

z/OS 2.5 Security Updates session - 83688

Julie Bergh

Cyber Security Architect

Sirius a CDW Company

Julie.bergh@siriuscom.com

Julie.bergh@cdw.com



Z/OSMF

z/OSMF

- z/OSMF Security Configuration Assistant is enhanced to support variables so that more security configuration checking can be validated automatically.
- This is designed to reduce the number of manual actions reported by the assistant.
- With the PTF for APAR PH17871, this enhancement is also available on z/OS V2.3 and later.

- The z/OSMF Security Configuration Assistant (SCA) plug-in is enhanced to support z/OS components, features, and products. Previously, the SCA was only able to give detailed information to a system programmer about the missing security rules for the z/OSMF component.
- In z/OS V2.5, this capability is extended to any piece of software.
- An easy-to-create JSON file can be provided by the exploiting software that defines the security requirements. A properly permitted system programmer or the security administrator can run this plug-in and see in one list all the security rules that are missing and what that might mean.

- The SCA is designed to help system programmers to understand security requirements of specific functions and to quickly identify the function failure that would be caused by the incorrect security setup.
- Used as a vehicle to communicate between system programmers and security administrators, this information can improve the time to value for software on z/OS.
- Several of the z/OS V2.5 DFSMS features are among the first exploiters of this function because they provide security JSON descriptor files that can be imported to SCA. With the PTF for APAR PH29907, this enhancement is available on z/OS V2.3 and later.

z/osmf

- **Log in to the z/OSMF server**
- You can use the POST method to log in to the z/OSMF server and obtain authentication tokens. This service creates a JSON Web Token, an LTPA token, or both, and returns the tokens to the requester.
- **Change the user password or passphrase**
- You can use a PUT request to change a user password or password phrase (passphrase). This service is available when you install the PTF for APAR PH34912.
- **Log out of the z/OSMF server**
- You can use the DELETE method to log out of the z/OSMF server and delete the user's authentication tokens (JSON Web Tokens and LTPA tokens). Your request cookie must include a valid JSON Web Token or LTPA token (or both).

Security Configuration Assistant task

Security Configuration Assistant


Validate for user ID Validate all

Please input a valid user id.

Security Configuration Assistant Nucleus Services Ad

Automated

Resources for z/OSMF Sysplex Management service	Description
IZUDFLT.ZOSMF.SYSPLEX	Allows the use
IZUDFLT.ZOSMF.SYSPLEX.MODIFY	Allows the use
IZUDFLT.ZOSMF.SYSPLEX.LOG	Allows the use

 ✕

ID *ADCDMST.* 8/10/20, 1:36 PM

IZUSA0002I Validation processing completed for user ✕
ID *IBMUSER.* 8/10/20, 1:40 PM

IZUSA0011E The requested user ID *johnwd* either does ✕
not exist or is not authorized to z/OSMF. 8/10/20, 1:41 PM

Close Clear

Security Configuration Assistant task

Security Configuration Assistant

Validate for user ID

Please input a valid user id.

[IZUSA0011E](#) The requested user ID *testjb* either does not exist or is not authorized to z/OSMF.

Security Configuration Assistant Nucleus Services **Advanced Configuration**

Passed Failed Unknown

Security Configuration Assistant task

- Security Configuration Assistant – Graphic view to display automatic validation result

Validation is done per user

- Validation can be done against
- All z/OSMF security configuration
 - Selected services
 - One specific security requirement

The screenshot shows the Security Configuration Assistant interface for user 'debug1'. It features a 'Validate all' button and tabs for 'Nucleus', 'Services 31', and 'Advanced Configuration 24'. A donut chart provides an overview of validation results: 23 Passed (green), 3 Failed (red), and 0 Unknown (grey). Below the chart, a table lists services and their validation status. A detailed table at the bottom shows 'Resources for z/OSMF Notifications' with columns for Description, Class, Who needs the access, Required Access, Validated User ID, Validation Result, and Action.

Resources for z/OSMF Notifications	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
IZUP03SF.ZOSMF.NOTIFICATION.SETTINGS	Allows the user to view the Notification Settings task.	ZMFAPLA	IZUUSER IZUADMIN	READ	debug1	Passed	Refresh
IZUP03SF.ZOSMF.NOTIFICATION.SETTINGS.ADMIN	Allows the user to modify the notification settings.	ZMFAPLA	IZUADMIN	READ	debug1	Passed	Refresh
IZUP03SF.ZOSMF.NOTIFICATION.MODIFY	Allows the user to send a notification.	ZMFAPLA	IZUUSER IZUADMIN	READ	debug1	Passed	Refresh
IRR.RUSERMAP	Allows notification settings task to get the user's email address configured to RACF.	FACILITY	IZUUSER IZUADMIN	READ	debug1	Failed	Refresh

Align with z/OSMF Lite configuration

Overview of validation result

Validation result by service

Validation result by specific requirement

Description is included for each security requirement

Security Configuration Assistant task

Validate for user ID

adcdmst

Validate all












Filters ▾

Security Configuration Assistant

Nucleus

Services **13**

Advanced Configuration **2**

Resources for z/OSMF Liberty Server	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
BBG.ANGEL.IZUANG1	Allow the z/OSMF server to access the angel process.	SERVER	IZUSVR	READ	IZUSVR	Passed	
BBG.AUTHMOD.BBGZSAFM	Enable z/OSMF server to use the z/OS Authorized services.	SERVER	IZUSVR	READ	IZUSVR	Passed	
BBG.AUTHMOD.BBGZSAFM.SAFCRED	To enable the SAF authorized user registry services and SAF authorization services(SAFCRED).	SERVER	IZUSVR	READ	IZUSVR	Passed	
BBG.AUTHMOD.BBGZSAFM.ZOSWLM	To enable the WLM services(ZOSWLM).	SERVER	IZUSVR	READ	IZUSVR	Passed	
BBG.AUTHMOD.BBGZSAFM.TXRRS	To enable the RRS transaction services(TXRRS).	SERVER	IZUSVR	READ	IZUSVR	Passed	
BBG.AUTHMOD.BBGZSAFM.ZOSDUMP	To enable the SVCDUMP services(ZOSDUMP).	SERVER	IZUSVR	READ	IZUSVR	Passed	
BBG.SECPFY.IZUDFLT	Allow the z/OSMF server to make authentication calls against the APPL-ID.	SERVER	IZUSVR	READ	IZUSVR	Passed	
BBG.SECCLASS.ZMFAPLA	Allow the z/OSMF server to authorize checks for the ZMFAPLA class.	SERVER	IZUSVR	READ	IZUSVR	Passed	
BBG.SYNC.IZUDFLT	Allow the z/OSMF server to authorize checks for the ZMFACLOUD class.	FACILITY	IZUSVR	CONTROL	IZUSVR	Passed	
BPX.WLMSEVER	Allows the z/OSMF server to use WLM functions to create and manage work requests.	FACILITY	IZUSVR	READ	IZUSVR	Passed	
BPX.CONSOLE	Allow the user to filter z/OS UNIX messages. Specifically, this setting suppresses the BPXM023I message prefix from any write-to-operator (WTO) messages that z/OSMF writes to the console.	FACILITY	IZUSVR	READ	IZUSVR	Passed	



DATA PRIVACY FOR DIAGNOSTICS

Data Privacy for Diagnostics

- Additional support for Data Privacy for Diagnostics, a z/OS security function that is available on IBM z15 to help clients maintain control when working with third party vendors by redacting data tagged as sensitive and creating a redacted diagnostic dump that can be shared externally. z/OS Diagnostics Analyzer, a new enhancement for Data Privacy for Diagnostics, is generally available and enhances sensitive data tagging and redaction in system dumps by enabling clients to customize sensitive data patterns that are unique to their organization.
- Data Privacy for Diagnostics helps clients improve their capability to address compliance challenges in the area of diagnostic data without compromising on serviceability.

Data Privacy for Diagnostics

- Supports redacting sensitive user data in dumps
- Mark sensitive memory areas and remove from a dump before sending to IBM or a vendor
- Supported for SYSMDUMP and TDUMP
- New options on z/OS API's to tag known sensitive memory areas
- New optional post-processing step will remove previously tagged sensitive pages, and new z/OS Diagnostics Analyzer will detect and redact additional sensitive data in untagged pages
- All intended to be done without impacting the dump capture time.
- Required and available maintenance for Data Privacy for Diagnostics:



PERVASIVE ENCRYPTION

Pervasive Encryption

- Pervasive Encryption simplification.
- Most notable is the support for additional z/OS data set types, including sequential basic format and large format System Managed Storage (SMS)-managed data sets.
- In most instances, clients are able to encrypt data without application changes and simplify the task of compliance.
- Applications using Execute Channel Program (EXCP) are supported with an access method encryption macro designed to enable programmers to change EXCP programs to read and write data sets that are compatible with encryption by IBM Basic Sequential Access Method (BSAM) and IBM Queued Sequential Access Method (QSAM).

Pervasive Encryption

- Encryption of basic and large format data sets, whether by an access method or EXCP, is designed to enable the installation to specify data sets to be encrypted through a policy such as IBM System Authorization Facility (SAF) or SMS, or manually.
- The data remains encrypted during administrative functions such as backup and restore, migration and recall, and replication.

Pervasive Encryption

- Read-only archive key support
 - Enables restricting the use of old keys from encrypting new data
 - Encrypted data can still be accessed but avoid creating new encrypted data with the archived key
-
- After installing PTFs for OA61207/OA61208, users can exploit the XFACILIT class resource, CSF.KDS.KEY.ARCHIVE.DATA.DECRYPT for encrypted VSAM data sets. This facility class indicates that data sets with archived encryption keys are only to be used for decryption operations. If defined, an open for output of an encrypted VSAM data set with an archived key will fail. This will result in an IEC161I 067 error message.



ZERT

zERT

- z/OS Encryption Readiness Technology (zERT) is enhanced to provide policy based enforcement of local network cryptography requirements.
- When TCP connections match user-defined zERT enforcement rules, you can obtain immediate notification of questionable or unacceptable network cryptographic protection through messages, SMF audit records, and even automatic termination of connections.



Z/OS AUTHORIZED CODE SCANNER

z/OS Authorized Code Scanner

- Support for an optional priced feature called z/OS Authorized Code Scanner, which dynamically scans a client's authorized code and provides diagnostic information for subsequent investigation to help support clients in their effort to strengthen the security posture of the z/OS development and test pipeline.
- The IBM z/OS Authorized Code Scanner is an optional priced feature of z/OS that provides automated system integrity testing in a dev/test environment as part of DevSecOpsmodernization. It scans for Program Calls (PCs) and Supervisor Calls (SVCs) available to all address spaces on a z/OS image and generates a series of tests that dynamically scan them for integrity.
- The output of this scan provides in-depth diagnostics whenever a potential vulnerability is found to facilitate remediation in order to further strengthen the security posture of the client's configuration of z/OS.



SDSF

SDSF

- As previously announced, SDSF requires configuration with SAF security. To that end, a new security migration guide is provided along with a REXX exec ISFACR to assist in migration to SAF security.

SDSF panels added in z/OS 2.2 & z/OS 2.3

APF Data Sets (APF)
Address Space Storage (AS)
Page Data Sets (PAG)
z/OS Parmlib Data Sets (PARM)
CF Connections (CFC)
CF Structures (CFS)
Device Activity (DEV)
z/OS Unix File Systems (FS)
Generic Tracker (GT)
Network Activity (NA)
SMS Storage Groups (SMSG)
Linklist Data Sets (LNK)
LPA List Data Sets (LPA)
Jobstep Information (JS)
JES2 Proclib Data Sets (PROC)
SMS Volumes (SMSV)
Subsystems (SSI)
Common Storage Remaining (CSR)
Virtual Storage Map (VMAP)
Job Modules (JC)
Job Tasks (JT)
Search Data Set Lists (SRCH)

SDSF Panels added in z/OS 2.4

- EMCS Extended Consoles
- ENQD Data Set Enqueues
- JES JES Subsystems
- JRI JES2 Resource Information
- JRJ JES2 Resource Usage By Jobname
- RMA JES2 Resource Monitor Alerts
- LPD Link Pack Directory
- OMVS z/OS Unix Options
- REPC WLM Report Classes
- RGRP WLM Resource Groups
- SRVC WLM Service Classes
- WKLD WLM Workloads
- WLM WLM Policy
- XCFM XCF Groups and Members

SDSF Panels added in z/OS 2.5

- AD Address Space Diagnostics
- CFD Coupling Facility Dataset
- CS Common Storage subpools
- LLS Link List Sets
- MEM Address Space Memory
- PC PC routines
- SYSP System Parameters
- SVC SVC routines

SDSF – Health Checker

```
-----  
SDSF OUTPUT DISPLAY SDSF_CLASS_SDSF_ACTIVE          LINE 0          COLUMNS 02- 81  
COMMAND INPUT ==>                                SCROLL ==> CSR  
***** TOP OF DATA *****  
CHECK( IBMSDSF,SDSF_CLASS_SDSF_ACTIVE)  
SYSPLEX:      ADCDPL      SYSTEM: S0W1  
START TIME: 04/15/2021 16:30:46.827342  
CHECK DATE: 20080324  CHECK SEVERITY: LOW  
  
ISFH1015I The class SDSF is active.  
  
END TIME: 04/15/2021 16:30:46.856328  STATUS: SUCCESSFUL
```

SDSF – Health Checker

***** TOP OF DATA *****

CHECK(IBMSDSF,SDSF_ISFPARMS_IN_USE)

SYSPLEX: ADCDPL SYSTEM: S0W1

START TIME: 04/15/2021 16:30:46.831880

CHECK DATE: 20170105 CHECK SEVERITY: LOW

ISFH1001I SDSF server SDSF is using statements from member ISFPRM00 of
data set ADCD.Z24A.PARMLIB.

END TIME: 04/15/2021 16:30:46.864591 STATUS: SUCCESSFUL

***** BOTTOM OF DATA *****

RACF / ACF2 / TSS Class

- **JESSPOOL**
- **LOGSTRM**
- **OPERCMD5**
- **SDSF**
- **WRITER**
- **XFACILIT**



RACF

- **Certificate fingerprint support**
 - z/OS V2.5 provides support to display the certificate fingerprint in the RACF DB
- **RACDCERT** command and store them in SMF records that handle certificates, as well as display and search for the certificate fingerprint through PKI Services web pages and store them in SMF records that handle certificates. The certificate fingerprint support helps to improve security policy management and implementation using certificates.

RACF

- RACF Enhanced PassTicketSupport
- z/OS V2.5 adds additional RACF PassTicketSupport. This includes:
 - Stronger cryptographic algorithm
 - Configurable expiration time
 - Optionally Expanded character set
 - Improved diagnostics
 - Recording to SMF
 - Co-existence and Migration

- **RACF Support for Restricted Profile Management**
- z/OS V2.5 Includes a new installation option to limit a user who has ALTER access to a discrete profile from changing the profile
- This is intended to separate profile management from the access rights that a profile represents which should improve compliance.
- The security administrator can be further in control of the security of the system and allow the user to retain control over everything else about the data

RACF

- **RACF VSAM Data Set**
- **Description:** The RACF VSAM Data Set function gives clients the option of using a VSAM linear data set as the a RACF data set in certain configurations.

RACF

- RACF has added a number of new health checks to help clients implement stronger security controls by adding a check to confirm that:
- All data sets are protected by RACF by implementing the SETROPTS
 - PROTECTALL(FAILURES) option
- Residual information is erased when data sets are deleted by implementing the
 - SETROPTS ERASE(ALL) option
- PassTicket keys are encrypted and stored in ICSF
- The RACF subsystem address space is active
- Either RACF sysplex communication mode or RACF data-sharing mode is active

RACF

- **CHECK (IBMRACF , RACF_PROTECTALL_FAIL)**
- **SYSPLEX: SESG SYSTEM: TST1**
- **START TIME: 03/22/2022 14:39:59.631117**
- **CHECK DATE: 20190520 CHECK SEVERITY: MEDIUM**
-
- **IRRH332I SETROPTS PROTECTALL(FAIL) is in effect.**
- **RCVTPRO = 1 RCVTPROF = 0**
-
- **END TIME: 03/22/2022 14:39:59.632389 STATUS: SUCCESSFUL**

RACF

RACF Health Checks

Description: New RACF Health Checks have been added:

Security Server (RACF)

74 z/OS: z/OS Introduction and Release Guide

- RACF_PROTECTALL_FAIL check will alert clients to disallow access when there is no rule which allows access.
- RACF_ERASE_ALL check will alert clients when data is CHECK (IBMRACF , RACF_ERASE_ON_SCRATCH)

```
SYSPLEX:      SESG      SYSTEM: TST1
START TIME: 03/22/2022 14:39:59.630911
CHECK DATE: 20190614  CHECK SEVERITY: MEDIUM
```

* Medium Severity Exception *

```
IRRH335E SETROPTS NOERASE is in effect.
```

Explanation: The RACF_ERASE_ON_SCRATCH check has determined that SETROPTS NOERASE is in effect. IBM recommends that all data set space which is freed during a SCRATCH or RELEASE operation be erased. This prevents the inadvertent disclosure of this data and can be enabled with RACF's SETROPTS ERASE(ALL) command.

```
RCVTEOS = 0 RCVTEOSL = 0 RCVTEOSA = 0
```

RACF

- CHECK(IBMTRACF,RACF_PTKTDATA_CLASS)
- SYSPLEX: SESG SYSTEM: TST1
- START TIME: 03/22/2022 14:40:00.856060
- CHECK DATE: 20200701 CHECK SEVERITY: MEDIUM
-
- * Medium Severity Exception *
-
- IRRH347E The user ID associated with the IBM Health Checker for z/OS
- address space does not have the SPECIAL, AUDITOR, or ROAUDIT
- attribute. IBM recommends the ROAUDIT attribute.
-
- Explanation: The RACF_PTKTDATA_CLASS check cannot verify that all
- Passticket keys are stored in ICSF as the health checker address
- space does not have the SPECIAL, AUDIT, or ROAUDIT attribute. IBM
- recommends the ROAUDIT attribute.
-
- System Action: The check continues processing. There is no effect on the system.
-
-
- System Programmer Response: Determine the user ID that is assigned
- to the IBM Health Checker for z/OS address space. Inform the RACF
- administrator that the user ID must have the SPECIAL, AUDITOR, or
- ROAUDIT attribute. IBM recommends the ROAUDIT attribute.
-
- Check Reason: IBM recommends using ICSF to encrypt Passticket keys.
-
- END TIME: 03/22/2022 14:40:00.857849 STATUS: EXCEPTION-MED

RACF

- **RACF_SENSITIVE_RESOURCES**
- **Description:** The RACF_SENSITIVE_RESOURCES check examines the security characteristics of several system-critical data sets and general resources other than data sets. The output of this check is a list of exceptions flagged.
- For each of these, the check examines:
 - For system-critical data sets, that the data set exists on the expected volume. If the data set does not exist on the volume, a V (volume exception) is placed in the Status (S) column.
 - That the resource has baseline protection. For example, APF data sets can have a general access as high as READ, while the data sets which comprise the RACF data base must have a general access of NONE.
 - The check verifies the protection of each resource by extracting its covering profile in its Class and examining the UACC, WARNING status, and the ID(*) entry in the access list if one exists. This extract does not take into account things like a GLOBAL profile or alterations by an exit. In addition, if there is no covering profile protecting a data set, then if NOPROTECTALL or PROTECTALL(WARN) is in effect, the check flags the data set as an exception. The customer can optionally specify a user ID to the check which, if specified, is used to perform a RACF authorization check for the next higher access authority after the highest expected general access authority.
- Some resources are “discrete resources”, that is, the resource name

RACF

Profiles with Maximum Public Access of NONE	
CLASS	PROFILE
FACILITY	BPX.DAEMON
FACILITY	BPX.DEBUG
FACILITY	BPX.FILEATTR.APF
FACILITY	BPX.FILEATTR.PROGCTL
FACILITY	BPX.SERVER
FACILITY	BPX.SUPERUSER
FACILITY	BPX.WLMSERVER
FACILITY	ICHBLP
FACILITY	IEAABD.DMPAKEY
FACILITY	IEAABD.DMPAUTH
FACILITY	IRR.PASSWORD.RESET
TSOAUTH	ACCT
TSOAUTH	CONSOLE
TSOAUTH	OPER
TSOAUTH	PARMLIB
TSOAUTH	TESTAUTH
UNIXPRIV	SUPERUSER.FILESYS
UNIXPRIV	SUPERUSER.FILESYS.CHANGEPERMS
UNIXPRIV	SUPERUSER.FILESYS.CHOWN
UNIXPRIV	SUPERUSER.PROCESS.GETPSENT
UNIXPRIV	SUPERUSER.PROCESS.KILL
UNIXPRIV	SUPERUSER.PROCESS.PTRACE

RACF

Profiles with Maximum Public Access of READ	
Class	Profile
OPERCMDS	MVS.SET.PROG
OPERCMDS	MVS.SETPROG
OPERCMDS	MVS.SLIP
OPERCMDS	MVS.HALT.EOD
OPERCMDS	MVS.HALT.NET
UNIXPRIV	SUPERUSER.FILESYS.MOUNT



ICSF

- In z/OS V2.5, ICSF supports the following:
- Updates to the key data sets to enable storage of larger keys, such as the Dilithium algorithm asymmetric keys
- Improved capability to audit the age and key rotation policies associated with CEX master keys
- New SAF protections for elliptic-curve cryptography (ECC) keys
- The capability to limit the use of archived keys to decryption operations
- Additional hardware exploitation for certain SSL/TLS ciphers
- Crypto Express 7 coprocessors. With HCR77D1, this support also is available on z/OS V2.4.

- With the PTFs for APAR OA58880, the following enhancements also are available on z/OS V2.4:
- New Edwards curves, Ed448 and Ed25519, for digital signatures
- New lattice-based algorithm for digital signatures
- CP Assist for Cryptographic Function (CPACF) protected key support for ECC Edwards and a subset of National Institute of Standards and Technology (NIST) curves
- TR-31 support for Hash-based Message Authentication Code (HMAC) keys
- Enhancements to Advanced Encryption Standard (AES) PIN(R) functions
- Additional options on TR-31 export services
- Europay, MasterCard, and Visa (EMV) service updates in support of CVN-18



COMMUNICATIONS SERVER

Communications Server

- More Granular Control Over FTP Level 2
- New System Authorization Facility (SAF) resource to control which z/OS users are permitted to use FTP server JES mode, available with PTF for APAR PH42618

Communications Server

- **IPsec Certificate Reporting**
- ipsec-k display command, NMI and SMF 119 subtype 73 and 74 records are updated to include IPsec X.509 certificate information
- This includes certificate serial number, certificate expiration, subject and issuer distinguished names
- The **ipsec -k** display command, the IPsec network management interface (NMI), and SMF type 119 subtype 73 and 74 records are enhanced to simplify the process of validating IPsec-related X.509 certificate configurations. The enhancements provide information about the X.509 certificates used during Internet Key Exchange (IKE) negotiations by the local and remote IKE peers, including certificate expiration information, certificate serial number, and subject and issuer distinguished names.

Communications Server

- **IPsec certificate reporting enhancements** - In V2R5, the z/OS UNIX ipsec command has been enhanced to display local and remote certificate information, such as serial number and expiration date, for phase 1 tunnels. The same certificate information is provided in the IPsec Network Management Interface (NMI) NMSec_GET_IKETUN and NMSec_GET_IKETUNCASCADE message responses, and the SMF type 119 IPsec IKE tunnel activation (subtype 73) and tunnel deactivation (subtype 74) records.
- **Restriction:** When using the z/OS UNIX ipsec command to retrieve phase 1 tunnel data from a remote system, both the local and remote system must be at z/OS V2R5 or later for the new certificate fields to be displayed.

Communications Server

- Improved auditability
- Support is added to the password syscall to include the caller's Port of Entry IP address when calling the System Authorization Facility (SAF)
- The security product can include this IP address in SMF Type 80 records.
- Improving logging and auditing

Communications Server

- z/OS V2.4 is the last release in which the z/OS TN3270E Telnet server, FTP server, and Digital Certificate Access Server (DCAS) will support direct invocation of System SSL APIs for TLS/SSL protection.
- In the future, the only TLS/SSL protection option for these servers will be Application Transparent Transport Layer Security (AT-TLS).
- The direct System SSL support in each of these components is functionally outdated and only supports TLS protocols up through TLSv1.1.
- IBM recommends converting your TN3270E Telnet, FTP server, and DCAS configurations to use AT-TLS, which supports the latest System SSL features, including the TLSv1.2 and TLSv1.3 protocols and related cipher suites.
- Note that while native TLS/SSL support for z/OS FTP client is not being withdrawn at this time, no future enhancements are planned for that support. IBM recommends using ATTLS to secure FTP client traffic.

Communications Server

- **AT-TLS and IPsec certificate diagnostics** - z/OS V2R5 Communications Server provides additional certificate diagnostic data to allow you to more quickly determine the cause of an AT-TLS or Ipsec negotiation failure. New syslogd messages are provided to identify certificate validation errors detected when processing a peer's certificate.
- **Restrictions:**
 - Certificate diagnostic messages are provided when the validation of the peer's certificate fails. For validation failures accessing the local certificate, certificate diagnostic data is not provided.
 - For IPsec negotiation failures due to errors with the peer's certificate, certificate diagnostic data will only be provided when the failure is detected by System SSL.
- **Dependencies:**
 - The syslog daemon (i.e. syslogd) must be active. For AT-TLS and IPsec, the additional certificate diagnostic messages are written to syslogd.



OTHER AREAS

IBM SMF New Signature Algorithms

- z/OS extends the digital signature support for SMF records written to log streams to optionally include a second digital signature. When enabled, the second signature provides an alternative to current algorithms
- SMF signature verification function is extended to include this second signature to help you determine if SMF records have been altered or removed. This function is intended to protect SMF data into the future.
- The support requires Cryptographic Support for z/OS V2.2 -V2.4 (HCR77D1) and IBM z15.

- **Improved auditability and serviceability for password syscall**
- Support is added to the password syscall to include the caller's Port of Entry IP address when calling the SAF to authenticate the user.
- The security product includes this IP address in SMF Type 80 records. This improves the logging and auditing capability of users by system security administrators.
- Also, this additional information in SMF is helpful in determining network setup issues. With the PTF for APAR OA59444, this enhancement is also available on z/OS V2.3 and later.

- **FIPS compliance support for platform interoperability**
- z/OS V2.5 provides FIPS compliance support for platform interoperability by completing the FIPS enablement to the UNIX-file-based Kerberos database, following the same support provided by the RACF Kerberos database in the last release.

SMF Records

- For record type 14, a new bit 3 (SMF14DSENCARCHKEY) of the SMF14DEF field is added for DFSMS archived key support indicating that the encrypted data set is being accessed with an archived key that only supports decryption operations.
- For record type 62, a new bit 7 (SMF62ARCKEY) of the SMF62IND field is added for DFSMS archived key support indicating that the encrypted data set is being accessed with an archived key that only supports decryption operations.
- For record types 70 - 79, bits 4 and 5 in the SMF7xFLA field in the RMF Product section are now defined.
- For record type 124, APAR OA59792 adds additional z/OS support for IBM Fibre Channel Endpoint Security in “Subtype 1 — Link diagnostic information”
- “Subtype 2 — Endpoint security information”
- “Subtype 4 — Endpoint security encryption key update”

Other Health Checks

- **IOS_ENDPOINT_SECURITY_LCUPATHS**

- **Description:**

- This check verifies, when IBM Fibre Channel Endpoint Security is enabled between the processor and a storage system, that all online channel paths to each device are either using or not using some form of endpoint security (authentication or encryption). For example, if some channel paths are using encryption and some are not, the data can be transmitted over the link between the processor and storage system unencrypted.
- The system runs this check when any of the following events occur:
 - IBM Health Check for z/OS starts.
 - A channel path for a device is brought online or taken offline by using a VARY PATH, VARY device, VARY CU, or CONFIG CHP command.
 - A channel path for a device becomes available or unavailable because of an I/O recovery event.
- **Reason for check:**
 - To ensure that business and customer data is protected from intrusion or tampering as it flows within or across data centers.

Other Areas

- **IBM SMF New Signature Algorithms**
- z/OS extends the digital signature support for SMF records written to log streams to optionally include a second digital signature. When enabled, the second signature provides an alternative to current algorithms
- SMF signature verification function is extended to include this second signature to help you determine if SMF records have been altered or removed. This function is intended to protect SMF data into the future.
- The support requires Cryptographic Support for z/OS V2.2 -V2.4 (HCR77D1) and IBM z15.

Other Areas

- Improved auditability
- Support is added to the password syscall to include the caller's Port of Entry IP address when calling the System Authorization Facility (SAF)
- The security product can include this IP address in SMF Type 80 records.
- Improving logging and auditing

Other Areas

- The z/OS NFS server has been enhanced with additional function to support Kerberos authentication with unique application-instance DVIPA. This support is designed to help clients preserve data security while enabling easier movement of the z/OS NFS server between LPARs. With the PTF for APAR OA58912 this enhancement is available on z/OS V2.3 and later.



PKI SERVICES

PKI Services

- A new header field is added to the ICL header to store the SHA256 fingerprint of the certificate when a certificate is generated.
- The pkiserv.conf configuration file has been updated to add certificate fingerprint support



SECURITY PORTAL

IBM Security Portal

- IBM utilizes internal and external sources to uncover potential vulnerabilities. IBM Z offers a Security Portal that allows clients to stay informed about patch data, associated Common Vulnerability Scoring System (CVSS) ratings for new APARs and Security Notices to address highly publicized security concerns.

IBM Z and LinuxONE Security Portal

Resource Link

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Tools

Customer Initiated Upgrade

Feedback

IBM Systems > IBM Z > Resource Link > Problem solving >

IBM Z and LinuxONE Security Portal

Primary resources

By accessing the IBM Z and LinuxONE Security Portal you agree the information contained in it is IBM Confidential, provided AS IS, may be used by you for internal purposes only and may not be disclosed to any third party without IBM's prior written consent.

If you do not agree to these conditions, you may not access the IBM Z and LinuxONE Security Portal.

Please ensure that you update all of your IBM Z and LinuxONE products to a supported version. Security and integrity fixes are generally only issued for supported versions of IBM Z and LinuxONE products.

Note: All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice. Any reliance on this Statement of Direction is at the relying party's sole risk and will not create any liability or obligation for IBM.

Primary resources

Security notices

APARs

Resource	Description	Last modified
IBM Z Security Portal	Introductory Material	9 Mar 2018
z/OS Security/Integrity ASSIGNs	Current ASSIGN File	15 Dec 2020
z/OS Security/Integrity CVSS	Current CVSS file	15 Dec 2020
z/OS Security/Integrity Data	Current HOLDDATA File	15 Dec 2020
z/VM Security/Integrity Data	Current APAR Data	10 Dec 2020
z/OS and z/VM SIA Cross Reference	SIA Cross Reference	15 Dec 2020
Security Portal File Download Automation	Sample Python code	20 Oct 2020

Subscribe

→ [Subscribe to this page](#)

Security Portal FAQs

[PDF: Frequently Asked Questions \(347KB\)](#)
Last modified 17 Jul 2018

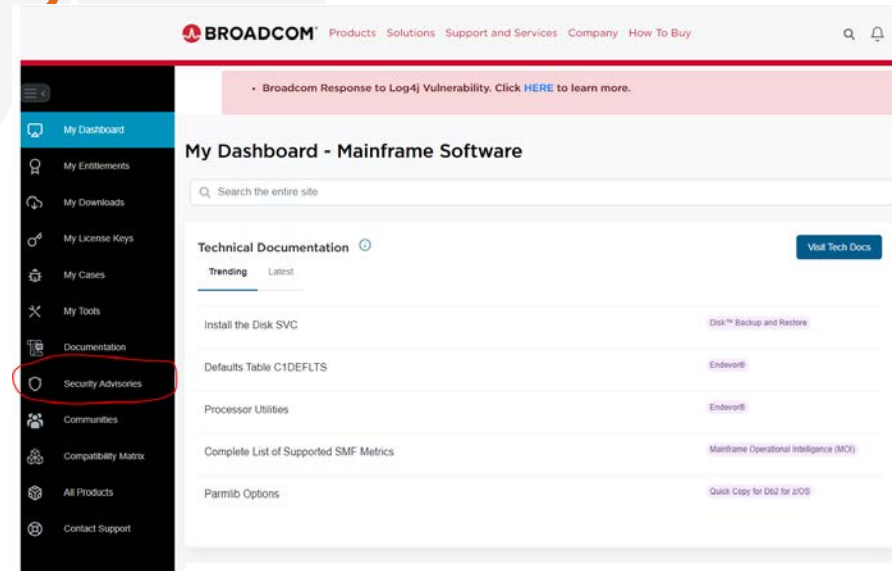
Broadcom Security Portal



Broadcom – Security Advisors

From the Mainframe Support page,
Select [Security Advisors](#).

Search By Title



Security Advisories - Mainframe Software

[Product Security Incident Response Contact Information](#)

1 - 3 Security Advisory of 3

Q ACF2

Notification Id	Title	Severity	Published	Updated
MFDSA19952	Web Administrator for ACF2 and Top Secret v15.0 Log4j 1.2.x vulnerability CVE-2021-4104	● CRITICAL	21 December 2021	21 days ago
MFDSA20352	ACF2 for z/OS 16.0 Vulnerability	● MEDIUM	24 February 2022	27 days ago
MFDSA18352	CA ACF2 Version 16.0 Vulnerability	● MEDIUM	29 June 2021	8 months ago

Your feedback is important!

Submit a session evaluation for each session you attend:

www.share.org/evaluation



Digital Badges



Earn Your DevOps Wizard or Security Warrior Badge

Submit a Digital Badge form for each session attended:

<https://forms.gle/mvqZPW7TNCwDCtmh9>



Session ID: [83688]
Badge code: [navy312]