Brought to you by:

IBM

Secure Hybrid Cloud

for dummies®

A Wiley Brand

Optimize the role of IBM Z® in hybrid cloud

Accelerate transformation with hybrid cloud

Build security into every layer of your cloud

Judith Hurwitz

Daniel Kirsch

2nd IBM Limited Edition

Secure Hybrid Cloud

2nd IBM Limited Edition

by Judith Hurwitz and Daniel Kirsch

for dummies®
A Wiley Brand

Secure Hybrid Cloud For Dummies®, 2nd IBM Limited Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-73549-6 (pbk); ISBN: 978-1-119-73552-6 (ebk). Some blank pages in the print version may not be included in the ePDF version.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Ashley Coffey

Business Development Representative: Molly Daugherty

IBM Contributors: Jax Shawley, Adam Jollans, Nathan Dotson, Damon Garcia, Pete McCaffrey, Sherri Hanna, Barbara Sannerud, TJ Aspden, Simon Hares

Table of Contents

Introduction

Welcome to *Secure Hybrid Cloud For Dummies,* 2nd IBM Limited Edition. The hybrid cloud is becoming the way enterprises are transforming their organizations to meet changing customer requirements. Businesses are discovering that in order to support the needs of customers there is an imperative to leverage the highly secure IBM Z platform as a strategy element in an enterprise's transition to hybrid cloud computing. IBM Z is purpose built to support mission critical workloads such as transaction management applications. The Z platform has been transformed over the years. The combination of z/OS, LinuxONE, and open application programming interfaces (APIs) and the inclusion of Kubernetes have made IBM Z a critical partner in the hybrid cloud world. Businesses are transforming their IBM Z environments into a secure, hybrid cloud. In addition, through IBM's public cloud, businesses can take advantage of IBM Z's security services to protect their data and applications.

About This Book

This book is designed to help you understand the value of a secure cloud and how it can help your business meet its technical and business goals. The book provides an understanding of the importance of security in the hybrid cloud environment and how the IBM Z platform and its services play an important role for enterprises.

Foolish Assumptions

The information in this book is useful to many people, but we have to admit that we did make a few assumptions about who we think you are:

- You're already familiar with cloud computing and need to understand the role of the hybrid cloud and how it relates to your data center and the IBM Z.

- You're planning a long-term cloud strategy and want to understand the value of the private cloud and how it can be used to support your business goals.
- You want to understand how security services can help protect your company as you move to the hybrid cloud.
- You want to understand how all the elements of cloud computing fit together and can support the software development, deployment, security, and compliance.
- You're a business leader who wants to apply the most important emerging cloud technologies to be as creative and innovative as possible.

Icons Used in This Book

The following icons are used to point out particular information throughout the book:

REMEMBER

This icon highlights important information that you should remember.

TIP

Tips help identify information that needs special attention. This content may just help you save some time and money.

WARNING

This icon points out content that you should pay attention to in order to avoid problems.

IN THIS CHAPTER

- Defining hybrid cloud
- Using hybrid cloud as a strategic model
- Powering your hybrid cloud strategy
- Supporting hybrid cloud with Red Hat OpenShift and IBM Cloud Paks

Chapter 1
Understanding the Business Value of Hybrid Cloud

The world of enterprise computing is quickly evolving. Only a few years ago, many businesses were uncertain whether to remain with a data center or move to a variety of public and private clouds. With the huge changes in business transformation, corporations are quickly modifying the way they leverage a variety of deployment models based on the requirements of performance, scalability, flexibility, and resilience.

Business disruption drives the need for hybrid cloud adoption. Across all industries, new competitors rapidly adopt innovative technologies to move faster and with more agility than larger, well-established companies. These technologies can provide significant benefits to well-established organizations as well. Established businesses benefit greatly from combining innovative technologies with deep intellectual property, industry knowledge, and a large existing customer base.

The hybrid cloud has become the architectural framework that allows companies to select the deployment model that best serves their business needs. The flexibility of hybrid computing gives

businesses the ability to change deployment models as business needs evolve.

To keep pace with agile competitors, enterprises are rethinking the ways they deliver services to their customers, suppliers, and partners. Crucial to this shift is an IT environment that's optimized for security, speed, and flexibility. The hybrid cloud can provide a technique to support business growth and change.

In this chapter, we define hybrid cloud and why it matters to your business. Then, we describe the key components of a successful hybrid cloud strategy and why the mainframe is a key part of that strategy.

What Is Hybrid Cloud?

Organizations today are challenged to manage complex issues, including service-level requirements, security and compliance, and internal data-storage rules. Therefore, organizations are required to evaluate and determine which computing service will best match the changing needs of the business.

Hybrid cloud enables a business to select a customized mix of services residing on the most appropriate platforms and location to support workloads with precise levels of protection and performance. In effect, the hybrid cloud represents the industrialization of the cloud. Typically, business units have adopted cloud services with a variety of public, private, and data center applications and services. This approach has proved to be the most pragmatic way to move forward and is the foundation for what's known as the hybrid cloud.

REMEMBER

Because of its unique blend of flexibility and performance, the hybrid computing model has become the preferred platform for many enterprises. A hybrid architecture combines the openness of public cloud and private cloud with the power of the data center. This powerful set of capabilities enables businesses to blend existing investments with modular, scalable, and flexible services to meet customer expectations and to support innovation and efficiency needs.

Hybrid cloud empowers enterprises to move away from a "one-cloud-fits-all" model and toward a model that selects the

right cloud service based on each business unit's needs. For example, developers in one business unit may discover a public cloud service that is a good match for the task at hand. Another unit may have expertise and experience with a different public cloud or Software as a Service (SaaS) application. Across the enterprise, one organization can use as many as five or six different public clouds and several SaaS applications that operate on many cloud platforms.

PUBLIC VERSUS PRIVATE CLOUD

All clouds aren't the same. A variety of public cloud services are commercially available. These services can be purchased on either a usage basis or via a service agreement. Some public clouds are commodity services while others are designed to meet the specific needs of a use case of an industry need. In contrast, private cloud services live inside an enterprise data center and may mirror all or many of the services provided in the public cloud. Managed cloud services can also be used on an as-needed basis.

Defining the public cloud

The *public cloud* has evolved over the years. Early public cloud use cases helped developers or businesses provision compute or storage power incrementally based on immediate needs. Over the past five years, however, public cloud providers have added a larger variety of services, ranging from security to mirrored disk to DevOps.

Within the context of a public cloud is the concept of a managed service. Like the traditional public cloud, the managed service is a hosted model in which a consumer pays per usage for a service to execute a specific function.

Defining the private cloud

The *private cloud* is an enterprise-class solution that delivers a single platform behind a firewall. Unlike a traditional data center environment, the private cloud is typically based on a software-defined interface that enables the services within to behave in a modular, scalable fashion. Because the private cloud lives behind the firewall, it offers a controlled layer of protection; it's self-contained and can be designed to support the service-level guarantees demanded by many customers.

With the hybrid cloud, organizations can manage data, applications, business rules, and security services as a set of related capabilities and services to meet a business need. A hybrid cloud allows enterprises to agilely innovate and transform without compromising security, governance, or performance.

Hybrid Cloud as a Strategic Model

Most organizations are committed to a hybrid cloud strategy. Many businesses leverage a variety of public cloud and managed services to develop applications, analyze data, and operate key workloads. In addition, these organizations use private cloud services based on security and cost considerations. To most enterprises, the cloud is no longer a means to an end, but a full-blown strategic function.

A well-planned hybrid cloud strategy must consider the need to protect a company's intellectual property and comply with corporate and governmental regulations. It must also take into account the following:

- Financial constraints and budgeting
- Security
- Scalability, performance, and resilience
- Operational management
- Management of data

Accounting for all these elements requires a flexible framework to support your hybrid cloud environment. The platform must allow you to manage all elements of the cloud in a consistent, predictable manner. This, in turn, will drive the on-time service delivery and rapid innovation that help you satisfy clients and keep pace with competitors.

REMEMBER

The hybrid framework must be scalable. As the data demands of your business grow, your platform should scale to meet them. This applies to data both on premises and in the public and private clouds. The platform must keep your data secure. Data breaches erode customer trust and cost millions. A platform supporting hybrid cloud should build an impenetrable fortress wall around all sensitive data. Finally, the platform must empower innovation

by simplifying and expediting development and implementation of new applications across platforms.

Understanding Why the Mainframe Is Essential to Hybrid Cloud Strategy

IBM Z uses Red Hat OpenShift as the foundation for its approach to the hybrid cloud (see the section "Red Hat OpenShift with IBM Cloud Paks" for more information). Therefore, IBM Z can be a critical element in your hybrid cloud strategy by

- **Ensuring a consistent, stable environment:** With high availability, the mainframe supports stability and reliability for your cloud applications.
- **Providing scalability:** The mainframe scales up, not out, allowing seamless data expansion of your systems of engagement as they grow from hybrid cloud innovation.
- **Keeping data secure:** IBM Z brings unparalleled security to the cloud with pervasive encryption of all data at the hardware, software, and cloud service level — whether at rest or in flight.
- **Empowering innovation through rapid development capabilities:** IBM Z provides a framework for rapidly developing, testing, and deploying cloud services and applications across platforms.

Today's mainframe is designed to work hand-in-hand with public cloud, private cloud, and other open technologies. As part of a connected ecosystem, IBM Z easily integrates with external systems and is compatible with new application development and deployment models.

If you run core systems of record on IBM Z, you may have decades' worth of valuable data embedded within it. Integrating IBM Z with hybrid cloud allows you to leverage this data to build new applications, launch new innovative services, and improve customer engagement. Hybrid cloud is fast becoming the standard platform for new service deployment. The connected mainframe enhances the security, stability, and flexibility of your computing environment.

Red Hat OpenShift with IBM Cloud Paks

IBM offers Cloud Paks, which is a set of modular services designed to meet the needs of businesses that require a consistent set of options to support the hybrid cloud. Modular services allow customers to select the most appropriate service as a starting point and add new services when needed.

Each Cloud Pak has a common Red Hat OpenStack foundation and is designed to support public and private clouds, and on premises infrastructure. Cloud Paks offer a unified installer to create and manage Kubernetes-based clusters that can be managed by Red Hat OpenShift. Find out more about this topic in Chapter 2.

IN THIS CHAPTER

- Looking at Red Hat OpenShift's role in hybrid cloud
- Recognizing the value of IBM Cloud Paks
- Delivering cloud-optimized services

Chapter 2
Exploring Red Hat OpenShift and IBM Cloud Paks

Businesses are turning to hybrid cloud to manage their workloads to support customers and partners. A single solution designed to support all workloads and business situations doesn't exist. Both corporations and cloud service providers (CSPs) are evaluating a new generation of cloud offerings as a solution. In this chapter, you explore Red Hat OpenShift and the IBM Cloud Paks. The Cloud Paks are containerized software solutions built on Red Hat OpenShift. IBM Z can be deployed in a variety of cloud use cases, including in the IBM Cloud as the foundation for IBM Cloud Hyper Protect Services or IBM Blockchain Platform, and running cloud-native applications built with Red Hat OpenShift and co-located with systems-of-record data.

Understanding the Role of Red Hat OpenShift

Red Hat OpenShift provides the foundational layer of the IBM hybrid cloud platform. Red Hat OpenShift is infrastructure agnostic, runs on multiple clouds and hardware architectures, and is

available for both IBM Z and IBM LinuxONE. Red Hat OpenShift Container Platform is built on Kubernetes and enables new cloud-native applications to be developed and existing applications to be modernized. These new and modernized applications are designed for high performance and for the flexibility to respond to customer and market changes. Applications built on Red Hat OpenShift and deployed on IBM Z inherit its enterprise qualities such as security, scalability, and reliability. These applications can also interact with data managed in systems of record and applications stored on the same system, whether running on IBM z/OS or Linux for IBM Z.

Seeing the Value of IBM Cloud Paks

IBM Cloud Paks are a family of containerized software solutions designed to help predict, secure, and automate applications, and they're infused with artificial intelligence (AI) designed for the hybrid cloud. Cloud Pak offerings are built on Red Hat OpenShift and can run on public clouds, private clouds, and on premises infrastructure. Cloud Paks are designed to sit on top of any public or private cloud. The benefit of this software abstraction layer is that clients can leverage flexibility of deployment and common skills across the hybrid cloud infrastructure, including IBM Z.

Multiple IBM Cloud Pak offerings are designed to help modernize, predict, automate, and secure applications. Cloud Paks are helping clients with

- **Integration:** A pre-integrated AI-based platform to support data integration, messaging and events, high-speed transfer, and integration security
- **Data management and analytics:** Designed to unify data services through an integrated data catalog, open source, and third-party microservices, along with the ability to build, deploy, and manage AI at scale in the hybrid cloud
- **AIOps:** A solution that provides consistent visibility, automation, and governance across a range of hybrid multicloud management capabilities, and leverages advanced and explainable AI to assess, diagnose, and resolve incidents

Serving Up Cloud-Optimized Software and Services

Because Cloud Pak solutions are based on Red Hat's OpenShift container architecture, several optimized services are part of the platform. Cloud Pak offerings give you a common catalog of services that increases developer productivity. The catalog helps manage microservices so they can scale both horizontally and vertically. The structure of the catalog makes it easier to govern, deploy, and maintain software and services to support rapid development, test, and deployment.

Red Hat OpenShift incorporates a broad range of managed middleware, data, and analytics services, supporting both cloud-native and existing applications. Developers can leverage existing application development skills such as Java, Spring, and Open Liberty through the Red Hat Runtimes and IBM middleware. Application programming interface (API) connectivity and management services make it possible to integrate services across public, private, and existing enterprise environments.

Delivering portability and scalability

Red Hat OpenShift is a trusted Kubernetes container platform focused on providing a hybrid computing application development and life cycle management environment for any application on any platform. The platform incorporates a multicloud consistent management layer. OpenShift is self-managed based on Red Hat Linux and incorporates container runtimes, networking, monitoring, container registry, authentication, and authorization.

TIP

One of the most important benefits of OpenShift is that it's an open platform by incorporating Open Containers Initiatives (OCI) containers and Cloud Native Computing Foundation (CNCF)-certified Kubernetes for container orchestration. Because of this open source foundation, OpenShift supports container portability.

Scalability is also a core benefit of OpenShift. In seconds, applications running on OpenShift can scale to thousands of instances across hundreds of nodes. Red Hat OpenShift also supports consolidated views of clusters through multicluster federation.

Providing infrastructure flexibility

IBM Cloud Paks can operate on any existing hardware environment, including IBM Z, IBM LinuxONE, IBM Power Systems, IBM Storage, IBM Hyperconverged Systems, and x86-based systems, that supports Red Hat OpenShift. It also supports a variety of clouds, including VMware, Amazon Web Services, Microsoft Azure, Google Cloud Platform, and IBM Cloud.

EXAMINING USE CASES FOR DEPLOYING OpenShift WITH IBM Z

Many banks and other businesses have invested in the IBM Z platform that supports their complex line of business (LoB) applications and customer data. One of the key goals for the digital transformation effort is to reduce latency between the applications and data across clouds and on premises systems.

In order to accomplish this goal, businesses are implementing Red Hat OpenShift as their Kubernetes foundation to support its applications modernization initiatives on IBM Z. By co-locating Red Hat OpenShift next to mission-critical customer data and applications on IBM Z, they're able to consistently support cloud-native applications across the hybrid cloud, while reducing latency and increasing performance when accessing data held on the IBM Z system.

To support the need to integrate data across the hybrid computing environment, the businesses can also take advantage of the IBM Cloud Pak for Data to provide a consistent way to manage the variety of data platforms across business units. In addition, using the IBM Cloud Pak for Integration can enable seamless integration between a variety of clouds and systems. To provide integration between the IBM z/OS platform and the Kubernetes based environment, businesses can use the IBM z/OS Cloud Broker.

By bringing together the investment in IBM Z with its scalability and security with the flexibility and modularity of OpenShift and IBM Cloud Paks, businesses are able to create a future-focused hybrid computing environment that can more easily adopt to changing customer requirements.

IN THIS CHAPTER

- Maintaining privacy in the cloud
- Protecting all your data
- Having a data privacy protecting cloud
- Looking at IBM's approach to protection and privacy
- Securing data across your hybrid cloud

Chapter 3
Providing Security with IBM Z

Managing data and intellectual property is imperative for businesses to survive and thrive. Therefore, security is a requirement for any corporate strategy and plan. Customer and employee data must be protected from cybercriminals while the process for managing this data must be in compliance with regulatory and governance requirements. As employees increasingly work remotely, businesses must balance the need to securely provide relevant data while complying with their regulation and governance requirements. At the same time, customers won't do business with a company if they feel that their data isn't protected. As cloud infrastructure becomes a primary development and deployment platform for many organizations, security and governance are top enterprise priorities.

Preserving Privacy in the Cloud

Increasingly, businesses are concerned about cybersecurity threats to the information that is the lifeblood of their relationship with their customers and partners. Valuable data including spreadsheets, documents, applications, transactions, and databases on

premises and in multiple clouds resides everywhere in your organization. Therefore, data protection is no longer just the concern of the chief security officer. Security has become a major issue at the board level in all corporations. Therefore, organizations must constantly improve their focus on data protection and stay current to conform to their regulatory controls.

The consequences of a data breach

There is an overriding concern caused by the potential for data breaches. Sensitive data could be exposed or lost, resulting in damage to the reputation of a company's brand (see the next section). Businesses that can't protect their clients and their own data will have trouble surviving.

A data breach can lead to catastrophic financial losses as well. Take, for instance, a renewable energy company that has found a novel way of designing solar panels that are lighter and more efficient than the competition's offerings. While it is important to be able to share engineering plans with suppliers and various vendors, the data must be secure. If plans fall into the wrong hands, the company risks losing all of its intellectual property (IP). The company could be outpaced by the competition using this IP overnight if it fails to properly secure its intellectual property.

The impact of reputational damage

Reputational damage can be almost as bad as direct financial and IP losses. Partners and customers are increasingly reevaluating the integrity of their business partners because of the requirement to protect their data. If a company experiences a data breach, many customers and partners will reconsider whether they should do business with that company.

Protecting Your Data

It is not enough to focus all your attention on regulatory compliance and audits when it comes to protecting your company's and your customers' data. The majority of cyber-threat headlines focus on third-party malicious attacks. However, businesses are concerned with a variety of other issues related to implementing cloud security.

Accidental exposure

Not all data leaks are a result of malicious actions. In fact, in many cases, well-meaning employees or partners accidently expose data. In some instances, employees may use public cloud services that expose sensitive data to unauthorized users. For example, they may use a cloud-sharing application as an easy way to collaborate and share large files. In addition, you must think about whether data sets can be viewed or copied to a development environment where the data could then be used by internal testing. Although actual customer data sets may be ideal for testing, they could expose personal and private customer data that's regulated in many regions. Another problem can arise when an incorrect version of data is restored to production by unauthorized personnel.

Insider attacks

Although the vast majority of employees and contractors want to help the business, there may be bad actors that have malicious intentions. Users with privileged access (like cloud administrators) become victims of social engineering attacks or cyberattacks. An employee may have recently been fired or overlooked for a raise or promotion. In some instances, someone may be looking to sell a company's data. It is important to understand who has access to what data and to be able to have full traceability of who has touched what and when.

Malicious third-party attacks

Companies typically have various moats (firewalls), gates, and encryption around their most sensitive data. However, increasingly organizations have data spread out across different departments and locations. As edge devices proliferate, it becomes harder to protect the perimeter. In addition, in an effort to help employees make data-driven decisions, companies have increasingly put valuable data in the hands of more and more employees. Besides the "crown jewels," most of an organization's data is never encrypted and is available to any hacker who penetrates a single endpoint. Criminals are becoming increasingly clever at finding vulnerable entry points into a company's data. For example, one employee falling victim to an email phishing exploit may lead to customer and corporate data being exposed.

Regulations and compliance

Having to comply with regulations, industry standards, and audits has always been a major security driver for organizations. Specific industry concerns include the Health Insurance Portability and Accountability Act (HIPAA) for health care and the Payment Card Industry Data Security Standard (PCI-DSS) for retailers. For example, violating the PCI-DSS may mean that a retailer can no longer accept credit card payments. In addition, nearly every business is rethinking its approach to data security and protection of personal information in light of the penalties that are now in effect for the European Union General Data Protection Regulation (GDPR). Failing to comply with these regulations can bring about harsh penalties.

Data Privacy in the Cloud

There's a common misconception that when a business trusts its data and applications to a cloud provider the business is no longer responsible for security. This isn't true. The business remains responsible for keeping track of this highly distributed data, including who is allowed to access the data and whether regulations are adhered to. To meet the security needs of the business, follow these best practices:

- Have a plan to keep track of where all your data is and the security mechanisms in place to protect it.
- Categorize your data based on its sensitivity and protection needs.
- Make sure that security is built into infrastructure platforms instead of relying on an assortment of third-party tools.
- Security must be part of every layer of the computing stack, including hardware, firmware, hypervisors, operating systems, middleware, and applications.

  Reliance on applications security carries a higher maintenance burden than having security built into platforms, operating systems, and databases.

PERVASIVE ENCRYPTION PROTECTS IP AND CUSTOMER DATA

The idea of encrypting all your data is new. In nearly every online interaction, data is left unencrypted at some point in the process. This very point when data is left unencrypted gives wrongdoers the opportunity to steal your data.

Take the example of an online insurance interaction. The customer's browsing session would be encrypted to protect customers from a variety of attack techniques — all the corporate data (the username, password, and so on) would be encrypted. However, there is a strong likelihood that the session isn't encrypted at some point on the insurance company's backend application and networking system. Wherever the unencrypted data resides, the data is vulnerable. So if an application performance testing group can access that browsing session, its system may provide a viable attack vector for criminals.

- Implement identity management into your hybrid cloud environment.

  In a complex multi-cloud environment, it's important to have a consistent and predictable way to keep security solutions up to date to protect and secure the environment from attack.
- A multi-cloud environment requires that you act as a systems integrator so all the elements of your computing platform are protected in a consistent and predictable manner.

Looking at IBM's Approach

One of the benefits of IBM Z is the significant level of security and data protection technologies inherent in the platform. Often, businesses are concerned that putting their highly sensitive

workloads in the cloud can put the company at risk. When you think of data protection, consider three key aspects:

- **Data at rest:** There is a need to protect data in storage such as on disk or tape and in archive media.
- **Data in flight:** It is imperative to protect data when information is being transferred over public or private networks and securing that traffic.
- **Data in use:** There is a need to protect data access as well as when data is stored in memory.

To be successful in managing data protection and privacy, it is imperative that all contingencies are considered. It isn't enough to protect one of these issues. In a hybrid cloud environment, you need to be able to protect your data no matter the circumstances. So, how do you balance the need for security with the flexibility of the cloud? We give you that information in this section.

Data at rest and data in flight: Pervasive encryption

Because of the architecture of IBM Z, security is pre-integrated at every level of the hardware and software stack, and you don't have to manage a variety of third-party security services. Fundamental to this is the ability to encrypt data in bulk. Therefore, it is possible to encrypt all the data associated with an application or a database.

Implementing encryption at every level is in stark contrast to the way encryption is typically approached. Most companies only encrypt a small amount of data, leaving the vast majority of data completely unencrypted. The unencrypted data remains at risk of being leaked or stolen either by mistake or by a criminal. On the other hand, when all the data is encrypted, even if it's exposed to people outside of your organization, it will be meaningless without the encryption key.

Pervasive encryption can encrypt data both at rest and in flight and can be used to protect both on premises private clouds and public cloud services. Moreover, pervasive encryption doesn't require application changes or administrators to determine precisely *which* data has to be encrypted because all data would automatically be encrypted as it's written. Being able to encrypt all your data no matter where it resides is important.

You may be wondering how a system can encrypt and decrypt data in real time without adding a tremendous amount of overhead and performance problems. IBM has developed specific on-chip accelerator hardware to handle the encryption in an efficient and fast manner.

Organizations can access Z security services through different techniques. For example, a client can build its own cloud on premises based on the IBM Z architecture so the cloud inherits all the built-in security capabilities. In other situations, a customer can gain access to Hyper Protect (see the section "IBM Hyper Protect Services") or secure services in the IBM Cloud.

IBM Hyper Protect Services

Data protection services must be able to protect intellectual property in a hybrid cloud environment. A variety of Z security services are hosted in the IBM Cloud. IBM now offers the IBM Hyper Protect Services built with mainframe-level data protection, made possible by bringing Z into IBM's global public cloud data centers. Now, developers and clients can build, deploy, and host applications with an industry-leading data protection that encrypts information in memory, in transit, and at rest. This technology is designed to help protect against threats, both inside and outside of an organization. The IBM Cloud Hyper Protect family intends to expand to include other security services that provide protected cloud capabilities, but currently it offers these two:

- IBM Cloud Hyper Protect Crypto Services
- IBM Hyper Protect Data Controller

Data in Use and Confidential Computing

While existing techniques can provide extensive protection of data in flight and data at rest, protecting the third state — data in use — is the new frontier. Protecting data while in use has been a challenge so far because applications need to have data that's unencrypted or not protected in order to run computations. This poses a significant security issue because this type of data remains exposed in memory and can be exploited by malware or other threat vectors to steal information. The Confidential

Computing Consortium is an industry wide movement to help protect data while it is in use through the implementation of hardware-based techniques such as Trusted Execution Environments (TEE).

IBM Secure Execution for Linux is an IBM Z and LinuxONE exclusive TEE technology that's built into the hardware and firmware of the system. It is designed to protect the confidentiality and integrity of data and code in use (during runtime). Unencrypted data and memory while in use can now be securely processed in a protected execution environment, often termed an enclave. Secure Execution offers workload isolation and access restrictions to help ensure that other guests or malicious administrators don't have access to your sensitive workloads. Secure Execution can help provide a highly secure and trustworthy hosting solution for enterprise ready multi-tenant workloads on premises or in the cloud and hybrid environments.

Secure Execution can maintain confidentiality and integrity for data in use, regardless of who may own or have access to the machine on which the software is running. By protecting data in use, the last pillar of data security, Secure Execution, makes it possible to run sensitive workloads more securely even on untrusted infrastructure and help you move one step closer to realizing a Zero Trust environment. Zero Trust is an approach aimed at protecting every user, every device, every connection at every time. Zero Trust gives your organization the ability to control who has access to data under any circumstance. One aspect of Zero Trust is to enable your security organization to ensure that no vendor can ever access the keys of your encrypted data. If there is a breach within a cloud provider, your data remains protected because the keys are protected inside your firewall.

IN THIS CHAPTER

- Cashing in on the API economy
- Seeing the value of application modernization
- Uncovering operational intelligence
- Incorporating Z into AIOps

Chapter 4
Modernizing Applications and Data in Place

Many enterprises continue to rely on the mainframe as the scalable, reliable, and strategic platform to support commerce with customers and partners. In addition, a large amount of complex business data remains on the mainframe because of compliance, security, and manageability, and that wealth of data and information needs to be exposed as critical runtime services in the hybrid cloud environment. Therefore, it's important that IBM Z be viewed as a strategic element of the overall cloud strategy.

In this chapter, you explore the approach needed to bring IBM Z forward as an integral platform to support a hybrid cloud computing environment. As a key player, IBM Z enables you to successfully move to application modernization through integration with application programming interfaces (APIs), highly distributed data, Agile/DevOps practices, and cloud-native software and services to discover and prepare traditional applications for a cloud future. In addition, we discuss how automation and artificial intelligence (AI) are helping organizations streamline their development and operations processes. By adding intelligence to your operational platform, your teams are able to focus on innovation and customer success instead of routine tasks.

Leveraging APIs

Well-designed APIs can transform the way organizations use core application services to create innovation to support changing customer needs. While APIs have existed for decades, the ability to provide a standard set of APIs means that organizations can successfully manage their hybrid cloud environment in new and innovative ways. In fact, the standardization of APIs is transforming the landscape of the hybrid cloud. APIs are instrumental to the process of modernizing applications based on a cloud native approach.

Representational State Transfer (REST) APIs are the de facto standard for creating mobile and cloud applications. These same APIs are a core element of the IBM Z platform. With the extension of REST to the mainframe, cloud developers can leverage critical business data and transactions, making IBM Z a focal point of the hybrid cloud environment. A service called z/OS Connect Enterprise Edition enables developers to expose IBM CICS, IBM Db2, IBM IMS data and applications, or Virtual Storage Access Method (VSAM) data as APIs with open standards and little Z subsystem knowledge.

IBM's API management solution accomplishes four goals: creating, running, managing, and securing the APIs. The main function of IBM API Connect is to manage the life cycle of APIs — those created internally and those used through a subscription model. API management enables developers to reuse existing assets to create new applications and link existing services together to launch new products and services that generate revenue.


TIP

To be successful, you must be able to manage the life cycle of APIs. API management services can be used to enforce security policy and to provide integration guidelines and testing of API services across mobile, web, clouds, and the mainframe. The use of consistent and predictable APIs can enable the business to rapidly monetize its application logic and its customer data.

Why Application Modernization?

With the addition of standards-based APIs, connectivity services, and application modernization, the mainframe can become a pragmatic platform to support enterprise scalability. This is

especially important for organizations that use the IBM Z platform as the central focus for managing business transactions. Typically, these organizations store decades' worth of data that provides historical context and access to customer trends and patterns.

The mainframe has been transformed through the support of containers and modern data integration services. Therefore, the scalability, performance, and security of the platform means that the value of the mainframe from a security and manageability perspective can become the focus of many hybrid cloud requirements. Because the mainframe is a data hub, data analytics can be executed at the source of the data instead of forcing the business to move data, which could introduce latency that impacts customers. The introduction of common APIs between the mainframe and a multi-cloud system is paramount in creating a seamless computing environment.

REMEMBER

The requirement to modernize existing enterprise applications is fundamental to making the transition to the hybrid cloud. The goal of modernization is the ability to deliver high-quality innovative software on demand as the business needs to change. One of the key challenges is to modernize IBM Z applications that are core to business continuity. One of the most pragmatic approaches to modernization is to leverage cloud-native microservices and a container-based approach to unlock the value of core application services running on IBM Z. A microservices approach allows you to leverage your existing investments in software while improving the ability to create new innovative customer centric applications and services. Adopting a DevOps culture is table stakes to bringing IBM Z into your modern hybrid cloud.

As you transform your enterprise applications environment to take advantage of the hybrid cloud approach, you need a well-designed strategy and plan. You can achieve value through adopting DevOps practices by implementing automation, CI/CD, and improved testing using market leading tools like Jenkins and VScode and Eclipse Che. In addition, by leveraging granular reusable services, you can decide where to host those services based on the needs of that workload.

For example, you may want to move some of these services to Linux on Z and run them in containers on Red Hat OpenShift with architecturally agnostic design patterns. This design pattern allows you to run these services anywhere. In addition, you may

decide to co-locate services on Linux on Z to minimize latency by keeping core applications running on Z/OS.


TIP

The benefit of leveraging OpenShift on Z Linux is that you have a trusted and consistent enterprise-grade management platform and a control plane that supports both your Z enterprise and your X86 environment as well as a variety of public cloud platforms. This approach enables your organization to exploit event-driven architectures to successfully integrate Z into your enterprise's end-to-end hybrid environment running Apache Kafka as a management platform on IBM with Linux, IBM Z, and LinuxONE.

Seeing Operational Intelligence in Action

As you begin to modernize your applications and data, you also need to rethink the way you manage systems. You can't assume that your business will have the financial and technical resources to know all the nuances of each element of the hybrid environment so it can be managed in a predictable manner. Automation is the key to keeping your systems operational. Data comes from a variety of disparate systems, including transactional management systems on the mainframe, data from business applications, cloud environments, and machine-generated log data. By leveraging Red Hat Ansible Automation Platform on z/OS as part of your operations automation strategy, you can gain control over every part of your enterprise. While simple automation can assist with routine tasks, automation infused with machine learning and AI help operations teams accelerate complex troubleshooting and spot anomalies before they become problems — shifting your operations team to a proactive stance.

Applying machine learning and predictive algorithms

Advanced analytics and machine learning algorithms make it possible to search for the hidden patterns in this complex data to determine if improvements in IT performance will enhance the customer experience. This begins by having a baseline understanding of what's expected and required for performance of a system. What is the service level demanded by the organization? When you incorporate data and processes from the mainframe and various cloud services, does the data from logs indicate that

services are performing as required? Are there anomalies that indicate there is a problem?

Each underlying system in your environment produces a massive amount of data about the health and operations of a software and hardware environment. This operations data is generated by numerous systems spanning mainframes, virtual servers, cloud environments, storage devices, networking devices, and various sensors. However, machine data is rarely used because there's simply too much information to easily gain actionable insights.

Combining this data can provide context so it can be used to take the best action to improve performance. The only way to effectively understand all your operations data is to apply machine learning and predictive algorithms. Through operational intelligence, the system is able to continuously monitor the behavior of the hybrid cloud.

REMEMBER

The best solutions are those that can bring together data from many different sources. Machine-learning-based models can be used to analyze and correlate data to understand what has happened, what may happen, and how to remedy a situation. For example, if there is a problem with a system or a network outage, the analytics model has been trained to identify the issue and suggest a correction or automatically implement corrective actions.

Operational intelligence on IBM Z

Organizations with deep expertise on the IBM Z platform have a number of tools that can help monitor and manage the overall performance of the hybrid computing environment. These operational intelligence capabilities include

- Easy insight into the health, availability, and performance management in near real time and historical metrics of your entire Z system
- Access to the wide variety of IBM Z operational data by streaming it in near real time to multiple analytics platforms
- Insight into IBM Z operational data across multiple analytics platforms that includes IBM zAware, which detects and diagnoses anomalies in IBM Z operational messages
- Visibility into transactions that span various IBM Z subsystems in multiple APM solutions

Integrating Z into Enterprise AIOps

IBM Cloud Pak for Watson AIOps enables customers to accelerate incident management, diagnosis, and resolution by using AI, natural language processing, and other advanced technologies. Watson AIOps address the core functions and capabilities critical to an AIOps solution, particularly in its ability to identify anomalies across data silos. IBM's solution also includes a series of connections to a variety of data sources and techniques to manage AI model training, empowering organizations to understand and refine their AI models.

REMEMBER

Adopting an AIOps platform is not a one-time event. Instead, it requires an iterative process that ensures that data and AI/ML models are always up-to-date. The availability of AIOps is especially important in a hybrid computing environment that incorporates IBM Z into a highly distributed computing environment, including both public and private clouds as well as hosted services.

IN THIS CHAPTER

- Understanding the value of DevOps
- Integrating IBM Z with DevOps processes
- Managing DevOps in a hybrid cloud environment

Chapter 5
Tying DevOps to Hybrid Cloud with IBM Z

An effective DevOps strategy and execution plan is the linchpin for hybrid cloud development. A DevOps strategy tied to the hybrid cloud is the price of entry to creating a world class implementation for digital transformation. These DevOps services help organizations build faster solutions with a high and effective quality of service. A hybrid cloud approach empowers the development organization with the agility needed to create new innovative applications. DevOps solutions in the cloud help businesses use the right platform with a common set of tools to support business outcomes.

IBM Z provides a cloud native experience that enables all the key constituents ranging from architects, developers, and administrators to adapt to a modern DevOps approach without having to learn IBM Z–specific programming skills. For developers with z/OS skills and for organizations with z/OS applications, IBM has created a cloud-native experience. The benefit of z/OS is that it's designed to execute enterprise transactions. This ensures that IBM Z can be a core element of your multicloud strategy. With the availability of Red Hat OpenShift on IBM Z, the team can develop and deploy new applications and services leveraging open-source tools and Kubernetes containerization. By combining the

scalability, reliability, and security of the IBM Z platform with the portability and agility of containers and Kubernetes, you get a powerful approach to support the industrial cloud for enterprises. The combined strengths enable your organization to build and maintain applications across platforms, including cloud.

In this chapter, we discuss how the need for a hybrid-cloud application environment has transformed the cloud-native developer experience.

Driving Agility with DevOps

To meet the increasing expectations of customers, businesses need to move quickly and adopt agile processes. This need to deliver new applications and high-quality software releases has led to the adoption of DevOps practices. The growth of visual development methodologies, automated code generation, and microservices based approaches are helping organizations deliver more value. These agile processes and methodology changes resulting from digital transformation and the cloud impact how applications are developed, deployed, secured, managed, and changed. Recent advances in cloud-native applications development supported by containers and microservices are good examples of how the cloud is forcing new ways to create applications.

In the world of a highly distributed hybrid cloud environment, DevOps has to produce software that's continuously updated and managed. To be successful, application developers need to be able to create new code quickly so new application services are designed and deployed to meet changing customer expectations. It is no longer feasible to have a development team write an application in isolation from those who test them, those who will deploy the application, and the business units responsible for driving success from the application.

REMEMBER

The goal of DevOps is to reduce the time from idea to delivery across the company. When you're moving to enterprise DevOps, what matters is how quickly your team can go from an idea to putting an application into the customers' hands. With a properly executed DevOps culture, companies can cut down the lead time and process time to provide value. Continuous delivery (CD) has to be executed in context with the business value for your company.

Creating a Seamless DevOps Environment

Changing business demands, coupled with new technologies, such as the cloud designed to meet them, have created an environment in which continuous innovation and speed to market have become critical success metrics. Performing well against these metrics requires a continuous development and integration process. The bottom line is that software development, deployment, and test can no longer be viewed as separate entities. Instead, they're integrated process steps with smooth transitions between them.

DevOps is all about meeting customers' increasing expectations by delivering high-quality software in a continuous manner. The three desired outcomes of a DevOps practice are as follows:

- The acceleration of innovation, enabled through collaborative dedication to an integrated approach to the software development life cycle
- The continuous delivery of innovation via the automation of software delivery processes and greater development quality, efficiency, and productivity
- The use of user and customer feedback as a mechanism to optimize software innovation

In an era of cloud infrastructure, software must be continuously modified based on changing customer needs and threats from emerging born-on-the-web solutions providers. To compete, processes must be standardized, consistent, and repeatable. This is especially important when a business is using a variety of public, private, and data center resources to operate a software environment. Applying agile software development techniques to make DevOps development processes more robust, and design thinking as a means to focus development efforts on solving actual problems, can greatly enhance the effectiveness of DevOps efforts.

Seeing DevOps in the World of Mainframes

As a business necessity, the new world of IT must be focused on Continuous Integration and Continuous Delivery (CI/CD) of applications. You may assume that mainframes don't represent an appropriate environment for creating, deploying, and managing modern applications. After all, the perception that public clouds and "commodity systems" are the platforms of choice pervade many data center conversations these days. Making this assumption about the mainframe would mistakenly ignore some important facts about enterprises and mainframes:

- Despite how the computing market has evolved over several decades, mainframes are still playing an important role within corporate data centers. Many critical applications still run on the mainframe, and valuable data is stored on the mainframe.
- Although customers have the perception that they must move to the cloud to gain flexibility and scalability, mainframes like IBM Z are a reliable option for hosting a variety of business applications. Linux on IBM Z provides you with the DevOps capabilities available on any platform but with the added security only available on the mainframe. Mainframes have a tested record of reliability, performance, and security. In several ways, mainframes address some of the concerns organizations have about sending their workloads and data outside the walls of their data centers.
- Enterprises run their businesses on applications, and for many, those applications were written on and for mainframes. While many of these applications can integrate with cloud and mobile applications, abandoning them isn't economically realistic (or necessary) from the perspective of cost and disruption to the business.

  IBM has several development tools that take the complexity out of monolithic application refactoring and allow businesses to leverage their incumbency and maintain competitive advantage in their industry.


TIP

One of the benefits of mainframe applications is that they incorporate complex business rules and logic that are difficult to design

from scratch. Emerging companies are at a disadvantage in trying to replicate this same level of sophistication.

Successful organizations are moving to more modern tools and approaches when deploying new mainframe capabilities. This new generation of tools enables the teams to move faster to support cloud-native development. The DevOps approach to application development is relevant to both of these application types, but for many organizations, the greatest challenge exists in the cloud enablement of existing mainframe applications. Modernizing these applications requires affordable DevOps methodologies and tools. This new generation of tools helps in a number of ways:

- Leveraging the same DevOps tools and techniques that are used elsewhere in the company
- Achieving the speed and quality that your business needs
- Building additional functions by using Java and other modern languages, such as Swift, Python, Go, and Node.js
- Incorporating usability features and modern programming techniques that make developers more efficient
- Supporting CD that enables the timely delivery of new code and services without relying on release schedules
- Migrating from host library software configuration management to modern parallel development tools
- Easing the migration from old compilers to new ones as seamlessly as possible

Additional requirements for creating a successful enterprise DevOps strategy include

- Analysis tools that provide the ability to efficiently analyze data flows and "where-used" information, program-control flows, source-code complexity, application inventories, batch-control flows, application logic change impacts, and other characteristics of enterprise applications
- Risk assessment capabilities that can identify performance and resource issues throughout the development life cycle as well as access and utilize usage and transaction data to anticipate potential production failures

- Automated testing at every level to identify issues as early as possible in the life cycle — including unit testing all the way through performance tests
- Automated application delivery that supports application performance analysis for improving online transaction and batch turnaround times

Ideally, these tools should offer visualization that makes it easy for developers to see and understand the analyses they need.

REMEMBER

As is the case with any DevOps effort, teams must share and support a common culture that facilitates a smooth integration with, and transition among, all the steps of the development life cycle. In many cases, operations staff may share the same tools as the development teams in order to facilitate these transitions. A successful DevOps effort should be based on a continuous process improvement that's facilitated by a well-defined methodology.

Putting DevOps into Practice

DevOps is about cultural change. Many successful businesses are implementing DevOps throughout their IT infrastructures — in cloud, distributed, and mainframe environments. Matching cloud services models with the scalability, reliability, and security of the mainframe can help optimize agility.

The need for CI

Making frequent software updates to quickly respond to changing customer needs and shifting market dynamics is a drastic difference from waterfall development, where there are typically one or two major product version releases a year. This new approach to software delivery created the need for continuous software improvement, meaning small enhancements are made across each step of the software delivery life cycle to incrementally deliver better software more frequently. This change gets new functionality into the hands of users more quickly and also reduces the risk inherent in "big bang" releases.

CI and CD have enabled successful development organizations to quickly iterate on software and release frequent updates. CI helps businesses engage in continuous software improvement by

having developers commit code more frequently. CD is the practice of keeping software in a release-ready state at all times. CI/CD requires automation to assure quality, security, and smoother deployments across the software delivery life cycle. This approach gives businesses the ability to push reliable new software updates more frequently.

Automating testing

For a robust software development life cycle, test code as early as possible in the DevOps process. By incorporating automation throughout the DevOps process, teams can shift left and identify potential problems early in the development cycle. With traditional development, the approach has been a step-by-step progression where each team hands off its work to the next team in the process. On the other hand, a shift-left approach is designed to identify and prevent potential problems as early in the process as possible. Automated testing includes unit testing, application integration testing, systems integration testing, functional testing, and user and performance testing. This testing cycle provides developers the self-service access to spinning up and destroying test environments to remove delays.


TIP

A shift-left strategy requires cross-team collaboration along with technology tools that can support the strategy. A platform with automation built into its core is critical — these systems can help facilitate the continuous testing as code progresses through the DevOps pipeline (see the later section "Creating a DevOps Pipeline" for more information).

Cloud-native development

As the cloud matures and becomes more sophisticated, it has evolved to support the way cloud applications are defined. Cloud-native applications are software offerings designed with microservices, containers, and dynamic orchestration as well as CD of software. Every part of the cloud-native application can be housed within its own container and dynamically orchestrated with other containers to optimize the way resources are utilized.

Cloud computing requires the infrastructure to be in place to support the needs of CI/CD. To be successful, developers need some advanced capabilities including debugging, unit testing, automated build solutions, and the ability to discover reusable

services and providing the organization with the ability to scale on demand. By providing integrated development environments (IDEs) — Eclipse, VS Code, or Eclipse Che — developers can be more productive while eliminating the risks associated with unsupported tools.

Creating a DevOps Pipeline

DevOps teams must be on board with sharing a common culture focused on smooth transitions across life cycle steps — from design to development to production, and across platforms. DevOps should be a fully integrated cycle or pipeline. The DevOps pipeline helps you bring people together with these practices instead of creating new silos. *Note:* Within the pipeline there are small loops; for example, after testing, a project can go to the release phase or revert to coding for additional improvements. In addition, the entire process is a cycle, so as code is put into production, teams manage and analyze it and then provide continuous updates based on feedback.

REMEMBER

Automation is built in throughout the DevOps pipeline to increase efficiency, decrease errors, and enhance collaboration across teams. In addition, DevOps teams can use their preferred tools within each step of the pipeline. The parts of the DevOps pipeline are as follows:

- **Code:** A parallel development and code repository that makes it easy for teams to collaborate in a secure, integrated environment that's highly scalable.
- **Build:** Build automation that allows teams to build and manage projects as they progress. This helps continuously make code integrated and ready to deploy more quickly.
- **Provision and deploy:** Automate the provisioning, delivery, and management of the entire IT stack through configuration automation and deployment tools.
- **Test:** The days of testing only after development finishes are over. Testing earlier in, and throughout, the development life cycle means that errors are detected earlier, which makes them easier to find, diagnose, and fix.

- **Release:** Manage the continuous release of interdependent applications, infrastructure changes, and the simultaneous deployments of multiple applications in a fully managed way.
- **Monitor:** By continually monitoring application performance throughout development, you can make sure applications are ready for production deployment.
- **Plan:** Use collaboration tools and roadmaps to facilitate teamwork and organize a team's workflow and terminology.
- **Analyze:** By applying rapid analysis to code to understand dependencies and relationships, it's easier to maintain and develop new code without deep Z skills.

Many of the steps in the DevOps on IBM Z pipeline have bidirectional arrows. These arrows, shown in Figure 5-1 in the DevOps pipeline, indicate that teams can pass code back and forth to improve it as it progresses through the pipeline. Fundamental to a successful pipeline is collaboration between all the teams involved in the software delivery process.

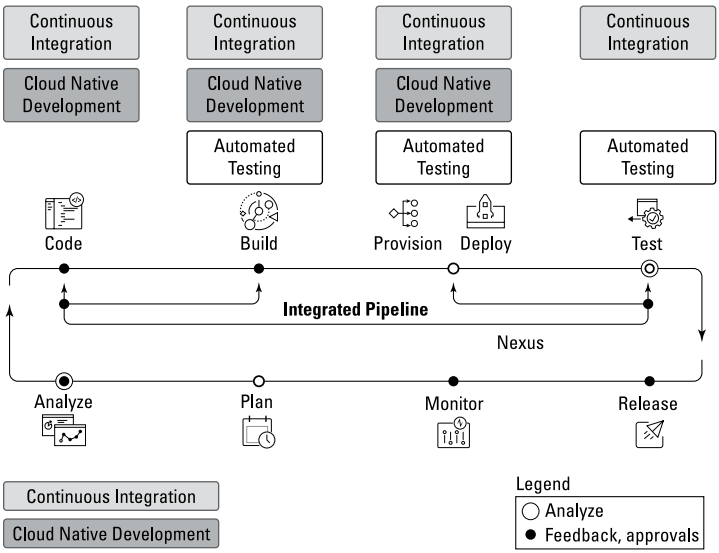

FIGURE 5-1: The DevOps pipeline on IBM Z.

CD MEANS RESPONSIVENESS

Some people have the misconception that adopting DevOps and CD means that staff will be continually putting code into production in an unplanned way that could be disruptive to the business. Instead, DevOps and CD mean that you're continuously delivering to a platform that may be delivered to a staging environment before it's ready for production. In a complex commercial environment, it's not always easy to know the optimal time to put new code into production. For example, there may be extenuating circumstances where a job must execute in full before new code is added. It may be better to select an evening with lower transaction volume. Clearly, you need to be careful on timing and processes for transactional systems. You don't want to change the functionality of the transactional system midday, or you may impact the final calculations. In this staging scenario, you're still continuously deploying and then staging until the appropriate time to implement the update.

DevOps frameworks

REMEMBER

DevOps is a culture that needs to be adopted across the entire business — not just a set of developer tools. As you make the transition to a DevOps culture, frameworks can help create consistent structures for applications. By using a framework, there can be dramatic improvements across the application delivery life cycle.

A variety of services can be incorporated into a DevOps development framework. For instance, developers use configuration management services to keep track of versions, changes, and code modules created during the software development life cycle. This configuration management information is stored in an online repository so all developers can share it.

The process by which an application is built involves writing, compiling, running, and testing code. In a DevOps environment, developers produce many code modules, each with its own set of dependencies. A DevOps framework should also therefore incorporate build services that support all these steps.

DevOps and the cloud

DevOps is changing dramatically with the advent of cloud computing. For example, mobile and web applications are often updated multiple times a week. Increasingly, emerging born-on-the-web businesses are able to innovate in near real time. Customers expect businesses to listen to their feedback and improve applications based on comments. Incumbent business leaders can't rest on their achievements; they must continue to innovate. However, at the same time, the business needs to provide the level of security and scalability required for complex services such as transaction management.

If you apply a consistent approach to DevOps practices, you can create a culture of continual improvement no matter what platform you're working with. The same best practices are effective across mobile apps, cloud services, and the mainframe. Therefore, think about a continuum of DevOps where you have common APIs, development tools, security services, and operational management across all your deployment platforms.


TIP

Because of this common set of services across deployment models, organizations can move workloads to the optimal platform. For example, some workloads that require sophisticated security, reliability, and scalability will determine that these workloads should be managed on the mainframe.

OPEN SOURCE AT THE CORE

Increasingly, businesses are adopting open source to protect their businesses from change. For more than three decades, open source has been a foundational capability of IBM Z. The foundation of open source on the mainframe means that open-source DevOps tools are native to the mainframe. Therefore, the mainframe can take advantage of modern languages that are typically used in other deployment models. You can easily think about the mainframe as a secure and predictable deployment model based on open-source capabilities.

Recognizing the Value of IBM Z as a Cloud-Native Platform

As organizations begin to leverage IBM Z as a cloud-native development platform, they're in a position to leverage core applications and assets in a modern way. Traditional IBM Z-based applications are the bedrock of many businesses. These applications often incorporate important business processes and rules that are fundamental to business operations.

WARNING

However, the code behind these applications was all written before modern coding standards and are therefore challenging to maintain or modernize. In addition, these legacy applications lack well-designed APIs that support integration with other services and other data sources.

The solution to bringing core IBM Z assets into a modern application hybrid cloud world is through a set of services. This section covers how DevOps tools offered on IBM Z can help make the platform an important part of your hybrid cloud strategy.

IBM Z cloud-native development

Flexibility is important in an era where businesses need to be agile and continually meet rising customer expectations. The hybrid cloud gives organizations the ability to quickly experiment, try new technologies, and spin up proofs of concept without lengthy IT provisioning processes. Likewise, developers need flexible tools. Software delivery on z/OS requires a new generation of skills and tools that aren't tied to an IBM Z-only environment. Many of the existing developers with deep knowledge of the Z platform are retiring. The new generations of developers demand cloud-native, graphical, and easy-to-use tools to support the entire DevOps life cycle. These developers require that testing can shift left to reduce delivery costs. DevOps for IBM Z brings together a comprehensive set of open enterprise-wide industry standard tools and processes to ensure the smooth adoption and migration to the hybrid cloud. This approach helps make the Z platform approachable to developers with a variety of skills and backgrounds.

TIP

An optimal way to approach the need for modernization with the IBM Z platform is to take advantage of IBM Cloud Paks. The benefit of this software abstraction layer is that IBM Z can become the high-end hybrid cloud platform. For more details on IBM Cloud Paks, check out Chapter 2.

Modernizing IBM Z applications

If your organization depends on complex mainframe-based applications that were written decades ago, it's understandable that there are risks if these applications aren't updated carefully. However, organizations have little choice if they're going to be able to digitally transform their software to meet changing business needs. Typically, the application's code is built with complex dependencies and business processes that aren't well understood or documented. To address these needs, IBM offers a series of solutions to address moving legacy applications into cloud-native services. These tools are intended to provide agility and speed of software delivery on z/OS without special Z skills. It provides development and testing environments to improve productivity and shift testing left to reduce delivery costs.

Bring your own IDE

One of the benefits of adopting cloud-native development on IBM Z is the choice that developers have to use their favorite. This capability, brought to market with IBM Wazi Developer for Red Hat CodeReady Workspace, saves time and money by leveraging the experience of developers and making them productive without deep Z skills. Cloud-native development is about *how* your applications are developed, not *where* they are deployed.

The need for rapid analysis

In order to make code changes rapidly, safely, and predictably, while maintaining quality, developers need to understand the impact of their changes to the overall application. You can't maintain or modernize what you don't understand. For years, organizations have had to depend on the vast knowledge of their experienced developers, but this has left them exposed as those developers switch jobs or retire.

IBM provides an analytical platform called Application Discovery and Delivery Intelligence (ADDI). ADDI enables transformation of existing applications to modernize applications. ADDI helps scan all your programs and the technology dependencies, such as databases and third-party applications, that surround the programs. The platform applies AI algorithms to analyze a mainframe application in order to discover dependencies and the impact of changing a service on the operation of the computing platform. ADDI provides a number of core analysis and visualization tools, including data flow and where-used analysis, program control flow analysis, source code complexity analysis, and impact analysis. These tools can identify which programs are critical to the business and which services are no longer being used by the business and can be deprecated to optimize efficiency.

For cloud-native developers working on smaller projects, a feature of ADDI called Wazi Analyze delivers a containerized rapid analysis capability with a graphics web-based user interface. It runs in a docker environment on the developer's machine with either a graphical or table view and visualizes the relationship between application components, data, and jobs. It analyzes applications that use custom abstraction layers to manage access to data or calls between programs. For example, it can understand the relationship between COBOL application components to analyze the impact of making changes and accelerates the tasks of migrating to a modern SCM or version of COBOL.

With modern tools, such as ADDI, that analyze code and discover dependencies, you can refactor code so it can be modernized and evolve into a set of services that can become well-architected APIs. ADDI can also, where appropriate, leverage IBM z/OS Connect Enterprise Edition to expose and connect cloud services with mainframe data and transactions.

Data services

IBM provides tools that make the connection between mainframe and cloud data services seamless. For example, z/OS Connect Enterprise Edition gives non-mainframe experts access to mainframe data. In addition, for mainframe Linux on Z customers, developers get access to mainframe data through Representational State Transfer (REST)-ful APIs. These standard APIs allow developers with no mainframe background to create web and mobile applications that can call and write to the mainframe.

IN THIS CHAPTER

- Creating a cloud strategy
- Strategizing your hybrid cloud
- Building the Z Cloud foundation

Chapter 6
Getting Started with Your Hybrid Cloud Strategy

Increasingly, large enterprises are adopting a hybrid cloud strategy that incorporates a variety of platforms based on business requirements. Many of these organizations rely on the IBM Z platform based on the need to support high-volume and secure transactions. IBM Z platform fits well into a hybrid computing environment because of its resilience and performance and its support of Red Hat OpenShift. The mainframe has been transformed into a more flexible platform that supports the movement to enterprise security, containers, and microservices. These systems of record are an integral part of the IT fabric for the business. In a cloud scenario, they can maintain their traditional roles and uses, be part of a private cloud delivering services to internal and external stakeholders, or serve as the on premises side of a hybrid cloud. The end result should encompass the best capabilities of both mainframe and cloud environments.

A Cloud Strategy for the Enterprise

As IBM Z evolves to become an integral element in the enterprise cloud, it has to support a hybrid computing model. This level of integration and interoperability is the essence of the value of IBM Z. The benefit of IBM Z is the fact that it's designed to support the combination of systems of record and systems of engagement (including public cloud services and software as a service applications). IT must move beyond application silos and become adept at building and deploying new functionality as shared business services. To support customer goals, assets will no longer stand alone. Therefore, to support customers, the process begins with the creation of a cloud strategy with IBM Z in the mix.


TIP

Create a security fabric framework that works in the potentially more complex environment of the cloud. IBM Z provides a level of security and governance that meets the stringent requirements of business management along with regulatory requirements. Your security evaluation should include an in-depth understanding of how participants in your hybrid cloud strategy maintain the level of security needed to protect your company.

Planning Your Hybrid Cloud Strategy

You can't take any shortcuts in planning your cloud strategy. In the age of the hybrid cloud, you have to look across all the services and platforms as a unified approach. To ensure your success, follow these five best practices:

- **Carefully assess requirements and limitations.** Businesses and IT must work closely together to determine what's actually needed from the cloud. Carefully plan your hybrid cloud strategy and understand how it helps the business overcome current challenges and meet increasing customer demands. Some of the questions you want to ask include
  - Do the applications currently in use to support the business meet the need, and are they well-managed?
  - What new services are needed?
  - How do your IT and business people need to be educated on the technical and usage aspects of a cloud solution?

- What financial constraints exist?
- Are you able to transform aging applications into a set of containerized services that prepare your company for a more agile future?

- **Choose the right cloud deployment models.** Many businesses select IBM Z to keep more of their business-critical workloads on premises. However, at the same time they selectively use outside public or virtual private clouds to manage other workloads. In addition to security, management, and functional concerns, costs and the mix of capital expenses versus operational expenses may have a strong influence on this decision.
- **Determine the best workload and data localities.** Data and application locality have never been more important. Because many options exist for where to deploy applications and store data, organizations need to consider a variety of factors such as performance, security, costs, and applicable regulations. When analyzing enterprise applications, many organizations quickly realize that it's critical for security and manageability to leave these applications on IBM Z because it's often difficult to make the business case for re-architecting these applications later. Businesses are transforming their mainframes into hybrid cloud application programming interface (API) hosts, modernizing applications on the mainframe, and offering them as API services for cloud consumption. After the mainframe application APIs are hosted in an API management portal, they appear like any other cloud service. Businesses choose IBM Z as an API host because APIs scale, are highly available, and have the throughput necessary to meet end-user expectations.

  While some applications may move to the cloud as part of a larger digital transformation effort, many new and existing core business applications reside on or require connections to IBM Z. To bring these applications closer to new development efforts, organizations are creating software-defined clouds on the mainframe. Rather than bringing the mainframe applications to the cloud, they're bringing the cloud, DevOps, and modern mobile and web applications to IBM Z.

REMEMBER

Data locality is particularly important given the large quantities, and varied types, of data used by businesses today. IT must be able to manage the location and synchronization across the cloud wherever it is needed and used.

Data locality can also depend on maintaining proximity to where the data and compute cycles are needed — an "edge" approach to cloud — which then requires a well-planned and executed approach to data synchronization and overall data management.

- **Understand and manage service levels, configurations, and licenses.** A cloud environment — particularly a hybrid one — makes the management of service level agreements (SLAs), configurations, and licenses more complex. Your team must understand how service levels are handled across the cloud environment — which may include internal policies as well as those of public cloud providers or partners. Configurations and licensing complexity add to the mix of challenges.
- **Make governance a priority.** Trying to replicate your well-planned on premises governance structure on the cloud can be difficult because of time, budget, and the way that the public cloud is architected. Addressing this complexity requires close collaboration across internal IT, your organization's line-of-business (LoB) stakeholders, cloud providers, and government entities. The result should be a governance framework that can ensure data and transaction integrity and protection.

Building the Z Cloud Foundation

Your IBM Z platform doesn't live in isolation. It is, and should be, only a part of an overall digital transformation effort as a manifestation of IT as an agent of change. Siloed business functions and IT assets must give way to a holistic approach to leveraging the cloud, along with existing platforms, technologies, and assets, to make IT more effective in supporting business goals. In this new way of conducting business, customers, partners, and suppliers collaborate with you, and among themselves to make conducting business smoother and more integrated.

The hybrid cloud can be an important enabler to achieving this transformation by making IT assets more accessible and useful to all stakeholders. If done correctly, a move to the cloud can yield significant financial and organizational benefits over time.

Accelerate digital transformation

Creating a hybrid cloud strategy is critical for enterprises that need both on premises and public cloud services. Your enterprise has a fiduciary responsibility to protect its intellectual property. To thrive, businesses need to have an approach that secures data and applications no matter where they reside. The IBM Z platform provides security at every layer of the computing infrastructure. In this book, you explore IBM Z's critical role in the secure hybrid cloud.

Inside...

- Digitally transform with a hybrid cloud strategy
- See IBM Z's role in the hybrid cloud
- Proactively respond to ITOps challenges
- Discover DevSecOps in the hybrid cloud
- Build customer trust with secure cloud

Judith Hurwitz, President, Hurwitz & Associates, is a consultant, thought leader, and coauthor of ten books, including Cognitive Computing and Big Data Analytics. **Daniel Kirsch,** Managing Director, Hurwitz & Associates, is a consultant and coauthor of three books in the areas of cloud, AI, and security.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-73549-6
Part #: 54017854USEN-01
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.