z/OS
2.5

z/OS Compliance Data Collection

Note

Before using this information and the product it supports, read the information in “Notices” on page 163.

This edition applies to Version 2 Release 5 of z/OS® (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2022-09-27

Contents

Tables

About z/OS compliance data collection

Purpose of this information This is a collection of the information needed to collect z/OS compliance data. Much of the information contained in this collection also exists elsewhere in the z/OS library.

Who should read this information This information is intended for compliance officers who are responsible for passing an audit. There is also information for people who write programs or subsystems that monitor performance.

Related information

For information about how to install, configure, deploy, and use the IBM Z® Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

To find the complete z/OS library, go to IBM Documentation (www.ibm.com/docs/en/zos).

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 xi.

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® Documentation function
If your comment or question is about the IBM Documentation functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Documentation Support at ibmdocs@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 mhvrcfs@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 section title of the specific information to which your comment relates
- The comprehensive content collection title: z/OS Compliance Data Collection
- 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.

Chapter 1. Enabling z/OS compliance data collection

z/OS 2.4 and 2.5 are enhanced to enable the collection of compliance data from IBM z16 CPACF counters and a number of z/OS products and components. A z/OSMF compliance fact collection REST API sends an ENF86 signal to selected systems, while participating products and components collect and write compliance data to SMF 1154 records associated with its unique subtype.

z/OS compliance data (SMF 1154 records) can be integrated into solutions, such as the IBM Z Security and Compliance Center. This IBM solution works with products and elements on your z/OS system to collect and validate compliance data. For more information, see the IBM Z Security and Compliance Center documentation (www.ibm.com/docs/en/zscc/1.1.0).

This topic lists a number of specific PTFs for enabling compliance data collection on a z/OS system. To identify and install the complete set of required PTFs, use the following fix category (FIXCAT), which is designated specifically for z/OS compliance data collection support:

```
IBM.Function.Compliance.DataCollection
```

Enabling z/OSMF

Install PTFs for the following core infrastructure components on z/OS 2.4 or later.

- z/OSMF: PH37308
- CEA: OA61443

Configure the z/OSMF nucleus on your system and then add the Compliance plug-in. This phase requires z/OS resources to be set up, commands to be run, and security setup to be performed for RACF (or the equivalent). Information for these activities is provided in the *IBM z/OS Management Facility Configuration Guide*.

Update the z/OSMF Systems table. For each sysplex in scope, at least one z/OSMF server must be active. The server provides REST API support and access to the Compliance plug-in. To add systems to z/OSMF, use the **Add** > **System** action in the z/OSMF Systems table. Information about this activity is provided in Defining your systems to z/OSMF (www.ibm.com/docs/en/zos/2.5.0?topic=systems-defining-your-zosmf).

Enable the Compliance plug-in, and create user authorizations for it. Information for these activities is provided in the *IBM z/OS Management Facility Configuration Guide*.

Authorize the z/OSMF server user ID to issue event notification facility (ENF) code 86. On a system with RACF, have your security administrator enter the following commands:

- RDEFINE SERVAUTH CEA.SIGNAL.ENF86 UACC(NONE)
- PERMIT CEA.SIGNAL.ENF86 CLASS(SERVAUTH) ID(IZUSVR) ACCESS(READ)
- SETR RACLIST(SERVAUTH) REFRESH

Unless you choose to manage the start-up and shutdown of the z/OSMF server through an automation product, z/OSMF is started automatically when you IPL your z/OS system. 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.

Enabling SMF

Install PTFs for the following core infrastructure components on z/OS 2.4 or later.

- SMF: OA61444

In parmlib member SMFPRMxx, select the SMF records that you want to write by specifying either the type that is desired with the TYPE option of the SYS or SUBSYS parmlib parameter.

On every image, edit the SMFPRMxx member to collect SMF record type 1154 records. Add 1154 to the list of record types that are currently specified on the TYPE= option.

For information about setting up and using SMF, see *z/OS MVS System Management Facilities (SMF)*

Collecting Data from z/OS Communications Server

Install PTFs for the following z/OS Communications Server components on z/OS 2.4 or later.

- TCP/IP: PH37372
- FTP: PH37372
- TN3270E: PH37372
- CSSMTP: PH37372

Verifying data from z/OS Communications Server

The z/OS client web enablement toolkit in *z/OS MVS Programming: Callable Services for High-Level Languages* can start the z/OS Compliance REST Interface in *IBM z/OS Management Facility Programming Guide* to drive the collection of compliance data. The request ID identifies the request for collecting data and can be correlated with the output SMF 1154 records.

After sending an HTTP request to collect compliance data, inspect the output in the SMF1154 subtype 1, 2, 3, 4 records.

- Verify that the request ID matches the REST interface call.
- Verify that the compliance data is collected and correct.

Collecting data from z/OS products and components

Install PTFs for additional products and components on z/OS 2.4 and 2.5 to enable compliance data collection. To identify and install the specific PTFs, use the following fix category (FIXCAT), which is designated specifically for compliance data collection support: IBM.Function.Compliance.DataCollection.

For information about how to use this fix category to identify and install the specific PTFs that enable compliance data collection, see IBM Fix Category Values and Descriptions (www-01.ibm.com/support/docview.wss?uid=isg3T1027683).

Validating data with the IBM Z Security and Compliance Center

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

Chapter 2. Modernized Reporting

For highly regulated industries, such as financial services, achieving compliance is a critical step toward protecting customer and application data. Compliance officers need to adhere to multiple regulations or laws at the same time. They are responsible for understanding and implementing the controls that are required for your business. They also have a responsibility to gather data that proves to external auditors that security checks are in place and systems are in continuous compliance.

z/OS is enhanced to enable the collection of compliance data from the IBM z16 CP Assist for Cryptographic Function (CPACF) counters and several z/OS products and components. A new z/OSMF compliance data collection REST API sends an event notification facility (ENF) signal to all systems. Participating products and components collect and write compliance data to new SMF 1154 records associated with its unique subtype. These new SMF 1154 records can be integrated into solutions, such as the IBM Z Security and Compliance Center.

This support requires PTFs for z/OS 2.4 and z/OS 2.5. The PTFs are identified by a fix category that is designated specifically for Compliance data collection support named `IBM.Function.Compliance.DataCollection`. Use this fix category to identify and install the specific PTFs that enable compliance data collection.

This collection includes updates to the following publications:

- *z/OS MVS Programming: Authorized Assembler Services Guide*
- *z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG*
- *z/OS MVS Initialization and Tuning Reference*
- *z/OS MVS System Commands*
- *z/OS MVS System Management Facilities (SMF)*
- *z/OS MVS System Messages, Vol 6 (GOS-IEA)*
- *z/OS MVS System Messages, Vol 7 (IEB-IEE)*

For more information regarding z/OS Compliance, visit the .

Event notification facility

A new event notification facility (ENF) code, 86, was added.

Table 1. ENF macro event codes

Event code	Description	Qualifier	Parameter list passed to the user exit	Exit type / Cross-system capable
86	Signaled by a z/OSMF Compliance REST API to initiate compliance evidence data collection by products and z/OS components that listen for the signal.	None	Mapped by CEAENF86 The parameter list identifies which systems are to collect and report the compliance data. Listen exits collect and report the data on the matching systems. Compliance data is recorded by participating products and z/OS components in an assigned subtype of the SMF type 1154 record. Each signal provides a request identifier in the parameter list. This request identifier is recorded in each SMF 1154 record.	EXIT or SRBEXIT / YES

Record type 1154

SMF record type 1154 (X'482') – z/OS compliance evidence is added, along with subtype 128.

Record type 1154 (X'482') — z/OS compliance evidence

The type 1154 record provides compliance evidence. A different subtype is assigned to each participating z/OS component or product.

On receiving an ENF86 signal from the z/OSMF Compliance REST API, participating components and products collect and write compliance data to their associated SMF 1154 subtype records. Each 1154 subtype record includes the SMF extended header, as defined by the IFASMFH macro, and the SMF 1154 common area, as defined by the IFAR1154 macro. The remainder of the subtype data in each SMF 1154 subtype record is unique to each participating component or product.

The type 1154 subtype specific records are mapped using the following mapping macros:

- IFASMFH, which maps the SMF standard and extended header area of the record.
- IFAR1154, which maps the SMF type 1154 common header that resides in the record just past the SMF extended header. This map contains triplets that are used to navigate to the subtype specific area of the record.
- A subtype-specific mapping macro, which maps the area that resides in the record just past the SMF 1154 common area.

All three mapping macros must be included in programs that process SMF 1154 subtype records.

Subtype-specific triplet information: The subtype specific area can be located in each SMF 1154 subtype record by using the following triplet fields. These fields are defined in the IFAR1154 mapping macro.

Offset
SMF1154_SubSpec_Offset

Length
SMF1154_SubSpec_Length

Number
SMF1154_SubSpec_Number

Record environment

The record environment varies for each subtype record. See the environment information for each subtype.

Record environment

The record environment varies for each subtype record. See the environment information for each subtype.

Record common area mapping

All subtypes of the type 1154 record begin as described in "Header/self-defining section". The offsets shown are relative to the beginning of the sections being described.

Header/self-defining section

The header/self-defining section consists of a common triplets section and a common header section.

Subtype specific sections

Each subtype specific section of record type 1154 begins with its own self-defining section that describes its contents.

Table 2 on page 5 lists the SMF type 1154 record subtypes and where to find their record mappings.

Table 2. Subtypes of SMF record type 1154

Subtype	Description	Where to find subtype record mapping
1	TCP/IP stack	Type 1154 SMF records in *z/OS Communications Server: IP Programmer's Guide and Reference*
2	FTP daemon	Type 1154 SMF records in *z/OS Communications Server: IP Programmer's Guide and Reference*
3	TN3270	Type 1154 SMF records in *z/OS Communications Server: IP Programmer's Guide and Reference*
4	CSSMTP	Type 1154 SMF records in *z/OS Communications Server: IP Programmer's Guide and Reference*
49	ICSF	See ICSF SMF records in *z/OS Cryptographic Services ICSF System Programmer's Guide*.
50	Consoles	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
51	DFSMSdfp	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
52	DFSMSrmm	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
53	DFSMShsm	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
54	DFSMSdss	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
77	z/OS UNIX System Services	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
78	SSHD	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
79	INETD	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
80	CICS® TS for z/OS	See SMF 1154 subtype 80 record (www.ibm.com/docs/en/cics-ts/6.1?topic=reference-smf-1154-subtype-80-record).
81	Db2® for z/OS	See **Db2 13 for z/OS** > **Securing Db2** in IBM Db2 for z/OS documentation (www.ibm.com/docs/en/db2-for-zos).
82	MQ region	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
83	RACF®	See Format of SMF type 1154 subtype 83 in *z/OS Security Server RACF Macros and Interfaces*.
85	IMS control region and IMS OTMA	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.

Table 2. Subtypes of SMF record type 1154 (continued)

Subtype	Description	Where to find subtype record mapping
86	IMS operation manager	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
87	IMS Connect	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
96	SMF global reporting options	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
97	SMF subsystem reporting options	See IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm) for the associated data stream description.
128	Processor activity	See "Subtype 128 - Processor activity compliance evidence".

CICS Transaction Server for z/OS

CICS Transaction Server, often called simply CICS, is a powerful, mixed-language application server that runs on z/OS.

An application server provides an environment to host applications. It can provide services to solve many concerns, such as security, transactionality, or exchanging data between new and existing applications. Developing custom enterprise-grade solutions for these issues is difficult and can take time away from focusing on what the application is intended to do for the business. Importantly, CICS can provide these services to applications that are composed of components written in different programming languages.

For z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 80 to check that security is on in all CICS regions, check that only authorized users can run programs, check that only authorized users can access files, and more.

Note: Compliance data collection for CICS requires CICS 6.1. For more information, see SMF 1154 subtype 80 record (www.ibm.com/docs/en/cics-ts/6.1?topic=reference-smf-1154-subtype-80-record).

Communications Server

CSSMPT

z/OS Communications Server provides a set of communications protocols that support peer-to-peer connectivity functions for both local and wide-area networks, including the most popular wide-area network, the Internet. z/OS Communications Server also provides performance enhancements that can benefit a variety of TCP/IP applications.

The Communication Server SMTP (CSSMTP) application is a mail forwarding SMTP client. CSSMTP processes data sets that are in the JES spool file that contain mail messages and then forwards the mail messages to a target server.

For z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 4 to check whether CSSMTP servers are configured to always use AT-TLS, check whether CSSMTP servers are configured to audit important events, and more.

Note: Compliance data collection for Comm Server: CSSMTP requires z/OS 2.4 or later and PTFs for PH37372.

SMF type 1154, subtype 4 – CSSMTP client compliance evidence record

The CSSMTP client compliance evidence record provides information that is collected from the CSSMTP configuration file, START parameters, and UNIX environment variables.

The triplets in the 1154 subtype 4 specific section indicate which sections (and how many instances of the section) are included in the record.

1154 subtype 4 specific section, self-defining section

This section defines the additional sections that are included in the record. A triplet is included for each defined section. The triplet includes the offset to the section from the start of the record, the length of a single instance of the section, and the number of instances of the section in the record.

Table 3. 1154 subtype 4 specific section, self-defining section

Offset	Name	Length	Format	Description
0(X'00')	SMF1154_4_TRN	2	Binary	Number of triplets (set to 4)
2(X'02')		2		Reserved (set to 0)
4(X'04')	SMF1154_4_S1_Offset	4	Binary	Offset to CSSMTP identification section (from the start of the record)
8(X'08')	SMF1154_4_S1_Length	2	Binary	Length of CSSMTP identification section
10(X'0A')	SMF1154_4_S1_Number	2	Binary	Number of CSSMTP identification sections (set to 1)
12(X'0C')	SMF1154_4_S2_Offset	4	Binary	Offset to CSSMTP configuration section (from the start of the record)
16(X'10')	SMF1154_4_S2_Length	2	Binary	Length of CSSMTP configuration section
18(X'12')	SMF1154_4_S2_Number	2	Binary	Number of CSSMTP configuration sections (set to 1)
20(X'14')	SMF1154_4_S3_Offset	4	Binary	Offset to CSSMTP target server section (from the start of the record)
24(X'18')	SMF1154_4_S3_Length	2	Binary	Length of CSSMTP target server section
26(X'1A')	SMF1154_4_S3_Number	2	Binary	Number of CSSMTP target server sections
28(X'1C')	SMF1154_4_S4_Offset	4	Binary	Offset to CSSMTP configuration data section (from the start of the record)
32(X'20')	SMF1154_4_S4_Length	2	Binary	Length of CSSMTP configuration data section
34(X'22')	SMF1154_4_S4_Number	2	Binary	Number of CSSMTP configuration data sections (set to 1)

CSSMTP identification section

This section identifies the CSSMTP client that created this SMF record.

Table 4. CSSMTP identification section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_4_MLCI_Ident	4	EBCDIC	Identifier - 'MLCI'
4(X'4')	SMF1154_4_MLCI_JMR	24	Structure	**Job Management Record**
4(X'4')	SMF1154_4_MLCI_Job	8	EBCDIC	Jobname
12(X'C')	SMF1154_4_MLCI_Entry	4	Binary	Time since midnight, in hundredths of a second, when CSSMTP was started.

Table 4. CSSMTP identification section (continued)				
Offset	**Name**	**Length**	**Format**	**Description**
16(X'10')	SMF1154_4_MLCI_EDate	4	Packed	Date when CSSMTP was started, in the form 0cyydddF.
20 (X'14')	SMF1154_4_MLCI_USEID	8	EBCDIC	User-defined identification field (taken from common exit parameter area, not from USER=parameter on job statement).
28 (X'1C')	SMF1154_4_MLCI_ExtWrt	8	EBCDIC	**External writer name** Configured with the ExtWrtName statement.
36(X'24')	SMF1154_4_MLCI_Jes	4	EBCDIC	**JES subsystem name**

CSSMTP configuration section

This section provides configuration settings for this CSSMTP client.

Table 5. CSSMTP configuration section				
Offset	**Name**	**Length**	**Format**	**Description**
0(X'0')	SMF1154_4_MLCF_Ident	4	EBCDIC	Identifier – 'MLCF'
4(X'4')	SMF1154_4_MLCF_Tcpip	8	EBCDIC	**TCP/IP stack with which CSSMTP has affinity** TCP/IP stack name if the CSSMTP client has stack affinity. Otherwise, set to blanks. Set from the -p/-P CSSMTP start option.
12(X'C')	SMF1154_4_MLCF_UserInfo	1	Binary	**CSSMTP user information included in mail header** • 0 – User information is not inserted into the mail message header by CSSMTP • 1 – User information is inserted into the mail message header by CSSMTP Configured with the UserInfo parameter on the Header statement.
13(X'D')	SMF1154_4_MLCF_SmfConf	1	Binary	**CSSMTP configuration SMF 119 records** • 0 – CSSMTP configuration SMF 119 records not requested • 1 – CSSMTP configuration SMF 119 records requested Configured with the Config parameter on the SMF119 statement.

Table 5. CSSMTP configuration section (continued)

Offset	Name	Length	Format	Description
14(X'E')	SMF1154_4_MLCF_SmfConn	1	Binary	**CSSMTP connection SMF 119 records** • 0 – CSSMTP connection SMF 119 records not requested • 1 – CSSMTP connection SMF 119 records requested Configured with the Connect parameter on the SMF119 statement.
15(X'F')	SMF1154_4_MLCF_SmfMail	1	Binary	**CSSMTP mail message SMF 119 records** • 0 – CSSMTP mail message SMF 119 records not requested • 1 – CSSMTP mail message SMF 119 records requested Configured with the Mail parameter on the SMF119 statement.
16(X'10')	SMF1154_4_MLCF_SmfSpool	1	EBCDIC	**CSSMTP spool SMF 119 records** • 0 – CSSMTP spool SMF 119 records not requested • 1 – CSSMTP spool SMF 119 records requested Configured with the Spool parameter on the SMF119 statement.
17(X'11')	SMF1154_4_MLCF_SmfStats	1	Binary	**CSSMTP statistics SMF 119 records** • 0 – CSSMTP statistics SMF 119 records not requested • 1 – CSSMTP statistics SMF 119 records requested Configured with the Stats parameter on the SMF119 statement.

Table 5. CSSMTP configuration section (continued)				
Offset	**Name**	**Length**	**Format**	**Description**
18(X'12')	SMF1154_4_MLCF_UserExit	1	Binary	**CSSMTP user exit version** SMF1154_4_MLCF_USEREXIT_NONE (0) - CSSMTP user exit is not configured or is not active SMF1154_4_MLCF_USEREXIT_VERSION2 (2) – CSSMTP user exit uses the exit facility token name EZBTCPIPSMTPEXIT. Only supports RFC 821 mail syntax. SMF1154_4_MLCF_USEREXIT_VERSION3(3) – CSSMTP user exit uses the exit facility token name EZATCPIPCSSMTPV3. Supports both RFC 821 and RFC 2821 mail syntax. Configured with the USEREXIT statement.
19(X'13')		1		Reserved. Set to 0.

CSSMTP target server section

This section provides configuration settings for a target server that is configured with the TargetServer statement. There can be multiple instances of this section, one for each target server.

Note: More than one target server can be defined with a single TargetServer statement.

Table 6. CSSMTP target server section				
Offset	**Name (Dim)**	**Length**	**Format**	**Description**
0(X'0')	SMF1154_4_MLTS_Ident	4	EBCDIC	Identifier – 'MLTS'
4(X'4')	SMF1154_4_MLTS_Port	2	Binary	**Target server port value** Configured with the ConnectPort parameter on the TargetServer statement.
6(X'6')	SMF1154_4_MLTS_Type	1	Binary	**Type of target server configuration** SMF1154_4_MLTS_TYPE_ADDRESS (0) - Target IP address SMF1154_4_MLTS_TYPE_NAME (1) - Target name SMF1154_4_MLTS_TYPE_MX (2) - Target mail exchange (MX) Configured with the TargetIP, TargetName, or TargetMx parameter on the TargetServer statement.

Table 6. CSSMTP target server section (continued)

Offset	Name (Dim)	Length	Format	Description
7(X'7')	SMF1154_4_MLTS_IPv6	1	Binary	**Target IP address IPv6 indicator** This field is valid if a target IP address is configured (SMF1154_4_MLTS_Type = 0). • 0 - IPv4 address provided in SMF1154_4_MLTS_IPaddr4 • 1 - IPv6 address provided in SMF1154_4_MLTS_IPaddr6
8(X'8')	SMF1154_4_MLTS_IPaddr4	4	Binary	**Target IPv4 address** This field is valid if a target IPv4 address is configured (SMF1154_4_MLTS_Type = 0 and SMF1154_4_MLTS_IPv6 = 0). Configured with the TargetIP parameter on the TargetServer statement.
8(X'8')	SMF1154_4_MLTS_IPaddr6	16	Binary	**Target IPv6 address** This field is valid if a target IPv6 address is configured (SMF1154_4_MLTS_Type = 0 and SMF1154_4_MLTS_IPv6 = 1). Configured with the TargetIP parameter on the TargetServer statement.
24(X'18')	SMF1154_4_MLTS_Secure	1	Binary	**TLS support required** Indicates whether Transport Layer Security (TLS) is required between the CSSMTP client and the target server. SMF1154_4_MLTS_SECURE_TLSNO (0) - TLS is not required SMF1154_4_MLTS_SECURE_TLSREQ (1) -TLS is required **Note:** If the STARTTLS SMTP command is used in the spool file, a TLS connection is attempted with the target server even if SMF1154_4_MLTS_Secure is 0. Configured with the Secure parameter on the TargetServer statement.
25(X'19')		3		Reserved. Set to 0.

CSSMTP configuration data section

This section provides configuration information for CSSMTP client configuration statements with variable-length values. There is one instance of this section with one or more variable-length entries.

The section includes a section identifier and a variable number of entries that are mapped by the SMF1154_4_MLCD_ITEM structure.

Table 7. CSSMTP configuration data section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_4_MLCD_Ident	4	EBCDIC	Identifier – 'MLCD'
4(X'4')	SMF1154_4_MLCD_Items			Configuration data items. This field consists of a variable number of entries that are mapped by the SMF1154_4_MLCD_ITEM structure (see Table 8 on page 12).

Table 8. CSSMTP configuration data section: SMF1154_4_MLCD_ITEM structure

Offset	Name	Length	Format	Description
0(X'00')	SMF1154_4_MLCD_Len	2	Binary	Configuration data length (including the lengths of the SMF1154_4_MLCD_Len and SMF1154_4_MLCD_Key fields)
2(X'02')	SMF1154_4_MLCD_Key	2	Binary	Configuration data key (See CSSMTP configuration data keys for possible values)
4(X'04')	SMF1154_4_MLCD_Data	Variable	EBCDIC	Configuration data value

Table 9. CSSMTP configuration data keys

SMF1154_4_MLCD_Key values	Data Length	Format	Description of value in SMF1154_2_FDCD_Data
SMF1154_4_MLCD_DomName (40)	1-256	EBCDIC	Resolver-supplied domain name
SMF1154_4_MLCD_HostName (41)	1-64	EBCDIC	Resolver-supplied host name
SMF1154_4_MLCD_TargSrv1 (42)	1-256	EBCDIC	**Target server 1 value** If the first instance of the target server section is defined as a TargetIP, the data field that is identified with this key contains a text version of the IP address. Otherwise, it contains a target name or target MX name value. Configured with the TargetIP, TargetName, or TargetMx parameter on the TargetServer statement.

Table 9. CSSMTP configuration data keys (continued)

SMF1154_4_MLCD_Key values	Data Length	Format	Description of value in SMF1154_2_FDCD_Data
SMF1154_4_MLCD_TargSrv2 (43)	1-256	EBCDIC	**Target server 2 value** If the second instance of the target server section is defined as a TargetIP, the data field that is identified with this key contains a text version of the IP address. Otherwise, it contains a target name or target MX name value. Configured with the TargetIP, TargetName, or TargetMx parameter on the TargetServer statement.
SMF1154_4_MLCD_TargSrv3 (44)	1-256	EBCDIC	**Target server 3 value** If the third instance of the target server section is defined as a TargetIP, the data field that is identified with this key contains a text version of the IP address. Otherwise, it contains a target name or target MX name value. Configured with the TargetIP, TargetName, or TargetMx parameter on the TargetServer statement.
SMF1154_4_MLCD_TargSrv4 (45)	1-256	EBCDIC	**Target server 4 value** If the fourth instance of the target server section is defined as a TargetIP, the data field that is identified with this key contains a text version of the IP address. Otherwise, it contains a target name or target MX name value. Configured with the TargetIP, TargetName, or TargetMx parameter on the TargetServer statement.

FTP

z/OS Communications Server provides a set of communications protocols that support peer-to-peer connectivity functions for both local and wide-area networks, including the most popular wide-area network, the Internet. z/OS Communications Server also provides performance enhancements that can benefit a variety of TCP/IP applications.

The FTP command runs the FTP client program that enables you to transfer data sets and files between your local host and another host running an FTP server. Using the FTP command and its subcommands, you can sequentially access multiple hosts without leaving the FTP client.

For z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 3 to check whether TELNETPARMS statements for all TN3270E servers are configured with appropriate inactivity timeouts, check whether PARMSGROUP statements for all TN3270E servers specify appropriate inactivity timeout values, and more.

Note: Compliance data collection for Comm Server: FTP requires z/OS 2.4 or later and PTFs for PH37372

SMF type 1154, subtype 2 – FTP daemon compliance evidence record

The FTP daemon compliance evidence record provides information collected from START parameters, the FTP.DATA data set, and UNIX environment variables. The data is provided in the following sections:

- FTP daemon general configuration section provides configuration information for values with a fixed length.
- FTP daemon configuration data section provides configuration information for values with a variable length. This section is a set of variable-length entries. Each entry contains the following fields:
  - Total length of the entry
  - Key of the entry to identify the value that the entry represents
  - Value

  In this section, entries are provided only for statements that are explicitly specified. Use the key field for each entry to determine which statements are included.

1154 subtype 2 specific section, self-defining section

This section defines the additional sections that are included in the record. A triplet is included for each defined section. The triplet includes the offset to the section from the start of the record, the length of a single instance of the section, and the number of instances of the section in the record.

Table 10. 1154 subtype 2 specific section, self-defining section

Offset	Name	Length	Format	Description
0(X'00')	SMF1154_2_TRN	2	Binary	Number of triplets (set to 2)
2(x'02')		2		Reserved (set to 0)
4(x'04')	SMF1154_2_S1_Offset	4	Binary	Offset to FTP daemon general configuration section (from the start of the record)
8(x'08')	SMF1154_2_S1_Length	2	Binary	Length of FTP daemon general configuration section
10(x'0A')	SMF1154_2_S1_Number	2	Binary	Number of FTP daemon general configuration sections (set to 1)
12(x'0C')	SMF1154_2_S2_Offset	4	Binary	Offset to FTP daemon configuration data section (from the start of the record)
16(x'10')	SMF1154_2_S2_Length	2	Binary	Length of FTP daemon configuration data section
18(x'12')	SMF1154_2_S2_Number	2	Binary	Number of FTP daemon configuration data sections (set to 1)

FTP daemon general configuration section

This section provides FTP daemon configuration information for values with a fixed length.

Table 11. FTP daemon general configuration section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_2_FDCFIdent	4	EBCDIC	Identifier - 'FDCF'

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
4(X'4')	SMF1154_2_FDCFApplName	8	EBCDIC	**FTP server application name**
12(X'C')	SMF1154_2_FDCFStartTime	4	Binary	**Time FTP daemon started** (UTC)
16(X'10')	SMF1154_2_FDCFStartDate	4	Binary	**Date FTP daemon started** (UTC)
20(X'14')	SMF1154_2_FDCFPort	2	Binary	**FTP server PORT**
22(X'16')	SMF1154_2_FDCFLowPasvDataPort	2	Binary	**Passive data port range start** • 0 – Passive data port range not configured. • >0 - Beginning value in port range FTP server is allowed to use as listening data socket port. Configured with the PASSIVEDATAPORTS statement
24(X'18')	SMF1154_2_FDCFHighPasvDataPort	2	Binary	**Passive data port range end** • 0 – Passive data port range not configured. • >0 - Ending value in port range FTP server is allowed to use as listening data socket port. Configured with the PASSIVEDATAPORTS statement
26(X'1A')		1		Reserved. Set to 0.
27(X'1B')	SMF1154_2_FDCFAnonSysHFS	1	Binary	**Anonymous user access to z/OS UNIX files** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. • 0 – Do not allow anonymous users access to z/OS UNIX System Services files. • 1 – Allow anonymous users access to z/OS UNIX System Service files. Configured with the ANONYMOUSFILEACCESS statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
28(X'1C')	SMF1154_2_FDCFAnonSysMVS	1	Binary	**Anonymous user access to MVS data sets** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. • 0 - Do not allow anonymous users access to MVS data sets. • 1 - Allows anonymous users access to MVS data sets. Configured with the ANONYMOUSFILEACCESS statement
29(X'1D')	SMF1154_2_FDCFAnonFTJES	1	Binary	**Anonymous user access to JES mode** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. • 0 - Anonymous users cannot access FTP JES mode • 1 – Anonymous users can access FTP JES mode Configured with ANONYMOUSFILETYPEJES statement
30(X'1E')	SMF1154_2_FDCFAnonFTSEQ	1	Binary	**Anonymous user access to SEQ mode** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. • 0 - Anonymous users cannot access FTP SEQ mode • 1 – Anonymous users can access FTP SEQ mode Configured with ANONYMOUSFILETYPESEQ statement
31(X'1F')	SMF1154_2_FDCFAnonFTSQL	1	Binary	**Anonymous user access to SQL mode** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. • 0 - Anonymous users cannot access FTP SQL mode • 1 – Anonymous users can access FTP SQL mode Configured with ANONYMOUSFILETYPESQL statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
32(X'20')	SMF1154_2_FDCFAnonUser	8	EBCDIC	**Anonymous logon user ID** If anonymous logon is not allowed, the value is blanks. Otherwise, the value is the SAF identity that is assigned to the anonymous user. Configured with the ANONYMOUS statement *userid* value or set to 'ANONYMO' if the ANONYMOUS statement is configured without a userid.
40(X'28')	SMF1154_2_FDCFAnonPass	1	Binary	**Anonymous logon password configured** • 0 – Anonymous logon is not configured with userid/password • 1 – Anonymous logon is configured with userid/password Configured with the *password* value on the ANONYMOUS statement
41(X'29')	SMF1154_2_FDCFAnonSurr	1	Binary	**Anonymous logon configured with SURROGATE option** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. • 0 – Anonymous logon is not configured with userid/SURROGATE • 1 – Anonymous logon is configured with userid/SURROGATE Configured with the SURROGATE value on the ANONYMOUS statement
42(X'2A')		6		Reserved, set to 0
48(X'30')	SMF1154_2_FDCFAnonHFSDirM	4	Binary	**z/OS Unix mode bits for directories created by anonymous users** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. The three octal digits describe the mode bits used for z/OS UNIX directories that are created by anonymous users. Configured with the ANONYMOUSHFSDIRMODE statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
52(X'34')	SMF1154_2_FDCFAnonHFSFileM	4	Binary	**z/OS Unix mode bits for files created by anonymous users** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. The three octal digits describe the mode bits used for z/OS UNIX files that are created by anonymous users. Configured with the ANONYMOUSHFSFILEMODE statement.
56(X'38')	SMF1154_2_FDCFAnonLevel	1	Binary	**Anonymous level** Type of access permitted to users logged in as an anonymous user. Levels 1, 2, and 3 are defined. Configured with the ANONYMOUSLEVEL statement
57(X'39')	SMF1154_2_FDCFAnonFTPLog	1	Binary	**FTP server activity logged for anonymous user** • 0 – FTP server does not log activity for an anonymous user • 1 – FTP server logs activity for an anonymous user Configured with the ANONYMOUSFTPLOGGING statement
58(X'3A')	SMF1154_2_FDCFAccErrMsg	1	Binary	**Detailed logon failure replies sent to client** • 0 – FTP server does not send detailed login failure replies • 1 – FTP server sends detailed login failure replies Configured with the ACCESSERRORMSGS statement
59(X'3B')	SMF1154_2_FDCFDebugOnSite	1	Binary	**SITE DEBUG command accepted** • 0 – FTP server does not accept a SITE DEBUG command • 1 – FTP server accepts SITE DEBUG command to change the general trace options for the current session Configured with the DEBUGONSITE statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
60(X'3C')	SMF1154_2_FDCFDumpOnSite	1	Binary	**SITE DUMP command accepted** • 0 – FTP server does not accept a SITE DUMP command • 1 – FTP server accepts a SITE DUMP command to change the extended trace options Configured with the DUMPONSITE statement
61(X'3D')	SMF1152_2_FDCFPassPhrase	1	Binary	**Passphrase login allowed** • 0 – FTP server does not allow an FTP client to login with a password phrase • 1 – FTP server allows an FTP client to login with a password phrase Configured with the PASSPHRASE statement
62(X'3E')	SMF1154_2_FDCFPortEntry4	1	Binary	**Resource profile class for login** • 0 (TERMINAL) – Use the TERMINAL class with the IPv4 address • 1 (SERVAUTH) – Use SERVAUTH class resource if the IPv4 client address is mapped into a network security zone by a NETACCESS statement, otherwise use the TERMINAL class with the IPv4 client address Configured with the PORTOFENTRY4 statement
63(X'3F')	SMF1152_2_FDCFSecImpZos	1	Binary	**TLS handshake timing for implicit secure ports** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) • 0 - FTP server expects the TLS handshake before it sends the initial reply 220 • 1 – FTP server expects the TLS handshake to occur after it sends the initial reply 220 Configured with the SECUREIMPLICITZOS statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
64(X'40')	SMF1154_2_FDCFSMFType119	1	Binary	**FTP server SMF 119 records** • 0 - FTP server SMF type 119 records are not requested • 1 – All FTP server SMF type 119 records are requested Configured with the SMF TYPE119 statement
65(X'41')	SMF1154_2_FDCFSMFJes119	1	Binary	**FTP server SMF 119 records when FILETYPE JES** • 0 – FTP server SMF type 119 records are not requested when FILETYPE JES • 1 – FTP server SMF type 119 records are requested when FILETYPE JES Configured with the SMFJES TYPE119 statement
66(X'42')	SMF1154_2_FDCFSMFSql119	1	Binary	**FTP server SMF 119 records when FILETYPE SQL** • 0 – FTP server SMF type 119 records are not requested when FILETYPE SQL • 1 – FTP server SMF type 119 records are requested when FILETYPE SQL Configured with the SMFSQL TYPE119 statement
67(X'43')	SMF1154_2_FDCFSMFAppe119	1	Binary	**FTP server SMF 119 append records** • 0 - SMF type 119, subtype 70 append records are not requested • 1 – SMF type 119, subtype 70 append records are requested Configured with the SMFAPPE or SMF TYPE119 statement
68(X'44')	SMF1154_2_FDCFSMFDcfg119	1	Binary	**FTP server SMF 119 configuration records** • 0 – SMF type 119, subtype 71 configuration records are not requested • 1 – SMF type 119, subtype 71 configuration records are requested Configured with the SMFDCFG or SMF TYPE119 statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
69(X'45')	SMF1154_2_FDCFSMFDele119	1	Binary	**FTP server SMF 119 delete records** • 0 - SMF type 119, subtype 70 delete records are not requested • 1 – SMF type 119, subtype 70 delete records are requested Configured with the SMFDEL or SMF TYPE119 statement
70(X'46')	SMF1154_2_FDCFSMFLogon119	1	Binary	**FTP server SMF 119 logon records** • 0 - SMF type 119, subtype 72 logon records are not requested • 1 – SMF type 119, subtype 72 logon records are requested Configured with the SMFLOGN or SMF TYPE119 statement
71(X'47')	SMF1154_2_FDCFSMFRen119	1	Binary	**FTP server SMF 119 rename records** • 0 - SMF type 119, subtype 70 rename records are not requested • 1 – SMF type 119, subtype 70 rename records are requested Configured with the SMFREN or SMF TYPE119 statement
72(X'48')	SMF1154_2_FDCFSMFRetr119	1	Binary	**FTP server SMF 119 retrieve records** • 0 - SMF type 119, subtype 70 retrieve records are not requested • 1 – SMF type 119, subtype 70 retrieve records are requested Configured with the SMFRETR or SMF TYPE119 statement
73(X'49')	SMF1154_2_FDCFSMFStor119	1	Binary	**FTP server SMF 119 store records** • 0 - SMF type 119, subtype 70 store records are not requested • 1 – SMF type 119, subtype 70 store records are requested Configured with the SMFSTOR or SMF TYPE119 statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
74(X'4A')	Smf1154_2_FDCFVerifyUser	1	Binary	**FTP server verifies access to SAF SERVAUTH PORT resource** • 0 – FTP server does not verify user ID access to SAF SERVAUTH PORT*xxxxx* resource (where *xxxxx* is the port on which the FTP server is listening) • 1 – FTP server verifies user ID access to SAF SERVAUTH PORT*xxxxx* resource Configured with the VERIFYUSER statement
75(X'4B')	SMF1154_2_FDCFTlscertcheck	1	Binary	**TLS certificate cross-check** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) • 0 – FTP does not perform cross-checking of certificates • 1 – FTP performs cross-checking to validate that certificates for the control and data connection are the same Configured with the TLSCERTCROSSCHECK statement
76(X'4C')	SMF1154_2_FDCFFTPLogging	1	Binary	**FTP session activity logged** SMF1154_2_FDCF_FTPLogging_FALSE(0) – FTP server does not log session activity SMF1154_2_FDCF_FTPLogging_TRUE (1) – FTP server logs session activity Configured with the FTPLOGGING statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
77(X'4D')	SFM1154_2_FDCFEmailAddrChk	1	EBCDIC	**Email addr checked on anonymous login** This field is only valid if SMF1154_2_FDCFAnonLevel = 3. SMF1154_2_FDCF_EmailAddrChk_NO ('N') – FTP server accepts an anonymous user login without validating the email address that is entered by the FTP client SMF1154_2_FDCF_EmailAddrChk_WARNING ('W') – FTP server generates a warning reply to an anonymous user login if the email address is not valid SMF1154_2_FDCF_EmailAddrChk_FAIL ('F') – FTP server rejects an anonymous user login if the email address is not valid Configured with the EMAILADDRCHECK statement
78(X'4E')	SMF1154_2_FDCFPasvDataConn	1	EBCDIC	**Verify peer IP address of data socket** SMF1154_2_FDCF_PasvDataConn_UNRESTRICT ('U') – FTP server accepts passive data connection from any IP address SMF1154_2_FDCF_PasvDataConn_NOREDIRECT ('N') – FTP server verifies that the peer address of the data socket is the client's IP address Configured with the PASSIVEDATACONN statement
79(X'4F')	SMF1154_2_FDCFJESIntLevel	1	Binary	**FTP JES interface level** Values are 1 or 2 Configured with the JESINTERFACELEVEL statement
80(X'50')	SMF1154_2_FDCFExt_AUTH_TLS	1	Binary	**TLS enabled** • 0 – TLS not enabled for FTP server • 1 – TLS enabled for FTP server Configured with the EXTENSIONS AUTH_TLS statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
81(X'51')	SMF1154_2_FDCFExt_AUTH_GSSAPI	1	Binary	**Kerberos enabled** • 0 – Kerberos not enabled for FTP server • 1 – Kerberos enabled for FTP server Configured with the EXTENSIONS AUTH_GSSAPI statement
82(X'52')		2		Reserved, set to 0
84(X'54')	SMF1154_2_FDCFInActive	4	Binary	**Inactivity timeout** FTP control connection inactivity timeout in seconds. The value is in the range of 0 – 86400 seconds. A value of 0 indicates that no inactivity timer is enabled. Configured with the INACTIVE statement
88(X'58')	SMF1154_2_FDCFJESPGTO	4	Binary	**JES PutGet timeout** JES PutGet timeout in seconds. The value is in the range of 0 – 86400. Configured with the JESPUTGETTO statement
92(X'5C')	SMF1154_2_FDCFPortcmd	1	EBCDIC	**PORT / EPRT command accepted** SMF1154_2_FDCF_Portcmd_ACCEPT ('A') – PORT and EPRT commands are accepted by the FTP server SMF1154_2_FDCF_Portcmd_REJECT ('R') – PORT and EPRT commands are rejected by the FTP server Configured with the PORTCOMMAND statement
93(X'5D')	SMF1154_2_FDCFPortcmdIPAddr	1	EBCDIC	**PORT / EPRT IP address restricted** Valid if SMF1154_2_FDCFPortCmd = A SMF1154_2_FDCF_PortcmdIPAddr_NOREDIRECT ('N') – PORT / EPRT command IP address must match the client IP address SMF1154_2_FDCF_PortcmdIPAddr_UNRESTRICT ('U') –Any IP address is accepted for the PORT and EPRT commands Configured with the PORTCOMMANDIPADDR statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
94(X'5E')	SMF1154_2_FDCFPortcmdPort	1	EBCDIC	**PORT / EPRT port restricted** Valid if SMF1154_2_FDCFPortCmd = A SMF1154_2_FDCF_PortcmdPort_NOLOWPORTS ('N') – PORT / EPRT rejected if port is less than 1024 SMF1154_2_FDCF_PortcmdPort_UNRESTRICTED ('U') – Any port is accepted for the PORT and EPRT commands Configured with the PORTCOMMANDPORT statement
95(X'5F')	SMF1154_2_FDCFRlySecLevel	1	Binary	**Restrict information in FTP replies** • 0 – No restrictions on information that is included in server FTP replies • 1 – No IP addresses, hostnames, port numbers, or server operating system level information is included in FTP replies Configured with the REPLYSECURITYLEVEL statement
96(X'60')	SMF1154_2_FDCFSecCtrConn	1	EBCDIC	**Kerberos security level for control connection** Valid if Kerberos is enabled (SMF1154_2_FDCFExt_AUTH_GSSAPI = 1) SMF1154_2_FDCF_SecCtrConn_CLEAR ('C') – Client determines whether data is protected and how SMF1154_2_FDCF_SecCtrConn_SAFE ('S') – Data must have integrity protection SMF1154_2_FDCF_SecCtrConn_PRIVATE ('P') - Data must have both integrity and privacy protection Configured with the SECURE_CTRLCONN statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
97(X'61')	SMF1154_2_FDCFSecDataConn	1	EBCDIC	**Security level for data connections (TLS and Kerberos)** Applies to TLS if TLS enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) Applies to Kerberos if Kerberos enabled (SMF1154_2_FDCFExt_AUTH_GSSAPI = 1) SMF1154_2_FDCF_SecDataConn_NEVER ('N') – Server requires data to be transferred with no cipher algorithm applied to the data SMF1154_2_FDCF_SecDataConn_CLEAR ('C') - Client determines whether data is protected and how SMF1154_2_FDCF_SecDataConn_PRIVATE ('P') • For TLS, server requires a cipher algorithm to be applied • For Kerberos, data must have both integrity and privacy protection SMF1154_2_FDCF_SecDataConn_SAFE ('S') • For TLS, this is the same as 'P' • For Kerberos, data must have integrity protection, and can also have privacy protection Configured with the SECURE_DATACONN statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
98(X'62')	SMF1154_2_FDCFSecFTP	1	EBCDIC	**Security mechanism required (TLS or Kerberos)** Applies to TLS if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) Applies to Kerberos if Kerberos is enabled (SMF1154_2_FDCFExt_AUTH_GSSAPI = 1) SMF1154_2_FDCF_SecFTP_REQUIRED ('R')– FTP client is required to login using TLS or Kerberos, depending on what is enabled SMF1154_2_FDCF_SecFTP_ALLOWED ('A') – FTP client is allowed but not required to login using TLS or Kerberos Configured with the SECURE_FTP statement
99(X'63')	SMF1154_2_FDCFSecLogin	1	EBCDIC	**Client Authentication (TLS or Kerberos)** Applies to TLS if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) Applies to Kerberos if Kerberos is enabled (SMF1154_2_FDCFExt_AUTH_GSSAPI = 1) For TLS, SMF1154_2_FDCF_SecLogin_NOCLIENTAUTH ('N') – No client authentication SMF1154_2_FDCF_SecLogin_REQUIRED ('R') – Server authenticates client certificate SMF1154_2_FDCF_SecLogin_VERIFYUSER ('V') – Certificate's user ID must match the login user ID For Kerberos, the client’s ticket is always processed: • N – Not applicable • R – Not applicable SMF1154_2_FDCF_SecLogin_VERIFYUSER ('V') – User ID in the client's ticket is verified to match the login user ID Configured with the SECURE_LOGIN statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
100(X'64')	SMF1154_2_FDCFSecPSW	1	EBCDIC	**Password required for TLS session** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) SMF1154_2_FDCF_SecPSW_OPTIONAL ('O') - Password is not required for a session protected by TLS if the client provides a certificate that can be used to authenticate the user SMF1154_2_FDCF_SecPSW_REQUIRED ('R') – Password is required for session protected by TLS Configured with the SECURE_PASSWORD statement
101(X'65')	SMF1154_2_FDCFSecPSWKerb	1	EBCDIC	**Password required by Kerberos session** Valid if Kerberos is enabled (SMF1154_2_FDCFExt_AUTH_GSSAPI = 1) SMF1154_2_FDCF_SecPSWKerb_OPTIONAL ('O') - Password is not required for a session protected by Kerberos if the user can be authenticated using a Kerberos ticket SMF1154_2_FDCF_SecPSWKerb_REQUIRED ('R') – Password is required for session protected by Kerberos Configured with the SECURE_PASSWORD_KERBEROS statement
102(X'66')	SMF1154_2_FDCFTLSMec	1	Binary	**TLS mechanism** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) SMF1154_2_FDCF_TLSMec_FTP (0) – TLS is performed by FTP (value no longer set in V2R5 or later) SMF1154_2_FDCF_TLSMec_ATTLS (1) – TLS is performed by ATTLS Configured with the TLSMECHANISM statement

Table 11. FTP daemon general configuration section (continued)

Offset	Name	Length	Format	Description
103(X'67')	SMF1154_2_FDCFTLSRfcLevel	1	Binary	**RFC4217 support level** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) SMF1154_2_FDCF_TLSRfcLevel_DRAFT (0) - DRAFT level support SMF1154_2_FDCF_TLSRfcLevel_RFC4217 (1) - RFC4217 level support SMF1154_2_FDCF_TLSRfcLevel_CCCNONOTIFY (2) - CCCNONOTIFY (value no longer set in V2R5 or later) Configured with the TLSRFCLEVEL statement
104(X'68')	SMF1154_2_FDCFTLSPort	2	Binary	**Implicit TLS port value** Configured with the TLSPORT statement
106(X'6A')	SMF1154_2_FDCFUmaskstr	3	EBCDIC	**File mode creation mask** Defines which permission bits are not to be set on when a z/OS UNIX file is created Configured with the UMASK statement
109(X'6D')	SMF1154_2_FDCFSecSessReuse	1	EBCDIC	**Secure session reuse** Valid if TLS is enabled (SMF1154_2_FDCFExt_AUTH_TLS = 1) SMF1154_2_FDCF_SecSessReuse_ALLOWED ('A') - Session reuse is allowed SMF1154_2_FDCF_SecSessReuse_REQUIRED ('R') - Reusing the FTP control connection’s TLS/SSL session is required for subsequent data connections Configured with the SECURE_SESSION_REUSE statement
110(X'6E')		2		Reserved (set to 0)

FTP daemon configuration data section

This section provides FTP daemon configuration information for values with a variable length. This section includes a set of variable-length entries. Entries are provided only for statements that are explicitly configured. Use the key field for each entry to determine which statements are included.

Table 12. FTP daemon configuration data section

Offset	Name	Length	Format	Description
0(X'00')	SMF1154_2_FDCDIdent	4	EBCDIC	Identifier – 'FDCD'
4(X'04')	SMF1154_2_FDCDItems			Configuration data items. This field consists of a variable number of entries mapped by the SMF1154_2_FDCD_ITEM structure (see Table 13 on page 30).

Table 13. FTP daemon configuration section: SMF1154_2_FDCD_ITEM structure

Offset	Name	Length	Format	Description
0(X'00')	SMF1154_2_FDCD_Len	2	Binary	Configuration data length (including the lengths of the SMF1154_2_FDCD_Len and SMF1154_2_FDCD_Key fields)
2(X'02')	SMF1154_2_FDCD_Key	2	Binary	Configuration data key (See Table 14 on page 30 for possible values)
4(X'04')	SMF1154_2_FDCD_Data	Variable	EBCDIC	Configuration data string

Table 14. FTP configuration data keys

Data type (SMF1154_2_FDCD_Key values)	Data Length	Format	Description of value in SMF1154_2_FDCD_Data
SMF1154_2_FDCD_ADMAILADDR (1)	1-256	EBCDIC	Email address of the FTP server administrator Configured with the ADMINEMAILADDRESS statement
SMF1154_2_FDCD_ANONHFSINFO (2)	1-256	EBCDIC	z/OS UNIX file mask used to find a z/OS UNIX information file whose contents are displayed when an anonymous user changes directory. The file mask can contain wildcards or can be a full file name Configured with the ANONYMOUSHFSINFO statement
SMF1154_2_FDCD_ANONLOGMSG (3)	1-1024	EBCDIC	z/OS UNIX file or MVS data set whose contents are displayed when an anonymous user logs in. Configured with the ANONYMOUSLOGINMSG statement
SMF1154_2_FDCD_ANONMVSINFO (4)	1-17	EBCDIC	MVS low-level qualifier (LLQ) used to find an MVS data set whose contents are displayed when an anonymous user changes directory to an MVS data set. The LLQ is appended to the current path. Configured with the ANONYMOUSMVSINFO statement

Table 14. FTP configuration data keys (continued)

Data type (SMF1154_2_FDCD_Key values)	Data Length	Format	Description of value in SMF1154_2_FDCD_Data
SMF1154_2_FDCD_BANNER (5)	1-1024	EBCDIC	z/OS UNIX file or MVS data set whose contents are displayed whenever a user connects to FTP. Configured with the BANNER statement
SMF1154_2_FDCD_HFSINFO (6)	1-256	EBCDIC	z/OS UNIX file mask used to find a z/OS UNIX information file whose contents are displayed when a known user changes directory. The file mask can contain wildcards or can be a full file name. Configured with the HFSINFO statement
SMF1154_2_FDCD_LOGINMSG (7)	1 – 1024	EBCDIC	z/OS UNIX file or MVS data set whose contents are displayed when a known user logs in. Configured with the LOGINMSG statement
SMF1154_2_FDCD_MVSINFO (8)	1 – 17	EBCDIC	MVS low-level qualifier (LLQ) used to find an MVS data set whose contents are displayed when a known user changes directory to an MVS data set. The LLQ is appended to the current path. Configured with the MVSINFO statement
SMF1154_2_FDCD_BPXK_SETIBMOPT_TRANSPORT (9)	1 – 8	EBCDIC	TCP/IP stack with which the FTP server has stack affinity Configured with the _BPXK_SETIBMOPT_TRANSPORT environment variable
SMF1154_2_FDCD_KRB5_SERVER_KEYTAB (10)	1 – 8	EBCDIC	KRB5_SERVER_KEYTAB environment variable value Configured with the KRB5_SERVER_KEYTAB environment variable

INETD

z/OS Communications Server provides a set of communications protocols that support peer-to-peer connectivity functions for both local and wide-area networks, including the most popular wide-area network, the Internet. z/OS Communications Server also provides performance enhancements that can benefit a variety of TCP/IP applications.

The inetd program is a generic listener program used by such servers as z/OS UNIX TELNETD and z/OS UNIX REXECD. Other servers such as z/OS UNIX FTPD have their own listener program and do not use inetd.

With the IBM Z Security and Compliance Center, you can automatically collect data from SMF Type 1154 Subtype 79 to check whether the restricted network services are provided by the inetd daemon, check whether the startup user account for the z/OS UNIX Telnet server is properly defined, and more.

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

SSHD

z/OS OpenSSH provides secure encryption for both remote login and file transfer. Some of the utilities that it includes are:

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 rcpt.

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 SSH protocol version 2. SSH protocol version 1 is no longer supported.

With the IBM Z Security and Compliance Center, you can automatically collect data from SMF Type 1154 Subtype 78 to check whether z/OS OpenSSH sshd daemon is configured to only use the SSHv2 protocol, check whether OpenSSH is running in FIPS 140-2 mode with all applicable cipher algorithms implemented using ICSF, and more.

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of industry-standard protocols and applications that enable you to share data and computing resources with other computers, both IBM and non-IBM. By using TCP/IP commands at your workstation, you can perform tasks and communicate easily with a variety of other systems and workstations. z/OS Communications Server enables the user to interactively run TCP/IP applications (TCP/IP commands) from both the Time Sharing Option (TSO) and the z/OS shell.

For z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 1 to check whether all TCP/IP stacks have AT-TLS enabled, check whether IP packet forwarding is disabled on all TCP/IP stacks, check whether TCP/IP stacks are configured to audit important events, and more.

Note: Compliance data collection for Comm Server: TCP/IP requires z/OS 2.4 or later and PTFs for PH37372

SMF type 1154, subtype 1 –TCP/IP stack compliance evidence record

The TCP/IP stack compliance evidence record provides information on current TCP/IP profile settings for a specific TCP/IP stack.

If the SMF 1154 information exceeds 32,756 bytes, multiple records are created to provide the complete set of information. In the SMF 1154 common header SMF1154_C_RecordInd indicates whether "more records follow" and SMF1154_C_SeqNum indicates the sequence number. The sequence number starts at 0 in the first record and is incremented by 1 with each additional record.

The triplets in the 1154 subtype 1 specific section indicate which sections (and how many instances of the section) are included in the record.

Records within a set of records can be correlated using the extended record subtype (SMFHDR1_STP) from the extended SMF header and the system name (SMF1154_C_SystemName), sysplex name (SMF1154_C_SysplexName), jobname (SMF1154_C_Jobname), and request ID (SMF1154_C_RequestID) from the SMF 1154 common header.

Each record contains an SMF extended header, an SMF 1154 common triplets section, an SMF 1154 common header section, and an SMF 1154 subtype 1 specific section (self-defining section). The subtype specific section indicates the additional sections that are included in the record.

1154 subtype 1 specific section, self-defining section

This section defines the additional sections that are included in the record. A triplet is included for each defined section. The triplet includes the offset to the section from the start of the record, the length of a single instance of the section, and the number of instances of the section in the record.

Table 15. 1154 subtype 1 specific section, self-defining section

Offset	Name	Length	Format	Description
0(X'00')	SMF1154_1_TRN	2	Binary	Number of triplets in this record (set to 9)
2(X'02')		2		Reserved (set to 0)
4(X'04')	SMF1154_1_S1_Offset	4	Binary	Offset to TCP/IP stack information section (from the start of the record)
8(X'08')	SMF1154_1_S1_Length	2	Binary	Length of TCP/IP stack information section
10(X'0A')	SMF1154_1_S1_Number	2	Binary	Number of TCP/IP stack information sections (set to 1)
12(X'0C')	SMF1154_1_S2_Offset	4	Binary	Offset to IPv4 configuration section (from the start of the record)
16(X'10')	SMF1154_1_S2_Length	2	Binary	Length of IPv4 configuration section
18(X'12')	SMF1154_1_S2_Number	2	Binary	Number of IPv4 configuration sections (set to 1)
20(X'14')	SMF1154_1_S3_Offset	4	Binary	Offset to IPv6 configuration section (from the start of the record)
24(X'18')	SMF1154_1_S3_Length	2	Binary	Length of IPv6 configuration section
26(X'1A')	SMF1154_1_S3_Number	2	Binary	Number of IPv6 configuration sections (set to 0 or 1)
28(X'1C')	SMF1154_1_S4_Offset	4	Binary	Offset to TCP configuration section (from the start of the record)
32(X'20')	SMF1154_1_S4_Length	2	Binary	Length of TCP configuration section
34(X'22')	SMF1154_1_S4_Number	2	Binary	Number of TCP configuration sections (set to 1)
36(X'24')	SMF1154_1_S5_Offset	4	Binary	Offset to UDP configuration section (from the start of the record)
40(X'28')	SMF1154_1_S5_Length	2	Binary	Length of UDP configuration section
42(X'2A')	SMF1154_1_S5_Number	2	Binary	Number of UDP configuration sections (set to 1)

Table 15. 1154 subtype 1 specific section, self-defining section (continued)

Offset	Name	Length	Format	Description
44(X'2C')	SMF1154_1_S6_Offset	4	Binary	Offset to Global configuration section (from the start of the record)
48(X'30')	SMF1154_1_S6_Length	2	Binary	Length of Global configuration section
50(X'32')	SMF1154_1_S6_Number	2	Binary	Number of Global configuration sections (set to 1)
52(X'34')	SMF1154_1_S7_Offset	4	Binary	Offset to Port configuration section (from the start of the record)
56(X'38')	SMF1154_1_S7_Length	2	Binary	Length of Port configuration section
58(X'3A')	SMF1154_1_S7_Number	2	Binary	Number of Port configuration sections
60(X'3C')	SMF1154_1_S8_Offset	4	Binary	Offset to Management configuration section (from the start of the record)
64(X'40')	SMF1154_1_S8_Length	2	Binary	Length of Management configuration section
66(X'42')	SMF1154_1_S8_Number	2	Binary	Number of Management configuration sections (set to 1)
68(X'44')	SMF1154_1_S9_Offset	4	Binary	Offset to Network access configuration section (from the start of the record)
72(X'48')	SMF1154_1_S9_Length	2	Binary	Length of Network access configuration section
74(X'4A')	SMF1154_1_S9_Number	2	Binary	Number of Network access configuration sections

TCP/IP stack information section

Table 16. TCP/IP stack information section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_PICOEye	4	EBCDIC	Identifier - 'PICO'
4(X'4')	SMF1154_1_PICOStartTime	8	Binary	**Time TCP/IP stack was started** (TOD clock value)
12(X'C')	SMF1154_1_PICOStartDate	4	Packed	**Date TCP/IP stack was started**
16(X'10')	SMF1154_1_PICOSysplexGrp Name	8	EBCDIC	**Sysplex group name** The value is populated when the TCP/IP stack joins the sysplex group. If the TCP/IP stack has never joined the sysplex group since it was initialized, this field is set to blanks.

Table 16. TCP/IP stack information section (continued)				
Offset	**Name**	**Length**	**Format**	**Description**
24(X'18')	SMF1154_1_PICOIpv6	1	Binary	**IPv6 support** • 0 - IPv6 is not enabled on this TCP/IP stack • 1 - IPv6 is enabled on this TCP/IP stack Configured in the BPXPRMxx parmlib member for this TCP/IP stack.
25(X'19')		3		Reserved. Set to 0.

IPv4 configuration section

The information that is provided in the IPv4 configuration section reflects fields that are configured on the IPCONFIG statement in the TCP/IP profile unless otherwise noted.

Table 17. IPv4 configuration section				
Offset	**Name**	**Length**	**Format**	**Description**
0(X'0')	SMF1154_1_V4CFEye	4	EBCDIC	Identifier – 'V4CF'
4(X'4')	SMF1154_1_V4CFDatagramFwd	1	Binary	**IPv4 Datagram forwarding** • 0 - Stack is not forwarding IPv4 datagrams • 1 - Stack is forwarding IPv4 datagrams Configured with the DATAGRAMFWD / NODATAGRAMFWD parameter.
5(X'5')	SMF1154_1_V4CFDynamicXcf	1	Binary	**IPv4 Dynamic XCF interfaces defined** • 0 - IPv4 dynamic XCF interfaces are not defined • 1 - IPv4 dynamic XCF interfaces are defined and the following fields contain dynamic XCF configured values: – SMF1154_1_V4CFDynXcfAddr – SMF1154_1_V4CFDynXcfMask – SMF1154_1_V4CFDynXcfSecClass Configured with the DYNAMICXCF / NODYNAMICXCF parameter.

Table 17. IPv4 configuration section (continued)

Offset	Name	Length	Format	Description
6(X'6')	SMF1154_1_V4CFIgnRedirectCfg	1	Binary	**Ignore ICMP redirects configured** • 0 - Ignore ICMP redirects is not configured in the TCP/IP profile • 1 - Ignore ICMP redirects is configured in the TCP/IP profile Configured with the IGNOREREDIRECT parameter.
7(X'7')	SMF1154_1_V4CFIgnRedirectAct	1	Binary	**Ignore ICMP redirects active** • 0 - ICMP redirects are not ignored • 1 - ICMP redirects are ignored, SMF1154_1_V4CFIgnRedirectRsn indicates the reason why ICMP redirects are being ignored.
8(X'8')	SMF1154_1_V4CFIPSecurity	1	Binary	**IP security enabled for IPv4** • 0 - IP security is not enabled for IPv4 • 1 - IP security is enabled for IPv4 Configured with the IPSECURITY parameter.
9(X'9')	SMF1154_1_V4CFDVIPSec	1	Binary	**IPsec tunnels eligible for sysplex-wide distribution and takeover** • 0 = Sysplex-wide tunnels are not enabled. • 1 = Sysplex-wide tunnels are enabled for both IPv4 and IPv6. Configured with the DVIPSEC parameter on the IPSEC statement in the TCP/IP profile.
10(X'A')		2		Reserved. Set to 0.
12(X'C')	SMF1154_1_V4CFArpTimeout	4	Binary	**ARP cache timeout for LCS devices** ARP cache timeout in seconds for LAN channel station (LCS) devices. The value is in the range of 60 – 86400 seconds. This value can be configured on the ARPAGE statement or on the ARPTO parameter of the IPCONFIG statement in the TCP/IP profile.

Table 17. IPv4 configuration section (continued)

Offset	Name	Length	Format	Description
16(X'10')	SMF1154_1_V4CFDynXcfAddr	4	Binary	**Dynamic XCF IPv4 address** This field is valid if SMF1154_1_V4CFDynamicXcf is set to 1. Configured with the DYNAMICXCF parameter.
20(X'14')	SMF1154_1_V4CFDynXcfMask	1	Binary	**Dynamic XCF number of mask bits** This field is valid if SMF1154_1_V4CFDynamicXcf is set to 1. This field has a value from 1 – 32. Configured with the DYNAMICXCF parameter.
21(X'15')	SMF1154_1_V4CFDynXcfSecClass	1	Binary	**Dynamic XCF security class** This field is valid if SMF1154_1_V4CFDynamicXcf is set to 1. Security class value (1 – 255) assigned to the XCF interface for use with IP filtering. Configured with the DYNAMICXCF SECCLASS parameter.
22(X'16')	SMF1154_1_V4CFIgnRedirectRsn	1	Binary	**Reason ICMP Redirects ignored** This field is valid if SMF1154_1_V4CFIgnRedirectAct is set to 1. SMF1154_1_V4CFIgnRedRsn_CFG (1) – IGNOREREDIRECT parameter configured on the IPCONFIG statement in the TCP/IP profile SMF1154_1_V4CFIgnRedRsn_OMP (2) – OMPROUTE set ignore redirects SMF1154_1_V4CFIgnRedRsn_IDS (3) – IDS policy configured to discard ICMP Redirects
23(X'17')	SMF1154_1_V4CFReasmTimeout	1	Binary	**Reassembly timeout** Reassembly timeout value in seconds. The value is in the range of 1 – 240 seconds. Configured with the REASSEMBLYTIMEOUT parameter.

Table 17. IPv4 configuration section (continued)				
Offset	**Name**	**Length**	**Format**	**Description**
24(X'18')	SMF1154_1_V4CFTTL	1	Binary	**Time to Live** Time to live or hop limit for an IPv4 packet. The value is in the range of 1 – 255. Configured with the TTL parameter.
25(X'19')		3	Binary	Reserved. Set to 0.

IPv6 configuration section

The information that is provided in the IPv6 configuration section reflects fields that are configured on the IPCONFIG6 statement in the TCP/IP profile unless otherwise noted. This section is included if IPv6 is enabled for the TCP/IP stack (SMF1154_1_PICOIpv6 = 1).

Table 18. IPv6 configuration section				
Offset	**Name**	**Length**	**Format**	**Description**
0(X'0')	SMF1154_1_V6CFEye	4	EBCDIC	Identifier – 'V6CF'
4(X'4')	SMF1154_1_V6CFDatagramFwd	1	Binary	**IPv6 datagram forwarding** • 0 - Stack is not forwarding IPv6 datagrams • 1 - Stack is forwarding IPv6 datagrams Configured with the DATAGRAMFWD / NODATAGRAMFWD parameter.
5(X'5')	SMF1154_1_V6CFDynamicXcf	1	Binary	**IPv6 Dynamic XCF interfaces defined** • 0 - IPv6 dynamic XCF interfaces are not defined • 1 - IPv6 dynamic XCF interfaces are defined and the following fields contain dynamic XCF configured values: – SMF1154_1_V6CFDynXcfAddr – SMF1154_1_V6CFDynXcfPfxRteLen – SMF1154_1_V6CFDynXcfSecClass Configured with the DYNAMICXCF / NODYNAMICXCF parameter.

Table 18. IPv6 configuration section (continued)

Offset	Name	Length	Format	Description
6(X'6')	SMF1154_1_V6CFDynXcfIfIDFlg	1	Binary	**Dynamic XCF IPv6 Interface ID configured** This field is valid if SMF1154_1_V6CFDynamicXcf is set to 1. • 0 - No IPv6 interface ID configured. Link-local address generated with a random value. • 1 - IPv6 interface ID configured and contained in the SMF1154_1_V6CFDynXcfIntrID field. Link-local address generated with the specified value. Configured with the DYNAMICXCF INTFID parameter.
7(X'7')	SMF1154_1_V6CFIgnRedirectCfg	1	Binary	**Ignore ICMPv6 redirects configured** • 0 - Ignore ICMPv6 redirects is not configured in the TCP/IP profile • 1 - Ignore ICMPv6 redirects is configured in the TCP/IP profile Configured with the IGNOREREDIRECT parameter.
8(X'8')	SMF1154_1_V6CFIgnRedirectAct	1	Binary	**Ignore ICMPv6 redirects active** • 0 - ICMPv6 redirects are not ignored • 1 - ICMPv6 redirects are ignored, SMF1154_1_V6CFIgnRedirectRsn indicates the reason why ICMPv6 redirects are being ignored.
9(X'9')	SMF1154_1_V6CFIgnoreRtrHopLim	1	Binary	**Ignore router advertised hop limit** • 0 – Do not ignore router advertised hop limits. • 1 – Ignore router advertised hop limits. Configured with the IGNOREROUTERHOPLIMIT / NOIGNOREROUTERHOPLIMIT parameter.
10(X'A')	SMF1154_1_V6CFIPSecurity	1	Binary	**IP security enabled for IPv6** • 0 - IP security is not enabled for IPv6 • 1 - IP security is enabled for IPv6 Configured with the IPSECURITY parameter.

Table 18. IPv6 configuration section (continued)

Offset	Name	Length	Format	Description
11(X'B')		1		Reserved. Set to 0
12(X'C')	SMF1154_1_V6CFDynXcfIntfID	8	Binary	**Dynamic XCF IPv6 interface ID** This field is valid if SMF1154_1_V6CFDynXcfIfIDFlg is set to 1. Configured with the DYNAMICXCF INTFID parameter.
20(X'14')	SMF1154_1_V6CFDynXcfAddr	16	Binary	**Dynamic XCF IPv6 address** This field is valid if SMF1154_1_V6CFDynamicXcf is set to 1. Configured with the DYNAMICXCF parameter.
36(X'24')	SMF1154_1_V6CFDynXcfPfxRteLen	1	Binary	**Dynamic XCF prefix route length** This field is valid if SMF1154_1_V6CFDynamicXcf is set to 1. The field is a value from 1 – 128. Configured with the DYNAMICXCF parameter.
37(X'25')	SMF1154_1_V6CFDynXcfSecClass	1	Binary	**Dynamic XCF security class** This field is valid if SMF1154_1_V6CFDynamicXcf is set to 1. Security class value (1 – 255) assigned to the IPv6 XCF interface for use with IP filtering. Configured with the DYNAMICXCF SECCLASS parameter.
38(X'26')	SMF1154_1_V6CFHopLimit	1	Binary	**IPv6 hop limit** Hop limit for an IPv6 packet. The value is in the range of 1 – 255. Configured with the HOPLIMIT parameter.
39(X'27')	SMF1154_1_V6CFIcmpErrLimit	1	Binary	**ICMPv6 error rate limit** Number of ICMPv6 error messages (1 – 20) that can be sent to a particular IPv6 destination per second. Configured with the ICMPERRORLIMIT parameter.

Table 18. IPv6 configuration section (continued)

Offset	Name	Length	Format	Description
40(X'28')	SMF1154_1_V6CFIgnRedirectRsn	1	Binary	**Reason ICMPv6 Redirects ignored** • SMF1154_1_V6CFIgnRedRsn_CFG (1) – IGNOREREDIRECT parameter configured on the IPCONFIG6 statement in the TCP/IP profile • SMF1154_1_V6CFIgnRedRsn_OMP (2) – OMPROUTE set ignore redirects • SMF1154_1_V6CFIgnRedRsn_IDS (3) – IDS policy configured to discard ICMP6 Redirects
41(X'29')	SMF1154_1_V6CFOSMSecClass	1	Binary	**OSM security class** Security class value (1 – 255) assigned to each OSM interface for use with IP filtering. Configured with the OSMSECCLASS parameter.
42(X'2A')		2		Reserved. Set to 0.

TCP configuration section

The information that is provided in the TCP configuration section reflects fields that are configured on the TCPCONFIG statement in the TCP/IP profile unless otherwise noted.

Table 19. TCP configuration section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_TCCFEye	4	EBCDIC	Identifier – 'TCCF'
4(X'4')	SMF1154_1_TCCFRestrictLowPorts	1	Binary	**Restrict TCP low ports** • 0 – TCP ports 1-1023 are not restricted • 1 – TCP ports 1-1023 are restricted Configured with the RESTRICTLOWPORTS / UNRESTRICTLOWPORTS parameter
5(X'5')	SMF1154_1_TCCFTimeStamp	1	Binary	**TCP timestamp option enabled** • 0 – TCP timestamp option is not enabled • 1 – TCP timestamp option is enabled Configured with the TCPTIMESTAMP / NOTCPTIMESTAMP parameter

Table 19. TCP configuration section (continued)

Offset	Name	Length	Format	Description
6(X'6')	SMF1154_1_TCCFTtls	1	Binary	**AT-TLS function activated** • 0 - Application transparent Transport Layer Security (AT-TLS) is not active for the TCP/IP stack. • 1 – AT-TLS is active for the TCP/IP stack Configured with the TTLS / NOTTLS parameter.
7(X'7')		1		Reserved. Set to 0.
8(X'8')	SMF1154_1_TCCFEphemPortBegNum	2	Binary	**TCP ephemeral port range start** The starting port for the range of ephemeral ports to be assigned when the bind is done. The value can be in the range 1024 - 65535. Configured with the EPHEMERALPORTS parameter.
10(X'A')	SMF1154_1_TCCFEphemPortEndNum	2	Binary	**TCP ephemeral port range end** The ending port for the range of ephemeral ports to be assigned when the bind is done. The value can be in the range 1024 - 65535. Configured with the EPHEMERALPORTS parameter.
12(X'C')	SMF1154_1_TCCFSoMaxConn	4	Binary	**Maximum queued connection requests** The maximum number of pending connection requests queued for any TCP listening socket. The value is in the range of 1-2147483647. Configured with the SOMAXCONN statement in the TCP/IP profile.
16(X'10')	SMF1154_1_TCCFFinWait2Time	2	Binary	**FINWAIT2 interval** The number of seconds a TCP connection should remain in the FINWAIT2 state. The value is in the range 1 – 3600 seconds. Configured with the FINWAIT2TIME parameter.

Table 19. TCP configuration section (continued)				
Offset	**Name**	**Length**	**Format**	**Description**
18(X'12')	SMF1154_1_TCCFTimeWaitInterval	2	Binary	**TIMEWAIT interval** The number of seconds a TCP connection remains in the TIMEWAIT state. The value is in the range 0 – 120 seconds. Configured with the TIMEWAITINTERVAL parameter.

UDP configuration section

The information that is provided in the UDP configuration section reflects fields that are configured on the UDPCONFIG statement in the TCP/IP profile unless otherwise noted.

Table 20. UDP configuration section				
Offset	**Name**	**Length**	**Format**	**Description**
0(X'0')	SMF1154_1_UDCFEye	4	EBCDIC	Identifier – 'UDCF'
4(X'4')	SMF1154_1_UDCFRestrictLowPorts	1	Binary	**Restrict UDP low ports** • 0 – UDP ports 1-1023 are not restricted • 1 – UDP ports 1-1023 are restricted Configured with the RESTRICTLOWPORTS / UNRESTRICTLOWPORTS parameter
5(X'5')	SMF1154_1_UDCFChkSum	1	Binary	**UDP checksum required** • 0 – UDP layer does not perform checksum processing for IPv4 packets • 1 – UDP layer performs checksum processing for IPv4 packets Configured with the UDPCHKSUM / NOUDPCHKSUM parameter
6(X'6')	SMF1154_1_UDCFQueueLimit	1	Binary	**UDP queue limit enabled** • 0 – No queue limit set for UDP. • 1 – Queue limit set for UDP. Maximum of 2000 incoming datagrams are queued on a UDP socket. Configured with the UDPQUEUELIMIT / NOUDPQUEUELIMIT parameter
7(X'7')		1		Reserved. Set to 0.

Table 20. UDP configuration section (continued)

Offset	Name	Length	Format	Description
8(X'8')	SMF1154_1_UDCFEphemPortBegNum	2	Binary	**UDP ephemeral port range start** The starting port for the range of ephemeral ports to be assigned when the bind is done. The value can be in the range 1024 - 65535. Configured with the EPHEMERALPORTS parameter.
10(X'A')	SMF1154_1_UDCFEphemPortEndNum	2	Binary	**UDP ephemeral port range end** The ending port for the range of ephemeral ports to be assigned when the bind is done. The value can be in the range 1024 - 65535. Configured with the EPHEMERALPORTS parameter.

Global configuration section

The information that is provided in the global configuration section reflects fields that are configured on the GLOBALCONFIG statement in the TCP/IP profile unless otherwise noted.

Table 21. Global configuration section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_GBCFEye	4	EBCDIC	Identifier – 'GBCF'
4(X'4')	SMF1154_1_GBCFExpBindPortRange	1	Binary	**Explicit bind port range defined** • 0 – TCP/IP stack does not participate in the allocation of ports from a pool guaranteed to be unique across the sysplex. • 1 – TCP/IP stack participates in the allocation of ports from a pool guaranteed to be unique across the sysplex, when processing an explicit Bind of a TCP socket to the IPv4 INADDR_ANY address, or to the IPv6 unspecified address (in6addr_any), and port 0. The following fields contain the port range values: – SMF1154_1_GBCFExpBindPortBegNm – SMF1154_1_GBCFExpBindPortEndNm Configured with the EXPLICITBINDPORTRANGE / NOEXPLICITBINDPORTRANGE parameter.

Table 21. Global configuration section (continued)

Offset	Name	Length	Format	Description
5(X'5')	SMF1154_1_GBCFMlsChkTerminate	1	Binary	**MLS check terminate** • 0 – TCP/IP stack is not terminated when inconsistent configuration information is discovered in a multilevel-secure environment. • 1 – TCP/IP stack is terminated when inconsistent configuration information is discovered in a multilevel-secure environment. Configured with MLSCHKTERMINATE / NOMLSCHKTERMINATE parameter.
6(X'6')	SMF1154_1_GBCFSMCR	1	Binary	**SMC-R enabled** • 0 – TCP/IP stack should not use Shared Memory Communications over Remote Direct Memory Access (SMC-R) • 1 – TCP/IP stack should use SMC-R Configured with the SMCR / NOSMCR parameter
7(X'7')	SMF1154_1_GBCFSMCD	1	Binary	**SMC-D enabled** • 0 – TCP/IP stack should not use Shared Memory Communications – Direct Memory Access (SMC-D) • 1 – TCP/IP stack should use SMC-D Configured with the SMCD / NOSMCD parameter
8(X'8')	SMF1154_1_GBCFAutoSMC	1	Binary	**SMC auto-monitoring** • 0 – TCP/IP stack does not monitor inbound TCP connections to determine whether the connections can benefit from using SMC. • 1 – TCP/IP stack monitors inbound TCP connections to determine whether the connections can benefit from using SMC. Configured with the AUTOSMC / NOAUTOSMC parameter

Table 21. Global configuration section (continued)

Offset	Name	Length	Format	Description
9(X'9')	SMF1154_1_GBCFZERT	1	Binary	**zERT enabled** • 0 – TCP and Enterprise Extender traffic will not be monitored by z/OS Encryption Readiness Technology (zERT) • 1 – TCP and Enterprise Extender traffic will be monitored by zERT Configured with the ZERT / NOZERT parameter.
10(X'A')	SMF1154_1_GBCFZERTAGG	1	Binary	**zERT aggregation enabled** • 0 – zERT aggregation is not enabled • 1 – zERT aggregation is enabled Configured with the ZERT AGGREGATION / ZERT NOAGGREGATION
11(X'B')	SMF1154_1_GBCFSysMonNoJoin	1	Binary	**Sysplex monitor – no join** • 0 – TCP/IP stack joins the TCP/IP sysplex group (EZBTCPCS) during stack initialization based on DELAYJOIN and DELAYJOINIPSEC settings. • 1 – TCP/IP stack does not join the TCP/IP sysplex group (EZBTCPCS) during stack initialization. Configured with the SYSPLEXMONITOR NOJOIN parameter
12(X'C')	SMF1154_1_GBCFSysMonDelayJoin	1	Binary	**Sysplex monitor – OMPROUTE delay join** • 0 – TCP/IP stack does not delay joining the sysplex group waiting for OMPROUTE to be active. • 1 – TCP/IP stack delays joining or rejoining the sysplex group until OMPROUTE is active. Configured with the SYSPLEXMONITOR DELAYJOIN / SYSPLEXMONITOR NODELAYJOIN parameter

Table 21. Global configuration section (continued)

Offset	Name	Length	Format	Description
13(X'D')	SMF1154_1_GBCFSysMonDelayJoinI	1	Binary	**Sysplex monitor – IPsec delay join** • 0 – TCP/IP stack does not delay joining the sysplex group waiting for the IPsec infrastructure to be active and operational. • 1 – TCP/IP stack delays joining or rejoining the sysplex group until the IPsec infrastructure is active and operational. Configured with the SYSPLEXMONITOR DELAYJOINIPSEC / SYSPLEXMONITOR NODELAYJOINIPSEC parameter
14(X'E')	SMF1154_1_GBCFSysMonIpsec	1	Binary	**Sysplex monitor – monitor IPsec** • 0 - TCP/IP stack does not monitor the IPsec infrastructure after the stack has joined the sysplex group. • 1 – TCP/IP stack monitors the IPsec infrastructure after the stack has joined the sysplex group, to detect if it becomes inactive or non-operational. Configured with the SYSPLEXMONITOR DELAYJOINIPSEC MONIPSEC / SYSPLEXMONITOR DELAYJOINIPSEC NOMONIPSEC parameter
15(X'F')	SMF1154_1_GBCFSysMonMonIntf	1	Binary	**Sysplex monitor – monitor interfaces** • 0 – TCP/IP stack does not monitor the status of specified network interfaces. • 1 – TCP/IP stack monitors the status of specified network interfaces. Configured with SYSPLEXMONITOR MONITORINTERFACE / SYSPLEXMONITOR NOMONITORINTERFACE parameter
16(X'10')	SMF1154_1_GBCFSysMonDynRoute	1	Binary	**Sysplex monitor - dynamic routes** • 0 – TCP/IP stack does not monitor the presence of dynamic routes over monitored interfaces. • 1 – TCP/IP stack monitors the presence of dynamic routes over monitored interfaces. Configured with the SYSPLEXMONITOR MONITORINTERFACE DYNROUTE / NODYNROUTE parameter

Table 21. Global configuration section (continued)

Offset	Name	Length	Format	Description
17(X'11')	SMF1154_1_GBCFSysMonRecovery	1	Binary	**Sysplex monitor – recovery** • 0 – TCP/IP stack does not leave the sysplex group when a problem is detected. • 1 – TCP/IP stack leaves the sysplex group when a problem is detected. Configured with the SYSPLEXMONITOR RECOVERY / SYSPLEXMONITOR NORECOVERY parameter
18(X'12')	SMF1154_1_GBCFSysMonAutoRejoin	1	Binary	**Sysplex monitor - auto-rejoin** • 0 – TCP/IP stack does not automatically rejoin the sysplex group after detected problems are resolved • 1 – TCP/IP stack automatically rejoins the sysplex group after detected problems are resolved Configured with the SYSPLEXMONITOR AUTOREJOIN / SYSPLEXMONITOR NOAUTOREJOIN parameter
19(X'13')		1	Binary	Reserved. Set to 0.
20(X'14')	SMF1154_1_GBCFSysMonTimerSecs	2	Binary	**Sysplex monitor timer** The number of seconds used by the sysplex monitor function to react to problems with needed sysplex resources. Valid values are in the range 10-3600 seconds. Configured with the SYSPLEXMONITOR TIMERSECS parameter
22(X'16')	SMF1154_1_GBCFIqdVlanId	2	Binary	**VLAN ID for dynamic XCF hipersockets interface** The VLAN ID used when Hipersockets (iQDIO) connectivity is used for dynamic XCF support. If not configured, the value is 0. Configured with the IQDVLANID parameter

Table 21. Global configuration section (continued)

Offset	Name	Length	Format	Description
24(X'18')	SMF1154_1_GBCFXcfGroupID	2	EBCDIC	**TCP XCF group ID suffix** The 2-digit suffix used to generate the sysplex group name that the TCP/IP stack joins. Valid values are in the range 2-31. If not configured, the field is set to blanks. Configured with the XCFGRPID parameter
26(X'1A')	SMF1154_1_GBCFExpBindPortBegNm	2	Binary	**Explicit bind port range start** This field is valid if SMF1154_1_GBCFExpBindPortRange is set to 1. The starting port for the range of ports to be assigned when an explicit bind of a TCP socket is done to the IPv4 INADDR_ANY or IPv6 unspecified address (in6addr_any), and port 0. The value can be in the range 1024 - 65535. Configured with EXPLICITBINDPORTRANGE parameter.
28(X'1C')	SMF1154_1_GBCFExpBindPortEndNm	2	Binary	**Explicit bind port range end** This field is valid if SMF1154_1_GBCFExpBindPortRange is set to 1. The ending port for the range of ports to be assigned when an explicit bind of a TCP socket is done to the IPv4 INADDR_ANY or IPv6 unspecified address (in6addr_any), and port 0. The value can be in the range 1024 - 65535. Configured with the EXPLICITBINDPORTRANGE parameter
30(X'1E')	SMF1154_1_GBCFAutoIQDC	1	Binary	**Dynamic IQD converged interfaces** • 0 - Dynamic IQD (HiperSockets) converged interfaces are not used. • 1 – Dynamic IQD (HiperSockets) converged interfaces are used for eligible traffic. Configured with the AUTOIQDC / NOAUTOIQDC parameter
31(X'1F')		1	Binary	Reserved. Set to 0.

Port configuration section

The information that is provided in a port configuration section entry reflects fields that are configured on the PORT or PORTRANGE statement in the TCP/IP profile unless otherwise noted. There can be multiple instances of this section in the record, one per PORT or PORTRANGE sub statement.

Table 22. Port configuration section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_PORTEye	4	EBCDIC	Identifier – 'PORT'
4(X'4')	SMF1154_1_PORTRange	1	Binary	**PORTRANGE entry** • 0 – Entry is for a single port (PORT statement) • 1 – Entry is for a range of ports (PORTRANGE statement) Configured with the PORT or PORTRANGE statement
5(X'5')	SMF1154_1_PORTUnrsv	1	Binary	**Unreserved port entry** • 0 – Entry applies to a reserved port or ports • 1 – Entry applies to an unreserved port Configured with the UNRSV parameter on the PORT statement
6(X'6')	SMF1154_1_PORTTCP	1	Binary	**TCP port entry** • 0 – UDP port entry • 1 – TCP port entry Configured with the TCP and UDP parameters on the PORT or PORTRANGE statements

Table 22. Port configuration section (continued)

Offset	Name	Length	Format	Description
7(X'7')	SMF1154_1_PORTUseType	1	Binary	**Port use type** Type of use for the port or ports. **SMF1154_1_PORTUTReserved(1)** None of the ports can be used by any user for the protocol (TCP or UDP) specified on this entry. This type applies only to reserved port entries (SMF1154_1_PORTUnrsv=0) **SMF1154_1_PORTUTAuthport(2)** The ports can be used only by the FTP server when the server is configured to use PASSIVEDATAPORTS. This type applies only to reserved port entries (SMF1154_1_PORTUnrsv=0) which were reserved as a range (SMF1154_1_PORTRange is set to 1). **SMF1154_1_PORTUTJobname(3)** The specified or unreserved port(s) can be used only based on an MVS job name value. If this use type value is set, then field SMF1154_1_PORTJobName contains the job name value. Configured with the RESERVED, jobname, or AUTHPORT parameter on the PORT or PORTRANGE statement. AUTHPORT can only be configured on PORTRANGE.
8(X'8')	SMF1154_1_PORTRSaf	1	Binary	**Reserved port SAF configured** This field is valid for a reserved (SMF1154_1_PORTUnrsv = 0) jobname entry (SMF1154_1_PORTUseType = SMF1154_1_PORTUTJobname). • 0 – SAF resource name is not configured for the entry. • 1 – A SAF resource name is configured for the entry and SMF1154_1_PORTSafName contains the name. Configured with the SAF parameter on the PORT or PORTRANGE statement.

Table 22. Port configuration section (continued)

Offset	Name	Length	Format	Description
9(X'9')	SMF1154_1_PORTRNoSMC	1	Binary	**Reserved port NOSMC** 1 – Override the setting of SMCGLOBAL AUTOSMC and do not allow SMC for inbound TCP connections that use this port If both SMF1154_1_PORTRNoSMC and SMF1154_1_PORTRSMC are 0, use the SMCGLOBAL AUTOSMC setting. Configured with the NOSMC parameter on the PORT or PORTRANGE statement
10(X'A')	SMF1154_1_PORTRSMC	1	Binary	**Reserved port SMC** 1 – Override the setting of SMCGLOBAL AUTOSMC and attempt to use SMC for inbound TCP connections that use this port. If both SMF1154_1_PORTRNoSMC and SMF1154_1_PORTRSMC are 0, use the SMCGLOBAL AUTOSMC setting. Configured with the SMC parameter on the PORT or PORTRANGE statement
11(X'B')		1	Binary	Reserved. Set to 0.
12(X'C')	SMF1154_1_PORTBegNum	2	Binary	**Reserved port range start** This field is valid for a reserved port entry (SMF1154_1_PORTUnrsv = 0) and contains one of the following values: • The reserved port number, if SMF1154_1_PORTRange = 0. • The beginning reserved port number in the range, if SMF1154_1_PORTRange = 1. Configured on the PORT or PORTRANGE statement.
14(X'E')	SMF1154_1_PORTEndNum	2	Binary	**Reserved port range end** This field is valid for a reserved port range entry (SMF1154_1_PORTUnrsv = 0 and SMF1154_1_PORTRange = 1). It is the ending reserved port number in the range. Based on the configuration of the port and number of ports on the PORTRANGE statement

Table 22. Port configuration section (continued)

Offset	Name	Length	Format	Description
16(X'10')	SMF1154_1_PORTUDeny	1	Binary	**Unreserved port deny** This field is valid for an unreserved entry (SMF1154_1_PORTUnrsv = 1). • 0 – Deny access to all unreserved ports is not configured. • 1 – Access to all unreserved ports is denied for the protocol (TCP or UDP) configured in this entry. Configured with the DENY parameter on the PORT statement.
17(X'11')	SMF1154_1_PORTUSaf	1	Binary	**Unreserved port SAF configured** This field is valid for an unreserved entry (SMF1154_1_PORTUnrsv = 1). • 0 – SAF resource name is not configured for the entry • 1 – A SAF resource name is configured for the entry and SMF1154_1_PORTSafName contains the name. Binding to, or listening on, any unreserved port is restricted to users that are permitted to the specified SAF SERVAUTH resource. Configured with the SAF parameter on the PORT statement.
18(X'12')		2	Binary	Reserved. Set to 0.
20(X'14')	SMF1154_1_PORTJobName	8	EBCDIC	**Job name** This field is valid if SMF1154_1_PORTUseType is SMF1154_1_PORTUTJobname. This field contains the MVS job name value associated with the port entry, padded with trailing blanks. Configured on the PORT or PORTRANGE statement
28(X'1C')	SMF1154_1_PORTSafName	8	EBCDIC	**SAF resource name** This field is valid if SMF1154_1_PORTRSaf or SMF1154_1_PORTUSaf is set to 1. This field contains the SAF resource name, padded with trailing blanks. Configured with the SAF parameter on the PORT or PORTRANGE statement

Management configuration section

The information that is provided in the management configuration section reflects fields that are configured on the NETMONITOR, SACONFIG, and SMFCONFIG statements in the TCP/IP profile unless otherwise noted.

Table 23. Management configuration section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_1_MGMTEye	4	EBCDIC	Identifier – 'MGMT'
4(X'4')	SMF1154_1_MGMT119FtpClient	1	Binary	**FTP client SMF 119 records** • 0 – FTP client SMF 119 records not requested • 1 – FTP client SMF 119 records requested Configured with the SMFCONFIG TYPE119 FTPCLIENT / NOFTPCLIENT parameter
5(X'5')	SMF1154_1_MGMT119IfStats	1	Binary	**Interface statistics SMF 119 records** • 0 – Interface statistics SMF 119 records not requested • 1 – Interface statistics SMF 119 records requested Configured with the SMFCONFIG TYPE119 IFSTATISTICS / NOIFSTATISTICS parameter
6(X'6')	SMF1154_1_MGMT119IPSec	1	Binary	**IPSec SMF 119 records** • 0 – IPSec SMF 119 records not requested • 1 – IPSec SMF 119 records requested Configured with the SMFCONFIG TYPE119 IPSECURITY / NOIPSECURITY parameter
7(X'7')	SMF1154_1_MGMT119PortStats	1	Binary	**Port statistics SMF 119 records** • 0 – Port statistics SMF 119 records not requested • 1 – Port statistics SMF 119 records requested Configured with the SMFCONFIG TYPE119 PORTSTATISTICS / NOPORTSTATISTICS parameter

Table 23. Management configuration section (continued)

Offset	Name	Length	Format	Description
8(X'8')	SMF1154_1_MGMT119Profile	1	Binary	**Profile SMF 119 records** • 0 – TCP/IP profile SMF 119 records not requested • 1 – TCP/IP profile SMF 119 records requested Configured with the SMFCONFIG TYPE119 PROFILE / NOPROFILE parameter
9(X'9')	SMF1154_1_MGMT119TcpInit	1	Binary	**TCP conn init SMF 119 records** • 0 – TCP connection initiation SMF 119 records not requested • 1 – TCP connection initiation SMF 119 records requested Configured with the SMFCONFIG TYPE119 TCPINIT / NOTCPINIT parameter
10(X'A')	SMF1154_1_MGMT119TcpipStats	1	Binary	**TCP/IP statistics SMF 119 records** • 0 – TCP/IP statistics SMF 119 records not requested • 1 – TCP/IP statistics SMF 119 records requested Configured with the SMFCONFIG TYPE119 TCPIPSTATISTICS / NOTCPIPSTATISTICS parameter
11(X'B')	SMF1154_1_MGMT119TcpStack	1	Binary	**Stack init/term SMF 119 records** • 0 – TCP/IP stack initiation and termination SMF 119 records not requested • 1 – TCP/IP stack initiation and termination SMF 119 records requested Configured with the SMFCONFIG TYPE119 TCPSTACK / NOTCPSTACK parameter
12(X'C')	SMF1154_1_MGMT119TcpTerm	1	Binary	**TCP conn term SMF 119 records** • 0 – TCP connection termination SMF 119 records not requested • 1 – TCP connection termination SMF 119 records requested Configured with the SMFCONFIG TYPE119 TCPTERM / NOTCPTERM parameter

Table 23. Management configuration section (continued)

Offset	Name	Length	Format	Description
13(X'D')	SMF1154_1_MGMT119TN3270Client	1	Binary	**Telnet client init/term SMF 119 records** • 0 – TSO Telnet client connection initiation and termination SMF 119 records not requested • 1 – TSO Telnet client connection initiation and termination SMF 119 records requested Configured with the SMFCONFIG TYPE119 TN3270CLIENT / NOTN3270CLIENT parameter
14(X'E')	SMF1154_1_MGMT119UdpTerm	1	Binary	**UDP term SMF 119 records** • 0 – UDP endpoint termination SMF 119 records not requested • 1 – UDP endpoint termination SMF 119 records requested Configured with the SMFCONFIG TYPE119 UDPTERM / NOUDPTERM parameter
15(X'F')	SMF1154_1_MGMT119Dvipa	1	Binary	**Dynamic VIPA SMF 119 records** • 0 – Dynamic VIPA SMF 119 records not requested • 1 – Dynamic VIPA SMF 119 records requested Configured with the SMFCONFIG TYPE119 DVIPA / NODVIPA parameter
16(X'10')	SMF1154_1_MGMT119SmcrGrpStats	1	Binary	**SMC-R group stats SMF 119 records** • 0 – SMC-R group statistics SMF 119 records not requested • 1 – SMC-R group statistics SMF 119 records requested Configured with the SMFCONFIG TYPE119 SMCRGROUPSTATISTICS / NOSMCRGROUPSTATISTICS parameter
17(X'11')	SMF1154_1_MGMT119SmcrLnkEvent	1	Binary	**SMC-R link event SMF 119 records** • 0 – SMC-R link event SMF 119 records not requested • 1 – SMC-R link event SMF 119 records requested Configured with the SMFCONFIG TYPE119 SMCRLINKEVENT / NOSMCRLINKEVENT parameter

Table 23. Management configuration section (continued)

Offset	Name	Length	Format	Description
18(X'12')	SMF1154_1_MGMT119SmcdLnkStats	1	Binary	**SMC-D link stats SMF 119 records** • 0 – SMC-D link statistics SMF 119 records not requested • 1 – SMC-D link statistics SMF 119 records requested Configured with the SMFCONFIG TYPE119 SMCDLINKSTATISTICS / NOSMCDLINKSTATISTICS parameter
19(X'13')	SMF1154_1_MGMT119SmcdLnkEvent	1	Binary	**SMC-D link event SMF 119 records** • 0 – SMC-D link event SMF 119 records not requested • 1 – SMC-D link event SMF 119 records requested Configured with the SMFCONFIG TYPE119 SMCDLINKEVENT / NOSMCDLINKEVENT parameter
20(X'14')	SMF1154_1_MGMT119ZertDetail	1	Binary	**zERT detail SMF 119 records** • 0 – zERT connection details SMF 119 records not requested • 1 – zERT connection details SMF 119 records requested Configured with the SMFCONFIG TYPE119 ZERTDETAIL / NOZERTDETAIL parameter
21(X'15')	SMF1154_1_MGMT119ZertSummary	1	Binary	**zERT summary SMF 119 records** • 0 – zERT summary information SMF 119 records not requested • 1 – zERT summary information SMF 119 records requested Configured with the SMFCONFIG TYPE119 ZERTSUMMARY / NOZERTSUMMARY parameter

Table 23. Management configuration section (continued)

Offset	Name	Length	Format	Description
22(X'16')	SMF1154_1_MGMT119ZertDtlPolicy	1	Binary	**zERT detail SMF 119 records by policy** • 0 – zERT connection details SMF 119 records not requested for use with zERT policy-based enforcement • 1 – zERT connection details SMF 119 records requested for use with zERT policy-based enforcement Configured with the SMFCONFIG TYPE119 ZERTDETAILBYPOLICY / NOZERTDETAILBYPOLICY parameter
23(X'17')	SMF1154_1_MGMTNMPktTrace	1	Binary	**NETMONITOR packet trace** • 0 – NETMONITOR packet trace (SYSTCPDA) not enabled • 1 – NETMONITOR packet trace (SYSTCPDA) enabled Configured with the PKTTRCSERVICE / NOPKTTRCSERVICE parameter on the NETMONITOR statement
24(X'18')	SMF1154_1_MGMTNMTcpConn	1	Binary	**NETMONITOR TCP connection** • 0 – NETMONITOR TCP connection (SYSTCPCN) not enabled • 1 – NETMONITOR TCP connection (SYSTCPCN) enabled Configured with the TCPCONNSERVICE / NOTCPCONNSERVICE parameter on the NETMONITOR statement
25(X'19')	SMF1154_1_MGMTNMSmf	1	Binary	**NETMONITOR SMF service** • 0 – NETMONITOR SMF service (SYSTCPSM) not enabled • 1 – NETMONITOR SMF service (SYSTCPSM) enabled Configured with the SMFSERVICE / NOSMFSERVICE parameter on the NETMONITOR statement

Table 23. Management configuration section (continued)

Offset	Name	Length	Format	Description
26(X'1A')	SMF1154_1_MGMTNMNTATrace	1	Binary	**NETMONITOR OSAENT trace** • 0 – NETMONITOR OSAENT trace (SYSTCPOT) not enabled • 1 – NETMONITOR OSAENT trace (SYSTCPOT) enabled Configured with the NTATRCSERVICE / NONTATRCSERVICE parameter on the NETMONITOR statement
27(X'1B')	SMF1154_1_MGMTNMZert	1	Binary	**NETMONITOR zERT detail** • 0 – NETMONITOR zERT detail service (SYSTCPER) not enabled • 1 – NETMONITOR zERT detail (SYSTCPER) enabled Configured with the ZERTSERVICE / NOZERTSERVICE parameter on the NETMONITOR statement
28(X'1C')	SMF1154_1_MGMTNMZertSumm	1	Binary	**NETMONITOR zERT summary** • 0 – NETMONITOR zERT summary service (SYSTCPES) not enabled • 1 – NETMONITOR zERT summary (SYSTCPES) enabled Configured with the ZERTSUMMARY / NOZERTSUMMARY parameter on the NETMONITOR statement
29(X'1D')	SMF1154_1_MGMTNMZertServP	1	Binary	**NETMONITOR zERT detail by policy** • 0 – NETMONITOR zERT detail service (SYSTCPER) not enabled for use with zERT policy-based enforcement • 1 – NETMONITOR zERT detail (SYSTCPER) enabled for use with zERT policy-based enforcement Configured with the ZERTSERVICEBYPOLICY / NOZERTSERVICEBYPOLICY parameter on the NETMONITOR statement
30(X'1E')	SMF1154_1_MGMTNMSmfIPSec	1	Binary	**SMFSERVICE IPSec records** • 0 – IPSec records not requested • 1 – IPSec records requested Configured with the IPSECURITY / NOIPSECURITY parameter on the NETMONITOR SMFSERVICE statement

Table 23. Management configuration section (continued)

Offset	Name	Length	Format	Description
31(X'1F')	SMF1154_1_MGMTNMSmfProfile	1	Binary	**SMFSERVICE profile records** • 0 – Profile records not requested • 1 – TCP/IP stack profile records and TN3270 Telnet server (Telnet) profile records requested Configured with the PROFILE / NOPROFILE parameter on the NETMONITOR SMFSERVICE statement
32(X'20')	SMF1154_1_MGMTNMSmfCSSMTP	1	Binary	**SMFSERVICE CSSMTP records** • 0 – CSSMTP records not requested • 1 – CSSMTP records requested Configured with the CSSMTP / NOCSSMTP parameter on the NETMONITOR SMFSERVICE statement
33(X'21')	SMF1154_1_MGMTNMSmfCSMail	1	Binary	**SMFSERVICE MAIL records** • 0 – CSSMTP MAIL records not requested • 1 – CSSMTP MAIL records requested Configured with the CSMAIL / NOCSMAIL parameter on the NETMONITOR SMFSERVICE statement
34(X'22')	SMF1154_1_MGMTNMSmfDvipa	1	Binary	**SMFSERVICE DVIPA records** • 0 – DVIPA records not requested • 1 – DVIPA records requested Configured with the DVIPA / NODVIPA parameter on the NETMONITOR SMFSERVICE statement
35(X'23')	SMF1154_1_MGMTNetMonMinLife	1	Binary	**TCPCONNSERVICE minimum lifetime** This field is valid if SMF1154_1_MGMTNMTcpConn is set to 1. The minimum connection lifetime, specified in seconds, for connections reported by the TCP connection information service (TCPCONNSERVICE). Configured with the MINLIFETIME parameter on the NETMONITOR TCPCONNSERVICE statement

Table 23. Management configuration section (continued)

Offset	Name	Length	Format	Description
36(X'24')	SMF1154_1_MGMTSAEnabled	1	Binary	**TCP/IP SNMP subagent enabled** • 0 – TCP/IP SNMP subagent not enabled • 1 – TCP/IP SNMP subagent enabled Configured with the ENABLED or DISABLED parameters on the SACONFIG statement
37(X'25')	SMF1154_1_MGMTSASetsEnabled	1	Binary	**SNMP SET requests enabled** This field is valid if SMF1154_1_MGMTSAEnabled is set to 1. • 0 – TCP/IP SNMP subagent does not process SNMP SET requests • 1 – TCP/IP SNMP subagent processes SNMP SET requests Configured with the SETSENABLED or SETSDISABLED parameters on the SACONFIG statement
38(X'26')	SMF1154_1_MGMTSACommunity	1	Binary	**Community name configured** This field is valid if SMF1154_1_MGMTSAEnabled is set to 1. • 0 – Community name not configured • 1 – Community name configured Configured with the COMMUNITY parameter on the SACONFIG statement
39(X'27')		1	Binary	Reserved. Set to 0.
40(X'28')	SMF1154_1_MGMTSAAgent	2	Binary	**SNMP agent port number** This field is valid if SMF1154_1_MGMTSAEnabled is set to 1. SNMP agent port number. The value can be in the range 1 – 65,535. Configured with the AGENT parameter on the SACONFIG statement

Table 23. Management configuration section (continued)				
Offset	**Name**	**Length**	**Format**	**Description**
42(X'2A')	SMF1154_1_MGMTSACacheTime	2	Binary	**TCP/IP SNMP agent cache time** This field is valid if SMF1154_1_MGMTSAEnabled is set to 1. Number of seconds that the TCP/IP subagent caches management data. The value can be from 0 – 3,600. Configured with the SACACHETIME parameter on the SACONFIG statement

Network access configuration section

The information that is provided in a network access configuration section entry reflects fields that are configured on the NETACCESS statement in the TCP/IP profile unless otherwise noted. There can be multiple instances of this section in the record, one per NETACCESS network sub statement.

Table 24. Network access configuration section				
Offset	**Name**	**Length**	**Format**	**Description**
0(X'0')	SMF1154_1_NETAEye	4	EBCDIC	Identifier – 'NETA'
4(X'4')	SMF1154_1_NETAIPv6	1	Binary	**NETACCESS IP address family** • 0 – IP addresses are IPv4 • 1 – IP addresses are IPv6 Configured on the NETACCESS network sub statement
5(X'5')	SMF1154_1_NETAInBound	1	Binary	**NETACCESS inbound checking** • 0 – Inbound network access control checking is not in effect. • 1 – Inbound network access control checking is in effect. Configured with the INBOUND / NOINBOUND parameter.
6(X'6')	SMF1154_1_NETAOutBound	1	Binary	**NETACCESS outbound checking** • 0 – Outbound network access control checking is not in effect. • 1 – Outbound network access control checking is in effect. Configured with the OUTBOUND / NOOUTBOUND parameter.

Table 24. Network access configuration section (continued)

Offset	Name	Length	Format	Description
7(X'7')	SMF1154_1_NETADefault	1	Binary	**NETACCESS DEFAULT entry** • 0 – This is not a DEFAULT entry. • 1 – This is a DEFAULT entry. Configured with the DEFAULT parameter
8(X'8')	SMF1154_1_NETADefaultHome	1	Binary	**NETACCESS DEFAULTHOME entry** • 0 – This is not a DEFAULTHOME entry. • 1 – This is a DEFAULTHOME entry. Configured with the DEFAULTHOME parameter
9(X'9')	SMF1154_1_NETANetwPfxLen	1	Binary	**Network address prefix length** Network address prefix length for the IPv4 or IPv6 network value Configured on the NETACCESS network sub statement

Table 24. Network access configuration section (continued)

Offset	Name	Length	Format	Description
10(X'A')	SMF1154_1_NETACache	1	Binary	**NETACCESS cache option** **SMF1154_1_NETACacheAll (1)** When a SAF call is made to check whether a user has access to a security zone, the result is cached regardless of whether access is permitted or denied. **SMF1154_1_NETACachePermit (2)** When a SAF call is made to check whether a user has access to a security zone: • The result is cached if access is permitted. • The result is not cached if access is denied. **SMF1154_1_NETACacheSame (3)** When a SAF call is made to check whether a user has access to a security zone: • The result is cached if access is permitted. • The result is not cached if access is denied. In addition, a new SAF call is made for a previously permitted security zone in one of the following situations: • If the user that is associated with the socket changes. • If the IP address that is being accessed changes from the IP address in the previous packet that was received or sent over the socket. Configured with the CACHEALL, CACHEPERMIT, or CACHESAME parameter.
11(X'B')		1	Binary	Reserved. Set to 0.
12(X'C')	SMF1154_1_NETASafName	8	EBCDIC	**NETACCESS SAF resource name** SAF resource name, padded with trailing blanks. Configured on the NETACCESS network sub statement

Table 24. Network access configuration section (continued)

Offset	Name	Length	Format	Description
20(X'14')	SMF1154_1_NETANetwAddr4	4	Binary	**Network address** This field is valid if SMF1154_1_NETADefault=0 (not a DEFAULT entry) and SMF1154_1_NETADefaultHome=0 (not a DEFAULTHOME entry). One of the following values: • If the SMF1154_1_NETAIPv6 field is 0, SMF1154_1_NETANetwAddr4 contains the IPv4 network value. The network value is the IPv4 network address ANDed with the prefix length. • If the SMF1154_1_NETAIPv6 field is 1, SMF1154_1_NETANetwAddr6 contains the IPv6 network value. The network value is the IPv6 network address ANDed with the prefix length. Configured on the NETACCESS network sub statement
20(X'14')	SMF1154_1_NETANetwAddr6	16	Binary	

TN3270E

Telnet is a terminal emulation protocol. With Telnet, users can log on to remote host applications as though they were directly attached to that host. Telnet protocol requires that the user have a Telnet client that emulates a type of terminal that the host application can understand. The client connects to a Telnet server, which communicates with the host application. The Telnet server acts as an interface between the client and host application.

The TN3270E Telnet server (Telnet) provides access to z/OS VTAM SNA applications on the MVS host using Telnet TN3270E, TN3270, or linemode protocol. Telnet acts as an interface between IP and SNA networks. End users in an IP network connect to Telnet, which is also a VTAM application.

For z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 3 to check whether TELNETPARMS statements for all TN3270E servers are configured with appropriate inactivity timeouts, check whether PARMSGROUP statements for all TN3270E servers specify appropriate inactivity timeout values, and more.

Note: Compliance data collection for Comm Server: TN3270E requires z/OS 2.4 or later and PTFs for PH37372

SMF type 1154, subtype 3 – TN3270 Telnet server compliance evidence record

The TN3270E Telnet server compliance evidence record provides information configured in the TN3270E Telnet server profile for a single server port instance. One or more server ports can be configured for a TN3270E Telnet server. A separate record (or set of records) is written for each server port instance.

If the SMF information for a single server port exceeds 32,756 bytes, multiple records are created to provide the complete set of information. In the SMF 1154 common header SMF1154_C_RecordInd indicates if "more records follow" and SMF1154_C_SeqNum indicates the sequence number. The

sequence number starts at 0 in the first record and is incremented by 1 with each additional record. SMF1154_C_Correlator provides a correlator value unique to the server port instance.

The triplets in the SMF 1154 subtype 3 specific section indicate which sections (and how many instances of the section) are included in the record.

Records within a set of records can be correlated by using the extended record subtype (SMFHDR1_STP) from the extended SMF header and the system name (SMF1154_C_SystemName), sysplex name (SMF1154_C_SysplexName), jobname (SMF1154_C_Jobname), request ID (SMF1154_C_RequestID), and correlator (SMF1154_C_Correlator) from the SMF 1154 common header.

Each record contains an SMF extended header, an SMF 1154 common triplets section, an SMF 1154 common header section, and an SMF 1154 subtype 3 specific section (self-defining section). The subtype specific section indicates the additional sections that are included in the record.

1154 subtype 3 specific section, self-defining section

This section defines the additional sections that are included in the record. A triplet is included for each defined section. The triplet includes the offset to the section from the start of the record, the length of a single instance of the section, and the number of instances of the section in the record.

Table 25. 1154 subtype 3 specific section, self-defining section

Offset	Name	Length	Format	Description
0(X'00')	SMF1154_3_TRN	2	Binary	Number of triplets (set to 8)
2(X'02')		2		Reserved (set to 0)
4(X'04')	SMF1154_3_S1_Offset	4	Binary	Offset to TN3270E Telnet general information section (from the start of the record)
8(X'08')	SMF1154_3_S1_Length	2	Binary	Length of TN3270E Telnet general information section
10(X'0A')	SMF1154_3_S1_Number	2	Binary	Number of TN3270E Telnet general information sections (set to 1)
12(X'0C')	SMF1154_3_S2_Offset	4	Binary	Offset to TelnetGlobals section (from the start of the record)
16(X'10')	SMF1154_3_S2_Length	2	Binary	Length of TelnetGlobals section
18(X'12')	SMF1154_3_S2_Number	2	Binary	Number of TelnetGlobals sections (set to 1)
20(X'14')	SMF1154_3_S3_Offset	4	Binary	Offset to TelnetParms section (from the start of the record)
24(X'18')	SMF1154_3_S3_Length	2	Binary	Length of TelnetParms section
26(X'1A')	SMF1154_3_S3_Number	2	Binary	Number of TelnetParms sections (set to 1)
28(X'1C')	SMF1154_3_S4_Offset	4	Binary	Offset to ParmsGroup section (from the start of the record)
32(X'20')	SMF1154_3_S4_Length	2	Binary	Length of ParmsGroup section
34(X'22')	SMF1154_3_S4_Number	2	Binary	Number of ParmsGroup sections
36(X'24')	SMF1154_3_S5_Offset	4	Binary	Offset to ParmsMap section (from the start of the record)
40(X'28')	SMF1154_3_S5_Length	2	Binary	Length of ParmsMap section

Table 25. 1154 subtype 3 specific section, self-defining section (continued)

Offset	Name	Length	Format	Description
42(X'2A')	SMF1154_3_S5_Number	2	Binary	Number of ParmsMap sections
44(X'2C')	SMF1154_3_S6_Offset	4	Binary	Offset to LUMap sections (from the start of the record)
48(X'30')	SMF1154_3_S6_Length	2	Binary	Length of LuMap section
50(X'32')	SMF1154_3_S6_Number	2	Binary	Number of LuMap sections
52(X'34')	SMF1154_3_S7_Offset	4	Binary	Offset to PrtMap section (from the start of the record)
56(X'38')	SMF1154_3_S7_Length	2	Binary	Length of PrtMap section
58(X'3A')	SMF1154_3_S7_Number	2	Binary	Number of PrtMap sections
60(X'3C')	SMF1154_3_S8_Offset	4	Binary	Offset to RestrictAppl section (from the start of the record)
64(X'40')	SMF1154_3_S8_Length	2	Binary	Length of RestrictAppl section
66(X'42')	SMF1154_3_S8_Number	2	Binary	Number of RestrictAppl sections

TN3270E Telnet server general information section

Table 26. TN3270E Telnet server general information section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNPIIdent	4	EBCDIC	Identifier - 'TNPI'
4(X'4')	SMF1154_3_TNPIStartStck	8	Binary	**Time TN3270E Telnet server was started** (TOD clock value)
12(X'C')	SMF1154_3_TNPIStartDate	4	Packed	**Date TN3270E Telnet was started**

TN3270E Telnet server TelnetGlobals section

This section provides TN3270E Telnet profile values that can be set only on a TelnetGlobals statement. Only one of these sections exists in the record.

Table 27. TN3270E Telnet server TelnetGlobals section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNTGIdent	4	EBCDIC	Identifier – 'TNTG'
4(X'4')	SMF1154_3_TNTGSMFProfile	1	Binary	**Profile SMF 119 records** • 0 – TN3270E Telnet profile SMF 119 records not requested • 1 – TN3270E Telnet profile SMF 119 records requested Configured with the SMFPROFILE / NOSMFPROFILE parameter

Table 27. TN3270E Telnet server TelnetGlobals section (continued)

Offset	Name	Length	Format	Description
5(X'5')	SMF1154_3_TNTGSMF_GrpDtl	1	Binary	**Profile SMF 119 records GroupDetail** Valid if SMF1154_3_TNTGSMFProfile = 1 • 0 – TN3270E Telnet profile SMF 119 records with GROUPDETAIL not requested • 1 – TN3270E Telnet profile SMF 119 records with GROUPDETAIL requested Configured with the SMFPROFILE GROUPDETAIL / NOGROUPDETAIL parameter
6(X'6')	SMF1154_3_TNTGSAEnable	1	Binary	**SNMP subagent enabled** • 0 – SNMP subagent disabled • 1 – SNMP subagent enabled Configured with the TNSACONFIG ENABLED / DISABLED parameter
7(X'7')	SMF1154_3_TNTGSACommName	1	Binary	**SNMP Community name configured** Valid if SMF1154_3_TNTGSAEnable = 1. • 0 – Community name "public" used • 1 – Community name configured to value other than public Configured with the TNSACONFIG COMMUNITY parameter
8(X'8')	SMF1154_3_TNTGSAPort	2	Binary	**SNMP agent port** Valid if SMF1154_3_TNTGSAEnable = 1. Configured with the TNSACONFIG AGENT parameter
10(X'A')	SMF1154_3_TNTGTCPName	8	EBCDIC	**TCP/IP stack name** TCP/IP stack name, if the TN3270 Telnet server has affinity to a specific TCP/IP stack Otherwise, set to blanks Configured with the TCPIPJOBNAME / NOTCPIPJOBNAME parameter

Common parameters structure

The common parameters structure is included in the TelnetParms and ParmsGroup sections. It begins at the same offset within each section.

Table 28. Common parameters structure

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TPCCConn	1	Binary	**Check client connections** SMF1154_3_TPCCConn_Chk (1) – Check connectivity of pre-existing connections when establishing a new connection with the same client identifier SMF1154_3_TPCCConn_NoChk (2) – Do not check connectivity of pre-existing connections when establishing a new connection with the same client identifier SMF1154_3_TPCCConn_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the CHECKCLIENTCONN / NOCHECKCLIENTCONN statement

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
1(X'1')	SMF1154_3_TPConnT	1	Binary	**Connection type** SMF1154_3_TPCONNT_SSL (1) – Secure, TLS session required for connection SMF1154_3_TPCONNT_NEGTSSL (2) - TN3270 negotiate secure, TLS session required for connection. However, a TN3270 negotiation is done to determine if the client is willing to negotiate a TLS session. If so, a TLS handshake begins. If not, the connection is closed. SMF1154_3_TPCONNT_BASIC (3) - Basic, connection is established without TLS protection SMF1154_3_TPCONNT_ANY (4) – Any, an attempt is made to establish a TLS session. If the attempt fails, the connection is established without TLS protection. SMF1154_3_TPCONNT_NONE (5) - None, client connection requests rejected SMF1154_3_TPCONNT_NA (0) - Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the CONNTYPE statement
2(X'2')	SMF1154_3_TPExpLogon	1	Binary	**Allow express logon using a passticket** SMF1154_3_TPEXPLOGON_ALLOW (1) – Allow express logon using a passticket based on the user's client X.509 certificate SMF1154_3_TPEXPLOGON_NOALLOW (2) – Do not allow express logon using a passticket based on the user's client X.509 certificate SMF1154_3_TPEXPLOGON_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the EXPRESSLOGON / NOEXPRESSLOGON statement

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
3(X'3')	SMF1154_3_TPExpLogonMFA	1	Binary	**Allow express logon using an MFA token** SMF1154_3_TPEXPLOGONMFA_ALLOW (1) – Allow express logon using a Multi-Factor Authentication (MFA) token based on the user's client X.509 certificate SMF1154_3_TPEXPLOGONMFA_NOALLOW (2) – Do not allow express logon using an MFA token based on the user's client X.509 certificate SMF1154_3_TPEXPLOGONMFA_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the EXPRESSLOGONMFA / NOEXPRESSLOGONMFA statement
4(X'4')	SMF1154_3_TPMFAFallback	1	Binary	**Allow fallback to express logon using a passticket** Valid if SMF1154_3_TPExpLogonMFA=1 SMF1154_3_TPMFAFALLBACK_ALLOW (1) – Allow fallback to express logon using a passticket, if MFA is active, but unavailable SMF1154_3_TPMFAFALLBACK_NOALLOW (2) – Do not allow fallback to express logon using a passticket when MFA is active, but unavailable SMF1154_3_TPMFAFALLBACK_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with EXPRESSLOGONMFA FALLBACK / NOFALLBACK statement

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
5(X'5')	SMF1154_3_TPPPhrase	1	Binary	**Passphrase can be accepted on solicitor screen** SMF1154_3_TPPPHRASE_PASSPHRASE (1) – Solicitor screen provides space for a passphrase SMF1154_3_TPPPHRASE_NOPASSPHRASE (2) – Solicitor screen provides space only for a password SMF1154_3_TPPPHRASE_DISPASSPHRASE (3) – Solicitor screen only provides password support SMF1154_3_TPPPHRASE_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the PASSWORDPHRASE / NOPPASSWORDPHRASE / DISABLEPASSWORDPHRASE statement
6(X'6')	SMF1154_3_TPTTLSPort	1	Binary	**Port is used for TLS connections** Valid for TelnetParms SMF1154_3_TPTTLSPORT_SECURE (1) – port is used for connections that are secured with TLS (TTLSPORT) SMF1154_3_TPTTLSPORT_UNSECURE (2) – port is used for unsecured connections (PORT) SMF1154_3_TPTTLSPORT_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the PORT or TTLSPORT statement

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
7(X'7')	SMF1154_3_TPSMFInit119	1	Binary	**TN3270E Telnet SNA Session Initiation SMF 119 records** SMF1154_3_TPSMFINIT119_REQ (1) – TN3270E Telnet SNA Session Initiation SMF 119 records requested SMF1154_3_TPSMFINIT119_NOREQ (2) – TN3270E Telnet SNA Session Initiation SMF 119 records not requested SMF1154_3_TPSMFINIT119_NA (0) - Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the SMFINIT TYPE119 statement
8(X'8')	SMF1154_3_TPSMFTerm119	1	Binary	**TN3270E Telnet SNA Session Termination SMF 119 records** SMF1154_3_TPSMFTERM119_REQ (1) – TN3270E Telnet SNA Session Termination SMF 119 records requested SMF1154_3_TPSMFTERM119_NOREQ (2) – TN3270E Telnet SNA Session Termination SMF 119 records not requested SMF1154_3_TPSMFTERM119_NA (0) – Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the SMFTERM TYPE119 statement

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
9(X'9')	SMF1154_3_TPTKOGenLu	1	Binary	**Generic LU takeover** SMF1154_3_TPTKOGENLU_NOTENABLED (1) - Generic LU takeover not enabled (NOTKOGENLU or NOTKO) SMF1154_3_TPTKOGENLU_ENABLED (2) - Generic LU takeover enabled, session not transferred to the taker connection (TKOGENLU) SMF1154_3_TPTKOGENLU_RECON (3) - Generic LU takeover enabled, session transferred to the taker (TKOGENLURECON) SMF1154_3_TPTKOGENLU_NA (0) - Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the TKOGENLU, NOTKOGENLU, TKOGENLURECON, or NOTKO statement
10(X'A')	SMF1154_3_TPTKOSpecLu	1	Binary	**Specific LU takeover** SMF1154_3_TPTKOSPECLU_NOTENABLED (1) - Specific LU takeover not enabled (NOTKOSPECLU or NOTKO) SMF1154_3_TPTKOSPECLU_ENABLED (2) - Specific LU takeover enabled, session not transferred to the taker connection (TKOSPECLU) SMF1154_3_TPTKOSPECLU_RECON (3) - Specific LU takeover enabled, session transferred to the taker (TKOSPECLURECON) SMF1154_3_TPTKOSPECLU_NA (0) - Value not configured for ParmsGroup, associated TelnetParms value in effect Configured with the TKOSPECLU, NOTKOSPECLU, TKOSPECLURECON, or NOTKO statement
11(X'B')		1	Binary	Reserved. Set to 0

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
12(X'C')	SMF1154_3_TPInact	1	Binary	**Terminal SNA session inactivity timer** SMF1154_3_TPINACT_ON (1) – Inactivity timer in effect SMF1154_3_TPINACT_OFF (2) – Inactivity timer not in effect SMF1154_3_TPINACT_NA (0) - Inactivity timer not configured for ParmsGroup, associated TelnetParms value in effect Configured with the INACTIVE statement
13(X'D')	SMF1154_3_TPKeepInact	1	Binary	**Session setup inactivity timer** SMF1154_3_TPKEEPINACT_ON (1) – Inactivity timer in effect SMF1154_3_TPKEEPINACT_OFF (2) – Inactivity timer not in effect SMF1154_3_TPKEEPINACT_NA (0) - Inactivity timer not configured for ParmsGroup, associated TelnetParms value in effect Configured with the KEEPINACTIVE statement
14(X'E')	SMF1154_3_TPPrtInact	1	Binary	**Printer inactivity timer** SMF1154_3_TPPRTINACT_ON (1) – Inactivity timer in effect SMF1154_3_TPPRTINACT_OFF (2) - Inactivity timer not in effect SMF1154_3_TPPRTINACT_NA (0) - Inactivity timer not configured for ParmsGroup, associated TelnetParms value in effect Configured using the PRTINACTIVE statement

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
15(X'F')	SMF1154_3_TPProfInact	1	Binary	**Timer for connections with a non-current profile** SMF1154_3_TPPROFINACT_ON (1) – Inactivity timer in effect SMF1154_3_TPPROFINACT_OFF (2) – Inactivity timer not in effect SMF1154_3_TPPROFINACT_NA (0) - Inactivity timer not configured for ParmsGroup, associated TelnetParms value in effect Configured using the PROFILEINACTIVE statement
16(X'10')	SMF1154_3_TPInactSec	4	Binary	**Terminal SNA session inactivity timeout (in seconds)** Valid if SMF1154_3_TPInact = 1 The timer applies to a KEEPOPEN connection only when an SNA session, with the VTAM application, is active. A connection that has no client-VTAM session activity for the specified time is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the inactivity timer. Configured with the INACTIVE statement
20(X'14')	SMF1154_3_TPKeepInactSec	4	Binary	**Session setup inactivity timeout (in seconds)** Valid if SMF1154_3_TPKeepInact = 1 The timer applies to a KEEPOPEN connection with no active SNA session. A connection that has no client-VTAM activity for the specified time is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the inactivity timer. Configured with the KEEPINACTIVE statement

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
24(X'18')	SMF1154_3_TPPrtInactSec	4	Binary	**Printer inactivity timeout (in seconds)** Valid if SMF1154_3_TPPrtInact = 1 A printer connection with no client-VTAM activity for the specified time is dropped. The value is in a range of 0 – 99999999. A value of 0 disables the inactivity timer. Configured using the PRTINACTIVE statement
28(X'1C')	SMF1154_3_TPProfInactSec	4	Binary	**Timeout for connections with a non-current profile (in seconds)** Valid if SMF1154_3_TPProfInact = 1 A connection that does not have a SNA session for the specified time and that is associated with a non-current profile is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the inactivity timer. Configured using the PROFILEINACTIVE statement
32(X'20')	SMF1154_3_TPMaxRcv	1	Binary	**MaxReceive limit** SMF1154_3_TPMAXRCV_ON (1) – MAXRECEIVE limit in effect SMF1154_3_TPMAXRCV_OFF (2) – MAXRECEIVE limit not in effect SMF1154_3_TPMAXRCV_NA (0) - MAXRECEIVE limit not configured for ParmsGroup, associated TelnetParms value in effect Configured using the MAXRECEIVE statement
33(X'21')	SMF1154_3_TPMaxReqSess	1	Binary	**MaxReqSess limit** SMF1154_3_TPMAXREQSESS_ON (1) – MAXREQSESS limit in effect SMF1154_3_TPMAXREQSESS_OFF (2) – MAXREQSESS limit not in effect SMF1154_3_TPMAXREQSESS_NA (0) - MAXREQSESS limit not configured for ParmsGroup, associated TelnetParms value in effect Configured using the MAXREQSESS statement

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
34(X'22')	SMF1154_3_TPMax_RUChain	1	Binary	**MaxRUChain limit** SMF1154_3_TPMAX_RUCHAIN_ON (1) –MAXRUCHAIN limit in effect SMF1154_3_TPMAX_RUCHAIN_OFF(2) – MAXRUCHAIN limit not in effect SMF1154_3_TPMAX_RUCHAIN_NA (0) - MAXRUCHAIN limit not configured for ParmsGroup, associated TelnetParms value in effect Configured using the MAXRUCHAIN statement
35(X'23')	SMF1154_3_TPMaxTcpSendQ	1	Binary	**MaxTCPSendQ limit** SMF1154_3_TPMAXTCPSENDQ_ON (1) –MAXTCPSENDQ limit in effect SMF1154_3_TPMAXTCPSENDQ_OFF (2) – MAXTCPSENDQ limit not in effect SMF1154_3_TPMAXTCPSENDQ_NA (0) - MAXTCPSENDQ limit not configured for ParmsGroup, associated TelnetParms value in effect Configured using the MAXTCPSENDQ statement
36(X'24')	SMF1154_3_TPMaxVtamSendQ	1	Binary	**MaxVTAMSendQ limit** SMF1154_3_TPMAXVTAMSENDQ_ON (1) –MAXVTAMSENDQ limit in effect SMF1154_3_TPMAXVTAMSENDQ_OFF (2) – MAXVTAMSENDQ limit not in effect SMF1154_3_TPMAXVTAMSENDQ_NA (0) - MAXVTAMSENDQ limit not configured for ParmsGroup, associated TelnetParms value in effect Configured using the MAXVTAMSENDQ statement
37(X'25')		3	Binary	Reserved, set to 0

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
40(X'28')	SMF1154_3_TPMaxRcvSize	4	Binary	**Bytes received from client without an EOR** Valid if SMF1154_3_TPMaxRcv = 1 The number of bytes that can be received from a client without an End of Record (EOR) being received. If the amount of data received exceeds the limit, the connection is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the limit check function. Protects against a client in a send-data loop. Configured using the MAXRECEIVE statement
44(X'2C')	SMF1154_3_TPMaxReqSessNum	4	Binary	**Number of session requests received in 10-second period** Valid if SMF1154_3_TPMaxReqSess = 1 Number of session requests that can be received in a 10-second period. If the limit is exceeded, the connection is dropped and an error is reported. The value is in a range of 0 - 99999999. A value of 0 disables the limit check function. Protects against session logon loops that are possibly created by an automatic CLSDST-PASS to an inactive application. Configured using the MAXREQSESS statement

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
48(X'30')	SMF1154_3_TPMaxRUChainNum	4	Binary	**Number of chained RUs received without an EC** Valid if SMF1154_3_TPMax_RUChain = 1 The number of chained RUs received from an application without an end of chain (EC) being received. If the number of RUs received exceeds the limit, the session, and conditionally the connection, is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the limit check function. This parameter protects against a host application sending too much chained data. Configured using the MAXRUCHAIN statement
52(X'34')	SMF1154_3_TPMaxTcpSndQNum	4	Binary	**Number of bytes queued to be sent to a client** Valid if SMF1154_3_TPMaxTcpSendQ = 1 The number of bytes that are queued to be sent to a client. If the queue size exceeds the limit, the connection is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the limit check function. This parameter prevents large amounts of storage from being held for data that is destined for an unresponsive client. Configured using the MAXTCPSENDQ statement

Table 28. Common parameters structure (continued)

Offset	Name	Length	Format	Description
56(X'38')	SMF1154_3_TPMxVtamSndQNum	4	Binary	**Number of RPLs queued to be sent to VTAM** Valid if SMF1154_3_TPMaxVtamSendQ = 1 The number of data segments (RPLs) queued to be sent to VTAM. If the queue size exceeds the limit, the connection is dropped. The value is in a range of 0 - 99999999. A value of 0 disables the limit check function. This parameter protects against using large amounts of storage to contain data destined for a host VTAM application that is not receiving data. Configured using the MAXVTAMSENDQ statement
60(X'3C')	SMF1154_3_TPNacUserId	8	EBCDIC	**Network access user ID** If not blank, user ID used for network access (NETACCESS) control checking. Otherwise (field is blank), the TN3270E Telnet's address space user ID is used for network access control checking. Configured with the NACUSERID / NONACUSERID statement

TN3270E Telnet server TelnetParms section

This section identifies the server port for which the record is being written. This section provides the profile values that can be set on the TelnetParms statement.

Note: A server port is identified with a port number, a port number and IP address, or a port number and link name.

The TelnetParms section includes a reference to the Common parameters structure.

Table 29. TN3270E Telnet server TelnetParms section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNTPIdent	4	EBCDIC	Identifier – 'TNTP'
4(X'4')	SMF1154_3_TNTPPortNum	2	Binary	**Port number** Configured with the PORT or TTLSPORT statement
6(X'6')	SMF1154_3_TNTPIndex	2	Binary	**Internal index used by IBM**

Table 29. TN3270E Telnet server TelnetParms section (continued)

Offset	Name	Length	Format	Description
8(X'8')	SMF1154_3_TNTPPortIpAddr4	4	Binary	**IPv4 address qualifying port** Valid if SMF1154_3_TNTPPQ_IPaddr = 1 and SMF1154_3_TNTPPQ_IPv6 = 0. Configured with the PORT or TTLSPORT statement
8(X'8')	SMF1154_3_TNTPPortIpAddr6	16	Binary	**IPv6 address qualifying port** Valid if SMF1154_3_TNTPPQ_IPaddr = 1 and SMF1154_3_TNTPPQ_IPv6 = 1. Configured with the PORT or TTLSPORT statement
24(X'18')	SMF1154_3_ TNTPPortLink	16	EBCDIC	**Link name qualifying port** Valid if SMF1154_3_TNTPPQ_Link = 1. Otherwise, set to blanks. Configured with the PORT or TTLSPORT statement
40(X'28')	SMF1154_3_TNTPPQ_Link	1	Binary	**Whether the port is qualified with link name** • 0 – Port is not qualified with a link name • 1 – Port is qualified with a link name Configured with the PORT or TTLSPORT statement
41(X'29')	SMF1154_3_TNTPPQ_IPaddr	1	Binary	**Whether the port is qualified with IP address** • 0 – Port is not qualified with an IP address • 1 – Port is qualified with an IP address Configured with the PORT or TTLSPORT statement
42(X'2A')	SMF1154_3_TNTPPQ_IPv6	1	Binary	**IPv6 indicator** This field is valid if the port is qualified with an IP address (SMF1154_3_TNTPPQ_IPaddr = 1). • 0 - IPv4 address provided in SMF1154_3_TNTPPortIpAddr4 • 1 - IPv6 address provided in SMF1154_3_TNTPPortIpAddr6
43(X'2B')		13	Binary	Reserved, set to 0
56(X'38')	SMF1154_3_TNTPCParms	68		See Common parameters structure

TN3270E Telnet server ParmsGroup section

This optional section provides the values of the ParmsGroup statements in the BEGINVTAM block for the server port.

Note: A server port can be identified with a port number, a port number and IP address, or a port number and link name. One entry exists for each ParmsGroup statement for the server port.

The ParmsGroup section includes a reference to the Common parameters structure.

Table 30. TN3270E Telnet server ParmsGroup section

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_TNPGIdent	4	EBCDIC	Identifier – 'TNPG'
4(X'4')	SMF1154_3_TNPGPortNum	2	Binary	**Port number** Port number for the server port instance.
6(X'6')	SMF1154_3_TNPGIndex	2	Binary	**Internal index used by IBM**
8(X'8')	SMF1154_3_TNPGPortIpAddr4	4	Binary	**IPv4 address qualifying port** Valid if SMF1154_3_TNPGPQ_IPaddr = 1 and SMF1154_3_TNPGPQ_IPv6 = 0. IPv4 address for the server port instance.
8(X'8')	SMF1154_3_TNPGPortIpAddr6	16	Binary	**IPv6 address qualifying port** Valid if SMF1154_3_TNPGPQ_IPaddr = 1 and SMF1154_3_TNPGPQ_IPv6 = 1. IPv6 address for the server port instance.
24(X'18')	SMF1154_3_ TNPGPortLink	16	EBCDIC	**Link name qualifying port** Valid if SMF1154_3_TNPGPQ_Link = 1. Otherwise, set to blanks. Link name for the server port instance.
40(X'28')	SMF1154_3_TNPGPQ_Link	1	Binary	**Whether the port is qualified with link name** • 0 – Port is not qualified with a link name • 1 – Port is qualified with a link name
41(X'29')	SMF1154_3_TNPGPQ_IPaddr	1	Binary	**Whether the port is qualified with IP address** • 0 – Port is not qualified with an IP address • 1 – Port is qualified with an IP address

Table 30. TN3270E Telnet server ParmsGroup section (continued)

Offset	Name	Length	Format	Description
42(X'2A')	SMF1154_3_TNPGPQ_IPv6	1	Binary	**IPv6 indicator** This field is valid if the port is qualified with an IP address (SMF1154_3_TNPGPQ_IPaddr = 1). • 0 - IPv4 address provided in SMF1154_3_TNPGPortIpAddr4 • 1 - IPv6 address provided in SMF1154_3_TNPGPortIpAddr6
43(X'2B')		5	Binary	Reserved, set to 0
48(X'30')	SMF1154_3_TNPGGroupName	8	EBCDIC	**ParmsGroup name**
56(X'38')	SMF1154_3_TNPGCParms	68		See Common parameters structure

Client ID structure

The client ID structure is included in the ParmsMap, LUMap, and PrtMap sections. The client ID can be one of several types. SMF1154_3_IDType identifies the type of client ID.

The size of the client ID structure is variable. The length of the section in the record must be used to parse the record.

If the client ID structure contains a host name, SMF1154_3_IDHlen contains the length of the host name.

Table 31. Client ID structure

Offset	Name	Length	Format	Description
0(X'0')	SMF1154_3_IDType	1	Binary	**Client ID type** **SMF1154_3_ID_EMPTY (0)** Unknown type **SMF1154_3_ID_USERID (1)** SMF1154_3_IDUser is a USERID **SMF1154_3_ID_HNAME (2)** SMF1154_3_IDHname is a HOSTNAME **SMF1154_3_ID_IPADDR (3)** SMF1154_3_IDIpAddr*x* is an IPADDR **SMF1154_3_ID_USERGRP (4)** SMF1154_3_IDGrpName is a USERGRP **SMF1154_3_ID_HNGRP (5)** SMF1154_3_IDGrpName is an HNGRP **SMF1154_3_ID_IPGRP (6)** SMF1154_3_IDGrpName is an IPGRP **SMF1154_3_ID_DESTIP (7)** SMF1154_3_IDIpAddr*x* is a DESTIP **SMF1154_3_ID_LNKNAME (8)** SMF1154_3_IDLinkName is a LINKNAME **SMF1154_3_ID_DIPGRP (9)** SMF1154_3_IDGrpName is a DESTIPGRP **SMF1154_3_ID_LNKGRP (10)** SMF1154_3_IDGrpName is a LINKGRP **SMF1154_3_ID_NULL (11)** No ID is associated
1(X'1')	SMF1154_3_IDIPv6	1	Binary	**IPv6 indicator** Valid if client identifier is an IP address (SMF1154_3_IDType = 3 or 7) • 0 - IPv4 address provided in SMF1154_3_IDIPAddr4 • 1 - IPv6 address provided in SMF1154_3_IDIPAddr6
1(X'1')	SMF1154_3_IDHlen	1	Binary	**Length of host name** Valid if client identifier is a host name (SMF1154_3_IDType = 2)

Table 31. Client ID structure (continued)				
Offset	**Name**	**Length**	**Format**	**Description**
2(X'2')	SMF1154_3_IDUser	8	EBCDIC	**User ID** Valid if client identifier is a user ID (SMF1154_3_IDType = 1)
2(X'2')	SMF1154_3_IDLinkName	16	EBCDIC	**Link name** Valid if client identifier is a link name (SMF1154_3_IDType = 8)
2(X'2')	SMF1154_3_IDGrpName	16	EBCDIC	**Group name** Valid if client identifier is group name (SMF1154_3_IDType = 4, 5, 6, 9, or 10)
2(X'2')	SMF1154_3_IDIPaddr4	4	Binary	**IPv4 address** Valid if client identifier is an IPv4 address (SMF1154_3_IDType = 3 or 7 and SMF1154_3_IDIPv6 = 0)
2(X'2')	SMF1154_3_IDIPaddr6	16	Binary	**IPv6 address** Valid if client identifier is an IPv6 address (SMF1154_3_IDType = 3 or 7 and SMF1154_3_IDIPv6 = 1)
2(X'2')	SMF1154_3_IDHName	255	EBCDIC	**Host name** Valid if client identifier is a host name (SMF1154_3_IDType = 2) **Note:** The length of a host name can be up to 255 bytes. However, SMF1154_3_IDHlen must be used to know the length of the host name.

TN3270E Telnet server ParmsMap section

This optional section provides the values of a ParmsMap statement in the BEGINVTAM block for the server port that is identified in the TelnetParms section. One entry exists for each ParmsMap statement for the server port.

The ParmsMap section includes a reference to a client ID that can be one of several types. See the Client ID structure for the definition of the client ID.

The size of the client ID structure is not fixed. The length of the ParmsMap section in the record must be used to parse the record.

Table 32. TN3270E Telnet server ParmsMap section				
Offset	**Name**	**Length**	**Format**	**Description**
0(X'0')	SMF1154_3_TNPMIdent	4	EBCDIC	Identifier – 'TNPM'
4(X'4')	SMF1154_3_TNPMName	8	EBCDIC	ParmsGroup name

Table 32. TN3270E Telnet server ParmsMap section (continued)				
Offset	**Name**	**Length**	**Format**	**Description**
12(X'C')	SMF1154_3_TNPMClid			**Client Identifier** See Client ID structure

TN3270E Telnet server LUMap section

This optional section provides the values of an LUMap statement in the BEGINVTAM block for the server port that is identified in the TelnetParms section. One entry exists for each LUMap statement for the server port.

The LUMap section includes a reference to a client ID that can be one of several types. See the Client ID structure for the definition of the client ID.

The size of the client ID structure is not fixed. The length of the LUMap section in the record must be used to parse the record.

Table 33. TN3270E Telnet server LUMap section				
Offset	**Name**	**Length**	**Format**	**Description**
0(X'0')	SMF1154_3_TNLMIdent	4	EBCDIC	Identifier – 'TNLM'
4(X'4')	SMF1154_3_TNLMName	8	EBCDIC	**LU or LUGroup name**
12(X'C')	SMF1154_3_TNLMPName	8	EBCDIC	**ParmsGroup name** ParmsGroup name if configured. Otherwise, set to blanks. Configured with the PMAP parameter on the LUMAP statement
20(X'14')	SMF1154_3_TNLMClid			**Client Identifier** See Client ID structure

TN3270E Telnet server PrtMap section

This optional section provides the values of a PrtMap statement in the BEGINVTAM block for the server port that is identified in the TelnetParms section. One entry exists for each PrtMap statement for the server port.

The PrtMap section includes a reference to a client ID that can be one of several types. See the Client ID structure for the definition of the client ID.

The size of the client ID structure is not fixed. The length of the PrtMap section in the record must be used to parse the record.

Table 34. TN3270E Telnet server PrtMap section				
Offset	**Name**	**Length**	**Format**	**Description**
0(X'0')	SMF1154_3_TNRMIdent	4	EBCDIC	Identifier – 'TNRM'
4(X'4')	SMF1154_3_TNRMName	8	EBCDIC	**Printer LU or PRTGroup name**

Table 34. TN3270E Telnet server PrtMap section (continued)				
Offset	**Name**	**Length**	**Format**	**Description**
12(X'C')	SMF1154_3_TNRMPName	8	EBCDIC	**ParmsGroup name** ParmsGroup name if configured. Otherwise, set to blanks. Configured with the PMAP parameter on the PRTMAP statement
20(X'14')	SMF1154_3_TNRMClid			**Client Identifier** See Client ID structure

TN3270E Telnet server RestrictAppl section

This optional section provides the values of the RestrictAppl statements in the BEGINVTAM block for the server port that is identified in the TelnetParms section.

Each section includes up to 10 user IDs associated with the RestrictAppl statement. If there are more than 10 user IDs, additional sections are included.

Table 35. TN3270E Telnet server RestrictAppl section				
Offset	**Name**	**Length**	**Format**	**Description**
0(X'0')	SMF1154_3_TNARIdent	4	EBCDIC	Identifier – 'TNAR'
4(X'4')	SMF1154_3_TNARName	8	EBCDIC	**Application name** The host application name, as specified in VTAMLST. Wild card characters can be included.
12(X'C')	SMF1154_3_TNARCertAuth	1	Binary	**Use derived user ID** • 0 – Use RestrictAppl password validation • 1 – Use derived user ID based on TLS client certificate, skipping the RestrictAppl password validation Configured with the RestrictAppl CertAuth statement
13(X'D')		3	Binary	Reserved, set to 0
16(X'10')	SMF1154_3_TNARLstCnt	4	Binary	Total number of user IDs defined
20(X'14')	SMF1154_3_TNARLstIdx	4	Binary	Index into user IDs defined
24(X'18')	SMF1154_3_TNARLstNum	4	Binary	Number of user IDs in this section
28(X'1C')	SMF1154_3_TNARLst	80		Array of 10 user IDs
28(X'1C')	SMF1154_3_TNARUser	8	EBCDIC	User ID

Consoles

Operating z/OS involves the following:

- Console operations or how operators interact with z/OS to monitor or control the hardware and software

- Message and command processing that forms the basis of operator interaction with z/OS and the basis of z/OS automation

Generally, operators on a z/OS system receive messages and enter commands on MCS and SMCS consoles.

- MCS consoles are devices that are locally attached to a z/OS system and provide the basic communication between operators and z/OS
- SMCS consoles use z/OS Communications Server to provide communication between operators and z/OS instead of direct I/O to the console device

With the IBM Z Security and Compliance Center, you can automatically collect data from SMF Type 1154 Subtype 50 to check whether auto sign-off time for Master, MCS and SMCS consoles is properly configured, check whether the console logon setting for Master, MCS and SMCS consoles is properly configured, and more.

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

Db2 for z/OS

Db2 for z/OS is a relational database management system that runs on the mainframe.

A relational database is a database in which all of the data is logically contained in tables. These databases are organized according to the relational model. In a relational database, referential integrity ensures data integrity by enforcing rules with referential constraints, check constraints, and triggers. You can rely on constraints and triggers to ensure the integrity and validity of your data, rather than relying on individual applications to do that work.

With Db2 for z/OS, you can define and manipulate your data by using structured query language (SQL). SQL is the standard language for accessing data in relational databases.

For z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 81 to check whether the installation specified default ID has been changed, check whether Db2 is configured to use a security port, check whether Db2 is configured to require authorization, and more.

Note: Compliance data collection for Db2 for z/OS requires Db2 v13. For more information, see IBM Db2 for z/OS (www.ibm.com/analytics/us/en/technology/db2/db2-for-zos.html).

DFSMS

DFSMSdfp

DFSMS comprises a suite of related data and storage management products for the z/OS system. DFSMS is an operating environment that helps automate and centralize the management of storage, based on the policies that your installation defines for availability, performance, space, and security.

DFSMSdfp provides:

- Storage management
- Tape mount management
- Data management
- Device management
- Distributed data success
- Advanced copy servers
- Object access method

With the IBM Z Security and Compliance Center, you can automatically collect data from SMF Type 1154 Subtype 51 to check whether the authority to rename non-SMS system data sets is restricted, check whether SMS settings are protected against modification, and more.

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

DFSMSdss

DFSMS comprises a suite of related data and storage management products for the z/OS system. DFSMS is an operating environment that helps automate and centralize the management of storage, based on the policies that your installation defines for availability, performance, space, and security.

DFSMSdss provides:

- Data movement and replication
- Space management
- Data backup and recovery
- Data set and volume conversion

With the IBM Z Security and Compliance Center, you can automatically collect data from SMF Type 1154 Subtype 54 to check whether authority to copy data sets is protected, check whether authority to move data sets is protected, check whether authority to dump data sets is protected, and more.

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

DFSMShsm

DFSMS comprises a suite of related data and storage management products for the z/OS system. DFSMS is an operating environment that helps automate and centralize the management of storage, based on the policies that your installation defines for availability, performance, space, and security.

DFSMShsm provides:

- Storage management
- Space management
- Tape mount management
- Availability management

With the IBM Z Security and Compliance Center, you can automatically collect data from:

- SMF Type 1154 Subtype 52 to check whether RMM audit and security records are generated, and more.
- SMF Type 1154 Subtype 53 to check whether adding a migration volume is protected, check whether backups of all data sets are protected, check whether storage admin LIST commands are protected, and more.

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

DFSMSrmm

DFSMS comprises a suite of related data and storage management products for the z/OS system. DFSMS is an operating environment that helps automate and centralize the management of storage, based on the policies that your installation defines for availability, performance, space, and security.

DFSMSrmm manages your removable media resources, including tape cartridges and reels. It provides:

- Library management
- Shelf management
- Volume management
- Data set management

ICSF

Integrated Cryptographic Services Facility (ICSF) provides the application programming interfaces by which applications request cryptographic services. ICSF callable services and programs can be used to generate, maintain, and manage keys that are used in cryptographic operations to:

- Protect data
- Protect and distribute additional keys
- Verify message integrity
- Generate, protect and verify PINs
- Generate and verify signatures

For z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 49 to check that weak algorithm DES56 is not in use, check that weak algorithm DES112 is not in use, check that weak algorithm SHA1 is not in use, and more.

Note: Compliance data collection for ICSF requires z/OS 2.4 or later and PTFs for OA61977.

Record type 1154 (X'482') Subtype 49 – ICSF Compliance Evidence

Record type 1154 Subtype 49 is written to record ICSF compliance evidence when an ENF86 signal is received. Record type 1154 Subtype 49 is mapped by the CSFZ1154 macro.

See *z/OS MVS System Management Facilities (SMF)* for a complete description of the SMF 1154 record and subtypes.

Record type 1154 (X'482') Subtype 49 header

Table 36. Record type 1154 Subtype 49 header

Offsets		Name	Length	Format	Description
0	0	Smf1154_49_Trn	2	Binary	Number of triplets: 2
2	2	Smf1154_49_Rsv1	2		Reserved (X'00')
4	4	Smf1154_49_1_Offset	4	Binary	Offset to first data section 1
8	8	Smf1154_49_1_Length	2	Binary	Length of data section 1
10	A	Smf1154_49_1_Number	2	Binary	Number of repeated data section 1's: 1
12	C	Smf1154_49_2_Offset	4	Binary	Offset to first data section 2
16	10	Smf1154_49_2_Length	2	Binary	Length of data section 2
18	12	Smf1154_49_2_Number	2	Binary	Number of repeated data section 2's: 1

Record type 1154 (X'482') Subtype 49 Data section 1

Data section 1 reports various ICSF security settings for ICSF key data sets, ICSF resource classes, key store policy, and other configuration and audit options.

Table 37. Record type 1154 Subtype 49 Data section 1

Offsets		Name	Length	Format	Description
0	0	SMF1154_49_1_VERSION	2	Binary	Version of this section: 1
2	2	SMF1154_49_1_PROTECTALLFAIL	1	Binary	RACF PROTECTALL setting: **X'01'** PROTECTALL(FAIL) **X'00'** PROTECTALL(WARN) or NOPROTECTALL
3	3	SMF1154_49_1_CHKAUTH	1	Binary	Setting of CHKAUTH keyword in ICSF options dataset.
4	4	SMF1154_49_1_RSV1	28		Reserved.
32	20	SMF1154_49_1_XFACILIT_ACT	1	Binary	XFACILIT class status: **X'01'** Active **X'00'** Not Active
33	21	SMF1154_49_1_XFACILIT_RACL	1	Binary	XFACILIT class RACLIST status: **X'01'** Raclisted **X'00'** Not Raclisted
34	22	SMF1154_49_1_KSPCTOKCHKLBLWARN	1	Binary	CSF.CKDS.TOKEN.CHECK.LABEL.WARN setting: **X'01'** Enabled **X'00'** Not Enabled
35	23	SMF1154_49_1_KSPCTOKCHKLBLFAIL	1	Binary	CSF.CKDS.TOKEN.CHECK.LABEL.FAIL setting: **X'01'** Enabled **X'00'** Not Enabled
36	24	SMF1154_49_1_KSPPTOKCHKLBLWARN	1	Binary	CSF.PKDS.TOKEN.CHECK.LABEL.WARN setting: **X'01'** Enabled **X'00'** Not Enabled
37	25	SMF1154_49_1_KSPPTOKCHKLBLFAIL	1	Binary	CSF.PKDS.TOKEN.CHECK.LABEL.FAIL setting: **X'01'** Enabled **X'00'** Not Enabled
38	26	SMF1154_49_1_KSPCTOKCHKDFLTLBL	1	Binary	CSF.CKDS.TOKEN.CHECK.DEFAULT.LABEL setting: **X'01'** Enabled **X'00'** Not Enabled
39	27	SMF1154_49_1_KSPPTOKCHKDFLTLBL	1	Binary	CSF.PKDS.TOKEN.CHECK.DEFAULT.LABEL setting: **X'01'** Enabled **X'00'** Not Enabled
40	28	SMF1154_49_1_KSP_CTOKNODUPS	1	Binary	CSF.CKDS.TOKEN.NODUPLICATES setting: **X'01'** Enabled **X'00'** Not Enabled

Table 37. Record type 1154 Subtype 49 Data section 1 (continued)

Offsets		Name	Length	Format	Description
41	29	SMF1154_49_1_KSP_PTOKNODUPS	1	Binary	CSF.PKDS.TOKEN.NODUPLICATES setting: **X'01'** Enabled **X'00'** Not Enabled
42	2A	SMF1154_49_1_KSP_XKEYENABLEAES	1	Binary	CSF.XCSFKEY.ENABLE.AES setting: **X'01'** Enabled **X'00'** Not Enabled
43	2B	SMF1154_49_1_KSP_XKEYENABLEDES	1	Binary	CSF.XCSFKEY.ENABLE.DES setting: **X'01'** Enabled **X'00'** Not Enabled
44	2C	SMF1154_49_1_KSP_KEYSAUTHWARN	1	Binary	CSF.CSFKEYS.AUTHORITY.LEVELS.WARN setting: **X'01'** Enabled **X'00'** Not Enabled
45	2D	SMF1154_49_1_KSP_KEYSAUTHFAIL	1	Binary	CSF.CSFKEYS.AUTHORITY.LEVELS.FAIL setting: **X'01'** Enabled **X'00'** Not Enabled
46	2E	SMF1154_49_1_KSP_ARCHUSE	1	Binary	CSF.KDS.KEY.ARCHIVE.USE setting: **X'01'** Enabled **X'00'** Not Enabled
47	2F	SMF1154_49_1_KSP_ARCHDATADEC	1	Binary	CSF.KDS.KEY.ARCHIVE.DATA.DECRYPT setting: **X'01'** Enabled **X'00'** Not Enabled **Note:** This field is reserved (X'00') on ICSF FMID HCR77D1.
48	30	SMF1154_49_1_KSP_KGUPAUTHCHK	1	Binary	CSF.KGUP.CSFKEYS.AUTHORITY.CHECK setting: **X'01'** Enabled **X'00'** Not Enabled
49	31	SMF1154_49_1_KSP_ECCPVTKEYNAME	1	Binary	CSF.CSFKEYS.ECC.PRIVATEKEYNAME.ENABLE setting: **X'01'** Enabled **X'00'** Not Enabled **Note:** This field is reserved (X'00') on ICSF FMID HCR77D1.
50	32	SMF1154_49_1_RSV2	16		Reserved.
66	42	SMF1154_49_1_AKL_CLBL	1	Binary	AUDITKEYLIFECKDS(LABEL()) **X'01'** YES **X'00'** NO

Table 37. Record type 1154 Subtype 49 Data section 1 (continued)

Offsets		Name	Length	Format	Description
67	43	SMF1154_49_1_AKL_CTOK	1	Binary	AUDITKEYLIFECKDS(TOKEN()) **X'01'** YES **X'00'** NO
68	44	SMF1154_49_1_AKL_PLBL	1	Binary	AUDITKEYLIFEPKDS(LABEL()) **X'01'** YES **X'00'** NO
69	45	SMF1154_49_1_AKL_PTOK	1	Binary	AUDITKEYLIFEPKDS(TOKEN()) **X'01'** YES **X'00'** NO
70	46	SMF1154_49_1_AKL_TTOKO	1	Binary	AUDITKEYLIFETKDS(TOKENOBJ()) **X'01'** YES **X'00'** NO
71	47	SMF1154_49_1_AKL_TSESSO	1	Binary	AUDITKEYLIFETKDS(SESSIONOBJ()) **X'01'** YES **X'00'** NO
72	48	SMF1154_49_1_RSV3	8		Reserved.
80	50	SMF1154_49_1_AKU_CLBL	1	Binary	AUDITKEYUSGCKDS(LABEL()) **X'01'** YES **X'00'** NO
81	51	SMF1154_49_1_AKU_CTOK	1	Binary	AUDITKEYUSGCKDS(TOKEN()) **X'01'** YES **X'00'** NO
82	52	SMF1154_49_1_AKU_PLBL	1	Binary	AUDITKEYUSGPKDS(LABEL()) **X'01'** YES **X'00'** NO
83	53	SMF1154_49_1_AKU_PTOK	1	Binary	AUDITKEYUSGPKDS(TOKEN()) **X'01'** YES **X'00'** NO
84	54	SMF1154_49_1_AKU_P11TOKO	1	Binary	AUDITPKCS11USG(TOKENOBJ()) **X'01'** YES **X'00'** NO

Table 37. Record type 1154 Subtype 49 Data section 1 (continued)

Offsets		Name	Length	Format	Description
85	55	SMF1154_49_1_AKU_P11SESSO	1	Binary	AUDITPKCS11USG(SESSIONOBJ()) **X'01'** YES **X'00'** NO
86	56	SMF1154_49_1_RSV4	32		Reserved.
118	76	SMF1154_49_1_CC_SERVICES	1	Binary	Existence of installation defined services in the ICSF installation options dataset. **X'01'** At least one SERVICE() entry specified in the ICSF installation options dataset. **X'00'** No SERVICE() entries are defined in the ICSF installation options dataset.
119	77	SMF1154_49_1_CC_EXITS	1	Binary	Existence of installation exits in the ICSF installation options dataset. **X'01'** At least one EXIT() entry specified in the ICSF installation options dataset. **X'00'** No EXIT() entries in the ICSF installation options dataset.
120	78	SMF1154_49_1_RSV5	4		Reserved.
124	7C	SMF1154_49_1_KDSFORMAT	3	Binary	ICSF key data set (KDS) format: Byte: **1** CKDS format. **2** PKDS format. **3** TKDS format. Byte meaning when set: **X'00'** Not defined. **X'01'** Empty KDS. **X'02'** Non-KDSR format. **X'03'** KDSR format. **X'04'** KDSRL format. **Note:** This value is applicable only on z/OS V2R5 (ICSF FMID HCR77D2).
127	7F	SMF1154_49_1_CLASS	292 * 4		ICSF class information. Four contiguous instances are each mapped by the SMF1154_49_CLASS definition in Table 38 on page 96. • The first instance is the CSFSERV class profile access information. • The second instance is the CSFKEYS class profile access information. • The third instance is the CRYPTOZ class profile access information. • The fourth instance is the XCSFKEY class profile access information.

Table 37. Record type 1154 Subtype 49 Data section 1 (continued)					
Offsets		**Name**	**Length**	**Format**	**Description**
1295	50F	SMF1154_49_1_DFLTLBL	292 * 2		Default label checking for CKDS and PKDS. Two contiguous instances each mapped by the SMF1154_49_DL_CLASS definition in Table 39 on page 97. • The first instance is the CKDS default label access controls. • The second instance is the PKDS default label access controls.
1879	757	SMF1154_49_1_KDS	327 * 3		CKDS, PKDS, and TKDS protection settings. Three contiguous instances each mapped by the SMF1154_49_KDS KDS access controls in Table 40 on page 98. • The first instance is the CKDS access controls. • The second instance is the PKDS access controls. • The third instance is the TKDS access controls.

Table 38. SMF1154_49_CLASS profile access					
Offsets		**Name**	**Length**	**Format**	**Description**
0	0	SMF1154_49_CLS_NAME	8	EBCDIC	Class Name. CSFSERV, CSFKEYS, CRYPTOZ, and XCSFKEY.
8	8	SMF1154_49_CLS_ACTIVE	1	Binary	Class ACTIVE: **X'01'** YES **X'00'** NO
9	9	SMF1154_49_CLS_RACLISTED	1	Binary	Class RACLISTed: **X'01'** YES **X'00'** NO
10	A	SMF1154_49_CLS_PROFLEN	1	Binary	Length of profile name.
11	B	SMF1154_49_CLS_PROF	246	Char	Profile name. '*' or '**'
257	101	SMF1154_49_CLS_PROFUACC	1	Binary	Profile UACC setting. **Bit** **Meaning When Set** **0** ALTER access. **1** CONTROL access. **2** UPDATE access. **3** READ access. **4** EXECUTE access. **5-6** Reserved for IBM's use. **7** NONE access.
258	102	SMF1154_49_CLS_PROFWARN	1	Binary	Profile WARN setting. Identifies the data set as having the WARNING attribute on (bit 0 or bit 7 is on) or not having the WARNING attribute on.

Table 38. SMF1154_49_CLASS profile access (continued)

Offsets		Name	Length	Format	Description
259	103	SMF1154_49_CLS_PROFIDSPLAT	1	Binary	ID(*) setting: **X'01'** ID(*) Access. **X'00'** ID(*) Not defined.
260	104	SMF1154_49_CLS_RSV	32		Reserved.

Table 39. SMF1154_49_DL_CLASS KDS default label access controls

Offsets		Name	Length	Format	Description
0	0	SMF1154_49_DL_CLS_NAME	8	EBCDIC	Class name. CSFKEYS.
8	8	SMF1154_49_DL_CLS_ACTIVE	1	Binary	Class ACTIVE: **X'01'** YES **X'00'** NO
9	9	SMF1154_49_DL_CLS_RACLISTED	1	Binary	Class RACLISTed: **X'01'** YES **X'00'** NO
10	A	SMF1154_49_DL_CLS_PROFLEN	1	Binary	Length of profile name.
11	B	SMF1154_49_DL_CLS_PROF	246	EBCDIC	Profile name. CSF-CKDS-DEFAULT and CSF-PKDS-DEFAULT.
257	101	SMF1154_49_DL_CLS_PROFUACC	1	Binary	Profile UACC setting. **Bit** **Meaning When Set** **0** ALTER access. **1** CONTROL access. **2** UPDATE access. **3** READ access. **4** EXECUTE access. **5-6** Reserved for IBM's use. **7** NONE access.
258	102	SMF1154_49_DL_CLS_PROFWARN	1	Binary	Profile WARN setting. Identifies the data set as having the WARNING attribute on (bit 0 or bit 7 is on) or not having the WARNING attribute on.
259	103	SMF1154_49_DL_CLS_PROFIDSPLAT	1	Binary	ID(*) setting: **X'01'** ID(*) Access. **X'00'** ID(*) Not defined.

Table 39. SMF1154_49_DL_CLASS KDS default label access controls (continued)					
Offsets		**Name**	**Length**	**Format**	**Description**
260	104	SMF1154_49_DL_CLS_RSV	32		Reserved.

Table 40. SMF1154_49_KDS KDS access controls					
Offsets		**Name**	**Length**	**Format**	**Description**
0	0	SMF1154_49_KDS_TYPE	1	Binary	The KDS type: **X'00'** Not defined. **X'01'** CKDS. **X'02'** PKDS. **X'03'** TKDS.
1	1	SMF1154_49_KDS_NAME	44	EBCDIC	KDS name.
45	2D	SMF1154_49_KDS_PROFLEN	1	Binary	Length of the profile protecting the KDS. If X'00', no profile has been defined to protect the KDS.
46	2E	SMF1154_49_KDS_PROF	246	EBCDIC	The name of the profile protecting the KDS.
292	124	SMF1154_49_KDS_PROFUACC	1	Binary	Profile UACC setting. **Bit** **Meaning When Set** **0** ALTER access. **1** CONTROL access. **2** UPDATE access. **3** READ access. **4** EXECUTE access. **5-6** Reserved for IBM's use. **7** NONE access.
293	125	SMF1154_49_KDS_PROFWARN	1	Binary	Profile WARN setting. Identifies the data set as having the WARNING attribute on (bit 0 or bit 7 is on) or not having the WARNING attribute on.
294	126	SMF1154_49_KDS_PROFIDSPLAT	1	Binary	ID(*) settings.
295	127	SMF1154_49_KDS_RSV	32		Reserved.

Record type 1154 (X'482') Subtype 49 Data section 2

Data section 2 reports the algorithm names and their counts used in ICSF services since the last ENF86 signal was received. You must have Cryptographic algorithm (ALG) usage statistics enabled for data section 2 to be included in the SMF type 1154 Subtype 49 record.

Table 41. Record type 1154 Subtype 49 Data section 2					
Offsets		**Name**	**Length**	**Format**	**Description**
0	0	Smf1154_49_2_Version	2	Binary	Version of this section: 1.
2	2	Smf1154_49_2_Rsv1	2		Reserved.

Table 41. Record type 1154 Subtype 49 Data section 2 (continued)					
Offsets		**Name**	**Length**	**Format**	**Description**
4	4	Smf1154_49_2_AlgsCount	4	Binary	Number of entries in Smf1154_49_2_Alg.
8	8	Smf1154_49_2_Alg	16 * Smf1154_49_2_AlgsCount		Algorithm count information since the ENF86 signal was received. Each instance is mapped by Table 42 on page 99.

Table 42. Smf1154_49_2_Alg algorithm count information					
Offsets		**Name**	**Length**	**Format**	**Description**
0	0	Smf1154_49_2_Alg_Func	8	EBCDIC	Algorithm name. See Table 46 on page 101.
8	8	Smf1154_49_2_Alg_Count	8	Binary	Number of times the algorithm was used during the ENF86 interval.

Cryptographic usage statistics

ICSF supports a cryptographic usage statistics section containing a header and a variable number of triplets.

Note: A single SMF record cannot exceed 32K bytes.

Table 43. Subtype 31 Cryptographic usage statistics				
Offsets (Dec)	**Name**	**Length**	**Format**	**Description**
0	SMF82STAT_VER	1	binary	Version number.
1	SMF82STAT_DOMAIN	1	binary	ICSF domain index.
2	SMF82STAT_LEN	2	binary	Length of this header.
4	SMF82STAT_TRIPL_OFF	2	binary	Offset from SMF82STAT into triplet section.
6	SMF82STAT_TRIPL_LEN	2	binary	Length of triplet section.
8	SMF82STAT_D_INTVAL_STARTE	16	binary	Start time (TOD clock) of the SMF interval in STCKE format.
24	SMF82STAT_D_INTVAL_ENDE	16	binary	End time (TOD clock) of the SMF interval in STCKE format.
40	SMF82STAT_D_USERID_AS	8	EBCDIC	The HOME address space user ID.
48	SMF82STAT_D_USERID_TK	8	EBCDIC	The task level user ID (if present).
56	SMF82STAT_D_JOBID	8	EBCDIC	The job ID for the HOME address space.
64	SMF82STAT_D_JOBNAME	8	EBCDIC	The job name for the HOME address space.

Table 43. Subtype 31 Cryptographic usage statistics (continued)				
Offsets (Dec)	**Name**	**Length**	**Format**	**Description**
72	SMF82STAT_D_JOBNAME2	8	EBCDIC	The job name of the SECONDARY address space (ICSF caller).
80	SMF82STAT_D_PLEXNAME	8	EBCDIC	The sysplex member name.

Each Tag-Length-Value (TLV) triplet is a structure called SMF82_TRIPL. The values for the tags, the format, and the maximum length of the data are defined in Table 44 on page 100.

Table 44. Subtype 31 SMF82_TRIPL				
Offsets (Dec)	**Name**	**Length**	**Format**	**Description**
0	SMF82_TRIPL_TAG	2	binary	Tag of the data.
2	SMF82_TRIPL_LENGTH	2	binary	Length of the tag, length, and data fields.
4	SMF82_TRIPL_DATA	*	varies	Value of the data.

The tag values and their corresponding information are described in Table 45 on page 100.

Table 45. Subtype 31 tag values				
Tag ID (2 bytes)	**Tag name**	**Length (2 bytes)**	**Format**	**Description**
Cryptographic engine (ENG) usage statistics				
X'0201'	SMF82STAT_ENG_CARD	20	structure	Crypto card usage count. • 4-byte EBCDIC identifier (for example, 5C01). • 8-byte EBCDIC serial number. • 4-byte binary card usage count.
X'0203'	SMF82STAT_ENG_CPACF	8	binary	CPACF usage count.
X'0204'	SMF82STAT_ENG_SOFTW	8	binary	Crypto software usage count.
Cryptographic service (SRV) usage statistics				
X'0205'	SMF82STAT_SRV	16	structure	ICSF callable service usage count. • 8-byte EBCDIC service name. • 4-byte binary service usage count. See “Resource names for CCA and ICSF entry points” on page 103 for service names.
X'0206'	SMF82STAT_SRVUDX	16	structure	UDX service usage count. • 8-byte EBCDIC UDX service name. • 4-byte binary UDX service usage count.

Table 45. Subtype 31 tag values (continued)				
Tag ID (2 bytes)	**Tag name**	**Length (2 bytes)**	**Format**	**Description**
Cryptographic algorithm (ALG) usage statistics				
X'0207'	SMF82STAT_ALG	16	structure	Crypto algorithm usage count. • 8-byte EBCDIC algorithm name. • 4-byte binary algorithm usage count. See Table 46 on page 101 for algorithm names.

Table 46. SMF82STAT_ALG algorithm names	
Algorithm name	**Description**
AES128	128-bit AES algorithm.
AES192	192-bit AES algorithm.
AES256	256-bit AES algorithm.
Blowfish	Blowfish algorithm (PKCS #11 only).
ChaCha20	ChaCha20 algorithm (PKCS #11 only).
DES112	112-bit DES algorithm.
DES168	168-bit DES algorithm.
DES56	56-bit DES algorithm.
DH	DH algorithm (PKCS #11 only).
DSA	DSA algorithm (PKCS #11 only).
ECCBP160	160-bit ECC algorithm.
ECCBP192	192-bit ECC algorithm.
ECCBP224	224-bit ECC algorithm.
ECCBP256	256-bit ECC algorithm.
ECCBP320	320-bit ECC algorithm.
ECCBP384	384-bit ECC algorithm.
ECCBP512	512-bit ECC algorithm.
ECCKB256	256-bit ECC algorithm.
ECCP192	192-bit ECC algorithm.
ECCP224	224-bit ECC algorithm.
ECCP256	256-bit ECC algorithm.
ECCP384	384-bit ECC algorithm.
ECCP521	521-bit ECC algorithm.
ED25519	ECC curve25519 signature algorithm.
ED448	ECC curve448 signature algorithm.
GenSec	Generic Secret algorithm (PKCS #11 only).

Table 46. SMF82STAT_ALG algorithm names (continued)	
Algorithm name	**Description**
HMAC	HMAC algorithm (CCA only).
KY1024R2	CRYSTALS-Kyber 1024 Round 2 Algorithm.
LI2	CRYSTALS-Dilithium (6,5) Round 2 algorithm.
LI2-65R3	CRYSTALS-Dilithium (6,5) Round 3 algorithm.
LI2-87R2	CRYSTALS-Dilithium (8,7) Round 2 algorithm.
LI2-87R3	CRYSTALS-Dilithium (8,7) Round 3 algorithm.
MD2	MD2 hashing algorithm (PKCS #11 only).
MD5	MD5 hashing algorithm.
PRNG	Pseudo-random number generator
PRNGFIPS	Pseudo-random number generator consistent with NIST SP800-90A PRNGFIPS (PKCS #11 Only).
RC4	RC4 algorithm (PKCS #11 only).
RPMD160	RPMD-160 hashing algorithm.
RSA1024	RSA algorithm with a key bit length from 1024 to 2047 bits.
RSA2048	RSA algorithm with a key bit length from 2048 to 4095 bits.
RSA4096	RSA algorithm with a key bit length of 4096 bits or greater.
RSA512	RSA algorithm with a key bit length from 512 to 1023 bits.
SHA1	SHA-1 hashing algorithm.
SHA224	SHA-224 hashing algorithm.
SHA256	SHA-256 hashing algorithm.
SHA3-224	SHA3-224 hashing algorithm
SHA3-256	SHA3-256 hashing algorithm
SHA3-384	SHA3-384 hashing algorithm
SHA3-512	SHA3-512 hashing algorithm
SHA384	SHA-384 hashing algorithm.
SHA512	SHA-512 hashing algorithm.
SHAKE128	SHAKE128 hashing algorithm
SHAKE256	SHAKE256 hashing algorithm
TLS-PRF	TLS Pseudo-Random Function derivation protocol (PKCS #11 Only).
X25519	ECC curve25519 key exchange algorithm.
X448	ECC curve448 key exchange algorithm.

See “Resource names for CCA and ICSF entry points” on page 103 for a list of possible values for the SMF82STAT_SRV tag.

Resource names for CCA and ICSF entry points

Table 47. Resource names for CCA and ICSF entry points

Descriptive service name	CCA entry point names		ICSF entry point names		SAF resource name	Callable service exit name
	31-bit	64-bit	31-bit	64-bit		
Authentication Parameter Generate	CSNBAPG	CSNEAPG	CSFAPG	CSFAPG6	CSFAPG	CSFAPG
Cipher Text Translate2	CSNBCTT2	CSNECTT2	CSFCTT2	CSFCTT26	CSFCTT2	CSFCTT2
Cipher Text Translate2	CSNBCTT3	CSNECTT3	CSFCTT3	CSFCTT36	CSFCTT3	CSFCTT3
CKDS Key Record Create	CSNBKRC	CSNEKRC	CSFKRC	CSFKRC6	CSFKRC	CSFKRC
CKDS Key Record Create2	CSNBKRC2	CSNEKRC2	CSFKRC2	CSFKRC26	CSFKRC2	CSFKRC2
CKDS Key Record Delete	CSNBKRD	CSNEKRD	CSFKRD	CSFKRD6	CSFKRD	CSFKRD
CKDS Key Record Read	CSNBKRR	CSNEKRR	CSFKRR	CSFKRR6	CSFKRR	CSFKRR
CKDS Key Record Read2	CSNBKRR2	CSNEKRR2	CSFKRR2	CSFKRR26	CSFKRR2	CSFKRR2
CKDS Key Record Write	CSNBKRW	CSNEKRW	CSFKRW	CSFKRW6	CSFKRW	CSFKRW
CKDS Key Record Write2	CSNBKRW2	CSNEKRW2	CSFKRW2	CSFKRW26	CSFKRW2	CSFKRW2
Clear Key Import	CSNBCKI	CSNECKI	CSFCKI	CSFCKI6	CSFCKI	CSFCKI
Clear PIN Encrypt	CSNBCPE	CSNECPE	CSFCPE	CSFCPE6	CSFCPE	CSFCPE
Clear PIN Generate	CSNBPGN	CSNEPGN	CSFPGN	CSFPGN6	CSFPGN	CSFPGN
Clear PIN Generate Alternate	CSNBCPA	CSNECPA	CSFCPA	CSFCPA6	CSFCPA	CSFCPA
Control Vector Generate	CSNBCVG	CSNECVG	CSFCVG	CSFCVG6	N/A	N/A
Control Vector Translate	CSNBCVT	CSNECVT	CSFCVT	CSFCVT6	CSFCVT	CSFCVT
Coordinated KDS Administration	N/A	N/A	CSFCRC	CSFCRC6	CSFCRC	N/A
Cryptographic Usage Statistic	N/A	N/A	CSFSTAT	CSFSTAT6	N/A	N/A
Cryptographic Variable Encipher	CSNBCVE	CSNECVE	CSFCVE	CSFCVE6	CSFCVE	CSFCVE
CVV Key Combine	CSNBCKC	CSNECKC	CSFCKC	CSFCKC6	CSFCKC	CSFCKC
Data Key Export	CSNBDKX	CSNEDKX	CSFDKX	CSFDKX6	CSFDKX	CSFDKX
Data Key Import	CSNBDKM	CSNEDKM	CSFDKM	CSFDKM6	CSFDKM	CSFDKM

Table 47. Resource names for CCA and ICSF entry points (continued)

Descriptive service name	CCA entry point names		ICSF entry point names		SAF resource name	Callable service exit name
Decipher	CSNBDEC	CSNEDEC	CSFDEC	CSFDEC6	CSFDEC	CSFDEC
Decipher	CSNBDEC1	CSNEDEC1	CSFDEC1	CSFDEC16	CSFDEC1	CSFDEC1
Decode	CSNBDCO	CSNEDCO	CSFDCO	CSFDCO6	CSFDCO	CSFDCO
Derive ICC MK	CSNBDCM	CSNEDCM	CSFDCM	CSFDCM6	CSFDCM	CSFDCM
Derive Session Key	CSNBDSK	CSNEDSK	CSFDSK	CSFDSK6	CSFDSK	CSFDSK
Digital Signature Generate	CSNDDSG	CSNFDSG	CSFDSG	CSFDSG6	CSFDSG	CSFDSG
Digital Signature Verify	CSNDDSV	CSNFDSV	CSFDSV	CSFDSV6	CSFDSV	CSFDSV
Diversified Key Generate	CSNBDKG	CSNEDKG	CSFDKG	CSFDKG6	CSFDKG	CSFDKG
Diversified Key Generate2	CSNBDKG2	CSNEDKG2	CSFDKG2	CSFDKG26	CSFDKG2	CSFDKG2
Diversify Directed Key	CSNBDDK	CSNEDDK	CSFDDK	CSFDDK6	CSFDDK	CSFDDK
DK Deterministic PIN Generate	CSNBDDPG	CSNEDDPG	CSFDDPG	CSFDDPG6	CSFDDPG	CSFDDPG
DK Migrate PIN	CSNBDMP	CSNEDMP	CSFDMP	CSFDMP6	CSFDMP	CSFDMP
DK PAN Modify in Transaction	CSNBDPMT	CSNEDPMT	CSFDPMT	CSFDPMT6	CSFDPMT	CSFDPMT
DK PAN Translate	CSNBDPT	CSNEDPT	CSFDPT	CSFDPT6	CSFDPT	CSFDPT
DK PIN Change	CSNBDPC	CSNEDPC	CSFDPC	CSFDPC6	CSFDPC	CSFDPC
DK PIN Verify	CSNBDPV	CSNEDPV	CSFDPV	CSFDPV6	CSFDPV	CSFDPV
DK PRW Card Number Update	CSNBDPNU	CSNEDPNU	CSFDPNU	CSFDPNU6	CSFDPNU	CSFDPNU
DK PRW Card Number Update2	CSNBDCU2	CSNBECU2	CSFDCU2	CSFDCU26	CSFDCU2	CSFDCU2
DK PRW CMAC Generate	CSNBDPCG	CSNEDPCG	CSFDPCG	CSFDPCG6	CSFDPCG	CSFDPCG
DK Random PIN Generate	CSNBDRPG	CSNEDRPG	CSFDRPG	CSFDRPG6	CSFDRPG	CSFDRPG
DK Random PIN Generate2	CSNBDRG2	CSNBERG2	CSFDRG2	CSFDRG26	CSFDRG2	CSFDRG2
DK Regenerate PRW	CSNBDRP	CSNEDRP	CSFDRP	CSFDRP6	CSFDRP	CSFDRP
ECC Diffie-Hellman	CSNDEDH	CSNFEDH	CSFEDH	CSFEDH6	CSFEDH	CSFEDH
EMV Scripting Service	CSNBESC	CSNEESC	CSFESC	CSFESC6	CSFESC	CSFESC
EMV Transaction (ARQC/ARPC) Service	CSNBEAC	CSNEEAC	CSFEAC	CSFEAC6	CSFEAC	CSFEAC

Table 47. Resource names for CCA and ICSF entry points (continued)

Descriptive service name	CCA entry point names		ICSF entry point names		SAF resource name	Callable service exit name
EMV Verification Functions	CSNBEVF	CSNEEVF	CSFEVF	CSFEVF6	CSFEVF	CSFEVF
Encipher	CSNBENC	CSNEENC	CSFENC	CSFENC6	CSFENC	CSFENC
Encipher	CSNBENC1	CSNEENC1	CSFENC1	CSFENC16	CSFENC1	CSFENC1
Encode	CSNBECO	CSNEECO	CSFECO	CSFECO6	CSFECO	CSFECO
Encrypted PIN Generate	CSNBEPG	CSNEEPG	CSFEPG	CSFEPG6	CSFEPG	CSFEPG
Encrypted PIN Translate	CSNBPTR	CSNEPTR	CSFPTR	CSFPTR6	CSFPTR	CSFPTR
Encrypted PIN Translate2	CSNBPTR2	CSNEPTR2	CSFPTR2	CSFPTR26	CSFPTR2	CSFPTR2
Encrypted PIN Translate Enhanced	CSNBPTRE	CSNEPTRE	CSFPTRE	CSFPTRE6	CSFPTRE	CSFPTRE
Encrypted PIN Verify	CSNBPVR	CSNEPVR	CSFPVR	CSFPVR6	CSFPVR	CSFPVR
Encrypted PIN Verify2	CSNBPVR2	CSNEPVR2	CSFPVR2	CSFPVR26	CSFPVR2	CSNBPVR2
Field Level Decipher	CSNBFLD	CSNEFLD	CSFFLD	CSFFLD6	N/A	N/A
Field Level Encipher	CSNBFLE	CSNEFLE	CSFFLE	CSFFLE6	N/A	N/A
Format Preserving Algorithms Decipher	CSNBFFXD	CSNEFFXD	CSFFFXD	CSFFFXD6	CSFFFXD	CSFFFXD
Format Preserving Algorithms Encipher	CSNBFFXE	CSNEFFXE	CSFFFXE	CSFFFXE6	CSFFFXE	CSFFFXE
Format Preserving Algorithms Translate	CSNBFFXT	CSNEFFXT	CSFFFXT	CSFFFXT6	CSFFFXT	CSFFFXT
FPE Decipher	CSNBFPED	CSNEFPED	CSFFPED	CSFFPED6	CSFFPED	CSFFPED
FPE Encipher	CSNBFPEE	CSNEFPEE	CSFFPEE	CSFFPEE6	CSFFPEE	CSFFPEE
FPE Translate	CSNBFPET	CSNEFPET	CSFFPET	CSFFPET6	CSFFPET	CSFFPET
Generate Issuer MK	CSNBGIM	CSNEGIM	CSFGIM	CSFGIM6	CSFGIM	CSFGIM
HMAC Generate	CSNBHMG	CSNEHMG	CSFHMG	CSFHMG6	CSFHMG	CSFHMG
HMAC Generate	CSNBHMG1	CSNEHMG1	CSFHMG1	CSFHMG16	CSFHMG1	CSFHMG1
HMAC Verify	CSNBHMV	CSNEHMV	CSFHMV	CSFHMV6	CSFHMV	CSFHMV
HMAC Verify	CSNBHMV1	CSNEHMV1	CSFHMV1	CSFHMV16	CSFHMV1	CSFHMV1
ICSF Multi-Purpose Service	N/A	N/A	CSFMPS	CSFMPS6	CSFMPS	CSFMPS
ICSF Query Algorithm	N/A	N/A	CSFIQA	CSFIQA6	CSFIQA	N/A
ICSF Query Facility	N/A	N/A	CSFIQF	CSFIQF6	CSFIQF	N/A
ICSF Query Facility2	N/A	N/A	CSFIQF2	CSFIQF26	N/A	CSFIQF2

Table 47. Resource names for CCA and ICSF entry points (continued)

Descriptive service name	CCA entry point names		ICSF entry point names		SAF resource name	Callable service exit name
Key Data Set List	N/A	N/A	CSFKDSL	CSFKDSL6	CSFKDSL	CSFKDSL
Key Data Set Metadata Read	N/A	N/A	CSFKDMR	CSFKDMR6	CSFKDMR	CSFKDMR
Key Data Set Metadata Write	N/A	N/A	CSFKDMW	CSFKDMW6	CSFKDMW	CSFKDMW
Key Data Set Record Retrieve	N/A	N/A	CSFRRT	CSFRRT6	CSFRRT (see notes)	N/A
Key Data Set Update	N/A	N/A	CSFKDU	CSFKDU6	CSFKDU (see notes)	N/A
Key Encryption Translate	CSNBKET	CSNEKET	CSFKET	CSFKET6	CSFKET	CSFKET
Key Export	CSNBKEX	CSNEKEX	CSFKEX	CSFKEX6	CSFKEX	CSFKEX
Key Generate	CSNBKGN	CSNEKGN	CSFKGN	CSFKGN6	CSFKGN	CSFKGN
Key Generate2	CSNBKGN2	CSNEKGN2	CSFKGN2	CSFKGN26	CSFKGN2	CSFKGN2
Key Import	CSNBKIM	CSNEKIM	CSFKIM	CSFKIM6	CSFKIM	CSFKIM
Key Part Import	CSNBKPI	CSNEKPI	CSFKPI	CSFKPI6	CSFKPI	CSFKPI
Key Part Import2	CSNBKPI2	CSNEKPI2	CSFKPI2	CSFKPI26	CSFKPI2	CSFKPI2
Key Test	CSNBKYT	CSNEKYT	CSFKYT	CSFKYT6	CSFKYT	CSFKYT
Key Test2	CSNBKYT2	CSNEKYT2	CSFKYT2	CSFKYT26	CSFKYT2	CSFKYT2
Key Test Extended	CSNBKYTX	CSNEKYTX	CSFKYTX	CSFKYTX6	CSFKYTX	CSFKYTX
Key Token Build	CSNBKTB	CSNEKTB	CSFKTB	CSFKTB6	N/A	N/A
Key Token Build2	CSNBKTB2	CSNEKTB2	CSFKTB2	CSFKTB26	N/A	N/A
Key Token Wrap	N/A	N/A	CSFWRP	CSFWRP6	CSFWRP	N/A
Key Translate	CSNBKTR	CSNEKTR	CSFKTR	CSFKTR6	CSFKTR	CSFKTR
Key Translate2	CSNBKTR2	CSNEKTR2	CSFKTR2	CSFKTR26	CSFKTR2	CSFKTR2
MAC Generate	CSNBMGN	CSNEMGN	CSFMGN	CSFMGN6	CSFMGN	CSFMGN
MAC Generate	CSNBMGN1	CSNEMGN1	CSFMGN1	CSFMGN16	CSFMGN1	CSFMGN1
MAC Generate2	CSNBMGN2	CSNEMGN2	CSFMGN2	CSFMGN26	CSFMGN2	CSFMGN2
MAC Generate2	CSNBMGN3	CSNEMGN3	CSFMGN3	CSFMGN36	CSFMGN3	CSFMGN3
MAC Verify	CSNBMVR	CSNEMVR	CSFMVR	CSFMVR6	CSFMVR	CSFMVR
MAC Verify	CSNBMVR1	CSNEMVR1	CSFMVR1	CSFMVR16	CSFMVR1	CSFMVR1
MAC Verify2	CSNBMVR2	CSNEMVR2	CSFMVR2	CSFMVR26	CSFMVR2	CSFMVR2
MAC Verify2	CSNBMVR3	CSNEMVR3	CSFMVR3	CSFMVR36	CSFMVR3	CSFMVR3
MDC Generate	CSNBMDG	CSNEMDG	CSFMDG	CSFMDG6	CSFMDG	CSFMDG
MDC Generate	CSNBMDG1	CSNEMDG1	CSFMDG1	CSFMDG16	CSFMDG1	CSFMDG1

Table 47. Resource names for CCA and ICSF entry points (continued)

Descriptive service name	CCA entry point names		ICSF entry point names		SAF resource name	Callable service exit name
Multiple Clear Key Import	CSNBCKM	CSNECKM	CSFCKM	CSFCKM6	CSFCKM	CSFCKM
Multiple Secure Key Import	CSNBSKM	CSNESKM	CSFSKM	CSFSKM6	CSFSKM	CSFSKM
One-Way Hash Generate	CSNBOWH	CSNEOWH	CSFOWH	CSFOWH6	CSFOWH	CSFOWH
One-Way Hash Generate	CSNBOWH1	CSNEOWH1	CSFOWH1	CSFOWH16	CSFOWH1	CSFOWH1
PCI Interface	N/A	N/A	CSFPCI	CSFPCI6	CSFPCI	CSFPCI
PIN Change/Unblock	CSNBPCU	CSNEPCU	CSFPCU	CSFPCU6	CSFPCU	CSFPCU
PKA Decrypt	CSNDPKD	CSNFPKD	CSFPKD	CSFPKD6	CSFPKD	CSFPKD
PKA Encrypt	CSNDPKE	CSNFPKE	CSFPKE	CSFPKE6	CSFPKE	CSFPKE
PKA Key Generate	CSNDPKG	CSNFPKG	CSFPKG	CSFPKG6	CSFPKG	CSFPKG
PKA Key Import	CSNDPKI	CSNFPKI	CSFPKI	CSFPKI6	CSFPKI	CSFPKI
PKA Key Token Build	CSNDPKB	CSNFPKB	CSFPKB	CSFPKB6	N/A	N/A
PKA Key Token Change	CSNDKTC	CSNFKTC	CSFPKTC	CSFPKTC6	CSFPKTC	CSFPKTC
PKA Key Translate	CSNDPKT	CSNFPKT	CSFPKT	CSFPKT6	CSFPKT	CSFPKT
PKA Public Key Extract	CSNDPKX	CSNFPKX	CSFPKX	CSFPKX6	CSFPKX	CSFPKX
PKCS #11 Derive Key	N/A	N/A	CSFPDVK	CSFPDVK6	CSF1DVK[1]	N/A
PKCS #11 Derive Multiple Keys	N/A	N/A	CSFPDMK	CSFPDMK6	CSF1DMK[1]	N/A
PKCS #11 Generate Keyed MAC	N/A	N/A	CSFPHMG	CSFPHMG6	CSF1HMG[1]	N/A
PKCS #11 Generate Key Pair	N/A	N/A	CSFPGKP	CSFPGKP6	CSF1GKP[1]	N/A
PKCS #11 Generate Secret Key	N/A	N/A	CSFPGSK	CSFPGSK6	CSF1GSK[1]	N/A
PKCS #11 Get Attribute Value	N/A	N/A	CSFPGAV	CSFPGAV6	CSF1GAV[1]	N/A
PKCS #11 One-Way Hash, Sign, or Verify	N/A	N/A	CSFPOWH	CSFPOWH6	CSFOWH	N/A
PKCS #11 Private Key Sign	N/A	N/A	CSFPPKS	CSFPPKS6	CSF1PKS[1]	N/A
PKCS #11 Private Key Structure Decrypt	N/A	N/A	CSFPPD2	CSFPPD26	CSFPKD	N/A

Table 47. Resource names for CCA and ICSF entry points (continued)

Descriptive service name	CCA entry point names		ICSF entry point names		SAF resource name	Callable service exit name
PKCS #11 Private Key Structure Sign	N/A	N/A	CSFPPS2	CSFPPS26	CSFDSG	N/A
PKCS #11 Pseudo-Random Function	N/A	N/A	CSFPPRF	CSFPPRF6	CSFRNG	N/A
PKCS #11 Public Key Structure Encrypt	N/A	N/A	CSFPPE2	CSFPPE26	CSFPKE	N/A
PKCS #11 Public Key Structure Verify	N/A	N/A	CSFPPV2	CSFPPV26	CSFDSV	N/A
PKCS #11 Public Key Verify	N/A	N/A	CSFPPKV	CSFPPKV6	CSF1PKV[1]	N/A
PKCS #11 Secret Key Decrypt	N/A	N/A	CSFPSKD	CSFPSKD6	CSF1SKD[1]	N/A
PKCS #11 Secret Key Encrypt	N/A	N/A	CSFPSKE	CSFPSKE6	CSF1SKE[1]	N/A
PKCS #11 Secret Key Reencrypt	N/A	N/A	CSFPSKR	CSFPSKR6	CSF1SKR[1]	N/A
PKCS #11 Set Attribute Value	N/A	N/A	CSFPSAV	CSFPSAV6	CSF1SAV[1]	N/A
PKCS #11 Token Record Create	N/A	N/A	CSFPTRC	CSFPTRC6	CSF1TRC[1]	N/A
PKCS #11 Token Record Delete	N/A	N/A	CSFPTRD	CSFPTRD6	CSF1TRD[1]	N/A
PKCS #11 Token Record List	N/A	N/A	CSFPTRL	CSFPTRL6	CSF1TRL[1]	N/A
PKCS #11 Unwrap Key	N/A	N/A	CSFPUWK	CSFPUWK6	CSF1UWK[1]	N/A
PKCS #11 Verify Keyed MAC	N/A	N/A	CSFPHMV	CSFPHMV6	CSF1HMV[1]	N/A
PKCS #11 Wrap Key	N/A	N/A	CSFPWPK	CSFPWPK6	CSF1WPK[1]	N/A
PKDS Key Record Create	CSNDKRC	CSNFKRC	CSFPKRC	CSFPKRC6	CSFPKRC	CSFPKRC
PKDS Key Record Delete	CSNDKRD	CSNFKRD	CSFPKRD	CSFPKRD6	CSFPKRD	CSFPKRD
PKDS Key Record Read	CSNDKRR	CSNFKRR	CSFPKRR	CSFPKRR6	CSFPKRR	CSFPKRR
PKDS Key Record Read2	CSNDKRR2	CSNFKRR2	CSFPRR2	CSFPRR26	CSFPRR2	CSFPRR2
PKDS Key Record Write	CSNDKRW	CSNFKRW	CSFPKRW	CSFPKRW6	CSFPKRW	CSFPKRW
Prohibit Export	CSNBPEX	CSNEPEX	CSFPEX	CSFPEX6	CSFPEX	CSFPEX

Table 47. Resource names for CCA and ICSF entry points (continued)

Descriptive service name	CCA entry point names		ICSF entry point names		SAF resource name	Callable service exit name
Prohibit Export Extended	CSNBPEXX	CSNEPEXX	CSFPEXX	CSFPEXX6	CSFPEXX	CSFPEXX
Public Infrastructure Certificate	CSNDPIC	CSNFPIC	CSFPIC	CSFPIC6	CSFPIC	CSFPIC
Random Number Generate	CSNBRNG	CSNERNG	CSFRNG	CSFRNG6	CSFRNG	CSFRNG
Random Number Generate	CSNBRNGL	CSNERNGL	CSFRNGL	CSFRNGL6	CSFRNGL	CSFRNGL
Recover PIN from Offset	CSNBPFO	CSNEPFO	CSFPFO	CSFPFO6	CSFPFO	CSFPFO
Remote Key Export	CSNDRKX	CSNFRKX	CSFRKX	CSFRKX6	CSFRKX	CSFRKX
Restrict Key Attribute	CSNBRKA	CSNERKA	CSFRKA	CSFRKA6	CSFRKA	CSFRKA
Retained Key Delete	CSNDRKD	CSNFRKD	CSFRKD	CSFRKD6	CSFRKD	CSFRKD
Retained Key List	CSNDRKL	CSNFRKL	CSFRKL	CSFRKL6	CSFRKL	CSFRKL
SAF ACEE Selection	N/A	N/A	CSFACEE	CSFACEE6	N/A (see notes)	N/A (see notes)
Secure Key Import	CSNBSKI	CSNESKI	CSFSKI	CSFSKI6	CSFSKI	CSFSKI
Secure Key Import2	CSNBSKI2	CSNESKI2	CSFSKI2	CSFSKI26	CSFSKI2	CSFSKI2
Secure Messaging for Keys	CSNBSKY	CSNESKY	CSFSKY	CSFSKY6	CSFSKY	CSFSKY
Secure Messaging for PINs	CSNBSPN	CSNESPN	CSFSPN	CSFSPN6	CSFSPN	CSFSPN
SET Block Compose	CSNDSBC	CSNFSBC	CSFSBC	CSFSBC6	CSFSBC	CSFSBC
SET Block Decompose	CSNDSBD	CSNFSBD	CSFSBD	CSFSBD6	CSFSBD	CSFSBD
Symmetric Algorithm Decipher	CSNBSAD	CSNESAD	CSFSAD	CSFSAD6	CSFSAD	N/A
Symmetric Algorithm Decipher	CSNBSAD1	CSNESAD1	CSFSAD1	CSFSAD16	CSFSAD1	N/A
Symmetric Algorithm Encipher	CSNBSAE	CSNESAE	CSFSAE	CSFSAE6	CSFSAE	N/A
Symmetric Algorithm Encipher	CSNBSAE1	CSNESAE1	CSFSAE1	CSFSAE16	CSFSAE1	N/A
Symmetric Key Decipher	CSNBSYD	CSNESYD	CSFSYD	CSFSYD6	N/A	N/A
Symmetric Key Decipher	CSNBSYD1	CSNESYD1	CSFSYD1	CSFSYD16	N/A	N/A
Symmetric Key Encipher	CSNBSYE	CSNESYE	CSFSYE	CSFSYE6	N/A	N/A

Table 47. Resource names for CCA and ICSF entry points (continued)

Descriptive service name	CCA entry point names		ICSF entry point names		SAF resource name	Callable service exit name
Symmetric Key Encipher	CSNBSYE1	CSNESYE1	CSFSYE1	CSFSYE16	N/A	N/A
Symmetric Key Export	CSNDSYX	CSNFSYX	CSFSYX	CSFSYX6	CSFSYX	CSFSYX
Symmetric Key Export with Data	CSNDSXD	CSNFSXD	CSFSXD	CSFSXD6	CSFSXD	CSFSXD
Symmetric Key Generate	CSNDSYG	CSNFSYG	CSFSYG	CSFSYG6	CSFSYG	CSFSYG
Symmetric Key Import	CSNDSYI	CSNFSYI	CSFSYI	CSFSYI6	CSFSYI	CSFSYI
Symmetric Key Import2	CSNDSYI2	CSNFSYI2	CSFSYI2	CSFSYI26	CSFSYI2	CSFSYI2
Symmetric MAC Generate	CSNBSMG	CSNESMG	CSFSMG	CSFSMG6	N/A	CSFSMG
Symmetric MAC Generate	CSNBSMG1	CSNESMG1	CSFSMG1	CSFSMG16	N/A	CSFSMG1
Symmetric MAC Verify	CSNBSMV	CSNESMV	CSFSMV	CSFSMV6	N/A	CSFSMV
Symmetric MAC Verify	CSNBSMV1	CSNESMV1	CSFSMV1	CSFSMV16	N/A	CSFSMV1
TR-31 Export	CSNBT31X	CSNET31X	CSFT31X	CSFT31X6	CSFT31X	CSFT31X
TR-31 Import	CSNBT31I	CSNET31I	CSFT31I	CSFT31I6	CSFT31I	CSFT31I
TR-31 Optional Data Build	CSNBT31O	CSNET31O	CSFT31O	CSFT31O6	N/A	N/A
TR-31 Optional Data Read	CSNBT31R	CSNET31R	CSFT31R	CSFT31R6	N/A	N/A
TR-31 Parse	CSNBT31P	CSNET31P	CSFT31P	CSFT31P6	N/A	N/A
TR-34 Bind-Begin	CSNDT34B	CSNFT34B	CSFT34B	CSFT34B6	CSFT34B	CSFT34B
TR-34 Bind-Complete	CSNDT34C	CSNFT34C	CSFT34C	CSFT34C6	CSFT34C	CSFT34C
TR-34 Key Distribution	CSNDT34D	CSNFT34D	CSFT34D	CSFT34D6	CSFT34D	CSFT34D
TR-34 Key Receive	CSNDT34R	CSNFT34R	CSFT34R	CSFT34R6	CSFT34R	CSFT34R
Transaction Validation	CSNBTRV	CSNETRV	CSFTRV	CSFTRV6	CSFTRV	CSFTRV
Trusted Block Create	CSNDTBC	CSNFTBC	CSFTBC	CSFTBC6	CSFTBC	CSFTBC
Unique Key Derive	CSNBUKD	CSNEUKD	CSFUKD	CSFUKD6	CSFUKD	CSFUKD
VISA CVV Service Generate	CSNBCSG	CSNECSG	CSFCSG	CSFCSG6	CSFCSG	CSFCSG
VISA CVV Service Verify	CSNBCSV	CSNECSV	CSFCSV	CSFCSV6	CSFCSV	CSFCSV

Notes:

- Key Data Set Update (CSFKDU and CSFKDU6) and Key Data Set Record Retrieve (CSFRRT and CSFRRT6) will only be granted access with an explicitly defined covering profile.
- SAF ACEE Selection (CSFACEE and CSFACEE6) does not have SAF checking or callable service exit support on its own. The service specified in the *service_name* parameter determines SAF checking and callable service exit capability.
- N/A is shown in a column when the callable service:
  - Does not have CCA entry points (CCA entry point names columns).
  - Does not call SAF to determine access to a CSFSERV resource (SAF resource name column).
  - Does not allow a callable service exit to be defined (Callable service exit name column).
- [1] CSF1*xxx* is just another name for the CSFP*xxx* service.

IMS for z/OS

Information Management System (IMS) is a message-based transaction manager and hierarchical-database manager for z/OS for online transaction processing (OLTP) and online batch processing. External applications can use transactions to interact with applications that run inside IMS.

IMS is one of the predominant database and transaction processing systems across a multitude of sectors, including banking, manufacturing, finance, healthcare, aerospace, communication, government, and retail.

With the IBM Z Security and Compliance Center, automatically collect data from SMF Type 1154 Subtype 85 to check whether the password re-verification function is activated, check whether IMS uses a user Id to check security of direct and non-direct routed transactions, and more.

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

Note: Compliance data collection for IMS for z/OS requires PTFs for PH42600.

MQ for z/OS

IBM Message Queue (MQ) supports the exchange of information between applications, systems, services and files by sending and receiving message data via messaging queues. This simplifies the creation and maintenance of business applications. IBM MQ works with a broad range of computing platforms and can be deployed across a range of different environments including on-premise, in cloud, and hybrid cloud deployments. IBM MQ supports a number of different APIs including Message Queue Interface (MQI), Java Message Service (JMS), REST, .NET, IBM MQ Light and MQTT.

With the IBM Z Security and Compliance Center, you can automatically collect data from SMF Type 1154 Subtype 82 to check whether Advanced Message Security (AMS) capabilities are available to the queue manager, check whether MQ security is active, and more.

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

Processor Activity

CP Assist for Cryptographic Functions (CPACF) is a set of z/Architecture instructions provided by the Message Security Assist (MSA) facility and its extensions. It is available on all CPs, including zIIPs, IFLs, and General Purpose CPUs. CPACF performs various cryptographic functions and supports clear and protected keys. CPACF provides significantly improved performance for many cryptographic operations.

z16 is enhanced with processor activity instrumentation to count cryptographic operations. Consequently, z/OS has been enhanced to capture crypto usage data for z/OS workloads in SMF 0, 30 and 1154 records.

With z16 running z/OS 2.4 and later, automatically collect data from SMF Type 1154 Subtype 128 to, check that clear key operation KM-AES-256 is not in use, check that weak algorithm KM-DEA is not in use, check that weak algorithm KM-Encrypted-DEA is not in use, and more.

Note: Compliance data collection for Processor Activity requires z/OS 2.4 or later with PTFs for OA61511 **and z16**.

Subtype 128 — Processor activity compliance evidence

The type 1154 subtype 128 record reports CPACF cryptographic instruction usage aggregated across all address spaces in a system.

Note: SMF is unable to report the use of instructions by the Linux® environment within zCX. This means that the use of these instructions by an application running within a zCX instance will not be included in this section.

Record environment

The following conditions exist for the generation of this record:

Macro
SMFEWTM, BRANCH=YES (record exits: IEFU84 and IEFU86)

Mode
Task

Storage residency
31-bit

Record mapping

The subtype 128 record is mapped by the following mapping macros:

- IFASMFH, which maps the SMF standard and extended header area of the record.
- IFAR1154, which maps the SMF type 1154 common area that resides in the record just past the SMF extended header. This map contains triplets that are used to navigate to the subtype-specific area of the record.
- IFAS4128, which maps the subtype 128 specific area that resides in the record just past the SMF 1154 common area. See "Record type 1154 (X'482') - z/OS compliance evidence" for information on how to locate the subtype 128 specific area of the record.

The subtype 128 specific area begins with a self-defining section that describes the crypto counters section of the record. The self-defining section is mapped as follows. The offsets shown are relative to the start of the subtype 128 specific area of the record.

Offsets		Name	Length	Format	Description
0	0	SMF1154_128_TRN	4	binary	Number of subtype-specific triplets
4	4	SMF1154_128_SDS_Length	2	binary	Length of this section
8	8	SMF1154_128_CrypCtrs_Offset	4	binary	Offset from record start to the Crypto counters section
12	C	SMF1154_128_CrypCtrs_Length	2	binary	Length of the Crypto counters section
14	E	SMF1154_128_CrypCtrs_Number	2	binary	Number of Crypto counter sections

Crypto counters section

This section contains the counters for each CPACF cryptographic instruction supported by the system that was used by the system in the period since the previous type 1154 subtype 128 record was written or since IPL.

Triplet information: The crypto counters section is located in the record using the following triplet fields. These fields are located in the subtype 128 specific self-defining section, which is described in "Subtype 128 - Processor activity compliance evidence".

Offset
SMF1154_128_CrypCtrs_Offset

Length
SMF1154_128_CrypCtrs_Length

Number
SMF1154_128_CrypCtrs_Number

The crypto counter section contains an array of counters whose description follows. The first entry in the array is index 1. The IFASMFCN macro contains equates and meanings for each index into this array. The names of the equates start with SMF_CrypCtrs. When evaluating an SMF record, the dimension of the array can be determined by dividing the length of the crypto counters section(SMF1154_128_CrypCtrs_Length) by 8, which is the length of SMF1154_128_CrypCtrs_Count.

Offsets		Name	Length	Format	Description
0	0	SMF1154_128_CrypCtrs_Count	8	binary	Crypto counter value. Valid up to a maximum of X'FFFFFFFFFFFFFFFF'.

RACF

Resource Access Control Facility (RACF) is a security program. It is a component of the Security Server for z/OS. RACF controls what you can do on the z/OS operating system. You can use RACF to protect your resources. RACF protects information and other resources by controlling the access to those resources.

RACF provides security by:

- Identifying and verifying users
- Authorizing users to access protected resources
- Recording and reporting access attempts

When the RACF subsystem is active and the system is enabled for collecting SMF type 1154 records, RACF collects and writes compliance data to SMF record type 1154 subtype 83, which is mapped by the IRRR1154 macro.

Record type 1154 subtype 83: RACF compliance data record

SMF record type 1154 provides compliance data from z/OS systems. A different subtype is assigned to each z/OS component or product that participates in compliance data collection. On receiving an ENF86 signal from the z/OSMF compliance REST API, participating components and products collect and write compliance data to their associated SMF 1154 subtype records.

RACF collects and writes compliance data to SMF record type 1154 subtype 83, which is mapped by the IRRR1154 macro.

Each SMF 1154 record contains an SMF extended header, SMF 1154 common information, a subtype-specific self-defining section, and sections containing data for the record, as follows:

SMF extended header
SMF type 1154 records use the Extended SMF record header. For a definition of the extended header, see the "Extended SMF record header version 1" table in Standard SMF record header in *z/OS MVS System Management Facilities (SMF)*. The extended record type, SMFHDR1_EXT_RTY, is set to 1154(x'482').

SMF 1154 common self-defining section and common header
For the common area mapping of Type 1154 SMF records common section, see Record type 1154 (X'482') — z/OS compliance evidence in *z/OS MVS System Management Facilities (SMF)*.

Following the common header, each SMF 1154 has a subtype-specific section that describes its contents. RACF provides SMF 1154 subtype 83 records to report compliance evidence.

Note: Compliance data collection for RACF requires z/OS 2.4 or later and PTFs for OA61933.

Table 48 on page 114 describes the format of subtype 83, which includes a header and four sections that collect RACE-specific compliance data.

Table 48. Structure of SMF type 1154 subtype 83

Section	Description
"Record type 1154 subtype 83: Header" on page 114	Common header. Appears in every record if multiple records are created.
"Data section 1 (RACFSMRY)" on page 115	Basic RACF configuration information, such as critical SETROPTS settings. A non-repeating section.
"Data section 2 (RACFCRIT)" on page 121	Information about resource profiles that are known to RACF and considered to be critical to proper system function. A possibly repeating section.
"Data section 3 (RACFAPFL)" on page 122	Information about data sets that are known to RACF, such as the following details: • APF authorized libraries. • Data sets used by RACF. • Data sets used by the RACF remote sharing facility (RRSF) • Parmlib data sets • Linklib data sets. A possibly repeating section.
"Data section 4 (RACFACTL)" on page 123	Information about RACF authorized callers. A possibly repeating section.

Record type 1154 subtype 83: Header

Table 49. Record type 1154 Subtype 83 Record header

Offsets	Field name	Length	Format	Description
0 0	SMF1154_83_0_RACFHTNU	2	Binary	Number of triplets: 4
2 2	SMF1154_83_0_RACFHRSV	2	Binary	Reserved
4 4	SMF1154_83_0_RT00001O	4	Binary	Offset to first data section 1 (RACFSMRY)
8 8	SMF1154_83_0_RT00001L	2	Binary	Length of a single data section 1
10 A	SMF1154_83_0_RT00001C	2	Binary	Count of RACFSMRY sections: 1
12 C	SMF1154_83_0_RT00002O	4	Binary	Offset to first data section 2 (RACFCRIT)
16 10	SMF1154_83_0_RT00002L	2	Binary	Length of a single data section 2
18 12	SMF1154_83_0_RT00002C	2	Binary	Count of RACFCRIT sections
20 14	SMF1154_83_0_RT00003O	4	Binary	Offset to data section 3 (RACFAPFL)

Table 49. Record type 1154 Subtype 83 Record header (continued)

Offsets	Field name	Length	Format	Description
24 18	SMF1154_83_0_RT00003L	2	Binary	Length of a single data section 3
26 1A	SMF1154_83_0_RT00003C	2	Binary	Count of RACFAPFL sections
28 1C	SMF1154_83_0_RT00004O	4	Binary	Offset to data section 4 (RACFACTL)
32 20	SMF1154_83_0_RT00004L	2	Binary	Length of a single data section 4
34 22	SMF1154_83_0_RT00004C	2	Binary	Count of RACFACTL sections

Data section 1 (RACFSMRY)

Data section 1 ("RACF Summary") reports overall RACF security settings.

Table 50. Record type 1154 Subtype 83 data section 1 (RACFSMRY)

Offsets	Field name	Length	Format	Description
0 0	SMF1154_83_1_RACFLEN	2	Binary	Length of this subsection
2 2	SMF1154_83_0_RACFHRSV	2	Binary	Reserved
4 4	SMF1154_83_0_RT00001O	4	Binary	Offset to first data section 1 (RACFSMRY)
8 8	SMF1154_83_0_RT00001L	2	Binary	Length of a single data section 1
10 A	SMF1154_83_0_RT00001C	2	Binary	Count of RACFSMRY sections: 1
12 C	SMF1154_83_0_RT00002O	4	Binary	Offset to first data section 2 (RACFCRIT)
16 10	SMF1154_83_0_RT00002L	2	Binary	Length of a single data section 2
18 12	SMF1154_83_0_RT00002C	2	Binary	Count of RACFCRIT sections
20 14	SMF1154_83_0_RT00003O	4	Binary	Offset to data section 3 (RACFAPFL)
24 18	SMF1154_83_0_RT00003L	2	Binary	Length of a single data section 3
26 1A	SMF1154_83_0_RT00003C	2	Binary	Count of RACFAPFL sections
28 1C	SMF1154_83_0_RT00004O	4	Binary	Offset to data section 4 (RACFACTL)
32 20	SMF1154_83_0_RT00004L	2	Binary	Length of a single data section 4
2 2	SMF1154_83_1_RACFVSN	2	Binary	Version (X'01')
4 4	SMF1154_83_1_RACFEYEC	4	EBCDIC	Eye catcher: C'RACF'
8 8	SMF1154_83_1_RACFVMRC	4	EBCDIC	RACF version (FMID)
12 C		6	Char	Reserved
18 12	SMF1154_83_1_RACFMULP	1	Binary	RACF status verification: **X'00'** Cannot determine status. The value of SMF1154_83_1_RACFMULV is meaningless. **X'01'** Status is known; see the value of SMF1154_83_1_RACFMULV.
19 13	SMF1154_83_1_RACFMULV	1	Binary	RACF status: **X'00'** RACF is active. **X'01'** RACF is in FAILSOFT mode.

Table 50. Record type 1154 Subtype 83 data section 1 (RACFSMRY) (continued)

Offsets	Field name	Length	Format	Description
20 14	SMF1154_83_1_RACFBYPP	1	Binary	RACF statistics verification: **X'00'** Cannot determine status. SMF1154_83_1_RACFBYPV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFBYPV.
21 15	SMF1154_83_1_RACFBYPV	1	Binary	RACF statistics status: **X'00'** RACF statistics are not being bypassed. **X'01'** RACF statistics are being bypassed.
22 16	SMF1154_83_1_RACFDRVP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFDRVV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFDRVV.
23 17	SMF1154_83_1_RACFDRVV	1	Binary	**X'00'** RACF default user (IBMUSER) is not revoked. **X'01'** RACF default user (IBMUSER) is revoked.
24 18	SMF1154_83_1_RACFARAP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFDRAV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFDRAV.
25 19	SMF1154_83_1_RACFARAV	1	Binary	**X'00'** RACF administrator access is not audited or logged **X'01'** SETROPTS SAUDIT is active. **X'02'** SETROPTS CMDVIOL is active. **X'03'** SETROPTS SAUDIT and SETROPTS CMDVIOL are active. **X'04'** SETROPTS OPERAUDIT is active. **X'05'** SETROPTS SAUDIT and SETROPTS OPERAUDIT are active. **X'06'** SETROPTS CMDVIOL and SETROPTS OPERAUDIT are active. **X'07'** SETROPTS SAUDIT and SETROPTS CMDVIOL and SETROPTS OPERAUDIT are active.

Table 50. Record type 1154 Subtype 83 data section 1 (RACFSMRY) (continued)

Offsets	Field name	Length	Format	Description
26 1A	SMF1154_83_1_RACFPSRP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFPSRV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFPSRV.
27 1B	SMF1154_83_1_RACFPSRV	1	Binary	Count of password rules. Values are stored in SMF1154_83_1_RACFSTXA.
28 1C	SMF1154_83_1_RACFSTXA	80	****	An eight element array in which each element is 10 bytes and consists of: • 1-byte minimum length • 8-byte string, which contains the RACF password value string as defined in the SETROPTS PASSWORD command. • 1-byte maximum length
108 6C	SMF1154_83_1_RACFPLCP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFPLCV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFPLCV.
109 6D	SMF1154_83_1_RACFPLCV	1	Binary	**X'00'** Lowercase characters not allowed in passwords. **X'01** Lowercase characters allowed in passwords.
110 6E	SMF1154_83_1_RACFPSCP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFPSCV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFPSCV.
111 6F	SMF1154_83_1_RACFPSCV	1	Binary	**X'00'** Special characters are not allowed in passwords. **X'01'** Special characters are allowed in passwords.
112 70	SMF1154_83_1_RACFPEXP	1	Binary	Reserved
113 71	SMF1154_83_1_RACFPEXV	1	Binary	Reserved
114 72	SMF1154_83_1_RACFPWXP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFPWXV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFPWXV.

Table 50. Record type 1154 Subtype 83 data section 1 (RACFSMRY) (continued)

Offsets	Field name	Length	Format	Description
115 73	SMF1154_83_1_RACFPWXV	1	Binary	Password exit status: **X'00'** No password exit is configured. **X'01'** Password exit is configured.
116 74	SMF1154_83_1_RACFPWIP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFPWIV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFPWIV.
117 75	SMF1154_83_1_RACFPWIV	1	Binary	Password interval. • X'FF' indicates NOINTERVAL.
118 76	SMF1154_83_1_RACFPWMP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFPWMV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFPWMV.
119 77	SMF1154_83_1_RACFPWMV	1	Binary	Password minimum lifetime.
120 78	SMF1154_83_1_RACFHISP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFHISV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFHISV.
121 79	SMF1154_83_1_RACFHISV	1	Binary	Password history count
122 7A	SMF1154_83_1_RACFRVKP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFRVKV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFRVKP.
123 7B	SMF1154_83_1_RACFRVKV	1	Binary	Maximum failed password attempts
124 7C	SMF1154_83_1_RACFINAP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFINAV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFINAV.
125 7D	SMF1154_83_1_RACFINAV	1	Binary	Maximum password inactivity in days
126 7E	SMF1154_83_1_RACFRVSP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFRVSV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFRVSV.

Table 50. Record type 1154 Subtype 83 data section 1 (RACFSMRY) (continued)

Offsets	Field name	Length	Format	Description
127 7F	SMF1154_83_1_RACFRVSV	1	Binary	**X'00'** Default RVARY SWITCH password is not in use. **X'01'** Default RVARY SWITCH password is in use.
128 80	SMF1154_83_1_RACFRVTP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFRVTV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFRVTV.
129 81	SMF1154_83_1_RACFRVTV	1	Binary	**X'00'** Default RVARY STATUS password is not in use. **X'01'** Default RVARY STATUS password is in use.
130 82	SMF1154_83_1_RACFPWEP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFPWEV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFPWEV.
131 83	SMF1154_83_1_RACFPWEV	1	Binary	**X'00'** Legacy password encryption is in effect. **X'01'** KDFAES password encryption is in effect.
132 84	SMF1154_83_1_RACFDPAP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFDPAV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFDPAV.
133 85	SMF1154_83_1_RACFDPAV	1	Binary	PROTECTALL(FAIL) status: **X'00'** PROTECTALL(FAIL) in not in effect. **X'01'** PROTECTALL(FAIL) in effect.
134 86	SMF1154_83_1_RACFDGPP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFDGPV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFDGPV.
135 87	SMF1154_83_1_RACFDGPV	1	Binary	**X'00'** Generic profiles are not enabled for the DATASET class. **X'01'** Generic profiles are enabled for the DATASET class.

Table 50. Record type 1154 Subtype 83 data section 1 (RACFSMRY) (continued)

Offsets	Field name	Length	Format	Description
136 88	SMF1154_83_1_RACFDUCP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFDUCV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFDUCV.
137 89	SMF1154_83_1_RACFDUCV	1	Binary	**X'00'** NOCATDSNS is in effect. **X'01'** CATDSNS is in effect.
138 8A	SMF1154_83_1_RACFEOSP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFDEOSV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFDEOSV.
139 8B	SMF1154_83_1_RACFEOSV	1	Binary	**X'00'** ERASE(ALL) is not enabled. **X'01'** ERASE(ALL) is enabled.
140 8C	SMF1154_83_1_RACFACEP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFACEV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFACEV.
141 8D	SMF1154_83_1_RACFACEV	1	Binary	**X'00'** ACEECHK class is not active. **X'01'** ACEECHK class is active.
142 8E	SMF1154_83_1_RACFACRP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFACRV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFACRV.
143 8F	SMF1154_83_1_RACFACRV	1	Binary	**X'00'** ACEECHK class is not RACLISTed. **X'01'** ACEECHK class is RACLISTed.
144 90	SMF1154_83_1_RACFJALP	1	Binary	**X'00'** Cannot determine status. SMF1154_83_1_RACFJALV is meaningless. **X'01'** Status is known; see SMF1154_83_1_RACFJALV.

Table 50. Record type 1154 Subtype 83 data section 1 (RACFSMRY) (continued)				
Offsets	**Field name**	**Length**	**Format**	**Description**
145 91	SMF1154_83_1_RACFJALV	1	Binary	**X'00'** NOBATCHALLRACF is in effect. **X'01'** BATCHALLRACF is in effect.
146 92	*	32	Char	Reserved

Data section 2 (RACFCRIT)

Data section 2 ("RACF Critical Settings") reports on RACF critical settings.

Table 51. Record type 1154 Subtype 83 data section 2 (RACFCRIT)				
Offsets	**Field name**	**Length**	**Format**	**Description**
0 0	SMF1154_83_X_RACFRINA	246	EBCDIC	Resource Name
246 F6	SMF1154_83_X_RACFRICL	8	EBCDIC	Class Name
254 FE	SMF1154_83_X_RACFRIPM	1	Binary	X'00': Cannot Determine Status. X'01': Results returned.
255 FF	SMF1154_83_X_RACFRIPX	1	Binary	**X'00'** Profile does not exist. **X'01'** Profile exists.
256 100	SMF1154_83_X_RACFRIUA	1	Binary	Universal access (UACC) values are documented in the UACC field; see “General template for the RACF database” on page 123.
257 101	SMF1154_83_X_RACFRIAU	1	Binary	AUDITValues are documented in the AUDIT field; see “General template for the RACF database” on page 123.
258 102	SMF1154_83_X_RACFRIAS	1	Binary	AUDIT Success QualifierValues are documented in the AUDITQS field; see “General template for the RACF database” on page 123.
259 103	SMF1154_83_X_RACFRIAF	1	Binary	AUDIT Failure QualifierValues are documented in the AUDITQF field; see “General template for the RACF database” on page 123.
260 104	SMF1154_83_X_RACFRIGU	1	Binary	GAUDIT values documented in the GAUDIT field; see “General template for the RACF database” on page 123.
261 105	SMF1154_83_X_RACFRIGS	1	Binary	GAUDIT Success Qualifier values documented in the GAUDITS field; see “General template for the RACF database” on page 123.
262 106	SMF1154_83_X_RACFRIGF	1	Binary	GAUDIT Failure Qualifier values documented in the GAUDITF field; see “General template for the RACF database” on page 123.
263 107	SMF1154_83_X_RACFRIWR	1	Binary	WARNING values documented in the WARNING field; see “General template for the RACF database” on page 123.
264 108	SMF1154_83_X_RACFRIIS	1	Binary	ID(*) usage: **X'00'** ID(*) not on access list. **X'01'** ID(*) on access list.
265 109	SMF1154_83_X_RACFRIIA	1	Binary	ID(*) access values are documented in the USERACS field; see “General template for the RACF database” on page 123.

Table 51. Record type 1154 Subtype 83 data section 2 (RACFCRIT) (continued)				
Offsets	**Field name**	**Length**	**Format**	**Description**
266 10A	*	14	Char	Reserved

Data section 3 (RACFAPFL)

Data section 3 ("RACF APF List") reports on APF-authorized programs.

Table 52. Record type 1154 Subtype 83 data section 3 (RACFAPFL)				
Offsets	**Field name**	**Length**	**Format**	**Description**
0 0	SMF1154_83_X_RACFRINA	246	EBCDIC	Resource Name
246 F6	SMF1154_83_X_RACFRICL	8	EBCDIC	Class Name
254 FE	SMF1154_83_X_RACFRIPM	1	Binary	**X'00'** Cannot determine status. **X'01'** Results returned.
255 FF	SMF1154_83_X_RACFRIPX	1	Binary	Profile status: **X'00'** Profile does not exist. **X'01'** Profile exists.
256 100	SMF1154_83_X_RACFRIUA	1	Binary	Universal access (UACC) values documented in the UACC field; see “General template for the RACF database” on page 123.
257 101	SMF1154_83_X_RACFRIAU	1	Binary	AUDIT values documented in the AUDIT field; see “General template for the RACF database” on page 123.
258 102	SMF1154_83_X_RACFRIAS	1	Binary	AUDIT success qualifier. Values are documented in the AUDITQS field; see “General template for the RACF database” on page 123.
259 103	SMF1154_83_X_RACFRIAF	1	Binary	AUDIT failure qualifier. Values are documented in the AUDITQF field; see “General template for the RACF database” on page 123.
260 104	SMF1154_83_X_RACFRIGU	1	Binary	GAUDIT values documented in the GAUDIT field; see “General template for the RACF database” on page 123.
0 0	SMF1154_83_X_RACFAINN	44	EBCDIC	Data set name
44 2C	SMF1154_83_X_RACFAINV	6	EBCDIC	Volume
50 32	SMF1154_83_X_RACFAINM	1	Binary	**X'00'** Cannot determine status. **X'01'** Results returned.
51 33	SMF1154_83_X_RACFAINX	1	Binary	Profile status: **X'00'** Profile does not exist. **X'01'** Profile exists.
52 34	SMF1154_83_X_RACFAINU	1	Binary	UACC values are documented in the UNIVACS field; see “Data set template for the RACF database” on page 140.
53 35	SMF1154_83_X_RACFAIWR	1	Binary	Warning values are documented in the WARNING field; see “Data set template for the RACF database” on page 140.

Table 52. Record type 1154 Subtype 83 data section 3 (RACFAPFL) (continued)				
Offsets	**Field name**	**Length**	**Format**	**Description**
54 36	SMF1154_83_X_RACFAIIS	1	Binary	ID(*) status: **X'00'** ID(*) not on access list **X'01'** ID(*) on access list.
55 37	SMF1154_83_X_RACFAIIA	1	Binary	ID(*) access. Values are documented in the USERACS field; see “Data set template for the RACF database” on page 140.
56 38	SMF1154_83_X_RACFAITY	1	EBCDIC	Data set type: **A** APF data set **F** RACF data set **L** Linklist data set **R** RRSF data set **P** Parmlib data set
57 39	Reserved	7	Char	Reserved

Data section 4 (RACFACTL)

Data section 4 ("RACF APF List") reports on the RACF authorized callers table.

Table 53. Record type 1154 Subtype 83 data section 4 (RACFACTL)				
Offsets	**Field name**	**Length**	**Format**	**Description**
0 0	SMF1154_83_X_RACFACTN	8	EBCDIC	Module name
8 8	SMF1154_83_X_RACFACTU	4	Binary	Authorization code: `B'cccccccrrrrrrrrrrrrrrrrrrrrrrrr'` Where *"cccccccc"* is the code and *"rrrr....."* is reserved. For descriptions of the authorization codes, see the format of the authorized caller table in *z/OS Security Server RACF System Programmer's Guide*.
12 C	SMF1154_83_X_RACFACTL	1	Binary	Module location: **X'00'** Not in LPA **X'01** In LPA
13 D	Reserved	3	Char	Reserved

General template for the RACF database

The general template describes the fields of general resource profiles in a RACF database.

NOT Programming Interface Information

ACL2RSVD AUDITQF AUDITQS CATEGORY CURKEY CURKEYV	ENCTYPE FIELD FLDCNT FLDFLAG FLDNAME FLDVALUE	GAUDITQF GAUDITQS MEMCNT MEMLIST NUMCTGY PREVKEY	PREVKEYV RACLDSP RACLHDR SALT SSKEY

End NOT Programming Interface Information

Note:

1. Application developers should not depend on being able to use RACROUTE REQUEST=EXTRACT for the BASE segment fields on any security product other than RACF. These products are expected to support only such segments as DFP and TSO.
2. The TME segment fields are intended to be updated by Tivoli® applications, which manage updates, permissions, and cross-references among the fields. The TME fields should only be directly updated on an exception basis. See *z/OS Security Server RACF Command Language Reference* for formats of the field data as enforced by the RACF commands. Use caution when directly updating TME fields, as the updates might be overridden by subsequent actions of Tivoli applications.

The contents of the general template are as follows:

Field name (character data)	Field ID	Flag 1	Flag 2	Field length decimal	Default value	Type	Field being described
The following is the BASE segment of the GENERAL template.							
GENERAL	001	00	00	00000000	00		
ENTYPE	002	00	00	00000001	05	Int	The number (5) corresponding to profiles for resources defined in the class descriptor table.
VERSION	003	00	00	00000001	01	Int	The version field from the profile. Always X'01'.
CLASTYPE	004	00	00	00000001	FF	Int	The class to which the resource belongs (from the ID=class-number operand of the ICHERCDE macro).
DEFDATE	005	00	20	00000003	FF	Date	The date the resource was defined to RACF.
OWNER	006	00	00	00000008	FF	Char	The owner of the resource.
LREFDAT	007	01	20	00000003	FF	Date	The date the resource was last referenced.
LCHGDAT	008	01	20	00000003	FF	Date	The date the resource was last updated.
ACSALTR	009	01	00	00000002	FF	Int	The number of times the resource was accessed with ALTER authority.
ACSCNTL	010	01	00	00000002	FF	Int	The number of times the resource was accessed with CONTROL authority.
ACSUPDT	011	01	00	00000002	FF	Int	The number of times the resource was accessed with UPDATE authority.
ACSREAD	012	01	00	00000002	FF	Int	The number of times the resource was accessed with READ authority.

Field name (character data)	Field ID	Flag 1	Flag 2	Field length decimal	Default value	Type	Field being described
UACC	013	20	80	00000001	00	Bin	The universal access authority for the resource. **Bit** **Meaning when set** **0** ALTER access **1** CONTROL access **2** UPDATE access **3** READ access **4** EXECUTE access **5–6** Reserved for IBM's use **7** NONE access.
AUDIT	014	20	00	00000001	00	Bin	Audit flags. **Bit** **Meaning when set** **0** Audit all accesses **1** Audit successful accesses **2** Audit accesses that fail **3** No auditing **4–7** Reserved for IBM's use
LEVEL	015	20	00	00000001	00	Int	Resource level.
GAUDIT	016	20	00	00000001	00	Bin	Global audit flags. **Bit** **Meaning when set** **0** Audit all accesses **1** Audit successful accesses **2** Audit accesses that fail **3** No auditing **4–7** Reserved for IBM's use
INSTDATA	017	00	00	00000000	00	Char	Installation data; maximum length = 255.

Field name (character data)	Field ID	Flag 1	Flag 2	Field length decimal	Default value	Type	Field being described
GAUDITQF	021	00	00	00000001	FF	Bin	Global audit FAILURES qualifier. **Value** **Meaning** **X'00'** Log access at READ authority **X'01'** Log access at UPDATE authority **X'02'** Log access at CONTROL authority **X'03'** Log access at ALTER authority
AUDITQS	018	00	00	00000001	FF	Bin	Audit SUCCESS qualifier. **Value** **Meaning** **X'00'** Log access at READ authority **X'01'** Log access at UPDATE authority **X'02'** Log access at CONTROL authority **X'03'** Log access at ALTER authority
AUDITQF	019	00	00	00000001	FF	Bin	Audit FAILURES qualifier. **Value** **Meaning** **X'00'** Log access at READ authority **X'01'** Log access at UPDATE authority **X'02'** Log access at CONTROL authority **X'03'** Log access at ALTER authority
GAUDITQS	020	00	00	00000001	FF	Bin	Global audit SUCCESS qualifier. **Value** **Meaning** **X'00'** Log access at READ authority **X'01'** Log access at UPDATE authority **X'02'** Log access at CONTROL authority **X'03'** Log access at ALTER authority
WARNING	022	20	00	00000001	00	Bin	Identifies the data set as having (bit 7 is on) or not having the WARNING attribute.

Field name (character data)	Field ID	Flag 1	Flag 2	Field length decimal	Default value	Type	Field being described
RESFLG	023	20	00	00000001	00	Bin	Resource profile flags: **Bit** **Meaning when set** **0** TAPEVOL can only contain one data set. **1** TAPEVOL profile is automatic. **2** Maintain TVTOC for TAPEVOL. **3–7** Reserved for IBM's use
TVTOCCNT	024	10	00	00000004	00	Int	The number of TVTOC entries.
TVTOCSEQ	025	80	00	00000002	00	Int	The file sequence number of tape data set.
TVTOCCRD	026	80	20	00000003	00	Date	The date the data set was created.
TVTOCIND	027	A0	00	00000001	00	Bin	Data set profiles flag (RACF indicator bit): **Bit** **Meaning when set** **1** Discrete data set profile exists **2–7** Reserved for IBM's use
TVTOCDSN	028	80	00	00000000	00	Char	The RACF internal name.
TVTOCVOL	029	80	00	00000000	00	Char	This field is a list of the volumes on which the tape data set resides.
TVTOCRDS	030	80	00	00000000	00	Char	The name used when creating the tape data set; maximum length = 255.
NOTIFY	031	00	00	00000000	00	Char	The user to be notified when access violations occur against resource protected by this profile.
LOGDAYS	032	20	00	00000001	00	Bin	The days of the week the TERMINAL cannot be used. (Bit 0 equals Sunday, bit 1 equals Monday, and so on).
LOGTIME	033	00	00	00000000	00	Time	The time of the day the TERMINAL can be used.
LOGZONE	034	00	00	00000000	00	Bin	The time zone in which the terminal is located.
NUMCTGY	035	10	00	00000004	00	Int	Number of categories.
CATEGORY	036	80	00	00000002	00	Int	List of categories.
SECLEVEL	037	00	00	00000001	FF	Int	Resource security level.
FLDCNT	038	10	00	00000004	00	Int	Reserved for IBM's use.
FLDNAME	039	80	00	00000008	00		Reserved for IBM's use.
FLDVALUE	040	80	00	00000000	00		Reserved for IBM's use.
FLDFLAG	041	A0	00	00000001	00		Reserved for IBM's use.
APPLDATA	042	00	00	00000000	00	Char	Application data.
MEMCNT	043	10	80	00000004	00	Int	The number of members.
MEMLST	044	80	80	00000000	00	Bin	The resource group member. For SECLABEL class, a 4-byte SMF ID.
VOLCNT	045	10	00	00000004	00	Int	Number of volumes in tape volume set.
VOLSER	046	80	00	00000006	00	Char	Volume serials of volumes in tape volume set.

Field name (character data)	Field ID	Flag 1	Flag 2	Field length decimal	Default value	Type	Field being described
ACLCNT	047	10	80	00000004	00	Int	The number of users and groups currently authorized to access the resource.
USERID	048	80	80	00000008	00	Char	The user ID or group name of each user or group authorized to access the resource.
USERACS	049	A0	80	00000001	00	Bin	The access authority that each user or group has for the resource. **Bit** **Meaning when set** **0** ALTER access **1** CONTROL access **2** UPDATE access **3** READ access **4** EXECUTE access **5–6** Reserved for IBM's use **7** NONE access **Note:** Each of the above access authority fields has mutually exclusive bits except for EXECUTE and NONE.
ACSCNT	050	80	00	00000002	00	Int	The number of times the resource was accessed by each user or group.
USRCNT USRNM USRDATA USRFLG	051 052 053 054	10 80 80 A0	00 00 00 00	00000004 00000008 00000000 00000001	00 00 00 00	Int	Reserved for installation use. Reserved for installation use. Reserved for installation use. Reserved for installation use.
SECLABEL	055	00	00	00000008	00	Char	Security label.
ACL2CNT	056	10	00	00000004	00	Int	Number of entries in conditional access list.
ACL2NAME	057	80	00	00000008	00	Bin	1 indicator byte; 7 bytes reserved for IBM's use.
ACL2UID	058	80	00	00000008	00	Char	User ID or group.
ACL2ACC	059	80	00	00000001	00	Bin	Access authority.
ACL2ACNT	060	80	00	00000002	00	Int	Access count.
ACL2RSVD	061	80	00	00000000	00	Bin	Conditional data. Reserved for IBM's use.
RACLHDR	062	00	00	00000020	00	Bin	RACGLIST header.
RACLDSP	063	00	00	00000000	00	Bin	RACGLIST dataspace information.
FILTERCT	064	10	00	00000004	00		Number of names that Hash to this DIGTNMAP Profile.
FLTRLABL	065	80	00	00000000	00		Label associated with this DIGTNMAP Mapping (matches NMAPLABL for user named by FLTRUSER or user irrmulti.)
FLTRSTAT	066	A0	00	00000001	00		Trust status – bit 0 on for trusted.
FLTRUSER	067	80	00	00000000	00		User ID or criteria profile name.

Field name (character data)	Field ID	Flag 1	Flag 2	Field length decimal	Default value	Type	Field being described
FLTRNAME	068	80	00	00000000	00		Unhashed issuer's name filter used to create this profile name, (max of 255), followed by a separator, (X'4A'), and the unhashed subject's name filter used to create this profile name (max of 255).
FLTRSVD1	069	80	00	00000000	00		Reserved for IBM's use.
FLTRSVD2	070	80	00	00000000	00		Reserved for IBM's use.
FLTRSVD3	071	80	00	00000000	00		Reserved for IBM's use.
FLTRSVD4	072	80	00	00000000	00		Reserved for IBM's use.
FLTRSVD5	073	80	00	00000000	00		Reserved for IBM's use.
RACDHDR	074	00	08	00000000	00	Bin	CACHECLS header.
DIDCT	075	10	00	00000004	00		Number of names that correspond to this IDIDMAP Profile.
DIDLABL	076	80	00	00000000	00		Label associated with this IDIDMAP class profile mapping (matches DMAPLABL for user named by DIDUSER).
DIDUSER	077	80	00	00000008	00		User ID.
DIDRNAME	078	80	00	00000000	00		Registry name (max of 255).
DIDRSVD1	079	80	00	00000000	00		Reserved for IBM's use.
DIDRSVD2	080	80	00	00000000	00		Reserved for IBM's use.

Field name	Field ID	Flag 1	Flag 2	Combination field IDs					Type	
The following is the COMBINATION segment of the GENERAL template.										
CREADATE	000	40	00	005	000	000	000	000		Combination.
AUTHDATE	000	40	00	005	000	000	000	000		Fields.
AUTHOR	000	40	00	006	000	000	000	000		
TVTOC	000	48	00	025	026	027	028	029		
	000	40	00	030	000	000	000	000		
LOGINFO	000	40	00	032	033	034	000	000		
FIELD	000	40	00	039	040	041	000	000		
ACL	000	40	00	048	049	050	000	000		
ACL1	000	40	00	048	049	000	000	000		
USERDATA	000	40	00	052	053	054	000	000		
ACL2	000	40	00	057	058	059	060	061		Conditional access list
ACL2A3	000	40	00	057	058	059	060	000		Conditional access list
FLTRLST1	000	40	00	065	066	067	068	000		Combo field for FILTER
FLTRLST2	000	40	00	065	067	068	000	000		Combo field for FILTER
CERTRING	000	40	00	010	011	009	000	000		Digital certificate data.
CERTRNG2	000	40	00	009	011	000	000	000		
CERTRNG3	000	40	00	009	012	013	000	000		
DIDLIST1	000	40	00	076	077	078	000	000		Combination for distributed identity.

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
The following is the SESSION segment of the GENERAL template.							
SESSION	001	00	00	00000000	00		Start of segment fields
SESSKEY	002	00	00	00000000	00	Bin	Session key; maximum length = 8
SLSFLAGS	003	20	00	00000001	00	Bin	Session flag byte **Bit** **Meaning when set** **0** SLSLOCK-This profile is locked out **1–7** Reserved for IBM's use
KEYDATE	004	00	00	00000004	00	Date	Last date session key was changed. It is in the format *0cyyddF* where *c*=0 for 1900–1999 and *c*=1 for 2000–2099. For more information on this MVS™-returned format, see *z/OS MVS Programming: Assembler Services Guide*.
KEYINTVL	005	00	00	00000002	00	Int	Number of days before session key expires
SLSFAIL	006	00	00	00000002	00	Int	Current® number of invalid attempts
MAXFAIL	007	00	00	00000002	00	Int	Number of invalid attempts before lockout
SENTCNT	008	10	00	00000004	00	Int	Number of session entities in list
SENTITY	009	80	00	00000035	00	Char	Entity name
SENTFLCT	010	80	00	00000002	00	Int	Number of failed attempts for this entity
CONVSEC	011	20	00	00000001	00	Bin	Conversation security. **Value** **Meaning** **X'40'** Conversation security **X'50'** Persistent verification **X'60'** User ID and password already verified **X'70'** User ID and password already verified plus persistent verification **X'80'** Security none
The following is the DLFDATA segment of the GENERAL template.							
DLFDATA	001	00	00	00000000	00		Start of segment fields
RETAIN	002	20	00	00000001	00	Bin	Retain flag byte
JOBNMCNT	003	10	00	00000004	00	Int	Count of jobnames
JOBNAMES	004	80	00	00000000	00	Char	Jobnames; maximum length = 8
The following is the SSIGNON segment of the GENERAL template.							
SSIGNON	001	00	00	00000000	00		Start of segment fields
SSKEY	002	00	00	00000000	00	Bin	Secured signon key
PTKEYLAB	003	00	00	00000000	00	Char	EPT key label
PTTYPE	004	00	00	00000000	00	Char	PassTicket Type

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
PTTIMEO	005	00	00	00000004	00	Int	PassTicket Timeout
PTREPLAY	006	00	00	00000001	00	Bin	PassTicket Replay
The following is the STDATA segment of the GENERAL template.							
STDATA	001	00	00	00000000	00		Start of segment fields
STUSER	002	00	00	00000008	40	Char	User ID or =MEMBER
STGROUP	003	00	00	00000008	40	Char	Group name or =MEMBER
FLAGTRUS	004	20	00	00000001	00	Bin	Trusted flag, X'80' = trusted
FLAGPRIV	005	20	00	00000001	00	Bin	Privileged flag, X'80' = privileged
FLAGTRAC	006	20	00	00000001	00	Bin	Trace usage flag X'80' = issue IRR8I2I
The following is the SVFMR segment of the GENERAL template.							
SVFMR	001	00	00	00000000	00		Start of segment fields
SCRIPTN	002	00	00	00000008	00	Char	Script name
PARMN	003	00	00	00000008	00	Char	Parameter name
The following is the CERTDATA segment of the GENERAL template.							
CERTDATA	001	00	00	00000000	00		Start of segment fields
CERT	002	00	00	00000000	00	Bin	Digital certificate
CERTPRVK	003	00	00	00000000	00	Bin	Private key or key label
RINGCT	004	10	00	00000004	00	Int	Number of key rings associated with this certificate
RINGNAME	005	80	00	00000000	00	Char	Profile name of a ring with which this certificate is associated
CERTSTRT	006	00	00	00000000	00		Date and time from which the certificate is valid. If the year is 2041 or earlier, this is an 8-byte TOD format field. If the year is later than 2041, this is the first 8 bytes of an ETOD format field. If the first byte is greater than X'38', the date is in TOD format; otherwise it is in ETOD format.
CERTEND	007	00	00	00000000	00		Date and time after which the certificate is not valid. If the year is 2041 or earlier, this is an 8-byte TOD format field. If the year is later than 2041, this is the first 8 bytes of an ETOD format field. If the first byte is greater than X'38', the date is in TOD format; otherwise it is in ETOD format.
CERTCT	008	10	00	00000004	00	Int	The number of certificates associated with this key ring. CERTCT is a repeat group that identifies the certificates associated with a key ring. CERTCT is used *only* with DIGTRING profiles.
CERTNAME	009	80	00	00000000	00	Char	The profile name of the certificate
CERTUSAG	010	80	00	00000004	00	Bin	Certificate usage in ring: • X'00000000' – PERSONAL • X'00000001' – SITE • X'00000002' – CERTAUTH
CERTDFLT	011	80	00	00000001	00	Bin	Verifies if it is the default certificate: • X'00' – Not the default • X'80' – The default

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
CERTSJDN	012	80	00	00000000	00	Bin	The subject name of the entity to whom the certificate is issued. This field is a BER-encoded format of the subject's distinguished name as contained in the certificate
CERTLABL	013	80	00	00000000	00	Char	Label associated with the certificate
CERTRSV1	014	80	00	00000000	00		Reserved for IBM's use.
CERTRSV2	015	80	00	00000000	00		Reserved for IBM's use.
CERTRSV3	016	80	00	00000000	00		Reserved for IBM's use.
CERTRSV4	017	80	00	00000000	00		Reserved for IBM's use.
CERTRSV5	018	80	00	00000000	00		Reserved for IBM's use.
CERTRSV6	019	80	00	00000000	00		Reserved for IBM's use.
CERTRSV7	020	80	00	00000000	00		Reserved for IBM's use.
CERTRSV8	021	80	00	00000000	00		Reserved for IBM's use.
CERTRSV9	022	80	00	00000000	00		Reserved for IBM's use.
CERTRSVA	023	80	00	00000000	00		Reserved for IBM's use.
CERTRSVB	024	80	00	00000000	00		Reserved for IBM's use.
CERTRSVC	025	80	00	00000000	00		Reserved for IBM's use.
CERTRSVD	026	80	00	00000000	00		Reserved for IBM's use.
CERTRSVE	027	80	00	00000000	00		Reserved for IBM's use.
CERTRSVF	028	80	00	00000000	00		Reserved for IBM's use.
CERTRSVG	029	80	00	00000000	00		Reserved for IBM's use.
CERTRSVH	030	80	00	00000000	00		Reserved for IBM's use.
CERTRSVI	031	80	00	00000000	00		Reserved for IBM's use.
CERTRSVJ	032	80	00	00000000	00		Reserved for IBM's use.
CERTRSVK	033	80	00	00000000	00		Reserved for IBM's use.
CERTPRVT	034	00	00	00000004	00	Bin	Associated key type: • X'00000000' – No associated key • X'00000001' – PKCS DER-encoded • X'00000002' – ICSF token label • X'00000003' – PCICC label • X'00000004' – DSA • X'00000005' – ICSF public token label • X'00000006' – Reserved for IBM's use • X'00000007' – NIST ECC key • X'00000008' – Brainpool ECC key • X'00000009' – NIST ECC token label in PKDS • X'0000000A' – Brainpool ECC token label in PKDS • X'0000000B' – RSA token label in TKDS • X'0000000C' – NIST ECC token label in TKDS • X'0000000D' – Brainpool ECC token label in TKDS
CERTPRVS	035	00	00	00000004	00	Int	Private key size in bits

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
CERTLSER	036	00	00	00000008	00	Bin	The low order 8 bytes of the last certificate that was signed with this key. This field is used with DIGTCERT profiles only
RINGSEQN	037	00	00	00000004	00	Int	Ring change count
CERTGREQ	038	00	00	00000001	00	Bin	Indicates if the certificate is used for generating a request
The following is the TME segment of the GENERAL template.							
TME	001	00	00	00000000	00		Start of segment fields
PARENT	002	00	00	00000000	00	Char	Parent name
CHILDN	003	10	00	00000004	00	Int	Count of children
CHILDREN	004	80	00	00000000	00	Char	Child names
RESN	005	10	00	00000004	00	Int	Count of resource-access specifications
RESOURCE	006	80	00	00000000	00		Resource-access specifications
GROUPN	007	10	00	00000004	00	Int	Count of groups
GROUPS	008	80	00	00000008	00		Group names
ROLEN	009	10	00	00000004	00	Int	Count of role-access specifications
ROLES	010	80	00	00000000	00	Char	Role-access specifications
The following is the KERB segment of the GENERAL template.							
KERB	001	00	00	00000000	00		Start of segment fields
KERBNAME	002	00	00	00000000	00	Char	Kerberos realm name
MINTKTLF	003	00	00	00000000	00	Char	Minimum ticket life
MAXTKTLF	004	00	00	00000000	00	Char	Maximum ticket life
DEFTKTLF	005	00	00	00000000	00	Char	Default ticket life
SALT	006	00	00	00000000	00	Char	Current key salt
ENCTYPE	007	00	00	00000000	00	Char	Encryption type
CURKEYV	008	00	00	00000000	00	Char	Current key version
CURKEY	009	00	00	00000000	00	Char	Current key value
PREVKEYV	010	00	00	00000000	00	Char	Previous key version
PREVKEY	011	00	00	00000000	00	Char	Previous key value
ENCRYPT	012	00	00	00000004	55	Char	Encryption type
CHKADDRS	013	00	00	00000001	00	Char	Check addresses flag
The following is the PROXY segment of the GENERAL template.							
PROXY	001	00	00	00000000	00		Start of segment fields
LDAPHOST	002	00	00	00000000	00	Char	LDAP server URL; maximum length: 1023
BINDDN	003	00	00	00000000	00	Char	Bind distinguished name; maximum length: 1023
BINDPW	004	00	08	00000000	00	Char	Bind password; maximum length: 128
BINDPWKY	005	00	08	00000071	00	Char	Bind password mask or encrypt key
The following is the EIM segment of the GENERAL template.							
EIM	001	00	00	00000000	00		Start of segment fields
DOMAINDN	002	00	00	00000000	00	Char	EIM Domain Distinguished Names

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
OPTIONS	003	00	00	00000004	55	Char	EIM Options
LOCALREG	004	00	00	00000000	00	Char	Local Registry Name
KERBREG	005	00	00	00000000	00	Char	Kerberos Registry Name
X509REG	006	00	00	00000000	00	Char	X509 Registry Name
The following is the ALIAS segment of the GENERAL template.							
ALIAS	001	00	00	00000000	00		Start of segment fields
IPLOOK	002	00	10	00000016	00	Bin	IP lookup value
The following is the CDTINFO segment of the GENERAL template.							
CDTINFO	001	00	00	0	0		Start of segment fields
CDTPOSIT	002	00	00	4	FF	Int	POSIT number for class
CDTMAXLN	003	00	00	1	8	Int	Maximum length of profile names
CDTMAXLX	004	00	00	4	FF	Int	Maximum resource or profile name length when using ENTITYX
CDTDFTRC	005	00	00	1	4	Int	Default return code
CDTKEYQL	006	00	00	4	0	Int	Number of key qualifiers
CDTGROUP	007	00	00	8	0	Char	Resource grouping class name
CDTMEMBR	008	00	00	8	0	Char	Member class name
CDTFIRST	009	00	00	1	X'C0'	Bin	Character restriction for first character of profile name **Value** **Meaning** **X'80'** Alphabetic **X'40'** National **X'20'** Numeric **X'10'** Special
CDTOTHER	010	00	00	1	X'C0'	Bin	Character restriction for characters of the profile name other than the first character **Value** **Meaning** **X'80'** Alphabetic **X'40'** National **X'20'** Numeric **X'10'** Special
CDTOPER	011	00	00	1	X'00'	Bin	Operations attribute considered **Value** **Meaning** **X'80'** RACF considers OPERATIONS attribute

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
CDTUACC	012	00	00	1	X'01'	Bin	Default UACC **Value** **Meaning** **X'80'** ALTER **X'40'** CONTROL **X'20'** UPDATE **X'10'** READ **X'08'** EXECUTE **X'04'** UACC from ACEE **X'01'** NONE
CDTRACL	013	00	00	1	X'00'	Bin	SETROPTS RACLIST **Value** **Meaning** **X'00'** RACLIST disallowed **X'80'** RACLIST allowed **X'40'** RACLIST required
CDTGENL	014	00	00	1	X'00'	Bin	SETROPTS GENLIST **Value** **Meaning** **X'80'** GENLIST allowed
CDTPRFAL	015	00	00	1	X'80'	Bin	Profiles allowed **Value** **Meaning** **X'80'** Profiles are allowed
CDTSLREQ	016	00	00	1	X'00'	Bin	Security labels required **Value** **Meaning** **X'80'** Security labels are required
CDTMAC	017	00	00	1	X'80'	Bin	Mandatory access checking (MAC) processing **Value** **Meaning** **X'80'** Normal mandatory access checks **X'40'** Reverse mandatory access checks **X'20'** Equal mandatory access checks

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
CDTSIGL	018	00	00	1	X'00'	Bin	ENF Signal **Value** **Meaning** **X'80'** ENF signal to be sent
CDTCASE	019	00	00	1	X'00'	Bin	Case of profile names **Value** **Meaning** **X'00'** Uppercase **X'80'** ASIS - preserve case
CDTGEN	020	00	00	1	X'80'	Bin	SETROPTS GENERIC **Value** **Meaning** **X'80'** GENERIC allowed
The following is the ICTX segment of the GENERAL template.							
ICTX	001	00	00	00000000	00		Start of segment fields
USEMAP	002	00	00	00000001	80	Bin	Application supplied mapping **Value** **Meaning** **X'80'** Use the mapping
DOMAP	003	00	00	00000001	00	Bin	Identity cache mapping **Value** **Meaning** **X'80'** Do the mapping
MAPREQ	004	00	00	00000001	00	Bin	**Value** **Meaning** **X'80'** Mapping is required
MAPTIMEO	005	00	00	00000002	00	Int	Mapping timeout adjustment
The following is the CFDEF segment of the GENERAL template.							
CFDEF	001	00	00	0	0		Start of segment fields for defining custom field attributes
CFDTYPE	002	00	00	1	01	Bin	Data type for custom field: • 01 - character • 02 - numeric • 03 - flag • 04 - hex
CFMXLEN	003	00	00	4	FF	Int	Maximum field length
CFMXVAL	004	00	00	4	FF	Int	Maximum numeric value
CFMNVAL	005	00	00	4	FF	Int	Minimum numeric value

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
CFFIRST	006	00	00	1	00	Bin	First character restrictions: • 01 - alpha • 02 - alphanum • 03 - any • 04 - nonatabc • 05 - nonatnum • 06 - numeric
CFOTHER	007	00	00	1	00	Bin	Other character restrictions: • 01 - alpha • 02 - alphanum • 03 - any • 04 - nonatabc • 05 - nonatnum • 06 - numeric
CFMIXED	008	20	00	1	00	Bin	If bit 0 is on, mixed case is allowed
CFHELP	009	00	00	00	00	Char	Help text; maximum length = 255
CFLIST	010	00	00	00	00	Char	List heading text; maximum length = 40
CFVALRX	011	00	00	00	00	Char	Custom field REXX validation exit
The following is the SIGVER segment of the GENERAL template.							
SIGVER	001	00	00	0	0		Start of segment fields
SIGREQD	002	00	00	1	0	Bin	Module must have a signature: **Value** **Meaning** **X'80'** Yes **X'00'** No
FAILLOAD	003	00	00	1	0	Bin	Loader failure conditions: **Value** **Meaning** **X'80'** Bad signature only **X'40'** Any failing signature condition **X'00'** Never

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
SIGAUDIT	004	00	00	1	0	Bin	RACF audit conditions: **Value** **Meaning** **X'80'** Bad signature only **X'40'** Any failing signature condition **X'20'** Success **X'01'** All **X'00'** None
The following is the ICSF segment of the GENERAL template.							
ICSF	01	00	00	00000000	00		Start of segment fields for defining ICSF attributes
CSFSEXP	02	00	00	00000001	00	Bin	Symmetric key export option: **Value** **Meaning** **X'80'** BYLIST **X'40'** BYNONE **X'00'** BYANY
CSFSKLCT	03	10	00	00000004	00	Int	Count of PKDS labels
CSFSKLBS	04	80	00	00000000	00	Char	PKDS labels that might be used to export this symmetric key
CSFSCLCT	05	10	00	00000004	0	Int	Count of certificate labels
CSFSCLBS	06	80	00	00000000	00	Char	Certificate labels that might be used to export this symmetric key
CSFAUSE	07	00	00	00000004	55	Bin	Asymmetric key usage. In byte 3: **Value** **Meaning** **X'08'** NOSECUREEXPORT **X'04'** SECUREEXPORT **X'02'** NOHANDSHAKE **X'01'** HANDSHAKE
CSFSCPW	08	00	00	00000001	00	Bin	Symmetric key CPACF wrap **Value** **Meaning** **X'80'** YES **X'00'** NO

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
CSFSCPR	09	00	00	00000001	00	Bin	Symmetric key CPACF return **Value** **Meaning** **X'80'** YES **X'00'** NO
The following is the MFA segment of the GENERAL template.							
MFA	001	00	00	00000000	00		Start of segment fields
MFDATA	002	00	00	00000000	00		Free-form factor metadata
The following is the MFPOLICY segment of the GENERAL template.							
MFPOLICY	001	00	00	00000000	00		Start of segment fields
MFFCTRN	002	10	00	00000004	00		Number of factors in policy
MFFCTRS	003	80	00	00000000	00		Policy factor list
MFTIMEO	004	00	00	00000004	00		Policy token timeout
MFREUSE	005	00	00	00000001	00		Policy reuse setting
The following is the CSDATA segment of the GENERAL template.							
CSDATA	001	00	00	00000000	00	Bin	Start of the segment fields for custom fields. **Note:** Intended usage for these fields is dictated by your installation. See *z/OS Security Server RACF Security Administrator's Guide* for more information on custom fields.
CSCNT	002	10	00	00000004	00	Char	Count of custom fields
CSTYPE	003	80	00	00000001	01	Char	Custom field type • 01 - character • 02 - numeric • 03 - flag • 04 - hex
CSKEY	004	80	00	00000000	00	Char	Custom field keyword
CSVALUE	005	80	00	00000000	00	Char	Custom field value
The following is the IDTPARMS segment of the GENERAL template.							
IDTPARMS	001	00	00	00000000	00		Start of segment field
IDTTOKN	002	00	00	00000000	00	Char	PKCS#11 Token Name
IDTSEQN	003	00	00	00000000	00	Char	PKCS#11 Sequence Number
IDTCAT	004	00	00	00000000	00	Char	PKCS#11 Category
IDTSALG	005	00	00	00000000	00	Char	Signature Algorithm
IDTTIMEO	006	00	00	00000004	00	Int	IDT Timeout
IDTANYAP	007	00	00	00000001	80	Bin	IDT Any Application

Field name	**Field ID**	**Flag 1**	**Flag 2**	**Combination field IDs**					**Type**	
The following is a COMBINATION field of the CSDATA segment of the GENERAL template.										
CSCDATA	000	40	00	003	004	005	000	000	Char	Combination field for custom fields

Data set template for the RACF database

The data set template describes the fields of the data set profiles in a RACF database.

NOT Programming Interface Information

ACL2VAR AUDITQF AUDITQS	CATEGORY FIELD FLDCNT	FLDFLAG FLDNAME	FLDVALUE NUMCTGY

End NOT Programming Interface Information

Note:

1. Application developers should not depend on being able to use RACROUTE REQUEST=EXTRACT for the BASE segment fields on any security product other than RACF. These products are expected to support only such segments as DFP and TSO.
2. The TME segment fields are intended to be updated by Tivoli applications, which manage updates, permissions, and cross-references among the fields. The TME fields should only be directly updated on an exception basis. See *z/OS Security Server RACF Command Language Reference* for formats of the field data as enforced by the RACF commands. Use caution when directly updating TME fields, as the updates might be overridden by subsequent actions of Tivoli applications.

The contents of the data set template are as follows:

Template							**Field being described**
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
DATASET	001	00	00	00000000	00		
ENTYPE	002	00	00	00000001	04	Int	The number (4) corresponding to data set profiles.
VERSION	003	00	00	00000001	01	Int	The version field from the profile. Always X'01'.
CREADATE	004	00	20	00000003	FF	Date	The date the data set was initially defined to RACF; 3-byte date.
AUTHOR	005	00	00	00000008	FF	Char	The owner of the data set.
LREFDAT	006	01	20	00000003	FF	Date	The date the data set was last referenced; 3-byte date.
LCHGDAT	007	01	20	00000003	FF	Date	The date the data set was last updated; 3-byte date.
ACSALTR	008	01	00	00000002	FF	Int	The number of times the data set was accessed with ALTER authority.
ACSCNTL	009	01	00	00000002	FF	Int	The number of times the data set was accessed with CONTROL authority.
ACSUPDT	010	01	00	00000002	FF	Int	The number of times the data set was accessed with UPDATE authority.
ACSREAD	011	01	00	00000002	FF	Int	The number of times the data set was accessed with READ authority.

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
UNIVACS	012	20	00	00000001	00	Bin	The universal access authority for the data set. **Bit** **Meaning when set** **0** ALTER access **1** CONTROL access **2** UPDATE access **3** READ access **4** EXECUTE access **5–6** Reserved for IBM's use **7** NONE access
FLAG1	013	20	00	00000001	00	Bin	Identifies whether the data set is a group data set. If bit 0 is on, the data set is a group data set.
AUDIT	014	20	00	00000001	00	Bin	Audit Flags. **Bit** **Meaning when set** **0** Audit all accesses **1** Audit successful accesses **2** Audit accesses that fail **3** No auditing **4–7** Reserved for IBM's use
GROUPNM	015	00	00	00000008	FF	Char	The current connect group of the user who created this data set.
DSTYPE	016	20	00	00000001	00	Bin	Identifies the data set as a VSAM, non-VSAM (or generic), MODEL or TAPE data set. **Bit** **Meaning when set** **0** VSAM data set (non-VSAM if this bit is set to 0) **1** MODEL profile **2** Type = TAPE when set on **3–7** Reserved for IBM's use
LEVEL	017	00	00	00000001	FF	Int	Data set level.
DEVTYP	018	00	00	00000004	FF	Bin	The type of device on which the data set resides; only for non-model, discrete data sets.

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
DEVTYPX	019	00	00	00000008	FF	Char	The EBCDIC name of the device type on which the data set resides; only for non-model, discrete data sets.
GAUDIT	020	20	00	00000001	00	Bin	Global audit flags. (Audit options specified by a user with the AUDITOR or group-AUDITOR attribute.) **Bit** **Meaning when set** **0** Audit all accesses **1** Audit successful accesses **2** Audit accesses that fail **3** No auditing **4–7** Reserved for IBM's use
INSTDATA	021	00	00	00000000	00	Char	Installation data; maximum length = 255.
GAUDITQF	025	00	00	00000001	FF	Bin	Global audit FAILURES qualifier. The AUDITQS, AUDITQF, GAUDITQS, and GAUDITQF fields have the following format: **Value** **Meaning when set** **X'00'** Log access at READ level **X'01'** Log access at UPDATE level **X'02'** Log access at CONTROL level **X'03'** Log access at ALTER level
AUDITQS	022	00	00	00000001	FF	Bin	Audit SUCCESS qualifier.
AUDITQF	023	00	00	00000001	FF	Bin	Audit FAILURES qualifier.
GAUDITQS	024	00	00	00000001	FF	Bin	Global audit SUCCESS qualifier.
WARNING	026	20	00	00000001	00	Bin	Identifies the data set as having (bit 7 is on) or not having the WARNING attribute.
SECLEVEL	027	00	00	00000001	FF	Int	Data set security level.
NUMCTGY	028	10	00	00000004	00	Int	The number of categories.
CATEGORY	029	80	00	00000002	00	Bin	A list of numbers corresponding to the categories to which this data set belongs.
NOTIFY	030	00	00	00000000	00	Char	User to be notified when access violations occur against a data set protected by this profile.
RETPD	031	00	00	00000000	00	Int	The number of days protection is provided for the data set. If used, the field is a two-byte binary number.
ACL2CNT	032	10	00	00000004	00	Int	The number of program and user combinations currently authorized to access the data set.

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
PROGRAM	033	80	00	00000008	00	Char	The name of a program currently authorized to access the data set, or a 1-byte flag followed by 7 bytes reserved for IBM's use.
USER2ACS	034	80	00	00000008	00	Char	User ID or group.
PROGACS	035	80	00	00000001	00	Bin	The access authority of the program and user combinations.
PACSCNT	036	80	00	00000002	00	Int	Access count.
ACL2VAR	037	80	00	00000000	00	Char	Additional conditional data, 9-byte length, in which the first byte tells what type of access is allowed and the remaining 8 bytes contain the data.
FLDCNT	038	10	00	00000004	00		Reserved for IBM's use.
FLDNAME	039	80	00	00000008	00		Reserved for IBM's use.
FLDVALUE	040	80	00	00000000	00		Reserved for IBM's use.
FLDFLAG	041	A0	00	00000001	00		Reserved for IBM's use.
VOLCNT	042	10	00	00000004	00	Int	The number of volumes containing the data set.
VOLSER	043	80	00	00000006	00	Char	A list of the serial numbers of the volumes containing the data set.
ACLCNT	044	10	00	00000004	00	Int	The number of users and groups currently authorized to access the data set.
USERID	045	80	00	00000008	00	Char	The user ID or group name of each user or group authorized to access the data set.
USERACS	046	A0	00	00000001	00	Bin	The access authority that each user or group has for the data set. **Bit** **Meaning when set** **0** ALTER access **1** CONTROL access **2** UPDATE access **3** READ access **4** EXECUTE access **5–6** Reserved for IBM's use **7** NONE access
ACSCNT	047	80	00	00000002	00	Int	The number of times the data set was accessed by each user or group.
USRCNT USRNM USRDATA USRFLG	048 049 050 051	10 80 80 A0	00 00 00 00	00000004 00000008 00000000 00000001	00 00 00 00	Int	Reserved for installation use. Reserved for installation use. Reserved for installation use. Reserved for installation use.
SECLABEL	052	00	00	00000008	00	Char	Security label.

Field name	Field ID	Flag 1	Flag 2	Combination field IDs					Type	
The following are the COMBINATION fields of the data set template.										
DEFDATE	000	40	00	004	000	000	000	000	Char	Combination.
AUTHDATE	000	40	00	004	000	000	000	000	Char	Fields.
OWNER	000	40	00	005	000	000	000	000	Char	
UACC	000	40	00	012	000	000	000	000		
ACL2	000	40	00	033	034	035	036	037		
ACL2A3	000	40	00	033	034	035	037	000		
ACL2A2	000	40	00	033	034	035	036	000		
ACL2A1	000	40	00	033	034	035	000	000		
FIELD	000	40	00	039	040	041	000	000		
VOLUME	000	40	00	043	000	000	000	000		
ACL	000	40	00	045	046	047	000	000		
ACL1	000	40	00	045	046	000	000	000		
USERDATA	000	40	00	049	050	051	000	000		

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
The following is the DFP segment of the data set template.							
DFP	001	00	00	00000000	00		Start of segment fields
RESOWNER	002	00	00	00000008	FF	Char	Resource owner; must represent a user ID or group name
DATAKEY	003	00	00	00000000	00	Char	CKDS label of default key

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
The following is the TME segment of the data set template.							
TME	001	00	00	00000000	00		Start of segment fields
ROLEN	002	10	00	00000004	00	Int	Count of role-access specifications
ROLES	003	80	00	00000000	00	Char	Role-access specifications

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
The following is the CSDATA segment of the data set template.							
CSDATA	001	00	00	00000000	00		Start of segment fields for custom fields. **Note:** Intended usage for these fields is dictated by your installation. See the *z/OS Security Server RACF Security Administrator's Guide* for more information on custom fields.
CSCNT	002	10	00	00000004	00	Char	Count of custom fields

Template							Field being described
Field name (character data)	**Field ID**	**Flag 1**	**Flag 2**	**Field length decimal**	**Default value**	**Type**	
CSTYPE	003	80	00	00000001	01	Char	Custom field type • 01 - character • 02 - numeric • 03 - flag • 04 - hex
CSKEY	0004	80	00	00000000	00	Char	Custom field keyword
CSVALUE	005	80	00	00000000	00	Char	Custom field value

Field name	**Field ID**	**Flag 1**	**Flag 2**	**Combination field IDs**					**Type**	
The following is a COMBINATION field of the CSDATA segment of the data set template.										
CSCDATA	000	40	00	003	004	005	000	000	Char	Combination field for custom fields

SMF

System management facilities (SMF) collects and records system and job-related information that to use in:

- Billing users
- Reporting reliability
- Analyzing the configuration
- Scheduling jobs
- Summarizing direct access volume activity
- Evaluating data set activity
- Profiling system resource use
- Maintaining system security

With the IBM Z Security and Compliance Center, you can automatically collect data from SMF Type 1154 Subtype 96 and 97 to check whether SMF is going to digitally sign the records that are being recorded for the log stream, check whether the SMF system identifier is set to the default value, and more.

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

z/OS UNIX

The z/OS UNIX System Services (z/OS UNIX) element is a UNIX operating environment implemented within the z/OS operating system. The z/OS support enables two open systems interfaces on the z/OS operating system: an application programming interface (API) and an interactive shell interface.

With the IBM Z Security and Compliance Center, you can automatically collect data from SMF Type 1154 Subtype 77 to check whether the LOGNAME environment variable is marked as read-only in /etc/profile file, check whether the umask variable is properly configured, and more.

For information about how to install, configure, deploy, and use the IBM Z Security and Compliance Center solution (program number 5655-CC1), see IBM Z Security and Compliance Center Guide (www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm).

Chapter 3. Simplified Auditing

CIS Benchmarks

What is a CIS Benchmark?

IBM has contributed to the IBM z/OS V2R5 with RACF Benchmark v1.0.0, which provides security best practices and guidance to clients and auditors. Consult system hardening guidelines for security configuration to understand how to audit and remediate your z/OS environment.

This benchmark is intended for system and application administrators, security specialists, auditors and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate IBM z/OS.

For more information, see CIS Benchmarks (www.cisecurity.org/cis-benchmarks/).

Chapter 4. Expedited Compliance

z/OS Exploitation of millicode counters

z/OS adds the following support for the exploitation of millicode counters.

SMF record updates

The following SMF record types were updated or added.

Record type 0

For SMF record type 0 (X'00') – IPL, the descriptions are updated for the SMF0RST and SMF0RS4K fields in the Header/self-defining section, and new fields are added at offsets 82 – 87.

Record type 30

For SMF record type 30 (X'1E') – Common address space work, the rules for SMF 30 continuation record processing are updated.

Rules for SMF type 30 continuation record processing: For all subtypes (except subtype 1), it is possible to have additional continuation records.

When the value in SMF30SOF is greater than 192 (X'C0'), the following record continuation rules apply:

- A record is a member of a group of continuation records if *any* of the following flags is on. A record is not a member of a group of continuation records if *all* of these flags are off.

  SMF30_RecCont_FirstRec
  SMF30_RecCont_AdditionalRec
  SMF30_RecCont_LastRec
- When a record is a member of a group of continuation records but not the last record in the group, the value in SMF30_Cont_Recs_To_Follow is the number of continuation records that follow the current record in the group. For the last record in the group of continuation records, SMF30_RecCont_LastRec is on and SMF30_Cont_Recs_To_Follow contains a value of zero.
- The contents of the SMF type 30 Identification section (DSECT SMF30ID) is the same for all records in a group of continuation records.

When the value in SMF30SOF is less than or equal to 192 (X'C0'), the following record continuation rules apply:

- A record is the *first record* if at least one of the following fields is non-zero:

  SMF30AON
  SMF30ARN
  SMF30CON
  SMF30DRN
  SMF30OON
  SMF30PON
  SMF30RON
  SMF30TON
  SMF30UON
- A record is an *additional record* if the following fields are all zero:

  SMF30AON
  SMF30ARN

SMF30CON
SMF30DRN
SMF30OON
SMF30PON
SMF30RON
SMF30TON
SMF30UON

- In either a *first* or *additional* record:
  - There are more records to follow if at least one of the following fields is non-zero:

    SMF30EOS
    SMF30MOS
    SMF30OPM
    SMF30RMS
    SMF30UDS
  - This is the *last record* if the following fields are all zero:

    SMF30EOS
    SMF30MOS
    SMF30OPM
    SMF30RMS
    SMF30UDS

For SMF record type 30 (X'1E') – Common address space work, fields at offsets 192 – 219 are added in the Header/self-defining section to locate the crypto counters and NNPI counters sections, and to indicate that a record is part of a continuation.

Offsets		Name	Length	Format	Description
0	0	SMF30LEN	2	binary	Record Length. This field along with the next, are referred to as the RDW (record descriptor word). See Standard SMF record header in *z/OS MVS System Management Facilities (SMF)* for a detailed description.
2	2	SMF30SEG	2	binary	Segment descriptor (see record length field).
4	4	SMF30FLG	1	binary	System indicator: **Bit** **Meaning when set** **0** Subsystem identification follows system identification **1** Subtypes used **2** Reserved **3-6** Version indicators (See Standard SMF record header in *z/OS MVS System Management Facilities (SMF)* for a detailed description.) **7** Reserved.
5	5	SMF30RTY	1	binary	Record type 30 (X'1E').
6	6	SMF30TME	4	binary	Time since midnight, in hundredths of a second, that the record was moved to the SMF buffer.

Offsets		Name	Length	Format	Description
10	A	SMF30DTE	4	packed	Date that the record was moved to the SMF buffer, in the form 0*cyydddF* (in local time). See Standard SMF record header in *z/OS MVS System Management Facilities (SMF)* for a detailed description.
14	E	SMF30SID	4	EBCDIC	System identification (from the SID parameter).
18	12	SMF30WID	4	EBCDIC	Work type indicator for the address space. The value identifies the type of address space that is being reported on (for example: “STC” for started tasks and system address spaces, “TSO” for TSO/E users, etc).
22	16	SMF30STP	2	binary	Record subtype. For a list of the record subtypes, see Record type 30 (X'1E') - Common address space work in *z/OS MVS System Management Facilities (SMF)*.
24	18	SMF30SOF	4	binary	Offset to subsystem section from start of record, including the record descriptor word (RDW).
28	1C	SMF30SLN	2	binary	Length of subsystem section.
30	1E	SMF30SON	2	binary	Number of subsystem sections.
32	20	SMF30IOF	4	binary	Offset to identification section from start of record, including the record descriptor word (RDW).
36	24	SMF30ILN	2	binary	Length of identification section.
38	26	SMF30ION	2	binary	Number of identification sections.
40	28	SMF30UOF	4	binary	Offset to I/O activity section from start of record, including the record descriptor word (RDW).
44	2C	SMF30ULN	2	binary	Length of I/O activity section.
46	2E	SMF30UON	2	binary	Number of I/O activity sections.
48	30	SMF30TOF	4	binary	Offset to completion section from start of record, including the record descriptor word (RDW).
52	34	SMF30TLN	2	binary	Length of completion section.
54	36	SMF30TON	2	binary	Number of completion sections.
56	38	SMF30COF	4	binary	Offset to processor section from start of record, including the record descriptor word (RDW).
60	3C	SMF30CLN	2	binary	Length of processor section.
62	3E	SMF30CON	2	binary	Number of processor sections.
64	40	SMF30AOF	4	binary	Offset to accounting section from start of record, including the record descriptor word (RDW).
68	44	SMF30ALN	2	binary	Total length of the single accounting section.
70	46	SMF30AON	2	binary	Number of variable length text segments.
72	48	SMF30ROF	4	binary	Offset to storage section from start of record, including the record descriptor word (RDW).
76	4C	SMF30RLN	2	binary	Length of storage section.
78	4E	SMF30RON	2	binary	Number of storage sections.
80	50	SMF30POF	4	binary	Offset to performance section from start of record, including the record descriptor word (RDW).
84	54	SMF30PLN	2	binary	Length of the performance section.
86	56	SMF30PON	2	binary	Number of performance sections.
88	58	SMF30OOF	4	binary	Offset to operator section from start of record, including the record descriptor word (RDW).
92	5C	SMF30OLN	2	binary	Length of the operator section.
94	5E	SMF30OON	2	binary	Number of operator sections.

Offsets		Name	Length	Format	Description
96	60	SMF30EOF	4	binary	Offset to the execute channel program (EXCP) section from start of record, including the record descriptor word (RDW).
100	64	SMF30ELN	2	binary	Length of the execute channel program (EXCP) section, in this record.
102	66	SMF30EON	2	binary	Number of execute channel program (EXCP) sections in this record.
104	68	SMF30EOR	2	binary	Number of execute channel program (EXCP) sections in subsequent records. When this number exceeds two bytes, it is not valid. See SMF30EOS for the correct value.
106	6A	SMF30RVD	2		Reserved.
108	6C	SMF30EOS	4	binary	Number of execute channel program (EXCP) sections in subsequent records.
112	70	SMF30DRO	4	binary	Offset to APPC/MVS resource section from start of record, including the record descriptor word (RDW).
116	74	SMF30DRL	2	binary	Length of APPC/MVS resource section.
118	76	SMF30DRN	2	binary	Number of APPC/MVS resource sections in this record (this number is 0 or 1).
120	78	SMF30ARO	4	binary	Offset to APPC/MVS cumulative resource section from start of record, including the record descriptor word (RDW).
124	7C	SMF30ARL	2	binary	Length of APPC/MVS cumulative resource section.
126	7E	SMF30ARN	2	binary	Number of APPC/MVS cumulative resource sections in this record (this number is 0 or 1).
128	80	SMF30OPO	4	binary	Offset to OpenMVS process section.
132	84	SMF30OPL	2	binary	Length of z/OS UNIX process section.
134	86	SMF30OPN	2	binary	Number of z/OS UNIX process sections on current record.
136	88	SMF30OPM	4	binary	Number of z/OS UNIX process sections on subsequent records.
140	8C	SMF30UDO	4	binary	Offset to first usage data section from the start of the record, including the record descriptor word (RDW).
144	90	SMF30UDL	2	binary	Length of each usage data section - ‘76’.
146	92	SMF30UDN	2	binary	Number of usage data sections in this record.
148	94	SMF30UDS	4	binary	Number of usage data sections in subsequent records.
152	98	SMF30RMO	4	binary	Offset to first automatic restart management section.
156	9C	SMF30RML	2	binary	Length of automatic restart management section.
158	9E	SMF30RMN	2	binary	Number of automatic restart management sections.
160	A0	SMF30RMS	4	binary	Number of automatic restart management sections in subsequent records.
164	A4	SMF30MOF	4	binary	Offset to the Multisystem Enclave Remote Data section.
168	A8	SMF30MLN	2	binary	Length of MultiSystem Enclave Remote System Data section.
170	AA	SMF30MNO	2	binary	Number of MultiSystem Enclave Remote System Data sections in this record.
172	AC	SMF30MOS	4	binary	Number of MultiSystem Enclave Remote System Data sections in subsequent records.

Offsets		Name	Length	Format	Description
176	B0	SMF30CDO	4	binary	Offset to the Counter Data Section.
180	B4	SMF30CDL	2	binary	Length of a Counter Data Section.
182	B6	SMF30CDN	2	binary	Number of Counter Data Sections.
184	B8	SMF30USO	4	binary	Offset to the zEDC usage statistics section.
188	BC	SMF30USL	2	binary	Length of the zEDC usage statistics section.
190	BE	SMF30USN	2	binary	Number of zEDC usage statistics sections.
192	C0	SMF30RPS_End_V1	0	n/a	End of version 1.
192	C0	SMF30CPO	4	binary	Offset to the first crypto counters section.
196	C4	SMF30CPL	2	binary	Length of a crypto counters section.
198	C6	SMF30CPN	2	binary	Number of crypto counters sections.
200	C8	SMF30CPA	4	binary	Number of crypto counters sections in subsequent (continuation) records.
204	CC	SMF30NPO	4	binary	Offset to the first NNPI counters section.
208	D0	SMF30NPL	2	binary	Length of a NNPI counters section.
210	D2	SMF30NPN	2	binary	Number of NNPI counters sections.
212	D4	SMF30NPA	4	binary	Number of NNPI counters sections in subsequent (continuation) records.
216	D8	SMF30_Record_Continuation_Info	3	binary	Record continuation information.
216	D8	SMF30_Cont_Recs_To_Follow	2	binary	The number of continuation records to follow this record. When SMF30_RecCont_LastRec is on, this field will be zero.
218	DA	SMF30_RecCont_Flags	1	binary	Record continuation flags: **Bit** **Meaning when set** **0 (SMF30_RecCont_FirstRec)** This record is the first of a set of two or more continuation records. **1 (SMF30_RecCont_AdditionalRec)** This record is the second or subsequent, but not last, record in a set of three or more continuation records. **2 (SMF30_RecCont_LastRec)** This record is the last of a set of two or more continuation records. **3 - 7** Reserved.
219	DB	SMF30RPS_End_V2	0	n/a	End of version 2.

For SMF record type 30 (X'1E') – Common address space work, new bits are defined within SMF30PFlags in the Subsystem section to indicate that crypto counters and NNPI counters are active.

Offsets		Name	Length	Format	Description
0	0	SMF30TYP	2	binary	Subtype identification **Value** **Meaning** **1** Job start or start of other work unit. **2** Activity since previous interval ended. Produced only when interval recording is active. **3** Activity for the last interval before step termination. Produced only when interval recording is active. **4** Step total **5** Job termination or termination of other work unit. **6** System address space.
2	2	SMF30RS1	1		Reserved.
3	3	SMF30PFlags	1	binary	Product flags. **Bit** **Meaning when set** **0** Reserved. **1 (SMF30_CrypCtrs_Active)** Indicates that crypto counter processing is active. **2 (SMF30_NNPICtrs_Active)** Indicates that NNPI counter processing is active **3 - 7** Reserved.
4	4	SMF30RVN	2	EBCDIC	Record version number **Value** **Meaning** **'05'** MVS/SP Version 5 **'04'** MVS/SP Version 4 **'03'** MVS/SP Version 3 **'02'** MVS/SP Version 2 **'01'** VS2
6	6	SMF30PNM	8	EBCDIC	Subsystem or product name, for example SMF.
14	E	SMF30OSL	8	EBCDIC	Code string for the operating system level to represent the version, release, and modification level, as described for CVTPRODN. Guaranteed to be larger in each release.
22	16	SMF30SYN	8	EBCDIC	System name (from the SYSNAME parameter in the IEASYSxx parmlib member).
30	1E	SMF30SYP	8	EBCDIC	Sysplex name (from the SYSPLEX parameter in the COUPLExx parmlib member).

For SMF record type 30 (X'1E') – Common address space work, the crypto counters section and the NNPI counters section are added.

Crypto counters section

The Crypto counters sections contain the counters for the CPACF cryptographic instructions used by a job for the period that the record represents. These sections are produced only for those instructions that are used. The IFASMFCN macro contains equates and meanings for the counter entry ID values in SMF30_CrypCtrs_Entry_ID. The names of the equates start with SMF_CrypCtrs.

Note: SMF is unable to report the use of instructions by the Linux environment within zCX. This means that the use of these instructions by an application running within a zCX instance will not be included in this section.

Triplet information: This section is located in the record using the following triplet fields, which are located in "Header/self-defining section":

Offset
SMF30CPO

Length
SMF30CPL

Number
SMF30CPN - Reports the number of sections in the current record. SMF30CPA reports the number of sections in subsequent SMF type 30 records.

Offsets		Name	Length	Format	Description
0	0	SMF30_CrypCtrs_Entry_ID	2	binary	Crypto counter entry identifier.
2	2	SMF30_CrypCtrs_Count	8	binary	Crypto counter count value. This field contains the instruction counts used within the scope of the record, either for the current interval, job step, or job.

NNPI counters section

The NNPI counters sections contain the counters for the NNPA instructions used by a job for the period that the record represents. These sections are produced only for those instructions that are used. The IFASMFCN macro contains equates and meanings for the counter entry ID values in SMF30_NNPICtrs_Entry_ID. The names of the equates start with SMF_NNPICtrs.

Note: SMF is unable to report the use of instructions by the Linux environment within zCX. This means that the use of these instructions by an application running within a zCX instance will not be included in this section.

Triplet information: This section is located in the record using the following triplet fields, which are located in "Header/self-defining section":

Offset
SMF30NPO

Length
SMF30NPL

Number
SMF30NPN - Reports the number of sections in the current record. SMF30NPA reports the number of sections in subsequent SMF type 30 records.

Offsets		Name	Length	Format	Description
0	0	SMF30_NNPICtrs_Entry_ID	2	binary	NNPI counters entry identifier
2	2	SMF30_NNPICtrs_Count	8	binary	NNPI counter count value. This field contains the instruction counts used within the scope of the record, either for the current interval, job step, or job.

START command

The START IEACTRS command was added.

Starting and stopping crypto counter set processing (IEACTRS)

Use the START IEACTRS command to control the state of crypto counter set processing.

The command with CRYPTO={ACTIVE|INACTIVE} will not be successful when run on a machine that does not support crypto counters or when MACHMIG CRYPCTRS is specified in LOADxx.

Syntax

The command syntax is:

```
S IEACTRS[,CRYPTO={UNCHANGED|ACTIVE|INACTIVE}]
```

Parameters

The parameters are:

IEACTRS
The name of the started procedure used to control crypto counter set processing.

CRYPTO=UNCHANGED
Specifies not to change the state of the crypto counters. This is the default.

CRYPTO=ACTIVE
On a machine that supports the crypto counter set, specifies that crypto counter set processing is to be set active, both for existing and new jobs or started tasks.

CRYPTO=INACTIVE
Specifies that crypto counter set processing is to be set inactive as of this point. No further crypto counter set processing is to be done.

Authorization

For IEACTRS with the CRYPTO={ACTIVE|INACTIVE} parameter, the command issuer must have UPDATE (or higher) authority to the IEACTRS.CRYPTO.*crypto_operand* resource in the FACILITY class. A matching profile must exist and the user ID being checked must not be *BYPASS*. (The *BYPASS* user ID is used for commands that are issued from MCS, HMCS, or SMCS consoles where an operator has not logged on to the console.)

Return codes

The return codes from the IEACTRS procedure are:

0
Success

4
Request for ACTIVE or INACTIVE ignored (either the machine does not support the counter set or MACHMIG CRYPCTRS is in effect)

8
Syntax error

12
Not authorized

16
System error

PARMLIB changes

The CRYPCTRS parameter was added in IEASYSxx, and the MACHMIG parameter in LOADxx was updated with CRYPCTRS and NNPICTRS facilities.

CRYPCTRS

CRYPCTRS={SYSTEM | ACTIVE | INACTIVE}

This parameter identifies the processing state for crypto counters.

CRYPCTRS=SYSTEM

This is the default. Same as CRYPCTRS=ACTIVE when the machine supports crypto counters; same as CRYPCTRS=INACTIVE when the machine does not support crypto counters.

CRYPCTRS=ACTIVE

When the machine supports crypto counters, crypto counters are initially active. Counting can be deactivated later by use of the START IEACTRS,CRYPTO=INACTIVE command. When the machine does not support crypto counters, this is the same as CRYPCTRS=INACTIVE.

CRYPCTRS=INACTIVE

Crypto counters are initially inactive. When the machine supports crypto counters, counting can be activated later by use of the START IEACTRS,CRYPTO=ACTIVE command. When the machine does not support crypto counters, no processing is done for the crypto counters.

When MACHMIG CRYPCTRS is specified in the LOAD*xx* member of parmlib, crypto counter processing will be treated as if the machine does not support crypto counters. When the MACHMIG CRYPCTRS parameter is used, the crypto counter set is never activated for this IPL. No processing is done related to crypto counters, and no storage is obtained for counter sets as is done for CRYPCTRS={ACTIVE | INACTIVE}. Any request to activate the crypto counters is rejected or ignored.

Value range: Not applicable

Default: CRYPCTRS=SYSTEM

Associated parmlib member: None

Statements and parameters for LOADxx

MACHMIG

Identifies one or more facilities that you do not want z/OS to use at this time because migration to another processor, z/OS release, or both is underway. Code the MACHMIG statement as described in Table 54 on page 157.

Table 54. MACHMIG statement

Column	Contents
1-7	MACHMIG

Table 54. MACHMIG statement (continued)

Column	Contents
10-72	A list of facilities not to use. When more than one facility is listed, separate each from the previous by one or more blanks or commas. The following facilities can be specified in upper, lower, or mixed case: • EDAT2 (the hardware-based enhanced-DAT facility 2) • TX (the hardware-based transactional-execution facility) This option is ignored as of z/OS V2R4. The facility will be used even if this is specified. z/OS V2R4 requires availability of the transactional-execution facility. • RI (a hardware-based facility that is reserved for IBM use only) • VEF (the hardware-based vector extension facility) This option is ignored as of z/OS V2R5. The facility will be used even if this is specified. z/OS V2R5 requires availability of the vector extension facility. • GSF (the hardware-based Guarded Storage Facility) • CRYPCTRS (the hardware-based crypto counter facility). This option also implies that the hardware-based NNPI counter facility will not be used. • NNPICTRS (the hardware-based NNPI counter facility)

This example shows a MACHMIG statement that tells the system not to use the enhanced DAT facility 2.

```
*
*---+----1----+----2----+----3----+----4----+----5----+----6----+----7--
MACHMIG  EDAT2
*
```

There is no default. If you do not specify a MACHMIG statement, the system does not limit its exploitation of machine facilities.

Messages

The following messages were added:

IEA700I IEACTRS request successful

Explanation

In response to the START IEACTRS command, the requested processing completed successfully.

System action

The system completed the request.

Operator response

None.

Source

Supervisor Control

Module

Supervisor Control

Routing code

*

Descriptor code

5

IEA701I IEACTRS {Request | CRYPTO request} unsuccessful - {syntax error | not authorized | no change allowed}

Explanation

In response to the START IEACTRS command, the processing did not complete successfully. The message text will contain one of:

- Request unsuccessful - syntax error
- Crypto request unsuccessful - not authorized
- Crypto request unsuccessful - no change allowed

System action

The system did not complete the request.

Operator response

Notify the system programmer.

System programmer response

When “syntax error”, have the operator provide a valid option and try the request again.

When “not authorized”, make sure the operator has UPDATE authority to FACILITY class entity IEACTRS.CRYPTO.crypto_operand and then have the operator try the request again.

When “no change allowed”, avoid using START IEACTRS,CRYPTO={ACTIVE | INACTIVE} when on a machine that does not support CRYPCTRS or when MACHMIG CRYPCTRS (via LOAD*xx*) is in effect.

Source

Supervisor Control

Module

Supervisor Control

Routing code

*

Descriptor code

5

IEE261I CRYPCTRS State: *state*

Explanation

The DISPLAY IPLINFO,CRYPCTRS,STATE command completed.

In the message text:

state
The current state of the crypto counter set, based on the CRYPCTRS system parameter and the START IEACTRS,CRYPTO= command, where *state* is one of the following values:

Active
Specified or defaulted by the system parameter or modified by the START IEACTRS,CRYPTO=ACTIVE command.

Inactive
Specified by the CRYPCTRS system parameter or modified by the START IEACTRS,CRYPTO=INACTIVE command.

Never
Either the machine does not support the counters or MACHMIG CRYPCTRS (via LOAD*xx*) is in effect.

The original specification can by viewed by the DISPLAY IPLINFO,*sysparm* command.

System action

The system continues.

Operator response

None required.

System programmer response

None required.

Source

Supervisor Control

Module

Supervisor Control

Routing code

*

Descriptor code

5

Appendix A. Accessibility

Accessible publications for this product are offered through IBM Documentation (www.ibm.com/docs/en/zos).

If you experience difficulty with the accessibility of any z/OS information, send a detailed message to the Contact the z/OS team web page (www.ibm.com/systems/campaignmail/z/zos/contact_z) 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

Notices

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 IBM Documentation. 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

Poughkeepsie, NY 12601-5400
USA

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 DFSMSdfp, 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

T

U

Z

Product Number: 5650-ZOS