eurex clearing

DEUTSCHE BÖRSE GROUP

Developing & Operating Mission Critical Applications with the OpenShift Container Platform

Clearing and Risk IT, Deutsche Börse AG

30. June 2022, Openshift Anwendertreffen Hanau, Alexander Buschmann

alexander.Buschmann@deutsche-boerse.com

Table of content

Welcome to Deutsche Börse AG !

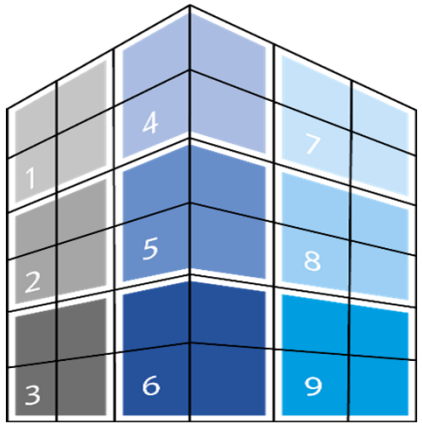
1. What means DevOps for Clearing/Risk IT and Xetra Eurex Operations
2. Challenge
3. DevOps Roadmap
4. Information Security: mandatory control framework + container adaption
5. DevOps - automated Software Build Tool Chain (Continuous Integration)
6. DevOps – automated fabric for Containers (Continuous Deployment)
7. Target Picture – Container in Action on OpenShift: Monitoring & Tracing

   DEMO (Graylog, Instana)

=> Q & A => Break Out Session Teaser

An overview of Deutsche Börse Group

Our key principles are trust, integrity and efficiency



1 Pre-IPO and listing
2 Trading
3 Clearing

4 Settlement
5 Custody
6 Collateral and liquidity management

7 Market data
8 Indices
9 Technology

Trusted

- Has a public mandate
- Operates neutral, fair & open infrastructures, preventing market abuse by design
- Creates no own risk
- Is crisis-proven
- Operates diverse reliable safeguards and surveillance
- Enhances financial stability with proven risk-management systems

Integrity

- Is highly regulated
- Follows clear and transparent rulebooks
- Is controlled by diverse supervisory authorities
- Ensures that authorities get information and data they need for regulatory scrutiny
- Includes users in governance

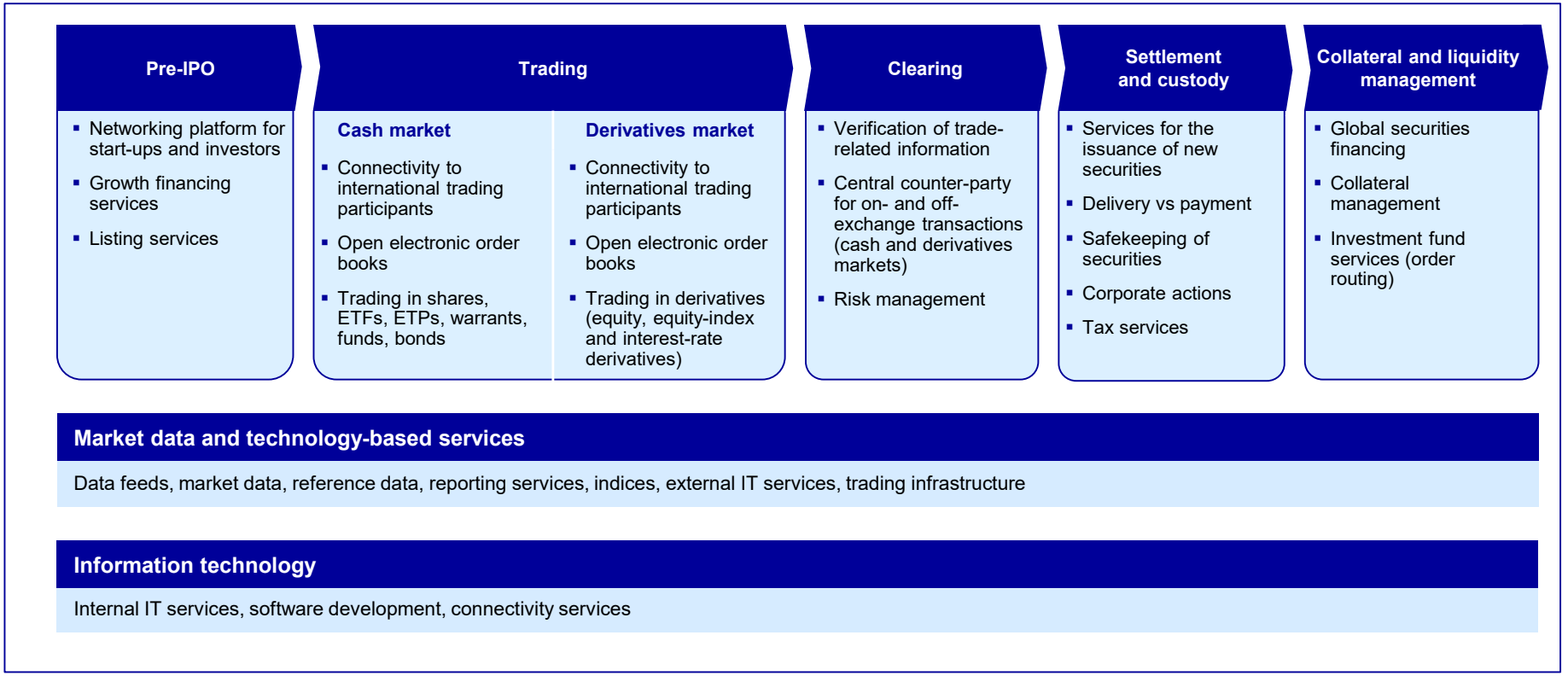
Efficient

- Builds and operates efficient, stable networks and platforms for financial markets
- Provides integrated and multi-asset solutions
- Develops strong and sustainable relationships
- Delivers resilient, state-of-the-art financial systems
- Promotes innovation, digitalisation and technology

Deutsche Börse Group operates trading venues, risk management, settlement systems and various market data services as well as technology and network services, which enable efficient and transparent pricing, guarantee of liquidity, reduction of contagion risks and thus the efficient use of capital.

An overview of Deutsche Börse Group

Financial services infrastructure with comprehensive product range



What is DevOps for Clearing and Risk IT and Xetra Eurex Operations ?

- **Who we are:**
  - Clearing and Risk IT Architects Office for Product Clearing
  - Clearing IT Application Development + Configuration Management
  - Xetra Eurex Operations (XEOPs) Technical Operations

- **What** we want to do:
  - Adopt and Integrate Market Demands faster in Clearing projects
  - Phase out Legacy Systems
  - Keep up with Security Patch Cycles
  - Automate “everything” and prevent high privileged (interactive) system access

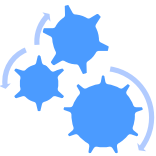
- **Why**:
  - Reduce time to market in order to be more competitive
  - Reduce the cycle time from idea to working implementation
  - Reduce the cycle time to fix defects and vulnerabilities faster
  - Achieve full compliance and robustness
  - More customer feedback + (re-)act faster, give fast feedback to the market

Challenges - “Agile development 2.0”

- ✓ Reduce complexity for Ops and Dev
  - ✓ ensure quality baselines and respect responsibilities (SoD)
  - ✓ ensure fulfillment of requirements and constraints
- ✓ Full Regulatory Compliance, e.g. BaIT/MA-Risk/KRITIS
- ✓ Adopt Information Security “Mandatory Control Framework” aligned with **ISO 2700x**

- ➢ **state-of-the-art IT-Security “CIA-A”** (incl. vulnerability checks & handling)
- ➢ **adopt** new technology stacks **faster**
- ➢ **provide monitoring and tracing** for 1st, 2nd and 3rd support
- ➢ adherence to DBG Technology Strategy: **“cloud push”**

What Agile DevOps has to respect



„Magic Square of Hell“

- Compliance with regulatory standards and policies
- Information Security Mandatory Control Framework
- Architecture and Planning
- Feature scope + quality + cost + delivery timelines = **„Magic Square of Hell“**

Mandatory Control Framework based on ISO 27000/27001

ISO Domain	Initiative	Description	IOCP IS-Baseline
A8	▪ Asset & licence management (CMS, uCMDB, SNOW)	▪ Openshift Cluster Inventory (API)	✓
A9	▪ Privileged Access Management (CyberArk setup)	▪ Map Openshift platform RBAC Model to DBG Standard	✓
		▪ Deploy CyberArk on Bastion Host. Workloads (pods) are sealed.	✓
	▪ DBG controlled secrets management (CyberArk Vault)	▪ Adopt Conjure Vault with optional CyberARK integration	✓
A10	▪ Secure key management	▪ Extend Openshift Default solution to DBG statndard	✓
	▪ Data at rest encryption (BYOK disk, database, storage)	▪ Persistent Datastore layer for Master State etc.	
	▪ Data in flight encryption (VPN)	▪ Openshift default (Intern). DBG PKI for external interfaces.	✓
A12	▪ Hardened baseline images	▪ Pre-selected and pre-tested RHEL Enterprise Linux Images from Red Hat.	✓
	▪ Alerting & Monitoring (ArcSight, Splunk and Slack)	▪ Collect OCP fluentd logs, develop use-cases and establish monitoring	✓
	▪ Vulnerability scanning	▪ Aquasec/Rapid7. Integrate into technology stack lifecycle	✓
	▪ Web Application Firewall (WAF)	▪ F5 Big IP WAF module for perimeter security	✓
A13	▪ Network Segregation & Setup[1]	▪ Configure SDN namespaces of Openshift for multi-tenacy for projects + services	✓
A17	▪ Business Continuity Management	▪ Redundancy in Control Plane. Pod Restart policy. Load Balancing with multi sides.	✓
A18	▪ Compliance checking (AquaSec)	▪ Datastore layer will be encrypted by one of the available encryption providers (aescbc, secretbox, and aesgcm) + TLS 1.2 + Redundancy.	✓
	▪ Compliance checking (AquaSec)	▪ Life Cycle Management in CD chain	✓

✓ Control deployed ✓ Control not in place – custom IS-Basline implementation

Updated Software Development Life Cycle

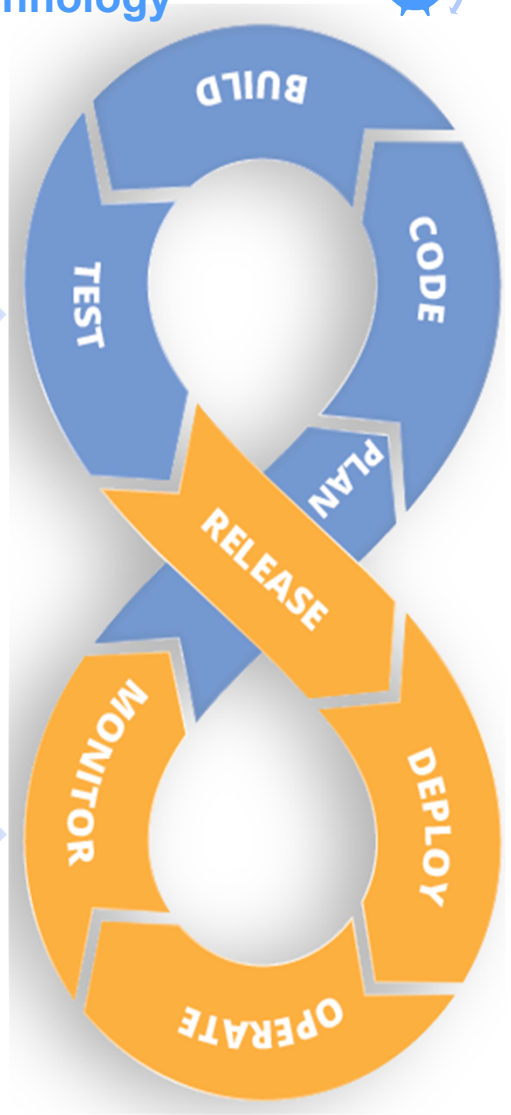
Repeatable and Fast with Job Control Automation + Container Technology

CI
Continuous Integration

- Quality: Code QA, Unit Tests
- **Compliance: Software Library dependencies, Open Source Software (OSS inventory)**
- **Secure: Source Code Scans, Baselines, Libraries**
- Transparency: Central Repositories

CD
Continuous Deployment

- **Deploy Anywhere**: Technology stack based on Containers into cloud or own datacenter
- **Orchestration + Control**: Application Lifecycle, Asset Management
- **Secure: Patch compliance, Secret Store usage**
- Efficient: Automated Tests and Quality Gateways
- **Monitoring**: Central Logging/Tracing + Access Control

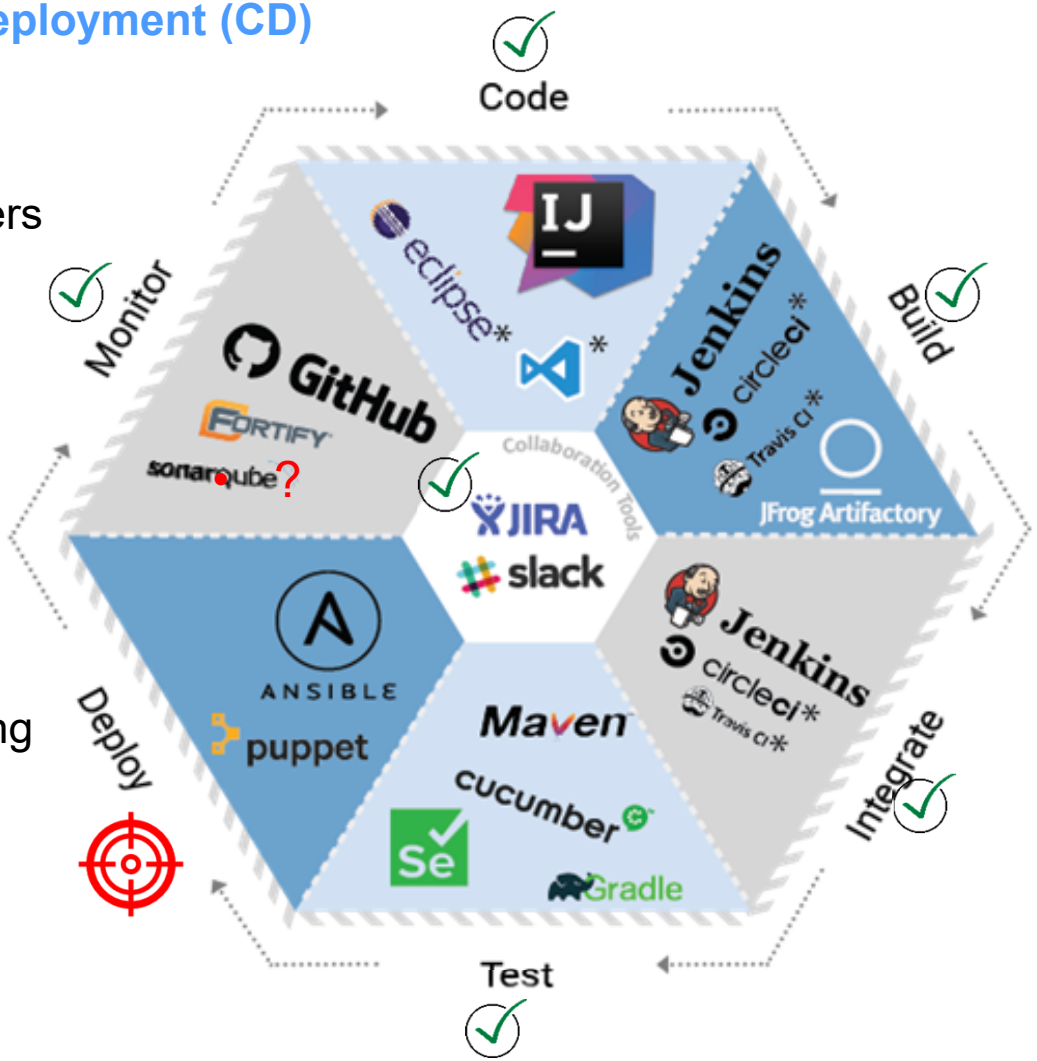


DevOps - Current Automation Software Build Tool Chain

Continuous Integration (CI) + Deployment (CD)

done

- our DevOps toolchain covers mainly the **software build** process



focus

- **infrastructure** provisioning
- **deployment** automation
- **security test** integration:
  - ❑ IS baseline checks
  - ❑ Vulnerability checks
  - ❑ WAF rule test
  - ❑ SIEM feedback

Evolve Security Approach with Containers for the Enterprise

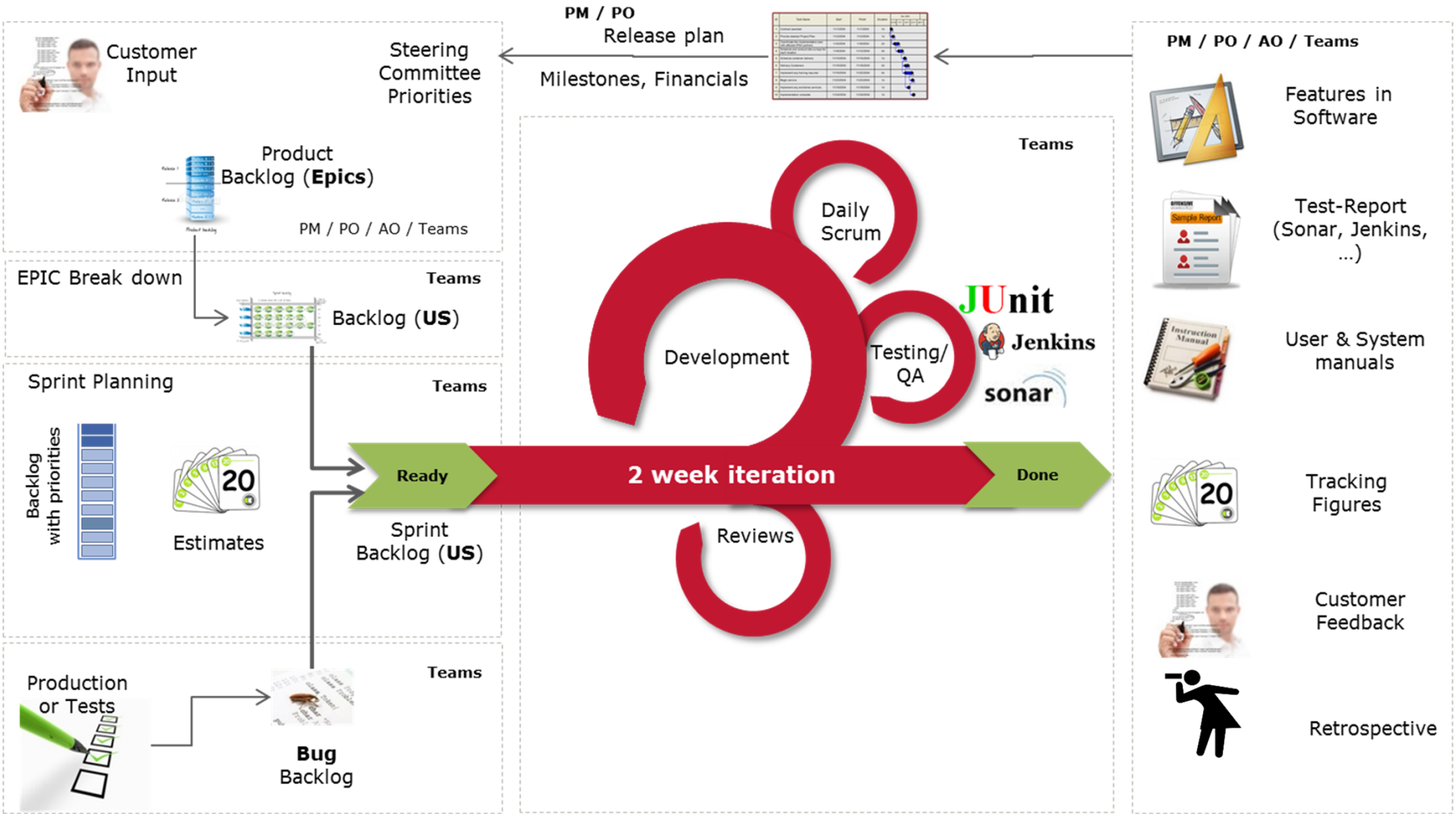
Static security policies & checklists no longer suffice and don't scale for containers in the enterprise.

- Security must be considered at every stage of your application and infrastructure lifecycle.

- Security must become a continuous activity.

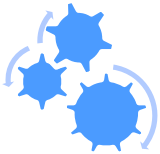
Continuous Integration Process for Clearing IT

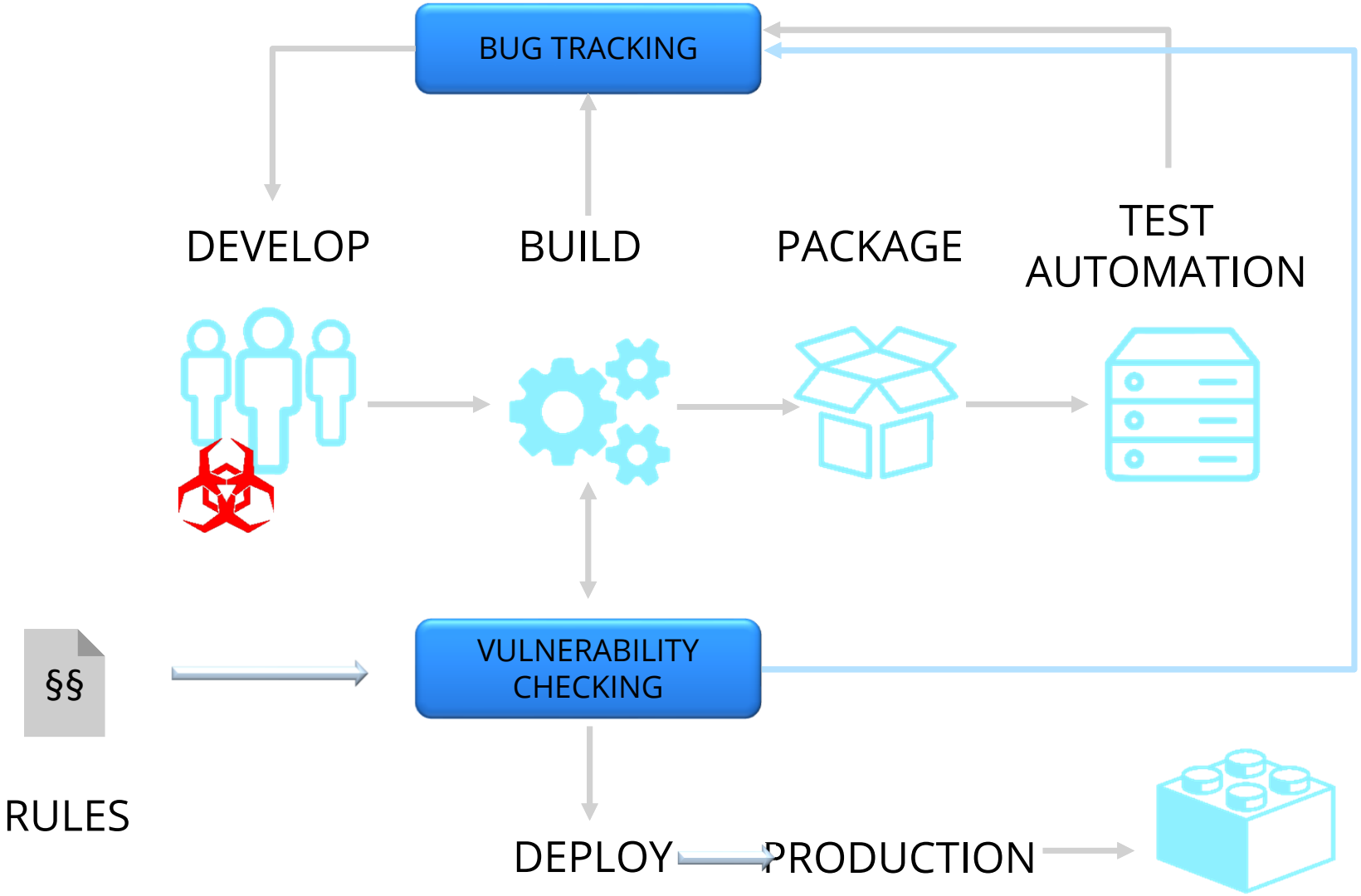
Overall "Waterfall" approach with embedded "Sprint" interations for Build & Test



Automated Fabric - Container Build Process

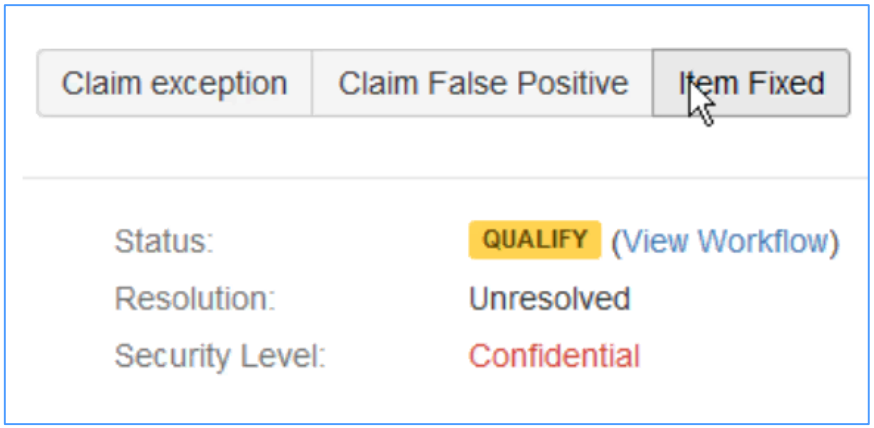
Continuous Development and Deployment (CI/CD)

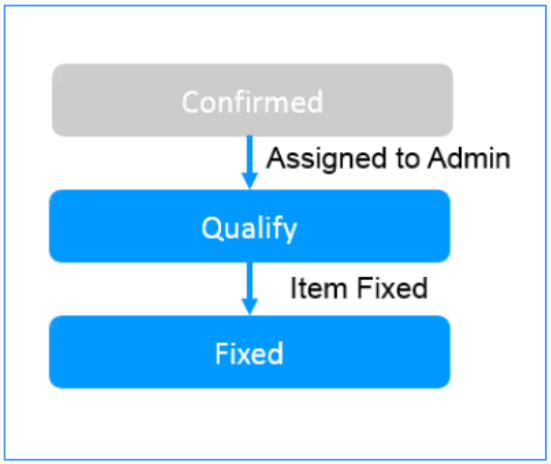


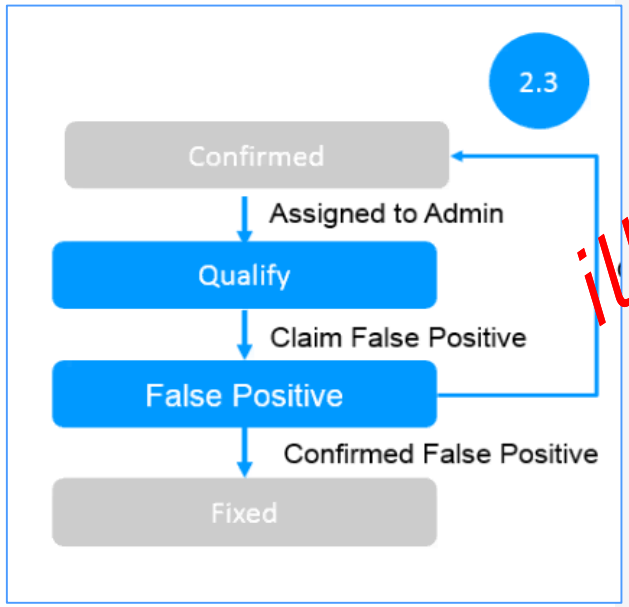


Example - Clearing IT Vulnerability Handling

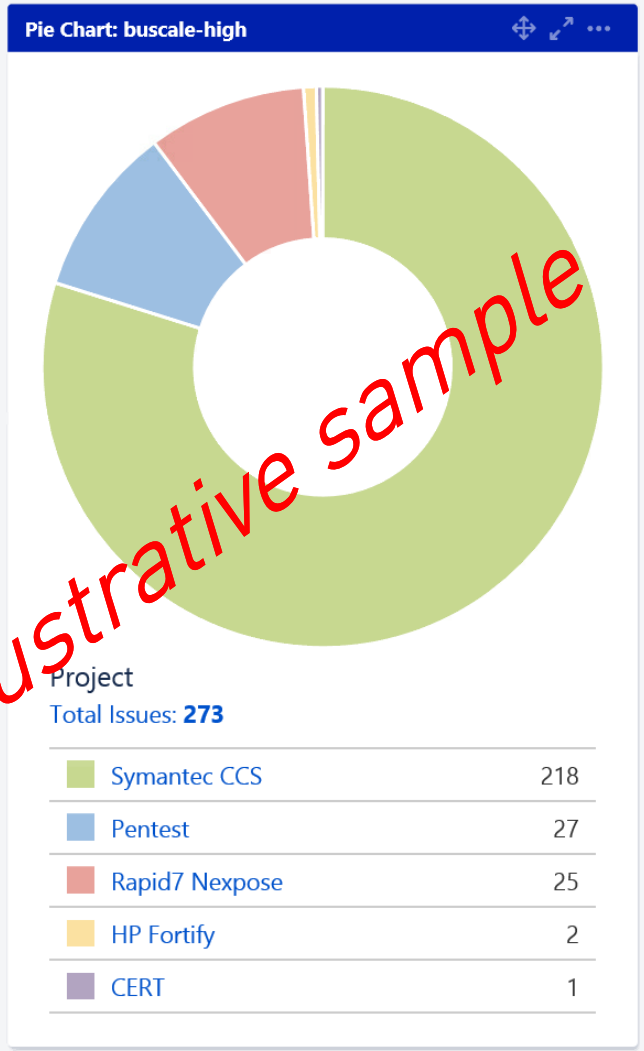
Information Security Issue Workflows with JIRA



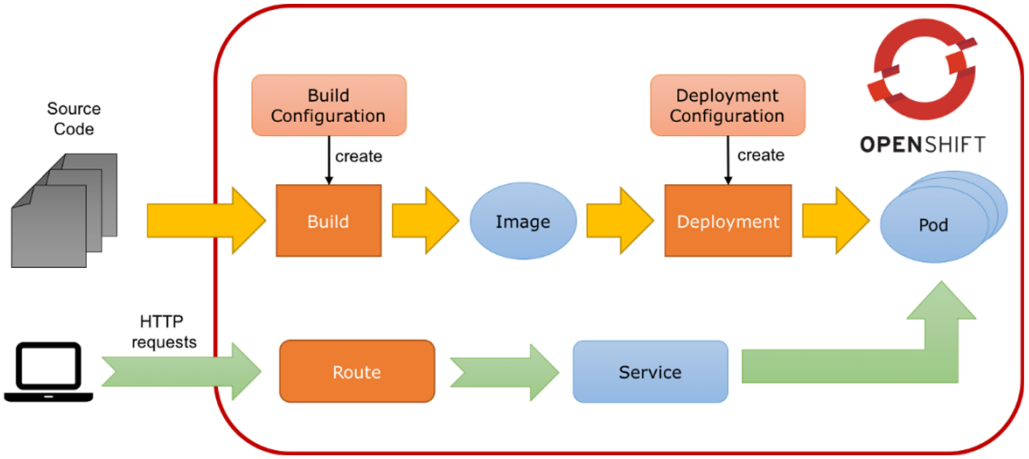


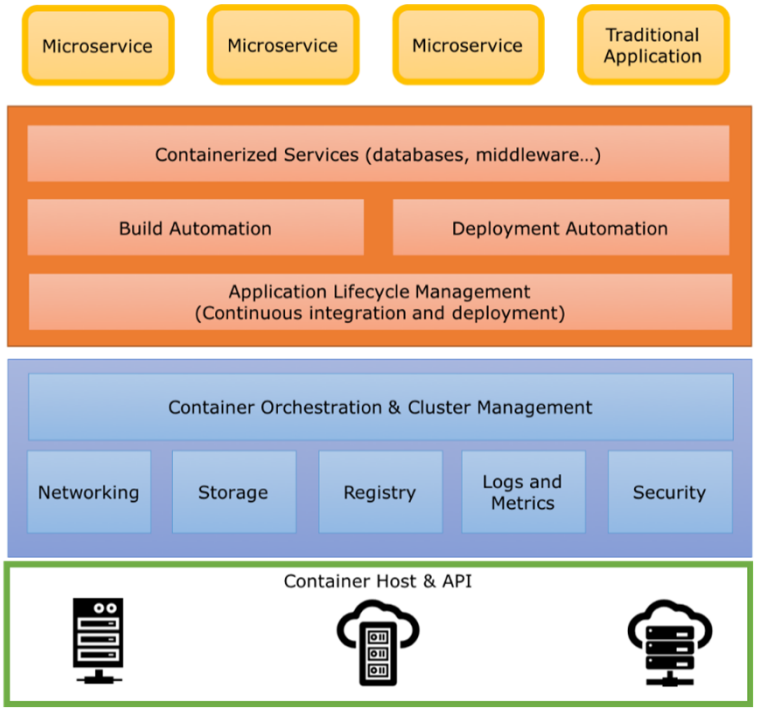


Clearing IT AO Dashboard



Target Picture –Service Routing and Service Layers





Build and Image with Docker files

- Create a CRIO Container by taking a Dockerfile as parameter

Source to Image Build S2I

- OpenShift also provides the concept of S2I (Source to Image) as a tool to provide reproducible images

OpenShift

OPENSHIFT

- OpenShift extends Kubernetes with build automation and a routing system, while inheriting all the primitives from Kubernetes

Kubernetes

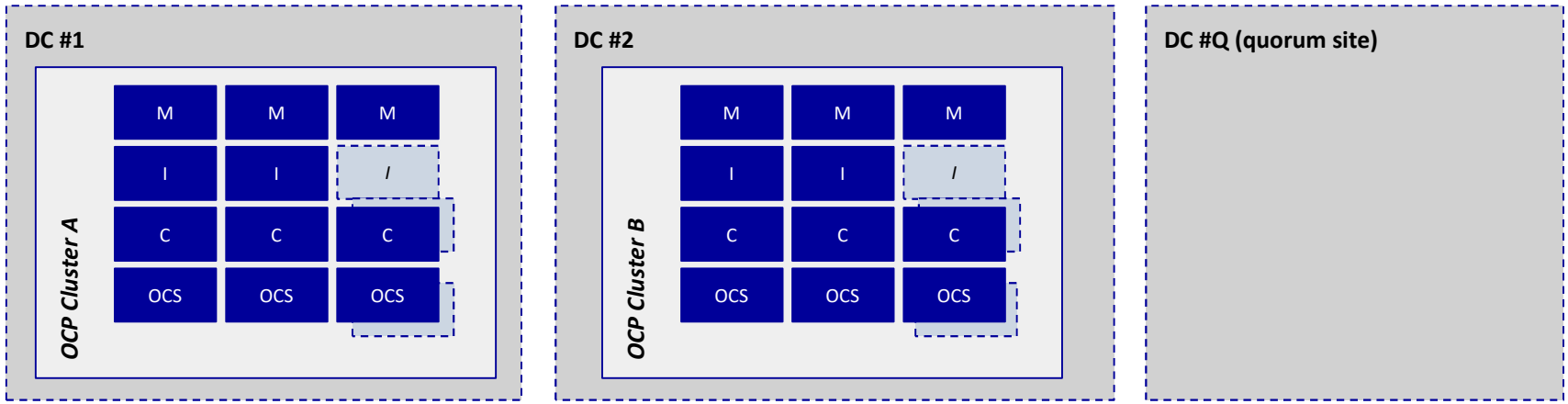
kubernetes

- defines a set of building blocks ("primitives") providing mechanisms for deploying, maintaining, and scaling applications packaged inside containers

OpenShift Infrastructure Proposal – Topology I (on-premise)

Platform Architecture Option: Multiple Clusters (OCPv3 plan, now OCP 4)

Usage of separate OpenShift clusters in each DC, without need for quorum site. Global traffic management for traffic routing to both clusters.



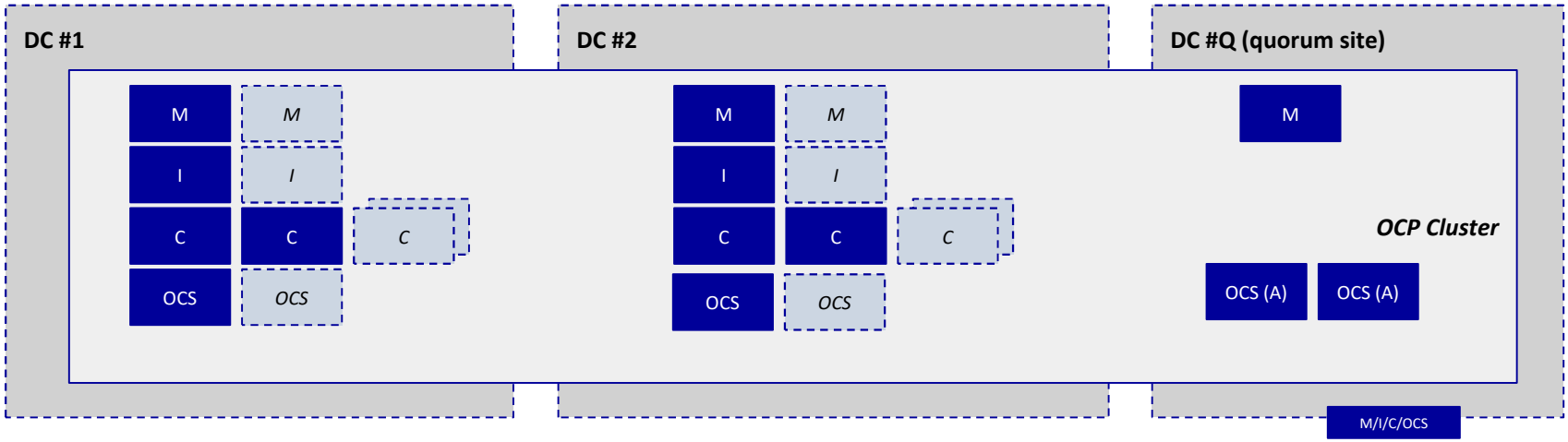
One OpenShift cluster is located solely in one data center.

- Master Nodes: co-located Master services and etcd
  - scaling: 3 masters
- Infra Nodes:
  - scaling: min. 2 nodes; better 3 nodes
- Compute Nodes:
  - scaling: min. 3 nodes
  - note: overall scaling depends on capacity requirements
- OpenShift Container Storage (OCS)
  - min. 3 nodes (with limitations), best 4 nodes (or more depending on storage/load requirements)

OpenShift Infrastructure Proposal – Topology II (on-premise)

Platform Architecture Option: Stretched Cluster (OCP v3 pan, now OCP 4)

*on-premise TARGET SOLUTION: A single OpenShift cluster is stretched across the **two main data centers** and having selected nodes on **a quorum site***



- Master Nodes: co-located Master services and etcd
  - scaling: min. 3 masters - 1 per DC (incl. quorum site)
  - opt. 5 masters - 2 per DC and 1 on quorum site (2 per DC additionally lowers outage risks in case only single DC available)
- Infra Nodes:
  - scaling: min. 2 nodes - 1 per DC
  - opt. 2x2 per DC for additional HA capabilities (in case only single DC available)
- Compute Nodes: distributed across both data centers
  - scaling: min. 2 per DC
  - note: overall scaling depends on capacity requirements
- OpenShift Container Storage (OCS)
  - min. 1 storage node per DC (or more depending on storage/load requirements) and 2 arbiter nodes in quorum site

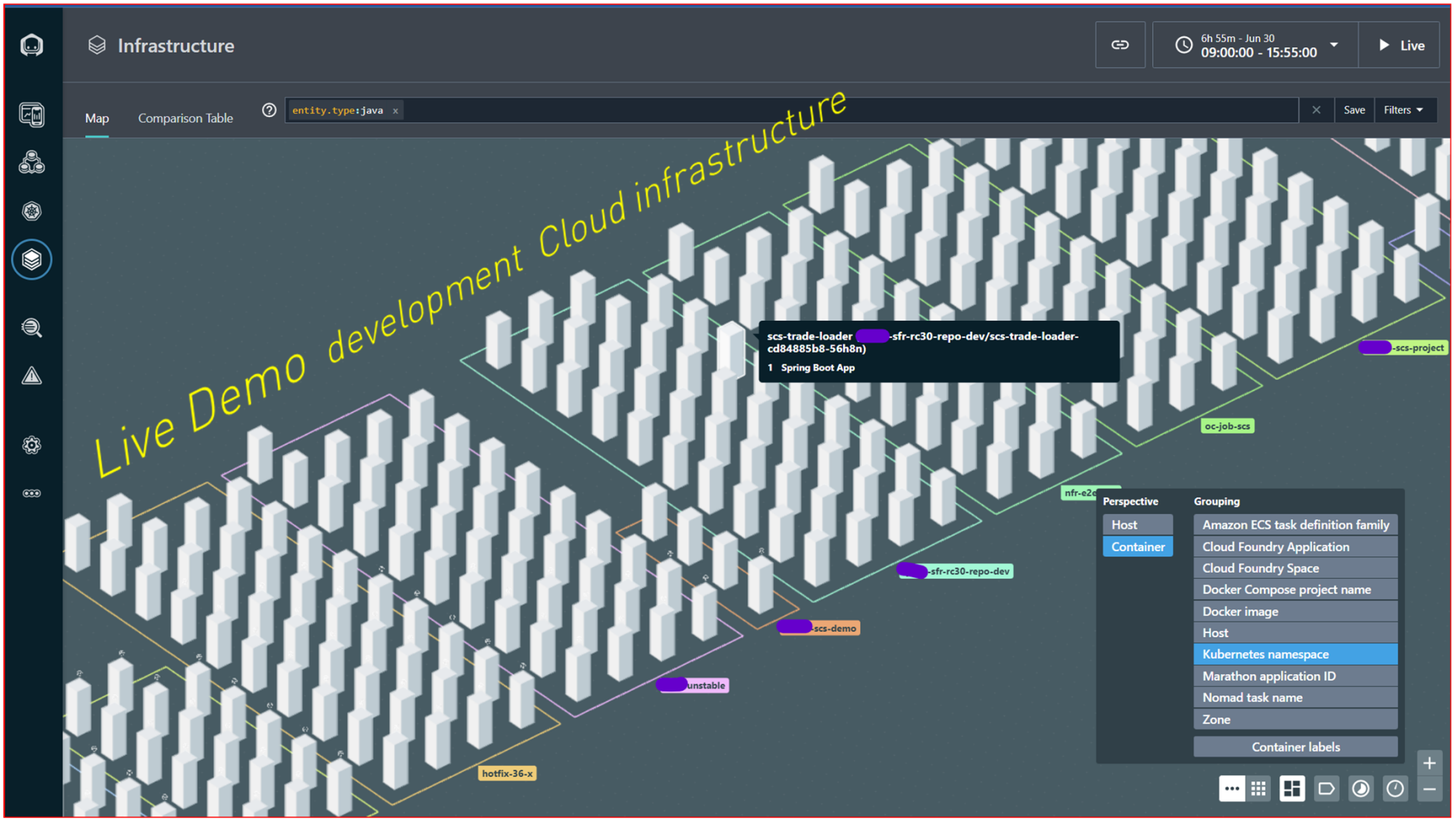
M(aster), I(nfra), C(ompute) Nodes, OCS (OCS Storage Node)

Infrastructure Live View – Dev&Test in **Cloud** (Instana View)

NODE VIEW: AWS node types: m5a.4xlarge (16vCPU, 64 GB) + r5.4xlarge (16vCPU, 128 GB)

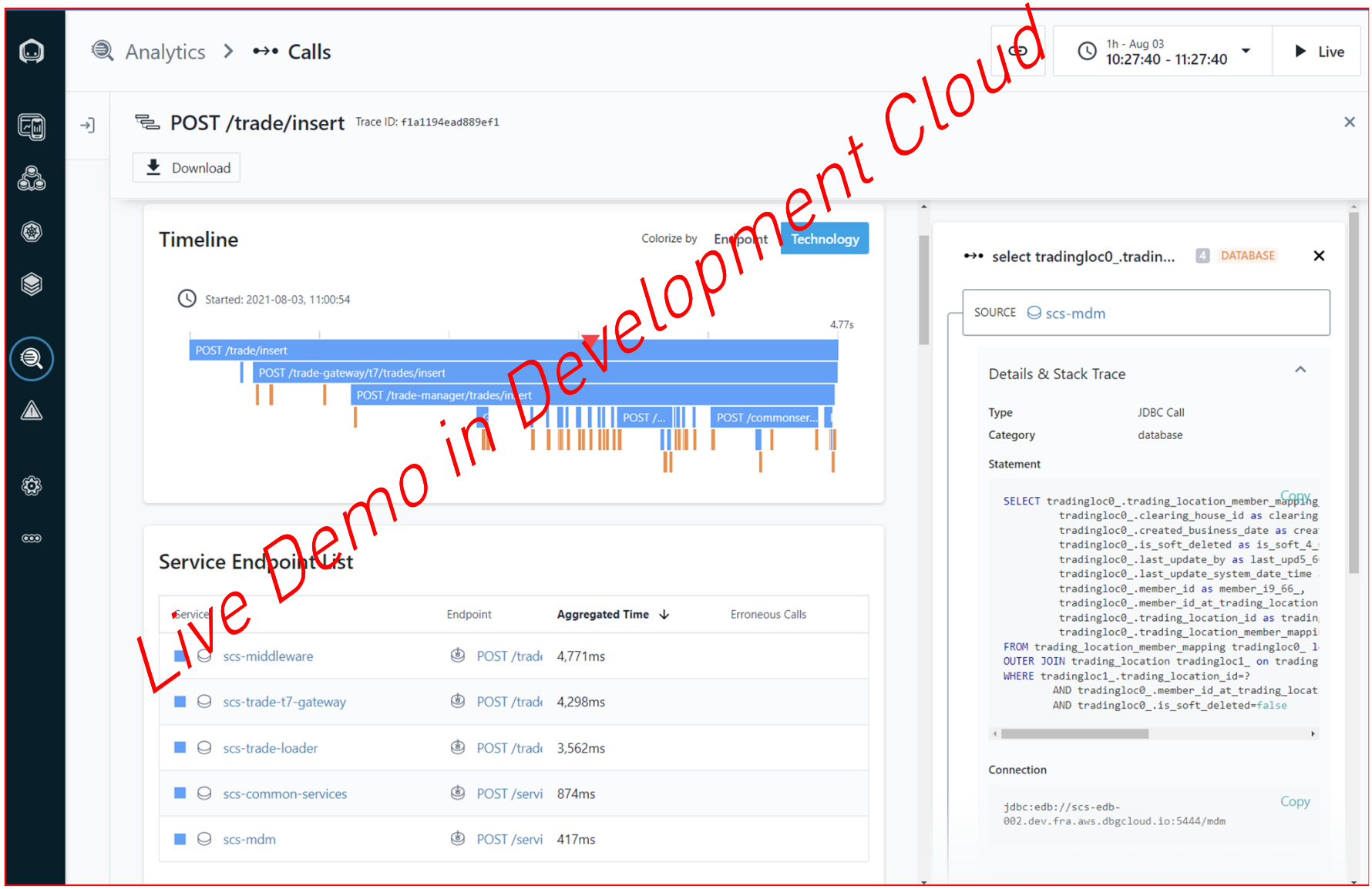
Infrastructure Live View – Dev&Test in **Cloud** (Instana View)

Openshift Kubernetes Name Spaces: Container View -> Multiple C7-SCS Clearing Versions in Test Spaces



Application Tracing - Live View (Instana View)

long query with performance issues



Thank you for your attention.

Clearing and Risk IT
Deutsche Börse AG
60485 Frankfurt am Main
alexander.buschmann@deutsche-boerse.com

Contact

Alexander Buschmann
IS-Lead Clearing IT
Architects Office, Clearing and Risk IT

post office: Deutsche Börse AG, D-60485 Frankfurt am Main
phone (+49) 69 211 - 0
email alexander.buschmann@deutsche-boerse.com

Disclaimer