

# zSCC - Erfahrungsbericht

98. GSE – Wislikofen, April 2024



## Table of Contents

IBM Z Security and Compliance Center (zSCC)	03
Prerequisite	04
Architecture and typical flow for validation	05
Installation	06
The puzzle	07
Experience from the installation	08
Demo?	09

# IBM Z Security and Compliance Center (zSCC)

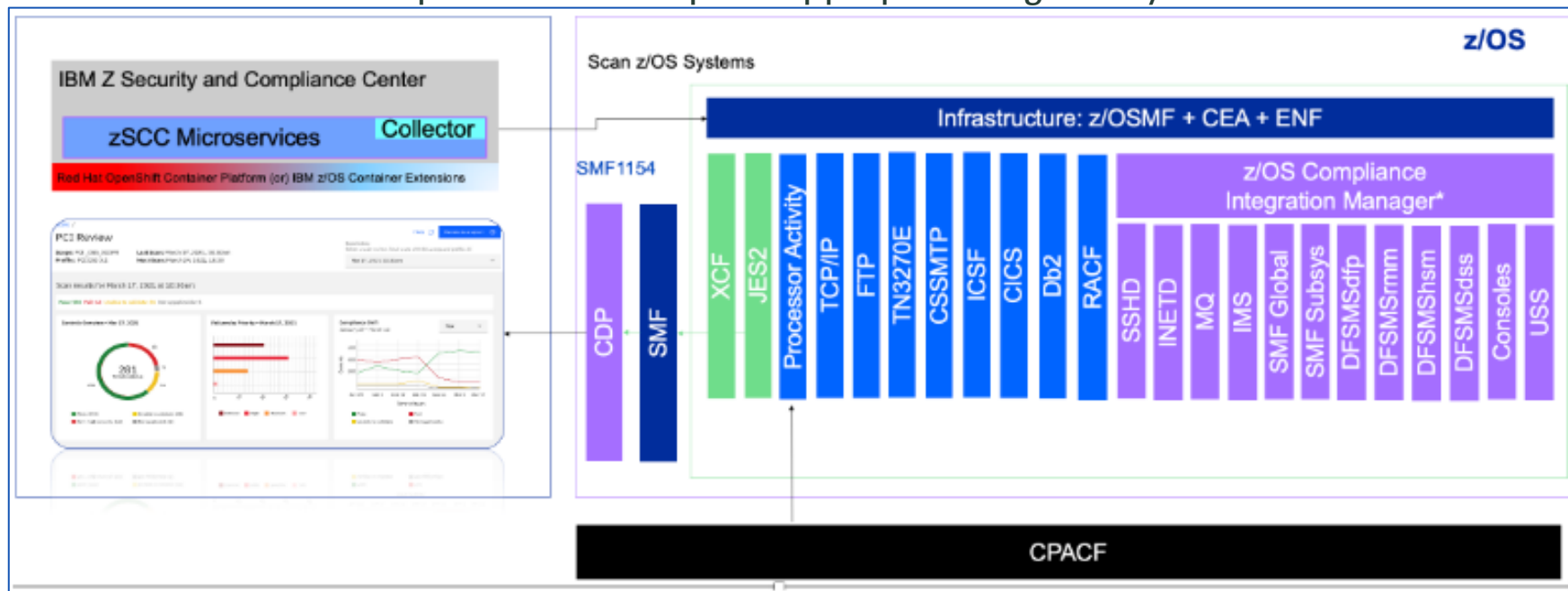
- IBM Z Security and Compliance Center consists of a collection of components that retrieve, validate, and report on the compliance status of a particular scope of components in the IBM Z environment.
- Supports regulatory frameworks such as PCI DSS, NIST and CIS.
- Multi Sysplex Support

# Prerequisite

- IBM Z Product 5655-CC1 – It is an OTC product and contains:
  - zSecure 3.1.0 – Compliance Integration Manager
  - Common Data Provider (CDP)
  - API key to download Docker Images from IBM Cloud Container Registry
- IBM z15 or z16
- IBM LinuxONE III or Emperor 4 with Product 5655-LC1
- IBM zCX or OpenShift → FIXCAT IBM.Function.zCX or IBM.Function.zCX-OCP
- zOS >=2.4 → FIXCAT IBM.Function.Compliance.DataCollection
- zOSMF (API) availability

# Architecture and typical flow for validation

1. Request compliance data.
2. For zOS the collector connects to the zOSMF Server.
3. zOSMF REST API issues notification signal ENF86 to trigger data collection.
4. Products listen for ENF86 signal and write SMF type 1154 record (each data provider has its own subtype).
  - Products without built in capability to write SMF 1154 records are covered by Compliance Integration Manager
5. SMF records are collected by Common Data Provider (CDP) and streamed to Logstash from zSCC.
6. zSCC evaluates the compliance data maps to appropriate regulatory controls.



# Installation

- Project plan for implementation with detailed steps available → [Project plan for implementing zSCC](#)
- Main steps:
  - Install and Configure zSCC into zOS Container Extension (zCX) or Red Hat OpenShift Container Platform (RHOCP).
  - Enable SMF type 1154 collection.
  - Install and Configure CDP (Streamer and Gatherer STCs) including zOSMF Plugin to create Policy.
  - Install and Configure zSecure (base) and Compliance Evidence STC.
  - Preparing a scope for host-defined profile validation.
  - Configure AT-TLS rules to protect traffic between Streamer-Gatherer and Streamer-Logstash(zSCC)

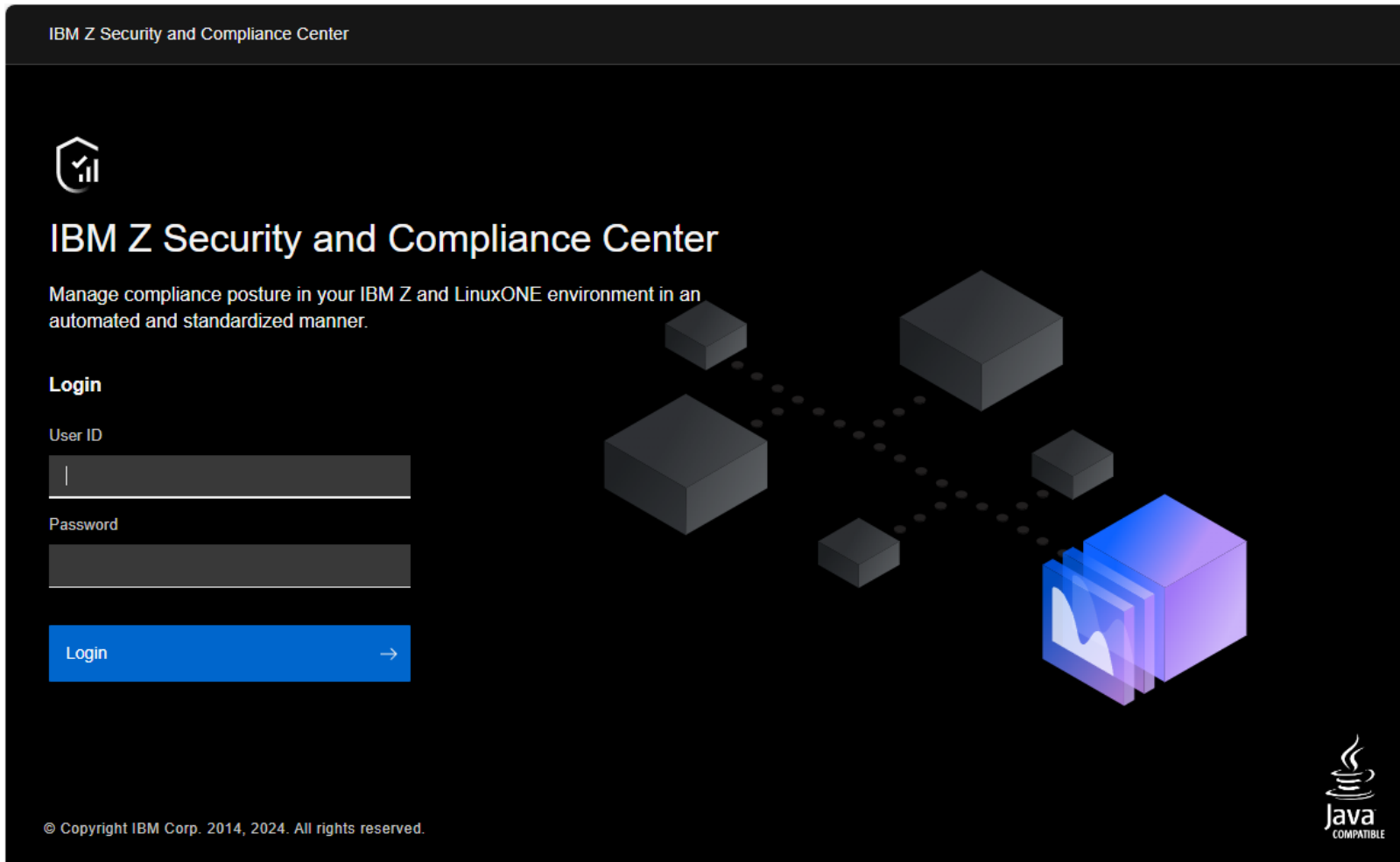


## Experience from the installation

- zCX Installation with compose container pretty simple and straight forward but be careful when creating/composing the required certificate files!
  - No empty lines between the certificate
  - Correct order of the certs when combining the files
- Prepare various config files for all deployment options to avoid updating the ,generic' config file (shutdown, backup, upgrade, restart)
- Apply zSecure PTF UJ94705
- zSCC and zOSMF communication not always working
- CKCJSCAN Job not equipped by default with SYSAFF/SYSTEM parameter to run on the expected LPAR (Job gets started where zOSMF is running).
- Debugging Sessions with IBM resulted in new PTFs and documentation updates
- POC 90 days, installation and configuration to get first results 30 days

# Demo?

IBM Z Security and Compliance Center



The image shows a screenshot of the IBM Z Security and Compliance Center login page. The page has a dark background with a central graphic of several 3D cubes of varying sizes and colors (grey, blue, purple) connected by dotted lines, suggesting a network or data flow. On the left side, there is a login form with the following elements:

- A shield icon with a checkmark and a bar chart.
- The title "IBM Z Security and Compliance Center".
- The subtitle "Manage compliance posture in your IBM Z and LinuxONE environment in an automated and standardized manner."
- A "Login" section header.
- A "User ID" label above a text input field.
- A "Password" label above a text input field.
- A blue "Login" button with a right-pointing arrow.

At the bottom left, there is a copyright notice: "© Copyright IBM Corp. 2014, 2024. All rights reserved." At the bottom right, there is the "Java COMPATIBLE" logo.



## Further Information

- [Installing the solution](#)
- [Enable your z/OS systems for data collection](#)
- [Setup of the Compliance Evidence started task](#)
- [Install IBM Z Common Data Provider](#)
- [Configure IBM Z Common Data Provider](#)
- [SMF record type 1154](#)
- [CDP - Configuring AT-TLS connections among the data gatherers, the Data Streamer, and subscribers](#)

Any  
questions?



# Thank you!

Contact us

Follow us



# Legal notice

©2024 Swiss Re. All rights reserved. You may use this presentation for private or internal purposes but note that any copyright or other proprietary notices must not be removed. You are not permitted to create any modifications or derivative works of this presentation, or to use it for commercial or other public purposes, without the prior written permission of Swiss Re.

The information and opinions contained in the presentation are provided as at the date of the presentation and may change. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for its accuracy or comprehensiveness or its updating. All liability for the accuracy and completeness of the information or for any damage or loss resulting from its use is expressly excluded.