCMD.ODSP.RESOURCE.system | Resource (RES) panel command |
| ISFCMD.ODSP.SO.jesx | Spool Offload (SO) panel command |
| ISFCMD.ODSP.SPOOL.jesx | Spool (SP) volume panel command |
| ISFCMD.ODSP.SR.system | System Request (SR) panel command |
| ISFCMD.ODSP.SYSLOG.jesx | Syslog and Operlog (LOG) panel command |
| ISFCMD.ODSP.ULOG.jesx | User Log (ULOG) panel command |
| ISFCMD.OPT.SERVER | Use of the SERVER parameter on the SDSF command |
| ISFENC.subsystem-type.subsystem-name | Resume and quiesce an enclave |
| ISFINIT.Ixx.jesx | Display information about an initiator |
| ISFINIT.Ixx.jesx | All other functions such as start, stop, and drain an initiator |
| ISFJOBCL.class.jesx | Display information about a job class |
| ISFJOBCL.class.jesx | Modify job class characteristics |

| Resource Name | Description |
|---------------------------------|---|
| ISFLINE.device-name.jesx | Display information about a line and associated transmitters and receivers |
| ISFLINE.device-name.jesx | Cancel data being transmitted and received |
| ISFLINE.device-name.jesx | All other functions such as start, stop, and disconnect a line |
| ISFMEMB.member-name.jesx | Display information about a MAS member |
| ISFMEMB.member-name.jesx | Stop and restart a member in a MAS |
| ISFMEMB.member-name.jesx | All other functions such as stop (abend) and stop (ignore activity) a MAS member |
| ISFNODE.node-name.jesx | Display information about a node |
| ISFNODE.node-name.jesx | All other functions such as start node communication |
| ISFNS.device-name.jesx | Network servers |
| ISFOPER.ANYDEST.jesx | Any destination name |
| ISFOPER.DEST.jesx | Browse and print Standard SYSIN/SYSOUT data sets |
| ISFOPER.SYSTEM | Command line commands (/) |
| ISFPROC.owner.process | Display information about a process |
| ISFPROC.owner.process | Cancel a process |
| ISFRES.resource.system | Display information about a WLM resource |
| ISFRES.resource.system | Modify the state of a WLM resource |
| ISFRM.resource.jesx | JES resources |
| ISFSE.sched-env.system | Display information about a scheduling environment |
| ISFSO.device-name.jesx | Display information about a spool offloader and associated transmitters and receivers |
| ISFSO.device-name.jesx | Cancel the job and output active on a transmitter and receiver |
| ISFSO.device-name.jesx | All other functions such as start and drain an offloader |
| ISFSOCK.device-name.jesx | Network connections |
| ISFSP.volser.jesx | Display information about a spool volume |
| ISFSP.volser.jesx | All other commands such as drain, start, and halt a spool volume |
| ISFSR.ACTION.org-system.jobname | Remove action messages from the display |
| ISFSR.REPLY.org-system.jobname | Reply to a system message |
| ISFSR.type.org-system.jobname | Display information about system request messages |
| SERVER.NOPARM | Reverting to ISFPARMS in assembler macro format |

- jesx is the name of the JES2 subsystem
- destname is destination name of the job
- xx is the number of the JES2 initiator

- device-name is the name of the line, offloader, transmitter, or receiver
- node-name is the name of the JES2 node
- member-name is the name of the member defined in the MAS configuration
- class is the job class
- sched-env is the name of the scheduling environment
- system is the name of the MVS system (sysplex support)
- resource is the name of the WLM resource
- type is the message type (ACTION or REPLY)
- org-system is the name of the originating system
- jobname is the name of the job issuing the message
- subsystem-type is the type of subsystem such as MQ or DB2
- subsystem-name is the name of the subsystem
- owner is the owner of the z/OS UNIX process
- process is the name of the z/OS UNIX process
- volser is the serial number of the spool volume

Table 11-28: SDSF Server OPERCMDS Resources

Referenced by: ZISF0021

| Resource Name | Description | Logging | User Group | Access |
|--|--|---------|----------------------------------|---------|
| <i>server</i> .MODIFY.DISPLAY | Use of the DISPLAY parameter on the MVS MODIFY command (F) for the SDSF server | | AUDTAUDT OPERAUDT SYSPAUDT | READ |
| <i>server</i> .MODIFY. <i>mod-parm</i> | Use of various parameters on the MVS MODIFY command for the SDSF server | UPDATE | SYSPAUDT | CONTROL |

In the table:

- *server* is the name of the SDSF server specified either by the ISFPMAC macro or SDSF command.
- *mod-parm* is one of the following parameters specified on the MVS MODIFY command: DEBUG, FOLDMSG, LOGCLASS, LOGTYPE, REFRESH, START, STOP, TRACE, and TRCLASS.
- The server START and STOP commands are protected by MVS. The resources are MVS.START.STC.*server* and MVS.STOP.STC.*server* respectively. They are defined to the OPERCMDS resource class and require update authority.

Table 11-29: WebSphere MQ Queue Definition Authority SAF Resources

| Resource Class | Resource Name | Description | Req'd Access | |
|----------------|--|--|--------------|--------|
| | | | Server | Client |
| MQCMDS | <i>ssid</i> .DEFINE.QMODEL | Define queues | ALTER | NONE |
| MQCMDS | <i>ssid</i> .DEFINE.QALIAS | Define a queue alias | ALTER | NONE |
| MQADMIN | <i>ssid</i> .QUEUE. <i>prefix</i> .MODEL.QUEUE | Define queues | ALTER | NONE |
| MQQUEUE | <i>ssid</i> .SYSTEM.COMMAND.REPLY.MODEL. | Model queue (used to create the temporary ReplyTo queue) | ALTER | NONE |
| MQQUEUE | <i>ssid</i> .SYSTEM.COMMAND.INPUT | Command input queue (used to submit DEFINE commands) | ALTER | NONE |

In the table:

- *ssid* is the MQ subsystem ID. This is the queue manager name specified on the COMM statement of ISFPARMS.
- *prefix* is a string that identifies the queue name. It is defined by the QPREFIX parameter of the COMM statement in ISFPARMS.

11.9 CL/SuperSession Requirements

Table 11-30: Required GLOBAL Common Profile Segment Options

Referenced by: ZCLS0040

| Required GLOBAL Common Profile Segment Options | | |
|--|--|----------------|
| Option | Description | Required Value |
| Administrator authority | Grants Administrator authority | N |
| Maintain customized menu | Allows the user to customize the application menu | Y |
| Add sessions to the menu | Allows the user to add VTAM sessions to the application menu | N |
| Note: The above options may be set to Yes only for the Administrator(s). | | |
| Resource validation | Resource name (<u>A</u> PPPLID and/or <u>S</u> ession Id) used when calling the ESM for dynamic application lists | A |

| Required GLOBAL Common Profile Segment Options | | |
|--|---|--|
| Option | Description | Required Value |
| Timeout interval | Interval after which the user's session should be terminated for inactivity | 00:15 |
| Group profile name | Associated group profile | Will only be specified in a user level profile |

Table 11-31: Required SuperSess GLOBAL Profile Segment Options

Referenced by: ZCLS0040

| Required SupSess GLOBAL Profile Segment Options | | |
|---|---|----------------|
| Option | Description | Required Value |
| Maintain trigger profile | Allows the user to save changes to the trigger (<i>hot-key</i> string) profile when logging off | N |
| Add triggers to profile | Allows the user to create trigger definitions and add them to the trigger (<i>hot-key</i> string) profile | N |
| Modify triggers in profile | Allows the user to modify existing trigger definitions in the trigger (<i>hot-key</i> string) profile | N |
| Switch terminals | Allows switching an active CL/SUPERSESSION session to another VTAM terminal | Y |
| Preserve sessions upon exit | Allows VTAM application sessions to remain active (until they time out) if the CL/SUPERSESSION session is terminated for some reason (e.g., switching to another CL/SUPERSESSION at another site or host) | N |

11.10 CA ROSCOE Requirements

11.10.1 Access Attribute Translation

Throughout this guide, access attributes are listed as CONTROL, READ, or UPDATE. Table 11.32 displays the Advantage CA-Roscoe access attributes and the corresponding attributes you must specify for your external security system.

Table 11-32: Advantage CA-Roscoe Access Attributes—External Security System

| Access Attribute | eTrust CA-ACF | eTrust CA-Top Secret | IBM RACF |
|------------------|---------------|----------------------|----------|
| CONTROL | DELETE | CONTROL | CONTROL |
| READ | READ | READ | READ |
| UPDATE | UPDATE | UPDATE | UPDATE |

Table 11-33: CA ROSCOE Resources

Referenced by: ZROS0020

| RESOURCE | ACCESS | USER GROUPS** | Note |
|-----------------------------|---------|---------------|----------|
| [rosid.]ROSCMD | CONTROL | | |
| | READ | * | |
| [rosid.]ROSCMD.ETSO.program | READ | * | |
| [rosid.]ROSCMD.ETSO.ROSTMP | READ | * | |
| [rosid.]ROSCMD.MONITOR.mon | READ | SYSPAUDT | |
| [rosid.]ROSCMD.MONITOR | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.MONITOR.AMS | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.AWS | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.MONITOR.CA1 | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.COB | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.CON | CONTROL | SYSPAUDT | |
| | | OPERAUDT | |
| [rosid.]ROSCMD.MONITOR.DIS | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.DMS | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.DOC | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.EXP | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.IMP | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.JCK | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.MON | READ | SYSPAUDT | |
| [rosid.]ROSCMD.MONITOR.PUR | READ | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.RTF | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.MONITOR.SIM | CONTROL | SECAAUDT | TSS ONLY |
| | CONTROL | SECDAUDT | TSS ONLY |
| | READ | AUDTAUDT | TSS ONLY |
| [rosid.]ROSCMD.MONITOR.SOR | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.TIQ | CONTROL | SYSPAUDT | |
| | READ | * | |
| [rosid.]ROSCMD.MONITOR.TSS | CONTROL | SECAAUDT | |
| | | SECDAUDT | |

| RESOURCE | ACCESS | USER GROUPS** | Note |
|---|----------|---------------|------|
| | | AUDTAUDT | |
| [rosid.]ROSCMD.MONITOR.ZAP | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ACCT.ACCT.BUFFERS | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ACCT.ACCT.FILES | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ACCT.ACCT.ROSCOE | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ACCT.ACCT.SMF | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ACCT.ACCT.STATUS | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ACCT.ACCT.SWITCH | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ACCT.RTM.DISPLAY | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ACCT.RTM.INCL | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ACCT.RTM.LIST | OPERATOR | | |
| [rosid.]ROSCMD.PRIV.ACCT.RTM.ON | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ETSO.CANCEL | OPERATOR | | |
| [rosid.]ROSCMD.PRIV.ETSO.FREE | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.ETSO.QUERY.ALLOCATE | OPERATOR | | |
| [rosid.]ROSCMD.PRIV.ETSO.QUERY.CALL | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.ADD | READ | | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.ANY | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.C | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.D | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.LAST | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.NAME | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.NEW | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.SDUMP | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.SPACE | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.SPIE | READ | | |
| [rosid.]ROSCMD.PRIV.OPER.DEBUG.SUBTST | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.LIBCACH.ON | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.LIBCACH.PURGE | READ | | |
| [rosid.]ROSCMD.PRIV.OPER.MESSAGE | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.INTERVAL | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.INTERVAL | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.LERPRT | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.LERPRT | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.MESSAGES | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.MESSAGES | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.NETSTAT | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.NETSTAT | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.OFF | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.RESTART | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.RETRY | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.ROSLOG | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.SEND | UPDATE | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.SPOOL | UPDATE | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.STATUS | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.STATUSX | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.STATUSX | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.OPER.STOP | CONTROL | SYSPAUDT | |

| RESOURCE | ACCESS | USER GROUPS** | Note |
|---|---------|---------------|------|
| [rosid.]ROSCMD.PRIV.OPER.OPER.VTAM | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.PEEK | READ | * | |
| [rosid.]ROSCMD.PRIV.OPER.RCSTRACE | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.ABEND | CONTROL | SYSPAUDT | |
| | | * | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.DUMP | CONTROL | SYSPAUDT | |
| | | * | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.ENABLE | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.FLUSH | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.LOCK | CONTROL | SYSPAUDT | |
| | | * | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.REFRESH | CONTROL | SYSPAUDT | |
| | | * | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.RELOAD | CONTROL | SYSPAUDT | |
| | | * | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.SHUTDOWN | CONTROL | SYSPAUDT | |
| | | * | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.SIGNON | CONTROL | SYSPAUDT | |
| | | * | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.SUBMIT | CONTROL | ROSCAUDT | |
| [rosid.]ROSCMD.PRIV.OPER.ROZAP.VTRACE | CONTROL | ROSCAUDT | |
| [rosid.]ROSCMD.PRIV.ROSLIB | CONTROL | ROSCAUDT | |
| | | SECAAUDT | |
| | | SECDAUDT | |
| [rosid.]ROSCMD.PRIV.ROSUPS | CONTROL | ROSCAUDT | |
| | | SECAAUDT | |
| | | SECDAUDT | |
| [rosid.]ROSCMD.PRIV.RPS.PRINT.CANCEL | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.RPS.PRINT.HOLD | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.RPS.PRINT.MOD | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.RPS.PRINT.ROUTE | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.PRIV.RPS.PRINT.START | CONTROL | SYSPAUDT | |
| [rosid.]ROSCMD.RPF.pfx.mem | READ | * | |

* - All Users

** **Note:** Consult the current Broadcom Advantage CA-Roscoe Security Administration Guide for the latest information on Roscoe resources. The information found in that reference as well as the information in this Addendum specifies suggested security specifications. However, the Site Security Plan should be the authoritative resource for access. Please note wherever an access or user group is missing, the Site Security Plan determines access and/or user group.

ROSCAUTH - ROSCOE Master and Maintenance IDs

11.11 Vanguard Security Solutions Requirements

Table 11-34: Vanguard Security Solutions Resources

Referenced by: ZVSS0020

| Resource Names | Logging | User Group | Access |
|-----------------------------|---------|--|--------|
| IRR.PASSWORD.RESET | | * | None |
| VIP\$.NOEDIT.COMMANDS | | * | None |
| VRA\$. | | * | None |
| VRA\$.ACSTASK | Read | AUDTAUDT SECAAUDT | Read |
| VRA\$.DIGTCERT.EDIT.COMMAND | | AUDTAUDT SECAAUDT | Read |
| VRA\$.LIVE.USER | | AUDTAUDT SECAAUDT SYSPAUDT | Read |
| VRA\$.PASSWORD | Read | AUDTAUDT SECAAUDT SECDAUDT | Read |
| VRA\$.REFRESH. | | AUDTAUDT SECAAUDT SECDAUDT | Read |
| VRA\$.REFRESH.GENERIC | | AUDTAUDT SECAAUDT SECDAUDT | Read |
| VRA\$.REFRESH.GLOBAL | | AUDTAUDT SECAAUDT SECDAUDT | Read |
| VRA\$.REFRESH.RACLIST | | AUDTAUDT SECAAUDT SECDAUDT | Read |
| VRA\$.REFRESH.WHENPROGRAM | | AUDTAUDT SECAAUDT SECDAUDT | Read |
| VRA\$.SCOPE | | * | None |
| | | AUDTAUDT SECAAUDT SECDAUDT SYSPAUDT | Read |
| VRA\$.VRAACCA | Read | AUDTAUDT SECAAUDT SECDAUDT SYSPAUDT | Read |
| VRA\$.VRAADUPA | Read | AUDTAUDT SECAAUDT SECDAUDT | Read |
| VRA\$.VRABRPT | Read | AUDTAUDT SECAAUDT SECDAUDT SYSPAUDT | Read |

| Resource Names | Logging | User Group | Access |
|----------------------------|---------|--|--------|
| VRA\$.VRACMND | Read | AUDTAUDT SECAAUDT SECDAUDT | Read |
| VRA\$.VRADSNA | Read | AUDTAUDT SECAAUDT SECDAUDT SYSPAUDT | Read |
| VRA\$.VRAEXTR | Read | AUDTAUDT SECAAUDT SECDAUDT SYSPAUDT | Read |
| VRA\$.VRAGRPT | Read | AUDTAUDT SECAAUDT SECDAUDT SYSPAUDT | Read |
| VRA\$.VRAOCMD | | AUDTAUDT SECAAUDT SECDAUDT | Read |
| VRA\$.VRAORPT | Read | AUDTAUDT SECAAUDT SECDAUDT SYSPAUDT | Read |
| VRA\$.VRASRPT | Read | AUDTAUDT SECAAUDT SECDAUDT | Read |
| VRA\$.VRAVTOC | Read | AUDTAUDT SECAAUDT SECDAUDT SYSPAUDT | Read |
| VRA\$.VRTRAA | Read | AUDTAUDT SECAAUDT SECDAUDT SYSPAUDT | Read |
| VRAADM\$.VARIABLES | Read | SECAAUDT SECDAUDT | Read |
| VRAIDM\$. | Read | SECAAUDT | Update |
| VRAIDM\$.classname.profile | Read | SECAAUDT SECDAUDT | Update |
| VRAPW\$.*.** | Read | * | None |
| VRAPW\$.ALL | Read | SECAAUDT | Read |
| VRAPW\$.ALLOW.HREVOKE | Read | SECAAUDT SECDAUDT | Read |
| VRAPW\$.groupid | Read | SECAAUDT SECDAUDT | Read |

| Resource Names | Logging | User Group | Access |
|--|---------|----------------------------------|--------|
| VRAPW\$.NOHISTCHK | Read | * | None |
| VRAPW\$.NONE.AUDITOR | Read | SECDAUDT | Read |
| VRAPW\$.NONE.OPERATIONS | Read | SECDAUDT | Read |
| VRAPW\$.NONE.SPECIAL | Read | SECDAUDT | Read |
| VRAPW\$.NONE.target-userid | Read | * | None |
| VRAPW\$.NONE.target-userid-default-group | Read | * | None |
| VRAPW\$.userid | Read | SECAAUDT SECDAUDT | Read |
| VRAPWHR\$.groupid | Read | SECAAUDT SECDAUDT | Read |
| VRAPWHR\$.userid | Read | SECAAUDT SECDAUDT | Read |
| VRAUD\$.classname | Read | SECAAUDT | Update |
| VRAUD\$.classname.fieldname | Read | SECAAUDT | Update |
| VRAUD\$.classname.fieldname.1stnode | Read | SECAAUDT SECDAUDT | Update |
| VSA\$.VSA | Read | SECAAUDT SECDAUDT | Read |
| VSR\$.** | | * | None |
| VSR\$.VSR | Read | AUDTAUDT SECAAUDT SECDAUDT | Read |

* - All Users

Table 11-35: Vanguard Security Solutions Resources Description

| Resource Names | Description |
|-----------------------|--|
| IRR.PASSWORD.RESET | This profile allows users to use NOEXPIRE. To use NOEXPIRE, you must allow the user UPDATE access to the RACF FACILITY class profile. |
| VIP\$.NOEDIT.COMMANDS | Controls the Security Server Command component. If READ access or greater is allowed, the user will not be presented with an ISPF edit session and the generated commands will be executed immediately. It is recommended that this profile be defined with a UACC of NONE. |
| VRA\$.ACSTASK | Specifies user(s) who are permitted to execute Administrator Automated Command Scheduler, VRAAJACS. A user with READ access or greater has authority to execute the Automated Command Scheduler. It is recommended that this profile be defined with a UACC of NONE. This profile is required for the Automated Command Scheduler. |

| Resource Names | Description |
|-----------------------------|---|
| VRA\$.DIGTCERT.EDIT.COMMAND | Controls RACDCERT command editing. If READ access or greater is allowed, the user will be presented with an ISPF edit session to allow review or modification of the RACDCERT command. |
| VRA\$.LIVE.USER | Controls the use of Live RACF database access in Administrator. If READ access or greater is allowed, Administrator user may access the live RACF database where available. It is recommended that this profile be defined with a UACC of NONE. It must have the APPLDATA field populated with a string userid/groupid. Userid is a RACF defined user who has READ access to the RACF database. Groupid is a RACF defined group, that userid is connected to. This userid/groupid combination is used to gain access to the live RACF database. |
| VRA\$.PASSWORD | Identity Manager - The RACFCMDS member also includes the commands to define profiles and permit access to Identity Manager functions. For information about these profile definitions, refer to the <i>Vanguard Administrator Technical Reference Guide</i> . |
| VRA\$.REFRESH.* | This profile is the High Level Control of SETROPTS REFRESH Command Generation. |
| VRA\$.REFRESH.GENERIC | This profile pertains to in-storage generic profiles. By permitting a user or group access to this profile with at least READ access, you enable the automatic generation of SETROPTS REFRESH commands for in-storage generic profiles within the specified general resource class that has had a change within one of its profiles. |
| VRA\$.REFRESH.GLOBAL | This profile controls frequently accessed profiles for public resources. By permitting user or group access to this profile with at least READ access, you enable the automatic generation of SETROPTS REFRESH commands for this class of resources when a profile within this class had been changed. |
| VRA\$.REFRESH.RACLIST | This profile controls general resource class profiles. By permitting user or group access to this profile with at least READ access, you enable the automatic generation of SETROPTS REFRESH commands for the particular general resource class which has had any of its profiles changed. |
| VRA\$.REFRESH.WHENPROGRAM | This profile has to do with activating program control. By permitting a user or group access to this profile with at least READ access, you enable the automatic generation of SETROPTS REFRESH commands for activating program control that provides both access |

| Resource Names | Description |
|----------------------------|--|
| | control to load modules and program access to data sets. |
| VRA\$.SCOPE | When this profile is defined with a UACC of NONE, GROUP SPECIAL administrators are only allowed to see those profiles within their RACF scope of authority. To allow a user or group to override scoping support, PERMIT the user/group READ access to this profile. |
| VRA\$.VRAACCA | Batch Access Analyzer |
| VRA\$.VRAADUPA | Access List Anomaly Analysis |
| VRA\$.VRABRPT | Batch RACF Reports |
| VRA\$.VRACMND | Batch Commands |
| VRA\$.VRADSNA | Data Set Access Analysis |
| VRA\$.VRAEXTR | Extract Process |
| VRA\$.VRAGRPT | Batch Group Tree Analysis |
| VRA\$.VRAOCMD | Online Commands |
| VRA\$.VRAORPT | Online RACF Reports |
| VRA\$.VRASRPT | VRA Scope of Authority Analysis |
| VRA\$.VRAVTOC | VTOC Data Set Reports |
| VRA\$.VRTRAA | On-line Access and Authorization |
| VRAADM\$.VARIABLES | Initialization Variable Maintenance |
| VRAIDM\$.*.* | VRA Inst Data High Level |
| VRAIDM\$.classname.profile | Controls access to the installation data field in RACF profiles when using the Administrator Installation Data Management function. It is recommended that these profiles be defined with a UACC of NONE, specifically permitting users READ or UPDATE access. The classname can be any valid RACF general resource class name, GROUP, USER, or DATASET. The profile can be a specific profile name, or a generic, to limit the profiles that can be administered. For example, if you define the profile VRAIDM\$.USER.* with a UACC of NONE, and PERMIT user FREDV to the profile with access of UPDATE, FREDV would be allowed to view and alter the installation data fields of any RACF user profiles. Note: Asterisks (*) or percent signs (%) encountered in a Dataset or General Resource profile are replaced by a lowercase x. If an ampersand (&), which indicates the presence of a &RACFVARS symbolic is encountered, the return and reason codes will be set to produce the USER NOT AUTHORIZED message on the panel. Therefore, profiles that contain these symbolics will not have their Installation Data updated via this method. |

| Resource Names | Description |
|----------------------------|---|
| VRAPW\$.*.* | This profile prevents unauthorized access to Identity Manager. Define it with a UACC of NONE, and do not permit any users or groups. - - Important: If you define this profile with a UACC greater than NONE or permit access to this profile, unpredictable results are likely to occur as a result of access to profiles, such as those listed in Table 7. Profiles Disallowing Identity Management. |
| VRAPW\$.ALL | Allows access to ALL users. |
| VRAPW\$.ALLOW.HREVOKE | Any non-System SPECIAL user that requires Hard Revoke authority must have READ access to this profile. In addition, the user needs READ access to an appropriate VRAPWHR\$ profile. |
| VRAPW\$.groupid | This profile allows access by group name. <i>groupid</i> in the profile name should be the same as the default group name of the user ID specified in the command. An optional profile, VRAPWCON.CONGRP, can be defined in the RACF FACILITY class to change the meaning of the VRAPW\$. <i>groupid</i> profile. If the user has READ access to this optional profile, the group name specified in the VRAPW\$. <i>groupid</i> profile changes to mean any group a user is connected to, not just the user's default group. |
| VRAPW\$.NOHISTCHK | By permitting user or group access to this profile with at least READ access, passwords changed by that user or group are not compared to the current password or the password history. If you want this to be the default action for all users that administer passwords, create the profile with a UACC of READ. |
| VRAPW\$.NONE.AUDITOR | By permitting user or group access to this profile with at least READ access, you prevent the user or group from administering passwords for any user with the RACF System Auditor attribute, regardless of other granted authority. |
| VRAPW\$.NONE.OPERATIONS | By permitting user or group access to this profile with at least READ access, you prevent the user or group from administering passwords for any user with the RACF Operations attribute, regardless of other granted authority. |
| VRAPW\$.NONE.SPECIAL | By permitting user or group access to this profile with at least READ access, you prevent the user or group from administering passwords for any user with the RACF System SPECIAL attribute, regardless of other granted authority. |
| VRAPW\$.NONE.target-userid | By permitting user or group access to this profile with at least READ access, you prevent the user or group |

| Resource Names | Description |
|--|--|
| | from administering passwords for this target User ID, regardless of other granted authority. You can therefore, prevent a user with READ access to the VRAPW\$.ALL profile from administering the password of a specific user, while allowing them to administer all other user passwords. |
| VRAPW\$.NONE.target-userid-default-group | By permitting user or group access to this profile with at least READ access, you prevent the user or group from administering passwords for a target Userid that has this group as a default group, regardless of other authority granted. You can, therefore prevent a user with READ access to the VRAPW\$.ALL profile from administering the password for all users with a specific default group, while allowing them to administer all other users' passwords. |
| VRAPW\$.userid | This profile allows access by user ID. <i>userid</i> in the profile name should be the same as the user ID specified in the command. |
| VRAPWHR\$.groupid | <i>groupid</i> is the ID of the default group of the user specified in the command. An optional profile, VRAPWCON.CONGRP, can be defined in the RACF FACILITY class to change the meaning of the VRAPWHR\$. <i>groupid</i> profile. If the user has read access to this optional profile, the Group ID in the VRAPWHR\$. <i>groupid</i> profile changes to mean any group a user is connected to, not just their default group. |
| VRAPWHR\$.userid | <i>userid</i> is the user ID specified in the command. |
| VRAUD\$.classname | Controls access to the User Data fields in the base segment of RACF profiles, when using the Administrator User Data Management function. It is recommended that these profiles be defined with a UACC of NONE. You must then define specific access to permit users READ or UPDATE access. The classname can be any valid RACF general resource class name, GROUP, USER, or DATASET. These profiles allow initial access to the User Data of each class. |
| VRAUD\$.classname.fieldname | Standard Authority Checking: Controls access to a specific User Data field in a given class. e.g., if you define the profile VRAUD\$.USER.FIRSTNME with a UACC of NONE, and PERMIT user FREDV to the profile with access of UPDATE, FREDV would be allowed to view and alter the User Data field named FIRSTNME of any RACF user profile. Note: Standard Authority Checking is the default. |

| Resource Names | Description |
|-------------------------------------|---|
| VRAUD\$.classname.fieldname.1stnode | Enhanced Authority Checking; Controls access to a specific User Data field in a specific profile in a given class. E.g., if you define the profile VRAUD\$.DATASET.CHKKEY.PAYROLL with a UACC of NONE, and PERMIT user FREDV to the profile with access of UPDATE, FREDV would be allowed to view and alter the Dataset User Data field named CHKKEY in all of the Dataset profiles with a lsnod of PAYROLL. Note: In order to use the Enhanced Authority Checking, the UDM_ENHANCED_SECURITY keyword must be set to Y in the VRAOPT00 , member of the VIPOPTS DDNAME. |
| VSA\$.VSA | Grants access to Analyzer online and batch reports |
| VSR\$.VSR | Grants access to Advisor online and batch reports |

11.12 Compuware Abend-AID Requirements

Table 11-36: Compuware Abend-AID Resources

Referenced by: ZAID0020

| Function | Resource Names | User Group |
|--------------|---|--|
| LOGON.FD | prefix.SERVER.LOGON.FD.servername | APPDAUDT APPSAUDT OPERAUDT SYSPAUDT |
| LOGON.IC | prefix.SERVER.LOGON.IC.servername | SYSPAUDT |
| LOGON.TC | prefix.SERVER.LOGON.TC.servername | OPERAUDT SYSPAUDT |
| DDIRTx | prefix.DDIRTx.servername.applid_of_CICS_region.tranid_of_entry_in_directory | APPDAUDT APPSAUDT SYSPAUDT |
| DDIRBx. | prefix.DDIRBx.servername.jobname_of_address_space_in_report | APPDAUDT APPSAUDT SYSPAUDT |
| DDIRSx | prefix.DDIRSx.servername.jobname_of_address_space_in_dump | APPDAUDT APPSAUDT SYSPAUDT |
| IMPORT | prefix.SERVER.IMPORT.servername | APPDAUDT APPSAUDT SYSPAUDT |
| IPCS | prefix.SERVER.IPCSCMD.servername | APPDAUDT APPSAUDT SYSPAUDT |
| SHUTDOW N | prefix.SERVER.CONTROL.servername | OPERAUDT SYSPAUDT |

| Function | Resource Names | User Group |
|----------|----------------------------------|----------------------------------|
| LOGSPOOL | prefix.SERVER.CONTROL.servername | OPERAUDT SYSPAUDT |
| REXX | prefix.SERVER.REXXAPI.servername | APPDAUDT APPSAUDT SYSPAUDT |

prefix - The value specified for the EXTERNAL_SECURITY_PREFIX of the Abend-AID Viewer server configuration parameter.

servername - The name of the viewing server specified as a parameter on the execute statement of the Abend-AID Viewer server JCL.

11.13 BMC MAINVIEW Requirements

Table 11-37: BMC MAINVIEW Resources

Referenced by: ZMVZ0020

| Resource | User Group |
|----------------------------------|---|
| BBM.ssid.CN | AUTOAUDT DASDAUDT MQSAAUDT MV STCs MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM.COMMON.ASU.PA | NONE |
| BBM.systemid.MVALARM.targetid.TC | MV STCs |
| BBM.systemid.MVALERT.targetid.TC | MV STCs |
| BBM.systemid.MVAO.targetid.TC | MV STCs |
| BBM.systemid.MVCSMON.targetid.TA | AUTOAUDT DASDAUDT MQSAAUDT MVUPDT PCSPAUDT SYSPAUDT |
| BBM.systemid.MVCSMON.targetid.TC | MV STCs |
| BBM.systemid.MVMVS.targetid.TA | AUTOAUDT DASDAUDT MQSAAUDT MV STCs MVUPDT PCSPAUDT SYSPAUDT |
| BBM.systemid.MVMVS.targetid.TC | MV STCs |
| BBM.systemid.MVSPS.targetid.TA | AUTOAUDT |

| Resource | User Group |
|----------------------------------|---|
| | DASDAUDT MQSAAUDT MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM.systemid.MVSPS.targetid.TC | MV STCs |
| BBM.systemid.MVSRM.targetid.TC | MV STCs |
| BBM.systemid.MVUSS.targetid.TA | AUTOAUDT DASDAUDT MQSAAUDT MV STCs MVUPDT PCSPAUDT SYSPAUDT |
| BBM.systemid.MVUSS.targetid.TC | MV STCs |
| BBM.systemid.PLEXMGR.targetid.TA | AUTOAUDT DASDAUDT MQSAAUDT MV STCs MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM. MVCICS.targetid.AA | AUTOAUDT DASDAUDT MQSAAUDT CICDAUDT PCSPAUDT SYSPAUDT |
| BBM.MVCICS.targetid.QQ210.* | SYSPAUDT |
| BBM.MVCICS.targetid.SET*.* | SYSPAUDT |
| BBM.MVCSMON.targetid.AA | AUTOAUDT DASDAUDT MQSAAUDT MVUPDT PCSPAUDT SYSPAUDT |
| BBM.MVCSMON.targetid.COMMON.AA | SYSPAUDT |
| BBM.MVCSMON.targetid.CSMON.PA | AUTOAUDT DASDAUDT MQSAAUDT MVUPDT PCSPAUDT SYSPAUDT |
| BBM.MVCSMON.targetid.MYA20. | SYSPAUDT |

| Resource | User Group |
|-------------------------------|--|
| BBM.MVCSMON.targetid.MYA30.OD | SYSPAUDT |
| BBM.MVDB2.targetid.AA | SYSPAUDT AUTOAUDT DASDAUDT DABAAUDT MV STCs MVREAD PCSPAUDT |
| BBM. MVCICS.targetid.*.AO | SYSPAUDT |
| BBM.MVDB2.targetid.*.AO | SYSPAUDT |
| BBM. MVCICS.targetid.*.OD | AUTOAUDT DASDAUDT DABAAUDT MV STCs CICDSAUDT PCSPAUDT SYSPAUDT |
| BBM.MVDB2.targetid.*.OD | AUTOAUDT DASDAUDT DABAAUDT MV STCs MVREAD PCSPAUDT SYSPAUDT |
| BBM. MVCICS.targetid.*.*.OA | AUTOAUDT DASDAUDT DABAAUDT CICDSAUDT PCSPAUDT SYSPAUDT |
| BBM.MVDB2.targetid.*.*.OA | AUTOAUDT DASDAUDT DABAAUDT MVREAD PCSPAUDT SYSPAUDT |
| BBM.MVMVS.targetid.AA | AUTOAUDT DASDAUDT MQSAAUDT MVUPDT PCSPAUDT SYSPAUDT |
| BBM.MVMVS.targetid.COMMON.AA | SYSPAUDT |
| BBM.MVMVS.targetid.D*.OD | AUTOAUDT DASDAUDT MQSAAUDT MV STCs |

| Resource | User Group |
|-----------------------------------|--|
| | MVUPDT PCSPAUDT SYSPAUDT |
| BBM.MVMVS.targetid.DC101.CLCMD.OA | AUTOAUDT DASDAUDT MVUPDT PCSPAUDT SYSPAUDT |
| BBM.MVMVS.targetid.MVSCOPE.PA | SYSPAUDT |
| BBM.MVMVS.targetid.MYA20. | SYSPAUDT |
| BBM.MVMVS.targetid.MYA30.OD | SYSPAUDT |
| BBM.MVSPS.targetid.*.OD | AUTOAUDT DASDAUDT MQSAAUDT MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM.MVSPS.targetid.AA | AUTOAUDT DASDAUDT MQSAAUDT MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM.MVSPS.targetid.COMMON.AA | SYSPAUDT |
| BBM.MVSPS.targetid.MYA20. | SYSPAUDT |
| BBM.MVSPS.targetid.MYA30.OD | SYSPAUDT |
| BBM.MVSPS.targetid.SYSPROG.PA | MVREAD MVUPDT SYSPAUDT |
| BBM.MVUSS.targetid.*.OD | DASDAUDT MQSAAUDT MV STCs MVUPDT SYSPAUDT |
| BBM.MVUSS.targetid.AA | MVUPDT SYSPAUDT |
| BBM.MVUSS.targetid.COMMON.AA | SYSPAUDT |
| BBM.MVUSS.targetid.MYA20. | SYSPAUDT |
| BBM.MVUSS.targetid.MYA30.OD | SYSPAUDT |
| BBM.MVUSS.targetid.UCE48.OD | SYSPAUDT |
| BBM.MVUSS.targetid.UCEC0.OD | SYSPAUDT |
| BBM.MVUSS.targetid.UCEC2.OD | SYSPAUDT |
| BBM.MVUSS.targetid.UCEC3.OD | SYSPAUDT |
| BBM.MVUSS.targetid.UCEC4.OD | AUTOAUDT |

| Resource | User Group |
|--------------------------------------|--|
| | MQSAAUDT MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM.MVUSS.targetid.UCECC.OD | SYSPAUDT |
| BBM.MVUSS.targetid.UCECE.OD | SYSPAUDT |
| BBM.MVUSS.targetid.UCED0.OD | SYSPAUDT |
| BBM.MVUSS.targetid.UCED1.OD | SYSPAUDT |
| BBM.MVUSS.targetid.UCED6.OD | MV STCs SYSPAUDT |
| BBM.MVUSS.targetid.UEC3A.AO | SYSPAUDT |
| BBM.MVUSS.targetid.UEC3A.BPXLIMIT.OA | SYSPAUDT |
| BBM.MVUSS.targetid.UEC3A.OD | AUTOAUDT MQSAAUDT MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM.MVUSS.targetid.UUSSD.ACTIVATE.OA | SYSPAUDT |
| BBM.MVUSS.targetid.UUSSD.AO | SYSPAUDT |
| BBM.MVUSS.targetid.UUSSD.DEACT.OA | SYSPAUDT |
| BBM.MVUSS.targetid.UUSSD.OD | SYSPAUDT |
| BBM.PLEXMGR.targetid. | SYSPAUDT |
| BBM.PLEXMGR.targetid.AA | SYSPAUDT |
| BBM.PLEXMGR.targetid.CCE92.OD | AUTOAUDT DASDAUDT MQSAAUDT MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM.PLEXMGR.targetid.COMMON.AA | SYSPAUDT |
| BBM.PLEXMGR.targetid.CYA10. | SYSPAUDT |
| BBM.PLEXMGR.targetid.CYA10.OD | AUTOAUDT DASDAUDT MQSAAUDT MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM.PLEXMGR.targetid.CYA50. | SYSPAUDT |
| BBM.PLEXMGR.targetid.CYA50.OD | AUTOAUDT DASDAUDT MQSAAUDT MVREAD |

| Resource | User Group |
|-------------------------------|--|
| | MVUPDT PCSPAUDT SYSPAUDT |
| BBM.PLEXMGR.targetid.CYA60.OD | AUTOAUDT DASDAUDT MQSAAUDT MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM.PLEXMGR.targetid.CYA70.OD | SYSPAUDT |
| BBM.PLEXMGR.targetid.CYA80. | SYSPAUDT |
| BBM.PLEXMGR.targetid.CYA90. | SYSPAUDT |
| BBM.PLEXMGR.targetid.CYAA0.OD | SYSPAUDT |
| BBM.PLEXMGR.targetid.CYAB0. | SYSPAUDT |
| BBM.PLEXMGR.targetid.CYAC0.OD | AUTOAUDT DASDAUDT MQSAAUDT MVREAD MVUPDT PCSPAUDT SYSPAUDT |
| BBM.PLEXMGR.targetid.CYAD0.OD | SYSPAUDT |
| BBM.PLEXMGR.targetid.CYAE0.OD | SYSPAUDT |
| BBM.PLEXMGR.targetid.CZZ01.OD | SYSPAUDT |
| BBM.PLEXMGR.targetid.CZZ02.OD | SYSPAUDT |
| BBM.PLEXMGR.targetid.MYA20. | SYSPAUDT |
| BBM.PLEXMGR.targetid.MYA20.OD | AUTOAUDT DASDAUDT MQSAAUDT MVUPDT PCSPAUDT SYSPAUDT |
| BBM.PLEXMGR.targetid.MYA30.OD | AUTOAUDT DASDAUDT MQSAAUDT MVUPDT PCSPAUDT SYSPAUDT |
| BBM.PLEXMGR.targetid.MYA40. | SYSPAUDT |
| BBM.PLEXMGR.targetid.MYB30.OD | MV STCs SYSPAUDT |
| BBM.PLEXMGR.targetid.MYD00.OD | MV STCs SYSPAUDT |

ssid - The subsystem id specified in the Mainview CAS and PAS procedures.

systemid - The SYSNAME specified in the IEASYSxx member of the SYS1.PARMLIB concatenation.

targetid - The SYSNAME specified in the IEASYSxx member of the SYS1.PARMLIB concatenation.

MV STCs - Mainview STCs.

11.14 CA MIM Requirements

Table 11-38: CA MIM Resource Sharing Resources

Referenced by: ZMIM0020

| Command | Resource | User Group | Access |
|--------------|----------------------|----------------------|--------|
| ACTIVATE | safprefix.ACTIVATE | SYSPAUDT | UPDATE |
| ADDQNAME | safprefix.ADDQNAME | SYSPAUDT | UPDATE |
| ALLOCATE | safprefix.ALLOCATE | SYSPAUDT | UPDATE |
| ALTER | safprefix.ALTER | SYSPAUDT | UPDATE |
| AUTHCHK | safprefix.AUTHCHK | OPERAUDT SYSPAUDT | UPDATE |
| COLLECT | safprefix.COLLECT | SYSPAUDT | UPDATE |
| CP | safprefix.CP | SYSPAUDT | UPDATE |
| CTC | safprefix.CTC | DASDAUDT SYSPAUDT | UPDATE |
| DEALLOCATE | safprefix.DEALLOCATE | SYSPAUDT | UPDATE |
| DEFALIAS | safprefix.DEFALIAS | SYSPAUDT | UPDATE |
| DELQNAME | safprefix.DELQNAME | SYSPAUDT | UPDATE |
| DEQJOB | safprefix.DEQJOB | PCSPAUDT SYSPAUDT | UPDATE |
| DIAGNOSE | safprefix.DIAGNOSE | OPERAUDT SYSPAUDT | UPDATE |
| DISPLAY ECMF | safprefix.DISPLAY | * | READ |
| DISPLAY EDIF | safprefix.DISPLAY | * | READ |
| DISPLAY GCMF | safprefix.DISPLAY | * | READ |
| DISPLAY GDIF | safprefix.DISPLAY | * | READ |
| DISPLAY GTAF | safprefix.DISPLAY | * | READ |
| DISPLAY ICMF | safprefix.DISPLAY | * | READ |
| DISPLAY MIM | safprefix.DISPLAY | * | READ |
| DISPLAY TPCF | safprefix.DISPLAY | * | READ |
| DOM | safprefix.DOM | OPERAUDT SYSPAUDT | UPDATE |
| DROPSYS | safprefix.DROPSYS | SYSPAUDT | UPDATE |
| DUMP GCMF | safprefix.DUMP | * | NONE |
| DUMP GDIF | safprefix.DUMP | * | NONE |
| DUMP GTAF | safprefix.DUMP | * | NONE |

| Command | Resource | User Group | Access |
|----------------|-----------------------|----------------------------------|--------|
| DUMP ICMF | safprefix.DUMP | * | NONE |
| DUMP MIM | safprefix.DUMP | * | NONE |
| DUMP TPCF | safprefix.DUMP | * | NONE |
| EDITEST | safprefix.EDITEST | OPERAUDT SYSPAUDT | UPDATE |
| EXEMPT | safprefix.EXEMPT | OPERAUDT SYSPAUDT | UPDATE |
| FREE | safprefix.FREE | AUTOAUDT SYSPAUDT | UPDATE |
| FREECONS | safprefix.FREECONS | OPERAUDT SYSPAUDT | UPDATE |
| GLOBALVALUE | safprefix.GLOBALVALUE | SYSPAUDT | UPDATE |
| ICMF | safprefix.ICMF | SYSPAUDT | UPDATE |
| IDEFSYS | safprefix.IDEFSYS | SYSPAUDT | UPDATE |
| LINK | safprefix.LINK | SYSPAUDT | UPDATE |
| MIGRATE | safprefix.MIGRATE | SYSPAUDT | UPDATE |
| MSGTABLE | safprefix.MSGTABLE | SYSPAUDT | UPDATE |
| QUIESCE | safprefix.QUIESCE | OPERAUDT SYSPAUDT | UPDATE |
| REMOVE | safprefix.REMOVE | SYSPAUDT | UPDATE |
| RESTART | safprefix.RESTART | OPERAUDT SYSPAUDT | UPDATE |
| RESYNCH | safprefix.RESYNCH | DASDAUDT SYSPAUDT | UPDATE |
| SETOPTION ECMF | safprefix.SETOPTION | SYSPAUDT | UPDATE |
| SETOPTION EDIF | safprefix.SETOPTION | SYSPAUDT | UPDATE |
| SETOPTION GCMF | safprefix.SETOPTION | SYSPAUDT | UPDATE |
| SETOPTION GDIF | safprefix.SETOPTION | SYSPAUDT | UPDATE |
| SETOPTION ICMF | safprefix.SETOPTION | SYSPAUDT | UPDATE |
| SETOPTION MIM | safprefix.SETOPTION | SYSPAUDT | UPDATE |
| SETOPTION TPCF | safprefix.SETOPTION | SYSPAUDT | UPDATE |
| SHUTDOWN | safprefix.SHUTDOWN | AUTOAUDT OPERAUDT SYSPAUDT | UPDATE |
| SYSDUMP | safprefix.SYSDUMP | SYSPAUDT | UPDATE |
| USERDATA | safprefix.USERDATA | SYSPAUDT | UPDATE |
| VARY | safprefix.VARY | DASDAUDT SYSPAUDT | UPDATE |
| VCF | safprefix.VCF | SYSPAUDT | UPDATE |

* - All Users

safprefix - Obtained from the value set in the MIMINIT SAFPREFIX option, the default value is MIMGR.

Note: The **safeprefix.DUMP** resources will only be given to SYSPAUDT with access of UPDATE only when CA Technical Support directs that the **DUMP** command be issued. Upon completion of the command execution request, the access to this resource will be removed.

11.15 NetView Requirements

Table 11-39: NetView Resources

Referenced by: ZNET0020

| Resource | Group | Access |
|--------------------------------|----------------------|--------|
| netid | * | NONE |
| netid.luname.ADDCMD | SYSPAUDT | READ |
| netid.luname.AFTER | AUTOAUDT SYSPAUDT | READ |
| netid.luname.ALLOCATE.CATALOG | AUTOAUDT SYSPAUDT | READ |
| netid.luname.ALLOCATE.DELETE | SYSPAUDT | READ |
| netid.luname.ALLOCATE.NEW | AUTOAUDT SYSPAUDT | READ |
| netid.luname.ALLOCATE.UNCATALO | SYSPAUDT | READ |
| netid.luname.AT | AUTOAUDT SYSPAUDT | READ |
| netid.luname.ATTACH | * | READ |
| netid.luname.ATTACH.DUMP | * | READ |
| netid.luname.AUTOTASK | AUTOAUDT SYSPAUDT | READ |
| netid.luname.AUTOTBL | AUTOAUDT SYSPAUDT | READ |
| netid.luname.AUTOTBL.STATUS | * | READ |
| netid.luname.AUTOTEST | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CHNGFP | SYSPAUDT | READ |
| netid.luname.CHRON | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CLOSE | SYSPAUDT | READ |
| netid.luname.CLRSTATS | SYSPAUDT | READ |
| netid.luname.CNME0001 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME0002 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME0006 | SYSPAUDT | READ |
| netid.luname.CNME0013 | SYSPAUDT | READ |
| netid.luname.CNME0015 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME0017 | AUTOAUDT SYSPAUDT | READ |

| Resource | Group | Access |
|--------------------------------|----------------------|--------|
| netid.luname.CNME0018 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME0019 | SYSPAUDT | READ |
| netid.luname.CNME0025 | SYSPAUDT | READ |
| netid.luname.CNME0030 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME0032 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME1016 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME1055 | SYSPAUDT | READ |
| netid.luname.CNME1057 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME1089 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME1098 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME2002 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME2007 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME2008 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME3006 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME7009 | SYSPAUDT | READ |
| netid.luname.CNME7201 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME7204.LISTCONN | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME7204.LISTOPID | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME7204.START | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME7204.STOP | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8004 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8200 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8205 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8206 | AUTOAUDT SYSPAUDT | READ |

| Resource | Group | Access |
|--------------------------------|----------------------|--------|
| netid.luname.CNME8206.LISTINFO | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8206.LSTSRVRS | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8206.START | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8206.STOP | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8221 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8225 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8250.START | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8250.STOP | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME8260 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNME9001 | SYSPAUDT | READ |
| netid.luname.CNME9002 | SYSPAUDT | READ |
| netid.luname.CNMEAUTB | SYSPAUDT | READ |
| netid.luname.CNMEMCXX | SYSPAUDT | READ |
| netid.luname.CNMEMCXY | SYSPAUDT | READ |
| netid.luname.CNMESNMP | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNMEXCON | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNMEXPRC | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNMSBWLK | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNMSGET | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNMSGETB | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNMSGETN | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNMSSET | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNMSTRAP | AUTOAUDT SYSPAUDT | READ |
| netid.luname.CNMSWALK | AUTOAUDT SYSPAUDT | READ |
| netid.luname.DEFAULTS | AUTOAUDT SYSPAUDT | READ |

| Resource | Group | Access |
|---|----------------------|--------|
| netid.luname.DELCMD | SYSPAUDT | READ |
| netid.luname.DSIMCAP | SYSPAUDT | READ |
| netid.luname.DSIPIINS.COMMON | SYSPAUDT | READ |
| netid.luname.DSIPTSO.TSOSERV | AUTOAUDT SYSPAUDT | READ |
| netid.luname.DSIPTSO.TSOSERV.CNMPROC/CNMSJTSO | * | READ |
| netid.luname.DSIPTSO.VERB | AUTOAUDT SYSPAUDT | READ |
| netid.luname.DSIPTSO.VERB.HOMETEST | * | READ |
| netid.luname.DSIPTSO.VERB.NETSTAT | * | READ |
| netid.luname.DSIPTSO.VERB.NSLOOKUP | * | READ |
| netid.luname.DSIPIXCF | AUTOAUDT SYSPAUDT | READ |
| netid.luname.DSIPIXTB | AUTOAUDT SYSPAUDT | READ |
| netid.luname.DSISAUTH | AUTOAUDT SYSPAUDT | READ |
| netid.luname.DSISRVR | AUTOAUDT SYSPAUDT | READ |
| netid.luname.DSIUSNDM | AUTOAUDT SYSPAUDT | READ |
| netid.luname.DSIZKNYJ | SYSPAUDT | READ |
| netid.luname.EKGVREXX | AUTOAUDT SYSPAUDT | READ |
| netid.luname.EVERY | AUTOAUDT SYSPAUDT | READ |
| netid.luname.EXCMD | AUTOAUDT SYSPAUDT | READ |
| netid.luname.EZLE600A | AUTOAUDT SYSPAUDT | READ |
| netid.luname.EZLE840A | SYSPAUDT | READ |
| netid.luname.EZLEAMAN | AUTOAUDT SYSPAUDT | READ |
| netid.luname.EZLEF002 | AUTOAUDT SYSPAUDT | READ |
| netid.luname.EZLEPOLY | AUTOAUDT SYSPAUDT | READ |
| netid.luname.FOCALPT | SYSPAUDT | READ |
| netid.luname.FREE.DELETE | SYSPAUDT | READ |
| netid.luname.FREE.UNCATALO | SYSPAUDT | READ |
| netid.luname.IDCAMS | AUTOAUDT SYSPAUDT | READ |
| netid.luname.MODIFY | AUTOAUDT SYSPAUDT | READ |
| netid.luname.MONIT | SYSPAUDT | READ |

| Resource | Group | Access |
|--------------------------------|----------------------|--------|
| netid.luname.MVS | SYSPAUDT | READ |
| netid.luname.MVS.\$D | * | READ |
| netid.luname.MVS.D | * | READ |
| netid.luname.MVS.D.MPF | SYSPAUDT | READ |
| netid.luname.MVS.D.NET | SYSPAUDT | READ |
| netid.luname.MVS.D.VTAM | SYSPAUDT | READ |
| netid.luname.MVS.DISPLAY | * | READ |
| netid.luname.MVS.DISPLAY.MPF | SYSPAUDT | READ |
| netid.luname.MVS.DISPLAY.NET | SYSPAUDT | READ |
| netid.luname.MVS.DISPLAY.VTAM | SYSPAUDT | READ |
| netid.luname.NLDM.DISABLE | AUTOAUDT SYSPAUDT | READ |
| netid.luname.NLDM.PURGE | AUTOAUDT SYSPAUDT | READ |
| netid.luname.NLDM.TRACE | AUTOAUDT SYSPAUDT | READ |
| netid.luname.NPDA.PURGE | AUTOAUDT SYSPAUDT | READ |
| netid.luname.OVERRIDE.DSIARPT | SYSPAUDT | READ |
| netid.luname.OVERRIDE.DSIASRC | SYSPAUDT | READ |
| netid.luname.OVERRIDE.DSICLD | SYSPAUDT | READ |
| netid.luname.OVERRIDE.DSILIST | SYSPAUDT | READ |
| netid.luname.OVERRIDE.DSIMSG | SYSPAUDT | READ |
| netid.luname.OVERRIDE.DSIOPEN | SYSPAUDT | READ |
| netid.luname.OVERRIDE.DSIPARM | SYSPAUDT | READ |
| netid.luname.OVERRIDE.DSIPRF | SYSPAUDT | READ |
| netid.luname.OVERRIDE.DSIVTAM | SYSPAUDT | READ |
| netid.luname.OVERRIDE.SLOGCMDR | AUTOAUDT SYSPAUDT | READ |
| netid.luname.PLEXCTL | AUTOAUDT SYSPAUDT | READ |
| netid.luname.PURGE.TIMER | AUTOAUDT SYSPAUDT | READ |
| netid.luname.REACC | SYSPAUDT | READ |
| netid.luname.READSEC | AUTOAUDT SYSPAUDT | READ |
| netid.luname.REFRESH | SYSPAUDT | READ |
| netid.luname.REFRESH.AUTHCHK | SYSPAUDT | READ |
| netid.luname.REFRESH.CMDAUTH | SYSPAUDT | READ |
| netid.luname.REFRESH.OPERs | SYSPAUDT | READ |
| netid.luname.REFRESH.OPERSEC | SYSPAUDT | READ |
| netid.luname.REFRESH.RMTSEC | SYSPAUDT | READ |
| netid.luname.RELCONID | SYSPAUDT | READ |
| netid.luname.RESETDB | AUTOAUDT SYSPAUDT | READ |

| Resource | Group | Access |
|----------------------------------|----------------------|--------|
| netid.luname.RESTORE | AUTOAUDT SYSPAUDT | READ |
| netid.luname.RESTYLE | AUTOAUDT SYSPAUDT | READ |
| netid.luname.REVISE | SYSPAUDT | READ |
| netid.luname.REVMSG | SYSPAUDT | READ |
| netid.luname.REVISRPT | SYSPAUDT | READ |
| netid.luname.RID | SYSPAUDT | READ |
| netid.luname.SETBQL | AUTOAUDT SYSPAUDT | READ |
| netid.luname.START.MOD | AUTOAUDT SYSPAUDT | READ |
| netid.luname.START.TASK | AUTOAUDT SYSPAUDT | READ |
| netid.luname.START.TASK.CNMTAMEL | * | READ |
| netid.luname.START.TSOSERV | AUTOAUDT SYSPAUDT | READ |
| netid.luname.START.UNIXSERV | SYSPAUDT | READ |
| netid.luname.START.XCFGROUP | SYSPAUDT | READ |
| netid.luname.SUBMIT | AUTOAUDT SYSPAUDT | READ |
| netid.luname.SUBMIT.BATCHTSO | * | READ |
| netid.luname.SUBMIT.SMTPJCL | * | READ |
| netid.luname.SWITCH | AUTOAUDT SYSPAUDT | READ |
| netid.luname.TE | SYSPAUDT | READ |
| netid.luname.TRACE | AUTOAUDT SYSPAUDT | READ |
| netid.luname.TS | SYSPAUDT | READ |
| netid.luname.VARY | AUTOAUDT SYSPAUDT | READ |
| netid.luname.WRITESEC | AUTOAUDT SYSPAUDT | READ |

SYSPAUDT - System programming personnel

AUTOAUDT - Automated operations users

* - All users authorized to access Netview

netid Obtained from the value specified for the NetID variable in the CxxSTYLE member.

luname Obtained from the value specified for the DOMAIN variable specified in the CNMPROC JCL. If the DOMAIN variable is null the DOMAIN statement in the CxxSTYLE member can be used.

Note: The values specified for NetID and DOMAIN are also returned by the netid() and domain() REXX™ functions.

Note: Additional resources are defined in the current release of the IBM Tivoli NetView for z/OS Security Reference.

11.16 RACF Password Exit Settings

Table 11-40: Parameters for RACF IRRPWREX

Referenced by RACF0462

| REXX Parameter | Setting |
|-------------------------------|--|
| STIG_Compliant | 'yes' |
| Pwd_minlen | 8 |
| numbers | '0123456789' |
| Lower_letters | 'abcdefghijklmnopqrstuvwxyz' |
| Upper_letters | 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' |
| special | '\$@#. < + & ! * - % _ > ? : ' |
| Pwd_allowed_chars | numbers Upper_letters special |
| Pwd_req_types | 4 |
| Pwd_name_allowed | 'no' |
| Pwd_name_minlen | 8 |
| Pwd_name_chars | 4 |
| Pwd_min_unique | 3 |
| Pwd_min_unique_upper | 'yes' |
| Pwd_max_unchanged | 3 |
| Pwd_max_unchanged_upper | 'yes' |
| Pwd_max_unchanged_consecutive | 'yes' |
| Pwd_all_unique | 'no' |
| Pwd_no_consecutive | 'no' |
| Pwd_no_consecutive_upper | 'yes' |
| Pwd_min_new | 4 |
| Pwd_userID_allowed | 'no' |
| Pwd_userID_chars | 4 |
| Pwd_repeat_chars | 0 |
| Pwd_repeat_upper | 'yes' |
| Pwd_dict.0 | 8 /* Change this as words are added and deleted */ |
| Pwd_dict.1 | 'IBM' |
| Pwd_dict.2 | 'RACF' |
| Pwd_dict.3 | 'PASSWORD' |
| Pwd_dict.4 | 'PHRASE' |
| Pwd_dict.5 | 'SECRET' |
| Pwd_dict.6 | 'IBMUSER' |

| REXX Parameter | Setting |
|----------------|---|
| Pwd_dict.7 | 'SYS1' |
| Pwd_dict.8 | '12345678' |
| Pwd_dict.9 | '99999999' |
| Pwd_prefix.0 | 33 /* Change this as values are added and deleted |
| Pwd_prefix.1 | 'APPL' |
| Pwd_prefix.2 | 'APR' |
| Pwd_prefix.3 | 'AUG' |
| Pwd_prefix.4 | 'ASDF' |
| Pwd_prefix.5 | 'BASIC' |
| Pwd_prefix.6 | 'CADAM' |
| Pwd_prefix.7 | 'DEC' |
| Pwd_prefix.8 | 'DEMO' |
| Pwd_prefix.9 | 'FEB' |
| Pwd_prefix.10 | 'FOCUS' |
| Pwd_prefix.11 | 'GAME' |
| Pwd_prefix.12 | 'IBM' |
| Pwd_prefix.13 | 'JAN' |
| Pwd_prefix.14 | 'JUL' |
| Pwd_prefix.15 | 'JUN' |
| Pwd_prefix.16 | 'LOG' |
| Pwd_prefix.17 | 'MAR' |
| Pwd_prefix.18 | 'MAY' |
| Pwd_prefix.19 | 'NET' |
| Pwd_prefix.20 | 'NEW' |
| Pwd_prefix.21 | 'NOV' |
| Pwd_prefix.22 | 'OCT' |
| Pwd_prefix.23 | 'PASS' |
| Pwd_prefix.24 | 'ROS' |
| Pwd_prefix.25 | 'SEP' |
| Pwd_prefix.26 | 'SIGN' |
| Pwd_prefix.27 | 'SYS' |
| Pwd_prefix.28 | 'TEST' |
| Pwd_prefix.29 | 'TSO' |
| Pwd_prefix.30 | 'VALID' |
| Pwd_prefix.31 | 'VTAM' |
| Pwd_prefix.32 | 'XXX' |
| Pwd_prefix.33 | '1234' |