IBM Z Security and Compliance Center

Pradeep Parameshwaran
Lead Architect, Security and Complianceon IBM Z & LinuxONE

Günter Weber
Technical Sales, IBM Mainframe Security Solutions

“We've heard from our clients that they are looking for solutions to help with the complexity and cost of compliance with the rapidly increasing number of regulations.”

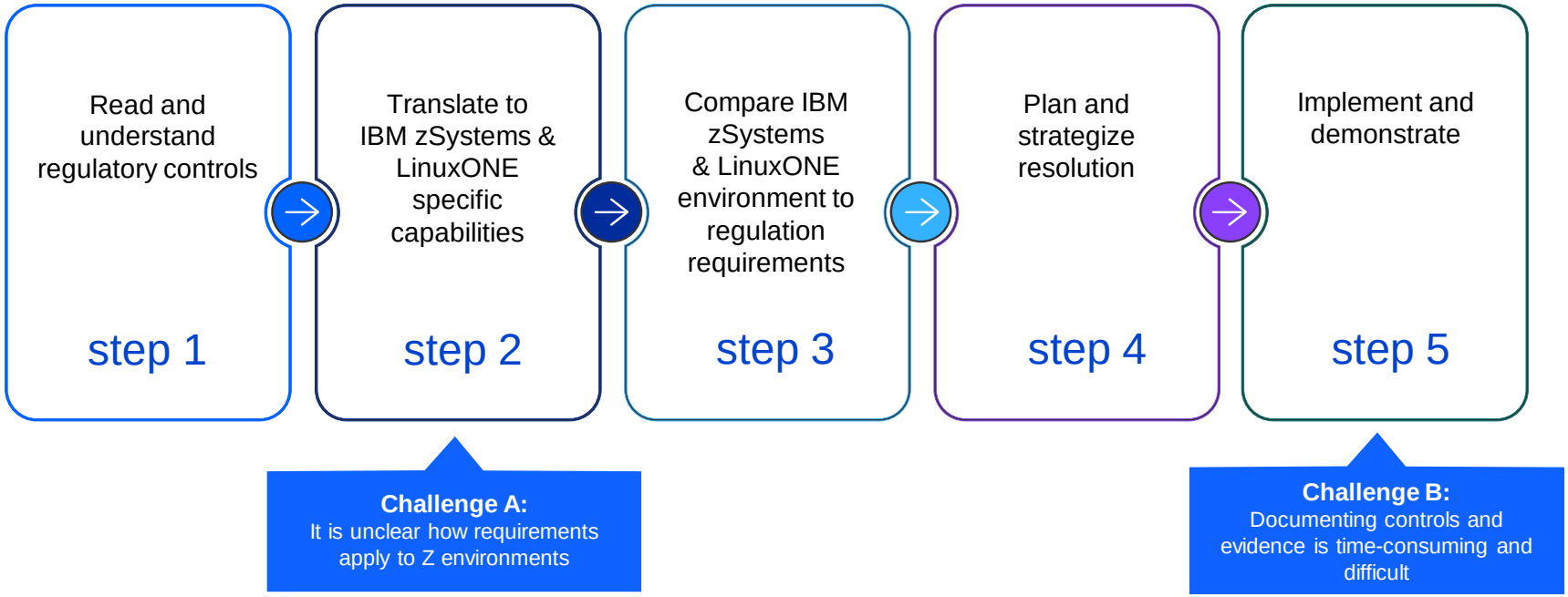
"[Compliance] is probably one of the largest business drivers for our policy. The second piece to that is reputational risk."

— VP IT Security, Financial Services

"In order to [grow our mainframe business, we] will need to provide and demonstrate adequate compliance for the departments being brought into Z... this includes many different standards."

—Director and Chief Information Officer, Public Sector

A Typical Audit Journey



Challenge on Mapping Controls

PK	CID	Requirement	Requirement Description	Control Description	Testing Procedures	Guidance
31	2.3	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.	2.3 Encrypt all non-console administrative access using strong cryptography. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	2.3 Select a sample of system components and verify that non-console administrative access is encrypted by performing the following: 2.3.a Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested. 2.3.b Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access. 2.3.c Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography. 2.3.d Examine vendor documentation and interview personnel to verify that strong cryptography for the	If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator's IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. To be considered "strong cryptography," industry- recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use. (Refer to "strong cryptography" in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms, and industry standards and best practices such as NIST SP 800-52 and SP 800-57, OWASP, etc.)
32	2.4	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are	2.4 Maintain an inventory of system components that are in scope for PCI DSS.	2.4.a Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each. 2.4.b Interview personnel to verify the documented inventory is kept current.	Maintaining a current list of all system components will enable an organization to accurately and efficiently define the scope of their environment for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from the organization's configuration standards.

Keeping Up With Compliance

In collaboration with IBM Security, IBM Research, IBM zSystems & LinuxONE

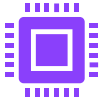
Interpret Regulations

Determine which regulations are relevant for your organization

Map IBM zSystems capabilities to those regulations

Easily show how IBM zSystems & LinuxONE capabilities meet or exceed industry standards.

Implement Controls



Discover new IBM zSystems capabilities to meet compliance

Engage IBM experts to deploy new features and submit RFEs to request new capabilities

Utilize new capabilities throughout the IBM stack to meet compliance.

Collect & Validate Evidence

Identify which data is essential for auditors.

Regularly collect and validate compliance data

Optimize your audit process to reduce time and effort.

Example: PCI DSS Requirement 3

PCI DSS 3.2.1

Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.

Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

3.1 Keep cardholder data storage to a minimum

3.2 Do not store sensitive authentication data after authorization

3.3 Mask PAN

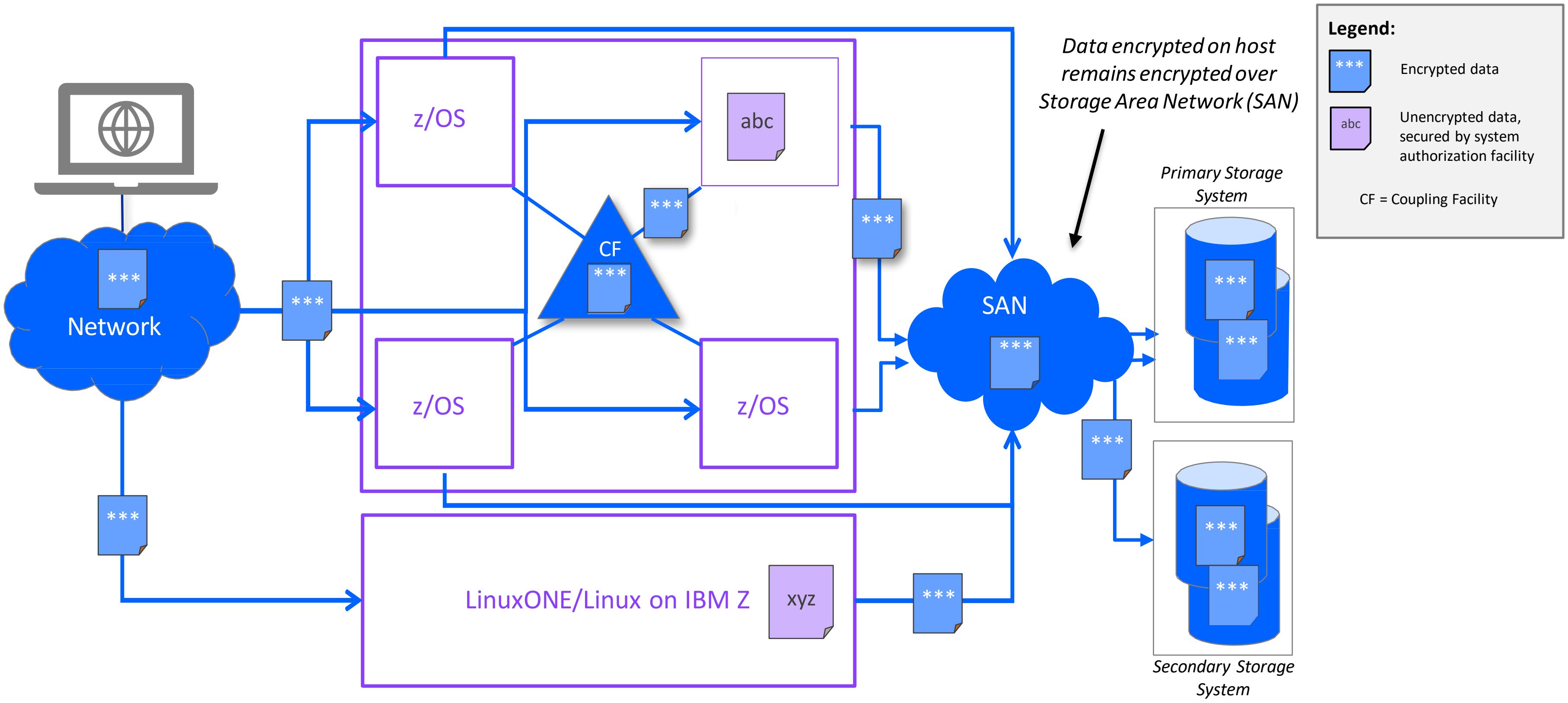
3.4 Render PAN unreadable anywhere it is stored

3.5 Protect keys used to secure stored cardholder data

3.6 Key management processes for cryptographic keys used for encryption of cardholder data

3.7 Policies and procedures are documented, in use and known to all affected parties

Do you know where your PAN is stored?



Compliance on IBM Z and LinuxONE

Dashboard

Assess

Scans

Configure

Scopes

Profiles

Goals

Settings

Z Security and Complian... / Scans /

PCI Review

PCI _DSS_SCOPE | PCI _DSS 3.2.1 | Validation

Details

Mar 16, 2022 1:10 PM

Feb 16, 202 1:10 AM

Jan 16, 202 1:10 AM

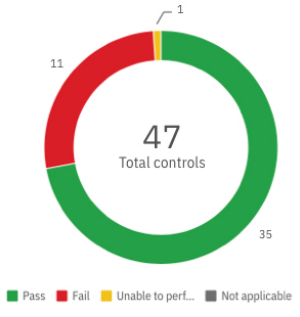
Dec 16, 202 1:10 AM

March 16, 2022 1:10 PM

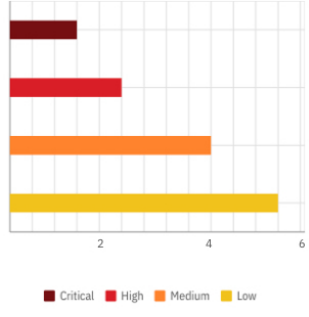
35 11 1 0

Download report

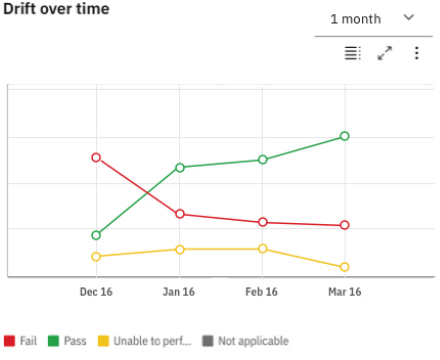
Controls



Failures



Drift over time

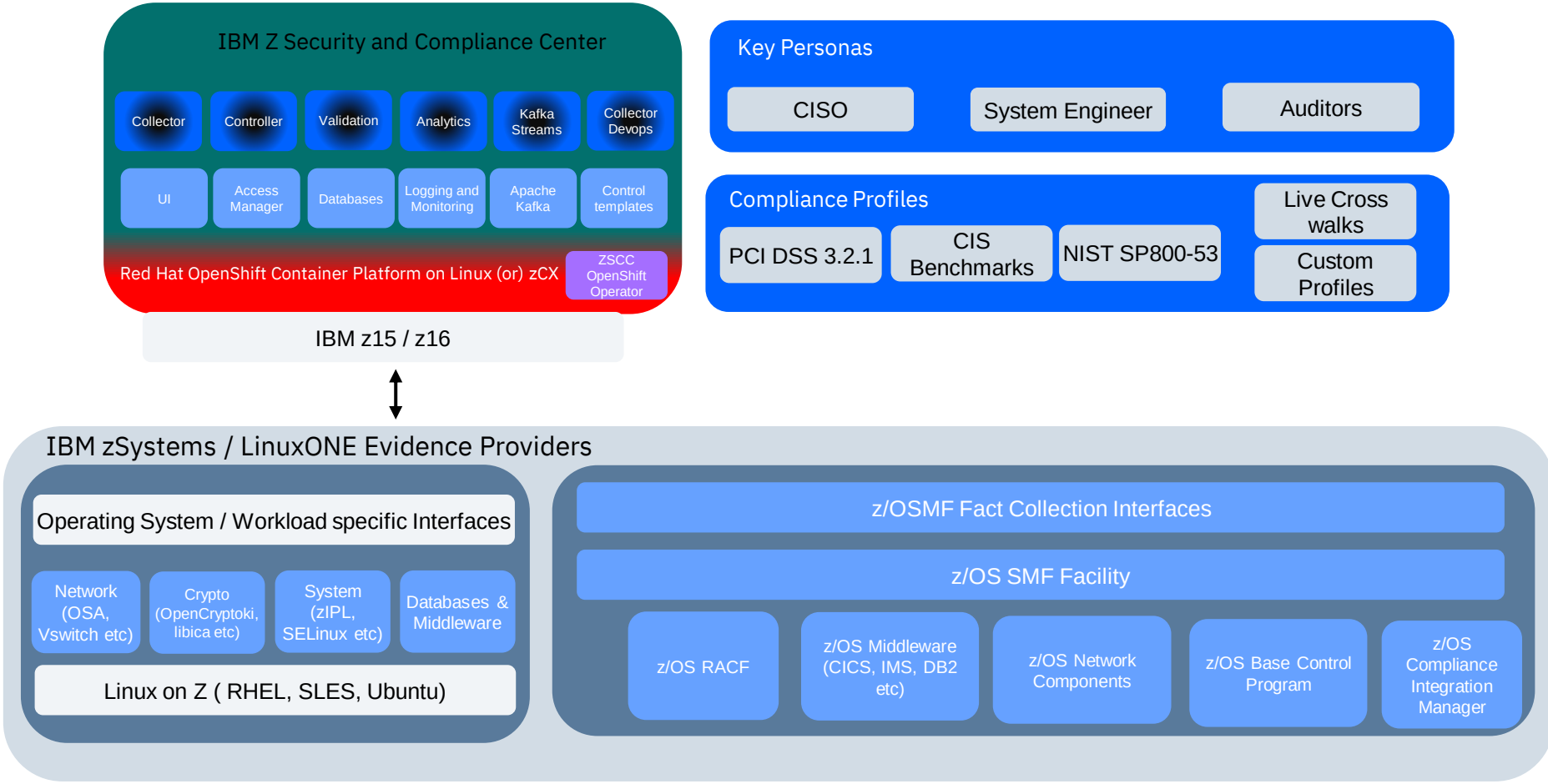


Control view | Resource view

Status Filter... | Severity Filter... | Search

Status	ID	Control	Severity	Resource details
⊘	1.1	Ensure the Appropriate Version/Patches for Oracle Software Is Installed	Critical	0 1 0 0
⊘	2.1.1	Ensure 'extproc' Is Not Present in listener config	Medium	0 1 0 0
!	2.1.2	Ensure 'ADMIN_RESTRICTIONS' is set to 'ON'	-	0 0 1 0
✓	2.2.1	Ensure 'AUDIT_SYS_OPERATIONS' Is Set to 'TRUE'	-	1 0 0 0

Reference Architecture of IBM Z Security and Compliance Center

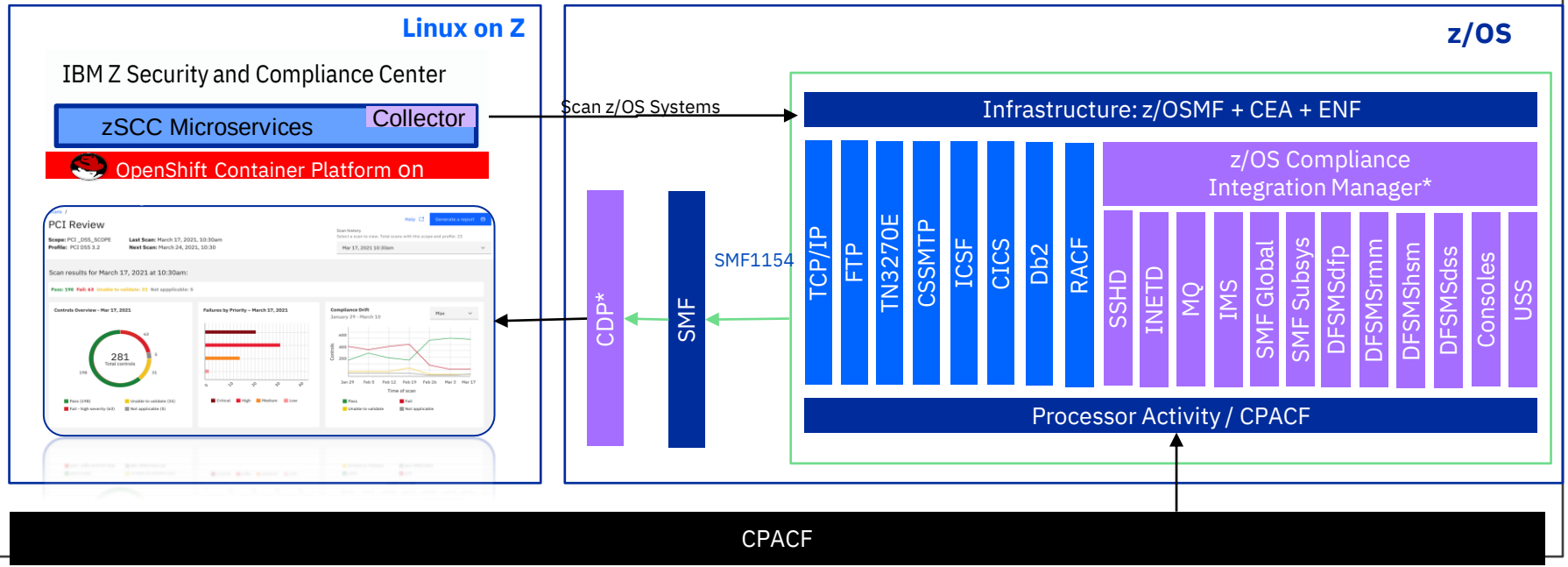


Solution Overview

z/OS Point of View

IBM Z Security & Compliance Center collector connects to a resource, such as z/OS or Linux on Z, and scans for compliance data. For z/OS, the collector connects to a z/OSMF compliance REST API which triggers sysplex-wide compliance data collection using an ENF86 signal.

Participating z/OS components and products listen for the new ENF86 signal. When received, these components write compliance data to SMF 1154 records associated with a unique subtype. The SMF records are streamed to IBM Z Security & Compliance Center using the Common Data Provider. Then, the IBM Z Security & Compliance Center maps the compliance data to the appropriate regulatory controls associated with a profile for validation, display and reporting.



* The z/OS Compliance Integration Manager and CDP are delivered with the IBM Z Security & Compliance Center

z/OS Compliance Data Collection Infrastructure

SMF 1154 records provide compliance evidence. A different subtype is assigned to each participating z/OS component or product.

See subsequent slides for z/OS component requirements

A new z/OSMF compliance REST API drives an ENF86 signal to participating z/OS components and products.

z/OSMF support requires z/OS 2.4 or later with PTFs for APAR PH37308

Upon receiving the ENF86 signal, participating z/OS components and products collect and write compliance data to their associated SMF1154 subtype records.

CEA support requires z/OS 2.4 or later with PTFs for APAR OA61443

The Common Data Provider streams SMF 1154 records to the IBM Z Security and Compliance Center for validation, display and reporting.

CDP support requires version 5.1

Concepts in IBM Z SCC

Inventory

An inventory will be built automatically when you define a scope and discover resources

An inventory will be built by the collector by ,

- Invoking z/OSMF System topology REST API in case of z/OS
- By manually uploading a JSON file with IP's in case of Linux on IBM zSystems

On a an inventory, you can

- Visualize the z/OSMF , Sysplex , z/OS Systems (or) Linux VM's defined under scope
- Edit inventory to customize which systems should be scanned
- In case of z/OS each time a scan is done , the discovery will be update the inventory with new systems which are added

The inventory granularity at the moment is at System level and not at component level

Profiles

- A profile is a group of controls which will be matched to applicable Regulatory frameworks (or) Security frameworks
- Primarily written with technical requirements in mind
- IBM Z SCC v1.1.0 supports **pre-defined profiles**
  - PCI DSS v3.21 for z/OS (**Subset of Controls**)
  - NIST SP800-53 for z/OS (**Subset of Controls**)
  - CIS Profile for z/OS (**Subset of CIS benchmarks for z/OS**)
  - & PCI , NIST, CIS for Linux Distro's, Oracle & PostgreSQL

A **Pre-defined profile,**

- Can be exported as pdf / csv for further references
- Cannot be edited and deleted

A **Custom profile,**

- Is a profile which can be built by customer based on a pre defined profile or his own enterprise controls
- Can have subset of goals which IBM ZSCC provides
- Can be a superset of pre-defined profiles

CIS Benchmarks

Center for Internet Security is a community-driven nonprofit org responsible for the CIS Benchmarks and CIS Controls and globally recognized best practices for securing IT systems and data.

The CIS Controls are a general set of recommended practices for securing a wide range of systems and devices

CIS Benchmarks are best practices for the secure configuration of a target system and developed through a unique consensus-based process comprised of cybersecurity professionals and SMEs around the world. The benchmarks are guidelines for hardening specific operating systems, middleware, software applications, and network devices.

The goal of all benchmark areas is to provide practical, security-specific guidance for a given technology that concisely *describes a generally applicable baseline for all organizations and recognizes the need to securely maintain operational effectiveness.*

Guidelines available in 1H22:

- IBM z/OS V2R5 with RACF Benchmark
- IBM Db2 13 for z/OS Benchmark
- IBM CICS Transaction Server 6.1 Benchmark
- Red Hat Enterprise Linux 8.0 for IBM Z

Link:https://www.cisecurity.org/benchmark/ibm_z

Goals

- A goal is specific technical check of a security (or) compliance setting implemened in IBM Z SCC
- Goals checks are done based on the facts which are collected from systems under scope
- The Goal parameters can be customized ,
  - For Example: if you want to change the password policy to be 20 characters instead of 16 characters for a PCI DSS Control, it can be done
- Each goals carries a unique identifier, description and the logic of the check that is done

A **Goal,**

- Can be mapped to any applicable control which can be specific to a regulatory profile / security profile
- Cannot be deleted but can be disabled from a custom profile

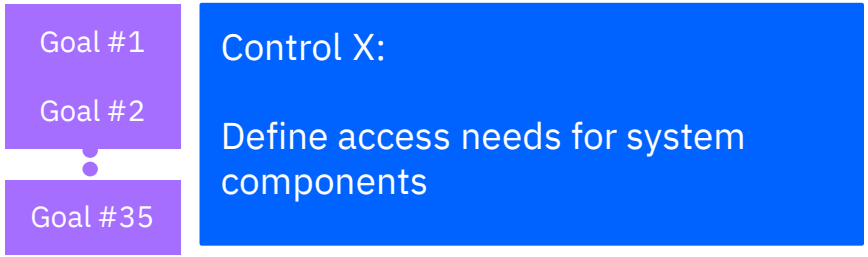
Only Goals which are implemented in zSCC can be mapped to a custom profile

Key Definitions

A goal is a specific technical check that can be run on data to produce a pass or fail

Goal #1 "Check whether only authorized users can access Db2 from CICS"

A control is a group of goals around a common theme which typically to a defined rule



A profile is a group of controls which will be match applicable regulatory frameworks

Software support for evidence providers

z/OS 2.4 and z/OS 2.5 have been enhanced to enable the collection of compliance data from IBM z16 CPACF counters and several z/OS products and components.

This support requires PTFs for z/OS 2.4 and z/OS 2.5. The PTFs will be identified by fix category designated specifically for compliance data collection support named IBM.Function.Compliance.DataCollection.

- See IBM Fix Category Values and Descriptions for information about how to use this fix category to identify and install the specific PTFs that enable compliance data collection.

Prerequisite enablement software details:

- z/OSMF with PTFs for APAR PH37308
- CEA with PTFs for APAR OA61443
- SMF with PTFs for APAR OA61444

Middleware and software evidence providers:

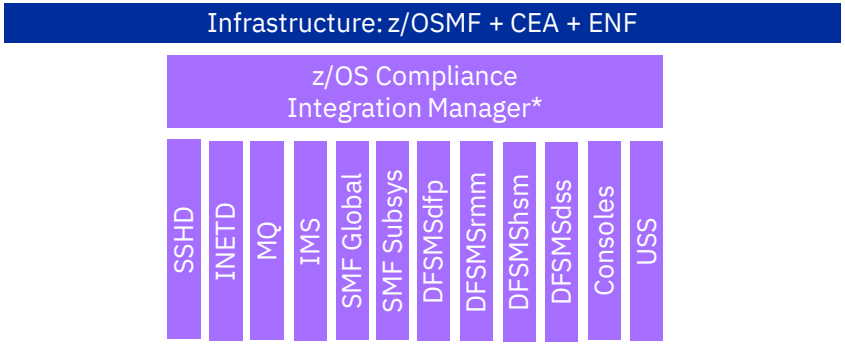
- CPACF usage counters with PTFs for APAR OA61511
- RACF® with PTFs for APAR OA61933
- Communication server (FTP, TCP/IP, CSSMTP, TN3270) with PTFs for APAR PH37372
- ICSF with PTFs for APAR OA61977
- Db2 V13 for z/OS
- CICS TS 6.1
- IMS V15 with PTFs for APAR PH42600
- MQ, SSHD, INETD, SMF, DFSMSrmm, DFSMSdfp, DFSMShsm, DFSMSdss, Consoles, USS

For CICS® Transaction Server for z/OS 6.1, see Software Announcement 222-092, dated April 5, 2022.

For Db2® 13 for z/OS powered by AI innovations, see Software Announcement 222-003, dated April 5, 2022.

Der z/OS Compliance Integration Manager

Für z/OS Komponenten/Subsysteme die (noch) keine eigenen SMF Records schreiben, wird der z/OS Compliance Integration Manager verwendet.



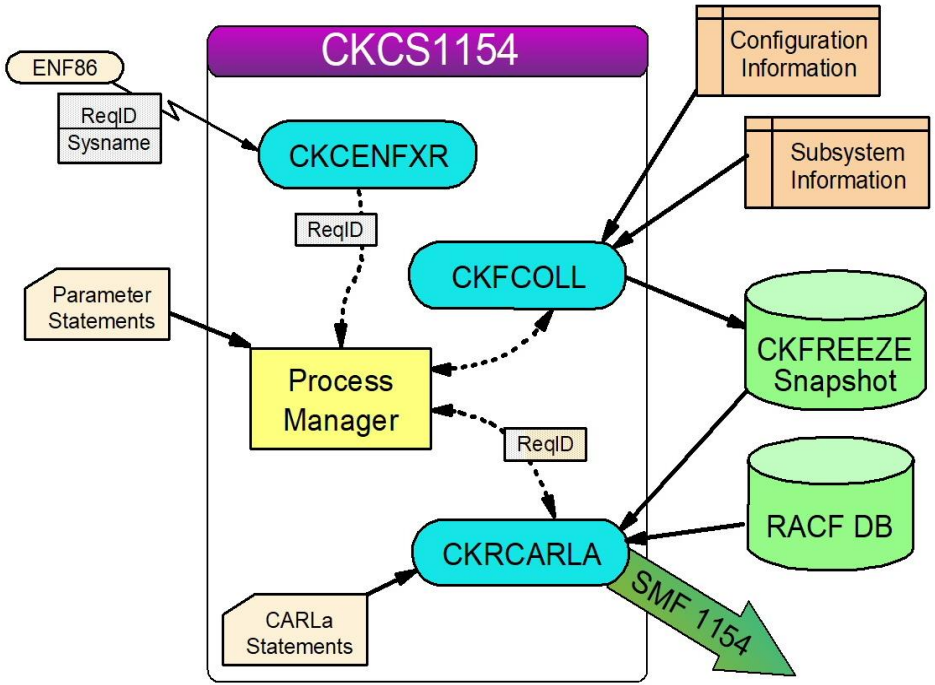
Started task CKCS1154

CKCS1154 – Compliance Integration Manager task

CKCENFXR – Exit routine listening for event 86

CKFCOLL – Security snapshot collector creates “mini snapshot”

CKRCARLA – CARLa engine executing Carla that generates SMF record (can write only built-in layout to SMF)



Installation – CKCS1154 – Optionen

Think about started task options

StaggerTime

Delay in seconds between systems in sysplex reacting to ENF 86. Default is 10.
Specifying 0 means all at the same time which might be noticeable performance wise.

SetSRVCLass

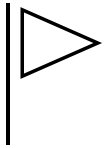
Add task to SYSSTC service class

NoSetSRVCLass

Do not add task to SYSSTC service class. Might be preferable on single processor systems. This is the default.

Troubleshooting

Locate output of Compliance Integration Manager started task called CKCS1154 and analyze in 3 stages



Look in JESMSGLG

Abend 806 etc. -> increase REGION, MEMLIMIT.

Abend 913 *-> Verify STARTED profile, user ID definition*

ICH408I messages *-> Verify user permissions*

CKC0119E ENF listen 86 request retcode=0C *-> z/OS missing relevant PTFs*

CKC0131W ENF86 does not include current system *-> modify collection request*

CKC0139I Finished writing SMF 1154 records *-> seems OK*

Look in CKCDEBUG

Message form: CKf*nnnn ss text*

Where *ss* is numeric severity

Look for severity higher than 08

Is either:

CKFCOLL mini-snapshot output

or

CKRCARLA SMF generation output

F CKCS1154,DEBUG

Enter DEBUG mode and ask for a renewed ENF 86 trigger

Analyze output messages:

CKC0124I SMF 1154 activated *-> An ENF 86 notification arrived*

CKC0126I ENF86 for current system: <sysname> *-> it contained current SYSNAME just fine*

Can experiment with DIAGNOSE ENF86 to simulate ENF 86 trigger

.

Entitlement zSCC (5655-CC1)

Implies functionality of:

z/OS Compliance Integration Manager
zSecure Audit for RACF (implies zSecure SIEM adapter for RACF)
zSecure Audit for ACF2 (implies zSecure SIEM adapter for ACF2)
zSecure Audit for TSS (implies zSecure SIEM adapter for TSS)

FMIDs needed for 5655-CC1

HCKRvrm, HC4Rvrm, JC2Avrm, JCKCvrm, JCKCvrX

Entitlement can optionally be *disabled* through IFAPRDxx. Enabled by default.

```
PRODUCT OWNER('IBM CORP')
      NAME('ZSCC')
      ID(5655-CC1)
      VERSION(*) RELEASE(*) MOD(*)
      STATE(DISABLED)
```

Support for formatting SMF-1154

CARLa Auditing and Reporting Language

NEWLIST TYPE=SMF more than 130 new fields

Field name structure
SMF1154_*nn_section_purpose*
where *nn* is the subtype, or ‘S2’ for common layout section S2 fields for SAF general resources

SAF general resource section S2_RES used by 77 USS, 51 DFP, 52 RMM, 53 HSM, 54 DSS, and more coming.

Because of CDP limitations, SMF 1154 exploits full byte fields for Booleans with value 0 or 1.

In CARLa, this is a new field format boolean_hex.

Important Links

IBM Z SCC Webpage: https://www.ibm.com/products/z-security-and-compliance-center

Solution Brief : https://www.ibm.com/downloads/cas/8NJA2R9P

IBM Z SCC Documentation (Guide): https://www.ibm.com/docs/en/SSO5Y9T_1.1.0/abstract.htm

IBM Z SCC Docs: https://www.ibm.com/docs/en/zscc/1.1.0

CIS Benchmarks: https://www.cisecurity.org/benchmark/ibm_z

Thank you

Pradeep Parameshwaran - Lead Architect, Security and Compliance on IBM Z & LinuxONE

Günter Weber 

Technical Sales – IBM Mainframe Security Solutions

Contact

E-Mail PRADEEP@de.ibm.com / weberg@de.ibm.com

LinkedIn https://www.linkedin.com/in/guenter-weber-bbba3b45/