IBM WW Z Security Conference

October 6-9, 2020

Hyper Protect Virtual Server in action

Corentin Grard

Apprentice

corentin.grard@ibm.com

IBM Hyper Protect Virtual Servers

A Secure Infrastructure Foundation

IBM Hyper Protect Virtual Servers serves as both a solution for external clients to securely build Docker based applications on IBM Z and LinuxONE and a foundational component of IBM solutions

Hyper Protect Digital Assets Platform

Enabling custodians, exchanges, & Distributed Ledger Technology (DLT) ecosystem participants to protect tokenized assets and valid participants for DLT transactions

Data Privacy Passports

Provide a secure host environment to deploy the Passport Controller, used for policy enforcement and data transformation in Data Privacy Passports

Client Workload

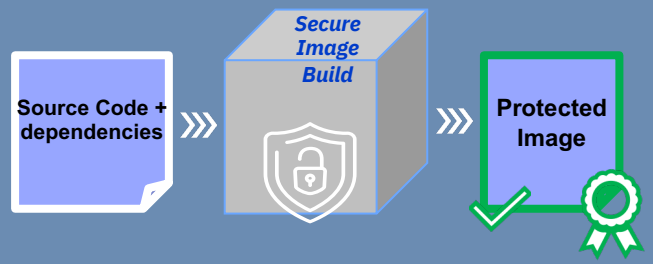
Target sensitive workloads that require a high degree of isolation and data protection to meet security & compliance needs for their organization, industry, or geography

Red Hat OpenShift

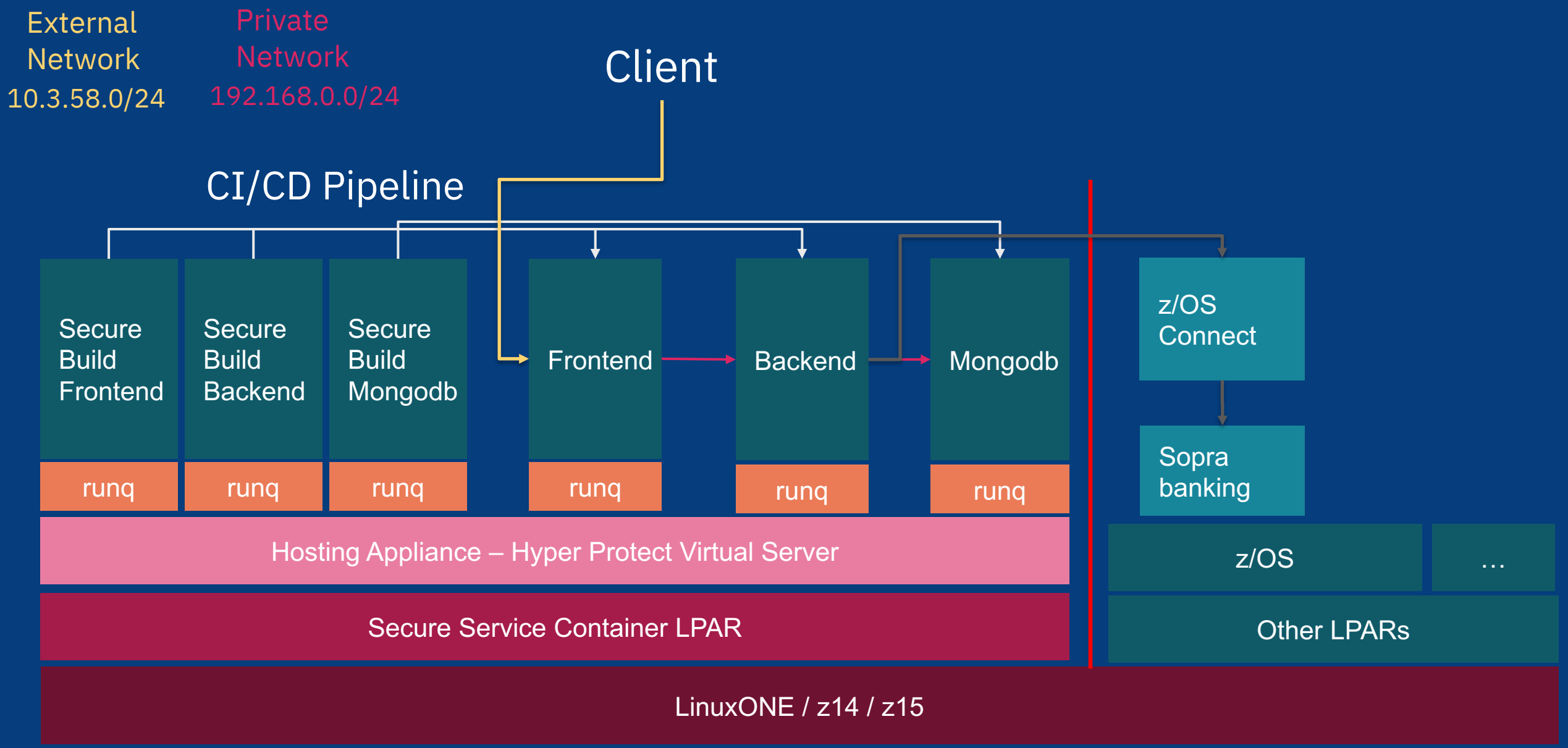
FUTURE / ROADMAP: Enable clients to securely build their Platform as a Service, protecting critical containerized workloads from even cloud / k8s administrators

IBM Hyper Protect Virtual Servers on-prem

Protect critical Linux workloads during build, deployment, and management on-premise for IBM Z and LinuxONE servers

Build	**Deploy**	**Manage**	**Secure**
code with security	**workloads with trust**	**workloads with simplicity**	**images with assurance**
Leverage the secure image build process to sign images, validate code, and integrate into CICD	*Provenance - Validate the origin of your applications before deployment*	*Manage infrastructure without visibility to sensitive code or data – RESTful API deployment invoked via CLI*	*Provide images access to industry leading FIPS 140-2 level 4 Hardware Security Module for signing and encryption*
Key Features: • Hosting Appliance • Virtual Server images • Secure Image Build • CLI Tool • Grep 11 Server Container • Host Monitoring Container			***GA since February 2020***

Demonstration : Architecture

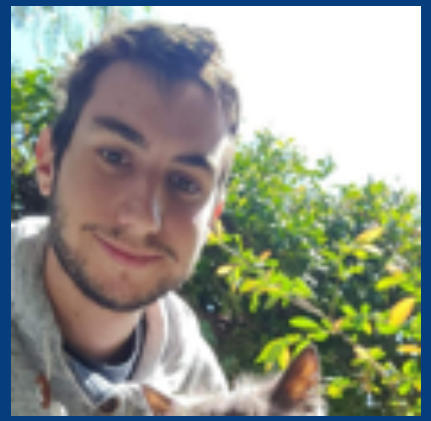


Demonstration : Roles

System Administrator

Appliance Administrator

Cloud Administrator



Developper

How to create a SSC LPAR for Hyper Protect Virtual Servers

System Administrator

1 Connect to HMC

2 Go in Activation Profiles and select SSC

3 Add :
- Default ID and Password
- IP address
- CPU and storage

4 Boot the partition

More details here : https://www.ibm.com/support/knowledgecenter/SSHPMH_1.2.x/topics/create_ssc.html

How to create an Hyper Protect Appliance

Appliance Administrator

1 Install the appliance

2 Login to the web interface with the id/pwd entered by the System administrator

3 Configure the network and the storage

More details here : https://www.ibm.com/support/knowledgecenter/SSHPMH_1.2.x/topics/setup_ssc.html

How to configure an Hyper Protect Virtual Servers

Cloud Administrator

1

Login to the management server

2

Run the initialisation script

Create signing keys

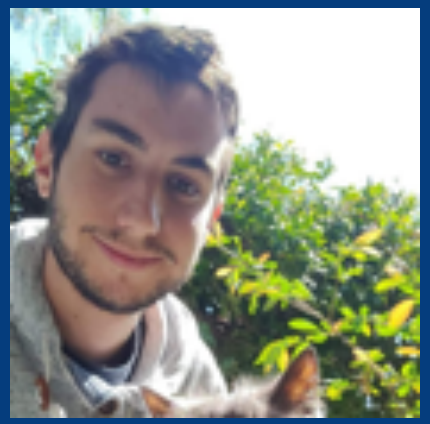
3

4

Deploy secure builds ar
virtual servers

More details here : https://www.ibm.com/support/knowledgecenter/SSHPMH_1.2.x/topics/setup_shscript.html

How to deploy application into Hyper Protect Virtual



Developer

1

Publish to GitHub

Generate & sign secure build

2

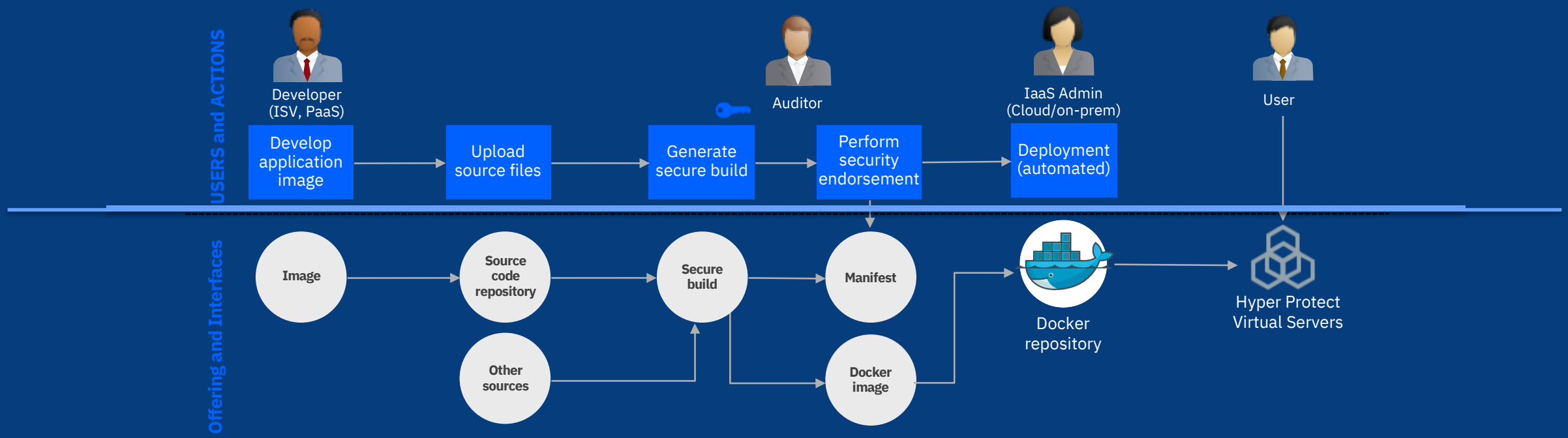
Store signed image in DCT

3

Docker Content Trust

4

Automated deploy with trust chain.



How Hyper Protect Virtual Servers COMBATS risks:

- **Sign** application via secure build flow
- **Encrypt** and **register** application configuration info
- **Check image provenance** via workload **manifest**
- **Decrypt** application **registration file** – only possible via Secure Service Container (trusted execution environment)
- **Manage** infrastructure **via only RESTful interfaces**

Thank you for your attention