Pervasive Encryption and High Security with Linux on IBM Z

Data protection and compliance are business imperatives

In the era of ever-present attacks and breaches, security and compliance regulations had become very important. Also new and emerging regulations are coming out all the time, the most important in 2018 had been the European Union General Data Protection Regulation (GDPR), New York's Cybersecurity Requirements for Financial Services Companies and Australia’s Notifiable Data Breach (NDB) scheme and some years ago, the Payment Card Industry Data Security Standard (PCI-DSS).

The rationale behind passing these standards is to help organizations better protect customers' privacy and security by design.

"Breaches are no longer a binary proposition where an organization either has or hasn't been breached. Instead they are wildly variable—having varying degrees of fallout—from breaches compromising entire global networks of highly sensitive data to others having little to no impact whatsoever."\(^1\)

Encryption

Extensive use of encryption is an extremely effective way to help reduce the risks and financial losses of a data breach and help meet regulatory requirements and compliance mandates.

However, when it comes to implementing encryption organizations struggle with questions such as:

- What data should be encrypted?
- Where should encryption occur?
- Who is responsible for encryption?

Designed for Pervasive Encryption

The IBM® z15™ (z15) and IBM z14® (z14) are designed for pervasive encryption, delivering a consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify encryption and reduce costs associated with protecting data and achieving compliance mandates.

Both, z15 and z14, excels with security features that are built into the hardware, firmware, and operating systems. This includes cryptographic performance improvements with the on-core hardware accelerated encryption via CPACF\(^2\), Crypto Express features—certified to FIPS 140-2 Level 4, and IBM Secure Service Container.

In addition, IBM Data Privacy Passports, in conjunction with z15 and available via a z15 only IBM software product, is designed to enforce security and data protection to data not only on IBM Z®, but across platforms.

Linux on IBM Z and the world of Comprehensive Encryption

Encryption support is an integral part of the Linux operating system, and the concept with Linux on IBM Z is providing differentiation without being different.

This is accomplished by integrating the exploitation of the IBM Z encryption hardware features into strategic components of the stack, such that applications can transparently benefit.

This enables organizations to exploit the z15 and z14 cryptographic hardware capabilities with their existing Linux cryptographic infrastructure, kernel, and standard libraries encryption, while improving the usability and performance of encrypting/decrypting the data.

---

\(^1\) Source: Breach Level Index, [http://breachlevelindex.com](http://breachlevelindex.com)

\(^2\) CPACF = Central Processor Assist for Cryptographic Function
Important for the pervasive encryption with Linux is the integration of the ‘protected key’ capability, which is unique to IBM Z servers.

‘Protected key’ encryption provides keys that are processed by the on-core cryptographic acceleration, while being protected by keys hidden in the IBM Z firmware, not accessible to any software. Protected keys are volatile in nature and are derived from secure keys that are encrypted using a master key that is protected by a tamper-responding HSM\(^3\) in the Crypto Express features.

All Linux workloads can benefit from the fast encryption in z15 and z14, since the encryption functions in the Linux kernel, and the libraries, openSSL, openCryptoki, GSKIT and Java 8/ JCE, are transparently delivering the performance to the applications.

Java applications can benefit from hardware support to accelerate the GCM\(^4\) cryptographic mode for block ciphering, and the on-core true random number generator allows to generate irreproducible unique data, which is the basis to generate high quality keys.

Linux on IBM Z is well equipped for encrypting all data in-flight using protocols like TLS, SSH, or IPSec. Exploiting the outstanding cryptographic performance of the z15 and z14, Linux users can afford to encrypt their network traffic in a transparent manner using OpenSSL, OpenSSH, and IPSec.

Organizations can protect their data during the complete journey from Linux on IBM Z through the cryptographic hardware, the SAN infrastructure into the storage server cache, and finally on the storage devices. They don’t have to change their encryption approach, they simply can get consumable data protection.

Enhancements to the z15 continue to deliver critical cryptographic capabilities which address the ever-changing requirements. The CPACF capabilities are extended, and performance improvements will be available with CPACF and the new Crypto Express7S adapter.

z/VM\(^7\) V7.1 and V6.4 and KVM provide support to enable the crypto hardware exploitation by Linux guests in support of encryption of data in-flight and data at-rest. As well, the z/VM versions support encrypted paging—using protected keys, ciphering occurs as data moves between active memory and a paging volume—protecting guest paging data from users and administrators.

**Specific IBM Z hardware security**

The IBM Z logical partitioning (LPAR) technology is the only commercial platform with an EAL5+ hardware security certification. This certification level means that workloads are isolated when running in separated LPARs.

The IBM Secure Service Container allows for deploying software appliances into LPARs that can’t be inspected by system administrators.

**Summary**

Data protection and compliance are no longer a matter of if, and with Linux on IBM Z you can provide comprehensive data protection that your organization and customers demand, and that can slash the associated.

Linux on IBM Z can provide the security demanded by your most valuable data.

---

\(^3\) HSM = Hardware Security Module

\(^4\) GCM = Galois Counter Mode