z/OS
Version 2 Release 4

Introduction and Release Guide

IBM
Note
Before using this information and the product it supports, read the information in “Notices” on page 91.

This edition applies to Version 2 Release 4 of z/OS (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2019-07-10

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
### Contents

**How to send your comments to IBM**
ix

If you have a technical problem...........................................................ix

**z/OS information**
xi

**Summary of changes**

- Summary of changes for z/OS V2R3 Introduction and Release Guide....................................................xv

**Chapter 1. z/OS elements and features**

- z/OS base elements.................................................................1
- z/OS optional features............................................................2

**Chapter 2. z/OS base elements descriptions**

- Alternate Library for REXX..................................................3
- BCP (Base Control Program)... ...........................................3
- BDT (Bulk Data Transfer)... ................................................4
- Common Information Model (CIM)... ...................................4
- Communications Server.....................................................4
- Cryptographic Services........................................................5
- DFSMSdp..............................................................................6
- Environmental Record Editing and Printing Program (EREP)...7
- ESCON Director Support....................................................7
- FFST/MVS (First Failure Support Technology/MVS)... ........7
- GDDM (includes PCLK and OS/2 LINK)... ..........................7
- HCD (Hardware Configuration Definition)... ..............7
- HLASM (High Level Assembler)... ........................................7
- IBM HTTP Server - Powered by Apache..............................8
- IBM Tivoli Directory Server for z/OS (IBM TDS for z/OS)... 8
- ICKDSF (Device Support Facility)... ....................................8
- Integrated Security Services................................................8
- ISPF..........................................................9
- JES2............................................................9
- Language Environment......................................................10
- MICR/OCR..........................................................11
- Metal C Runtime Library....................................................11
- Network File System (NFS)... ............................................11
- Run-Time Library Extensions............................................12
- SMP/E..........................................................12
- Time Sharing Option/Extensions (TSO/E)... .......................12
- Terminal Input Output Controller (TIOC)... .......................12
- z/OS File System (zFS)... ..............................................12
- z/OS Font Collection.........................................................12
- z/OS Management Facility (z/OSMF)... ............................12
- z/OS OpenSSH............................................................13
- z/OS UNIX System Services (X/Open UNIX 95 functions)... 14
- z/OS Xvfb..............................................................14
- 3270 PC File Transfer Program........................................14

**Chapter 3. z/OS optional features descriptions**

- .................................15
Bulk Data Transfer (BDT) File-to-File................................................................. 15
Bulk Data Transfer (BDT) SNA NJE........................................................................... 15
Communications Server Security Level 3............................................................... 15
DFSM Features (DFSMsdss, DFSMShsm, DFSMSrmm, and DFSMStvs)................ 15
DFSORT.................................................................................................................... 16
GDDM-PGF,.............................................................................................................. 16
GDDM-REXX.......................................................................................................... 16
Hardware Configuration Manager (HCM).............................................................. 16
High Level Assembler Toolkit................................................................................ 17
IBM Knowledge Center for z/OS........................................................................... 17
Infoprint Server...................................................................................................... 18
JES3......................................................................................................................... 18
RMF (Resource Measurement Facility)................................................................ 19
Restricted use common service area (RUCSA)................................................... 19
SDSF (System Display and Search Facility).......................................................... 19
Security Server...................................................................................................... 19
XL C/C++.............................................................................................................. 19
z/OS Security Level 3............................................................................................ 20

Chapter 4. What is new in z/OS (V2R3 - V2R4)................................................... 21
Elements and features with no enhancements in V2R4......................................... 21
z/OS system-level new functions to consider....................................................... 21
BCP (MVS) new functions to consider................................................................. 22
    BCPii considerations......................................................................................... 22
    CEA considerations......................................................................................... 23
    Consoles considerations................................................................................ 24
    IBM Function Registry for z/OS considerations............................................ 24
    IOS considerations........................................................................................ 25
    Real Storage Manager (RSM) considerations............................................. 25
    System logger considerations....................................................................... 27
    Unicode considerations................................................................................ 28
    XES/XCF considerations.............................................................................. 28
Communications Server new functions to consider............................................ 29
    Support considerations................................................................................ 29
    Hardware support......................................................................................... 29
    Usability and skills...................................................................................... 30
    Scalability and performance....................................................................... 31
    Systems management.................................................................................. 33
    Enhancing security...................................................................................... 33
    Application development............................................................................ 37
Cryptographic Services new functions to consider............................................. 38
    ICSF............................................................................................................. 38
    PKI Services............................................................................................... 45
    System SSL................................................................................................. 47
DFSMs new functions to consider....................................................................... 48
    DFSMS device support new functions....................................................... 48
    Advanced Copy Services new functions.................................................... 48
    DADSM/CVAF new functions.................................................................... 49
    DFSMS catalog new functions.................................................................... 49
    DFSMSdss new functions............................................................................ 49
    DFSMShsm new functions.......................................................................... 50
    DFSMSrmm new functions........................................................................ 50
    DFSMSStvs new functions......................................................................... 51
    DFSM Object Access Method (OAM) new functions to consider............... 51
    SMS new functions..................................................................................... 51
    DFSMS VSAM new functions..................................................................... 52
    DFSMS data set encryption new functions................................................ 52

iv
<table>
<thead>
<tr>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Configuration Definition (HCD) new functions to consider</td>
<td>53</td>
</tr>
<tr>
<td>HCD hardware support</td>
<td>53</td>
</tr>
<tr>
<td>HCD processor support</td>
<td>53</td>
</tr>
<tr>
<td>Hardware Configuration Manager (HCM) new functions to consider</td>
<td>54</td>
</tr>
<tr>
<td>HCM processor support</td>
<td>54</td>
</tr>
<tr>
<td>HCM PCIe function enhancements</td>
<td>54</td>
</tr>
<tr>
<td>HCM CHPID type enhancements</td>
<td>54</td>
</tr>
<tr>
<td>IBM Tivoli Directory Server for z/OS new functions to consider</td>
<td>54</td>
</tr>
<tr>
<td>Enhanced SDBM search</td>
<td>54</td>
</tr>
<tr>
<td>Enhanced activity logging</td>
<td>55</td>
</tr>
<tr>
<td>Transport Layer Security (TLS) protocol version 1.3</td>
<td>55</td>
</tr>
<tr>
<td>MFA Support</td>
<td>55</td>
</tr>
<tr>
<td>Health Checks</td>
<td>55</td>
</tr>
<tr>
<td>FIPS Compliant</td>
<td>56</td>
</tr>
<tr>
<td>Multi-Row Fetch</td>
<td>56</td>
</tr>
<tr>
<td>Support DB2 partitioning by Growth for ITDS TDBM and GDBM database</td>
<td>56</td>
</tr>
<tr>
<td>Prevent visibility of sensitive data in debug trace</td>
<td>56</td>
</tr>
<tr>
<td>Infoprint Server new functions to consider</td>
<td>56</td>
</tr>
<tr>
<td>Accessible and signed PDFs</td>
<td>57</td>
</tr>
<tr>
<td>Enhanced PDF encryption with AES options</td>
<td>57</td>
</tr>
<tr>
<td>Dynamic configuration at all times</td>
<td>57</td>
</tr>
<tr>
<td>Dynamic tracing</td>
<td>57</td>
</tr>
<tr>
<td>IP PrintWay backup printer capability</td>
<td>58</td>
</tr>
<tr>
<td>Infoprint Central enhancements</td>
<td>58</td>
</tr>
<tr>
<td>Security enhancements</td>
<td>59</td>
</tr>
<tr>
<td>Sendmail to CSSMTP bridge</td>
<td>59</td>
</tr>
<tr>
<td>TSO/E 8-character user IDs</td>
<td>60</td>
</tr>
<tr>
<td>Integrated Security Services new functions to consider</td>
<td>60</td>
</tr>
<tr>
<td>Flexible Authentication Secure Tunneling (FAST)</td>
<td>60</td>
</tr>
<tr>
<td>Crypto Algorithm Currency</td>
<td>60</td>
</tr>
<tr>
<td>Federal Information Processing Standard (FIPS)</td>
<td>61</td>
</tr>
<tr>
<td>ISPF new functions to consider</td>
<td>61</td>
</tr>
<tr>
<td>JES2 new functions to consider</td>
<td>62</td>
</tr>
<tr>
<td>JES2 policies</td>
<td>62</td>
</tr>
<tr>
<td>JES2 disk reader support</td>
<td>62</td>
</tr>
<tr>
<td>Health Check for JES2 Checkpoint Configuration</td>
<td>63</td>
</tr>
<tr>
<td>Instruction Execution Protection (IEP)</td>
<td>63</td>
</tr>
<tr>
<td>Reporting JES2 resiliency data</td>
<td>63</td>
</tr>
<tr>
<td>JES2 email support</td>
<td>64</td>
</tr>
<tr>
<td>JCL Simplification</td>
<td>64</td>
</tr>
<tr>
<td>Dynamic groups added</td>
<td>64</td>
</tr>
<tr>
<td>Managing JES2 resources</td>
<td>64</td>
</tr>
<tr>
<td>JES3 JCL support</td>
<td>64</td>
</tr>
<tr>
<td>JES3 new functions to consider</td>
<td>65</td>
</tr>
<tr>
<td>JES3 support for 8-character TSO/E user IDs</td>
<td>65</td>
</tr>
<tr>
<td>Language Environment new functions to consider</td>
<td>65</td>
</tr>
<tr>
<td>Support for tracking specific price metrics</td>
<td>65</td>
</tr>
<tr>
<td>Japanese New Era support</td>
<td>65</td>
</tr>
<tr>
<td>Enabling non-executable memory</td>
<td>65</td>
</tr>
<tr>
<td>Year 2038/2040 support</td>
<td>66</td>
</tr>
<tr>
<td>Detecting buffer overflows</td>
<td>66</td>
</tr>
<tr>
<td>64-bit support for Enterprise PL/I</td>
<td>66</td>
</tr>
<tr>
<td>Metal C Runtime Library new functions to consider</td>
<td>66</td>
</tr>
<tr>
<td>Prefix data block</td>
<td>66</td>
</tr>
<tr>
<td>Debug data block</td>
<td>67</td>
</tr>
<tr>
<td>Metal C function descriptors</td>
<td>67</td>
</tr>
<tr>
<td>NFS new functions to consider</td>
<td>67</td>
</tr>
<tr>
<td>chkloop site attribute</td>
<td>67</td>
</tr>
<tr>
<td>Feature</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>looptreshold site attribute</td>
<td>67</td>
</tr>
<tr>
<td>enhmaplower attribute</td>
<td>68</td>
</tr>
<tr>
<td>exportck operand</td>
<td>68</td>
</tr>
<tr>
<td>Resource Measurement Facility (RMF) new functions to consider</td>
<td>68</td>
</tr>
<tr>
<td>New features, functions, and support for z/OS V2R3</td>
<td>68</td>
</tr>
<tr>
<td>Security Server (RACF) new functions to consider</td>
<td>71</td>
</tr>
<tr>
<td>RACF Custom Fields</td>
<td>71</td>
</tr>
<tr>
<td>RACF IBM Multi-factor Authentication (IBM MFA) Enhancements</td>
<td>71</td>
</tr>
<tr>
<td>RACF Pervasive encryption support</td>
<td>72</td>
</tr>
<tr>
<td>RACF Privilege Escalation Detection</td>
<td>72</td>
</tr>
<tr>
<td>RACF Improved PassTicket Security</td>
<td>72</td>
</tr>
<tr>
<td>RACF RACDCERT TLS1.3 RSAPSS support</td>
<td>73</td>
</tr>
<tr>
<td>RACF Parmlib support</td>
<td>73</td>
</tr>
<tr>
<td>RACF ODM classes support</td>
<td>74</td>
</tr>
<tr>
<td>RACF CICS Auditing support</td>
<td>74</td>
</tr>
<tr>
<td>SMP/E new functions to consider</td>
<td>74</td>
</tr>
<tr>
<td>GIMUNZIP enhancements</td>
<td>74</td>
</tr>
<tr>
<td>TSO/E new functions to consider</td>
<td>75</td>
</tr>
<tr>
<td>LOGON timeout</td>
<td>75</td>
</tr>
<tr>
<td>Allow special characters within passwords</td>
<td>75</td>
</tr>
<tr>
<td>Server-Requester Programming Interface (SRPI) and TSO/E Enhanced Connectivity Facility removal</td>
<td>75</td>
</tr>
<tr>
<td>8 character user ID</td>
<td>75</td>
</tr>
<tr>
<td>TSO/E Support for JES2 Resiliency</td>
<td>76</td>
</tr>
<tr>
<td>XL C/C++ new functions to consider</td>
<td>76</td>
</tr>
<tr>
<td>New and changed compiler options</td>
<td>76</td>
</tr>
<tr>
<td>Enhanced vector programming support</td>
<td>76</td>
</tr>
<tr>
<td>New LEGACY option for the DSECT Utility</td>
<td>77</td>
</tr>
<tr>
<td>New SOS info utility</td>
<td>77</td>
</tr>
<tr>
<td>Updates to CDAHLASM and as utilities</td>
<td>78</td>
</tr>
<tr>
<td>z/OS File System (zFS) new functions to consider</td>
<td>78</td>
</tr>
<tr>
<td>Improved reliability and availability for zFS file systems</td>
<td>78</td>
</tr>
<tr>
<td>zFS File Snapshot</td>
<td>78</td>
</tr>
<tr>
<td>Removal of Distributed File Service/Server Message Block (DFS/SMB)</td>
<td>78</td>
</tr>
<tr>
<td>Identifying SMB-exported file systems</td>
<td>79</td>
</tr>
<tr>
<td>Repairing mounted zFS file systems</td>
<td>79</td>
</tr>
<tr>
<td>Shrinking zFS aggregates</td>
<td>79</td>
</tr>
<tr>
<td>Encrypting and compressing zFS file system data</td>
<td>79</td>
</tr>
<tr>
<td>Enhanced mounting of VSAM linear data sets</td>
<td>79</td>
</tr>
<tr>
<td>Dynamically changing attributes that were assigned when a file system is first mounted</td>
<td>80</td>
</tr>
<tr>
<td>SMF support for zFS</td>
<td>80</td>
</tr>
<tr>
<td>z/OS Management Facility (z/OSMF)</td>
<td>80</td>
</tr>
<tr>
<td>z/OSMF enabled during IPL</td>
<td>80</td>
</tr>
<tr>
<td>z/OSMF Sysplex Management task</td>
<td>80</td>
</tr>
<tr>
<td>z/OSMF z/OS Operator Consoles</td>
<td>81</td>
</tr>
<tr>
<td>z/OS UNIX System Services new functions to consider</td>
<td>81</td>
</tr>
<tr>
<td>z/OS UNIX forkcopy processing</td>
<td>81</td>
</tr>
<tr>
<td>z/OS UNIX kernel stack allocation</td>
<td>81</td>
</tr>
<tr>
<td>Loading RMODE64 programs into common storage</td>
<td>82</td>
</tr>
<tr>
<td>Obtaining information about RMODE64 modules that were loaded by the debugged process</td>
<td>82</td>
</tr>
<tr>
<td>Migrating HFS and zFS file systems to zFS file systems</td>
<td>82</td>
</tr>
<tr>
<td>Maintaining a single configuration file across the sysplex</td>
<td>82</td>
</tr>
<tr>
<td>Migrating HFS and zFS file systems to zFS file systems</td>
<td>82</td>
</tr>
<tr>
<td>Support for z/OS UNIX syscall exits</td>
<td>83</td>
</tr>
<tr>
<td>Mounting and unmounting file systems with the SETUID option</td>
<td>83</td>
</tr>
<tr>
<td>Checking for unsecure services that are configured for the inetd daemon</td>
<td>83</td>
</tr>
<tr>
<td>Debugging enhancements for dbx</td>
<td>83</td>
</tr>
<tr>
<td>Reporting CPU time in microseconds</td>
<td>83</td>
</tr>
</tbody>
</table>
How to send your comments to IBM

We invite you to submit comments about the z/OS® product documentation. Your valuable feedback helps to ensure accurate and high-quality information.

Important: If your comment regards a technical question or problem, see instead “If you have a technical problem” on page ix.

Submit your feedback by using the appropriate method for your type of comment or question:

Feedback on z/OS function
If your comment or question is about z/OS itself, submit a request through the IBM RFE Community (www.ibm.com/developerworks/rfe/).

Feedback on IBM® Knowledge Center function
If your comment or question is about the IBM Knowledge Center functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Knowledge Center Support at ibmkc@us.ibm.com.

Feedback on the z/OS product documentation and content
If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to mhvrdfs@us.ibm.com. We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:
• Your name, company/university/institution name, and email address
• The following deliverable title and order number: z/OS Introduction and Release Guide, GA32-0887-40
• The section title of the specific information to which your comment relates
• The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive authority to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem
If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:
• Go to the IBM Support Portal (support.ibm.com).
• Contact your IBM service representative.
• Call IBM technical support.
This information explains how z/OS references information in other documents and on the web. When possible, this information uses cross document links that go directly to the topic in reference using shortened versions of the document title. For complete titles and order numbers of the documents for all products that are part of z/OS, see z/OS Information Roadmap.

To find the complete z/OS library, go to IBM Knowledge Center (www.ibm.com/support/knowledgcenter/SSLTBW/welcome).
Summary of changes

This information includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations for the current edition are indicated by a vertical line to the left of the change.


The following content is new, changed, or no longer included in V2R4.

New

The following content is new.

- New system-level functions to consider, such as new base elements, optional features, or interfaces are listed in “z/OS system-level new functions to consider” on page 21.
- BCP (MVS™) has new functions to consider. For details, see “Cross-System Coupling Facility (XCF) enhancements for z/OS V2R4” on page 28.
- Cryptographic Services has new functions to consider. For details, see “Cryptographic Services new functions to consider” on page 38:
  - “ICSF: Enhancements for Crypto Express5S (CCA Release 5.4 and later) and Crypto Express6S (CCA Release 6.2 and later)” on page 38
  - “ICSF: CCA redirection for Regional Crypto Enablement” on page 39
  - “ICSF: ChaCha20 and Poly1305 algorithms” on page 39
  - “ICSF: Dynamic Service update: Applying service to a running ICSF instance without causing an interruption to your applications” on page 40
  - “ICSF: Early ICSF availability” on page 40
  - “ICSF: KGUP and SAF profile prefixing” on page 40
  - “ICSF: New BSI mode (BSI 2017)” on page 40
  - “ICSF: Updates to PKCS#11 Wrap Key (CSFPWPK) and PKCS#11 Unwrap Key (CSFPUWK)” on page 41
  - “ICSF: New DISPLAY ICSF, MKVPs operator command” on page 41
  - “PKI Services Enrollment over Secure Transport (EST)” on page 45
  - “System SSL: PKCS #7 signed data message has been enhanced to support detached (external) signatures” on page 47
  - “System SSL: RSASSA-PSS support” on page 47
  - “System SSL: TLS 1.3 support” on page 47
- DFSMS has new functions to consider. For details, see “SMS enhancements for z/OS V2R4” on page 52.
- HCD has new functions to consider. For details, see “Hardware Configuration Definition (HCD) new functions to consider” on page 53.
- HCM has new functions to consider. For details, see “Hardware Configuration Manager (HCM) new functions to consider” on page 54.
- InfoPrint Server has new functions to consider. For details, see “Infoprint Server new functions to consider” on page 56:
  - “Accessible and signed PDFs” on page 57
- “Enhanced PDF encryption with AES options” on page 57
- “Dynamic configuration at all times” on page 57
- “Infoprint Central enhancements for V2R4” on page 58
- “Security enhancements” on page 59

- JES2 has new functions to consider. For details, see:
  - “JES2 policies” on page 62
  - “Health Check for JES2 Checkpoint Configuration” on page 63
  - “JES2 disk reader support” on page 62
  - “Instruction Execution Protection (IEP)” on page 63
  - “Reporting JES2 resiliency data” on page 63

- Language Environment® has new functions to consider. For details, see:
  - “Support for tracking specific price metrics” on page 65
  - “Japanese New Era support” on page 65
  - “Enabling non-executable memory” on page 65

- RSM has new functions to consider. For details, see “Real Storage Manager (RSM) considerations” on page 25.

- Security Server (RACF®) has new functions to consider. For details, see “Security Server (RACF) new functions to consider” on page 71.

- SMB has changes to consider. For details, see:
  - “Removal of Distributed File Service/Server Message Block (DFS/SMB)” on page 78

- TSO/E has new functions to consider. For details, see:
  - “LOGON timeout” on page 75
  - “Allow special characters within passwords” on page 75
  - “Server-Requester Programming Interface (SRPI) and TSO/E Enhanced Connectivity Facility removal” on page 75

- IBM Tivoli® Directory Server has new functions to consider. For details, see:
  - “Enhanced SDBM search” on page 54
  - “Enhanced activity logging” on page 55
  - “Transport Layer Security (TLS) protocol version 1.3” on page 55

- z/OS Communications Server has new functions to consider. For details, see “Communications Server new functions to consider” on page 29
  - “Hardware support” on page 29
  - “Usability and skills” on page 30
  - “Scalability and performance” on page 31
  - “Systems management” on page 33
  - “Enhancing security” on page 33
  - “Application development” on page 37

- z/OS File System (zFS) has new functions to consider. For details, see:
  - “Improved reliability and availability for zFS file systems” on page 78
  - “zFS File Snapshot” on page 78

- z/OS UNIX System Services has new functions to consider. For details, see:
  - “z/OS UNIX forkcopy processing” on page 81
  - “z/OS UNIX kernel stack allocation” on page 81
– “Loading RMODE64 programs into common storage” on page 82
– “Obtaining information about RMODE64 modules that were loaded by the debugged process” on page 82
– “Migrating HFS and zFS file systems to zFS file systems” on page 82

**Changed**
The following content is changed.

• Distributed File System (DFS) is now z/OS File System (zFS). For more information, see “Removal of Distributed File Service/Server Message Block (DFS/SMB)” on page 78. “z/OS base elements” on page 1 was also updated.

**Deleted**
The following content was deleted.

• All content that is not related to z/OS versions V2R3 or V2R4 was removed.
• The following base elements are deleted in z/OS V2R4:
  – BookManager® READ
  – Library Server
  – OSA Support Facility (OSA/SF)

---

**Summary of changes for z/OS V2R3 Introduction and Release Guide**

The following changes are made for z/OS Version 2 Release 3 (V2R3).

**New**

• New system level functions to consider, such as new base elements, optional features, or interfaces are listed in “z/OS system-level new functions to consider” on page 21.

• BCP (MVS) has new functions to consider. For details, see “BCP (MVS) new functions to consider” on page 22.
  – “Remote TSO/E Address Space Manager” on page 23, for APAR OA51597
  – “z/OS System Logger support for encrypted log stream data sets” on page 27
  – “Logstream staging datasets greater than 4GB” on page 27
  – “BCPii considerations” on page 22
  – “IBM Function Registry for z/OS considerations” on page 24
  – “Real Storage Manager (RSM) considerations” on page 25

• Communications Server has new functions to consider. For details, see “Communications Server new functions to consider” on page 29.
  – “Hardware support” on page 29
  – “Usability and skills” on page 30
  – “Scalability and performance” on page 31
  – “Systems management” on page 33
  – “Enhancing security” on page 33
  – “Application development” on page 37

• Cryptographic Services has new functions to consider. For details, see “Cryptographic Services new functions to consider” on page 38.
  – “ICSF: CCA service algorithm updates” on page 41
- “ICSF: Cryptographic services enhancements” on page 41
- “ICSF: Digital Signature Generate and Digital Signature Verify enhancements” on page 42
- “ICSF: EMV simplification services” on page 42
- “ICSF: Enhanced PKCS#11 Secret Key Encrypt and PKCS#11 Secret Key Decrypt” on page 42
- “ICSF: Enhancements for Crypto Express5” on page 42
- “ICSF: FIPS 140-2 certification of PKCS11” on page 43
- “ICSF: Improved Key Lifecycle and Key Usage auditing” on page 43
- “ICSF: Key Encryption Translate” on page 43
- “ICSF: New ICSF_OPTIONS_CHECKS health check” on page 44
- “ICSF: Operator commands” on page 44
- “ICSF: Options Data Set Refresh function” on page 44
- “ICSF: Regional crypto enablement” on page 44
- “ICSF: Support for German Banking Industry defined PIN processing functions” on page 45
- “ICSF: Support for secure key tokens in Field Level Encipher and Field Level Decipher” on page 45
- “ICSF: Unsupported key detection” on page 45
- “PKI Services SCEP usability” on page 46
- “PKI Services FIPS support” on page 46
- “PKI Services Liberty support” on page 46
- “PKI Services DB2 Optimization” on page 46
- “System SSL: GSKIT V4 CMS certificate store” on page 47
- “System SSL: FIPS enforcement” on page 47
- “System SSL: Server Key Label List” on page 47
- “System SSL: Standards Currency” on page 48

• DFSMS has new functions to consider. For details, see “DFSMS new functions to consider” on page 48.
  - “Advanced Copy Services enhancements for z/OS V2R3” on page 49
  - “DFSMS catalog enhancements for z/OS V2R3” on page 49
  - “DFSMS data set encryption enhancements for z/OS V2R3” on page 52
  - “Object Access Method (OAM) enhancements for z/OS V2R3” on page 51
  - “SMS enhancements for z/OS V2R3” on page 51
  - “VSAM and VSAM RLS enhancements for z/OS V2R3” on page 52
  - “DFSMShsm enhancements for z/OS V2R3” on page 50

• DFSMSrmm has new functions to consider. For details, see “DFSMStvs new functions” on page 51.

• DFSMStvs has new functions to consider. For details, see “DFSMStvs new functions” on page 51.
• Distributed File Service (DFS) has new functions to consider.
  - “zFS File Snapshot” on page 78
  - “Identifying SMB-exported file systems” on page 79
  - “Enhanced mounting of VSAM linear data sets” on page 79
  - “Repairing mounted zFS file systems” on page 79
  - “Shrinking zFS aggregates” on page 79
  - “Encrypting and compressing zFS file system data” on page 79
  - “Dynamically changing attributes that were assigned when a file system is first mounted” on page 80.
  - “SMF support for zFS” on page 80
• IBM Tivoli Directory Server for z/OS has new functions to consider. For details, see “IBM Tivoli Directory Server for z/OS new functions to consider” on page 54
  - “MFA Support” on page 55
  - “Health Checks” on page 55
  - “FIPS Compliant” on page 56
  - “Multi-Row Fetch” on page 56
  - “Support DB2 partitioning by Growth for ITDS TDBM and GDBM database” on page 56
  - “Prevent visibility of sensitive data in debug trace” on page 56
• IBM z/OS Liberty Embedded is now a base element of z/OS.
• Infoprint Server has new functions to consider. For details, see:
  - “Dynamic tracing” on page 57
  - “IP PrintWay backup printer capability” on page 58
  - “Infoprint Central enhancements for V2R3” on page 59
  - “Sendmail to CSSMTP bridge” on page 59
  - “TSO/E 8-character user IDs” on page 60
• JES2 has new functions to consider. For details, see:
  - “JES2 email support” on page 64
  - “JCL Simplification” on page 64
  - “Dynamic groups added” on page 64
  - “Managing JES2 resources” on page 64
  - “JES3 JECL support” on page 64
• JES3 has new functions to consider. For details, see:
  - “JES3 support for 8-character TSO/E user IDs” on page 65
• Language Environment has new functions to consider.
  - “Japanese New Era support” on page 65
  - “Year 2038/2040 support” on page 66
  - “Detecting buffer overflows” on page 66
  - “64-bit support for Enterprise PL/I” on page 66
• Metal C Runtime Library new functions to consider.
  - “Prefix data block” on page 66
  - “Debug data block” on page 67
  - “Metal C function descriptors” on page 67
• Security Server (RACF) has new functions to consider. For details, see:
  - “RACF Parmlib support” on page 73
  - “RACF ODM classes support” on page 74
  - “RACF CICS Auditing support” on page 74
• TSO/E has new functions to consider. For details, see:
  - “8 character user ID” on page 75
  - “TSO/E Support for JES2 Resiliency” on page 76
• z/OS Management Facility (z/OSMF) has new functions to consider.
  - “z/OS Management Facility (z/OSMF)” on page 80
• z/OS UNIX has new functions to consider.
• z/OS XL C/C++ has new functions to consider.
  – “New and changed compiler options” on page 76
  – “New LEGACY option for the DSECT Utility” on page 77
  – “New SOS info utility” on page 77
  – “Updates to CDAHLASM and as utilities” on page 78
  – “Enhanced vector programming support” on page 76

**Changed**

• Changed system level functions to consider are listed in “z/OS system-level new functions to consider” on page 21.

**Deleted**

All content that is not related to z/OS versions V2R3 or V2R2 was removed.
Chapter 1. z/OS elements and features

z/OS base elements

z/OS provides function that is equivalent to the following elements. For the version and release numbers of those elements that also exist as separately orderable products, see z/OS Planning for Installation.

For an extra set of integrated features that is available on an optional basis, see “z/OS optional features” on page 2.

The following base elements are included in z/OS:

• Alternate Library for REXX
• Base Control Program (BCP)
• Bulk Data Transfer (BDT)
• Common Information Model (CIM)
• Communications Server
• Cryptographic Services (includes ICSF, OCSF Base, PKI Services, and System SSL)
• DFSMSdfp
• EREP
• ESCON Director Support
• FFST
• GDDM (includes PCLK and OS/2 Link)
• Hardware Configuration Definition (HCD)
• High Level Assembler (HLASM)
• IBM HTTP Server - Powered by Apache (includes IBM HTTP Server NA Secure)
• IBM Knowledge Center for z/OS
• IBM Tivoli Directory Server for z/OS
• IBM z/OS Liberty Embedded
• ICKDSF
• Integrated Security Services (includes Enterprise Identity Mapping (EIM), Network Authentication Service, and Open Cryptographic Enhanced Plug-ins (OCEP))
• ISPF
• JES2
• Language Environment
• Metal C Runtime Library
• MICR/OCR Support
• Network File System
• OpenSSH
• Runtime Library Extensions
• SMP/E
• TIOC
• TSO/E
• Xvfb
• z/OS Font Collection
• z/OS Management Facility (z/OSMF)
• z/OS File System
• z/OS UNIX System Services
• 3270 PC File Transfer Program

z/OS optional features

Some optional features are not priced, but priced as well as unpriced features are included in z/OS integration-testing. All priced, host-based features are capable of being dynamically enabled or disabled. For the version and release levels of those features that also exist independently, see z/OS Planning for Installation.

The following is a list of z/OS optional features:
• Bulk Data Transfer (BDT) File-to-File
• Bulk Data Transfer (BDT) SNA NJE
• Communications Server Security Level 3
• DFSMSdss
• DFSMSHsm
• DFSMSrmm
• DFSMSstvs
• DFSORT
• GDDM-PGF
• GDDM-REXX
• High Level Assembler (HLASM) Toolkit
• Hardware Configuration Manager (HCM)
• Infoprint Server
• JES3
• RMF
• Restricted use common service area (RUCSA)
• SDSF
• Security Server (includes RACF)
• XL C/C++
• zEnterprise® Data Compression (zEDC)
Chapter 2. z/OS base elements descriptions

The following is a description of each base element in z/OS.

Alternate Library for REXX

Alternate Library for REXX enables users who do not have the REXX on IBM Z® library installed to run compiled REXX programs. It contains a language processor that transforms the compiled programs and runs them with the REXX interpreter, which is shipped as part of the z/OS operating system.

Software developers are no longer required to distribute the Alternate Library for REXX with their compiled REXX programs. Customers who have the REXX on IBM Z® Library installed will gain the performance benefits of running compiled REXX, while those customers who have the Alternate Library for REXX installed may still run the programs as interpreted.

By using the Alternate Library for REXX with z/OS, software developers gain the benefits of shipping compiled REXX programs without the source code:

• Maintenance of the program is simplified since the code can not be modified inadvertently.
• Compiled programs can be shipped in load module format, simplifying packaging and installation.
• The Alternate Library for REXX does not need to be shipped and installed with the software program.
• Maintenance of the Alternate Library for REXX is handled by the z/OS system administrator.

BCP (Base Control Program)

The backbone of the z/OS system is the Multiple Virtual Storage (MVS) Base Control Program with JES2 or JES3. These provide the essential services that make z/OS the system of choice when you need to process your workloads reliably, securely, with complete data integrity and without interruption.

Unicode support:

The Unicode Standard is the universal character encoding standard used for representation of text for computer processing; it provides the capacity to encode all of the characters used for the written languages of the world. z/OS Unicode support is based on Version 6.0 of the Unicode Standard, although lower versions are supported by some services. Review each individual service to see the Unicode Standard versions supported. z/OS Unicode Services supports the following services:

• Character conversion
• Case conversion
• Normalization
• Collation
• Stringprep
• Bidirectional transformation
• Conversion information service
• Dynamic locale service

Find summary and complete details about these services in z/OS Unicode Services User’s Guide and Reference.
**z/OS XML System Services:**

z/OS XML System Services is an integrated component of the BCP. It is a system-level XML parser intended for use by system components, middleware, and applications that need a simple, efficient, non-validating XML parser. It provides a buffer-in, buffer-out processing model in which the document to parse is provided by the caller in one buffer; the z/OS XML System Services parser creates a parsed record stream in another buffer, also provided by the caller. Large documents can be processed by replenishing the input buffer with more data, and reusing the output buffer or specifying a new one when it is filled. z/OS XML System Services is invoked as a callable service and provides an assembler interface for callers to use. It is accessible from normal environments such as batch and z/OS Unix System Services, as well as from more esoteric environments such as SRB mode and cross-memory.

**BDT (Bulk Data Transfer)**

Bulk Data Transfer (BDT) provides the base services that BDT File-to-File and BDT SNA NJE need to transfer data from one computer system to another.

**Common Information Model (CIM)**

The Common Information Model (CIM) is a standard data model for describing and accessing systems management data in heterogeneous environments. It allows system administrators or vendors to write applications (CIM monitoring clients) that measure system resources in a network with different operating systems and hardware. With z/OS CIM, it is possible to use the DMTF CIM open standard for systems management which is also implemented on further major server platforms (for example, Linux on zSeries, Linux on xSeries, i5/OS, or AIX®).

z/OS CIM implements the CIM server which is based on the OpenPegasus open source project. A CIM client invokes the CIM server which, in turn, collects z/OS data from the system and returns it to the calling client. To get the z/OS data, the CIM server invokes a CIM provider which retrieves the data from z/OS system resources.

The metrics obtained by this new API are common across server platforms so you can use it to create end-to-end monitoring applications.

**Communications Server**

**IP**

IP (formerly known as IBM TCP/IP) is a set of industry standard protocols and applications that allow you to share data and computing resources with other computers, both IBM and non-IBM. UNIX applications use IP. By using IP commands at your workstation, you can perform tasks and communicate easily with a variety of other systems and workstations. IP allows you to perform tasks independent of the computer type. Some common uses of IP include: electronic mail, file transfer, remote logon, and the Internet.

**IP CICS® Sockets**

IP CICS Sockets, which is integrated into the base TCP/IP stack, provides the ability to use the generalized Application Programming Interface (API) and socket applications in COBOL, PL/I, and assembler.

**IP IMS Sockets**

IMS IP support, also integrated into the base TCP/IP stack, allows the development of peer-to-peer applications in which IMS and an IP-connected peer form a client/server relationship. Using this support, IMS can be either client or server.

This element consists of three parts:

- The Sockets Extended Application Programming Interface. Using this API, IMS message processing programs can communicate with remote IP-connected hosts using socket protocol.
• If IMS is acting as the server, the IMS Listener can be used to collect incoming transaction requests from remote IP-connected hosts and schedule IMS message processing programs to service these requests.

• The IBM Assist module provides support for the IMS application programmer who wishes to code IP client/server application programs using the IMS API. When used, this optional function intercepts IMS message queue calls and replaces them with socket calls.

**SNA**
Formerly known as VTAM®, Systems Network Architecture (SNA) is a network communication access method and provides Advanced Peer-to-Peer Networking (APPN). SNA is the interface between application programs in a host processor and other resources in an SNA network, and links peer users of the network. It establishes and terminates sessions between users of the network, forwarding session data to and from each session partner.

In addition to establishing and terminating sessions, it activates and deactivates resources under its control, including application programs and devices to which SNA is directly attached. SNA also maintains information on the network configuration, active sessions, and network conditions.

To help users control a network, SNA receives commands from an operator to perform network services. Through operator messages, the operator is kept informed about those services and about any network conditions.

**Cryptographic Services**
Cryptographic Services includes ICSF, PKI Services, OCSF, and System SSL, and provides cryptographic functions for data secrecy, data integrity, personal identification, digital signatures, and the management of cryptographic keys.

ICSF and PKI Services are provided through the combination of secure cryptographic hardware, the ICSF cryptographic API, and the ICSF administration interface. ICSF supports the Common Cryptographic Architecture (CCA), as well as the DES algorithm, RSA public key cryptography, and the Digital Signature Standard. Cryptographic services support a wide variety of applications with high performance, security, and availability.

Additional functions include:

• Trusted Key Entry—the key entry unit for master keys has been replaced by a secure channel version implemented on a workstation known as the Trusted Key Entry Workstation. The unit is an optional cost feature.

• Commercial Data Masking Facility supports privacy functions.

• Public Key API (PKA Support) provides additional formatting or message digest standards.

• Public Key Cryptography Standards #11 (PKCS #11)

Public Key Infrastructure Services (PKI Services) allows you to establish a PKI infrastructure and serve as a certificate authority for your internal and external users, issuing and administering digital certificates in accordance with your own organization’s policies. You can use a PKI Services application to request and obtain certificates through their own Web browsers, while your authorized PKI administrators approve, modify, or reject these requests through their own Web browsers. The Web applications provided with PKI Services are customizable, and a programming exit is also included for advanced customization. The approval for certificate requests can be manual or automatic if additional authentication such as RACF user IDs, is provided. You can issue certificates for different purposes, such as virtual private network (VPN) devices, smart cards, and secure e-mail, through different types of templates. PKI Services supports Public Key Infrastructure for X.509 version 3 (PKIX) and Common Data Security Architecture (CDSA) cryptographic standards.

The OCSF Architecture consists of a set of layered security services and associated programming interfaces designed to furnish an integrated set of information and communication security capabilities. Each layer builds on the more fundamental services of the layer directly below it.
These layers start with fundamental components such as cryptographic algorithms, random numbers, and unique identification information in the lower layers, and build up to digital certificates, key management and recovery mechanisms, and secure transaction protocols in higher layers. The OCSF Architecture is intended to be the multiplatform security architecture that is both horizontally broad and vertically robust.

System SSL supports the SSL V2.0, SSL V3.0, TLS (Transport Layer Security) V1.0, TLS V1.1, TLS V1.2, and TLS V1.3 protocols. TLS V1.3 is the latest version of the secure sockets layer protocol.

z/OS provides a set of SSL C/C++ callable application programming interfaces that, when used with the z/OS Sockets APIs, provide the functions required for applications to establish this secure sockets communications.

In addition to providing the API interfaces to exploit the Secure Sockets Layer and Transport Layer Security protocols, System SSL is also providing a suite of Certificate Management APIs. These APIs give the capability to create/manage your own certificate databases, utilize certificates stored in key database and key rings for purpose other than SSL and to build/process PKCS #7 standard messages.

**DFSMSdfp**

DFSMSdfp provides the foundation for:

- **Storage management**
  DFSMSdfp includes ISMF, an interactive facility that lets you define and maintain policies to manage your storage resources. These policies help to improve the use of storage devices, and to increase levels of service for user data, with minimal effort required from users. SMS manages these policies for the operating system. You can also use the NaviQuest tool under ISMF to help you migrate to SMS, maintain your SMS configuration, and perform many testing, implementation, and reporting tasks in batch.

- **Tape mount management**
  SMS provides a means for implementing tape mount management, a methodology for improving tape usage and reducing tape costs. This methodology involves intercepting selected tape data set allocations through the SMS automatic class selection (ACS) process, and redirecting them to a DASD buffer. Once on DASD, these data sets can be migrated to a single tape or small set of tapes, thereby reducing the overhead associated with multiple tape mounts.

- **Data management**
  DFSMSdfp helps you store and catalog information on DASD, optical, and tape resources, so that it can be quickly identified and retrieved from the system. You can use the catalog search interface, now part of DFSMSdfp, to access the catalog.

- **Program management**
  DFSMSdfp combines programs into executable modules, prepares them to run on the operating system, stores them in libraries, and reads them into storage for execution.

- **Device management**
  DFSMSdfp is involved in defining your input and output devices to the system, and in controlling the operation of those devices in the z/OS environment.

- **Distributed data access**
  Distributed data access allows all authorized systems and users in a network to exploit the powerful features of system-managed storage, or automated storage management provided by DFSMS. DFSMSdfp uses the Distributed FileManager (DFM) to support remote access of z/OS data and storage resources from workstations, personal computers, or any other system on a SNA LU 6.2 network.

  The z/OS UNIX System Services (z/OS UNIX) file system works in conjunction with z/OS UNIX to provide a full UNIX environment within the z/OS system. z/OS becomes a full-feature UNIX client or server when coupled with the z/OS Network File System (z/OS NFS). With the z/OS UNIX file system, z/OS programs can directly access UNIX data. When the z/OS NFS client and z/OS UNIX are used together, z/OS can act as a client and access data from any remote system, including another z/OS or UNIX system that is connected using a TCP/IP network served by a Network File System server.
Environmental Record Editing and Printing Program (EREP)

The Environmental Record Editing and Printing Program (EREP) edits and prints reports for the records placed in the error recording data set (ERDS), helping IBM service representatives fix problems.

ESCON Director Support

When your installation uses ESCON directors, the ESCON Director Device Support feature enables reporting of ESCON director device errors to z/OS.

FFST/MVS (First Failure Support Technology/MVS)

FFST/MVS provides immediate notification and first failure data capture for software events. FFST/MVS also incorporates its own technology by including software probes in its own code. When one of these probes is triggered, FFST/MVS issues a symptom string that describes the event.

FFST/MVS provides the following services for IBM products:

- Customized dumps
- Symptom strings
- Symptom records
- Messages
- Network notification

GDDM (includes PCLK and OS/2 LINK)

GDDM provides presentation services and device-driving capability. GDDM has a powerful application-programming interface for creating, displaying, and storing vector graphics, images and alphanumerics. GDDM drives displays, printers and plotters, and includes several utilities for end users. GDDM's excellence as a graphics program and device driver is recognized worldwide, and as a result it is used extensively as a graphics enabler by other licensed programs, including other elements of z/OS.

HCD (Hardware Configuration Definition)

HCD is used to define both the operating system configuration and the processor hardware configuration for a system. Because HCD validates data when it is defined rather than when a device is accessed, inconsistencies can be corrected right away and unplanned system outages resulting from inconsistent definitions avoided. The defined configuration can be used to POR/IPL or dynamically reconfigure your system.

HLASM (High Level Assembler)

High Level Assembler integrates almost all functions of past assemblers. It also provides extensions and improvements including:

- Many new and expanded cross reference facilities and diagnostics that enable substantial savings in time and in human and machine resources, and support integration of HLASM into tool and development environments.
- Numerous language enhancements that improve the speed and accuracy of application development and the quality and reliability of the resulting code.
• Assembly-time options extensions and enhancements that allow increased flexibility and precision in controlling the processes you use to manage application development.

HLASM helps to maximize the productivity of application programmers by relieving them of many tedious and unproductive tasks that can now be done by the assembler itself and helps organizations avoid the necessity for converting existing -- and working -- applications from Assembler Language to other languages.

**IBM HTTP Server - Powered by Apache**

The IBM HTTP Server - Powered by Apache is a full-featured web server. This element was previously known as a base element of z/OS under the names Lotus® Domino® Go, the Internet Connection Secure Server (ICSS), and the Internet Connection Server (ICS).

Included in IBM HTTP Server - Powered by Apache is IBM HTTP Server North America (NA) Secure. With IBM HTTP Server - Powered by Apache, IBM HTTP Server NA Secure uses Secure Sockets Layer (SSL) to provide secure communications over an open communications network, such as the Internet. The HTTP server uses SSL to initiate a secure connection between the client and itself. The server then uses SSL to decrypt and encrypt all of the information in the client request and the server response.

**IBM Tivoli Directory Server for z/OS (IBM TDS for z/OS)**

The IBM Tivoli Directory Server for z/OS (IBM TDS for z/OS) provides secure access for applications and systems on the network to directory information held on z/OS using the Lightweight Directory Access Protocol (LDAP). This component consists of the LDAP server, LDAP client, and utilities.

**ICKDSF (Device Support Facility)**

ICKDSF enables you to perform functions needed for the installation and use of IBM DASD. You can also use it to perform service functions, error detection, and media maintenance.

**Integrated Security Services**

Integrated Security Services includes:

**Enterprise Identity Mapping (EIM)**

EIM is an architecture that serves as a security technology to make it easier to manage users in a cross-platform environment.

**Network Authentication Service**

Network Authentication Service, which is based on Kerberos Version 5, provides Kerberos security services. These services include native Kerberos application programming interface (API) functions, including the Generic Security Service application programming interface (GSS-API) functions defined in Internet RFC 2078, Generic Security Service Application Program Interface, Version 2 and Internet RFC 2744, Generic Security Service API Version 2: C-bindings. Network Authentication Service performs authentication as a trusted third-party authentication service by using conventional shared secret-key cryptography. Network Authentication Service provides a means of verifying the identities of principals, without relying on authentication by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network, and under the assumption that packets traveling along the network can be read, modified, and inserted at will.

**Open Cryptographic Services Facility (OCSF)**

Open Cryptographic Services Facility (OCSF) is a derivative of the IBM Keyworks technology, which is an implementation of the Common Data Security Architecture (CDSA) for applications running in the UNIX Services environment. It is an extensible architecture that provides mechanisms to manage service provider security modules, which use cryptography as a computational base to build security...
protocols and security systems. Figure 1 shows the four basic layers of the OCSF: Application Domains, System Security Services, OCSF Framework, and Service Providers. The OCSF Framework is the core of this architecture. It provides a means for applications to directly access security services through the OCSF security application programming interface (API), or to indirectly access security services by way of layered security services and tools that are implemented over the OCSF API. The OCSF Framework manages the service provider security modules and directs application calls through the OCSF API to the selected service provider module that services the request. The OCSF API defines the interface for accessing security services. The OCSF service provider interface (OCSF SPI) defines the interface for service providers who develop plug-able security service products.

**ISPF**

ISPF provides facilities for all aspects of host-based software development.

- Programmers can use ISPF to develop and document batch and interactive programs.
- Data center administrators and system programmers can monitor and control program libraries, and communicate with MVS through TSO commands, CLISTs, or REXX EXECs.
- Terminal users can work with interactive applications called dialogs.
- Managers can prepare and print memos by using ISPF Edit and the Hardcopy utility.

ISPF has four major components:

**Dialog Manager (DM)**

The Dialog Manager (DM) provides services to dialogs and users. These services include:

- Display
- Variable services
- Input and output
- User and application profiles
- Table management
- System interface services
- Dialog testing and debugging aids

**Program Development Facility (PDF)**

The Program Development Facility (PDF) provides services to assist dialog or application developers. These include:

- Edit and Browse functions
- A wide range of foreground and batch compilers
- Data set and catalog utilities
- TSO or CMS command interfaces
- Data set search and compare functions.

**Software Configuration and Library Manager (SCLM)**

The Software Configuration and Library Manager (SCLM) is a tool that automatically controls, maintains, and tracks all of the software components of the application throughout the development cycle.

**Client/Server component**

The Client/Server component provides users who have a workstation that runs Windows or UNIX with a Graphical User Interface to ISPF application panels.

**JES2**

JES2 accepts the submission of work for the BCP. Major JES2 functions and design features include:
• The interpretation of job control language (JCL) statements
• The disposition of output
• A single-system image
• The ability to run multiple copies of JES2 (poly-JES)
• JES2 WLM for Sysplex

JES2 differs from JES3 in two main processing areas:
• JES2 exercises independent control over its job processing functions. JES3 exercises centralized control. Each JES2 processor in a multi-processor environment controls its own job input, job scheduling, and job output processing.
• JES3 does pre-execution of job setup. JES2 does not do this.

Language Environment

Language Environment provides common services and language-specific routines in a single run-time environment. It ensures consistent and predictable results for your language applications, independent of the language they are written in.

Language Environment is the prerequisite run-time environment for applications generated with the following IBM compiler products:
• z/OS XL C/C++
• OS/390® C/C++
• C/C++ for MVS/ESA
• COBOL for OS/390 & VM
• COBOL for MVS & VM (formerly COBOL/370)
• Enterprise COBOL for z/OS
• Enterprise COBOL for z/OS and OS/390
• AD/Cycle C/370 Compiler
• Enterprise PL/I for z/OS
• Enterprise PL/I for z/OS and OS/390
• VisualAge® PL/I for OS/390
• PL/I for MVS & VM
• AD/Cycle PL/I for MVS & VM
• VisualAge for Java™, Enterprise Edition for OS/390
• VS FORTRAN and FORTRAN IV (in compatibility mode)

Language Environment supports the VS FORTRAN compiler’s object/load module compatibility, which means FORTRAN load modules can be run under Language Environment and object code can be link-edited with Language Environment and run under it. Language Environment also provides a set of assembler macros for running assembler language routines.

Language Environment supports, but is not required for, an interactive debug tool for debugging applications in your native z/OS environment. The interactive IBM Debug Tool is available with the latest release of the PL/I compiler or this product can be ordered separately for use with the IBM XL C/C++, COBOL, and PL/I compilers on z/OS. For more information, see Debug Tool Utilities and Advanced Functions (www.ibm.com/software/awdtools/debugtool).

Some benefits are that you can:
• Mix old code with new code.
• Handle conditions, such as program checks or abends, in your COBOL programs without having to use assembler.
• Share common run-time services.
• Run applications that conform to the POSIX 1003.1 standard or the X/Open Single UNIX Specification, also known as UNIX 95 or XPG4.2.
• Access CICS and IMS transactions and data through a C, COBOL, or PL/I server from any client in your network.
• Perform interlanguage communication more efficiently.
• Manage storage dynamically for your C/C++, COBOL, and PL/I routines with a common storage manager.
• Access a rich set of math services.

**MICR/OCR**

MICR/OCR provides the device support code for the following devices:

• 1287/1288 - IBM Optical reader and page reader respectively
• 3540 - IBM Disk device
• 3886 - IBM Optical Character reader
• 3890 - IBM Magnetic Ink Reader
• 3895 - IBM Printer device

**Metal C Runtime Library**

The Metal C runtime library element provides a set of header files and functions for use with the XL C METAL compiler option.

The XL C METAL compiler option generates code that does not require access to the Language Environment support at run time. Instead, the METAL option provides C-language extensions that allow you to specify assembly statements that call system services directly. Using these language extensions, you can provide almost any assembly macro, and your own function prologs and epilogs, to be embedded in the generated HLASM source file. When you understand how the METAL-generated code uses MVS linkage conventions to interact with HLASM code, you can use this capability to write freestanding programs.

Prior to the introduction of Metal C runtime library, all z/OS XL C compiler-generated code required Language Environment. In addition to depending on the C runtime library functions that are available only with Language Environment, the generated code depended on the establishment of an overall execution context, including the heap storage and dynamic storage areas. These dependencies prohibit you from using the XL C compiler to generate code that runs in an environment where Language Environment did not exist.

**Network File System (NFS)**

The z/OS NFS server acts as an intermediary to read, write, create or delete z/OS UNIX files and MVS data sets that are maintained on a z/OS host system. The remote MVS data sets or z/OS UNIX files are mounted from the host processor to appear as local directories and files on the client system. This server makes the strengths of a z/OS host processor (storage management, high-performance disk storage, security, and centralized data) available to the client platforms.

The NFS uses the communication services provided by TCP/IP, a suite of protocols that includes the remote procedure call (RPC) and external data representation (XDR) protocols. RPC allows a program on one machine to start a procedure on another machine, as if the procedure is local. XDR resolves the differences in data representation of different machines. The NFS, then, can be used for file sharing between platforms and file serving (as a data repository).
Run-Time Library Extensions

Run-Time Library Extensions delivers the following libraries and utilities to support existing programs:

**Common Debug Architecture (CDA) Libraries**
Introduced in z/OS V1R5, CDA provides a consistent format for debug information on z/OS. The CDA Libraries provide a set of APIs to access this information.

**c89 Utility**
This utility compiles, assembles, and binds z/OS UNIX System Services C/C++ and assembler applications.

**UNIX System Laboratories (USL) Libraries**
The USL I/O Stream Library provides the standard input and output capabilities for C++. The USL Complex Mathematics Library provides the facilities to manipulate complex numbers and to perform standard mathematical operations.

**Note:** The UNIX System Laboratories (USL) I/O Stream Library and Complex Mathematics Library are still supported on z/OS. Although support for these classes is not being removed at this time, it is recommended that you migrate to the Standard C++ iostream and complex classes. This is especially important if you are migrating other USL streaming classes to Standard C++ Library streaming classes, because combining USL and Standard C++ Library streams in one application is not recommended. For more information about the Standard C++ I/O Stream Library, see [Standard C++ Library Reference](#).

**SMP/E**
SMP/E is a tool for installing and maintaining software, and for managing the inventory of software that has been installed. SMP/E provides a consistent and reliable method for installing and upgrading the software in a z/OS system.

**Time Sharing Option/Extensions (TSO/E)**
TSO Extensions is a base interactive interface that provides non-DP professionals, end users, system and application programmers, and administrators with an extensive set of commands, services, facilities and programming languages to do productive work on z/OS, and helps to ease systems management. TSO/E is an integral part of z/OS, and serves as a platform for other elements, such as HCD and ISPF.

**Terminal Input Output Controller (TIOC)**
TIOC is the interface between TSO and VTAM. It allows TSO to communicate with the terminal hardware.

**z/OS File System (zFS)**
The z/OS File System (zFS) support provides a physical file system (PFS). zFS file systems contain files and directories that are accessed with the z/OS application programming interfaces. They can be mounted into the z/OS UNIX hierarchy along with other local (or remote) file system types such as HFS, TFS, and NFS. zFS typically provides improved performance over HFS.

**z/OS Font Collection**
The z/OS Font Collection consists of character sets, coded fonts, and Advanced Function Presentation (AFP) code pages for printing documents. The z/OS Font Collection includes these fonts:

- AFP outline fonts
• AFP raster fonts, including a complete set of IBM expanded core fonts and a set of Math, PI, and Sonoran 240-pel raster fonts
• TrueType and OpenType fonts, including a prebuilt resource access table (RAT) that can be used for AFP printing

**z/OS Management Facility (z/OSMF)**

IBM z/OS Management Facility (z/OSMF) provides system management functions in a task-oriented, web browser-based user interface with integrated user assistance, so that you can more easily manage the day-to-day operations and administration of your mainframe z/OS systems. By streamlining some traditional tasks and automating others, z/OSMF can help to simplify some areas of z/OS system management.

z/OSMF provides a framework for managing various aspects of a z/OS system through a web browser interface.

z/OSMF provides you with a single point of control for:

• Viewing, defining, and updating policies that affect system behavior
• Monitoring the performance of the systems in your enterprise
• Managing your z/OS software
• Performing problem data management tasks
• Consolidating your z/OS management tools.

z/OSMF allows you to communicate with the z/OS system through a web browser, so you can access and manage your z/OS system from anywhere. Multiple users can log into z/OSMF using different computers, different browsers, or multiple instances of the same browser.

Find more information about z/OSMF in *IBM z/OS Management Facility Configuration Guide*.

**z/OS OpenSSH**

z/OS OpenSSH is a port of Open Source Software release OpenSSH 6.4p1 and provides secure encryption for both remote login and file transfer.

z/OS OpenSSH includes the following utilities:

• `ssh`, a z/OS client program for logging into a z/OS shell. It can also be used to log into other platform's UNIX shells. It is an alternative to `rlogin`.
• `scp` for copying files between networks. It is an alternative to `rcp`.
• `sftp` for file transfers over an encrypted `ssh` transport. It is an interactive file transfer program similar to `ftp`.
• `sshd`, a daemon program for `ssh` that listens for connections from clients. The z/OS OpenSSH implementation of `sshd` supports both SSH protocol versions 1 and 2 simultaneously.

  The default `sshd` configuration only runs protocol version 2.

Other basic utilities such as `ssh-add`, `ssh-agent`, `ssh-keysign`, `ssh-keyscan`, `ssh-keygen` and `sftp-server` are also included.

To ensure secure encrypted communications, OpenSSH uses ciphers such as AES, Blowfish and 3DES.

z/OS OpenSSH provides the following z/OS extensions:

• System Authorization Facility (SAF) key ring. z/OS OpenSSH can be configured to allow z/OS OpenSSH keys to be stored in SAF key rings.
• Multilevel security. It is a security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories.
• System Management Facility (SMF). z/OS OpenSSH can be configured to collect SMF Type 119 records for both the client and the server.

• Hardware Crypto Support. OpenSSH can be configured to choose Integrated Cryptographic Service Facility (ICSF) callable service for implementing the applicable SSH session ciphers and HMACs.

**z/OS UNIX System Services (X/Open UNIX 95 functions)**

**z/OS UNIX System Services Application Services (Shell, Utilities, and Debugger)**

Shell and Utilities provides the standard command interface familiar to interactive UNIX users. z/OS includes all of the commands and utilities specified in the X/Open Company's Single UNIX Specification, also known as UNIX 95 or XPG4.2. This feature will allow your UNIX programmers and other users to interact with z/OS as a UNIX system without necessarily having to learn the z/OS command language or other interactive interfaces. The z/OS UNIX Services Debugger provides a set of commands that allow a C language program to be debugged interactively. The command set is familiar to many UNIX users.

**z/OS UNIX System Services Kernel**

These services add the world of open UNIX-based computing to the z/OS operating system. With Language Environment, they support industry standards for C programming, shell and utilities, client/server applications, and the majority of the standards for thread management and the X/Open Single UNIX Specification. Application developers and interactive users using these interfaces can exploit the capabilities of z/OS without having to understand z/OS itself. The combination of open computing and z/OS allows the transparent exchange of data, easy portability of applications, cross-network management of data and applications, and the exploitation of traditional MVS system strengths in an open environment.

**z/OS Xvfb**

Xvfb is an X server that can run on machines with no display hardware and no physical input devices. It emulates a dumb framebuffer using virtual memory. Xserver and other command line options are available for use with Xvfb.

**3270 PC File Transfer Program**

This program transfers files from the host to the workstation for off-line data manipulation or transfers local data for storage on the host.
Chapter 3. z/OS optional features descriptions

The following is a description of each optional feature in z/OS.

**Bulk Data Transfer (BDT) File-to-File**

The BDT File-to-File element allows users at one z/OS system in a SNA network to copy data sets to or from another z/OS system in the network.

**Bulk Data Transfer (BDT) SNA NJE**

The BDT JES3 SNA NJE element allows users with the JES3 element to transmit jobs, output (SYSOUT), commands, and messages from one computer system to another within a SNA network.

**Communications Server Security Level 3**

This feature provides authentication and security services in an IP network environment. It provides support for packet filtering, tunnels, and network address translation (NAT), which enables secure communication over private and public networks. It uses the Triple DES (TDES) and AES encryption algorithms, and it includes SSL/TLS with TDES and AES, SNMPv3 with TDES, and IPSec with TDES and AES.

**DFSMS Features (DFSMSdss, DFSMShsm, DFSMSrmm, and DFSMStvs)**

There are four DFSMS features:

**DFSMSdss**

DFSMSdss is a DASD data and space management tool. DFSMSdss can be used to copy and move data sets between volumes; dump and restore data sets, entire volumes, or tracks; convert data sets and volumes to and from SMS management; compress partitioned data sets; release unused space in data sets; and consolidate free space and data sets on volumes.

**DFSMShsm**

DFSMShsm is a DASD storage management and productivity tool for managing low-activity and inactive data. It improves DASD use by automatically managing space and data availability in a storage hierarchy. Working with SMS, DFSMShsm performs space management and availability management of data sets as directed by their management class attributes.

**DFSMSrmm**

DFSMSrmm allows you to manage your removable media as one enterprise-wide library across systems. DFSMSrmm manages your installation's tape volumes and the data sets on those volumes. DFSMSrmm manages all tape media, such as cartridge system tapes and 3420 reels, as well as other removable media you define to it. For example, DFSMSrmm can record the shelf location for optical disks and track their vital record status; it does not manage the objects on optical disks.

**DFSMStvs**

DFSMStvs Transactional VSAM Services, an optional feature, enables running batch jobs concurrently with CICS online transactions to allow updates to the shared VSAM data sets. Multiple batch jobs and online transactions can be run against the same VSAM data sets. DFSMStvs ensures data integrity for concurrent batch updates while CICS provides it for online updates.
**DFSORT**

DFSORT is IBM's high performance sort, merge, copy, analysis and reporting product for z/OS. This high-speed, flexible data processing tool provides fast and efficient sorting, merging, copying, reporting and analysis of business information, as well as versatile data manipulation at the record, field and bit level.

DFSORT is designed to optimize the efficiency and speed with which operations are completed through synergy with processor, device, and system features (for example, memory objects, hiperspace, data space, striping, compression, extended addressing, DASD and tape device architecture, processor memory, processor cache, and so on) and other products (for example, The SAS System**, COBOL, PL/I, IDCAMS BLDINDEX, and so on).

DFSORT includes the high-performance ICEGENER facility, the versatile ICETOOL utility, multiple output and reporting capability with the powerful OUTFIL feature, the time-saving ability to use Symbols for fields and constants in DFSORT and ICETOOL statements, and much more.

For more information on DFSORT, visit the DFSORT Web site.

**GDDM-PGF**

GDDM-PGF (Presentation Graphics Facility), a set of programs for creating presentation material in a variety of styles, provides:

**Interactive Chart Utility**
- The Interactive Chart Utility (ICU), an easy-to-use end-user program for creating business charts.

**Vector Symbol Editor**
- The (VSE), a means of creating and modifying symbols for use with the ICU or other GDDM functions.

**An application programming interface**
- An application programming interface that enables programs to call either the ICU or a set of presentation-graphics routines for chart creation.

**Online Presentation Services (OPS)**
- GDDM-PGF now incorporates an enhanced presentation-producing capability, Online Presentation Services (OPS). GDDM-OPS provides a command interface, which is simple and easy to use, yet which is also powerful enough to allow the very concise creation of high-quality presentations. These can then be used from displays (perhaps using the built-in automatic scrolling feature), or can be saved for printing or plotting.

Typical applications of GDDM-OPS are:
- Public presentations using a video monitor or projector
- Educational sessions for private or public display
- Scrollable interactive presentations of business charts
- Production of high-quality foils.

**GDDM-REXX**

GDDM-REXX/MVS is a productivity tool that enables programmers to prototype GDDM applications and to create small routines and utility programs quickly and easily.

**Hardware Configuration Manager (HCM)**

Hardware Configuration Manager (HCM) is a PWS-based client/server interface to z/OS Hardware Configuration Definition (HCD). It combines the logical and physical aspects of z/OS hardware configuration management. In addition to defining the logical connections (accomplished via HCD), you
can also manage the physical aspects of your configuration. For example, you can effectively manage the flexibility offered by the ESCON infrastructure.

All updates are done with HCM’s intuitive graphical user interface, and all changes are written into the IODF and fully validated for accuracy and completeness by HCD, avoiding unplanned system outages that are due to incorrect definitions.

**High Level Assembler Toolkit**

This toolkit provides a powerful set of capabilities to improve application development, debugging, and recovery.

The Toolkit provides six components:

- A disassembler which converts binary machine language to assembler language source statements.
- A flexible source-code analysis and cross-referencing tool to help determine variable and macro usage, analyze high-level control flows, and locate specific uses of arbitrary strings of characters in single or multiple modules.
- A workstation-based program analysis tool that displays control-flow graphs and source-code views within single programs or across entire application modules.
- A powerful and sophisticated low-level symbolic debugger for applications written in assembler and other compiled languages. It handles programs using 24, 31, and 64-bit addressing. (It does not support debugging privileged or supervisor-state code.)
- A rich set of macro instructions that implement a complete menu of the most widely used structured-programming constructs (IF/ELSE/ELSEIF, DO/ITERATE/ASMLEAVE, CASE, SEARCH, SELECT/WHEN/OTHERWISE, etc.). These macros simplify and clarify coding, and help eliminate errors in writing additional labels and branch instructions.
- A versatile file searching and comparison tool (SuperC) that scans or compares single file or groups of files with an extensive set of selection and rejection criteria.

**IBM Knowledge Center for z/OS**

IBM Knowledge Center is the IBM strategic platform for delivering technical content. z/OS includes IBM Knowledge Center for z/OS, which is an SMP/E packaging of the customer installable version of IBM Knowledge Center for use on the z/OS platform. The customer installable version uses an enhanced version of search technology that is available in IBM information centers.

- IBM Knowledge Center for z/OS provides the ability to display, navigate and search content in a manner similar to IBM Knowledge Center on ibm.com.
- IBM Knowledge Center for z/OS serves IBM product publication content to web browser clients from the z/OS server system.
- Content can be manually added to and maintained in IBM Knowledge Center for z/OS zFS repositories using information in the IBM Knowledge Center for z/OS Configuration and User Guide, SC27-6805.
- By adding and maintaining content, IBM Knowledge Center for z/OS can be made to serve product publications for many different IBM products.

Use IBM Knowledge Center for z/OS to create your own enterprise document repository for local use. IBM Knowledge Center for z/OS is especially valuable for:

- Enterprises with no Internet access either for security reasons or as a valuable backup when Internet access is disrupted
- Personalizing or controlling the content of an enterprise library
Infoprint Server

Infoprint Server consists of several components that support printing on a z/OS system:

Print Interface
This component accepts print requests from z/OS UNIX System Services and remote systems in your IP network. It allocates output data sets on the JES2 or JES3 spool for printing.

NetSpool
This component receives print output from VTAM applications and allocates output data sets on the JES2 or JES3 spool for printing.

Transform Manager
This component calls separate IBM transform products to transform data to and from Advanced Function Presentation (AFP) format. For example, IBM transform products can transform PCL, PDF, PostScript, SAP R/3, and Xerox data to AFP format, and can transform AFP data to PCL, PDF, and PostScript format.

IP PrintWay
This component sends output data from the JES2 or JES3 spool to remote printers or print servers in your IP or SNA network. IP PrintWay can also send output data to email destinations. You can run IP PrintWay in basic or extended mode. In extended mode, IP PrintWay provides better performance, improved usability, and more function.

Printer Inventory
This component provides a single set of printer definitions that all the components of Infoprint Server use. The Printer Inventory also contains printer customization information that Print Services Facility (PSF) for z/OS uses.

Infoprint Central
This component is a web application that lets help desk operators and other authorized users work with print jobs on the JES spool, printers controlled by IP PrintWay extended mode or PSF, NetSpool logical units, and job selection rules. It also lets users see Infoprint Server system status and printer definitions in the Printer Inventory.

Infoprint Port Monitor for Windows
This component sends documents and job attributes from Windows systems to Infoprint Server for printing on any printers that are defined in the Infoprint Server Printer Inventory.

JES3

You might choose to enable JES3 as an alternative to the base JES2 element. It also accepts the submission of work for the BCP. Major JES3 functions and design features include:

- The interpretation of job control language (JCL) statements
- The disposition of output
- A single system image
- Workload balancing
- Deadline scheduling
- Dependent job control
- Control flexibility

JES3 differs from JES2 in two main processing areas:

- JES3 exercises centralized control over its job processing functions. JES2 exercises independent control. With JES3, a single, global processor controls job, device, and workflow for all processors in a multi-processor environment.
- JES3 does pre-execution of job setup. JES2 does not do this.
RMF (Resource Measurement Facility)

RMF is the window on z/OS resource usage. It gathers information at sysplex, single-system or address-space level, and provides reports at any system in a sysplex. The user can choose between reports about activities and delays, and can focus on storage, I/O or processor data. A wide range of options allows selection of the relevant information, including the attainment of Workload Manager goals.

The RMF monitors present snap-shot and short-term reports real-time in ISPF dialogs with on-line help, and you can have the results printed if you wish. The RMF Postprocessor provides long-term reports for detailed analysis of historical data gathered by RMF. These reports can be printed or displayed.

In addition to host-based reporting functions in RMF, there are other components available that offer reporting capabilities at the workstation. The RMF PM Java Edition provides an interface between the workstation and the z/OS sysplex through a TCP/IP connection that gives you the flexibility to create unique scenarios to monitor the performance of your sysplex. The Spreadsheet Reporter, running on your Windows workstation, gives you the ability to extract reports from RMF Postprocessor output to convert them into a common spreadsheet format and allows your spreadsheet application to use the RMF data. This function enables you to integrate RMF data into your business process. It also means you can easily produce presentation graphics which illustrate performance analysis results.

Restricted use common service area (RUCSA)

For installations that cannot eliminate user-key (8 - 15) common storage usage, RUCSA provides a way to isolate user-key common storage to a select set of users, thus controlling or eliminating the security risk associated with common user-key storage.

SDSF (System Display and Search Facility)

SDSF provides you with information to monitor, manage and control your z/OS system. SDSF provides an easy and efficient way to control job processing (hold, release, cancel and purge jobs) and to control devices (such as printers, lines and initiators). It allows you to monitor jobs while they are running and browse output without printing it. You can also browse the system log, including the sysplex-wide operations log. SDSF provides sort, filter, arrange, search, and print functions to help you locate and organize information. Single-character commands eliminate the need to learn and remember complex system commands. You can easily change characteristics of an object, such as a job or node, by typing over a displayed value. An optional action bar and pop-up windows make it easy to find and use SDSF functions. You can establish security for SDSF using SDSF's own security parameters, or with IBM's standard interface, SAF (System Authorization Facility). You can access SDSF function through REXX execs or Java programs.

SDSF provides complete online help and an interactive tutorial.

Security Server

The Security Server includes:

Resource Access Control Facility (RACF)

RACF provides a strong security base that enables the Security Server element of z/OS to incorporate additional components that aid in securing your system as you make your business data and applications accessible by your intranet, extranets, or the Internet.

XL C/C++

This language-centered XL C/C++ application development environment on the z/OS platform includes a C compiler, a C++ compiler, and C/C++ application development utilities. This feature exploits the C/C++
runtime environment and library of runtime services available with the Language Environment and Run-Time Library Extensions elements of z/OS.

### z/OS Security Level 3

Chapter 4. What is new in z/OS (V2R3 - V2R4)

The following major enhancements were introduced in z/OS V2R4 and V2R3. Some enhancements require customization actions before you can use them. This information helps ensure that you can locate the documents that describe the customization actions.

**Note:** The document lists for each function are not exhaustive and generally omit links to purely reference books for items that include system messages, system codes, and data areas.

### Elements and features with no enhancements in V2R4

If an element or feature that is included in z/OS V2R4 is not listed in this section, is listed on the Usage information for the following z/OS elements and features was not updated for this release:

- Alternate Library for REXX
- Bulk Data Transfer (BDT)
- Common Information Model (CIM)
- DFSORT
- EREP
- ESCON Director Support
- FFST
- GDDM (includes PCLK and OS/2 Link)
- High Level Assembler (HLASM)
- IBM HTTP Server - Powered by Apache
- IBM Knowledge Center for z/OS
- IBM z/OS Liberty Embedded
- ICKDSF
- MICR/OCR Support
- OpenSSH
- Restricted use common service area (RUCSA)
- Runtime Library Extensions
- SDSF
- TIOC
- Xvfb
- zEnterprise® Data Compression (zEDC)
- z/OS Font Collection
- z/OS Security Level 3
- 3270 PC File Transfer Program

### z/OS system-level new functions to consider

This information describes z/OS system-level enhancements in this and the previous release.
**z/OS Font Collection: base element**

**Description:**
z/OS Font Collection is a comprehensive set of fonts for IBM products that were traditionally ordered separately. The fonts include selected object fonts, AFP, and IBM Infoprint fonts. z/OS Font Collection is updated with these enhancements:

- AFP raster fonts from these IBM products:
  - APL2 Fonts, Version 1 Release 1 (5771-ADB)
  - Data1 Fonts, Version 1. Release 1 (5771-ADA)
  - Sonoran Sans Serif Font, Version 1 Release 1 (5771-ABB)
  - Sonoran Sans Serif Condensed Font, Version 1 Release 1 (5771-AFL)
  - Sonoran Sans Serif Expanded Font, Version 1 Release 1 (5771-AFN)
  - Sonoran Sans Serif Headliner Font, Version 1 Release 1 (5771-ADX)
  - Sonoran Serif Font, Version 1 Release 1 (5771-ABA)
  - Sonoran Serif Headliner Font, Version 1 Release 1 (5771-ADW)
- Version 8.2 of WorldType fonts

**When change was introduced:**
z/OS V2R3

**Reference information:**
- z/OS Font Collection.
- z/OS Upgrade Workflow

**HTTP streaming support for the z/OS Client Web Enablement Toolkit**

**Description:**
The z/OS Client Web Enablement Toolkit adds new streaming send and receive functionality to support the sending of very large request and response bodies. Instead of the current requirement to have all data sent from and received into a single contiguous buffer, the streaming support allows an application to stage its sending and receiving into multiple buffers. This allows toolkit applications to send and receive a virtually unlimited amount of data. New optional streaming exits (streaming send and streaming receive) can be set to enable the streaming method of processing outgoing and incoming data. For both exits, the toolkit takes an input of buffers from the exit, sends from or receives into these buffers, and then drives the exit again to potentially receive new buffers for it to process until all the data has been processed. All languages except REXX are supported.

**When change was introduced:**
z/OS V2R3

**Reference information:**
- z/OS MVS Programming: Callable Services for High-Level Languages

**BCP (MVS) new functions to consider**

This topic describes the new features and function in the base control program (BCP), also called MVS.

**BCPii considerations**

The following BCPii function is new in z/OS V2R3:

- **z/OS BCPii performance improvements:** The z/OS BCPii HWIQUERY and HWILIST services have been enhanced to process capacity record and activation profile requests in a more efficient manner when the target CPC is at the IBM z13 GA2 level or later. This results in significantly faster response times for these two services when targeting the newer hardware levels. The functionality is available in z/OS V2.3, and in both z/OS V2.2 and z/OS V2.1 with a service update.
• **New z/OS BCPIi HWICMD2 service:** The existing HWICMD service has been enhanced with the introduction of the new HWICMD2 service. HWICMD2 has a new version number parameter that allows the caller to indicate to BCPIi which command parameter mapping it should use to process the command request. The LOAD, SCSILOAD, and SCSIDUMP commands have been enhanced to have a new version of the command parameters to allow for 5-character IPL device addresses. This enhancement also enables future enhancements to specific commands to either accept additional parameters or to change the sizes of its parameters. The functionality is available in z/OS V2.3, and in both z/OS V2.2 and z/OS V2.1 with a service update.

• **z/OS BCPIi support for larger data returned from SE:** z/OS BCPIi has been updated to allow the receipt of larger amounts of data coming from the SE, alleviating buffer storage shortages that can arise when querying hardware attributes that return significant amounts of data. Even large data, such as the engineering change / MCL information attribute (HWI_EC_MCL_INFO), will no longer experience problems on the HWIQUERY service. The functionality is available in z/OS V2.3, and in both z/OS V2.2 and z/OS V2.1 with a service update.

• **z/OS BCPIi support for absolute capping for a single LPAR:** The z/OS BCPIi HWIQUERY and HWISET services have been updated to support LPAR absolute capping attributes, which are supported when targeting a CPC at the zEC12 GA2 level or later. The new image and image activation profile attributes allow an LPAR's absolute capping status (enablement or disablement) as well as the LPAR's absolute capping value (maximum usage capacity) to be both queried and set for every processor type. The functionality is available in z/OS V2.3, and in both z/OS V2.2 and z/OS V2.1 with a service update.

• **z/OS BCPIi support for absolute capping for an LPAR group:** The z/OS BCPIi HWIQUERY and HWISET services have been updated to support absolute capping attributes for an LPAR group, which are supported when targeting a CPC at the z13 GA2 level or later. The new image attributes allow an LPAR group's absolute capping status (enablement or disablement) as well as the LPAR group's absolute capping value (maximum usage capacity) to be both queried and set for every processor type.

• **z/OS BCPIi support for Dynamic CPC name change:** z/OS BCPIi exploits a new enhancement in the firmware on zEC12 and z13 CPCs to allow an installation to dynamically change the name of the CPC in the HMC network while BCPIi has active connections to that CPC. When BCPIi detects that either the local CPC has changed its name or that a request going to a remote CPC no longer is targeting the same physical machine, BCPIi terminates all connections associated with the affected CPC and broadcasts a name change ENF event to notify all parties on the local image that the CPC name change has occurred.

• **New z/OS BCPIi HWISET2 service:** The existing HWISET service has been enhanced with the introduction of the new HWISET2 service to allow for multiple attributes to be set on a single API call. This support can provide quicker adjustments to multiple attributes in the hardware configuration, helping to reduce periods of potential configuration inconsistency when setting a single attribute at a time. An additional benefit of this support is having a "two-phase commit" like behavior where either all changes or none of the changes are made when targeting a CPC at the z13 GA2 level or later.

**When change was introduced:** z/OS V2R3 or V2R4, as indicated in the preceding paragraphs.

**Reference information:** z/OS MVS Programming: Callable Services for High-Level Languages.

### CEA considerations

The following Common Event Adapter (CEA) function is new in z/OS V2R3.

**Remote TSO/E Address Space Manager**

**Description:** A calling application can create and log in to a TSO/E address space on a different system in the sysplex (a remote system). This support allows users of z/OSMF ISPF plug-in and exploiters of the TSO/E address space manager (TSOASMgr) services to create TSO/E address spaces on another system in the sysplex. The TSOASMGR services use XCF to perform communications between the caller and the remote TSO/E address space.

This support, Version 2, allows the caller to work with any system in the sysplex. This support differs from the prior version (Version 1) of TSOASMGR services, which allowed sessions to be created only on the system on which the function was invoked (the local system).
Applications that use the version 1 support work directly with z/OS UNIX queues to implement message queuing. The Version 2 support uses CEA for message queuing. This function requires the use of the new APIs to perform queue functions.

To use the new functions to access other systems in the sysplex, the application must be modified or created to use the new version (version 2) of the APIs. With this change, message passing is done through CEA APIs and no longer directly with z/OS UNIX queues.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS MVS Programming: Callable Services for High-Level Languages
- z/OS MVS System Messages, Vol 4 (CBD-DMO)

### Consoles considerations

This topic describes new consoles function in z/OS.

**Shared consoles support removal**

**Description:** In z/OS V2R1, the statement of direction was updated to indicate that z/OS V2R2 would be the last system level to support shared mode for consoles. The concept of shared mode is eliminated from z/OS V2R3. IPL parameters and command syntax no longer accept shared or distributed mode. For compatibility, the options are ignored with a message indicating they are no longer supported.

**When change was introduced:** z/OS V2R3.

**Reference information:**
- z/OS MVS System Commands
- z/OS MVS Initialization and Tuning Reference
- z/OS MVS Diagnosis: Reference
- z/OS MVS System Messages, Vol 6 (GOS-IEA)
- z/OS MVS Planning: Operations

### IBM Function Registry for z/OS considerations

This topic describes new function for IBM Function Registry for z/OS.

**Using and registering functions with the IBM Function Registry for z/OS**

**Description:**

IBM Function Registry for z/OS provides a simple way to find and enable functions on a z/OS system. A function is anything provided by IBM or a vendor within any z/OS product (such as, for IBM, XCF or CICS). For example, a function registered with the IBM Function Registry for z/OS could be representing a particular service or an operational mode a product offers.

The IBM Function Registry for z/OS provides:

- Information about registered functions, such as whether a function is available on the system, whether it has been enabled, whether it has been used, and optionally, how often it has been used.
- Ways to enable and disable registered functions within a product. For example, users might want to disable new registered functions shipped in the service stream.

Note that the IBM Function Registry for z/OS is simply a repository of information about functions. It is not a legal instrument, nor is it related to usage rates, or licensing.

**Release introduced:**

z/OS V2R3.
Reference information:

- If you are using the IBM Function Registry for z/OS to find functions, get information about functions, or enable and disable functions, see the topic on using IBM Function Registry for z/OS in z/OS MVS Programming: Authorized Assembler Services Guide.

- If you want to register your function with the IBM Function Registry for z/OS, see the topic on registering functions in the IBM Function Registry for z/OS in z/OS MVS Programming: Authorized Assembler Services Guide.

IOS considerations

This topic describes new function for Input/Output Supervisor in z/OS.

SuperPAV dynamic alias management

Description:
SuperPAV is an extension of the HyperPAV architecture and implements multiple logical subsystems (LSS) within an alias management group (AMG). With SuperPAV, when a new I/O request occurs and there are no alias PAV devices available in the alias pool for the base PAV device's LSS, z/OS attempts to use an alias PAV device from another LSS within the AMG subgroup.

SuperPAV may provide some relief for systems that experience I/O queue time (IOSQ) during periods of peak I/O load. When a small number of aliases have been defined in an LSS, it is possible that during a heavy I/O period, no aliases might be available. z/OS may then check peer LSS alias pools to borrow an alias to start I/O requests that previously would have been left queued because no aliases were available.

Release introduced:
z/OS V2R2 with APAR OA49090 applied.

Reference information:
- z/OS HCD Planning
- z/OS MVS Initialization and Tuning Reference
- z/OS MVS System Commands
- z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG

Real Storage Manager (RSM) considerations

This information describes new RSM features and functions in z/OS.

Restricted use common service area (RUCSA)

Description:
For installations that cannot eliminate user-key (8 - 15) common storage usage, RUCSA provides a way to isolate user-key common storage to a select set of users, thus controlling or eliminating the security risk associated with common user-key storage.

When change was introduced:
z/OS V2R4

Reference information:
- z/OS MVS Initialization and Tuning Guide
- z/OS MVS Initialization and Tuning Reference
IARV64 GETSTOR enhancement

Description:
For programs that need to obtain private storage starting at a specific virtual address to meet alignment-sensitive needs, the IARV64 REQUEST=GETSTOR service now provides an INORIGIN parameter. You can use the INORIGIN parameter to obtain this storage without exceeding the virtual area of certain virtual range areas, such as 2GTO64GAREA or LOCALSYSAREA.

When change was introduced:
z/OS V2R4

Reference information:
• z/OS MVS Programming: Assembler Services Reference IAR-XCT
• z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG

Frame management enhancements

Description:
Before z/OS V2R3, real memory was carved into various pools of different frame sizes (4 KB frames, quad frames, 1 MB pageable, and fixed frames, and 2 GB frames) and frame types (preferred frames, and reconfigurable frames). With a few exceptions, requests for a certain frame size/type could use real memory from other frame sizes/types when the primary frame size/type was depleted. As more frame sizes/types were introduced, this frame management system became complex. With z/OS V2R3, the system no longer designates pools of real memory for most frame sizes (2 GB pages is the exception). There is now just one pool that supports all frame size requests (minus 2 GB pages). With this frame management system, a larger pool of real memory can be used for whatever frame size the current workload demands.

As a result of these frame management changes:
• The LFAREA INCLUDE1MAFC(NO) specification in IEASYSxx is no longer applicable. Since there is no designated pool of real memory created as a result of a 1 M LFAREA specification, all real storage is always included in the available frame count (RCEAFC). The INCLUDE1MAFC keyword is still parsed, but effectively ignored.
• The number of available pageable 1 MB frames in the system is no longer limited to approximately one-eighth of real memory above the 2 GB bar. There is no longer a designated pool of real memory for pageable 1 MB frames. As such, the number of pageable 1 MB frames available is only limited to the amount of available real memory installed on the system (minus any defined 2 GB frames and reconfigurable frames).

When change was introduced:
z/OS V2R3

Reference information:
• z/OS MVS Initialization and Tuning Reference.
• z/OS MVS Initialization and Tuning Guide.
• z/OS MVS System Messages, Vol 6 (GOS-IEA).

IARV64 PAGEFIX / PAGEUNFIX enhancement

Description:
The IARV64 service is used to request 64-bit storage. Using the PAGEFRAMESIZE keyword, users can request that the storage is backed with pageable 1 MB frames, if available. Before z/OS V2R3, when backed with pageable 1 MB frames, certain IARV64 PAGEFIX invocations can result in demotion of the pageable 1 MB frame into 256 pageable 4 KB frames.

This can occur when:
• The starting address of the data to be acted on is not on a megabyte boundary (RANGLIST, VSA).
• The number of 4 K frames to be acted on is not a multiple of 256 (RANGLIST, NUMPAGES).
With z/OS V2R3, these restrictions no longer apply. IARV64 PAGEFIX requests against storage backed with pageable 1 MB frames no longer causes demotions in the above scenarios. In addition, IARV64 PAGEUNFIX requests that do not start on a megabyte boundary or do not specify a multiple of 256 4 K frames are supported.

**Note:** This is the 64-bit follow-on of the PGSER FIX/FREE enhancement that is introduced in z/OS V2R2. The z/OS V2R2 enhancement addressed 31-bit address space storage backed with pageable 1 MB frames. It allowed PGSER FIX/FREE requests that do not start on a megabyte boundary or do not specify a length in megabyte multiples to be processed without resulting in the demotion of the pageable 1 MB frame.

**When change was introduced:**

z/OS V2R3

**Reference information:**

- z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG.

**System logger considerations**

The following enhancements are made to system logger.

**z/OS System Logger support for encrypted log stream data sets**

**Description:**

An enhancement to the System Logger component is planned to allow data set level encryption for log stream data sets. Log stream data level encryption is established when system logger creates a new log stream data set using new specifications in either a DFSMS data class definition for extended format type, or through RACF data set profiles.

**Release introduced**

z/OS V2R3

**Reference information:**

- z/OS MVS Setting Up a Sysplex
- z/OS MVS System Messages, Vol 10 (IXC-IZP)
- z/OS Release Upgrade Reference Summary

**Logstream staging datasets greater than 4GB**

**Description:**

System Logger allows logstream staging datasets to be allocated greater than 4GB in size in z/OS Version 2 Release 3. The new allowable maximum staging dataset size is 16TB - for example, 16384GB or 17,592,186,044,416 bytes.

Allowing larger logstream dataset sizes, provides for greater scalability in the higher availability and recoverability logstream configuration. Installations can get an improved tuned log data flow through their logstreams.

**Release introduced**

z/OS V2R3

**Reference information:**

- z/OS MVS Setting Up a Sysplex
- z/OS Upgrade Workflow
- z/OS MVS Programming: Assembler Services Guide
- z/OS MVS Programming: Assembler Services Reference IAR-XCT
- z/OS MVS System Commands
- z/OS MVS System Messages, Vol 10 (IXC-IZP)
- z/OS Release Upgrade Reference Summary
Unicode considerations

This topic describes new Unicode function in z/OS.

• **INITCAP case conversion** - INITCAP case conversion support is now available in z/OS V2R3.
• **Unicode standard 9.0** - Unicode standard 9.0 support is now available in z/OS V2R3.

**When change was introduced:** z/OS V2R3.

**Reference information:**

• [z/OS Unicode Services User's Guide and Reference](#)

XES/XCF considerations

This topic describes new XES and Cross-System Coupling Facility (XCF) functions in z/OS.

**Cross-System Coupling Facility (XCF) enhancements for z/OS V2R4**

**Description:** XCF improvements in z/OS V2R4 include:

• **Transport Class Simplification:** XCF transport classes no longer need to be defined to segregate signals purely by size. The number of signal paths only needs to be appropriate for the workload. XCF ensures that signal throughput and timely transfer are maintained for the signal workload independent of any particular transport class configuration.

  - There is a new XCF switch XTCSIZE to enable or disable the new behavior. There is a new XCF defined pseudo-transport class named _XCFMGD that is used to report XCF signal activity when the new behavior is enabled. You obtain the new behavior only when both the sender and target systems are running on z/OS V2R4 (and the XTCSIZE switch is enabled).
  
  - There are new metrics available using XCF accounting and measurement services (IXCMG and IXCYAMDA) that are intended to provide additional information to help understand the number of signal paths that are needed. Specifically, there are new metrics to describe signal path utilization and signal transfer delays induced by inbound signal path "no buffer" conditions.

For more information, see [z/OS MVS Setting Up a Sysplex](#).

**When change was introduced:** z/OS V2R4.

**Cross-System Coupling Facility (XCF) enhancements for z/OS V2R3**

**Description:** XCF/XES improvements in z/OS V2R3 include:

• **Encryption of coupling facility structure user data:** XES provides support to secure customer information by encrypting customer data while it is being transferred to and from the coupling facility (CF) and while it resides in the coupling facility.

  - Use new ENCRYPT administrative data utility parameter to control the desired encryption state for each CF structure in the CFRM policy.
  
  - Use new parameter ENCRYPTKEY on the SETXCF MODIFY command to change encryption keys for CF structures.
  
  - Use new parameters on the DISPLAY XCF to filter structures by encryption state.
  
  - Use new check XCF_CF_STR_ENCRYPT to verify that structure data in an allocated structure is consistent with the effective ENCRYPT parameter and cryptographic encryption key for the structure (when the structure data is encrypted) in the CFRM policy.

For more information, see the section on encrypting coupling facility structure data in [z/OS MVS Setting Up a Sysplex](#).

**When change was introduced:** z/OS V2R3.
Communications Server new functions to consider

The following section covers Communications Server function by type and support considerations.

Support considerations

Description: z/OS Communications Server includes the following enhancement for support considerations.

- **Support considerations in V2R3** - Support for the following functions is discontinued.
  - Several TCP/IP device drivers:
    - FDDI and Token Ring (LCS with LINKs FDDI and IBMTR)
    - Token Ring (MPCIPA with LINK IPAQTR)
    - Ethernet and FDDI (MPCOSA with LINKs OSAENET and OSAFDDI)
  
    You must migrate from these device types to later types, such as OSA-Express QDIO and HiperSockets.

  Note: Support for SNA device drivers is not affected.

  - The Trivial File Transfer Protocol function. Anyone using this function should use an alternate file transfer protocol.

  - Simple Mail Transport Protocol Network Job Entry (SMTPD NJE) mail transport

  - Sendmail mail transport

  - Several migration health checks:
    - ZOSMIGV2R2_NEXT_CS_LEGACYDEVICE
    - ZOSMIGV2R2_NEXT_CS_TFTP
    - CSAPP_SMTPD_MAIL_RELAY
    - ZOSMIGV2R2_NEXT_CS_SENDMAILCLIEN
    - ZOSMIGV2R2_NEXT_CS_SENDMAILDAEMN
    - ZOSMIGV2R2_NEXT_CS_SENDMAILMSA
    - ZOSMIGV2R2_NEXT_CS_SENDMAILMTA
    - ZOSMIGV2R2_NEXT_CS_SMTPDDAEMON
    - ZOSMIGV2R2_NEXT_CS_SMTPDMTA

When change was introduced: z/OS V2R3

Reference information: See the following topic in z/OS Communications Server: New Function Summary for detailed descriptions that include any applicable restrictions, dependencies, and steps on using the functions:

- **Support considerations in V2R3**

Hardware support

Description: z/OS Communications Server includes the following enhancements for hardware:

- **Communications Server miscellaneous enhancements** - Starting with z/OS Communications Server V2R4, read errors, if any, on the OSA inbound queues are displayed under the queue ID when VTAM TRLE display commands are issued.

  When change was introduced: z/OS V2R4

- **Communications Server support for OSA-Express7S 25 GbE features** - z/OS V2R4 Communications Server is enhanced to support the OSA-Express7S feature with 25 GbE bandwidth.
When change was introduced: z/OS V2R4 and with the PTFs for APARs PI95703 and OA55256 for z/OS V2R3

- **Communications Server support for 25 GbE RoCE Express2 features** - z/OS Communications Server V2R3 is enhanced to support IBM 25 GbE RoCE Express2 features.

When change was introduced: z/OS V2R3

- **Shared Memory Communications - Direct Memory Access** - Significant performance improvements are provided for TCP protocol workloads that are deployed on the same IBM Z® CPC. This solution uses Shared Memory Communications - Direct Memory Access (SMC-D) for TCP connections to local peers which also support this function.

**Incompatibilities:** This function does not support IPAQENET and IPAQIDIO interfaces that are defined by using the DEVICE, LINK, and HOME statements. Convert your IPAQENET and IPAQIDIO definitions to use the INTERFACE statement to enable this support.

**Dependencies:**
- This function requires an IBM z13® GA2 level of hardware.
- This function requires at least one Internal Shared Memory (ISM) device that is configured in the Hardware Configuration Definition (HCD).

When change was introduced: z/OS V2R3 and with the PTFs for APARs OA48411 and PI45028 for z/OS V2R2

- **Communications Server support for RoCE Express2 features** - z/OS Communications Server extends the Shared Memory Communications over Remote Direct Memory Access (SMC-R) function to support the next generation IBM 10 GbE RoCE Express2® feature. The IBM 10 GbE RoCE Express2® feature allows TCP/IP stacks on different LPARs within the same central processor complex (CPC) to leverage the power of these state-of-the-art adapters to optimize network connectivity for mission critical workloads by using Shared Memory Communications technology.

**Incompatibilities:** This function does not support IPAQENET interfaces that are defined by using the DEVICE, LINK, and HOME statements. Convert your IPAQENET definitions to use the INTERFACE statement to enable this support.

**Dependencies:** This function requires the IBM z14 or later systems.

When change was introduced: z/OS V2R3 and with the PTFs for APARs OA51950 and PI75200 for z/OS V2R2 and with the PTF for APAR OA51949

**Reference information:** See the following topics in *z/OS Communications Server: New Function Summary* for detailed descriptions that include any applicable restrictions, dependencies, and steps on using the functions:

- **Communications Server miscellaneous enhancements**
- **Communications Server support for OSA-Express7S 25 GbE features**
- **Communications Server support for 25 GbE RoCE Express2 features**
- **Shared Memory Communications - Direct Memory Access**
- **Communications Server support for OSA Express6S**
- **Communications Server support for RoCE Express2 features**

**Usability and skills**

z/OS Communications Server includes the following enhancements for usability and skills:

- **HiperSockets Converged Interface support** - z/OS Communications Server provides HiperSockets Converged Interface (HSCI) solution to support the z/VM bridge environment. With this solution, a Linux guest can connect to z/OS via Layer 2 HiperSockets and to the external network by using a single IP interface. This support also significantly improves HiperSockets usability by dynamically provisioning and activating a HiperSockets interface when an OSD interface is activated for the same physical network ID (PNetID). With this support, the TCP/IP stack only sees the OSD interface. This design
approach greatly reduces the network administration costs as HiperSockets interfaces no longer are required to be configured, operated, or managed in z/OS Communications Server. This solution allows a single IP interface (OSD) to provide access to the external Ethernet LAN and transparent access to HiperSockets for LPAR to LPAR communications within the central processor complex (CPC). This solution also eliminates the need to reconfigure z/OS HiperSockets interfaces when moving a z/OS instance from one CPC to another. The HSCI is also referred to as an IQDC interface.

**Incompatibilities:**

- This function does not support IPAQENET interfaces that are defined by using the DEVICE, LINK, and HOME statements. Convert your IPAQENET definitions to use the INTERFACE statement to enable this support.
- This function also requires the virtual MAC (VMAC) operand be specified on your IPAQENET interfaces to request OSA-generated VMACs.

**Dependencies:**

- This function minimally requires a zEnterprise EC12 (zEC12).
- This function requires an Internal Queued Direct I/O (IQD) channel path ID (CHPID) configured with the external bridge function.

**When change was introduced:** z/OS V2R4 and with the PTFs for APARs PI83372 and OA53198 for z/OS V2R3

- **z/OS Configuration Assistant for Communications Server support for import of TCP/IP configuration** - The Configuration Assistant for z/OS Communications Server includes TCP/IP technology, with which you can create and manage TCP/IP profiles. You can import your current TCP/IP stack profiles into the Network Configuration Assistant, to help you transition to using the Network Configuration Assistant for your TCP/IP profile management.

  **Dependencies:** z/OSMF is required to be installed and running in your network, with the Configuration Assistant for z/OS Communications Server plug-in installed.

  **When change was introduced:** z/OS V2R3 and with the PTFs for Configuration Assistant APAR PI66143 and TCP/IP APAR PI63449 for z/OS V2R2

- **Enhanced wildcard support for jobnames on PORT and PORTRANGE statements** - The wildcard support is enhanced for the jobname parameter on the PORT and PORTRANGE TCP/IP configuration statements. Asterisks can be used in any position to indicate zero or more unspecified characters. The question mark can be used in any position to indicate a single unspecified character.

  **When change was introduced:** z/OS V2R3

**Reference information:** See the following topics in *z/OS Communications Server: New Function Summary* for detailed descriptions that include any applicable restrictions, dependencies, and steps on using the functions:

- **HiperSockets Converged Interface support**
- **z/OS Configuration Assistant for Communications Server support for import of TCP/IP configuration**
- **Enhanced wildcard support for jobnames on PORT and PORTRANGE statements**

**Scalability and performance**

z/OS Communications Server includes the following enhancements for scalability and performance:

- **Sysplex notification of TCP/IP stack join or leave** - z/OS V2R4 has enhanced Event Notification Facility code 80 to send a signal when a stack joins or leaves a sysplex group.

  **When change is introduced:** z/OS V2R4

- **Network support for z/OS Container Extensions** - z/OS Container Extensions provides native z/OS support for Linux Docker based application workloads. The Communications Server support provides network support for z/OS Container Extensions workloads by introducing a new type of DVIPA called a zCX DVIPA. The zCX DVIPA represents an instance of a Docker server allowing TCP/IP to provide unique
IP routing and apply various TCP/IP QoS functions for container workloads running within each Docker server address space.

The Communications Server VTAM support introduces a new type of zCX network transport that dynamically provides optimized internal network connectivity from each Docker server address space ID (ASID) to TCP/IP for providing access to and from the external network. The VTAM support also introduces the z/OS Container Extensions Direct Network Interface Component (DNIC) that provides a Virtual NIC for the Docker server virtualization environment.

**When change was introduced:** z/OS V2R4

- **IWQ support for IPSec** - z/OS Communications Server is enhanced to support inbound workload queueing for IPSec workloads for OSA-Express in QDIO mode. Inbound workload queueing uses multiple input queues for each QDIO data device (subchannel device) to improve TCP/IP stack scalability and general network optimization. To implement the performance improvements for IPSec workloads, enable inbound workload queueing to process IPSec, EE, sysplex distributor, and streaming bulk data traffic all concurrently with other types of inbound QDIO traffic. When you enable these improvements for a QDIO interface, inbound IPSec, EE, sysplex distributor, and streaming bulk data traffic are each processed on their own ancillary input queue (AIQ). All other inbound traffic is processed on the primary input queue.

**Incompatibilities:** This function does not support IPAQENET interfaces that are defined by using the DEVICE, LINK, and HOME statements. Convert your IPAQENET definitions to use the INTERFACE statement to enable this support.

**Dependencies:**

- This function is limited to OSA-Express6S Ethernet features or later in QDIO mode running on IBM z14”. For more information about the QDIO inbound workload queueing function and the OSA-Express features that support it, see “QDIO inbound workload queueing” in z/OS Communications Server: IP Configuration Guide. See the 3906DEVICE or 3907DEVICE Preventive Service Planning (PSP) bucket for more information.
- This function is supported only for interfaces that are configured to use a virtual MAC (VMAC) address.

**When change was introduced:** z/OS V2R4 and with the PTF for APAR PI77649 for z/OS V2R3

- **Improved control over default VTAM VIT options** - Two levels of operator control are provided for managing VTAM Internal Trace (VIT) internal mode record collection:
  
  - You can use “Full VIT control” to control the use of all VIT options, at any time, using VTAM start options or the MODIFY TRACE and MODIFY NOTRACE commands. This includes the ability to disable all internal mode VIT recording. The DISPLAY TRACE command always displays the current settings of all VIT options.
  
  - You can use “Base VIT control” to allow VTAM to enforce that certain VIT options (API, CIO, MSG, NRM, PIU and SSCP) remain active at all times. The DISPLAY TRACE command displays the settings of these VIT options only if you have explicitly enabled the options, otherwise the settings are not displayed. This is the default behavior, and this was the only level of VIT control provided originally.

**Restriction:** The two levels of VIT control apply to internal mode recording only. External mode recording of VIT records is unchanged regardless of the level of VIT control used for internal mode recording.

**When change was introduced:** z/OS V2R3 and with the PTF for APAR OA50271 for z/OS V2R2

- **Sysplex-wide security associations (SWSA) scalability improvement** - Sysplex-wide security associations (SWSA) scalability is improved by increasing the number of lists that can be configured for the EZBDVIPA coupling facility structure. In previous releases, the EZBDVIPA structure had a fixed number of lists (2048 lists). With this enhancement, the number of lists in the EZBDVIPA structure can be configured with up to 16,384 lists. This allows more IPSec security associations to be distributed and taken over.

**Restriction:**
– All VTAMs in a sysplex or a VTAM subplex must be at z/OS V2R3 or later before the number of lists for an EZBDVIPA structure can be increased above 2048 lists.
– The number of lists that are configured for an EZBDVIPA structure must be the same for all VTAMs in a sysplex or a VTAM subplex. If the configured number of lists is different, the actual number of lists is unpredictable. IPSec distribution and takeover data can be inaccessible to some TCP/IP stacks in the sysplex or VTAM subplex, potentially resulting in errors.

**When change was introduced:** z/OS V2R3

**Reference information:** See the following topics in *z/OS Communications Server: New Function Summary* for detailed descriptions that include any applicable restrictions, dependencies, and steps on using the functions:

- Network support for z/OS Container Extensions
- IWQ support for IPSec
- Improved control over default VTAM VIT options
- Sysplex-wide security associations (SWSA) scalability improvement

**Systems management**

**Description:** z/OS Communications Server includes the following enhancements for systems management:

- **Communications Server support for enhanced system symbols** - The use of MVS system symbols is enhanced to support the underscore character as a valid character in symbol names and to support longer symbol substitution values.

**When change was introduced:** z/OS V2R3

**Reference information:** See the following topics in *z/OS Communications Server: New Function Summary* for detailed descriptions that include any applicable restrictions, dependencies, and steps on using the functions:

- Communications Server support for enhanced system symbols

**Enhancing security**

z/OS Communications Server includes the following security enhancements:

- **AT-TLS support for TLS v1.3** - z/OS V2R4 Communications Server adds support for TLS Version 1.3 for Application Transparent Transport Layer Security (AT-TLS). This includes support for the following new TLSv1.3 cipher suites: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, and TLS_CHACHA20_POLY1305_SHA256.

z/OS V2R4 Communications Server enhances the z/OS Encryption Readiness Technology (zERT) function to detect and report TLSv1.3 security session information using SMF Type 119 subtype 11 and 12 records. The IBM zERT Network Analyzer z/OSMF plug-in is also enhanced to accept and display TLSv1.3 information and to allow IBM zERT Network Analyzer users to query database content using the new TLSv1.3 security session characteristics.

**Restrictions:**

Support for TLS Version 1.3 is provided only for AT-TLS. Native TLS support for the FTP server and client, the TN3270E server, and DCAS is not updated to support TLSv1.3.

**Incompatibilities:**

– The cipher suites supported for TLS Version 1.2 and earlier are not supported for TLS Version 1.3. And the cipher suites supported for TLS Version 1.3 are not supported by earlier versions of TLS. If TLSv1.3 and earlier versions are enabled, the configured list of supported cipher suites must include values supported for TLSv1.3 and values supported by earlier TLS versions.
– The FIPS 140-2 standard does not define support for TLSv1.3 or the new cipher suites defined for it. Enabling both the TLSv1.3 protocol and FIPS support results in an error.
Dependency:
The Integrated Cryptographic Services Facility (ICSF) must be active to provide support for all TLSv1.3 cipher suites.

When change was introduced: z/OS V2R4

• IBM zERT Network Analyzer - IBM zERT (z/OS Encryption Readiness Technology) Network Analyzer is a web-based graphical user interface that z/OS network security administrators can use to analyze and report on data reported in zERT Summary records.

Dependency:
– You must have installed z/OSMF to use IBM zERT Network Analyzer.
– The IBM zERT Network Analyzer task requires either Db2 11 for z/OS or Db2 12 for z/OS.

When change was introduced: z/OS V2R4 and with the PTFs for zERT Network Analyzer V2R3 APAR PH03137 and z/OSMF V2R3 APARs PH04391 and PH00712

• z/OS Encryption Readiness Technology (zERT) aggregation - z/OS Communications Server introduced a new function called z/OS Encryption Readiness Technology (zERT). With zERT, the TCP/IP stack acts as a focal point in collecting and reporting the cryptographic security attributes of IPv4 and IPv6 application traffic that is protected using the TLS/SSL, SSH, and IPSec cryptographic network security protocols. The collected connection level data is written to SMF in SMF 119 subtype 11 records. If the volume of SMF 119 subtype 11 records can be large, z/OS V2R4 Communications Server provides an alternative SMF view of the collected security session data. This alternative view is written in the form of new SMF 119 subtype 12 records that summarize the use of security sessions by many application connections over time and which are written at the end of each SMF interval. This alternative view condenses the volume of SMF record data while still providing all the critical security information.

Restrictions:
The following restrictions apply to both zERT discovery and zERT aggregation functions.

zERT collects information for TCP and Enterprise Extender (EE) connections. Information is not collected for non-EE UDP traffic or traffic using other IP protocols.

zERT collects cryptographic security attributes for the TLS, SSL, SSH, and IPSec protocols. No other cryptographic security protocols are supported.

The following z/OS cryptographic protocol providers are fully enabled for zERT: z/OS Communications Server IPSec and AT-TLS, z/OS Cryptographic Services System SSL, and z/OS OpenSSH. Detailed security attribute data is available for connections using these protocol providers. Other TLS, SSL, and SSH implementations running on z/OS are monitored through stream observation only. A limited amount of security attribute data is available for these connections.

For information on the specific cases where security attribute data is limited or unavailable, see zERT discovery limitations in z/OS Communications Server: IP Configuration Guide.

Dependency: To properly monitor IBM Sterling Connect:Direct traffic when it is protected through SecurePlus TLS/SSL support, apply Connect:Direct APAR PI77316.

When change was introduced: z/OS V2R4 and with the PTF for APAR PI83362 for z/OS V2R3

• TN3270E Telnet server ELF support for MFA - The TN3270 Telnet server Express Logon Feature (ELF) is extended to support IBM Multi-Factor Authentication (MFA) for z/OS. With this support, TN3270 clients can experience the same single sign-on behavior that is already offered by the PassTicket-based ELF, but now via an MFA token that is assigned by a SAF-compliant external security manager like IBM Security Server RACF. With the new EXPRESSLOGONMFA parameter in the TN3270E Telnet server profile, ELF attempts to authenticate clients by using their X.509 client certificate through MFA. If no MFA token is available for the user, the authentication fails by default. ELF can be configured to revert back to PassTicket authentication in certain cases where MFA authentication is unsuccessful.

Dependencies:
– IBM Security Server RACF APAR OA53002
IBM Multi-Factor Authentication for z/OS APAR PI86470 and PI93341

When change was introduced: z/OS V2R4, and z/OS V2R3 with the PTFs for APAR PI85185, RACF APAR OA53002, and IBM MFA for z/OS APARs PI86470 and PI93341

- AT-TLS currency with system SSL - Application Transparent TLS (AT-TLS) is enhanced to support the following features provided by System SSL.
  - Support for NIST SP800-131A (key length transition recommendations). Add support for higher security strengths (larger key sizes) as defined in NIST SP800-131A, which allows a more secure FIPS 140-2 implementation.
  - Support for NIST SP800-52A Revision 1 (TLS implementation guidelines) which adds new certificate processing controls.
  - Support for several RFCs governing OCSP (RFC 6066, RFC 6277, RFC 6960 and RFC 6961)
  - Support for RFCs regarding Suite B Profile clarifications (RFCs 6460 and 5759)
  - Support for Signaling Cipher Suite Values (SCSV) to protect against protocol downgrade attacks (RFC 7507).

When change was introduced: z/OS V2R3

- z/OS Encryption Readiness Technology (zERT) - z/OS Encryption Readiness Technology (zERT) is a new capability provided by the z/OS V2R3 Communications Server. With zERT, the TCP/IP stack acts as a focal point in collecting and reporting the cryptographic security attributes of IPv4 and IPv6 application traffic that is protected using the TLS/SSL, SSH and IPSec cryptographic network security protocols. The collected connection level data is written to SMF in new SMF 119 subtype 11 records for analysis.

Restrictions:

zERT collects cryptographic security attributes for TCP and Enterprise Extender (EE) connections. Information is not collected for non-EE UDP traffic or traffic that uses other IP protocols.

zERT collects cryptographic security attributes for the TLS, SSL, SSH, and IPsec protocols. No other cryptographic security protocols are supported.

The following z/OS cryptographic protocol providers are fully enabled for zERT: z/OS Communications Server IPSec and AT-TLS, z/OS Cryptographic Services System SSL, and z/OS OpenSSH. Detailed security attribute data is available for connections using these protocol providers. Other TLS, SSL, and SSH implementations running on z/OS are monitored through stream observation only. A limited amount of security attribute data is available for these connections.

For information on the specific cases where security attribute data is limited or unavailable, see zERT discovery limitations in z/OS Communications Server: IP Configuration Guide.

Dependency: To properly monitor IBM Sterling Connect:Direct traffic when it is protected through SecurePlus TLS/SSL support, apply Connect:Direct APAR PI77316.

When change was introduced: z/OS V2R3

- IBM Health Checker for z/OS FTP ANONYMOUS JES - A new IBM Health Checker for z/OS application health check is provided to help determine whether your FTP server allows anonymous users to submit jobs. When ANONYMOUS is enabled, it is recommended that ANONYMOUSLEVEL be set to 3 and ANONYMOUSFILETYPEJES be set to FALSE. Otherwise, anonymous users can submit jobs to run on the system.

Dependency: You must start the IBM Health Checker for z/OS to use the new application health check.

When change was introduced: z/OS V2R3 and with the PTF for APAR PI47637 and OA49668 for z/OS V2R2

- IBM Health Checker for z/OS MVRSHD RHOSTS DATA - A new IBM Health Checker for z/OS application health check is provided to help determine whether your MVRSHD server is active and whether RSH clients are using RHOSTS.DATA datasets for authentication. The MVRSHD server supports the RSH and REXEC protocols which transfer user ID and password information in the clear. There is also the potential of weak authentication for RSH clients using RHOSTS.DATA datasets. This
authentication method allows remote command execution without requiring the RSH client to supply a password.

**Dependency:** You must start the IBM Health Checker for z/OS to use the new application health check.

**When change was introduced:** z/OS V2R3 and with the PTF for TCP/IP APAR PI51640 and SNA APAR OA50122 for z/OS V2R2

**IBM Health Checker for z/OS SNMP agent public community name** - A new IBM Health Checker for z/OS application health check is provided to help determine whether your SNMP agent is configured with a community name of public. Because the SNMP community name of public is a well-known name, it should not be used with community-based security due to security considerations.

**Dependency:** You must start the IBM Health Checker for z/OS to use the new application health check.

**When change was introduced:** z/OS V2R3 and with the PTF for APAR PI51640 and OA50122 for z/OS V2R2

**SMF 119 TCP connection termination record (subtype 2) enhanced to provide IP filter information** - IP filter information is provided in the SMF 119 TCP connection termination record (subtype 2). The name of the IP filter rules associated with inbound and outbound traffic for a connection are included in a new section of the record, if IP filtering is being done for a connection. The data is also available through the SYSTCPCN real-time network monitoring interface (NMI).

**Restrictions:**

The IP filter section is included if IP filtering is active and an IP filter rule applies to the traffic. The IP filter section is not included for intra-host connections because IP filtering is not done for those connections.

The filter rule information reflects the IP filter rules in place at the time that the connection is terminated. If IP filter policy changes while a connection is active, only the names of the IP filter rules in place at the time of the termination are included.

**Dependency:**

SMF configuration option TCPTERM must be configured on the SMFCONFIG TCP/IP profile statement for the SMF 119 TCP connection termination record (subtype 2) to be generated.

The TCPCONNSERVICE parameter must be configured on the NETMONITOR TCP/IP profile statement for the SMF 119 TCP connection termination data to be available through the SYSTCPCN real-time NMI interface.

**When change was introduced:** z/OS V2R3 and with the PTF for APAR PI69920 for z/OS V2R2

**VTAM 3270 intrusion detection services** - 3270 data stream intrusion detection services (IDS) is enabled to detect and act on violations of the 3270 data stream protocol. The 3270 IDS function monitors all 3270 data streams for primary logical units (PLUs) that are connected to the z/OS VTAM instance. Specific types of 3270 sessions can be exempted from IDS monitoring at the VTAM or application major node level if IDS monitoring is not needed for those sessions.

The 3270 IDS function monitors 3270 data streams for any attempt to write past the end of input fields or to modify protected fields. When these types of events are detected, appropriate actions are taken according to the VTAM configuration. The possible actions include logging the event, tracing the relevant inbound and outbound PIUs for later analysis, notifying the PLU of the event with a sense code, and even terminating the SNA session.

**When change was introduced:** z/OS V2R3 and with the PTF for APAR OA49911 for z/OS V2R2

**Reference information:** See the following topics in *z/OS Communications Server: New Function Summary* for detailed descriptions that include any applicable restrictions, dependencies, and steps on using the functions:

- AT-TLS support for TLS v1.3
- IBM zERT Network Analyzer
- z/OS Encryption Readiness Technology (zERT) aggregation
Application development

z/OS Communications Server includes the following enhancements for application, middleware, and workload enablement:

- **Communications Server miscellaneous enhancements** - The Resolver caching function provided users with the ability to set a maximum time-to-live (TTL) value for cached Domain Name System (DNS) name server information, but the MAXTTL resolver setup statement applied to all types of cached DNS name server entries. Starting with z/OS V2R4 Communications Server, users can specify two different maximum TTL values: a new MAXNEGTTL resolver setup statement for negative cache entries and the existing MAXTTL resolver setup statement for all other cache entries. In addition, the output of the MODIFY RESOLVER,DISPLAY|REFRESH command is enhanced to include the name of the most recently used resolver setup file.

  **When change was introduced:** z/OS V2R4

- **Code page enhancements for CSSMTP** - z/OS V2R4 Communications Server is enhanced to support multi-byte character sets with the Communications Server SMTP (CSSMTP) application. This enhancement allows migration from SMTPD to CSSMTP for customers that use multi-byte character set code pages, and provides improved code page support for characters in the mail subject line.

  **When change was introduced:** z/OS V2R4 and with the PTF for APAR PI93278 for z/OS V2R3

- **CSSMTP customizable ATSIGN character for mail addresses** - The Communications Server SMTP (CSSMTP) application is enabled to recognize a different character as the industry standard at sign (@) symbol in a mail address. The specified character is recognized as the at sign symbol only in the SMTP commands and headers in mail messages. This enhancement simplifies migration from SMTPD to CSSMTP for customers that use a code page other than the default IBM-1047 and that have modified mail generation programs to generate mail addresses with an at sign character other than @.

  **When change was introduced:** z/OS V2R3 and with the PTF for APAR PI52704 for z/OS V2R2

- **Improved CSSMTP code page compatibility with target servers** - z/OS V2R3 Communications Server enables the Communications Server SMTP (CSSMTP) application to use a code page other than the standard ISO8859-1 code page to send mail messages to a target server. With this support, CSSMTP can send mail messages with special characters, such as the Euro sign (€), embedded in the body of the mail message in the code page expected by the mail server.

  **Restriction:** The commands and headers of a mail message are first translated to code page IBM-1047 and then to the code page that is configured for the target server. Characters in the headers might not be translated correctly.

  **When change was introduced:** z/OS V2R3 and with the PTF for APAR PI73909 for z/OS V2R2

- **Improved CSSMTP TLS compatibility with mail servers** - The Communications Server SMTP (CSSMTP) application is enabled to optionally send an EHLO command after a successful TLS negotiation. RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security) specifies that sending an EHLO command is optional for a SMTP client after a successful TLS negotiation. However, some SMTP servers require an EHLO command after a successful TLS negotiation. To accommodate these servers, a configuration option is provided to enable the sending of an EHLO command after a successful TLS negotiation.

  **When change was introduced:** z/OS V2R3 and with the PTF for APAR PI56614 for z/OS V2R2
• **sendmail to CSSMTP bridge** - z/OS V2R3 Communications Server removes support for z/OS UNIX sendmail. The z/OS sendmail to CSSMTP bridge (sendmail bridge) is provided to emulate sendmail so that z/OS UNIX users can still use the sendmail command to send the mail message. The sendmail bridge parses input options from the command line, reads the mail message from the UNIX System Services file, and processes the mail message. The input mail message is updated by adding SMTP commands and SMTP headers if there is no header specified in the input mail message. The updated mail message is transmitted to the JES spool data set for the Communications Server SMTP (CSSMTP) application to process.

**When change was introduced:** z/OS V2R3 and with the PTF for APAR PI71175 for z/OS V2R2

• **Communications Server support for 8 character TSO User IDs** - z/OS V2R3 Communications Server is enhanced to support a maximum TSO/E user ID size of eight characters.

**When change was introduced:** z/OS V2R3

• **IPv6 getaddrinfo() API standards compliance** - The z/OS Resolver GetAddrInfo API is enhanced. The new enhancement allows the Resolver to return both IPv4 and IPv6 addresses when the following settings are true:
  - `AF_UNSPEC` is specified for `ai_family` type.
  - `AI_ALL` flag is not specified.
  - IPv6 is enabled on the z/OS system.

**When change was introduced:** z/OS V2R3

**Reference information:** See the following topics in *z/OS Communications Server: New Function Summary* for detailed descriptions that include any applicable restrictions, dependencies, and steps on using the functions:

• **Communications Server miscellaneous enhancements**
• **Code page enhancements for CSSMTP**
• **CSSMTP customizable ATSIGN character for mail addresses**
• **Improved CSSMTP code page compatibility with target servers**
• **Improved CSSMTP TLS compatibility with mail servers**
• **sendmail to CSSMTP bridge**
• **Communications Server support for 8 character TSO User IDs**
• **IPv6 getaddrinfo() API standards compliance**

---

**Cryptographic Services new functions to consider**

This topic describes new Cryptographic Services functions in z/OS.

**ICSF**

This topic describes new ICSF function in z/OS.

**ICSF: Enhancements for Crypto Express5S (CCA Release 5.4 and later) and Crypto Express6S (CCA Release 6.2 and later)**

**Description:** Enhancements include:

• ISO-4 format PIN blocks as described in the ISO-9564-4 standard. In addition to a new service, PIN Translate 2 (CSNBPTR2), the following services are updated to support ISO-4 format PIN blocks: Clear PIN Encrypt (CSNBCPE), DK PIN Verify (CSNBDKPV), DK PIN Change (CSNBDKPC), and DK PAN Modify in Transaction (CSNBKDSTM).

• Three-key TDES Keys. Currently, only DATA key types are available in 3-key TDES key types. This enhancements allows for the following key types to be operational as a 3-key TDES key: CIPHER,
ENCIPHER, DECIPHER, EXPORTER, IMPORTER, MAC, MACVER, IPINENC, OPINENC, PINGEN, and PINVER.

- DK Key Diversification: The German Banking Industry Committee (GBIC) introduced a new key diversification scheme such that a single diversification key can be used to generate keys with different key usage attributes. A new key type is introduced, KDKGENKY, as well as a new callable service Diversify Directed Key (CSNBDDK). The following callable services are updated in support of DK Key Diversification: Diversified Key Generate 2 (CSNPDK2), Key Token Build 2 (CSNBKT2), and Key Generate 2 (CSKBKGN2).

- ISO-20038 Key Wrapping: In support of the ISO-20038 standard, the TR-31 Import (CSNBTR31I) and TR-31 Export (CSNBTR31X) callable services are updated to use AES IMPORTER and EXPORTER key types for key wrapping.

- Crypto Express6S, in addition to the enhancements above, symmetric keys can now be restricted from being eligible for CPACF protected key. With updated flags in the control vector, it is possible to mark a key as either eligible or ineligible for being exported for CPACF use as a protected key. In addition, CCA provides the ability for 3-key TDES keys to be “tagged” such that they are restricted to PCI HSM compliance usage.

**When change was introduced:** PTF for APAR OA55184, rolled into the base of Cryptographic Support for z/OS V2R2 - z/OS V2R3 (FMID HCR77D0) and z/OS V2R4.

**Reference information:**
- z/OS Cryptographic Services ICSF Overview
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide
- z/OS Cryptographic Services ICSF Messages

**ICSF: CCA redirection for Regional Crypto Enablement**

**Description:** Certain CCA callable services have the ability to direct the request to a regional crypto server. This enhancement introduces the concept of "RCS Redirection" through a new XFACILIT resource, and adds the concept of an "RCS Token" to existing symmetric key token types.

**When change was introduced:** PTF for APAR OA54132, rolled into the base of Cryptographic Support for z/OS V2R2 - z/OS V2R3 (FMID HCR77D0) and z/OS V2R4.

**Reference information:**
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide
- z/OS Cryptographic Services ICSF Messages

**ICSF: ChaCha20 and Poly1305 algorithms**

**Description:** These new algorithms are available via the PKCS#11 interfaces and clear key only.

**When change was introduced:** Cryptographic Support for z/OS V2R2 - z/OS V2R3 (FMID HCR77D0) and z/OS V2R4.

**Reference information:**
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide
- z/OS Cryptographic Services ICSF Writing PKCS #11 Applications
ICSF: Dynamic Service update: Applying service to a running ICSF instance without causing an interruption to your applications

Description: ICSF has a new operator command that allows running requests to finish, pause incoming requests, prepare to restart with the service libraries, and then stop ICSF. Through system automation (preferred), ICSF is restarted and the paused requests are resumed without a visible interruption.

When change was introduced: Cryptographic Support for z/OS V2R2 - z/OS V2R3 (FMID HCR77D0) and z/OS V2R4.

Reference information:
- z/OS Cryptographic Services ICSF Overview
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer’s Guide
- z/OS Cryptographic Services ICSF System Programmer’s Guide
- z/OS Cryptographic Services ICSF Messages

ICSF: Early ICSF availability

Description: ICSF is now able to start much earlier in the IPL process, such that ICSF should be available for work as early as full function start. ICSF also added new ways to provide installation options via a more standard PARMLIB interface.

When change was introduced: Cryptographic Support for z/OS V2R2 - z/OS V2R3 (FMID HCR77D0) and z/OS V2R4.

Reference information:
- z/OS Cryptographic Services ICSF Application Programmer’s Guide
- z/OS Cryptographic Services ICSF System Programmer’s Guide
- z/OS Cryptographic Services ICSF Messages

ICSF: KGUP and SAF profile prefixing

Description: KGUP can now be made to honor CSFKEYS resource profiles and can be configured to require higher permission when performing destructive operations on an existing key (such as UPDATE or DELETE). In addition, CSFKEYS resources can now permit a user or group to a CSFKEYS resource (but only for specific callable services), and the CSFSERV and CSFKEYS resources can now have ICSF prepend a system name resource name prior to the SAF check.

When change was introduced: Cryptographic Support for z/OS V2R2 - z/OS V2R3 (FMID HCR77D0) and z/OS V2R4.

Reference information:
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer’s Guide
- z/OS Cryptographic Services ICSF System Programmer’s Guide
- z/OS Cryptographic Services ICSF Messages

ICSF: New BSI mode (BSI 2017)

Description: A new compliance mode, BSI 2017, has been added to the EP11 Coprocessor.

When change was introduced: Cryptographic Support for z/OS V2R2 - z/OS V2R3 (FMID HCR77D0) and z/OS V2R4.

Reference information:
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer’s Guide
- z/OS Cryptographic Services ICSF System Programmer’s Guide
- z/OS Cryptographic Services ICSF Messages
- z/OS Cryptographic Services ICSF Writing PKCS #11 Applications
ICSF: Updates to PKCS#11 Wrap Key (CSFPWPK) and PKCS#11 Unwrap Key (CSFPUWK)

**Description:** Callable services PKCS#11 Wrap Key (CSFPWPK) and PKCS#11 Unwrap Key (CSFPUWK) have been updated to accept AES-GCM as a key wrapping mechanism for secret and private clear keys.

**When change was introduced:** Cryptographic Support for z/OS V2R2 - z/OS V2R3 (FMID HCR77D0) and z/OS V2R4.

**Reference information:**
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide
- z/OS Cryptographic Services ICSF Writing PKCS #11 Applications

ICSF: New DISPLAY ICSF, MKVPs operator command

**Description:** A new DISPLAY ICSF, MKVPs operator command is used to display the master key verification patterns recorded in the ICSF key data stores in comparison with the same MKVPs in online crypto coprocessors in such a way that discrepancies can be detected.

**When change was introduced:** Cryptographic Support for z/OS V2R2 - z/OS V2R3 (FMID HCR77D0) and z/OS V2R4.

**Reference information:**
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide

ICSF: CCA service algorithm updates

**Description:** ICSF provides these additional Common Cryptographic Architecture (CCA) support:
- Support for the RSAES-OAEP format for the PKA Decrypt and PKA Encrypt callable services.
- Support in the Key Generate callable service for the CIPHER, DATAC, and DATAM key types in the OP, IM, or EX key forms.
- Operational Key Load support for HMAC keys loaded from the TKE workstation.
- Limiting length of Master key verification patterns displayed on the ICSF Hardware Status panel.
- Access control point offsets displayed on the Domain Role panel.

**When change was introduced:** PTFs for APAR OA47781, rolled into the base of Cryptographic Support for z/OS V1R13 - z/OS V2R2 web deliverable (HCR77B1), and z/OS V2R3.

**Reference information:**
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide

ICSF: Cryptographic services enhancements

**Description:** ICSF provides these cryptographic services enhancements:
- Support for a new key check value using CMAC algorithm for Key Test2 (CSNBKYT2).
- Support for AES Galois/Counter mode encryption for Symmetric Algorithm Encipher (CSNBSAE) and Symmetric Algorithm Decipher (CSNBSAD) services.
- Support for a new key derivation algorithm for EC Diffie-Hellman (CSNDEDH) service.
- Support for a new Encrypted PIN Translate Enhanced (CSNBPTRE) callable service to support PAN that is encrypted using format preserving encryption.

This support requires a minimum microcode level (MCL) for Crypto Express5S coprocessors on IBM z13 and later processors.
When change was introduced: PTF for APAR OA49064, rolled into the base of Cryptographic Support for V2R1 - z/OS V2R2 web deliverable (HCR77C0), and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide

ICSF: Digital Signature Generate and Digital Signature Verify enhancements

Description: The Digital Signature Generate (CSNDDSG) and Digital Signature Verify (CSNDDSV) callable services have been enhanced to take as input the message to be signed or verified as well as the prehashed message that is already supported.

When change was introduced: Cryptographic Support for z/OS V2R1 - z/OS V2R2 web deliverable (HCR77C0) and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Application Programmer's Guide

ICSF: EMV simplification services

Description: ICSF provides new callable services that simplify EMV payment processing:
- Derive ICC MK (CSNBDCM and CSNEDCM).
- Derive Session Key (CSNBDSK and CSNEDSK).
- EMV Scripting Service (CSNBESC and CSNEESC).
- EMV Transaction (ARQC/ARPC) Service (CSNBESC and CSNEESC).
- EMV Verification Functions (CSNBVEF and CSNEEVF).
- Generate Issuer MK (CSNGBIM and CSNEGIM).

When change was introduced: PTFs for APAR OA47016, rolled into the base of Cryptographic Support for z/OS V1R13 - z/OS V2R2 web deliverable (HCR77B1), and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Overview
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide

ICSF: Enhanced PKCS#11 Secret Key Encrypt and PKCS#11 Secret Key Decrypt

Description: Enhancement to PKCS#11 Secret Key Encrypt (CSFPSKE) and PKCS#11 Secret Key Decrypt (CSFPSKD) callable services to support clear key AES ciphertext stealing, specifically CS1.

When change was introduced: Cryptographic Support for z/OS V2R1 - z/OS V2R2 web deliverable (HCR77C0) and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF Writing PKCS #11 Applications

ICSF: Enhancements for Crypto Express5

Description: ICSF exploits new algorithm support and extends existing support for asymmetric algorithms as well as:
- The Digital Signature Generate (CSNDDSG), Digital Signature Verify (CSNDDSV), and PKA Key Token Build (CSNDPKB) callable services support RSA-PSS Signatures to provide higher assurance and stronger signature support.
• The PKA Key Generate (CSNDPKG) and PKA Key Token Build (CSNDPKB) callable services support selectable public exponents in the generation of RSA private/public key pairs.

This support requires a minimum microcode level (MCL) for Crypto Express5S coprocessors on IBM z13 and later processors.

**When change was introduced:** Cryptographic Support for z/OS V2R1 - z/OS V2R2 web deliverable (HCR77C0) and z/OS V2R3.

**Reference information:**
- z/OS Cryptographic Services ICSF Overview
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide

**ICSF: FIPS 140-2 certification of PKCS11**

**Description:** ICSF added four new callable services which allows SSL to exploit ICSF’s FIPS compliant PKCS#11 services for RSA operations. Rather than specifying a handle to an existing PKCS#11 key object, these services accept ASN.1 clear key structures. The new services are:

• PKCS #11 Private key structure decrypt (CSFPPD2 and CSFPPD26).
• PKCS #11 Private key structure sign (CSFPPPS2 and CSFPPS26).
• PKCS #11 Public key structure encrypt (CSFPPE2 and CSFPPE26).
• PKCS #11 Public key structure verify (CSFPVV2 and CSFPVV26).

**When change was introduced:** PTFs for APAR OA50113 and rolled into the base of Cryptographic Support for z/OS V2R1 - z/OS V2R2 web deliverable (HCR77C0) and z/OS V2R3.

**Reference information:**
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide
- z/OS Cryptographic Services ICSF Writing PKCS #11 Applications

**ICSF: Improved Key Lifecycle and Key Usage auditing**

**Description:** ICSF has improved Key Lifecycle and Key Usage auditing to assist with audit compliance and understanding of the state of keys within an environment.

**When change was introduced:** Cryptographic Support for z/OS V2R1 - z/OS V2R2 web deliverable (HCR77C0) and z/OS V2R3.

**Reference information:**
- z/OS Cryptographic Services ICSF System Programmer's Guide
- z/OS Cryptographic Services ICSF Messages

**ICSF: Key Encryption Translate**

**Description:** ICSF provides new callable service Key Encryption Translate (CSNBKET). The CSNBKET service changes the method of encryption of DES key material.

**When change was introduced:** PTFs for APAR OA49443, rolled into the base of Cryptographic Support for V2R1 - z/OS V2R2 web deliverable (HCR77C0), and z/OS V2R3.

**Reference information:**
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide
ICSF: New ICSF_OPTIONS_CHECKS health check

Description: ICSF added a new health check, ICSF_OPTIONS_CHECKS, to verify that certain ICSF options are set to the expected values during initialization.

When change was introduced: PTFs for APAR OA48452, rolled into the base of Cryptographic Support for V2R1 - z/OS V2R2 web deliverable (HCR77C0), and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Messages

ICSF: Operator commands

Description: New operator commands with Parallel Sysplex wide scope, if needed, that can be used to perform certain cryptographic administrative functions:
- Activating, deactivating, and restarting cryptographic coprocessors.
- Displaying status for available cryptographic devices.
- Displaying information about active key data sets (KDSs).

When change was introduced: Cryptographic Support for z/OS V1R3 - z/OS V2R2 (HCR77B1) and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide

ICSF: Options Data Set Refresh function

Description: Use the Options Data Set Refresh function through the SETICSF command or the ICSF Multi-Purpose service (CSFMPS) to remove the need for restarting ICSF and prevent outages.

When change was introduced: Cryptographic Support for z/OS V2R1 - z/OS V2R2 web deliverable (HCR77C0) and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide
- z/OS Cryptographic Services ICSF Messages

ICSF: Regional crypto enablement

Description: ICSF can communicate with network attached cryptographic hardware as long as that hardware adheres to the IBM Enterprise PKCS#11 (EP11) interface specification and can be authenticated by an IBM supplied certificate. ICSF added support for Chinese specific encryption and hashing algorithms SM2, SM3, and SM4.

This support requires a vendor based hardware solution as associated with feature code (0901) Regional Crypto Enablement (RCE) and associated software from the vendor.

When change was introduced: PTF for APAR OA49069, rolled into the base of Cryptographic Support for V2R1 - z/OS V2R2 web deliverable (HCR77C0), and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Overview
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide
- z/OS Cryptographic Services ICSF Messages
ICSF: Support for German Banking Industry defined PIN processing functions

Description: ICSF provided additional Common Cryptographic Architecture (CCA) support for German Banking Industry defined PIN processing functions. These functions include three types of AES key derivation as well as AES Secure Messaging Keys, which can be used in AES-based EMV transactions. This support requires a minimum microcode level (MCL) for Crypto Express4S and Crypto Express5S coprocessors on EC12 and later processors.

When change was introduced: PTFs for APAR OA46466, rolled into the base of Cryptographic Support for z/OS V1R13 - z/OS V2R2 web deliverable (HCR77B1), and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide

ICSF: Support for secure key tokens in Field Level Encipher and Field Level Decipher

Description: ICSF allows encrypted key tokens that are not stored in the CKDS to be specified for the key identifier parameter of the Field Level Encipher (CSNBFLE and CSNEFLE) and Field Level Decipher (CSNBFLD and CSNEFLD) callable services.

When change was introduced: PTF for APAR OA51102 and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Overview
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide

ICSF: Unsupported key detection

Description: ICSF provides two ways to easily identify unsupported keys:

- The ICSF Health Check, ICSF_UNSUPPORTED_CCA_KEYS, displays a list of records in the active CKDS and PKDS that are no longer supported.
- The Key Data Set List (CSFKDSL) callable service provides an option that generates a list of records in the active key data sets of keys that are no longer supported.

When change was introduced: Cryptographic Support for z/OS V2R1 - z/OS V2R2 web deliverable (HCR77C0) and z/OS V2R3.

Reference information:
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF System Programmer's Guide

PKI Services

This topic describes new PKI Services function in z/OS.

PKI Services Enrollment over Secure Transport (EST)

Description: PKI Services Enrollment over Secure Transport (EST) permits PKI to support the certificate enrollment protocol standardized in RFC7030, which is a successor protocol to Simple Certificate Enrollment Protocol (SCEP). Cisco IOS Software and Cisco IOS XE support protocol.

When change was introduced: z/OS V2R4

Reference information:
- z/OS Cryptographic Services PKI Services Guide and Reference
PKI synchronous certificate fulfillment

**Description:** PKI synchronous certificate fulfillment enables the web page interface to generate a synchronous certificate request. When the requestor obtains a transaction ID the certificate has been generated and the requestor can pick up the certificate immediately as the function provides a switch to request certificate synchronously through the PKI Services web interface.

**When change was introduced:** z/OS V2R4

**Reference information:**
- z/OS Cryptographic Services PKI Services Guide and Reference
- z/OS Security Server RACF Callable Services

PKI RSAPSS algorithm support

**Description:** PKI RSAPSS algorithm support permits PKI Services to validate requests and sign issued certificates using the RSA Probabilist Signature Scheme (RSASSA-PSS). RSAPSS algorithms using SHA-256, SHA-384, and SHA512 hasing algorithms are supported.

**When change was introduced:** z/OS V2R4

**Reference information:**
- z/OS Cryptographic Services PKI Services Guide and Reference
- z/OS Security Server RACF Callable Services

PKI Services SCEP usability

**Description:** Enables the client name of the preregistration record to be retained in the SCEP request and SCEP certificate.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS Cryptographic Services PKI Services Guide and Reference

PKI Services FIPS support

**Description:** Enables PKI Services to operate in the FIPS level specified.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS Cryptographic Services PKI Services Guide and Reference

PKI Services Liberty support

**Description:** Enables PKI Services to run on WebSphere® Liberty.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS Cryptographic Services PKI Services Guide and Reference

PKI Services DB2 Optimization

**Description:** Enables PKI Services to shut down or to stay on to wait for DB2’s availability to resume its functions.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS Cryptographic Services PKI Services Guide and Reference
System SSL

This topic describes new System SSL function in z/OS.

System SSL: PKCS #7 signed data message has been enhanced to support detached (external) signatures

Description: System SSL supports the creation of a detach signature style SignData message. A detached signature SignedData message is a message where the content or application data is included in the data when the digital signatures are generated, but are not included in the final SignedData message.

When change was introduced: z/OS V2R4 and with the PTF for APAR OA54821 for z/OS V2R3.

Reference information:
- z/OS Cryptographic Services System SSL Programming

System SSL: RSASSA-PSS support

Description: System SSL supports a number of signature algorithms and extends support to RSA Signature Scheme with Appendix-Probabilistic Signature Scheme (RSASSA-PSS) operations.

When change was introduced: z/OS V2R4.

Reference information:
- z/OS Cryptographic Services System SSL Programming

System SSL: TLS 1.3 support

Description: System SSL supports the TLS V1.3 protocol so that TLS applications can be protected with the most current TLS protocol and continue to inter-operate with other TLS V1.3 applications.

When change was introduced: z/OS V2R4.

Reference information:
- z/OS Cryptographic Services System SSL Programming

System SSL: FIPS enforcement

Description: System SSL provides FIPS 140-2 security levels that can be specified by the application to enforce different cryptographic strengths.

When change was introduced: z/OS V2R3

Reference information: z/OS Cryptographic Services System SSL Programming
- z/OS Cryptographic Services System SSL Programming

System SSL: GSKIT V4 CMS certificate store

Description: System SSL supports certificates and certificate keys that are stored in GSKIT V4 CMS certificate stores. A GSKIT V4 CMS certificate store is used by System SSL as a means to identify certificates and certificate keys to be used when establishing a SSL/TLS secure connection.

When change was introduced: z/OS V2R3

Reference information: z/OS Cryptographic Services System SSL Programming
- z/OS Cryptographic Services System SSL Programming

System SSL: Server Key Label List

Description: System SSL allows multiple certificates to be specified for use by a server when the server is negotiating secure connections. This ability allows a server to be able to negotiate with a wide range of clients with varying SSL capabilities that might require more than one type of certificate to be used.

When change was introduced: z/OS V2R3
System SSL: Standards Currency

**Description:** System SSL supports RFC 5759, RFC 6277, RFC 6460, RFC 6818, RFC 6960, RFC 6961, and RFC 7507 to keep current with the standards:

- **GSK_SUITE_B_PROFILE** is updated to support the setting of the 128MIN and 192MIN profiles.
- **GSK_SERVER_FALLBACK_SCSV** is a new attribute type and environment variable that allows server applications the ability to accept the Signaling Cipher Suite Value (SCSV) when included in the client's cipher list.
- **GSK_OCSP_RESPONSE_SIGALG_PAIRS** specifies a signature algorithm pairs list in preference order that can be used by the OCSP responder to sign the OCSP response.
- **GSK_SERVER_OCSP_STAPLING** is a new environment variable and attribute type that is supported in the gsk_attribute_set_enum() routine, which allows the server application the ability to specify support for the 'Certificate Status Request' or 'Multiple Certificate Status Request' extensions.
- **GSK_TLSEXT_SERVER_OCSP_STAPLING** is a new enum type that is supported in the gsk_attribute_get_enum() routine to determine whether the 'Certificate Status Request' or 'Multiple Certificate Status Request' extension was negotiated on the connection.
- **GSK_SERVER_OCSP_STAPLING_CERTSTATUS** is a new enum type that is supported in the gsk_attribute_get_enum() to query if the server sent a CertificateStatus message.

**When change was introduced:** z/OS V2R3

**Reference information:** z/OS Cryptographic Services System SSL Programming

### DFSMS new functions to consider

This topic describes new DFSMS functions in z/OS.

### DFSMS device support new functions

This topic describes new DFSMS device support functions in z/OS.

### DFSMS device support enhancements for z/OS V2R3

DFSMS device support provides the following enhancement:

**Access to Read-only DASD devices**

DFSMS provides read-only access to data sets on DASD devices that have been defined as read-only using HCD.

For more information about accessing data sets on read-only devices, including the types of data sets and access methods supported, see [z/OS DFSMS Using Data Sets](https://www.ibm.com). Applications might need to provide specific keywords when allocating and opening data sets on read-only devices. For details, see information about the DALROAC and DALROA2 text units in [z/OS MVS Programming: Authorized Assembler Services Guide](https://www.ibm.com), the ROACCESS keyword on the JCL DD statement in [z/OS MVS JCL Reference](https://www.ibm.com), and the CONCURRENTRW keyword in the DCBE at OPEN.

The DEVTYPE macro will return the read-only device attributes in the copy of the UCBTYP field. The programmer should consult the IECDUCBD macro to define the three new bits returned by DEVTYPE.

### Advanced Copy Services new functions

This topic describes new Advanced Copy Services functions in z/OS.
Advanced Copy Services enhancements for z/OS V2R3

z/OS V2R3 adds the following Advanced Copy Services enhancement:

- Support for extent space efficient volumes. Extent space efficient volumes, also commonly called thin provisioned volumes, have no physical space allocated to them until the first write is done to the volume. Physical space is allocated on demand to the volume in extents, directly from the extent pool where the volume is defined, rather than on a track by track basis from a space efficient repository. This improves the performance of space efficient volumes. Extent space efficient volumes are not limited to being FlashCopy targets, and their FlashCopy relationships are not limited to NOCOPY. No special keywords are required to create FlashCopy or PPRC relationships with extent space efficient volumes.

DADSM/CVAF new functions

This topic describes new DADSM/CVAF functions in z/OS.

DADSM/CVAF enhancements for z/OS V2R3

- A new CVAFDIR ACCESS=WRITE parameter checks to insure the caller did not accidentally change fields that could corrupt the VTOC or cause the Index to be disabled.

Validate=(YES,NO) performs a comparison of the existing Data Set Control Blocks (DSCBs) with the ones passed by the caller, prior to updating the VTOC.

You can use VALIDATE=YES with CVAFDIR ACCESS=WRITE to ensure essential fields in the DSCB are not being modified. Refer to z/OS DFSMSdfp Advanced Services for more information.

DFSMS catalog new functions

This topic describes new DFSMS catalog functions in z/OS.

DFSMS catalog enhancements for z/OS V2R3

DFSMS provides the following enhancements:

Catalog enhancements

- **IDCAMS small enhancements:** The DEFINE CLUSTER command has a new zFS parameter which specifies that the cluster being defined is for linear data, and the linear data set is a z/OS UNIX File System. When zFS is specified, the linear data set is defined as extended addressable. LISTCAT will display

  ZFS when the data set is LINEAR and zFS indicator flag is on, or when the zFS initialized flag is on.

DFSMSdss new functions

This topic describes new DFSMSdss functions in z/OS.

DFSMSdss enhancements for z/OS V2R3

z/OS V2R3 introduces the following enhancements for DFSMSdss:

- New keywords on the DUMP command let you backup DASD data to an object storage cloud. See the section on backing up data sets, and descriptions of the CLOUD, CLOUDCREDENTIALS, CONTAINER, OBJECTPREFIX, and DEBUG keywords for the DUMP command, in z/OS DFSMSdss Storage Administration.

- New and updated keywords on the RESTORE command let you restore backed up DASD data from an object storage cloud. See the section on restoring data sets, and descriptions of the CLOUD, CLOUDCREDENTIALS, CONTAINER, OBJECTPREFIX, and DEBUG keywords for the RESTORE command in z/OS DFSMSdss Storage Administration.

- The new SPACEREL command is added, allowing you to release physical space associated with free space extents on specified extent space efficient (ESE) volumes.
• The maximum number of data sets that can potentially reside in a logical data set backup is increased, from 131,070 to 2,147,483,392. For more information, see z/OS DFSMS Using the New Functions.

• A reason code has been added to message ADR383W, to identify specific causes for a data set not being selected and specific actions to be taken.

**DFSMShsm new functions**

This topic describes new DFSMShsm functions in z/OS.

**DFSMShsm enhancements for z/OS V2R3**

DFSMShsm provides the following enhancements:

• **DFSMS UNIX file backup**

  APAR OA52703 provides DFSMS backup of UNIX files. This support gives you the ability to perform availability management of your z/OS UNIX files using DFSMSdss and DFSMShsm command.

• **Common recover queue (CVQ) enhancements**

  With this enhancement, storage administrators have the ability to distribute the processing of volume restores (RECOVER *, FRRECOV COPYPOOL, and FRRECOV TOVOLUME with FROMDUMP) to all DFSMShsm tape resources available in a group of DFSMShsm hosts. New parameters on the SETSYS COMMONQUEUE command define the common recover group and its members (hosts) in the HSMplex. The HOLD, RELEASE, QUERY, CANCEL, and ALTERPRI commands all now support this function. XCF system facilities are used to provide this support. Message simplification supports a host running a common recover queue.

• **Message simplification**

  To simplify the analysis of fast replication errors during FRBACKUP, FRRECOV COPYPOOL and copy pool auto dump, and FRRECOV TOVOLUME FROMDUMP, DFSMShsm now collects all related DFSMShsm and DFSMSdss messages and records them in a unique fast replication message data set. (These messages continue to be recorded in their respective logs.) You can choose and control this option with the new MESSAGEDATASET(YES|NO HLQ(\hlq)) parameters on the SETSYS FASTREPLICATION command.

  For more information, refer to SETSYS command in z/OS DFSMShsm Storage Administration.

  On the FRBACKUP and FRRECOV COPYPOOL commands, use a MESSAGEDATASET parameter to specify the date and time used in the message data set name. The message simplification function supports distributed tape processing, common dump queue, and common recover queue processing.

  MESSAGEDATASET is an optional parameter that allows you to specify the date and time used in the name of the fast replication command message data set. Specifying the date and time ensures that you can identify the message data set that corresponds with the FRRECOV request. If you don't specify the date and time with the MESSAGEDATASET parameter, DFSMShsm uses the date and time when the message data set name is generated.

  For more information, refer to the FRRECOV command in z/OS DFSMShsm Storage Administration.

**DFSMSrmm new functions**

This topic describes new DFSMSrmm functions in z/OS.

**DFSMSrmm enhancements for z/OS V2R3**

The functional enhancements available with z/OS V2R3 DFSMSrmm provide you with these benefits:

• **DFSMSrmm operational enhancements**
  
  - *Specify expiration time for added volumes and data sets:* The ADDDATASET, ADDVOLUME, and GETVOLUME subcommands have been enhanced to enable the user to specify the time (in hhmmss format) that should be used, in addition to the date, when deciding when to expire volumes and data sets.
Specify that an added data set not expire while cataloged: A new WHILECATALOG option has been added to the EDGRMMxx parmlib member OPTION command and to the ADDDDATASET TSO subcommand to enable the user to specify either that:

- the added dataset will be kept as long as it is cataloged. If the dataset is uncataloged, it will still be kept if the expiration date has not been reached yet.
- the added dataset will be kept as long as it is cataloged, but no later than the expiration date.

**DFSMStvs new functions**

This topic describes new DFSMStvs functions in z/OS.

**DFSMStvs enhancements for z/OS V2R3**

DFSMStvs provides the following enhancement:

**Automatic commit support**

DFSMStvs provides a new parameter on the JCL EXEC statement that you can use to enable the automatic issuing of commit points on behalf of a batch application. The TVSAMCOM parameter lets you specify how many updates (an exact number or a range of numbers) should occur before a commit point is issued. You can also specify a default value for this parameter in the IGDSMSxx member of SYS1.PARMLIB.

For more information about using automatic commit, including the types of batch jobs that are good candidates for it, see z/OS DFSMStvs Planning and Operating Guide.

**DFSMS Object Access Method (OAM) new functions to consider**

This topic describes new DFSMS Object Access Method (OAM) functions in z/OS.

**Object Access Method (OAM) enhancements for z/OS V2R3**

z/OS DFSMS V2R3 provides the following enhancements to the Object Access Method (OAM):

- The LIBRARY DISPDRV command is enhanced with new MOUNTED and MOUNTED,ALL parameters to optionally display:
  - Status information for volumes that are mounted in the TS7700 Virtualization Engine for a specified composite or distributed library. Information pertaining to the distributed library that owns the device for the mount as well as distributed library information associated with the primary and the secondary tape volume cache (TVC) is displayed.
  - For a distributed library in a TS7700 Virtualization Engine, additional drives that are not owned by the specified distributed library can be displayed using MOUNTED,ALL. The additional drives are displayed if the distributed library specified is the primary or secondary TVC for the mounted volume. This option can be useful when a distributed library is going into service and can be used to determine if the specified distributed library is associated with a mount request from another distributed library.

This support was introduced with APAR OA47487 (z/OS V1R13 and above).

For more information, refer to z/OS DFSMS OAM Planning, Installation, and Storage Administration Guide for Tape Libraries.

**SMS new functions**

This topic describes new SMS functions in z/OS.

**SMS enhancements for z/OS V2R3**

SMS provides the following enhancements:
**SMS support for zHyperlink storage class granularity**

DFSMS supports the ability to specify whether data sets associated with a storage class are eligible to use zHyperLinks for reading and writing. zHyperlinks can dramatically reduce latency by interconnecting the z14 Central processor complex directly to the I/O bays in the IBM DS8880. This can improve application response time, without significant application changes. For more information, see the section "Defining use of zHyperlinks," in z/OS DFSMSdfp Storage Administration.

**SMS support for object storage clouds**

DFSMS supports the backup and retrieval of DASD data in object storage clouds, using DS8000 storage hardware. ISMF panel options allow you to define a cloud construct to DFSMS, which you can then specify on DFSMSdss and DFSMShsm commands to perform data backups and retrievals. For more information, see Defining clouds.

**SMS enhancements for z/OS V2R4**

SMS provides the following enhancements:

**Virtual storage constraint relief**

Prior to z/OS V2R4, each online DASD volume obtained a volume statistics block (VSB) which consumed 616 bytes of 31-bit common storage. In z/OS V2R4 (or earlier releases with APAR OA55711), each online DASD volume consumes 48 bytes in 31-bit common storage and an additional 896 bytes above the 2G bar. This change provides virtual storage constraint relief.

**DFSMS VSAM new functions**

This topic describes new DFSMS VSAM functions in z/OS.

**VSAM and VSAM RLS enhancements for z/OS V2R3**

z/OS V2R3 introduces the following enhancements for VSAM and VSAM RLS:

- Data set statistics block (DSSB) above the bar for VSAM data sets: In V2R3, the DSSB resides in 64-bit storage (“above the 2G bar”) for VSAM data sets. This change provides virtual storage constraint relief.

**DFSMS data set encryption new functions**

This topic describes new functions in DFSMS related to DASD data set level encryption in z/OS.

**DFSMS data set encryption enhancements for z/OS V2R3**

z/OS DFSMS introduces pervasive encryption of data at rest for extended format data sets accessed through access methods without requiring application changes. z/OS data set encryption through RACF command and SMS policies can be used to identify the data sets or groups of data sets that require encryption.

You can protect viewing the data in the clear based on SAF access to the key label that is associated with the data set used by the access methods to encrypt and decrypt the data. The data set owner specifies an encryption key label, which refers to an AES 256-bit encryption key that exists in the ICSF key repository (CKDS).

z/OS DFSMS data set encryption can be used to encrypt the following types of data sets:

- Sequential extended format data sets that are accessed through BSAM and QSAM.
- VSAM extended format data sets (KSDS, ESDS, RRDS, VRRDS, LDS) that are accessed through base VSAM and VSAM/RLS.

To create an encrypted data set, you must assign a key label to the data set when it is first allocated (that is, when the data set is created). A key label can be specified through any of the following methods:

- RACF data set profile
Encrypted data sets must be SMS-managed extended format; they can be in compressed format, also.

DFSMSe and DFSMShsm support backup and migration of encrypted data sets while preserving the data in encrypted form. You can identify data sets that are encrypted through interfaces, such as LISTCAT, IEHLIST LISTVTOC, ISMF, SMF, and DCOLLECT.

For an overview of restrictions, dependencies, and steps on using the new function, see the following publications:

**Note:** When change was introduced: z/OS V2R3 (Also V2R2 with APAR OA50569)

**References:**
- z/OS DFSMS Using the New Functions
- z/OS DFSMS Access Method Services Commands
- z/OS DFSMSdfp Storage Administration
- z/OS DFSMSdss Storage Administration
- z/OS DFSMShsm Storage Administration

---

### Hardware Configuration Definition (HCD) new functions to consider

New function, features, and support for Hardware Configuration Definition (HCD).

**HCD hardware support**

**Description:**

- Support of new PCIe functions:
  1. The processor supports a new PCIe function type called zHyperLink (HYL). They require a new PCIe function attribute for identifying a port on the adapter to which the function is related.
  2. The processor supports a new PCIe function type called RoCE-2 (ROC2). Similar to the existing RoCE adapter as it is a network adapter that supports a port attribute. Each port connects to one network and there can only be one PNETID being defined for that adapter.
- New chpid type - CL5
  - A new coupling link for extended distances is supported as a new chpid type CL5. The new adapter card (based on the RoCE adapter) is a mixture of a HCA (host communication adapter) and a 'normal' chpid. It is defined by a combination of PCHID and PORT attributes.
- Support for dynamically changing the I/O configuration of IBM Z servers that do not run HCD
  - HCD allows for processors with corresponding hardware support to remotely initiate a dynamic I/O configuration change for hardware-only changes. The functionality is for IBM Z servers that do not run an instance of z/OS or z/VM (for example: sandalone coupling facilities).

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS HCD User’s Guide
- z/OS and z/VM HCD Messages

### HCD processor support

**Description:** HCD supports the following IBM processor families:

- processor types 2964-N30, -N63, -N96, -NC9, -NE1 (new support level H161231)
Hardware Configuration Manager (HCM) new functions to consider

New function, features, and support for Hardware Configuration Manager (HCM).

HCM processor support

**Description:** HCM supports a new processor family (processor types 3906-M01, -M02, -M03, -M04, -M05) and a new processor family (processor type 3906-LM1, -LM2, -LM3, -LM4, -LM5).

**When change was introduced:** z/OS V2R3

**Reference information:**

z/OS and z/VM HCM User's Guide

HCM PCIe function enhancements

**Description:** HCM supports two new PCIe function types ZHYPERLINK and ROCE-2 are supported on the new processor family. The PCIe functions of type ZHYPERLINK and ROCE-2 require a PORT value.

**When change was introduced:** z/OS V2R3

**Reference information:**

z/OS and z/VM HCM User's Guide

HCM CHPID type enhancements

**Description:** HCM supports a new channel path (CHPID) type called CL5. The CL5 adapter is defined with a physical channel ID (PCHID) value and a PORT value.

**When change was introduced:** z/OS V2R3

**Reference information:**

z/OS and z/VM HCM User's Guide

IBM Tivoli Directory Server for z/OS new functions to consider

Enhanced SDBM search

**Description:**

The SDBM extended search mode offers enhanced search capabilities, including full search filter support, and the removal of 4096-line output restriction on searching the RACF profiles.

**Release introduced:**

z/OS V2R4

**Reference information:**

z/OS IBM Tivoli Directory Server Client Programming for z/OS
z/OS IBM Tivoli Directory Server Administration and Use for z/OS
**Enhanced activity logging**

**Description:**
To reduce resource contention, activity logging can be run in asynchronous mode if the LDAP server configuration has been customized with the new LogFileSync keyword.

**Release introduced:**
z/OS V2R4

**Reference information:**
/z/OS IBM Tivoli Directory Server Administration and Use for z/OS

---

**Transport Layer Security (TLS) protocol version 1.3**

**Description:**
In z/OS® V2R4, z/OS IBM® Tivoli® Directory Server introduces support for the TLS V1.3 protocol as specified in RFC 8446 to z/OS Cryptographic Services' System SSL component and to the z/OS Communications Server’s Application Transparent TLS (AT-TLS) function. This support is intended to make the latest and most secure TLS standard available to use by any z/OS System SSL application and any application that accesses System SSL through AT-TLS.

**When change was introduced:**
z/OS V2R4

**Reference information:**
/z/OS IBM Tivoli Directory Server Administration and Use for z/OS
/z/OS Cryptographic Services System SSL Programming
/z/OS Communications Server: IP Configuration Guide

---

**MFA Support**

**Description:** Multi-factor Authentication (MFA) is a new feature of RACF. The SDBM backend of the LDAP server provides an interface to RACF so that RACF profiles can be managed remotely through LDAP protocols. This line item provides MFA support for SDBM. It includes the following three capabilities:

- Allows users to input MFA credentials to RACF through an LDAP simple bind.
- Allows a RACF administrator to alter, search, or compare MFA data in a user profile through SDBM.
- Allows a RACF administrator to add, alter, search, or compare MFA policy data in a resource profile through SDBM.

**When change was introduced:** z/OS V2R3

**Reference information:**
/z/OS IBM Tivoli Directory Server Administration and Use for z/OS
/z/OS IBM Tivoli Directory Server Messages and Codes for z/OS

---

**Health Checks**

**Description:** The objective of the IBM Health Checker for z/OS is to identify potential problems before they impact availability or cause outages. LDAP users will benefit from a z/OS Health Check that notifies them if they deploy large directories in a TDBM backend. This line item delivers a TDBM health check to notify users when DB2® REORG or RUNSTATS utilities should be run to avoid performance issues.

**When change was introduced:** z/OS V2R3

**Reference information:**
/z/OS IBM Tivoli Directory Server Administration and Use for z/OS
/z/OS IBM Tivoli Directory Server Messages and Codes for z/OS
FIPS Compliant

**Description:** This line item provides improved security capability in secure sockets communication within the LDAP server. Cryptographic Services System SSL augmented FIPS support to enable the specification of a security strength level when FIPS mode is enabled. FIPS mode enablement is required when LDAP client and server communications are over an SSL/TLS protected TCP/IP socket connection.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS IBM Tivoli Directory Server Administration and Use for z/OS
- z/OS IBM Tivoli Directory Server Client Programming for z/OS
- z/OS IBM Tivoli Directory Server Messages and Codes for z/OS

Multi-Row Fetch

**Description:** This line item provides a performance enhancement to the LDAP server. A new configuration file option is included to enable the specification of a fetch size value in the retrieval of data from the TDBM database.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS IBM Tivoli Directory Server Administration and Use for z/OS

Support DB2 partitioning by Growth for ITDS TDBM and GDBM database

**Description:** This line item provides support for DB2 partitioning by Growth for TDBM and GDBM databases. A partition-by-growth table space is useful for those table spaces whose tables do not have a suitable partitioning key, but are expected to exceed the 64 GB limit that has been in place for simple or segmented table space. A partition-by-growth (PBG) table space can grow up to 128 TB.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS IBM Tivoli Directory Server Administration and Use for z/OS
- z/OS IBM Tivoli Directory Server Messages and Codes for z/OS

Prevent visibility of sensitive data in debug trace

**Description:** It provides a new approach to prevent the potential disclosure of sensitive data. With the appropriate security controls in place, a new console command allows these sensitive trace points to be enabled if the data is needed for diagnostic purposes.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS IBM Tivoli Directory Server Administration and Use for z/OS
- z/OS IBM Tivoli Directory Server Messages and Codes for z/OS

Infoprint Server new functions to consider

This topic describes z/OS Infoprint Server enhancements.
**Accessible and signed PDFs**

InfoPrint Server has added job attributes and corresponding fields on the ISPF panels to support accessible and signed PDFs.

**Description:**
To support accessible PDFs, new attributes specify the values of the PDF title, author, subject, and keyword properties. Another new attribute specifies the UNIX file name of the Index Control File (ICF), which contains rules that the Accessible PDF Transform uses to tag input. To support signed PDFs, new attributes specify the name of the signer, contact information for the signer, the location where the PDF was signed, the reason for signing it, and the name of the digital certificate used to create the signed PDF document.

**When change was introduced:**
z/OS V2R4.

**Reference information:**
- z/OS Infoprint Server Operation and Administration
- z/OS Infoprint Server User’s Guide

**Enhanced PDF encryption with AES options**

InfoPrint Server has added values for the `pdf-encryption` job attribute and the *Encryption level* field on the Processing ISPF panel to support AES encryption.

**Description:**
To support AES encryption of PDFs, the `ae128` and `ae256` values are added for the `pdf-encryption` job attribute. The *AES (128-bit key) AES (256-bit key)* values are added for the corresponding *Encryption level* field on the Processing ISPF panel. These values provide increased levels of security.

**When change was introduced:**
z/OS V2R4.

**Reference information:**
- z/OS Infoprint Server Operation and Administration
- z/OS Infoprint Server User’s Guide

**Dynamic configuration at all times**

Dynamic configuration is now always enabled.

**Description:**
Dynamic configuration lets you change Infoprint Server configuration attributes without stopping and restarting Infoprint Server. It lets administrators use the Infoprint Server ISPF panels or the Printer Inventory Definition Utility to change most system configuration attributes instead of editing the `aopd.conf` file. You must still edit a few startup attributes in `aopd.conf`.

**When change was introduced:**
z/OS V2R4.

**Reference information:**
- z/OS Infoprint Server Customization
- z/OS Infoprint Server Messages and Diagnosis
- z/OS Infoprint Server Operation and Administration
- z/OS Infoprint Server Printer Inventory for PSF

**Dynamic tracing**

The Infoprint Server trace facility now adjusts trace parameters dynamically while the daemon is running.

**Description:**
As an option, the trace facility for Infoprint Server can use cross-system coupling facility (XCF) signaling to adjust trace parameters dynamically while the target daemon is running. The dynamic...
trace facility uses new trace fields in the ISPF System Configuration panel or new PIDU attributes instead of environment variables to start or stop tracing for Infoprint Server daemons. With dynamic tracing, users do not need to change environment variables and then stop and restart one or more Infoprint Server daemons.

**When change was introduced:**

z/OS V2R3.

**Reference information:**

- z/OS Infoprint Server Customization
- z/OS Infoprint Server Messages and Diagnosis
- z/OS Infoprint Server Operation and Administration

**IP PrintWay backup printer capability**

You can now use IP PrintWay extended mode to define printer definitions for backup printers.

**Description:**

The print administrator can use IP PrintWay extended mode to define a backup printer in case a print failure occurs on the primary printer. The backup printer is defined in ISPF printer definition panels or PIDU.

**When change was introduced:**

z/OS V2R3.

**Reference information:**

- z/OS Infoprint Server Customization
- z/OS Infoprint Server Operation and Administration
- z/OS Infoprint Server User's Guide

**Infoprint Central enhancements**

The Infoprint Central user interface is updated with usability and accessibility enhancements.

**Infoprint Central enhancements for V2R4**

Infoprint Central is updated with functional and usability enhancements in V2R4.

**Description**

- **Predictable JVM user ID:**
  
  By setting the new `use-http-userid` attribute (Use Apache server ID on the ISPF System Configuration panel) to *yes*, you can start the Java virtual machine (JVM) using the user ID of the IBM HTTP Server—Powered by Apache instead of the user ID of the first user to log into Infoprint Central. Using a predictable user ID lets you use that ID to customize Work Load Manager (WLM) parameters. It improves performance because the WLM can identify JVM jobs and allocate more system resources to them. It also allows all users to view trace files, and prevents the JVM from crashing when it tries to write to a trace file created by a different user ID.

- **Security enhancement:**

  By default, InfoPrint Central now requires you to enable and use the Secure Sockets Layer (SSL) on the IBM HTTP Server—Powered by Apache. The SSL provides an encrypted and authenticated connection between the web browser and the server and lets you use Resource Access Control Facility (RACF) to restrict access to printers and print jobs. If you do not want SSL encryption for this connection, set the new `use-unencrypted-connection` attribute (Use unencrypted connection on the ISPF System Configuration panel) to *yes*.

  **Note:** IBM does not recommend setting `use-unencrypted-connection` to *yes*.

- **More classes for printer work selection criteria:**

  You can specify up to 36 output classes that a printer can select for processing.

- **Usability and accessibility enhancement:**
The new Limit field lets you specify the maximum number of objects to display on a search page.

**When change was introduced:**
z/OS V2R4.

**Reference information:**
- z/OS Infoprint Server Operation and Administration

### Infoprint Central enhancements for V2R3

**Description:**
The Infoprint Central user interface is updated with these enhancements in V2R3:
- The user interface now includes support for Microsoft Edge 25 or later.
- You can now search for up to eight FORMS names on the Work with Print Jobs page.

**When change was introduced:**
z/OS V2R3.

**Reference information:**
- z/OS Infoprint Server Operation and Administration

### Security enhancements

Infoprint Server is updated with security enhancements in V2R4.

**Description**
- InfoPrint Central uses SSL by default:
  
  InfoPrint Central now requires you to enable and use the Secure Sockets Layer (SSL) on the IBM HTTP Server—Powered by Apache by default. The SSL provides an encrypted and authenticated connection between the web browser and the server and lets you use Resource Access Control Facility (RACF) to restrict access to printers and print jobs. If you do not want to use SSL, you can set the new **use-unencrypted-connection** attribute (**Use unencrypted connection** on the ISPF System Configuration panel) to **yes**.

  **Note:** IBM does not recommend setting **use-unencrypted-connection** to **yes**.

  - RACF messages about unauthorized access attempts:

    New messages are written to the common message log when an unauthorized user tries to access objects protected by the Resource Access Control Facility (RACF).

**When change was introduced:**
z/OS V2R4.

**Reference information:**
- z/OS Infoprint Server Messages and Diagnosis

### Sendmail to CSSMTP bridge

IP PrintWay now uses the sendmail to Communications Server SMTP (CSSMTP) bridge that z/OS V2R3 provides.

**Description:**
The sendmail program that IP PrintWay used is now replaced with a sendmail bridge that uses Communications Server SMTP (CSSMTP) as the mail transport. Programming changes are not required; however, the sendmail bridge does not support these functions:
- Email delivery to local TSO and UNIX System Services mailboxes.
- The –m option on the **lp** command.

Also, only a limited number of options are supported by the AOPMAILER_OPTIONS environment variable that the sendmail bridge uses.
When change was introduced:
z/OS V2R3.

Reference information:
- z/OS Infoprint Server Customization
- z/OS Infoprint Server Messages and Diagnosis
- z/OS Infoprint Server Operation and Administration
- z/OS Infoprint Server User's Guide

TSO/E 8-character user IDs

Description:
Infoprint Server now supports 8-character TSO/E user IDs.

When change was introduced:
z/OS V2R3.

Integrated Security Services new functions to consider

For security related products, see “Security Server (RACF) new functions to consider” on page 71 and “Cryptographic Services new functions to consider” on page 38.

Flexible Authentication Secure Tunneling (FAST)

Description: Integrated Security Services is enhanced to implement the following mandatory requirements on the Flexible Authentication Secure Tunneling (FAST) mechanism:

- Clients must support the PA-FX-COOKIE pre-authentication data type. This padata type is used to maintain KDC state information and is sent to the client by the KDC in cases where multiple messages are required to authenticate the client. The client is required to copy the PA-FX-COOKIE padata into subsequent messages to a KDC in the specified realm.
- Clients, servers, and the KDC must support the Kerberos FAST Padata. The FAST Padata does not authenticate the client or the KDC; instead, it provides a typed hole to allow pre-authentication data to be tunneled. A pre-authentication data element used within FAST is called a "FAST factor". A FAST factor captures the minimal work required for extending Kerberos to support a new pre-authentication scheme.
- The FX_FAST_ARMOR_AP_REQUEST armor type must be supported.
- The encrypted challenge FAST factor must be supported.

When change was introduced: z/OS V2R4

Reference information:
- z/OS Integrated Security Services Network Authentication Service Administration
- z/OS Integrated Security Services Network Authentication Service Programming

Crypto Algorithm Currency

Description: Integrated Security Services is enhanced to include two new encryption types and two new checksum types for Kerberos 5 using AES with 128 bit and 256 bit keys. The encryption and checksum types are intended to support environments that use SHA-256 or SHA-384 as hash algorithms. A key derivation function using the SHA-256 or SHA-384 hash algorithm is used to produce keys for encryption, integrity protection, and checksum operations. The pseudorandom function used by PBKDF2 (password based key derivation function) is HMAC-SHA-256 or HMAC-SHA-384.

The new encryption types are:
- aes128-cts-hmac-sha256-128
- aes256-cts-hmac-sha384-192
The new checksum types are:

- hmac-sha256-128-aes128
- hmac-sha384-192-aes256

When change was introduced: z/OS V2R4

Reference information:

- z/OS Integrated Security Services Network Authentication Service Administration
- z/OS Integrated Security Services Network Authentication Service Programming
- z/OS Security Server RACF Data Areas

Federal Information Processing Standard (FIPS)

Description: Integrated Security Services is enhanced to support SP800-131A in two ways:

- SP800-131A with exception: The 112-bit security will be enforced when creating new keys or performing digital signature generation and encryption type operations. Digital signature verification, decryption using TDS, and RSA decryption with 80-bit key lengths will be allowed when processing already protected information.
- SP800-131A without exception: The 112 bit or higher security strength is enforced for all operations.

Additionally, beginning in z/OS V2R3, Integrated Security Services will have a dependency on ICSF. It will use ICSF PKCS#11 functions:

- the calls on the CCA functions will be replaced by PKCS#11 functions
- the internal crypto functions will be replaced by PKCS#11 functions.

READ access to the CSFRNG, CSF1TRC, CSF1SKE, and CSF1SKD resources in the CSFSERV class are required if the class is active.

ICSF PKCS#11 and System SSL functions also enables Integrated Security Services to run under FIPS mode with different levels provided by ICSF PKCS#11 and System SSL with their most current support.

New configuration options ‘SKDC_FIPSLEVEL’, ‘fipslevel’ will be provided in the envar file for the KDC and the krb5.conf file for the client respectively.

When change was introduced: z/OS V2R3

Reference information:

- z/OS Integrated Security Services Network Authentication Service Administration
- z/OS Integrated Security Services Network Authentication Service Programming
- z/OS Security Server RACF Data Areas
- z/OS Security Server RACF Callable Services

ISPF new functions to consider

TSO 8-character user ID enhancement

Description: This enhancement provides ISPF support for the expansion of the TSO user ID from a maximum of 7 characters to a maximum of 8 characters. User ID and prefix values that are up to 8 characters in length are supported.

Introduced: z/OS V2R3

Reference information:

- See the topic about "Member list display panel fields" in z/OS ISPF User’s Guide Vol I.
Extended statistics usability enhancement

**Description:**
This enhancement provides automatic generation of PDS member extended statistics when at least one of the line count values for the member exceeds 65535. Non-extended statistics are automatically generated when none of the line count values for the member exceed 65535. The ability to request extended statistics for a member is removed.

**Introduced:**
z/OS V2R3

**Reference information:**
- See the topics about "ISPF member statistics" and "Member list display panel fields" in *z/OS ISPF User’s Guide Vol I.*
- See the topic about "Edit site-wide profile customizations" in *z/OS ISPF Planning and Customizing.*
- See the topic about "STATS—Generate Library Statistics" in *z/OS ISPF Edit and Edit Macros.*
- See the topics about the "LMMADD, LMMDISP, LMMFIND, LMMREP, and LMMSTATS services" in *z/OS ISPF Services Guide.*

JES2 new functions to consider

This topic describes new JES2 functions in z/OS.

**JES2 policies**

**Description:**
Support for JES2 policies is introduced in z/OS V2R4, while providing facilities for incremental addition of more function in future releases. JES2 policies are an alternative to JES2 installation exits. JES2 polices allow you to customize JES2 processing of z/OS jobs and system output without programming installation exit programs.

**When change was introduced:**
z/OS V2R4.

**Reference information:**
- *z/OS JES2 Commands.*
- *z/OS JES2 Initialization and Tuning Guide.*
- *z/OS JES2 Installation Exits.*
- *z/OS JES2 Messages.*
- *z/OS JES2 Macros.*

**JES2 disk reader support**

**Description:**
JES2 is adding a JES2 command to submit JCL from a predefined DD. The source DD is SUBMITLIB.
- The SUBMITLIB(name) statement (alias SUBLIB) is added and is used to identify a series of partitioned data sets. Operator commands for $ADD, $DEL, and $T (modify) SUBMITLIB are added (including display with $D). The concatenation supports any format PDS (LRECL and RECFM) that can be used to pass JCL into input processing.
• The SUBMITRDR statement (or SUBRDR) is added and is used to specify JES2 defaults for jobs submitted this way. The parameters are similar to the INTRDR statement with the addition of a default DD name for the new $SUBMIT command.
• The $SUBMIT command is added to cause a member of a SUBMITLIB concatenation and is submitted by using SUBMITRDR. The command supports a DD name (SUBMITLIB subscript), a member name, and a HOLD= override.
• Job security is based on the source of the $SUBMIT command.

When change was introduced:
z/OS V2R4.

Reference information:
- z/OS JES2 Messages.
- z/OS JES2 Commands.
- z/OS JES2 Initialization and Tuning Guide.
- z/OS JES2 Initialization and Tuning Reference.

Health Check for JES2 Checkpoint Configuration

Description:
A new Health Check is provided to report issues with the JES2 checkpoint configuration that prevents JES2 from automatically recovering checkpoint device errors without operator intervention. In addition, the Health Check verifies that the JES2 checkpoint is configured using best practices.

When change was introduced:
z/OS V2R4.

Reference information:
- z/OS MVS System Messages, Vol 6 (GOS-JEA)
- z/OS MVS Using the Subsystem Interface
- IBM Health Checker for z/OS User’s Guide

Instruction Execution Protection (IEP)

Description:
Instruction Execution Protection is a feature of z14 hardware. It allows programmers to allocate storage in a non-executable state. Starting in z/OS V2R4, JES2 uses this by changing the default behavior of the $GETMAIN macro. If you upgrade to z/OS V2R4 and you are running on z13 or earlier hardware, JES2 continues to function normally, but you do not receive the benefits of the IEP service.

When change was introduced:
z/OS V2R4.

Reference information:
- z/OS JES2 Initialization and Tuning Guide
- z/OS JES2 Macros

Reporting JES2 resiliency data

Description:
Starting in z/OS V2R4, reporting JES2 Resiliency data to the user through an SSI interface can occur. New functions are added to the JES Job Information Services SSI 71 to request JES Resource Limits Information. Filters can now be supplied so that specific types of data are returned and/or data specific to a supplied resource type is returned.

When change was introduced:
z/OS V2R4.

Reference information:
- z/OS JES2 Macros
JES2 email support

**Description:** JES2 now accepts an email address instead of a user name in JCL for jobs and job groups. JES2 also now allows email as additional delivery method for job notification messages and messages that are sent by the Notify user message service. In addition, JES2 now accepts password phrases for user authentication in JCL for jobs and job groups.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS JES2 Commands.
- z/OS JES2 Initialization and Tuning Guide.
- z/OS JES2 Initialization and Tuning Reference.
- z/OS JES2 Messages.
- z/OS MVS JCL Reference.

JCL Simplification

**Description:** JES2 is adding support for longer character DLM= and two new JCL symbols, &SYSJOBNM and &SYSJOBID. The length is increased from 2 characters to at least 8 characters.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS JES Application Programming.
- z/OS MVS JCL Reference.

Dynamic groups added

**Description:** JES2 is adding support for dynamic groups by using the SCHEDULE card. This support provides the ability to run a job before or after another job.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS MVS JCL Reference.

Managing JES2 resources

**Description:** JES2 is expanding how it manages some of its resources that an installation might need to run workloads on its systems, specifically, tracking use of resources. JES2 is also adding support for a privileged user to have access to resources during a shortage so actions can be taken to resolve the shortage.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS JES2 Commands.
- z/OS JES2 Messages.

JES3 JECL support

**Description:** JES2 is adding more JECL support to reduce the JECL conversion needed to run jobs originally coded for the JES3 environment in a JES2 environment. This support also helps to identify the use of JES2 and JES3 JECL statements by using the jobname.

**When change was introduced:** z/OS V2R3
JES3 new functions to consider

This topic describes new JES3 functions in z/OS.

**JES3 support for 8-character TSO/E user IDs**

**Description:** JES3 supports the use of 8-character TSO/E user IDs. In prior releases, TSO/E has been limited to 7-character user IDs.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS JES3 Messages
- z/OS MVS JCL Reference

Language Environment new functions to consider

This topic describes new Language Environment functions in z/OS.

**Support for tracking specific price metrics**

**Description:**
New Language Environment interfaces such as the CEEUSGD callable service were added to enable the use of the IFAUSAGE interface to track specific price metrics.

**Release introduced:**
z/OS V2R4

**Reference information:**
- z/OS Language Environment Programming Guide
- z/OS Language Environment Programming Reference
- z/OS Language Environment Concepts Guide
- z/OS Language Environment Programming Guide for 64-bit Virtual Addressing Mode
- z/OS XL C/C++ Runtime Library Reference

**Japanese New Era support**

**Description:**
Previously, the Japanese era was Heisei. As of 1 May 2019, the era is Reiwa. Updates were made to the set of date and time services that support the Japanese calendaring scheme.

**Release introduced:**
z/OS V2R4 and z/OS V2R3 with the PTF for APAR PH05611 applied.

**Reference information:**
- z/OS Language Environment Programming Reference

**Enabling non-executable memory**

**Description:**
To enhance program security, certain memory regions such as the library heap are now allocated as non-executable by default.

**Release introduced:**
z/OS V2R4
Year 2038/2040 support

Description:
Support was added for POSIX time values beyond year 2038 and z/OS time-of-day values beyond year 2042.

Release introduced:
z/OS V2R3

Reference information:
- z/OS Language Environment Debugging Guide
- z/OS Language Environment Vendor Interfaces
- z/OS MVS Initialization and Tuning Reference
- z/OS MVS System Commands

Detecting buffer overflows

Description:
Stack guards now enhance the security of Language Environment programs by aiding in the detection of buffer overflows and preventing them from causing program misbehavior or from becoming serious security vulnerabilities.

Release introduced:
z/OS V2R3

Reference information:
- z/OS Language Environment Programming Guide
- z/OS Language Environment Debugging Guide
- z/OS Language Environment Programming Guide for 64-bit Virtual Addressing Mode
- z/OS Language Environment Vendor Interfaces
- z/OS XL C/C++ Programming Guide

64-bit support for Enterprise PL/I

Description:
Previously, Language Environment did not provide 64-bit support for Enterprise PL/I. In V2R3, this support is provided with new 64-bit compiler writer interfaces (CWIs) and 64-bit event handlers. (64-bit support for Enterprise PL/I is provided in V2R2 with appropriate service level.)

Release introduced:
z/OS V2R3

Reference information:
- z/OS Language Environment Vendor Interfaces

Metal C Runtime Library new functions to consider

This topic describes new Metal C Runtime Library functions in z/OS.

Prefix data block
Description:
The Metal C compiler sets two new flags and adds two new optional fields in the prefix data block. The flag on bit 2 in Flag Set 4 indicates the presence of the optional field that contains the offset of the end of current CSECT. The flag on bit 3 in Flag Set 4 indicates the presence of the optional field that contains the offset of the debug data block.

Release introduced:
z/OS V2R3

Reference information:
/z/OS Metal C Programming Guide and Reference

Debug data block

Description:
A new debug data block is added for each CSECT, which can be used to check whether the debug side file matches the object file. The debug data block contains the debug data block signature, size of the debug data block, reserved bytes, MD5 signature, Metal C source file name, and debug side file name.

Release introduced:
z/OS V2R3

Reference information:
/z/OS Metal C Programming Guide and Reference

Metal C function descriptors

Description:
You can declare a function pointer with the new __fdptr keyword so that this function pointer points to a Metal C function descriptor. Metal C function descriptors can point to and call functions with their own set of associated data for the particular program or invocation.

Release introduced:
z/OS V2R3

Reference information:
/z/OS Metal C Programming Guide and Reference

NFS new functions to consider

This topic describes new Network File System (NFS) functions in z/OS.

chkloop site attribute

Description: This site attribute enables/disables NFS Error Client Loop Detection Facility and sets the values of the site attributes LOOPThreshold(x) and TIMETHreshold(y).

When change was introduced: z/OS V2R3

Reference information: z/OS Network File System Guide and Reference

loopthreshold site attribute

Description: This site attribute detects a loop situation, identifies the remote system causing the loop and issues series of GFSA1036E console error messages.

When change was introduced: z/OS V2R3

Reference information: z/OS Network File System Guide and Reference
enhmaplower attribute

**Description:** This attribute maps PDS/PDSE member names to upper case when received from the client in an NFS request in lower case.

**When change was introduced:** z/OS V2R3

**Reference information:** *z/OS Network File System Guide and Reference*

exportchk operand

**Description:** This modify command operand checks the Exports file about export and checklist values without rebuilding the new export list.

**When change was introduced:** z/OS V2R3

**Reference information:** *z/OS Network File System Guide and Reference*

---

**Resource Measurement Facility (RMF) new functions to consider**

The following topic provides an overview of the new features, functions, and support for Resource Measurement Facility (RMF) that are available in z/OS V2R4 and V2R3.

**New features, functions, and support for z/OS V2R3**

Resource Measurement Facility (RMF) provides these new features, functions, and support in z/OS V2R3.

**Enhanced Crypto Hardware Activity report**

RMF has enhanced the Postprocessor Crypto Hardware Activity report to provide activity measurements from the Crypto Express6S (CEX6) card configured in one of these ways:

- Cryptographic CCA coprocessor
- Cryptographic PKCS11 coprocessor
- Cryptographic accelerator

**When change was introduced:** z/OS V2R3 (Also V2R2 with APAR OA50693)

**Reference information:**

See *z/OS RMF Report Analysis* for a description of this report.

See *z/OS MVS System Management Facilities (SMF)* for a description of the enhanced SMF record 70-2.

**RMF support for monitoring and reporting of 2 GB memory frames**

RMF support for the gathering and reporting of performance measurements collected for usage of 2 GB memory frames.

To exploit 2 GB memory frames, the Enhanced DAT Facility 2 (EDAT-2) must be available.

RMF has enhanced the following reports:

- Postprocessor Paging Activity report
- Postprocessor Virtual Storage Activity report
- Monitor III STORM Report

Following SMF records have been changed:

- SMF 70 to 79, RMF Product section.
- SMF 71, Paging Data section
- SMF 78 subtype 2, Virtual Storage Private Area Data section

New overview conditions have been added based on SMF record 71.
When change was introduced: z/OS V2R3 (Also V2R2 with APAR OA48913)

Reference information:
See z/OS RMF Report Analysis for a description of the reports.
See z/OS MVS System Management Facilities (SMF) for a description of the enhanced SMF record types 71 and 78.

Enhanced reporting of device numbers

In IBM zHyperWrite environments, RMF reports on PPRC Primary as well as on PPRC Secondary devices, which are configured for control unit based mirroring and software mirroring. In order to allow users to distinguish device addresses of PPRC Primary devices from those of PPRC Secondary devices, RMF displays 5-digit device numbers in most of the RMF device reports. The first digit of the device number represents the ID of the subchannel that the physically configured device is set to.

When change was introduced: z/OS V2R3

Reference information:
See z/OS RMF User's Guide.
See z/OS RMF Programmer's Guide.
See z/OS RMF Report Analysis.
See z/OS MVS System Management Facilities (SMF).

RMF Synchronous I/O Link Support

RMF has enhanced its monitoring and reporting capabilities to cover zSynchronous I/O environments. It now gathers and provides performance data on synchronous data transfers to and from storage controllers via PCIE Synchronous I/O links and reports on the response times and data transfer rates of DASD devices actively performing synchronous I/O requests.

When change was introduced: z/OS V2R3 (Also V2R1 and V2R2 with APAR OA50755)

Reference information:
See z/OS RMF Report Analysis for a description of the affected reports.
See z/OS MVS System Management Facilities (SMF) for a description of the enhanced SMF records 74-1 and 74-9.

RMF SMF for CF Encryption Metrics

RMF has been enhanced to gather the Coupling Facility structure related metrics and to capture the metrics in SMF74 subtype 4 records. By providing the Coupling Facility read / write statistics in SMF 74 subtype 4 records, zBNA tooling can be used to predict the overhead of CF encryption and decryption, prior to actually turning on CF encryption.

When change was introduced: z/OS V2R3 (Also V2R2 with HRM77A0 SPE OA52003.)

Reference information:
See z/OS RMF Report Analysis for a description of the affected reports.
See z/OS RMF Programmer's Guide.
See z/OS MVS System Management Facilities (SMF) for a description of the enhanced SMF records 74-4.

RMF reporting enhancements for z14

RMF has been enhanced to ensure correct monitoring and reporting of new z14 hardware features:
• Multi-Threading support for SAPs,
• IBM Virtual Flash Memory support, and
• RoCE Express 2 support.

**When change was introduced:** z/OS V2R3 (Also V2R2 with APARs OA50761, OA50762, OA51913 and V2R1 with APARs OA50762, OA51913 and V1R13 with APAR OA51913)

**Reference information:**
See **z/OS RMF Report Analysis** for a description of the affected reports.

See **z/OS MVS System Management Facilities (SMF)** for a description of the enhanced SMF records 74-10 and 74-9.

**RMF support for new WLM Policy attributes**
RMF is enhanced with the introduction of WLM Specialty Engines Containment (also known as “HonorPriority by Service Class”) and Memory Capping.

The following RMF reports are enhanced:
- Postprocessor WLMGL report.
- Monitor II ASD/ASDJ report.
- Monitor III Group report.
- Monitor III RG report.

The following SMF records are changed:
- SMF 72 subtype 3:
  - Workload Manager Control section.
  - Resource Group Data section
- SMF 72 subtype 4:
  - Swap Reason Data section
- SMF 79 subtype 1:
  - ASD and ASDJ Data section
- SMF 79 subtype 2:
  - ARD and ARDJ Data section

The Monitor III Reporter Table ERBSUMT3 is enhanced.

**When change was introduced:** z/OS V2R3 RMF, z/OS V2R2 RMF, and z/OS V2R1 RMF with APAR OA50760.

**Reference information:**
See **z/OS RMF Programmer’s Guide**.
See **z/OS RMF Report Analysis** for a description of the affected reports.
See **z/OS MVS System Management Facilities (SMF)** for the revised SMF 72-3 record.

**RMF support for WLM Shorter Response Time Goals**
RMF is enhanced to report on the changed WLM definition of performance goals for service classes. For service class periods with an average response time goal or a response time goal with percentile, the lowest goal which can be specified changes from 15 milliseconds to one millisecond, allowing to specify meaningful goal values for very fast running transactions.

RMF provides these shorter response time goals together with more precise transaction times in Monitor I and III, Postprocessor Reporting, in the Distributed Data Server and the Spreadsheet Reporter:

In detail:
• Extend SMF record type 72 subtype 3 (Workload Activity) to provide transaction elapsed and execution times in microseconds.
• Extend SMF record type 72 subtype 4 (Storage Data) to provide transaction execution and queued times in microseconds.
• Adapt the Postprocessor Workload Activity (WLMGL) reporting to present the response time goal, transaction times, and response time distributions with higher precision to reflect actual response times lower than one millisecond.
• Adapt the Monitor III SYSINFO, SYSRTD, SYSSUM, SYSWKM, and GROUP reports to display response time goals and actual response times with higher precision, i.e. in milliseconds.

When change was introduced: z/OS V2R3 RMF.

Reference information:

See z/OS RMF User's Guide.
See z/OS RMF Programmer's Guide.
See z/OS RMF Report Analysis for a description of the affected reports.
See z/OS MVS System Management Facilities (SMF) for the revised SMF 72-3 record.

Security Server (RACF) new functions to consider

This topic describes new Security Server (RACF) functions in z/OS.

RACF Custom Fields

Description: RACF is enhanced to allow custom fields to be added to the RACF general resource and DATASET class profiles in a consistent fashion with the existing ability for user and group profiles. For all profile types, the ability to validate the value of a field using a System REXX program is also provided.

RACF is also enhanced to allow retrieval of DATASET class profile fields using the R_admin callable service (IRRSEQ00) and the IRRXUTIL REXX interface.

The IRRXUTIL REXX interface is enhanced to allow retrieval of a general resource class definition from either the static or dynamic Class Descriptor Table (CDT). There is a corresponding "next" function that allows a caller to iterate through CDT entries. The current SETROPTS settings for the class can be optionally requested.

When change was introduced: z/OS V2R4

Reference information:

z/OS Security Server RACF System Programmer's Guide
z/OS Security Server RACF Macros and Interfaces
z/OS Security Server RACF Command Language Reference
z/OS Security Server RACF Messages and Codes
z/OS Security Server RACF Security Administrator's Guide
z/OS Security Server RACF Data Areas
z/OS Security Server RACROUTE Macro Reference
z/OS Security Server RACF Callable Services

RACF IBM Multi-factor Authentication (IBM MFA) Enhancements

Description: RACF IBM MFA is enhanced to improve the MFA user authentication experience:

Identity Token
An Identity Token is used to encode details about a user who can be trusted by the consumer of the token.
RACROUTE Support for Identity Tokens
Support is added to RACROUTE authentication processing to generate and validate Identity Tokens (IDT). An application can call RACROUTE to authenticate a user with an IDT specified instead of a credential such as a password.

IDT Configuration
The security administrator can create profiles in the IDTDATA class to configure how certain fields in an IDT are generated and validated. The profiles can be used to control options such as which key is used to sign the IDT and its validity period.

JSON Web Token (JWT)
A JSON Web Token (JWT) is a token technology used to assert claims between parties. They are often used by a single sign-on system to prove that a user has been authenticated.

When change was introduced: z/OS V2R4

Reference information:
- z/OS Security Server RACF Command Language Reference
- z/OS Security Server RACF Data Areas
- z/OS Security Server RACROUTE Macro Reference
- z/OS Security Server RACF Callable Services

RACF Pervasive encryption support

Description: RACF is enhanced to allow RRSF users to reallocate their RRSF VSAM datasets in order to change their attributes, move them to different volumes, or encrypt them using Pervasive Encryption. Tracing is also added to more parts of the RRSF subsystem, making it easier for IBM support to debug problems.

When change was introduced: z/OS V2R4

Reference information:
- z/OS Security Server RACF System Programmer's Guide
- z/OS Security Server RACF Command Language Reference
- z/OS Security Server RACF Messages and Codes
- z/OS Security Server RACF Security Administrator's Guide

RACF Privilege Escalation Detection

Description: RACF is enhanced to add checking in strategic areas to detect when an ACEE is modified. When a modification is detected, a message will be issued, while still allowing the function to proceed. The function allows normal auditing to proceed so that all the relevant information related to the event can be logged.

Users can implement automation on this message, which will contain as much environmental information as possible to allow such automation to take action, if necessary.

When change was introduced: z/OS V2R4

Reference information:
- z/OS Security Server RACF System Programmer's Guide
- z/OS Security Server RACF Messages and Codes
- z/OS Security Server RACF Security Administrator's Guide
- z/OS Security Server RACF Data Areas
- z/OS Security Server RACROUTE Macro Reference

RACF Improved PassTicket Security

Description: RACF is enhanced to promote the use of ICSF to protect PassTicket keys using the following new functions:
• RACF will display the name of the key label it generates for a particular key when that key is defined using the KEYENCRYPTED keyword in the SSIGNON segment of the RDEFINE and RALTER commands. This will allow the security administration to correlate the keys defined in the ICSF CKDS with the RACF profile in the PTKTDATA class that is using it. IRRDBU00 and the extract functions of the R-admin callable service will return the method of protection or key label name.

• RACF will provide a new ENCRYPTKEY keyword that will convert a masked key to an encrypted key without requiring knowledge of the key and without requiring the key to be changed.

• RACF will provide a new KEYLABEL keyword that will store the specified key label in the PTKTDATA profile. This will allow admins to pre-define the keys in the ICSF using ICSF interfaces, which is consistent with the approach taken with data set encryption.

**When change was introduced:** z/OS V2R4

**Reference information:**

- z/OS Security Server RACF Macros and Interfaces
- z/OS Security Server RACF Command Language Reference
- z/OS Security Server RACF Messages and Codes
- z/OS Security Server RACF Security Administrator’s Guide
- z/OS Security Server RACF Callable Services

---

**RACF RACDCERT TLS1.3 RSAPSS support**

**Description:** RACF is enhanced to support RACDCERT TLS1.3 RSAPSS. The new function changes the RACF RACDCERT command from handling certificates signed by the hash/signature algorithm pair to the signature algorithm used in the ClientHello message in the TLS1.3 protocol. The support will include the RACDCERT functions GENCERT, REKEY, LIST, LISTCHAIN, and CHECKCERT.

The new algorithm supported is RSA Probabilistic Signature Scheme (RSASSA-PSS). It is a signature algorithm and an RSA key. The new functionality requires that the parameter field in AlgorithmIdentifier cannot be null if present, it must be omitted if there is no value.

Beginning in V2R4, the RACDCERT will store the RSA private key in PKDS protected by the ECC master key. This change will cause the RACDCERT command with RSA(PKDS) sub keyword to fail if the ECC master key is not activated in the system.

The new supported signature algorithms are:

- SHA1RSAPSS
- SHA224RSAPSS
- SHA256RSAPSS
- SHA384RSAPSS
- SHA512RSAPSS

**When change was introduced:** z/OS V2R4

**Reference information:**

- z/OS Security Server RACF Command Language Reference
- z/OS Security Server RACF Messages and Codes
- z/OS Security Server RACF Security Administrator’s Guide

---

**RACF Parmlib support**

**Description:** A new parmlib member, IRRPRMxx, is introduced. The IRRPRMxx parmlib member contains data for the RACF data set name table, range table, and sysplex communications options. Use an IRRPRMxx member to specify statements that describe the RACF data set name table and the range table, that were previously defined by ICHRDSNT and ICHRNG.

**When change was introduced:** z/OS V2R3
Reference information:

z/OS Security Server RACF System Programmer's Guide
z/OS Security Server RACF Callable Services
z/OS Security Server RACF Command Language Reference
z/OS Security Server RACF Messages and Codes
z/OS Security Server RACF Security Administrator's Guide
z/OS MVS Initialization and Tuning Reference

RACF ODM classes support

Description: RACF is enhanced to include three new general resource classes: HBRADMIN, HBRCNN, and HBRCMD in support of the IBM Operational Decision Manager (ODM) for z/OS.

When change was introduced: z/OS V2R3

Reference information:

z/OS Security Server RACF Macros and Interfaces
z/OS Security Server RACF System Programmer's Guide
z/OS Security Server RACF Security Administrator's Guide
z/OS Security Server RACF Command Language Reference

RACF CICS Auditing support

Description: RACF is enhanced to support the ICSF logging of CICS client identity on RACROUTE REQUEST=FASTAUTH calls for the CSFSERV, CSFKEYS, and XCSFKEY classes.

When change was introduced: z/OS V2R3

Reference information:

z/OS Security Server RACF Macros and Interfaces
z/OS Security Server RACROUTE Macro Reference
z/OS Security Server RACF Auditor's Guide

SMP/E new functions to consider

GIMUNZIP enhancements

Description: The GIMUNZIP file extraction service routine is used to extract the data sets, files, and directories from the archive files in GIMZIP packages. Previously, new sequential and partitioned data sets created by GIMUNZIP were always catalogued, and new data sets could not be allocated using specified storage, management, or data classes. With APAR IO23270, GIMUNZIP is extended to support creating new, uncataloged, data sets, and when allocating new data sets, to use optional storage class, data class, and management class specifications. In addition, a work volume and device unit may be used for temporary data set allocations when extracting partitioned and VSAM data sets.

When change was introduced: APAR IO23270.

Reference information:

z/OS SMP/E Messages, Codes, and Diagnosis
z/OS SMP/E Commands
z/OS SMP/E Reference
z/OS SMP/E User's Guide
TSO/E new functions to consider

This topic describes new TSO/E functions in z/OS.

LOGON timeout

**Description:** This support automatically terminates the LOGON process if it takes longer than a predefined amount of time prompting the user for LOGON information, therefore, freeing resources in an address space.

*When change was introduced:* z/OS V2R4

**Reference information:**
- z/OS TSO/E Customization
- z/OS MVS System Codes
- z/OS MVS System Messages, Vol 9 (IGF-IWM)

Allow special characters within passwords

**Description:** TSO/E positional operands for IKJPOSIT USERID8 and UID82PWD, are updated to allow special characters within passwords, enabling line mode LOGON to also accept these characters.

*When change was introduced:* z/OS V2R4

**Reference information:**
- z/OS TSO/E Programming Services

Server-Requester Programming Interface (SRPI) and TSO/E Enhanced Connectivity Facility removal

**Description:** z/OS support for Server-Requester Programming Interface (SRPI) and TSO/E Enhanced Connectivity Facility is discontinued. The information about Server-Requester Programming Interface and Enhanced Connectivity Facility are removed. The MVSSERV command is no longer issued.

*When change was introduced:* z/OS V2R4

**Reference information:**
- z/OS TSO/E General Information
- z/OS TSO/E Command Reference
- z/OS TSO/E Messages
- z/OS TSO/E Customization
- z/OS TSO/E Programming Services
- z/OS TSO/E Programming Guide
- z/OS TSO/E User's Guide

8 character user ID

**Description:** TSO/E has been limited to 7-character user IDs. This line item provides TSO/E to now have the use of 8-character user IDs.

*When change was introduced:* z/OS V2R3

**Reference information:**
- z/OS TSO/E Administration
- z/OS TSO/E Command Reference
- z/OS TSO/E Customization
- z/OS TSO/E Messages
- z/OS TSO/E Primer
TSO/E Support for JES2 Resiliency

**Description:** JES2 now provides an emergency subsystem that can access reserved JES2 resources to react to resource shortage problems. For TSO/E, the LOGON and SUBMIT commands are updated to allow the specification of the subsystem name to be routed to an emergency subsystem.

**When change was introduced:** z/OS V2R3

**Reference information:**
- z/OS TSO/E Command Reference
- z/OS TSO/E Messages

XL C/C++ new functions to consider

This topic describes new XL C/C++ functions in z/OS.

**New and changed compiler options**

**Description:**

The following compiler options or suboptions are new or changed in z/OS V2R4:

- TARGET(zOSV2R4)

**Release introduced:**

z/OS V2R4

**Description:**

The following compiler options or suboptions are new or changed in z/OS V2R3:

- AGGREGATE(OFFSETDEC | OFFSETHEX)
- ARCHITECTURE(12)
- DEBUG(NOFILE)
- INFO(STP | NOSTP)
- STACKPROTECT | NOSTACKPROTECT
- TARGET(zOSV2R3)
- TUNE(12)

**Release introduced:**

z/OS V2R3

**Enhanced vector programming support**

**Description:**

The vector programming support is enhanced in the following aspects to take advantage of the Vector Facility for z/Architecture.

**Vector data types**

The vector float data type is supported under ARCH(12).

**Operators**

Operators are extended to support the vector float data type. Use of certain vector data types with some operators is deprecated. These vector data types are still accepted as operands of these operators, but their usage is discouraged.
**Vector built-in functions**

The following vector built-in functions are added:

- `vec_bperm_u128`: Vector Bit Permute
- `vec_double`: Vector Convert from long long to double
- `vec_doublee`: Vector Convert from float (even elements) to double
- `vec_eqv`: Vector XNOR
- `vec_floate`: Vector Convert from double to float (even elements)
- `vec_load_len_r`: Vector Load Rightmost with Length
- `vec_msum_u128`: Vector Multiply Sum Logical
- `vec_nand`: Vector NAND
- `vec_nmadd`: Vector Negative Multiply Add
- `vec_nmsub`: Vector Negative Multiply Subtract
- `vec_orc`: Vector OR with Complement
- `vec_rint`: Vector Round to Integer
- `vec_signed`: Vector Convert double to signed long long
- `vec_store_len_r`: Vector Store Rightmost with Length
- `vecUnsigned`: Vector Convert double to unsigned long long
- `vec_xl`: Vector Load
- `vec_xst`: Vector Store

Some vector built-in functions are extended to support the vector float data type, or other data types at a minimum ARCH level of 11 or higher.

Use of certain vector data types with some operators is deprecated. These vector data types are still accepted as operands of these operators, but their usage is discouraged.

Some vector built-in functions are deprecated. You can still use these vector built-in functions at a minimum ARCH level of 11, but their usage is discouraged.

**Release introduced:**

z/OS XL C/C++ V2R3

**Reference information:**

- z/OS XL C/C++ Programming Guide

**New LEGACY option for the DSECT Utility**

**Description:**

The default option is changed to NOLEGACY, which makes the output match the output of the DSECT utility that is generated by HLASM.

**Release introduced:**

z/OS V2R3

**Reference information:**

- z/OS XL C/C++ User's Guide

**New SOS info utility**

**Description:**

You can use the SOS info utility to decode Saved Options String (SOS) information from an executable file and produce a list of compiler options that were used to control the code generation of a program.

**Release introduced:**

z/OS V2R3
Updates to CDAHLASM and as utilities

Description:
The CDAHLASM and as utilities get the MD5 signature from the debug data block if the block exists and puts the signature in the debug side file. In addition, if the CDAHLASM and as utilities have the write permission to the assembly file, they will update the assembly file by replacing the debug side file name in the debug data block with the user provided name or a default debug side file name.

Release introduced:
z/OS V2R3

Reference information:
• z/OS XL C/C++ User's Guide

z/OS File System (zFS) new functions to consider

Improved reliability and availability for zFS file systems

Description:
With the zFS high availability option, if the file system owner experiences an outage, applications that are accessing that file system on other systems are not affected.

When change was introduced:
z/OS V2R4

Reference information:
z/OS File System Administration

zFS File Snapshot

Description:
With zFS File Snapshot, you can create a point-in-time snapshot (or copy) of a file in a zFS file system and allow subsequent read requests from that snapshot. Each time files are changed, backup programs can save only the changed files in a file system instead of saving all the files in the file system.

Release introduced:
z/OS V2R4 and in V2R3 with the PTF for APAR OA56145 applied.

Reference information:
z/OS File System Administration

Removal of Distributed File Service/Server Message Block (DFS/SMB)

Description:
In z/OS V2R3, the statement of direction was updated to indicate that V2R3 would be the last release to support the DFS/SMB (Distributed File System/Server Message Block) functionality. IBM had previously announced that the Network File System (NFS) was the strategic file sharing protocol for the z/OS platform.

Release introduced:
z/OS V2R4

Reference information:
The following book is removed:
Identifying SMB-exported file systems

Description:
Because z/OS V2R3 is planned to be the last release to support the DFS/SMB functionality, the ZOSMIGV2R3_NEXT_USS_SMB_DETECTED health check was made available. It provides a list of SMB-exported file systems.

Release introduced:
z/OS V2R3 with APAR OA56251.

Reference information:
IBM Health Checker for z/OS User's Guide

Repairing mounted zFS file systems

Description:
File systems no longer need to be unmounted in order to be salvaged. Use the new zfsadm salvage command to salvage them while they are still mounted.

Release introduced:
V2R3

Reference information:
z/OS File System Administration

Shrinking zFS aggregates

Description:
The size of a zFS aggregate can be reduced by using the new zfsadm shrink command to release space from the associated VSAM data set.

Release introduced:
V2R3

Reference information:
z/OS File System Administration

Encrypting and compressing zFS file system data

Description:
zFS has added support for encrypting file system data using the DFSMS access method encryption. Support has also been added to compress file system data using the zEDC compression method. New file systems can be defined and formatted so that any data added to them are automatically encrypted, compressed, or both. Existing file systems can have their data encrypted or compressed with the new zfsadm encrypt and zfsadm compress commands.

Release introduced:
V2R3

Reference information:
z/OS File System Administration

Enhanced mounting of VSAM linear data sets

Description:
VSAM linear data sets that are created with the zfsadm define command no longer need to be formatted before they are mounted.

Release introduced:
V2R3

Reference information:
z/OS File System Administration
Dynamically changing attributes that were assigned when a file system is first mounted

**Description:**
Users can dynamically change aggregate attributes that were assigned during mount processing, such as AGGRFULL and AGGREGROW, without having to unmount and remount the file system.

**Release introduced:**
z/OS V2R3

**Reference information:**
[Smf support for zFS](#)

SMF support for zFS

**Description:**
System Management Facilities (SMF) can be used to collect and record file system events, performance data, and per-file system statistics for ZFS.

**Release introduced:**
z/OS V2R3

**Reference information:**
[z/OS File System Administration](#)

**z/OS Management Facility (z/OSMF)**

This topic describes new z/OSMF functions in z/OS.

**z/OSMF enabled during IPL**

**Description:**
In z/OS V2R3, the base element z/OSMF is started by default at system IPL. This behavior, which is referred to as z/OSMF autostart, means that z/OSMF is available for use as soon as the system is up.

Related to this support are the following enhancements:

- Statements and keywords are added to the z/OSMF parmlib member, IZUPRMxx.
- Parameters are added to the z/OSMF started procedure, IZUSVR1.
- System parameter IZU= is added to the IEASYSxx parmlib member. Use the IZU= parameter to identify one or more IZUPRMxx parmlib members to be used for your z/OSMF configuration.

With z/OSMF autostart, it is no longer necessary for your installation to explicitly start the z/OSMF server after each system IPL, whether through automation or commands entered manually at the operations console.

Authorized programs can use the event notification facility (ENF) to determine whether the z/OSMF server is up or down.

**Release introduced:**
z/OS V2R3.

**Reference information:**
- [z/OS Upgrade Workflow](#)
- [IBM z/OS Management Facility Configuration Guide](#)

**z/OSMF Sysplex Management task**

**Description:**
The z/OSMF Sysplex Management task displays sysplex resources and their relationships. You can work with sysplex resources using graphic and table views. Topology and physical views show resources such as sysplexes, systems, coupling facilities, CPCs, and couple data sets. You can view
physical connections between systems and coupling facilities, including channel path identifiers (CHPIDs) and ports.

**Release introduced:**
z/OS V2R3.

**Reference information:**
- IBM z/OS Management Facility Configuration Guide
- z/OSMF online help.

### z/OSMF z/OS Operator Consoles

**Description:**
The z/OSMF z/OS Operator Consoles task provides function to work with z/OS consoles. You can issue system commands and view system messages. You can search and filter the messages, and lock the console. A summary provides a graphic view of system message activity, with colors that reflect the colors of the messages that are displayed in the console.

**Release introduced:**
z/OS V2R3.

**Reference information:**
- IBM z/OS Management Facility Configuration Guide
- z/OSMF online help.

### z/OS UNIX System Services new functions to consider

This topic describes new z/OS UNIX functions in z/OS.

#### z/OS UNIX forkcopy processing

**Description:**
Previously, with the FORKCOPY option in the BPXPRMxx parmlib member, copy-on-write (COW) mode could be specified for fork processing. The default was FORKCOPY(COW). In V2R4, the COW option is disabled. FORKCOPY will use the copy option whether COPY or COW is specified.

**Release introduced:**
z/OS V2R4

**Reference information:**
- z/OS MVS Initialization and Tuning Reference
- z/OS MVS System Commands
- z/OS UNIX System Services Planning
- IBM Health Checker for z/OS User’s Guide

#### z/OS UNIX kernel stack allocation

**Description:**
Previously, with the KERNELSTACK option in the BPXPRMxx parmlib member, stacks could be allocated either above or below the bar. The default was KERNELSTACKS(BELOW). In V2R4, stacks are always allocated above the bar. If KERNELSTACKS(BELOW) is specified, it is ignored and the stacks are allocated above the bar.

**Release introduced:**
z/OS V2R4

**Reference information:**
- z/OS MVS Initialization and Tuning Reference
- z/OS MVS System Commands
Loading RMODE64 programs into common storage

Description:
The loadHFS extended (BPX1LDX/BPX4LDX) callable service can now be used to load RMODE 64 programs directly into 64-bit common storage. After the program is loaded, it is ready to be added to the dynamic link pack area (LPA).

Release introduced:
z/OS V2R4

Reference information:
z/OS UNIX System Services Programming: Assembler Callable Services Reference

Obtaining information about RMODE64 modules that were loaded by the debugged process

Description:
With the new PT_LD64INFO option, information can be returned about the RMODE64 modules that were loaded by the debugged process.

Release introduced:
z/OS V2R4

Reference information:
z/OS UNIX System Services Programming: Assembler Callable Services Reference

Migrating HFS and zFS file systems to zFS file systems

Description:
Previously, you could only migrate mounted HFS file systems to zFS. You can now migrate mounted zFS file systems to zFS.

Release introduced:
z/OS V2R4

Reference information:
z/OS UNIX System Services Planning
z/OS UNIX System Services Command Reference

Maintaining a single configuration file across the sysplex

Description:
In V2R3, a new directory, /g1oba1, is available in the sysplex root and can be used to store and maintain a single copy of a configuration file that can be referenced by all members of the sysplex. Prior to V2R3, individual copies of the same configuration file had to be maintained in each member of the sysplex.

Release introduced:
z/OS V2R3.

Reference information:
z/OS UNIX System Services Planning
z/OS Upgrade Workflow

Migrating HFS and zFS file systems to zFS file systems

Description:
Previously, you could only migrate mounted HFS file systems to zFS. You can now migrate mounted zFS file systems to zFS.

Release introduced:
z/OS V2R4
Support for z/OS UNIX syscall exits

Description:
Pre-system call and post-system call exit routines can be enabled for select z/OS UNIX callable services.

Release introduced:
V2R3

Reference information:
z/OS UNIX System Services Programming: Assembler Callable Services Reference
z/OS UNIX System Services Planning
z/OS MVS Initialization and Tuning Reference

Mounting and unmounting file systems with the SETUID option

Description:
If a nonprivileged user has UPDATE access to the SUPERUSER.FILESYS.USERMOUNT resource in the UNIXPRIV class, the user can mount and unmount file systems with the SETUID option.

Release introduced:
V2R3

Reference information:
z/OS UNIX System Services Planning

Checking for unsecure services that are configured for the inetd daemon

Description:
A new health check, USS_INETD_UNSECURE_SERVICES, provides a report on unsecure services that are configured for the inetd daemon.

Release introduced:
V2R3

Reference information:
z/OS UNIX System Services Planning
IBM Health Checker for z/OS User's Guide

Debugging enhancements for dbx

Description:
dbx can debug applications whose debug information was merged into the NOLOAD section of the executable file if the application was compiled with options -Wc,DEBUG(NOFILE) or -qdebug=nofile.

Release introduced:
V2R3

Reference information:
z/OS UNIX System Services Programming Tools

Reporting CPU time in microseconds

Description:
The getthent() callable service (BPX1GTH/BPX4GTH) returns CPU usage in microseconds.

Release introduced:
V2R2 APAR OA49485
Automatically unmounting unused version root file systems in a shared file system

Description:
Version file systems in a shared file system that are no longer being used can be automatically unmounted.

Release introduced:
z/OS V2R3

Reference information:
z/OS UNIX System Services Planning

Displaying lines before or after matching lines

Description:
The `grep`, `fgrep`, and `egrep` commands have been enhanced so that users can specify the number of lines to be displayed either before or after the matching lines.

Release introduced:
z/OS V2R3

Reference information:
z/OS UNIX System Services Command Reference

Year 2038/2042 support

Description:
Support was added for POSIX time values beyond year 2038 and z/OS time-of-day values beyond year 2042.

Release introduced:
z/OS V2R3

Reference information:
z/OS UNIX System Services Programming: Assembler Callable Services Reference

Invoking `pthread_security_np()` without a password or superuser authority

Description:
If a user has UPDATE access to the BPX.DAEMON resource, the user can now invoke the `pthread_security_np()` service without a password or superuser authority.

Release introduced:
V2R2 APAR OA50425

Reference information:
z/OS UNIX System Services Programming: Assembler Callable Services Reference

Updated monitoring of the current usage of private below-the-bar storage

Description:
The USS_KERNEL_PVTSTG_THRESHOLD health check now supports dynamic severity check parameters when KERNELSTACKS(BELOW) is specified.

Release introduced:
z/OS V2R2, with APAR OA50127 installed.

Reference information:
IBM Health Checker for z/OS User's Guide
Enhancements to the logger shell command

**Description:**
You can use the `logger` shell command to send messages that are longer than 126 characters. Messages can also be sent to the syslogd daemon.

**Release introduced:**
z/OS V2R3

**Reference information:**
*z/OS UNIX System Services Command Reference*

Assigning default umask values to all z/OS UNIX users

**Description:**
The new UMASK statement of the BPXPRMxx parmlib member can be used to assign a default umask value for all z/OS UNIX users. It lists the disallowed permission settings of files and directories that are created by users or processes.

**Release introduced:**
z/OS V2R2, with APAR OA51000 installed.

**Reference information:**
*z/OS MVS Initialization and Tuning Reference*
Appendix A. Accessibility

Accessible publications for this product are offered through IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

If you experience difficulty with the accessibility of any z/OS information, send a detailed message to the Contact z/OS web page (www.ibm.com/systems/z/os/zos/webqs.html) or use the following mailing address.

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
United States

Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features in z/OS can help users do the following tasks:

• Run assistive technology such as screen readers and screen magnifier software.
• Operate specific or equivalent features by using the keyboard.
• Customize display attributes such as color, contrast, and font size.

Consult assistive technologies

Assistive technology products such as screen readers function with the user interfaces found in z/OS. Consult the product information for the specific assistive technology product that is used to access z/OS interfaces.

Keyboard navigation of the user interface

You can access z/OS user interfaces with TSO/E or ISPF. The following information describes how to use TSO/E and ISPF, including the use of keyboard shortcuts and function keys (PF keys). Each guide includes the default settings for the PF keys.

• z/OS TSO/E Primer
• z/OS TSO/E User's Guide
• z/OS ISPF User's Guide Vol I

Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users who access IBM Knowledge Center with a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line because they are considered a single compound syntax element.
Each line starts with a dotted decimal number; for example, 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that the screen reader is set to read out punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number 3.1) are mutually exclusive alternatives. If you hear the lines 3.1 USERID and 3.1 SYSTEMID, your syntax can include either USERID or SYSTEMID, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The * symbol is placed next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element *FILE with dotted decimal number 3 is given the format 3 \* FILE. Format 3* FILE indicates that syntax element FILE repeats. Format 3* \* FILE indicates that syntax element FILE repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol to provide information about the syntax elements. For example, the lines 5.1*, 5.1 LASTRUN, and 5.1 DELETE mean that if you use more than one of the LASTRUN and DELETE syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, it indicates a reference that is defined elsewhere. The string that follows the % symbol is the name of a syntax fragment rather than a literal. For example, the line 2.1 %OP1 means that you must refer to separate syntax fragment OP1.

The following symbols are used next to the dotted decimal numbers.

? indicates an optional syntax element

The question mark (?) symbol indicates an optional syntax element. A dotted decimal number followed by the question mark symbol (?) indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example 5? NOTIFY). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines 5 ?, 5 NOTIFY, and 5 UPDATE, you know that the syntax elements NOTIFY and UPDATE are optional. That is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.

! indicates a default syntax element

The exclamation mark (!) symbol indicates a default syntax element. A dotted decimal number followed by the ! symbol and a syntax element indicate that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the dotted decimal number can specify the ! symbol. For example, if you hear the lines 2? FILE, 2.1! (KEEP), and 2.1 (DELETE), you know that (KEEP) is the default option for the FILE keyword. In the example, if you include the FILE keyword, but do not specify an option, the default option KEEP is applied. A default option also applies to the next higher dotted decimal number. In this example, if the FILE keyword is omitted, the default FILE (KEEP) is used. However, if you hear the lines 2? FILE, 2.1, 2.1! (KEEP), and 2.1.1 (DELETE), the default option KEEP applies only to the next higher dotted decimal number, 2.1 (which does not have an associated keyword), and does not apply to 2? FILE. Nothing is used if the keyword FILE is omitted.

* indicates an optional syntax element that is repeatable

The asterisk or glyph (*) symbol indicates a syntax element that can be repeated zero or more times. A dotted decimal number followed by the * symbol indicates that this syntax element can be used zero or more times; that is, it is optional and can be repeated. For example, if you hear the line 5.1* data area, you know that you can include one data area, more than one data area, or no data area. If you
hear the lines 3*, 3 HOST, 3 STATE, you know that you can include HOST, STATE, both
together, or nothing.

Notes:
1. If a dotted decimal number has an asterisk (*) next to it and there is only one item with that dotted
decimal number, you can repeat that same item more than once.
2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal
number, you can use more than one item from the list, but you cannot use the items more than
once each. In the previous example, you can write HOST STATE, but you cannot write HOST HOST.
3. The * symbol is equivalent to a loopback line in a railroad syntax diagram.

+ indicates a syntax element that must be included
The plus (+) symbol indicates a syntax element that must be included at least once. A dotted decimal
number followed by the + symbol indicates that the syntax element must be included one or more
times. That is, it must be included at least once and can be repeated. For example, if you hear the line
6.1+ data area, you must include at least one data area. If you hear the lines 2+, 2 HOST, and
2 STATE, you know that you must include HOST, STATE, or both. Similar to the * symbol, the +
symbol can repeat a particular item if it is the only item with that dotted decimal number. The +
symbol, like the * symbol, is equivalent to a loopback line in a railroad syntax diagram.
This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for the Knowledge Centers. Use of hyperlinks in other output formats of this information is at your own risk.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Site Counsel
2455 South Road

© Copyright IBM Corp. 2000, 2019
Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or
reproduce, distribute or display these publications or any portion thereof outside your enterprise, without
the express consent of IBM.

**Rights**

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either
express or implied, to the publications or any information, data, software or other intellectual property
contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of
the publications is detrimental to its interest or, as determined by IBM, the above instructions are not
being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable
laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE
PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,
INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT,
AND FITNESS FOR A PARTICULAR PURPOSE.

---

**IBM Online Privacy Statement**

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies
or other technologies to collect product usage information, to help improve the end user experience, to
tailor interactions with the end user, or for other purposes. In many cases no personally identifiable
information is collected by the Software Offerings. Some of our Software Offerings can help enable you to
collect personally identifiable information. If this Software Offering uses cookies to collect personally
identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect
each user’s name, email address, phone number, or other personally identifiable information for purposes
of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling
them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect
personally identifiable information from end users via cookies and other technologies, you should seek
your own legal advice about any laws applicable to such data collection, including any requirements for
notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see
IBM’s Privacy Policy at ibm.com/privacy and IBM’s Online Privacy Statement at ibm.com/privacy/details in
the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM Software Products
and Software-as-a-Service Privacy Statement” at ibm.com/software/info/product-privacy.

---

**Policy for unsupported hardware**

Various z/OS elements, such as DFSMS, JES2, JES3, and MVS, contain code that supports specific
hardware servers or devices. In some cases, this device-related element support remains in the product
even after the hardware devices pass their announced End of Service date. z/OS may continue to service
element code; however, it will not provide service related to unsupported hardware devices. Software
problems related to these devices will not be accepted for service, and current service activity will cease if
a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.
Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and Trademark information (www.ibm.com/legal/copytrade.shtml).
Index

Special Characters
/gLOBAL directory 82

Numerics
64-bit support for Enterprise PL/I 66
8 character user ID 65, 75, 76

A
accessibility
contact IBM 87
features 87
Advanced Copy Services catalog 48
Advanced Copy Services enhancements 49
aggregate attributes (zFS)
changing 80
zFS (z/OS File System)
changing aggregate attributes 80
application development 37
assistive technologies 87

B
base element
fonts 21
z/OSMF 80
Base element
z/OS Font Collection 12
base elements 1
BCP
new function 22
BCPii 22

C
Catalog enhancements 49
Communications Server
new function 29
support considerations 29
console 24
contact
z/OS 87
CPU usage
reporting in microseconds 83
cross-system coupling facility (XCF) 28

D
DADSM/CVAF 49
DADSM/CVAF enhancements 49
data set encryption enhancements 52
dbx
debugging enhancement 83
db data block 67
DFSMS catalog 49
DFSMS data set encryption 52
DFSMS device support 48
DFSMS device support enhancements 48
DFSMS Object Access Method (OAM) 51
DFSMS VSAM 52
DFSMsdss 49
DFSMsdss enhancements 49
DFSMShsm 50
DFSMShsm enhancements 50
DFSMSrmm 50
DFSMSrmm enhancements 50
DFSMSTvs 51
DFSMSTvs enhancements 51
diagnosis
new 21
Distributed File Service/Server Message Block (DFS/SMB)
removal of 78

F
feedback ix
fonts 12, 21
Function Registry 24

G
grep shell command
displaying lines before or after matching lines 84

H
Hardware Configuration Manager (HCM) 16
hardware support 29
health check
for z/OS UNIX 83
identifying SMB-exported file systems 79
Health Check for JES2 Checkpoint Configuration 63

I
IBM Function Registry for z/OS 24
IBM HTTP Server - Powered by Apache 8
IBM Knowledge Center for z/OS 17, 21
IBM Tivoli Directory Server
enhanced activity logging 55
enhanced SDBM search 54
Transport Layer Security (TLS) protocol version 1.3 55
Infoprint Server
new function 56
overview 18
V2R3 new function 57–60
V2R4 new function 57–59
Input/Output Supervisor 25
Instruction Execution Protection (IEP) 63
Integrated Security Services 95
Integrated Security Services
new function 60
ISPF
new function 61

J
Japanese New Era support 65
JES2 62
JES2 disk reader support 62
JES2 Dynamic groups support 64
JES2 Email support 64
JES2 JCL Simplification 64
JES2 JES3 JCL support 64
JES2 Managing JES2 resources 64
JES2 policies 62
JES3 65

K
kernel stack allocation
for z/OS UNIX 81
forkcopy processing 81
keyboard
navigation 87
PF keys 87
shortcut keys 87

L
Language Environment
64-bit support for Enterprise PL/I 66
detecting buffer overflows 66
enabling non-executable memory 65
Japanese New Era Support 65
tracking specific price metrics 65
Library Server
optional feature
 IBM Knowledge Center for z/OS 21
loading RMODE64 programs
into common storage for z/OS UNIX 82
logger shell command
sending messages longer than 126 characters 85
sending messages to the syslogd daemon 85
LOGON timeout 75

M
migrating from HFS or zFS to zFS 82
monitoring current usage of private below-the-bar storage
updated in V2R2 (APAR OA50127) 84
mounting and unmounting file systems
with the SETUID option 83
multi-row fetch 56
MVS
new function 22

N
navigation
keyboard 87
new function 22
BCP 22

new function (continued)
Integrated Security Services 60
MVS 22
NFS 67

O
Object Access Method (OAM) enhancements 51
OpenSSH
overview 13
optional feature
 IBM Knowledge Center for z/OS 21
optional features 2

P
prefix data block 66, 67
price metrics, tracking 65
pthread_security_np() enhancement 84

R
Reporting JES2 resiliency data 63
Resource Measurement Facility (RMF)
V2R3 68
RMODE64 modules
returning information about 82
RSM 25

S
scalability and performance 31
Security Server (RACF)
new function 71
sending to IBM
 reader comments ix
Server-Requester Programming Interface (SRPI) and TSO/E
Enhanced Connectivity Facility removal 75
shared consoles 24
shortcut keys 87
SMB support of zFS
listing SMB files (health check) 79
SMF records
for zFS 80
SMS 51
SMS enhancements 51, 52
storage management 25
summary of changes
z/OS Introduction and Release Guide xiii
SuperPAV dynamic alias management 25
support consideration 29
syscall exits
support for z/OS UNIX 83
sysplex services 28
system logger 27
system-level
new element
 fonts 21
new function
 component diagnosis 21
 systems management 33
T
trademarks 94

U
umask
assigning values to all z/OS UNIX users 85
Unicode 3, 28
usability and skills 30
Use special characters within passwords 75
user interface
  ISPF 87
  TSO/E 87

V
V2R3 xv
version root file systems
unmounting automatically 84
VSAM enhancements 52
VSAM RLS enhancements 52

W
What's new
  z/OS V2R3 21
  z/OS V2R4 21

X
XL C/C++
  CDAHLASM and as utilities 78
  compiler options 76
  DSECT Utility 77
  SOS info utility 77
  vector programming support 76
XML 3
Xvfb
  overview 14

Y
year 2038/2042 support 84
year 2038/2048 support 66

Z
z/OS
  base elements 1
  optional features 2
z/OS Communications Server
  security 33
z/OS File System (zFS)
  zFS support 12
z/OS File System (zFS)
  high availability option 78
  zFS File Snapshot 78
z/OS Font Collection 12, 21
z/OS Introduction and Release Guide
  summary of changes xiii
z/OS Introduction and Release Guide> (continued)
  content, changed xv
  content, deleted xv
  content, new xiii
z/OS Management Facility (z/OSMF) 13, 80
z/OS Problem Management 21
z/OS UNIX
  forkcopy processing 81
  kernel stack allocation 81
  loading RMODE64 programs into common storage 82
  migrating from HFS or zFS to zFS 82
  returning information about RMODE64 modules 82
z/OS UNIX health check 83
z/OSMF 80, 81
zFS (z/OS File System)
  compressing file system data 79
  encrypting file system data 79
  repairing mounted file system 79
  SMF records for 80
zFS aggregates
  mounting VSAM linear data sets 79
  shrinking 79
zFS (z/OS File System)
  mounting VSAM linear data sets 79
  shrinking aggregates 79