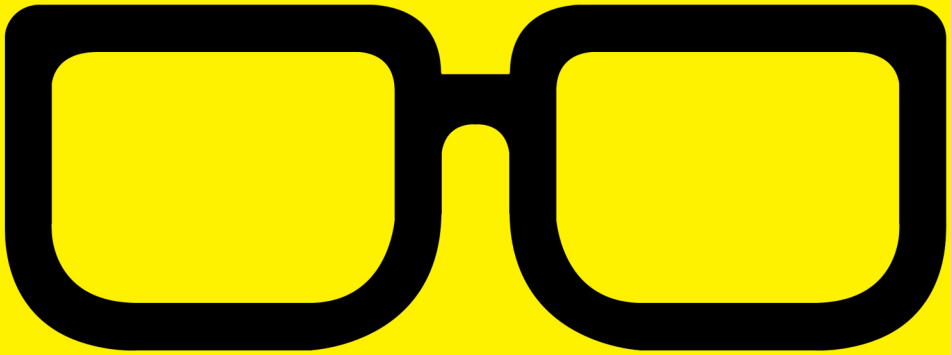
SPONSORED BY

IBM®

GEEK GUIDE



Hybrid Cloud Security with z Systems

LINUX™ JOURNAL

Table of Contents

PETROS KOUTOUPIS is currently a senior software developer at Cleversafe, an IBM Company. He is also the creator and maintainer of the RapidDisk Project (http://www.rapiddisk.org). Petros has worked in the data storage industry for more than a decade and has helped to pioneer the many technologies unleashed in the wild today.

GEEK GUIDES:
Mission-critical information for the most technical people on the planet.

About the Sponsor

IBM

IBM is a globally integrated technology and consulting company headquartered in Armonk, New York. With operations in more than 170 countries, IBM attracts and retains some of the world's most talented people to help solve problems and provide an edge for businesses, governments and non-profits.

Innovation is at the core of IBM's strategy. The company develops and sells software and systems hardware and a broad range of infrastructure, cloud and consulting services.

Hybrid Cloud is helping businesses deliver unprecedented levels of agility for quicker time to market and richer customer experiences. But not all cloud infrastructures are equal. IBM z Systems and LinuxONE are the world's leading cloud platforms for enterprise transactions, systems of record and application workloads.

Today, IBM is focused on four growth initiatives—business analytics, cloud computing, growth markets and Smarter Planet. IBMers are working with customers around the world to apply the company's business consulting, technology and R&D expertise to build systems that enable dynamic and efficient organizations, better transportation, safer food, cleaner water and healthier populations.

Hybrid Cloud Security with z Systems

PETROS KOUTOUPIS

Introduction

Data—it is what drives the market and has led to the creation of the Internet of Things (IoT) in this little thing we call the cloud. In the past decade alone, the paradigm shift toward a wider and more accessible network has forced both hardware vendors and service providers to rethink their

IBM z Systems are omnipresent in today's enterprise computing, and without realizing it, most people interact with mainframes multiple times in a given day.

strategies and cater to a new model of storing information. As more individuals and businesses connect themselves to the greater world, it becomes increasingly necessary to secure the information that travels across our networks.

This ebook highlights the many challenges service providers face in their respective cloud deployments and showcases the numerous ways IBM z Systems are well equipped to take on those same challenges with a greater emphasis on security and application integration. Read on to learn how IBM z Systems can enable you to transfer and store data securely.

z Systems: the Unsung Hero

A descendant of the System/360 (1964) and the System/370 (1970s), the introduction of the z Systems marked a pivotal point in enterprise-scale computing. The technology was, and still is, designed for accelerated transaction processing and data serving, providing modern capabilities for analytics and mobile integration solutions. IBM z Systems are omnipresent in today's enterprise computing, and without realizing it, most people interact with mainframes multiple times in a given day.

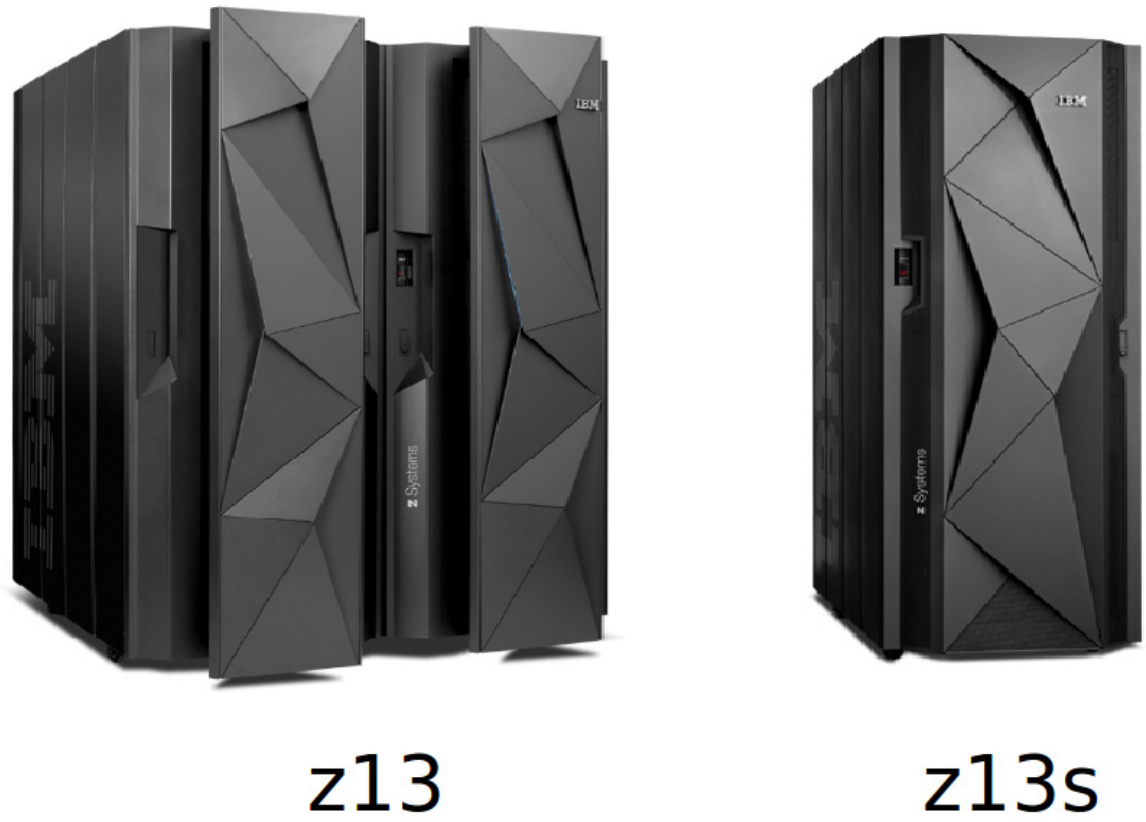


FIGURE 1. IBM z13 and z13s (Image courtesy of IBM.)

The release of the IBM z13s (2016) marks the latest in the family of z models. The z13s is a highly scalable symmetric multiprocessor (SMP) system incorporating the advanced technologies announced with IBM z13 in 2015 in a much smaller single cabinet footprint.

Resiliency: The "z" stands for zero downtime. Fault tolerance on z Systems is built on a very basic principle: Reliability, Availability, Serviceability (RAS). Through RAS, z Systems are able to achieve continuous and reliable operation. This includes detecting, preventing and correcting error cases through constant system analysis.

These systems are designed with redundancy of physical components at every level (all the way down to the CPU) that are fully capable of tolerating all kinds of failures. Another area where fault tolerance is emphasized is z Systems' ability to handle memory failures. Memory modules are pooled into a RAID-like technology referred to as a Redundant Array of Independent Memory (RAIM) that supplies an N+1 tolerance of failures. The RAIM design detects and recovers automatically from all sorts of memory failures across DIMMs to sockets, memory channels and more, further ensuring data integrity.

Performance: Looking at just the IBM LinuxONE Emperor, a system enabled for enterprise-grade Linux, one is impressed with its 5GHz processor, capable of supporting up to 141 customer-configuration cores, and delivering I/O bandwidth through up to 320 I/O co-processors and 24 dedicated I/O cores. The same system supports a multi-level cache subsystem and as much as 10TB of memory.

All lines of communication are passed through what is referred to as the Fibre Connections (FICON) protocol across extremely performant 16Gbps Fibre Channel switches connected via fiber-optic cables. To maintain data integrity, IBM employs a technique called FICON Forward Error Correction (FEC). Errors across communication lines happen. With the FEC, the impact of such low-level errors are reduced significantly, which in turn limits the effect on overall workload performance, typically a result of high-level I/O errors and an application's attempt to re-issue those same failed commands.

Each z Systems processor core has a dedicated co-processor that delivers cryptographic and hashing capabilities in support of clear-key operations.

The Enterprise Data Compress (zEDC) adapter is yet another distinguishing feature of the z Systems. It allows applications to offload zlib-compatible compression work to a hardware co-processor, resulting in good compression ratio without wasting the CPU cycles. In some cases, zEDC has been known to improve compression performance by a factor of five, allowing more data to process in the same amount of time. An added benefit to the built-in compression is the reduction of the overall footprint in datasets and, in turn, storage costs.

An optional feature, Flash Express can help improve performance on critical business workloads by implementing a Storage Class Memory (SCM) through internal NAND Flash Solid State Drives (SSDs) fitted onto a PCIe card form factor. This allows for Logical Partitions (more on this below) to be configured with its own address space on the SCM.

Security: The architecture includes hardware support for cryptography. Each z Systems processor core has a dedicated co-processor that delivers cryptographic and hashing capabilities in support of clear-key operations.

This is known as the Central Processor Assist for Cryptographic Functions (CPACF).

Just when you thought all of this was enough, the z Systems also offer a cryptographic acceleration feature dubbed the Crypto Express5S. This feature provides a state-of-the-art tamper-resistant cryptographic co-processor for secure key operations.

IBM z Systems are the only commercially available systems certified under the Common Criteria at Evaluated Assurance Level (EAL) 5+ for its Logical Partition (LPAR).

These features alone become increasingly vital as the number of transactions continue to grow in the mobile world, all while helping protect sensitive transactions, minimizing business risk and client exposure. It isn't often that a single solution can ensure end-to-end privacy and protection of data and transactions.

LinuxONE: a Trustworthy Ally in the Data Center

Driving the Hybrid Cloud platform is the recently announced line of Linux server technology, LinuxONE (2015). LinuxONE is an enterprise-grade system that supports a variety of Linux distributions including Red Hat, SUSE and Ubuntu. Today, LinuxONE is offered in two versions: the business-class Rockhopper and the enterprise-class Emperor.

LinuxONE offers users an open solution so administrators and developers can choose the tools and applications

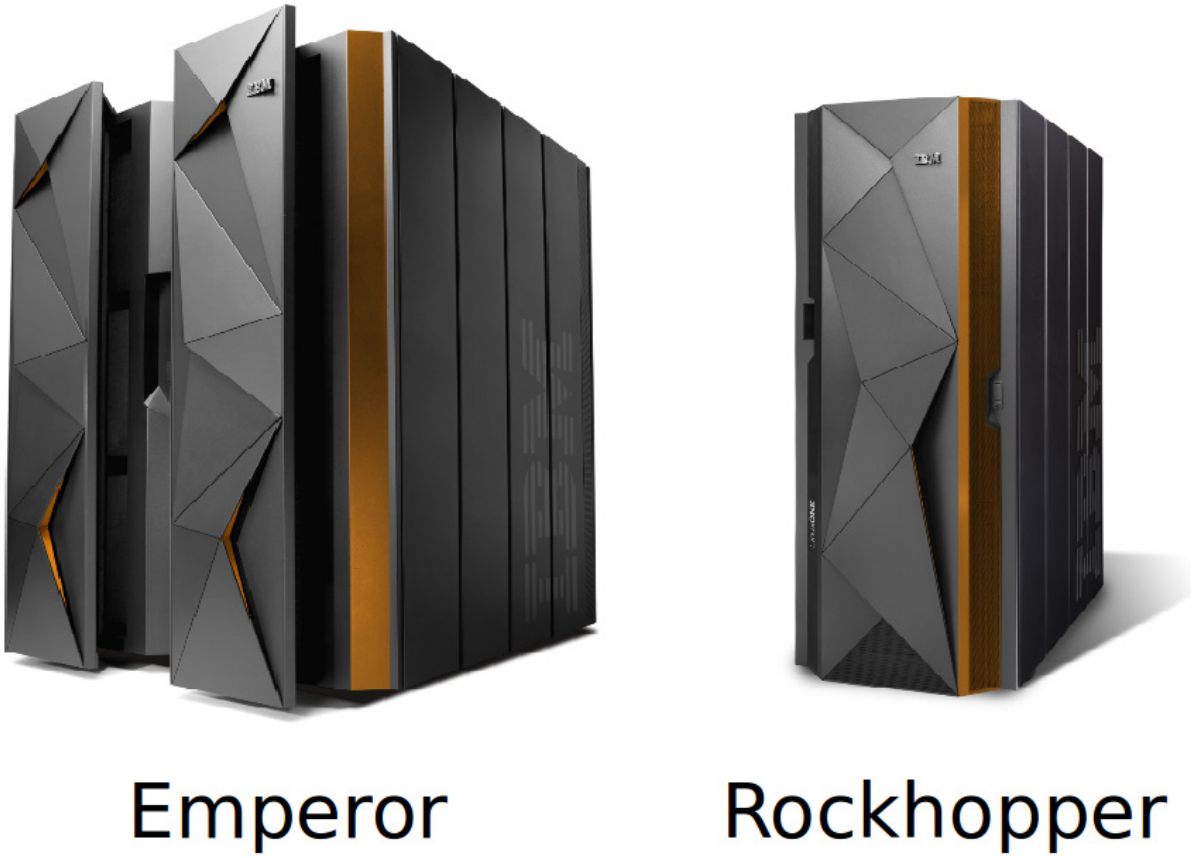


FIGURE 2. IBM LinuxONE Emperor and Rockhopper (Image courtesy of IBM.)

they have grown to appreciate, and flexibly and efficiently deploy them to meet consumer demand at virtually limitless scale, with less complexity and lower costs. Users can unleash thousands of virtual machines and tens of thousands of containers at a fraction of the cost.

The Evolution of Linux on z

The earliest incarnations of Linux on z Systems date to as early as 1999, with a collection of patches submitted

by IBM to the Linux 2.2.13 kernel. Some of those initial patches included object-code-only modules, but this eventually would be replaced by open-source modules. By the year 2000, a fully formed product was being distributed by IBM around this architecture.

In 2001, these patches were adapted to the then experimental 2.4. It did not take long for commercial Linux distributors to introduce support for z Systems in their respective Linux distributions. For example, in 2002, Red Hat redistributed this kernel as part of Red Hat Linux 7. With wider visibility and support, the codebase would continue to mature. During the past two decades, the distribution has taken on different identities, each with its own name, but today, we refer to it simply as Linux on z.

Fast-forward to the present, and Linux on z is completely free and open-source software licensed under the GNU General Public License (GPL).

Note: the z Systems architecture is designed to run multiple operating systems, including the z/OS and Linux on z.

Virtualization at Its Finest: LinuxONE re-defines large-scale Linux deployment where virtualization is a requirement and supports a variety of Linux distributions including Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES) and Canonical's Ubuntu. LinuxONE is a responsive service delivery platform capable of provisioning new virtual Linux servers in seconds. LinuxONE Emperor can scale up to 8,000+ virtual machines (or VMs) or tens of thousands of containers in a single footprint. This is significantly more than any other Linux system on any other existing hardware platform.

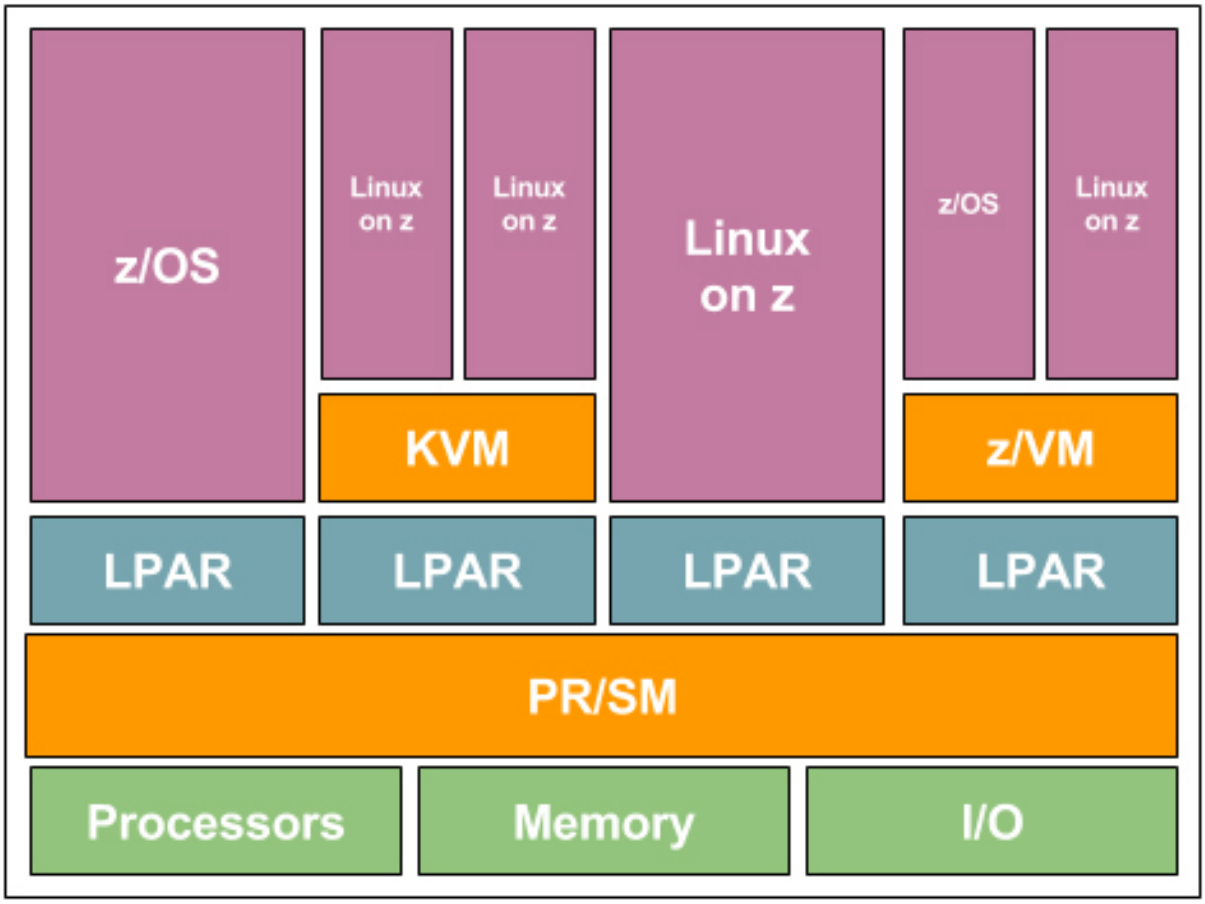


FIGURE 3. A Sample of z System Hypervisor Configuration

These virtualization capabilities are delivered by the Processor Resource and System Manager (PR/SM) Type-1 hypervisor and also the well known KVM and IBM z/VM Type-2 hypervisors. On z Systems, the PR/SM runs on bare metal and carves out what is referred to as Logical Partitions (LPARs) to host single instances of operating systems (more on this below). In the second layer of virtualization, KVM and z/VM are more flexible, in that it can host multiple instances of operating systems, all capable of sharing its resources in that same LPAR.

The best part of LinuxONE is that it brings a level of familiarity to developers and users already employing Linux technologies.

Simplified Application Deployment: IBM has natively enabled key open-source and industry-proven software for LinuxONE including Apache Spark, Docker, Node.js, MariaDB, MongoDB, PostgreSQL, OpenStack, Chef and more, all of which work seamlessly at greater performance on z Systems and requiring no additional skills to maintain. On a fully loaded z13 system, IBM benchmarks published spectacular results while performing 30 billion Representational State Transfer (RESTful) transactions a day using Node.js and MongoDB on Docker containers.

The best part of LinuxONE is that it brings a level of familiarity to developers and users already employing Linux technologies. The LinuxONE ecosystem enables organizations and DevOps specialists to port and/or migrate their applications with little to no effort or concern—and, they can do so in an environment that is known for its 100% uptime and completely reliable handling of transactions.

High Availability: Although the z Systems hardware boasts fault tolerance and high availability, further ensuring that the 100% uptime requirement is met, the software also has its own fair share of tricks up its sleeve. In LinuxONE, the majority of this heavy lifting can be accomplished with

KVM. The KVM hypervisor has been optimized for the z architecture and continues to provide the standard Linux, KVM and OpenStack interfaces for management operations.

At the software layer, the goal of configuring for high availability is to provide continuous and uninterrupted service for sometimes critical business applications, all while masking both planned and unplanned outages. These include failures that may be a result of system crashes, network failures, storage issues and more. Downtime can cost a company time and resources and potentially a loss in business. The requirement for this is to identify any and all single points of failure and eliminate them by configuring redundant instances, sometimes even balancing the workload across these same redundant instances via a concept typically referred to as Multipath. High-availability technologies are designed to detect failures automatically and recover from them immediately.

As mentioned earlier, a typical configuration usually consists of one or more z hosts sharing resources to the KVM host partition (that is, the LPAR). On z Systems, each KVM instance is hosted in the LPAR, and each KVM instance hosts one or more Linux guests from that same LPAR. Virtualized as a separate computer, the LPAR is a subset of a computer's hardware resources. When one or more guest virtual machines or a z host suffers from a failure, the virtual machine(s) immediately become active on the same or an accompanying z host.

Remember, LinuxONE will inherit the full z Systems RAS, hardware/firmware recovery, error checking (in

message logs for inconsistencies and anomalies), near-real-time diagnostics (to help identify and correct potential problems) and so on. With systems such as these, the majority of the time, hardware failures will be unnoticeable to the operating system and its applications.

Hybrid Cloud: Setting a New Standard

A new phenomenon to the cloud computing industry, the hybrid cloud provides a mixture of on-premises, private and public cloud services, with transparent and seamless access across all platforms. In the case of IBM, this seamless connectivity across all implementations is facilitated by OpenStack and enabled by the IBM Bluemix.

OpenStack: If you haven't heard of it already, you definitely are behind the times. OpenStack is an Apache-licensed open-source framework designed to build and manage both public and private clouds. Its interrelated components control hardware pools of processing, storage and networking resources that all can be managed through a Web-based dashboard, a set of command-line utilities or through a RESTful Application Program Interface (API). The primary goal of OpenStack was to create a single and universal framework to deploy and manage various technologies in the data center dynamically. Originally started in 2010, the project has since grown exponentially and has attracted a large number of supporters and users, and if you haven't realized it by now, this includes IBM. OpenStack is integrated into the IBM Cloud Manager and is offered for KVM and z/VM for z Systems.

VMs hosted on z Systems can be managed with VMware through the same OpenStack API. This makes it an ideal solution to pre-existing VMware shops, where they do not need to maintain a separate and parallel management environment.

All components of OpenStack are designed and deployed around a modular architecture, which simplifies configuration and management. Each major component focuses on one particular grouping of technologies. For instance, all virtual machines are managed under the compute component referred to by the codename, Nova; all block level storage, Cinder; Object Storage, Swift; networking, Neutron; and the list goes on.

VMs hosted on z Systems can be managed with VMware through the same OpenStack API. This makes it an ideal solution to pre-existing VMware shops, where they do not need to maintain a separate and parallel management environment.

Although OpenStack exports and publishes its own unique API, the project does strive to maintain compatibility with competing APIs, which include Amazon's Elastic Cloud 2 (EC2) and Swift3 (S3), and also the Google Compute Engine (GCE). The idea is to allow developers to migrate their technologies from competing ecosystems into OpenStack with little effort.

IBM Bluemix: It should come as no surprise that more and more leading companies are moving IT workloads from local data centers into the cloud. Why wouldn't they? It reduces overall costs (hardware, power, labor and so on), simplifies infrastructure management, enables elasticity and allows digital ecosystems to grow or shrink dynamically to accommodate the demand. And, the best part is companies still are able to maintain a certain degree of control over what's considered theirs. At the end of the day, this shift toward the cloud provides adaptability. Workload trends are never constant and always are subject to change. And although most cloud deployments offer a fair share of resources and adaptability, not all are created equal. This is where IBM begins to shine with its hybrid cloud, placing a greater emphasis on security.

Bluemix is the IBM Platform as a Service (PaaS) solution running in the cloud and hosted by IBM SoftLayer Infrastructure as a Service (IaaS) offering. It can be a lot to take in, I know. Bluemix's objective is to enable developers to build and deploy applications easily by re-using existing components and services, resulting in the reduction of custom code. This is just a fancy way of saying that it caters to DevOps. Bluemix supports several programming languages, including Java, Node.js, Go, PHP, Python, Ruby Sinatra and Ruby on Rails.

Security, Security, Security: Bluemix securely sends requests to/from z Systems through secured connections. These are accomplished through a series of options: the IBM DataPower Gateway, Secure Connectors and the

IBM Secure Gateway for Bluemix.

Available in both physical and digital forms, the DataPower Gateway features high availability, failover load balancing, message security, data conversion and so on. It has been optimized to process XML and RESTful Web services more efficiently. It also enhances cloud and on-premises security through its own built-in cryptography engine. The DataPower Gateway can be managed by an API.

Secure Connectors establish a protected line of communication between the cloud-hosted Bluemix applications and on-premises systems. Secure Connectors come in two forms: the Standard (Cast Iron) Connector and via the DataPower Gateway. The most simple is the Standard Connector. It is software-based and acts as an intermediary between a Bluemix application active in the cloud and the back-end z System. The secure connection is established from the Bluemix application, which then connects to the on-premises system securely. Remember that API I spoke of earlier for the DataPower Gateway? This is where it truly can come into play. Through this API, the DataPower Gateway can be more than a standalone appliance and act as a connector endpoint.

Based on bidirectional Web sockets, the IBM Secure Gateway for Bluemix is a Bluemix service that creates secure tunnels between Bluemix applications in the cloud and back-end resources. Aside from secure connectivity, this service also provides traffic monitoring and local endpoint mapping to on-premises applications and data resources. These features all can be managed

from a dashboard. The Secure Gateway client is provided by IBM as a Docker image that can run on on-premises Linux systems.

Another method by which data residing on a z/OS system can be accessed securely is through a function called z/OS Connect. Built on top of the Liberty Profile server runtime application, z/OS Connect is a software function for z/OS and serves as an enabler of connectivity between mobile environments and back-end z/OS systems. It's very lightweight and dynamic, and it also provides a RESTful API and accepts JSON data payloads. z/OS Connect is configurable, giving you control of what back-end programs or applications are exposed and accessible.

Application-Level Security in Bluemix: At the end of the day, all data should be treated as critical data, and often it is not enough when accessing that data via a secure connection through a secure tunnel. Bluemix takes the extra step by providing more security services at the application level.

For instance, consider the IBM Mobile Application Security for Bluemix. This feature helps protect applications and data by preventing unauthorized users and devices (this includes stolen and compromised devices) from accessing critical information.

Another feature is the OAuth 2.0-supported IBM Advanced Mobile Access for Bluemix, which is a protocol that enables users to log in using identity providers like Facebook, Google and so on. Advanced Mobile Access OAuth tokens provision access at deployment time. Nothing is embedded into application code.

A third form of application-level security offered by Bluemix is the Single Sign-On (SSO), which supports identity sources from a Security Assertion Markup Language (SAML) Enterprise user registry, a cloud directory hosted in the IBM cloud or the same social identity sources using OAuth 2.0.

Unleash the Next Generation of Cloud Applications: The support for open standards like XML, JSON (JavaScript Object Notation) and REST is what makes this hybrid model truly powerful. Fortunately, for things like this, IBM hosts a complete API ecosystem and has transformed the way businesses develop APIs for their applications accessing IBM solutions. This ecosystem is marketed as the API Economy.

For those less familiar, an API is what glues services, applications and entire systems together. Typically, an API acts as a public persona for a company or a product by exposing business capabilities and services. An API geared for the cloud can be invoked from a browser, mobile application or any other Internet-enabled endpoint.

The purpose of the API Economy is to provide platforms, tools, resources and, most important, an entire community to enable enterprises in building and publishing to the existing API ecosystem that can be shared with potential partners or future customers.

Completing the Puzzle

The biggest selling point of the hybrid cloud using IBM's z Systems technologies is that it potentially can lower the total cost of ownership by as much as 60%

over three years when compared to that of a traditional public cloud while gaining the additional benefits of added security and resiliency.

Virtualization is key to enabling this hybrid cloud. It allows for minimizing the over-provisioning of resources and, in turn, re-using them at the end of the virtual server lifecycle. This is another area where z Systems truly shine, allowing users to run as many virtual machines of whatever operating system as they require.

Apart from the raw computing power, if you recall from earlier, IBM z Systems can speed up the compression and encryption of sensitive datasets through its zEDC and CPACF co-processor features. Offloading the compression of Apache Spark Resilient Distributed Datasets (RDDs) or Docker containers frees CPU cycles to perform other functions. Couple these z Systems with IBM's public and private cloud offerings and unleash their full potential with Bluemix. Whether you purchase from IBM or bring your own hardware, implementing a world-class hybrid cloud is at your fingertips.

The best part is that all of these layers can be managed from the IBM Cloud Manager with OpenStack. So, if you are looking to deploy a hybrid cloud solution, IBM will cover you 100%, from end to end.■