Can you Trust your Cloud?
How to Build a Secure Hybrid Cloud
with IBM LinuxONE/Z and SUSE

Adam Jollans, IBM
Mike Friesenegger, SUSE

SUSECON
April 2019
Trust, Growth, and Digital Transformation

**Business Drivers**

- Building Trust
- Enabling Growth
- Delivering Digital Transformation

**Infrastructure Requirements**

- Security
- High Availability
- Scalability
- Performance
- Next Gen Applications
- Cloud Integration
Questions to ask your IT infrastructure

Scalability
– Can your IT infrastructure sustain Growth?

Security
– Can your IT infrastructure deliver and prove Security?

Availability
– Can your IT infrastructure deliver always-on services that you can rely on?

Flexibility
– Can your IT support applications in the public cloud, private cloud and on-prem?
Case Study – ICU IT Services (Rockhopper)

Business challenge
ICU IT Services aims to create the next generation of Enterprise IT by developing innovative solutions and services that break new ground and provide game-changing benefits to clients.

Transformation
ICU IT Services is the first in BeNeLux to deploy an IBM® LinuxONE™ platform, which it plans to use to develop innovative solutions and deliver dramatic IT savings for businesses that want to combine the best of enterprise server and Linux technologies.

Business benefits
Up to 50% estimated savings on IT costs for clients
Grows the company’s influence, market share and revenues
Drives innovation through the creation of an exclusive IT laboratory set-up

ICU IT Services
Merging the best of open-source and enterprise technology for solutions built to capture new clients

"With the IBM LinuxONE Rockhopper, ICU IT Services helps businesses slash their IT costs by up to 50 percent."
—Ron Eland, Managing Partner and CEO, ICU IT Services

ICU IT Services is a Dutch IT infrastructure specialist that wants to create the next generation of Enterprise IT. Specialized in designing and implementing large and complex Enterprise IT infrastructures, ICU helps businesses to construct more efficient and secure IT environments. With its team of 40 highly skilled professionals, the company focuses on the interaction between platforms and applications; in particular availability, scalability, security, management and reliability of the z/OS and Linux platforms.
IBM LinuxONE

- Enterprise-class Linux system
- Highly-engineered data server
- Agile and flexible cloud platform

Key Ingredients

- IBM Z technology
- Linux – SUSE, other distributions
- Open source databases, containers, runtimes,…
- IBM and ISV business applications
SUSE Linux Enterprise Server
Common Code Base

Benefits across 3 dimensions:
Hardware Architecture, Applications and Systems Management

Ensure Consistency
Improve systems management
Simplicity in support and services
Silicon agnostic computing
Support IBM LinuxONE to Raspberry Pi

“IDC believes the common code base of SLE 15 makes the product a multi-platform OS that is well suited for heterogeneous computing environments.”
IDC Market Note, 2018
Items included in a SLES subscription for Z and LinuxONE that may be overlooked

- Support SLES running in an LPAR and as a z/VM guest
- KVM included and fully supported
- SLE Modules*
  - Server Applications
  - Web and Scripting
  - Desktop Applications
  - Development Tools
  - Public Cloud
  - Containers
  - Legacy

- Package Hub
  - Over 12,800 packages available**

* Module names may be different between SLES 12 and 15
** SLES15 Package Hub
SLE Extensions

- **High Availability**
  - Has been available for SLES for Z for many years
  - Is included in the SLES for Z subscription*
  - A use case is Oracle and DB2 database failover when Oracle RAC or DB2 pureScale is not needed
    - SHARE presentations are available on this topic

- **Live Patching**
  - Not available of SLES for Z
  - Customers are interested – contact SUSE if you are interested
  - Use case is delayed reboot after kernel patch of mission critical database servers

* Exceptions exist depending on special offerings
SUSE Manager

Easily manage large complex deployments

- **Formulas with Forms** improved/extended to model even complex parameters (e.g. for user management) and fully API-enabled
- Salt states can now be created and edited completely from the UI
- **Action chains for Salt minions** *(update Salt through Salt, reboots, …)*

SUSE Manager 3.x is supported on IBM Z and LinuxONE

- Look at the SUSE Manager Advanced Topic Guide for server installation details
- **Version 3.2 Includes**
  - Salt 2018.3.0
  - Spacewalk 2.8
  - PostgreSQL 9.6
  - SLE 15 enablement

---

[Uyuni](https://www.uyuni-project.org)

New upstream project for SUSE Manager
Container support in SLES for IBM Z and LinuxONE

- docker container engine (part of Containers module)
- Base SLES images from registry.suse.com
  - SLES12 SP3 & 4: `docker pull registry.suse.com/suse/sles12spX`
  - SLES15: `docker pull registry.suse.com/suse/sle15`
- Local registry via docker-distribution-registry package
  - Enable SUSE Package Hub repo to install
The IBM LinuxONE Portfolio

IBM LinuxONE Emperor™ II

Built on decades of trusted IBM Technology

IBM LinuxONE Rockhopper™ II

The world’s premier Linux systems for highly secured data and cloud serving

Engineered for performance and scale

Foundation for data serving and next generation apps

Machine Type: 3907
Model: LR1
Up to 30 cores and 8TB

Machine Type: 3906
Models: LM1, LM2, LM3, LM4, LM5
Up to 171 cores and 32TB

Built for the cloud with Standardization and Simplicity

Lower cost than x86 for mission critical data serving

Right sized for your business needs
# Rich Open-source Ecosystem at a Glance

<table>
<thead>
<tr>
<th>Distributions</th>
<th>Hypervisors</th>
<th>PaaS / IaaS</th>
<th>Languages</th>
<th>Runtimes</th>
<th>Management</th>
<th>Database</th>
<th>Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUSE</td>
<td>LPA</td>
<td>docker</td>
<td>python</td>
<td>node</td>
<td>chef</td>
<td>kubernetes</td>
<td>Oracle</td>
</tr>
<tr>
<td>redhat</td>
<td>R</td>
<td>KVM</td>
<td>php</td>
<td>rails</td>
<td>puppet labs</td>
<td>juju</td>
<td>Spark</td>
</tr>
<tr>
<td>ubuntu</td>
<td>LXD</td>
<td>IBM Cloud Private</td>
<td>R</td>
<td>LLVM</td>
<td>Ansible</td>
<td>MySQL</td>
<td>Elasticsearch</td>
</tr>
<tr>
<td>supported by Canonical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debian</td>
<td>openstack</td>
<td>OpenShift</td>
<td>Scala</td>
<td>OpenJDK</td>
<td>etcd</td>
<td>Sysdig</td>
<td>MongoDB</td>
</tr>
<tr>
<td>Fedora</td>
<td>Mesos</td>
<td></td>
<td>Clojure</td>
<td>LLVM</td>
<td>Apache Zookeeper</td>
<td>PostgreSQL</td>
<td>Solr</td>
</tr>
<tr>
<td>openSUSE</td>
<td>LXD (Ubuntu)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>MariaDB Foundation</td>
<td>Tensorflow</td>
</tr>
<tr>
<td>CentOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Anaconda</td>
</tr>
<tr>
<td>Community Versions</td>
<td>Community Versions</td>
<td>Community Versions</td>
<td>Community Versions</td>
<td>Community Versions</td>
<td>Community Versions</td>
<td>Community Versions</td>
<td>Community Versions</td>
</tr>
<tr>
<td>CentOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ubuntu</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Hypervisors**
- LPA
- R
- KVM

**Distributions**
- SUSE
- Red Hat
- Ubuntu
- Debian
- Fedora
- openSUSE
- CentOS

**PaaS / IaaS**
- docker
- IBM Cloud Private
- LXD

**Languages**
- python
- php
- R
- Scala
- Clojure
- JavaScript
- Java
- Swift

**Runtimes**
- node
- rails
- OpenJDK
- LLVM
- OCaml
- Lua

**Management**
- chef
- puppet labs
- Ansible

**Database**
- MySQL
- MongoDB
- Solr

**Analytics**
- ES
- TensorFlow
- RethinkDB
- Db2

---

**Community Versions**
- openSUSE
- CentOS
- Debian
- Fedora
- Ubuntu

---

**Open Mainframe**

---

**The Linux Foundation**
IBM LinuxONE: Engineered for Security, Scalability, and Cloud

TRUST
The world's premier Linux® system for highly secured data & cloud serving

- Pervasive Encryption for data at rest and in flight
- Industry-leading workload and tenant isolation
- Secure Service Container technology to help protect data and applications from internal and external threats

GROWTH
Engineered for performance and scale

- Consolidate hundreds of x86 cores on a single system¹
- Dedicated I/O processors to move massive amounts of data with uncompromised data integrity
- Vertical Scale architecture for responsiveness and efficiency

DIGITAL TRANSFORMATION
Foundation for data serving and next generation apps

- Performance and scale to consistently deliver on client and business demands
- Security and reliability to keep businesses up and running
- Support for vast portfolio of IBM, ISV and open source SW to support new application development and deployment
- Ability to reduce costs over x86²

¹ IBM LinuxONE / LUP12389 / April 10, 2018 / © 2018 IBM Corporation
² IBM LinuxONE / LUP12389 / April 10, 2018 / © 2018 IBM Corporation
A Different Approach to IT Infrastructure – IBM LinuxONE

- Centralized
- Optimized
- Flexible
- Modern
Security

Pervasive Encryption
- On-chip crypto
- CryptoExpress

Crypto Key Protection
- HSM

Workload Isolation
- Logical Partitions

Secure Service Container
- Software appliance environment
Fast encryption of Linux workloads, delivered with near-zero overhead via hardware accelerated encryption by Central Processor Assist for Cryptographic Function (CPACF) and new Crypto Express6S
- All encryption functions within the Linux kernel and the openSSL, open Cryptoki and GSKIT libraries are benefiting and transparently delivering the performance to the applications and middleware

LinuxONE enhanced security via “protected key” encryption for data at-rest
- Protected key encryption is processed in the CPACF for high speed, stored in a hardware security module (HSM), and enables fast encrypting and decrypting of complete disks (volumes) or selected partitions

LinuxONE enablement to create true unique cryptographic data using the new true random number generator (TRNG) with CPACF

Performance boost for Java with new Galois Counter Mode (GCM) encryption for minimal latency and operational overhead

Note: All claims noted on this slide are based on IBM Internal measurements. Results may vary. Additional information is available upon request.
Pervasive encryption support in SUSE Linux Enterprise Server

SLES12 SP4

• Data-at-rest support
  – CEX6S crypto card in the z14 is fully supported
  – Protected key crypto for dm-crypt disks in plain format
  – zkey in s390-tools, enables management of a key repository and association of secure keys
    with disk partitions or logical volumes

• Data-in-flight support
  – Kernel services exploit IBM z14 cryptography hardware for the AES-GCM cipher
  – openSSL libraries 1.0.2p and 1.1.1 available

Additional enhancements included in SLES15

Planned how-to guide for at-rest and in-flight with SLES15 SP1
IBM Secure Service Container
For secure deployment of software virtual appliances

Positions LinuxONE® as a viable platform for hosting modern, cloud-native, container-based applications in line with the organization’s overall Docker container strategy; with it you can:

– Create enriched services and product offerings that are built on a security-rich container foundation

– Isolate and protect the container data from misuse of privileged user credentials, helping to protect the data and execution code from internal or external threats, inadvertent or malicious

– Minimize the risk of tampering or malware to the solution code

Supports pervasive encryption principles
Solitaire Report – “Scaling the Digital Mountain”

Research-based study

- Data gathered on market evolution and production behaviour over 40 years
- Based on data from thousands of clients, and built into a granular repository
- Predictive modeling used to compare platforms on a range of dimensions

Key Findings

- Customers running LinuxONE realize up to 2 times more consistency in the delivery of end-user requests than recorded on other platforms
- SIL risk profiling sets the LinuxONE platform risk rating at less than 1/20 of any of the alternative solutions
- The TCO for LinuxONE implementations is lower by as much as 82.12% less than for those of other platforms
Scalability

Vertical
- Up to 170 cores
- Up to 32TB memory
- Up to 600 I/O procs

Horizontal
- Up to 86 Logical Partitions
- Tens of thousands of virtual machines
- Millions of containers

Diagonal

LinuxONE Hardware
- CryptoExpress
- HSM
- Processor
- Crypto
- Memory
- I/O
- Comms

LinuxONE Software
- App
- App
- App
- Linux
- Linux + DB
- Blockchain
- Linux
- App
- App
- App
- Linux + IBM Cloud Private

Software Virtualization

Firmware Virtualization

Secure Service Container

Linux + DB App

Blockchain App

Secure Service Container

Comms
Linux workloads benefits from Co-location on IBM Z with core transaction systems

| Integration with transaction systems | • ‘Systems of interaction’ and ‘Systems of record’ run on one server  
• Integration of Blockchain apps with existing transaction systems, such as IBM CICS, IBM WebSphere apps, or IBM Db2 |
| Performant communication | • Quick response times and less application waits with minimal latency based on large cache and high I/O bandwidth  
• Fast internal connections, Small Memory Communication (SMC), HiperSockets, or shared OSA cards  
• Applications and analytics processing next-to the data |
| Scalability 'Data center-in-a-box' | • Up to thousands workloads on a single Z server  
• Non-disruptive horizontally and vertically growth inside Z - On demand  
• Simply adding: cores, I/O adapters, memory, devices, and network |
| Operational efficiency | • Same arrangements for administration of security, backup and disaster recovery (IBM GDPS), etc.; elimination of network traffic handling  
• Temporary resource activation through ‘On/Off Capacity on Demand’  
• Technology upgrades is easy and fast; often done on a weekend |
Business challenge
Taking on tens of millions of members each year, how could SinfoníaRx ensure fast, accurate analysis of prescription data to help improve patient outcomes and save healthcare providers millions?

Transformation
As demand for its healthcare data analytics services rocketed, SinfoníaRx needed a data-processing platform capable of huge scalability and uninterrupted performance. Choosing IBM® LinuxONE™ has helped the company grow to serve one in every seven U.S. citizens, and deliver billion-dollar cost savings to the nation's healthcare industry.

SinfoníaRx
Delivering better patient outcomes and billion-dollar savings through analytics

SinfoníaRx is an industry leader in Medication Therapy Management (MTM) services, helping optimize medication use and improve the health of patients with chronic illness. Its highly customizable MTM programs support approximately 50 million patients in across more than 350 health plans.

Solution components
- IBM® Db2®
- IBM LinuxONE™

Business benefits
>$1B
in cumulative savings delivered to the healthcare industry

>20M
members onboarded within a single year with no impact on performance

1 in 7
U.S. citizens served with potentially life-saving analytics

“LinuxONE gives us the confidence that we can meet our clients’ needs even as our business continues to grow rapidly.”

—Jeffrey Pochily, VP of Network Infrastructure, SinfoníaRx

Share this

© 2017 IBM Corporation
Challenges and Concerns for IT Leaders

Less than 20% of enterprise workloads have moved to the cloud

82% of customers are concerned about how they will connect public, private clouds, other SaaS applications, and traditional IT

Source: McKinsey research

Businesses with IBM Z are integrating across platforms

- Maintain a hybrid or other cloud ecosystem
- Develop applications for cross platform deployment
- Use of APIs for the mainframe

73%+

Source: Initial results from 5 in-depth interviews as part of the 2019 IDC Business Value Connected Mainframe study co-sponsored by Broadcom & IBM.
20% of workloads have moved, but what’s preventing Rapid Modernization of the remaining 80%?

**Unique workload needs** – compliance, security, location—requires more choice

**Multiple clouds and vendors** – hard to connect/manage across clouds and IT

**Lack of necessary skills** – how do you prioritize and deliver modernization

**Open, highly secure public and private** optimizes data/workload placement without lock in

**Hybrid integration & multi-cloud management** delivers end-to-end visibility and control

**Expertise & methods** industry experience, proven methods and tools to help prioritize and modernize

---

**IBM.**

**Expertise**

Cloud
- 90,000 experts
- 100,000 migrations
- 38 global studios

Security
- 60 billion security events managed per day

Data
- 20,000 data scientists, developers, and consultants

Industry
- Depth in 20 industries
- $6 billion in R&D
- Patent leader 25 yrs
Five Key Principles Define IBM’s Approach...

1. Hybrid
   Enable enterprises across Public, Private, and traditional environments

2. Multicloud
   Manage other vendors’ Clouds, acknowledging the reality that client environments are heterogeneous

3. Open
   Build capabilities that are open by design, enabling client flexibility and reducing vendor “lock in”

4. Secure
   Provide reliability and continuous security for the client’s environment

5. Management
   Consistent service level, support, logging, management & delivery across complete cloud environments

Delivered by a composable cloud platform that is uniquely...

Multimodal
(VM, Containers, Bare metal, Serverless)

Multiarchitecture
(x86, Power, IBM i, AIX, IBM Z)

IBM Cloud Platform

Addressing both Enterprise and Hyperscale workloads
Bringing the resiliency of IBM LinuxONE to IBM Cloud

A new standard for “hyper protection” of data at rest, in memory and in motion, with minimal work for your developers.

**Built-in tamper proof security**

**Pervasive encryption** of data at rest, and in transit

**No cloud / system admin access** (ssh not possible once appliance image is built) which prevents malicious attacks

Signed **Docker images inherit security without any code changes**, prevent access to data while being processed in the database

**Secure Key technology** designed to meet **FIPS 140-2 Level 4** security (crypto) certification, the highest level of security possible, which leads all other cloud providers

**Unmatched scale and performance**

**Unmatched vertical scale** *

Up to 170 cores, 32 TB memory, 85 LPARs in a single Emperor II system and no need for application re-

**Faster data serving** *

- 1.5x - 2.8x better throughput (Java, Node, PostgreSQL, MongoDB)
- Ability to scale to 1,344 concurrent databases executing 377B transactions/day and <1ms response time,
- e.g - Scale a single MongoDB to 17TB with no sharding

* LinuxONE versus the x86 platform
IBM Cloud Private

Optimize your investment and modernize your applications
• Self-service catalog
• Agility, scalability, and elasticity
• Self-healing
• Enterprise security
• No vendor lock-in

One solution across multiple architectures

Choose your infrastructure:

- Enterprise Content Catalog
  Open Source and IBM Middleware, Data, Analytics, and AI Software
- Core Operational Services
  Log Management, Monitoring, Metering, Security, Alerting
- Kubernetes Container Orchestration Platform

Choose your infrastructure:

- Power Systems
- OpenStack
- IBM Spectrum

Choose your infrastructure:

- VMware
- IBM Z
- Intel
Next steps

- IBM stand at SUSECON - 211
- LinuxONE for Dummies
  - printed copy in SUSECON bag
- LinuxONE website
  - https://www.ibm.com/linuxone

Information for developers

- IBM continues to invest in open source and Linux.
- IBM has a robust developer community (developerWorks) and partner ecosystem (IBM PartnerWorld) that you are welcome to join at no additional fee. The websites are listed here and the QR codes are displayed for your convenience.
  - http://ibm.com/partnerworld/
Notice and disclaimers

© 2018 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM. Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply. Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.
Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.